IBM Tivoli Monitoring
Version 6.3

Guía del administrador

SC22-5446-00

IBM Tivoli Monitoring
Version 6.3

Guía del administrador

SC22-5446-00

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 627.

Esta edición se aplica a la versión 6, release 3 de IBM Tivoli Monitoring (número de producto 5724-C04) y a todos los releases y modificaciones posteriores mientras no se indique lo contrario en nuevas ediciones.

© Copyright IBM Corporation 2005, 2013.

Contenido

Figuras ix

Tablas xi

Acerca de esta información xiii

Capítulo 1. Introducción 1
Novedades de este release 1
Novedades de la versión 6.3 1
Familia de productos de IBM Tivoli Monitoring . . 5
Componentes de Tivoli Management Services . . . 5
Cliente de Tivoli Enterprise Portal 8
Clientes de escritorio, navegador y Java Web Start 8
Recopilación de datos históricos 9
Tareas de administrador del sistema 10
Proveedor de servicios de Performance Monitoring 10

Capítulo 2. Preparación del entorno de Tivoli Enterprise Portal 13
Cliente de navegador 13
Versiones de Java Runtime Environment (JRE) . . 13
Primer inicio de sesión 14
Valores de seguridad de Internet Explorer . . . 14
Privilegios de grabación y supresión de Windows 15
Adición del logotipo y del URL de empresa . . 15
Inicio del cliente de Tivoli Enterprise Portal . . . 16
Utilización de Web Start para descargar y ejecutar el cliente de escritorio 16
Instalación de IBM JRE 17
Habilitación del rastreo para JRE 18
Descarga y ejecución del cliente de escritorio . . 19
Creación manual de un atajo para el cliente de Web Start 20
Inicio del cliente de navegador en otro servidor de portal 21
Inicio del cliente de navegador en otro servidor de portal. 22
Especificación del navegador utilizado para iniciar aplicación y para ayuda en línea 23
Adición de plataformas operativas a la vista de Navigator 25

Capítulo 3. Preparación de su entorno de panel de control 27
Hojas de ruta 27
Configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario 27
Configuración de un entorno de panel de control de supervisión con inicio de sesión único y con controles de autorización por usuario. 32
Migración de un entorno de panel de control de supervisión básico a un entorno de panel de control con inicio de sesión único y controles de autorización por usuario 45
Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring . . 52
Creación de páginas de panel de control personalizadas que muestran datos de supervisión . 55
Control de las importaciones de UISolutions . . . 58

Capítulo 4. Edición de los valores de configuración del entorno 61
Valores de configuración del cliente de Tivoli Enterprise Portal. 61
Edición de parámetros del cliente 61
Lista de parámetros del cliente de portal . . . 62
Habilitación del servidor proxy HTTP 69
Establecimiento de las propiedades de aplicación para sistemas Linux y UNIX. 70
Establecimiento de la variable de entorno cuando el concentrador está en un sistema z/OS . . . 71
Valores de configuración del servidor de Tivoli Enterprise Portal. 72
Edición del archivo de entorno del servidor de portal 72
Variables de entorno del servidor de portal. . . 73
Poda de sucesos en la base de datos del servidor de portal 75
Control del tamaño de adjuntos de sucesos. . . 76
Control del número de intentos de inicio de sesión 77
Valores de configuración del servidor de Tivoli Enterprise Monitoring 78
Edición del archivo de entorno del servidor de supervisión 78
Proceso duper para optimizar situaciones . . . 79
Valores de configuración de Tivoli Enterprise Monitoring Automation Server 80
Edición del Tivoli Enterprise Monitoring Automation Server 81

Capítulo 5. Habilitación de la autenticación de usuarios 83
Autenticación de usuarios a través del servidor de supervisión concentrador. 86
Requisitos previos para configurar la autenticación en el servidor de supervisión concentrador 86
Procedimiento de configuración 89
Información sobre ldapsearch para LDAP . . . 91
Autenticación de usuarios LDAP a través del servidor de portal 94
Requisitos previos para configurar la autenticación LDAP en el servidor de portal . . 95
Acerca del inicio de sesión único 98

© Copyright IBM Corp. 2005, 2013

Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único 100
Utilización de Manage Tivoli Enterprise Monitoring Services para configurar el servidor de portal para la autenticación de LDAP . . . 104
Utilización de la línea de mandatos de Linux o UNIX para configurar el servidor de portal para la autenticación LDAP 108
Utilización de la consola de administración de TEPS/e 110
Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP 118
Reconfiguración del cliente de navegador para SSO 120
Importación y exportación de claves de LTPA 120
Gestión de usuarios LDAP nuevos 123
Inhabilitación de la autenticación de LDAP en el servidor de portal 123
Migración de la autenticación LDAP del servidor de supervisión al servidor de portal 124
Autenticación a través del Tivoli Enterprise Monitoring Automation Server 126
Autenticación de usuarios de LDAP mediante Microsoft Active Directory 127
Antes de comenzar 128
Descripción general de la Hoja de ruta 132
Planificación y creación de usuarios del servidor de portal dentro de Active Directory 133
Creación y configuración de cuentas y permisos de usuarios del servidor de portal, si se desea . 133
Habilitación y configuración de la autenticación de usuarios de LDAP para el servidor de portal, si se desea 134
Configuración de TEPS/e para TLS/SSL, si es necesario 141
Habilitación y configuración de la autenticación de usuarios de LDAP para el servidor de supervisión, si se desea 142
Herramientas de verificación de LDAP de Active Directory 144
Casos de usuarios 146

Capítulo 6. Utilización de la autorización de usuario de Tivoli Enterprise Portal 163

Administrar usuarios 164
Usuarios y grupos de usuarios 165
Permisos 165
Aplicaciones 169
vistas de Navigator 170
Miembro de y Miembros 171
Gestión de los ID de usuario 171
Añadir ID de usuario 171
Visualización y edición de un ID de usuario . . 172
Eliminar un ID de usuario 174
Usuario predeterminado 174
Gestión de grupos de usuarios 175
Visualización de los miembros de un grupo de usuarios 175
Adición de un grupo de usuarios 176
Revisión y edición de un grupo de usuarios . . 177
Eliminación de un grupo de usuarios 178
Notas sobre la administración de usuarios 178
Resolución de mensajes de error de inicio de sesión 182

Capítulo 7. Utilización de políticas de autorización basadas en roles 185

Conceptos sobre la política de autorización . . . 186
Roles y permisos predefinidos 189
Preparación para habilitar las políticas de autorización 190
Escenarios de gestión de políticas 192
Prácticas recomendadas para crear políticas de autorización 192
Creación y asignación de roles de administrador 194
Creación y asignación de roles de distribuidor de políticas 195
Ejemplos de gestión de políticas 196
Habilitación de políticas de autorización en el servidor de portal 199
Auditoría de la política de autorización 204
Cambio de las propiedades de configuración del Servidor de políticas de autorización después de la instalación y la configuración 204
Gestión del almacén de políticas de autorización 207
Utilización de varios dominios 207
Escenarios de despliegue 208
Creación de políticas para dominios específicos de IBM Tivoli Monitoring 210

Capítulo 8. Protección de las comunicaciones 215

Configuración de la comunicación TLS/SSL entre el servidor de supervisión concentrador y el servidor LDAP 218
Configuración de la comunicación TLS/SSL entre Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos . . 219
Utilización de certificados firmados de entidad emisora de certificados de terceros para el servidor de portal 219
Configuración de la comunicación TLS/SSL para el servidor Dashboard Application Services Hub 222
Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización 223
Utilización de los certificados generados por WebSphere para configurar TLS/SSL para el Servidor de políticas de autorización 224
Utilización de certificados de terceros para configurar TLS/SSL para el Servidor de políticas de autorización 225
Configuración de la CLI tivcmd para TLS/SSL 227
Configuración de la comunicación TLS/SSL entre el servidor de portal y el Servidor de políticas de autorización 229
Habilitación de FIPS para IBM Tivoli Monitoring 230

Importación de los certificados de TEPS/e a la base de datos de archivos de claves del servidor de portal 235
Utilización de la interfaz de línea de mandatos de GSKit para trabajar con bases de datos de claves y certificado 236
Utilización del programa de utilidad GSKit iKeyman para trabajar con bases de datos de claves y certificados 237
Configuración de JRE para GSKit e inicio del gestor de claves 238
Creación de una nueva base de datos de claves 238
Creación de un nuevo par de claves privada-pública y de una solicitud de certificado 239
Utilización de un certificado autofirmado temporal 240
Recepción del certificado firmado por la entidad emisora de certificados 240
Cómo guardar la contraseña en un archivo stash 241

Capítulo 9. Registro de auditoría . . . 243
Elementos XML del registro de auditoría correlacionados con el grupo de atributos de auditoría de ITM 245
Ejemplo de XML de registro de auditoría 249
Variables de entorno de auditoría 251
Actuación y registro de auditoría de la ejecución del mandato. 253

Capítulo 10. Integración de sucesos de situación con Tivoli Enterprise Console. 255
Correlación predeterminada de sucesos de situación con sucesos de IBM Tivoli Enterprise Console 255
Expansión de una descripción de situación de mensaje de suceso genérica. 257
Correlación genérica para ranuras específicas de agente. 258
Asignación de gravedad para sucesos de Tivoli Enterprise Console 259
Localización de ranuras de mensaje 259
Estatus de suceso de situación y generación de sucesos de IBM Tivoli Enterprise Console . . . 260
Sincronización de sucesos de situación 262
Comprobación de la memoria caché de sucesos de IBM Tivoli Enterprise Console. 263
Cambio de la configuración de la sincronización de sucesos en el servidor de sucesos. 264
Definición de servidores de supervisión adicionales para la sincronización de sucesos en el servidor de sucesos 264
Cierre de sucesos muestreados 265
Cambio de parámetros de conjunto de reglas para el archivo de conjunto de reglas omegamon.rls . . 265
Consideraciones para el ajuste. 267
Utilización del programa de utilidad de comprobación de reglas 267
Edición de la configuración de Recurso de integración de sucesos 268
Especificación del reenvío de EIF para un suceso de situación 272
Personalización del mensaje de suceso 274
Actualización del XML utilizado por el Servicio de atributos MCS 275
Visualización de sucesos desde Universal Agent en Tivoli Enterprise Console 278
Utilización de la consola de NetView a través del visor de sucesos de IBM Tivoli Enterprise Console . 279

Capítulo 11. Integración de sucesos de situación con Tivoli Netcool/OMNIbus. 281

Capítulo 12. Configuración de conectores para la consola de sucesos comunes 283
Ventana Configuración de la Consola de sucesos comunes 283
Separador Conector ITM 284
Separador Conector TEC 284
Separador Conector OMNIbus. 286
Separador Nombres de las columnas adicionales 288
Prácticas recomendadas para utilizar la sincronización de sucesos 289
Resolución de problemas con la conexión al servidor de Tivoli Enterprise Console en sistemas Linux 290

Capítulo 13. Mantenimiento de agentes de supervisión 291
Tareas de agente en Tivoli Enterprise Portal . . . 291
Adición de un agente mediante Tivoli Enterprise Portal 291
Configuración de un agente mediante Tivoli Enterprise Portal 292
Inicio, detención y reciclaje de un agente mediante Tivoli Enterprise Portal. 293
Actualización de un agente mediante Tivoli Enterprise Portal 294
Eliminación de un agente mediante Tivoli Enterprise Portal 295
Actualización de un agente mediante la interfaz de línea de mandatos. 296
Borrado de la tabla Estatus de despliegue 297
Cambio del servidor de supervisión con el que se conecta un agente 299
Agentes de supervisión de autodescripción . . . 300
Flujo de sucesos de autodescripción en el servidor de supervisión 304
Instalación del agente de autodescripción . . . 306
Suspensión de la función de autodescripción 312
Renovación automática e inicialización de autodescripción. 312
Habilitación o inhabilitación de la función de autodescripción en el servidor de supervisión . 315
Habilitación o inhabilitación de la función de autodescripción en el agente 316

Determinación de si los agentes están habilitados para la autodescripción 317
Variables de entorno que controlan la función de autodescripción 319

Capítulo 14. Servicios de gestión de agentes 321
Características de Tivoli Agent Management Services 321
Instalación y configuración de Tivoli Agent Management Services 323
Supervisión de la disponibilidad de los agentes 327
Gestión manual del agente 328

Capítulo 15. Autonomía del agente 331
Funciones autónomas. 331
Variables de entorno para comportamiento autónomo 335
Limitaciones de las situaciones 342
Archivos XML codificados en UTF-8. 345
Configuración de los Servicios de gestión de agentes en agentes de Tivoli System Monitor . . . 346
Situaciones privadas 347
Operación de situaciones privadas 348
Especificación XML de situaciones privadas . . 351
Especificación XML de situaciones de empresa exportadas 360
Ejemplos de situaciones privadas. 365
Historial privado 370
Especificación XML de alteración temporal de situación de empresa 373
Alertas SNMP 378
Configuración de alertas de SNMP 378
Especificación XML del elemento Trap 380
Emisiones del agente y de alertas MIB para SNMP 390
Configuración de OMNIbus para SNMP . . . 390
Sucesos de EIF 396
Configuración de sucesos de EIF 396
Especificación XML de correlación de sucesos de EIF 399
Especificación XML de configuración de destinos de sucesos de EIF 405
Ranuras comunes para sucesos emitidos de EIF 407
Suceso de ciclo de vida de EIF 409
Suceso de latido de EIF 410
Suceso de restablecimiento maestro 411
Envío de sucesos de situación privada utilizando la comunicación TLS/SSL 412
Interfaz de servicio del agente. 416
Inicio de la interfaz de servicio del agente. . . 416
Perfil de grupo de autorización de acceso . . . 417
Interfaz de servicio del agente - Información de agente. 422
Interfaz de servicio del agente - Situaciones . . 424
Interfaz de servicio del agente - Historial . . . 425
Interfaz de servicio del agente - Consultas. . . 426
Interfaz de servicio del agente - Solicitud de interfaz de servicio 427

Capítulo 16. configuración centralizada 447
Visión general de la configuración centralizada . . 447
Diseño de la configuración centralizada 448
Especificación XML de la lista de carga de configuración 452
Sustitución de palabras clave en la lista de carga de configuración 459
Variables de entorno de la lista de carga de configuración 460
Arranque del lista de carga de configuración 462
Variables de entorno para la configuración centralizada 462
Habilitación del cifrado de contraseña en los archivos de configuración en z/OS 466
Configuración de muestra de configuración centralizada 467
Arranque de la configuración centralizada. . . . 471
Iniciación de la configuración centralizada con variables de entorno del agente 471
Iniciación de la configuración centralizada con un archivo de lista de carga 474
Iniciación de la configuración centralizada con una solicitud de interfaz de servicio 477
Autonomía de agente en z/OS 479

Capítulo 17. Gestión de datos históricos 481
Acerca de la recopilación de datos históricos . . . 481
Configuración de la recopilación de datos históricos. 484
Cambio del directorio de archivos históricos a corto plazo 488
Impacto de rendimiento de las solicitudes de datos históricos. 489
Impacto de grandes cantidades de datos históricos en el servidor o agente de supervisión 489
Solicitudes de datos históricos de tablas grandes 490
Planificación del almacenamiento de datos históricos. 490
Utilización de una despensa de datos para mejorar consultas largas o complejas 491
Configuración de historial a corto plazo de Tivoli Data Warehouse 493
Migraciones de particiones por rangos de Tivoli Data Warehouse 496
Migración de tablas no particionadas a tablas particionadas para DB2 en Linux, UNIX y Windows. 497
Migración de tablas no particionadas a tablas particionadas para DB2 en z/OS 500
Migración de tablas no particionadas a tablas particionadas para Oracle 504
Configuración del resumen y poda 507
Acerca del Summarization and Pruning agent 507
Prácticas recomendadas para resumen y poda 510
Disponibilidad de los datos de resumen y poda 512
Configuración del resumen y poda para los grupos de atributos 513
Cambio de los valores de configuración globales 514

Cómo inhabilitar el Summarization and Pruning agent 517
Registro de errores para datos almacenados . . . 518
Recopilación del historial de registro de operaciones de agente 518
Proceso de conversión para utilizar archivos planos delimitados 520
Estimación de espacio necesario para contener tablas de datos históricos 521
Limitación del crecimiento de archivos históricos a corto plazo 522
Qué hacer cuando el directorio de archivos históricos a corto plazo alcanza su límite . . . 523
Conversión de archivos de historial a corto plazo en archivos planos delimitados 523
Conversión de archivos utilizando el programa krarloff 523
Conversión de archivos de historial en archivos planos delimitados en sistemas Windows . . . 526
Conversión de archivos de historial en archivos planos delimitados en sistemas IBM i 527
Conversión de archivos de historial en archivos planos delimitados en sistemas UNIX 529
Conversión de archivos de historial en archivos planos delimitados en sistemas HP NonStop Kernel 530
Conversión de archivos de historial en archivos planos delimitados en sistemas z/OS 532

Capítulo 18. Tivoli Common Reporting 537
Visión general de la Tivoli Common Reporting . . 537
Requisitos previos para Tivoli Common Reporting 538
Actualización desde una versión anterior 539
Limitaciones. 540
Asegurarse de que se han habilitado los informes históricos. 541
Creación y mantenimiento de las tablas de dimensiones. 542
Utilización del Summarization and Pruning agent para mantener las tablas de dimensiones . 543
Creación y mantenimiento manual de las tablas de dimensiones. 547
Importación de informes mediante el instalador de informes 553
Importación y ejecución de informes IBM Cognos 556
Ejecución de una exploración de requisitos previos 556
Conexión a Tivoli Data Warehouse utilizando el cliente de base de datos mediante ODBC . . . 557
Importación de informes a través de Dashboard Application Services Hub 558
Creación de un informe de Dashboard Application Services Hub 559
Importación y ejecución de informes BIRT. 560
Importar un paquete de informes BIRT. 560
Configurar el origen de datos 561
Generar un informe BIRT de ejemplo 562

Capítulo 19. Réplica de la base de datos del Tivoli Enterprise Portal Server 565
Visión general de la base de datos del Tivoli Enterprise Portal Server 565
Ejecución del script de migración-exportación . . 566
Ejecución del script de migración-importación . . 567
Ejecución del script de migración-importación desde Windows de origen a Windows de destino 568
Ejecución del script de migración-importación desde Windows de origen a Linux o UNIX de destino 568
Ejecución del script de migración-importación desde Linux o UNIX de origen a Windows de destino 569
Ejecución del script de migración-importación desde Linux o UNIX de origen a Linux o UNIX de destino 570

Apéndice A. IBM Tivoli Monitoring Web Services para el servidor SOAP . 573
Acerca del cliente SOAP. 573
Configuración de Tivoli Monitoring Web Services (servidor SOAP) 573
Definición de concentradores 574
Añadir usuarios 575
Configuración de IBM Tivoli Monitoring Web Services (SOAP Server) en sistemas UNIX y Linux 576
Ajuste del rendimiento de transacción SOAP en sistemas AIX 577
Habilitación de la seguridad SOAP 577
Utilización de IBM Tivoli Monitoring Web Services 578
ID de usuario 579
Inicio del cliente SOAP y realización de una solicitud 579
Uso del navegador 579
Utilización del programa de utilidad de línea de mandatos de cliente SOAP (kshsoap) 580
Emisión de solicitudes SOAP como mandatos de sistema 581
Métodos de SOAP. 582
Emisión de solicitudes SOAP de segundo nivel 591
Solicitud CT_Get de SOAP de ejemplo 593
Casos de ejemplo de IBM Tivoli Monitoring Web Services 594
Generación de resúmenes y gráficos de operaciones lógicas diarias 594
Obtención de instantáneas de datos y de tabla y gráficos fuera de línea 594
Envío de alertas a una plataforma de IBM Tivoli Monitoring 595
Creación de automatización colaboradora utilizando SA IO 596
Reconocimiento de un suceso en una plataforma de IBM Tivoli Monitoring 597
Contenido de informe 597

Apéndice B. Habilitación del servicio web de representación gráfica de IBM Tivoli Monitoring 599

Apéndice C. Utilización de Tivoli Management Services Discovery Library Adapter 601
Dependencia del agente de sistema operativo . . 603
Filtrado de direcciones de red privadas. 604

Apéndice D. Utilización de z/OS Tivoli Management Services Discovery Library Adapter 607

Apéndice E. Descripciones de sucesos del agente SNMP de MIB . . 611

Apéndice F. Registro de operaciones del agente. 617

Biblioteca de documentación 619
Biblioteca de IBM Tivoli Monitoring. 619
Documentación para los agentes base 620
Publicaciones relacionadas 621
Otras fuentes de información 621

Información de soporte 623

Avisos 627

Índice. 631

Figuras

1. Jerarquía de usuarios de LDAP sugerida para servidores de Tivoli Monitoring 129
2. Propiedades de usuario del servidor de portal 130
3. Propiedades de usuario de LDAP. 131
4. Permisos de usuario del Tivoli Enterprise Portal Server. 132
5. Acepte estos valores predeterminados 135
6. Configure el repositorio 136
7. Adición de la entrada base al territorio 139
8. Guarde la actualización de la configuración de TEPS/e 139
9. Mensaje de error de configuración de TEPS/e 140
10. Pantalla Administrar usuarios de Tivoli Enterprise Portal 140
11. Panel de configuración de LDAP para usuarios del servidor de supervisión. 143
12. Resultados de la consulta de LDP. 145
13. Listado de usuarios de Active Directory 148
14. Propiedades de un usuario de Tivoli Monitoring individual 149
15. Ventana de ldapbrowser 150
16. Parámetros de LDAP del servidor de supervisión 151
17. Resultados de ldapsearch para ID de servidor de supervisión 152
18. El separador del cuaderno Configuración de Integrated Solutions Console 155
19. La pantalla Gestionar repositorios de Integrated Solutions Console 156
20. La pantalla Propiedades generales de Integrated Solutions Console 156
21. La pantalla de verificación de Integrated Solutions Console 157
22. El separador del cuaderno Configuración de Integrated Solutions Console 158
23. El separador Configuración de Integrated Solutions Console 158
24. La pantalla Referencia de repositorio de Integrated Solutions Console 159
25. La pantalla de verificación de Integrated Solutions Console 159
26. La pantalla de repositorios de Integrated Solutions Console del territorio 160
27. La pantalla de verificación de Integrated Solutions Console 160
28. La pantalla de inicio de sesión de Integrated Solutions Console 160
29. La pantalla inicial de Integrated Solutions Console 161
30. Interacciones de los componentes de los Servicios de gestión de agentes con componentes de IBM Tivoli Monitoring. . . . 322
31. Gráfico y tabla de instantánea de datos 595
32. Tabla de instantáneas de datos. 595
33. Consola de Mensaje universal que muestra los mensajes recibidos. 596
34. Detalles de registro de mensajes 596
35. Conexiones entre productos para el servicio web de representación gráfica 600

© Copyright IBM Corp. 2005, 2013

Tablas

1. Hoja de ruta para la configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario 28
2. Tareas adicionales necesarias para la configuración del entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario 30
3. Hoja de ruta para configurar un entorno de paneles de control de supervisión con inicio de sesión único y controles de autorización por usuario 35
4. Tareas adicionales necesarias para la configuración del entorno de supervisión avanzado con inicio de sesión único y con controles de autorización por usuario 42
5. Hoja de ruta para migrar a un entorno de paneles de control avanzado 46
6. Códigos de idioma y entorno local 68
7. Ubicaciones de archivo para cambiar propiedades de aplicación para sistemas UNIX y Linux 70
8. Hoja de ruta para la autenticación de usuarios 86
9. Tareas a seguir antes de configurar la autenticación 86
10. Parámetros de configuración de LDAP . . . 88
11. Parámetros TLS/SSL para la comunicación entre el concentrador y el servidor LDAP . . 89
12. Opciones de línea de mandatos de ldapsearch y parámetros de configuración correspondientes del servidor de supervisión . 92
13. Parámetros de configuración de LDAP . . . 96
14. Parámetros de SSO 98
15. Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único 101
16. Tipos de recursos de política de autorización y sus permisos y elementos soportados . . . 187
17. Permisos de RoleAdministrator 189
18. Permisos de PolicyDistributor 189
19. Permisos LinuxOperator, UNIXOperator y WindowsOperator 190
20. Permisos VCenterOperator 190
21. Información de configuración para el Servidor de políticas de autorización 201
22. Varios dominios con roles y requisitos de despliegue de políticas compartidos 209
23. Tareas para asegurar la comunicación 217
24. Hoja de ruta para configurar TLS/SSL para el proveedor de datos de panel de instrumentos. 219
25. Hoja de ruta para configurar TLS/SSL para el Servidor de políticas de autorización. . . . 224
26. Atributos de clase de suceso de IBM Tivoli Enterprise Console 256
27. Caracteres especiales para grupos y nombres de atributos de sucesos IBM Tivoli Enterprise Console generados a partir de sucesos de situación reenviados. 259
28. Correlación entre sufijos de nombres de situaciones y gravedad de sucesos de Tivoli Enterprise Console 259
29. Disponibilidad de funciones de fórmula de situación cuando un agente de empresa está conectado o desconectado y cuando la situación es privada. 343
30. Especificación XML del elemento TrapDest 381
31. Especificación XML del elemento TrapAttrGroup 384
32. Especificación XML del elemento Situation 385
33. Condiciones de excepción de estatus de ciclo de vida del agente 387
34. Especificación XML del elemento StatTrap 388
35. Conjunto de ranuras comunes para sucesos de EIF emitidos 408
36. Sucesos de ciclo de vida de EIF 409
37. Valores de ranura de clase ITM_StatEvent de suceso de ciclo de vida de EIF 410
38. Contenido del suceso de restablecimiento maestro 411
39. Permisos del grupo de autorización de acceso para los mandatos de la interfaz de servicio . 418
40. Interfaz de servicio del agente - Listado de atributos de muestra de consultas. 427
41. Interfaz de servicio del agente - Informe de muestra de consultas 427
42. Solicitud <AGENTINFO> de la Interfaz de servicio del agente 427
43. Salida de la solicitud <AGENTINFO> de la Interfaz de servicio del agente 428
44. Solicitud <LISTSUBNODE> de la Interfaz de servicio del agente 429
45. Salida de la solicitud <LISTSUBNODE> de la Interfaz de servicio del agente 429
46. Solicitud <ATTRLIST> de la Interfaz de servicio del agente 429
47. Salida de la solicitud <ATTRLIST> de la Interfaz de servicio del agente 430
48. Solicitud <READATTR> de la Interfaz de servicio del agente 430
49. Salida de la solicitud <READATTR> de la Interfaz de servicio del agente 431
50. Solicitud <REPORT> de la Interfaz de servicio del agente 432
51. Salida de la solicitud <REPORT> de la Interfaz de servicio del agente 433
52. Solicitud <TABLESIT> de la Interfaz de servicio del agente 436
53. Salida de la solicitud <TABLESIT> de la Interfaz de servicio del agente 437

© Copyright IBM Corp. 2005, 2013

54. Solicitud <PVTCONTROL> de la Interfaz de servicio del agente 438
55. Salida de la solicitud <PVTCONTROL> de la Interfaz de servicio del agente 438
56. Solicitud <SITSUMMARY> de la Interfaz de servicio del agente 438
57. Salida de la solicitud <SITSUMMARY> de la Interfaz de servicio del agente 439
58. Solicitud <AGENTSTAT> de la Interfaz de servicio del agente 440
59. Salida de la solicitud <AGENTSTAT> de la Interfaz de servicio del agente 440
60. Solicitud <HISTREAD> de la Interfaz de servicio del agente 442
61. Salida de la solicitud <HISTREAD> de la Interfaz de servicio del agente 442
62. Elemento <ConfigFile> de la lista de carga de configuración y opciones de activación disponibles para el tipo Disp. 459
63. Funciones de resumen 509
64. Parámetros para el programa de acumulación krarloff 525
65. Nombres DD necesarios 534
66. Parámetros de KPDXTRA 534
67. Campos TCP/IP en diálogo de especificación de concentrador. 574
68. Campos SNA en el diálogo de especificación de concentrador. 575
69. Variables de condición de excepción de SNMP para agentStatusEvent 611
70. Variables de condición de excepción de SNMP para agentSitSampledEvent 612
71. Variables de condición de excepción de SNMP para agentSitPureEvent 614

Acerca de esta información

El manual *IBM®Tivoli Monitoring: Guía del administrador* describe la administración de la infraestructura de IBM Tivoli Monitoring, Tivoli Management Services.

Los temas de los capítulos cubren las tareas siguientes:

- Configurar, personalizar y mantener los clientes y el servidor de Tivoli Enterprise Portal
- Configurar el cifrado asimétrico mediante archivos de claves públicas y privadas
- Habilitar la autenticación de usuario en el registro del servidor de supervisión concentrador o un registro LDAP externo
- Mantener ID de usuario y grupos de usuarios en Tivoli Enterprise Portal
- Integrar las actividades de sucesos de situación entre el servidor de sucesos IBM Tivoli Enterprise Console o la Netcool/OMNIbus Probe for Tivoli EIF y el servidor de supervisión concentrador
- Configurar conectores para los sistemas de sucesos que envían información de sucesos a Tivoli Enterprise Portal
- Utilizar Tivoli Enterprise Portal para mantener agentes que soportan la característica de despliegue de agente remoto
- Configurar los agentes de Tivoli Enterprise Monitoring para un funcionamiento autónomo
- Configurar y habilitar la configuración centralizada
- Gestionar la recopilación de datos históricos y Tivoli Data Warehouse
- Importar informes para Tivoli Common Reporting que son exclusivos de los productos que se ejecutan en Tivoli Enterprise Portal y utilizan Tivoli Data Warehouse como el origen de los datos históricos para generar informes. Esta información va dirigida al administrador que configura Tivoli Common Reporting e instala los paquetes de informes.
- Replicar la base de datos del Tivoli Enterprise Portal Server en otro sistema o conservarla como copia de seguridad
- Utilizar los métodos SOAP de IBM Tivoli Monitoring Web Services para consultar y controlar el entorno supervisado

Los usuarios de esta publicación deben estar familiarizados con los conceptos de supervisión de rendimiento y con la administración. Si utiliza Tivoli Data Warehouse, debe estar familiarizado con el sistema operativo que aloja el almacén. Para obtener más información sobre esta familia de productos, consulte Tivoli solutions for Service Availability and Performance Management.

© Copyright IBM Corp. 2005, 2013

Capítulo 1. Introducción

En este capítulo se revisan las nuevas características y las mejoras realizadas en la interfaz de Tivoli Enterprise Portal y las características administrativas de Tivoli Management Services y, a continuación, se muestra una lista de las tareas administrativas que puede realizar.

Para obtener información sobre cómo utilizar las características de la Versión 6.3 de Tivoli Enterprise Portal, consulte la ayuda integrada (Ayuda → Contenido e índice) o el manual *Tivoli Enterprise Portal: Guía del usuario*.

Novedades de este release

Revise las últimas mejoras de los componentes de Tivoli Enterprise Portal y de Tivoli Management Services que sean relevantes para la *IBM Tivoli Monitoring: Guía del administrador*.

Novedades de la versión 6.3

Las siguientes mejoras en los componentes de Tivoli Management Services afectan al administrador del sistema en la versión 6.3.

Jazz for Service Management

Jazz for Service Management reúne a las especificaciones abiertas de la comunidad de Open Services for Lifecycle Collaboration (OSLC) para el enlace de datos, servicios administrativos compartidos, servicios de creación de informes y panel de control. A través de estas facetas, Jazz for Service Management acelera el despliegue, la integración y la automatización del flujo de trabajo entre herramientas de IBM, partners y terceros. Jazz for Service Management se incluye con IBM Tivoli Monitoring.

Jazz for Service Management tiene varios servicios de integración: Administración, Registro, IBM Tivoli Common Reporting, Seguridad e IBM Dashboard Application Services Hub. Estos servicios de integración proporcionan características clave, incluidas:

- Repositorio de datos compartidos para productos integrados a través de Jazz for Service Management.
- Experiencia de IU coherente a través de Dashboard Application Services Hub en Jazz for Service Management.
- Administración simplificada de integración de productos y soluciones a través de Jazz for Service Management.
- Ad hoc, creación de informes de autoservicio a través de Tivoli Common Reporting en Jazz for Service Management.

Para obtener más información acerca de Jazz para Service Management, vaya a Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html).

El proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring para recuperar datos de supervisión para visualizarlos en paneles de control de IBM Dashboard Application Services Hub

El proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring

© Copyright IBM Corp. 2005, 2013

recupera datos del agente de supervisión para visualizarlos en el componente de IBM Dashboard Application Services Hub de Jazz for Service Management. El proveedor de datos de panel de instrumentos se instala de forma opcional durante la configuración del Tivoli Enterprise Portal Server. Con el proveedor de datos de panel de instrumentos habilitado, los usuarios de Dashboard Application Services Hub pueden recuperar datos de sólo lectura del servidor de supervisión concentrador y del agente de supervisión para su visualización en los paneles de instrumentos proporcionados por los agentes o en paneles de instrumentos personalizados. IBM Tivoli Monitoring V6.3 incluye al Infrastructure Management Dashboards for Servers que muestra datos para los agentes de SO. Estos paneles de control de servidor utilizan a proveedor de datos de panel de instrumentos para recuperar datos. Se debe configurar una conexión al proveedor de datos de panel de instrumentos en Dashboard Application Services Hub. Consulte Capítulo 3, “Preparación de su entorno de panel de control”, en la página 27 y “Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring” en la página 52.

IBM Infrastructure Management Dashboards for Servers en ejecución en Dashboard Application Services Hub V3.1 o posterior

Con el proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring habilitado, los usuarios de Dashboard Application Services Hub pueden recuperar grupos y sucesos de sistemas gestionados para todos los agentes de supervisión y las métricas de salud del agente de sistema operativo Linux, el agente de sistema operativo UNIX y el agente de sistema operativo Windows utilizando la aplicación Infrastructure Management Dashboards for Servers. Esta aplicación se instala y configura en Dashboard Application Services Hub V3.1 o posterior utilizando IBM Installation Manager. Para obtener más información, consulte “Instalación y configuración de IBM Infrastructure Management Dashboards for Servers” en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Proveedor de servicios de Open Services Lifecycle Collaboration Performance Monitoring

El componente Tivoli Enterprise Monitoring Automation Server contiene el proveedor de servicios de Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) y está instalado en los mismos sistemas que el Tivoli Enterprise Monitoring Server concentrador. El proveedor de servicios registra recursos de supervisión con el componente Jazz for Service Management Registry Services y da soporte a la integración con otros productos utilizando interfaces de datos enlazados con OSLC. Para obtener más información, consulte “Proveedor de servicios de Performance Monitoring” en la página 10.

Políticas de autorización basadas en roles

La característica Servidor de políticas de autorización de Tivoli proporciona funciones de mayor control de acceso que lo que es posible con el modelo de autorización existente de Tivoli Enterprise Portal Server. Puede proteger los recursos del acceso no autorizado por parte de los usuarios de paneles de control de supervisión en IBM Dashboard Application Services Hub. IBM Tivoli Monitoring V6.3 con la característica Servidor de políticas de autorización habilitada proporciona las funciones siguientes:

- La posibilidad de restringir el acceso para los usuarios de panel de control a grupos de sistemas gestionados específicos y a sistemas gestionados individuales.

- La posibilidad de asignar políticas basadas en roles a usuarios y grupos de usuarios en un registro de usuarios de LDAP federado para simplificar la gestión de políticas.
- Una interfaz de línea de mandatos nueva que es muy automatizable.
- Gestión central de políticas de autorización para varios entornos de IBM Tivoli Monitoring, también denominados dominios.

Para implementar la característica, debe instalar paquetes de IBM Installation Manager para el Servidor de políticas de autorización de Tivoli y la Interfaz de línea de mandatos tivcmd para la política de autorización. El Servidor de políticas de autorización se instala con Dashboard Application Services Hub y la CLI tivcmd se instala en los sistemas utilizados por los administradores que crearán políticas de autorización. Tras la instalación satisfactoria de estos dos paquetes, puede ejecutar varios mandatos CLI según sea necesario para crear roles, otorgar permisos, excluir permisos, etc. Para obtener información sobre cómo trabajar con políticas, consulte Capítulo 7, "Utilización de políticas de autorización basadas en roles", en la página 185.

Informe Explorador de requisitos previos de informes de agentes de SO
El informe Explorador de requisitos previos de informes de agentes de SO que se entrega e instala mediante el paquete de informes del agente de SO se puede utilizar para comprobar si los requisitos previos de IBM Tivoli Monitoring del sistema están configurados correctamente para utilizar Tivoli Common Reporting sin errores. Consulte el apartado "Ejecución de una exploración de requisitos previos" en la página 556.

Creación y mantenimiento de las tablas de dimensión necesarias para Tivoli Common Reporting utilizando el Summarization and Pruning agent
Ya no necesita ejecutar periódicamente Tivoli Common Reporting ni los scripts de agente de SO para mantener el esquema IBM_TRAM y llenar la tabla MANAGEDSYSTEM. Puede configurar el Summarization and Pruning agent para crear, llenar y mantener las tablas de dimensiones. Consulte el apartado "Creación y mantenimiento de las tablas de dimensiones" en la página 542.

Particionamiento por rangos de Tivoli Data Warehouse
El particionamiento por rangos es una característica de organización de datos de base de datos que puede mejorar considerablemente el rendimiento de consulta y poda en bases de datos grandes de Tivoli Data Warehouse. Puede migrar las tablas existentes a una tabla particionada para beneficiarse de las mejoras de rendimiento proporcionadas con tablas particionadas. El particionamiento por rangos permite a la base de datos limitar el ámbito de las consultas cuando la columna que forma parte de la clave de particionamiento se utiliza en la cláusula WHERE. Consulte el apartado "Migraciones de particiones por rangos de Tivoli Data Warehouse" en la página 496.

Auditoría de la identidad de actuación
Ahora puede auditar los mandatos que se ejecutan en un sistema en el nivel de agente. El ID de usuario del originador y la información de red se transfieren de forma segura al agente y, a continuación, se registran en el registro de auditoría del agente. El registro de auditoría puede recopilarse históricamente. Puede crear situaciones y supervisar centralmente desde Tivoli Enterprise Portal. Consulte el apartado "Actuación y registro de auditoría de la ejecución del mandato" en la página 253.

Controles de autorización AAGP

La infraestructura de autorizaciones de Perfil de grupo de autorización de acceso (AAGP) se integra ahora con la auditoría de identidad de actuación. Las políticas de AAGP permiten ahora de forma selectiva a usuarios específicos ejecutar actuaciones de Tivoli Enterprise Portal o utilizando **tacmd executeaction**, ejecutar mandatos utilizando **tacmd executecommand** o crear y modificar situaciones y políticas de flujo de trabajo que especifique un mandato de actuación. La política de AAGP ya no necesita el servidor de configuración central para entregar la política de AAGP. La política se puede configurar desde la interfaz de servicio del agente y almacenar localmente en el propio agente. Consulte "Perfil de grupo de autorización de acceso" en la página 417 y Capítulo 16, "configuración centralizada", en la página 447.

Mejoras de la seguridad SOAP

Ahora puede habilitar la seguridad para las solicitudes CT_EMail y CT_Export utilizando la variable de entorno SOAP_IS_SECURE en el servidor de supervisión. Consulte el apartado "Habilitación de la seguridad SOAP" en la página 577.

Optimización del proceso duper

El proceso duper ahora da soporte a situaciones que contienen acciones reflejas o elementos de visualización. Consulte el apartado "Proceso duper para optimizar situaciones" en la página 79.

Cambios en el comportamiento predeterminado del agente de autodescripción y nuevos mandatos tacmd

Ahora puede especificar qué productos y versiones el proceso automático del agente de autodescripción instala en el servidor de supervisión y el servidor de portal. Consulte el apartado "Agentes de supervisión de autodescripción" en la página 300 y el apartado "Actualización dinámica de las opciones de instalación de autodescripción" en la página 311.

Actualizaciones para situaciones privadas

- Función de predicado *REGEX

  IBM Tivoli Monitoring con frecuencia requiere exploración de texto y coincidencia de patrón en los datos de ejemplo y sucesos, como nombre, dirección, mensaje y registro. Puede añadir el filtro de predicado de Expresión regular a situaciones privadas para mejorar la detección de sucesos de supervisión del agente.
- Supresión dinámica de una situación privada

  Ahora puede utilizar el atributo DELETE= en una situación privada para eliminar dinámicamente una situación privada sin reiniciar el agente o suprimir el archivo XML de situación privada local.

Para obtener más información, consulte "Especificación XML de situaciones privadas" en la página 351.

Capacidad de borrar las transacciones de la tabla Estatus de despliegue

Cada vez que emite un mandato **tacmd** de IBM Tivoli Monitoring o utiliza el navegador de Tivoli Enterprise Portal para gestionar de forma remota un Tivoli Enterprise Monitoring Agent, la información sobre la transacción se conserva en la tabla Estatus de despliegue del Tivoli Enterprise Monitoring Server. Para facilitar la gestión del contenido de esta tabla, especialmente en entornos grandes, puede planificar la eliminación periódica de transacciones completadas desde la tabla. Consulte el apartado "Borrado de la tabla Estatus de despliegue" en la página 297.

Uso de scripts daemon de inicio de sesión disponibles en IBM Service Management Connect

En IBM Tivoli Monitoring V6.3 o posterior, los servidores de supervisión pueden ahora utilizar la solución de daemon de inicio de sesión de IBM Tivoli Monitoring que está disponible en IBM Service Management Connect para cambiar el servidor de supervisión al que un agente se conecta. Consulte el apartado "Cambio del servidor de supervisión con el que se conecta un agente" en la página 299.

Establecimiento del entorno local para el cliente de navegador

Los administradores ya no puede establecer el entorno local para el cliente del navegador de Tivoli Enterprise Portal en toda la empresa. El idioma puede cambiarse mediante el panel de control de Java™ en el sistema cliente si la plataforma de sistema operativo subyacente se ha instalado utilizando un entorno local distinto del que desea utilizar con Tivoli Enterprise Portal. Consulte los parámetros **user.language** y **user.region** en "Lista de parámetros del cliente de portal" en la página 62.

Cambio de nombre de Tivoli Integrated Portal

Ahora se hace referencia al release V3.1 de Tivoli Integrated Portal como Dashboard Application Services Hub.

Cambio de nombre del agente de i5/OS

El agente de supervisión de i5/OS ahora se conoce como el agente de supervisión de IBM i.

Familia de productos de IBM Tivoli Monitoring

La siguiente información ofrece una breve descripción general de las aplicaciones de la familia de productos IBM Tivoli Monitoring.

Los productos de IBM Tivoli Monitoring le ayudan a gestionar el rendimiento y la disponibilidad de sistemas operativos y aplicaciones distribuidos. Estos productos se basan en un conjunto de componentes de servicio comunes, denominados colectivamente como Tivoli Management Services. Tivoli Management Services proporciona seguridad, transferencia y almacenamiento de datos, mecanismos de notificación, presentación de interfaz de usuario y servicios de comunicaciones en una arquitectura de agente-servidor-cliente. Estos servicios son comunes a muchas suites de productos tales como supervisión de sistema principal IBM Tivoli OMEGAMON XE e IBM Tivoli Composite Application Manager.

Después de haber instalado y configurado inicialmente Tivoli Management Services y los productos que se basan en ellos, consulte esta guía para aplicar una personalización adicional en un entorno distribuido. (*Configuración de Tivoli Enterprise Monitoring Server en z/OS* se proporciona en la guía del mismo nombre.) Ésta también contiene información administrativa general para los sistemas gestionados que comparten estos servicios comunes. La información administrativa específica de producto se proporciona en las guías correspondientes a los productos individuales.

Componentes de Tivoli Management Services

Los siguientes componentes de Tivoli Management Services ofrecen la infraestructura para los agentes de Tivoli Enterprise Monitoring.

Para obtener una lista completa de los componentes, consulte *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm).

Cliente

El cliente de IBM Tivoli Monitoring, Tivoli Enterprise Portal, es una interfaz de usuario basada en Java para ver y supervisar la red de la empresa. En función de cómo se haya instalado, puede iniciar Tivoli Enterprise Portal como una aplicación de escritorio o mediante el navegador como una aplicación web.

Servidor de presentación

El cliente Tivoli Enterprise Portal se conecta al Tivoli Enterprise Portal Server. El Tivoli Enterprise Portal Server es un conjunto de servicios de software para el cliente que permite la recuperación, la manipulación y el análisis de datos de los agentes de supervisión de la empresa.

El Tivoli Enterprise Portal Server también incluye el proveedor de datos de panel de instrumentos opcional que se utiliza para recuperar los datos de supervisión de solo lectura para su visualización en los paneles de control de supervisión.

Servidor de gestión

El Tivoli Enterprise Portal Server se conecta al Tivoli Enterprise Monitoring Server principal o *concentrador*. El servidor de supervisión actúa como una recopilación y un punto de control para las alertas recibidas de los agentes de supervisión de la empresa y recopila datos de rendimiento y disponibilidad de éstos. El servidor de supervisión concentrador correlaciona los datos de supervisión recopilados por los agentes de supervisión y los servidores de supervisión remotos y los pasa al servidor de portal para presentarlos en la consola de portal.

El **servidor de automatización**, Tivoli Enterprise Monitoring Automation Server, es un componente opcional que puede instalarse en el mismo sistema que el servidor de supervisión concentrador. Amplía la funcionalidad del servidor de supervisión concentrador. El servidor de automatización incluye el proveedor de servicios de Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM). Para obtener más información, consulte “Proveedor de servicios de Performance Monitoring” en la página 10.

Servidor de panel de control

IBM Dashboard Application Services Hub es un componente de Jazz for Service Management que proporciona la visualización del panel de control y servicios de informes. Los operadores del panel de control acceden a él a través de una interfaz de navegador web. IBM Dashboard Application Services Hub utiliza el componente de proveedor de datos de panel de instrumentos del servidor de portal para recuperar datos de supervisión.

Puede instalar la **aplicación IBM Infrastructure Management Dashboards for Servers** en Dashboard Application Services Hub para visualizar información de sucesos de situación, grupos de sistemas gestionados y métricas de estado clave para agentes de SO Windows, agentes de SO Linux y agentes de SO UNIX. También puede crear páginas de panel de control personalizadas que muestren datos de supervisión.

También puede instalar **Servidor de políticas de autorización** e **Interfaz de línea de mandatos tivcmd para la política de autorización (tivcmd CLI)** para utilizar políticas de autorización basadas en roles para controlar qué recursos supervisados se visualizan en los paneles de control. Para obtener

más información, consulte Capítulo 7, “Utilización de políticas de autorización basadas en roles”, en la página 185.

Servidor de ayuda
El sistema de ayuda de interfaz de usuario de IBM basado en Eclipse se instala con el servidor de portal y ofrece funciones de presentación y búsqueda para el sistema de ayuda integrado.

Interfaz tacmd de línea de mandatos (CLI tacmd)
La CLI tacmd se utiliza para gestionar el entorno de supervisión y también se puede utilizar para automatizar muchas de las funciones administrativas realizadas utilizando Tivoli Enterprise Portal. Los mandatos de CLI envían solicitudes al servidor de supervisión concentrador o al servidor de portal.

Los agentes
Los agentes de Tivoli Enterprise Monitoring se instalan en los sistemas o subsistemas cuyas aplicaciones y recursos desea supervisar. Un agente recopila los datos de supervisión del *sistema gestionado* y los pasa al servidor de supervisión al que está conectado. El cliente de portal y el servidor de paneles control reúnen los valores actuales de los atributos y produce informes formateados como tablas, gráficos y vistas de topología relacionales basadas en tablas. Los agentes y los servidores de supervisión también pueden probar los valores de los atributos actuales en un umbral. Cuando se excede un umbral o cuando un valor coincide, puede visualizarse un icono de alerta en el cliente de portal o el panel de control de supervisión y el servidor de supervisión concentrador puede reenviar un suceso a un servidor de sucesos como IBM Tivoli Netcool/OMNIbus. Las condiciones del valor de atributo que se deben probar se denominan *situaciones*.

Los agentes de SO se pueden instalar fuera de la empresa como *agentes de Tivoli System Monitor*. No se conectan con el Tivoli Enterprise Monitoring Server ni se basan en el mismo. Pueden ejecutar *situaciones privadas*, que son independientes del servidor de supervisión, guardar muestras de datos para grupos de atributos como *historial privado* y enviar alertas SNMP o sucesos EIF a IBM Tivoli Netcool/OMNIbus.

Almacén de datos
Tivoli Data Warehouse es un componente opcional para almacenar datos históricos recopilados de los agentes en el entorno. El almacén de datos está ubicado en una base de datos soportada (por ejemplo SQL DB2, Oracle o Microsoft SQL).

Registro de usuarios compartido
Un registro de usuarios compartido es un servidor LDAP como Tivoli Directory Server o Microsoft Active Directory que se puede utilizar para autenticar los usuarios del servidor de portal, los usuarios de IBM Dashboard Application Services Hub y otros usuarios de aplicaciones como los usuarios de la GUI web Netcool/OMNIbus. Cuando se utiliza un registro de usuarios compartido, los usuarios se autentican por el primer servidor al que acceden y se pasan señales de autenticación a los otros servidores de forma que el usuario no tiene que volver a especificar sus credenciales.

Sincronización de sucesos
El componente de sincronización de sucesos es opcional. Está configurado para devolver al servidor de supervisión actualizaciones de sucesos de situación que se han reenviado a un servidor de sucesos IBM Tivoli Enterprise Console o a un Netcool/OMNIbus ObjectServer.

Cliente de Tivoli Enterprise Portal

Tivoli Enterprise Portal es una de las interfaces de usuario para los productos basados en IBM Tivoli Monitoring. De mismo modo que utiliza la página de inicio del navegador como punto de partida para navegar en Internet, utilice Tivoli Enterprise Portal para obtener una visión general de alto nivel del entorno de red.

Una sección de la ventana visualiza Navigator, una vista similar a un árbol de la red supervisada, descendiendo desde el nivel superior hasta las agrupaciones individuales de información recopilada por los agentes de supervisión. El resto de la ventana se llena con vistas pertinentes al elemento elegido del árbol de Navigator. Desde el nivel superior o desde el espacio de trabajo de inicio, puede navegar a ubicaciones específicas para comprobar la actividad e investigar problemas.

Este espacio de trabajo se ha personalizado para el elemento de selección del árbol. Este espacio de trabajo se ha diseñado con un diagrama de barras, dos diagramas de trazos y una tabla que visualiza un color de fondo para los valores de celdas que exceden un determinado umbral. Puede crear y personalizar espacios de trabajo adicionales para cada elemento del árbol.

Los indicadores de sucesos que se visualizan en el árbol, o Navigator, son los resultados de las pruebas, denominadas situaciones, que se ejecutan en los sistemas supervisados. Cuando la condición descrita en la situación es verdadera, un icono de color se superpone en los elementos afectados del árbol. Utilice el editor de situaciones para configurar alertas condiciones que supervisen el entorno automáticamente. Utilice el editor de flujo de trabajo para configurar políticas a fin de automatizar el entorno.

Clientes de escritorio, navegador y Java Web Start

El cliente de Tivoli Enterprise Portal se puede desplegar de tres formas, tal como se describe brevemente aquí y más detalladamente en la publicación *Guía de instalación y configuración*.

Escritorio

El cliente de escritorio necesita que se cargue y se ejecute el software de instalación en cada sistema donde se ejecutará el cliente de escritorio. Los usuarios inician Tivoli Enterprise Portal del mismo modo que inician otras aplicaciones instaladas localmente. Con el cliente de escritorio, también puede crear varias instancias para conectarse a diferentes servidores de portal.

Navegador

El software de instalación del cliente de navegador reside en el Tivoli Enterprise Portal Server. El software de cliente se descarga de allí al sistema la primera vez que inicia la sesión en el servidor de portal desde el navegador y, a partir de entonces, sólo cuando hay actualizaciones de software.

Puede iniciar el cliente de navegador desde cualquier sistema habilitado para navegador entrando el URL para el servidor de portal. En esta modalidad de funcionamiento, cada espacio de trabajo de portal tiene un URL, de forma que puede guardar un espacio de trabajo en la lista de Favoritos.

Con el cliente de navegador puede iniciar desde Tivoli Enterprise Portal en otras aplicaciones habilitadas para web y basadas en web de Tivoli y desde dichas aplicaciones en el portal, sin tener que volver a escribir las credenciales de inicio de sesión. Esta solución de inicio de sesión único utiliza un registro de usuarios central basado en LDAP para autenticar las credenciales de inicio de sesión.

Java Web Start

Con Java Web Start, al igual que con el cliente de navegador, se accede al software de cliente mediante un URL y dicho software se descarga desde el servidor de portal. A diferencia del cliente de navegador, que se ejecuta siempre en el navegador, el cliente Web Start se ejecuta como una aplicación de escritorio. Siempre que hay actualizaciones disponibles para el software de cliente, éstas se descargan automáticamente del servidor de portal. En las referencias al comportamiento de *cliente de escritorio* que se hacen en esta guía también se supone el cliente Java Web Start a menos que se indique lo contrario. El inicio de sesión único en un ejemplo; al igual que con el cliente de navegador, puede utilizar el inicio de sesión único con el cliente de Web Start.

Recopilación de datos históricos

Además de los informes en tiempo real ofrecidos por los espacios de trabajo de Tivoli Enterprise Portal, puede configurar la recopilación de datos históricos para que almacene los datos que los agentes de supervisión están recopilando para informes históricos y situaciones. Puede especificar lo siguiente:

- Grupos de atributos para la recopilación de datos históricos
- Intervalo de recopilación de datos.
- Intervalos de almacén de datos si elige grabar datos en Tivoli Data Warehouse
- Cómo se agrupan las muestras de datos de Tivoli Data Warehouse para la poda
- Planificación de poda de los datos guardados en el almacén.
- Ubicación de almacenamiento para los archivos históricos a corto plazo antes de que se envíen al almacén de datos. Las muestras de datos se pueden almacenar en el agente de supervisión o en el Tivoli Enterprise Monitoring Server.

Para asegurarse de que las muestras de datos se guardan para llenar los espacios de trabajo históricos predefinidos, primero debe configurar e iniciar la recopilación de datos históricos. Los espacios de trabajo de tiempo real están disponibles tanto si inicia la recopilación de datos como si no la inicia.

Tareas de administrador del sistema

Un administrador del sistema tiene el nivel más alto de autorización y puede acceder a todas las características de IBM Tivoli Monitoring en Tivoli Enterprise Portal.

Esta lista representa los tipos de tareas que puede realizar un administrador del sistema:

- Establece los ID de usuario y los grupos de usuarios de Tivoli Enterprise Portal con los permisos apropiados para sus trabajos.
- Diseña espacios de trabajo para elementos de Navigator y deja estos espacios de trabajo disponibles para los usuarios basándose en los permisos establecidos.
- Define consultas que se pueden aplicar a vistas de tabla y gráfico para especificar los atributos y los rangos de valores de atributo a recuperar del servidor de supervisión.
- Graba definiciones para iniciar aplicaciones y las deja disponibles a los usuarios basándose en los permisos establecidos.
- Crea acciones de línea de mandatos que se pueden ejecutar en el sistema gestionado especificado desde el cliente de portal y las deja disponibles a los usuarios a los que se ha otorgado autorización.
- Crea situaciones utilizando los recursos de programación visuales
- Establece la gravedad de una situación para un elemento determinado de Navigator y qué sonido, si existe, se reproduce cuando la situación es verdadera y se abre un suceso
- Decide qué situaciones se aplican a qué sistemas gestionados, proceso que se denomina distribución
- Proporciona consejo experto a visualizar cuando determinadas situaciones se evalúan verdaderas
- Crea flujos de trabajo de política, que son acciones a realizar cuando las situaciones se evalúan verdaderas
- Crea, instala, actualiza, distribuye y configura agentes en hosts remotos desde una ubicación central
- Inicia, detiene y recicla procesos de agente

Proveedor de servicios de Performance Monitoring

El componente Tivoli Enterprise Monitoring Automation Server contiene el proveedor de servicios de Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) y está instalado en los mismos sistemas que el Tivoli Enterprise Monitoring Server concentrador.

El proveedor de servicios de Performance Monitoring registra recursos de supervisión con el Registry Services. Registry Services es un servicio de integración Jazz for Service Management que proporciona un repositorio de datos compartidos para productos en un entorno de gestión de servicios integrados. Los productos que descubren y gestionan recursos de TI compartidos pueden registrar estos recursos de TI y los servicios que ofrecen con Registry Services. Otros productos pueden consumir datos consultando en Registry Services los recursos gestionados o los proveedores de servicios asociados que le interesen.

El proveedor de servicios de Performance Monitoring registra tipos de recursos como sistemas, servidor de software, módulo de software, base de datos, dirección IP y punto de acceso de servidor en nombre de los agentes de supervisión. Estos

tipos de recursos se definen utilizando el vocabulario de tipo de recurso común (CRTV) OSLC. Los agentes ofrecen una plantilla que correlaciona sus datos de supervisión con los recursos CRTV. La plantilla se instala con el soporte de aplicación del servidor de supervisión del agente.

El proveedor de servicios de Performance Monitoring también da soporte a la API RESTful OSLC-PM para recuperar los datos enlazados sobre los recursos supervisados. Incluye los tipos de contenido RDF/XML, XML compacto y HTML en solicitudes HTTP GET. Cuando se solicita contenido RDF/XML y HTML, la API devuelve métricas de estado recursos definidas por el dominio OSLC-PM y por el espacio de nombres privado de IBM Tivoli Monitoring.

Para descubrir los recursos que tienen métricas de estado disponibles del proveedor de servicios de Performance Monitoring, debe consultar Registry Services desde el proveedor de servicios de Performance Monitoring no proporciona la posibilidad de consulta OSLC. Los Registry Services proporcionan una interfaz de consulta para recuperar registros de los proveedores de servicios, registros de registro de recurso y registros de recursos conciliados. Los registros de recurso conciliados contienen URL de HTTP que se pueden utilizar para recuperar información sobre el recurso desde el proveedor de servicios que ha registrado el recurso. La publicación *Jazz for Service Management Integration Guide* de Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) contiene información sobre la consulta de Registry Services para obtener información sobre proveedores de servicios y recursos.

Los servicios de seguridad son un componente opcional de Jazz for Service Management que permite que las aplicaciones no basadas en WebSphere como el proveedor de servicios de Performance Monitoring participen en el inicio de sesión único basado en LTPA. Deben estar instalados y configurados si desea que el proveedor de servicios de Performance Monitoring para autenticar las solicitudes que recibe de los clientes de OSLC. Este es el único método de autenticación soportado por el proveedor de servicios. Consulte “Autenticación a través del Tivoli Enterprise Monitoring Automation Server” en la página 126 para obtener más información.

Puede utilizar el proveedor de servicios de Performance Monitoring con el servidor del panel de instrumentos de Tivoli Business Service Manager V6.1.1 para visualizar las principales métricas de estado de los agentes de supervisión en el árbol de servicios sin iniciar en contexto en Tivoli Enterprise Portal. Las métricas de estado están disponibles si un recurso como ComputerSystem o SoftwareServer se ha registrado en Registry Services por el proveedor de servicios de Performance Monitoring y el recurso también se ha descubierto por IBM Tivoli Monitoring Discovery Library Adapter o por el sensor de Tivoli Application Dependency Discovery Manager cuando el proveedor de servicios de TADDM OSLC también se está utilizando. Las métricas se visualizan en un diálogo de vista previa contextual que también muestra información de otros proveedores de servicios que han registrado el mismo recurso. Por ejemplo, el proveedor de servicios OSLC para Tivoli Application Dependency Discovery Manager proporciona información de historial de cambios y configuración para recursos registrados en el diálogo de vista previa contextual. Para obtener más información sobre cómo configurar la integración entre el proveedor de servicios de Performance Monitoring, Tivoli Business Service Manager, Registry Services y otros proveedores de servicios soportados, busque "Integración de productos cruzados para IBM Tivoli

Monitoring" en IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home).

También puede crear sus propias aplicaciones cliente OSLC que recuperan información de recurso de Registry Services y métricas de estado para estos recursos del proveedor de servicios de Performance Monitoring. Como alternativa, puede crear su propia implementación de proveedor de servicios OSLC para aumentar la información disponible para los recursos registrados. Para obtener más información sobre cómo crear estos tipos de aplicaciones, consulte Cómo empezar con Servicios de registro en la wiki de Jazz for Service Management.

Para obtener más información sobre OSLC y la integración fácil, consulte los enlaces siguientes:

- Comunidad de OSLC
- Grupo de trabajo de Performance Monitoring
- Grupo de trabajo de reconciliación y vocabulario de tipos de recursos comunes
- Integración fácil en ISM Connect
- Esquema de espacio de nombres privado OSLC de IBM Tivoli Monitoring

Para obtener información sobre cómo instalar y configurar el Tivoli Enterprise Monitoring Automation Server y el proveedor de servicios de Performance Monitoring, consulte *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm).

Capítulo 2. Preparación del entorno de Tivoli Enterprise Portal

Revise estos temas para conocer la configuración adicional del entorno de cliente de Tivoli Enterprise Portal.

Cliente de navegador

Los usuarios inician el cliente de navegador entrando el URL del servidor HTTP integral en el Tivoli Enterprise Portal Server.

Las ventajas del cliente de navegador son:

- Despliegue fácil. El cliente de navegador se instala la primera vez que los usuarios inician la sesión en el URL para el servidor HTTP integral de Tivoli Enterprise Portal.
- Las actualizaciones de software son automáticas. Cuando los usuarios inician la sesión, se comprueba el cliente de navegador con el del Tivoli Enterprise Portal Server; si se detecta una nueva versión, se descarga del servidor.
- Se establecen valores de parámetros globales para todos los usuarios conectados al mismo Tivoli Enterprise Portal Server.
- Los espacios de trabajo tienen URL de identificación a los que se puede hacer referencia en las páginas web y cuando se inicia la sesión desde otra aplicación web.
- Incluye un mensaje de cabecera que se puede personalizar con el logotipo y el URL de su empresa.

Versiones de Java Runtime Environment (JRE)

El Tivoli Enterprise Portal Server y el cliente ejecutan software basado en Java. Cuando se instala el servidor de portal o el cliente de escritorio, IBM Java 7 se instala automáticamente.

Antes de utilizar IBM Web Start for Java para descargar el cliente de escritorio de Tivoli Enterprise Portal Server:

- Tivoli Enterprise Portal Server debe estar instalado. (Consulte el manual *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm).)
- IBM Runtime Environment para Windows (de 32 o 64 bits), versión 7.0, debe estar instalado en el sistema en el que desea descargar el cliente de escritorio.

  Puede descargar el instalador de IBM JRE desde Tivoli Enterprise Portal Server. IBM JRE debe instalarse como la JVM del sistema.

  Si desea ejecutar el cliente de escritorio en un sistema que ya tiene instalado un componente base de Tivoli Management Services (por ejemplo, un servidor de supervisión o el servidor de portal), no hay necesidad de instalar IBM JRE. La versión correcta de IBM JRE se instala con el componente de Tivoli Management Services.

Cuando el usuario inicia una sesión desde un navegador, se comprueba el nivel de Java asociado con el navegador. La versión necesaria de Java se controla en el servidor de portal y es posible que se le solicite que actualice a IBM Java 7 al conectarse.

© Copyright IBM Corp. 2005, 2013

Primer inicio de sesión

La primera vez que se entra en el URL de Tivoli Enterprise Portal desde un sistema, el plug-in Java transfiere los archivos necesarios del Tivoli Enterprise Portal Server (en Windows, los archivos residen en la ramificación <*install_dir*>\cnb; en sistemas operativos como UNIX, están en la ramificación <*install_dir*>/cw).

A partir de ese momento no es necesario descargar otra vez el software de cliente de navegador hasta que se haya instalado una nueva versión. El plug-in Java mantiene los niveles de versión de los archivos en los sistemas del usuario y los compara con los niveles de versión del servidor HTTP integral. Si detecta archivos más antiguos que los del servidor HTTP, descarga los archivos más recientes.

Asegúrese de tener suficiente espacio libre para los archivos descargados. Si el disco se queda sin espacio durante la descarga, no se le avisará.

Valores de seguridad de Internet Explorer

Acerca de esta tarea

Si tiene establecido el nivel de seguridad de Internet Explorer en alto, debe ajustar los valores para ejecutar Tivoli Enterprise Portal. De lo contrario, el cliente de navegador de Tivoli Enterprise Portal no se puede ejecutar.

Comprobación de los valores de seguridad

El siguiente procedimiento debe utilizarse para comprobar los valores de seguridad actuales.

Procedimiento

1. En Internet Explorer, seleccione **Herramientas** → **Opciones de Internet**.
2. Seleccione el separador **Seguridad**.
3. Pulse **Internet** si ejecuta Tivoli Enterprise Portal a través de Internet o **Intranet** si ejecuta Tivoli Enterprise Portal a través de la intranet.
4. Cambie los valores de seguridad al **Nivel predeterminado**
5. Pulse **Aceptar** para guardar.

Mantener los valores de seguridad actuales

Puede integrar el sitio web de Tivoli Enterprise Portal con Internet Explorer sin cambiar los valores de seguridad. Si desea mantener los valores de seguridad actuales, puede añadir el sitio web de Tivoli Enterprise Portal a la zona de sitios fiables.

Procedimiento

1. En Internet Explorer, seleccione **Herramientas** → **Opciones de Internet**
2. Seleccione el separador **Seguridad**.
3. Pulse **Sitios fiables** → **Sitios** y entre el URL para Tivoli Enterprise Portal.
4. Pulse el recuadro de selección que comprueba (https:) todos los sitios de esta zona y pulse **Añadir**.

   Elija el nivel de seguridad medio o más bajo para todos los sitios de la zona **Sitios fiables**.
5. Pulse **Aceptar** para guardar los cambios.

Privilegios de grabación y supresión de Windows

A partir de Windows 2000, se eliminaron del grupo Usuarios los privilegios de grabación y supresión para determinadas carpetas y claves de registro. Estos privilegios son necesarios para cualquier persona que tenga la intención de utilizar el cliente de Java WebStart o el cliente de navegador. De lo contrario, se encuentran errores de excepción de Java durante los intentos de inicio del producto.

Para que los usuarios puedan descargar el cliente de Java WebStart o iniciar el cliente de navegador, el administrador de Windows debe asignar los permisos necesarios a ID de usuario individuales o al grupo Usuarios o bien crear un nuevo grupo con los permisos necesarios y asignar los usuarios a este grupo además del grupo Usuarios. Los permisos necesarios son:

- Permisos para grabar y suprimir en el directorio donde está instalado Windows, por ejemplo C:\WINDOWS.
- Permisos para establecer valor, crear subclave y suprimir en la clave de registro HKEY_LOCAL_MACHINE\SOFTWARE.

Nota: El esquema de permisos de Windows afecta a la modalidad de navegador de Tivoli Enterprise Portal y al software de otras empresas instalado mediante Internet Explorer.

Adición del logotipo y del URL de empresa

La aplicación de navegador de Tivoli Enterprise Portal es muy similar a la de la modalidad de escritorio, salvo que tiene un mensaje de cabecera con un enlace a ibm.com. Puede personalizar el cliente de navegador de Tivoli Enterprise Portal sustituyendo el logotipo y el URL por los de su organización.

Acerca de esta tarea

Realice estos pasos para personalizar el mensaje de cabecera del cliente del portal:

Procedimiento

1. En el sistema donde ha instalado el servidor de Tivoli Enterprise Portal, abra el archivo siguiente en un editor HTML o un editor de texto:

   dir_instalación\cnb\bannerimage.html
2. Edite las etiquetas HREF e IMG SRC para el archivo de gráficos de logotipo y de URL de su organización:
   a. Sustituya el marcador **href** ' + URL + ' por el URL de su organización.
   b. Sustituya el marcador **img src** ' + URL + ' por el nombre del archivo GIF o JPG de logotipo de su organización.
   c. Sustituya el marcador **alt** ' + URL + ' por el texto que se debe visualizar cuando el puntero del ratón está sobre la imagen, por ejemplo el URL.
3. Guarde el archivo y salga del editor.
4. Copie el gráfico del logotipo en el directorio *dir_instalación*\cnb\ .

Resultados

Ahora los usuarios verán el logotipo en el lado derecho del mensaje de cabecera la siguiente vez que inicien la modalidad de navegador.

Inicio del cliente de Tivoli Enterprise Portal

Inicie una sesión en el servidor de Tivoli Enterprise Portal para iniciar una sesión de trabajo de Tivoli Enterprise Portal.

Antes de empezar

El Tivoli Enterprise Monitoring Server concentrador y el servidor de portal deben estar en ejecución para que el cliente de portal se inicie correctamente. También debe tener un ID de usuario válido.

Acerca de esta tarea

Tras haber instalado y configurado correctamente todos los componentes del entorno de IBM Tivoli Monitoring, puede verificar la instalación y la configuración iniciando Tivoli Enterprise Portal para ver los datos de supervisión. Puede acceder al portal utilizando el cliente de escritorio o el cliente de navegador. El ID de usuario predeterminado es sysadmin.

Procedimiento

- Inicie el cliente de escritorio:
  - Windows Pulse **Inicio → Programas → IBM Tivoli Monitoring → Tivoli Enterprise Portal**. Cuando se muestre la ventana de inicio de sesión, escriba el ID de usuario y la contraseña y pulse **Aceptar**.
  - Linux UNIX Escriba `./itmcmd agent start cj` en la línea de mandatos.
- Inicie el cliente de navegador:
  1. Inicie el navegador.
  2. Escriba el URL del servidor de Tivoli Enterprise Portal en el campo **Dirección** del navegador, donde *nombresistema* es el nombre de host del sistema donde se ha instalado el servidor de portal y *15200* es el número de puerto para el cliente de navegador: `http://nombresistema:15200`
  3. Pulse **Sí** en la ventana Aviso - Seguridad.
  4. Cuando se muestre la ventana de inicio de sesión, escriba el ID de usuario y la contraseña y pulse **Aceptar**.

Utilización de Web Start para descargar y ejecutar el cliente de escritorio

Un cliente de escritorio obtenido del Tivoli Enterprise Portal Server mediante IBM Web Start para Java se beneficia de la administración centralizada del servidor. Igual que el cliente de navegador, se configura automáticamente con las actualizaciones más recientes cada vez que se inicia el cliente y no es necesario configurar soporte de aplicación.

Esta sección pertenece a la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* y se ha reproducido aquí para su comodidad.

Antes de utilizar IBM Web Start for Java para descargar el cliente de escritorio de Tivoli Enterprise Portal Server:

- Tivoli Enterprise Portal Server debe estar instalado. (Consulte el manual *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm).)

- IBM Runtime Environment para Windows (de 32 o 64 bits), versión 7.0, debe estar instalado en el sistema en el que desea descargar el cliente de escritorio.

  Puede descargar el instalador de IBM JRE desde Tivoli Enterprise Portal Server. IBM JRE debe instalarse como la JVM del sistema.

  Si desea ejecutar el cliente de escritorio en un sistema que ya tiene instalado un componente base de Tivoli Management Services (por ejemplo, un servidor de supervisión o el servidor de portal), no hay necesidad de instalar IBM JRE. La versión correcta de IBM JRE se instala con el componente de Tivoli Management Services.

Instalación de IBM JRE

Acerca de esta tarea

Si tiene previsto descargar y ejecutar el cliente de escritorio utilizando Web Start en un sistema donde no se ha instalado ningún componente base de IBM Tivoli Monitoring, primero debe instalar IBM Java. Se descarga un instalador del sistema donde el Tivoli Enterprise Portal Server está instalado.

Windows: Instalación de IBM JRE

Instale IBM Java Runtime Environment en el sistema en el que piensa iniciar el cliente de escritorio utilizando Java Web Start.

Acerca de esta tarea

Siga estos pasos para descargar el instalador de IBM JRE desde el Tivoli Enterprise Portal Server e instale JRE en un sistema Windows.

Nota: El procedimiento siguiente presupone que está instalando IBM JRE en una plataforma Windows de 32 bits. Si está utilizando una plataforma Windows de 64 bits, el nombre para el ejecutable del instalador de IBM JRE es `ibm-java7_64.exe`.

Procedimiento

1. Inicie el navegador en el sistema en el que desea descargar el instalador.
2. Escriba el URL siguiente en el campo **Dirección** del navegador, donde *<nombre_host_servidor_portal>* es el nombre de host completo del sistema donde se ha instalado el servidor de portal (por ejemplo, `myteps.itmlab.company.com`):

   ```
   http://<portal_server_host_name>:15200/java/ibm-java7.exe
   ```
3. Cuando se le solicite, guarde el archivo **ibm-java7.exe** en un directorio del disco duro.
4. Vaya al directorio donde ha guardado el archivo **ibm-java7.exe** y efectúe una doble pulsación en el archivo a fin de iniciar el instalador de JRE para iniciar el programa de instalación.
5. En la ventana emergente, seleccione el idioma en la lista desplegable y pulse en **Aceptar**.
6. Pulse **Siguiente** en la página de bienvenida.
7. Pulse **Sí** para aceptar el acuerdo de licencia.
8. Acepte la ubicación predeterminada para instalar el JRE o vaya a un directorio diferente. Pulse en **Siguiente**.
9. Si no tiene ningún otro sistema JVM de instalado, pulse **YES** en el mensaje que solicita si desea instalar este JRE como el sistema JVM. De lo contrario, pulse **NO**.

10. Si ya hay otro JRE instalado actualmente como sistema JVM, se le solicitará si desea sobregrabar el sistema JVM actual, pulse **NO**. Si se sobregraba el JVM del sistema actual puede hacer que fallen aplicaciones que dependen del JVM actual.
11. Pulse en **Siguiente** en la ventana Iniciar la copia de archivos para iniciar la instalación de JRE.
12. En la ventana de registro del navegador, seleccione los navegadores a los que desee que IBM JRE esté asociado. Normalmente deben seleccionarse los navegadores que desee utilizar con el cliente de navegador.
13. Pulse en **Siguiente**.
14. Pulse en **Finalizar** para completar la instalación.

Linux: Instalación de IBM JRE

Instale IBM Java Runtime Environment en el sistema en el que piensa iniciar el cliente de escritorio utilizando Java Web Start.

Acerca de esta tarea

Realice los pasos siguientes para descargar el instalador de IBM JRE desde el Tivoli Enterprise Portal Server e instalar el JRE en un sistema Linux o instalar JRE sin descargar el instalador, especificado el URL para rpm en el mandato.

```
rpm -ivh http://nombre_host_servidor_portal:15200/java/ibm-java7.rpm
```

Nota: El procedimiento siguiente presupone que está instalando IBM JRE en una plataforma Linux de 32 bits. Si está utilizando una plataforma Linux de 64 bits, el nombre para el archivo `.rpm` de IBM JRE es `ibm-java7_64.rpm`.

Procedimiento

1. Inicie el navegador en el sistema en el que desea descargar el instalador.
2. Entre el URL siguiente en el campo **Dirección** del navegador:

   `http://nombre_host_servidor_portal:15200/java/ibm-java7.rpm`

   donde *nombre_host_servidor_portal* es el nombre de host totalmente calificado del sistema donde está instalado el servidor de portal (por ejemplo `myteps.itmlab.company.com`).
3. Cuando se le solicite, guarde el instalador en disco.
4. Vaya al directorio donde ha guardado el archivo `ibm-java7.rpm` y lance el instalador para iniciar el programa de instalación utilizando el mandato siguiente:

   ```
   rpm -ivh ibm-java7.rpm
   ```

Habilitación del rastreo para JRE

Los archivos de registro no se crean para el cliente de escritorio iniciado mediante Web Start a menos que se habilite el rastreo para JRE.

Antes de empezar

Los registros de un cliente de Web Start están ubicados en un lugar diferente de los registros para el cliente de navegador y el cliente de escritorio instalados desde el soporte. En sistemas Windows, los registros para el cliente de Web Start están ubicados en los directorios `C:\Documents and Settings\Administrator\Application Data\IBM\Java\Deployment\log` o `%USERPROFILE%\AppData\LocalLow\IBM\Java\Deployment\log`. En sistemas Linux y UNIX, los registros están ubicados en el directorio `.java/deployment/log` del directorio de inicio del ID de usuario

bajo el cual se ha instalado Java JRE. Java Web Start creará un archivo de rastreo con nombre exclusivo para cada inicio independiente de la aplicación. Los archivos se denominan `javaws.nnnnn.trace`, donde *nnnnn* es un identificador arbitrario de cinco dígitos.

Acerca de esta tarea

Realice los pasos siguientes para habilitar el rastreo:

Procedimiento

1. Inicie el Panel de control de IBM para Java.
   - En Windows, seleccione **Inicio > Panel de control** y a continuación efectúe una doble pulsación en Panel de control de IBM para Java. Debe conmutar a la vista Clásica para ver y seleccionar el Panel de control. Alternativamente, puede iniciar el Panel de control seleccionando **Inicio > Ejecutar > "C:\Archivos de programa\IBM\Java70\jre\bin\javacpl.exe"**.
   - En Linux, vaya a <*dir_instalación*>/jre/<*plataforma*>/bin y ejecute el panel de control: `./ControlPanel`
2. Seleccione el separador **Avanzado**.
3. Expanda el nodo Depuración en el árbol **Valores** y marque **Habilitar rastreo**.
4. Pulse **Aceptar** para guardar el valor y cerrar el Panel de control de Java.

Descarga y ejecución del cliente de escritorio

Tivoli Enterprise Portal se puede iniciar como una aplicación de escritorio o como una aplicación web. Tiene tres modos de instalar la aplicación de escritorio: desde un navegador especificando el URL del cliente de Java Web Start en el Tivoli Enterprise Portal Server, iniciando el cliente de escritorio desde el panel de control de IBM Java o iniciando el cliente de escritorio utilizando Java Web Start desde la línea de mandatos.

Antes de empezar

Estas son las instrucciones básicas para descargar y ejecutar el cliente de escritorio utilizando Java Web Start. Las instrucciones completas, con las notas de configuración se proporcionan en la *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Acerca de esta tarea

Realice uno de estos pasos para instalar e iniciar el cliente de escritorio utilizando Java Web Start:

Procedimiento

- Escriba el URL del servidor de portal en un navegador:
  1. Inicie el navegador en el sistema en el que desea utilizar el cliente de escritorio.
  2. Escriba el URL siguiente en el campo **Dirección** del navegador, donde <*nombre_host_servidor_portal*> es el nombre de host completo del sistema donde se ha instalado el Tivoli Enterprise Portal Server.

     `http://<nombre_host_servidor_portal>:15200/tep.jnlp`
  3. Pulse **Ejecutar** en el mensaje de seguridad.
  4. Si desea crear un atajo en el escritorio para Tivoli Enterprise Portal, pulse **Sí** cuando se le pregunte. El cliente de escritorio se inicia y visualiza la ventana

de inicio de sesión. Si IBM Java 1.7 no es la JVM del sistema, no podrá utilizar este atajo. Debe crear el suyo propio, como se describe en el tema "Creación manual de un atajo para el cliente de Web Start" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

5. Entre el ID de usuario y la contraseña para iniciar la sesión en Tivoli Enterprise Portal o pulse **Cancelar** si no desea iniciar la sesión en este momento. El ID de usuario predeterminado es *sysadmin*.

Si establece la opción de rastreo RAS para el cliente de Tivoli Enterprise Portal como se describe en la publicación *IBM Tivoli Monitoring: Guía de resolución de problemas*, cuando reinicie el cliente, se deberá crear el archivo `kcjras1.log` en la ubicación donde se ha iniciado el cliente. De forma predeterminada, en Windows es `\Documents and Settings\<id_usuario>\Desktop`.

- Inicie el cliente de escritorio desde el panel de control de IBM Java:
  1. Inicie el Panel de control de IBM Java:
     Windows En el panel de control de Windows, efectúe una doble pulsación en el **Panel de control de IBM Java**. Debe encontrarse en la vista Clásica para ver el **Panel de control de IBM Java**.
     Linux Vaya al directorio `<dir_instalación>/jre/<plataforma>/bin` y escriba `./ControlPanel`.
  2. En el separador **General**, la sección Archivos de Internet temporales, pulse en **Valores**. Se visualizará la ventana Valores de archivos temporales.
  3. Pulse **Ver aplicaciones**.
  4. En el separador **Usuario**, seleccione Tivoli Enterprise Portal y después pulse en **Iniciar en línea**.

  Java Web Start descarga e inicia el cliente de escritorio. Cuando se inicie la aplicación, podrá cerrar las ventanas de Panel de control.
- Inicie el cliente de escritorio utilizando Java Web Start desde la línea de mandatos:
  1. Abra una ventana de línea de mandatos y vaya al directorio donde está instalado Java Web Start.
     Windows
     ```
     C:\Program Files\IBM\Java70\jre\bin
     ```
     Linux
     ```
     <dir_instalación>/jre/<plataforma>/bin
     ```
  2. Escriba el mandato siguiente, donde *<nombre_host_servidor_portal>* es el nombre de host completo del sistema donde se ha instalado el Tivoli Enterprise Portal Server.
     Windows
     ```
     javaws http://<nombre_host_servidor_portal>:15200/tep.jnlp
     ```
     Linux
     ```
     ./javaws http://<nombre_host_servidor_portal>:15200/tep.jnlp
     ```

  Java Web Start descarga e inicia el cliente de escritorio.

Creación manual de un atajo para el cliente de Web Start

En Windows, el archivo ejecutable Web Start para la JVM Java predeterminada se copia en el directorio Windows\System32. Cuando se permite que Web Start cree un atajo para iniciar el cliente de escritorio, aquél utiliza el archivo del directorio System32 como destino. Si la JVM predeterminada no es IBM Java 1.7, el atajo no iniciará el cliente de escritorio. Deberá crear un atajo manualmente.

Acerca de esta tarea

Para crear un atajo a fin de iniciar el cliente de escritorio utilizando el Inicio web, siga estos pasos:

Procedimiento

1. Pulse el botón derecho del ratón en el escritorio de Windows y seleccione **Nuevo > Acceso directo** en el menú emergente.
2. En la ventana Crear atajo, escriba la vía de acceso siguiente o pulse **Examinar** y navegue hasta el ejecutable como se muestra a continuación:

   ```
   C:\Program Files\IBM\Java70\jre\bin\javaws.exe
   ```
3. Pulse **Siguiente** y escriba un nombre para el atajo en la ventana Seleccionar un título para el programa. Por ejemplo:

   ```
   Cliente ITM Web Start
   ```
4. Pulse en **Finalizar**. El atajo aparece en el escritorio.

Inicio del cliente de navegador en otro servidor de portal

Al instalar el cliente de escritorio, se designa un Tivoli Enterprise Portal Server de inicio. Si el entorno de supervisión tiene varios servidores de portal, puede definir una instancia de escritorio independiente para apuntar a otro servidor de portal.

Antes de empezar

Un caso de ejemplo típico para tener varios servidores de portal es aquel en que hay un servidor de portal de prueba y producción o cuando hay varias redes gestionadas con un servidor de portal conectado a cada servidor de supervisión concentrador.

Acerca de esta tarea

Realice estos pasos para crear otra instancia de cliente de portal que se conecta a un servidor de portal diferente.

Procedimiento

- Windows
  1. En el sistema donde está instalado el cliente de escritorio, seleccione **Inicio** → **Programas** → **IBM Tivoli Monitoring** → **Manage Tivoli Enterprise Monitoring Services**.
  2. Pulse con el botón derecho del ratón **Cliente de escritorio de Tivoli Enterprise Portal** y pulse **Crear instancia**. Si se han creado otras instancias de Tivoli Enterprise Portal, verá más de una en la lista. **Crear instancia** está inhabilitado para todas las instancias, excepto para la instancia de Tivoli Enterprise Portal original.
  3. En la ventana Tivoli Enterprise Portal, escriba un nombre que identifique la instancia y pulse **Aceptar**.
  4. En la ventana Configurar instancia de aplicación, escriba el nombre de host del Tivoli Enterprise Portal Server al que desea conectarse.
  5. Pulse **Aceptar**.
- Linux UNIX Utilizando la línea de mandatos:
  1. Vaya al directorio (cd) *install_dir*/bin.
  2. Cree una nueva instancia utilizando el mandato siguiente:

```
./itmcmd config -A cj
```

3. Inicie la nueva instancia utilizando el mandato siguiente:
   ```
   ./itmcmd agent -o <nombre_instancia> start cj
   ```

   Para ver completa información sobre la sintaxis, consulte la publicación *IBM Tivoli Monitoring: Consulta de mandatos*.

Utilizando la GUI:

1. Vaya al directorio (cd) *install_dir*/bin.
2. Para iniciar Manage Tivoli Enterprise Monitoring Services, utilice el mandato siguiente:
   ```
   ./itmcmd manage
   ```
3. Pulse con el botón derecho del ratón en **Cliente de escritorio de Tivoli Enterprise Portal** y pulse **Configurar**.
4. Especifique el nombre de instancia y el nombre de host de servidor de portal y a continuación pulse **Guardar**.
5. Para iniciar la instancia, pulse con el botón derecho del ratón en **Cliente de escritorio de Tivoli Enterprise Portal** y a continuación pulse **Iniciar servicio** y especifique el nombre de instancia.

Resultados

La nueva instancia de Tivoli Enterprise Portal se añade a la lista.

Qué hacer a continuación

Ahora puede iniciar la instancia en cualquier momento pulsando dos veces su entrada.

Si ya no necesita una instancia de Tivoli Enterprise Portal, puede suprimirla pulsando la entrada con el botón derecho del ratón y pulsando **Eliminar instancia**.

Inicio del cliente de navegador en otro servidor de portal.

Inicie una instancia diferente del navegador e inicie sesión en el Tivoli Enterprise Portal Server de una red gestionada diferente para ver dos redes gestionadas desde el mismo sistema.

Antes de empezar

Su red gestionada puede tener un servidor de portal y un concentrador Tivoli Enterprise Monitoring Server. Puede iniciar la sesión en el servidor de portal mediante Windows Internet Explorer o Mozilla Firefox.

Acerca de esta tarea

Antes de iniciar las instancias del cliente de navegador, realice estos pasos en cada sistema en que esté instalado un servidor de portal con el que desea conectarse.

Procedimiento

- Windows
  1. En los Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho del ratón la entrada de **Tivoli Enterprise Portal Server** y seleccione **Reconfigurar**.

2. En la ventana Configurar navegador de Tivoli Enterprise Portal que se abre, efectúe una doble pulsación en el parámetro **cnp.browser.installdir** .
3. En la ventana Editar parámetros del navegador de Tivoli Enterprise Portal que se abre, escriba la vía de acceso al directorio donde se deben instalar los archivos de navegador, por ejemplo, `C:\\temp\\cnpBrowserFiles`.
4. Seleccione el recuadro de selección ☑ **En uso** y pulse **Aceptar**.
5. Pulse **Aceptar** para guardar los cambios.

- Linux

1. Vaya al directorio en el que se encuentra `applet.html`: *`dir_instalación`*`/platform/cw`, donde plataforma es el tipo actual de sistema operativo.
2. Abra `applet.html` en un editor de texto.
3. Busque la línea **<!--END OF PARAMS-->** y añada una línea nueva encima.
4. En la nueva línea, añada este parámetro, donde *dir_instalación_navegador* es la vía de acceso del directorio donde están instalados los archivos del navegador.

   ```
   document.writeln( '<PARAM NAME= "cnp.browser.installdir"
   VALUE="dir_instalación_navegador">' )
   ```

5. Guarde y cierre `applet.html`.

Qué hacer a continuación

Si está utilizando Internet Explorer, inicie cada instancia del cliente de portal que desee.

Si utiliza el navegador Firefox, debe crear un perfil diferente para cada instancia que desee iniciar. El sitio de soporte de Mozilla tiene un tema sobre Gestión de perfiles (http://support.mozilla.com/en-US/kb/Managing+Profiles) donde puede consultar la ayuda acerca de cómo configurar los perfiles. Después de crear los perfiles, inicie cada instancia con este mandato **<*vía_acceso_completa_de_firefox*> -p <*nombre_perfil*> -no-remote**

Referencia relacionada:

"Lista de parámetros del cliente de portal" en la página 62
La mayor parte de los valores predeterminados de los parámetros del cliente de Tivoli Enterprise Portal no se modifican. Edite los parámetros de los clientes para modificar un comportamiento específico.

Especificación del navegador utilizado para iniciar aplicación y para ayuda en línea

Si está ejecutando el cliente de escritorio en Linux o desea ver la ayuda en línea con un navegador distinto al predeterminado, debe especificar en el servidor de portal la ubicación del navegador que desea utilizar.

Acerca de esta tarea

Siga estos pasos para especificar un navegador diferente para utilizarlo para la ayuda en línea y para iniciar la aplicación:

Procedimiento

- Windows

1. Inicie Manage Tivoli Enterprise Monitoring Services (**Inicio > (Todos los) programas > IBM Tivoli Monitoring > Manage Tivoli Enterprise Monitoring Services**).
2. En la ventana Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho del ratón en el cliente de escritorio o de navegador y seleccione **Reconfigurar**. Se visualiza la ventana Configurar el navegador de Tivoli Enterprise Portal. (Si configura el cliente de escritorio, se visualizará la ventana Configurar instancia de aplicación.)
3. Desplácese hacia abajo en la lista de variables hasta que vea la variable `kjr.browser.default`.
4. Efectúe una doble pulsación en `kjr.browser.default`. Se visualiza la ventana Editar parámetros del navegador de Tivoli Enterprise Portal.
5. En el campo Valor, escriba la vía de acceso y el nombre de la aplicación de navegador alternativa. Por ejemplo, `C:\Archivos de programa\Mozilla Firefox\firefox.exe`
6. Pulse **Aceptar** para cerrar la ventana de edición y guardar el cambio.
7. Pulse **Aceptar** para cerrar la ventana de reconfiguración.

- Linux UNIX

  1. Vaya a *dir_instalación*/bin/cnp.sh y edite el script de shell cnp.sh.
  2. Añada la ubicación del navegador web a la última línea del archivo. En el ejemplo siguiente, la ubicación del navegador web es */opt/foo/bin/launcher*. `-Dkjr.browser.default=/opt/foo/bin/launcher` La línea es muy larga y tiene varias opciones en ella, incluidas otras varias opciones –D para definir otras propiedades. Es muy importante añadir la opción en el lugar correcto.

  Si la última línea de bin/cnp.sh tenía originalmente el aspecto siguiente:

  ```
  ${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
  -Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
  -Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
  -Dvbroker.agent.enableLocator=false
  -Dhttp.proxyHost=
  -Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
  ```

  Para establecer la ubicación de navegador en */opt/foo/bin/launcher*, cambie la línea para que tenga este aspecto:

  ```
  ${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
  -Dkjr.browser.default=/opt/foo/bin/launcher
  -Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
  -Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
  -Dvbroker.agent.enableLocator=false
  -Dhttp.proxyHost=
  -Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
  ```

- Java Web Start:

  Las aplicaciones desplegadas por Java Web Start se describen en los archivos de despliegue de jnlp. Para IBM Tivoli Monitoring, hay un archivo de despliegue que describe el componente de infraestructura de Tivoli Enterprise Portal principal, y archivos jar asociados, y un archivo de despliegue para cada una de las soluciones de supervisión basadas en Tivoli Enterprise Portal instaladas. El archivo central de despliegue del Tivoli Enterprise Portal Server se denomina `tep.jnlp`. El archivo de despliegue de la aplicación normalmente se denomina k*xx*_resources.jnlp o k*xx*.jnlp, donde *xx* es el identificador de la aplicación (un código de producto como, por ejemplo, `nt`, `ux` o `lz`). En un sistema Windows donde está instalado Tivoli Enterprise Portal Server, el archivo se encuentra en `<`*dir_instalación_itm*`>\CNB` (por ejemplo, `c:\IBM\ITM\CNB`). En un sistema Linux

donde se ha instalado Tivoli Enterprise Portal Server, el archivo se encuentra en <*dir_instalación_itm*>/<arch>/cw (por ejemplo, /opt/IBM/ITM/li6263/cw).

Las instancias de archivo de despliegue se generan siempre que se instala o se reconfigura el Tivoli Enterprise Portal Server (por ejemplo, al añadir una nueva solución de supervisión al entorno). El contenido de estos archivos se basa en dos archivos plantilla de despliegue (.jnlpt). El archivo de despliegue de plantilla de Tivoli Enterprise Portal de núcleo se denomina tep.jnlpt. El archivo de despliegue de plantilla de aplicación se denomina component.jnlpt. En un sistema Windows donde se ha instalado Tivoli Enterprise PortalTivoli Enterprise Portal, el archivo se encuentra en <*dir_instalación_itm*>\Config (por ejemplo: c:\IBM\ITM\Config). En sistemas UNIX, el archivo se encuentra en <*dir_instalación_itm*>/config (por ejemplo, /opt/IBM/ITM/config).

Para añadir o modificar argumentos JVM (por ejemplo el tamaño de almacenamiento dinámico máximo) u otras propiedades basadas en Tivoli Enterprise Portal (por ejemplo opciones de rastreo RAS1), es necesario editar el archivo de despliegue tep.jnlp o el archivo de plantilla de despliegue tep.jnlpt. El archivo de despliegue es simplemente sintaxis XML que describe la aplicación Web Start que se está desplegando. Se utiliza el elemento <resources> para definir los argumentos JVM, las propiedades de Tivoli Enterprise Portal, los archivos jar y las referencias a archivos de despliegue de componente.

- Modifique el archivo tep.jnlp si el cambio va a ser temporal (por ejemplo, establecer una opción de rastreo para reunir diagnósticos adicionales).
- Modifique el archivo tep.jnlpt si el cambio va a ser permanente (por ejemplo, el aumento del tamaño máximo de almacenamiento dinámico para acomodar un entorno supervisado mayor o un aumento de carga de sucesos).

  Si modifica el archivo de plantilla de despliegue, asegúrese de reconfigurar a continuación el Tivoli Enterprise Portal Server para volver a generar los archivos de despliegue .jnlp a nivel de instancia con los cambios.

Para especificar la ubicación del navegador que se debe utilizar para visualizar la ayuda en línea, añada la siguiente propiedad a la sección <resources> del archivo adecuado:

```
<property name="kjr.browser.default" value="<vía_acceso_navegador>" >
```

Adición de plataformas operativas a la vista de Navigator

Edite el archivo osnames del servidor de Tivoli Enterprise Portal para crear ramificaciones adicionales en la vista Navigator de Tivoli Enterprise Portal para otros nombres de sistema operativo.

La vista física de Navigator de Tivoli Enterprise Portal muestra la plataforma operativa bajo el nivel de empresa. El nombre de la plataforma operativa va seguido de la palabra *Systems* como en Linux Systems o z/OS Systems. Se pueden agregar algunas plataformas operativas. Si el entorno tiene dichas plataformas y desea que cada una tenga su propio elemento de Navigator, con todos los sistemas de ese tipo contenidos allí, puede añadirlas al archivo osnames en el directorio del servidor de portal (por ejemplo, C:\IBM\ITM\CNPS y /opt/IBM/ITM/config).

Capítulo 3. Preparación de su entorno de panel de control

Revise estos temas para configurar adicionalmente el entorno del panel de control.

Hojas de ruta

Las tareas para configurar su entorno dependen de muchos factores. Hay dos tipos principales de entornos de paneles de control que puede tener: un entorno básico sin inicio de sesión único ni controles de autorización por usuario, o un entorno avanzado con inicio de sesión único y controles de autorización por usuario. Si originariamente ha creado un entorno sin inicio de sesión único ni controles de autorización por usuario, más adelante puede cambiar los valores para utilizar el inicio de sesión único y los controles de autorización por usuario.

Configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario

Configure un entorno de paneles de control básico si desea utilizar IBM Dashboard Application Services Hub con aplicaciones de paneles de control de supervisión como los IBM Infrastructure Management Dashboards for Servers e IBM Infrastructure Management Dashboards for VMwar o con paneles de control personalizados, sin utilizar el inicio de sesión único ni controles de autorización por usuario.

El entorno debe cumplir los requisitos siguientes:

- Dashboard Application Services Hub y Tivoli Enterprise Portal Server no están configurados para utilizar un registro de usuarios de LDAP federado para la autenticación de usuarios.
- Los usuarios de paneles de control no lanzarán el cliente de navegador de Tivoli Enterprise Portal desde páginas de IBM Dashboard Application Services Hub o, si lo hacen, deben proporcionar sus credenciales cuando se inicia el cliente de navegador.
- Todos los usuarios de paneles de control pueden estar autorizados para ver los mismos sistemas gestionados y grupos de sistemas gestionados en las páginas de panel de control de supervisión.

Si no se cumplen estos requisitos en el entorno, siga los pasos de “Configuración de un entorno de panel de control de supervisión con inicio de sesión único y con controles de autorización por usuario” en la página 32.

Nota: También puede empezar con un entorno de paneles de control básico para familiarizarse con IBM Dashboard Application Services Hub con paneles de control de supervisión y luego añadir el inicio de sesión único y la autorización por usuario siguiendo los pasos de “Migración de un entorno de panel de control de supervisión básico a un entorno de panel de control con inicio de sesión único y controles de autorización por usuario” en la página 45.

Dashboard Application Services Hub utiliza una conexión HTTP o HTTPS al componente de proveedor de datos de panel de instrumentos del servidor de portal para recuperar datos de supervisión. Los datos de supervisión en tiempo real se recuperan del servidor de supervisión de hub y los agentes de supervisión y datos de supervisión históricos se recuperan de Tivoli Data Warehouse. No todas

© Copyright IBM Corp. 2005, 2013

las aplicaciones de paneles de control de supervisión dan soporte a la recuperación de datos históricos de Tivoli Data Warehouse.

Puede configurar una conexión de proveedor de datos de panel de instrumentos en el Dashboard Application Services Hub que especifique el nombre de host, protocolo, puerto, nombre de usuario y contraseña del servidor de portal. El ID de usuario configurado para la conexión de proveedor de datos se incluye en todas las solicitudes HTTP para el proveedor de datos de panel de instrumentos en lugar del usuario que ha iniciado sesión en Dashboard Application Services Hub y utiliza una aplicación de panel de control. El usuario de conexión debe estar definido como un ID de usuario de Tivoli Enterprise Portal y debe asignarse a las aplicaciones de supervisión cuyos datos se mostrarán en los paneles de control de supervisión. Dashboard Application Services Hub utiliza roles, para los usuarios o grupos de usuarios, para controlar las páginas a las que puede acceder un usuario. Sin embargo, proveedor de datos de panel de instrumentos lleva a cabo la autorización de los recursos de supervisión que se muestran en estas páginas. Debido a que al proveedor de datos de panel de instrumentos solo se le envían las credenciales del usuario configurado para la conexión del proveedor de datos, se imponen los permisos de Tivoli Enterprise Portal y las asignaciones de aplicaciones de supervisión del usuario de conexión y no de los usuarios de paneles de control. Por este motivo, todos los usuarios del panel de control de supervisión verán los datos de supervisión del mismo conjunto de sistemas gestionados y grupos de sistemas gestionados.

Requisitos previos

- Instale y configure el servidor de supervisión base de IBM Tivoli Monitoring, el servidor de portal y los componentes del cliente de portal utilizando las instrucciones de *IBM Tivoli Monitoring: Guía de instalación y configuración*. Al configurar el servidor de portal, habilite la proveedor de datos de panel de instrumentos.
- Instale y configure los agentes de supervisión cuyos datos se mostrarán en los paneles de control de supervisión. Instale el soporte de aplicaciones en los servidores de supervisión, el servidor de portal y el cliente de portal de escritorio si está siendo utilizado, utilizando las instrucciones de *IBM Tivoli Monitoring: Guía de instalación y configuración*.
- Instale y configure Dashboard Application Services Hub y las aplicaciones de supervisión de panel de control, consulte "Requisitos necesarios de software y memoria para un entorno de paneles de control" en *IBM Tivoli Monitoring: Guía de instalación y configuración*. Consulte también "Instalación y configuración de IBM Infrastructure Management Dashboards for Servers" en *IBM Tivoli Monitoring: Guía de instalación y configuración*, si va a instalar la aplicación de panel de control.

Hoja de ruta

Utilice la siguiente hoja de ruta para ayudarle a empezar:

Tabla 1. Hoja de ruta para la configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario

Paso	Descripción	Dónde encontrar información
1 (obligatorio)	Verifique que proveedor de datos de panel de instrumentos esté habilitado en la configuración de servidor de portal.	Para ver los pasos detallados, consulte "Verificación de que el proveedor de datos de panel de control está habilitado" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Tabla 1. Hoja de ruta para la configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario (continuación)

Paso	Descripción	Dónde encontrar información
2 (obligatorio)	Determine qué usuario de Tivoli Enterprise Portal debe estar configurado para la conexión de proveedor de datos de panel de instrumentos y asegúrese de que el usuario tenga esta autorización: • El usuario debe tener asignadas las aplicaciones de supervisión cuyos datos se mostrarán en los paneles de control de supervisión. • Si las aplicaciones de panel de control muestran sucesos de situación, el usuario debe tener permiso para ver sucesos de situación.	"Administrar usuarios" en la página 164 y "Gestión de los ID de usuario" en la página 171
3 (obligatorio)	Inicie sesión en IBM Dashboard Application Services Hub como un usuario administrativo y cree una conexión del proveedor de datos de panel de instrumentos que utilice el protocolo HTTP y que no requiera configuración de inicio de sesión único.	"Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring" en la página 52 Al crear la conexión, **no** seleccione el recuadro **Utilizar las credenciales del usuario (requiere la configuración de SSO)**.
4 (método recomendado opcional)	Inicie sesión en IBM Dashboard Application Services Hub como un usuario administrativo y cree un rol que controle el acceso a las páginas de la aplicación de paneles de control y asigne usuarios o grupos de usuarios de paneles de control al rol. **Nota:** Algunas aplicaciones de paneles de control como IBM Infrastructure Management for VMware crean automáticamente un rol para sus páginas cuando se instala la aplicación de paneles de control. Sin embargo, otras aplicaciones de paneles de control como IBM Infrastructure Management Dashboards for Servers no crean un rol durante la instalación por lo que debe crear uno o asignar las páginas de panel de control a un rol existente.	Consulte la *Jazz for Service Management Guía del administrador* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con roles que controlan el acceso a las páginas de paneles de control.
5 (obligatorio)	Inicie sesión en IBM Dashboard Application Services Hub como un usuario con permiso para ver las páginas de panel de control, lance las aplicaciones de paneles de control y verifique que se visualizan los datos.	Consulte la guía del usuario de la aplicación de paneles de control para obtener detalles sobre cómo iniciar y utilizar el panel de control. **Consejo:** Primero seleccione **Estado y salud del sistema** > **Panel de control Comprobaciones de salud** para verificar que el entorno funcione correctamente. A continuación, si está utilizando Infrastructure Management Dashboards for Servers, seleccione **Estado y salud del sistema** > **Paneles de control del servidor**. Para obtener más información sobre la utilización de Infrastructure Management Dashboards for Servers, consulte las guías del usuario del agente del sistema operativo.

Tabla 1. Hoja de ruta para la configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario (continuación)

Paso	Descripción	Dónde encontrar información
6 (opcional)	Si desea utilizar HTTPS entre Dashboard Application Services Hub y proveedor de datos de panel de instrumentos, realice estas tareas:	
	1. Configure TLS/SSL entre el concentrador de paneles de control y el proveedor de datos.	"Configuración de la comunicación TLS/SSL entre Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos" en la página 219
	2. Inicie sesión en IBM Dashboard Application Services Hub como usuario administrativo al que se ha asignado los roles `administrador` e `iscadmins` y suprima la conexión de proveedor de datos de panel de instrumentos que ha creado anteriormente.	Consulte la ayuda en línea de IBM Dashboard Application Services Hub y *Jazz for Service Management Integration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con conexiones de proveedor de datos.
	3. Mientras sigue conectado a IBM Dashboard Application Services Hub como usuario administrativo, cree la conexión de nuevo y esta vez especifique HTTPS como protocolo.	"Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring" en la página 52 Al crear la conexión, **no** seleccione el recuadro **Utilizar las credenciales del usuario (requiere la configuración de SSO)**.
	4. Inicie sesión en IBM Dashboard Application Services Hub como un usuario que tenga permiso para ver las páginas de panel de control y, a continuación, inicie la aplicación de paneles de control y verifique que los datos se visualizan.	Consulte la guía del usuario de la aplicación de paneles de control para obtener detalles sobre cómo iniciar y utilizar el panel de control. **Consejo:** Primero seleccione **Estado y salud del sistema** > **Panel de control Comprobaciones de salud** para verificar que el entorno funcione correctamente. A continuación, si está utilizando Infrastructure Management Dashboards for Servers, seleccione **Estado y salud del sistema** > **Paneles de control del servidor**. Para obtener más información sobre la utilización de Infrastructure Management Dashboards for Servers, consulte las guías del usuario del agente del sistema operativo.

Después de haber configurado el entorno de supervisión de panel de control básico, también puede que necesite realizar las tareas siguientes:

Tabla 2. Tareas adicionales necesarias para la configuración del entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario

Tarea	Dónde encontrar información
Cree definiciones de situación para los sucesos que supervisarán los usuarios del panel de control.	Consulte Situaciones para la supervisión de sucesos en *Tivoli Enterprise Portal: Guía del usuario* y también consulte *IBM Tivoli Monitoring: Consulta de mandatos* para obtener información sobre los mandatos **tacmd** que se utilizan para trabajar con situaciones.

Tabla 2. Tareas adicionales necesarias para la configuración del entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario (continuación)

Tarea	Dónde encontrar información
Cree grupos de sistemas gestionados que se puedan utilizar para agrupar sistemas gestionados para mostrarlos en las páginas de panel de control.	Consulte Gestión del entorno en *Tivoli Enterprise Portal: Guía del usuario* y también consulte *IBM Tivoli Monitoring: Consulta de mandatos* para obtener información sobre los mandatos **tacmd** que se utilizan para trabajar con listas de sistema.
Configure la colección de datos históricos si desea mostrar datos históricos en las páginas de panel de control. **Nota:** No todas las aplicaciones de paneles de control de supervisión dan soporte a la recuperación de datos históricos de Tivoli Data Warehouse.	Capítulo 17, "Gestión de datos históricos", en la página 481
Autorice el acceso de un nuevo usuario o grupo de usuarios a las páginas de panel de control en Dashboard Application Services Hub.	Consulte la *Jazz for Service Management Guía del administrador* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con roles que controlan el acceso a las páginas de paneles de control. **Consejo:** El método recomendado es crear un grupo de usuarios, añadir los usuarios al grupo y después asignarle al grupo un rol de Dashboard Application Services Hub que tenga permiso para ver las páginas de panel de control adecuadas.
Para cada usuario del panel de control que también utilizará el cliente de Tivoli Enterprise Portal, cree un ID de usuario de Tivoli Enterprise Portal y asígnele aplicaciones de supervisión y cualquier otro permiso que podría necesitar cuando utilice el cliente de portal.	"Administrar usuarios" en la página 164 y "Gestión de los ID de usuario" en la página 171
Cree páginas de panel de control personalizadas y asegúrese de que se asigna a los usuarios de paneles de control un rol de Dashboard Application Services Hub con permiso para ver las páginas personalizadas.	"Creación de páginas de panel de control personalizadas que muestran datos de supervisión" en la página 55

Tabla 2. Tareas adicionales necesarias para la configuración del entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario (continuación)

Tarea	Dónde encontrar información
Instale una nueva aplicación de panel de control de supervisión en Dashboard Application Services Hub, asigne las páginas de panel de control a un rol nuevo o existente, y asigne usuarios o grupos de usuarios al rol que controla el acceso a las páginas. Verifique que el usuario de Tivoli Enterprise Portal configurado para la conexión del proveedor de datos de panel de instrumentos tiene asignadas las aplicaciones de supervisión cuyos datos se mostrarán en la nueva aplicación de paneles de control y tiene asignado el permiso de vista para los sucesos si la aplicación de paneles de control muestra datos de sucesos de situación. **Nota:** El soporte de aplicaciones para el agente debe instalarse en el servidor de portal y el servidor de supervisión antes de poder ver los datos del agente en los nuevos paneles de control. Si el soporte de la aplicación se instala utilizando la función de agente de autodescripción, el servidor de portal se debe reiniciar para que el proveedor de datos de panel de instrumentos pueda utilizar el nuevo paquete de soporte.	Siga la documentación de instalación de aplicación de panel de control. A continuación, consulte la *Jazz for Service Management Guía del administrador* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con roles que controlan el acceso a las páginas de panel de control. Además, consulte "Administrar usuarios" en la página 164 para obtener detalles sobre cómo asignar aplicaciones de supervisión a un usuario de Tivoli Enterprise Portal. *IBM Tivoli Monitoring: Guía de instalación y configuración* incluye información sobre cómo instalar el soporte de aplicaciones.
Migre desde un entorno de panel de control básico a un entorno de panel de control con inicio de sesión único y por autorización de usuarios.	"Migración de un entorno de panel de control de supervisión básico a un entorno de panel de control con inicio de sesión único y controles de autorización por usuario" en la página 45
Determine si desea controlar las importaciones de UISolutions. (Las aplicaciones de paneles de control nuevas y actualizadas importan automáticamente sus definiciones de UISolutions al proveedor de datos de panel de instrumentos).	"Control de las importaciones de UISolutions" en la página 58

Configuración de un entorno de panel de control de supervisión con inicio de sesión único y con controles de autorización por usuario

Configure un entorno de paneles de control avanzado si desea utilizar IBM Dashboard Application Services Hub con aplicaciones de panel de control de supervisión como IBM Infrastructure Management Dashboards for Servers e IBM Infrastructure Management Dashboards for VMware o con paneles de control personalizados, que utilizan el inicio de sesión único y permisos que controlan los recursos de supervisión a los que un usuario puede acceder en los paneles de control.

Mediante la utilización del inicio de sesión único, los usuarios de IBM Dashboard Application Services Hub pueden lanzar el cliente del navegador de Tivoli Enterprise Portal sin entrar credenciales cuando se inicia el cliente del navegador del portal. Puede utilizar políticas de autorización o permisos de Tivoli Enterprise Portal para controlar los sistemas gestionados y grupos de sistemas gestionados a los que pueden acceder los usuarios individuales o miembros de grupos de usuarios en los paneles de control y si pueden visualizar sucesos de situación.

Para utilizar el inicio de sesión único, debe instalar y configurar un registro de usuarios LDAP que contendrá las credenciales de los usuarios que iniciarán sesión en IBM Dashboard Application Services Hub y el servidor de portal. A continuación, configure IBM Dashboard Application Services Hub y el servidor de portal para que utilicen el mismo registro de usuarios LDAP para autenticar los usuarios y para realizar el inicio de sesión único utilizando señales LTPA (Lightweight Third Party Authentication). También puede utilizar el mismo registro de usuarios LDAP para autenticar los usuarios de otras aplicaciones como WebGUI de Netcool/OMNIbus o Tivoli Business Service Manager si dichos usuarios van a iniciar el navegador del cliente de portal o Dashboard Application Services Hub.

A continuación, debe configurar una conexión de proveedor de datos de panel de control desde Dashboard Application Services Hub al servidor de portal e indicar que debe utilizarse el inicio de sesión único. Dashboard Application Services Hub utiliza una conexión HTTP o HTTPS al componente de proveedor de datos de panel de instrumentos del servidor de portal para recuperar datos de supervisión. Los datos de supervisión en tiempo real se recuperan del servidor de supervisión de hub y los agentes de supervisión y datos de supervisión históricos se recuperan de Tivoli Data Warehouse. No todas las aplicaciones de paneles de control de supervisión dan soporte a la recuperación de datos históricos de Tivoli Data Warehouse.

Dashboard Application Services Hub utiliza roles, para los usuarios o grupos de usuarios, para controlar las páginas a las que puede acceder un usuario. Sin embargo, proveedor de datos de panel de instrumentos lleva a cabo la autorización de los recursos de supervisión que se muestran en estas páginas. Tiene dos opciones para autorizar los recursos de supervisión a los que pueden acceder los usuarios de panel de control:

- Utilice el Servidor de políticas de autorización de Tivoli y la Interfaz de línea de mandatos tivcmd para la política de autorización para crear roles y permisos, que se denominan colectivamente políticas de autorización.

  Estas políticas de autorización controlan los sistemas gestionados y grupos de sistemas gestionados a los que puede acceder un usuario del panel de control. Se crean roles para las funciones de trabajo con permisos para ver determinados sistemas gestionados o grupos de sistemas gestionados. Los usuarios adquieren permisos basados en el rol (o roles) a los que pertenece el usuario. Los usuarios pueden asignarse a roles directamente o los grupos de usuarios de los que son miembro pueden asignarse a roles. Los permisos también especifican el tipo de objeto al que se puede acceder para un sistema gestionado o grupo de sistemas gestionados. Los tipos de objeto soportados son sucesos (para los sucesos de situación) y grupo de atributos (para la supervisión de datos recuperados de un agente).

  O BIEN
- Utilice permisos de autorización de Tivoli Enterprise Portal y asignaciones de aplicación supervisada para los usuarios del panel de control. Este es el método de autorización predeterminado si las políticas de autorización no están habilitados en la configuración del servidor de portal.

  Con esta opción, puede crear usuarios de Tivoli Enterprise Portal para cada uno de los usuarios del panel de control que utilizan el diálogo Administración de usuarios de Tivoli Enterprise Portal. Utilizando el mismo diálogo, puede otorgar permiso a un usuario para ver sucesos y asignar al usuario una o más aplicaciones supervisadas que se pueden ver. Estos pasos también se pueden realizar utilizando la CLI **tacmd**.

La autorización de Tivoli Enterprise Portal es menos granular que las políticas de autorización. Mientras que las políticas de autorización le permiten otorgar permiso a un usuario de panel de control para visualizar sólo determinados sistemas gestionados o miembros de grupos de sistemas gestionados específicos, la autorización de Tivoli Enterprise Portal está en el nivel de aplicación supervisada. Es decir, a un usuario se le asigna permiso para ver todos los sistemas gestionados de un tipo de aplicación de agente determinado, por ejemplo, todos los agentes del sistema operativo Windows.

Las políticas de autorización sólo controlan los recursos supervisados a los que se puede acceder en paneles de control de supervisión. Si los usuarios de panel control también van a utilizar el cliente de Tivoli Enterprise Portal, los permisos de Tivoli Enterprise Portal y las asignaciones de aplicación de agente van a controlar los recursos supervisados a los que se puede acceder en el cliente de portal. El conjunto de recursos supervisados que los usuarios pueden ver en los paneles de control pueden ser diferentes de los recursos supervisados que pueden ver en el cliente de Tivoli Enterprise Portal. Esto puede ocurrir si los permisos son incoherentes o si las políticas de autorización son más restrictivas.

Ejemplo de políticas de autorización más restrictivas

Supongamos que se otorga al usuario permiso para ver un subconjunto agentes del sistema operativo Windows en Dashboard Application Services Hub utilizando políticas de autorización y se asigna al usuario el tipo de aplicación del sistema operativo Windows en ss permisos de Tivoli Enterprise Portal. En este caso, el usuario solo verá los agentes del sistema operativo Windows autorizados en los paneles de control, pero verán todos los agentes del sistema operativo Windows cuando accedan al cliente de Tivoli Enterprise Portal.

Ejemplo de permisos incoherentes

Supongamos que se otorga al usuario permiso para ver un subconjunto de agentes del sistema operativo Windows en Dashboard Application Services Hub utilizando políticas de autorización pero el usuario no tiene asignado el tipo de aplicación del sistema operativo Windows en sus permisos de Tivoli Enterprise Portal. En este caso, el usuario verá los agentes del sistema operativo Windows autorizados en los paneles de control, pero no verán ningún agente del sistema operativo Windows cuando accedan al cliente de Tivoli Enterprise Portal.

Cuando esté configurando su entorno de panel de control y supervisión inicialmente, el método recomendado es que comience con permisos de Tivoli Enterprise Portal y asignaciones de aplicación supervisada. Después de que pueda ver los datos de supervisión en Dashboard Application Services Hub y de que los administradores hayan creado políticas de autorización, vuelva a configurar el servidor de portal si desea iniciar utilizando políticas de autorización.

Nota: Los permisos y políticas de autorización de Tivoli Enterprise Portal solo controlan el acceso a recursos supervisados en los paneles de control. No controlan el acceso a los recursos supervisados que aparecen en los informes utilizando Tivoli Common Reporting.

Requisitos previos

- Instale y configure el servidor de supervisión base de IBM Tivoli Monitoring, el servidor de portal y los componentes del cliente de portal utilizando las instrucciones de *IBM Tivoli Monitoring: Guía de instalación y configuración*. Al configurar el servidor de portal, habilite la proveedor de datos de panel de instrumentos.

- Instale y configure los agentes de supervisión cuyos datos se mostrarán en los paneles de control de supervisión. Instale el soporte de aplicaciones en los servidores de supervisión, el servidor de portal y el cliente de portal de escritorio si está siendo utilizado, utilizando las instrucciones de *IBM Tivoli Monitoring: Guía de instalación y configuración*.
- Instale y configure Dashboard Application Services Hub y las aplicaciones de supervisión de panel de control, consulte "Requisitos necesarios de software y memoria para un entorno de paneles de control" en *IBM Tivoli Monitoring: Guía de instalación y configuración*. Consulte también "Instalación y configuración de IBM Infrastructure Management Dashboards for Servers" en *IBM Tivoli Monitoring: Guía de instalación y configuración*, si va a instalar la aplicación de panel de control.
- Determine si va a utilizar políticas de autorización o la autorización de Tivoli Enterprise Portal para los usuarios de panel de control. Si piensa utilizar políticas de autorización, instale y configure el Servidor de políticas de autorización de Tivoli y los componentes de la Interfaz de línea de mandatos tivcmd para la política de autorización utilizando las instrucciones del tema "Instalación y configuración del Servidor de políticas de autorización de Tivoli y la interfaz de línea de mandatos tivcmd para la política de autorización" en *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Hoja de ruta

Utilice la siguiente hoja de ruta para ayudarle a empezar:

Tabla 3. Hoja de ruta para configurar un entorno de paneles de control de supervisión con inicio de sesión único y controles de autorización por usuario

Paso	Descripción	Dónde encontrar información
1 (obligatorio)	Configure un servidor LDAP como Tivoli Directory Server o Microsoft Active Directory para autenticar los usuarios de Dashboard Application Services Hub y del servidor de portal y añada sus usuarios a este registro.	Consulte "Requisitos previos para configurar la autenticación LDAP en el servidor de portal" en la página 95, a continuación, consulte la documentación para el servidor LDAP.
2 (obligatorio)	Asegúrese de que la hora está sincronizada con UTC en el servidor de portal y Dashboard Application Services Hub.	Para obtener más información y para planificar las consideraciones para utilizar el inicio de sesión único, consulte "Acerca del inicio de sesión único" en la página 98.

Tabla 3. Hoja de ruta para configurar un entorno de paneles de control de supervisión con inicio de sesión único y controles de autorización por usuario (continuación)

Paso	Descripción	Dónde encontrar información
3 (obligatorio)	Utilice la consola de administrador de WebSphere de IBM Dashboard Application Services Hub para configurar el servidor de aplicaciones de Dashboard Application Services Hub para que utilice el registro de usuarios LDAP para autenticar los usuarios y para habilitar el inicio de sesión único. **Nota:** Durante la configuración, especifique un nombre de reino y un nombre de dominio. Estos mismos valores deben especificarse al configurar el servidor de portal y cualquier otra aplicación que realice el inicio de sesión único con el servidor de portal o el servidor de paneles de control. • El nombre de dominio es el dominio de Internet o Intranet para el que SSO se ha configurado, por ejemplo, micompañía.com. Solo las aplicaciones disponibles en este dominio o sus subdominios se habilitan para SSO. • Un reino identifica un conjunto de repositorios federados utilizados por el servidor de portal y otros servidores de aplicaciones. Puede elegir su propio nombre de reino, pero el valor debe ser el mismo en todas las aplicaciones que se configuran para SSO dentro del dominio especificado.	Consulte *Jazz for Service Management Guía de configuración* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre la configuración de Jazz for Service Management para utilizar un registro de usuarios central, configurar SSO, configurar los valores de tiempo de espera de la señal LTPA y configurar una conexión TLS/SSL para el servidor LDAP.

Tabla 3. Hoja de ruta para configurar un entorno de paneles de control de supervisión con inicio de sesión único y controles de autorización por usuario (continuación)

Paso	Descripción	Dónde encontrar información
4 (obligatorio)	Configure el servidor de portal para que utilice un registro de usuarios LDAP y especifique el nombre de reino y de dominio utilizados para el inicio de sesión único. Para configurar el servidor de portal para que utilice LDAP, puede utilizar las siguientes opciones: • Programa de utilidad IBM Manage Tivoli Enterprise Monitoring Services • Interfaz de línea de mandatos **itmcmd** en Linux y UNIX • TEPS/e consola de administración Puede utilizar IBM Manage Tivoli Enterprise Monitoring Services o el mandato **itmcmd** para habilitar la validación de usuarios LDAP para el servidor de portal. También puede utilizar estos programas de utilidad para configurar los parámetros de conexión LDAP a menos que: • Desee utilizar un servidor además de Microsoft Active Directory o Tivoli Directory Server • Desee configurar TLS/SSL entre el servidor de portal y el servidor LDAP • Deba especificar parámetros de configuración LDAP avanzados En estos casos, debe especificar el tipo **Otro** al configurar el servidor de portal y, a continuación, utilizar la consola de administración de TEPS/e para completar la configuración de LDAP. **Nota:** También puede exportar la clave LTPA del servidor de portal o importar la clave LTPA de otra aplicación al mismo tiempo que configura la autenticación de usuarios LDAP o puede realizar estos pasos después de haber verificado que la autenticación LDAP del servidor de portal funciona.	Siga las instrucciones de uno de los temas siguientes para habilitar la validación de usuarios LDAP en el servidor de portal: • "Utilización de Manage Tivoli Enterprise Monitoring Services para configurar el servidor de portal para la autenticación de LDAP" en la página 104 • "Utilización de la línea de mandatos de Linux o UNIX para configurar el servidor de portal para la autenticación LDAP" en la página 108 A continuación, siga las instrucciones de "Utilización de la consola de administración de TEPS/e" en la página 110 si ha especificado el tipo de servidor LDAP **Otro** al habilitar la validación de usuarios LDAP para el servidor de portal. **Notas de uso:** Si está utilizando Microsoft Active Directory, consulte "Autenticación de usuarios de LDAP mediante Microsoft Active Directory" en la página 127 para obtener información sobre la planificación y la configuración específica para este tipo de servidor LDAP. Si está utilizando Tivoli Directory Server, consulte Descripción de inicio de sesión único entre IBM Tivoli Monitoring y Tivoli Integrated Portal utilizando Tivoli Directory Server en IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home). Estas instrucciones explican cómo correlacionar entradas configuradas en Tivoli Directory Server con la información configurada utilizando la TEPS/e consola de administración. Ignore los pasos proporcionados para Tivoli Integrated Portal.

Tabla 3. Hoja de ruta para configurar un entorno de paneles de control de supervisión con inicio de sesión único y controles de autorización por usuario (continuación)

Paso	Descripción	Dónde encontrar información
5 (obligatorio)	Inicie sesión en el cliente de Tivoli Enterprise Portal como sysadmin, a continuación, correlacione los ID de usuario de Tivoli Enterprise Portal existentes con los nombres distinguidos de LDAP excepto sysadmin. Si no tiene ningún ID de usuario de Tivoli Enterprise Portal además de `sysadmin`, cree un ID de usuario de Tivoli Enterprise Portal para al menos uno de los usuarios de LDAP y, cuando cree el ID de usuario, especifique el nombre distinguido de LDAP del usuario. Iniciará sesión como uno de los usuarios de LDAP en una tarea posterior para verificar que los datos pueden visualizarse en los paneles de control de supervisión. Utilice el cliente de Tivoli Enterprise Portal para asignar a este usuario las aplicaciones de supervisión que se visualizarán en los paneles de control y el permiso para ver sucesos si se visualizan datos de sucesos de situación en el panel de control.	Si tiene usuarios de Tivoli Enterprise Portal existentes, consulte "Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP" en la página 118. Si necesita crear un nuevo ID de usuario de Tivoli Enterprise Portal, consulte "Añadir ID de usuario" en la página 171. Consulte "Administrar usuarios" en la página 164 para ver los detalles sobre la asignación de aplicaciones de supervisión y permisos a usuarios de Tivoli Enterprise Portal. Consulte "Reconfiguración del cliente de navegador para SSO" en la página 120 si Dashboard Application Services Hub y el servidor de portal están en el mismo sistema.
6 (método recomendado opcional)	Verifique que puede iniciar sesión en el cliente de Tivoli Enterprise Portal como usuario DAP correlacionado con un ID de usuario de Tivoli Enterprise Portal.	N/D
7 (práctica recomendada opcional)	Configure una conexión TLS/SSL entre el servidor de portal y el servidor LDAP si desea asegurar esta comunicación.	"Configuración de la comunicación TLS/SSL entre el servidor de portal y el servidor LDAP" en la página 116
8 (práctica recomendada opcional)	Verifique que puede iniciar sesión en el cliente de Tivoli Enterprise Portal como usuario DAP correlacionado con un ID de usuario de Tivoli Enterprise Portal.	N/D
9 (obligatorio)	Debe asegurarse de que las aplicaciones siguientes están utilizando la misma clave LTPA que el servidor de portal: • Una aplicación basada en la web o habilitada para la web que inicia Tivoli Enterprise Portal • Una aplicación basada en la web o habilitada para la web que puede iniciarse desde el cliente de Tivoli Enterprise Portal • IBM Dashboard Application Services Hub • Otra aplicación como Tivoli Integrated Portal que utiliza el servicio web de representación gráfica IBM Tivoli Monitoring Determine qué aplicación será el origen de las claves LTPA para todas las demás aplicaciones SSO participantes y exporte sus claves LTPA. El archivo de claves y la contraseña utilizados para cifrar la clave deben proporcionarse a los administradores de las demás aplicaciones participantes.	Si decide que el servidor de portal será el origen de la clave LTPA, exporte su clave LTPA utilizando las instrucciones de exportación de "Importación y exportación de claves de LTPA" en la página 120. Si IBM Dashboard Application Services Hub será el origen de la clave LTPA, consulte "Exportación de claves LTPA" en *Jazz for Service Management Guía de configuración* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html). De lo contrario, consulte la documentación de la aplicación cuya clave LTPA se exportará para determinar cómo realizar la operación de exportación.

Tabla 3. Hoja de ruta para configurar un entorno de paneles de control de supervisión con inicio de sesión único y controles de autorización por usuario (continuación)

Paso	Descripción	Dónde encontrar información
10 (obligatorio)	Los administradores de las otras aplicaciones SSO participantes deben importar la clave LTPA que se ha exportado en el paso anterior. Necesitan el archivo de claves y la contraseña que se ha utilizado para cifrar la clave.	Para importar una clave LTPA al servidor de portal, consulte las instrucciones de importación en "Importación y exportación de claves de LTPA" en la página 120. Para importar una clave LTPA a IBM Dashboard Application Services Hub consulte el tema sobre "importación de claves LTPA" de *Jazz for Service Management Configuration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html). Consulte la documentación para las demás aplicaciones SSO participantes para obtener instrucciones sobre la importación de la clave LTPA.
11 (necesario)	Inicie sesión en IBM Dashboard Application Services Hub como usuario LDAP que también es usuario administrativo del concentrador de paneles de control y cree una conexión de proveedor de datos de panel de instrumentos.	"Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring" en la página 52 Al crear la conexión, marque el recuadro **Utilizar las credenciales del usuario (requiere configuración de SSO)**.
12 (obligatorio)	Después de iniciar sesión en IBM Dashboard Application Services Hub como usuario administrativo, cree un rol que controle el acceso a las páginas de la aplicación de paneles de control y asigne usuarios o grupos de usuarios de paneles de control al rol. **Nota:** Algunas aplicaciones de paneles de control como IBM Infrastructure Management for VMware crean automáticamente un rol para sus páginas cuando se instala la aplicación de paneles de control. Sin embargo, otras aplicaciones de paneles de control como IBM Infrastructure Management Dashboards for Servers no crean un rol durante la instalación por lo que debe crear uno o asignar las páginas de panel de control a un rol existente.	Consulte la *Jazz for Service Management Guía del administrador* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con roles que controlan el acceso a las páginas de paneles de control.

Tabla 3. Hoja de ruta para configurar un entorno de paneles de control de supervisión con inicio de sesión único y controles de autorización por usuario (continuación)

Paso	Descripción	Dónde encontrar información
13 (práctica recomendada opcional)	Inicie sesión en IBM Dashboard Application Services Hub como usuario LDAP con permiso para ver las páginas de panel de control y con ID de usuario de Tivoli Enterprise Portal que tenga asignada aplicaciones de supervisión y permisos para ver sucesos. A continuación, inicie las aplicaciones de panel de control y verifique que se visualicen los datos.	Consulte la guía del usuario de la aplicación de paneles de control para obtener detalles sobre cómo iniciar y utilizar el panel de control. **Consejo:** Primero seleccione **Estado y salud del sistema** > **Panel de control Comprobaciones de salud** para verificar que el entorno funcione correctamente. A continuación, si está utilizando Infrastructure Management Dashboards for Servers, seleccione **Estado y salud del sistema** > **Paneles de control del servidor**. Para obtener más información sobre la utilización de Infrastructure Management Dashboards for Servers, consulte las guías del usuario del agente del sistema operativo.
14 (práctica recomendada opcional)	Si desea utilizar HTTPS entre Dashboard Application Services Hub y proveedor de datos de panel de instrumentos, realice estas tareas:	
	1. Configure TLS/SSL entre el concentrador de paneles de control y el proveedor de datos.	"Configuración de la comunicación TLS/SSL entre Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos" en la página 219
	2. Inicie sesión en IBM Dashboard Application Services Hub como usuario administrativo al que se ha asignado los roles `administrador` e `iscadmins` y suprima la conexión de proveedor de datos de panel de instrumentos que ha creado anteriormente.	Consulte la ayuda en línea de IBM Dashboard Application Services Hub y *Jazz for Service Management Integration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con conexiones de proveedor de datos.
	3. Mientras sigue conectado a IBM Dashboard Application Services Hub como usuario administrativo, cree la conexión de nuevo y esta vez especifique HTTPS como protocolo.	"Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring" en la página 52 Al crear la conexión, marque el recuadro **Utilizar las credenciales del usuario (requiere configuración de SSO)**.
	4. Inicie sesión en IBM Dashboard Application Services Hub como un usuario que tenga permiso para ver las páginas de panel de control y, a continuación, inicie la aplicación de paneles de control y verifique que los datos se visualizan.	Consulte la guía del usuario de la aplicación de paneles de control para obtener detalles sobre cómo iniciar y utilizar el panel de control. **Consejo:** Primero seleccione **Estado y salud del sistema** > **Panel de control Comprobaciones de salud** para verificar que el entorno funcione correctamente. A continuación, si está utilizando Infrastructure Management Dashboards for Servers, seleccione **Estado y salud del sistema** > **Paneles de control del servidor**. Para obtener más información sobre la utilización de Infrastructure Management Dashboards for Servers, consulte las guías del usuario del agente del sistema operativo.

Tabla 3. Hoja de ruta para configurar un entorno de paneles de control de supervisión con inicio de sesión único y controles de autorización por usuario (continuación)

Paso	Descripción	Dónde encontrar información
15 (opcional)	Si desea utilizar políticas de autorización, realice estas tareas:	
	1. Utilice la CLI **tivcmd** para asignar administradores de políticas de autorización, asignar permiso a un usuario para distribuir políticas de autorización y crear políticas de autorización para controlar a qué recursos supervisados pueden acceder los usuarios de paneles de control. **Nota:** Después de haber verificado que puede utilizar la CLI **tivcmd** para iniciar sesión en el Servidor de políticas de autorización, configure TLS/SSL entre la CLI **tivcmd** y el Servidor de políticas de autorización de modo que los mandatos subsiguientes sean seguros.	"Preparación para habilitar las políticas de autorización" en la página 190 y"Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización" en la página 223
	2. Habilite la comprobación de política de autorización en el servidor de portal. **Nota:** Una vez que se realiza esta tarea, sólo los usuarios de panel de control a los que se ha asignado un rol de política de autorización podrán ver los recursos supervisados en los paneles de control.	"Habilitación de políticas de autorización en el servidor de portal" en la página 199
	3. Inicie sesión en IBM Dashboard Application Services Hub como un usuario de LDAP que tiene permiso para ver las páginas de panel de control y al que se ha asignado uno o más roles de políticas de autorización que dan permiso al usuario para ver datos de grupo de atributos, datos de sucesos de situación, o ambos, para los sistemas gestionados o grupos de sistemas gestionados que pueden visualizarse en las páginas de panel de control. Inicie las páginas de panel de control y verifique que el usuario sólo pueda ver los recursos supervisados para los que tiene autorización.	Consulte la guía del usuario de la aplicación de paneles de control para obtener detalles sobre cómo iniciar y utilizar el panel de control. **Consejo:** Primero seleccione **Estado y salud del sistema** > **Panel de control Comprobaciones de salud** para verificar que el entorno funcione correctamente. A continuación, si está utilizando Infrastructure Management Dashboards for Servers, seleccione **Estado y salud del sistema** > **Paneles de control del servidor**. Para obtener más información sobre la utilización de Infrastructure Management Dashboards for Servers, consulte las guías del usuario del agente del sistema operativo.
	4. Configure el servidor de portal para que utilice TLS/SSL al recuperar las políticas de autorización de Dashboard Application Services Hub donde el Servidor de políticas de autorización está instalado.	"Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización" en la página 223

Después de haber configurado el entorno de supervisión de panel de control avanzado, también puede que necesite realizar las tareas siguientes:

Tabla 4. Tareas adicionales necesarias para la configuración del entorno de supervisión avanzado con inicio de sesión único y con controles de autorización por usuario

Tarea	Dónde encontrar información
Cree definiciones de situación para los sucesos que supervisarán los usuarios del panel de control.	Consulte Situaciones para la supervisión de sucesos en *Tivoli Enterprise Portal: Guía del usuario* y también consulte *IBM Tivoli Monitoring: Consulta de mandatos* para obtener información sobre los mandatos **tacmd** que se utilizan para trabajar con situaciones.
Cree grupos de sistemas gestionados que se puedan utilizar para agrupar sistemas gestionados para mostrarlos en las páginas de panel de control.	Consulte Gestión del entorno en *Tivoli Enterprise Portal: Guía del usuario* y también consulte *IBM Tivoli Monitoring: Consulta de mandatos* para obtener información sobre los mandatos **tacmd** que se utilizan para trabajar con listas de sistema.
Configure la colección de datos históricos si desea mostrar datos históricos en las páginas de panel de control. **Nota:** No todas las aplicaciones de paneles de control de supervisión dan soporte a la recuperación de datos históricos de Tivoli Data Warehouse.	Capítulo 17, “Gestión de datos históricos”, en la página 481
Para cada nuevo usuario de panel de control: Asegúrese de que el usuario de panel de control tiene permiso para acceder a las páginas del panel de control con las que va a trabajar. Determine si el usuario puede añadirse a un grupo de LDAP existente que se asigna a un rol de Dashboard Application Services Hub. Si no hay un grupo de LDAP existente al que se pueda asignar el usuario, realice una de las tareas siguientes: • El método recomendado es crear un grupo de LDAP nuevo, añadir el usuario al grupo y, a continuación, asignar el grupo a un rol de Dashboard Application Services Hub que tenga permiso para ver las páginas de panel de control adecuadas. O BIEN • Asignar el usuario de panel de control directamente a un rol de Dashboard Application Services Hub que tenga permiso para ver las páginas de panel de control adecuadas.	Consulte la *Jazz for Service Management Guía del administrador* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con roles que controlan el acceso a las páginas de paneles de control. Consulte la documentación del servidor LDAP para obtener información detallada sobre la adición de usuarios a grupos de LDAP.

Tabla 4. Tareas adicionales necesarias para la configuración del entorno de supervisión avanzado con inicio de sesión único y con controles de autorización por usuario (continuación)

Tarea	Dónde encontrar información
Para cada nuevo usuario de panel de control: Si se están utilizando políticas de autorización, asegúrese de que el usuario de panel de control se asigne a uno o varios roles de políticas de autorización que dan al usuario permiso para ver datos de grupo de atributos, datos de sucesos de situación, o ambos para los sistemas gestionados o grupos de sistemas gestionados que van a supervisar. Determine si el usuario puede añadirse a un grupo de LDAP existente que ya tenga asignados roles de política de autorización con los permisos necesarios. Si el usuario no se puede añadir a un grupo de LDAP existente, realice una de las tareas siguientes: • El método recomendado es crear un nuevo grupo de LDAP, añadir el usuario al grupo y, a continuación, asignar el grupo a los roles de política de autorización. O BIEN • Asignar el usuario de panel de control directamente a los roles de política de autorización.	Consulte la documentación del servidor LDAP para obtener información detallada sobre la adición de usuarios a grupos de LDAP. Consulte el capítulo "Escenarios de gestión de políticas" en la página 192 y *IBM Tivoli Monitoring: Consulta de mandatos* en la CLI **tivcmd** para obtener detalles sobre la creación y el trabajo con políticas de autorización.

Tabla 4. Tareas adicionales necesarias para la configuración del entorno de supervisión avanzado con inicio de sesión único y con controles de autorización por usuario (continuación)

Tarea	Dónde encontrar información
Para cada nuevo usuario de panel de control: Si se está utilizando la autorización de Tivoli Enterprise Portal para controlar que los recursos supervisados se puedan acceder en los paneles de control, o si el nuevo usuario de paneles de control utilizará el cliente de Tivoli Enterprise Portal, asegúrese de que el usuario de Tivoli Enterprise Portal tiene el permiso correcto. Primero asegúrese de que haya un ID de usuario de Tivoli Enterprise Portal correlacionado con el nombre distinguido de LDAP del usuario de panel de control. A continuación, determine si el usuario de Tivoli Enterprise Portal debe estar asignado a un grupo existente de Tivoli Enterprise Portal que tenga asignados los permisos y las aplicaciones de supervisión requeridos por el nuevo usuario de panel de control. Si no hay un grupo existente que pueda utilizarse, complete una de las siguientes tareas: • El método recomendado es crear un grupo nuevo de Tivoli Enterprise Portal, añadir el usuario al grupo y asignar al grupo los permisos y tipos de aplicación apropiados. • Asigne al usuario de Tivoli Enterprise Portal los permisos adecuados y las aplicaciones de supervisión directamente. Si un usuario de panel de control no va a utilizar el cliente de Tivoli Enterprise Portal, solo necesita permiso para ver sucesos y se le deben asignar las aplicaciones de supervisión que va a supervisar en las páginas de panel de control. Por ejemplo, si el usuario del panel de control va a utilizar Infrastructure Management Dashboards for Servers, debe tener asignado uno o más de estos tipos de aplicación: sistema operativo Linux, sistema operativo UNIX o sistema operativo Windows. Si el usuario de panel de control también va a utilizar el cliente de Tivoli Enterprise Portal, podría necesitar permisos adicionales.	Consulte "Gestión de los ID de usuario" en la página 171 para obtener detalles sobre la creación de nuevos ID de usuario de Tivoli Enterprise Portal. Consulte "Gestión de grupos de usuarios" en la página 175 para obtener detalles sobre la adición de grupos de ID de usuario de Tivoli Enterprise Portal. Consulte "Administrar usuarios" en la página 164 para obtener detalles sobre la asignación de aplicaciones de supervisión y permisos a usuarios y grupos de Tivoli Enterprise Portal.
Cree páginas de panel de control personalizadas y asegúrese de que se asigna a los usuarios de paneles de control un rol de Dashboard Application Services Hub con permiso para ver las páginas personalizadas.	"Creación de páginas de panel de control personalizadas que muestran datos de supervisión" en la página 55

Tabla 4. Tareas adicionales necesarias para la configuración del entorno de supervisión avanzado con inicio de sesión único y con controles de autorización por usuario (continuación)

Tarea	Dónde encontrar información
Instale una aplicación de panel de control de supervisión nueva en Dashboard Application Services Hub, asigne las páginas del panel de control a un rol nuevo o existente, y asigne usuarios de LDAP o grupos de usuarios al rol que controla el acceso a las páginas. **Nota:** Algunas aplicaciones de panel de control crean automáticamente un rol para sus páginas cuando se instala la aplicación de paneles de control. Si se están utilizando políticas de autorización, asegúrese de que los usuarios de panel de control que tienen acceso a las páginas nuevas se asignen a uno o varios roles de políticas de autorización que dan a los usuarios permiso para ver datos de grupo de atributos, datos de sucesos de situación, o ambos para los sistemas gestionados o grupos de sistemas gestionados que van a supervisar utilizando la aplicación de panel de control nueva. Asigne al usuario del panel de control el ID de usuario de Tivoli Enterprise Portal o agrupe las aplicaciones de supervisión que se visualizarán en la nueva aplicación de paneles de control, si el usuario de paneles de control también va a utilizar el cliente de Tivoli Enterprise Portal o si también se utiliza la autorización de Tivoli Enterprise Portal en lugar de políticas de autorización. **Nota:** El soporte de aplicaciones para el agente debe instalarse en el servidor de portal y el servidor de supervisión antes de poder ver los datos del agente en los nuevos paneles de control. Si el soporte de la aplicación se instala utilizando la función de agente de autodescripción, el servidor de portal se debe reiniciar para que el proveedor de datos de panel de instrumentos pueda utilizar el nuevo paquete de soporte.	Siga la documentación de instalación de la aplicación de panel de control. A continuación, consulte la *Jazz for Service Management Guía del administrador* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con roles que controlan el acceso a las páginas de panel de control. Consulte el capítulo Capítulo 7, "Utilización de políticas de autorización basadas en roles", en la página 185 y *IBM Tivoli Monitoring: Consulta de mandatos* en la CLI **tivcmd** para obtener detalles sobre la creación y el trabajo con políticas de autorización. Además, consulte "Administrar usuarios" en la página 164 para obtener detalles sobre cómo asignar aplicaciones de agente a un usuario de Tivoli Enterprise Portal. *IBM Tivoli Monitoring: Guía de instalación y configuración* incluye información sobre cómo instalar el soporte de aplicaciones.
Determine si desea controlar las importaciones de UISolutions. (Las aplicaciones de paneles de control nuevas y actualizadas importan automáticamente sus definiciones de UISolutions al proveedor de datos de panel de instrumentos).	"Control de las importaciones de UISolutions" en la página 58

Migración de un entorno de panel de control de supervisión básico a un entorno de panel de control con inicio de sesión único y controles de autorización por usuario

Migre el entorno de paneles de control básico a un entorno de paneles de control avanzado.

Después de configurar un entorno de supervisión básico tal como se describe en "Configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario" en la página 27, puede migrar a un entorno de paneles de control avanzado con inicio de sesión único.

Hoja de ruta

Utilice la siguiente hoja de ruta para ayudarle a empezar:

Tabla 5. Hoja de ruta para migrar a un entorno de paneles de control avanzado

Paso	Descripción	Dónde encontrar información
1 (obligatorio)	Configure un servidor LDAP como Tivoli Directory Server o Microsoft Active Directory para autenticar los usuarios de Dashboard Application Services Hub y del servidor de portal y añada sus usuarios a este registro.	Consulte "Requisitos previos para configurar la autenticación LDAP en el servidor de portal" en la página 95, a continuación, consulte la documentación para el servidor LDAP.
2 (obligatorio)	Asegúrese de que la hora está sincronizada con UTC en el servidor de portal y Dashboard Application Services Hub.	Para obtener más información y para planificar las consideraciones para utilizar el inicio de sesión único, consulte "Acerca del inicio de sesión único" en la página 98.
3 (obligatorio)	Utilice la consola de administrador de WebSphere de IBM Dashboard Application Services Hub para configurar el servidor de aplicaciones de Dashboard Application Services Hub para que utilice el registro de usuarios LDAP para autenticar los usuarios y para habilitar el inicio de sesión único. **Nota:** Durante la configuración, especifique un nombre de reino y un nombre de dominio. Estos mismos valores deben especificarse al configurar el servidor de portal y cualquier otra aplicación que realice el inicio de sesión único con el servidor de portal o el servidor de paneles de control. • El nombre de dominio es el dominio de Internet o Intranet para el que SSO se ha configurado, por ejemplo, micompañía.com. Solo las aplicaciones disponibles en este dominio o sus subdominios se habilitan para SSO. • Un reino identifica un conjunto de repositorios federados utilizados por el servidor de portal y otros servidores de aplicaciones. Puede elegir su propio nombre de reino, pero el valor debe ser el mismo en todas las aplicaciones que se configuran para SSO dentro del dominio especificado.	Consulte *Jazz for Service Management Guía de configuración* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre la configuración de Jazz for Service Management para utilizar un registro de usuarios central, configurar SSO, configurar los valores de tiempo de espera de la señal LTPA y configurar una conexión TLS/SSL para el servidor LDAP.

Tabla 5. Hoja de ruta para migrar a un entorno de paneles de control avanzado (continuación)

Paso	Descripción	Dónde encontrar información
4 (obligatorio)	Configure el servidor de portal para que utilice un registro de usuarios LDAP y especifique el nombre de reino y de dominio utilizados para el inicio de sesión único. Para configurar el servidor de portal para que utilice LDAP, puede utilizar las siguientes opciones: • Programa de utilidad IBM Manage Tivoli Enterprise Monitoring Services • Interfaz de línea de mandatos **itmcmd** en Linux y UNIX • TEPS/e consola de administración Puede utilizar IBM Manage Tivoli Enterprise Monitoring Services o el mandato **itmcmd** para habilitar la validación de usuarios LDAP para el servidor de portal. También puede utilizar estos programas de utilidad para configurar los parámetros de conexión LDAP a menos que: • Desee utilizar un servidor además de Microsoft Active Directory o Tivoli Directory Server • Desee configurar TLS/SSL entre el servidor de portal y el servidor LDAP • Deba especificar parámetros de configuración LDAP avanzados En estos casos, debe especificar el tipo **Otro** al configurar el servidor de portal y, a continuación, utilizar la consola de administración de TEPS/e para completar la configuración de LDAP. **Nota:** También puede exportar la clave LTPA del servidor de portal o importar la clave LTPA de otra aplicación al mismo tiempo que configura la autenticación de usuarios LDAP o puede realizar estos pasos después de haber verificado que la autenticación LDAP del servidor de portal funciona.	Siga las instrucciones de uno de los temas siguientes para habilitar la validación de usuarios LDAP en el servidor de portal: • "Utilización de Manage Tivoli Enterprise Monitoring Services para configurar el servidor de portal para la autenticación de LDAP" en la página 104 • "Utilización de la línea de mandatos de Linux o UNIX para configurar el servidor de portal para la autenticación LDAP" en la página 108 A continuación, siga las instrucciones de "Utilización de la consola de administración de TEPS/e" en la página 110 si ha especificado el tipo de servidor LDAP **Otro** al habilitar la validación de usuarios LDAP para el servidor de portal. **Notas de uso:** Si está utilizando Microsoft Active Directory, consulte "Autenticación de usuarios de LDAP mediante Microsoft Active Directory" en la página 127 para obtener información sobre la planificación y la configuración específica para este tipo de servidor LDAP. Si está utilizando Tivoli Directory Server, consulte Descripción de inicio de sesión único entre IBM Tivoli Monitoring y Tivoli Integrated Portal utilizando Tivoli Directory Server en IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home). Estas instrucciones explican cómo correlacionar entradas configuradas en Tivoli Directory Server con la información configurada utilizando la TEPS/e consola de administración. Ignore los pasos proporcionados para Tivoli Integrated Portal.

Tabla 5. Hoja de ruta para migrar a un entorno de paneles de control avanzado (continuación)

Paso	Descripción	Dónde encontrar información
5 (obligatorio)	Inicie sesión en el cliente de Tivoli Enterprise Portal como sysadmin, a continuación, correlacione los ID de usuario de Tivoli Enterprise Portal existentes con los nombres distinguidos de LDAP excepto sysadmin. Si no tiene ningún ID de usuario de Tivoli Enterprise Portal además de `sysadmin`, cree un ID de usuario de Tivoli Enterprise Portal para al menos uno de los usuarios de LDAP y, cuando cree el ID de usuario, especifique el nombre distinguido de LDAP del usuario. Iniciará sesión como uno de los usuarios de LDAP en una tarea posterior para verificar que los datos pueden visualizarse en los paneles de control de supervisión. Utilice el cliente de Tivoli Enterprise Portal para asignar a este usuario las aplicaciones de supervisión que se visualizarán en los paneles de control y el permiso para ver sucesos si se visualizan datos de sucesos de situación en el panel de control.	Si tiene usuarios de Tivoli Enterprise Portal existentes, consulte "Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP" en la página 118. Si necesita crear un nuevo ID de usuario de Tivoli Enterprise Portal, consulte "Añadir ID de usuario" en la página 171. Consulte "Administrar usuarios" en la página 164 para ver los detalles sobre la asignación de aplicaciones de supervisión y permisos a usuarios de Tivoli Enterprise Portal. Consulte "Reconfiguración del cliente de navegador para SSO" en la página 120 si Dashboard Application Services Hub y el servidor de portal están en el mismo sistema.
6 (método recomendado opcional)	Verifique que puede iniciar sesión en el cliente de Tivoli Enterprise Portal como usuario DAP correlacionado con un ID de usuario de Tivoli Enterprise Portal.	N/D
7 (práctica recomendada opcional)	Configure una conexión TLS/SSL entre el servidor de portal y el servidor LDAP si desea asegurar esta comunicación.	"Configuración de la comunicación TLS/SSL entre el servidor de portal y el servidor LDAP" en la página 116
8 (práctica recomendada opcional)	Verifique que puede iniciar sesión en el cliente de Tivoli Enterprise Portal como usuario DAP correlacionado con un ID de usuario de Tivoli Enterprise Portal.	N/D
9 (obligatorio)	Debe asegurarse de que las aplicaciones siguientes están utilizando la misma clave LTPA que el servidor de portal: • Una aplicación basada en la web o habilitada para la web que inicia Tivoli Enterprise Portal • Una aplicación basada en la web o habilitada para la web que puede iniciarse desde el cliente de Tivoli Enterprise Portal • IBM Dashboard Application Services Hub • Otra aplicación como Tivoli Integrated Portal que utiliza el servicio web de representación gráfica IBM Tivoli Monitoring Determine qué aplicación será el origen de las claves LTPA para todas las demás aplicaciones SSO participantes y exporte sus claves LTPA. El archivo de claves y la contraseña utilizados para cifrar la clave deben proporcionarse a los administradores de las demás aplicaciones participantes.	Si decide que el servidor de portal será el origen de la clave LTPA, exporte su clave LTPA utilizando las instrucciones de exportación de "Importación y exportación de claves de LTPA" en la página 120. Si IBM Dashboard Application Services Hub será el origen de la clave LTPA, consulte "Exportación de claves LTPA" en *Jazz for Service Management Guía de configuración* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html). De lo contrario, consulte la documentación de la aplicación cuya clave LTPA se exportará para determinar cómo realizar la operación de exportación.

Tabla 5. Hoja de ruta para migrar a un entorno de paneles de control avanzado (continuación)

Paso	Descripción	Dónde encontrar información
10 (obligatorio)	Los administradores de las otras aplicaciones SSO participantes deben importar la clave LTPA que se ha exportado en el paso anterior. Necesitan el archivo de claves y la contraseña que se ha utilizado para cifrar la clave.	Para importar una clave LTPA al servidor de portal, consulte las instrucciones de importación en "Importación y exportación de claves de LTPA" en la página 120. Para importar una clave LTPA a IBM Dashboard Application Services Hub consulte el tema sobre "importación de claves LTPA" de *Jazz for Service Management Configuration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html). Consulte la documentación para las demás aplicaciones SSO participantes para obtener instrucciones sobre la importación de la clave LTPA.
11 (necesario)	Inicie sesión en IBM Dashboard Application Services Hub como un usuario LDAP que también es un usuario administrativo del concentrador de paneles de control y **suprima** la conexión existente del proveedor de datos de panel de instrumentos. A continuación, **cree una nueva** conexión del proveedor de datos de panel de instrumentos que soporte el inicio de sesión único.	"Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring" en la página 52 Al crear la conexión, marque el recuadro **Utilizar las credenciales del usuario (requiere configuración de SSO)**.
12 (práctica recomendada opcional)	Inicie sesión en IBM Dashboard Application Services Hub como usuario LDAP con permiso para ver las páginas de panel de control y con ID de usuario de Tivoli Enterprise Portal que tenga asignada aplicaciones de supervisión y permisos para ver sucesos. A continuación, inicie las aplicaciones de panel de control y verifique que se visualicen los datos.	Consulte la guía del usuario de la aplicación de paneles de control para obtener detalles sobre cómo iniciar y utilizar el panel de control. **Consejo:** Primero seleccione **Estado y salud del sistema** > **Panel de control Comprobaciones de salud** para verificar que el entorno funcione correctamente. A continuación, si está utilizando Infrastructure Management Dashboards for Servers, seleccione **Estado y salud del sistema** > **Paneles de control del servidor**. Para obtener más información sobre la utilización de Infrastructure Management Dashboards for Servers, consulte las guías del usuario del agente del sistema operativo.

Tabla 5. Hoja de ruta para migrar a un entorno de paneles de control avanzado (continuación)

Paso	Descripción	Dónde encontrar información
13 (práctica recomendada opcional)	Si **no** ha configurado HTTPS entre Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos, realice estas tareas.	
	1. Configure TLS/SSL entre el concentrador de paneles de control y el proveedor de datos.	"Configuración de la comunicación TLS/SSL entre Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos" en la página 219
	2. Inicie sesión en IBM Dashboard Application Services Hub como usuario administrativo al que se ha asignado los roles `administrador` e `iscadmins` y suprima la conexión de proveedor de datos de panel de instrumentos que ha creado anteriormente.	Consulte la ayuda en línea de IBM Dashboard Application Services Hub y *Jazz for Service Management Integration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener detalles sobre cómo trabajar con conexiones de proveedor de datos.
	3. Mientras sigue conectado a IBM Dashboard Application Services Hub como usuario administrativo, cree la conexión de nuevo y esta vez especifique HTTPS como protocolo.	"Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring" en la página 52 Al crear la conexión, marque el recuadro **Utilizar las credenciales del usuario (requiere configuración de SSO)**.
	4. Inicie sesión en IBM Dashboard Application Services Hub como un usuario que tenga permiso para ver las páginas de panel de control y, a continuación, inicie la aplicación de paneles de control y verifique que los datos se visualizan.	Consulte la guía del usuario de la aplicación de paneles de control para obtener detalles sobre cómo iniciar y utilizar el panel de control. **Consejo:** Primero seleccione **Estado y salud del sistema** > **Panel de control Comprobaciones de salud** para verificar que el entorno funcione correctamente. A continuación, si está utilizando Infrastructure Management Dashboards for Servers, seleccione **Estado y salud del sistema** > **Paneles de control del servidor**. Para obtener más información sobre la utilización de Infrastructure Management Dashboards for Servers, consulte las guías del usuario del agente del sistema operativo.

Tabla 5. Hoja de ruta para migrar a un entorno de paneles de control avanzado (continuación)

Paso	Descripción	Dónde encontrar información
14 (opcional)	Cree políticas de autorización y habilite la comprobación de políticas de autorización si desea el control basado en rol en lugar de los permisos de Tivoli Enterprise Portal y la asignación de aplicaciones de supervisión.	
	1. Utilice la CLI **tivcmd** para asignar administradores de políticas de autorización, asignar permiso a un usuario para distribuir políticas de autorización y crear políticas de autorización para controlar a qué recursos supervisados pueden acceder los usuarios de paneles de control. **Nota:** Después de haber verificado que puede utilizar la CLI **tivcmd** para iniciar sesión en el Servidor de políticas de autorización, configure TLS/SSL entre la CLI **tivcmd** y el Servidor de políticas de autorización de modo que los mandatos subsiguientes sean seguros.	"Preparación para habilitar las políticas de autorización" en la página 190 y"Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización" en la página 223
	2. Habilite la comprobación de política de autorización en el servidor de portal. **Nota:** Una vez que se realiza esta tarea, sólo los usuarios de panel de control a los que se ha asignado un rol de política de autorización podrán ver los recursos supervisados en los paneles de control.	"Habilitación de políticas de autorización en el servidor de portal" en la página 199
	3. Inicie sesión en IBM Dashboard Application Services Hub como un usuario de LDAP que tiene permiso para ver las páginas de panel de control y al que se ha asignado uno o más roles de políticas de autorización que dan permiso al usuario para ver datos de grupo de atributos, datos de sucesos de situación, o ambos, para los sistemas gestionados o grupos de sistemas gestionados que pueden visualizarse en las páginas de panel de control. Inicie las páginas de panel de control y verifique que el usuario sólo pueda ver los recursos supervisados para los que tiene autorización.	Consulte la guía del usuario de la aplicación de paneles de control para obtener detalles sobre cómo iniciar y utilizar el panel de control. **Consejo:** Primero seleccione **Estado y salud del sistema** > **Panel de control Comprobaciones de salud** para verificar que el entorno funcione correctamente. A continuación, si está utilizando Infrastructure Management Dashboards for Servers, seleccione **Estado y salud del sistema** > **Paneles de control del servidor**. Para obtener más información sobre la utilización de Infrastructure Management Dashboards for Servers, consulte las guías del usuario del agente del sistema operativo.
	4. Configure el servidor de portal para que utilice TLS/SSL al recuperar las políticas de autorización de Dashboard Application Services Hub donde el Servidor de políticas de autorización está instalado.	"Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización" en la página 223

Tabla 5. Hoja de ruta para migrar a un entorno de paneles de control avanzado (continuación)

Paso	Descripción	Dónde encontrar información
15 (opcional)	Para cada nuevo usuario de panel de control: Si se está utilizando la autorización de Tivoli Enterprise Portal para controlar que los recursos supervisados se puedan acceder en los paneles de control, o si el nuevo usuario de paneles de control utilizará el cliente de Tivoli Enterprise Portal, asegúrese de que el usuario de Tivoli Enterprise Portal tiene el permiso correcto. Primero asegúrese de que haya un ID de usuario de Tivoli Enterprise Portal correlacionado con el nombre distinguido de LDAP del usuario de panel de control. A continuación, determine si el usuario de Tivoli Enterprise Portal debe estar asignado a un grupo existente de Tivoli Enterprise Portal que tenga asignados los permisos y las aplicaciones de supervisión requeridos por el nuevo usuario de panel de control. Si no hay un grupo existente que pueda utilizarse, complete una de las siguientes tareas: • El método recomendado es crear un grupo nuevo de Tivoli Enterprise Portal, añadir el usuario al grupo y asignar al grupo los permisos y tipos de aplicación apropiados. • Asigne al usuario de Tivoli Enterprise Portal los permisos adecuados y las aplicaciones de supervisión directamente. Si un usuario de panel de control no va a utilizar el cliente de Tivoli Enterprise Portal, solo necesita permiso para ver sucesos y se le deben asignar las aplicaciones de supervisión que va a supervisar en las páginas de panel de control. Por ejemplo, si el usuario del panel de control va a utilizar Infrastructure Management Dashboards for Servers, debe tener asignado uno o más de estos tipos de aplicación: sistema operativo Linux, sistema operativo UNIX o sistema operativo Windows. Si el usuario de panel de control también va a utilizar el cliente de Tivoli Enterprise Portal, podría necesitar permisos adicionales.	Consulte “Gestión de los ID de usuario” en la página 171 para obtener detalles sobre la creación de nuevos ID de usuario de Tivoli Enterprise Portal. Consulte “Gestión de grupos de usuarios” en la página 175 para obtener detalles sobre la adición de grupos de ID de usuario de Tivoli Enterprise Portal. Consulte “Administrar usuarios” en la página 164 para obtener detalles sobre la asignación de aplicaciones de supervisión y permisos a usuarios y grupos de Tivoli Enterprise Portal.

Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring

Para recuperar métricas sobre los sistemas gestionados y los sucesos de situación de la aplicación de paneles de control de supervisión en IBM Dashboard Application Services Hub como IBM Infrastructure Management Dashboards for Servers o IBM Infrastructure Management Dashboards for VMwar o en paneles de instrumentos personalizados, primero debe tener una conexión establecida con el IBM Tivoli Monitoring proveedor de datos de panel de instrumentos que está en Tivoli Enterprise Portal Server.

Este procedimiento de conexión no lo necesita repetir a menos que la configuración del servidor de portal cambie.

Antes de empezar

Las conexiones se definen en la consola de Dashboard Application Services Hub. Antes de crear la conexión, debe asegurarse de que los pasos siguientes ya se hayan llevado a cabo:

- Asegúrese de que proveedor de datos de panel de instrumentos está habilitado en la configuración de servidor de portal. Consulte "Verificación de que el proveedor de datos de panel de control está habilitado" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

  Si el entorno de IBM Tivoli Monitoring está configurado para espera activa, debe configurar un valor de alteración temporal de dominio para el proveedor de datos de panel de instrumentos en la configuración de servidor de portal antes de crear una conexión al proveedor de datos de panel de instrumentos. El valor de alteración temporal de dominio garantiza que el valor de ID de conexión de proveedor de datos no cambia cuando se reconfigura el servidor de portal para conectar al servidor de supervisión concentrador en espera.
- Debe iniciar sesión en Dashboard Application Services Hub como un usuario al que se le han asignado los roles `administrador` e `iscadmins` de Dashboard Application Services Hub. Estos roles son necesarios para crear y gestionar conexiones. Para obtener información sobre la asignación de estos roles a los usuarios, consulte la publicación *Jazz for Service Management Administrator's Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html).

  Si tiene previsto utilizar el inicio de sesión único, también debe haber iniciado sesión en Dashboard Application Services Hub como un usuario que sea miembro del registro de usuarios de LDAP federado compartido por el servidor de concentrador de panel de control y el servidor de portal cuando crea la conexión.Para ver los pasos adicionales que debe realizar antes de crear una conexión de proveedor de datos que utiliza el inicio de sesión único, consulte "Configuración de un entorno de panel de control de supervisión con inicio de sesión único y con controles de autorización por usuario" en la página 32.
- Para definir una conexión con el proveedor de datos de panel de instrumentos, debe saber qué protocolo de red se necesita, el nombre de host y el número de puerto para el servidor de portal, las credenciales para autenticarse en el servidor de portal y si debe utilizarse el inicio de sesión único.
- Si piensa utilizar HTTPS como la conexión de protocolo, debe configurar TLS/SSL entre Dashboard Application Services Hub y el servidor de portal antes de crear la conexión de proveedor de datos. Para obtener más información, consulte "Configuración de la comunicación TLS/SSL entre Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos" en la página 219.

  Consejo: Puede crear la conexión con el protocolo HTTP para la prueba inicial. Una vez que el entorno esté funcionando, puede configurar TLS/SSL entre los servidores, suprimir la conexión y volver a añadirla con el protocolo HTTPS.

Procedimiento

1. En la consola de Dashboard Application Services Hub, pulse **Valores de la consola** y seleccione **Conexiones** (en **General**).
2. Pulse **Crear nuevo proveedor remoto**. Se muestran los campos para especificar la conexión al proveedor de datos de panel de instrumentos.

3. En el campo **Protocolo**, seleccione el protocolo de aplicación para la conexión al servidor de portal: `HTTP`, `HTTPS-SSL` (capa de sockets seguros) o `HTTPS-TLS` (seguridad de capa de transporte).
4. Pulse en el campo **Nombre de host** y especifique la dirección IP o el nombre completo del sistema del servidor de portal.
5. Pulse en el campo **Puerto** y especifique el número de puerto de la aplicación eWAS del servidor de portal: 15200 para HTTP o 15201 para HTTPS.
6. Si la configuración tiene un cortafuegos entre el servidor de Dashboard Application Services Hub y el servidor de portal, marque el recuadro de selección **La conexión atraviesa un cortafuegos** y escriba el nombre de host completo y el número de puerto (el puerto predeterminado es 16324) del sistema donde está instalado Dashboard Application Services Hub.
7. En los campos **Nombre** y **Contraseña**, especifique un nombre de usuario y contraseña que pueda autenticarse con el servidor de portal.

   Si está configurando un entorno de panel de control básico sin inicio de sesión único ni autorización por usuario, especifique un usuario al que se le haya otorgado la autorización de Tivoli Enterprise Portal que se describe en la primera tabla en "Configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario" en la página 27. Este usuario se utilizará para crear la conexión y enviar todas las solicitudes posteriores a proveedor de datos de panel de instrumentos en nombre de los usuarios del panel de control.

   Si está configurando un entorno de panel de control con el inicio de sesión único y autorización por usuario, escriba su nombre de usuario y contraseña. El nombre de usuario y la contraseña se utilizarán para enviar la solicitud al servidor de portal para obtener la lista de proveedores de datos disponibles en el servidor de portal. Después de este punto, todas las solicitudes posteriores al proveedor de datos incluirán el nombre del usuario que ha iniciado sesión en Dashboard Application Services Hub.
8. Pulse **Buscar** para llenar la tabla con los proveedores de datos que están en el servidor de portal.
9. Pulse el botón de selección del proveedor de datos de panel de instrumentos para seleccionarlo y complete los demás campos.
10. Edite las entradas en los campos siguientes:
    - **Nombre** es el mismo que el nombre de proveedor de datos original.Puede dejar esto como está.
    - **Descripción** es la misma que la descripción de proveedor de datos original. Puede dejar esto como está.
    - **ID de proveedor** es, de forma predeterminada, inicialmente `itm.`*`nombre_servidor_supervisión_concentrador.nombre_host_servidor_portal`* para conexiones de proveedor de datos del panel de control. Si se ha configurado un valor de alteración temporal de dominio durante la configuración de servidor de portal, el valor de alteración temporal sustituye la parte *hub_monitoring_server_name* de la cadena de ID original.

      Debe cambiar el ID de proveedor a `ITMSD` si utiliza una de las aplicaciones siguientes:
      – IBM Infrastructure Management Dashboards for Servers proporcionados con IBM Tivoli Monitoring
      – IBM Infrastructure Management Dashboards for VMware
      – IBM Infrastructure Management Capacity Planner for VMware
      – IBM Infrastructure Management Capacity Planner for PowerVM

Si no utiliza ninguna de las aplicaciones de panel de control listadas más arriba, pero ha instalado aplicaciones de panel de control para otros agentes de supervisión, consulte la documentación para esos agentes para determinar si sus paneles de control requieren que utilice `ITMSD`. Si no utiliza una de las aplicaciones de panel de control mencionadas anteriormente, pero es posible que lo haga en el futuro, o si no está seguro de qué ID de proveedor debe utilizar, la práctica recomendada es utilizar `ITMSD`.

11. Seleccione el recuadro de selección **Utilizar las credenciales del usuario (requiere configuración de SSO)** si está configurando un entorno de panel de control que utilice el inicio de sesión único y la autorización por usuario. Cuando esta opción está seleccionada, la señal de LTPA del usuario que ha iniciado sesión en Dashboard Application Services Hub se incluye en las solicitudes a proveedor de datos de panel de instrumentos cuando se recuperan datos de supervisión.
12. Cuando haya terminado de definir la conexión, pulse **Aceptar** para guardarla y conectar al proveedor de datos de panel de instrumentos.

Resultados

La conexión se realiza al proveedor de datos y la columna **Estado** de la tabla de conexiones muestra el progreso: `Pendiente`, `En funcionamiento`, `Anómalo`, `No hay orígenes de datos` o `No configurado`.

Si se produce un error al crear la conexión de proveedor de datos, consulte *IBM Tivoli Monitoring: Guía de resolución de problemas*.

Consulte “Configuración de un entorno de supervisión básico sin inicio de sesión único y sin controles de autorización por usuario” en la página 27 o “Configuración de un entorno de panel de control de supervisión con inicio de sesión único y con controles de autorización por usuario” en la página 32 para ver los pasos adicionales a realizar.

Creación de páginas de panel de control personalizadas que muestran datos de supervisión

IBM Dashboard Application Services Hub permite crear páginas de paneles de control personalizadas.

Una *página* es una disposición de uno o más widgets en el área de trabajo de la consola. Un *widget* es un componente de la interfaz de usuario que muestra información en un panel de control de la consola. Dashboard Application Services Hub proporciona un conjunto de widgets predefinidos. Cada widget está configurado para recuperar información de un proveedor de datos que tiene una conexión definida en Dashboard Application Services Hub. Cada proveedor de datos divide su información en conjuntos de datos.

Antes de empezar

Para obtener información detallada sobre widgets predefinidos, cómo editar y personalizar cada tipo de widget y cómo crear catálogos y páginas con widgets, consulte la ayuda en línea de Dashboard Application Services Hub o *Jazz for Service Management Integration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html).

Acerca de esta tarea

Puede añadir los widgets predefinidos a páginas de panel de control o puede personalizar los widgets predefinidos para cambiar su apariencia. Hay widgets para tablas, listas, indicadores, diagramas de barras, gráficos circulares, topología, etcétera. Los widgets también se pueden organizar lógicamente colocándolos en catálogos.

Los conjuntos de datos del proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring corresponden a los grupos de atributos del agente. Son los mismos grupos de atributos para los que se crean consultas al personalizar las vistas del espacio de trabajo de Tivoli Enterprise Portal. El proveedor de datos de panel de instrumentos también tiene conjuntos de datos de topología si se proporcionan por un agente de supervisión como IBM Tivoli Monitoring para el agente de supervisión VMware. Consulte las guías del usuario del agente para ver una descripción de los grupos de atributos del agente y para determinar si el agente proporciona un conjunto de datos de topología.

Cuando se crea o edita una página, puede elegir los widgets y su ubicación en la página. Puede editar cada widget para elegir un conjunto de datos y seleccionar qué información del conjunto de datos debe visualizarse en el widget. Al editar un widget, proporcione la siguiente información:

Procedimiento

1. Elija un conjunto de datos.

   Cuando se edita un widget, se puede elegir un conjunto de datos de la lista de proveedores de datos configurados en Dashboard Application Services Hub. Puede optar por ver todos los nombres de los conjuntos de datos o especificar criterios de búsqueda para el nombre del conjunto de datos. Si lista todos los nombres de conjuntos de datos, verá los conjuntos de datos para todos los agentes cuyo soporte de aplicación se ha instalado en el Tivoli Enterprise Portal Server así como los conjuntos de datos disponibles de otros proveedores de datos. Dado que esta puede ser una lista larga de conjuntos de datos, puede filtrar los conjuntos de datos buscando en una parte del nombre del conjunto de datos. Por ejemplo, para ver todos los conjuntos de datos (grupos de atributos) para el agente del sistema operativo Linux, especifique "`Linux`" en el campo de búsqueda.
2. Correlacione las columnas del conjunto de datos con los atributos de visualización del widget.

   En función del tipo de widget, es posible que se le solicite que especifique qué columna(s) del conjunto de datos desea que se visualicen en el widget. Por ejemplo, si está editando un widget de indicador analógico para mostrar la utilización de disco de un agente del sistema operativo Linux, seleccione la columna **Porcentaje de disco utilizado** para el valor de indicador.
3. Configure las opciones de visualización del widget.

   También puede configurar las opciones de visualización del widget como etiquetas, unidades de medida, etc.
4. Especifique los parámetros de configuración del conjunto de datos.

   Si ha seleccionado un conjunto de datos que se correlaciona con un grupo de atributos de un agente, debe especificar el nombre del sistema gestionado o grupo de sistemas gestionados de los que se recuperan los datos. También puede especificar un valor de filtro de tiempo para recuperar datos históricos si el widget soporta mostrar datos a lo largo de un periodo de tiempo y ha configurado la recopilación de datos históricos.

El conjunto de datos puede tener otros parámetros de configuración para filtrar más la información que se visualiza en el widget. Por ejemplo, si está editando un widget como un indicador que muestra valores de una sola fila en un grupo de atributos del agente, los parámetros de configuración del conjunto de datos permiten especificar otras columnas del conjunto de datos (atributos) que identifican de forma exclusiva qué fila de datos se visualiza en el elemento. Por ejemplo, si está visualizando la utilización de disco para un agente del sistema operativo Linux, en un widget de indicador los parámetros de configuración del conjunto de datos del disco Linux le permiten especificar de qué disco y punto de montaje se debe mostrar la utilización.

También puede especificar la frecuencia con la que el proveedor de datos de panel de instrumentos proporciona renovaciones de los datos si el widget soporta la renovación automática y no ha seleccionado el conjunto de datos de sucesos.

Para los conjuntos de datos de topología, pueden especificarse los siguientes parámetros de configuración:

SourceToken
El identificador de nodo de inicio en el que comienza el cruce topológico.

Depth
La profundidad máxima topológica (número de niveles) que el proveedor de datos del panel de control atravesará y devolverá.

Amplitud
El número máximo de nodos por nivel que el proveedor de datos de panel de control atravesará y devolverá.

MaxNodes
El número máximo de nodos que el proveedor de datos del panel de control devolverá.

TraversalOrder
El orden en el que los nodos de la topología se deben atravesar y añadir al resultado del conjunto de datos. Los valores soportados son:

DepthFirst
El cruce es del orden de primera profundidad.

BreadthFirst
El cruce es del orden del nivel.

Nota: Si se especifican los parámetros **Depth** o **Breadth**, se ignora el parámetro **TraversalOrder**.

Muchos de los widgets de Dashboard Application Services Hub pueden dar soporte a conexiones entre widgets para que puedan intercambiar mensajes entre sí. Cuando se produce una acción en un widget de origen, se crea un suceso que contiene información que puede enviarse a otros widgets. El proveedor de datos de panel de instrumentos no da soporte a intercambiar sucesos con otros widgets.

Dashboard Application Services Hub utiliza roles, para los usuarios o grupos de usuarios, para controlar qué usuarios pueden crear páginas y trabajar con widgets y qué páginas que un usuario puede visualizar. Sin embargo, el proveedor de datos de panel de instrumentos realiza la autorización de los recursos de supervisión que se muestran en un widget que utiliza uno de los conjuntos de datos del proveedor de datos. Las páginas de panel de control personalizadas utilizan el tipo de autorización que está configurado para el

entorno del panel de control de supervisión, políticas de autorización o permiso de suceso de Tivoli Enterprise Portal y asignaciones de aplicación de supervisión.

Qué hacer a continuación

Para ver ejemplos de cómo crear páginas de panel de control personalizadas con datos de supervisión, consulte Creating custom monitoring dashboard pages en IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home).

Control de las importaciones de UISolutions

Cuando se inicia una aplicación de paneles de control como IBM Infrastructure Management Dashboards for Servers, la aplicación de paneles de control envía una solicitud al proveedor de datos de panel de instrumentos para importar las UISolutions de la aplicación. UISolutions del proveedor de datos de panel de instrumentos definen las características de qué datos de los paneles de control pueden visualizar. La importación se realiza una vez por aplicación de instrumentos y se produce automáticamente. Cuando una aplicación de paneles de control se actualiza y contiene UISolutions actualizadas, la importación también se produce automáticamente.

Puede inhabilitar la importación de UISolutions después de haber instalado e iniciado todas las aplicaciones de paneles de control, o puede controlar qué usuarios pueden importar UISolutions configurando el servidor de portal.

Acerca de esta tarea

Si inhabilita UISolutions por completo, debe volver a habilitar la importación de UISolutions cuando se instale una aplicación de paneles de control nueva o se actualice una aplicación de paneles de control existente en IBM Dashboard Application Services Hub. Cuando complete la instalación o actualización de la aplicación de paneles de control, la inicie y verifique que los datos se pueden visualizar, puede inhabilitar de nuevo la importación de UISolutions.

Si desea controlar qué usuario puede importar UISolutions tenga en cuenta que las aplicaciones de paneles de control nuevas o actualizadas con UISolutions no se podrán utilizar hasta que el usuario especificado en el archivo de entorno del servidor de portal inicie la aplicación de paneles de control.

La variable `KD8_VM_IMPORT_ID` es opcional y no se establece de forma predeterminada, lo que significa que cualquier usuario de paneles de control que se ha autenticado puede desencadenar la solicitud de importar UISolutions cuando se inicia la aplicación de paneles de control.

Procedimiento

1. Abra el archivo de variables de entorno del Tivoli Enterprise Portal Server.

   Windows *install_dir*\CNPS\kfwenv

   Linux UNIX *install_dir*/config/cq.ini

2. Establezca la variable de entorno `KD8_VM_IMPORT_ID`.

   Para controlar qué usuario tiene permiso para realizar la importación, establezca esta variable en un ID concreto como `KD8_VM_IMPORT_ID=user1`.

Para inhabilitar todos los usuarios para realizar una importación de UISolutions, establezca `KD8_VM_IMPORT_ID=$nouser@` o en cualquier nombre que sepa que no coincide con un ID de usuario de paneles de control.

3. Reinicie el Tivoli Enterprise Portal Server para implementar los cambios efectuados.

Capítulo 4. Edición de los valores de configuración del entorno

El cliente de Tivoli Enterprise Portal tiene varias docenas de parámetros que se pueden establecer para influir en el comportamiento y el rendimiento de los sistemas de usuario. Asimismo, el Tivoli Enterprise Portal Server tiene un archivo de entorno que se puede editar para ajustar o añadir variables para influir en todos los clientes de portal conectados al mismo así como en la interacción con el servidor de supervisión concentrador. También puede controlar las variables de entorno en Tivoli Enterprise Monitoring Server y Tivoli Enterprise Monitoring Automation Server.

Los temas siguientes incluyen información correspondiente a las variables de entorno a las que se hace referencia en la *Guía del administrador*. Para obtener una lista completa de variables de entorno, consulte "Variables de entorno" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Valores de configuración del cliente de Tivoli Enterprise Portal

El cliente de Tivoli Enterprise Portal tiene parámetros que afectan el rendimiento, por ejemplo el tamaño máximo de los archivos conectados a los reconocimientos de sucesos y el tiempo durante el cual se debe conservar la lista de sucesos comunes en la memoria caché.

Edición de parámetros del cliente

Los cambios efectuados en el cliente de navegador se aplican globalmente porque se descargan automáticamente mediante el servidor HTTP que se instala con el servidor de portal. Si los usuarios despliegan ellos mismos el cliente de escritorio mediante Java WebStart, los cambios también se aplicarán globalmente. De lo contrario, los cambios de cliente de escritorio se deben realizar en cada sistema donde está instalado si desea que el cambio afecte a todos los usuarios.

Acerca de esta tarea

Realice estos pasos para ajustar los parámetros de cliente:

Procedimiento

1. Inicie Manage Tivoli Enterprise Monitoring Services. Para el cliente de navegador y Java WebStart, éste es el sistema donde está instalado el servidor de portal; de lo contrario, es dónde está instalado el cliente de escritorio.
   - Windows Pulse **Inicio** → **Programas** → **IBM Tivoli Monitoring** → **Manage Tivoli Enterprise Monitoring Services**.
   - Linux Vaya al directorio *install_dir*/bin y escriba `./itmcmd manage`.
2. Pulse el botón derecho del ratón en **Tivoli Enterprise Portal – Escritorio** o **Tivoli Enterprise Portal – Navegador** y pulse **Reconfigurar**. Se visualiza la ventana Configurar instancia de aplicación para el cliente de escritorio (también se utiliza para Java WebStart); se visualiza la ventana Configurar navegador de Tivoli Enterprise Portal para el cliente de navegador.
3. Efectúe una doble pulsación en el valor de parámetro que desea cambiar.

© Copyright IBM Corp. 2005, 2013

4. Para activar el parámetro, escriba un valor y seleccione **En uso** en la ventana Editar parámetros de Tivoli Enterprise Portal.
5. Cuando haya terminado de editar los parámetros, pulse **Aceptar** para guardar los cambios. Los cambios entrarán en vigor la siguiente vez que los usuarios inicien la sesión en el servidor de portal. Los usuarios que ya han iniciado la sesión no verán ningún cambio hasta que salgan e inicien la sesión otra vez.

Referencia relacionada:

"Lista de parámetros del cliente de portal"
La mayor parte de los valores predeterminados de los parámetros del cliente de Tivoli Enterprise Portal no se modifican. Edite los parámetros de los clientes para modificar un comportamiento específico.

Lista de parámetros del cliente de portal

La mayor parte de los valores predeterminados de los parámetros del cliente de Tivoli Enterprise Portal no se modifican. Edite los parámetros de los clientes para modificar un comportamiento específico.

Algunos parámetros pertenecen solo al cliente de escritorio, solo al cliente de escritorio y al cliente de Java WebStart o solo al cliente de navegador y están indicados como tales.

browser.cache.memory.capacity
Indica la cantidad máxima de memoria en KB que se utiliza para almacenar en la memoria caché las imágenes decodificadas y otras características mediante las vistas del navegador (un entero positivo no de cero). Especifique un valor de 0 para inhabilitar el almacenamiento en memoria caché. Valor predeterminado: **-1**, mediante el cual el valor de capacidad se decide automáticamente en función de la cantidad total de memoria.

Memoria física	Memoria caché en KB
32 MB	2048
64 MB	4096
128 MB	6144
256 MB	10240
512 MB	14336
1 GB	18432
2 GB	24576
4 GB	30720
8 GB y más	32768

cnp.agentdeploy.timeout
Es el tiempo que debe transcurrir antes de que exceda el tiempo de espera de la solicitud de despliegue de agente. Valor predeterminado: **1800** segundos (30 minutos).

cnp.attachment.segment.maxsize
Para la transmisión a través de la red, los adjuntos de archivos se dividen en segmentos y, a continuación, se vuelven a ensamblar en el Tivoli Enterprise Portal Server. Por ejemplo, un archivo de 8 MB se transmite en ocho segmentos de 1 MB. Ajuste este parámetro para el tamaño de segmento que mejor se ajuste al entorno. Entre el tamaño máximo en bytes, por ejemplo 250000 para 250 KB. Valor predeterminado: **1000000** (1 MB).

Este parámetro también está disponible como una variable del entorno del servidor de portal. Consulte el apartado “Control del tamaño de adjuntos de sucesos” en la página 76.

cnp.attachment.total.maxsize
Utilice este parámetro para establecer el tamaño máximo de cada archivo adjunto a un reconocimiento. Entre el tamaño máximo en bytes, por ejemplo 2500000 para 2,5 MB. Valor predeterminado: **10000000** (10 MB).

Este parámetro también está disponible como variable de entorno de servidor de portal. Consulte el apartado “Control del tamaño de adjuntos de sucesos” en la página 76.

cnp.authentication.skip_dns
Valor: “N”. Determina si la validación de certificado de servidor intenta resolver y comparar el nombre DNS de host.

cnp.browser.installdir
El componente navegador WebRenderer Java se utiliza para las funciones de vistas del navegador en el cliente de portal. La primera vez que un usuario crea una vista del navegador, automáticamente se crea un subdirectorio en el sistema del usuario.

Windows *%HOMEPATH%*\wr*WebRendererVersion*\.webrendererswing.
Ejemplo: C:\Documents and Settings\Administrator\wr4.2.14\ .webrendererswing

Linux %HOME/wr*WebRendererVersion*/.webrendererswing

En este subdirectorio se colocan los archivos jar extraídos y se crean otros artefactos WebRenderer para las vistas del navegador. Utilice este parámetro para especificar una vía de acceso diferente para guardar los archivos de vistas del navegador en las máquinas de los usuarios. Si los usuarios ejecutarán varias instancias del cliente de portal, y pueden iniciar la sesión en diferentes versiones del servidor de portal, será necesaria una vía de acceso diferente.

cnp.commonevent.cache.timeout
Número de minutos durante los cuales se debe retener la memoria caché para la consola de sucesos comunes cuando el usuario ha conmutado a un espacio de trabajo que no contiene la vista de consola de sucesos comunes (lo que significa que la memoria caché no se está utilizando). Si finaliza este periodo de tiempo antes de que se vuelva a utilizar la memoria caché, ésta se borra. Entonces, la memoria caché se vuelve a crear cuando la necesita una vista de consola de sucesos comunes.

Un valor de -1 significa que hay que retener siempre la memoria caché, incluso aunque no se esté utilizando. Un valor de 0 significa borrar inmediatamente la memoria caché cuando el usuario haya conmutado a un espacio de trabajo que no contiene la vista de consola de sucesos comunes. Valor predeterminado: **30**.

cnp.databus.pageSize
En la interfaz de usuario de Tivoli Enterprise Portal, el editor de Propiedades tiene un campo para ajustar el tamaño de página para vistas basadas en consultas individuales. Este parámetro establece el número de filas que hay que buscar en una sola página lógica para todas las vistas basadas en consultas. Valor predeterminado: **100** filas. Aunque no hay ningún límite en el valor que puede establecer aquí, cuanto mayor es el tamaño de página, más memoria se necesitará en el servidor y cliente de portal.

Por ejemplo, es aconsejable establecer un tamaño de página mayor para la búsqueda en la vista de tabla en un número mayor de filas. O es posible que desee menos páginas en las que desplazarse al interactuar con vistas que recuperan un gran número de filas (o instancias). Sin embargo, necesita asegurarse de que tiene suficientes recursos en el servidor y el cliente de portal para manejar los datos adicionales que se están empaquetando, transportando y finalmente entregando como resultado del incremento del valor de tamaño de página. Probablemente el mejor modo de encontrar aquí el número correcto es incrementarlo gradualmente (por ejemplo en incrementos de 100) hasta que el tiempo de respuesta en un amplio muestreo de espacios de trabajo empiece a empeorar. En ese momento, es aconsejable reducir el número por el último incremento (por ejemplo 100 filas menos) porque ese número estará más cerca del valor óptimo para el entorno.

Otro valor que afecta el tiempo de respuesta de vista basada en consulta es KFW_REPORT_NODE_LIMIT, que es una variable de entorno del servidor de portal.

cnp.drag.sensitivity
Número de píxeles que el ratón se debe mover para que empiece la operación de arrastre. Valor predeterminado: **7**.

cnp.encoding.codeset
Identificación de conjunto de códigos de codificación de cadena.

cnp.eventcon.autoresume.delay
El número de segundos que hay que esperar antes de reanudar automáticamente las actualizaciones en la Consola de sucesos de situación y en la Consola de sucesos comunes después de que se hayan colocado en pausa para realizar desplazamientos. Valor predeterminado: **60** segundos.

cnp.heartbeat.interval
Intervalo de ping de latido entre el cliente y el servidor de Tivoli Enterprise Portal. Un incremento del intervalo significa que el cliente tardará más tiempo en detectar que el servidor de portal está fuera de línea. Un intervalo más corto significa que se notificará al cliente más pronto pero también incrementa el tráfico entre el cliente y el servidor. Valor predeterminado: **30** segundos.

cnp.history.depth
Número de espacios de trabajo a mantener en la pila de navegación de historial de retrocesos y avances. Valor predeterminado: **20**.

cnp.http.proxy.password
Contraseña utilizada para la autenticación de proxy utilizando la vista de navegador.

cnp.http.proxy.user
ID de usuario utilizado para la autenticación de proxy utilizando la vista de navegador.

cnp.http.url.host
Solo cliente de escritorio y cliente de Java WebStart: Host de URL para captación de IOR.

cnp.http.url.path
Solo cliente de escritorio y cliente de Java WebStart: Vía de acceso de URL para captación de IOR.

cnp.http.url.port
Solo cliente de escritorio y cliente de Java WebStart: Puerto de URL para captación de IOR.

cnp.http.url.protocol
Solo cliente de escritorio y cliente de Java WebStart: Protocolo de URL para captación de IOR.

cnp.http.url.DataBus
Sólo cliente de escritorio y cliente de Java WebStart: URL para el archivo `cnps.ior`, que es necesario para que el servidor de portal localice las imágenes de vista gráficas y las hojas de estilo. El valor predeterminado, que no se muestra, supone el servidor HTTP integral. Si, por alguna razón, se ha inhabilitado, debe entrar el URL para el servidor HTTP integral. Consulte la publicación *IBM Tivoli Monitoring: Guía de resolución de problemas* para obtener detalles. Cuando este parámetro está establecido, se alteran temporalmente los valores de los demás parámetros cnp.http.url para el protocolo, el puerto y la vía de acceso.

cnp.pipeline.factor
Factor de supervisión de interconexión de databus a servidor (en ciclos de latido). Valor predeterminado: **2**.

cnp.playsound.interval
Número de segundos antes de que se pueda reproducir otra vez el mismo archivo de sonido. Si se abren frecuentemente los sucesos, este valor proporciona una pausa de sonido. Valor predeterminado: **10** segundos.

cnp.publishurl.delay
Sólo cliente de navegador: Cuando se realiza una conmutación de espacio de trabajo, permite que se complete la representación de interfaz de usuario antes de que el navegador inicialice la nueva applet y destruya la applet anterior. Valor predeterminado: **1** segundo.

Importante: Modifique este parámetro sólo después de consultar el servicio de soporte de software de IBM.

cnp.systemtray.offset
Factores de Tivoli Enterprise Portal de la barra de tareas de Windows en la parte inferior de la pantalla al ajustar el tamaño de los menús y las ventanas para la visualización. Valor predeterminado: **true**.

cnp.terminal.cache.entries
Número máximo de sesiones de emulador de terminal activas. Valor predeterminado: **50**.

cnp.terminal.host
Nombre de host de emulador de terminal predeterminado.

cnp.terminal.port
Número de puerto de emulador de terminal predeterminado. Valor predeterminado: **23**.

cnp.terminal.script.entries
Número máximo de scripts de emulador de terminal de usuario que se pueden guardar. Valor predeterminado: **256**.

cnp.terminal.type
Tipo de emulador de terminal predeterminado. Al especificar un tipo de terminal, escriba el tipo de terminal entre comillas dobles y entre uno de estos nombres soportados:

IBM 3270 (24x80)

IBM 3270 (32x80)

IBM 3270 (43x80)

IBM 3270 (27x132)

IBM 5250 (24x80)

VT100 (24x80)

cnp.view.change_remove.warning
Mensaje de aviso cuando el usuario está a punto de cambiar o eliminar una vista.

Valor predeterminado: **True**. Se visualiza el mensaje. Cambie el valor a False para impedir que se visualice el mensaje.

cnp.workspace.switch.rate
Cantidad mínima de tiempo que debe transcurrir para que el espacio de trabajo se pueda sustituir por el siguiente seleccionado. Valor predeterminado: **1000** (1 segundo).

cnp.workspacerender.delay
Sólo modalidad de navegador: Retardo posterior a la presentación de espacio de trabajo en milisegundos.

http:agent
Define el nombre del servidor HTTP integral. Si éste o el proxy necesitan una identidad de navegador diferente antes de que se habilite la vista de navegador para acceder a Internet, se puede entrar un nombre de una palabra para el navegador. Puede ser cualquier nombre a condición de que el servidor proxy no lo rechace. Normalmente no necesitará añadir una definición de nombre http a menos que los usuarios reciban un error cuando intenten acceder a Internet mediante una vista de navegador del espacio de trabajo.

http.nonproxyhosts
Cuando se selecciona ☑ **Habilitar solicitudes de servidor proxy HTTP**, los servidores de esta lista ignoran el proxy. Separe cada nombre de servidor con una línea vertical (|). Consulte el apartado “Habilitación del servidor proxy HTTP” en la página 69.

http.proxyHost
Cliente de navegador: Se utiliza para especificar el nombre de host o la dirección IP del servidor proxy http si se utiliza uno.

http.proxyPort
Cliente de navegador: Se utiliza con el parámetro http.proxyHost para especificar el número de puerto de escucha para el servidor proxy HTTP. El puerto **80** es el valor predeterminado para servidores HTTP de otros proveedores.

kjr.browser.default
Es el nombre de vía de acceso y el nombre de la aplicación de navegador a utilizar al iniciar la ayuda según contexto. Para abrir la ayuda con un navegador específico u otro distinto del valor predeterminado, entre la vía de acceso y el nombre de aplicación, por ejemplo `C:\Archivos de programa\Mozilla Firefox\firefox.exe`.

kjr.trace.file
Nombre de archivo de registro de rastreo RAS1 si la modalidad de rastreo es LOCAL.

kjr.trace.mode
Opción de rastreo de RAS1. Valor predeterminado: LOCAL.

kjr.trace.params
Opciones de rastreo de RAS1. Valor predeterminado: ERROR.

kjr.trace.qdepth
Establece la profundidad de cola de hebras de rastreo en **15000** de forma predeterminada.

kjr.trace.thread
Determina si las llamadas de rastreo tienen hebras. Valor predeterminado: **true**.

sun.java2d.noddraw
Cuando Tivoli Enterprise Portal se ejecuta como imagen de cliente en un entorno de emulación que no soporta la función de escritura de pantalla DirectDraw, desactive la función estableciendo esta variable en true en los clientes de navegador y de escritorio. De lo contrario, los usuarios encuentran condiciones de alto uso de CPU porque el proceso Java intenta escribir en la pantalla. Valor predeterminado: **true**.

user.language
Sólo cliente de escritorio y cliente de Java Web Start: Especifica el código de idioma de la preferencia de entorno local del usuario (por ejemplo, cs, de, en, es, fr, hu, it, ja, ko, pl, pt, ru, th y zh). Puede crear otra instancia del cliente de escritorio y cambiar esta variable (y user.region) a otro entorno local. De este modo, puede tener dos o más instancias del cliente de escritorio que se ejecuta en el mismo sistema, cada una en un idioma diferente. Si especifica un entorno local no soportado, se utiliza en_US.

Sólo cliente de navegador: En el sistema cliente, especifique el texto siguiente directamente en los parámetros de tiempo de ejecución del plug-in Java utilizados por el navegador, donde *xx* es el idioma y *XX* es el entorno local.

```
-Duser.language=xx -Duser.region=XX
```

Nota: El cliente de portal utiliza hoja de estilo en cascada para ofrecer el texto de la aplicación. Si no hay disponible una versión traducida de una hoja de estilos, como por ejemplo `ws_press.css`, se utilizará la versión en inglés.
Para editar los parámetros de tiempo de ejecución, complete las tareas siguientes:

1. Abra el panel de control de Java:

   Windows Inicie el **Panel de control de IBM para Java** o el Panel de control de **Java**.

   Linux Busque el ejecutable **ControlPanel** de Java en *dir_instalación_jre* e inícielo. Por ejemplo: `/opt/IBM/ibm-java2-i386-70/jre/bin/ControlPanel`.
2. Pulse el separador **Java**.
3. En el área Valores de tiempo de ejecución de applet Java, pulse **Ver**.
4. Si dispone de múltiples versiones de Java, verifique que tiene abierto el panel de control correcto leyendo la columna **Ubicación** para confirmar la versión de Java y que el JRE está en la vía de acceso correcta.Por ejemplo: `C:\Program Files\IBM\Java70\jre\bin` para IBM Java en Windows.
5. Edite el parámetro que desea cambiar.

6. Guarde los cambios.

user.region
Especifica el código de país de la preferencia de entorno local del usuario (como BR, CN, CZ, DE, ES, FR, HU, IT, JP, KR, PL, RU, TH, TW y US). Consulte también la descripción de **user.language**.

Utilice la tabla siguiente para encontrar códigos de lenguaje y códigos de entorno local:

Tabla 6. Códigos de idioma y entorno local

Idioma	**Código de idioma (xx)**	**Código de entorno local (XX)**
Chino simplificado	zh	CN
Chino tradicional	zh	TW
Checo	cs	CZ
Inglés	en	US
Francés	fr	FR
Alemán	de	DE
Húngaro	hu	HU
Italiano	it	IT
Japonés	ja	JP
Coreano	ko	KR
Polaco	pl	PL
Portugués de Brasil	pt	BR
Ruso	ru	RU
Español	es	ES
Tailandés	th	TH

Tareas relacionadas:

"Edición de parámetros del cliente" en la página 61
Los cambios efectuados en el cliente de navegador se aplican globalmente porque se descargan automáticamente mediante el servidor HTTP que se instala con el servidor de portal. Si los usuarios despliegan ellos mismos el cliente de escritorio mediante Java WebStart, los cambios también se aplicarán globalmente. De lo contrario, los cambios de cliente de escritorio se deben realizar en cada sistema donde está instalado si desea que el cambio afecte a todos los usuarios.

"Control del tamaño de adjuntos de sucesos" en la página 76
De forma predeterminada, el tamaño máximo de cada archivo adjunto a un reconocimiento de suceso es 10 MB y 1 MB para el tamaño de los segmentos de información enviados a través de la red. Se proporcionan variables de entorno que le permiten cambiar el máximo en Tivoli Enterprise Portal o en el Tivoli Enterprise Portal Server. Los valores de adjunto de suceso que se cambian en el cliente de escritorio prevalecen sobre los del servidor de portal.

"Inicio del cliente de navegador en otro servidor de portal." en la página 22
Inicie una instancia diferente del navegador e inicie sesión en el Tivoli Enterprise Portal Server de una red gestionada diferente para ver dos redes gestionadas desde el mismo sistema.

Referencia relacionada:

"Variables de entorno del servidor de portal" en la página 73
El archivo de configuración del entorno para Tivoli Enterprise Portal Server se puede editar para añadir ciertos valores de entorno y para cambiar los valores de otros.

Habilitación del servidor proxy HTTP

Los entornos que utilizan un servidor proxy HTTP necesitan una configuración adicional del cliente para permitir el acceso de URL desde la vista de navegador del espacio de trabajo de Tivoli Enterprise Portal.

Acerca de esta tarea

Para habilitar el servidor proxy HTTP, siga estos pasos en cada sistema en el que se utilice el cliente de Tivoli Enterprise Portal que también utiliza un proxy HTTP para la vista del navegador:

Procedimiento

1. Abra un espacio de trabajo que contenga una vista de navegador o añada una vista de navegador al espacio de trabajo actual.
2. En el recuadro de dirección de la vista de navegador, escriba: `about:config`
3. En el campo de filtro que aparece en la parte superior de la página, escriba lo siguiente para ver los campos de proxy de red: `network.proxy`
4. Aparte del conjunto reducido que se muestra, las tres siguientes entradas son interesantes. Pulse dos veces una entrada o selecciónela y pulse Intro para modificar sus valores:

   network.proxy.http
   Escriba en identificador de DNS o la dirección IP del host proxy que desea utilizar para el protocolo HTTP.

   network.proxy.http_port
   Escriba `80`, el número de puerto predeterminado o un número diferente que utilice el host proxy.

network.proxy.no_proxies_on
Agregue nombres de host completos o direcciones IP a los que se debe acceder sin el proxy. Por ejemplo, este valor omite el servidor proxy para los archivos del sistema local y del servidor de portal (myteps.uk.ibm.com) a los que se accede desde la vista de navegador: `localhost,127.0.0.1, myteps.uk.ibm.com`.

Resultados

Después de pulsar **Aceptar** en el panel de edición de propiedades, el cambio se guarda en el cliente de Tivoli Enterprise Portal.

Establecimiento de las propiedades de aplicación para sistemas Linux y UNIX

Para cambiar una propiedad, como la ubicación del navegador web que el cliente de navegador Tivoli Enterprise Portal inicia en UNIX, actualice el archivo o los archivos de script de shell que se ejecutan y la plantilla que se utiliza cuando el cliente de navegador se configura para crear el archivo o los archivos script que se ejecutan.

Acerca de esta tarea

Es posible que tenga que actualizar uno o varios de los archivos siguientes:

Nota: Todas las vías de acceso de archivo son relativas al directorio *dir_instalación* donde ha instalado IBM Tivoli Monitoring.

Tabla 7. Ubicaciones de archivo para cambiar propiedades de aplicación para sistemas UNIX y Linux

Ubicación de archivo	Finalidad del archivo
bin/cnp.sh	Script de shell predeterminado que inicia el cliente de navegador de Tivoli Enterprise Portal.
bin/cnp_*instancia*.sh	El script de shell para una instancia específica que ha creado, donde *instancia* es el nombre de la instancia que inicia el cliente de navegador de Tivoli Enterprise Portal.
plataforma/cj/original/cnp.sh_template	La plantilla de la que se generan los scripts de shell bin/cnp.sh y bin/cnp_*instancia*.sh durante la configuración, donde *plataforma* es el código de la plataforma de sistema operativo en la que está instalado IBM Tivoli Monitoring. Por ejemplo: *li6243* para Linux 2.4 en una CPU Intel de 32 bits). Si sólo cambia bin/cnp.sh o bin/cnp_instance.sh y no cambia esta plantilla, la siguiente vez que configure el cliente, se crea una nueva versión del script sin los cambios que ha realizado en bin/cnp.sh o bin/cnp_instance.sh.

También puede establecer las propiedades de nombre de instancia, navegador y Tivoli Enterprise Portal Server en Linux. Consulte la publicación *IBM Tivoli Monitoring: Consulta de mandatos* para obtener más detalles.

Para cambiar la ubicación del navegador web, debe cambiar el archivo o los archivos anteriores para que incluyan una nueva propiedad, siguiendo este procedimiento:

Procedimiento

1. Vaya a *install_dir*/bin/cnp.sh y edite el script de shell cnp.sh.
2. Añada la ubicación del navegador web a la última línea del archivo. En el ejemplo siguiente, la ubicación del navegador web es */opt/foo/bin/launcher*.
   ```
   -Dkjr.browser.default=/opt/foo/bin/launcher
   ```

   Importante: La línea es muy larga y tiene varias opciones en ella, incluidas otras varias opciones –D para definir otras propiedades. Es muy importante añadir la opción en el lugar correcto.
   Si la última línea de bin/cnp.sh tenía originalmente el aspecto siguiente:
   ```
   ${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
   -Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
   -Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
   -Dvbroker.agent.enableLocator=false
   -Dhttp.proxyHost=
   -Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
   ```

   Para establecer la ubicación de navegador en */opt/foo/bin/launcher*, cambie la línea para que tenga este aspecto:
   ```
   ${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
   -Dkjr.browser.default=/opt/foo/bin/launcher
   -Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
   -Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
   -Dvbroker.agent.enableLocator=false
   -Dhttp.proxyHost=
   -Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
   ```

Establecimiento de la variable de entorno cuando el concentrador está en un sistema z/OS

En z/OS, GSKit se conoce como Integrated Cryptographic Service Facility o ICSF. El Tivoli Enterprise Monitoring Server soporta el cifrado de contraseñas a través de ICSF, que proporciona un potente esquema de cifrado y descifrado para las contraseñas almacenadas y es el método preferido de cifrado de contraseñas.

Acerca de esta tarea

Si el Tivoli Enterprise Monitoring Server concentrador está en un sistema z/OS que no tiene instalado ICSF, se utiliza un esquema de cifrado alternativo menos seguro. El servidor de supervisión concentrador y el servidor de portal deben utilizar el mismo esquema. Por lo tanto, si el sistema concentrador no utiliza ICSF, debe configurar Tivoli Enterprise Portal para utilizar el esquema menos seguro (EGG1) también. Esto incluye la edición del archivo de entorno del Tivoli Enterprise Portal Server para añadir una nueva línea.

Para añadir la nueva línea al archivo de entorno, realice los pasos siguientes:

Procedimiento

- Windows
  1. En el sistema en el que el Tivoli Enterprise Portal Server está instalado, seleccione **Inicio** → **Programas** → **IBM Tivoli Monitoring** → **Manage Tivoli Enterprise Monitoring Services**.

2. Pulse con el botón derecho del ratón Tivoli Enterprise Portal Server, apunte a **Avanzado** y seleccione **Editar archivo ENV** en la lista.
3. Si se visualiza el mensaje del Tivoli Enterprise Portal Server, pulse **Aceptar** para cerrarlo.
4. Añada una nueva línea: `USE_EGG1_FLAG=1`.
5. Pulse **Guardar**.
6. Pulse **Sí** para implementar los cambios y reciclar el servicio.

- Linux UNIX
  1. Vaya al directorio (cd) *dir_instalación*`/config`
  2. Añada la línea siguiente al archivo cq.ini: `USE_EGG1_FLAG=1`
  3. Guarde el archivo.
  4. Recicle el servidor de portal.

Qué hacer a continuación

Consulte el apartado *Configuring the Tivoli Enterprise Monitoring Server on z/OS* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/ztemsconfig/ztemsconfig.htm).

Valores de configuración del servidor de Tivoli Enterprise Portal

El Tivoli Enterprise Portal Server ejecuta un proceso denominado KfwServices, que tiene un conjunto de variables de entorno que se pueden editar y habilitar para determinados requisitos de configuración. Esto se puede realizar mediante la aplicación Manage Tivoli Enterprise Monitoring Services o en la línea de mandatos utilizando `itmcmd manage`.

Por ejemplo, cuando tenga habilitada la seguridad, podrá controlar el número de intentos de inicio de sesión antes de que se bloquee a un usuario en el portal.

Si desea establecer las propiedades de aplicación para funciones de configuración avanzadas en UNIX o Linux, por ejemplo la ubicación del navegador web que el cliente de navegador Tivoli Enterprise Portal inicia, esta operación se tiene que realizar manualmente.

Si el servidor de portal se conecta a un servidor de supervisión concentrador que está en un sistema z/OS que no tiene instalado ICSF (Integrated Cryptographic Service Facility - Recurso de servicio criptográfico integrado), debe editar el archivo de entorno para añadir una nueva línea.

Nota: Las personalizaciones realizadas dentro de la TEPS/e consola de administración, como por ejemplo para configurar las comunicaciones TLS/SSL para el servidor LDAP, se sobregraban y borran cada vez que el servidor de portal se reconfigura a no ser que elija el tipo de LDAP **Otro** durante la configuración del servidor de portal a través de Manage Tivoli Monitoring Services. Para evitar que esto suceda, elija el tipo de LDAP **Otro** durante la configuración del servidor de portal. Cuando se selecciona **Otro**, la información del registro de usuarios de LDAP se maneja mediante TEPS/e y no se ve afectada por Tivoli Management Services directamente. Consulte el paso 5 en la página 105.

Edición del archivo de entorno del servidor de portal

Edite el archivo de entorno del servidor de Tivoli Enterprise Portal, KFWENV, para volver a configurar los parámetros del servidor de portal.

Acerca de esta tarea

Realice estos pasos para editar el archivo de entorno del servidor de portal:

Procedimiento

1. Abra el archivo de entorno en el sistema donde se ha instalado el servidor de portal:
   - Windows En Manage Tivoli Monitoring Services (**Inicio → Programas→ IBM Tivoli Monitoring→ Manage Tivoli Monitoring Services**), pulse con el botón derecho del ratón en **Servidor de Tivoli Enterprise Portal** y pulse **Avanzados → Editar archivo ENV** para abrir el archivo `kfwenv`.
   - Linux UNIX Vaya al directorio *dir_instalación*`/config` y abra el archivo `cq.ini` en un editor de texto.
2. Edite el archivo para habilitar (suprima # al principio de la línea), inhabilitar (escriba # al principio de la línea) o modificar cualquiera de las variables de entorno.
3. Guarde `kfwenv` (Windows) o `cq.ini` (Linux y sistemas operativos como UNIX) y salga del editor de texto.
4. Pulse **Sí** cuando un mensaje le solicita si desea reciclar el servicio. Pulse **No** si prefiere que los cambios realizados entren en vigor posteriormente, reciclando manualmente el servidor de portal.

Referencia relacionada:

"Variables de entorno del servidor de portal"
El archivo de configuración del entorno para Tivoli Enterprise Portal Server se puede editar para añadir ciertos valores de entorno y para cambiar los valores de otros.

Variables de entorno del servidor de portal

El archivo de configuración del entorno para Tivoli Enterprise Portal Server se puede editar para añadir ciertos valores de entorno y para cambiar los valores de otros.

El archivo muestra diversas variables de entorno que se han habilitado y otras que se han inhabilitado de forma predeterminada o como resultado del modo en que se ha configurado el servidor de portal. Para habilitarlas, se deben añadir manualmente otras variables de esta lista.

KFW_AUTHORIZATION_MAX_INVALID_LOGIN=0

Puede controlar el número de intentos que un usuario puede realizar para iniciar la sesión en el Tivoli Enterprise Portal Server estableciendo esta variable de entorno en un valor de 0 a 15. El valor predeterminado, 0, indica que no hay ningún límite en el número de intentos anómalos que un usuario puede realizar antes de quedar bloqueado.

Este valor de configuración sólo es efectivo cuando se ha habilitado la seguridad mediante el Tivoli Enterprise Monitoring Server concentrador como se describe en el tema "Control del número de intentos de inicio de sesión" en la página 77.

KFW_CMW_DETECT_AGENT_ADDR_CHANGE=N

La función de Navigator detecta cuándo se descubre la dirección IP para un agente. Si el entorno de agente cambia constantemente o tiene configuraciones incorrectas que generan excesivas reconstrucciones de

árbol de Navigator, tenga en cuenta la posibilidad de añadir esta variable de entorno para que se ignore cualquier descubrimiento de cambios o adiciones de la dirección IP.

KFW_CMW_DETECT_AGENT_HOSTNAME_CHANGE=N
Esta variable es como la de la detección de cambio de dirección de agente excepto en que impide la reconstrucción de Navigator si cambia un nombre de host de agente.

KFW_CMW_DETECT_AGENT_PROPERTY_CHANGE=N
Es igual que la detección de cambio de dirección de agente excepto en que impide la reconstrucción de Navigator si cambia una versión de afinidad o una afinidad de agente.

KFW_CMW_SITUATION_ADMIN_SUPPRESS=N
Cuando se detiene una situación, no se envía ningún mensaje a la consola de sucesos de situación. Si prefiere que el mensaje se grabe en la consola de sucesos de situación para cada sistema en el que se ha distribuido la situación, habilite (elimine el signo de almohadilla (#) al principio de la línea) esta variable de entorno. El mensaje `Detenido` alerta al usuario que la situación se ha detenido, por consiguiente el estado es desconocido.

KFW_CMW_SPECIAL_HUB_ENTERPRISE=Y
Asocia situaciones al elemento raíz de la vista física de Navigator, **Enterprise**. El valor predeterminado es **Y** para permitir la asociación de situaciones en línea y fuera de línea del sistema gestionado al elemento Empresa de Navigator. El valor **N** inhabilita la asignación automática del grupo de sistemas gestionados *HUB al elemento Empresa de Navigator.

KFW_ECLIPSE_HELP_SERVER_PORT=9999
El número de puerto predeterminado para el servidor de ayuda de Eclipse es 9999. Si otro dispositivo ya utiliza 9999, añada esta variable y especifique un número de puerto de 1 a 65535. Este valor se pasará como propiedad de servidor de portal al cliente en el inicio de sesión.

KFW_FIPS_ENFORCED=N
Los componentes agente y servidor de supervisión de Tivoli Management Services ya son compatibles con FIPS. Esta variable especifica si los métodos de cifrado que utiliza el servidor de portal deben cumplir con la especificación Federal Information Processing Standard (FIPS) 140–2. Si el entorno debe cumplir con el estándar FIPS 140–2, especifique `Y`.

KFW_REPORT_NODE_LIMIT=200
Cuando un espacio de trabajo que contiene una vista basada en consulta se abre o se renueva, la consulta de la vista solicita datos de los sistemas gestionados asignados a dicho elemento de Navigator (a no ser que haya editado la definición de la consulta de la vista para asignar sistemas gestionados o grupos de sistemas gestionados específicos). El número de sistemas gestionados de los que una consulta puede recuperar datos puede ser 200 como máximo. Se impone esta limitación para conservar el tráfico y el uso de recursos del sistema gestionado a un nivel aceptable. Puede ajustar el número máximo con esta variable pero tenga presente que si aumenta el número máximo de sistemas gestionados que se están consultando, puede tardar más tiempo en presentarse la vista.

Tenga en cuenta la posibilidad de crear consultas filtradas, grupos de sistemas gestionados o vistas personalizadas de Navigator con asignaciones de sistemas gestionados en elementos de Navigator que

limitan el número de sistemas gestionados de los que se recuperan datos. Estas características se describen en la ayuda en línea y la guía del usuario de Tivoli Enterprise Portal.

Otro valor que afecta al tiempo de respuesta de vista basada en consulta es el parámetro de cliente `cnp.databus.pageSize`.

KFW_REPORT_TERM_BREAK_POINT=86400
Ajuste este valor para cambiar el punto, en segundos, donde una solicitud histórica selecciona datos de historial de corto plazo o largo plazo. El valor predeterminado es que se recopilen datos de historial de corto plazo de las 24 horas anteriores hasta *ahora* y de largo plazo durante las siguientes 24 horas a partir de este momento. Establézcalo en **0** para seleccionar sólo datos de historial de largo plazo.

Tareas relacionadas:

"Edición del archivo de entorno del servidor de portal" en la página 72
Edite el archivo de entorno del servidor de Tivoli Enterprise Portal, KFWENV, para volver a configurar los parámetros del servidor de portal.

Referencia relacionada:

"Lista de parámetros del cliente de portal" en la página 62
La mayor parte de los valores predeterminados de los parámetros del cliente de Tivoli Enterprise Portal no se modifican. Edite los parámetros de los clientes para modificar un comportamiento específico.

Poda de sucesos en la base de datos del servidor de portal

La información de sucesos se almacena en las tablas KFW de la base de datos del Tivoli Enterprise Portal Server (TEPS). Dado la cantidad de espacio que consume esta información puede aumentar, ésta se poda automáticamente.

Acerca de esta tarea

De forma predeterminada, los sucesos cerrados se eliminan de la base de datos de TEPS un día después de haberse cerrado, durante las 12:00 AM y las 4:00 AM en el servidor de portal local. Puede controlar la poda de estos datos cambiando las variables de entorno siguientes en el archivo de configuración del Tivoli Enterprise Portal Server.

Procedimiento

1. Abra el archivo de entorno del Tivoli Enterprise Portal Server para editar:
   - Windows En Manage Tivoli Monitoring Services, pulse con el botón derecho en **Tivoli Enterprise Portal Server** y pulse **Avanzado** → **Editar archivo ENV**.
   - Linux UNIX Vaya al directorio *dir_instalación*/config y abra el archivo **cq.ini** en un editor de texto.
2. Localice y edite los parámetros de poda de sucesos de la base de datos de TEPS:
   - `KFW_EVENT_RETENTION=0` es el número de días durante los cuales se debe conservar un suceso cerrado. Por ejemplo, para podar un suceso 2 días después de haberse cerrado, especifique 2.
   - `KFW_PRUNE_START=00:00` es la hora del día para iniciar la poda de datos, en notación de 24 horas. Por ejemplo, para empezar la poda de datos a las 11:00 PM, especifique `23:00`.

- `KFW_PRUNE_END=04:00` es la hora del día para detener la poda de datos, especificada en notación de 24 horas. Por ejemplo, para finalizar la poda de datos a la 1:00 AM, especifique `01:00`.

3. Guarde y cierre el archivo de entorno.
4. Pulse **Sí** cuando un mensaje le pregunte si desea reciclar el servicio; o bien pulse **No** si prefiere que los cambios entren en vigor más tarde al reciclar el servidor de portal.

Control del tamaño de adjuntos de sucesos

De forma predeterminada, el tamaño máximo de cada archivo adjunto a un reconocimiento de suceso es 10 MB y 1 MB para el tamaño de los segmentos de información enviados a través de la red. Se proporcionan variables de entorno que le permiten cambiar el máximo en Tivoli Enterprise Portal o en el Tivoli Enterprise Portal Server. Los valores de adjunto de suceso que se cambian en el cliente de escritorio prevalecen sobre los del servidor de portal.

Acerca de esta tarea

Siga los pasos para editar los valores de entorno de Tivoli Enterprise Portal o del Tivoli Enterprise Portal Server.

Procedimiento

- Edite el archivo de entorno de Tivoli Enterprise Portal:
  1. Inicie Manage Tivoli Enterprise Monitoring Services:
     Windows Pulse **Inicio** → **Programas** → **IBM Tivoli Monitoring** → **Manage Tivoli Enterprise Monitoring Services**.
     Linux Vaya al directorio *install_dir*`/bin` y escriba `./itmcmd manage`.
  2. Pulse el botón derecho del ratón en **Tivoli Enterprise Portal – Escritorio** o **Tivoli Enterprise Portal – Navegador** y pulse **Reconfigurar**. Se visualiza la ventana Configurar instancia de aplicación para el cliente de escritorio (también se utiliza para Java WebStart); se visualiza la ventana Configurar navegador de Tivoli Enterprise Portal para el cliente de navegador.
  3. Realice una doble pulsación en **cnp.attachment.total.maxsize** y especifique el tamaño máximo, en bytes, para archivos individuales que se pueden adjuntar a un reconocimiento de suceso (como por ejemplo 2500000 para 2,5 MB), y seleccione ☑ **En uso**.
  4. Si desea cambiar el tamaño de segmento (el valor predeterminado 1000000 es 1 MB, por lo que un adjunto de 5 MB se transmitiría en 5 segmentos de 1 MB), realice una doble pulsación en **cnp.attachment.segment.maxsize** y especifique un nuevo tamaño de segmento, en bytes, y seleccione ☑ **En uso**.
  5. Pulse **Aceptar** para guardar los cambios. Los cambios entrarán en vigor la siguiente vez que el usuario inicie una sesión en el servidor de portal. Los usuarios que ya han iniciado la sesión no verán ningún cambio hasta que salgan e inicien la sesión otra vez.
- Edite el archivo de entorno de Tivoli Enterprise Portal Server:
  1. Abra el archivo de entorno del Tivoli Enterprise Portal Server para editar:
     Windows En Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho en **Tivoli Enterprise Portal Server** y pulse **Avanzado** → **Editar archivo ENV**.
     Linux UNIX Vaya al directorio *install_dir*`/config` y abra el archivo **cq.ini** en un editor de texto.
  2. Suprima el símbolo de almohadilla # al principio de las dos líneas KFW_ATTACHMENT y edite los valores como sea necesario.

KFW_ATTACHMENT_MAX=10000000 es 10 MB. Especifique el nuevo tamaño máximo de adjunto de archivo.
KFW_ATTACHMENT_SEGMENT_MAX=1000000 es 1 MB. Especifique el nuevo tamaño máximo de los segmentos de archivo en los que se divide un archivo adjunto para su transmisión.

3. Guarde y cierre el archivo de entorno.
4. Pulse **Sí** cuando un mensaje le pregunte si desea reciclar el servicio; o bien pulse **No** si prefiere que los cambios entren en vigor más tarde al reciclar el servidor de portal.

Referencia relacionada:

"Lista de parámetros del cliente de portal" en la página 62
La mayor parte de los valores predeterminados de los parámetros del cliente de Tivoli Enterprise Portal no se modifican. Edite los parámetros de los clientes para modificar un comportamiento específico.

Control del número de intentos de inicio de sesión

Puede especificar el número de intentos que puede realizar un usuario para iniciar una sesión en Tivoli Enterprise Portal estableciendo la variable de entorno KFW_AUTHORIZATION_MAX_INVALID_LOGIN.

Acerca de esta tarea

Consulte los procedimientos de **Qué realizar a continuación** al final de este tema para no permitir que un usuario acceda al portal, independientemente del valor de KFW_AUTHORIZATION_MAX_INVALID_LOGIN. Siga estos pasos para controlar el número de intentos de inicio de sesión en el servidor de portal:

Procedimiento

1. Abra el archivo de entorno del Tivoli Enterprise Portal Server para editar:
   - Windows En Manage Tivoli Monitoring Services, pulse con el botón derecho en **Tivoli Enterprise Portal Server** y pulse **Avanzado → Editar archivo ENV**.
   - Linux UNIX Vaya al directorio *dir_instalación*/config y abra el archivo **cq.ini** en un editor de texto.
2. Localice KFW_AUTHORIZATION_MAX_INVALID_LOGIN=0 y especifique un valor comprendido entre 0 y 15. El valor predeterminado, **0**, indica que no hay ningún límite en el número de intentos anómalos que un usuario puede realizar antes de bloquearse.
3. Guarde y cierre el archivo de entorno.
4. Pulse **Sí** cuando un mensaje le pregunte si desea reciclar el servicio; o bien pulse **No** si prefiere que los cambios entren en vigor más tarde al reciclar el servidor de portal.

Resultados

La próxima vez que un usuario intente iniciar una sesión en el servidor de portal, el número de intentos quedará restringido por el valor establecido en KFW_AUTHORIZATION_MAX_INVALID_LOGIN en el archivo de entorno.

Qué hacer a continuación

☑ **Seguridad: Validar usuario**

El valor de inicio de sesión no válido sólo entra en vigor cuando se ha habilitado la seguridad mediante el servidor de supervisión concentrador.

Linux UNIX Debe habilitar también la característica **Bloqueo de inicio** activando el valor de validación en el archivo de configuración del servidor de supervisión: `KDS_VALIDATE_EXT="Y"`.

Los archivos de configuración del servidor de supervisión se denominan *hostname*`_ms_`*address*`.config` y `ms.ini` y están en el directorio *dir_instalación*`/config/`.

Restauración de acceso de usuario

Si un usuario queda bloqueado, tiene dos opciones para restaurar el acceso a Tivoli Enterprise Portal:

- En Tivoli Enterprise Portal, pulse **Administrar usuarios** y seleccione el ID de usuario. En el separador Permisos, pulse **Administración de usuario** y habilite el recuadro de selección ☑ **Inicio de sesión permitido**.
- En el sistema donde está instalado el Tivoli Enterprise Portal Server, ejecute este programa de utilidad de línea de mandatos para habilitar o inhabilitar el acceso:

  Windows Vaya al directorio *dir_instalación*`\cnps\` y escriba

  ```
  KfwAuthorizationAccountClient.exe ENABLE|DISABLE
    id_usuario
  ```

  Por ejemplo, `KfwAuthorizationAccountClient.exe disable guest01` bloquea al usuario guest01 hasta que se vuelve a habilitar el ID de usuario.

  Linux UNIX Vaya al directorio *dir_instalación*`/bin` y escriba

  ```
  ./itmcmd execute cq "KfwAuthorizationAccountClient
     enable | disable nombre_usuario"
  ```

Valores de configuración del servidor de Tivoli Enterprise Monitoring

El Tivoli Enterprise Monitoring Server es el punto de recopilación y control de datos y alertas de rendimiento y disponibilidad recibidos de los agentes de supervisión. También es responsable de realizar un seguimiento del estado en línea o fuera de línea de los agentes de supervisión. Las variables de entorno controlan el comportamiento del servidor de supervisión.

Edición del archivo de entorno del servidor de supervisión

Edite el archivo de entorno del Tivoli Enterprise Monitoring Server, KBBENV, para volver a configurar los parámetros del servidor de supervisión.

Acerca de esta tarea

Realice estos pasos para editar el archivo de entorno del servidor de supervisión:

Procedimiento

1. Abra el archivo de entorno en el sistema donde se ha instalado el servidor de supervisión:
   - Windows Desde Manage Tivoli Enterprise Monitoring Services (Inicio → Programas → IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring

Services), pulse con el botón derecho del ratón en el Tivoli Enterprise Monitoring Server y pulse **Avanzado** → **Editar archivo ENV** para abrir el archivo `KBBENV`.

- Linux UNIX Vaya al directorio *dir_instalación*`/config` y abra el archivo `ms.ini` en un editor de texto.

2. Edite el archivo para habilitar (suprima # al principio de la línea), inhabilite (escriba # al principio de la línea) o modifique cualquiera de las variables de entorno.
3. Guarde el archivo y salga del editor de texto.
4. Pulse **Sí** cuando un mensaje le solicita si desea reciclar el servicio. Debe reiniciar el servidor de supervisión para implementar los cambios.

Proceso duper para optimizar situaciones

El Tivoli Enterprise Monitoring Server tiene un mecanismo denominado *duper* que optimiza la activación de varias situaciones cuando están evaluando los mismos datos con el mismo intervalo de muestreo. En este tema se describe cómo funciona el proceso duper, cómo identificar situaciones que lo utilizan, por qué puede ser recomendable inhabilitarlo y cómo configurar el archivo de entorno del Tivoli Enterprise Monitoring Server para inhabilitarlo.

Proceso duper

Una situación duper se crea y se ejecuta en el agente para recopilar datos del grupo de atributos una vez y cargarlos en el servidor de supervisión. El servidor de supervisión evalúa las diversas situaciones utilizando los datos recopilados por la situación duper. Puesto que la evaluación de situaciones tiene lugar en el servidor de supervisión, cuando el agente se desconecta estas situaciones dejan de evaluarse.

Si los agentes están habitualmente fuera de línea o desconectados del servidor de supervisión y se ejecutan de forma autónoma, probablemente envíen sucesos directamente del agente a un receptor de sucesos que no sea el servidor de supervisión. Puede ser preferible definir *situaciones privadas* en el agente en lugar de utilizar las situaciones de empresa definidas en el servidor de supervisión.

Situaciones aptas para el proceso duper

Para que una situación sea apta para el proceso duper, debe tener estas cualidades:

- Supervisa el mismo grupo de atributos en el mismo sistema gestionado y con el mismo intervalo de supervisión que al menos otra situación
- Solo utiliza la función de fórmula VALUE
- No especifica permanencia, una cláusula Until ni un umbral dinámico con alteración temporal de expresión
- Definido en AutoStart
- No incorpora otra situación
- Coincide con el elemento de visualización de otra situación (sólo se aplica si se utiliza el elemento de visualización)

Consideración de automatización de reflejo

En IBM Tivoli Monitoring V6.3, duper se aplica automáticamente a situaciones con acciones reflejas. No se requiere ninguna configuración adicional.

Si tiene un gran número de situaciones con acciones reflejas establecido en Tivoli Enterprise Portal como ◉ **Ejecutar la acción en el sistema**

gestionado (agente), puede establecer la variable de entorno de agente de supervisión KMS_EVAL_REFLEX_AT_TEMS=Y en el archivo KBBENV para aumentar el nivel de optimización de duper.

Establezca la variable de entorno KMS_EVAL_REFLEX_AT_TEMS en cada servidor de supervisión del entorno para hacer que duper gestione las evaluaciones de las acciones en el servidor de supervisión, mientras que las acciones se siguen dirigiendo a los sistemas gestionados. Si desea implementar esta variable, los sistemas gestionados deben estar conectados a un servidor de supervisión a fin que se puedan ejecutar las acciones.

Atención: Utilice la variable de entorno KMS_EVAL_REFLEX_AT_TEMS con precaución.

Nota: La variable KMS_EVAL_REFLEX_AT_TEMS no tiene ningún efecto en la situación si se ha establecido ◉ **Ejecutar la acción en el sistema de gestión (TEMS)**.

Identificador _Z_ de situación duper
Puede comprobar que una situación de duper está recopilando datos del agente examinando el registro LG0 en el agente, por ejemplo, `C:\ibm\ITM\TMAITM6\logs\Primary_IBM_MyComputer_NT.LG0`. Habrá una entrada que empiece por **_Z_** que muestre que el agente está iniciando una situación en el grupo de atributos que supervisan las múltiples situaciones. Ejemplo: `Starting _Z_WTSYSTEM0 <3207594896,3996125040> for KNT.WTSYSTEM`.

Inhabilitación de duper
Si añade un parámetro al servidor de supervisión, puede inhabilitar el proceso duper. Esto se hace añadiendo esta línea al archivo KBBENV: `CMS_DUPER=NO`

Cuando se reinicia el servidor de supervisión, duper se omite.

Para editar el archivo de variable de entorno del servidor de supervisión, KBBENV en Windows y KDSENV en z/OS, siga estos pasos:

Windows

Utilice Manage Tivoli Enterprise Monitoring Services (Inicio → Programas → IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services) para editar archivos de entorno. Pulse con el botón derecho en el componente que desea modificar y pulse **Avanzado** → **Editar archivo ENV**. Debe reciclar el componente para implementar los cambios.

Linux UNIX

Edite directamente el archivo de entorno. Edite las variables de entorno del archivo `<install_dir>/config/ms.ini` y a continuación reconfigure y reinicie el servidor de supervisión para implementar los cambios.

z/OS

Consulte *Configuración de Tivoli Enterprise Monitoring Server en z/OS* para obtener más información.

Valores de configuración de Tivoli Enterprise Monitoring Automation Server

Tivoli Enterprise Monitoring Automation Server amplía la funcionalidad del concentrador Tivoli Enterprise Portal Server e incluye el proveedor de servicio Open Services Lifecycle Collaboration Performance Monitoring (OSLC).

Edición del Tivoli Enterprise Monitoring Automation Server

Edite el archivo de entorno de Tivoli Enterprise Monitoring Automation Server, KASENV, para volver a configurar los parámetros del servidor de automatización.

Acerca de esta tarea

Siga estos pasos para editar el archivo de entorno del servidor de automatización:

Procedimiento

1. Abra el archivo de entorno en el sistema donde el servidor de supervisión concentrador está instalado:
   - Windows En Manage Tivoli Enterprise Monitoring Services (Inicio → Programas → IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services), pulse con el botón derecho del ratón en Tivoli Enterprise Monitoring Automation Server y pulse **Avanzado → Editar archivo ENV** para abrir el archivo `KASENV`.
   - Linux UNIX Vaya al directorio *`dir_instalación`*`/config` y abra el archivo `as.ini` en un editor de texto.
2. Edite el archivo para habilitar (suprima # al principio de la línea), inhabilite (escriba # al principio de la línea) o modifique cualquiera de las variables de entorno.
3. Guarde el archivo y salga del editor de texto.
4. Pulse **Sí** cuando un mensaje le solicita si desea reciclar el servicio.Debe reciclar el servidor de automatización para implementar los cambios.

Capítulo 5. Habilitación de la autenticación de usuarios

El acceso de inicio de sesión al cliente de Tivoli Enterprise Portal está controladopor las cuentas de usuario que se definen en el Tivoli Enterprise Portal Server. La autenticación de contraseñas está controlada por un registro, el registro de usuarios del sistema operativo del servidor de supervisión concentrador o un registro de usuario LDAP externo que está configurado en el servidor de supervisión concentrador o en el servidor de portal.

El acceso de inicio de sesión de la CLI tacmd y las solicitudes de cliente SOAP para el concentrador de Tivoli Enterprise Monitoring Server se controlan mediante las cuentas de usuario que se definen en el servidor de supervisión concentrador utilizando el registro del sistema operativo del servidor de supervisión o un servidor LDAP externo que está configurado en el servidor de supervisión concentrador.

El acceso de inicio de sesión al IBM Dashboard Application Services Hub se controla por el registro de usuarios del sistema operativo, un registro de usuarios LDAP o un registro de usuarios autónomo personalizado. Si piensa utilizar las aplicaciones de panel de control de supervisión o los paneles de control de supervisión personalizados en IBM Dashboard Application Services Hub, debe configurar el Tivoli Enterprise Portal Server y Dashboard Application Services Hub para utilizar un registro de usuarios LDAP federado y el inicio de sesión único, si desea que los usuarios de paneles de control lancen el cliente de Tivoli Enterprise Portal sin que se les solicite sus credenciales y si desea controlar la autorización para los recursos supervisados por usuario. Vea las hojas de ruta de Capítulo 3, “Preparación de su entorno de panel de control”, en la página 27 para determinar si desea utilizar un registro de usuarios LDAP federado y el inicio de sesión único.

Acceso de inicio de sesión al componente de proveedor de servicios de Open Services Lifecycle Collaboration Performance Monitoring de Tivoli Enterprise Monitoring Automation Server se controla mediante un registro de usuarios LDAP y utilizando el componente de los servicios de seguridad de Jazz for Service Management.

El ID de usuario sysadmin

Se proporciona un ID de usuario **sysadmin** inicial con autorización de administrador completa en la instalación de modo que puede iniciar sesión en el cliente de Tivoli Enterprise Portal y añadir más cuentas de usuario. No se necesita ninguna contraseña para iniciar sesión en el cliente de portal a menos que el servidor de supervisión concentrador se haya configurado para habilitar ☑ **Seguridad: Validar usuario**.

Tivoli Enterprise Portal perfil de usuario

Para iniciar sesión utilizando un cliente de Tivoli Enterprise Portal, un usuario debe estar autenticado por el servidor de portal y tener un ID de usuario de Tivoli Enterprise Portal. Cada ID de usuario que se define en Tivoli Enterprise Portal tiene asignado un conjunto de permisos que determinan las características de cliente de portal que el usuario tiene autorización para ver y utilizar, las aplicaciones supervisadas que el usuario tiene autorización para ver y las vistas de Navigator (y el nivel superior de una vista) a las que el usuario puede acceder.

© Copyright IBM Corp. 2005, 2013

Los ID de usuario que vayan a tener los mismos permisos se pueden organizar en grupos de usuarios para que los cambios en los permisos se apliquen a todos los ID de usuario miembros.

Si Dashboard Application Services Hub y el servidor de portal están configurados para el inicio de sesión único, un ID de usuario de Tivoli Enterprise Portal debe existir para cada usuario de paneles de control de supervisión. La primera vez que un usuario de paneles de control accede a los datos de supervisión, se crea automáticamente un ID de usuario de Tivoli Enterprise Portal para el usuario si no hay ya un ID de usuario correlacionado con el nombre distinguido del usuario LDAP. En este caso, el ID de usuario de Tivoli Enterprise Portal es un ID generado aleatoriamente y el usuario no tiene asignado ningún permiso. Si se están utilizando permisos de Tivoli Enterprise Portal para controlar el acceso a los recursos supervisados en los paneles de control en lugar de políticas de autorización, o si el usuario de paneles de control puede iniciar Tivoli Enterprise Portal, asigne los permisos de ID de usuario y las aplicaciones supervisadas que se pueden acceder.

Para obtener más información sobre la asignación de permisos de Tivoli Enterprise Portal y aplicaciones de supervisión, consulte Capítulo 6, “Utilización de la autorización de usuario de Tivoli Enterprise Portal”, en la página 163.

Autenticación mediante el servidor de supervisión concentrador

Los ID de usuario autenticados mediante el servidor de supervisión concentrador se pueden autenticar mediante el registro del sistema operativo local o un registro de usuarios central externo habilitado para LDAP.

Los ID de usuario que utilizan los mandatos **tacmd** que envían solicitudes al servidor de supervisión concentrador o que realizan solicitudes de servidor SOAP, deben autenticarse mediante el servidor de supervisión concentrador.

Limitaciones:

1. La autentificación LDAP no recibe soporte para servidores de supervisión concentradores en z/OS.
2. El cliente de Tivoli Directory Server LDAP utilizado por Tivoli Enterprise Monitoring Server no soporta referencias LDAP, como las soportadas por Microsoft Active Directory.
3. Cuando el servidor de supervisión concentrador se instala en un sistema operativo distribuido y se utiliza para autenticar usuarios de Tivoli Enterprise Portal, los ID de usuario de Tivoli Enterprise Portal deben tener 10 caracteres o menos. Sin embargo, para los usuarios de cliente SOAP y los usuarios de la CLI **tacmd** que se han autenticado por el servidor de supervisión concentrador, los ID de usuario puede tener hasta 15 caracteres.
4. Cuando el servidor de supervisión concentrador está instalado en z/OS, la longitud del ID de usuario está limitada a 8 caracteres si la autenticación utiliza la seguridad de RACF (Resource Access Control Facility) para z/OS.

Autenticación LDAP a través del servidor de portal

El servidor de portal autentica los usuarios de Tivoli Enterprise Portal, los usuarios de Dashboard Application Services Hub que acceden a los datos de supervisión, usuarios del servicio de representación gráfica de IBM

Tivoli Monitoring y usuarios de la CLI **tacmd** que utilizan mandatos que envían solicitudes al servidor de portal.

De forma predeterminada, el servidor de portal se pone en contacto con el servidor de supervisión concentrador para realizar la autenticación. No obstante, la práctica recomendada es configurar el servidor de portal para realizar su propia autenticación a través de un registro de usuarios LDAP federado para estos casos:

- Tivoli Enterprise Portal se inicia desde otras aplicaciones basadas en web y no desea que los usuarios vuelvan a especificar sus credenciales.
- Tivoli Enterprise Portal se utiliza para lanzar otras aplicaciones basadas en web o habilitadas para web y no desea que los usuarios vuelvan a especificar sus credenciales.
- IBM Dashboard Application Services Hub se utiliza para visualizar los datos de supervisión recuperados utilizando el componente de proveedor de datos de panel de instrumentos del servidor de portal. La práctica recomendada es utilizar el inicio de sesión único en este caso, de modo que los usuarios de paneles de control puedan lanzar Tivoli Enterprise Portal y el usuario no tiene que volver a especificar sus credenciales. Además, el inicio de sesión único deben utilizarse si desea controlar la autorización para los recursos supervisados por usuario.
- El servicio web de representación gráfica de IBM Tivoli Monitoring se utiliza por otra aplicación como Tivoli Integrated Portal.

Cuando el servidor de portal está configurado para autenticar con un servidor LDAP, los usuarios inician sesión en Tivoli Enterprise Portal utilizando su nombre distinguido relativo de LDAP (que normalmente se correlaciona con los valores de `cn=` o `uid=`) y no su ID de usuario de Tivoli Enterprise Portal. Debido a que el servidor de portal utiliza los ID de usuario de Tivoli Enterprise Portal para controlar los permisos, debe correlacionar los nombres distinguidos de LDAP con los ID de usuario de Tivoli Enterprise Portal. Aunque los ID de usuario de Tivoli Enterprise Portal están limitados a 10 caracteres, los nombres distinguidos de LDAP puede ser mucho más largos.

Puede configurar el servidor de portal para utilizar un registro de usuarios LDAP mediante el programa de utilidad Manage Tivoli Enterprise Monitoring Services, la interfaz de línea de mandatos **itmcmd** en Linux y UNIX, o la consola de administración de TEPS/e (ISCLite). Si configura LDAP utilizando la consola de administración de TEPS/e, debe reiniciar manualmente ISCLite a través de Manage Tivoli Enterprise Monitoring Services después de cada reinicio del servidor de portal.

Autenticación mediante el servidor de supervisión concentrador y el servidor de portal El servidor de supervisión concentrador y el servidor de portal pueden conectarse al mismo servidor LDAP si tiene usuarios que necesitan acceso de inicio de sesión en ambos servidores. Puede utilizar el mismo ID de usuario para iniciar sesión en el cliente de Tivoli Enterprise Portal que se utiliza para el mandato **tacmd login**. Para ello, debe ir a **Administrar usuarios** en el cliente de portal para correlacionar el ID de usuario de Tivoli Enterprise Portal con el nombre distinguido utilizado por el registro de usuario LDAP del servidor de portal que, de forma predeterminada, utiliza `o=ITMSSOEntry` y *no* el nombre distinguido que utiliza `o=DEFAULTWIMITMBASEDREALM`.

Migración de la autenticación de LDAP del concentrador al servidor de portal Si el concentrador Tivoli Enterprise Monitoring Server ya se ha

configurado para autenticar usuarios en un registro de usuarios LDAP, y ahora desea configurar el servidor de portal para utilizar un registro de usuarios LDAP, tiene que cambiar el nombre distinguido que se ha establecido para los ID de usuario en la ventana Administrar usuarios de Tivoli Enterprise Portal.

Hoja de ruta para la autenticación de usuarios

Utilice la siguiente hoja de ruta para comenzar con la autenticación de usuarios.

Tabla 8. Hoja de ruta para la autenticación de usuarios

Tarea	Dónde encontrar información
Configure la autenticación de usuarios a través del servidor de supervisión concentrador utilizando el registro de usuarios del sistema operativo local o un registro de usuarios LDAP.	"Autenticación de usuarios a través del servidor de supervisión concentrador"
Configure el servidor de portal para utilizar un registro de usuarios LDAP para autenticar los usuarios cuando el inicio de sesión único se utiliza con IBM Dashboard Application Services Hub u otras aplicaciones.	Si el servidor de supervisión concentrador no utiliza un registro de usuarios LDAP, consulte "Autenticación de usuarios LDAP a través del servidor de portal" en la página 94. Si el servidor de supervisión concentrador utiliza un registro de usuarios LDAP, consulte "Migración de la autenticación LDAP del servidor de supervisión al servidor de portal" en la página 124.
Configure Tivoli Enterprise Monitoring Automation Server y su proveedor de servicios de Performance Monitoring para autenticar las solicitudes HTTP GET de clientes OSLC.	"Autenticación a través del Tivoli Enterprise Monitoring Automation Server" en la página 126

Autenticación de usuarios a través del servidor de supervisión concentrador

La autenticación de usuarios a través del servidor de supervisión concentrador utiliza el registro de usuarios del sistema operativo local o un registro central externo habilitado para LDAP.

Requisitos previos para configurar la autenticación en el servidor de supervisión concentrador

Realice estas tareas antes de habilitar la autenticación de usuarios en el servidor de supervisión concentrador.

Acerca de esta tarea

Tabla 9. Tareas a seguir antes de configurar la autenticación

Tarea	Dónde encontrar información
Configurar cuentas de usuario de Tivoli Enterprise Portal.	"Añadir ID de usuario" en la página 171

Tabla 9. Tareas a seguir antes de configurar la autenticación (continuación)

Tarea	Dónde encontrar información
Configurar cuentas de usuario en el registro de autenticación.	Consulte la documentación para configurar cuentas de usuario en el sistema operativo local o en el servidor de directorios de LDAP. Para obtener información sobre la configuración de usuarios en z/OS, consulte *Configuración de Tivoli Enterprise Monitoring Server en z/OS*. **Nota:** • Cuando el servidor de supervisión concentrador se instala en un sistema operativo distribuido y se utiliza para autenticar usuarios de Tivoli Enterprise Portal, los ID de usuario de Tivoli Enterprise Portal deben tener 10 caracteres o menos. Sin embargo, los usuarios de supervisión de concentrador que solo utilizan los mandatos de la CLI **tacmd** que envían solicitudes al concentrador o que envían solicitudes SOAP, pueden tener un ID de usuario de hasta 15 caracteres. Las contraseña de los usuarios de mandatos tacmd y SOAP también están limitadas a 15 caracteres o menos. • Cuando el servidor de supervisión concentrador está instalado en z/OS, la longitud del ID de usuario está limitada a 8 caracteres si la autenticación utiliza la seguridad de RACF (Resource Access Control Facility) para z/OS.
Configuración de la comunicación TLS/SSL entre el concentrador y un servidor LDAP.	"Configuración de la comunicación TLS/SSL entre el servidor de supervisión concentrador y el servidor LDAP" en la página 218

Si tiene intención de realizar la autenticación mediante el Tivoli Enterprise Monitoring Server concentrador, asegúrese de que las cuentas de usuario para los ID de inicio de sesión del Tivoli Enterprise Portal Server estén configuradas en el registro de autenticación antes de que se habilite la autenticación. Como mínimo, añada el ID de usuario **sysadmin** al registro local del usuario del sistema operativo en el sistema concentrador, de modo que **sysadmin** pueda iniciar sesión después de que se haya habilitado la autenticación.

Nota: En Windows, el instalador crea una cuenta de usuario **sysadmin** en el registro de usuarios de Windows y le solicita que especifique una contraseña para dicho ID. La contraseña no se necesita a no ser que la autenticación esté habilitada.

Consejo: El instalador de Windows no establece la opción "La contraseña nunca caduca" cuando crea la cuenta **sysadmin**. Si no establece esta opción, la contraseña caducará según la política de seguridad del sistema concentrador y no podrá iniciar una sesión en el servidor de portal. Utilice las Herramientas administrativas de Windows para asegurarse de que la opción "La contraseña nunca caduca" esté seleccionada para la cuenta de usuario **sysadmin**.

Antes de habilitar la autenticación, debe obtener la siguiente información:

Procedimiento

- Si está utilizando un servidor LDAP externo para la autenticación, obtenga la información que se muestra en la siguiente tabla del administrador de LDAP antes de configurar la autenticación de usuarios.

Tabla 10. Parámetros de configuración de LDAP

Parámetro	Descripción

Filtro de usuarios de LDAP	Los atributos utilizados para correlacionar los ID de usuario de Tivoli Enterprise Portal con los ID de inicio de sesión de LDAP. El atributo debe contener el mismo nombre que el ID de inicio de sesión de Tivoli Enterprise Portal. Normalmente, el ID de usuario del portal se convertirá en "%v" en el filtro de usuarios LDAP. Por ejemplo:
	`IBM Tivoli Directory Server: (&(mail=%v@yourco.com) (objectclass=inetOrgPerson))`
	`Microsoft Windows Active Directory: (&(mail=%v@yourco.com) (objectclass=user))`
	`Sun Java System Directory Server: (&(mail=%v@yourco.com) (objectclass=inetOrgPerson)`
	
	No todos los LDAP tienen atributo de correo para la persona. Por ejemplo, es posible que el administrador de LDAP sólo establezca el nombre común, en cuyo caso el filtro se parecería al siguiente:
	`(&(cn=%v) (objectclass=inetOrgPerson))`
	
	El administrador de Tivoli Enterprise Portal debe verificar exactamente qué atributo de LDAP se debe utilizar para buscar el usuario. Con Active Directory, por ejemplo, `cn` equivale al Nombre completo del usuario de Active Directory y éste *debe* ser exactamente igual que el usuario de Tivoli Monitoring y no puede contener espacios (por ejemplo, "S Smith" debe ser "SSmith").

Base LDAP	El nodo base de LDAP del registro de usuarios de LDAP que se utiliza en búsquedas de usuarios. Por ejemplo:
	`IBM Tivoli Directory Server: dc=yourdomain,dc=yourco,dc=com`
	`Microsoft Windows Active Directory: dc=yourdomain,dc=yourco,dc=com`
	`Servidor de Sun Java System Directory: dc=yourdomain,dc=yourco,dc=com`

ID de vinculación LDAP	El ID de usuario de LDAP para autenticación de vinculación, en notación de LDAP. Este ID de usuario de LDAP debe tener autorización para buscar usuarios de LDAP. Este valor se puede omitir si un usuario anónimo puede buscar usuarios de LDAP.
Contraseña de vinculación LDAP	La contraseña para la autenticación de vinculación LDAP. Este valor se puede omitir si un usuario anónimo puede vincular con el servidor de LDAP. El instalador cifra este valor.
Nombre de host LDAP	El nombre de host de servidor LDAP. Este valor se puede omitir si el servidor LDAP está a la escucha en el mismo host que Tivoli Enterprise Monitoring Server. (El valor predeterminado es localhost).
Número de puerto LDAP	El número de puerto del servidor LDAP. Este valor se puede omitir si el servidor de LDAP está escuchando en el puerto 389.

- Si está utilizando Microsoft Active Directory, consulte "Autenticación de usuarios de LDAP mediante Microsoft Active Directory" en la página 127 para obtener información sobre la planificación y la configuración específica para este tipo de servidor LDAP.
- Si piensa utilizar la comunicación TLS/SSL entre el concentrador de Tivoli Enterprise Monitoring Server y el servidor LDAP, obtenga la información descrita en la tabla siguiente.

Tabla 11. Parámetros TLS/SSL para la comunicación entre el concentrador y el servidor LDAP

Parámetro	Descripción
Archivo de almacén de claves de LDAP	La ubicación del archivo de base de datos del almacén de claves de GSKit. Puede especificar la ubicación que desee. Por ejemplo: `C:\IBM\ITM\keyfiles`
Stash de almacén de claves de LDAP	La ubicación del archivo de contraseñas de base de datos GSKit. Por ejemplo: `C:\IBM\ITM\keyfiles\keyfile.sth`
Etiqueta de almacén de claves de LDAP	La etiqueta de almacén de claves. Por ejemplo: `IBM_Tivoli_Monitoring_Certificate`
Contraseña de almacén de claves de LDAP	La contraseña necesaria para acceder al almacén de claves.

Procedimiento de configuración

Configure la autenticación de usuarios en el servidor de supervisión concentrador basado en Windows, Linux o UNIX.

Para obtener instrucciones para configurar la autenticación en un servidor de supervisión concentrador instalado en z/OS, consulte *IBM Tivoli Management Services en z/OS: Configuración de Tivoli Enterprise Monitoring Server en z/OS*. No se da soporte a la autenticación mediante un registro de LDAP externo en un concentrador z/OS.

Windows: Configuración de la autenticación de usuarios a través del concentrador

Configure un Tivoli Enterprise Monitoring Server concentrador en Windows para autenticar usuarios.

Acerca de esta tarea

Para configurar la autenticación de usuarios a través del concentrador en un sistema Windows, complete el procedimiento siguiente:

Procedimiento

1. Seleccione **Inicio → Programas → IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services**
2. Pulse con el botón derecho del ratón en el servidor de supervisión concentrador y pulse en **Reconfigurar**.
3. En la ventana de configuración que se muestra, seleccione **Seguridad: Validar usuario**. La opción **Seguridad de LDAP: Validar usuario con LDAP** para a estar disponible.
4. Si desea utilizar LDAP para la autenticación de usuarios, marque la opción **Validar usuario con LDAP** y luego pulse **Aceptar** para abrir la ventana de LDAP. Si desea utilizar el registro local, salte al paso 7.
5. Especifique los valores de LDAP necesarios correspondientes a su sitio.

6. Si desea utilizar TLS/SSL para asegurar las comunicaciones entre el concentrador y el servidor LDAP, marque **Comunicaciones SSL de LDAP: ¿Utilizar SSL?** y proporcione los valores adecuados. Si es necesario, especifique una contraseña para el almacén de claves.
7. Pulse **Aceptar**. Aparecerá la ventana Configuración de TEMS concentrador.
8. Pulse **Aceptar** para aceptar los valores actuales.
9. En la ventana Manage Tivoli Enterprise Monitoring Services, reinicie el servidor de supervisión concentrador pulsando con el botón derecho del ratón en su nombre y seleccionado **Iniciar**.

Linux o UNIX: Configuración de la autenticación de usuarios a través del concentrador

Configure la autenticación de usuarios para un entorno en el que se ha instalado el concentrador en Linux o UNIX.

Configuración de la autenticación de usuarios desde la línea de mandatos:

Con el procedimiento siguiente puede configurar la autenticación de usuarios desde la línea de mandatos.

Acerca de esta tarea

Para configurar el concentrador desde la línea de mandatos, siga este procedimiento:

Procedimiento

1. Vaya al directorio *dir_instalación*/bin y ejecute el mandato siguiente:

   ```
   ./itmcmd config -S -t nombre_tems
   ```

   donde *dir_instalación* es el directorio de instalación de IBM Tivoli Monitoring y *nombre_tems* es el nombre del servidor de supervisión concentrador. El directorio de instalación predeterminado en Linux o UNIX es /opt/IBM/ITM. Verá la siguiente solicitud:

   ```
   Configurando TEMS...
   ```
2. Acepte los valores predeterminados para las siguientes solicitudes. Los valores predeterminados deberían reflejar las secciones realizadas durante la instalación.
3. Cuando vea la solicitud:

   ```
   Seguridad: ¿Validar usuario?
   ```

   escriba 1 y pulse Intro.
4. Si no desea utilizar LDAP para la autenticación, pulse Intro para seleccionar el valor predeterminado (NO). Si desea utilizar LDAP para la autenticación, escriba 1 y pulse Intro. Responda a las siguientes solicitudes especificando los valores. Para habilitar las comunicaciones TLS/SSL entre el concentrador y el servidor LDAP, especifique los valores adecuados.
5. Acepte los valores predeterminados para Tivoli Event Integration Facility y Workflow Policy/Tivoli Emitter Agent Forwarding.
6. En la siguiente solicitud, escriba 6 (Guardar/salir) y pulse Intro:

   ```
   Concentradores
   ##      Nombre_CMS
   1       ip.pipe:elsrmt1[4441]
   ```
7. Reinicie el Tivoli Enterprise Monitoring Server concentrador:

```
./itmcmd server stop nombre_tems
./itmcmd server start nombre_tems
```

Configuración de la autenticación mediante Manage Tivoli Enterprise Monitoring Services:

Configuración de la autenticación mediante Manage Tivoli Enterprise Monitoring Services.

Acerca de esta tarea

Para configurar la autenticación utilizando Manage Tivoli Enterprise Monitoring Services, siga estos pasos:

Procedimiento

1. Vaya al directorio *install_dir*/bin y ejecute el mandato siguiente:
   ```
   ./itmcmd manage [-h install_dir]
   ```

   donde *install_dir* es el directorio de instalación para IBM Tivoli Monitoring. El directorio de instalación predeterminado en Linux o UNIX es /opt/IBM/ITM. Se mostrará la ventana Manage Tivoli Enterprise Monitoring Services.
2. Pulse con el botón derecho del ratón en el servidor de supervisión y pulse en **Configurar**.
3. Pulse en el separador **Valores avanzados**. Seleccione **Seguridad: Validar usuario**.
4. Si desea utilizar LDAP para autenticar los usuarios en lugar del registro del sistema, seleccione **Autenticación de usuarios LDAP**.
5. Pulse **Aceptar**. Si ha seleccionado la opción LDAP, aparecerá el panel de configuración de LDAP.
6. Especifique los valores y pulse **Aceptar**.
7. Pulse **Aceptar**.
8. Reinicie el servidor de supervisión concentrador utilizando uno de los métodos siguientes:
   - En la ventana Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho del ratón en el servidor de supervisión concentrador y seleccione **Reciclar**.
   - En la línea de mandatos, especifique:
     ```
     ./itmcmd server stop nombre_tems
     ./itmcmd server start nombre_tems
     ```

Información sobre ldapsearch para LDAP

L es una herramienta de línea de mandatos disponible en proveedores de servidores LDAP que puede utilizar para verificar la información de LDAP antes de la configuración y para solucionar los problemas que encuentre durante la configuración. Puede ahorrarse bastante tiempo ejecutando **ldapsearch** para verificar la información de LDAP antes de configurar un servidor de supervisión concentrador para la autentificación de LDAP.

Nota: Utilice esta herramienta únicamente si está configurando la autenticación de LDAP a través del servidor de supervisión concentrador. Si está configurando la autenticación de LDAP a través del Tivoli Enterprise Portal Server, utilice la consola de administración de TEPS/e (servidor de extensión del Tivoli Enterprise Portal Server) para verificar los parámetros de configuración.

Lo recomendable es que el administrador de LDAP ejecute **ldapsearch**. El mandato **ldapsearch** funciona de forma parecida al mandato ping. Si los valores utilizados como entrada para el mandato son correctos, el mandato devuelve una versión de los valores que se utilizan en la búsqueda. Si los valores no son correctos, el mandato no devuelve nada o devuelve un mensaje de error que le puede ayudar a determinar qué valor está implicado, como por ejemplo una contraseña incorrecta o un nombre de host erróneo.

ldapsearch de IBM Tivoli Directory Server se adapta mejor a IBM Tivoli Monitoring. **ldapsearch** de Tivoli Directory Server soporta las operaciones de TLS/SSL de GSkit que se utilizan en Tivoli Monitoring y tiene opciones de línea de mandatos adicionales que soportan las búsquedas TLS/SSL de LDAP. Tivoli Monitoring no incluye ldapsearch en instalaciones de producción. Para obtener información sobre ldapsearch de Tivoli Directory Server, consulte "Programas de utilidad de cliente" en *Tivoli Directory Server Command Reference* en Centro de información de IBM Security Systems.

ldp.exe es una herramienta de búsqueda de LDAP de Microsoft Windows que tiene las mismas funciones básicas que la herramienta **ldapsearch**. Puede descargar esta herramienta del sitio web de Microsoft para su versión de Windows. La herramienta **ldp.exe** se incluye en las herramientas de soporte del CD de Windows Server 2003. Para obtener información sobre cómo utilizar el mandato **ldp** de Microsoft Windows, consulte http://support.microsoft.com/kb/224543.

Otra herramienta que le puede ayudar en la configuración de LDAP es la herramienta LDAP Browser de Softerra.

opciones de línea de mandatos de ldapsearch

La tabla siguiente lista las opciones de ldapsearch de la línea de mandatos y sus parámetros correspondientes ubicados en el archivo de configuración del servidor de supervisión.

Tabla 12. Opciones de línea de mandatos de ldapsearch y parámetros de configuración correspondientes del servidor de supervisión

Opción	Descripción	Parámetro correspondiente en el archivo de configuración del servidor de supervisión
-h *host*	El nombre de host del servidor LDAP.	KGL_LDAP_HOST_NAME
-p *puerto*	El número de puerto LDAP.	KGL_LDAP_PORT
-D *dn*	El ID de vinculación LDAP No utilice esta opción de línea de mandatos si no es necesario un ID de vinculación LDAP.	KGL_LDAP_BIND_ID
-w contraseña	La contraseña de vinculación LDAP Utilice el valor descifrado para la opción de línea de mandatos de **ldapsearch**. No utilice esta opción de línea de mandatos si no es necesario un ID de vinculación LDAP.	KGL_LDAP_BIND_PASSWORD
-b dn_base	La base LDAP.	KGL_LDAP_BASE
-K archivoclaves	El archivo de almacén de claves de LDAP (solo se utiliza con SSL de LDAP).	KGL_KEYRING_FILE

Tabla 12. Opciones de línea de mandatos de ldapsearch y parámetros de configuración correspondientes del servidor de supervisión (continuación)

Opción	Descripción	Parámetro correspondiente en el archivo de configuración del servidor de supervisión
-P ctr_claves	La contraseña del almacén de claves de LDAP (solo se utiliza con LDAP TLS/SSL). Utilice el valor descifrado para la opción de línea de mandatos de ldapsearch.	Valor descifrado de KGL_KEYRING_PASSWORD
-N nombre_claves	La etiqueta del almacén de claves de LDAP (solo se utiliza con SSL de LDAP).	KGL_KEYRING_LABEL
Filtro	Filtro de usuarios LDAP. Sustituya `%v` por el ID de usuario de Tivoli Enterprise Portal, SOAP o tacmd.	KGL_LDAP_USER_FILTER

Mandato `ldapsearch` de ejemplo (no TLS/SSL)

A continuación se muestra un mandato ldapsearch de ejemplo y sus datos de salida correspondientes para una configuración con TLS/SSL inhabilitado.

Utilice los siguientes valores para configurar el mandato ldapsearch en un entorno en el que TLS/SSL no está habilitado y no se necesita ningún ID de usuario ni contraseña:

Nombre de host LDAP	ldap.itm62.com
Nombre de puerto LDAP	389
Base LDAP	ou=itm62users,o=itm62.com
Filtro de usuarios LDAP	"(mail=%v@us.ibm.com)"

Utilice la siguiente sintaxis de mandato para esta configuración de muestra:

```
ldapsearch -h ldap.itm62.com -p 389 -b "ou=itm62users,o=itm62.com"
 -s sub "(mail=sysadmin@itm62.com)"
```

Se genera la siguiente salida:

```
uid=12345678,ou=itm62users,o=itm62.com
objectClass=person
objectClass=organizationalPerson
...
mail=sysadmin@itm62.com
...
```

Mandato `ldapsearch` de ejemplo (con TLS/SSL)

A continuación se muestra un mandato ldapsearch de ejemplo y sus datos de salida correspondientes para una configuración con TLS/SSL habilitado.

Utilice los siguientes valores para configurar el mandato ldapsearch en un entorno en el que TLS/SSL está habilitado y se necesita un ID de enlace y una contraseña:

Nombre de host LDAP	ldap.itm62.com
Nombre de puerto LDAP	636
ID de vinculación LDAP	uid=1,ou=itm62users,o=itm62.com

Contraseña de vinculación LDAP	itm62
Base LDAP	ou=itm62users,o=itm62.com
Almacén de claves LDAP	C:\IBM\ITM\itm62keyfiles\keyfile.kdb
Stash de claves LDAP	C:\IBM\ITM\itm62keyfiles\keyfile.sth
Etiqueta de almacén de claves LDAP	BM_Tivoli_Monitoring_Certificate
Contraseña de almacén de claves LDAP	itm62
Filtro de usuarios LDAP	"(mail=%v@us.ibm.com)"

Utilice la siguiente sintaxis de mandato para esta configuración de muestra:

```
ldapsearch -h ldap.itm62.com -p 636 -D uid=1,ou=itm62users,o=itm62.com
    -w itm62 -b "ou=itm62users,o=itm62.com" -s sub
    -K C:\IBM\ITM\itm62keyfiles\keyfile.kdb -P itm62
    -N "IBM_Tivoli_Monitoring_Certificate" "(mail=sysadmin@itm62.com)"
```

Se genera la siguiente salida:

```
uid=12345678,ou=itm62users,o=itm62.com
objectClass=person
objectClass=organizationalPerson
...
mail=sysadmin@itm62.com
...
```

Autenticación de usuarios LDAP a través del servidor de portal

Puede configurar el Tivoli Enterprise Portal Server para utilizar un registro de usuarios LDAP para autenticar usuarios.

Esto es necesario si tiene la intención de proporcionar la prestación de inicio de sesión único (SSO) para estos casos:

- Tivoli Enterprise Portal se inicia desde otras aplicaciones basadas en web y no desea que los usuarios vuelvan a especificar sus credenciales.
- Tivoli Enterprise Portal se utiliza para lanzar otras aplicaciones basadas en web o habilitadas para web y no desea que los usuarios vuelvan a especificar sus credenciales.
- IBM Dashboard Application Services Hub se utiliza para visualizar los datos de supervisión recuperados utilizando el componente de proveedor de datos de panel de instrumentos del servidor de portal. La práctica recomendada es utilizar el inicio de sesión único en este caso, de modo que los usuarios de paneles de control puedan lanzar Tivoli Enterprise Portal y el usuario no tiene que volver a especificar sus credenciales. Además, el inicio de sesión único deben utilizarse si desea controlar la autorización para los recursos supervisados por usuario.
- El servicio web de representación gráfica de IBM Tivoli Monitoring se utiliza por otra aplicación como Tivoli Integrated Portal.

Requisitos previos para configurar la autenticación LDAP en el servidor de portal

Antes de configurar la autenticación LDAP en el Tivoli Enterprise Portal Server, tiene que crear las cuentas de usuario en Tivoli Enterprise Portal y en el registro LDAP de autenticación y tener a mano los parámetros de configuración del registro LDAP.

Verifique los ID de usuario en el registro de LDAP

Añada o verifique los ID de usuario del registro, pero *no* cree ninguna cuenta para **sysadmin** hasta que haya habilitado la autenticación y haya iniciado una sesión en Tivoli Enterprise Portal.

El nombre de usuario predeterminado para el administrador de los Servicios ampliados de Tivoli Enterprise Portal Server (TEPS/e) es **wasadmin**. Si este UID se ha añadido al registro, solicite al administrador del registro de usuarios que cambie el nombre o que elimine la entrada. En un registro de usuarios de LDAP federado, dos entradas con el mismo nombre causan un conflicto.

Una práctica recomendada consiste en no añadir **sysadmin** al registro de usuarios de LDAP. Si el servidor LDAP no está disponible, no puede iniciar la sesión en Tivoli Enterprise Portal utilizando cuentas de usuarios LDAP, pero puede iniciar sesión en el portal utilizando **sysadmin** porque está correlacionado con el reino predeterminado de Tivoli Monitoring que se autentica por el servidor de supervisión concentrador.

Configurar cuentas de usuario de Tivoli Enterprise Portal.

Añada los ID de usuario que tiene intención de autenticar con un registro de LDAP. Esto se puede hacer antes o después de que se haya configurado el servidor de portal para la autenticación de LDAP. Tras la configuración de LDAP, tiene que volver a la ventana Administrar usuarios en el cliente de portal para asociar el ID de usuario a su nombre distinguido desde el registro de usuarios de LDAP.

Windows **La contraseña de sysadmin**

El instalador de IBM Tivoli Monitoring Windows crea una cuenta de usuario **sysadmin** en el registro de usuarios de Windows del servidor de supervisión concentrador y le solicita que especifique una contraseña para dicho ID. La contraseña no se necesita a no ser que la autenticación esté habilitada.

El instalador no establece la opción “La contraseña nunca caduca” cuando crea la cuenta **sysadmin**. Si no establece esta opción, la contraseña caducará según la política de seguridad del Tivoli Enterprise Monitoring Server concentrador y no podrá iniciar una sesión en el servidor de portal. Utilice las herramientas administrativas de Windows para asegurarse de que la opción “La contraseña nunca caduca” esté seleccionada para la cuenta de usuario **sysadmin**.

Información sobre configuración de LDAP

Obtenga la información que se muestra en la siguiente tabla del administrador de LDAP antes de configurar el servidor de portal para la autenticación de usuarios de LDAP. El servidor de portal y las aplicaciones SSO participantes deben estar configurados para utilizar el mismo registro de usuarios LDAP.

Tabla 13. Parámetros de configuración de LDAP

Parámetro	Descripción
Tipo de LDAP	Se puede definir uno de los siguientes tipos de servidores de LDAP ante el servidor de portal utilizando los programas de utilidad de instalación y configuración de Tivoli Management Services: • Active Directory Server 2000 • Active Directory Server 2003 • Active Directory Server 2008 • Active Directory Server 2008 R2 • Tivoli Directory Server 6.x • Otro Se especifica **Otro** si está configurando un tipo diferente de servidor LDAP, tiene previsto habilitar TLS/SSL entre el servidor de portal y el servidor LDAP, o debe especificar parámetros de configuración avanzada de LDAP además de los listados en esta tabla. Cuando selecciona **Otro**, debe utilizar la TEPS/e consola de administración para configurar y modificar los detalles del registro de usuarios LDAP. Consulte el apartado "Utilización de la consola de administración de TEPS/e" en la página 110.
Base LDAP	Este parámetro especifica el nombre distinguido (DN) para la entrada base en el registro LDAP. Es el punto de partida para las búsquedas de usuario en el servidor LDAP. Por ejemplo, para un usuario con un nombre distinguido de `cn=John Doe,ou=Rochester,o=IBM,c=US`, especifique `ou=Rochester,o=IBM,c` para este parámetro. **Nota:** Si utiliza la TEPS/e consola de administración para configurar LDAP, este parámetro se denomina **Nombre distinguido de la entrada base en el repositorio** en la TEPS/e consola de administración.

Tabla 13. Parámetros de configuración de LDAP (continuación)

Parámetro	Descripción
Entrada base de DN de LDAP	El valor predeterminado es `o=ITMSSOEntry`. Sin embargo, la práctica recomendada es elegir un valor que tenga más significado para su organización. Normalmente, se establece este parámetro en el nombre distinguido de la entrada base en el registro LDAP para los usuarios de servidor de portal. Por ejemplo, para un usuario con un nombre distinguido de `cn=John Doe,ou=Rochester,o=IBM,c=US`, especifique `ou=Rochester,o=IBM,c` para este parámetro. Sin embargo, cuando se están configurando varios repositorios LDAP para el servidor de portal, utilice este campo para definir un nombre distinguido (DN) adicional que identifica de forma exclusiva el conjunto de usuarios LDAP desde este servidor LDAP. Por ejemplo, el registro `LDAP1` y el registro `LDAP2`, pueden utilizar los dos `o=ibm,c=us` como su entrada base. En este caso, utilice este parámetro para especificar de forma exclusiva una entrada base diferente para cada servidor LDAP dentro del reino. Por ejemplo, especifique `o=ibm1,c=us` al configurar el registro `LDAP1` y `o=ibm2,c=us` al configurar el registro `LDAP2`. **Nota:** Si dispone de varios registros LDAP, no pueden contener nombres de usuario que se solapen. El valor de este parámetro se visualiza en el diálogo Administrar usuarios de Tivoli Enterprise Portal cuando se listan los nombres distinguidos que se pueden correlacionar con los ID de usuario de Tivoli Enterprise Portal. **Nota:** Si utiliza la TEPS/e consola de administración para configurar LDAP, este parámetro se denomina **Nombre distinguido de la entrada base que identifica de forma exclusiva este conjunto de entradas en el reino** en la TEPS/e consola de administración.
ID de vinculación LDAP	Este es el ID de usuario de LDAP para la autenticación de vinculación, en notación de LDAP, y debe tener autorización para buscar usuarios de LDAP. El ID de vinculación se puede omitir si un usuario anónimo puede buscar usuarios de LDAP.
Contraseña de vinculación LDAP	Esta es la contraseña de usuario de LDAP para la autenticación de vinculación de LDAP. Este valor se puede omitir si un usuario anónimo puede vincular con el servidor de LDAP. El instalador cifra este valor.
Número de puerto LDAP	Este es el número de puerto en el que escucha el servidor LDAP. Este valor se puede omitir si el puerto es 389.
Nombre de host LDAP	Es el nombre de host o la dirección IP del servidor LDAP. se puede omitir si el servidor LDAP está en el mismo sistema que el servidor de portal. Si utiliza Microsoft Active Directory, utilice el nombre de host del controlador de dominio del Active Directory Forest que aloja las cuentas de usuario para el servidor de portal.

Información para la configuración de SSO

Si tiene previsto configurar SSO, trabaje con los administradores de las otras aplicaciones que piensan utilizar el inicio de sesión único con el servidor de portal, para determinar los valores para los parámetros listados en la tabla siguiente. Cada aplicación SSO participante debe tener el mismo valor para estos parámetros.

Tabla 14. Parámetros de SSO

Parámetro	Descripción
Nombre de dominio	Este es el dominio de Internet o Intranet para el que se ha configurado SSO, por ejemplo, micompañía.com. Solo las aplicaciones disponibles en este dominio o sus subdominios se habilitan para SSO. Ejemplo: `ibm.com`
Nombre de territorio	Un reino identifica un conjunto de repositorios federados en TEPS/e y otros WebSphere Application Server. Puede elegir su propio nombre de reino, pero el valor debe ser el mismo en todas las aplicaciones que se configuran para SSO dentro del dominio especificado. Las aplicaciones configuradas para el mismo nombre de dominio, pero para otro nombre de reino, no funcionan como parte de la misma infraestructura de SSO. Ejemplo: `ibm_tivoli_sso`

Acerca del inicio de sesión único

La característica de inicio de sesión único (SSO) proporciona a los usuarios la capacidad de iniciar otras aplicaciones basadas en la web o habilitadas para la web de Tivoli desde Tivoli Enterprise Portal, o iniciar Tivoli Enterprise Portal desde otras aplicaciones, sin tener que volver a especificar sus credenciales. También se utiliza cuando IBM Dashboard Application Services Hub recupera datos de supervisión del servidor de portal u otra aplicación utiliza el servicio de representación gráfica de IBM Tivoli Monitoring.

Las credenciales autenticadas se comparten entre las aplicaciones participantes utilizando señales LTPA (Lightweight Third Party Authentication). Lea este tema para ver el uso y los requisitos de SSO.

Inicio de sesión de usuario
Los usuarios inician una sesión en una de las aplicaciones participantes, autentican su ID de usuario y contraseña y luego inician desde la aplicación original en otra aplicación para ver datos relacionados o para realizar acciones necesarias sin tener que volver a especificar su ID de usuario y contraseña.

Cliente de navegador de Tivoli Enterprise Portal o cliente de Java Web Start
Con un cliente de navegador o un cliente de Java Web Start, puede iniciar otra aplicación web de Tivoli participante desde Tivoli Enterprise Portal utilizando **Iniciar aplicación** o escribiendo el URL de la aplicación en una vista del navegador.

Puede iniciar el cliente de navegador de Tivoli Enterprise Portal desde una aplicación web habilitada para SSO. SSO también recibe soporte cuando se inicia el cliente Java Web Start.

Nota: Si utiliza SSO y desea utilizar el cliente de navegador en el mismo sistema que el Tivoli Enterprise Portal Server, debe reconfigurar el cliente para que utilice el nombre completo del sistema host.

Cliente de escritorio de Tivoli Enterprise Portal
Con el cliente de escritorio, puede iniciar otra aplicación desde un espacio de trabajo utilizando SSO. Para ello, especifique el URL de la aplicación en el campo de dirección de una vista de navegador. Sin embargo, no puede iniciar Tivoli Enterprise Portal desde otra aplicación en el cliente de escritorio.

Dashboard Application Services Hub

Los usuarios de paneles de control inician sesión en IBM Dashboard Application Services Hub. Cuando acceden a un panel de control que visualiza datos de supervisión, el concentrador de paneles de control envía una solicitud al componente de proveedor de datos de panel de instrumentos del servidor de portal e incluye la señal LTPA del usuario que ha iniciado sesión. El servidor de portal valida la señal LTPA, extrae el ID de usuario LDAP de la señal LTPA, y determina qué recursos supervisados el usuario está autorizado a acceder.

Servicio web de representación gráfica de IBM Tivoli Monitoring

Cuando los usuarios inician sesión en Tivoli Integrated Portal, pueden acceder a una página con un diagrama configurado para utilizar el servicio web de representación gráfica de IBM Tivoli Monitoring. Se envía una solicitud al servicio web de representación gráfica en el servidor de portal e incluye una señal LTPA del usuario que ha iniciado sesión. El servidor de portal valida la señal LTPA, extrae el ID de usuario LDAP de la señal LTPA, y determina qué recursos supervisados el usuario está autorizado a acceder.

Las aplicaciones habilitadas para SSO pertenecen al mismo dominio de seguridad y territorio

Para habilitar SSO, se debe configurar la autenticación a través del Tivoli Enterprise Portal Server para un registro de usuarios LDAP externo que se comparte por todas las aplicaciones participantes de Tivoli. También se denomina registro de usuarios LDAP federado. Todas las aplicaciones participantes deben configurarse para SSO y deben pertenecer al mismo dominio de Internet o intranet y reino.

El dominio es el dominio de Internet o Intranet para el que se debe configurar SSO, por ejemplo, micompañía.com. Solo las aplicaciones disponibles en este dominio o sus subdominios se habilitan para SSO.

El territorio es un parámetro compartido entre varias aplicaciones que utilizan la implementación de SSO de LTPA.

Señales de LTPA

Las credenciales autenticadas se comparten entre las aplicaciones participantes utilizando señales LTPA. Una señal LTPA es datos cifrados que contienen los datos relacionados con la autenticación para un usuario que ya ha sido autenticado utilizando el registro de usuarios LDAP compartido. Las aplicaciones SSO participantes pasan la señal LTPA del usuario utilizando una cookie del navegador.

Las señales LTPA son seguras porque se crean utilizando un cifrado seguro. Las señales están tanto cifradas como firmadas. El servicio que crea una señal LTPA utiliza un conjunto de claves de cifrado. Las claves de cifrado se utilizan para codificar la señal de modo que la señal codificada que viaja al navegador del usuario no pueda ser decodificada por alguien que no tenga las claves de cifrado. Las claves de cifrado también se utilizan para validar la señal de modo que la integridad de la señal se pueda verificar y se pueda detectar rápidamente su manipulación. Cuando un servidor SSO recibe una solicitud HTTP y ver que se incluye la señal LTPA, el servidor verifica la señal utilizando su copia de las claves de cifrado compartidas y la información de la señal válida permite al servidor reconocer el usuario que ha iniciado la sesión.

Por lo tanto, las claves LTPA se deben intercambiar entre los servidores SSO participantes, de modo que todos los servidores estén utilizando la

misma clave LTPA. Elija uno de los servidores para que sea el origen de la clave LTPA. A continuación, exporte su clave LTPA y proporciónela a los administradores de los otros servidores para que puedan importarla. Cuando realice el paso de exportación, debe exportar la clave a un archivo de claves. Debe proporcionar un nombre para el archivo de claves y la contraseña que se debe utilizar para cifrar la clave. El archivo de claves y la contraseña deben proporcionarse a los administradores de las otras aplicaciones SSO participantes para que puedan importar la clave LTPA.

Por ejemplo, si varias aplicaciones pueden iniciar el cliente de Tivoli Enterprise Portal, puede exportar la clave LTPA desde el servidor de portal y proporcionar el archivo de claves y la contraseña a los administradores de las otras aplicaciones para que puedan importar la clave LTPA.

Sincronización de la hora entre los servidores participantes

Las señales LTPA son sensibles a la hora. Verifique que la fecha, hora y huso horario del sistema servidor de portal y los sistemas de las aplicaciones SSO participantes estén establecidos correctamente y relativos a la hora universal coordinada (UTC). Por ejemplo, el servidor de portal de Nueva York se ha establecido en UTC -5:00 y Dashboard Application Services Hub de París se ha establecido en UTC 1:00.

Tareas relacionadas:

"Reconfiguración del cliente de navegador para SSO" en la página 120
Reconfigure el cliente de navegador para especificar el nombre completo del Tivoli Enterprise Portal Server si desea tener la capacidad de SSO cuando inicie una sesión en Tivoli Enterprise Portal desde el mismo sistema.

Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único

Después de que los ID de usuario disponibles para el inicio de sesión único (SSO) se hayan establecido en el registro de usuarios LDAP, habilite SSO completando las tareas de este tema.

- Verifique que se cumplen todos los requisitos previos para habilitar la autenticación y el inicio de sesión único.
- Defina cuentas de usuario de Tivoli Enterprise Portal. (Esto se puede realizar después de que se haya configurado la autenticación de LDAP y SSO.)
- Configure la autenticación de LDAP y SSO a través del servidor de portal.
- Intercambie las claves LTPA con las aplicaciones SSO participantes.
- Correlacione los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP.

Hoja de ruta

Utilice la hoja de ruta del caso siguiente para ayudarle a configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único.

Tabla 15. Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único

Paso	Tarea	Dónde encontrar información
1	Configure el servidor de portal para que utilice un registro de usuarios LDAP y especifique el nombre de reino y de dominio utilizados para el inicio de sesión único. Para configurar el servidor de portal para que utilice LDAP, puede utilizar las siguientes opciones: • Programa de utilidad IBM Manage Tivoli Enterprise Monitoring Services • Interfaz de línea de mandatos **itmcmd** en Linux y UNIX • TEPS/e consola de administración Puede utilizar IBM Manage Tivoli Enterprise Monitoring Services o el mandato **itmcmd** para habilitar la validación de usuarios LDAP para el servidor de portal. También puede utilizar estos programas de utilidad para configurar los parámetros de conexión LDAP a menos que: • Desee utilizar un servidor además de Microsoft Active Directory o Tivoli Directory Server • Desee configurar TLS/SSL entre el servidor de portal y el servidor LDAP • Deba especificar parámetros de configuración LDAP avanzados En estos casos, debe especificar el tipo **Otro** al configurar el servidor de portal y, a continuación, utilizar la consola de administración de TEPS/e para completar la configuración de LDAP. **Nota:** También puede exportar la clave LTPA del servidor de portal o importar la clave LTPA de otra aplicación al mismo tiempo que configura la autenticación de usuarios LDAP o puede realizar estos pasos después de haber verificado que la autenticación LDAP del servidor de portal funciona.	Consulte el apartado "Requisitos previos para configurar la autenticación LDAP en el servidor de portal" en la página 95. Luego, utilice las instrucciones de uno de los temas siguientes para habilitar la validación de usuarios LDAP en el servidor de portal: • "Utilización de Manage Tivoli Enterprise Monitoring Services para configurar el servidor de portal para la autenticación de LDAP" en la página 104 • "Utilización de la línea de mandatos de Linux o UNIX para configurar el servidor de portal para la autenticación LDAP" en la página 108 A continuación, siga las instrucciones de "Utilización de la consola de administración de TEPS/e" en la página 110 si ha especificado el tipo de servidor LDAP **Otro** al habilitar la validación de usuarios LDAP para el servidor de portal. **Notas de uso:** Si está utilizando Microsoft Active Directory, consulte "Autenticación de usuarios de LDAP mediante Microsoft Active Directory" en la página 127 para obtener información sobre la planificación y la configuración específica para este tipo de servidor LDAP. Si está utilizando Tivoli Directory Server, consulte Descripción de inicio de sesión único entre IBM Tivoli Monitoring y Tivoli Integrated Portal utilizando Tivoli Directory Server en IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home). Estas instrucciones explican cómo correlacionar entradas configuradas en Tivoli Directory Server con la información configurada utilizando la TEPS/e consola de administración. Ignore los pasos proporcionados para Tivoli Integrated Portal.

Tabla 15. Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único (continuación)

Paso	Tarea	Dónde encontrar información
2	Configure las otras aplicaciones SSO participantes para que utilicen el mismo registro de usuarios LDAP, el reino y el nombre de dominio de Internet o intranet que el servidor de portal y habilite SSO. Asimismo, verifique que la fecha, la hora y el huso horario del sistema servidor de portal y los sistemas de las aplicaciones SSO participantes estén establecidos correctamente y relativos a la hora universal coordinada (UTC).	Si está utilizando el inicio de sesión único con Dashboard Application Services Hub, consulte los temas sobre la "configuración de Jazz for Service Management para un registro de usuarios central" y la "configuración de SSO en el servidor de aplicaciones" en *Jazz for Service Management Configuration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html). Para otras aplicaciones, consulte la documentación del producto para determinar cómo configurarlas para que utilicen el registro de usuarios LDAP, para habilitar SSO y cómo especificar el nombre de reino y el nombre de dominio como el servidor de portal.
3	Correlacione los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP.	"Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP" en la página 118
4	Vuelva a configurar el cliente de navegador para SSO si Tivoli Enterprise Portal se va a lanzar por otra aplicación en el mismo sistema que el servidor de portal.	"Reconfiguración del cliente de navegador para SSO" en la página 120
5	Verifique que los usuarios de Tivoli Enterprise Portal pueden iniciar el cliente de portal e iniciar sesión satisfactoriamente. **Nota:** Los usuarios del cliente de portal deben especificar el valor de su nombre distinguido relativo al iniciar sesión. Por ejemplo, si su nombre distinguido relativo es `cn=John Doe`, debe especificar `John Doe` cuando se le soliciten sus credenciales.	Si los usuarios de Tivoli Enterprise Portal no pueden iniciar sesión en Tivoli Enterprise Portal, revise el registro de TEPS/e para obtener información de diagnóstico. Es el archivo `SystemOut.log` ubicado en el sistema en el que está instalado el servidor de portal en *`install_dir`*`\CNPSJ\profiles\ITMProfile\logs`; *`install_dir`*`/Platform/iw/profiles/ITMProfile/log`. Si se producen errores de autenticación y no puede resolverlos, puede inhabilitar la autenticación LDAP siguiendo los pasos de "Inhabilitación de la autenticación de LDAP en el servidor de portal" en la página 123.
6	Configure TLS/SSL entre el servidor de portal y el servidor LDAP si desea asegurar esta comunicación.	"Configuración de la comunicación TLS/SSL entre el servidor de portal y el servidor LDAP" en la página 116
7	Verifique que los usuarios de Tivoli Enterprise Portal puedan iniciar sesión.	N/D

Tabla 15. Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único (continuación)

Paso	Tarea	Dónde encontrar información
8	Debe asegurarse de que las aplicaciones siguientes están utilizando la misma clave LTPA que el servidor de portal: • Una aplicación basada en la web o habilitada para la web que inicia Tivoli Enterprise Portal • Una aplicación basada en la web o habilitada para la web que puede iniciarse desde el cliente de Tivoli Enterprise Portal • IBM Dashboard Application Services Hub cuando utiliza el componente de proveedor de datos de panel de instrumentos del servidor de portal para recuperar datos de supervisión • Otra aplicación como Tivoli Integrated Portal que utiliza el servicio web de representación gráfica IBM Tivoli Monitoring Determine qué aplicación será el origen de las claves LTPA para todas las demás aplicaciones SSO participantes y exporte sus claves LTPA. El archivo de claves y la contraseña utilizados para cifrar la clave deben proporcionarse a los administradores de las demás aplicaciones participantes.	Si decide que el servidor de portal será el origen de la clave LTPA, exporte su clave LTPA utilizando las instrucciones de exportación de "Importación y exportación de claves de LTPA" en la página 120. Si está utilizando IBM Dashboard Application Services Hub para los paneles de control de supervisión y va a ser el origen de la clave LTPA, consulte el tema sobre "exportación de claves de LTPA" de *Jazz for Service Management Configuration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html). De lo contrario, consulte la documentación de la aplicación cuya clave LTPA se exportará para determinar cómo realizar la operación de exportación.
9	Los administradores de las otras aplicaciones SSO participantes deben importar la clave LTPA que se ha exportado en el paso anterior. Necesitan el archivo de claves y la contraseña que se ha utilizado para cifrar la clave.	Para importar una clave LTPA al servidor de portal, consulte las instrucciones de importación en "Importación y exportación de claves de LTPA" en la página 120. Para importar una clave LTPA a IBM Dashboard Application Services Hub consulte el tema sobre "importación de claves LTPA" de *Jazz for Service Management Configuration Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html). Consulte la documentación para las demás aplicaciones SSO participantes para obtener instrucciones sobre la importación de la clave LTPA.

Tabla 15. Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único (continuación)

Paso	Tarea	Dónde encontrar información
10	Verifique que el inicio de sesión único funciona entre el servidor de portal y cada una de las aplicaciones SSO participantes realizando las tareas siguientes que sean aplicables a su entorno SSO: 1. Verifique que otra aplicación pueda iniciar Tivoli Enterprise Portal y que no se solicitan las credenciales a los usuarios. 2. Verifique que Tivoli Enterprise Portal se puede utilizar para iniciar otra aplicación y que no se solicita al usuario que vuelva a especificar sus credenciales. 3. Verifique que los recursos supervisados pueden visualizarse en los paneles de control de supervisión de Dashboard Application Services Hub después de crear una conexión de proveedor de datos y configurarla para SSO. 4. Verifique que otra aplicación pueda utilizar el servicio web de representación gráfica de IBM Tivoli Monitoring para recuperar datos de supervisión.	N/D
11	Cree ID de usuario de Tivoli Enterprise Portal cuando se añaden nuevos usuarios en el registro de usuarios LDAP.	"Gestión de usuarios LDAP nuevos" en la página 123

Utilización de Manage Tivoli Enterprise Monitoring Services para configurar el servidor de portal para la autenticación de LDAP

Puede utilizar Manage Tivoli Enterprise Monitoring Services para habilitar la autenticación de usuarios LDAP y el inicio de sesión único en el servidor de portal y, opcionalmente, para configurar los detalles de la conexión del servidor LDAP.

Puede utilizar este programa de utilidad para configurar la información de conexión de servidor LDAP, si todas las condiciones siguientes se cumplen:

- Está utilizando Microsoft Active Directory Server o Tivoli Directory Server para el servidor LDAP.
- No tiene previsto configurar TLS/SSL entre el servidor de portal y el servidor LDAP.
- No es necesario que configure los parámetros de configuración de LDAP aparte de los listados en la Tabla 13 en la página 96.

Para todos los demás casos, utilice Manage Tivoli Enterprise Monitoring Services para habilitar la validación de usuarios LDAP y SSO para el servidor de portal y especifique el tipo de servidor **Otro**. A continuación, utilice la TEPS/e consola de administración para completar la configuración de LDAP.

La configuración del servidor de portal para que utilice un registro de usuarios LDAP implica añadir información de LDAP como el ID de vinculación y el número de puerto a la configuración del servidor de portal. Al mismo tiempo, la práctica recomendada es para habilitar el inicio de sesión único especificando el nombre de reino y el nombre de dominio de Internet o intranet utilizado por otras

aplicaciones SSO participantes. Para obtener más información sobre estos parámetros, consulte “Requisitos previos para configurar la autenticación LDAP en el servidor de portal” en la página 95.

También puede exportar la clave LTPA del servidor de portal o importar la clave LTPA de una aplicación SSO participante si ya ha decidido qué aplicación será el origen de la clave LTPA. (Todas las aplicaciones SSO participantes deben utilizar la misma clave). Los pasos de exportación o importación también se pueden realizar en un momento posterior si desea concentrarse en lograr el funcionamiento de la autenticación de usuarios LDAP o no tiene una clave LTPA para importar.

Antes de empezar

Tenga a mano la información de configuración del servidor LDAP, así como el reino y el nombre de dominio de Internet o intranet para SSO.

Si desea exportar o importar claves LTPA, asegúrese de que el servidor de portal se está ejecutando antes de comenzar la configuración. Obtendrá un mensaje que indica que el servidor de portal se detendrá durante la configuración, pero el servidor solo se detiene al final del procedimiento de configuración después de que el usuario pulse **Aceptar** para cerrar el último diálogo. Si está importando una clave LTPA, necesita el archivo de claves y la contraseña que se ha utilizado cuando se ha generado el archivo de claves.

Acerca de esta tarea

Siga estos pasos para reconfigurar el servidor de portal para la validación de usuarios con un registro LDAP, habilitar SSO y, opcionalmente, exportar o importar claves LTPA.

Procedimiento

1. Inicie Manage Tivoli Enterprise Monitoring Services en el sistema en el que está instalado el servidor de portal:
   - Windows Pulse **Inicio → Programas →IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services**.
   - Linux UNIX Donde *install_dir* es el directorio de instalación de IBM Tivoli Monitoring, vaya al directorio *install_dir*/bin y ejecute `./itmcmd manage [-h install_dir]`.
2. Pulse con el botón derecho del ratón en el **Tivoli Enterprise Portal Server:**
   - Windows Pulse **Reconfigurar**, luego pulse **Aceptar** para aceptar la configuración existente e ir a la segunda ventana Configuración del servidor TEP.
   - Linux UNIX Pulse **Configurar**.
3. En el área Seguridad de LDAP, seleccione ☑ **¿Validar usuario con LDAP?**. En Linux y UNIX, el área Seguridad de LDAP está en el separador **Conexión de TEMS**.
4. Opcional: Si piensa utilizar SSO, seleccione ☑ **¿Habilitar inicio de sesión único?**.
5. Seleccione el **Tipo LDAP** en la lista ▾:
   - **AD2000** para Active Directory Server 2000
   - **AD2003** para Active Directory Server 2003
   - **AD2008** para Active Directory Server 2008
   - **IDS6** para IBM Tivoli Directory Server Versión 6.x.

- **Otro** si el servidor LDAP no es uno de los que aparecen listados, tiene la intención de personalizar la configuración de LDAP para Active Directory Server o Tivoli Directory Server, o está configurando las comunicaciones SSL en el servidor LDAP. Después de completar este procedimiento, inicie la TEPS/e consola de administración para completar la configuración del servidor LDAP. Consulte el apartado "Utilización de la consola de administración de TEPS/e" en la página 110.

  Importante: Si cree que puede que necesite editar la configuración de Active Directory Server o Tivoli Directory Server en un momento posterior, como por ejemplo para configurar las comunicaciones TLS/SSL en el servidor LDAP, asegúrese de seleccionar **Otro** y utilizar la TEPS/e consola de administración para configurar el servidor (sáltese el paso 6). De lo contrario, cualquier personalización realizada en la TEPS/e consola de administración se pierde la próxima vez que reconfigure el servidor de portal.

6. Si ha seleccionado **AD2000**, **AD2003** o **IDS6** como **Tipo de LDAP**, complete los otros campos para especificar el servidor LDAP:
   - **Base LDAP** es el nombre distinguido (DN) para la entrada base en el registro LDAP.

     Es el punto de partida para las búsquedas de usuario en el servidor LDAP. Por ejemplo, para un usuario con un nombre distinguido de `cn=John Doe,ou=Rochester,o=IBM,c=US`, especifique `ou=Rochester,o=IBM,c` para este parámetro.
   - **Entrada base de DN de LDAP** se establece normalmente en el nombre distinguido de la entrada base del registro LDAP para los usuarios del servidor de portal. Por ejemplo, para un usuario con un nombre distinguido de `cn=John Doe,ou=Rochester,o=IBM,c=US`, especifique `ou=Rochester,o=IBM,c` para este parámetro.

     Sin embargo, cuando se están configurando varios repositorios LDAP para el servidor de portal, utilice este campo para definir un nombre distinguido (DN) adicional que identifica de forma exclusiva el conjunto de usuarios LDAP desde este servidor LDAP. Por ejemplo, el registro `LDAP1` y el registro `LDAP2`, pueden utilizar los dos `o=ibm,c=us` como su entrada base. En este caso, utilice este parámetro para especificar de forma exclusiva una entrada base diferente para cada servidor LDAP. Por ejemplo, especifique `o=ibm1,c=us` al configurar el registro `LDAP1` y `o=ibm2,c=us` al configurar el registro `LDAP2`.

     Nota: Si dispone de varios registros LDAP, no pueden contener nombres de usuario que se solapen.

     El valor de este parámetro se visualiza en el diálogo Administrar usuarios de Tivoli Enterprise Portal cuando se listan los nombres distinguidos que se pueden correlacionar con los ID de usuario de Tivoli Enterprise Portal.
   - **ID de vinculación de LDAP** es el ID de usuario de LDAP para la autenticación de vinculación, en notación de LDAP, y debe tener autorización para buscar usuarios de LDAP. El ID de vinculación se puede omitir si un usuario anónimo puede buscar usuarios de LDAP.
   - **Contraseña de vinculación de LDAP** es la contraseña de usuario de LDAP para la autenticación de vinculación de LDAP. Este valor se puede omitir si un usuario anónimo puede vincular con el servidor de LDAP. El instalador cifra este valor.
   - **Número de puerto de LDAP** en el que escucha el servidor LDAP. Este valor se puede omitir si el puerto es 389.

- **Nombre de host de LDAP**, que se puede omitir si el servidor LDAP está en el mismo sistema que el servidor de portal. Valor predeterminado: **localhost**.

7. Pulse **Aceptar**.
   - Si ha seleccionad ☑ **¿Habilitar inicio de sesión único?**, se muestra el diálogo Inicio de sesión único con los campos **Nombre de territorio** y **Nombre de dominio** y los botones **Importar claves** y **Exportar claves**.
   - Si no habilita el inicio de sesión único en este momento, pulse **Aceptar** para cerrar los otros diálogos de configuración del servidor de portal y vaya al paso 12 en la página 108.
8. Para SSO, especifique el territorio y el dominio en el diálogo Inicio de sesión único:
   a. **Nombre de reino** es un parámetro compartido entre aplicaciones que participan en SSO. Las aplicaciones configuradas para el mismo nombre de dominio, pero para otro nombre de territorio, no funcionarán como parte de la misma infraestructura de SSO.
   b. **Nombre de dominio** es el dominio de Internet o Intranet para el que se ha configurado SSO, por ejemplo, micompañía.com. Solo las aplicaciones disponibles en este dominio o sus subdominios se habilitan para SSO.
9. En este momento, puede exportar la clave LTPA del servidor de portal si desea que sea la clave utilizada por todas las demás aplicaciones SSO participantes. Pulse **Exportar claves** y complete los pasos siguientes:
   a. Vaya al directorio en el que desea crear el archivo o cambiar el tipo de archivo, o ambos. El directorio que se muestra inicialmente en Windows es *dir_ITM*\InstallITM y en Linux y UNIX es el directorio raíz.
   b. Escriba un nombre para el archivo en el que debe colocarse la clave LTPA y pulse **Guardar**.
   c. En la ventana Exportar claves, escriba la contraseña que desea utilizar para cifrar el archivo y pulse **Aceptar**. Verá una ventana de consola mientras se crea y se cifra el archivo; luego volverá a la ventana Único inicio de sesión.

   Nota: Después de completar la configuración de LDAP, proporcione el archivo de claves y la contraseña a los administradores de las aplicaciones que lanzan Tivoli Enterprise Portal, utilizan el proveedor de datos de panel de instrumentos de IBM Dashboard Application Services Hub o utilizan el servicio web de representación gráfica de IBM Tivoli Monitoring.
10. Si otra aplicación SSO participante proporciona la clave LTPA, puede importarla ahora si tiene el archivo de claves y la contraseña que se ha utilizado para cifrar la clave. Pulse **Importar claves** y complete los pasos siguientes:
    a. En la ventana **Abrir** que se muestra, vaya al directorio en el que se encuentra el archivo de claves. El directorio que se muestra inicialmente en Windows es *dir_ITM*\InstallITM y en Linux y UNIX es el directorio raíz.
    b. Escriba el nombre del archivo que desea importar y pulse **Abrir**. Verá una ventana de consola mientras se crea y se cifra el archivo; luego volverá a la ventana Único inicio de sesión. Repita el proceso de importación para importar claves de otros servidores participantes.
    c. Escribe la contraseña necesaria para descifrar el archivo y pulse **Aceptar**. Verá una ventana de consola mientras se crea y se cifra el archivo; luego volverá a la ventana Único inicio de sesión.
    d. Repita el proceso de importación para importar claves de otros servidores participantes.

11. Pulse **Aceptar**.
12. Windows Si se le solicita que reconfigure la información de conexión con el almacén, responda **No**. Tras procesar algunos valores de configuración, se muestra la ventana Configuración de la Consola de sucesos comunes. A veces esta ventana no se abre en primer plano y queda oculta por otras ventanas. Si parece que el proceso tarda más de lo esperado, minimice otras ventanas y busque la ventana de configuración. Cuando se muestre la ventana Configuración de la Consola de sucesos comunes, pulse **Aceptar**.
13. Si es necesario, recicle el servidor de portal seleccionando el **Tivoli Enterprise Portal Server** y pulsando **Reciclar** o deteniendo y luego iniciando el servidor de portal.

Qué hacer a continuación

Si elige **Otro** como tipo de LDAP, la configuración de LDAP debe estar completa en la TEPS/e consola de administración.Consulte el apartado "Utilización de la consola de administración de TEPS/e" en la página 110.

De lo contrario, para todos los demás tipos de LDAP, siga los pasos 1 y 2 en el procedimiento anterior para comprobar si **¿Validar usuario con LDAP?** está aún seleccionado. Si no lo está, se ha producido un error cuando el programa de utilidad de configuración ha intentado conectar con el servidor LDAP y la validación LDAP se ha inhabilitado. Si está inhabilitada, compruebe el archivo *install_dir*/logs/ConfigureLDAPRepo.log.

Una vez que el registro LDAP está totalmente configurado, puede correlacionar los ID de usuario de Tivoli Enterprise Portal con los nombres distinguidos de LDAP para completar la configuración de LDAP. Debe iniciar la sesión en Tivoli Enterprise Portal con el ID de usuario **sysadmin** o un ID de usuario que tenga la misma autorización administrativa y no sea un usuario LDAP. Consulte el apartado "Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP" en la página 118.

Si ha habilitado SSO, tendrá que exportar o importar claves LTPA. Consulte "Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único" en la página 100 para determinar cuándo debe realizar estos pasos.

Utilización de la línea de mandatos de Linux o UNIX para configurar el servidor de portal para la autenticación LDAP

Si el Tivoli Enterprise Portal Server está en Linux o UNIX, puede habilitar la autenticación de usuarios LDAP y el inicio de sesión único en el servidor de portal y, opcionalmente, configurar los detalles de la conexión del servidor LDAP, utilizando la interfaz de línea de mandatos itmcmd.

Puede utilizar la línea de mandatos para configurar la información de conexión de servidor LDAP, si todas las condiciones siguientes se cumplen:

- Está utilizando Microsoft Active Directory Server o Tivoli Directory Server para el servidor LDAP.
- No tiene previsto configurar TLS/SSL entre el servidor de portal y el servidor LDAP.
- No es necesario que configure los parámetros de configuración de LDAP aparte de los listados en la Tabla 13 en la página 96.

Para todos los demás casos, utilice el mandato itmcmd para habilitar la validación de usuarios LDAP y SSO para el servidor de portal y especifique el tipo de servidor **Otro**. A continuación, utilice la TEPS/e consola de administración para completar la configuración de LDAP.

La configuración del servidor de portal para que utilice un registro de usuarios LDAP implica añadir información de LDAP como el ID de vinculación y el número de puerto a la configuración del servidor de portal. Al mismo tiempo, la práctica recomendada es para habilitar el inicio de sesión único especificando el nombre de reino y el nombre de dominio de Internet o intranet utilizado por otras aplicaciones SSO participantes. Para obtener más información sobre estos parámetros, consulte "Requisitos previos para configurar la autenticación LDAP en el servidor de portal" en la página 95.

Acerca de esta tarea

Siga estos pasos para configurar el servidor de portal desde la línea de mandatos:

Procedimiento

1. Inicie la sesión en el sistema en el que está instalado el Tivoli Enterprise Portal Server.
2. En la línea de mandatos, vaya al directorio *dir_instalación*/bin, donde *dir_instalación* es el directorio en el que ha instalado el producto.
3. Ejecute el siguiente mandato para empezar a configurar el Tivoli Enterprise Portal Server: **./itmcmd config -A cq**. Verá el mensaje "Se ha iniciado la configuración del agente...", seguido de una solicitud:

   ```
   ¿Editar valores de "Consola de sucesos comunes para IBM Tivoli Monitoring"?
   [ 1=Sí, 2=No ] (el valor predeterminado es: 1)
   ```

4. Especifique **2**. Se visualizará la siguiente solicitud:

   ```
   ¿Se conectará este agente a TEMS? [1=SÍ, 2=NO]
   (El valor predeterminado es: 1):
   ```

5. Acepte los valores predeterminados de esta indicación y las indicaciones que sigan hasta que vea la siguiente indicación Los valores predeterminados deberían reflejar las secciones realizadas durante la configuración original.

   ```
   Seguridad LDAP: ¿Validar usuario con LDAP? (1=Sí, 2=No)
   (El valor predeterminado es: 2):
   ```

6. Escriba 1 para comenzar la configuración de la autenticación de LDAP y especifique los valores de los parámetros de LDAP.

   ```
   Tipo de LDAP: [AD2000, AD2003, AD2008, IDS6, OTHER]
   (El valor predeterminado es: OTHER):
   ```

   Para el tipo de LDAP, seleccione **Otro** si el servidor LDAP no es uno de los que aparecen listados o si tiene intención de personalizar la configuración de LDAP para Active Directory Server o Tivoli Directory Server, o tiene previsto configurar TLS/SSL entre el servidor de portal y el servidor LDAP. Después de completar este procedimiento, inicie la TEPS/e consola de administración para completar la configuración del servidor LDAP. Consulte el apartado "Utilización de la consola de administración de TEPS/e" en la página 110.

   Importante: Si cree que puede que necesite editar la configuración de Active Directory Server o Tivoli Directory Server en un momento posterior, por ejemplo para configurar las comunicaciones TLS/SSL en el servidor LDAP, asegúrese de seleccionar **Otro** y utilice la TEPS/e consola de administración

para configurar el servidor. De lo contrario, cualquier personalización realizada en la TEPS/e consola de administración se pierde la próxima vez que reconfigure el servidor de portal.

7. Si no ha especificado el tipo **Otro**, se le solicita que especifique valores de configuración de LDAP adicionales (consulte Tabla 13 en la página 96 para obtener más información sobre estos parámetros):

```
LDAP base: o=IBM
LDAP DN Base Entry(Default is: o=ITMSSOEntry):  o=IBM
LDAP bind ID: cn=root
LDAP bind password:
Re-type: LDAP bind password:
LDAP Port number(Default is: 389):
LDAP host name(Default is: localhost): itmxseries04
```

8. Si también desea habilitar el inicio de sesión único como autenticación de LDAP, escriba 1 en el indicador de mandatos y luego especifique el Nombre de territorio y Nombre de dominio.

```
¿Habilitar inicio de sesión único? (1=Sí, 2=No)
(El valor predeterminado es: 2):
```

   a. **Nombre de territorio** es un parámetro compartido entre aplicaciones que participan en SSO. Las aplicaciones configuradas para el mismo nombre de dominio, pero para otro nombre de territorio, no funcionarán como parte de la misma infraestructura de SSO.
   b. **Nombre de dominio** es el dominio de Internet o Intranet para el que se ha configurado SSO, por ejemplo, micompañía.com. Solo las aplicaciones disponibles en este dominio o sus subdominios se habilitan para SSO.

   Cuando el instalador finalice la configuración, se mostrará el siguiente mensaje:

```
Ha finalizado la configuración del agente...
```

9. Recicle el servidor de portal.

```
./itmcmd agent stop cq
./itmcmd agent start cq
```

Qué hacer a continuación

Si elige **Otro** como tipo de LDAP, la configuración de LDAP debe estar completa en la TEPS/e consola de administración.Consulte el apartado “Utilización de la consola de administración de TEPS/e”.

Una vez que el registro LDAP está totalmente configurado, puede correlacionar los ID de usuario de Tivoli Enterprise Portal con los nombres distinguidos de LDAP para completar la configuración de LDAP. Debe iniciar la sesión en Tivoli Enterprise Portal con el ID de usuario **sysadmin** o un ID de usuario que tenga la misma autorización administrativa y no sea un usuario LDAP. Consulte el apartado “Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP” en la página 118.

Si ha habilitado SSO, tendrá que exportar o importar claves LTPA. Consulte “Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único” en la página 100 para determinar cuándo debe realizar estos pasos.

Utilización de la consola de administración de TEPS/e

Servicios ampliados de Tivoli Enterprise Portal Server (TEPS/e) tiene una consola administrativa (ISCLite) a la que puede acceder para configurar el registro LDAP

que no está soportado por los programas de instalación de IBM Tivoli Monitoring: los programas de utilidad de configuración Manage Tivoli Enterprise Monitoring Services y línea de mandatos de **itmcmd**.

También puede utilizar la TEPS/e consola de administración para configurar SSL para la comunicación con el servidor LDAP y con otras aplicaciones que envían solicitudes al proveedor de datos de panel de instrumentos o al servicio web de representación gráfica de IBM Tivoli Monitoring.

Debe utilizar la TEPS/e consola de administración para configurar la autenticación de usuarios LDAP del servidor de portal si ha especificado **Otro** como el tipo de LDAP al configurar el servidor de portal durante la instalación, o cuando se ha utilizado el programa de utilidad Manage Tivoli Enterprise Monitoring Services o la interfaz de línea de mandatos **itmcmd**. También debe utilizar la TEPS/e consola de administración para configurar los detalles de conexión LDAP si tiene la intención de realizar las tareas siguientes:

- Utilizar un servidor LDAP distinto de Microsoft Active Directory Server o Tivoli Directory Server.
- Configurar la comunicación TLS/SSL entre el servidor de portal y el servidor LDAP.
- Configurar los parámetros avanzados de configuración de LDAP que se pueden especificar en la TEPS/e consola de administración, pero no en los demás programas de utilidad de configuración del servidor de portal.

Importante: Las personalizaciones de LDAP realizadas dentro de la TEPS/e consola de administración se sobregraban y se borran cuando se vuelve a configurar el servidor de portal, a no ser que elija el tipo de LDAP **Otro** durante la configuración del servidor de portal a través de Manage Tivoli Monitoring Services o el mandato **itmcmd**. Cuando se elige **Otro**, la información de registro de usuarios LDAP se maneja por TEPS/e y no se ve afectada por los otros programas de utilidad de configuración del servidor del portal.

Inicio de la consola de administración de TEPS/e

Utilice la TEPS/e consola de administración para configurar un servidor LDAP con el tipo **Otro**, para configurar SSL entre el servidor de portal y otras aplicaciones como el servidor LDAP, y para verificar la configuración de LDAP.

Antes de empezar

La TEPS/e consola de administración está inhabilitada de forma predeterminado por motivos de seguridad y para ahorrar recursos del sistema. El Tivoli Enterprise Portal Server debe estar en ejecución antes de habilitar la consola.

Acerca de esta tarea

Siga estos pasos para habilitar y luego iniciar la TEPS/e consola de administración:

Procedimiento

1. Habilite la TEPS/e consola de administración:
   - Windows En la ventana Manage Tivoli Enterprise Monitoring Services, resalte **Tivoli Enterprise Portal Server** y luego seleccione **Avanzado → Administración de TEPS/e → Habilitar administración de TEPS/e**.
   - Linux UNIX Desde la línea de mandatos, vaya al directorio `scripts` (Intel Linux: *dir_ITM*`/li6263/iw/scripts`; zLinux:*dir_ITM*`/ls3266/iw/scripts`;

AIX®:*dir_ITM*/aix533/iw/scripts) y especifique el siguiente mandato, donde `true` inicia la consola y `false` la detiene:

```
./enableISCLite.sh {true/false}
```

Ahora la TEPS/e consola de administración está habilitada para inicio de sesión y permanecerá habilitada hasta que se detenga el servidor de portal.

2. Si es la primera vez que habilita la consola, debe establecer la contraseña del administrador:
   - Windows En la ventana Manage Tivoli Enterprise Monitoring Services, resalte **Tivoli Enterprise Portal Server** y seleccione **Avanzado → Administración de TEPS/e → Contraseña de administración de TEPS/e**.
   - Linux UNIX Desde el directorio `scripts`, escriba el siguiente mandato, donde <*nombreusuario*> es **wasadmin** y <*contraseña*> es la nueva contraseña:

     ```
     updateTEPSEPass.sh <nombreusuario> <contraseña>
     ```

     A partir de este momento, si se especifica una contraseña de administración de TEPS/e se restablecerá la contraseña.
3. Escriba el siguiente URL en el navegador Internet Explorer o Firefox: `http://localhost:15205/ibm/console` o `https://localhost:15206/ibm/console`
4. Inicie una sesión en la consola utilizando **wasadmin** para el ID de usuario y la contraseña que ha especificado como la contraseña de administración de TEPS/e.

Resultados

Se abre la ventana Integrated Solutions Console (TEPS/e consola de administración). Incluso después de finalizar la sesión de la consola de administración, permanece inhabilitada hasta que se detiene el Tivoli Enterprise Portal Server.Debe reiniciar manualmente la TEPS/e consola de administración a través de Manage Tivoli Enterprise Monitoring Services después de cada reinicio del servidor de portal.

Qué hacer a continuación

Ahora puede configurar una conexión de servidor LDAP externo, SSL, o verificar la configuración.

Si la TEPS/e consola de administración se está ejecutando cuando se recicla el servidor de portal, debe finalizar la sesión y volver a habilitar la consola para que se vuelva a sincronizar con el servidor de portal.

Configuración del servidor de portal para la autenticación LDAP utilizando la TEPS/e consola de administración

Debe utilizar la consola de administración de Servicios ampliados de Tivoli Enterprise Portal Server (TEPS/e) para configurar los parámetros de conexión de servidor LDAP si ha especificado **Otro** como tipo de LDAP al configurar el servidor de portal.

Antes de empezar

Inicie la TEPS/e consola de administración.

Atención: La práctica recomendada es seleccionar el tipo de LDAP **Otro** en el programa de utilidad Manage Tivoli Enterprise Monitoring Services de interfaz de línea de mandatos **itmcmd** antes de utilizar la TEPS/e consola de administración para cambiar la configuración del servidor LDAP para que los cambios futuros persistan. Por ejemplo, si ha seleccionado **IDS6** como el tipo de LDAP al configurar el servidor de portal utilizando el mandato itmcmd y realiza cambios en los parámetros de conexión LDAP a través de la TEPS/e consola de administración, los cambios se pierden la próxima vez que reconfigura el servidor de portal.

Procedimiento

1. En el árbol de navegación de la TEPS/e consola de administración, pulse **Seguridad → Seguridad global**.
2. En la página que se muestra, asegúrese de que `Repositorios federados` esté seleccionado para **Definición de reino disponible** y pulse **Configurar**.
3. Configure el repositorio federado:
   a. Verifique o especifique el valor **Nombre de territorio**. Un reino identifica un conjunto de repositorios federados en TEPS/e y otros WebSphere Application Server. Puede elegir su propio nombre de reino, pero el valor debe ser el mismo en todas las aplicaciones configuradas para SSO en el dominio de Internet o intranet. Si ha habilitado el inicio de sesión único al configurar el servidor de portal, este campo muestra el valor que ha especificado para el nombre del reino. Para obtener más detalles sobre la especificación del dominio, consulte el paso 9 en la página 114
   b. En la misma página, pulse **Añadir entrada base al reino**.
4. En la página **Referencia de repositorio**, pulse **Añadir repositorio** y seleccione **Repositorio LDAP** en la lista desplegable. Ahora la página muestra las propiedades que se pueden configurar para la conexión del servidor de portal con LDAP.
5. Proporcione los valores adecuados para los parámetros siguientes:
   - Para **Identificador de repositorio**, escriba un nombre para el repositorio que tenga significado para identificar el tipo de usos en el repositorio LDAP. Por ejemplo, `ITMtepUsers`.
   - Para **Tipo de directorio**, seleccione el tipo de servidor LDAP que se utiliza en el entorno.
   - Para **Nombre de host primario**, especifique el nombre de host completo o la dirección IP del servidor LDAP.
   - Para **Puerto**, especifique el número de puerto del servidor LDAP. El valor predeterminado es 389.
   - Para **Nombre distinguido de vinculación**, especifique el nombre distinguido de un usuario que tenga autorización para buscar usuarios LDAP. Por ejemplo, `cn=root`. El ID de vinculación se puede omitir si un usuario anónimo puede buscar usuarios de LDAP.
   - Para **Contraseña de enlace**, especifique la contraseña para el usuario especificado en el campo **Nombre distinguido de vinculación**. Este valor se puede omitir si un usuario anónimo puede vincular con el servidor de LDAP.

Si es necesario, también puede personalizar otros parámetros de esta página para que coincidan con las posibilidades del servidor LDAP. Para obtener más información sobre los demás parámetros que se pueden configurar en este panel, consulte la ayuda en línea de la TEPS/e consola de administración.

6. Pulse **Aceptar** para aceptar los valores.
7. En la página **Referencia de repositorio**, escriba estos valores:
   - Para **Nombre distinguido de la entrada base que identifica de forma exclusiva este conjunto de entradas en el reino**, especifique un valor que identifique de forma exclusiva el conjunto de entradas de usuario LDAP desde el servidor LDAP para el que está configurando una conexión.

     Normalmente, se establece este parámetro en el nombre distinguido de la entrada base en el registro LDAP para los usuarios de servidor de portal. Por ejemplo, para un usuario con un nombre distinguido de `cn=John Doe,ou=Rochester,o=IBM,c=US`, especifique `ou=Rochester,o=IBM,c` para este parámetro.

     Sin embargo, cuando se están configurando varios repositorios LDAP para el servidor de portal, utilice este campo para definir un nombre distinguido (DN) adicional que identifica de forma exclusiva el conjunto de usuarios LDAP desde este servidor LDAP. Por ejemplo, el registro `LDAP1` y el registro `LDAP2`, pueden utilizar los dos `o=ibm,c=us` como su entrada base. En este caso, utilice este parámetro para especificar de forma exclusiva una entrada base diferente para cada servidor LDAP dentro del reino. Por ejemplo, especifique `o=ibm1,c=us` al configurar el registro `LDAP1` y `o=ibm2,c=us` al configurar el registro `LDAP2`.

     Nota: Si dispone de varios registros LDAP, no pueden contener nombres de usuario que se solapen.

     El valor de este parámetro se visualiza en el diálogo Administrar usuarios de Tivoli Enterprise Portal cuando se listan los nombres distinguidos que se pueden correlacionar con los ID de usuario de Tivoli Enterprise Portal.\
   - Para **Nombre distinguido de la entrada base en este repositorio**, especifique el nombre distinguido (DN) para la entrada base en el registro LDAP.

     Es el punto de partida para las búsquedas de usuario en el servidor LDAP. Por ejemplo, para un usuario con un nombre distinguido de `cn=John Doe,ou=Rochester,o=IBM,c=US`, especifique `ou=Rochester,o=IBM,c` para este parámetro. Normalmente, este parámetro es el mismo que el parámetro base de LDAP, a menos que haya personalizado el nombre distinguido de la entrada base en el reino de modo que no coincida con el nombre distinguido en el servidor LDAP.
8. Pulse **Aceptar** para aceptar los valores.
9. Para habilitar SSO, vuelva a la página **Seguridad global** y complete los pasos siguientes:
   a. Asegúrese de que **LTPA** esté seleccionado como el mecanismo de autenticación.
   b. Expanda la opción **Seguridad web**.
   c. Seleccione el enlace **Inicio de sesión único (SSO)** para completar la configuración de SSO.
10. En la página **Inicio de sesión único (SSO)**, haga lo siguiente:
    a. Verifique que SSO esté habilitado.
    b. Verifique que el parámetro **Nombre de dominio** sea correcto. **Nombre de dominio** es el dominio de Internet o intranet para el que se ha configurado

SSO, por ejemplo, micompañía.com. Solo las aplicaciones disponibles en este dominio o sus subdominios se habilitan para SSO. Todas las aplicaciones SSO participantes también deben estar configuradas con el mismo nombre de reino. Si ha habilitado el inicio de sesión único al configurar el servidor de portal, este campo muestra el valor que ha especificado para el nombre de dominio.

c. Seleccione **Aceptar** para aceptar los valores.

11. Para guardar los cambios, pulse la opción **Guardar** que hay junto a la parte superior de la pantalla y luego finalice la sesión de la consola de administración.
12. Si desea exportar o importar claves LTPA en este momento, consulte los pasos de la TEPS/e consola de administración en "Importación y exportación de claves de LTPA" en la página 120.

    Nota: Si exporta o importa las claves ahora, también necesita realizar los otros pasos listados en "Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único" en la página 100 antes de intentar verificar que SSO está funcionando.
13. Reinicie el Tivoli Enterprise Portal Server.

Qué hacer a continuación

Correlacione el ID de usuario de Tivoli Enterprise Portal con los nombres distinguidos de LDAP. Consulte el apartado "Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP" en la página 118.

Debe habilitar la consola de administración tras un reciclado del servidor de portal para poder volver a iniciar la consola.

Importante: Cualquier personalización de LDAP realizada dentro de la TEPS/e consola de administración se sobregraban y se borran cada vez que el servidor de portal se reconfigura a no ser que elija el tipo de LDAP **Otro** durante la instalación de servidor de portal o cuando se utiliza el programa de utilidad Manage Tivoli Enterprise Monitoring Services de la interfaz de línea de mandatos **itmcmd** para realizar la configuración del servidor de portal. Cuando se elige **Otro**, la información de registro se maneja por TEPS/e y no se ve afectada por estos programas de utilidad de configuración. Consulte el paso 5 en la página 105 en "Utilización de Manage Tivoli Enterprise Monitoring Services para configurar el servidor de portal para la autenticación de LDAP" en la página 104 y 6 en la página 109 en "Utilización de la línea de mandatos de Linux o UNIX para configurar el servidor de portal para la autenticación LDAP" en la página 108.

Inicio y detención de TEPS/e

Si tiene que iniciar o detener la instancia del servidor de aplicaciones de TEPS/e en la que el Tivoli Enterprise Portal Server se está ejecutando, debe hacerlo iniciando o deteniendo el Tivoli Enterprise Portal Server.

No puede utilizar los mandatos de iniciar y detener de TEPS/e para controlar TEPS/e. Si ya ha utilizado mandatos de TEPS/e, puede recuperar siguiendo el procedimiento siguiente.

Inicio y detención del Tivoli Enterprise Portal Server

- Windows En la ventana Manage Tivoli Monitoring Services, resalte el **Tivoli Enterprise Portal Server** y seleccione **Detener** o **Iniciar**.

- Linux UNIX utilice el programa de utilidad itmcmd, situado en ITM_home/bin.
  - Para iniciar:

    ```
    cd ITM_home/bin
    ./itmcmd agent start cq
    ```

  - Para detener:

    ```
    cd ITM_home/bin
    ./itmcmd agent stop cq
    ```

Inicio y detención de otras instancias de servidor de TEPS/e

Si tiene que iniciar o detener otra instancia del servidor de aplicaciones en TEPS/e, por ejemplo si tiene su propio perfil, celda o servidor creados en TEPS/e, debe utilizar los dos scripts siguientes:

- Windows

  ```
  <ITM_home>/CNPSJ/profiles/<nombre_del_perfil>/bin/startServer.bat
  <nombre_del_servidor>
  <ITM_home>/CNPSJ/profiles/<nombre_del_perfil>/bin/stopServer.bat
   <nombre_del_servidor>
  ```

- UNIX

  ```
  <ITM_home>/<arch>/iw/profiles/<nombre_del_perfil>/bin/startServer.sh
  <nombre_del_servidor>
  <ITM_home>/<arch>/iw/profiles/<nombre_del_perfil>/bin/stopServer.sh
  <nombre_del_servidor>
  ```

Ejemplos::

- Windows Si utiliza un perfil creado por IBM Tivoli Monitoring, y su propio servidor llamado <*SuServidor*>, debe utilizar el siguiente mandato:

  ```
  <ITM_home>/CNPSJ/profiles/<ITMProfile>/bin/startServer.bat
  <SuServidor>
  ```

- UNIX Si ha creado su propio perfil llamado <*SuPerfil*>, y su propio servidor llamado TEPS/e, para detener el servidor en la plataforma UNIX (por ejemplo RHEL4), debe utilizar el mandato siguiente:

  ```
  <ITM_home>/<arch>/iw/profiles/<SuPerfil>/bin/stopServer.sh
  <SuServidor>
  ```

Configuración de la comunicación TLS/SSL entre el servidor de portal y el servidor LDAP

Utilice la TEPS/e consola de administración para configurar TLS (Transport Layer Sockets) o SSL (Secure Socket Layers) entre el servidor de portal y el servidor LDAP.

Antes de empezar

Asegúrese de que ya tiene una conexión existente para un servidor LDAP y que los usuarios de Tivoli Enterprise Portal pueden iniciar sesión en el servidor de portal y ser autenticados por el servidor LDAP. También debe asegurarse de que el Tivoli Enterprise Portal Server está configurado para utilizar el tipo de LDAP **Otro** ya que la configuración de la comunicación de TLS/SSL para el servidor LDAP debe realizarse utilizando la TEPS/e consola de administración.

El servidor LDAP debe estar configurado para aceptar conexiones TLS/SSL y estar en ejecución en el número de puerto seguro, normalmente el puerto 636. Consulte

la documentación del servidor LDAP si es necesario crear un certificado de firmante que, como parte de esta tarea, debe importarse desde el servidor LDAP al almacén de confianza de TEPS/e.

TLS/SSL de LDAP requiere algunas acciones de un administrador de LDAP que no se cubren en la documentación de Tivoli Monitoring. Los temas siguientes de Centro de información de IBM Security Systems incluyen información sobre cómo configurar servidores LDAP para TLS/SSL:

- Configuración de Microsoft Active Directory para el acceso SSL
- Configuración del cliente de Tivoli Directory Server para el acceso SSL
- Configuración de Oracle Java System Directory Server para acceso SSL

Inicie la TEPS/e consola de administración utilizando las instrucciones de "Inicio de la consola de administración de TEPS/e" en la página 111 antes de comenzar el procedimiento.

Procedimiento

1. Realice los pasos siguientes para importar el certificado de firmante del servidor LDAP al almacén de confianza de TEPS/e:
   a. Pulse **Seguridad → Gestión de certificados SSL y claves**.
   b. En el área Elementos relacionados de la página, pulse el enlace **Almacenes de claves y certificados** y en la tabla que se muestra, pulse el enlace **NodeDefaultTrustStore**.
   c. En el área Propiedades adicionales, pulse el enlace **Certificados de firmante** y pulse el botón **Recuperar del puerto**.
   d. En los campos pertinentes proporcione el nombre de host, puerto (normalmente `636` para las conexiones SSL), detalles de configuración SSL, así como el alias del certificado para el servidor LDAP. A continuación, pulse el botón **Recuperar información de firmante** y, a continuación, pulse **Aceptar**.
2. Siga estos pasos para habilitar las comunicaciones TLS/ SSL para el servidor LDAP:
   a. Pulse **Seguridad → Seguridad global**.
   b. En el área Elementos relacionados cerca de la parte inferior de la página, seleccione **Gestionar repositorios**.
   c. En la tabla de repositorios, seleccione el enlace para el identificador de repositorio del servidor LDAP.
   d. Marque el recuadro de selección **Requerir comunicaciones SSL** y seleccione la opción **Gestionado centralmente**.
   e. Cambie el número de puerto `389` por el número de puerto que utiliza el servidor LDAP para las conexiones SSL (normalmente `636`).
   f. Pulse **Aceptar**.
   g. Guarde los cambios efectuados en la configuración.
3. Reiniciar el servidor de portal.

Qué hacer a continuación

Verifique que los usuarios de Tivoli Enterprise Portal puedan iniciar sesión y ser autenticados por el servidor LDAP.

Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP

Cuando el servidor de portal está configurado para autenticar los usuarios utilizando el registro de usuarios LDAP, el usuario inicia sesión en el servidor de portal utilizando el valor del identificador exclusivo (UID) del nombre distinguido relativo. Este nombre no es necesariamente el ID de usuario de Tivoli Enterprise Portal. Por esta razón, los ID de usuario de Tivoli Enterprise Portal deben estar correlacionados con los nombres distinguidos de LDAP (que incluyen el UID).

Cada entrada en el registro de usuarios LDAP tiene un nombre distinguido (DN). El DN es el nombre que identifica de forma exclusiva una entrada en el directorio. Un nombre distinguido se compone de pares de atributo=valor, separados por comas, por ejemplo:

```
cn=Jim Grey,ou=users,ou=SWG,o=IBM,c=US
cn=Sally White,ou=users,ou=SWG,o=IBM,c=US
```

El orden de los pares de atributo y valor es importante. El DN contiene un componente para cada nivel de la jerarquía de directorios desde la raíz hasta el nivel en el que reside la entrada. Los DN de LDAP comienzan con el atributo más específico, normalmente una especie de nombre y continúan con atributos cada vez más amplios, finalizando a menudo con un atributo de país. El primer componente del DN se conoce como el nombre distinguido relativo (RDN). Identifica una entrada de forma distinta de las demás entradas que tienen el mismo padre. En los ejemplos anteriores, RDN `cn=Jim Grey` separa la primera entrada de la segunda entrada, (RDN `cn=Sally White`). Estos dos ejemplos de DN son por lo demás equivalentes. Estos dos usuarios iniciarán sesión en Tivoli Enterprise Portal como `Jim Grey` y `Sally Casa`.

El nombre distinguido predeterminado para los usuarios nuevos que cree para Tivoli Enterprise Portal tiene la siguiente estructura:

```
UID=tep_userid,O=DEFAULTWIMITMBASEDREALM
```

Este nombre distinguido indica que el usuario se autentica por el servidor de supervisión concentrador. Utilizando el procedimiento de este tema, actualice el nombre distinguido para cualquier usuario de Tivoli Enterprise Portal que esté definido en el registro de usuarios LDAP del servidor de portal para especificar su nombre distinguido en el registro de usuarios LDAP en lugar de `UID=idusuario_tep,O=DEFAULTWIMITMBASEDREALM`.

El sufijo de DN predeterminado para el registro de usuarios de TEPS/e es `o=defaultWIMFileBasedRealm`. El registro de usuarios de TEPS/e contiene el ID de usuario wasadmin para el acceso a la TEPS/e consola de administración: `UID=wasadmin,o=defaultWIMFileBasedRealm`.

No actualice los nombres distinguidos para ningún ID de usuario de Tivoli Enterprise Portal que utilice el sufijo `o=defaultWIMFileBasedRealm`.

Antes de empezar

Los ID de usuario se correlacionan con nombres distinguidos de LDAP en la ventana Administrar usuarios de Tivoli Enterprise Portal por un usuario con autorización de administrador. La interfaz de línea de mandatos **tacmd** también se puede utilizar para realizar esta correlación. Para obtener más información, consulte el mandato **tacmd edituser** en *IBM Tivoli Monitoring: Consulta de mandatos*.

Si la autenticación LDAP se configura a través del Tivoli Enterprise Monitoring Server, los ID de usuario se correlacionan editando la variable de entorno KGL_LDAP_USER_FILTER en el archivo de configuración de Tivoli Enterprise Monitoring Server.

Acerca de esta tarea

Siga estos pasos para correlacionar los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP utilizando la ventana de diálogo Administrar usuarios de Tivoli Enterprise Portal:

Procedimiento

1. Inicie una sesión en el portal utilizando **sysadmin** u otra cuenta de usuario con autorización completa de administración.
2. Pulse **Administrar usuarios**.
3. En la ventana Administrar usuarios, pulse con el botón derecho del ratón en la fila del ID de usuario que desee correlacionar y seleccione **Modificar usuario**.
4. En el recuadro de diálogo Modificar usuario, pulse **Buscar** para localizar el nombre distinguido de LDAP que se debe asociar con el ID de usuario de Tivoli Enterprise Portal. Ejemplo: `UID=TEPUSER,O=SS`.

   Nota:

   - El sufijo predeterminado para los nombres distinguidos de LDAP que se han configurado a través de los programas de utilidad configuración del Tivoli Enterprise Portal Server es `o=ITMSSOEntry`, pero este valor puede que se haya personalizado cuando el servidor de portal se ha configurado para LDAP.
   - Si el nombre distinguido de LDAP seleccionado contiene caracteres no alfanuméricos, estos caracteres se deben colocar con un carácter de escape de barra inclinada invertida antes de que se guarde la correlación. Por ejemplo, si un ID de usuario contiene un signo de almohadilla, `#`, coloque una barra inclinada invertida antes del signo de almohadilla, `\#`.
5. Pulse en **Aceptar** para guardar la correlación y volver a la ventana Administrar usuarios.
6. Repita los pasos del 3 al 5 hasta que haya correlacionado todos los usuarios que desea autenticar con el registro de LDAP configurado.
7. Pulse **Aceptar** para salir de la ventana Administrar usuarios.

Qué hacer a continuación

Vuelva a configurar el cliente de navegador para SSO si Tivoli Enterprise Portal se va a lanzar por otra aplicación en el mismo sistema que el servidor de portal. Consulte el apartado “Reconfiguración del cliente de navegador para SSO” en la página 120.

Verifique que los usuarios de Tivoli Enterprise Portal que tienen los ID que se correlacionan con nombres distinguidos de LDAP, puedan iniciar sesión en el cliente de Tivoli Enterprise Portal. Deben utilizar su nombre distinguido relativo de LDAP para iniciar sesión. Si los usuarios no pueden iniciar sesión en Tivoli Enterprise Portal, revise el registro de TEPS/e para obtener información de diagnóstico. Es el archivo `SystemOut.log` ubicado en el sistema en el que está instalado el servidor de portal en Windows *dir_instalación*`\CNPSJ\profiles\ITMProfile\logs`; Linux UNIX *dir_instalación*`/`*Plataforma*`/iw/profiles/ITMProfile/log`.

Consulte “Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único” en la página 100 para ver los pasos adicionales que se deben realizar después de que el registro de usuarios LDAP del servidor de portal pueda autenticar satisfactoriamente los usuarios de Tivoli Enterprise Portal.

Reconfiguración del cliente de navegador para SSO

Reconfigure el cliente de navegador para especificar el nombre completo del Tivoli Enterprise Portal Server si desea tener la capacidad de SSO cuando inicie una sesión en Tivoli Enterprise Portal desde el mismo sistema.

Antes de empezar

De forma predeterminada, el URL de inicio asociado al cliente de navegador que se ejecuta en el mismo sistema que el Tivoli Enterprise Portal Server es `localhost`. Si desea utilizar un cliente de navegador en el mismo sistema que el servidor de portal, este valor debe ser el nombre completo del sistema, como por ejemplo `dev1.myco.com`. El sufijo `myco.com` es el valor de dominio que especifica el usuario en el panel de configuración de SSO. El uso del sufijo asegura que las señales de SSO solo están visibles para los servidores que están bajo el mismo sufijo de dominio.

Acerca de esta tarea

Siga estos pasos para reconfigurar el cliente de navegador:

Procedimiento

1. Inicie el programa de utilidad Manage Tivoli Enterprise Monitoring Services.
2. Pulse con el botón derecho del ratón en la entrada Navegador de Tivoli Enterprise Portal y pulse **Reconfigurar** para abrir la ventana Configurar navegador de Tivoli Enterprise Portal.
3. En el campo **Host** que hay bajo el área de servidor de portal, escriba el nombre completo del sistema. Ejemplo: `myhost.mycompany.com`

Conceptos relacionados:

“Acerca del inicio de sesión único” en la página 98
La característica de inicio de sesión único (SSO) proporciona a los usuarios la capacidad de iniciar otras aplicaciones basadas en la web o habilitadas para la web de Tivoli desde Tivoli Enterprise Portal, o iniciar Tivoli Enterprise Portal desde otras aplicaciones, sin tener que volver a especificar sus credenciales. También se utiliza cuando IBM Dashboard Application Services Hub recupera datos de supervisión del servidor de portal u otra aplicación utiliza el servicio de representación gráfica de IBM Tivoli Monitoring.

Importación y exportación de claves de LTPA

Las credenciales autenticadas se comparten entre las aplicaciones participantes utilizando las claves LTPA.

Asegúrese de que las aplicaciones siguientes están utilizando la misma clave LTPA que el servidor de portal:

- Una aplicación basada en la web o habilitada para la web que inicia Tivoli Enterprise Portal
- Una aplicación basada en la web o habilitada para la web que puede iniciarse desde el cliente de Tivoli Enterprise Portal

- IBM Dashboard Application Services Hub cuando utiliza el componente de proveedor de datos de panel de instrumentos del servidor de portal para recuperar datos de supervisión
- Otra aplicación como Tivoli Integrated Portal que utiliza el servicio web de representación gráfica IBM Tivoli Monitoring

Determine qué aplicación será el origen de las claves LTPA para todas las demás aplicaciones SSO participantes y exporte sus claves LTPA.

Si opta por exportar la clave LTPA del servidor de portal, debe exportar la clave LTPA a un archivo de claves. Cuando realice el paso de exportación, debe proporcionar un nombre para el archivo de claves y la contraseña que se debe utilizar para cifrar la clave. El archivo de claves y la contraseña deben proporcionarse a los administradores de las aplicaciones listadas más arriba para que puedan importar la clave LTPA.

Si otra aplicación no va a proporcionar la clave LTPA, el administrador de esa aplicación debe exportar la clave LTPA de la aplicación a un archivo de claves y luego proporcionarle el archivo de claves y la contraseña que se ha utilizado para cifrar la clave. Debe importar la clave LTPA al servidor de portal y escribir la contraseña.

Antes de empezar

El Tivoli Enterprise Portal Server se debe estar ejecutando para poder realizar operaciones de importación y exportación.

Si está utilizando la TEPS/e consola de administración para importar o exportar claves, debe iniciar la consola. Consulte el apartado “Inicio de la consola de administración de TEPS/e” en la página 111.

Antes de poder importar una clave LTPA, el administrador de la aplicación que ha exportado la clave debe proporcionarle un archivo de claves que contenga la clave LTPA y la contraseña que se ha utilizado para cifrar la clave.

Acerca de esta tarea

Siga estos pasos para su entorno para importar o exportar claves de LTPA:

Procedimiento

- **En la ventana Manage Tivoli Enterprise Monitoring Services, complete el siguiente procedimiento para exportar claves:**
  1. Pulse con el botón derecho del ratón en el Tivoli Enterprise Portal Server y pulse **Avanzado → Administración de TEPS/e → Exportar claves**.
  2. Vaya al directorio en el que desea crear el archivo o cambiar el tipo de archivo, o ambos. El directorio que se muestra inicialmente en Windows es *dir_ITM*\InstallITM y en Linux y UNIX es el directorio raíz.
  3. Escriba un nombre para el archivo en el que debe colocarse la clave LTPA y pulse **Guardar**.
  4. En la ventana Exportar claves, escriba la contraseña que desea utilizar para cifrar el archivo y pulse **Aceptar**. Verá una ventana de consola mientras se crea y se cifra el archivo; luego volverá a la ventana Único inicio de sesión.
- **En la ventana Manage Tivoli Enterprise Monitoring Services, complete el siguiente procedimiento para importar claves:**

1. Pulse con el botón derecho del ratón en el Tivoli Enterprise Portal Server y pulse **Avanzado → Administración de TEPS/e → Importar claves**.
2. En la ventana **Abrir** que se muestra, vaya al directorio en el que se encuentra el archivo de claves. El directorio que se muestra inicialmente en Windows es *dir_ITM*\InstallITM y en Linux y UNIX es el directorio raíz.
3. Escriba el nombre del archivo que desea importar y pulse **Abrir**. Verá una ventana de consola mientras se crea y se cifra el archivo; luego volverá a la ventana Único inicio de sesión. Repita el proceso de importación para importar claves de otros servidores participantes.
4. Escribe la contraseña necesaria para descifrar el archivo y pulse **Aceptar**. Verá una ventana de consola mientras se crea y se cifra el archivo; luego volverá a la ventana Único inicio de sesión.
5. Repita el proceso de importación para importar claves de otros servidores participantes.

- **En la línea de mandatos de AIX and Linux, para exportar una clave, ejecute ./exportKeys.sh <*nombre_archivo*> <*contraseña*>.** El script está instalado en *dir_ITM*/*plataforma*/iw/scripts. Ejemplos: /opt/IBM/ITM/aix533/iw/scripts en AIX, /opt/IBM/ITM/li6263/iw/scripts en Linux, y /opt/IBM/ITM/ls3263/iw/scripts en zLinux.
- **En la línea de mandatos de AIX y Linux, para importar una clave, ejecute ./importKeys.sh <*nombre_archivo*> <*contraseña*>.** El script está instalado en *dir_ITM*/*plataforma*/iw/scripts.
- **En la TEPS/e consola de administración, complete el procedimiento siguiente para exportar la clave LTPA:**
  1. Seleccione **Seguridad→ Seguridad global**.
  2. Seleccione **LTPA**.
  3. En los campos **Contraseña** y **Confirmar contraseña**, escriba la contraseña para cifrar el archivo de claves.
  4. En el campo **Nombre de archivo de claves completo**, especifique la vía de acceso y nombre de archivo completo para el archivo de claves.
  5. Pulse **Exportar claves**.
  6. Pulse **Aceptar** y después, **Guardar**.
- **En la TEPS/e consola de administración, complete el procedimiento siguiente para importar la clave LTPA:**
  1. Seleccione **Seguridad→ Seguridad global**.
  2. Seleccione **LTPA**.
  3. En los campos **Contraseña** y **Confirmar contraseña**, introduzca la contraseña para descifrar el archivo de claves.
  4. En el campo **Nombre de archivo de claves completo**, especifique la vía de acceso y nombre de archivo completo para el archivo de claves.
  5. Pulse **Importar claves**.
  6. Pulse **Aceptar** y después, **Guardar**.

Qué hacer a continuación

Si ha exportado la clave LTPA del servidor de portal, proporcione el archivo de claves y la contraseña que se ha utilizado para cifrarla a los administradores de las otras aplicaciones SSO participantes para que puedan importar la clave.

Gestión de usuarios LDAP nuevos

Cuando se añaden usuarios nuevos al registro de usuarios LDAP del servidor de portal y los usuarios deben tener acceso de inicio de sesión en Tivoli Enterprise Portal u otras aplicaciones SSO participantes como, por ejemplo, IBM Dashboard Application Services Hub, debe crear un ID de usuario de Tivoli Enterprise Portal para el usuario y correlacionarlo con su nombre distinguido de LDAP.

También debe asignarse al ID de usuario de Tivoli Enterprise Portal permisos de Tivoli Enterprise Portal y las aplicaciones de supervisión que se pueden acceder. Consulte "Gestión de los ID de usuario" en la página 171 y "Administrar usuarios" en la página 164. Los únicos usuarios de Tivoli Enterprise Portal que no necesitan ningún permiso ni asignaciones de aplicaciones de supervisión, son los usuarios de paneles de control que no utilizan el cliente de Tivoli Enterprise Portal cuando se utilizan políticas de autorización.

Nota: La primera vez que un usuario de paneles de control accede a los datos de supervisión, se crea automáticamente un ID de usuario de Tivoli Enterprise Portal para el usuario si no hay ya un ID de usuario correlacionado con el nombre distinguido del usuario LDAP. En este caso, el ID de usuario de Tivoli Enterprise Portal es un ID generado aleatoriamente y el usuario no tiene asignado ningún permiso. Si se están utilizando permisos de Tivoli Enterprise Portal para controlar el acceso a los recursos supervisados en los paneles de control en lugar de políticas de autorización, o si el usuario de paneles de control puede iniciar Tivoli Enterprise Portal, asigne los permisos de ID de usuario y las aplicaciones supervisadas que se pueden acceder.

Se pueden utilizar scripts para mantener la sincronización automatizada del registro de usuarios LDAP y los usuarios de Tivoli Enterprise Portal users. Los scripts para gestionar cuentas de usuario del servidor LDAP puede garantizar que las modificaciones en cuentas de usuario (por ejemplo, los usuarios añadidos o suprimidos) también se realizan para el correspondiente ID de usuario de Tivoli Enterprise Portal mediante los mandatos **tacmd createuser** y **tacmd deleteuser**. Ejecute el script de sincronización de usuarios como una acción planificada con la frecuencia que requiera el entorno para garantizar que los usuarios de Tivoli Enterprise Portal y del registro de usuarios LDAP se mantienen sincronizados.

Inhabilitación de la autenticación de LDAP en el servidor de portal

Es posible que tenga que inhabilitar la autenticación de LDAP en el servidor de portal si se producen errores.

Acerca de esta tarea

Si la conexión LDAP se interrumpe y el procedimiento normal para desactivar la autenticación de LDAP no funciona, siga este procedimiento.

Procedimiento

Windows

1. Detenga el servicio del servidor de portal mediante la aplicación Manage Tivoli Enterprise Monitoring Services.
2. Ejecute el script **disableLDAPRepository.bat** desde scripts *candle_home*\CNPSJ\.

3. Vuelva a configurar el servidor de portal utilizando la aplicación Manage Tivoli Enterprise Monitoring Services e inhabilite la opción "Validar usuario con LDAP".
4. Inicie el servicio del servidor de portal mediante la aplicación Manage Tivoli Enterprise Monitoring Services. La autenticación del servidor de portal a través del servidor de supervisión está habilitada.
5. Si el servidor de supervisión se ha configurado para utilizar LDAP y utiliza este procedimiento porque LDAP no funciona, debe cambiar también la configuración del servidor de supervisión para que no utilice LDAP para la autenticación. Siga estos cambios en la configuración utilizando la ayuda de configuración del servidor de supervisión.

AIX Linux

1. Detenga el servidor de portal emitiendo el mandato **./itmcmd agent stop cq** en un indicador de mandatos desde el directorio de instalación.
2. Ejecute el script **./disableLDAPRepository.sh** desde scripts *candle_home*/*arq*/iw/, donde *arq* es la arquitectura de la máquina, por ejemplo li6263 o aix533.
3. Vuelva a configurar el servidor de portal e inhabilite la autenticación de LDAP emitiendo el mandato **./itmcmd config -A cq** en un indicador de mandatos desde el directorio de instalación.
4. Inicie el servidor de portal emitiendo el mandato **./itmcmd agent start cq** en un indicador de mandatos desde el directorio de instalación. La autenticación del servidor de portal a través del servidor de supervisión está habilitada.
5. Si el servidor de supervisión se ha configurado para utilizar LDAP y utiliza este procedimiento porque LDAP no funciona, debe cambiar también la configuración del servidor de supervisión para que no utilice LDAP para la autenticación. Siga estos cambios en la configuración utilizando la ayuda de configuración del servidor de supervisión.

Migración de la autenticación LDAP del servidor de supervisión al servidor de portal

Si el entorno ya se ha configurado para la autenticación de LDAP utilizando el servidor de supervisión concentrador y ahora desea configurar el servidor de portal para utilizar un registro de usuarios LDAP para el inicio de sesión único, siga los pasos de este tema.

Antes de empezar

Asegúrese de que todos los usuarios finalicen la sesión de Tivoli Enterprise Portal antes de comenzar el procedimiento y que no vuelva a iniciar una sesión hasta que el procedimiento haya finalizado.

Acerca de esta tarea

Siga estos pasos para inhabilitar temporalmente la validación de seguridad en el servidor de supervisión concentrador, configurar el servidor de portal para utilizar un registro de usuarios LDAP, correlacionar los ID de usuario de Tivoli Enterprise Portal con el nombre distinguido del registro de usuarios LDAP y, a continuación, volver a habilitar la validación de seguridad en el servidor de supervisión concentrador.

Procedimiento

1. Inhabilite temporalmente la seguridad de Tivoli Enterprise Monitoring Server:
   - Windows utilice el programa de utilidad Manage Tivoli Enterprise Monitoring Services para reconfigurar el servidor de supervisión concentrador:
     a. Pulse con el botón derecho del ratón en el Tivoli Enterprise Monitoring Server y pulse **Reconfigurar** .
     b. En la ventana Configuración del Tivoli Enterprise Monitoring Server, inhabilite □ **Seguridad: Validar usuario** y pulse **Aceptar**.
     c. Pulse **Aceptar** para aceptar los valores existentes en la siguiente ventana.
     d. Reinicie el servidor de supervisión concentrador.
   - Linux UNIX En la línea de mandatos:
     a. Vaya al directorio `/opt/IBM/ITM/bin` (o al directorio en el que ha instalado Tivoli Management Services).
     b. Ejecute el siguiente mandato, donde *nombre_tems* es el nombre del servidor de supervisión (por ejemplo, `HUB_itmdev17`):
        `./itmcmd config -S -t nombre_tems`
     c. Pulse Intro para aceptar los valores existentes hasta que vea el indicador **Seguridad: Validar usuario**.
     d. Escriba `NO` para inhabilitar la seguridad.
     e. Continúe pulsando Intro hasta que finalice la configuración.
     f. Reinicie el servidor de supervisión concentrador.
2. Cambie el nombre del UID **sysadmin** en el registro de LDAP (por ejemplo, sysadmin_tems).
3. Configure la autenticación LDAP y el inicio de sesión único para el servidor de portal. Utilice el programa de utilidad Manage Tivoli Enterprise Monitoring Services, la interfaz de línea de mandatos **itmcmd** en Linux y UNIX, o la TEPS/e consola de administración para configurar el servidor de portal. Para obtener instrucciones, consulte "Autenticación de usuarios LDAP a través del servidor de portal" en la página 94.
4. Inicie el Tivoli Enterprise Portal Server e inicie una sesión en Tivoli Enterprise Portal como **sysadmin**.
5. Ajuste todas las correlaciones con los ID de usuario de LDAP:
   a. Pulse **Administrar usuarios** para abrir la ventana Administrar usuarios.
   b. Pulse con el botón derecho del ratón en la fila del ID de usuario que desea volver a correlacionar y pulse **Modificar usuario**.
   c. Pulse **Buscar** para localizar el nombre distinguido de LDAP que se va a asociar al servidor de portal.
   d. Seleccione el nombre distinguido para el usuario. Si ve varias entradas, seleccione la que tenga el sufijo de LDAP correcto (entrada padre). Ejemplos: `UID=TIVOLIUSER,O=MYCOMPANY` y `uid=myname, dc=tivoli, dc=ibm, dc=us`. Si ve una entrada con uno de estos valores de organización, no la elija: `O=DEFAULTWIMITMBASEDREALM` es el sufijo predeterminado para los ID de usuario que se autentican a través del servidor de supervisión concentrador; y o=defaultWIMFileBasedRealm es el valor predeterminado para el registro de usuarios TEPS/e.
   e. Pulse **Aceptar** para guardar la correlación y volver a la ventana Administrar usuarios; luego continúe para modificar el DN de cada ID de usuario.
6. Antes de finalizar la sesión de Tivoli Enterprise Portal, solicite al administrador de LDAP que vuelva a asignar a la cuenta sysadmin de LDAP el nombre

sysadmin y luego correlacione la cuenta de usuario sysadmin de Tivoli Enterprise Portal con el DN sysadmin de LDAP.

7. Guarde los cambios y finalice la sesión del Tivoli Enterprise Portal.
8. Vuelva a habilitar la validación de seguridad de Tivoli Enterprise Monitoring Server realizando el paso 1 de nuevo, pero esta vez habilite la validación de seguridad.

Resultados

En este momento finaliza la migración.

Qué hacer a continuación

Verifique los cambios de autenticación siguiendo estos pasos:

1. Utilice el mandato de inicio de sesión de **tacmd** para verificar que la seguridad del servidor de supervisión concentrador está habilitado. Intente iniciar sesión con un nombre de usuario y contraseña válidos y con un nombre de usuario o contraseña que no es válido.
2. Inicie sesión en Tivoli Enterprise Portal utilizando el usuario sysadmin.
3. Inicie sesión en Tivoli Enterprise Portal utilizando un usuario del registro de usuarios LDAP configurado para el servidor de portal.

Autenticación a través del Tivoli Enterprise Monitoring Automation Server

Tivoli Enterprise Monitoring Automation Server amplía el servidor de supervisión concentrador proporcionando el proveedor de servicios de Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM). El proveedor de servicios registra recursos de supervisión como sistemas, servidores de software y bases de datos con el componente de Jazz for Service Management Registry Services y también responde a las solicitudes HTTP GET para métricas de salud de recursos de clientes OSLC.

De forma predeterminada, el proveedor de servicios de Performance Monitoring no autentica solicitudes HTTP GET de clientes de OSLC. Si desea que el proveedor de servicios de Performance Monitoring autentique estas solicitudes, debe instalar y configurar el componente Servicios de seguridad de Jazz for Service Management. Los servicios de seguridad permiten que aplicaciones no basadas en WebSphere, como el proveedor de servicios de Performance Monitoring, participar en el inicio de sesión único basado en Lightweight Third Party Authentication (LTPA). Los Registry Services y los Servicios de seguridad deben estar instalados en el mismo WebSphere Application Server. También deben estar configurados para utilizar el mismo registro de usuarios LDAP que las aplicaciones cliente OSLC y estar configurados para el inicio de sesión único.

Nota: Los Registry Services y los Servicios de seguridad y las aplicaciones de cliente OSLC deben estar en el mismo domino de Internet e Intranet, por ejemplo, micompañía.com, o en uno de sus subdominios. También deben estar configurados para utilizar el mismo nombre de reino que se establece al configurar un WebSphere Application Server para que utilice un repositorio de LDAP.

Para configurar los Registry Services y los Servicios de seguridad para el inicio de sesión único, genere la clave LTPA para el servidor de aplicaciones donde están instalados, exporte la clave y, a continuación, importe la clave LTPA a las

aplicaciones de cliente OSLC que van a enviar solicitudes HTTP GET al proveedor de servicios de supervisión de rendimiento. Consulte "Configuración de Jazz for Service Management para un registro de usuarios central" y "Configuración de Jazz for Service Management para SSO" en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html). Estos capítulos contienen instrucciones para configurar los Registry Services y los Servicios de seguridad para utilizar un registro de usuarios LDAP y generar y exportar la clave LTPA.

El proveedor de servicios de Performance Monitoring debe estar configurado para utilizar los Servicios de seguridad para autenticar las solicitudes de cliente OSLC estableciendo la variable de entorno Tivoli Enterprise Monitoring Automation Server `KAS_SECURITY_SERVICES_ENABLED` en `YES` y reiniciando el servidor de automatización.

Cuando el proveedor de servicio de Performance Monitoring recibe una solicitud HTTP GET de un cliente OSLC, reenvía la señal LTPA a los Servicios de seguridad para autenticar la solicitud. Si la solicitud no contiene una señal LTPA, o si los Servicios de seguridad indican que la señal no es válida o que ha caducado, el proveedor de servicios de Performance Monitoring devuelve el código de estado HTTP 401 para indicar que la solicitud no se ha podido autenticar.

Nota: El proveedor de servicios de Performance Monitoring utiliza la autenticación básica cuando envía solicitudes a los Registry Services de modo que las señales LTPA no están involucradas en las interacciones del registro de recursos del proveedor de servicios.

Autenticación de usuarios de LDAP mediante Microsoft Active Directory

Utilice estos temas para ayudarle a configurar la autenticación de usuarios utilizando el producto Active Directory basado en LDAP de Microsoft.

Estos temas cubren los pasos que debe completar para incorporar LDAP como implementado en un entorno de Active Directory, mientras presenta los procedimientos desde una perspectiva de Active Directory. Se proporcionan dos casos de usuarios (uno que ilustra la integración del servidor de supervisión con Active Directory, el otro la integración del servidor de portal con Active Directory) para de mostrarle cómo este proceso puede ayudarle a implementar la seguridad de Tivoli Monitoring en el entorno de trabajo; consulte "Casos de usuarios" en la página 146.

Este procedimiento utiliza la interfaz del navegador web de TEPS/e para completar la configuración del servidor de portal; consulte "Utilización de la consola de administración de TEPS/e" en la página 110.

Notas:

1. La configuración del servidor de portal para que utilice un servidor LDAP para autenticar los usuarios tiene la ventaja de que permite ID de usuario con más de 10 caracteres, un límite que se impone por la autenticación del servidor de supervisión. También da soporte a SSO (inicio de sesión único), al que la autenticación del servidor de autenticación no da soporte.

   Solo en la autenticación de usuarios basada en el servidor de supervisión permite los ID de usuario realizar solicitudes de servidor SOAP o emitir mandatos de la CLI que invocan métodos del servidor SOAP.

2. Los procedimientos y pasos de la configuración para habilitar la autenticación de usuarios de LDAP de IBM Tivoli Monitoring son los mismos para todas las implementaciones de LDAP (Active Directory, Tivoli Directory Server, etc.), pero los valores de configuración que debe especificar el usuario varían. Estas diferencias se deben a las diferencias dentro de las propias implementaciones de LDAP. Las diferencias más pronunciadas son la sintaxis de los nombres distinguidos de los objetos del directorio. Además, las diferencias del esquema de LDAP entre implementaciones de LDAP y personalizaciones de esquema de LDAP tendrán un gran impacto en los valores de configuración de autenticación de usuarios de LDAP proporcionados.
3. Aunque los casos de este conjunto de temas se suponen un entorno de Microsoft Active Directory versión 2003, estas instrucciones y casos también se han verificado utilizando Active Directory Server 2008 y Active Directory Server 2008 R2.

La configuración utiliza toda la información que se proporciona para conectar, enlazar, consultar y filtrar registros procedentes de una base de LDAP especificada destinados al registro de usuarios de LDAP de destino para la autenticación de usuarios. Las configuraciones de la autenticación de usuarios de LDAP del servidor de supervisión y del servidor de portal son operaciones separadas; estas configuraciones (una vez finalizadas) se pueden habilitar e inhabilitar independientemente. No cuente con que los pasos para configurar la autenticación de usuarios LDAP del servidor de supervisión se puedan utilizar para la autenticación de usuarios LDAP del servidor de portal, ni viceversa.

Antes de comenzar

Debe tener un entorno de Active Directory que funcione y estar familiarizado con los conceptos de Active Directory siguientes:

- Unidades organizativas

  Conector ADSI Edit MMC
- Gestión de políticas de grupo
- Administración de usuarios

  Esquema de objetos de usuario de Active Directory

Debe tener instalado Tivoli Enterprise Monitoring Server y el Tivoli Enterprise Portal Server tal como se explica en *IBM Tivoli Monitoring: Guía de instalación y configuración*. Familiarícese con la información preliminar en Capítulo 5, “Habilitación de la autenticación de usuarios”, en la página 83.

Debe trabajar con el administrador de Active Directory del sitio cuando decida qué usuarios de LDAP tendrán autorización para la autenticación del servidor de supervisión o del servidor de portal.

La práctica recomendada es crear también una jerarquía de OU que contenga los usuarios. Esto facilitará una búsqueda en el directorio de nombres base y limitará el tiempo de búsqueda a la vez que aumentará el rendimiento de la autenticación de usuarios entre Tivoli Monitoring y LDAP. La Figura 1 en la página 129 muestra una configuración de ejemplo que comprende una jerarquía de `OU=ITMUsers` con los contenedores `ITMtepsUsers` e `ITMtemsUsers`. Con este esquema, la base para buscar usuarios del servidor de supervisión que se van a autenticar será `CN=ITMtemsUsers,OU=ITMUsers,DC=`*`company`*`,DC=com`, y la base para los usuarios del servidor de portal que se van a autenticar será `CN=ITMtepsUsers,OU=ITMUsers,DC=`*`company`*`,DC=com`.

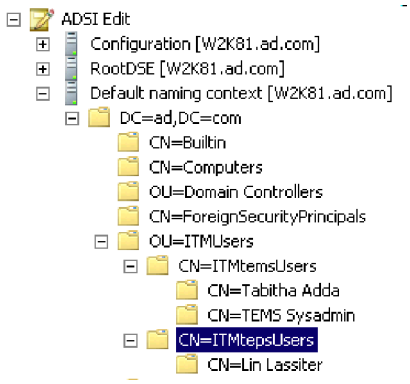

Figura 1. Jerarquía de usuarios de LDAP sugerida para servidores de Tivoli Monitoring

También debe conocer el esquema de objetos/atributos de usuarios de Active Directory. Esta información se necesita cuando se codifica la configuración de filtro de LDAP del servidor de supervisión y para la propiedad de inicio de sesión de seguridad de repositorio de TEPS/e del servidor de portal. La Figura 2 en la página 130 muestra una posible configuración de cuenta de usuario (este usuario del Tivoli Enterprise Portal Server también debe estar autorizado como un usuario del Tivoli Enterprise Monitoring Server).

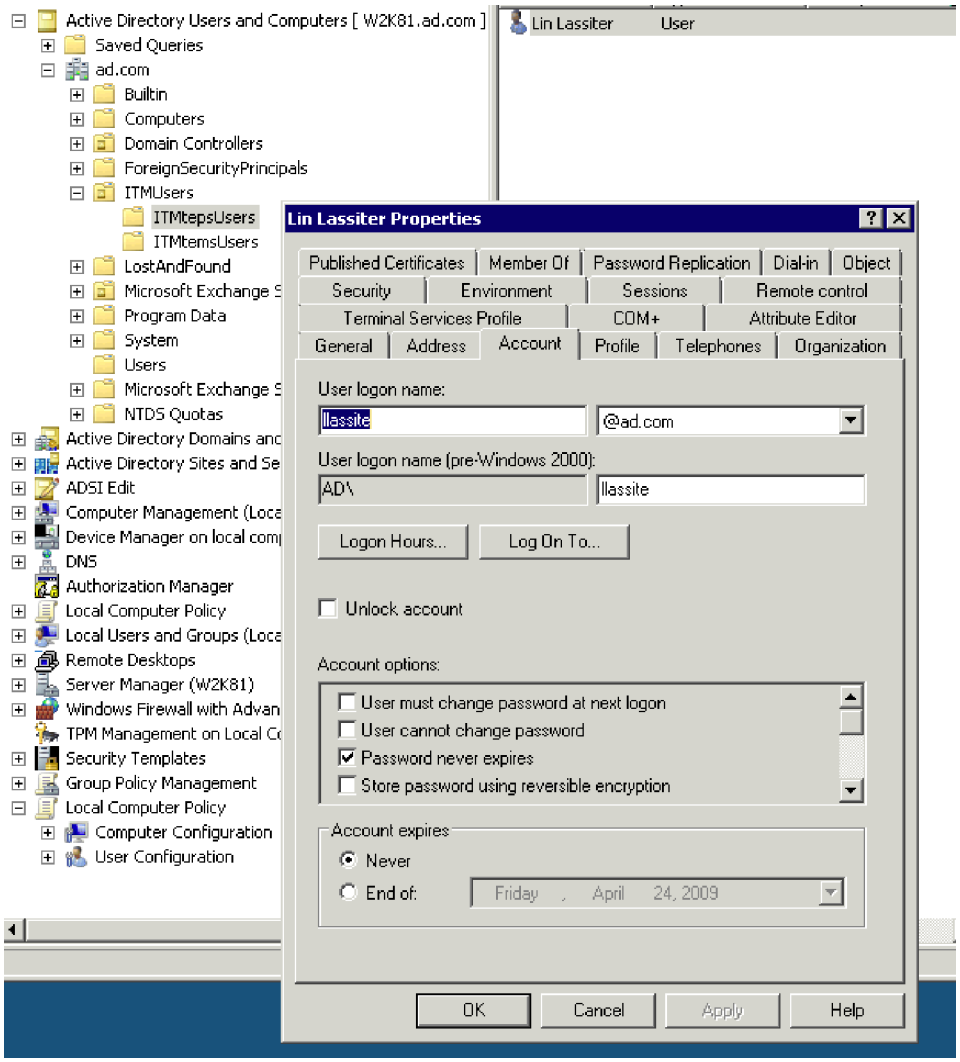

Figura 2. Propiedades de usuario del servidor de portal

La configuración de la autenticación de usuarios de LDAP de TEPS/e necesita que especifique el atributo de objeto de usuario de Active Directory Login Property (propiedad de inicio de sesión), que contendrá el nombre de usuario coincidente (en este ejemplo, *llassite*). Figura 3 en la página 131 muestra la instancia de clase de usuario de Active Directory para el usuario *llassite*.

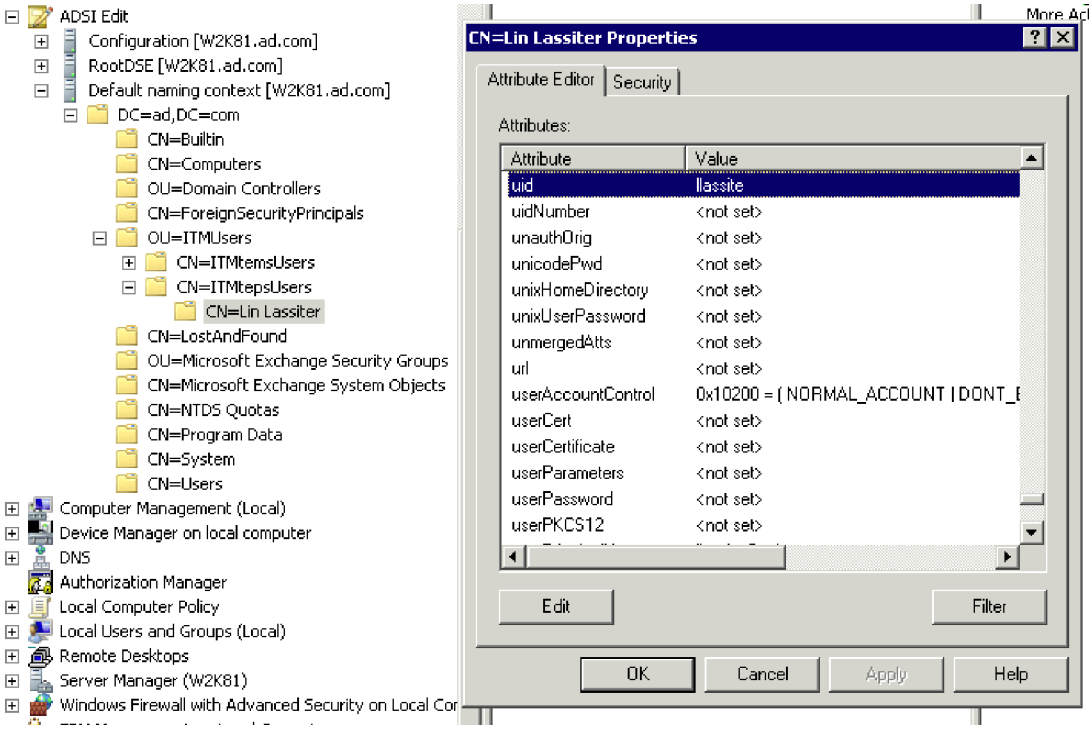

Figura 3. Propiedades de usuario de LDAP

Debe hacer que la propiedad de autenticación del usuario de LDAP de TEPS/e **uid** coincida con la cuenta de usuario del servidor de portal. Para ello, edite el atributo user/uid de Active Directory para el usuario *llassite* y establezca **uid=llassite** para que la cuenta de usuario del servidor de portal *llassite* coincida con *uid=llassite* en el objeto de LDAP
`CN=Lin Lassiter,CN=ITMtepsUsers,OU=ITMUsers,DC=`*`company`*`,DC=com` (que se encuentra buscando el directorio que comienza por el registro base `CN=ITMtepsUsers,OU=ITMUsers,DC=`*`company`*`,DC=com`).

Se proporcionan la Figura 1 en la página 129, la Figura 2 en la página 130 y la Figura 3 para ofrecerle una idea de las propiedades de Active Directory que se utilizarán para la autenticación de LDAP. El conocimiento de dónde residen los usuarios de LDAP dentro de Active Directory (la base que consultar o buscar para usuarios de Tivoli Monitoring en el directorio) y el esquema de usuario (el atributo de objeto de usuario que contiene el nombre de usuario exacto utilizado para la autenticación) resultan críticos para la configuración correcta de la autenticación de usuarios de LDAP del Tivoli Enterprise Monitoring Server o del Tivoli Enterprise Portal Server.

Nota: Los permisos de la cuenta de usuario del servidor de portal para este tipo de funciones de Tivoli Monitoring como aplicaciones, vistas y grupos se continuará gestionando dentro de la herramienta de administración de usuarios del servidor de portal, tal como se muestra en la Figura 4 en la página 132.

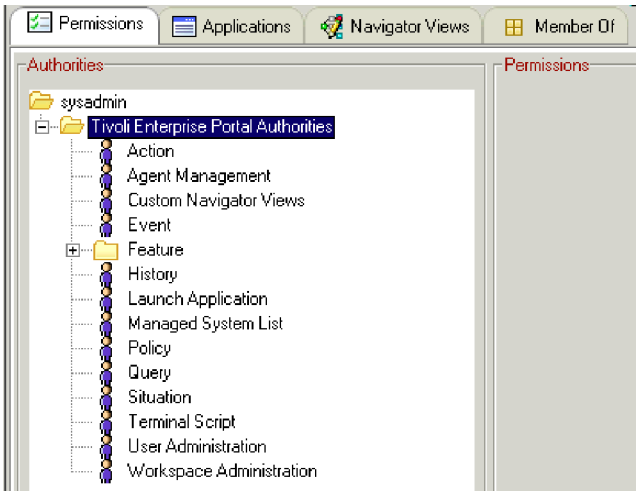

Figura 4. Permisos de usuario del Tivoli Enterprise Portal Server

La autenticación de usuarios de LDAP solo está disponible para usuarios y grupos de usuarios individuales de Tivoli Monitoring. La habilitación de la autenticación de LDAP para usuarios individuales de Tivoli Monitoring garantiza la máxima flexibilidad tanto en IBM Tivoli Monitoring como en LDAP. Se pueden utilizar scripts para mantener la sincronización automática de usuarios de Active Directory y de Tivoli Monitoring. Scripts de recopilación de datos para cuentas de usuario de Active Directory pueden garantizar que las modificaciones en cuentas de Active Directory (por ejemplo, usuarios añadidos o suprimidos) se reflejan en los usuarios correspondientes de Tivoli Enterprise Portal a través de la CLI **tacmd**.

Descripción general de la Hoja de ruta

Para integrar su entorno de autenticación de usuarios de IBM Tivoli Monitoring con la implementación de Active Directory del sitio, lleve a cabo los pasos descritos en este tema.

1. "Planificación y creación de usuarios del servidor de portal dentro de Active Directory" en la página 133

   Siga los pasos descritos en este tema.

2. "Creación y configuración de cuentas y permisos de usuarios del servidor de portal, si se desea" en la página 133

   Omitir este paso: Si no desea utilizar un servidor LDAP para autenticar usuarios de Tivoli Enterprise Portal y no es necesario configurar el inicio de sesión único para la integración con otros productos como IBM Dashboard Application Services Hub.

   Utilice la interfaz Administrar usuarios de Tivoli Enterprise Portal o la interfaz de línea de mandatos **tacmd**, si el sitio requiere la autenticación de usuarios del servidor de portal.

   Estas cuentas de usuario utilizarán LDAP para la autenticación; por lo tanto, los ID de usuario elegidos deben coincidir exactamente con los especificados en Active Directory. Para ver los atributos que debe elegir, seleccione Figura 3 en la página 131.

3. "Habilitación y configuración de la autenticación de usuarios de LDAP para el servidor de portal, si se desea" en la página 134

Omitir este paso: Si no desea utilizar un servidor LDAP para autenticar usuarios de Tivoli Enterprise Portal y no es necesario configurar el inicio de sesión único para la integración con otros productos como IBM Dashboard Application Services Hub.

Lleve a cabo este paso si el sitio requiere autenticación de servidor de portal.

4. "Configuración de TEPS/e para TLS/SSL, si es necesario" en la página 141

   Normalmente, TEPS/e está habilitado para TLS/SSL de forma predeterminada. Si tiene que configurar la comunicación TLS/SSL entre el servidor de portal y el servidor LDAP, utilice la TEPS/e consola de administración.
5. "Habilitación y configuración de la autenticación de usuarios de LDAP para el servidor de supervisión, si se desea" en la página 142

   Omitir este paso: Si no desea utilizar un usuario LDAP para autenticar los usuarios del servidor de supervisión.

   Lleve a cabo este paso si el sitio requiere autenticación de servidor de supervisión.

Planificación y creación de usuarios del servidor de portal dentro de Active Directory

Cuando cree usuarios de Active Directory para el Tivoli Enterprise Monitoring Server o el Tivoli Enterprise Portal Server, haga lo siguiente:

1. (Opcional) Cree la jerarquía de OU para los usuarios del servidor de supervisión y servidor de portal.

   Consulte el apartado Figura 1 en la página 129. Utilice las Microsoft Management Console (MMC) **Edición de ADSI**.
2. Cree los usuarios del servidor de supervisión y servidor de portal (y, opcionalmente, grupos) en Active Directory.

   Consulte el apartado Figura 2 en la página 130.Utilice la función de MMC **Usuarios y sistemas de AD**.
3. Aplique las políticas de usuario/grupo que desee a los nuevos usuarios y grupos de Active Directory.

   Utilice el conector de MMC para GPO.

Actualmente no existe ninguna sincronización de usuarios entre Tivoli Monitoring y LDAP. Las cuentas de usuario se pueden sincronizar mediante scripts. Utilice scripts de Active Directory para mantener un reconocimiento de modificaciones en cuentas de usuario (limitado al OU que se aplica a IBM Tivoli Monitoring). Estas modificaciones detectadas se pueden aplicar luego a los usuarios de Tivoli Monitoring mediante el mandato de CLI **tacmd** y a los usuarios de Active Directory mediante scripts. Tendrá que ejecutar el script de sincronización de usuarios como una acción planificada con la frecuencia que requiera el entorno para garantizar que los usuarios de Tivoli Monitoring y Active Directory se mantengan sincronizados.

Creación y configuración de cuentas y permisos de usuarios del servidor de portal, si se desea

Omitir este paso: Si no desea utilizar un servidor LDAP para autenticar usuarios de Tivoli Enterprise Portal y no es necesario configurar el inicio de sesión único para la integración con otros productos como IBM Dashboard Application Services Hub.

Cada cuenta de Active Directory creada anteriormente necesita una cuenta de usuario del Tivoli Enterprise Portal coincidente. El ID de usuario del Tivoli Enterprise Portal debe coincidir exactamente con el campo del atributo Objeto de usuario de TEPS de Active Directory planificado para su uso dentro de la configuración de TEPS/e (consulte la Figura 3 en la página 131).

Configure todos los permisos, aplicaciones, vistas y grupos necesarios para operaciones de cuenta de usuario dentro de IBM Tivoli Monitoring, consulte Capítulo 6, "Utilización de la autorización de usuario de Tivoli Enterprise Portal", en la página 163 para obtener más información. (Tenga en cuenta que estos permisos, aplicaciones, vistas y grupos de las cuentas no estarán disponibles en Active Directory ni se convertirán de Tivoli Monitoring a Active Directory; consulte la Figura 4 en la página 132.)

Nota: Podría actualizar el esquema de objetos de usuario de Active Directory para correlacionar los permisos, aplicaciones, vistas y grupos de usuarios de IBM Tivoli Monitoring con Active Directory. A continuación, puede utilizar estos nuevos atributos de esquema como ayuda para la sincronización de usuarios entre Tivoli Monitoring y Active Directory y con la gestión de Active Directory de propiedades de usuarios de servidor de portal mediante scripts de Active Directory y el mandato **tacmd** de la CLI Tivoli Monitoring.

No se recomienda añadir la cuenta **sysadmin** predeterminada al directorio de LDAP. La cuenta **sysadmin** se debe reservar para la autorización local del servidor de supervisión **Seguridad: Validar usuario**, manteniendo así un método no LDAP para acceder al servidor de supervisión y al servidor de portal.

ID de usuario y **Descripción de usuario** tienen formato libre, pero, para mantener un formato adecuado, debe intentar combinar el **Nombre de usuario** y **Descripción de usuario** que ya ha creado en Active Directory.

El nombre distinguido resulta crítico para vincular el ID de usuario de Tivoli Monitoring con la cuenta de usuario de LDAP basada en la configuración de TEPS/e LDAP. Este punto se trata detalladamente más adelante; por ahora, seleccione la entrada `UID=idusuario,O=DEFAULTWIMITMBASEDREALM`.

Habilitación y configuración de la autenticación de usuarios de LDAP para el servidor de portal, si se desea

Omitir este paso: Si no desea utilizar un servidor LDAP para autenticar usuarios de Tivoli Enterprise Portal y no es necesario configurar el inicio de sesión único para la integración con otros productos como IBM Dashboard Application Services Hub.

Ahora que se han creado los ID de usuario de Tivoli Enterprise Portal con los permisos de IBM Tivoli Monitoring deseados y estos mismos ID de usuario existen en Active Directory, debe habilitar la autenticación de usuarios LDAP para estos usuarios del servidor de portal. Utilice la interfaz de navegador web de TEPS/e para establecer los detalles de configuración de registro de usuarios de LDAP del servidor de portal y la configuración de nombres base de Active Directory. El procedimiento completo para la configuración de TEPS/e LDAP se explica detalladamente en el tema "Configuración del servidor de portal para la autenticación LDAP utilizando la TEPS/e consola de administración" en la página 112.

Inicio de la consola de administración de TEPS/e

Si tiene problemas para acceder a `http://localhost:15205/ibm/console`, asegúrese de haber completado los pasos de habilitación de TEPS/e y establecimiento de contraseña que se detallan en “Inicio de la consola de administración de TEPS/e” en la página 111. Además, si desea utilizar la interfaz de TEPS/e, debe habilitarla cada vez que reinicie el servidor de portal. (Tenga en cuenta que la habilitación de TEPS/e controla únicamente la interfaz de TEPS/e; no controla la habilitación de LDA del servidor de portal.) Encontrará información de registro para eta actividad en:

- Windows `%CANDLE_HOME%\CNPSJ\profiles\ITMProfile\logs\ITMServer`
- Linux `$CANDLEHOME/$INTERP/iw/profiles/ITMProfile/logs/ITMServer`

Cuando lleve a cabo los pasos descritos en “Configuración del servidor de portal para la autenticación LDAP utilizando la TEPS/e consola de administración” en la página 112, tenga en cuenta las notas siguientes.

- Un reino identifica un conjunto de repositorios federados en TEPS/e y otros WebSphere Application Server. Puede elegir su propio nombre de reino, pero el valor debe ser el mismo en todas las aplicaciones configuradas para SSO en el dominio de Internet o intranet. Si no está configurando SSO, debe aceptar el valor predeterminado para el **Nombre de reino**, a menos que este nombre ya se utilice en el entorno.

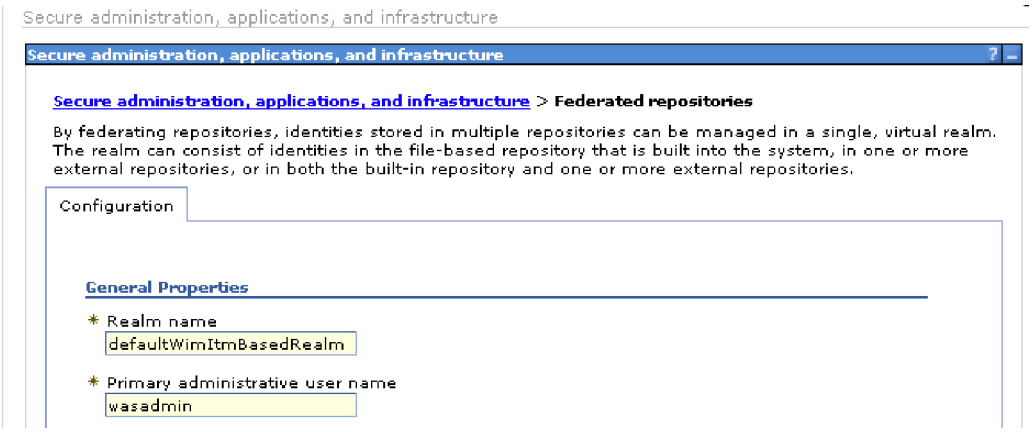

Figura 5. Acepte estos valores predeterminados

- Al entrar el **Identificador de repositorio**, elija un nombre descriptivo.

  El **Identificador de repositorio** se convertirá en una etiqueta de referencia para un contenedor de configuración dentro de TEPS/e que albergará la información del servidor LDAP, la **Contraseña de vinculación de LDAP** y las **Propiedades de inicio de sesión de LDAP**; este es el atributo Clase de usuario de Active Directory para buscar un ID de usuario de servidor de portal que coincida exactamente (consulte la Figura 3 en la página 131).

  Además, este repositorio se asociará a uno o varios valores base de LDAP (contenedores) que la autenticación LDAP del servidor del portal buscará. De nuevo, tal como se ha descrito en el apartado “Antes de comenzar” en la página 128, se recomienda planificar OU para este paso de configuración. Una buena planificación de OU restringe las búsquedas de la autenticación de usuarios de LDAP de IBM Tivoli Monitoring a la base y por debajo de la misma. Se recomienda agrupar usuarios dentro del OU ITMtepsUsers (consulte la Figura 1 en la página 129) para poder realizar búsquedas base eficientes y para mejorar la

autenticación de usuarios de LDAP.

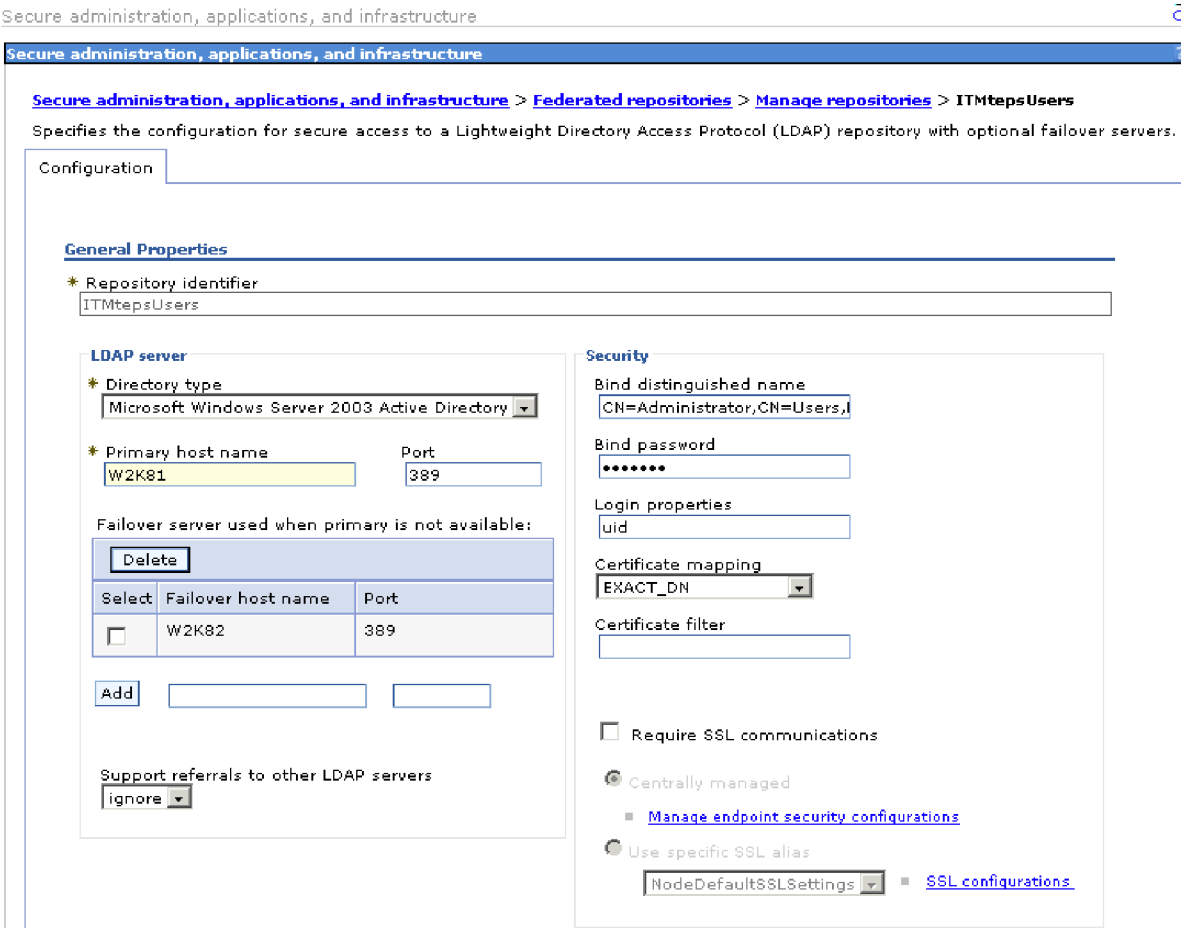

Figura 6. Configure el repositorio

Propiedad general → Identificador de repositorio
Es un campo de formato libre. Se recomienda elegir un nombre significativo que los administradores puedan asociar fácilmente con los usuarios definidos dentro del entorno de Active Directory. En este caso se especifica ITMtepsUsers, ya que este será el único repositorio creado para la autenticación de usuarios de LDAP del servidor de portal. También resultaría adecuado nombrar el repositorio siguiendo un convenio que refleje la cuenta de **contraseña de vinculación de LDAP** configurada. Un ejemplo para este caso sería utilizar un derivado de Nombre de bosque o de Nombre de dominio si necesita distintos repositorios para poder configurar distintas **contraseñas de vinculación de LDAP** que se ajusten a sus requisitos.

Propiedad de servidor de LDAP → Tipo de directorio
El valor proporcionado debe coincidir con el nivel de bosque. Nuestro bosque de ejemplo se está ejecutando en un nivel de Active Directory 2003.

Propiedad de servidor de LDAP → Nombre de host principal
Un controlador de dominio dentro del bosque de Active Directory que alberga las cuentas de usuario que ha creado anteriormente para la autenticación de usuarios de LDAP del servidor de portal. Esta opción debe basarse en el nivel de jerarquía dentro del bosque que alberga el

OU de los usuarios de IBM Tivoli Monitoring. Tenga en cuenta la selección que haga aquí cuando analice posibles problemas con la autenticación de LDAP de IBM Tivoli Monitoring debidos a la conectividad de Active Directory o a errores de replicación de los objetos de usuario de Active Directory.

Propiedad de servidor de LDAP → Puerto
El valor de puerto predeterminado LDAP de Active Directory es 389. Compare este valor con la asignación de puerto del entorno de LDAP.

Propiedad de servidor de LDAP → Servidor de migración tras error utilizado cuando el principal no esté disponible
Se pueden añadir servidores de LDAP de Active Directory (DC) adicionales para compensar los problemas de replicación o de conectividad. Este valor se debe completar con DC de migración tras error (preferiblemente con roles de GC).

Propiedad de servidor de LDAP → Derivaciones de soporte a otros servidores de LDAP
Esta es su opción. Tenga en cuenta si el entorno está cerrado o abierto (es decir, no hay ningún DC dentro de DMZ).

Seguridad → Nombre distinguido de vinculación
El usuario especificado aquí necesita autorización suficiente (es decir, una política aplicada) para buscar en la base del directorio de Active Directory. Este usuario es la cuenta que conectará, vinculará y consultará las **Propiedades de inicio de sesión** especificadas. Este valor se puede omitir si usuarios anónimos pueden buscar en el registro.

En nuestro ejemplo se utiliza `CN=Administrator,CN=Users,DC=company,DC=com`, aunque esto no es estrictamente necesario si el usuario especificado existe dentro del contenedor `CN=Users,DC=company,DC=com` para Active Directory. Sin embargo, esto no se recomienda, puesto que es mejor ser específico y utilizar un nombre distinguido completo.

Seguridad → Contraseña de vinculación
La contraseña de la cuenta de **Nombre distinguido de vinculación** anterior.

Seguridad → Propiedades de inicio de sesión
Esta propiedad de configuración resulta crítica para Active Directory ya que es el nombre del atributo dentro del objeto de nombre de Active Directory que se utiliza para reflejar exactamente el nombre de usuario del servidor de portal (consulte la Figura 3 en la página 131).

Seguridad → Certificado
El valor predeterminado **EXACT_DN** se establece para buscar en Active Directory y comparar con un DN exacto. Se recomienda conservar este valor predeterminado.

Seguridad → Filtro de certificado
Para seleccionar **CERTIFICATE_FILTER** en el campo **Certificado**, se necesitan parámetros de filtro de LDAP. Estos parámetros correlacionan atributos del certificado del cliente con entradas del directorio de LDAP.

Seguridad → Requerir comunicaciones SSL
Seleccione esta opción si desea comunicaciones LDAP de TLS/SSL. Pulse los botones de selección para las siguientes opciones que se aplican a la implementación de TLS/SSL:

Gestionado centralmente

Utilizar alias de SSL específico

- Cuando se especifica un **Nombre distinguido de entrada base que identifica de forma exclusiva este conjunto de entradas en el reino** y **Nombre distinguido de entrada base en este repositorio**, consulte Figura 7 en la página 139 para referencia.

  Ahora que tiene un repositorio configurado, debe añadir la entrada base como punto de partida para buscar OU de usuarios de servidor de portal definidos por Active Directory. Puede definir varias entradas base para el repositorio si lo necesita. Solo se necesitarán varias entradas base si ha definido varias ubicaciones base del directorio (varias jerarquías de OU) para los usuarios del servidor de portal de Active Directory.

  La información que se proporciona en este panel para la propiedad **Nombre distinguido de entrada base que identifica de forma exclusiva este conjunto de entradas en el territorio** se reflejará en las opciones de nombre distinguido de usuario de Tivoli Enterprise Portal, tal como se muestra en la Figura 10 en la página 140. Este campo está disponible desde la configuración del servidor de portal de TEPS/e para asociar el ID de usuario definido por el servidor de portal con una conexión de LDAP, vinculación, consulta o selección (consulte las propiedades de inicio de sesión del paso 5 en la página 113).

  Esta propiedad tiene formato libre; es el DN de configuración de TEPS/e. Se recomienda utilizar el convenio `O=`*`DNelegido`*. La elección de DN debe resultar significativa para su relación con el contenedor base de usuarios de TEPS definido por Active Directory (mejor que sea corto). Los ejemplos aquí mostrados han asignado `O=ITMtepsUser`, que resulta clarificador cuando se consultan los nombres distinguidos de los usuarios de Tivoli Enterprise Portal en la interfaz **Administrar usuarios** (consulte la Figura 10 en la página 140). El ejemplo que se utiliza aquí es redundante, puesto que el nombre de repositorio y el DN base son muy parecidos, pero queda claro que este repositorio y la base están configurados para acceder y vincular nuestros usuarios definidos por Active Directory.

  Para **Nombre distinguido de entrada base en este repositorio**, especifique el nombre distinguido (DN) para la entrada base en el registro LDAP. Es el punto de partida para las búsquedas de usuario en el servidor LDAP.

Figura 7. Adición de la entrada base al territorio. Observe que esta entrada está asociada a la sección ITMtepsUsers del repositorio.

- Al guardar el paso del trabajo de configuración de TEPS/e, utilice Figura 8 como referencia. Pulse **Guardar**.

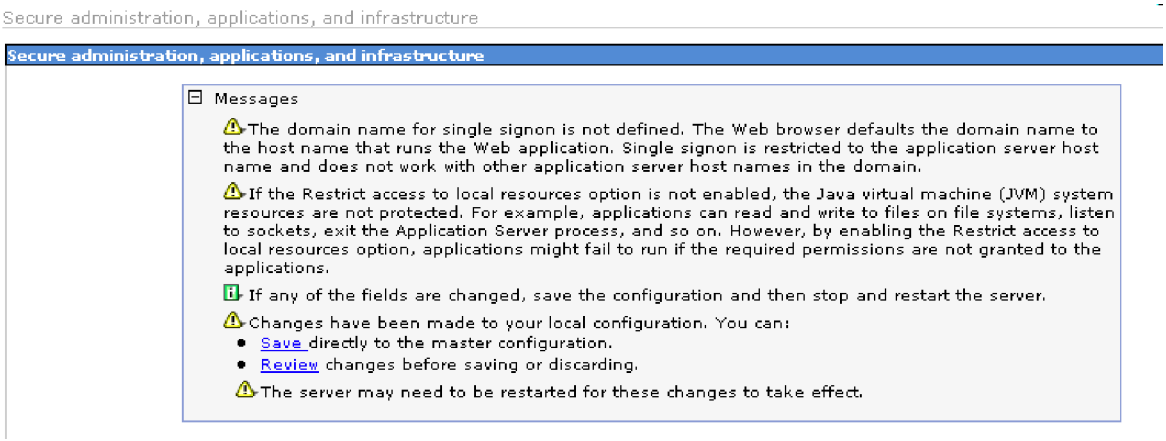

Figura 8. Guarde la actualización de la configuración de TEPS/e

Además, mientras configure los valores de repositorio y de base, recuerde pulsar Aceptar cuando se le solicite que verifique los valores de configuración. Al pulsar Aceptar o Aplicar se conecta, vincula y consulta la base de datos de LDAP de Active Directory utilizando los valores de configuración actualizados. Si hay algún problema, el panel de configuración devuelve un mensaje de error rojo como el que se muestra en la Figura 9 en la página 140.

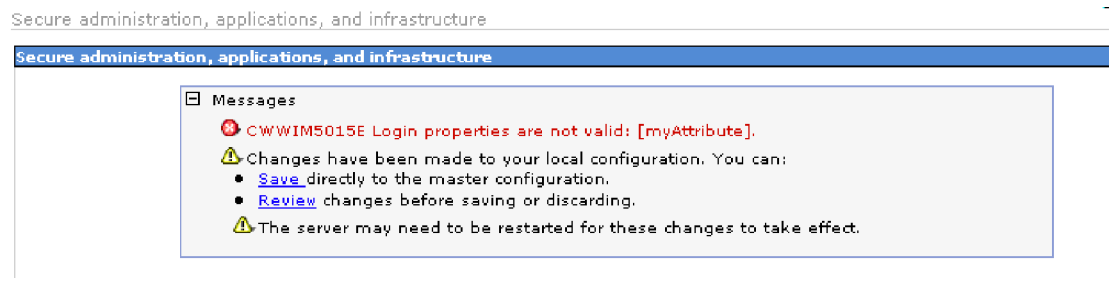

Figura 9. Mensaje de error de configuración de TEPS/e

Debe corregir estos errores antes de guardar la configuración.

Nota: Cuando haya completado y guardado la configuración de TEPS/e, debe reciclar el Tivoli Enterprise Portal Server para ver los usuarios configurados por TEPS/e como nombres distinguidos (consulte el ejemplo correspondiente a *llassite* en la Figura 10).

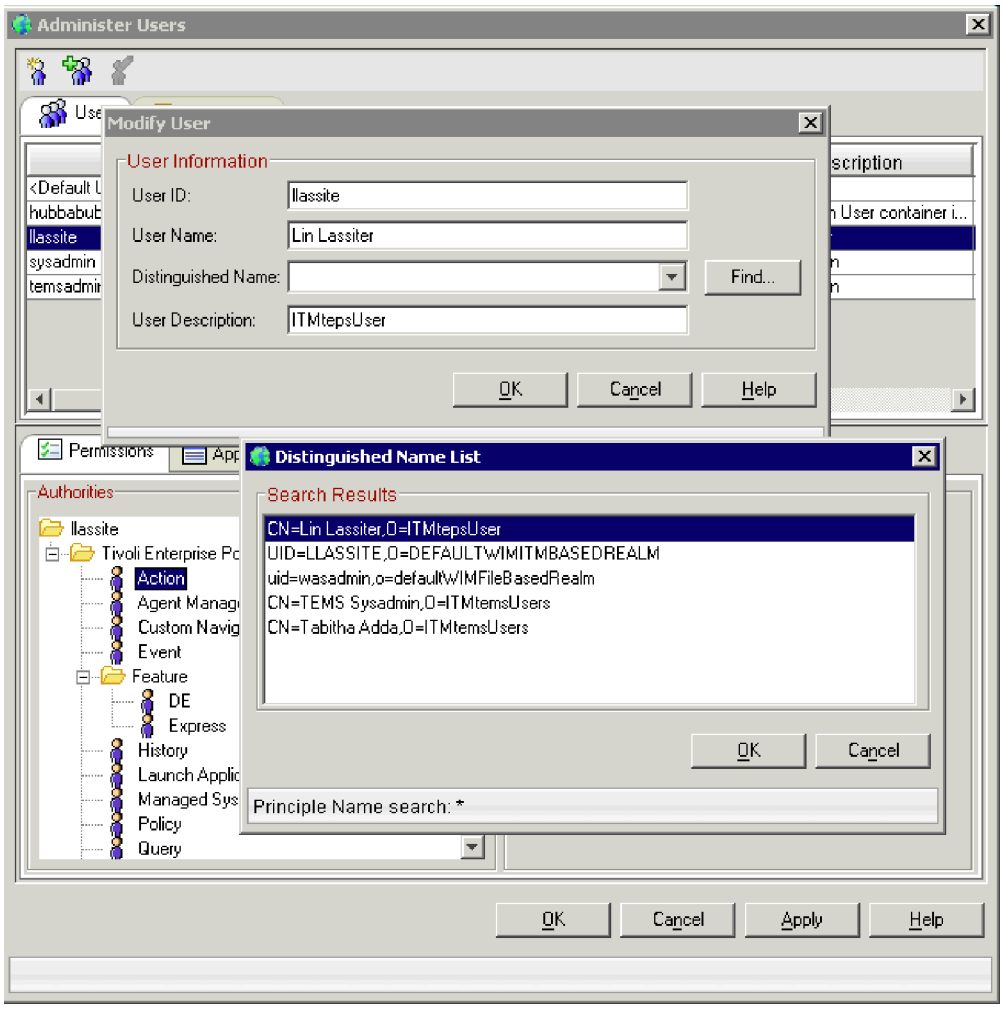

Figura 10. Pantalla Administrar usuarios de Tivoli Enterprise Portal. Los nombres distinguidos se resuelven en nombres base configurados dentro de TEPS/e para el repositorio; compare los valores que se presentan aquí con los mostrados en la Figura 2 en la página 130.

Correlación de ID de usuario de cliente de portal con nombres distinguidos de LDAP

"Correlación de los ID de usuario de Tivoli Enterprise Portal con nombres distinguidos de LDAP" en la página 118 ofrece los pasos necesarios para asociar los nuevos ID de usuario del servidor de portal con nombres distinguidos disponibles gracias a los pasos de configuración de TEPS/e anteriores. Los nombres distinguidos disponibles se relacionan directamente con la propiedad de configuración de base asociada a repositorio de TEPS/e **Nombre distinguido de una entrada base que identifica de forma exclusiva este conjunto de entradas en el territorio**.

Para mostrar todos los nombres distinguidos disponibles, primero suprima cualquier entrada del campo **Nombre distinguido**; luego pulse el botón **Buscar**. Toda la configuración de Territorio → Repositorio → Nombre distinguido base que identifica de forma exclusiva este conjunto de entradas en el territorio se muestra con los usuarios que ha devuelto IBM Tivoli Monitoring al realizar una consulta sobre Active Directory utilizando el valor **Propiedades de inicio de sesión**.

Estos usuarios se mostrarán utilizando su formato de CN de Active Directory (consulte la Figura 10 en la página 140).

Opción: Los pasos de configuración LDAP de Active Directory recomiendan que se creen ID de usuario de Tivoli Enterprise Portal antes de la configuración de TEPS/e. Opcionalmente, la creación de ID de servidor de portal puede esperar hasta después de que se haya completado la configuración de TEPS/e y los ID de usuario de Active Directory. Aquí la ventajaa consiste en que puede utilizar la función Crear usuario de la interfaz **Administrar usuarios** mientras tiene acceso a los nombres distinguidos para asegurarse de que el ID de usuario que asigna coincide con el nombre distinguido disponible.

Habilitación de la autenticación de LDAP en el servidor de portal

"Utilización de Manage Tivoli Enterprise Monitoring Services para configurar el servidor de portal para la autenticación de LDAP" en la página 104 y "Utilización de la línea de mandatos de Linux o UNIX para configurar el servidor de portal para la autenticación LDAP" en la página 108 proporcionan los pasos necesarios para habilitar la autenticación de usuarios del servidor de portal utilizando un registro de usuarios LDAP.

Nota: Cuando se le solicite que seleccione el tipo de LDAP, seleccione **Otro** y no proporcione valores ningún otro parámetro LDAP.

Después de haber terminado de configurar el servidor de portal para utilizar LDAP, consulte el tema "Hoja de ruta para configurar el servidor de portal para utilizar un registro de usuarios LDAP y el inicio de sesión único" en la página 100 para los pasos adicionales para completar la configuración.

Configuración de TEPS/e para TLS/SSL, si es necesario

Normalmente, TEPS/e está habilitado para TLS/SSL de forma predeterminada.

La comunicación SSL entre el servidor de portal y el servidor LDAP se configura utilizando la TEPS/e consola de administración. Siga los pasos descritos en "Configuración de la comunicación TLS/SSL entre el servidor de portal y el servidor LDAP" en la página 116.

Habilitación y configuración de la autenticación de usuarios de LDAP para el servidor de supervisión, si se desea

Omitir este paso: Si no desea utilizar un usuario LDAP para autenticar los usuarios del servidor de supervisión.

La configuración de usuarios para el Tivoli Enterprise Monitoring Server es un proceso distinto del correspondiente al Tivoli Enterprise Portal Server. TEPS/e no interviene.

Ni la configuración ni la habilitación de LDAP del servidor de portal afectan a la configuración o habilitación de LDAP del servidor de supervisión. No es necesario que los usuarios del servidor de supervisión se creen o existan en la lista de usuarios **Administrar usuarios** de Tivoli Enterprise Portal. Los usuarios del servidor de supervisión solo son necesarios si desea crear ID de usuario que se puedan autenticar mediante la opción **Seguridad: Validar usuario** o si desea habilitar o prohibir solicitudes SOAP al servidor SAP del servidor de supervisión (consulte el apartado "Configuración de Tivoli Monitoring Web Services (servidor SOAP)" en la página 573).

El apartado "Autenticación de usuarios a través del servidor de supervisión concentrador" en la página 86 contiene los pasos necesarios para habilitar la autenticación de usuarios de LDAP para el Tivoli Enterprise Monitoring Server. Aquí se proporcionan comentarios adicionales correspondientes a los pasos específicos de este proceso.

Nota: Los ID de usuario del servidor de supervisión tienen una limitación de 10 caracteres. lo que significa que los nombres de usuario de Active Directory que elija no pueden superar los 10 caracteres.

La configuración de LDAP del servidor de supervisión solo permite una base de LDAP y un filtro de usuario de LDAP (para consultar el directorio de LDAP en busca de atributos de ID de usuario). Se recomienda planificar OU para crear la base y la jerarquía de OU de Active Directory que mejor se ajusten a sus requisitos. Utilice una base que limite las búsquedas en el subárbol de directorios, mientras maximiza el rendimiento de la autenticación de usuarios de LDAP de Active Directory (consulte la Figura 1 en la página 129).

- Paso 5 en la página 89: consulte Figura 11 en la página 143.

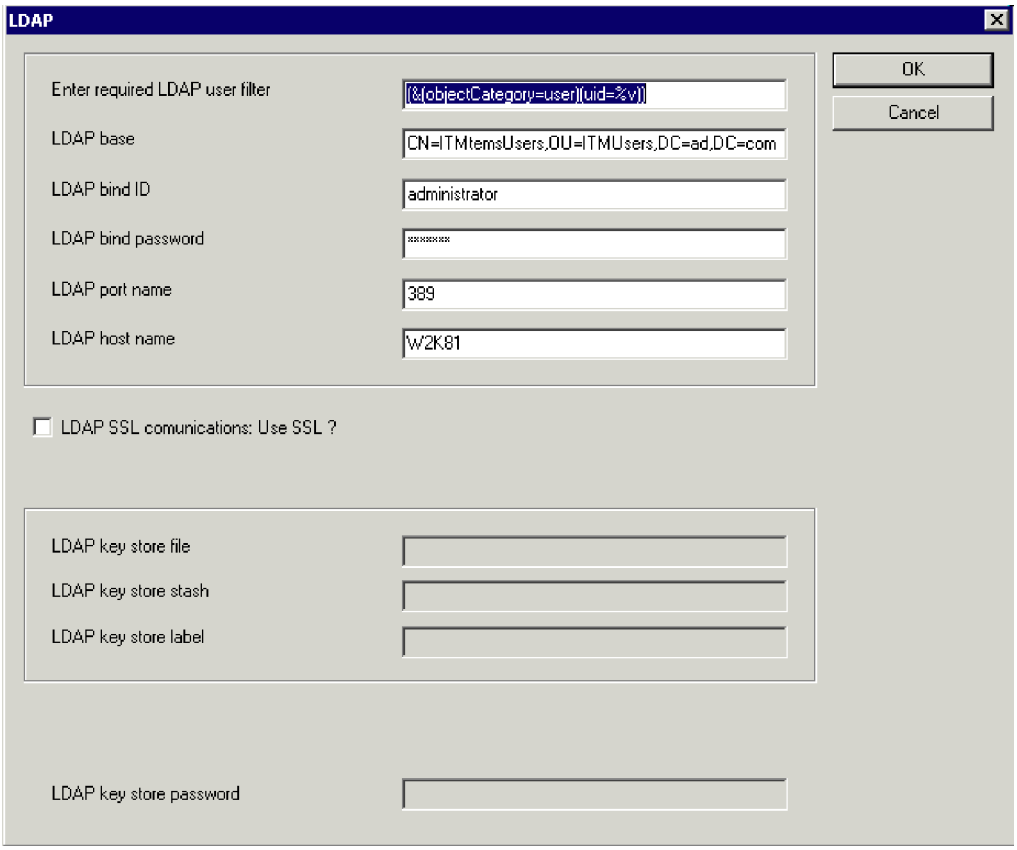

Figura 11. Panel de configuración de LDAP para usuarios del servidor de supervisión

Entrar filtro de usuario LDAP necesario
Esto define el atributo que se consultará y se recopilará para la autenticación de LDAP del Tivoli Enterprise Monitoring Server. El ID de usuario del servidor de supervisión para el inicio de sesión (**tacmd login –s nombre_tems –u nombreusuario –p contraseña**) se comparará con el usuario coincidente filtrado por Active Directory para valorar su autenticación.

Filtro de usuarios LDAP
Ejemplo: `(&(objectCategory=user)(userPrincipalName=%v@company.com))` donde `%v` es una variable que IBM Tivoli Monitoring sustituye por el ID de usuario especificado al iniciar la sesión.

este filtro consulta Active Directory, recopilando todos los objetos de usuario de la base especificada. Los valores del atributo **userPrincipalName** que devuelve esta consulta se analizarán contra la cadena de caracteres `%v@company.com`, ocasionando una comparación del ID de usuario del servidor de supervisión sólo con la parte de sustitución `%v` de **userPrincipalName** (en este caso, `userPrincipalName=llassite@company.com | userPrincipalName=%v@company.com == llassite`).

Base LDAP
IBM le recomienda que especifique una base de LDAP que le proporcione visibilidad del contenedor de OU que contiene los usuarios del servidor de supervisión definidos por Active Directory.

ID de vinculación LDAP
IBM recomienda que especifique un ID de LDAP que pueda acceder a la jerarquía de OU de Active Directory para localizar los usuarios de servidor de portal definidos por Active Directory.

Contraseña de vinculación LDAP
La contraseña del ID de vinculación de LDAP.

Nombre de puerto LDAP
Este valor se establece para el puerto de LDAP de Active Directory predeterminado. Especifique el número de puerto configurado por LDAP.

Nombre de host LDAP
Un controlador de dominio dentro del bosque de Active Directory que alberga las cuentas de usuario que ha creado anteriormente para la autenticación de usuarios de LDAP del servidor de supervisión. Esta opción debe basarse en el nivel de jerarquía dentro del bosque que alberga el OU de los usuarios de Tivoli Monitoring. Tenga en cuenta la selección que haga aquí cuando analice posibles problemas con la autenticación de usuarios de LDAP de IBM Tivoli Monitoring debidos a la conectividad de Active Directory o a errores de replicación de los objetos de usuario de Active Directory.

Herramientas de verificación de LDAP de Active Directory

Microsoft Active Directory ofrece varias herramientas que puede utilizar para gestionar el entorno de LDAP del sitio; las dos siguientes resultan especialmente útiles cuando se enlaza con IBM Tivoli Monitoring:

ADSI Edit
Utilice este conector de Microsoft Management Console conector para ver los atributos de los objetos de usuario y para confirmar que los atributos que especifica para las **Propiedades de inicio de sesión** del Tivoli Enterprise Portal Server y para el parámetro de sustitución **attributename=%v** del Tivoli Enterprise Monitoring Server estén definidos y disponibles.

LDP.exe
Utilice esta herramienta para validar los valores base de configuración de LDAP del servidor de supervisión y del servidor de portal. Esta herramienta le permite conectar, vincular y consultar el entorno de LDAP desde la estación de trabajo; consulte la Figura 12 en la página 145.

LDP.exe para Windows XP está disponible desde Microsoft en este URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en

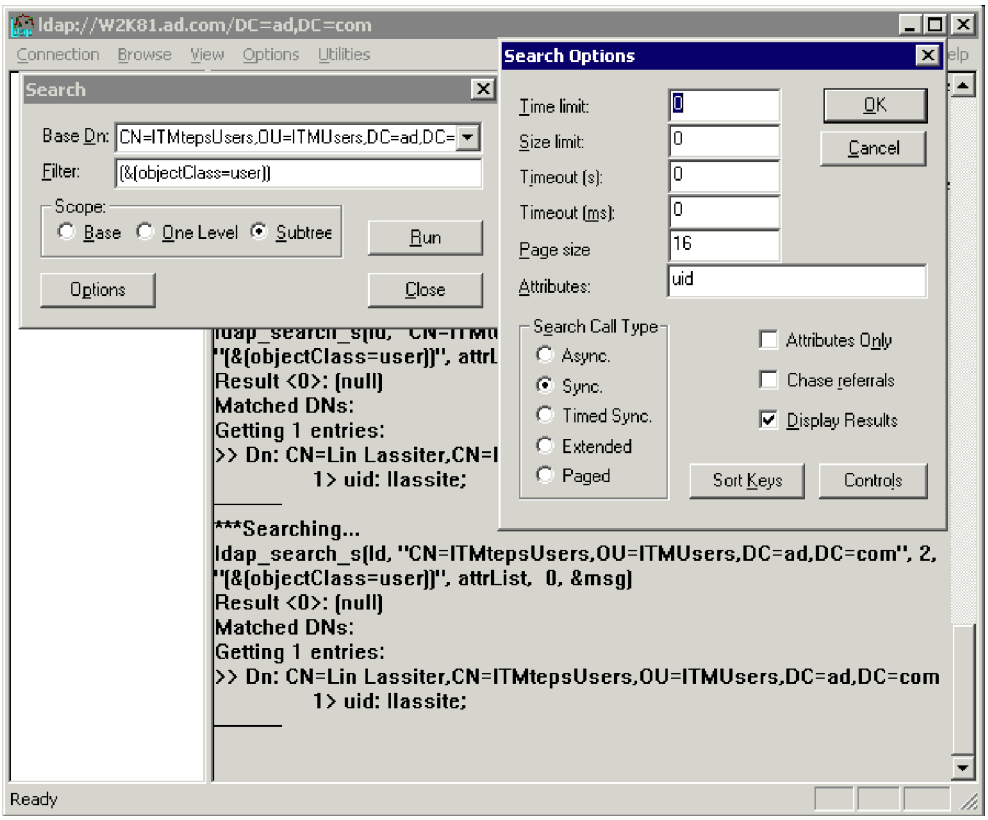

Figura 12. Resultados de la consulta de LDP

Este ejemplo muestra la verificación de una configuración utilizando:

```
LDAP filter object = (&(objectCategory=user)(uid=%v))
LDAP base = CN=ITMtemsUsers,OU=ITMUsers,DC=company,DC=com
```

Como alternativa, este ejemplo muestra la verificación de una configuración utilizando:

```
LDAP base = CN=ITMtepsUsers,OU=ITMUsers,DC=company,DC=com
Login properties = uid
```

Para configurar correctamente la autenticación de LDAP de Microsoft Active Directory, necesita el administrador del dominio o necesita disponer de dos herramientas muy útiles que le permitan buscar en el directorio de LDAP desde fuera. Estas herramientas son:

ldapsearch

Utilice esta herramienta para probar las cadenas de conexión desde la línea de mandatos y para verificar que está apuntando a la ubicación correcta dentro del registro de usuarios de LDAP. La Figura 17 en la página 152 muestra información de salida de `ldapsearch` de ejemplo.

El apartado "Información sobre ldapsearch para LDAP" en la página 91 contiene información adicional sobre este mandato y sus usos y opciones.

Las opciones de `ldapsearch` que especifique (consulte el apartado "opciones de línea de mandatos de ldapsearch" en la página 92) se basan en la configuración de LDAP del Tivoli Enterprise Monitoring Server del sitio:

-h es el nombre de host de LDAP.

-p es el nombre de puerto de LDAP.

-b es el valor base de LDAP.

-D es el ID de vinculación de LDAP.

-w es la contraseña de vinculación de LDAP.

Nota: Si no especifica la opción -w, tendrá que especificar la contraseña de vinculación de LDAP desde el teclado.

Especifique siempre la opción `ldapsearch` -s *sub*, ya que el cliente LDAP del servidor de supervisión la utiliza al autenticar usuarios de Tivoli Monitoring. Sustituya `%v` por el ID de usuario de Tivoli Monitoring cuando especifique el filtro de usuarios de LDAP (esta cadena es la última parte de la línea de mandatos de `ldapsearch`).

Ejemplo: Para verificar el usuario `sysadmin` con la configuración de LDAP del servidor de supervisión mostrada en la Figura 16 en la página 151, especifique el siguiente mandato `ldapsearch`:

```
ldapsearch -h 192.168.1.241 -p 389 -b "DC=bjomain,CN=users,DC=bjomain,
      DC=com"
           -D "CN=Administator,CN=users,DC=bjomain,DC=com" -w admin10admin
           -s sub "(mail=sysadmin@bjomain.com)"
```

Siga este enlace para descargar una versión gratuita de `ldapsearch`: http://publib.boulder.ibm.com/infocenter/wasinfo/v4r0/index.jsp?topic=/com.ibm.support.was40.doc/html/Security/swg21113384.html

ldapbrowser

Utilice esta herramienta para atravesar gráficamente el registro de usuarios de LDAP y para especificar los nombres distinguidos y otros parámetros que necesita para completar la configuración. Para verificar que IBM Tivoli Monitoring pueda acceder al registro de usuarios de LDAP a través de la red, instale el navegador de LDAP en un servidor de Tivoli Monitoring. La Figura 15 en la página 150 muestra una pantalla de `ldapbrowser` de ejemplo.

El navegador LDAP también le permite recuperar información de LDAP del propio servidor de portal.

Siga este enlace para descargar una versión gratuita de `ldapbrowser`: http://www.ldapbrowser.com/download.htm; luego pulse el separador **Navegador de LDAP**. `ldapbrowser` está disponible también para UNIX/Linux y para Windows en este URL: http://www.mcs.anl.gov/~gawor/ldap/

Casos de usuarios

En estos casos, lo deseable es que toda la autenticación de usuarios se realice mediante el registro de usuarios de LDAP de Microsoft Server 2003 Active Directory del sitio. Hay dos formas posibles de configurar la autenticación para los usuarios de IBM Tivoli Monitoring:

Autenticación de LDAP del servidor de supervisión

Configure la autenticación en el Tivoli Enterprise Monitoring Server utilizando un filtro de nombres de usuario que correlacione un ID de usuario especificado en Tivoli Enterprise Portal (como por ejemplo *name*) con *name*`@company.com`. El usuario inicia la sesión como *name*, que luego se convierte a través del filtro para que coincida con la búsqueda de LDAP necesaria.

Este método se describe en "Autenticación de ID de usuario del servidor de supervisión con Microsoft Active Directory".

Autenticación de LDAP del servidor de portal
Configure la autenticación en el Tivoli Enterprise Portal Server de modo que el ID de usuario que especifica el usuario al iniciar la sesión en Tivoli Enterprise Portal se pueda buscar y autenticar en un registro de usuarios de LDAP. En este caso, el usuario inicia una sesión con *firstname.lastname@company.com*.

Este método se describe en "Autenticación de ID de usuario del servidor de portal con Microsoft Active Directory" en la página 152.

Autenticación de ID de usuario del servidor de supervisión con Microsoft Active Directory

Este caso muestra cómo puede configurar el Tivoli Enterprise Monitoring Server para que utilice Microsoft Active Directory para autenticar usuarios del servidor de supervisión.

Este caso no necesita la configuración de TEPS/e para que funcione. El inconveniente de esta solución es que SSO (inicio de sesión única) no se puede implementar y que los ID de usuario están limitados a 10 caracteres como máximo. La ventaja es que la autenticación de usuarios basada en el servidor de supervisión permite a los usuarios realizar solicitudes de servidor SOAP y utilizar el mandato **tacmd** que envían las solicitudes al servidor de supervisión concentrador.

Entorno

El entorno comprende dos sistemas, uno que ejecuta el servidor de supervisión Tivoli Monitoring (dirección IP 192.168.1.240) y uno que ejecuta Microsoft Windows 2003 Advanced Server configurado como controlador de dominio de Microsoft Active Directory (dirección IP 192.168.1.241). Observe que el sistema Tivoli Monitoring es un servidor autónomo llamado **itm6210** y no forma parte del dominio configurado. El dominio de muestra se llama **bjomain.com** y el servidor de Active Directory se llama **msad**.

Configuración de Microsoft Active Directory:

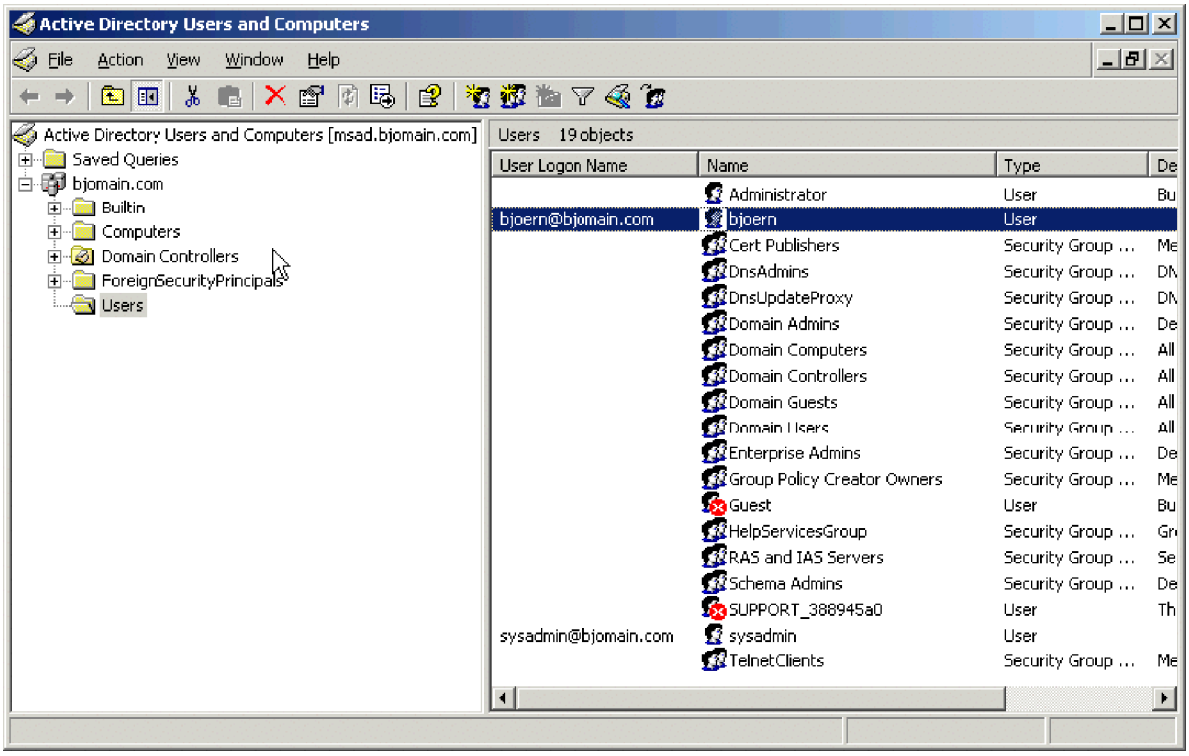

Figura 13. Listado de usuarios de Active Directory

Tal como se muestra en la Figura 13, se han configurado dos usuarios en Active Directory, *sysadmin* y *bjoern*, ambos con direcciones de correo electrónico, tal como se muestra en la Figura 14 en la página 149 (verá cuando se configure el filtro de LDAP en IBM Tivoli Monitoring por qué la dirección de correo electrónico es importante). Puede utilizar otros parámetros, pero este es el que recomiendan las instrucciones del apartado "Autenticación de usuarios a través del servidor de supervisión concentrador" en la página 86.

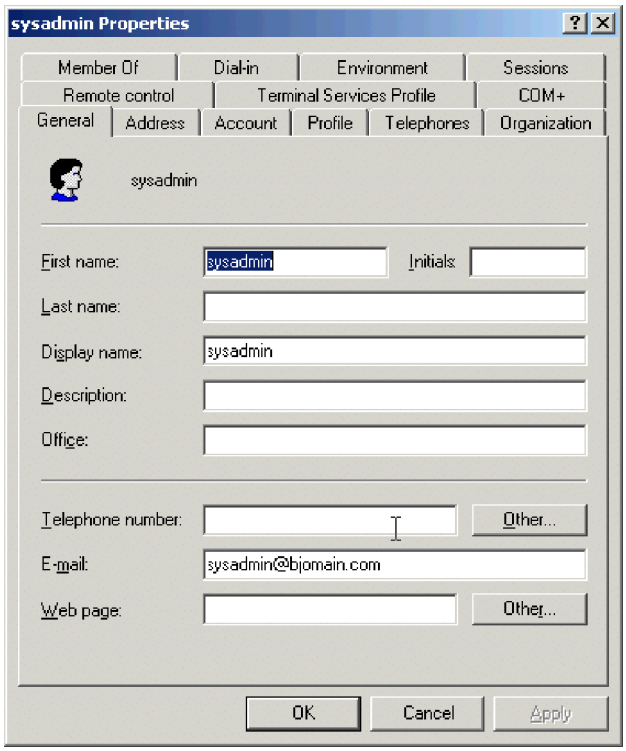

Figura 14. Propiedades de un usuario de Tivoli Monitoring individual

Examen de Active Directory: El examen de Active Directory Repository con el examinador de GUI, `ldapbrowser`, muestra todos los parámetros que necesita, como Nombre distinguido y dirección de correo electrónico para el usuario *sysadmin* (consulte la Figura 15 en la página 150).

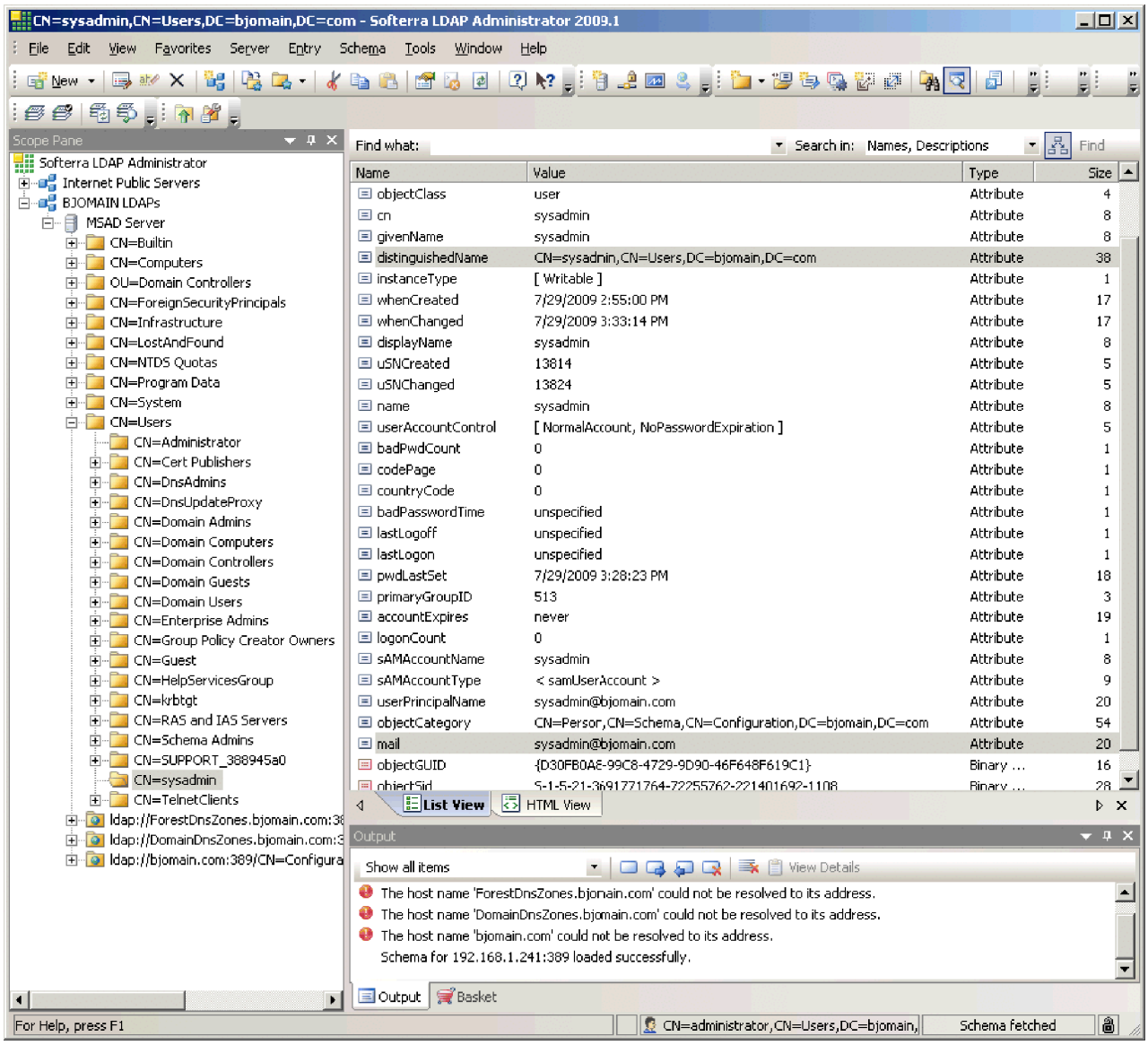

Figura 15. Ventana de ldapbrowser

Si pulsa con el botón derecho en **Servidor MSAD** en la parte superior del árbol y selecciona **Propiedades**, puede ver que el DN base (el punto en el que Tivoli Monitoring comenzará a buscar usuarios) es **DC=bjomain,DC=com**.

El siguiente paso consiste en comparar esta información con los campos adecuados en el diálogo de configuración del Tivoli Enterprise Monitoring Server.

Agrupación de piezas: La Figura 16 en la página 151 muestra los valores de LDAP del servidor de supervisión que le permiten iniciar una sesión como *sysadmin* o *bjoern* (sólo estos usuarios están definidos en el servidor de supervisión).

Nota: Si tiene que activar Secure Sockets Layer, SSL, seguridad para comunicaciones entre Tivoli Monitoring y Active Directory, consulte el Capítulo 8, “Protección de las comunicaciones”, en la página 215. Asegúrese también de tener a mano los valores de parámetros que aparecen en la Tabla 11 en la página 89.

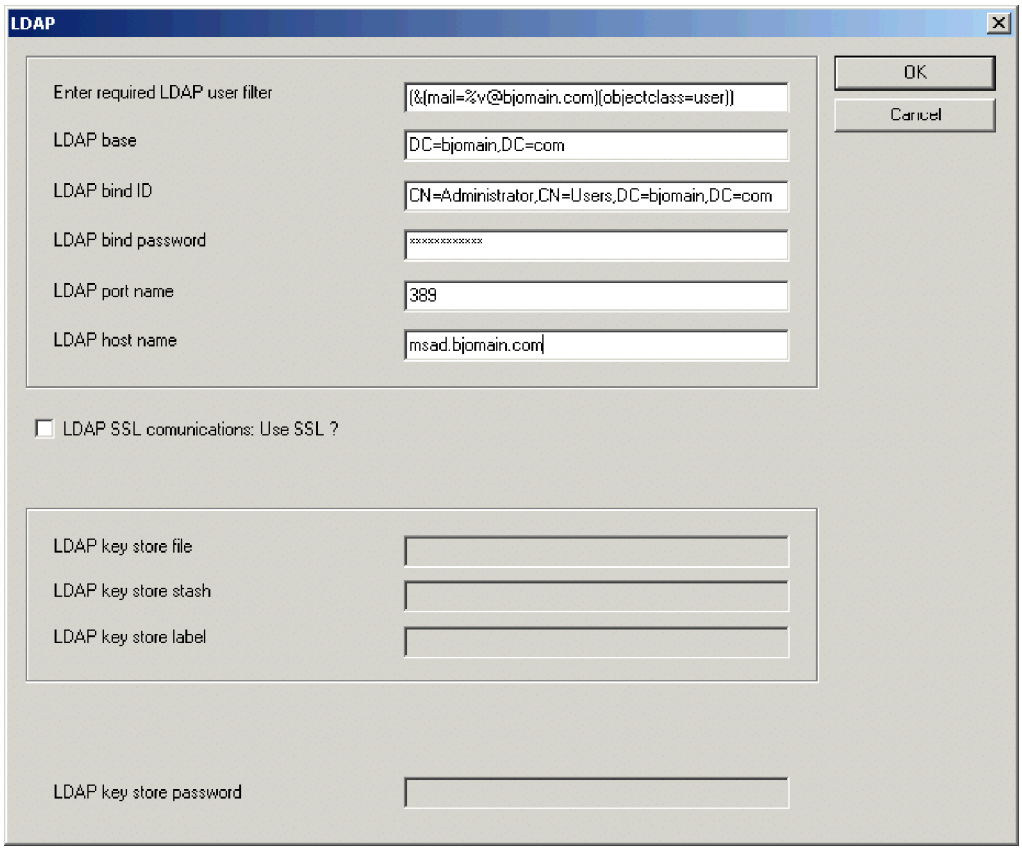

Figura 16. Parámetros de LDAP del servidor de supervisión

A continuación se muestran algunos de los parámetros más importantes que aparecen en la Figura 16:

Entrar filtro de usuario LDAP necesario
Este parámetro indica que hay que buscar el parámetro **correo** dentro del objeto de usuario.

Es la razón por la que ha incluido la dirección de correo electrónico en la entrada de Active Directory del usuario.

%v Es una variable que Tivoli Monitoring sustituye por el ID de usuario especificado en la pantalla de inicio de sesión.

Base LDAP
Es el DN base completo que aparece en el apartado "Examen de Active Directory" en la página 149.

Si IBM Tivoli Monitoring indica que el usuario ha especificado una contraseña errónea, esto es señal de que aquí se ha especificado un DN de base de LDAP erróneo, en cuyo caso Tivoli Monitoring comienza su búsqueda en la ubicación de LDAP equivocada.

ID de vinculación LDAP
Especifique el nombre distinguido de un usuario que tenga permiso de lectora sobre el DN base completo donde Tivoli Monitoring comenzará a buscar sus usuarios.

Nota: No es suficiente especificar sólo el nombre de usuario, por ejemplo *sysadmin*.

Cuando tenga los parámetros correctamente definidos, utilice el mandato **grep** para buscar la cadena de caracteres `LDAP` en el archivo de registro del servidor de supervisión para verificar que no haya errores. Si lo desea, puede utilizar el programa de utilidad `ldapsearch` para probar los parámetros sin iniciar el servidor de supervisión: si `ldapsearch` no devuelve una información de salida parecida a la que se muestra en la Figura 17, significa que la entrada es incorrecta. Debe verificar los parámetros de LDAP del sitio antes de reiniciar el servidor de supervisión, ya que una configuración de LDAP incorrecta impedirá que los usuarios inicien una sesión.

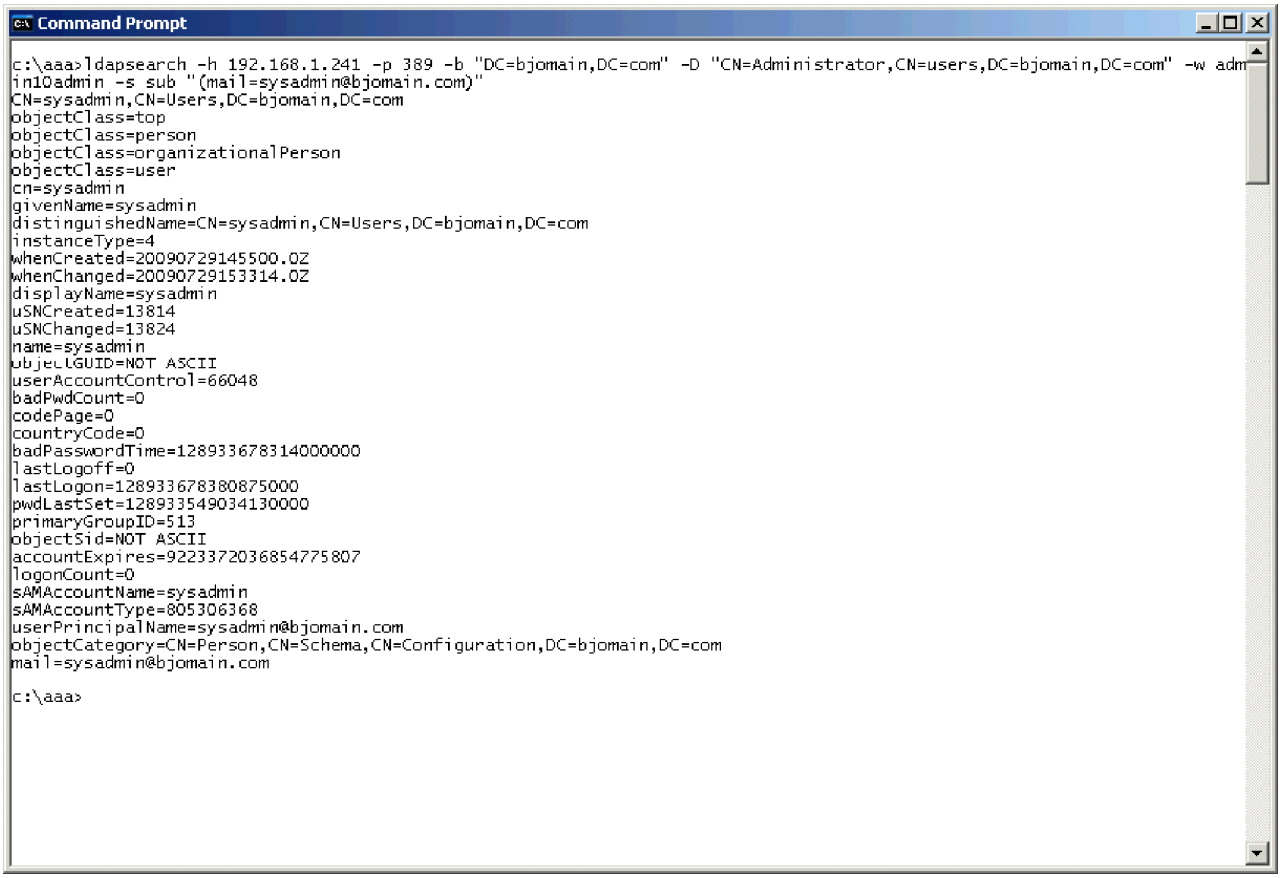

Figura 17. Resultados de ldapsearch para ID de servidor de supervisión

Autenticación de ID de usuario del servidor de portal con Microsoft Active Directory

En este caso, se configura el servidor de portal para utilizar el servidor para autenticar los usuarios porque se desea utilizar el inicio de sesión único con otras aplicaciones o se desea que los usuarios de Tivoli Enterprise Portal inicien sesión con ID de usuario de más de 10 caracteres.

El sitio ha intentado utilizar el programa de utilidad Manage Tivoli Enterprise Monitoring Services o la interfaz de línea de mandatos **itmcmd** del servidor de portal para configurar la autenticación LDAP. Esto no ha resultado satisfactorio porque el mecanismo de autenticación integrado intenta buscar un campo de LDAP llamado **uid**; los registros de LDAP de Active Directory de este cliente no tienen ningún campo **uid**.

El resto de esta sección muestra los pasos de autenticación de usuarios que debe seguir mediante la consola de administración de TEPS/e, el servidor eWAS integrado del servidor de portal que define las correlaciones de usuarios de LDAP personalizadas para el acceso a Tivoli Enterprise Portal en esta empresa.

Información necesaria sobre el entorno de LDAP

Para autenticar usuarios ante el registro de usuarios de LDAP de Active Directory, se necesitan varias piezas de información:

1. El tipo y la ubicación del almacén de información de LDAP.
2. El método de recuperación de dicha información — especialmente si se debe utilizar o no SSL.
3. Un **ID de vinculación** y una **Contraseña**, una combinación de ID de usuario y contraseña que el sistema utilizará para iniciar una sesión en el almacén de LDAP y buscar cuentas de usuario.

   Este ID debe estar en formato completo de nombre distinguido de LDAP.
4. Las **Propiedades de inicio de sesión** que se deben utilizar — especialmente qué cambio de LDAP hay que buscar. Este campo debe estar dentro del almacén de información de LDAP e identificar de forma exclusiva un usuario en el entorno.

   En las instrucciones del apartado "Autenticación de usuarios LDAP a través del servidor de portal" en la página 94 se da por supuesto que tiene el campo **uid** disponible; este no es el caso del directorio de LDAP del cliente.
5. Una **Base de LDAP**, el nombre distinguido de LDAP completo de una entrada base del registro de usuarios de LDAP.

En este ejemplo, el administrador de Active Directory del sitio ha proporcionado la siguiente información sobre LDAP:

1. Tipo de LDAP: Microsoft Active Directory Server versión 2003; ubicación: Nombre de host `adhost.`*`company`*`.com`
2. Puerto que utilizar: 636 (lo que indica que se necesita SSL para la conexión)
3. ID de vinculación de `svc.tivolisec@`*`company`*`.com`, junto con la contraseña adecuada
4. El campo **Propiedades de inicio de sesión** que se debe utilizar: la **dirección de correo electrónico** del usuario
5. La **Base de LDAP**: `DC=US,DC=GLOBAL,DC=`*`company`*`,DC=COM`

A pesar de tener toda la información sobre conexión necesaria, cada intento de conectar con el registro de usuarios de LDAP falla. Puede utilizar los programas de utilidad de LDAP descritos en el apartado "Herramientas de verificación de LDAP de Active Directory" en la página 144 para buscar y verificar la información sobre conexión y determinar por qué cada intento de conexión falla.

En este ejemplo, se utilizan dos programas de utilidad: `LDP.exe` y `ldapbrowser`. Estos programas de utilidad muestran que la comunicación SSL no es necesaria en este entorno de cliente; por lo tanto la conexión en el puerto LDAP sin cifrar normal 389 es válida. Las herramientas también muestran que el nombre distinguido de LDAP completo asociado a la dirección `svc.tivolisec@`*`company`*`.com` es `CN=svc.tivolisec,OU=ServiceAccount,DC=us,DC=global,DC=`*`company`*`,DC=com`.

Una vez validadas estas entradas, es el momento de utilizar las herramientas de administración de TEPS/e (eWAS) para definir los parámetros de búsqueda de LDAP para la administración de usuarios de Tivoli Monitoring.

Habilitación de la administración de TEPS/e: La habilitación de la consola de administración de TEPS/e (eWAS), Integrated Solutions Console, requiere que complete los pasos siguientes.

Nota: El paso 1 se debe realizar sólo una vez. Los pasos restantes se deben realizar cada vez que desee utilizar la consola de administración de TEPS/e.

Defina la contraseña de wasadmin: Antes de completar la administración de TEPS/e, debe establecer una contraseña para la cuenta `wasadmin` que le admita en el servidor de eWAS. Para ello, invoque el script `updateTEPSEPass.sh` en el directorio `$CANDLEHOME/iw/scripts` o utilice la interfaz de Manage Tivoli Enterprise Monitoring Services.

Este procedimiento solo se tiene que realizar una vez, a no ser que posteriormente desee cambiar la contraseña del usuario `wasadmin`.

Mediante la línea de mandatos

Para definir la contraseña de `wasadmin` mediante la línea de mandatos, invoque el script `updateTEPSEPass.sh` en el directorio `$CANDLEHOME/$INTERP/iw/scripts`:

```
# cd $CANDLEHOME/$INTERP/iw/scripts
# ./updateTEPSEPass.sh wasadmin newpw
WASX7209I: Conectado a proceso "ITMServer" en nodo ITMNode mediante conector SOAP;
El tipo de proceso es: UnManagedProcess
WASX7303I: Se pasan las siguientes opciones al entorno de script y están
disponibles como argumentos que se almacenan en la variable argv: "[wasadmin, newpw]"
```

Mediante Manage Tivoli Enterprise Monitoring Services

1. Pulse con el botón derecho del ratón en la entrada de **Tivoli Enterprise Portal Server** y seleccione la opción de menú **Administración de TEPS/e → Habilitar administración de TEPS**.
2. En la ventana **Especificar contraseña**, proporcione la nueva contraseña `wasadmin` y pulse **Aceptar**.

   El efecto del intento de cambio de contraseña se muestra en el panel de mensajes de Manage Tivoli Enterprise Monitoring Services. Por ejemplo:

   ```
   La contraseña del usuario wasadmin se ha cambiado
   ```

Habilitación de ISCLite (administración de servidores TEPS/e eWAS): Siempre que necesite gestionar la autenticación de LDAP del sitio, primero debe habilitar la administración de TEPS/e mediante Integrated Solutions Console. Tenga en cuenta que cuando vuelva a configurar o detenga y luego reinicie el Tivoli Enterprise Portal Server, la consola de TEPS/e se inhabilitará automáticamente.

Mediante la línea de mandatos

Para habilitar la consola de TEPS/e mediante la línea de mandatos, invoque el script `enableISCLite.sh` desde el subdirectorio `$CANDLEHOME/platformcode/iw/scripts` en la máquina del servidor de portal:

```
# pwd /apps/TEPS_s11154cdc/li6263/iw/scripts

# ./enableISCLite.sh true
WASX7209I: Conectado a proceso "ITMServer" en nodo ITMNode mediante conector SOAP;
El tipo de proceso es: UnManagedProcess
```

```
WASX7303I: Se pasan las siguientes opciones al entorno de script y están
disponibles como argumentos que se almacenan en la variable argv: "[true]"

ISCLite iniciado
```

Mediante Manage Tivoli Enterprise Monitoring Services

1. Pulse con el botón derecho del ratón en la entrada de **Tivoli Enterprise Portal Server** y seleccione la opción de menú **Administración de TEPS/e → Habilitar administración de TEPS/e**.
2. El efecto del intento de habilitación se muestra en el panel de mensajes de Manage Tivoli Enterprise Monitoring Services. Por ejemplo:

   ```
   ISCLite se ha habilitado satisfactoriamente
   ```

Inicio de sesión en la consola de administración de TEPS/e: Inicie eWAS Integrated Solutions Console en el navegador utilizando la siguiente dirección:

`http://tepsserver.company.com:15205/ibm/console`

Inicie la sesión con el nombre de usuario `wasadmin` y la contraseña que haya establecido para dicho usuario en "Defina la contraseña de `wasadmin`" en la página 154.

Definición del registro de usuarios de LDAP en Integrated Solutions Console: Cuando utilice Integrated Solutions Console para definir el registro de usuarios de LDAP, siga estos pasos:

1. En la parte izquierda de la pantalla principal de Integrated Solutions Console, amplíe la lista de opciones de **Seguridad** y seleccione **Seguridad global**. Se muestra el panel **Seguridad global**.
2. Bajo la sección **Repositorio de cuentas de usuario**, pulse **Configurar**.
3. En el separador **Configuración**, pulse **Gestionar repositorios** en la parte inferior bajo **Elementos relacionados** para que aparezca la pantalla en la que puede definir su registro de usuarios de LDAP:

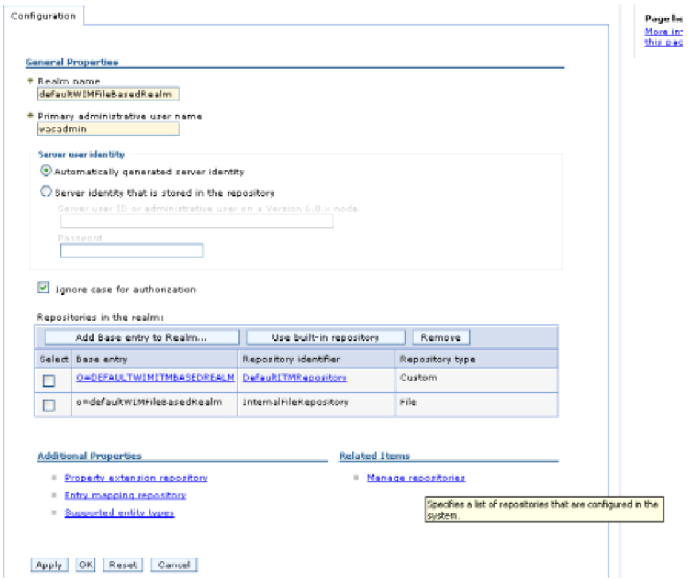

Figura 18. El separador del cuaderno Configuración de Integrated Solutions Console

4. En la pantalla **Gestionar repositorios**, pulse **Añadir**:

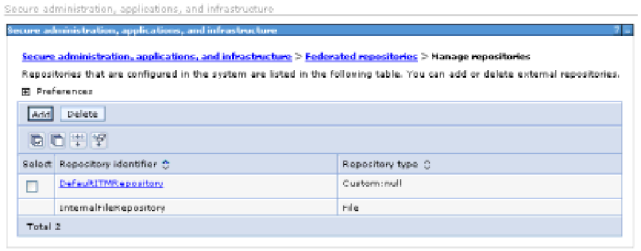

Figura 19. La pantalla Gestionar repositorios de Integrated Solutions Console

Aparece la pantalla **Propiedades generales**, que se muestra en la Figura 20. Aquí es donde suministra la información que define la ubicación y la configuración del registro de usuarios de LDAP.

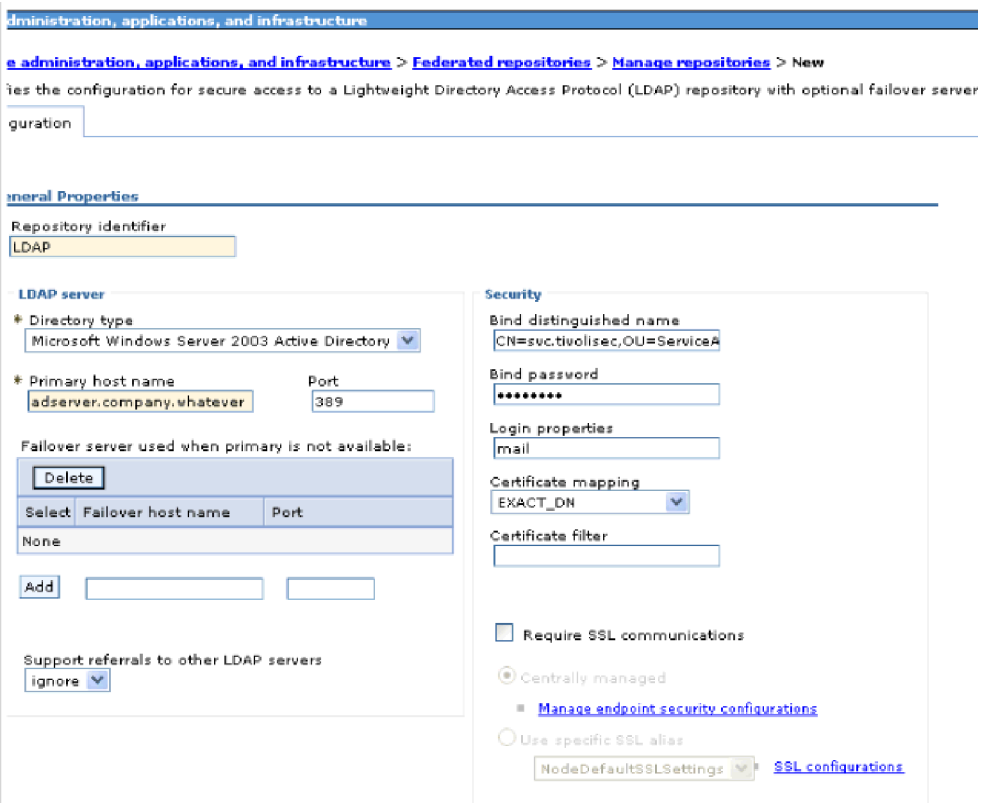

Figura 20. La pantalla Propiedades generales de Integrated Solutions Console

5. Complete esta pantalla con la información siguiente:

   Identificador de repositorio
   Un nombre en formato libre para el registro, en este caso es simplemente **LDAP**.

   Nombre de host principal
   Nombre de host del servidor LDAP, en este caso `adhost.company.com`.

   Puerto Puerto en el que escucha el servidor LDAP. En este ejemplo, 389 es el valor válido.

   Nombre distinguido de vinculación
   El nombre distinguido completo de LDAP del ID de vinculación. En

este caso, el nombre distinguido completo de LDAP para la cuenta `svc.tivolisec` que ha suministrado el administrador de LDAP del sitio es `CN=svc.tivolisec,OU=ServiceAccount,DC=us,DC=global,DC=`*`company`*`,DC=com`.

Contraseña de vinculación
La contraseña del ID de vinculación.

Propiedades de inicio de sesión
Las propiedades de inicio de sesión que se utilizarán para este nombre distinguido, en este caso la propiedad **mail**.

Cuando haya completado esta página, pulse **Aceptar**. Se muestra la pantalla de verificación:

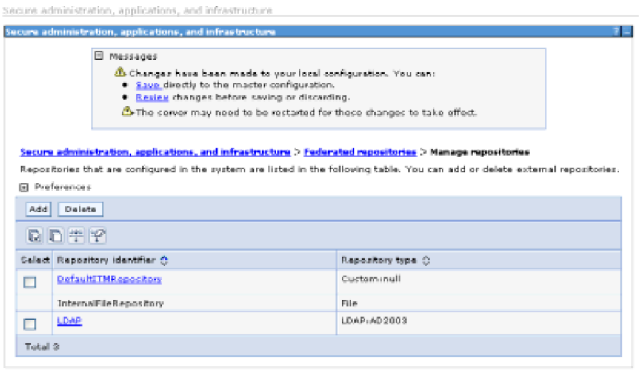

Figura 21. La pantalla de verificación de Integrated Solutions Console

6. Pulse **Guardar**.

Ya está definido el registro de usuarios de LDAP del sitio.

Añada su registro de usuarios de LDAP al territorio de eWAS: El siguiente paso consiste en añadir el registro recién definido al territorio de eWAS para que el sitio pueda utilizar LDAP para buscar ID de usuario.

1. En la parte izquierda de la pantalla principal de Integrated Solutions Console, bajo las opciones de seguridad, seleccione **Seguridad global**.
2. En la sección **Repositorio de cuentas de usuario**, pulse **Configurar** (en la parte inferior, junto a Repositorios federados).

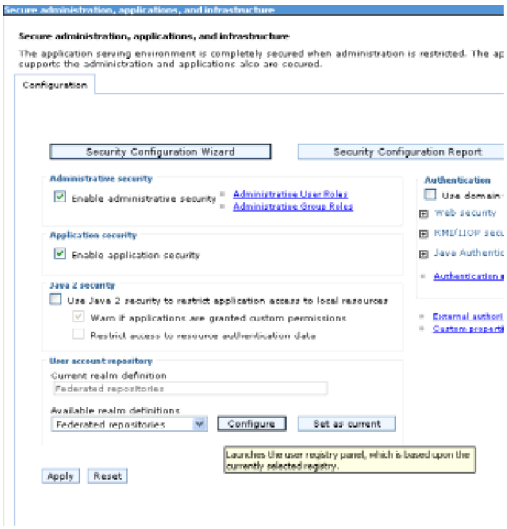

Figura 22. El separador del cuaderno Configuración de Integrated Solutions Console

Se abrirá la pantalla en la que puede añadir registros al territorio.

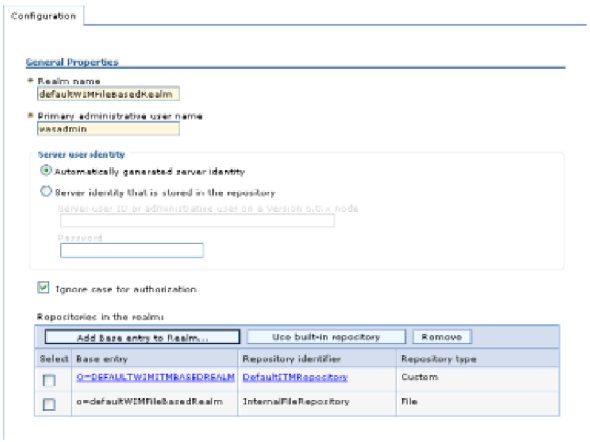

Figura 23. El separador Configuración de Integrated Solutions Console

3. Para añadir el repositorio definido en el apartado “Definición del registro de usuarios de LDAP en Integrated Solutions Console” en la página 155, pulse **Añadir entrada base a territorio**.

   Se muestra la pantalla **Referencia de repositorio**, en la que puede añadir el registro de usuarios de LDAP al territorio de eWAS del sitio:

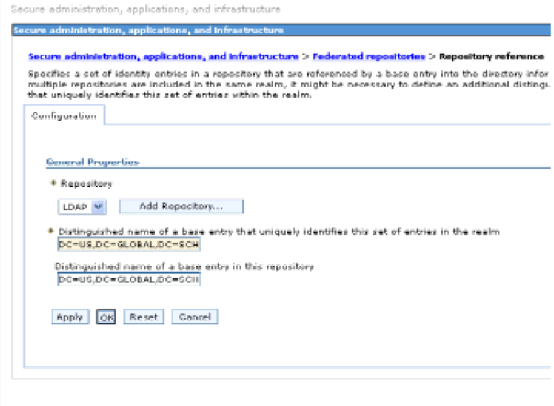

Figura 24. La pantalla Referencia de repositorio de Integrated Solutions Console

En esta pantalla, asegúrese de que **Repositorio** tenga el valor **LDAP** (o el **Identificador de repositorio** que ha asignado en el apartado "Definición del registro de usuarios de LDAP en Integrated Solutions Console" en la página 155). En los dos campos de entrada, especifique el **Nombre distinguido de vinculación**, que en esta instancia se ha definido como `DC=US,DC=GLOBAL,DC=`*`company`*`,DC=COM`. Luego pulse **Aceptar**.

4. En la pantalla de verificación de Integrated Solutions Console, pulse **Guardar**.

Figura 25. La pantalla de verificación de Integrated Solutions Console

5. Esto le devuelve a la lista de registros del territorio actual.

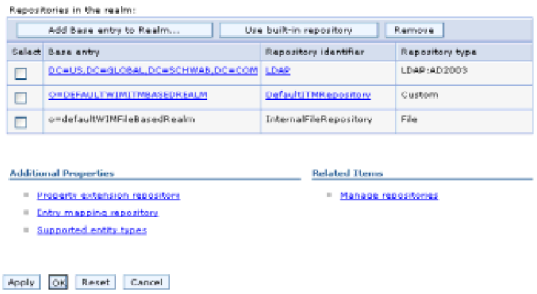

Figura 26. La pantalla de repositorios de Integrated Solutions Console del territorio

Pulse **Aceptar**.

6. En la pantalla de verificación de Integrated Solutions Console, pulse **Guardar**:

Figura 27. La pantalla de verificación de Integrated Solutions Console

7. esto le devuelve a la pantalla inicial de inicio de sesión de Integrated Solutions Console:

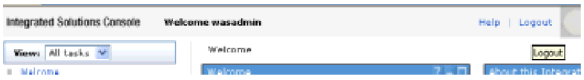

Figura 28. La pantalla de inicio de sesión de Integrated Solutions Console

Pulse **Finalizar sesión**.

8. Reinicie el Tivoli Enterprise Portal Server.

(Opcionalmente) probar la búsqueda de LDAP dentro de TEPS/e: Puede probar la búsqueda de LDAP dentro de la propia consola de TEPS/e. Si la búsqueda funciona aquí correctamente, funcionará dentro del Tivoli Enterprise Portal Server.

1. Vuelva a habilitar la consola de TEPS/e (consulte el apartado "Habilitación de ISCLite (administración de servidores TEPS/e eWAS)" en la página 154) y vuelva a iniciar una sesión utilizando el ID de usuario `wasadmin` y la contraseña recién asignada (consulte el apartado "Inicio de sesión en la consola de administración de TEPS/e" en la página 155).

   Se muestra la pantalla inicial de TEPS/e:

Figura 29. La pantalla inicial de Integrated Solutions Console

2. Amplíe la lista de **Usuarios y grupos**; luego seleccione **Gestionar usuarios**.
3. Dentro del panel **Gestionar usuarios**, establezca **Buscar por** en **Correo electrónico** y especifique el ID de usuario de prueba (es decir, la dirección de correo electrónico) en el campo **Buscar**.
4. Pulse **Buscar**.

Si la dirección de correo electrónico que ha especificado se encuentra, sus características se muestran en la parte inferior del panel **Gestionar usuarios**.

Definición de un ID de usuario de prueba utilizando la administración de usuarios del servidor de portal:

1. Inicie una sesión en un cliente del Tivoli Enterprise Portal utilizando el ID de usuario `sysadmin`. Tenga en cuenta que `sysadmin` aún está definido como ID del servidor de portal local (es decir, no está almacenado dentro del registro de usuarios de LDAP ni se recupera del mismo).
2. Mediante la administración de usuarios del Tivoli Enterprise Portal (tal como se explica en el apartado "Autenticación de usuarios LDAP a través del servidor de portal" en la página 94), cree un nuevo usuario con el ID de usuario que desee.
3. En el campo Nombre distinguido, especifique una parte suficiente de la dirección de correo electrónico de dicha persona para que la especificación sea exclusiva; luego pulse el botón **Buscar**.

   Se realiza la búsqueda de LDAP y se encuentra el nombre distinguido de LDAP completo para la dirección de correo electrónico.
4. Resalte el nombre distinguido y pulse **Aceptar**.
5. Complete los campos de ID de usuario restantes del usuario y luego pulse **Aceptar** para añadirlo.

Ahora esta persona puede iniciar sesión en el cliente de Tivoli Enterprise Portal utilizando su dirección de correo electrónico, *longemailaddress@customer*.com, como ID de usuario y su contraseña de Active Directory como contraseña. El usuario iniciará la sesión en su espacio de trabajo principal predeterminado.

Capítulo 6. Utilización de la autorización de usuario de Tivoli Enterprise Portal

Cada sesión de trabajo de portal empieza con un inicio de sesión satisfactorio y una conexión con Tivoli Enterprise Portal. Los ID de usuario y los grupos de usuarios de inicio de sesión se crean y se perfilan mediante la ventana Administrar usuarios.

Administrar usuarios es una ventana con varios separadores y dos paneles. El panel superior tiene dos separadores: **Usuarios** y **Grupos de usuarios**, que listan los ID de usuario, los nombres distinguidos si el servidor del portal se ha configurado para la autenticación en un registro de usuarios de LDAP y los grupos de usuarios que se almacenan en el servidor del portal. El perfil del usuario o del grupo de usuarios seleccionado se refleja en el marco inferior:

Permisos muestra una lista de las funciones de portal en el recuadro Autorizaciones. A la derecha se encuentran las operaciones posibles para la característica seleccionada. Si se ha marcado un recuadro de selección, significa que el usuario o grupo de usuarios seleccionado tiene permiso para ejecutar esa operación; el indicador situado a continuación del recuadro de selección significa que el permiso se ha añadido a un grupo de usuarios al que pertenece el usuario.

Aplicaciones muestra todas las aplicaciones que se están supervisando y que se pueden asignar al usuario o grupo de usuarios. Por ejemplo, se puede crear un perfil de un usuario o un grupo de usuarios para que sólo se vean las aplicaciones de OMEGAMON, otro para ver solamente middleware de Linux y Oracle y otro para ver todas las aplicaciones.

Vistas de Navigator muestra todas las vistas de Navigator que están en el servidor de portal y que están disponibles para asignar al usuario o grupo de usuarios. Se puede restringir el usuario o el grupo de usuarios para que sólo vea una determinada ramificación de una vista de Navigator en lugar de la jerarquía entera.

Miembro de, cuando el separador Usuarios está seleccionado, o **Miembros**, cuando está seleccionado el separador Grupos de usuarios, es una lista de los grupos a los que pertenece el usuario o una lista de los nombres de usuario pertenecientes al grupo.

La función Administración de usuarios le permite mantener los ID de usuario y los grupos de usuarios en el servidor de portal, y proporciona niveles diferentes de acceso a las características y las vistas del entorno supervisado para incluir cualquier combinación de roles de trabajo, como *operadores*, que responden a las alertas y las dirigen a la persona apropiada para que las maneje; y *administradores* que planifican, diseñan, personalizan y gestionan el entorno supervisado.

En algunas empresas gestionadas, una sola persona puede asumir todos estos roles. En empresas más grandes, normalmente los roles se dividen. Puede asignar roles por usuario individual o tipo de usuario o por ambas cosas.

Los ID de usuario de Tivoli Enterprise Portal también son necesarios para los usuarios que acceden a los paneles de control de supervisión en IBM Dashboard Application Services Hub. La forma en que se pueden gestionar los usuarios de paneles de control depende del tipo de autorización configurada en el servidor de

© Copyright IBM Corp. 2005, 2013

portal y si los usuarios de paneles de control también utilizarán el cliente de Tivoli Enterprise Portal. Hay dos tipos de autorización que se pueden configurar para controlar el acceso a recursos supervisados en IBM Dashboard Application Services Hub:

Políticas de autorización basadas en roles
Estas políticas se crean utilizando la Interfaz de línea de mandatos tivcmd para la política de autorización. Proporcionan autorización más granular que las asignaciones de aplicaciones de supervisión de Tivoli Enterprise Portal. Con las políticas de autorización basadas en roles, puede asignar un permiso de usuario para ver grupos de sistemas gestionados específicos o sistemas gestionados. Cuando las políticas de autorización basadas en roles están habilitadas en el servidor de portal, los usuarios de paneles de control necesitan un ID de usuario de Tivoli Enterprise Portal, pero no requieren ninguna asignación aplicaciones de supervisión ni de permisos de Tivoli Enterprise Portal a menos que sean también usuarios cliente de Tivoli Enterprise Portal. En este caso, las políticas de autorización basadas en roles controlan los recursos que pueden acceder en los paneles de control de supervisión y las asignaciones de aplicaciones de supervisión y permisos de Tivoli Enterprise Portal controlan lo que pueden acceder en el cliente de Tivoli Enterprise Portal.

Autorización de Tivoli Enterprise Portal
Este es el mecanismo de autorización predeterminado para los usuarios de paneles de control. Un usuario de paneles de control debe tener un ID de usuario de Tivoli Enterprise Portal y tener asignados los permisos y aplicaciones de supervisión para controlar su acceso a los recursos en los paneles de control de supervisión. Si un usuario de paneles de control es también un usuario cliente de Tivoli Enterprise Portal, se le asigna un solo conjunto de permisos que controlan qué recursos supervisados pueden acceder en ambas aplicaciones.

La configuración del servidor de portal y Dashboard Application Services Hub para compartir un registro de usuarios LDAP es la práctica recomendada para tener un conjunto de usuarios federado de paneles de control y usuarios cliente de Tivoli Enterprise Portal. En este caso, los usuarios de paneles de control inician la sesión en el concentrador de paneles de control con su nombre de usuario LDAP y debe correlacionar su nombre distinguido de LDAP con un ID de usuario de Tivoli Enterprise Portal con los permisos necesarios.

Los ID de usuario de Tivoli Enterprise Portal se crean automáticamente sin permisos si un usuario de paneles de control solicita datos de supervisión y no tiene un ID de usuario correlacionado con su nombre distinguido. Consulte “Notas sobre la administración de usuarios” en la página 178 para obtener más información.

Administrar usuarios

Su ID de usuario y los grupos de usuarios de los que es miembro se configuran con un conjunto de permisos que determina qué funciones de Tivoli Enterprise Portal está autorizado a ver y utilizar, una lista de aplicaciones supervisadas que está autorizado a ver y una lista de vistas de Navigator (y el nivel más alto dentro de una vista) a las que puede acceder.

Al pulsar **Administrar usuarios** se abre la ventana Administrar usuarios. Esta ventana tiene dos paneles: un panel superior con los separadores Usuarios y Grupos de usuarios, y un panel inferior con varios separadores. Esta disposición

permite al administrador gestionar perfiles de usuario por usuarios individuales, por grupos de usuarios, o por una combinación de ambos. Puede crear un perfil de usuario, copiarlo para cada usuario adicional y cambiar los valores del perfil según sea necesario (por ejemplo, para la función Acción, otorgar el permiso Ver a un usuario y el permiso Modificar a un usuario diferente). O puede crear un grupo de usuarios con un perfil determinado y añadir usuarios al grupo. A continuación, puede modificar los permisos una vez para un grupo y aplicarlo a todos los miembros de manera automática.

Cuando se modifican los permisos o la lista de aplicaciones supervisadas para un usuario o grupo de usuarios de Tivoli Enterprise Portal, el cambio de autorización no surte efecto hasta que el usuario finaliza la sesión del cliente de Tivoli Enterprise Portal y vuelve a iniciarla. Si los permisos de Tivoli Enterprise Portal se utilizan para autorizar los recursos supervisados para los usuarios de paneles de control, los cambios de autorización no surtirán efecto hasta que el usuario finalice la sesión de Dashboard Application Services Hub y vuelva a iniciarla.

Tareas relacionadas:

"Añadir ID de usuario" en la página 171
Cree un ID de usuario para todos los usuarios que deben poder iniciar la sesión en el Tivoli Enterprise Portal Server utilizando un cliente de portal o el mandato **tacmd tepsLogin**. También se necesita un ID de usuario para los usuarios de IBM Dashboard Application Services Hub que solicitan datos de supervisión. Puede utilizar el perfil de usuario predeterminado o puede copiar el perfil de un usuario existente.

"Visualización y edición de un ID de usuario" en la página 172
Después de añadir un usuario a la lista **Usuarios** en la ventana Administrar usuarios, puede examinar y editar los valores del perfil de usuario en cualquier momento.

Usuarios y grupos de usuarios

Los separadores **Usuarios** y **Grupos de usuarios** listan los ID de usuario y grupos de usuarios que están almacenados en el servidor de portal.

Después de seleccionar un usuario o un grupo de usuarios de una de las listas, puede pulsar en cualquiera de los separadores de la mitad inferior de la ventana para ver qué permisos se han otorgado y las asignaciones. Los grupos de usuarios permiten al administrador autorizar el mismo conjunto de permisos funcionales, aplicaciones y vistas de Navigator a varios usuarios a la vez. La gestión de la autorización de usuario la pueden realizar los grupos y también se puede realizar individualmente. Un usuario puede estar asociado a uno o más grupos de usuarios; la autorización otorgada por grupos se realiza por inclusión y no exclusión (se pueden utilizar grupos anidados). La autorización también puede ser por autorización global y por asociación con sistema gestionado y grupos de sistemas gestionados. Esta seguridad no depende de una autorización externa.

Permisos

Puede autorizar para el mismo conjunto de permisos funcionales a varios usuarios, un grupo de usuario o cada ID de usuario de una sola vez.

Las funciones siguientes se habilitan o inhabilitan individualmente para cada ID de usuario o grupo de usuarios.

Acción

Ver permite al usuario ver y ejecutar un mandato de actuación de entre los disponibles en la vista Actuación y el menú emergente del elemento de Navigator.

Modificar permite al usuario crear y guardar mandatos de Actuación. Cuando está habilitada, la opción **Editar acción** aparece en el menú emergente de Navigator.

Al emitir un mandato de actuación, el usuario debe tener autorización en el sistema pertinente para el mandato solicitado. Por ejemplo, para emitir un mandato TSO, el ID de usuario debe ser un ID de TSO válido y un ID de usuario válido en el servidor de portal. El ID de usuario se debe escribir exactamente con las mismas mayúsculas y minúsculas con las que se ha escrito al iniciar la sesión en el servidor de portal (con las mismas mayúsculas y minúsculas).

Gestión de agentes

Gestionar permite al usuario realizar el despliegue de agentes en toda la red gestionada. Esto incluye instalar un producto supervisado, mantener al día las revisiones de software y eliminar un agente de la red gestionada. Este permiso también necesita que se habilite Acción - Modificar.

Iniciar/Detener permite al usuario iniciar un agente de supervisión o detener su ejecución.

Vistas personalizadas de Navigator

Modificar permite al usuario crear nuevas vistas de Navigator, editarlas y suprimirlas. Si Modificar no está marcado, el usuario no verá **Editar vista de Navigator** en la barra de herramientas.

Suceso

Adjuntar permite al usuario adjuntar un archivo (por ejemplo, notas detalladas) al suceso de situación. Este permiso necesita que el usuario también tenga los permisos Reconocimiento y Ver. y Ver.

Cerrar le permite cerrar un suceso puro o un suceso que se abrió antes de detener manualmente una situación. Cuando está habilitado, **Cerrar suceso de situación** aparece en el menú emergente de la lista flotante de sucesos de situación, el elemento de Navigator de suceso y la vista de consola de sucesos de situación cuando el suceso seleccionado es un suceso puro o la situación se ha detenido.

Ver permite ver indicadores de suceso de situación en Navigator cuando las situaciones pasan a ser verdaderas.

Reconocer permite reconocer un suceso de situación. Cuando este permiso está habilitado, **Reconocer suceso** aparece en el menú emergente de la lista flotante de sucesos de situación, el elemento de Navigator de suceso y la vista de consola de sucesos de situación.

Característica

Habilitar aparece atenuado porque no se puede cambiar. El acceso a esta función está determinado por la licencia de su empresa para IBM Tivoli Monitoring.

Historial

Configurar permite al usuario abrir la ventana Configuración de la recopilación de historial, configurar los archivos históricos y la acumulación de datos e iniciar y detener la recopilación de datos para los

distintos grupos de atributos. Cuando este permiso está habilitado, **Configuración de historial** aparece en la barra de herramientas principal.

Iniciar aplicación

Iniciar permite al usuario invocar cualquiera de las definiciones de inicio disponibles para el elemento de Navigator, la vista de tabla, la vista de diagrama o la vista de consola de sucesos de situación. Cuando este permiso está habilitado, **Configuración de historial** aparece en la barra de herramientas principal.

Ver permite al usuario ver la composición de la definición de inicio seleccionada.

Modificar permite al usuario crear, editar y suprimir definiciones de inicio.

Grupo de sistemas gestionados

Ver permite al usuario acceder al editor de grupos de objetos para ver los grupos de sistemas gestionados. El usuario también necesita el permiso Modificar para que las herramientas del Editor de grupos de objetos estén disponibles.

Modificar permite al usuario acceder al editor de grupos de objetos para crear, editar y suprimir grupos de sistemas gestionados.

Política

Ver permite al usuario abrir la ventana Flujos de trabajo para ver las políticas y sus definiciones. Con el permiso Ver, el **Editor de flujos de trabajo** está disponible en la barra de herramientas principal y **Gestionar políticas** está disponible en el menú emergente de Navigator a nivel de agente .

Iniciar/detener permite al usuario iniciar y detener políticas. Con este permiso habilitado, **Iniciar política** y **Detener política** están disponibles cuando selecciona una política.

Modificar permite al usuario abrir el Editor de flujos de trabajo para crear y editar políticas. Con el permiso Modificar habilitado **Nueva política** está disponible después de que el usuario seleccione una política, así como también están disponibles las demás herramientas de edición: **Editar flujo de trabajo**, **Copiar política** y **Suprimir política**.

Consulta

Ver permite al usuario acceder al Editor de consultas a través del Editor de propiedades y seleccionar una consulta para la tabla o diagrama seleccionado. Con el permiso para Ver habilitado, el usuario puede asignar una consulta mediante el separador Consulta del editor de propiedades.

Modificar permite al usuario crear, editar y suprimir consultas en el Editor de consultas. Con el permiso para Modificar habilitado, el **Editor de consultas** está disponible en la barra de herramientas principal, igual que las herramientas de edición de consultas.

Situación

Ver permite al usuario ver las situaciones en el Editor de situaciones, incluida cualquier alteración temporal de las expresiones, y en la ventana Gestionar situaciones del sistema gestionado. Con el permiso Ver habilitado, **Editor de situaciones** está disponible en la barra de herramientas principal y en el menú emergente del elemento de Navigator (excepto en el nivel de plataforma).

☑ **Modificar** le permite crear situaciones nuevas y gestionarlas. Cuando se ha otorgado el permiso Modificar, las herramientas de edición de situaciones y las opciones de menú emergente están disponibles en el Editor de situaciones y también en el botón **Alterar temporalmente fórmula** del separador Distribución para las situaciones aptas.

☑ **Iniciar/Detener** le permite iniciar o detener una situación y habilitar o inhabilitar una alteración temporal de situación. Cuando este permiso está habilitado, **Iniciar situación** y **Detener situación** están disponibles en la lista flotante de sucesos de situación, vista de la consola de sucesos de situación, menú emergente del editor de situaciones y la ventana Gestionar situaciones en el sistema gestionado; y **Habilitar alteraciones temporales de situación** e **Inhabilitar alternaciones temporales de situación** están disponibles en el menú emergente del editor de situaciones.

Script de terminal

☑ **Ver** permite al usuario ejecutar o detener la ejecución de un script de emulador de terminal y ver scripts, pero no editarlos. Si se inhabilita Ver, el usuario sólo puede ejecutar o detener los scripts.

☑ **Modificar** permite al usuario crear o registrar nuevos scripts de emulador de terminal, editarlos y suprimirlos.

Administración de usuarios

Si está viendo su propio ID de usuario, verá que Ver y Modificar están inhabilitados; no puede cambiar sus permisos de Administración de usuarios.

☑ **Inicio de sesión permitido** habilita el inicio de sesión en el servidor de portal con este ID de usuario. El administrador puede deseleccionar el recuadro de selección para denegar el acceso al portal a un usuario. Esta opción funciona junto con el parámetro KFW_AUTHORIZATION_MAX_INVALID_LOGIN (el valor predeterminado es 0, se permite un número ilimitado de intentos) en el archivo de configuración del entorno del servidor de Tivoli Enterprise Portal, *kfwenv*. Cuando se ha establecido el valor y se han excedido el número máximo de intentos no válidos, el recuadro de selección se deselecciona automáticamente y el administrador debe seleccionar el recuadro de selección para restablecer el recuento de intentos de inicio de sesión. Consulte la publicación *IBM Tivoli Monitoring: Guía del administrador* para obtener detalles.☐ **Modificar** permite editar los ID de usuario y eliminarlos. Cuando se habilita este permiso, **Administrar usuarios** está disponible en la barra de herramientas principal y las herramientas están disponibles en la ventana Administrar usuarios.

☑ **Modalidad de autor elegible** permite al usuario habilitar o inhabilitar el permiso de Modalidad de autor en **Administración de espacios de trabajo** (ver autorización siguiente), pero no para ninguno de los demás ID de usuario.

☐ **Ver** permite al usuario abrir la ventana Administrar usuarios y ver su perfil de usuario.

☑ **Modalidad de administración elegible** permite al usuario habilitar o inhabilitar su permiso de modalidad de administración bajo la **Modalidad de administración de espacios de trabajo** (vea la autorización siguiente) pero no así los otros ID de usuario.

Administración de espacios de trabajo

☑ **Modalidad de autor de espacio de trabajo** permite al usuario crear y

editar espacios de trabajo, enlaces y scripts de emulador de terminal. Si la Modalidad de autor de espacio de trabajo está inhabilitada, el usuario no puede realizar ninguno de estos cambios, pero puede seguir supervisando y respondiendo a las alertas; las herramientas siguen siendo visibles, pero están inhabilitadas.

☐ **Modalidad de administración de espacios de trabajo** sólo está disponible para el ID de usuario SYSADMIN y para las nuevos ID creados a partir de SYSADMIN desde la ventana Crear otro usuario. Cuando la modalidad de administración está habilitada, los cambios realizados en los espacios de trabajo afectan a todos los usuarios que se conectan al mismo servidor de portal. Cuando está inhabilitada, los cambios realizados en los espacios de trabajo no se comparten con otros usuarios. Seleccione ☑ **No permitir modificaciones** en las Propiedades del espacio de trabajo cada vez que cree o edite un espacio de trabajo en la modalidad de administración. De lo contrario, si un usuario edita ese espacio de trabajo, ya no será propietario del espacio de trabajo y no podrá alterar temporalmente los cambios.

Autoridades de configuración de WebSphere MQ
IBM Tivoli OMEGAMON XE for Messaging: Las instalaciones de WebSphere MQ Configuration verán esta carpeta.

☑ **Ver** permite que el usuario vea la configuración de WebSphere MQ de la organización en la vista Configuración de Navigator, pero no cambiarla.

☑ **Modificar** permite que el usuario cambie la configuración de WebSphere MQ de la organización o planifique actualizaciones en la vista Configuración.

Autorizaciones del subsistema de almacenamiento
Las instalaciones de IBM Tivoli OMEGAMON XE for Storage verán esta carpeta. Seleccione ☑ **Ver** para permitir al usuario ver datos, pero no cambiarlos. Seleccione ☑ **Modificar** para permitir al usuario cambiar datos.

Configuración de la recopilación de datos permite al usuario ver o modificar el intervalo de control de la recopilación para el espacio de trabajo Estatus de DFSMSrmm y el espacio de trabajo Resumen del sistema de atributos del conjunto de datos.

Intervalo de recopilación de grupos de conjuntos de datos permite al usuario ver o modificar el intervalo de control para el espacio de trabajo Resumen del grupo del conjunto de datos.

Definir/actualizar grupos de conjuntos de datos permite al usuario ver o modificar las definiciones de grupo para el espacio de trabajo Resumen del grupo del conjunto de datos.

Aplicaciones

El ID de usuario se establece para que pueda ver algunos o todos los tipos de aplicación que se supervisan. Por ejemplo, es posible que un usuario sólo pueda ver las aplicaciones de sistema principal mientras que otro sólo pueda ver middleware y otro pueda ver todas las aplicaciones.

Aplicaciones permitidas
Muestra las aplicaciones a las que el usuario puede acceder desde Tivoli Enterprise Portal.

Aplicaciones disponibles

Muestra las aplicaciones que están disponibles para asignarlas al usuario seleccionado. Si **<Todas las aplicaciones>** se encuentra en la lista de **Aplicaciones permitidas**, no es posible añadir otras entradas. Debe trasladar la entrada a **Aplicaciones disponibles** para poder seleccionar un subconjunto de aplicaciones para asignar.

Seleccione las aplicaciones que desee añadir o seleccione **<Todas las aplicaciones>** y ◂ muévalas a la lista **Aplicaciones permitidas**. Después de seleccionar la primera aplicación, puede pulsar con el ratón mientras mantiene pulsada la tecla Control para seleccionar otras aplicaciones o pulsar con el ratón mientras mantiene pulsada la tecla Mayús para seleccionar todas las aplicaciones desde la primera hasta la última en la que pulse.

vistas de Navigator

Cuando se crea una vista de Navigator, sólo el autor puede ver la vista, pero ésta está disponible para que los administradores la asignen a los usuarios. Una vista de Navigator asignada permite que el usuario puede abrirla. Para cada vista asignada, se puede restringir al usuario que sólo vea una determinada ramificación en lugar de la jerarquía entera.

Vistas asignadas

Muestra las vistas de Navigator que el usuario puede ver y acceder. La primera vista de Navigator contenida en esta lista es la vista predeterminada del usuario; se muestra cada vez que el usuario inicia la sesión. Pueden seleccionarse todas las vistas a las que no se desee que tenga acceso el usuario y pulsar la flecha a la derecha ➡ para moverlas a la lista **Vistas disponibles**. Seleccione las entradas apropiadas y pulse la ◂ flecha izquierda para moverlas a las **Vistas asignadas** Puede mover una vista de Navigator al principio de la lista para convertirla en la vista predeterminada pulsando en la flecha hacia arriba ▲ .

Vistas disponibles

Muestra las vistas de Navigator no asignadas al usuario y que están disponibles para su asignación. Seleccione las vistas de Navigator que desee añadir y muévalas a la lista **Vistas asignadas** utilizando la flecha a la izquierda ◂ . Después de seleccionar la primera vista, puede pulsar con el ratón mientras mantiene pulsada la tecla Control para seleccionar otras vistas o pulsar con el ratón mientras mantiene pulsada la tecla Mayúsculas para seleccionar todas las vistas comprendidas entre la primera selección y la actual.

Raíz asignada

Muestra la vista de Navigator elegida en Vistas asignadas, con la raíz de Navigator asignada del usuario resaltada. La raíz es el nivel que se encuentra más arriba de esta vista de Navigator a la que el usuario puede acceder. El usuario puede acceder a este elemento y a todos los elementos bajo él, pero a ningún elemento paralelo o que esté por encima de él en Navigator.

Por ejemplo, puede asignar Sistemas UNIX como la raíz asignada. El usuario verá los espacios de trabajo de Sistemas UNIX y aquellos situados por debajo pero no podrá ver los espacios de trabajo de Empresa ni verá nada bajo Sistemas Windows.

Miembro de y Miembros

Cuando selecciona un usuario o grupo de usuarios en la lista, el último separador en el conjunto inferior de separadores tiene la indicación **Miembro de** o **Miembros** (en consonancia con la selección de un usuario o grupo de usuarios). La asignación de usuarios a grupos se puede realizar en cualquier separador.

Gestión de los ID de usuario

La gestión de ID de usuario empieza con la planificación de las autorizaciones a otorgar a los usuarios y la determinación de si pertenecerán a grupos de usuarios.

La ventana Administrar usuarios proporciona las herramientas para crear y mantener los ID de usuario y para ajustar permisos. Aquí también es donde los ID de usuario se correlacionan con sus identificadores exclusivos en el registro de usuarios de LDAP si se ha configurado la autenticación de usuarios mediante el servidor de portal.

Añadir ID de usuario

Cree un ID de usuario para todos los usuarios que deben poder iniciar la sesión en el Tivoli Enterprise Portal Server utilizando un cliente de portal o el mandato **tacmd tepsLogin**. También se necesita un ID de usuario para los usuarios de IBM Dashboard Application Services Hub que solicitan datos de supervisión. Puede utilizar el perfil de usuario predeterminado o puede copiar el perfil de un usuario existente.

Antes de empezar

Para utilizar esta función, el ID de usuario debe tener permiso de Modificar para la Administración de usuarios.

Procedimiento

1. Pulse **Administrar usuarios**.
2. Cree un ID de usuario nuevo o cree uno a partir de otro:
   - Para crear un nuevo ID de usuario con el perfil de usuario predeterminado, pulse **Crear nuevo usuario**.
   - Para crear un nuevo ID de usuario a partir de uno existente, seleccione el perfil que desee utilizar en la lista **Usuarios** y pulse **Crear otro usuario**.
3. En la ventana Crear nuevo usuario, entre la información de usuario:
   - **ID de usuario**: Nombre de inicio de sesión. El nombre debe utilizar caracteres ASCII, puede contener hasta 10 caracteres y puede no contener espacios. El nombre tiene un límite de ocho caracteres si la autentificación de usuario se realiza en el servidor de supervisión concentrador y utiliza RACF (Resource Access Control Facility) para z/OS.
   - **Nombre de usuario**: Nombre del usuario o clasificación del trabajo o ambos. Este nombre puede incluir espacios y tener un máximo de 32 caracteres. El nombre de usuario se muestra en la lista **Usuarios**.
   - **Nombre distinguido:** El identificador exclusivo en el registro de usuarios de Lightweight Directory Access Protocol (LDAP) correspondiente al nombre especificado en el campo **ID de usuario**. Pulse **Buscar** para localizar e insertar el nombre distinguido, como por ejemplo UID=FRIDA,O=DEFAULTWIMITMBASEDREALM
   - **Descripción del usuario:** Descripción opcional correspondiente al usuario. El texto puede incluir espacios y signos de puntuación.

4. Pulse **Aceptar** para cerrar la ventana y ver el nuevo ID de usuario ordenado alfabéticamente en la lista **Usuarios**.
5. Para cambiar los **Permisos**, seleccione una función en el árbol **Autorizaciones** y seleccione o deseleccione la opción correspondiente a cada función cuyos permisos deba cambiar.
6. Para asignar privilegios de acceso a aplicaciones (tipos de sistemas gestionados), pulse el separador **Aplicaciones**, a continuación, seleccione **<Todas las aplicaciones>** o las aplicaciones individuales que deba ver el usuario y pulse la para moverlas a la lista **Aplicaciones permitidas**. Después de seleccionar la primera aplicación, puede pulsar con el ratón mientras mantiene pulsada la tecla Control para seleccionar otras aplicaciones o pulsar con el ratón mientras mantiene pulsada la tecla Mayús para seleccionar todas las aplicaciones desde la primera hasta la última en la que pulse.
7. Para asignar las vistas de Navigator, pulse el separador **Vistas de Navigator**:
   a. Seleccione una vista de Navigator (o más listas pulsando Ctrl + clic y Mayúsculas + clic) en **Vistas disponibles** y pulse para moverla a las **Vistas asignadas**.
   b. Utilice para colocar la vista que desea que sea el valor predeterminado en la parte superior de la lista. Utilice y para organizar las vistas de Navigator en el orden en que deben aparecer en la vista de la lista de vistas de la barra de herramientas de Navigator .
   c. Para la vista de Navigator seleccionada, cambie **Raíz asignada** como corresponda.
8. Cuando termine de crear el perfil de usuario, pulse **Aplicar** para guardar los cambios realizados y mantener abierta la ventana Administrar usuarios, o pulse **Aceptar** para guardar los cambios y cerrar la ventana.

Qué hacer a continuación

La ventana de inicio de sesión de cliente de Tivoli Enterprise Portal tiene un campo para entrar un ID de usuario y contraseña. Si desea que el ID de usuario y contraseña se autentiquen, configure el servidor de supervisión o el servidor de portal para autenticar los usuarios. Consulte Capítulo 5, “Habilitación de la autenticación de usuarios”, en la página 83 para ver detalles.

Referencia relacionada:

“Administrar usuarios” en la página 164
Su ID de usuario y los grupos de usuarios de los que es miembro se configuran con un conjunto de permisos que determina qué funciones de Tivoli Enterprise Portal está autorizado a ver y utilizar, una lista de aplicaciones supervisadas que está autorizado a ver y una lista de vistas de Navigator (y el nivel más alto dentro de una vista) a las que puede acceder.

Visualización y edición de un ID de usuario

Después de añadir un usuario a la lista **Usuarios** en la ventana Administrar usuarios, puede examinar y editar los valores del perfil de usuario en cualquier momento.

Antes de empezar

Para utilizar esta función, el ID de usuario debe tener permiso de Modificar para la Administración de usuarios.

Acerca de esta tarea

Utilice los pasos siguientes para editar un ID de usuario:

Procedimiento

1. Pulse **Administrar usuarios**.
2. Realice una de las acciones siguientes en la lista **Usuarios**:
   - Pulse dentro del campo **Nombre** o **Descripción** para editar cualquiera de los dos.
   - Efectúe una doble pulsación en cualquier lugar de una fila para abrir la ventana Modificar usuario para editar cualquiera de los campos.
   - Pulse con el botón derecho del ratón en el perfil de usuario que desea editar y pulse **Modificar usuario**.
3. Edite el **Nombre de usuario**, el **Nombre distinguido** o la **Descripción del usuario** y luego pulse en **Aceptar**. El nombre distinguido es necesario si la autenticación de usuarios se realiza por medio del servidor del portal a un registro de usuarios de LDAP. El único cambio que puede realizar en el ID de usuario de una sola palabra es el de las mayúsculas y minúsculas. Para editar el ID de usuario de una sola palabra, debe suprimir el perfil de usuario y crear uno de nuevo.
   - Si no ha añadido el nombre distinguido, pulse **Buscar** para localizar el nombre que coincide con el ID de usuario.
     Si el entorno supervisado se ha configurado anteriormente para autenticación a través del servidor de Tivoli Enterprise Monitoring y luego se ha reconfigurado para autenticar a través del servidor de Tivoli Enterprise Portal, es posible que vea dos entradas correspondientes al nombre. Seleccione o=defaultWIMFileBasedRealm y no O=DEFAULTWIMITMBASEDREALM.
4. Para cambiar los Permisos, seleccione una función en el árbol **Autorizaciones** y seleccione o deseleccione la opción correspondiente a cada función cuyos permisos deba cambiar. Puede cambiar sus propios permisos de usuario, excepto Crear y Modificar para Administración de usuarios
5. Para asignar privilegios de acceso para aplicaciones (tipos de sistemas gestionados), pulse el separador Aplicaciones, seleccione las aplicaciones que desee eliminar de la lista **Aplicaciones permitidas** y muévalas a la lista **Aplicaciones disponibles**; seleccione las aplicaciones que desea añadir de la lista **Aplicaciones disponibles** (o seleccione **<Todas las aplicaciones>**) y muévalas a la lista **Aplicaciones permitidas**.

   Después de seleccionar la primera aplicación, puede pulsar con el ratón mientras mantiene pulsada la tecla Control para seleccionar otras aplicaciones o pulsar con el ratón mientras mantiene pulsada la tecla Mayús para seleccionar todas las aplicaciones desde la primera hasta la última en la que pulse.
6. Para cambiar cualquier asignación de vistas de Navigator, pulse el separador Vistas de Navigator, a continuación, añada o elimine vistas de Navigator de la lista **Vistas asignadas**, y utilice para colocar al principio de la lista la vista que desee que sea la vista predeterminada. Para cada vista de Navigator, cambie la **Raíz asignada** como sea necesario.
7. Cuando haya terminado de editar el perfil de usuario, guarde los cambios con **Aplicar** si desea mantener abierta la ventana Administrar usuarios o **Aceptar** si desea cerrarla.

Resultados

Los cambios realizados en los permisos serán efectivos la próxima vez que el usuario inicie la sesión.

Referencia relacionada:

"Administrar usuarios" en la página 164
Su ID de usuario y los grupos de usuarios de los que es miembro se configuran con un conjunto de permisos que determina qué funciones de Tivoli Enterprise Portal está autorizado a ver y utilizar, una lista de aplicaciones supervisadas que está autorizado a ver y una lista de vistas de Navigator (y el nivel más alto dentro de una vista) a las que puede acceder.

Eliminar un ID de usuario

Puede eliminar un ID de usuario, según sea necesario.

Acerca de esta tarea

Para utilizar esta función, el ID de usuario debe tener permiso de Modificar para la Administración de usuarios.

Utilice los pasos siguientes para eliminar un ID de usuario:

Procedimiento

1. Pulse **Administrar usuarios**.
2. Seleccione el ID de usuario que desee suprimir. Puede seleccionar más de un ID de usuario pulsando el ratón mientras mantiene pulsada la tecla Control, o puede pulsar el ratón mientras mantiene pulsada la tecla Mayúsculas para seleccionar todos los ID de usuario comprendidos entre la primera selección y la actual.
3. Pulse **Eliminar usuarios** para suprimir el ID de usuario y el perfil seleccionados de la lista.
4. Cuando un mensaje le solicite que confirme la eliminación del ID de usuario, pulse **Sí**. El usuario se elimina permanentemente de la lista de ID de usuario. Si el usuario tiene actualmente una sesión iniciada, esto no afectará a su sesión de trabajo, pero no podrá iniciar la sesión de nuevo.

   Nota: No puede eliminar el ID de usuario (con el que ha iniciado la sesión) o el ID de <Usuario predeterminado>.

Usuario predeterminado

El primer ID de usuario de la lista **Usuarios** es el <Usuario predeterminado>.

Para utilizar esta función, el ID de usuario debe tener permiso de Modificar para la Administración de usuarios.

El ID se utiliza como plantilla de ID para los usuarios creados con **Crear nuevo usuario**. Edite este ID de usuario si desea cambiar cualquiera de los valores predeterminados. Los valores predeterminados iniciales permiten todas las funciones listadas bajo Autorizaciones de Tivoli Enterprise Portal, excepto Crear y Modificar de Administración de usuarios. Los cambios que realice en el ID de <Usuario predeterminado> se aplican a los usuarios creados a partir de ese momento; no afectan a los valores de ID de usuario existentes.

Gestión de grupos de usuarios

Los grupos de usuarios permiten al administrador autorizar el mismo conjunto de permisos funcionales, aplicaciones y vistas de Navigator a varios usuarios a la vez. La gestión de la autorización de usuario la pueden realizar los grupos y también se puede realizar individualmente.

Un usuario se puede asociar con uno o varios grupos de usuarios. Si se otorga un permiso a un usuario directamente mediante su ID de usuario, el usuario mantiene ese permiso aunque un grupo de usuarios al que pertenece el usuario no otorgue ese permiso. Lo contrario también es cierto, por lo que si no se otorga un permiso a un ID de usuario individual, pero sí se otorga al ID de grupo, el usuario tendrá el permiso a través de su pertenencia al grupo de usuarios. De esta forma, el conjunto de permisos del usuario se obtiene a partir de los permisos dados al ID de usuario individual y a todos los grupos de usuarios a los que pertenezca.

La autorización también puede ser por autorización global y por asociación con sistema gestionado y grupos de sistemas gestionados. Esta seguridad no depende de una autorización externa.

Cuando el separador superior activo sea **Usuarios**, el último separador del conjunto de separadores de la parte inferior indicará **Miembro de**. Cuando el separador superior activo sea **Grupos de usuarios**, también tendrá un separador **Miembros**. La asignación de usuarios a grupos se puede realizar en uno de los dos separadores inferiores.

Pulse en el grupo en la vista de detalles superior, luego vaya al separador **Miembros** para ver la lista de usuarios que pertenecen a ese grupo. Lo mismo es válido para ver los grupos a los que pertenece un usuario.

Visualización de los miembros de un grupo de usuarios

Puede ver los grupos a los que pertenece un ID de usuario y la lista de los ID de usuario que pertenecen a un grupo de usuarios.

Acerca de esta tarea

Para utilizar esta función, el ID de usuario debe tener permiso de Modificar para la Administración de usuarios.

Procedimiento

1. Pulse **Administrar usuarios**. La ventana Administrar usuarios está dividida en dos mitades, con los separadores **Usuarios** y **Grupos de usuarios** en la parte superior, y **Permisos**, **Aplicaciones**, **Vistas de Navigator** y **Miembro de** en la parte inferior.
2. Para ver los grupos a los que pertenece un usuario, seleccione un nombre en la lista **Usuarios** y, a continuación, pulse el separado **Miembro de**. Los grupos a los que pertenece el usuario aparecen en la lista **Miembros de asignados**.
3. Para ver los ID de usuario asignados a un grupo, seleccione un nombre en la lista **Grupos de usuarios** y, a continuación, pulse el separador **Miembros**. Los usuarios pertenecientes al grupo aparecen en la lista **Miembros asignados**.

Adición de un grupo de usuarios

Puede crear un nuevo grupo de usuarios o puede copiar un grupo que tenga permisos y asignaciones de usuarios similares a lo que desea, y luego modificar la copia.

Antes de empezar

Para utilizar esta función, el ID de usuario debe tener permiso de Modificar para la Administración de usuarios.

Acerca de esta tarea

Realice estos pasos para añadir un grupo de usuarios:

Procedimiento

1. Pulse **Administrar usuarios** para abrir la ventana Administrar usuarios.
2. Pulse el separador **Grupos de usuarios**.
3. Realice una de las acciones siguientes:
   - Para crear un nuevo grupo de usuarios, pulse en **Crear nuevo grupo**.
   - Para copiar un grupo de usuarios existente, seleccione el nombre del grupo en la lista y pulse **Crear otro grupo**.
4. En la ventana Crear nuevo grupo o Crear otro grupo, entre la siguiente información de usuario:
   a. **ID de grupo:** El identificador de grupo. Este nombre puede tener un máximo de 10 caracteres y no puede contener espacios en blanco. El nombre está limitado a ocho caracteres si el servidor de supervisión concentrador utiliza seguridad mediante RACF (Resource Access Control Facility) para z/OS.
   b. **Nombre de grupo:** El nombre o clasificación de trabajo del grupo de usuarios. Este nombre puede incluir espacios en blanco.
   c. **Descripción del grupo:** Texto para describir el grupo de usuarios, tal como sus funciones. La descripción puede incluir espacios en blanco y signos de puntuación.
5. Pulse **Aceptar** para cerrar la ventana y ver el nuevo grupo de usuarios ordenado alfabéticamente en la lista Grupo de usuarios.
6. Añada miembros al grupo en el separador **Miembros** seleccionando uno o varios ID de usuario de la lista **Miembros disponibles** y pulsando para trasladar miembros a la lista **Miembros asignados**.
7. Para cambiar los Permisos para el grupo, seleccione una función del árbol **Autorizaciones** y seleccione o borre cada recuadro de selección de opción para todas las funciones.
8. Para asignar privilegios de acceso a aplicaciones (tipos de sistemas gestionados), pulse el separador Aplicaciones, a continuación, seleccione **<Todas las aplicaciones>** o las aplicaciones individuales que deba ver el usuario y pulse la para moverlas a la lista **Aplicaciones permitidas**. Después de seleccionar la primera aplicación, puede pulsar con el ratón mientras mantiene pulsada la tecla Control para seleccionar otras aplicaciones o pulsar con el ratón mientras mantiene pulsada la tecla Mayús para seleccionar todas las aplicaciones desde la primera hasta la última en la que pulse.
9. Para asignar vistas de Navigator al grupo, pulse el separador Vistas de Navigator, y a continuación, añada o elimine vistas de Navigator en la lista

Vistas asignadas y utilice para poner la vista predeterminada en la parte superior de la lista. Para cada vista de Navigator, cambie la **Raíz asignada** como sea necesario.

10. Cuando termine de crear el grupo de usuarios, pulse **Aplicar** para guardar los cambios y mantener abierta la ventana Administrar usuarios, o pulse **Aceptar** para guardar los cambios y cerrar la ventana.

Revisión y edición de un grupo de usuarios

Después de añadir un grupo de usuarios a la lista **Grupos de usuarios** en la ventana Administrar usuarios, puede examinar y editar los valores de perfil en cualquier momento.

Acerca de esta tarea

Para utilizar esta función, el ID de usuario debe tener permiso de Modificar para la Administración de usuarios.

Utilice los pasos siguientes para editar un ID de usuario:

Procedimiento

1. Pulse **Administrar usuarios** para abrir la ventana Administrar usuarios.
2. Pulse el separador **Grupos de usuarios**.
3. Pulse con el botón derecho del ratón en el grupo de usuarios que debe editar y pulse .
4. Edite el **Nombre de grupo** y la **Descripción de grupo**, y luego pulse **Aceptar**. No puede cambiar el ID de grupo, que está formado por una sola palabra. En lugar de ello, debe crear un segundo grupo de usuarios a partir del primero, asignarle un nombre nuevo, y después suprimir el primer grupo.
5. Para cambiar los Permisos, seleccione una función en el árbol **Autorizaciones** y seleccione o deseleccione la opción correspondiente a cada función cuyos permisos deba cambiar.
6. Para cambiar los privilegios de acceso de grupo a aplicaciones (tipos de sistema gestionado), pulse el separador Aplicaciones, seleccione las aplicaciones que desea eliminar en la lista **Aplicaciones permitidas** y pulse ; seleccione las aplicaciones que desea añadir en la lista **Aplicaciones disponibles** (o seleccione **<Todas las aplicaciones>**) y pulse . Después de seleccionar la primera aplicación, puede pulsar con el ratón mientras mantiene pulsada la tecla Control para seleccionar otras aplicaciones o pulsar con el ratón mientras mantiene pulsada la tecla Mayús para seleccionar todas las aplicaciones desde la primera hasta la última en la que pulse.
7. Para cambiar cualquier asignación de vistas de Navigator para un grupo, pulse el separador Vistas de Navigator, a continuación, añada o elimine vistas de Navigator de la lista **Vistas asignadas** y utilice para colocar al principio de la lista la vista que desee que sea la vista predeterminada. Para cada vista de Navigator, cambie la **Raíz asignada** como sea necesario.
8. Cuando haya terminado de editar el grupo de usuarios, guarde los cambios con **Aplicar** para mantener abierta la ventana Administrar usuarios o **Aceptar** para cerrarla. Los cambios de grupo de usuarios entran en vigor la siguiente vez que cada miembro de grupo inicia la sesión.

   Nota: Puede cambiar los permisos, excepto Crear y Modificar de administración de usuarios, de cualquier grupo del cual sea miembro.

Eliminación de un grupo de usuarios

Puede eliminar un grupo de usuarios.

Acerca de esta tarea

Para utilizar esta función, el ID de usuario debe tener permiso de Modificar para la Administración de usuarios.

Utilice los pasos siguientes para eliminar un ID de usuario:

Procedimiento

1. Pulse **Administrar usuarios** para abrir la ventana Administrar usuarios.
2. Pulse el separador **Grupos de usuarios**.
3. Seleccione en la lista el grupo de usuarios a suprimir y pulse **Eliminar grupo seleccionado**. Puede seleccionar ID de usuario adicionales pulsando con el ratón mientras mantiene pulsada la tecla Control o pulsando con el ratón mientras mantiene pulsada la tecla Mayús para seleccionar todos los grupos de usuarios entre la primera y la última selección.
4. Cuando un mensaje le solicite que confirme la eliminación del grupo de usuarios, pulse **Sí**. El grupo se elimina permanentemente de la lista de grupos de usuarios. Los miembros de este grupo de usuarios que reciben permisos del grupo no se verán afectados hasta la próxima vez que inicien la sesión en el servidor de portal.

Notas sobre la administración de usuarios

Lea estas notas para comprender la contribución del ID de usuario a las funciones y modalidades de Tivoli Enterprise Portal.

Modalidad de administración de espacios de trabajo

Cualquier cambio que realice en espacios de trabajo, enlaces y scripts de sesión de host de terminal en el Tivoli Enterprise Portal solamente son visibles para su ID de usuario. La excepción se produce mientras está habilitada la modalidad de administración de espacios de trabajo.

La modalidad de administración de espacios de trabajo le permite personalizar y añadir espacios de trabajo, enlaces y scripts de emulador de terminal que son utilizados de forma compartida por todos los usuarios que están conectados al mismo Tivoli Enterprise Portal. Consulte el apartado Inicio de la modalidad de administración de espacio de trabajo.

ID de inicio de sesión SYSADMIN

Tivoli Enterprise Portal necesita su ID de inicio de sesión siempre que inicia una sesión de trabajo. Cada ID debe haberse registrado antes en el servidor de portal. Puede iniciar la sesión en el servidor de portal con **SYSADMIN** y registrar otros ID de usuario mediante la ventana Administrar usuarios. El ID de usuario inicial, **SYSADMIN**, tiene acceso completo y autorización total de administrador. El administrador del sistema registra usuarios adicionales y define sus privilegios de acceso y autorización.

ID de usuario y grupos

Cada ID de usuario se almacena en el servidor de Tivoli Enterprise Portal y contiene:

- El nombre de usuario
- La descripción de trabajo
- Permisos para ver o modificar funciones de Tivoli Enterprise Portal
- Vistas de Navigator asignadas y qué elemento de Navigator de cada vista aparece como raíz (de forma predeterminada, el elemento raíz es el primer elemento)
- El acceso a aplicaciones de supervisión específicas
- Los grupos de usuarios a los que pertenece el usuario e indicadores para denotar cuando un grupo de usuarios ha otorgado un permiso al usuario

Cada grupo de usuarios también se almacena en el servidor de portal y tiene el mismo contenido que los ID de usuario individuales. Pero, en lugar de una lista de grupos de usuarios, tiene una lista de los ID de usuario asignados al grupo.

Usuario predeterminado

El primer ID de usuario de la lista es **<Usuario predeterminado>** y se utiliza como ID modelo para los usuarios creados con la opción Crear nuevo usuario. Edite este ID de usuario si desea cambiar cualquiera de los valores predeterminados. Los valores predeterminados iniciales habilitan todas las funciones listadas en Autorizaciones de Tivoli Enterprise Portal, excepto el permiso Modificar para la **Administración de usuarios**. Cualquier cambio que realice en el ID del <Usuario predeterminado> se aplica a los usuarios creados a partir de este momento; no afecta a los valores de ningún ID de usuario existente.

Otorgamiento de acceso a un usuario

Establezca los privilegios de autorización para cada usuario cuando cree los ID de usuario. Para proporcionar a los usuarios acceso a las áreas operativas y las opciones de personalización es necesaria una planificación. Tenga en cuenta las responsabilidades de trabajo de cada usuario y los requisitos de seguridad de empresa al especificar los privilegios de autorización.

Importante: Cualquier persona con permiso para crear consultas personalizadas obtiene acceso a todos los nombres de las fuentes de datos ODBC (DSN) creadas en el Tivoli Enterprise Portal Server. Añada los ID de usuario de base de datos, que se deberán utilizar en el DSN, al software de base de datos, asegurándose de restringir el acceso de usuario sólo a las tablas, columnas, etc., permitidas por las políticas de seguridad de la organización.

Creación automática de ID de usuario de Tivoli Enterprise Portal

La primera vez que un nuevo usuario accede a un panel de control de supervisión en IBM Dashboard Application Services Hub, un ID de usuario de Tivoli Enterprise Portal se crea automáticamente y se correlaciona con el nombre distinguido LDAP del usuario si aún no existe un ID de usuario de Tivoli Enterprise Portal para el usuario. El ID de usuario de Tivoli Enterprise Portal es una serie generada aleatoriamente. Si necesita asignar permisos de Tivoli Enterprise Portal y aplicaciones de supervisión a un usuario de paneles de control

y su ID de usuario de Tivoli Enterprise Portal se ha creado automáticamente, puede asignar los permisos para el ID de usuario generado aleatoriamente o realizar estos pasos:

1. Suprima el ID de usuario de Tivoli Enterprise Portal que se ha creado automáticamente.
2. Crear un nuevo ID de usuario de Tivoli Enterprise Portal, correlaciónelo con el nombre distinguido de LDAP para el usuario y, a continuación, asígnele permisos y aplicaciones de supervisión.

Validación del acceso de los usuarios

El Tivoli Enterprise Portal Server verifica los ID de usuario siempre que los usuarios inician sesión. Si una descripción del trabajo cambia y el usuario necesita un acceso diferente al servidor del portal, deberá revisar y tal vez cambiar los permisos del usuario.

El ID de usuario para iniciar la sesión en el servidor del portal puede incluir una contraseña. No establezca contraseñas en el portal. En lugar de ello, debe definir un ID de usuario que corresponda a la contraseña para las cuentas de usuario del dominio de red o para el sistema operativo donde reside el Tivoli Enterprise Monitoring Server:

- Cuentas de usuario en el sistema Windows
- Archivo de contraseñas en el sistema UNIX
- Sistema de seguridad de host RACF o ACF/2 en el sistema z/OS

Asimismo, se debe configurar el servidor de supervisión para Validar usuario. Cuando los usuarios inician una sesión en el servidor de portal, el servidor de supervisión concentrador solicita al dominio o al sistema operativo que valide el ID de usuario y la contraseña.

Si el servidor de supervisión se ha instalado en un sistema distribuido, puede comprobar si se ha configurado para Validar usuario:

1. Inicie el programa Manage Tivoli Enterprise Monitoring Services:

   Windows Inicio → Programas → IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services.

   UNIX Vaya al directorio *install_dir*/bin y ejecute el siguiente mandato: `./itmcmd manage [-h install_dir]` donde *install_dir* es el directorio de instalación (el valor predeterminado es opt/IBM/ITM).
2. Pulse con el botón derecho del ratón en la fila del Tivoli Enterprise Monitoring Server correspondiente a TEMS1 (concentrador) y seleccione **Reconfigurar**.
3. En la ventana Configuración del servidor de Tivoli Enterprise Monitoring, observe el valor del recuadro de selección ☑ **Seguridad: Validar usuario**.

   Si esta opción está seleccionada, se necesitará una contraseña siempre que un usuario inicie sesión en el servidor del portal; si, por el contrario, no está seleccionada, necesitará el nombre de usuario para iniciar sesión, aunque no la contraseña.

Nota: Tenga en cuenta que las contraseñas deben cumplir los requisitos de seguridad de su empresa. Si entre ellos se incluyen cambios de contraseña periódicos, es posible que obtenga el mensaje **La contraseña de inicio de sesión ha caducado** cuando intente iniciar la sesión en el servidor de portal. Si esto sucede,

deberá cambiar la contraseña del sistema para poder iniciar la sesión. Por ejemplo, en Windows esto significa modificar la contraseña utilizando Cuentas de usuario de las Herramientas administrativas.

Inicio en el portal desde otras aplicaciones

Además de cualquier requisito de seguridad para iniciar en Tivoli Enterprise Portal (por ejemplo, los requisitos de inicio de sesión único), el ID de usuario de Tivoli Enterprise Portal que recibe el control después de un inicio desde una aplicación externa, debe tener una autorización previa para acceder al sistema gestionado y a los espacios de trabajo de destino. El ID de usuario también debe tener autorización para emitir los mandatos de actuación necesarios.

ID de usuario para mandatos de actuación

Cuando Tivoli Enterprise Portal envía un mandato de actuación a un sistema gestionado, puede que se compruebe o no la autorización del ID de usuario para realizar la acción. En el caso más simple, el mandato se envía al sistema gestionado y se ejecuta utilizando el UD de usuario bajo el que se ejecuta el agente. El ID de usuario de Tivoli Enterprise Portal se envía junto con el mandato de actuación en los contextos siguientes:

- Bajo demanda: ID de usuario conectado actualmente
- Acción de situación: ID de usuario de la última persona que actualizó la situación
- Acción de flujo de trabajo: ID de usuario de la última persona que actualizó la política

No obstante, el sistema gestionado ignora el ID a menos que un prefijo de mandato indique lo contrario. Esto son gestores de mandatos implementados en los productos IBM Tivoli Monitoring para controlar si el ID de usuario de Tivoli Enterprise Portal se debe validar antes de pasar el mandato al agente para su ejecución.

Prefijo de mandato
Cuando existe un prefijo de mandato en el mandato de actuación, el agente pasa el mandato al gestor de aplicaciones en lugar de ejecutar el mandato. La sintaxis del prefijo y del mandato de actuación es **códigoproducto:IDusuarioCNP:mandato** y el agente lo direcciona a la aplicación para ejecutarlo. La aplicación es libre de ejecutar el mandato con el ID de usuario que sea apropiado. En el caso de OMEGAMON XE para WebSphere MQ en z/OS, se utiliza el ID de usuario de Tivoli Enterprise Portal.

Si falta el prefijo especial, el agente ejecuta el mandato con el ID de usuario bajo el que se ejecuta el agente.

La mayoría de los productos no utilizan ningún prefijo de mandato. IBM Tivoli Monitoring para WebSphere MQ sí lo utiliza y, de hecho, añade delante de todos los mandatos de Actuación bajo demanda un prefijo **MQ:CNPuserID:** oculto, aunque no pueda verse.

Mandato setuid de UNIX
Además del prefijo de mandato y la salida de seguridad, UNIX ofrece otra opción: un mandato setuid, que hace que el proceso cambie dinámicamente su ID de usuario. De esta manera, el agente se puede cambiar para establecer el ID en el valor pasado como parámetro, emitir el mandato y luego cambiar de nuevo el ID de usuario una vez emitido el mandato.

Resolución de mensajes de error de inicio de sesión

Se visualizan solicitudes de inicio de sesión y mensajes de progreso en la barra de estado de la ventana Inicio de sesión. Si un usuario no puede iniciar la sesión, se visualiza un mensaje.

Si un usuario no puede iniciar la sesión, se muestra uno de los mensajes siguientes:

Conexión fallida con el servidor de Tivoli Enterprise Portal

1. En el sistema donde está instalado el servidor de Tivoli Enterprise Portal, pulse **Inicio** -> **Programas** -> **IBM Tivoli Monitoring** -> **Manage Tivoli Monitoring Services**.
2. Opcional: Pulse con el botón derecho del ratón en la entrada Servidor de Tivoli Enterprise Portal y pulse en **Cambiar inicio**. En la ventana que se abrirá, seleccione ◉ **Cuenta del sistema** y ☑ **Permitir que el servicio interactúe con el escritorio** y pulse en **Aceptar**.

   Se abre una ventana de línea de mandatos cuando se inicia el servidor de Tivoli Enterprise Portal y se visualizan los mandatos internos.
3. Asegúrese que el servidor de Tivoli Enterprise Portal se haya iniciado:

   Si está iniciado, reinícielo.

   Si está detenido, inícielo.
4. Si sigue sin poder conectarse, revise la información siguiente. Si la información no es aplicable a su situación, póngase en contacto con el servicio de soporte de software de IBM.

Si está trabajando en la modalidad de navegador y atraviesa redes para acceder al servidor de Tivoli Enterprise Portal, es posible que el sistema de red no pueda resolver el nombre de host. Si este es el caso, realizar las acciones siguientes debe normalmente resolver el problema:

1. En el sistema donde está instalado el servidor de Tivoli Enterprise Portal, pulse **Inicio** -> **Programas** -> **IBM Tivoli Monitoring** -> **Manage Tivoli Monitoring Services**.
2. Pulse con el botón derecho del ratón en el servicio del navegador de Tivoli Enterprise Portal y pulse **Reconfigurar.**
3. Cambie el nombre de host por la dirección IP en dos lugares:

   En el campo **URL de inicio**, cambie *nombrehost* en http://*nombrehost*:15200 a la dirección IP del servidor de Tivoli Enterprise Portal. Por ejemplo, `http://10.21.2.166:15200`.

   En el campo **Host**, cambie el nombre de host a la dirección IP del servidor de Tivoli Enterprise Portal.
4. Pulse **Aceptar**.
5. Inicie la modalidad de navegador de Tivoli Enterprise Portal utilizando la dirección IP en lugar del nombre de host.
6. Si todavía sigue sin poderse conectarse, póngase en contacto con el soporte de software de IBM.

La contraseña de inicio de sesión ha caducado

Si el Tivoli Enterprise Monitoring Server concentrador está configurado para Validar usuarios, entonces es necesario utilizar contraseñas. Las contraseñas deben cumplir los requisitos de seguridad de su empresa. Si esto incluye cambios periódicos de contraseñas, puede recibir este mensaje al intentar iniciar la sesión en el servidor de portal. Si esto sucede, deberá cambiar la contraseña del sistema para poder iniciar la sesión. Por ejemplo,

en Windows esto significa modificar la contraseña utilizando Cuentas de usuario de las Herramientas administrativas.

La autorización de usuario ha fallado - O - No se ha podido procesar la solicitud de inicio de sesión

Tivoli Enterprise Portal utiliza la base de datos TEPS para validar los usuarios localmente. Si el servidor de supervisión concentrador se ha establecido para la validación de usuario (valor predeterminado en Windows), el ID de usuario también se valida en el servidor de supervisión para verificar la contraseña.

El servidor de portal no validó las credenciales de usuario tal como se entraron. Para el mensaje "No se puede procesar la solicitud de inicio de sesión", el servidor de portal pudo validar las credenciales de usuario, pero no completó la solicitud de inicio de sesión. En cualquiera de los dos casos, haga que el usuario intente de nuevo el inicio de sesión. Si el mensaje se muestra de nuevo, realice lo siguiente:

1. En el sistema donde está instalado el servidor de supervisión, compruebe que el servidor se está ejecutando en Manage Tivoli Monitoring Services.
2. Si el servidor de supervisión está en ejecución, asegúrese de que el ID de usuario se haya definido en Tivoli Enterprise Portal: Pulse **Administrar usuarios** y, a continuación, localice el ID en la lista **Usuarios**.
3. Si se ha definido el usuario, compruebe si se ha activado la seguridad a nivel de host para el servidor de supervisión concentrador y que el ID de usuario se haya autorizado en el entorno de host:

   En Manage Tivoli Monitoring Services, pulse con el botón derecho del ratón en **Servidor de Tivoli Enterprise Monitoring** y pulse **Reconfigurar.** Si se ha configurado la seguridad a nivel de host, el recuadro **Seguridad: Validar usuario** está seleccionado.

   Si el servidor de supervisión se ha configurado para Validar usuario, el ID de usuario de Tivoli Enterprise Portal también se debe añadir a las cuentas de usuario del dominio de red o al sistema operativo donde está instalado el servidor de supervisión, así como una contraseña.

   Si se han incluido caracteres no ASCII en el ID de usuario, no se guardan con el ID de usuario.
4. Intente iniciar la sesión en Tivoli Enterprise Portal con el ID de usuario en cuestión.
5. Si no consigue conectarse a Tivoli Enterprise Portal y el servidor de supervisión se ejecuta correctamente, es posible que el problema sea del servidor de Tivoli Enterprise Portal. Intente reciclar el servidor de portal. Si el usuario todavía no puede iniciar la sesión, consulte al servicio de soporte de software de IBM.

Este mensaje también se muestra después de un período de reintento de varios minutos (el valor predeterminado es 10 minutos y se puede cambiar mediante Manage Tivoli Monitoring Services) donde la barra de estado muestra **Validando credenciales de usuario** de forma continuada. Esto puede ser un síntoma de que el servidor de supervisión está detenido.

Capítulo 7. Utilización de políticas de autorización basadas en roles

La característica de Servidor de políticas de autorización de Tivoli proporciona posibilidades de control de acceso basado en roles para proteger los recursos de supervisión contra el acceso no autorizado de usuarios del panel de control de IBM Dashboard Application Services Hub.

La utilización de políticas de autorización proporciona las prestaciones siguientes:

- La posibilidad de restringir el acceso para los usuarios de panel de control a grupos de sistemas gestionados específicos y a sistemas gestionados individuales.
- La posibilidad de asignar políticas basadas en roles a usuarios y grupos de usuarios en un registro de usuarios de LDAP federado para simplificar la gestión de políticas.
- Una interfaz de línea de mandatos nueva que es muy automatizable.
- Gestión central de políticas de autorización para varios entornos de IBM Tivoli Monitoring, también denominados dominios.

Los permisos de Tivoli Enterprise Portal son el método de autorización predeterminado para controlar el acceso a los recursos en los paneles de control de supervisión. También son el mecanismo utilizado para autorizar a usuarios del cliente de Tivoli Enterprise Portal. Sin embargo, las políticas de autorización proporcionan un mayor control sobre el acceso a recursos. Con las políticas de autorización, se puede otorgar a un usuario de panel de control el permiso para ver datos de grupos de sistemas gestionados o sistemas gestionados específicos, a diferencia de la autorización de Tivoli Enterprise Portal que asigna el permiso de vista para aplicaciones de supervisión (agentes de supervisión). Es decir, con la autorización de Tivoli Enterprise Portal, se asigna a un usuario el permiso para ver todos los sistemas gestionados de un tipo de aplicación del agente determinado, por ejemplo, todos los agentes del sistema operativo Windows.

Si desea utilizar el control de acceso basado en roles proporcionado por las políticas de autorización, debe instalar el Servidor de políticas de autorización de Tivoli y la Interfaz de línea de mandatos tivcmd para la política de autorización. El Servidor de políticas de autorización se instala con IBM Dashboard Application Services Hub junto con aplicaciones de panel de control de supervisión, como Infrastructure Management Dashboards for Servers o los paneles de control personalizados. La CLI tivcmd se instala en sistemas utilizados por administradores de políticas de autorización y proporciona la interfaz de línea de mandatos para crear y trabajar con políticas de autorización. Envía solicitudes HTTP o HTTPS al Servidor de políticas de autorización, que mantiene el almacén maestro de políticas. Para obtener información de instalación, consulte “Instalación y configuración del Servidor de políticas de autorización de Tivoli y la interfaz de línea de mandatos tivcmd para la política de autorización” en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Tras la instalación satisfactoria de estos dos paquetes, puede ejecutar mandatos de CLI tivcmd según sea necesario para crear y trabajar con roles, otorgar permisos,

© Copyright IBM Corp. 2005, 2013

excluir permisos, revocar permisos y asignar usuarios y grupos de usuarios a un rol. Para obtener una lista completa de mandatos de la CLI tivcmd, consulte *IBM Tivoli Monitoring: Consulta de mandatos*.

Una vez que el conjunto de políticas de autorización se han creado, puede habilitar la comprobación de políticas de autorización en el Tivoli Enterprise Portal Server. El servidor de portal descarga periódicamente las políticas de autorización de la aplicación del Servidor de políticas de autorización. Cuando un usuario del panel de control solicita datos de supervisión, IBM Dashboard Application Services Hub reenvía la solicitud al componente de proveedor de datos de panel de instrumentos del servidor de portal. El proveedor de datos de panel de instrumentos utiliza las políticas de autorización para determinar a qué recursos supervisados está autorizado a acceder el usuario.

Puesto que Dashboard Application Services Hub y el servidor de portal deben tener conocimiento del usuario del panel de control, un entorno de paneles de control típico incluye un registro de usuarios federado proporcionado por un servidor LDAP y el inicio de sesión único. Para obtener información detallada sobre el conjunto de tareas implicadas en configurar un entorno de paneles de control que utiliza políticas de autorización, consulte "Configuración de un entorno de panel de control de supervisión con inicio de sesión único y con controles de autorización por usuario" en la página 32.

Conceptos sobre la política de autorización

Una política de autorización otorga o excluye un permiso a un *usuario* o *grupo de usuarios*, actuando en uno o varios *roles*, para realizar una *operación* en un tipo de *objeto*, para un *recurso* cuyo ámbito es su *tipo de recurso*.

Los elementos de una política de autorización se describen a continuación:

Usuario	El que inicia la operación.
Grupo de usuarios	Un conjunto de usuarios que pueden iniciar la operación.
Rol	Una colección de permisos que se pueden asignar a usuarios o grupos de usuarios.
Operación	Una acción como `crear`, `suprimir`, `modify`, `distribuir` o `ver`.
Tipo de objeto	Una categorización del objeto en el que se realiza la operación. Por ejemplo, datos de supervisión (`attributegroup`), `suceso` o `rol`.
Recurso	La entidad en la que se realiza la operación como un sistema gestionado o grupo de sistemas gestionados específicos.
Tipo de recurso	Una categorización del recurso. Grupos de sistemas gestionados (`managedsystemgroup`), sistemas gestionados (`managedsystem`) y conjuntos de roles (`rolegroup`) son los tipos de recursos predefinidos.

Para crear una política de autorización, realice las tareas siguientes:

1. Cree grupos de sistemas gestionados a los que desee controlar el acceso. Los grupos de sistemas gestionados se cran utilizando el cliente de Tivoli Enterprise Portal y el mandato **`tacmd createsystemlist`**.

   Pueden ser los mismos grupos de sistemas gestionados que también puede utilizar para distribuir situaciones y recopilaciones históricas.
2. Cree grupos de usuarios de LDAP que contienen usuarios que realizan una función de trabajo similar.
3. Cree un rol que represente una función de trabajo dentro de su organización.

Por ejemplo, puede definir un rol llamado `Administradores de Windows de la región oriental` para controlar los recursos supervisados a los que pueden acceder los administradores del sistema operativo Windows en el centro de datos de la región oriental.

4. A continuación otorgue o excluya uno o más permisos para el rol.
   - Un *otorgamiento de permiso* especifica la operación que se puede realizar en un tipo de objeto para uno o más recursos de un tipo especificado.

     Por ejemplo, puede otorgar permiso para ver datos de supervisión para el grupo de sistemas gestionados `EasternRegionWindowsComputers`, donde la operación es `ver`, el tipo de objeto es `attributegroup` (que representa datos de supervisión), el recurso es `EasternRegionWindowsComputers` y el tipo de recurso es `managedsystemgroup`.
   - Una *exclusión de permiso* permite restringir el acceso a uno o varios miembros de un grupo de sistemas gestionados. Debe crear una exclusión de permiso si no desea que un rol tenga acceso a todos los miembros de un grupo de sistemas gestionados. Por ejemplo, el grupo de sistemas gestionados `EasternRegionWindowsComputers` puede contener dos o tres sistemas para los que desea que los administradores de Windows de la región oriental no tengan acceso. En este caso, puede otorgar el permiso de `vista` para el grupo de sistemas gestionados `EasternRegionWindowsComputers` y `excluir` permiso para sistemas gestionados específicos. Una exclusión de permiso impide que se realice cualquier operación sobre los objetos de un sistema gestionado.
5. El paso final es asignar el rol a uno o varios usuarios o grupos de usuarios. Solo los usuarios o grupos de usuarios que se han asignado a un rol de política de autorización pueden acceder a los recursos supervisados en un panel de control. Los nombres de usuario y los nombres de grupos de usuarios se definen en el registro de usuarios LDAP que se comparte por IBM Dashboard Application Services Hub y el servidor de portal.

También puede revocar los permisos de un rol si más adelante decide que necesita eliminar un otorgamiento o exclusión de permiso de un rol. Las políticas de autorización también se utilizan para controlar qué usuarios pueden crear y trabajar con roles.

La tabla siguiente lista los tipos de recursos soportados, sus tipos de objeto y operaciones asociados, así como el tipo de permiso que se puede asignar para los recursos de este tipo.

Tabla 16. Tipos de recursos de política de autorización y sus permisos y elementos soportados

Permiso	Operación	Tipo de objeto	Tipo de recurso	Descripción
otorgar	ver	grupo de atributos	grupo sistemas gestionados	Con esta combinación, puede otorgar permiso para ver datos de supervisión como las métricas o el estado para todos los sistemas gestionados de un grupo de sistemas gestionados.
otorgar	ver	suceso	grupo sistemas gestionados	Con esta combinación, puede otorgar permiso para ver sucesos de situación de todos los sistemas gestionados de un grupo de sistemas gestionados. **Nota:** Si desea otorgar permiso para ver los datos de supervisión que han desencadenado el suceso de situación, debe otorgar permiso para ver los datos de supervisión para el grupo de sistemas gestionados.
otorgar	ver	grupo de atributos	sistema gestionado	Con esta combinación, puede otorgar permiso para ver datos de supervisión como métricas o el estado de un sistema gestionado específico.

Tabla 16. Tipos de recursos de política de autorización y sus permisos y elementos soportados (continuación)

Permiso	Operación	Tipo de objeto	Tipo de recurso	Descripción
otorgar	ver	suceso	sistema gestionado	Con esta combinación, puede otorgar permiso para ver sucesos de situación de un sistema gestionado específico. **Nota:** Si desea otorgar permiso para ver los datos de supervisión que han desencadenado el suceso de situación, debe otorgar permiso para ver los datos de supervisión para el grupo de sistemas gestionados.
excluir			sistema gestionado	Con esta combinación, puede excluir el permiso para realizar cualquier operación para un sistema gestionado específico.
otorgar	crear	rol	grupo de roles	Con esta combinación, puede otorgar permiso para crear roles o sucesos para sistemas gestionados específicos.
otorgar	suprimir	rol	grupo de roles	Con esta combinación, puede otorgar permiso para suprimir roles.
otorgar	distribuir	rol	grupo de roles	Con esta combinación, puede otorgar permiso para distribuir políticas desde el Servidor de políticas de autorización para Tivoli Enterprise Portal Server.
otorgar	modificar	rol	grupo de roles	Con esta combinación, puede otorgar permiso para modificar roles.
otorgar	ver	rol	grupo de roles	Con esta combinación, puede otorgar permiso para ver los roles y los permisos que tiene asignados. Este permiso puede utilizarse si tiene usuarios que deben poder ver sus permisos, pero no los permisos para otros usuarios.
otorgar	ver todo	rol	grupo de roles	Con esta combinación, puede otorgar el permiso para ver todos los roles y los permisos.

Cuando se le otorga permiso para ver grupos de atributos (datos de supervisión) o sucesos para un grupo de sistemas gestionados, se le otorga permiso para ver el grupo y también se le otorga permiso para ver todos los miembros del grupo, a menos que haya una exclusión de permiso para un miembro del grupo.

En un entorno de despliegue de IBM Tivoli Monitoring, puede tener varios dominios de supervisión. Un *dominio* de supervisión se define como una colección de componentes de IBM Tivoli Monitoring como servidores de portales, servidores de supervisión, agentes de supervisión y Tivoli Data Warehouse que se centran alrededor de un servidor de supervisión concentrador en particular. En este tipo de despliegue, puede tener algunas políticas de autorización que son comunes entre los dominios de supervisión, así como políticas de autorización que son específicas de un dominio concreto. Al crear permisos, la CLI tivcmd permite especificar si la política de autorización se aplica a todos los dominios (comportamiento predeterminado) o a dominios específicos.

Un *grupo de roles* es un conjunto de roles compartidos en todos los dominios de IBM Tivoli Monitoring que utilizan un único Servidor de políticas de autorización. El Servidor de políticas de autorización soporta solo un grupo de roles denominado `default`. Se especifica como el nombre de recurso al crear permisos que realizan operaciones en roles.

Para obtener información sobre cómo trabajar con políticas de autorización en un despliegue de varios dominios, consulte “Utilización de varios dominios” en la página 207.

Roles y permisos predefinidos

El Tivoli Servidor de políticas de autorización proporciona roles y permisos predefinidos para ayudarle a empezar. Los roles predefinidos también se denominan *roles principales*. Estos roles no se pueden modificar ni suprimir, pero se pueden copiar para crear nuevos roles.

Están predefinidos los siguientes roles y permisos:

RoleAdministrator

El rol de administrador de seguridad principal con autorización para gestionar todos los roles y políticas.

Nota: Cuando se instala el Servidor de políticas de autorización, el programa de instalación solicita un ID de usuario administrativo y contraseña de IBM Dashboard Application Services Hub. El instalador asigna el ID de usuario al rol RoleAdministrator. Para permitir que otros usuarios creen y trabajen con roles y asignen permisos, debe instalar la CLI tivcmd y utilizarla para iniciar sesión en el Servidor de políticas de autorización con las credenciales que se han especificado durante la instalación. A continuación, utilice los mandatos de tivcmd para asignar otros usuarios al rol RoleAdminisrator o un rol personalizado. Para obtener más detalles, consulte “Creación y asignación de roles de administrador” en la página 194.

Tabla 17. Permisos de RoleAdministrator

Operación	Tipo de objeto	Tipo de recurso	Recurso
ver	grupo de atributos	gruposistemasgestionados	cualquiera
ver	suceso	gruposistemasgestionados	cualquiera
ver	grupo de atributos	sistemagestionado	cualquiera
ver	suceso	sistemagestionado	cualquiera
crear, suprimir, modificar, ver, ver todo	rol	grupo de roles	default

PolicyDistributor

El rol con permiso para descargar políticas de autorización.

Este rol, o un rol personalizado con el mismo permiso, debe estar asignado al ID de usuario que se especifica cuando las políticas de autorización están habilitados en el servidor de portal. El servidor de portal utiliza el ID de usuario especificado y otras propiedades de conexión para conectarse periódicamente al Servidor de políticas de autorización y descargar la última política. Si el Servidor de políticas de autorización recibe una solicitud de políticas de autorización, verifica que el usuario que ha enviado la solicitud tiene otorgado el permiso para distribuir políticas.

Tabla 18. Permisos de PolicyDistributor

Operación	Tipo de objeto	Tipo de recurso	Recurso
distribuir	rol	grupo de roles	default

LinuxOperator
Un rol que tiene permisos de visualización del grupo de atributos y sucesos para todos los agentes de Linux.

UNIXOperator
Un rol que tiene permisos de visualización del grupo de atributos y sucesos para todos los agentes de UNIX.

WindowsOperator
Un rol que tiene permisos de visualización del grupo de atributos y sucesos para todos los agentes de Windows.

Tabla 19. Permisos LinuxOperator, UNIXOperator y WindowsOperator

Rol	Operación	Tipo de objeto	Tipo de recurso	Recurso
LinuxOperator	ver	grupo de atributos y suceso	gruposistemasgestionados	*LINUX_SYSTEM
UNIXOperator	ver	grupo de atributos y suceso	gruposistemasgestionados	*ALL_UNIX
WindowsOperator	ver	grupo de atributos y suceso	gruposistemasgestionados	*NT_SYSTEM

VCenterOperator
Un rol que tiene acceso a todos los centros virtuales de VMWARE y servidores ESX.

Tabla 20. Permisos VCenterOperator

Operación	Tipo de objeto	Tipo de recurso	Recurso
ver	grupo de atributos	gruposistemasgestionados	*VMWARE_VI_AGENT *VMWARE_VI
ver	suceso	gruposistemasgestionados	*VMWARE_VI_AGENT *VMWARE_VI

Preparación para habilitar las políticas de autorización

Antes de habilitar políticas de autorización, asegúrese de que está preparado leyendo y siguiendo la información proporcionada en este tema.

Cuando se instala un Tivoli Enterprise Portal Server, la obligatoriedad de las políticas de autorización se inhabilita de forma predeterminada. Hay un recuadro de selección **Habilitar políticas de autorización** en los paneles de configuración de Tivoli Enterprise Portal Server que controla esta característica. Si el recuadro no está seleccionado, significa que el proveedor de datos de panel de instrumentos no utilizará las políticas de autorización para controlar el acceso al grupo de sistemas gestionados y al sistema gestionado. En su lugar se utiliza la autorización de Tivoli Enterprise Portal para controlar el acceso a los recursos supervisados en los paneles de control.

Realice los pasos siguientes antes de habilitar la obligatoriedad de las políticas de autorización:

1. Identifique qué usuarios necesitarán administrar políticas de autorización.

   Cuando se instala el Servidor de políticas de autorización, el programa de instalación solicita un ID de usuario administrativo y contraseña de IBM Dashboard Application Services Hub. El instalador asigna el ID de usuario al rol RoleAdministrator predefinido. Para permitir que otros usuarios creen y

trabajen con roles y asignen permisos, debe instalar la CLI tivcmd y utilizarla para iniciar sesión en el Servidor de políticas de autorización con las credenciales que se han especificado durante la instalación. A continuación, utilice los mandatos tivcmd para añadir otros administradores de políticas al rol RoleAdministrator predefinido o para crear un rol equivalente con permisos similares y añadirlos a ese rol. Para ver pasos detallados, consulte "Creación y asignación de roles de administrador" en la página 194.

Para obtener más detalles sobre la instalación de la CLI tivcmd, consulte "Instalación y configuración del Servidor de políticas de autorización de Tivoli y la interfaz de línea de mandatos tivcmd para la política de autorización" en *IBM Tivoli Monitoring: Guía de instalación y configuración*.

2. Asigne al menos un usuario a un rol, normalmente el rol PolicyDistributor predefinido, que tenga permiso para distribuir políticas.

   El mismo usuario debe especificarse en el panel de configuración del Tivoli Enterprise Portal Server cuando esté listo para volver a configurar el servidor de portal para habilitar las políticas de autorización.

   Debe asignar a un usuario el permiso para distribuir políticas a fin de que el proveedor de datos de panel de instrumentos tenga autoridad para recuperar actualizaciones de políticas desde el Servidor de políticas de autorización. Para ver pasos detallados, consulte "Creación y asignación de roles de distribuidor de políticas" en la página 195.

3. Cree roles y permisos, o aprovechar los roles y permisos predefinidos, para todos los grupos de sistemas gestionados existentes y los sistemas gestionados que se puedan visualizar en vistas de panel de control y, a continuación, añada usuarios o grupos de usuarios a estos roles. Para ver ejemplos detallados, consulte "Ejemplos de gestión de políticas" en la página 196.

   Nota: El conjunto de roles y permisos predefinidos están pensados como una conveniencia para cubrir algunas, y quizás incluso la mayoría de sus necesidades de seguridad. Sin embargo, puede tener grupos de sistemas gestionados adicionales y sistemas gestionados en su entorno que requieran sus propias definiciones de política. La información de "Escenarios de gestión de políticas" en la página 192 está pensada para ayudarle a comprender mejor cómo utilizar la CLI tivcmd para crear estas políticas adicionales.

4. Determine con qué frecuencia el proveedor de datos de panel de control debe recuperar políticas de autorización del servidor de políticas de autorización.

   Para evitar accesos que consumen tiempo a través de la red, el proveedor de datos de panel de instrumentos recupera su propia copia local del almacén de políticas maestro del Servidor de políticas de autorización. La recuperación de la política se produce una vez durante el inicio de proveedor de datos de panel de instrumentos, y después se repite a intervalos regulares, que toman el valor predeterminado de 30 minutos. Puede cambiar el valor predeterminado a través de los paneles de configuración del Tivoli Enterprise Portal Server cuando se habilitan las políticas de autorización y puede especificar un valor entre 5 y 1440 minutos. Tenga en cuenta que los cambios de políticas efectuados utilizando la CLI tivcmd no entrarán en vigor en el proveedor de datos de panel de instrumentos hasta su próxima recuperación de almacén de políticas satisfactoria.

Cuando esté listo para empezar a utilizar políticas de autorización, vuelva a configurar el servidor de portal para habilitar las políticas de autorización y especificar las propiedades de conexión para el Servidor de políticas de autorización. Las propiedades de conexión incluyen el ID de usuario al que se ha asignado un rol con permiso para distribuir políticas.

Para obtener una lista de las tareas que se deben realizar antes de habilitar las políticas de autorización, consulte “Configuración de un entorno de panel de control de supervisión con inicio de sesión único y con controles de autorización por usuario” en la página 32.

Escenarios de gestión de políticas

En Tivoli Servidor de políticas de autorización, no hay permiso universal que pueda asignarse a un rol que proporcione a un usuario acceso a todo. A los roles se les debe otorgar acceso explícito a los grupos de sistemas gestionados específicos o sistemas gestionados.Además un usuario de panel de control solo puede ver los recursos en los paneles de control de supervisión si están asignados a un rol con acceso a grupos de sistemas gestionados o sistemas gestionados.

Prácticas recomendadas para crear políticas de autorización

Revise las prácticas recomendadas para crear políticas de autorización en el entorno.

- Otorgar permisos a grupos de sistemas gestionados en lugar de a sistemas gestionados individuales.

  Este enfoque tiene la ventaja de que las actualizaciones de políticas de autorización no son necesarias cuando se añaden sistemas gestionados a su entorno. En su lugar, se añade un nuevo sistema gestionado a un grupo de sistemas gestionados al que ya se ha otorgado permiso de vista y que contiene sistemas similares que utilizan el mismo conjunto de definiciones de situación o definiciones de recopilación de datos históricos. Para obtener nuevos sistemas gestionados, solo es necesario crear una política de autorización nueva en estos casos:

  – No hay un grupo de sistemas gestionados existente al que pueda añadirse el sistema gestionado. En este caso, añada un nuevo grupo de sistemas gestionados que contenga el nuevo sistema gestionado. A continuación, otorgue el permiso de vista para el grupo de sistemas gestionados a uno o más roles.

  – Se crea un permiso de exclusión para el sistema gestionado porque no deben acceder a él los usuarios a los que se les ha otorgado permiso de vista para los grupos de sistemas gestionados que contienen el nuevo sistema gestionado.

- Asignar grupos de usuarios a roles en lugar de asignar usuarios individuales a roles.

  Cuando siga este enfoque, las actualizaciones de políticas de autorización no son necesarias cuando hay un nuevo usuario de panel de control. En su lugar, se añade el nuevo usuario a un grupo de usuarios en LDAP que ya se ha asignado a un rol de política de autorización que coincide con la función del trabajo del nuevo usuario.

  Crear una nueva política de autorización para un nuevo usuario si no hay un grupo de usuarios existente al que se pueda añadir el usuario. En este caso, añada un nuevo grupo de usuarios de LDAP, añada el nuevo usuario al grupo y asigne el grupo a uno o varios roles de política de autorización. Si es necesario, cree un rol nuevo que coincida con ámbito de permisos del grupo de usuarios nuevo.

- Crear un grupo de usuarios en LDAP para los administradores de políticas de autorización y asignar el grupo de usuarios a un rol al que se ha otorgado permiso para crear, modificar, suprimir y ver roles. El rol de RoleAdministrator predefinido tiene estos permisos. Asimismo, asegúrese de que varios usuarios

sean miembros del grupo de usuarios, de modo que las actualizaciones de autorización puedan realizarse por más de un usuario.

- Si desea que los usuarios del panel de control vean los datos de supervisión y los sucesos de situación para los recursos, cree roles que otorguen permiso para ver datos de supervisión (grupos de atributos) y para ver los sucesos de situación para los recursos con los que pueden trabajar.

  Solo otorgar permiso para ver sucesos, pero no supervisar datos y viceversa para aquellos usuarios que necesitan un acceso más restrictivo.

  Cuando se otorga a un grupo de usuarios (o usuario) el permiso para ver los grupos de atributos y sucesos, se otorga el permiso para ver los dos tipos de objetos con el mismo tipo de recurso (o grupo de sistemas gestionados o sistema gestionado).

  – Práctica recomendada de ejemplo: Otorgar permiso para ver sucesos y grupos de atributos para los recursos del grupo de sistemas gestionados.

    ```
    tivcmd grant --rolename "Administradores de la Costa Oeste" --resourcetype
    managedsystemgroup --resources "West_Coast_Systems" --objecttype
    attributegroup --operations view

    tivcmd grant --rolename "West Coast Administrators" --resourcetype
    managedsystemgroup --resources "West_Coast_Systems" --objecttype event
    --operations view
    ```

  – Variación de la práctica recomendada: Otorgar permiso para ver sucesos y grupos de atributos para un sistema gestionado.

    ```
    tivcmd grant --rolename "West Coast Administrators" --resourcetype
    managedsystem --resources "Primary:server1:NT" --objecttype
    attributegroup --operations view

    tivcmd grant --rolename "West Coast Administrators" --resourcetype
    managedsystem --resources "Primary:server1:NT" --objecttype event
    --operations view
    ```

  – Ejemplo de una política que no cumple con los criterios de la práctica recomendada:

    ```
    tivcmd grant --rolename "West Coast Administrators" --resourcetype
    managedsystemgroup --resources "West_Coast_Systems" --objecttype
    attributegroup --operations view

    tivcmd grant --rolename "West Coast Administrators" --resourcetype
    managedsystem --resources "Primary:server1:NT" --objecttype event
    --operations view
    ```

    donde, `Primary:server1:NT` es miembro del grupo de sistemas gestionados `West_Coast_Systems`

  – Ejemplo de una política que no cumple con los criterios de la práctica recomendada:

    ```
    tivcmd grant --rolename "West Coast Administrators" --resourcetype
    managedsystem --resources "Primary:server1:NT" --objecttype
    attributegroup --operations view

    tivcmd grant --rolename "West Coast Administrators" --resourcetype
    managedsystemgroup --resources "West_Coast_Systems" --objecttype event
    --operations view
    ```

    donde, `Primary:server1:NT` es miembro del grupo de sistemas gestionados `West_Coast_Systems`

- Prácticas recomendadas adicionales y consideraciones específicas de la aplicación Infrastructure Management Dashboards for Servers:

– Si desea que los usuarios del panel de control utilicen la página **Grupos de sistemas gestionados**, deben tener asignado un rol que otorgue el permiso para ver sucesos o grupos de atributos o ambos para grupos de sistemas gestionados. Si un usuario se asigna a roles que solo tienen permiso de vista para uno o varios sistemas gestionados, no verá ningún recurso supervisado en la página **Grupos de sistemas gestionados**.
– Si desea que los usuarios del panel de control utilicen la página **Sucesos de situación**, deben tener asignado un rol que otorgue permiso para ver los sucesos para grupos de sistemas gestionados (práctica recomendada) o sistemas gestionados individuales. Si desea que el usuario vea los datos de supervisión que han causado que el suceso de situación se abra, el usuario también debe estar asignado a un rol que otorgue permiso para ver grupos de atributos para grupos de sistemas gestionados (práctica recomendada) o sistemas gestionados individuales.

Creación y asignación de roles de administrador

Cuando se instala el Servidor de políticas de autorización, un usuario administrativo de Dashboard Application Services Hub se asigna al rol RoleAdministrators predefinido. Normalmente, este es tipadmin. Puede añadir sus propios usuarios administrativos al rol RoleAdministrator predefinido, o crear sus propios roles personalizados con los mismos permisos.

Una práctica recomendada es crear un grupo de usuarios de LDAP para los administradores de políticas y asignar el grupo de usuarios a los roles que tienen permiso para crear y trabajar con políticas de autorización. Al tomar este enfoque, solo puede actualizar la pertenencia a grupos (y no las políticas de autorización) al añadir o eliminar administradores de políticas.

Acerca de esta tarea

Los roles que se utilizan para la administración de roles deben tener el permiso siguiente:

Definición de permiso de administración de roles	
Parámetro	**Valor**
Operación	'create', 'delete', 'modify', 'view', 'viewall'
Tipo de objeto	'role'
Tipo de recurso	'rolegroup'
Recurso	'default'

Procedimiento

- Para asignar a un usuario o grupo de usuarios el rol RoleAdministrator predefinido, utilice los pasos siguientes:
  1. Defina un usuario de LDAP, por ejemplo `uid=JohnDoe,cn=itm,o=ibm` o defina un grupo de usuarios, por ejemplo, `cn=Administrators,cn=itm,o=ibm`. A continuación, añada el ID de usuario del administrador de políticas, como `uid=JohnDoe,cn=itm,o=ibm`, al grupo en LDAP.
  2. Añada el grupo de usuarios al rol RoleAdministrator predefinido utilizando el mandato siguiente:

     ```
     tivcmd addtorole --rolename RoleAdministrator
     --groups gid=Administrators,cn=itm,o=ibm
     ```

3. De forma alternativa, añada el usuario al rol RoleAdministrator predefinido utilizando el mandato siguiente:

```
tivcmd addtorole --rolename RoleAdministrator
--users uid=JohnDoe,cn=itm,o=ibm
```

- Para crear un rol nuevo con el mismo permiso que el rol RoleAdministrator, utilice los pasos siguientes:
  1. Defina un usuario en LDAP, por ejemplo `uid=JohnDoe,cn=itm,o=ibm` O defina un grupo en LDAP, por ejemplo `cn=Administrators,cn=itm,o=ibm` y, a continuación, añada los ID de usuario administrador de políticas al grupo en LDAP.
  2. Cree un nuevo rol y añada los permisos para crear y trabajar con políticas de autorización para el nuevo rol. A continuación, asigne el usuario o grupo de usuarios al nuevo rol. Los siguientes mandatos de ejemplo muestran que puede añadir usuarios y grupos al rol personalizado para la administración de políticas:

```
tivcmd createrole --rolename EastCoastAdministrators --description
"East Coast users with permission to manage roles and policies"

tivcmd grant --rolename EastCoastAdministrators --resourcetype rolegroup
--resources default --objecttype role --operations create delete modify
view viewall

tivcmd addtorole --rolename EastCoastAdministrators
 --users uid=JohnDoe,cn=itm,o=ibm
 --groups cn=Administrators,cn=itm,o=ibm
```

  3. De forma alternativa, puede duplicar el rol RoleAdministrator existente y asignar el nuevo rol al grupo de usuarios utilizando los mandatos siguientes:

```
tivcmd copyrole --fromrolename RoleAdministrator --torolename
EastCoastAdministrators --description "East Coast users allowed to
administer roles and policies for this authorization policy server"
--permissionsonly

tivcmd addtorole --rolename EastCoastAdministrators
 --groups cn=Administrators,cn=itm,o=ibm
```

Creación y asignación de roles de distribuidor de políticas

Al configurar un nuevo entorno de paneles de control, los ID de usuario deben crearse en el registro de usuarios LDAP para cada usuario de paneles de control y administrador de políticas. También necesita un ID de usuario al que se le ha otorgado permiso para distribuir políticas. Este ID de usuario debe especificarse al habilitar políticas de autorización en el servidor de portal. El servidor de portal incluye que el ID de usuario en las solicitudes que envía al Servidor de políticas de autorización para descargar la versión más reciente de las políticas de autorización. El Servidor de políticas de autorización verifica que el usuario tiene permiso para recuperar las políticas. IBM Tivoli Monitoring proporciona el rol PolicyDistributor predefinido que ya tiene este permiso. Los administradores pueden crear nuevos roles con este permiso, o utilizar el rol predefinido.

Acerca de esta tarea

Los roles que se utilizan para la distribución de políticas deben tener el permiso siguiente:

Definición de permiso de distribución de políticas	
Parámetro	**Valor**
Operación	'distribute'

Definición de permiso de distribución de políticas	
Tipo de objeto	'role'
Tipo de recurso	'rolegroup'
Recurso	'default'

Procedimiento

- Para asignar a un usuario el rol de PolicyDistributor predefinido, utilice los pasos siguientes:
  1. Defina un usuario en LDAP, por ejemplo `uid=PolicyAdmin,cn=itm,o=ibm`.
  2. Añada el usuario al rol PolicyDistributor predefinido utilizando el mandato siguiente:

     ```
     tivcmd addtorole --rolename PolicyDistributor
       --users uid=PolicyAdmin,cn=itm,o=ibm
     ```
- Para crear un rol nuevo con el mismo permiso que el rol PolicyDistributor, utilice los pasos siguientes:
  1. Defina un usuario en LDAP, por ejemplo `uid=PolicyAdmin,cn=itm,o=ibm`.
  2. Cree un nuevo rol con permiso para distribuir políticas y asígnelo al usuario utilizando los mandatos siguientes:

     ```
     tivcmd createrole --rolename EastCoastDistributor --description
     "East Coast user IDs for downloading policy"

     tivcmd grant --rolename EastCoastDistributor --resourcetype rolegroup
     --resources default --objecttype role --operations distribute

     tivcmd addtorole --rolename EastCoastDistributor
     --users uid=PolicyAdmin,cn=itm,o=ibm
     ```
  3. De forma alternativa, puede duplicar el rol PolicyDistributor existente utilizando los mandatos siguientes:

     ```
     tivcmd copyrole --fromrolename PolicyDistributor --torolename
     EastCoastDistributor --description "East Coast user IDs to
     download policy" --permissionsonly

     tivcmd addtorole --rolename EastCoastDistributor
       --users uid=PolicyAdmin,cn=itm,o=ibm
     ```

Ejemplos de gestión de políticas

El objetivo de las políticas de autorización es darle control granular sobre los recursos supervisados. Al configurar un entorno nuevo de paneles de control, los ID de usuario de panel de control deben crearse en los repositorios de usuarios de LDAP. La práctica recomendada es configurar también los grupos LDAP que contienen el conjunto de usuarios que están asignados a roles de política de autorización. Esto hace que la gestión de políticas sea más fácil, en lugar de la asignación de cada ID de usuario individual a un rol. Utilice los ejemplos de este tema como ayuda para empezar a utilizar con políticas.

Puede utilizar los mandatos de la Interfaz de línea de mandatos tivcmd para la política de autorización para gestionar sus políticas. Para obtener información detallada sobre los mandatos, consulte *IBM Tivoli Monitoring: Consulta de mandatos*.

En este ejemplo se presupone que hay un rol existente denominado `West Coast Administrators` y que desea otorgar a este rol la posibilidad de ver todos los datos y sucesos del grupo de atributos para el grupo de sistemas gestionados denominado `West_Coast_DataCenter_Systems` y de otro grupo de sistemas

gestionados denominado West_Coast_Regional_Systems y asignar este rol al grupo de usuarios cn=westcoastadmins,cn=itm,o=ibm.

```
tivcmd grant --rolename "West Coast Administrators"
--resourcetype  managedsystemgroup --resources
"West_Coast_DataCenter_Systems"
 --objecttype attributegroup --operations viewtivcmd grant --rolename "West Coast Administrators"
--resourcetype managedsystemgroup --resources
"West_Coast_DataCenter_Systems"
--objecttype event  --operations view

tivcmd grant --rolename "West Coast Administrators"
--resourcetype managedsystemgroup --resources "West_Coast_Regional_Systems"
 --objecttype attributegroup --operations viewtivcmd grant --rolename "West Coast Administrators"
--resourcetype managedsystemgroup --resources "West_Coast_Regional_Systems"
--objecttype event  --operations view

tivcmd addtorole --rolename "West Coast Administrators"
--groups cn=westcoastadmins,cn=itm,o=ibm
```

En este ejemplo se presupone que desea impedir que miembros del grupo de usuarios cn=westcoastadmins,cn=itm,o=ibm vean los datos y sucesos del grupo de atributos para el sistema gestionado Primary:server1:NT. En este caso, Primary:server1:NT es un miembro del grupo de sistemas gestionados West_Coast_DataCenter_Systems para el que se ha otorgado al grupo de usuarios el permiso de vista en el ejemplo anterior.

```
tivcmd exclude --rolename "West Coast Administrators" --resourcetype
managedsystem --resources Primary:server1:NT
```

En este ejemplo se presupone que desea eliminar la otorgación de permisos para ver los datos y sucesos del grupo de atributos para el grupo de sistemas gestionados West_Coast_DataCenter_Systems y la exclusión del permiso para el sistema gestionado Primary:server1:NT del rol West Coast Administrators, pero dejar el otorgamiento de permisos para el grupo de sistemas gestionados West_Coast_Regional_Systems.

```
tivcmd revoke --rolename "West Coast Administrators" --resourcetype
managedsystemgroup --resources "West_Coast_DataCenter_Systems"
--objecttype attributegroup --operations view  --grantcommand

tivcmd revoke --rolename "West Coast Administrators" --resourcetype
managedsystemgroup --resources "West_Coast_DataCenter_Systems"
--objecttype event  --operations view --grantcommand

tivcmd revoke --rolename "West Coast Administrators" --resourcetype
managedsystem --resources Primary:server1:NT  --excludecommand
```

En este ejemplo, será un administrador de IBM Tivoli Monitoring que desea controlar el acceso de paneles de control a los sistemas gestionados pertenecientes a tres regiones geográficas: oriental, central y occidental. El servidor de supervisión ha gestionado las definiciones de grupos de sistemas de EasternRegionSystems, CentralRegionSystems y WesternRegionSystems, que contienen los sistemas gestionados para las respectivas regiones geográficas. Desea acceder a los sistemas gestionados de las tres regiones, pero desea que el operador denominado Annette que solo tenga acceso a los sistemas de la región occidental. En este ejemplo se presupone que el registro de usuarios de LDAP local incluye los grupos de usuarios llamados EasternRegionOperators, CentralRegionOperators y WesternRegionOperators y que Annette es miembro del grupo WesternRegionOperators.

1. Inicie sesión en el Servidor de políticas de autorización:

   ```
   tivcmd login --username <user> --password <password>
   ```

2. Cree tres nuevos roles, uno para cada región geográfica:

```
tivcmd createrole --rolename EasternRegionOperator --description
"Un rol para controlar el acceso a los datos de los sistemas de la región central"

tivcmd createrole --rolename CentralRegionOperator --description
"Un rol para controlar el acceso a los datos para los sistemas de la región central"

tivcmd createrole --rolename WesternRegionOperator --description
"Un rol para controlar el acceso a los datos de los sistemas de la región occidental"
```

3. Confirme que los nuevos roles se han creado:

```
tivcmd listroles --rolename EasternRegionOperator --showdescription

tivcmd listroles --rolename CentralRegionOperator --showdescription

tivcmd listroles --rolename WesternRegionOperator --showdescription
```

4. Visualice las reglas de uso para **tivcmd grant**:

```
tivcmd grant -?
```

5. Emita mandatos de otorgamiento que permitan que el rol EasternRegionOperator tenga acceso a datos de atributos y sucesos para EasternRegionSystems:

```
tivcmd grant --rolename EasternRegionOperator --resourcetype managedsystemgroup
--resources EasternRegionSystems --objecttype attributegroup --operations view

tivcmd grant --rolename EasternRegionOperator --resourcetype managedsystemgroup
--resources EasternRegionSystems --objecttype event --operations view
```

6. Confirme que el rol EasternRegionOperator tiene los permisos correctos:

```
tivcmd listroles --rolename EasternRegionOperator --showpermissions
```

7. Repita los mandatos para otorgar a los otros dos roles los mismos permisos para sus respectivas regiones geográficas:

```
tivcmd grant --rolename CentralRegionOperator --resourcetype managedsystemgroup
--resources CentralRegionSystems --objecttype attributegroup --operations view

tivcmd grant --rolename CentralRegionOperator --resourcetype managedsystemgroup
--resources CentralRegionSystems --objecttype event --operations view

tivcmd grant --rolename WesternRegionOperator --resourcetype managedsystemgroup
--resources WesternRegionSystems --objecttype attributegroup --operations view

tivcmd grant --rolename WesternRegionOperator --resourcetype managedsystemgroup
--resources WesternRegionSystems --objecttype event --operations view
```

8. Visualice las reglas de uso para el mandato **tivcmd addtorole**:

```
tivcmd addtorole -?
```

9. Asocie cada grupo de usuarios de LDAP a su papel correspondiente:

```
tivcmd addtorole --rolename EasternRegionOperator --groups
cn=EasternRegionOperators,cn=itm,o=tivoli

tivcmd addtorole --rolename CentralRegionOperator --groups
cn=CentralRegionOperators,cn=itm,o=tivoli

tivcmd addtorole --rolename WesternRegionOperator --groups
cn=WesternRegionOperators,cn=itm,o=tivoli
```

10. Muestre los miembros de cada rol para confirmar que las asociaciones del grupo de usuarios se han completado correctamente:

```
tivcmd listroles --rolename EasternRegionOperator --showmembership

tivcmd listroles --rolename CentralRegionOperator --showmembership

tivcmd listroles --rolename WesternRegionOperator --showmembership
```

11. Asegúrese de que tiene acceso a los sistemas de las tres regiones. Esto puede lograrse añadiendo su ID de usuario a cada uno de los tres roles nuevos:

```
tivcmd addtorole --rolename EasternRegionOperator --users
uid=<userid>,cn=itm,o=tivoli

tivcmd addtorole --rolename CentralRegionOperator --users
uid=<userid>,cn=itm,o=tivoli

tivcmd addtorole --rolename WesternRegionOperator --users
uid=<userid>,cn=itm,o=tivoli
```

12. Añada el ID de usuario al rol PolicyDistributor predefinido. Este mandato asegura que el proveedor de datos de panel de instrumentos puede utilizar su ID para descargar actualizaciones de almacén de archivos de políticas del Servidor de políticas de autorización:

```
tivcmd addtorole --rolename PolicyDistributor
--users uid=<userid>,cn=itm,o=tivoli
```

13. Visualice todos los roles a los que el ID de usuario pertenece:

```
tivcmd listroles --username uid=<userid>,cn=itm,o=tivoli
```

La configuración de seguridad se ha completado.

- Annette solo es un miembro del grupo de usuarios `WesternRegionOperators`.
- El grupo de usuarios `WesternRegionOperators` solo se ha asignado al rol `WesternRegionOperator`.
- El rol `WesternRegionOperator` solo tiene otorgado el acceso al grupo de sistemas gestionados `WesternRegionSystems`.
- Annette solo puede ver los datos de atributos y sucesos para los sistemas gestionados que pertenecen a `WesternRegionSystems`.

Habilitación de políticas de autorización en el servidor de portal

Una vez que haya creado el conjunto inicial de las políticas de autorización y asignado un usuario al rol con permiso para distribuir políticas, habilite la obligatoriedad de la política de autorización en la proveedor de datos de panel de instrumentos mediante la configuración del Tivoli Enterprise Portal Server utilizando Manage Tivoli Enterprise Monitoring Services o la línea de mandatos.

Procedimiento

- Utilización de Manage Tivoli Enterprise Monitoring Services
  1. Inicie Manage Tivoli Enterprise Monitoring Services en el sistema en el que está instalado el servidor de portal:

     Windows Pulse **Inicio → Programas →IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services**.

     Linux UNIX Donde *install_dir* es el directorio de instalación de IBM Tivoli Monitoring, vaya al directorio *install_dir*`/bin` y ejecute `./itmcmd manage [-h` *install_dir*`]`.

  2. Pulse con el botón derecho del ratón en el **Tivoli Enterprise Portal Server:**

     Windows Pulse **Reconfigurar**, luego pulse **Aceptar** para aceptar la configuración existente e ir a la segunda ventana Configuración del servidor TEP.

     Linux UNIX Pulse **Configurar**.Se visualizará la ventana Configuración de la Consola de sucesos comunes. Pulse **Aceptar** para aceptar los valores actuales. En la ventana Configurar Tivoli Enterprise Portal, seleccione el separador **Proveedor de datos de panel de control**.

3. En el área del proveedor de datos de panel de instrumentos de la ventana de configuración, verifique que el recuadro de selección **Habilitar políticas de autorización** esté seleccionado. Si no lo está, debe seleccionarlo.
   a. Cuando el proveedor de datos de panel de instrumentos está habilitado, puede especificar un valor de sustitución de dominio. Este valor es opcional. Cambia el ID del proveedor de datos de panel de instrumentos y el nombre de dominio para políticas de autorización de `itm.<nombre_servidor_supervisión_concentrador>` por `itm.<valor_sustitución_dominio>`. El valor no puede superar los 124 caracteres. Debe configurar un valor de sustitución de dominio para estos casos:
      – Se utiliza la característica de alta disponibilidad de Espera activa para el servidor de supervisión concentrador. Al configurar un valor de sustitución de dominio, el ID del proveedor de datos de panel de instrumentos y el nombre de dominio no cambiarán cuando el servidor de portal se configure para conectarse al nuevo servidor de supervisión concentrador activo. Si no configura un valor de sustitución de dominio en este escenario, debe volver a configurar la conexión entre IBM Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos, así como actualizar cualquier política de autorización específica de dominio cuando el servidor de portal se configure para conectarse al nuevo servidor de supervisión concentrador activo.
      – Tiene varios servidores de supervisión concentradores que utilizan un conjunto común de políticas de autorización para controlar el acceso del panel de control y desea crear algunas políticas de autorización específicas de dominio. Debe especificar un valor de sustitución de dominio para este escenario si desea utilizar, en las políticas de autorización, un nombre de dominio más descriptivo que el valor predeterminado de `itm.<nombre_servidor_supervisión_concentrador>`.

      Si modifica la sustitución del dominio después de configurar una conexión en Dashboard Application Services Hub para el proveedor de datos de panel de instrumentos, debe suprimir la conexión y volverla a añadir. Consulte “Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring” en la página 52 para obtener detalles sobre cómo configurar una conexión de proveedor de datos de panel de instrumentos. Además, si ha creado alguna política de autorización específica de dominio utilizando el nombre de dominio predeterminado, debe suprimir los permisos que utilizan el nombre de dominio anterior y crear nuevos permisos que utilicen el nombre de dominio nuevo cuando cambie el valor de sustitución de dominio.
   b. La opción **Habilitar políticas de autorización** se selecciona si desea utilizar políticas de autorización para controlar a qué sistemas gestionados y grupos de sistemas gestionados puede acceder un usuario en los paneles de control de supervisión. Solo se deben habilitar políticas de autorización si se está configurando un entorno de paneles de control con inicio de sesión único, tiene la intención de utilizar políticas de autorización para controlar el acceso a los paneles de control de supervisión y los administradores ya han creado el conjunto inicial de políticas de acceso de usuario del panel de control.
4. En la ventana Configuración del Servidor de políticas de autorización, especifique la siguiente información:

Tabla 21. Información de configuración para el Servidor de políticas de autorización

Campo	Descripción
Nombre de host o dirección IP	Dirección IP o nombre de host completo de IBM Dashboard Application Services Hub con el Servidor de políticas de autorización. Este parámetro es necesario.
Protocolo	Elija el protocolo utilizado para conectarse a IBM Dashboard Application Services Hub con el Servidor de políticas de autorización. El valor predeterminado es HTTPS. Este parámetro no es necesario. **Nota:** Solo debe seleccionar HTTPS si ya ha configurado TLS/SSL entre el servidor de portal y el Servidor de políticas de autorización. Consulte "Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización" en la página 223.
Puerto	Elija el puerto utilizado para conectarse a IBM Dashboard Application Services Hub con el Servidor de políticas de autorización. El valor predeterminado es 16311 para el protocolo HTTPS y 16310 para el protocolo HTTP. Los valores de puerto válidos están entre 1 y 65535 inclusive. Este parámetro no es necesario.
Intervalo de sondeo	La frecuencia con la que el almacén de datos local se actualiza desde el Servidor de políticas de autorización por el cliente de la política que se ejecuta en el servidor de portal. El valor predeterminado es 30 minutos. Los valores válidos son de 5 a 1440 minutes inclusive. Este parámetro no es necesario.
Intervalo de caducidad de almacén de políticas	Si el almacén de políticas no se puede actualizar desde el Servidor de políticas de autorización, este intervalo es el período de tiempo que el almacén de políticas local se seguirá utilizando desde la última actualización. Si el Servidor de políticas de autorización no se puede acceder durante el intervalo de tiempo especificado por este parámetro, todas las solicitudes subsiguientes para datos de panel de control fallarán con un error de autorización hasta que el Servidor de políticas de autorización esté disponible de nuevo. El valor predeterminado es 7 días y 0 horas. El valor especificado para las horas debe estar en el rango de 0 a 23 horas. Si el intervalo de caducidad se establece en 0 días y 0 horas, el almacén de políticas nunca caduca. Este parámetro no es necesario.
ID de usuario	El nombre del usuario que el servidor de portal utilizará para acceder a IBM Dashboard Application Services Hub con el Servidor de políticas de autorización. Este usuario debe añadirse al rol de núcleo de políticas de autorización PolicyDistributor o a un rol personalizado al que se ha otorgado permiso para realizar la operación de distribución para el tipo de objeto de rol. Este parámetro es necesario.
Contraseña	La contraseña para el usuario. Este parámetro es necesario.
Confirmar contraseña	Confirme la contraseña especificándola de nuevo. Este parámetro es necesario.

Escriba la información necesaria para los parámetros de conexión del

Servidor de políticas de autorización en los campos proporcionados y pulse **Aceptar**.

5. Se le solicitará que si desea reconfigurar la información de conexión de almacén, responda **No**.
6. En Windows, después de un proceso de los valores de configuración, se visualiza la ventana Configuración de la Consola de sucesos comunes. A veces esta ventana no se abre en primer plano y queda oculta por otras ventanas. Si parece que el proceso tarda más de lo esperado, minimice otras ventanas y busque la ventana de configuración. Cuando se muestre la ventana Configuración de la Consola de sucesos comunes, pulse **Aceptar**.
7. Si ha realizado cambios en la configuración, asegúrese de que el servidor de portal se reinicia.

- Utilización de la línea de mandatos

  Si el Tivoli Enterprise Portal Server está en Linux o UNIX, puede modificar la configuración del servidor de portal desde la línea de mandatos y habilitar políticas de autorización si no están habilitadas.

  1. Inicie la sesión en el sistema en el que está instalado el Tivoli Enterprise Portal Server.
  2. En la línea de mandatos, vaya al directorio *install_dir*/bin, donde *install_dir* es el directorio donde se ha instalado el producto.
  3. Ejecute el mandato siguiente para configurar el Tivoli Enterprise Portal Server: **./itmcmd config -A cq**.

     Aparece el mensaje `Agente de configuración iniciado`, seguido de la solicitud: `Tivoli Enterprise Portal Server se detendrá durante la configuración. ¿Desea continuar? [1=Sí, 2=No] (el valor predeterminado es 2).`
  4. Escriba 1. Se visualiza la siguiente solicitud: `¿Editar valores de "Consola de sucesos comunes para IBM Tivoli Monitoring"? [ 1=Sí, 2=No ] (el valor predeterminado es 1).`
  5. Escriba 2. Se visualiza la siguiente solicitud: `¿Se conectará este agente a un TEMS? [1=SÍ, 2=NO] (el valor predeterminado es 1).`
  6. Acepte los valores predeterminados de esta solicitud y las solicitudes que le sigan hasta que vea la solicitud acerca de la configuración del proveedor de datos de panel de instrumentos. Si no está habilitado, seleccione el valor 1 para habilitarlo.
  7. A continuación, se le pregunta si desea especificar un valor de sustitución de dominio. Escriba 1 para Sí y 2 para No.

     Cuando el proveedor de datos de panel de instrumentos está habilitado, puede especificar un valor de sustitución de dominio. Este valor es opcional. Cambia el ID del proveedor de datos de panel de instrumentos y el nombre de dominio para políticas de autorización de `itm.<nombre_servidor_supervisión_concentrador>` por `itm.<valor_sustitución_dominio>`. El valor no puede superar los 124 caracteres. Debe configurar un valor de sustitución de dominio para estos casos:

     – Se utiliza la característica de alta disponibilidad de Espera activa para el servidor de supervisión concentrador. Al configurar un valor de sustitución de dominio, el ID del proveedor de datos de panel de instrumentos y el nombre de dominio no cambiarán cuando el servidor de portal se configure para conectarse al nuevo servidor de supervisión concentrador activo. Si no configura un valor de sustitución de dominio en este escenario, debe volver a configurar la conexión entre IBM

Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos, así como actualizar cualquier política de autorización específica de dominio cuando el servidor de portal se configure para conectarse al nuevo servidor de supervisión concentrador activo.

– Tiene varios servidores de supervisión concentradores que utilizan un conjunto común de políticas de autorización para controlar el acceso del panel de control y desea crear algunas políticas de autorización específicas de dominio. Debe especificar un valor de sustitución de dominio para este escenario si desea utilizar, en las políticas de autorización, un nombre de dominio más descriptivo que el valor predeterminado de `itm.<nombre_servidor_supervisión_concentrador>`.

Si modifica la sustitución del dominio después de configurar una conexión en Dashboard Application Services Hub para el proveedor de datos de panel de instrumentos, debe suprimir la conexión y volverla a añadir. Consulte "Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring" en la página 52 para obtener detalles sobre cómo configurar una conexión de proveedor de datos de panel de instrumentos. Además, si ha creado alguna política de autorización específica de dominio utilizando el nombre de dominio predeterminado, debe suprimir los permisos que utilizan el nombre de dominio anterior y crear nuevos permisos que utilicen el nombre de dominio nuevo cuando cambie el valor de sustitución de dominio.

8. Si el proveedor de datos de panel de instrumentos está habilitado, se le solicitará si desea habilitar políticas de autorización. Utilice la información incluida en Tabla 21 en la página 201.

   Solo se deben habilitar políticas de autorización si se está configurando un entorno de paneles de control con inicio de sesión único, tiene la intención de utilizar políticas de autorización para controlar el acceso a los paneles de control de supervisión y los administradores ya han creado el conjunto inicial de políticas de acceso de usuario del panel de control.

9. Después de que el mandato haya completado la configuración, aparece el siguiente mensaje: `Ha finalizado la configuración del agente` y se le preguntará si desea reiniciar el servidor de portal. Seleccione 1 para reiniciarlo.

Resultados

Ha habilitado satisfactoriamente las políticas de autorización en el servidor de portal.

Después de haber reciclado el Tivoli Enterprise Portal Server con el recuadro **Habilitar de autorización de políticas** seleccionado, el proveedor de datos de panel de instrumentos empezará a hacer llamadas de autorización al almacén de políticas local para permitir o excluir el acceso del grupo de sistemas gestionados y el sistema gestionado para usuarios del panel de control.

Si los usuarios del panel de control no ven ningún recurso supervisado en los paneles de control o no ven el conjunto correcto de recursos, consulte *IBM Tivoli Monitoring Troubleshooting Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/trouble/itm_trouble.htm) para conocer los pasos para diagnosticar este problema.

Auditoría de la política de autorización

El Servidor de políticas de autorización genera mensajes de auditoría cuando un usuario ejecuta uno de los siguientes mandatos tivcmd que modifican las políticas de autorización: addtorole, copyrole, createrole, deleterole, exclude, grant, removefromrole y revoke. También se genera un mensaje de auditoría si un usuario intenta ejecutar un mandato tivcmd que no está autorizado a utilizar.

Por ejemplo, un mensaje de auditoría se genera si un usuario ejecuta el mandato **tivcmd createrole**, pero no está asignado a un rol con permiso para crear roles.

Los mensajes de auditoría utilizan el formato de registro de auditoría del IBM Tivoli Monitoring y se graban en los archivos de registro de auditoría en el sistema en el que el Servidor de políticas de autorización está instalado. La ubicación predeterminada es `<dir_instalación_JazzSM>/AuthPolicyServer/PolicyServer/audit`. Durante la instalación del Servidor de políticas de autorización, puede personalizar la ubicación del directorio de archivos de registro de auditoría, el tamaño máximo de los archivos de registro de auditoría y el número máximo de archivos de registro de auditoría que se van a mantener a la vez. Después de la instalación, puede cambiar estos parámetros siguiendo las instrucciones de "Cambio de las propiedades de configuración del Servidor de políticas de autorización después de la instalación y la configuración". Puesto que el Servidor de políticas de autorización no está asociado con un agente de supervisión, sus mensajes de auditoría no se pueden ver en Tivoli Enterprise Portal ni guardar en Tivoli Data Warehouse. Además, no puede grabar situaciones en los mensajes de auditoría. En su lugar, debe visualizar los archivos de registro de auditoría si desea ver los mensajes de auditoría.

Los mensajes de auditoría para la imposición de la política de autorización se generan por el componente del proveedor de datos de panel de instrumentos del Tivoli Enterprise Portal Server. El proveedor de datos de panel de instrumentos genera un mensaje de auditoría si un usuario solicita datos del grupo de atributos o sucesos de situación para un grupo de sistemas gestionados o el sistema gestionado para los que no tienen permiso de vista. Los mensajes de auditoría también se generan cuando las políticas de autorización se descargan desde el Servidor de políticas de autorización y cuando las políticas no se pueden recuperar. Puesto que el proveedor de datos de panel de instrumentos es un componente del sistema gestionado del servidor de portal, estos mensajes de auditoría pueden verse desde el cliente de Tivoli Enterprise Portal y guardarse en Tivoli Data Warehouse.

Para obtener más detalles sobre la auditoría, incluyendo cómo ver los mensajes de auditoría para el servidor de portal y el formato de registro de auditoría, consulte Capítulo 9, "Registro de auditoría", en la página 243.

Cambio de las propiedades de configuración del Servidor de políticas de autorización después de la instalación y la configuración

Después de instalar y configurar el paquete del Servidor de políticas de autorización de Tivoli, puede cambiar los parámetros de configuración del Servidor de políticas de autorización para el registro de auditoría y la política de distribución.

Antes de empezar

Propiedades de la auditoría
Puede modificar las propiedades que especifican la ubicación de los archivos de registro de auditoría del Servidor de políticas de autorización, el tamaño máximo de un archivo de registro de auditoría y el número máximo de archivos de registro de auditoría que se van a mantener a la vez.

Propiedades de la distribución de políticas
El Servidor de políticas de autorización comprime periódicamente un archivo con el conjunto actual de las políticas de autorización que está disponible para la distribución. En un intervalo periódico, el componente de proveedor de datos de panel de instrumentos del servidor de portal realiza una solicitud al Servidor de políticas de autorización del último archivo de políticas comprimido. Si hay un nuevo archivo, se obtiene y extrae, y este conjunto de políticas se convierte en el conjunto actual de políticas que se utilizan por el proveedor de datos de panel de instrumentos. Puede modificar las propiedades que especifican el directorio donde las políticas de autorización se guardan para la distribución y con qué frecuencia las políticas de autorización actuales se copian en este directorio.

Acerca de esta tarea

Puede utilizar la consola de administrador de WebSphere Application Server en Dashboard Application Services Hub donde el Servidor de políticas de autorización está instalado para cambiar las propiedades de configuración del servidor de políticas. Después de cualquier cambio realizado, debe reiniciar WebSphere Application Server para que Dashboard Application Services Hub recoja los cambios en las propiedades.

Realice los pasos siguientes para cambiar las propiedades de configuración para el registro de auditoría y la política de distribución:

Procedimiento

1. Inicie sesión en la consola administrativa de WebSphere de Dashboard Application Services Hub donde el Servidor de políticas de autorización está instalado.
   a. En un navegador, abra la consola de Dashboard Application Services Hub. De forma predeterminada, el URL es `https://hostname:16311/ibm/console`.

      Si el entorno se ha configurado con un número de puerto distinto del correspondiente al valor predeterminado, especifique ese número en su lugar. La vía de acceso predeterminada al servidor es `/ibm/console`. Sin embargo, esta vía de acceso se puede configurar y puede diferir del valor predeterminado en el entorno.
   b. Escriba un nombre de usuario y contraseña y pulse **Ir**. El nombre de usuario debe tener asignados los roles `administrador` e `iscadmins` de Dashboard Application Services Hub .
   c. Pulse el icono **Valores de consola** y seleccione **Consola administrativa de WebSphere**.
   d. Pulse **Iniciar consola administrativa de WebSphere**.
2. Vaya a la página que contiene las propiedades de configuración para el registro de auditoría y la distribución de políticas.
   a. Pulse **Recursos → Entorno de recursos → Entradas de entorno de recursos**.

b. En la página que se abre, pulse el enlace **AuthzResourceReference**.
c. En la página que se abre, bajo **Propiedades adicionales**, pulse **Propiedades personalizadas**.
d. Se visualiza una tabla con las propiedades siguientes:

AUDIT_COUNT
El número máximo de archivos de registro de auditoría que se van a mantener a la vez. El valor predeterminado es 5. El rango es mayor que 1 y menor que 99999.

AUDIT_FILE_SIZE
El tamaño máximo de cada archivo de registro en megabytes.

AUDIT_ROOT_DIRECTORY
El directorio en el que se almacenan los archivos de registro de auditoría.

El valor predeterminado es `<DIR_INSTALACIÓN_JAZZSM>\AuthPolicyServer\PolicyServer\audit`

DIST_POLL_INTERVAL
Esta propiedad especifica la frecuencia con la que el Servidor de políticas de autorización actualiza el archivo comprimido que contiene las políticas de autorización que el proveedor de datos de panel de instrumentos descarga.

El valor predeterminado es 5. El rango es de 1 a 1440 minutos.

DIST_ROOT_DIRECTORY
El directorio en el que se almacena la versión de las políticas para la distribución.

El valor predeterminado es `<DIR_INSTALACIÓN_JAZZSM>\AuthPolicyServer\PolicyServer\dist`

SEED_ROOT_DIRECTORY
El directorio de inicio del almacén de políticas. No debe modificar esta propiedad.

XACML_ROOT_DIRECTORY
El directorio raíz del almacén de políticas. No debe modificar esta propiedad.

3. Modifique el valor de una propiedad.
   a. Pulse un enlace de nombre de propiedad en la tabla de propiedades personalizadas, por ejemplo, **AUDIT_COUNT**.
   b. En la página que se abre, modifique el campo **Valor** según sea necesario.
   c. Pulse **Aceptar**.
   d. Repita estos pasos para cada propiedad que se deba cambiar.
4. Guarde los cambios.
   a. En el recuadro de mensaje que se abre después de cambiar la primera propiedad, pulse **Guardar**.
   b. Finalice la sesión de la consola administrativa de WebSphere.
   c. Recicle WebSphere Application Server de Dashboard Application Services Hub.

Gestión del almacén de políticas de autorización

El Servidor de políticas de autorización de Tivoli almacena las políticas en varios archivos en el sistema de archivos. Revise los detalles de más abajo para comprender la forma de gestionar el almacén de políticas.

Alta disponibilidad

El Servidor de políticas de autorización no tiene mecanismos de alta disponibilidad incorporados y no está soportado cuando Dashboard Application Services Hub está configurado para el equilibrio de carga.

Debido a que el servidor de portal tiene su propia copia de las políticas de autorización, puede imponer las políticas, incluso si el Servidor de políticas de autorización no está disponible. Puede configurar la cantidad máxima de tiempo que el servidor de portal puede utilizar su almacén de políticas local después de la última actualización. Si el Servidor de políticas de autorización no se puede acceder durante el intervalo de tiempo especificado por este parámetro, todas las solicitudes subsiguientes para datos de panel de control fallarán con un error de autorización hasta que el Servidor de políticas de autorización esté disponible de nuevo. El valor predeterminado es de 7 días.

Migración y copia de seguridad

El Servidor de políticas de autorización no ofrece herramientas para la migración, copia de seguridad o exportación e importación para el almacén de archivos de políticas. Con el paso del tiempo, puede crear muchas definiciones de política. Si el almacén de políticas se daña o suprime accidentalmente, volver a crear las definiciones de políticas no sería fácil.

La práctica recomendada es que implemente copias de seguridad periódicas, que pueden hacerse con programas de utilidad zip o tar. Los archivos que contienen el almacén de políticas se mantienen en el subdirectorio `/xacml` bajo el directorio donde el Servidor de políticas de autorización está instalado. Por ejemplo, supongamos que ha instalado el Servidor de políticas de autorización en el directorio siguiente en Windows: `C:\Archivos de programas\IBM\JazzSM\AuthPolicyServer`. Al comprimir todos los archivos en el directorio `C:\Archivos de programa\IBM\JazzSM\AuthPolicyServer\PolicyServer\xacml` se hace una copia de seguridad de todo el almacén de políticas. Posteriormente puede utilizar este archivo zip como ayuda para la migración, por ejemplo, desde un Servidor de políticas de autorización de prueba a producción. Al descomprimir el archivo en un sistema de producción nuevo creará y llenará el subdirectorio `/xacml` con todos los roles de la política y los permisos que previamente había definido en el sistema de prueba. Estos archivos descomprimidos se pueden utilizar tal cual por el Servidor de políticas de autorización de producción.

Utilización de varios dominios

Puede utilizar el Servidor de políticas de autorización para gestionar políticas para varios entornos de servidor de supervisión concentrador, también denominados dominios.

Un *dominio* se define como una colección de componentes de IBM Tivoli Monitoring tales como servidores de portal, servidores de supervisión, agentes de supervisión y agentes de Proxy de almacén que se centren en torno a un determinado servidor de supervisión de hub. Cada dominio tiene su propio espacio de nombres para situaciones, actuaciones, nombres de sistemas

gestionados, grupos de sistemas gestionados, consultas, políticas de flujo de trabajo y cualquier otro objeto de IBM Tivoli Monitoring.

Una política de autorización que se crea sin especificar un nombre de dominio (o con el nombre de dominio 'any') se aplica en todos los dominios de IBM Tivoli Monitoring que el Servidor de políticas de autorización gestiona. Los nombres de dominio son los mismos que el ID del proveedor de datos de panel de instrumentos y están en el formato `itm.`*`nombre_servidor_supervisión_concentrador`*. Puede crear una serie más descriptiva para utilizarla en lugar del nombre de servidor de supervisión concentrador al configurar el servidor de portal y habilitar el proveedor de datos de panel de instrumentos.

Para listar los dominios, utilice el mandato **tivcmd listdomains**. Por ejemplo:

```
tivcmd listdomains
itm.HUB_DOMAIN1
itm.HUB_DOMAIN2
itm.HUB_DOMAIN3
```

El mandato **tivcmd listdomains** devuelve la lista de proveedores de datos de panel de control para los que se ha definido una conexión en Dashboard Application Services Hub donde está instalado el Servidor de políticas de autorización. El mandato también devuelve los nombres de dominio que se han especificado al crear un permiso. Normalmente, hay una única conexión de proveedor de datos de panel de instrumentos definida por Dashboard Application Services Hub.

Para determinar los nombres de concentrador para cada uno de los dominios, utilice uno de los métodos siguientes:

- Ejecute el mandato **tacmd listsystems** en cada servidor de supervisión concentrador para determinar el nombre del sistema del servidor de supervisión concentrador gestionado. Los servidores de supervisión utilizan el código de producto `EM`.
- De forma alternativa, puede iniciar sesión en Dashboard Application Services Hub para cada dominio y visualizar la información de conexión del proveedor de datos de panel de instrumentos. En un entorno típico, puede ver que el ID de proveedor se ha establecido en `ITMSD` en lugar del nombre de concentrador. Sin embargo, el nombre de conexión es el nombre del concentrador si no se ha personalizado cuando se ha creado la conexión.

Una vez que se conoce el nombre del servidor de supervisión concentrador, el nombre de dominio es `itm.`*`nombre_servidor_supervisión_concentrador`*, por ejemplo `itm.HUB_server1`.

Escenarios de despliegue

Los escenarios de despliegue de este tema pueden ayudarle a tomar decisiones en su entorno.

Varios dominios con roles y políticas de autorización compartidos

Este caso de ejemplo de despliegue utiliza estrategias similares para la gestión y configuración de usuarios que el despliegue de un único dominio, pero con la posibilidad añadida de apuntar a las políticas de autorización para determinados dominios de IBM Tivoli Monitoring.

Este caso de ejemplo de despliegue es útil si desea compartir la misma infraestructura de administración de políticas de autorización para un conjunto de dominios. Le permite crear un conjunto de políticas de autorización comunes para todos los dominios, así como políticas que son específicas de uno o varios dominios. Cuando se otorga o excluye un permiso para un rol, se especifica si la política se aplica a todos los dominios o a un dominio específico. Si no especifica un nombre de dominio con los mandatos **tivcmd grant**, **tivcmd exclude** o **tivcmd revoke**, la política se aplica a todos los dominios. Para crear una política específica del dominio, utilice el argumento `--domain` con estos mandatos. Para obtener más información sobre los mandatos de CLI tivcmd, consulte *IBM Tivoli Monitoring: Consulta de mandatos*.

Preparación para el despliegue

La tabla siguiente describe lo que necesita para este despliegue:

Tabla 22. Varios dominios con roles y requisitos de despliegue de políticas compartidos

Cantidad	Componente	Descripción
1 por dominio **Nota:** Si se utiliza el equilibrio de carga, puede haber varios concentradores de servicios de paneles de control por dominio.	Dashboard Application Services Hub	Las aplicaciones de paneles de control como los Infrastructure Management Dashboards for Servers también se instalan con el concentrador de servicios de paneles de control de cada dominio.
1	Tivoli Servidor de políticas de autorización	El Servidor de políticas de autorización puede instalarse con Dashboard Application Services Hub para uno de los dominios o puede instalar una instancia de Dashboard Application Services Hub que se utilice únicamente para la administración de políticas de autorización y que no tenga ninguna aplicación de panel de control instalada.
1 por dominio	Concentrador Tivoli Enterprise Monitoring Server	Si se utiliza la modalidad de Espera activa, puede haber dos servidores de supervisión concentrador por dominio. Cada servidor de supervisión concentrador puede tener varios servidores de supervisión remotos conectados a él. Los agentes de supervisión están conectados a los servidores de supervisión.
1 por dominio	Tivoli Enterprise Portal Server	Cada servidor de portal está configurado para recuperar políticas de autorización del mismo Servidor de políticas de autorización, ya que existe un servidor de políticas compartido por todos los dominios.

Tabla 22. Varios dominios con roles y requisitos de despliegue de políticas compartidos (continuación)

Cantidad	Componente	Descripción
1 o más	Registro de usuarios LDAP	Configure todos los servidores de portal y cada Dashboard Application Services Hub para utilizar el mismo conjunto de registros de usuarios LDAP con el fin de compartir políticas de autorización.

Varios dominios con políticas de autorización independientes

Si piensa no tener ninguna política de autorización común entre los dominios y también tiene la intención de tener un conjunto separado de administradores de políticas de autorización por dominio, instale un Servidor de políticas de autorización con Dashboard Application Services Hub en cada dominio y gestione las políticas de autorización de forma independiente.

En este caso, no utilice el argumento `--domain` porque cada Servidor de políticas de autorización solo gestiona políticas para un único dominio.

Creación de políticas para dominios específicos de IBM Tivoli Monitoring

En un despliegue de varios dominios, el método recomendado consiste en crear políticas para los usuarios a través de roles que diferencian el acceso por el dominio.

Las políticas que se utilizan para determinados dominios de IBM Tivoli Monitoring deben tener el permiso siguiente:

Definición de permiso de sistema gestionado o grupo de sistemas gestionados	
Parámetro	**Valor**
Dominio	'any' o un nombre de dominio específico **Nota:** Si se especifica el valor 'any' o se omite el parámetro de dominio, indica que el permiso se aplica a todos los dominios.
Operación	'view'
Tipo de objeto	'attributegroup', 'event'
Tipo de recurso	'managedsystemgroup', 'managedsystem'
Recurso	*nombre_sistema_gestionado* o *nombre_grupo_sistemas_gestionados*

Ejemplo: Creación de políticas comunes y políticas específicas de dominio

Este ejemplo muestra cómo otorgar a un usuario acceso a todos los agentes del sistema operativo UNIX de un determinado dominio, pero no los de otro dominio. El grupo de sistemas gestionados *ALL_UNIX se crea automáticamente y se gestiona por cada servidor de supervisión concentrador. Además, se otorga a un administrador el acceso a todos los sistemas del sistema operativo UNIX en todos los dominios.

Los siguientes grupos de sistemas gestionados se utilizan en este ejemplo:

Grupos de sistemas gestionados		
Tipo	**Dominio**	**Nombre**
gruposistemasgestionados	itm.eastcoast	*ALL_UNIX
gruposistemasgestionados	itm.westcoast	*ALL_UNIX

Los roles siguientes se utilizan en este ejemplo:

- EastCoastOperators
- WestCoastOperators
- SuperAdministrator

1. Defina un usuario en LDAP, por ejemplo `uid=John,cn=itm,o=ibm` y defina un grupo en LDAP, por ejemplo `cn=EastCoastMachineUsers,cn=itm,o=ibm` y, a continuación, añada el ID de usuario al grupo en LDAP.
2. Defina un usuario en LDAP, por ejemplo `uid=Jane,cn=itm,o=ibm` y defina un grupo en LDAP, por ejemplo `cn=WestCoastMachineUsers,cn=itm,o=ibm` y, a continuación, añada el ID de usuario al grupo en LDAP.
3. Defina un usuario en LDAP, por ejemplo `uid=Joe,cn=itm,o=ibm` y defina un grupo en LDAP, por ejemplo `cn=SuperAdministratorUsers,cn=itm,o=ibm` y, a continuación, añada el ID de usuario al grupo en LDAP.
4. Cree roles nuevos:

```
tivcmd createrole --rolename EastCoastOperators --description
"East Coast users with permission to access the east coast machine
ITM Domain"

tivcmd createrole --rolename WestCoastOperators --description
"West Coast users with permission to access the west  coast machines
for the itm.westcoast domain"

tivcmd createrole --rolename SuperAdministrator --description
"Users with permission to access machines from all domains"
```

5. Otorgue acceso al grupo de atributos y sucesos al grupo de sistemas gestionados *ALL_UNIX para el dominio itm.eastcoast al rol EastCoastOperators:

```
tivcmd grant --rolename EastCoastOperators --resourcetype
managedsystemgroup --resources "*ALL_UNIX"
--objecttype attributegroup --operations view --domain itm.eastcoast

tivcmd grant --rolename EastCoastOperators --resourcetype
managedsystemgroup --resources "*ALL_UNIX"
--objecttype event --operations view --domain itm.eastcoast
```

6. Otorgue acceso al grupo de atributos y sucesos al grupo de sistemas gestionados *ALL_UNIX para el dominio itm.westcoast al rol WestCoastOperators:

```
tivcmd grant --rolename WestCoastOperators --resourcetype
managedsystemgroup --resources "*ALL_UNIX" --objecttype
attributegroup --operations view --domain itm.westcoast

tivcmd grant --rolename WestCoastOperators --resourcetype
managedsystemgroup --resources "*ALL_UNIX" --objecttype event
--operations view --domain itm.westcoast
```

7. Otorgue acceso al grupo de atributos y sucesos al grupo de sistemas gestionados *ALL_UNIX para todos los dominios al rol SuperAdministrator:

```
tivcmd grant --rolename SuperAdministrator --resourcetype
managedsystemgroup --resources "*ALL_UNIX"
--objecttype attributegroup --operations view  --domain any
```

```
tivcmd grant --rolename SuperAdministrator --resourcetype
managedsystemgroup --resources "*ALL_UNIX"
--objecttype event --operations view --domain any
```

8. Asigne los grupos de usuarios a los roles nuevos:

```
tivcmd addtorole --rolename EastCoastOperators --groups
cn=EastCoastMachineUsers,cn=itm,o=ibm

tivcmd addtorole --rolename WestCoastOperators --groups
cn=WestCoastMachineUsers,cn=itm,o=ibm

tivcmd addtorole --rolename SuperAdministrator --groups
cn=SuperAdministrator,cn=itm,o=ibm
```

Cuando un usuario del grupo EastCoastOperators accede a la página Paneles del servidor en Dashboard Application Services Hub para el dominio itm.eastcoast, ve el grupo de sistemas gestionados *ALL_UNIX y sus miembros para este dominio. Si el mismo usuario inicia sesión en Dashboard Application Services Hub para el dominio itm.westcoast, no ve el grupo de sistemas gestionados *ALL_UNIX.

Cuando un usuario del grupo WestCoastOperators accede a la página Paneles del servidor en Dashboard Application Services Hub para el dominio itm.westcoast, ven el grupo de sistemas gestionados *ALL_UNIX y sus miembros para este dominio. Si el mismo usuario inicia sesión en Dashboard Application Services Hub para el dominio itm.eastcoast, no ve el grupo de sistemas gestionados *ALL_UNIX.

Cuando un usuario del grupo SuperAdministrator accede a la página Paneles del servidor en Dashboard Application Services Hub para el dominio, ve el grupo de sistemas gestionados *ALL_UNIX y sus miembros para el dominio conectado al servidor de paneles de control.

Ejemplo: Creación de políticas de autorización para grupos de sistemas gestionados comunes

Si tiene los mismos nombres de grupos de sistemas gestionados en varios dominios y desea que los usuarios de paneles de control vean los datos de los grupos de sistemas gestionados para todos los dominios, cree un rol y otorgue permisos, tal como se muestra en los mandatos de ejemplo siguiente:

```
tivcmd createrole --rolename  WindowsDataCenterOperators

tivcmd grant --rolename WindowsDataCenterOperators  --operations view
--objecttype attributegroup  --resources DataCenterServers
--resourcetype managedsystemgroup

tivcmd grant --rolename WindowsDataCenterOperators  --operations view
--objecttype event   --resources DataCenterServers
--resourcetype managedsystemgroup
```

Debido a que el argumento `--domain` no se ha especificado en el mandato de ejemplo anterior, la política de autorización se aplica a todos los dominios. Como resultado, cualquier usuario o grupo de usuarios asignado al rol WindowsAdministrators puede ver los datos del grupo de sistemas gestionados DataCenterServers en todos los dominios.

Ejemplo: Utilización de un rol común para gestionar recursos específicos de dominio

Si no tiene los mismos nombres de grupo de sistemas gestionados en varios dominios, pero tiene usuarios o grupos de usuarios que realizan el mismo rol para

varios dominios, puede crear un rol común con permisos específicos de dominio, como se muestra en los mandatos de ejemplo siguientes:

```
tivcmd createrole --rolename  LinuxRegionalOperators

tivcmd grant --rolename LinuxRegionalOperators  --operations view
--objecttype attributegroup  --resources SeattleServers
--resourcetype managedsystemgroup --domain itm.HUB_west

tivcmd grant --rolename LinuxRegionalOperators  --operations view
--objecttype event   --resources SeattleServers
--resourcetype managedsystemgroup  --domain itm.HUB_west

tivcmd grant --rolename LinuxRegionalOperators  --operations view
--objecttype attributegroup  --resources BostonServers
--resourcetype managedsystemgroup --domain itm.HUB_east

tivcmd grant --rolename LinuxRegionalOperators  --operations view
--objecttype event   --resources AustinServers
--resourcetype managedsystemgroup  --domain itm.HUB_east
```

En este caso, cualquier usuario o grupo de usuarios asignado al rol LinuxRegionalOperators puede ver datos del grupo de sistemas gestionados SeattleServers cuando inician sesión en Dashboard Application Services Hub para el dominio itm.HUB_west y pueden ver los datos del grupo de sistemas gestionados BostonServers cuando inician sesión en Dashboard Application Services Hub para el dominio itm.HUB_east.

Ejemplo: Creación de una política de autorización específica de dominio

Para los roles que no son comunes entre los dominios, puede crear un rol que solo tenga permisos para un único dominio tal como se muestra en los mandatos de ejemplo siguientes:

```
tivcmd createrole --rolename  ChicagoDataCenterOperators

tivcmd grant --rolename ChicagoDataCenterOperators   --operations view
--objecttype attributegroup  --resources ChicagoServers
--resourcetype managedsystemgroup --domain itm.HUB_midwest

tivcmd grant --rolename ChicagoDataCenterOperators   --operations view
--objecttype event   --resources ChicagoServers
--resourcetype managedsystemgroup  --domain itm.HUB_midwest
```

En este caso, un usuario o grupo de usuarios asignados al rol ChicagoDataCenterOperators solo pueden ver los datos de un grupo de sistemas gestionados en un único dominio.

Capítulo 8. Protección de las comunicaciones

Para proteger la comunicación entre el Tivoli Enterprise Monitoring Agent, el Tivoli Enterprise Monitoring Server y el Tivoli Enterprise Portal Server, utilice SPIPE como protocolo al configurar las comunicaciones entre el servidor de portal y el servidor de supervisión concentrador, entre servidores de supervisión concentrador y remoto, y entre los agentes de supervisión y los servidores de supervisión.

Dos protocolos adicionales se utilizan para proteger la comunicación entre clientes de Tivoli Enterprise Portal y el servidor de portal:

- Secure Hypertext Transport Protocol (HTTPS) para recuperar archivos e Interoperable Object Reference (IOR)
- Internet Inter-ORB Protocol (IIOP) para proteger las comunicaciones entre el servidor de portal y el cliente

Nota: De forma predeterminada, se utilizan ambos protocolos. Sin embargo, puede configurar un cliente de portal para que solo utilice HTTPS para comunicarse con el servidor de portal.

HTTPS también se puede utilizar para proteger la comunicación entre estos componentes:

- Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring
- La interfaz de línea de mandatos tacmd y el concentrador de Tivoli Enterprise Monitoring Server
- La Interfaz de línea de mandatos tivcmd para la política de autorización y Dashboard Application Services Hub donde el Servidor de políticas de autorización de Tivoli está instalado
- El proveedor de servicios Open Services Lifecycle Collaboration Performance Monitoring y clientes de Registry Services, Security Services y OSLC
- Tivoli Integrated Portal y el servicio de representación gráfica IBM Tivoli Monitoring el servidor de portal

Además, estos tipos de comunicaciones seguras también están soportadas:

- Utilización de TLS/SSL para proteger la comunicación entre el servidor de supervisión concentrador y un servidor LDAP
- Utilización de TLS/SSL para proteger la comunicación entre el servidor de portal y un servidor LDAP
- Utilización de TLS/SSL para proteger la comunicación entre un agente de supervisión e IBM IBM Tivoli Netcool/OMNIbus Probe for Tivoli EIF Versión 12 o posterior

Además de elegir un protocolo como IP.SPIPE o HTTPS que da soporte a las comunicaciones seguras, debe configurar el cifrado asimétrico de TLS/SSL mediante el uso de archivos de claves pública-privada, que implica realizar las tareas siguientes:

- Utilización de una base de datos de claves
- Solicitud de un nuevo par de claves pública-privada si no desea utilizar el certificado autofirmado enviado con el producto

© Copyright IBM Corp. 2005, 2013

- Adición de un certificado de firmante de entidad emisora de certificados y un certificado digital firmado a la base de datos de claves si no desea utilizar los certificados autofirmados enviados con el producto
- Adición de los certificados de firmante para las aplicaciones que a las que los componentes de IBM Tivoli Monitoring envían solicitudes
- Habilitación de componentes para realizar la autenticación de certificados

Nota: La solicitud de nuevos certificados es la práctica recomendada, pero también puede utilizar los certificados autofirmados enviados con el producto en un entorno de prueba para familiarizarse con los procedimientos para configurar comunicaciones seguras.

IBM Tivoli Monitoring proporciona dos aplicaciones que se utilizan para trabajar con claves y almacenes de certificados al configurar comunicaciones seguras:

- El programa Global Security Toolkit (GSKit) se instala con los componentes de IBM Tivoli Monitoring en plataformas distribuidas. Incluye el programa de utilidad iKeyman y una interfaz de línea de mandatos para trabajar con certificados y claves.
- La consola de administración de los servicios ampliados (TEPS/e) del Tivoli Enterprise Portal Server extended (también denominada ISCLite) se utiliza con el servidor de portal para asegurar las comunicaciones para los servicios que se ejecutan en TEPS/e.

Se proporcionan un certificado autofirmado predeterminado y una clave al instalar IBM Tivoli Monitoring. Si prefiere utilizar un certificado firmado de entidad emisora de certificados, utilice los programas de utilidad GSKit para crear una solicitud de certificado y, a continuación, crear una base de datos de claves e importar los certificados. Un archivo de ocultación proporciona la contraseña de base de datos de claves para la operación desatendida. Cuando GSKit se instala con un componente de IBM Tivoli Monitoring, los nombres de archivo de claves se especifican utilizando las siguientes variables de entorno:

- KDEBE_KEYRING_FILE=C:\IBM\ITM\keyfiles\keyfile.kdb
- KDEBE_KEYRING_STASH=C:\IBM\ITM\keyfiles\keyfile.sth
- KDEBE_KEY_LABEL=IBM_Tivoli_Monitoring_Certificate

Trabaje con los administradores de los otros productos con los que IBM Tivoli Monitoring se comunica para configurar comunicaciones seguras. Si está utilizando cualquiera de los componentes de Jazz for Service Management (Dashboard Application Services Hub, Registry Services o Servicios de seguridad) con IBM Tivoli Monitoring, utilice la consola de administración de WebSphere Application Server para trabajar con sus almacenes de confianza y certificados.

La tabla siguiente lista los flujos de comunicaciones que pueden protegerse y dónde encontrar información sobre cómo proteger la interacción.

Nota: A menos que se indique lo contrario, las tareas siguientes se utilizan para configurar TLS/SSL y la autenticación de certificados del servidor. Cuando se utiliza la autenticación de certificados del servidor, el cliente (el origen de la solicitud) autentica el certificado que recibe del servidor (el destino de la solicitud).

Tabla 23. Tareas para asegurar la comunicación

Tarea para asegurar la comunicación	Dónde encontrar información
Utilice TLS/SSL entre los clientes de Tivoli Enterprise Portal el servidor de portal.	Consulte "Utilización de SSL entre el servidor y el cliente de portal" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.
Utilice IP.SPIPE con la validación de certificados para asegurar la comunicación para estas interacciones: • comunicación de concentrador y servidor de supervisión remoto • comunicación de servidor de supervisión concentrador y servidor de portal • comunicación de servidor de supervisión y agente de supervisión Utilice HTTPS con la validación de certificados para asegurar las comunicaciones para estas interacciones: • comunicación de la CLI tacmd o el cliente SOAP con el servidor de supervisión concentrador • solicitudes del servidor de supervisión, el servidor de portal y la consola de servicio de agente de supervisión	Consulte ITM Certificate Authentication Configuration Guide for ITM V6.2.2 and later en IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home).
Utilice TLS/SSL entre el servidor de supervisión concentrador y un servidor LDAP.	"Configuración de la comunicación TLS/SSL entre el servidor de supervisión concentrador y el servidor LDAP" en la página 218
Utilice TLS/SSL entre el servidor de portal y un servidor LDAP.	"Configuración de la comunicación TLS/SSL entre el servidor de portal y el servidor LDAP" en la página 116
Utilice TLS/SSL cuando IBM Dashboard Application Services Hub envía solicitudes al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring.	"Configuración de la comunicación TLS/SSL entre Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos" en la página 219
Utilice TLS/SSL cuando el proveedor de datos de panel de instrumentos envía solicitudes para recuperar políticas de autorización del Servidor de políticas de autorización.	"Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización" en la página 223
Utilice TLS/SSL cuando la Interfaz de línea de mandatos tivcmd para la política de autorización envía solicitudes al Servidor de políticas de autorización.	"Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización" en la página 223
Utilice TLS/SSL para enviar sucesos de situación privada desde los agentes de supervisión a IBM Tivoli Netcool/OMNIbus Probe for Tivoli EIF. Para esta interacción, la autenticación de certificado de cliente se configura para que el analizador utilice certificados para autenticar los agentes de supervisión (los clientes).	"Envío de sucesos de situación privada utilizando la comunicación TLS/SSL" en la página 412

Tabla 23. Tareas para asegurar la comunicación (continuación)

Tarea para asegurar la comunicación	Dónde encontrar información
Utilice TLS/SSL cuando Tivoli Business Service Manager o Tivoli Integrated Portal envían solicitudes HTTPS al servicio web de representación gráfica del servidor de portal.	"Integración de Tivoli Business Service Manager y Tivoli Enterprise Portal Server en SSL" de la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.
Habilite el Estándar federal de procesamiento de información (FIPS) para los componentes de IBM Tivoli Monitoring.	"Habilitación de FIPS para IBM Tivoli Monitoring" en la página 230
Después de actualizar el certificado de IBM Tivoli Monitoring, importe los certificados de TEPS/e a la base de datos de archivos de claves del servidor de portal para asegurarse de que el plug-in del servidor web del servidor de portal y TEPS/e pueden continuar comunicándose de forma segura.	"Importación de los certificados de TEPS/e a la base de datos de archivos de claves del servidor de portal" en la página 235

Configuración de la comunicación TLS/SSL entre el servidor de supervisión concentrador y el servidor LDAP

Puede configurar la comunicación TLS/SSL del servidor de supervisión concentrador con un servidor LDAP para asegurar las solicitudes para autenticar los usuarios y grupos.

Después de configurar el servidor LDAP para TLS/SSL y obtener su certificado de firmante público, utilice la interfaz de línea de mandato o el programa de utilidad GSKit iKeyman del servidor de supervisión concentrador para configurar una nueva base de datos de claves de tipo `CMS` y un archivo de ocultación que contiene la contraseña para la base de datos de claves. A continuación, importe el certificado de firmante público del servidor LDAP a la nueva base de datos de claves y especifique un nombre de etiqueta para el certificado. Consulte "Utilización de la interfaz de línea de mandatos de GSKit para trabajar con bases de datos de claves y certificado" en la página 236 y "Utilización del programa de utilidad GSKit iKeyman para trabajar con bases de datos de claves y certificados" en la página 237 para obtener información sobre el uso de GSKit.

A continuación, vuelva a configurar el servidor de supervisión concentrador para habilitar la comunicación TLS/SSL de LDAP. Al volver a configurar el servidor de supervisión concentrador, debe proporcionar la ubicación de la base de datos de claves (también denominado archivo del almacén de claves LDAP), el archivo de ocultación que contiene la base de datos de claves (también denominado ocultación de almacén de claves LDAP), el nombre de etiqueta para el certificado de firmante público y la contraseña de la base de datos de claves. Asimismo, compruebe con el administrador del servidor LDAP para determinar si debe modificar el valor de puerto LDAP ya que el número de puerto seguro es normalmente el puerto `636`.

Nota:

TLS/SSL de LDAP requiere algunas acciones de un administrador de LDAP que no se cubren en la documentación de Tivoli Monitoring. Los temas siguientes de Centro de información de IBM Security Systems incluyen información sobre cómo configurar servidores LDAP para TLS/SSL:

- Configuración de Microsoft Active Directory para el acceso SSL
- Configuración del cliente de Tivoli Directory Server para el acceso SSL

- Configuración de Oracle Java System Directory Server para acceso SSL

Configuración de la comunicación TLS/SSL entre Dashboard Application Services Hub y el proveedor de datos de panel de instrumentos

Si desea utilizar HTTPS, puede configurar la comunicación TLS/SSL de Dashboard Application Services Hub al proveedor de datos de panel de instrumentos en el servidor de portal.

Dashboard Application Services Hub se comunica con IBM Tivoli Monitoring proveedor de datos de panel de instrumentos utilizando el protocolo de transferencia de hipertexto (HTTP) o el protocolo seguro de transferencia de hipertexto (HTTPS). HTTPS está diseñado para ejecutarse en la parte superior de seguridad de la capa de transporte (TLS) o su predecesor, capa de sockets seguros (SSL). Estas capas proporcionan cifrado utilizando intercambios de claves.

Hoja de ruta

Para utilizar HTTPS y sus funciones de cifrado de seguridad, realice las tareas siguientes en la hoja de ruta.

Tabla 24. Hoja de ruta para configurar TLS/SSL para el proveedor de datos de panel de instrumentos

Paso	Descripción e información proporcionada
1	Tiene dos opciones para obtener el par de claves pública-privada utilizada por el servidor de portal: • Utilice los certificados autofirmados predeterminados instalados con IBM Tivoli Monitoring. Si elige esta opción, continúe en el paso 2. O BIEN • Utilice un certificado digital que haya sido firmado por una entidad emisora de certificados. En este caso, debe crear una solicitud de certificado y enviarla a la entidad emisora de certificados para la firma. Una vez que el certificado digital ha sido firmado, puede añadir el certificado del firmante de entidad emisora de certificados a los almacenes de confianza del servidor de portal y, a continuación, añadir la nueva firma digital a los almacenes de claves del servidor de portal. Para obtener más información, consulte "Utilización de certificados firmados de entidad emisora de certificados de terceros para el servidor de portal".
2	En cada Dashboard Application Services Hub con una conexión configurada con el proveedor de datos de panel de instrumentos del servidor de portal, añada el certificado de firmante público utilizado por el servidor de portal al almacén de confianza de Dashboard Application Services Hub WebSphere. Siga los pasos descritos en "Configuración de la comunicación TLS/SSL para el servidor Dashboard Application Services Hub" en la página 222.

Utilización de certificados firmados de entidad emisora de certificados de terceros para el servidor de portal

Puede utilizar certificados de terceros para configurar TLS/SSL para el proveedor de datos de panel de instrumentos añadiendo el certificado de firmante y el certificado digital privado a la base de datos de claves gestionada por GSKit y a los almacenes de confianza y de claves utilizados por TEPS/e.

Antes de empezar

Obtenga el certificado de firmante de la entidad emisora de certificados.

Asegúrese de que la TEPS/e consola de administración está habilitada. Para ver los pasos detallados, incluyendo la información sobre cómo iniciar sesión, consulte "Inicio de la consola de administración de TEPS/e" en la página 111.

Procedimiento

1. Utilice la TEPS/e consola de administración o la interfaz de línea de mandatos GSKit para crear una solicitud de certificado privado para que sea firmado por la entidad emisora de certificados. Las instrucciones siguientes explican cómo realizar este paso utilizando la TEPS/e consola de administración.
   a. Inicie sesión en TEPS/e consola de administración.
   b. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
   c. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultKeyStore**.
   d. En el área Propiedades adicionales, pulse el enlace **Solicitudes de certificados personales** y, en la página que se muestra, pulse **Nueva**.
   e. En la página que aparece, especifique la siguiente información:
      - Establezca **Nombre de archivo** en la ubicación que debe almacenar la solicitud de certificado privado. Por ejemplo, `C:\dashboardcerts\TEPSCertRequest.arm`.
      - Establezca la **Etiqueta de clave** en la etiqueta deseada para el certificado. Por ejemplo, `TEPS Certificate.`
      - Establezca **Tamaño de clave** en `2048`.
      - Deje a **Algoritmo de firma** como `SHA1withRSA`.
      - Establezca **Nombre común** en un nombre exclusivo para el sistema de TEPS/e. Normalmente, se trata de un nombre de host.
      - Establezca a **Organización** en un valor significativo. Normalmente, este es un nombre de compañía.
      - Establezca a **Unidad organizativa** en un nombre significativo. Por ejemplo, `TEPS`.
      - Establezca a **País o región** en el valor deseado. Por ejemplo, `US`.
   f. Pulse **Aceptar** y, a continuación, **Guardar**.
2. Envíe la solicitud de certificado generada anteriormente a la entidad emisora de certificados para solicitar un nuevo certificado digital. La entidad emisora de certificados puede tardar de dos a tres semanas en generar el nuevo certificado digital.
3. Después de que la entidad emisora de certificados devuelva el nuevo certificado digital, guárdelo en una ubicación en el sistema donde el servidor de portal y TEPS/e están instalados. Por ejemplo, `C:\dashboardcerts\TEPSSignedCert.arm`.
4. Utilice la interfaz de línea de mandatos GSKit para crear una nueva base de datos de claves de tipo `CMS` y guarde la contraseña de la base de datos de claves en un archivo de ocultación. A continuación, importe el certificado de firmante de la entidad emisora de certificados y el nuevo certificado digital a la nueva base de datos de claves. El servidor HTTP incluido del servidor de portal utiliza esta base de datos de claves.

5. También debe añadir el certificado de firmante de la entidad emisora de certificados al almacén de confianza de TEPS/e utilizando la TEPS/e consola de administración.
   a. Inicie sesión en TEPS/e consola de administración.
   b. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
   c. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultTrustStore**.
   d. En el área Propiedades adicionales, pulse el enlace **Certificados de firmante** y, en la página que se muestra, pulse **Añadir**.
   e. En la página que aparece, especifique la siguiente información:
      - Establezca **Alias** en la etiqueta deseada para el certificado. Por ejemplo, `TEPS Signer Certificate`.
      - Establezca **Nombre de archivo** en la ubicación del certificado de firmante de la entidad emisora de certificados extraído. Por ejemplo, `C:\dashboardcerts\CASignerCert.arm`.
      - Deje a **Tipo de datos** como **Datos ASCII codificados en Base64**.
   f. Pulse **Aceptar** y, a continuación, **Guardar**.
6. Reciba el certificado digital firmado en el almacén de claves de TEPS/e utilizando la TEPS/e consola de administración.
   a. Inicie sesión en TEPS/e consola de administración.
   b. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
   c. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultKeyStore**.
   d. En el área Propiedades adicionales, pulse el enlace **Certificados personales** y en la página que se muestra, pulse **Recibir de una entidad emisora de certificados**.
   e. En la página que aparece, especifique la siguiente información:
      - Establezca **Nombre de archivo** en la ubicación del certificado digital firmado. Por ejemplo, `C:\dashboardcerts\TEPSSignedCert.arm`.
      - Deje a **Tipo de datos** como **Datos ASCII codificados en Base64**.
   f. Pulse **Aceptar** y, a continuación, **Guardar**.
7. Establezca el nuevo certificado privado como el certificado de servidor predeterminado para TEPS/e.
   a. Inicie sesión en TEPS/e consola de administración.
   b. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
   c. En el área Elementos relacionados, pulse el enlace **Configuraciones de SSL** y, en la tabla, pulse el enlace **NodeDefaultSSLSettings**.
   d. En la página que aparece, pulse **Alias de certificado de servidor predeterminado** y seleccione el certificado firmado de TEPS/e. Por ejemplo, `TEPS Certificate`.
   e. Pulse **Aceptar** y, a continuación, **Guardar**.
   f. Seleccione **Seguridad → Gestión de certificados SSL y claves** de nuevo.
   g. Pulse el enlace **Gestionar configuraciones de seguridad de punto final**.
   h. Pulse el enlace del nombre de nodo que se encuentra en **Entrada → thecellname → nodos**.
   i. Pulse **Alias de certificado en almacén de claves** y seleccione el certificado firmado de TEPS/e. Por ejemplo, `TEPS Certificate`.
   j. Pulse **Aceptar** y, a continuación, **Guardar**.

Configuración de la comunicación TLS/SSL para el servidor Dashboard Application Services Hub

Añada el certificado de firmante público utilizado por el servidor de portal al almacén de confianza de Dashboard Application Services Hub WebSphere para configurar TLS/SSL.

Nota: Si ha solicitado un nuevo certificado digital para el servidor de portal, espere hasta que el certificado se haya recibido antes de realizar este procedimiento.

Procedimiento

1. Inicie sesión en consola administrativa de Dashboard Application Services Hub WebSphere.
   a. Escriba el siguiente URL en el navegador Internet Explorer o Firefox: `https://hostname:16311/ibm/console`.

      Si el entorno se ha configurado con un número de puerto distinto del correspondiente al valor predeterminado, especifique ese número en su lugar. La vía de acceso predeterminada al servidor es `/ibm/console`. Sin embargo, esta vía de acceso se puede configurar y puede diferir del valor predeterminado en el entorno.
   b. Escriba el ID de usuario administrativo y la contraseña de Dashboard Application Services Hub y luego pulse **Ir**.

      El ID de usuario debe tener asignados los roles `administrador` e `iscadmins`.
   c. En el área Valores de consola, pulse **Consola administrativa de WebSphere** y, a continuación, pulse el botón **Iniciar consola administrativa de WebSphere**.
2. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
3. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultTrustStore**.
4. En el área Propiedades adicionales, pulse el enlace **Certificados de firmante** y en la página que se muestra, pulse **Recuperar de puerto**.
5. Entre el nombre de host del servidor de portal.
6. Escriba el puerto `15201`.
7. Entre un nombre de alias, por ejemplo `ITM-TEPS`.
8. Pulse **Recuperar información de firmante**.
9. Pulse **Aceptar** y, a continuación, **Guardar**.

Resultados

Los certificados están configurados para la comunicación entre el servidor de Dashboard Application Services Hub y el servidor de portal y su proveedor de datos de panel de instrumentos.

Vuelva a las instrucciones de la hoja de ruta de Capítulo 3, “Preparación de su entorno de panel de control”, en la página 27 para obtener información sobre cómo reconfigurar la conexión del proveedor de datos de panel de instrumentos para utilizar HTTPS en lugar de HTTP.

Configuración de la comunicación TLS/SSL con el Servidor de políticas de autorización

Si desea utilizar HTTPS, puede configurar la comunicación TLS/SSL con el Servidor de políticas de autorización de Tivoli.

Hay dos componentes de IBM Tivoli Monitoring que se comunican con el Servidor de políticas de autorización utilizando el protocolo de transferencia de hipertexto (HTTP) o protocolo seguro de transferencia de hipertexto (HTTPS):

- La Interfaz de línea de mandatos tivcmd para la política de autorización envía solicitudes HTTP/HTTPS al Servidor de políticas de autorización para procesar mandatos CLI.
- El Tivoli Enterprise Portal Server envía solicitudes HTTP/HTTPS al Servidor de políticas de autorización para obtener el último almacén de políticas.

HTTPS está diseñado para ejecutarse en la parte superior de seguridad de la capa de transporte (TLS) o su predecesor, capa de sockets seguros (SSL). Estas capas proporcionan cifrado utilizando intercambios de claves.

Hoja de ruta

Para utilizar HTTPS y sus funciones de cifrado de seguridad, realice las tareas siguientes en la hoja de ruta.

Nota: Las siguientes instrucciones suponen que el servidor de portal y la CLI tivcmd envían las solicitudes directamente al servidor de aplicaciones de IBM Dashboard Application Services Hub y no a un servidor HTTP que puede utilizarse conjuntamente con el concentrador de panel de control. Si está utilizando un servidor HTTP con IBM Dashboard Application Services Hub, también debe actualizar los certificados que utiliza el servidor HTTP.

Tabla 25. Hoja de ruta para configurar TLS/SSL para el Servidor de políticas de autorización

Paso	Descripción e información proporcionada
1	Utilización de la consola administrativa de WebSphere Application Server para Dashboard Application Services Hub donde el Servidor de políticas de autorización está instalado, puede elegir una de las opciones siguientes para obtener un par de claves pública-privada: • "Utilización de los certificados generados por WebSphere para configurar TLS/SSL para el Servidor de políticas de autorización" en la página 224 Durante la instalación, WebSphere Application Server genera un certificado de firmante público y un certificado firmado privado predeterminado. Estos certificados pueden utilizarse si lo desea. • "Utilización de certificados de terceros para configurar TLS/SSL para el Servidor de políticas de autorización" en la página 225 Añada el certificado de firmante de un tercero al almacén de confianza de WebSphere Application Server. Una solicitud de certificado se crea en WebSphere Application Server y se reenvía a la entidad emisora de certificados para la firma. Una vez firmado, se añade al almacén de claves de WebSphere Application Server. El certificado firmado privado debe establecerse como el certificado predeterminado.

2	En cada instalación de Interfaz de línea de mandatos tivcmd para la política de autorización: 1. Cree una base de datos de claves vacía nueva 2. Añada el certificado de firmante público utilizado por el Servidor de políticas de autorización a la nueva base de datos de claves. 3. Establezca una variable de entorno para habilitar la validación del certificado del servidor. De forma predeterminada, la utilización de HTTPS entre la CLI tivcmd y el Servidor de políticas de autorización no intercambia certificados ni utiliza el cifrado de seguridad. Esta variable de entorno debe establecerse para que esto ocurra. Siga los pasos descritos en "Configuración de la CLI tivcmd para TLS/SSL" en la página 227.
3	En cada servidor de portal configurado para comunicarse con el Servidor de políticas de autorización, añada el certificado de firmante público utilizado por el Servidor de políticas de autorización al almacén de confianza de TEPS/e. Siga los pasos descritos en "Configuración de la comunicación TLS/SSL entre el servidor de portal y el Servidor de políticas de autorización" en la página 229.
4	Utilice el argumento `-s` para el mandato **`tivcmd login`** para indicar que se utiliza el protocolo HTTPS cuando se envían solicitudes al Servidor de políticas de autorización. Si la variable de entorno de la CLI tivcmd `ITM_AUTHENTICATE_SERVER_CERTIFICATE` se establece en `Y`, se produce el intercambio de certificados TLS/SS y los datos de la solicitud de la CLI se cifra.

Utilización de los certificados generados por WebSphere para configurar TLS/SSL para el Servidor de políticas de autorización

Durante la instalación de WebSphere Application Server utilizado por el Servidor de políticas de autorización y Dashboard Application Services Hub, se generan de forma predeterminada un certificado de firmante público y un certificado firmado privada. Puede utilizar estos certificados para la comunicación TLS/SSL extrayendo el certificado de firmante público.

Procedimiento

1. Inicie sesión en la consola administrativa de WebSphere para el Servidor de políticas de autorización y Dashboard Application Services Hub.
   a. Escriba el siguiente URL en el navegador Internet Explorer o Firefox: `https://hostname:16311/ibm/console`.

      Si el entorno se ha configurado con un número de puerto distinto del correspondiente al valor predeterminado, especifique ese número en su lugar. La vía de acceso predeterminada al servidor es `/ibm/console`. Sin embargo, esta vía de acceso se puede configurar y puede diferir del valor predeterminado en el entorno.
   b. Escriba el ID de usuario administrativo y la contraseña de Dashboard Application Services Hub y luego pulse **Ir**.

      El ID de usuario debe tener asignados los roles `administrador` e `iscadmins`.
   c. En el área Valores de consola, pulse **Consola administrativa de WebSphere** y, a continuación, pulse el botón **Iniciar consola administrativa de WebSphere**.
2. Seleccione **Seguridad → Gestión de certificados SSL y claves**.

3. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultTrustStore**.
4. En el área Propiedades adicionales, pulse el enlace **Certificados de firmante** y, en la tabla que se visualiza, seleccione el recuadro de selección de la entrada `root`.
5. Pulse **Extraer** y, en la página que se muestra, en el campo **Nombre de archivo**, especifique un nombre de archivo de certificado. Por ejemplo, `C:\policyauthcerts\PolicyAuthServerSignerCert.arm`.
6. En la lista **Tipo de datos**, seleccione la opción **Datos ASCII codificados en Base64** y pulse **Aceptar**.

Qué hacer a continuación

El certificado de firmante público extraído puede distribuirse ahora al servidor de portal y sistemas de Interfaz de línea de mandatos tivcmd para la política de autorización para la importación.

Utilización de certificados de terceros para configurar TLS/SSL para el Servidor de políticas de autorización

Puede utilizar certificados de terceros para configurar TLS/SSL para el Servidor de políticas de autorización.

Antes de empezar

Muchos de los siguientes pasos requieren que se haya iniciado la sesión en la consola administrativa de WebSphere para el Servidor de políticas de autorización y Dashboard Application Services Hub. Utilice los pasos siguientes para iniciar sesión en la consola:

1. Escriba el siguiente URL en el navegador Internet Explorer o Firefox: `https://hostname:16311/ibm/console`.

   Si el entorno se ha configurado con un número de puerto distinto del correspondiente al valor predeterminado, especifique ese número en su lugar. La vía de acceso predeterminada al servidor es `/ibm/console`. Sin embargo, esta vía de acceso se puede configurar y puede diferir del valor predeterminado en el entorno.
2. Escriba el ID de usuario administrativo y la contraseña de Dashboard Application Services Hub y luego pulse **Ir**.

   El ID de usuario debe tener asignados los roles `administrador` e `iscadmins`.
3. En el área Valores de consola, pulse **Consola administrativa de WebSphere** y, a continuación, pulse el botón **Iniciar consola administrativa de WebSphere**.

Procedimiento

- Añada el certificado de firmante público entidad emisora de certificados al almacén de confianza de WebSphere Application Server.
  1. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
  2. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultTrustStore**.
  3. En el área Propiedades adicionales, pulse el enlace **Certificados de firmante** y, en la página que se muestra, pulse **Añadir**.
  4. En la página que aparece, especifique la siguiente información:
     – Establezca **Alias** en la etiqueta deseada para el certificado. Por ejemplo, `Servidor de políticas de autorización Signer Certificate`.

- Establezca **Nombre de archivo** en la ubicación del certificado de firmante de entidad emisora de certificados. Por ejemplo, `C:\policyauthcerts\CASignerCert.arm`.
- Deje a **Tipo de datos** como **Datos ASCII codificados en Base64**.

5. Pulse **Aceptar** y, a continuación, **Guardar**.

El certificado de firmante de la entidad emisora de certificados se puede ahora distribuir al servidor de portal y sistemas de CLI tivcmd para la importación.

- Cree una solicitud de certificado privado para que sea firmado por la entidad emisora de certificados.
  1. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
  2. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultKeyStore**.
  3. En el área Propiedades adicionales, pulse el enlace **Solicitudes de certificados personales** y, en la página que se muestra, pulse **Nueva**.
  4. En la página que aparece, especifique la siguiente información:
     - Establezca **Nombre de archivo** en la ubicación que debe almacenar la solicitud de certificado privado. Por ejemplo, `C:\policyauthcerts\PolicyAuthServerCertRequest.arm`.
     - Establezca la **Etiqueta de clave** en la etiqueta deseada para el certificado. Por ejemplo, `Servidor de políticas de autorización Certificate.`
     - Deje a **Algoritmo de firma** como **SHA1withRSA**.
     - Establezca al **Tamaño de clave** en 2048.
     - Establezca el **Nombre común** en un nombre exclusivo para el Servidor de políticas de autorización. Normalmente, este es un nombre de sistema.
     - Establezca a **Organización** en un valor significativo. Normalmente, este es un nombre de compañía.
     - Establezca a **Unidad organizativa** en un nombre significativo. Por ejemplo, `PolicyAuth`.
     - Establezca a **País o región** en el valor deseado. Por ejemplo, `US`.
  5. Pulse **Aceptar** y, a continuación, **Guardar**.

  Envíe la solicitud de certificado generada anteriormente a la entidad emisora de certificados para solicitar un nuevo certificado digital. La entidad emisora de certificados puede tardar de dos a tres semanas en generar el nuevo certificado digital.

  Después de que la entidad emisora de certificados devuelva el nuevo certificado digital, guárdelo en una ubicación del sistema del Servidor de políticas de autorización. Por ejemplo, `C:\policyauthcerts\PolicyAuthServerSignedCert.arm`.
- Reciba el certificado digital firmado utilizando la consola administrativa de WebSphere.
  1. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
  2. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultKeyStore**.
  3. En el área Propiedades adicionales, pulse el enlace **Certificados personales** y en la página que se muestra, pulse **Recibir de una entidad emisora de certificados**.
  4. En la página que aparece, especifique la siguiente información:
     - Establezca **Nombre de archivo** en la ubicación del certificado digital firmado. Por ejemplo, `C:\policyauthcerts\PolicyAuthServerSignedCert.arm`.

– Deje a **Tipo de datos** como **Datos ASCII codificados en Base64**.

5. Pulse **Aceptar** y, a continuación, **Guardar**.

- Establezca el nuevo certificado privado como el certificado de servidor predeterminado.
  1. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
  2. En el área Elementos relacionados, pulse el enlace **Configuraciones de SSL** y, en la tabla, pulse el enlace **NodeDefaultSSLSettings**.
  3. En la página que aparece, pulse **Alias de certificado de servidor predeterminado** y elija el certificado de Servidor de políticas de autorización firmado. Por ejemplo, `Certificado del Servidor de políticas de autorización`.
  4. Pulse **Aceptar** y, a continuación, **Guardar**.
  5. Seleccione **Seguridad → Gestión de certificados SSL y claves** de nuevo.
  6. Pulse el enlace **Gestionar configuraciones de seguridad de punto final**.
  7. Pulse el enlace del nombre de nodo que se encuentra en **Entrada → thecellname → nodos**.
  8. Pulse **Alias de certificado en almacén de claves** y elija el certificado de Servidor de políticas de autorización firmado. Por ejemplo, `Certificado del Servidor de políticas de autorización`.
  9. Pulse **Aceptar** y, a continuación, **Guardar**.

Configuración de la CLI tivcmd para TLS/SSL

Para utilizar TLS/SSL con el Servidor de políticas de autorización debe preparar la interfaz de línea de mandatos tivcmd, crear una base de datos de claves nueva, añadir el certificado de firmante público utilizado por el Servidor de políticas de autorización a la base de datos de claves nueva y, a continuación, modificar el archivo de variables de entorno de la CLI tivcmd.

Nota: Si ha solicitado un certificado digital para el Servidor de políticas de autorización, espere hasta que el certificado se haya recibido antes de realizar este procedimiento.

Antes de empezar

Las instrucciones siguientes para gestionar certificados en los sistemas de CLI tivcmd utilice la herramienta de línea de mandatos GSKit que se instala con el componente de la CLI tivcmd. Estas instrucciones deben seguirse en cada sistema en el que la CLI tivcmd está instalada.

Consulte “Utilización de la interfaz de línea de mandatos de GSKit para trabajar con bases de datos de claves y certificado” en la página 236 para los términos que se utilizan en este procedimiento. La mayoría de los términos se basan en el directorio en el que la CLI tivcmd está instalada.

Procedimiento

1. Establezca la vía de acceso para invocar la herramienta de línea de mandatos GSKit utilizando los mandatos siguientes:
   - Windows de 64 bits:

     ```
     set PATH=<gskithome>\lib64;%PATH%
     cd <gskithome>\bin
     ```

   - Windows de 32 bits:

```
set PATH=<gskithome>\lib;%PATH%
cd <gskithome>\bin
```

- Linux y UNIX de 32 bits:

```
export LD_LIBRARY_PATH=<gskithome>/lib:$LD_LIBRARY_PATH
cd <gskithome>/bin
```

- Linux y UNIX de 64 bits:

```
export LD_LIBRARY_PATH=<gskithome>/lib64:$LD_LIBRARY_PATH
cd <gskithome>/bin
```

2. Guarde la base de datos de claves de la CLI tivcmd existente.

   Para recuperar temas, la práctica recomendada es guardar la versión instalada de la base de datos de claves de la CLI tivcmd en cada sistema CLI tivcmd.

   Copie los archivos siguientes con las extensiones `.crl`, `.kdb`, `.rdb` y `.sth`, en otra ubicación:

   - Windows: *<keydbdir>\<oldkeydbname>.**
   - Linux and UNIX: *<keydbdir>/<oldkeydbname>.**

3. Cree una nueva base de datos de claves de la CLI tivcmd.

   a. Cree una base de datos nueva y elimine todos los certificados de firmante público externos con el siguiente mandato:

   ```
   <gskittoolcmd> -keydb -create -db <newkeydb>
   -pw <newkeydbpw> -expire 3650 -stash -fips
   ```

   b. Verifique que la base de datos esté vacía con el siguiente mandato:

   ```
    <gskittoolcmd> -cert -list -db <newkeydb>
   -pw <newkeydbpw> -fips
   ```

   Si la base de datos no está vacía, utilice el mandato de supresión para eliminar los certificados restantes.

4. Añada el certificado de firmante público a la nueva base de datos de claves de la CLI tivcmd.

   En este paso se presupone que el certificado de firmante público se ha colocado en una ubicación en el sistema de CLI tivcmd. Por ejemplo, `C:\policyauthcerts\PolicyAuthSignerCert.arm` o `C:\policyauthcerts\CASignerCert.arm`. Esta ubicación está referenciada en este paso como *<policyauthsignercert>*.

   Añada el certificado de firmante público a la nueva base de datos de claves de la CLI tivcmd utilizando el mandato siguiente:

   ```
   <gskittoolcmd> -cert -add -db <newkeydb> -pw <newkeydbpw>
   -label "Certificado de firmante de política de autorización" -trust enable
   -format ascii -file <policyauthsignercert> -fips
   ```

5. Habilite el intercambio de certificados TLS/SSL en todos los sistemas de CLI tivcmd.

   En cada sistema de CLI tivcmd, utilice los pasos siguientes para habilitar el intercambio de certificados TLS/SSL utilizando el certificado firmado público.

   a. Suprima la base de datos de claves actual. Elimine los archivos *<oldkeydbname>.** en el directorio *<keydbdir>*.

   b. Renombre todos los nuevos archivos de base de datos de claves. Por ejemplo, *<newkeydbname>.** por *<oldkeydbname>.** en el directorio *<keydbdir>*.

   c. Establezca la variable de entorno para habilitar la autenticación del certificado de Servidor de políticas de autorización.

- Windows: edite el archivo de entorno de la CLI tivcmd <*authclidir*>\KDQ\bin\KDQENV mediante la adición de la variable ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y después de la variable KDEBE_KEY_LABEL.
- Linux y UNIX: edite el archivo de entorno de la CLI tivcmd <*authclidir*>/bin/tivcmd mediante la adición de la variable export ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y después de la variable KDEBE_KEY_LABEL.

Configuración de la comunicación TLS/SSL entre el servidor de portal y el Servidor de políticas de autorización

Añada el certificado de firmante público utilizado por el Servidor de políticas de autorización de Tivoli al almacén de confianza de TEPS/e del servidor de portal para configurar TLS/SSL.

Nota: Si ha solicitado un nuevo certificado digital para el Servidor de políticas de autorización, espere hasta que el certificado se haya recibido antes de realizar este procedimiento.

Antes de empezar

Asegúrese de que la TEPS/e consola de administración está habilitada. Para ver los pasos detallados, incluyendo información sobre cómo iniciar la sesión, consulte "Inicio de la consola de administración de TEPS/e" en la página 111.

Acerca de esta tarea

En este paso se presupone que el certificado de firmante público se encuentra en el sistema de servidor de portal. Por ejemplo, C:\policyauthcerts\PolicyAuthSignerCert.arm o C:\policyauthcerts\CASignerCert.arm. Esta ubicación está referenciada en este procedimiento como <*policyauthsignercert*>.

Procedimiento

1. Inicie sesión en TEPS/e consola de administración.
2. Seleccione **Seguridad → Gestión de certificados SSL y claves**.
3. En el área Elementos relacionados, pulse el enlace **Certificados y almacenes de claves** y, en la tabla, pulse el enlace **NodeDefaultTrustStore**.
4. En el área Propiedades adicionales, pulse el enlace **Certificados de firmante** y, en la página que se muestra, pulse **Añadir**.
5. En la página que aparece, especifique la siguiente información:
   - Establezca **Alias** en la etiqueta deseada para el certificado. Por ejemplo, Servidor de políticas de autorización Signer Certificate.
   - Establezca **Nombre de archivo** en la ubicación del certificado de firmante público. Por ejemplo, <*policyauthsignercert*>.
   - Deje a **Tipo de datos** como **Datos ASCII codificados en Base64**.
6. Pulse **Aceptar** y, a continuación, **Guardar**.
7. Vuelva a configurar el servidor de portal para utilizar HTTPS en lugar de HTTP para la conexión del Servidor de políticas de autorización. Para obtener más detalles sobre la reconfiguración de los parámetros de conexión del Servidor de políticas de autorización, consulte "Habilitación de políticas de autorización en el servidor de portal" en la página 199.

Resultados

HTTPS se utiliza ahora entre el Servidor de políticas de autorización y el servidor de portal.

Habilitación de FIPS para IBM Tivoli Monitoring

Debe configurar los componentes de IBM Tivoli Monitoring para habilitar Federal Information Processing Standard (FIPS).

Procedimiento

Complete la configuración de los componentes siguientes:

- Servidor de portal
- Servidor de supervisión y agente de supervisión
- Servidor de automatización de supervisión
- Proxy de almacén
- Resumen y poda
- Base de datos de almacén
- Cliente de portal
- interfaz de línea de mandatos tacmd
- interfaz de línea de mandatos tivcmd

Nota:

La práctica recomendada consiste en reconfigurar cualquier componente tras editar variables de entorno para asegurar que los cambios se implementan.

Si está utilizando Jazz for Service Management con IBM Tivoli Monitoring, consulte *Jazz for Service Management Installation Guide* en Jazz for Service Management Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) para obtener información sobre cómo habilitar FIPS para sus componentes.

Configuración del servidor de portal:

1. Edite el archivo de entorno de Tivoli Enterprise Portal Server en el sistema en el que está instalado el servidor de portal.

   Windows Edite el archivo `KFWENV`.

   Linux UNIX Edite el archivo `cq.ini`.

   Cambie o añada las siguientes variables de entorno:

   KDEBE_FIPS_MODE_ENABLED=YES

   KFW_FIPS_ENFORCED=YES

   Modifique KFW_JAVA_PARMS para añadir
   `-Dcom.ibm.crypto.provider.FIPSMODE=true`
2. Edite el archivo `java.security`. Ejecute los siguientes mandatos:

   Windows

   cd <*dir_ITM*>\<*dir_instalación*>

   CandleGetJavaHome.bat (para obtener la ubicación de JRE)

   notepad <*ubicación_JRE*>\lib\security\java.security

   Linux UNIX

cd <*dir_ITM*>/<*dir_instalación*>

CandleGetJavaHome (para obtener la ubicación de JRE)

Edite <*ubicación_JRE*>/lib/security/java.security

Cambie la lista de proveedores por la siguiente:

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL

com.ibm.jsse2.JSSEFIPS=true
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

3. Windows Edite el archivo <*dir_ITM*>\CNPSJ\java\jre\lib\security\java.security.

   Linux UNIX Edite el archivo <*dir_ITM*>/<*plataforma*>/iw/java/jre/lib/security/java.security

   Cambie la lista de proveedores por la siguiente:

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.crypto.pkcs11.provider.IBMPKCS11
security.provider.7=com.ibm.security.cmskeystore.CMSProvider
security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

   Si procede, comente WebSphere Socket Factories y defina las siguientes variables:

```
com.ibm.jsse2.JSSEFIPS=true
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

Configuración del servidor de supervisión y del agente de supervisión:

1. Edite los siguientes archivos de entorno:

   Windows Edite el archivo KBBENV y el archivo K*XX*ENV para cada agente de supervisión (donde *XX* es el código de producto de 2 letras).

   Linux UNIX Edite el archivo ms.ini en el servidor de supervisión y *.ini para cada agente de supervisión.

   Cambie o añada la siguiente variable de entorno:

   KDEBE_FIPS_MODE_ENABLED=YES

   Si utiliza agentes autónomos, debe añadir la variable anterior al archivo de entorno personalizado.

Servidor de automatización de supervisión

1. Edite el archivo de entorno de Tivoli Enterprise Monitoring Automation Server:

   Windows Edite el archivo KASENV.

   Linux UNIX Edite el archivo as.ini en el sistema en el que el servidor de automatización está instalado.

2. Cambie o añada la siguiente variable de entorno:

   KDEBE_FIPS_MODE_ENABLED=YES

Configuración del proxy de almacén:

1. Edite los siguientes archivos de entorno:

   Windows Edite el archivo KHDENV.

   Linux UNIX Edite el archivo hd.ini.

   Cambie o añada las siguientes variables de entorno:

   KDEBE_FIPS_MODE_ENABLED=YES

   Modifique KHD_JAVA_ARGS para añadir
   -Dcom.ibm.crypto.provider.FIPSMODE=true

Configuración del agente de resumen y poda:

1. Edite el archivo java.security. Ejecute los siguientes mandatos:

   Windows

   cd <*dir_ITM*>\<*dir_instalación*>

   CandleGetJavaHome.bat (para obtener la ubicación de JRE)

   notepad <*ubicación_JRE*>\lib\security\java.security

   Cambie la lista de proveedores por la siguiente:

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL

com.ibm.jsse2.JSSEFIPS=true
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

2. Edite los siguientes archivos de entorno:

   Windows Edite el archivo KSYENV.

   Linux UNIX Edite el archivo sy.ini.

   Modifique KSZ_JAVA_ARGS para añadir
   -Dcom.ibm.crypto.provider.FIPSMODE=true

Configuración de la base de datos de almacén:

La configuración de la base de datos de almacén es específica de la instalación y queda fuera del ámbito de esta configuración. Debe configurar el cliente ODBC para que acceda al servidor de bases de datos utilizando TLS/SSL. A continuación se muestran enlaces de configuración para ejecutar la base de datos en modalidad FIPS 140-2.

- MSSQL 2005

  Consulte el siguiente artículo de la base de conocimientos de Microsoft para ver detalles sobre cómo configurar Microsoft SQL Server para que se ejecute en modalidad FIPS 140-2. Consulte el apartado http://support.microsoft.com/kb/920995.

- DB2 v9.1 Fixpack 2+

  Para DB2 9.1 Fixpack 2 y superiores, las conexiones TLS/SSL siempre están en modalidad FIPS 140-2. Consulte el siguiente documento de soporte de IBM para obtener más detalles sobre la configuración de la conexión ODBC TLS/SSL. Consulte el apartado http://www-01.ibm.com/support/docview.wss?uid=swg21249656.

- Oracle

Consulte el siguiente documento de soporte para configurar Oracle 10g (9.0.4) o posterior en modalidad FIPS 140-2. Consulte el apartado http://download.oracle.com/docs/cd/B14099_19/core.1012/b13999/fips.htm.

Configuración del cliente de portal:

1. Edite el archivo `cnp.bat`. Modifique la línea `_CMD` para incluir la siguiente definición:

   ```
   -Dcom.ibm.crypto.provider.FIPSMODE=true
   -Dcom.ibm.TEPS.FIPSMODE=true
   ```

   Esta etiqueta limita la capacidad del proveedor JCE no FIPS a la funcionalidad X509CertificateFactory y JKS/JCEKS de almacén de claves únicamente.

   Windows Edite el archivo *<dir_ITM>*`\CNP\cnp.bat`.

   Linux UNIX Utilice el siguiente mandato:

   ```
   set _CMD= %_JAVA_CMD% -Xms64m -Xmx256m -showversion -noverify -
   classpath %CPATH% -Dcom.ibm.crypto.provider.FIPSMODE=true -
   Dcom.ibm.TEPS.FIPSMODE=true -Dkjr.trace.mode=LOCAL -
   Dkjr.trace.file=C:\IBM\ITM\CNP\LOGS\kcjras1.log -Dkjr.trace.params=ERROR -
   DORBtcpNoDelay=true -Dibm.stream.nio=true -Dcnp.http.url.host=9.42.15.121 -
   Dvbroker.agent.enableLocator=false -Dnv_inst_flag=%NV_INST_FLAG% -
   Dnvwc.cwd=%NVWC_WORKING_DIR% -Dnvwc.java=%NVWC_JAVA%
   candle.fw.pres.CMWApplet %1 %2 %3 %4 %5 %6 %7 %8 %9 %10
   ```

2. Edite el archivo `java.security`. Ejecute los siguientes mandatos:

   Windows

   cd <*dir_ITM*>\<*dir_instalación*>

   CandleGetJavaHome.bat (para obtener la ubicación de JRE)

   notepad <*ubicación_JRE*>\lib\security\java.security

   Cambie la lista de proveedores por la siguiente:

   ```
   security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.3=com.ibm.crypto.provider.IBMJCE
   security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.5=com.ibm.security.cert.IBMCertPath

   com.ibm.jsse2.JSSEFIPS=true
   ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
   ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
   ```

3. Vuelva configurar el cliente de portal para que se ejecute en modalidad FIPS 140-2.

   Edite el archivo `cnp.bat` para añadir `-Dcom.ibm.crypto.provider.FIPSMODE=true`.

   Nota: En Windows, el cliente de portal se puede configurar parcialmente definiendo la propiedad `com.ibm.TEPS.FIPSMODE` en true.

Configuración de la interfaz de línea de mandatos tacmd:

Windows

1. Edite el archivo *<dir_ITM>*`\BIN\KUIENV`.

   Cambie o añada las siguientes variables de entorno:

   TEPS_FIPS_MODE=YES

   KDEBE_FIPS_MODE_ENABLE=YES

Linux UNIX

1. Edite el script de shell <*dir_ITM*>/bin/ tacmd.
   Cambie o añada las siguientes variables de entorno:
   export TEPS_FIPS_MODE=YES
   export KDEBE_FIPS_MODE_ENABLE=YES
2. Edite el archivo `java.security`. Ejecute los siguientes mandatos:
   cd <*dir_ITM*>\<*dir_instalación*>
   CandleGetJavaHome.bat (para obtener la ubicación de JRE)
   notepad <*ubicación_JRE*>\lib\security\java.security
   Cambie la lista de proveedores por la siguiente:

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.crypto.pkcs11.provider.IBMPKCS11
security.provider.7=com.ibm.security.cmskeystore.CMSProvider
security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

Configuración de la interfaz de línea de mandatos tivcmd:

Windows

1. Edite el archivo <*dir_instalación_tivcmd*>\BIN\KDQENV.
   Cambie o añada las siguientes variables de entorno:
   KDEBE_FIPS_MODE_ENABLE=YES

Linux UNIX

1. Edite el script de shell <*dir_instalación_tivcmd*>/bin/tivcmd.
   Cambie o añada las siguientes variables de entorno:
   export KDEBE_FIPS_MODE_ENABLE=YES

Resultados

Ahora está ejecutando una configuración conforme a FIPS 140-2 Nivel 1.

Qué hacer a continuación

Cuando está en modalidad FIPS 140-2, los componentes de Tivoli Management Services y Tivoli Enterprise Monitoring Agent utilizan uno o más de estos proveedores criptográficos aprobados por FIPS 140-2: IBMJCEFIPS (certificado 497), IBMJSSEFIPS (certificado 409), e IBM Crypto for C (ICC (certificado 775) para la criptografía. Los certificados están listados en el sitio web de NIST, en http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

Todas las conexiones IP.SPIPE y las conexiones habilitadas para TLS/SSL utilizan el protocolo TLS 1.0 solamente. TLS/SSL debe estar habilitado entre el cliente de Tivoli Enterprise Portal y el Tivoli Enterprise Portal Server, y se describe en el tema "Utilización de SSL entre el servidor y el cliente de portal" de *IBM Tivoli Monitoring: Guía de instalación y configuración*. El error al habilitar TLS/SSL puede exponer las credenciales.

Habilite IP.SPIPE entre todos los componentes de IBM Tivoli Monitoring para conservar la integridad y la confidencialidad de los datos que utilizan cifrado conforme con FIPS 140-2. Los certificados utilizados en la comunicación IP.SPIPE

necesitan la potencia de cifrado prescrita por NIST y FIPS. Capítulo 5, “Habilitación de la autenticación de usuarios”, en la página 83 describe los detalles sobre cómo sustituir certificados de cifrado. Si el entorno utiliza los programas de utilidad GSKit proporcionados, se debe incluir el distintivo `-fips` en todas las operaciones. Póngase en contacto con el administrador de seguridad local o consulte el sitio web de NIST para ver más detalles sobre la conformidad con FIPS 140-2.

Referencia relacionada:

http://www-01.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoring.html
Búsqueda en el soporte de IBM Tivoli Monitoring de directrices sobre la configuración de componentes para conformidad con FIPS 140-2.

http://csrc.nist.gov/
La División de seguridad de sistemas de National Institute of Standards and Technology tiene publicaciones sobre la conformidad con FIPS 140-2.

Importación de los certificados de TEPS/e a la base de datos de archivos de claves del servidor de portal

Si ha creado una base de datos de archivos claves personalizada en el sistema donde se ha instalado el servidor de portal y contiene un nuevo certificado de IBM Tivoli Monitoring autofirmado o firmado por CA, también debe importar los certificados utilizados por TEPS/e a la base de datos de archivos de claves nueva. Esto permite que TEPS/e y el plug-in de servidor web del Tivoli Enterprise Portal Server se comuniquen internamente en una conexión segura.

Acerca de esta tarea

Utilice el siguiente procedimiento para importar manualmente los certificados de TEPS/e a la base de datos de archivos de claves de IBM Tivoli Monitoring para el servidor de portal.

Procedimiento

1. Abra un indicador de mandatos (Windows) o shell (AIX o Linux).
2. Establezca la variable *JAVA_HOME* tal como se describe en “Configuración de JRE para GSKit e inicio del gestor de claves” en la página 238, pero *no* inicie el gestor de claves GSKit.
3. Vaya al directorio bin bajo el directorio inicial de GSKit.
4. Ejecute los siguientes mandatos:
   - Windows
     ```
     <gskittoolcmd> -cert -import -file ../../cnpsj/profiles/itmprofile/
     config/cells/itmcell/nodes/itmnode/default-signers.p12 -pw WebAS -type
     pkcs12 -target ../../keyfiles/keyfile.kdb -target_pw <password>
     -target_type cms
     <gskittoolcmd> -cert -import -file ../../cnpsj/profiles/itmprofile/
     config/cells/itmcell/nodes/itmnode/key.p12 -pw WebAS -type pkcs12
     -target ../../keyfiles/keyfile.kdb -target_pw <password> -target_type
     cms
     ```
   - Linux AIX
     ```
     ././<gskittoolcmd> -cert -import -file ../../../<arch>/profiles/
     itmprofile/config/cells/itmcell/nodes/itmnode/default-signers.p12 -pw
     WebAS -type pkcs12 -target ../../../keyfiles/keyfile.kdb -target_pw
     ```

```
<password> -target_type cms
./<gskittoolcmd> -cert -import -file ../../../<arch>/profiles/
itmprofile/config/cells/itmcell/nodes/itmnode/key.p12 -pw WebAS -type
pkcs12 -target ../../../keyfiles/keyfile.kdb -target_pw <password>
-target_type cms
```

donde *<password>* es la contraseña de la base de datos de archivo de claves, para sistemas Linux y AIX, *<arch>* es el subdirectorio de arquitectura donde el servidor de portal está instalado y *<gskittoolcmd>* es el mandato para iniciar la herramienta GSKit.

5. Reinicie el servidor de portal.

Utilización de la interfaz de línea de mandatos de GSKit para trabajar con bases de datos de claves y certificado

La herramienta de línea de mandatos GSKit se instala con cada componente de IBM Tivoli Monitoring en una plataforma distribuida y se utiliza para gestionar los archivos de claves y certificados.

Para obtener información acerca de la interfaz de línea de mandatos GSKit, consulte *IBM Global Security Kit GSKCapiCmd V8.0 User's Guide*.

Antes de comenzar

La tabla siguiente lista los términos que se utilizan en los procedimientos relacionados con GSKit. La mayoría de los términos se basan en el directorio en el que el componente de IBM Tivoli Monitoring y GSKit están instalados:

<authclidir>	El directorio en el que el está instalado el componente de IBM Tivoli Monitoring. Por ejemplo: • `c:\IBM\ITM` u `/opt/IBM/ITM` para el servidor de supervisión, el servidor de automatización, el servidor de portal, la CLI tacmd y los agentes • `c:\IBM\TivoliMonitoring` u `/opt/IBM/TivoliMonitoring` para la CLI tivcmd
<interp>	La interp específica de la máquina. Por ejemplo, sol296, li6263 o aix536.
<gskithome>	El directorio en el que está instalado GSKit. Windows de 32 bits: *<itmcompdir>*`\GSK8`. Windows de 64 bits: *<itmcompdir>*`\GSK8_64`. Linux y UNIX de 32 bits: *<itmcompdir>*`/`*<interp>*`/gs` Linux y UNIX de 64 bits: *<itmcompdir>*`/`*<interp>*`/gs`
<gskittoolcmd>	La sintaxis del mandato de CLI de GSKit real. Windows de 32 bits: *<gskithome>*`\bin\gsk8capicmd.exe` Windows de 64 bits: *<gskithome>*`\bin\gsk8capicmd_64.exe` Linux y UNIX de 32 bits: `./`*<gskithome>*`/bin/gsk8capicmd.exe` Linux y UNIX de 64 bits: `./`*<gskithome>*`/bin/gsk8capicmd_64.exe`
<keydbdir>	El directorio en el que está almacenada la base de datos de claves predeterminada. Windows: *<itmcompdir>*`\keyfiles` Linux and UNIX: *<itmcompdir>*`/keyfiles`

<*oldkeydbname*>	El nombre base de la base de datos de claves instalada con el componente de IBM Tivoli Monitoring. El nombre de base de datos de claves base es keyfile (archivo de claves). Los cuatro archivos asociados con esta base de datos de claves son: `keyfile.crl`, `keyfile.kdb`, `keyfile.rdb` y `keyfile.sth`.
<*oldkeydb*>	El nombre de la base de datos de claves instalada con el componente de IBM Tivoli Monitoring. El nombre de la base de datos de claves es <*oldkeydbname*>`.kdb`.
<*oldkeydbpw*>	La contraseña de la base de datos de claves instalada. El valor predeterminado es IBM61TIV.
<*newkeydbname*>	El nombre base de la nueva base de datos de claves. Puede elegirse cualquier nombre que no sea keyfile. Por ejemplo, `itmcompkeyfile`.
<*newkeydb*>	El nombre de la nueva base de datos de claves. El nombre de la base de datos de claves es <*newkeydbname*>`.kdb`.
<*newkeydbpw*>	La contraseña asociada con la base de datos de claves nueva. Puede elegirse cualquier contraseña válida.

Establecimiento de la vía de acceso para invocar la herramienta de línea de mandatos GSKit

Para ejecutar la herramienta de la línea de mandatos GSKit, el directorio `lib` de la herramienta GSKit debe estar incluido en la vía de acceso del sistema.

Windows **de 32 bits**

```
set PATH=<gskithome>\lib;%PATH%
cd <gskithome>\bin
```

Windows **de 64 bits**

```
set PATH=<gskithome>\lib64;%PATH%
cd <gskithome>\bin
```

Linux UNIX **de 32 bits**

```
export LD_LIBRARY_PATH=<gskithome>/lib:$LD_LIBRARY_PATH
cd <gskithome>/bin
```

Linux UNIX **de 64 bits**

```
export LD_LIBRARY_PATH=<gskithome>/lib64:$LD_LIBRARY_PATH
cd <gskithome>/bin
```

Utilización del programa de utilidad GSKit iKeyman para trabajar con bases de datos de claves y certificados

Se proporcionan un certificado autofirmado predeterminado y una clave al instalar IBM Tivoli Monitoring. Si prefiere utilizar un certificado firmado de entidad emisora de certificados, utilice los programas de utilidad iKeyman para crear una solicitud de certificado y, a continuación, crear una base de datos de claves e importar los certificados en la base de datos.

Nota: El programa de utilidad iKeyman está disponible en los sistemas distribuidos donde se instala el servidor de supervisión, los servidores de portal, el cliente de escritorio del cliente de portal y la CLI tacmd.

Para obtener información acerca de la interfaz gráfica de usuario iKeyman y su interfaz de línea de mandatos, consulte *IBM Developer Kit and Runtime Environment iKeyman V8.0 User's Guide*.

Configuración de JRE para GSKit e inicio del gestor de claves

Debe establecer la vía de acceso en Java Runtime Environment antes de iniciar GSKit.

De lo contrario, podría obtener un error parecido a `No se ha podido analizar el valor JAVA_HOME`.

Procedimiento

- Windows
  1. Desde el indicador de mandatos, ejecute este script para obtener la ubicación de IBM Java:
     dir_instalación`\InstallITM\GetJavaHome.bat`
  2. Establezca la variable JAVA_HOME para que apunte a la ubicación de IBM Java.
  3. Obtenga la ubicación de GSKit ejecutando este script:
     dir_instalación`\InstallITM\GetGSKitHome.bat`
  4. Ejecute el mandato siguiente:
     `$JAVA_HOME\jre\bin\ikeyman.exe` *[propiedades]*

     donde, *[propiedades]* puede ser cero o más propiedades del sistema.
- AIX Linux Solaris
  1. Desde la consola, ejecute este script para obtener la ubicación de IBM Java:
     dir_instalación`/bin/CandleGetJavaHome.sh`
  2. Exporte la variable JAVA_HOME para que apunte a la vía de acceso de IBM Java.
  3. Ejecute el mandato siguiente:
     `$JAVA_HOME\jre\bin\ikeyman.exe` *[propiedades]*

     donde *[propiedades]* puede ser cero o más propiedades del sistema.
- HP-UX
  1. Desde la consola, ejecute este script para obtener la ubicación de IBM Java:
     dir_instalación`/bin/CandleGetJavaHome.sh`
  2. Exporte la variable JAVA_HOME para que apunte a la vía de acceso de IBM Java. Para 64 bits, gsk7ikm tiene que ser Java de 64 bits.
  3. Compruebe la vía de acceso del GSKit local examinando este archivo:
     dir_instalación`/config/gsKit.config`

     `GskitInstallDir` apunta a un GSKit de 32 bits y `GskitInstallDir_64` apunta a un GSKit de 64 bits.
  4. Inicie IBM Key Management (a través del programa de utilidad gráfico que necesita X Windows System) ejecutando el mandato siguiente:
     `GskitInstallDir/bin/gsk7ikm_32`

Creación de una nueva base de datos de claves

Creación de una nueva base de datos de claves mediante el programa de utilidad iKeyman.

Acerca de esta tarea

Siga estos pasos para crear una nueva base de datos de claves:

1. Si todavía no lo ha hecho, inicie iKeyman.

2. Pulse **Archivo de base de datos de claves → Nuevo**.
3. Seleccione **CMS** en el campo **Tipo de base de datos de claves**.
4. Escriba `keyfile.kdb` en el campo **Nombre de archivo**.
5. Escriba la ubicación siguiente en el campo **Ubicación**: *<dir_instalación_itm>*/`keyfiles`.
6. Pulse **Aceptar**. Se abre la ventana Indicador de contraseña.
7. Escriba una contraseña en el campo **Contraseña** y vuélvala a confirmar en el campo **Confirmar contraseña**. Pulse **Aceptar**.
8. Aparecerá una ventana de confirmación. Pulse **Aceptar**.

Se visualiza la ventana IBM Key Management.Esta ventana refleja el nuevo archivo de base de datos de claves CMS y los certificados digitales del firmante.

Creación de un nuevo par de claves privada-pública y de una solicitud de certificado

Creación de un nuevo par de claves privada-pública y de una solicitud de certificado en iKeyman.

Acerca de esta tarea

Siga estos pasos para crear un nuevo par de claves pública-privada y una solicitud de certificado:

Procedimiento

1. Si todavía no lo ha hecho, inicie iKeyman.
2. Pulse **Archivo de base de datos de claves → Abrir**.
3. Seleccione la base de datos de claves keyfile.kdb y pulse **Abrir**.
4. Escriba la contraseña para la base de datos de claves y pulse en **Aceptar**.
5. Seleccione **Solicitudes de certificado personal** en la lista desplegable y pulse en **Nuevo**.
6. Pulse **Nuevo**.
7. Escriba `IBM_Tivoli_Monitoring_Certificate` en el campo **Etiqueta de clave**.
8. Escriba un **Nombre común** y **Organización** y seleccione un **País**. Para los campos restantes, acepte los valores predeterminados, o escriba o seleccione nuevos valores.
9. En la parte inferior de la ventana, escriba un nombre para el archivo.
10. Pulse **Aceptar**. Aparecerá una ventana de confirmación, verificando que ha creado una solicitud para un nuevo certificado digital.
11. Pulse **Aceptar**.

Resultados

Se visualiza la ventana IBM Key Management.

Qué hacer a continuación

Envíe el archivo a una entidad emisora de certificados para solicitar un nuevo certificado digital o bien corte y peque la solicitud en los formularios de solicitud del sitio web de la entidad emisora de certificados.

Utilización de un certificado autofirmado temporal

Puede tardar entre dos y tres semanas en recibir un certificado digital firmado por la entidad emisora de certificados. Si desea utilizar un certificado digital que no sea el que se suministra con IBM Tivoli Monitoring y aún no ha recibido el certificado digital firmado por la entidad emisora de certificados, puede crear un certificado autofirmado en el servidor de portal. Un certificado digital autofirmado no es tan seguro como un certificado firmado por la entidad emisora de certificados; constituye estrictamente una medida temporal hasta que llega el certificado firmado por la entidad emisora de certificados.

Acerca de esta tarea

Para crear y utilizar un certificado autofirmado, siga este procedimiento:

Procedimiento

1. Crear una base de datos de claves de entidad emisora de certificados.
2. Crear el certificado autofirmado.
3. Exportar el certificado autofirmado.
4. Recibir el certificado autofirmado en las bases de datos de claves del servidor de portal.

Qué hacer a continuación

Cuando reciba el certificado firmado por la entidad emisora de certificados, tiene que suprimir el certificado autofirmado.

Recepción del certificado firmado por la entidad emisora de certificados

Acerca de esta tarea

Después de que la entidad emisora de certificados devuelva el nuevo certificado digital, guárdelo en el sistema donde el servidor de portal se ejecuta. Repita lo mismo para el cliente. Si la entidad emisora de certificados devuelve el certificado como parte de un mensaje de correo electrónico, cópielo y péguelo del correo electrónico en un archivo de texto.

Lleve a cabo el siguiente procedimiento para recibir el certificado digital de la entidad emisora de certificados en la base de datos de claves de cada sistema:

Procedimiento

1. Si todavía no lo ha hecho, inicie iKeyman.
2. Pulse **Archivo de base de datos de claves → Abrir**.
3. Seleccione la base de datos keyfile.kdb y pulse en **Abrir**.
4. Escriba la contraseña para la base de datos y pulse en **Aceptar**.
5. Seleccione **Certificados personales** en la lista desplegable.
6. Pulse **Recibir**.
7. Pulse **Tipo de datos** y seleccione el tipo de datos del nuevo certificado digital, como por ejemplo **Datos ASCII codificados en Base64**.
8. Escriba `keyfile.sth` para el **Nombre de archivo de certificados** y `<dirinstalación_itm>/keyfiles` como la **Ubicación** para el nuevo certificado digital.

9. Pulse **Aceptar**.
10. Escriba `IBM_Tivoli_Monitoring_Certificate` para el nuevo certificado digital y pulse **Aceptar**.

Cómo guardar la contraseña en un archivo stash

Puesto que muchos de los componentes de IBM Tivoli Monitoring funcionan sin la intervención del usuario, tiene que guardar la contraseña de la base de datos de claves en un archivo stash del sistema. Guarde esta contraseña para que los componentes del producto puedan utilizar TLS/SS sin necesitar ninguna intervención del usuario.

Acerca de esta tarea

Lleve a cabo el siguiente procedimiento para guardar la contraseña en un archivo stash:

Procedimiento

1. Si todavía no lo ha hecho, inicie iKeyman.
2. Seleccione **Archivo de base de datos de claves → Archivo stash**. Aparecerá una ventana de información que le indicará que la contraseña se ha guardado en un archivo stash.
3. Pulse **Aceptar**.

Capítulo 9. Registro de auditoría

Con la nueva función de auditoría, puede capturar sucesos significativos producidos en el entorno de IBM Tivoli Monitoring. También puede registrar estos sucesos en el almacenamiento permanente para su posterior recuperación y análisis. Cada registro de auditoría describe con detalle algún suceso que ha cambiado el estado del sistema IBM Tivoli Monitoring.

Estos registros de auditoría y de registro se pueden guardar en Tivoli Data Warehouse. Se proporcionan informes estándares mediante la función Tivoli Common Reporting.

El recurso de auditoría cubre los nuevos agentes autodescriptivos (incluida su función de renovación automática), acciones del agente de proxy de almacén, conexiones EIF-SSL, mandatos de actuación automatizados y la integración de IBM Tivoli Monitoring con Tivoli Application Dependency Discovery Manager.

Las plataformas soportadas incluyen los sistemas Windows, Linux, UNIX, IBM i y z/OS.

Los registros de auditoría se guardan en dos lugares:

Datos de atributos de auditoría de ITM recopilados accesibles desde el cliente de portal

En el espacio de trabajo Estatus de sistemas gestionados, puede pulsar con el botón derecho en los componentes de supervisión y seleccionar Registro de auditoría para ver información de registro de auditoría recopilada específica del componente. A continuación puede crear situaciones sobre la tabla Auditoría de ITM para supervisar sucesos auditados y recopilar datos de auditoría históricamente en Tivoli Data Warehouse.

Cuando examine información de auditoría, busque los resultados con valores distintos de cero. El valor 0 indica que es correcto. La creación de situaciones que supervisan los registros con resultados con valores distintos de cero puede ayudar a filtrar los mensajes informativos generales.

El manual *Tivoli Enterprise Portal: Guía del usuario* contiene más información sobre el espacio de trabajo y el grupo de atributos de auditoría de ITM. Para obtener información sobre el espacio de trabajo Registro de auditoría y sobre cómo habilitar la recopilación histórica para el grupo de atributos Auditoría de ITM, consulte Espacio de trabajo Estatus de sistemas gestionados. Para ver definiciones de atributos, consulte Atributos de auditoría de ITM.

Archivo de registro con formato XML almacenado localmente

El archivo de registro puede ser utilizado por un producto de otro proveedor para analizar y evaluar la información de auditoría. Utilice el SAPM DTD proporcionado como ayuda con productos de otros proveedores. El DTD se proporciona en el DVD de herramientas de IBM Tivoli Monitoring en el directorio `XML`; consulte el archivo `SAPMAudit.dtd`.

© Copyright IBM Corp. 2005, 2013

Los archivos de registro se almacenan en el directorio `auditlogs` bajo el directorio `<dir_instalación>`. Cada agente procesa su propio archivo de registro y se formatea como XML. Consulte los siguientes nombres de archivo de registro:

Windows Linux UNIX

Para una sola instancia: *<IDUsuario>*.*<nombrehost>*_*<cp>*_audit.log

Para varias instancias: *<IDUsuario>*.*<nombrehost>*_*<cp>*_*<instancia>*_audit.log

IBM i

/QIBM/ProdData/IBM/ITM/support

z/OS

Recopile el registro desde el recurso SMF.

Si están habilitados, los registros de auditoría de ITM se almacenan en registros de tipo 112 en el formato de Systems Management Facility (SMF), codificados en UTF8, y se incluyen en un repositorio común (conjuntos de datos SYS1.MANn) con todos los demás datos de sucesos de z/OS. Para obtener más información, consulte *Configuring the Tivoli Enterprise Monitoring Server on z/OS* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/ztemsconfig/ztemsconfig.htm).

Niveles de rastreo de auditoría

Los sucesos de auditoría tienen tres niveles de rastreo distintos: Mínimo, Básico y Detallado. A cada suceso se le asigna un nivel de rastreo. Es posible que desee aumentar o reducir el nivel de rastreo para recopilar datos adicionales.

Mínimo: Cambios principales en el estado del producto

Básico: Cualquier acción que modifique objetos o que ocasione un error de acceso

Detallado: Cualquier acción que ocasione un control de acceso correcto o erróneo

Tipos de registros de sucesos

Se asocia un tipo de registro con cada suceso de auditoría para indicar la naturaleza del registro de auditoría. Los tipos de registros de sucesos se muestran en la tabla siguiente:

Nombre completo del suceso	Nombre abreviado (mostrado en los registros)	Descripción
Comprobación de autorización	CHECKING	Sucesos relacionados con la comprobación de si un usuario tiene permiso para realizar una determinada operación o suceso.
Validación de la autenticación	VALIDATE	Sucesos relacionados con la autenticación de la identificación del usuario o entidad.

Nombre completo del suceso	Nombre abreviado (mostrado en los registros)	Descripción
Suceso contextual	CONTEXT	Cualquier otro suceso que pueda producirse contextualmente dentro de una aplicación.
Mantenimiento de objetos	OBJMAINT	Sucesos relacionados con el cambio de un objeto, como actualización, supresión, creación y movimiento de cualquier objeto o tabla de IBM Tivoli Monitoring.
Administración del sistema	SYSADMIN	Sucesos relacionados con el inicio y cierre de programas, cambios en el sistema de auditoría y autorización, cambios en la configuración, creación de tablas y configuración de la sincronización de datos.
Mantenimiento de seguridad	SECMAINT	Sucesos relacionados con otorgar y revocar privilegios.

Elementos XML del registro de auditoría correlacionados con el grupo de atributos de auditoría de ITM

El registro de auditoría XML contiene elementos que se coordinan con atributos de auditoría de ITM.

Para obtener información detallada de la sintaxis XML, consulte `SAPMAudit.dtd` en el DVD de las herramientas de IBM Tivoli Monitoring.

Para ver descripciones de los atributos, consulte Atributos de auditoría de ITM.

Utilice la tabla siguiente como consulta:

Nota:

- Algunas celdas se han dejado en blanco a propósito para representar la estructura XML del registro de auditoría. Celdas de atributos de auditoría de ITM vacías indican que el atributo de coordinación aún no se ha creado para el elemento XML de coordinación.
- Los elementos XML y atributos de XML entre paréntesis () indican que IBM Tivoli Monitoring no ha implementado el elemento.
- *Atributos adicionales significa que el elemento XML o atributo se inserta como un par Nombre=Valor en la columna Atributo adicional en la tabla de registro de auditoría.

Grupo lógico	Elementos(s) XML	Atributo XML	Atributo de auditoría de ITM
AuditEvt	AuditEvt	Dominio	Dominio
		Nivel	Nivel de rastreo
		Tipo	Tipo de registro de suceso
		Ver	Versión de registro de auditoría
Who	AuthID		ID de autorización
		(Repositorio)	
	Ejecutar como		Ejecutar como
		(Repositorio)	
	UserID		ID de usuario
		(Repositorio)	
	Entidad		Entidad
		Tipo	Tipo de entidad
What	Op	(CDMID)	
		Nombre	Nombre de operación
		Tipo	Tipo de operación
		OpObjType	Tipo de objeto de operación
	Msg	Texto	Mensaje
		RBKey	Clave de paquete de recursos
	Param		Atributos adicionales*
		Orden	Atributos adicionales*
	Resultado		Resultado
Cuando	Corr		Correlacionador
	Seq		Secuencia
	EvtTS	MS	Indicación de fecha y hora (MS)
		ITM	Indicación de fecha y hora
		(UTC)	
	(LogTS)		

Grupo lógico	Elementos(s) XML		Atributo XML	Atributo de auditoría de ITM
OnWhat	Obj		Tipo	Tipo de objeto
			(Ver)	Versión de objeto
			Nombre	Nombre de objeto
			(CDMID)	Atributos adicionales*
			Vía de acceso	Vía de acceso de objeto
	(SecMaint)	Receptor	Tipo	
		SecPolicy		
		Restricción		
	(SecPolicy)			Nombre de política de seguridad
	(Grantee)			Receptor
			Tipo	Tipo de receptor
	(PriAuthEvt)			Suceso de privilegio o autorización
			Tipo	Tipo de privilegio o autorización
			AuthID	ID de autorización asumible
			Repositorio	
	(AuthVal)			
	(AuthCheck)			Atributos adicionales*
	(AuthPlugin)		Tipo	Tipo de plugin de autorización
			Servidor	Atributos adicionales*

Grupo lógico	Elementos(s) XML		Atributo XML	Atributo de auditoría de ITM
Where	Origen	Node	Nombre	Nombre de origen
			Tipo	Tipo de origen
			AddrType	Protocolo de origen
			Addr	Dirección de origen
			Host	Nombre de host de origen
			Puerto	Puerto de origen
			SYSID	Origen
	App		Código	Código de aplicación
			Ver	Versión de la aplicación
			Comp	Componente de aplicación
	SvcPt			Punto de servicio
WhereFrom	Origen	Node	Nombre	Nombre de fuente
			Tipo	Tipo de fuente
			AddrType	Protocolo de fuente
			Addr	Dirección de fuente
			Host	Nombre de host de fuente
			Puerto	Puerto de fuente
			SYSID	Origen
	Relay	Node	Nombre	
			Tipo	
			AddrType	
			Addr	
			Host	
			Puerto	
			SYSID	

Grupo lógico	Elementos(s) XML		Atributo XML	Atributo de auditoría de ITM
WhereTo	Destino	Node	Nombre	Nombre de destino
			Tipo	Tipo de destino
			AddrType	Protocolo de destino
			Addr	Dirección de destino
			Host	Nombre de host de destino
			Puerto	Puerto de destino
			SYSID	Destino

Ejemplo de XML de registro de auditoría

El siguiente registro de auditoría de ejemplo se ha generado durante el arranque e indica que los servicios del agente de autodescripción de un determinado servidor de supervisión están inhabilitados.

```
<AuditEvt Domain="" Type="SYSADMIN" Level="Minumum" Ver="1">
 <Who>
  <UserID/>
  <AuthID>SYSTEM</AuthID>
 </Who>
 <What>
  <Op Name="Self-Describing Agent Status"
   OpObjType="ibm-prod-tivoli-itm:SelfDescribingAgentInstall" Type="Disable"/>
  <Msg Text="Self-Descrbing Agent Feature disabled at the local TEMS."
   RBKey="KFASD010"/>
  <Result>0</Result>
 </What>
 <When>
  <EvtTS MS="1307723083106" ITM="1110610162443106"/>
  <Seq>1</Seq>
 </When>
 <OnWhat>
  <Obj Type="ibm-prod-tivoli-itm:SelfDescribingAgentInstall" Name="SDA Services"/>
 </OnWat>
 <Where>
  <Origin>
   <Node Name=Tivoli Enterprise Monitoring Server" Type="SERVER" AddrType="IPv4"
    Addr="10.1.1.1" SYSID="HUB_NC051039"/>
  </Origin>
  <App Code="KMS" Ver="06.23.00" Comp="KFA"/>
  <SvcPt>system.nc051039_ms</SvcPt>
 </Where>
 <WhereFrom>
  <Source>
   <Node Name="Tivoli Enterprise Monitoring Server" Type"SERVER" SYSID="HUB_NC051039"
    Addr="10.1.1.1" AddrType="IPv4"/>
  </Source>
 </WhereFrom>
 <WhereTo>
  <Target>
   <Node Name="Tivoli Enterprise Monitoring Server" Type="SERVER" AddrType="IPv4"
```

```
    Addr="10.1.1.1" SYSID="HUB_NC051039"/>
  </Target>
 </WhereTo>
</AuditEvt>
```

En este ejemplo, se pueden responder las siguientes preguntas:

Pregunta	Etiqueta(s)	Valor	Interpretación
Quién	UserID	Vacío	La etiqueta UserID vacía indica que este suceso ha sido generado por un ID de usuario desconocido o un proceso autónomo que realiza una acción que no ha sido iniciada directamente por un usuario.
	AuthID	SYSTEM	Indica el ID bajo el que se ha autorizado este suceso.
Qué	Op	Estatus del agente de autodescripción	La operación “Self-Describing Agent Status” ("Estatus del agente de autodescripción") se ha realizado correctamente (Resultado 0) con el mensaje explicativo que indica que la función del agente de autodescripción se ha inhabilitado.
	Msg	La función de autodescripción se ha inhabilitado en el TEMS local.	
	Resultado	0	
	Tipo	Inhabilitar	Indica que esta operación particular es del tipo genérico “disable” ("inhabilitar"). Las operaciones suelen ser autoexplicativas, pero todas están clasificadas en un tipo de modelo de suceso genérico (GEM), especificado por Tivoli Security and Information Event Manager.
Cuándo	ITM	1110610162443106	La hora a la que se ha generado el suceso (no registrado) en formato de Hora universal coordinada (UTC) (SAAMMDDhhmmssms). La fecha indica: 10 de junio de 2011 a las 04:24:43 106 ms.
Sobre qué	Nombre	Servicios SDA	El nombre del objeto es el código, componente u otro identificador contextualmente relevante afectado que recibe la operación. En este ejemplo, el objeto “SDA Services” ha recibido la operación “Self-Describing Agent Status” que se ha realizado correctamente (con el resultado 0) sobre el objeto “SDA Services”.
Dónde	SYSID	HUB_NC051039	Indica dónde se ha registrado el suceso. KMS de la aplicación en el sistema gestionado ID HUB_NC051039 (IP 10.1.1.1) ha registrado este suceso. Este sistema se identifica como Tivoli Enterprise Monitoring Server.
	Dirección	10.1.1.1	
	Nombre	Tivoli Enterprise Monitoring Server	
	Aplic	KMS	
Desde dónde	SYSID	HUB_NC051039	Este suceso se ha iniciado en MSN HUB_NC051039 (IP 10.1.1.1). Este sistema se identifica como Tivoli Enterprise Monitoring Server.
	Dirección	10.1.1.1	
	Nombre	Tivoli Enterprise Monitoring Server	
A dónde	SYSID	HUB_NC051039	El suceso está destinado a MSN HUB_NC051039 (IP 10.1.1.1). Este sistema de destino se identifica como Tivoli Enterprise Monitoring Server.
	Dirección	10.1.1.1	
	Nombre	Tivoli Enterprise Monitoring Server	

Variables de entorno de auditoría

Las variables de entorno se pueden modificar para controlar la función de auditoría.

Variables de entorno

Se han definido las siguientes variables de entorno para configurar el recurso de auditoría:

Variable de entorno	Descripción	Entrada aceptable	Valor predeterminado no definido
AUDIT_FILE	Se utiliza para inhabilitar la creación de un archivo xml audit.log. Los sucesos de auditoría se crean en la tabla de auditoría de ITM.	• Inhabilitada • Habilitado **Nota:** No soportado es un estado no se acepta como entrada pero se puede devolver en plataformas que no crean registros de auditoría, como por ejemplo, sistemas z/OS.	Habilitado
AUDIT_LOG_DIR _PATH	La vía de acceso al directorio en el que se conservan los archivos de registro de auditoría. No disponible en sistemas z/OS. **Nota:** Si cambia el directorio de salida, la herramienta pdcollect no puede recopilar el registro de auditoría asociado.	Especifique una vía de acceso específica del sistema operativo.	*<dir_instalación>*/ auditlogs
AUDIT_LOG_FILE _LIMIT_MB	El tamaño máximo del archivo de registro en megabytes (2^20 bytes).	1 - MAXINT-1	9
AUDIT_LOG_FILE _NAME	El nombre del archivo de registro. No disponible en sistemas z/OS.	Especifique el nombre del archivo de registro.	*<IDUsuario>*. *<nombrehost>* _*<cp>*_audit.log

Variable de entorno	Descripción	Entrada aceptable	Valor predeterminado no definido
AUDIT_LOG_MAX _FILES_COUNT	Número máximo de archivos de registro que se pueden acumular. Esta variable solo se aplica a plataformas distribuidas. No disponible en sistemas z/OS.	1...MAXINT-1 (en distribuidas)	5
AUDIT_MAX_HIST	Número máximo de registros que se conservan en la memoria a corto plazo para consultas directas.	1...MAXINT-1	100
AUDIT_TRACE	El nivel de rastreo para pasar mensajes. Los niveles de rastreo de mensaje (entre bajo y alto) son Mínimo, Básico, Detalles. Los niveles superiores rastrean todos los niveles inferiores.	• Mínimo • Básico • Detalles • Inhabilitada	Básico
ITM_DOMAIN	Un identificador opcional de 128 caracteres en sistemas distribuidos y un identificador de 32 caracteres en sistemas z/OS que puede utilizar para asociar con estos registros. Se adapta mejor a agentes de identificación común asociados entre sí. Puede utilizar esta variable para clasificar registros por un determinado cliente. Se conservan las mayúsculas y minúsculas.	Especifique una cadena alfanumérica que puede contener los caracteres más (+), menos (-), punto y coma (;) y dos puntos (:).	No se proporciona ningún dominio.

Modificación de las variables de entorno de auditoría

Puede configurar la variable de entorno de rastreo para el recurso de auditoría utilizando los siguientes procedimientos. Puede modificar cualquiera de las variables de entorno anteriormente mencionadas.

Windows

Utilice Manage Tivoli Enterprise Monitoring Services (Inicio → Programas → IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services)

para editar archivos de entorno. Pulse con el botón derecho en el componente que desea modificar y pulse **Avanzado → Editar archivo ENV**. Debe reciclar el componente para implementar los cambios.

Linux UNIX

1. Vaya al directorio *<dir_instalación>*/config y abra el archivo de coordinación:

   Para el servidor de supervisión:
   *<nombrehost>*_ms_*<nombre_tems>*.config

   Para el servidor de portal y agentes de una sola instancia: *<cp>*.ini

   Para agentes de varias instancias: *<cp>*_*<instancia>*.config
2. En una nueva línea, añada la variable de entorno seguida del valor. Por ejemplo, AUDIT_TRACE=BASIC
3. Guarde y cierre el archivo.
4. Recicle el componente para que los cambios entren en vigor.

z/OS

Consulte *Configuración de Tivoli Enterprise Monitoring Server en z/OS* para obtener más información.

Actuación y registro de auditoría de la ejecución del mandato

Si tiene IBM Tivoli Monitoring V6.3 o posterior, se generan registros de auditoría para Actuación y la ejecución de **tacmd executecommand**. La ejecución de Actuación incluye Actuaciones iniciadas en Tivoli Enterprise Portal, la ejecución del mandato **tacmd executeaction**, los mandatos de Actuación de situación y los mandatos de Actuación de políticas de flujo de trabajo. La identidad del usuario que ha iniciado la actuación se pasa al agente de supervisión utilizando una señal de sesión segura.

La señal de sesión aprovecha la clave de cifrado común de IBM Tivoli Monitoring y la sincronización de tiempo entre los servidores de IBM Tivoli Monitoring y los agentes de supervisión. Si la clave de cifrado no está sincronizada, los mandatos se rechazan como no válidos debido a errores de validación con la identidad. Si las horas del sistema entre el servidor de portal (para los usuarios de Tivoli Enterprise Portal) o el servidor de supervisión concentrador (para los usuarios de mandatos tacmd) tienen una diferencia de más de 25 minutos de sincronización con la del agente de supervisión de destino según la Hora Universal Coordinada (UTC), el mandato se rechaza como no autorizado debido a que se agota tiempo de espera del permiso.

La ejecución de la Actuación de situación y la ejecución de la Actuación de política de flujo de trabajo registran la identidad del último usuario que ha modificado la situación o la política de flujo de trabajo.

Los mensajes de auditoría están disponibles en el registro de auditoría en el agente de supervisión o a través del Tivoli Enterprise Portal como datos históricos o consultas en tiempo real del registro de auditoría.

La modalidad de compatibilidad de seguridad TEMS permite que os componentes del servidor IBM Tivoli Monitoring que están en una versión anterior de V6.3 ejecuten mandatos o Actuaciones para los agentes de supervisión con Tivoli Enterprise Monitoring Agent Framework V6.3 o posterior. Si la modalidad de compatibilidad de seguridad TEMS no está habilitada y tiene un servidor de portal o el servidor de supervisión de la versión anterior a V6.3, las Actuaciones o

mandatos **tacmd executecommand** pueden rechazarse como no autorizados y auditados. Cuando se habilita la modalidad de compatibilidad de seguridad TEMS, la identidad del usuario original no está disponible en los registros de auditoría. La práctica recomendada es actualizar la infraestructura a IBM Tivoli Monitoring V6.3 o posterior e inhabilitar la modalidad de compatibilidad de TEMS para lograr la máxima seguridad y garantía de que la identidad de las ejecuciones de Actuaciones y **tacmd executecommand** se audita debidamente.

También puede utilizar políticas de AAGP para controlar qué usuarios pueden ejecutar una Actuación o **tacmd executecommand** en un sistema gestionado. Para obtener más detalles, consulte "Perfil de grupo de autorización de acceso" en la página 417.

Capítulo 10. Integración de sucesos de situación con Tivoli Enterprise Console

Si el entorno de supervisión incluye el Tivoli Enterprise Console event server y el reenvío de sucesos de situación se ha configurado en el Tivoli Enterprise Monitoring Server concentrador, puede reenviar sucesos de situación generados por los agentes de Tivoli Enterprise Monitoring al servidor de sucesos.

El manual *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm) contiene las instrucciones para habilitar el reenvío de sucesos de situación: configuración del servidor de sucesos para que reciba los sucesos, instalación del componente de sincronización de sucesos en el servidor de sucesos, habilitación del reenvío de situaciones en el servidor de supervisión concentrador y definición de un destino de Event Integration Facility (EIF) predeterminado.

Correlación predeterminada de sucesos de situación con sucesos de IBM Tivoli Enterprise Console

Este apartado proporciona información sobre la correlación de atributos de sucesos de situación con sucesos de IBM Tivoli Enterprise Console. Puede utilizar esta información de correlación al reenviar un suceso de situación a IBM Tivoli Enterprise Console y desea escribir reglas de correlación en IBM Tivoli Enterprise Console.

El reemisor de sucesos de situación genera un suceso de IBM Tivoli Enterprise Console con una clase de suceso basándose en el grupo de atributos asociado con la situación. Cuando el suceso de situación se reenvía al servidor de sucesos, la clase de suceso generada asociada hereda las definiciones de atributo de clase de sucesos (directa o indirectamente) del padre: clase *Omegamon_Base*. Dado que IBM Tivoli Enterprise Console utiliza clases de sucesos jerárquicas, utilice la clase padre Omegamon_Base cuando desee escribir una regla para todos los sucesos de situación que reenvíe al servidor de sucesos.

Omegamon_Base se describe del modo siguiente:

```
Omegamon_Base ISA EVENT
DEFINES {
   cms_hostname: STRING;
   cms_port: STRING;
   integration_type: STRING;
   master_reset_flag: STRING;
   appl_label:STRING;
   situation_name: STRING;
   situation_origin: STRING;
   situation_displayitem: STRING;
   situation_time: STRING;
   situation_status: STRING;
   situation_eventdata: STRING;
  situation_type: STRING;
  situation_thrunode: STRING;
   situation_group: STRING;
   situation_fullname: STRING;  }; END;
```

© Copyright IBM Corp. 2005, 2013

En casos especializados donde se correlaciona un suceso de situación en una clase de suceso de IBM Tivoli Enterprise Console existente y no se puede modificar la jerarquía de sucesos (Omegamon_Base no se puede añadir a la jerarquía) es importante que las ranuras de Omegamon_Base se incluyan en la clase de sucesos existente o en una clase de algún lugar de la jerarquía. Este mecanismo no es el preferido porque no permite que una regla reconozca la presencia de Omegamon_Base en la jerarquía de sucesos.

Como parte de la correlación genérica para estas situaciones, el reemisor de sucesos de IBM Tivoli Monitoring asigna valores asociados para los atributos definidos de la clase de sucesos al reenviar un suceso al Tivoli Enterprise Console event server. Además de estos atributos de clase de sucesos, se asignan valores a los siguientes atributos heredados de la clase EVENT, si están disponibles: source, hostname, fqhostname, origin, sub_origin, adapter_host, origin, severity y atributos de mensaje que se heredan de la clase EVENT base.

Tabla 26. Atributos de clase de suceso de IBM Tivoli Enterprise Console

Atributos de clases de sucesos	**Valores y significado**
adapter_host	Atributo de clase EVENT base. Igual que hostname (véase más abajo). Son datos específicos de aplicación relacionados con el suceso, si existen.
appl_label	Reservado para uso futuro.
cms_hostname	Nombre de host TCP/IP del Tivoli Enterprise Monitoring Server que reenvía el suceso.
cms_port	El puerto del servidor de supervisión en el que el servicio web está a la escucha.
fqhostname	Atributo de clase EVENT base que contiene el nombre de host totalmente calificado, si está disponible.
nombre_host	Atributo de clase EVENT base que contiene el nombre de host TCP/IP del sistema gestionado donde se origina el suceso, si está disponible.
integration_type	Indicador para ayudar al rendimiento de IBM Tivoli Enterprise Console. • `N` para un suceso nuevo, la primera vez que se genera el suceso • `U` para el suceso de actualización y los siguientes cambios de estado de sucesos
master_reset_flag	Indicador de restablecimiento maestro establecido para sucesos de restablecimiento maestros. El valor es NULL para todos los demás sucesos: • `R` para master_reset de reinicio del servidor de Tivoli Enterprise Monitoring • `S` para master_reset en espera activa
msg	Atributo de clase EVENT base que contiene el nombre de situación y la fórmula.
origin	Atributo de clase EVENT base contenido en la dirección TCP/IP del sistema gestionado donde se origina el suceso, si está disponible. La dirección es en formato decimal con puntos.
severity	Atributo de clase EVENT base que contiene la gravedad resuelta.

Tabla 26. Atributos de clase de suceso de IBM Tivoli Enterprise Console (continuación)

Atributos de clases de sucesos	**Valores y significado**
situation_displayitem	Elemento de visualización de situación asociada, si está disponible.
situation_eventdata	Datos de suceso de situación sin formato de la segunda fila de datos de suceso, si existen. Los atributos de datos de suceso están en formato de pares de clave-valor. Los datos de sucesos se pueden truncar porque el Event Integration Facility impone un límite de tamaño de 2 KB.
situation_group	Uno o varios nombres de grupos de situaciones (con un máximo de 5) de los que la situación es miembro.
situation_fullname	Nombre visualizado de la situación asociada.
situation_name	Identificador exclusivo asignado a la situación.
situation_origin	Nombre de sistema gestionado donde se ha originado el suceso de situación. Tiene el mismo valor que sub_source.
situation_status	Estatus actual del suceso de situación.
situation_time	Indicación de fecha y hora del suceso de situación.
situation_type	Tipo de suceso de situación: **S** para suceso muestreado, **P** para suceso puro.
situation_thrunode	Reservado para uso futuro.
source	Atributo de clase EVENT base que contiene **ITM**
sub_origin	Atributo de clase EVENT base. Es igual que el nombre de sistema gestionado para el situation_displayitem asociado, si existe.
sub_source	Atributo de clase EVENT base que contiene el nombre de sistema gestionado de origen para la situación asociada.

Expansión de una descripción de situación de mensaje de suceso genérica

La ranura de mensaje le proporciona un modo descriptivo de examinar un suceso en IBM Tivoli Enterprise Console.

El nombre de situación solo no proporciona identificación de suceso detallada donde haya una gran cantidad de sucesos parecidos de diversos orígenes. En lugar de ello, el nombre de situación en la ranura de mensaje enviada del servidor de supervisión concentrador al servidor de sucesos se expande para incluir los siguientes atributos de suceso:

Nombre-Situación [(fórmula) ON Nombre-Sistema-Gestionado ON ELEMENTO-VISUALIZACIÓN (pares Nombre-Valor de umbral)]

donde:

Situation-Name
Nombre de la situación.

formula
La fórmula indica cómo se evalúa la situación.

Managed-System-Name
Agente o sistema gestionado.

DISPLAY-ITEM
Identificador que ha desencadenado la situación si hay más de una instancia. Es opcional y sólo se utiliza si se especifica un elemento de visualización en la definición de situación.

pares Nombre-Valor de umbral
Datos sin procesar que la situación utiliza para evaluar si se desencadena.

```
Ejemplos:
NT_Critical_Process [(Process_CPU > 4 AND Thread_Count > 50)
  ON IBM-AGX02:NT
  (Process_CPU = 8 AND Thread_Count = 56)]

NT_Disk_Full [(Free_Megabytes < 1000000)
  ON "IBM-AGX02:NT"
  ON D: (Free_Megabytes = 100)]
```

Correlación genérica para ranuras específicas de agente

La correlación genérica identifica la clase de suceso de destino basándose en información de una situación que se desencadena y se reenvía al servidor de sucesos.

El nombre de clase del suceso de IBM Tivoli Enterprise Console se deriva del grupo de atributos asociado con la situación. Es una combinación de **ITM_** más el nombre de grupo de atributos asociado con la situación. Por ejemplo, una situación que utiliza el atributo de atributos NT_Process generará un suceso de IBM Tivoli Enterprise Console con la clase *ITM_NT_Process*.

Nota: Algunos agentes tienen nombres de grupo de atributos muy largos, lo que puede causar que el nombre de clase de suceso generado exceda el límite impuesto por el servidor de sucesos. En estos casos, el nombre de clase de suceso será una combinación de **ITM_** más el nombre de tabla del grupo de atributos.

Los valores de atributo de suceso adicionales se llenan con los valores de atributo de situación de los datos de sucesos de situación. Los nombres de ranura son los nombres de atributo después del proceso de caracteres especiales.

Por ejemplo, una situación que utiliza el atributo Process_CPU hace que se genere una ranura process_cpu en el suceso de IBM Tivoli Enterprise Console. En el caso de que el nombre de atributo esté en conflicto con los nombres de ranura en la clase EVENT de IBM Tivoli Enterprise Console o la clase Omegamon_Base, el *nombreaplicación* asociado con el grupo de atributos, por ejemplo: *knt_*, se añade delante del nombre de atributo para formar el nombre de ranura.

Para situaciones complejas, la definición de situación puede implicar más de un grupo de atributos. En este caso, la clase de suceso IBM Tivoli Enterprise Console utilizada se deriva del primer grupo de atributos encontrado en los datos de suceso de la situación desencadenante. La excepción se produce cuando el primer grupo de atributos encontrado es Local_Time o Universal_Time; entonces se pasa de largo y se utiliza el siguiente grupo de atributos diferente, si existe.

Por ejemplo, si se escribe una situación para los grupos de atributos NT_Process y NT_System, donde NT_Process es el primer grupo de atributos, se utiliza la clase de suceso IBM Tivoli Enterprise Console event *ITM_NT_Process*. Se generan ranuras de sucesos adicionales basándose en los atributos del grupo de atributos seleccionado.

Tabla 27. Caracteres especiales para grupos y nombres de atributos de sucesos IBM Tivoli Enterprise Console generados a partir de sucesos de situación reenviados.

El carácter:	**Se convierte en:**
<mayúsculas> (sólo se aplica a nombre de atributo)	<minúsculas> (sólo se aplica a nombre de atributo)
signo de porcentaje %	pct_
E/S	io
R/3	r3
barra inclinada /	_per_
barra inclinada invertida \	_ (subrayado)
<espacio>	_ (subrayado)
(paréntesis de apertura) paréntesis de cierre	_ (subrayado)
< signo menor que >signo mayor que	_ (subrayado)

Nota: Después del proceso de caracteres especiales, se elimina el subrayado inicial y de cola del nombre de ranura o clase de suceso final, si existe.

Asignación de gravedad para sucesos de Tivoli Enterprise Console

La gravedad de un suceso de Tivoli Enterprise Console asociado a una situación se asigna automáticamente desde el nombre de la situación o bien puede establecer una gravedad en el editor de situaciones de Tivoli Enterprise Portal.

La gravedad de un suceso de Tivoli Enterprise Console asociado a una situación se puede especificar directamente bajo el separador EIF del Editor de situaciones. Si no se especifica ninguna gravedad de Tivoli Enterprise Console para una situación, el remisor de sucesos intenta derivar una gravedad a partir del sufijo del nombre de la situación siguiendo esta regla:

Tabla 28. Correlación entre sufijos de nombres de situaciones y gravedad de sucesos de Tivoli Enterprise Console

Sufijo de nombre de situación	**Gravedad de IBM Tivoli Enterprise Console asignada**
Warn o _Warning	AVISO
Cri, _Crit, _Critical	CRÍTICO
ninguno de las anteriores	DESCONOCIDO

Localización de ranuras de mensaje

Edite la variable KMS_OMTEC_GLOBALIZATION_LOC para habilitar la globalización de las ranuras de mensajes de sucesos EIF que se correlacionan con los resúmenes de alertas mediante Tivoli Enterprise Console event server.

Acerca de esta tarea

Algunos productos se envían con archivos de correlación de sucesos y paquetes de idiomas. Las ranuras de mensaje de estos sucesos de IBM Tivoli Enterprise Console

definidos están globalizadas. La selección de idioma se realiza mediante una variable de entorno del Tivoli Enterprise Monitoring Server denominada KMS_OMTEC_GLOBALIZATION_LOC.

De forma predeterminada, esta variable se establece en inglés de EE.UU. y las ranuras de mensaje se llenan con los mensajes en inglés de EE.UU. Edite la variable para habilitar uno de los paquetes de idioma que se han instalado en el entorno.

Procedimiento

1. En el sistema en el que se instala el servidor de Tivoli Enterprise Monitoring concentrador, abra el archivo KBBENV:
   - Windows Inicie Manage Tivoli Monitoring Services, pulse con el botón derecho del ratón **Tivoli Enterprise Monitoring Server** y pulse **Avanzado → Editar archivo ENV**.
   - Linux UNIX En un editor de texto, abra el archivo *<dir_instalación>*/config/*<nombre_tems>*_ms_*<dirección>*.cfg, donde *<nombre_tems>* es el valor suministrado durante la configuración del servidor de supervisión y *<dirección>* es la dirección IP o el nombre completo del sistema.
2. Localice (o añada) la variable de entorno KMS_OMTEC_GLOBALIZATION_LOC y escriba el código de idioma y país que desee, donde xx es el código de idioma y XX es el código de idioma: de_DE, en_US, en_GB, es_ES, fr_FR, it_IT, ja_JP, ko_KR, pt_BR, zh_CN, o zh_TW (por ejemplo pt_BR para portugués de Brasil o zh_CN para chino simplificado).

   ```
   KMS_OMTEC_GLOBALIZATION_LOC=xx_XX
   ```
3. Guarde y cierre el archivo de entorno del servidor de supervisión.

Estatus de suceso de situación y generación de sucesos de IBM Tivoli Enterprise Console

Este tema describe el significado de los estatus de suceso de situación y el valor de las ranuras comunes del suceso de IBM Tivoli Enterprise Console generado.

la situación es verdadera

integration_type: N, la primera vez que la situación es verdadera; U, todas las veces subsiguientes

situation_status: Y

situation_name: Nombre de la situación

situation_display_item: Valor del atributo seleccionado como elemento de visualización en la definición de situación, si existe.

master_reset_flag: Ninguno

restablecimiento de situación (ya no es verdadera)

integration_type: U

situation_status: N

situation_name: Nombre de la situación

situation_display_item: Valor del atributo seleccionado como elemento de visualización en la definición de situación, si existe.

master_reset_flag: Ninguno

acknowledge

integration_type: U

situation_status: A

situation_name: Nombre de la situación

situation_display_item: Valor del atributo seleccionado como elemento de visualización en la definición de situación, si existe.

master_reset_flag: Ninguno

inicio de situación

integration_type: Ninguno

situation_status: S

situation_name: Nombre de la situación

situation_display_item: Ninguno

master_reset_flag: Ninguno

No se reenvía ningún suceso de IBM Tivoli Enterprise Console.

detención de situación

integration_type: U

situation_status: P

situation_name: Nombre de la situación

situation_display_item: Ninguno

master_reset_flag: Ninguno

Todos los sucesos de situación abiertos que se han originado en este Tivoli Enterprise Monitoring Server se cerrarán en el servidor de sucesos.

error de arranque de situación

integration_type: Ninguno

situation_status: X

situation_name: Nombre de la situación

situation_display_item: Ninguno

master_reset_flag: Ninguno

No se reenvía ningún suceso de IBM Tivoli Enterprise Console.

reconocimiento caducado

integration_type: U

situation_status: F

situation_name: Nombre de la situación

situation_display_item: Valor del atributo seleccionado como elemento de visualización en la definición de situación, si existe.

master_reset_flag: Ninguno

La caducidad que se ha especificado en el reconocimiento ha caducado.

resurface

integration_type: U

situation_status: E

situation_name: Nombre de la situación

situation_display_item: Valor del atributo seleccionado como elemento de visualización en la definición de situación, si existe.

master_reset_flag: Ninguno

El reconocimiento se ha eliminado antes de que caducara y la situación sigue siendo verdadera.

hub start

integration_type: Ninguno

situation_status: N

situation_name: "**'

situation_display_item: Ninguno

master_reset_flag: R

Una vez que se hayan iniciado los servidores de supervisión concentrador, se envía un suceso de restablecimiento maestro con situation_status=N. El restablecimiento maestro hace que el servidor de sucesos cierre todos los sucesos de situación abiertos del servidor de supervisión concentrador (valor `cms_hostname`).

hub restart

integration_type: Ninguno

situation_status: N

situation_name: "**'

situation_display_item: Ninguno

master_reset_flag: R

Una vez iniciado el servidor de supervisión concentrador, se envía un suceso de restablecimiento maestro con situation_status=N. El restablecimiento maestro hace que el servidor de sucesos cierre todos los sucesos de situación abiertos del servidor de supervisión concentrador (valor `cms_hostname`).

toma de control en espera de concentrador

integration_type: Ninguno

situation_status: N

situation_name: "**"

situation_display_item: Ninguno

master_reset_flag: S

Después de que se lleve a cabo la conmutación del servidor de supervisión concentrador, se envía un suceso de restablecimiento maestro de espera activa con situation_status=N. El restablecimiento maestro hace que el servidor de sucesos cierre todos los sucesos de situación abiertos del servidor de supervisión concentrador. El nombre del concentrador primario antiguo está en la ranura `situation_origin`.

Nota: El valor de `integration_type` lo utiliza únicamente la regla de sincronización de IBM Tivoli Enterprise Console para mejorar el rendimiento. No tiene ningún otro significado relacionado con el suceso.

Sincronización de sucesos de situación

El componente de sincronización de sucesos, Event Integration Facility o EIF, devuelve al Tivoli Enterprise Monitoring Server actualizaciones de sucesos de situación que se reenvían al servidor de sucesos de Tivoli Enterprise Console. Las vistas de sucesos de la consola de sucesos de situación, la consola de sucesos comunes y Tivoli Enterprise Console se sincronizan con el estado actualizado de los sucesos. Si está supervisando datos de sucesos de supervisión desde un sistema

de gestión de sucesos soportado en la vista de sucesos de Tivoli Enterprise Console o en la vista de la consola de sucesos comunes, podrá filtrar los sucesos reenviados.

Comprobación de la memoria caché de sucesos de IBM Tivoli Enterprise Console

La memoria caché de sucesos de reglas del servidor de sucesos debe ser suficientemente grande para contener el volumen de sucesos esperados en un momento determinado.

Para comprobar el tamaño de memoria caché de reglas para un servidor de sucesos en ejecución, ejecute el siguiente mandato de IBM Tivoli Enterprise Console:

```
wlsesvrcfg -c
```

Para establecer este tamaño de memoria caché de reglas, ejecute el mandato de IBM Tivoli Enterprise Console:

```
wsetesvrcfg -c número_de_sucesos
```

Nota: Para obtener más información sobre estos dos mandatos, consulte el tema sobre "Mandatos del servidor de sucesos" en el manual *Tivoli Enterprise Console Command and Task Reference*.

Si la memoria caché de sucesos de reglas se llena, el motor de reglas de IBM Tivoli Enterprise Console genera un suceso TEC_Notice `Rule Cache full: forced cleaning` (Memoria caché de sucesos llena: limpieza forzosa), que indica que se ha eliminado el 5 por ciento de los sucesos de la memoria caché. Los sucesos se eliminan en orden de antigüedad, eliminando primero los sucesos más antiguos y dejando que se procesen los sucesos más nuevos.

Cuando el servidor de supervisión concentrador reenvía una actualización de estatus para un suceso de situación anteriormente reenviado al Tivoli Enterprise Console event server, si el suceso de situación original se suprime de la memoria caché de sucesos de reglas, se genera un suceso TEC_ITM_OM_Situation_Sync_Error para indicar que el servidor de supervisión y el servidor de sucesos están desincronizados.

Cuando se utiliza cualquier visor de IBM Tivoli Enterprise Console para reconocer o cerrar cualquier suceso de situación, si el suceso de situación se ha suprimido de la memoria caché de sucesos de reglas, el motor de reglas de IBM Tivoli Enterprise Console no procesa el cambio de estatus. Asimismo, la actualización de suceso de situación no se reenvía al Tivoli Enterprise Monitoring Server de origen. Este comportamiento se produce porque el motor de reglas de IBM Tivoli Enterprise Console no procesa ningún cambio de estatus de suceso para ningún suceso que no esté contenido en la memoria caché de sucesos de reglas. En este caso, el cambio de estatus de sucesos sólo se actualiza en la base de datos de IBM Tivoli Enterprise Console.

Ambas situaciones se pueden remediar realizando un análisis de parámetros de configuración de servidor de IBM Tivoli Enterprise Console y un análisis de rendimiento para determinar los valores de parámetros de configuración óptimos y los requisitos de rendimiento deseados. Consulte el tema sobre "Conceptos sobre el motor de reglas" en el manual *IBM IBM Tivoli Enterprise Console Rule Developer's Guide* para obtener más información.

Cambio de la configuración de la sincronización de sucesos en el servidor de sucesos

Si desea cambiar cualquiera de los valores de la sincronización de sucesos en el servidor de sucesos, utilice el mandato **sitconfig.sh**.

Acerca de esta tarea

Puede ejecutar este mandato utilizando una de las opciones siguientes:

Procedimiento

- Modifique manualmente el archivo de configuración para la sincronización de sucesos (denominado `situpdate.conf` de forma predeterminada y ubicado en el directorio `/etc/TME/TEC/OM_TEC` en sistemas operativos como UNIX y en el directorio %SystemDrive%\Archivos de programa\TME\TEC\OM_TEC\etc en Windows) y, a continuación, ejecute el mandato siguiente:

  ```
  sitconfig.sh update <nombre_archivo_configuración>
  ```

- Ejecute el mandato **sitconfig.sh** directamente, especificando únicamente los valores que desea cambiar. Consulte la publicación *IBM Tivoli Monitoring: Consulta de mandatos* para ver la sintaxis completa de este mandato.

Qué hacer a continuación

Después de cambiar la configuración de la sincronización de sucesos, debe detener y reiniciar manualmente el proceso de reemisor de actualizaciones de la situación desde el directorio `$BINDIR/TME/TEC/OM_TEC/bin` con los mandatos **stopSUF** y **startSUF**.

Definición de servidores de supervisión adicionales para la sincronización de sucesos en el servidor de sucesos

Para cada servidor de supervisión que está reenviando sucesos de situación al servidor de sucesos, debe tener definida la información de servidor necesaria para que el proceso de reenvío de actualizaciones de situaciones reenvíe las actualizaciones de sucesos de situaciones al servidor de supervisión de origen.

Acerca de esta tarea

Ejecute el mandato siguiente para añadir información de servidor de supervisión nueva:

```
sitconfsvruser.sh add serverid=servidor
userid=usuario password=contraseña
```

donde:

serverid=*servidor*
: El nombre de host completamente calificado del servidor de supervisión.

userid=*usuario*
: ID de usuario para acceder al sistema donde se ejecuta el servidor de supervisión.

password=*contraseña*
: Contraseña para acceder al sistema.

Repita este mandato para cada servidor de supervisión que desea añadir.

Qué hacer a continuación

Después de cambiar la configuración de la sincronización de sucesos, debe detener y reiniciar manualmente el proceso de remisor de actualizaciones de situaciones desde el directorio `$BINDIR/TME/TEC/OM_TEC/bin` con los mandatos **stopSUF** y **startSUF** (extensión de archivo .cmd en Windows; .sh en sistemas operativos como UNIX).

Cierre de sucesos muestreados

Cuando se reenvía un suceso de situación desde una situación muestreada al IBM Tivoli Enterprise Console y dicho suceso se cierra a continuación en el servidor de sucesos, el comportamiento de la sincronización de sucesos es enviar una solicitud al Tivoli Enterprise Monitoring Server para que reconozca la situación con un tiempo de espera especificado. Esto se debe a que, si se cierran sucesos de situaciones muestreadas, se producen problemas con la posibilidad de activación de la situación después del cierre en IBM Tivoli Monitoring.

Acerca de esta tarea

Si el reconocimiento de la situación caduca y la situación sigue siendo verdadera, se abre un nuevo suceso de situación en IBM Tivoli Enterprise Console. Si la situación se convierte en falsa, se restablece a sí misma en IBM Tivoli Monitoring y el suceso permanece cerrado en IBM Tivoli Enterprise Console.

El tiempo de caducidad de reconocimiento predeterminado es de 59 minutos. Esto se puede cambiar en el archivo de configuración de tiempos de espera de situación del servidor de sucesos (`sit_timeouts.conf`). Asimismo, en este archivo se pueden configurar tiempos de caducidad para situaciones individuales. Después de editar este archivo, puede hacer que se carguen dinámicamente los tiempos de caducidad en la regla de IBM Tivoli Enterprise Console utilizando el mandato de renovación `sitconfig.sh` en `$BINDIR/TME/TEC/OM_TEC/bin`.

Cambio de parámetros de conjunto de reglas para el archivo de conjunto de reglas omegamon.rls

El archivo de conjunto de reglas omegamon.rls tiene parámetros que puede editar, de acuerdo con el entorno, para ajustar el rendimiento o para establecer sus propios valores personalizados. Con estos parámetros, puede escribir y personalizar las reglas de IBM Tivoli Enterprise Console. Durante la instalación, puede elegir la ubicación de la base de reglas. De lo contrario, puede utilizar wrb -lscurrb -path para buscar la base de reglas actual.

A continuación se proporcionan algunas razones por las que es aconsejable cambiar el comportamiento de la regla:

- Para el archivo omegamon.rls, *omegamon_admin* es el nombre del conjunto de reglas pero puede dar al conjunto de reglas el nombre del administrador o algún otro valor.
- De forma similar, el nombre del conjunto de reglas *sit_ack_expired_def_action* se establece en REJECT de forma predeterminada. Este valor significa que siempre que caduca un reconocimiento de suceso de situación en Tivoli Enterprise Portal y el suceso queda abierto (OPEN) en el portal, el servidor de sucesos de IBM Tivoli Enterprise Console rechaza la acción y vuelve a reconocer el suceso en el portal. Tiene la opción de aceptar el cambio iniciado por el portal y, en su lugar, cambiar el estatus en IBM Tivoli Enterprise Console.

Dispone de los siguientes parámetros que el usuario puede configurar:

omegamon_admin
Utilice este identificador cuando una regla definida en este conjunto de reglas cierra un suceso. Este identificador se utiliza para diferenciar las operaciones cerradas que se han originado automáticamente en lugar de que las haya iniciado el operador de consola.

omsync_timeout
Este atributo establece el periodo en segundos durante los que debe esperar para distinguir entre la sincronización de un solo suceso o de varias sucesos. El tiempo de espera predeterminado es de 3 segundos.

omsync_maxentries
Este atributo establece el número máximo de sucesos permitidos por proceso por lotes. El tamaño de proceso por lotes predeterminado es de 100 sucesos.

Aviso: Si se establece este valor en menos de 20 sucesos se pueden producir contenciones en el proceso de tareas de IBM Tivoli Enterprise Console, lo que causará un rendimiento pobre de los sucesos sincronizados al devolverlos al Tivoli Enterprise Monitoring Server.

sit_resurface_def_action
Este atributo determina la acción predeterminada de las reglas en caso de que llegue un suceso de actualización de situación del Tivoli Enterprise Monitoring Server para que resurja o se vuelva a abrir un suceso que ya se ha reconocido. Los dos valores posibles son ACCEPT y REJECT. El valor predeterminado es ACCEPT.

sit_ack_expired_def_action
Este atributo determina la acción predeterminada de las reglas en caso de que llegue un suceso de actualización de situación del Tivoli Enterprise Monitoring Server para que se vuelva a abrir un suceso que ya se ha reconocido. Esto sucede cuando caduca el reconocimiento de una situación en el servidor de supervisión y se vuelve a abrir el suceso de situación. Los dos valores posibles son ACCEPT y REJECT. El valor predeterminado es REJECT.

sf_check_timer
Este atributo especifica el intervalo en el que se comprueba el estado del reemisor de actualización de situación. Lee los sucesos de los archivos de memoria caché y los envía al Tivoli Enterprise Monitoring Server utilizando Web Services. El valor predeterminado es de 10 minutos.

Después de modificar los parámetros de configuración y de guardar omegamon.rls, debe volver a compilar y volver a cargar la base de reglas y reciclar el servidor de sucesos. Para volver a compilar la base de reglas, escriba el siguiente mandato, donde `Nombre_Basereglas` es el nombre de la base de reglas cargada activamente que contiene el conjunto de reglas omegamon.rls:

```
wrb -comprules Nombre_Basereglas
```

Para volver a cargar la base de reglas, emita el mandato siguiente:

```
wrb -loadrb Nombre_Basereglas
```

Para detener el servidor de sucesos, emita el mandato siguiente:

```
wstopesvr
```

Para reiniciar el servidor de sucesos, emita el mandato siguiente:

```
wstartesvr
```

Para obtener más información relacionada con los mandatos **wrb, wstopesvr y wstartesvr**, consulte el manual de consulta de mandatos y tareas (*Command and Task Reference*) en el Centro de información de Tivoli Enterprise Console (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.itec.doc_3.9/welcome_nd.html).

Consideraciones para el ajuste

Los parámetros de integración que soportan acciones en la consola de sucesos de IBM Tivoli Enterprise Console que se reflejan en la consola de sucesos de Tivoli Enterprise Portal proporcionan tiempos de respuesta buenos con una inversión razonable de recursos del sistema.

Los parámetros de ajuste a tener en cuenta incluyen:

- `omsync_timeout` en `omegamon.rls` con un valor predeterminado de 3 segundos.
- `PollingInterval` en la sincronización de sucesos con un valor predeterminado de 3 segundos.
- El intervalo de renovación de consola de sucesos de IBM Tivoli Enterprise Console con un valor predeterminado de 60 segundos
- Intervalo de renovación de consola de sucesos de Tivoli Enterprise Portal

Nota: Los intervalos más cortos hacen que se consuman más recursos de sistema.

El tiempo de entrega de cambios de situación de la consola de sucesos de IBM Tivoli Enterprise Console a la consola de sucesos de Tivoli Enterprise Portal es el resultado del funcionamiento en paralelo de los valores de `omsync_timeout` y `PollingInterval`. Para mejorar el tiempo de respuesta, puede reducir estos valores a un mínimo de 1 segundo. .

Puede ajustar el intervalo de renovación para ambas consolas:

- Para IBM Tivoli Enterprise Console, cambie el rango permitido utilizando la consola de sucesos de IBM Tivoli Enterprise Console – Configuración. En las visualizaciones subsiguientes de vista de sucesos, ajuste las preferencias.
- Para la consola de sucesos de Tivoli Enterprise Portal, pulse **Ver > Renovar cada** para acceder a los intervalos de renovación.

Utilización del programa de utilidad de comprobación de reglas

El programa de utilidad de comprobación de reglas le proporciona la posibilidad de valorar el impacto en un conjunto de reglas existente siempre que cambian los diseños de las clases de sucesos BAROC (Registrador básico de objetos en C). Este programa de utilidad le permite verificar qué reglas puedan quedar afectadas por estos cambios de definición de clase de sucesos.

Existen dos conjuntos de archivos importantes que se utilizan y son necesarios para el programa de utilidad de comprobación de reglas a fin de comprobar los posibles impactos de los cambios de diseño de clases de sucesos en las reglas:

- Archivos de definiciones de clases de suceso BAROC:

  Las definiciones de clases de IBM Tivoli Enterprise Console son jerárquicas por naturaleza con las herencias. Una clase puede heredar de otra clase y todos los atributos de la clase padre están disponibles en la clase hijo. La clase EVENT es

la clase base de IBM Tivoli Enterprise Console. Las demás clases suelen derivar de la clase EVENT de IBM Tivoli Enterprise Console.

En IBM Tivoli Enterprise Console, los archivos de definiciones de clases de suceso BAROC (archivos *.baroc) están ubicados en el subdirectorio TEC_CLASSES de la base de reglas cargada activamente. Proporcionan las definiciones de clase de sucesos utilizadas por el servidor de IBM Tivoli Enterprise Console. Aunque la herramienta está totalmente integrada con IBM Tivoli Enterprise Console y utiliza el subdirectorio TEC_CLASSES de la base de reglas activa por entrada predeterminada, la herramienta no es dependiente de este subdirectorio y acepta como entrada alternativa cualquier otro directorio que contenga los archivos BAROC correctos y en los que el usuario tenga privilegios de lectura.

- Archivos de reglas:

  El lenguaje de reglas de productos de IBM Tivoli Enterprise Console también soporta la naturaleza de herencia de las definiciones de clase de IBM Tivoli Enterprise Console. Cuando un predicado de la regla de IBM Tivoli Enterprise Console busca una clase determinada, todas las clases que heredan de dicha clase en particular también satisfacen el predicado de regla.

En IBM Tivoli Enterprise Console, los archivos de conjunto de reglas (archivos *.rls) están ubicados en el subdirectorio TEC_RULES de la base de reglas carga activamente. Proporcionan los conjuntos de reglas y se despliegan en el servidor de IBM Tivoli Enterprise Console. Aunque la herramienta está totalmente integrada con IBM Tivoli Enterprise Console y utiliza el subdirectorio TEC_RULES de la base de reglas activa por entrada predeterminada, la herramienta no es dependiente de este subdirectorio. La herramienta acepta como entrada alternativa cualquier otro directorio que contenga los conjuntos de reglas correctos y en los que el usuario tenga privilegios de lectura.

El programa de utilidad de comprobación de reglas se incluye con IBM Tivoli Monitoring. Este programa de utilidad se instala en el directorio $BINDIR/TME/TEC/OM_TEC/bin como parte de la instalación de sincronización de sucesos de IBM Tivoli Enterprise Console. No necesita ninguna configuración de directorio específica si se otorgan los privilegios necesarios para el acceso a los archivos de entrada y salida.

Para ejecutar el mandato de comprobación de reglas debe tener:

- Acceso de lectura a los archivos *.rls y *.baroc que se utilizan como entradas.
- Acceso de grabación a la salida que se utiliza para almacenar los resultados de la comprobación.
- Autorización de administrador de IBM Tivoli Enterprise Console.
- Cuando no se especifican las opciones `–cd` y `–rd`, el usuario que emite el mandato debe tener la autorización TME apropiada y verificar el nivel de submandatos que son necesarios.

Para ejecutar el programa de utilidad de comprobación de reglas y ver la salida de ejemplo, consulte la publicación *Consulta de mandatos*.

Edición de la configuración de Recurso de integración de sucesos

Edite el archivo EIF (**Tivoli Event Integration Facility**) para personalizar la configuración como, por ejemplo, para especificar hasta cinco servidores EIF de toma de control o para ajustar el tamaño de la memoria caché de sucesos.

Antes de empezar

Después de que se habilite EIF (**Tivoli Event Integration Facility**) en el servidor de supervisión concentrador y se especifique el servidor EIF predeterminado (Tivoli Enterprise Console event server o prueba de Netcool/OMNIbus EIF) y el número de puerto, se actualiza el archivo de configuración de EIF con esta información. Este archivo de configuración especifica el receptor de EIF predeterminado de los sucesos de situación reenviados.

Consulte el documento *Consulta del recurso de integración de sucesos de Tivoli Event* para obtener más detalles sobre los parámetros y los valores.

Si está habilitando EIF después de que se haya instalado y configurado el entorno, debe habilitar EIF a través de Manage Tivoli Enterprise Monitoring Services o con el mandato de CLI **itmcmd config -S** y a continuación reiniciar el servidor de supervisión y el servidor de portal.

Consulte la publicación *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm) para obtener instrucciones sobre cómo configurar el servidor de supervisión para habilitar el Recurso de integración de sucesos de Tivoli.

Acerca de esta tarea

Realice estos pasos para editar el archivo de configuración EIF:

Procedimiento

1. Abra el archivo `om_tec.config`:
   - Windows En la ventana Manage Tivoli Monitoring Services, pulse con el botón derecho del ratón en el servidor de Tivoli Enterprise Monitoring y pulse **Avanzado → Editar configuración EIF**.
   - Linux UNIX Abra *dir_instalación*`/tables/`*nombre_host*`/TECLIB/om_tec.config` en un editor de texto.
2. Edite cualquiera de los parámetros de configuración del editor de sucesos para el recurso de integración de sucesos.

Opción	Descripción
ServerLocation=	Es el *nombre de host* o la *dirección ip* del servidor de sucesos. Para proporcionar la toma de control de sucesos, puede indicar un máximo de cinco servidores de sucesos predeterminados, separando cada uno con una coma. Cuando el servidor de sucesos predeterminado no está disponible, el suceso de situación va al siguiente servidor de la lista. Valor: **tec_server_addr**

Opción	Descripción
ServerPort=	El puerto de escucha de servidor, cuyo valor predeterminado es 5529. Especifique `0` si el servidor de sucesos utiliza el correlacionador de puertos. Si ha especificado varias ubicaciones de servidor, añada aquí los números de puerto correspondientes, separando cada uno con una coma. Valor: **[port:0]**
EventMaxSize=	Número máximo de caracteres permitidos en el suceso. Este número está inhabilitado de forma predeterminada. Para habilitarlo, elimine el símbolo de almohadilla (#) al principio de la línea. Valor: **4096**
RetryInterval=	Número de veces que se debe reintentar la conexión con el servidor de sucesos antes de devolver un error. Valor: **5**
getport_total_timeout_usec=	El número de segundos durante los cuales se debe continuar intentando la conexión al puerto de servidor de sucesos antes de que se exceda el tiempo de espera. El valor predeterminado es 14 horas. Valor: **50500**
NO_UTF8_CONVERSION=	Los sucesos ya están en formato UTF8; no es necesaria ninguna conversión. Este parámetro se debe establecer en `YES`. Valor: **YES**
ConnectionMode=	Modalidad de conexión. Valor: **co**
BufferEvents=	Indica si EIF pone el suceso en el almacenamiento intermedio. Se debe establecer en YES. Valor: **YES**
BufEvtMaxSize=	Tamaño máximo de la memoria caché de sucesos. El valor predeterminado es inicialmente 4096 KB y puede cambiarlo aquí. Valor: **4096**
BufEvtPath=	Vía de acceso del archivo de memoria caché de sucesos. El valor predeterminado es ./TECLIB/om_tec.cache. Valor: **./TECLIB/om_tec.cache**
FilterMode=	Habilite el filtro de sucesos. Éste se establece en OUT de forma predeterminada. Valor: **OUT**

Opción	Descripción
TcpTimeout=	Utilice este parámetro para la modalidad orientada a la conexión, que permite que el agente exceda el tiempo de espera en la llamada de conexión al servidor primario si éste no está disponible, y a continuación realice la migración tras error al servidor secundario. Por ejemplo, utilice este parámetro cuando el cortafuegos bloquee las llamadas de ping de ICMP. El valor está en segundos. Valor: **75** **Restricción:** No se puede utilizar con los parámetros PingTimeout y NumberOfPingCalls.
PingTimeout=	Tiempo máximo de espera cuando la llamada de ping intenta acceder al servidor de destino. Si no se especifica PingTimeout, EIF no ejecuta una llamada de ping antes de realizar la llamada de conexión de socket. Este parámetro se puede utilizar con los tipos de conexión orientado a conexión o sin conexión. Este parámetro se debe utilizar con NumberOfPingCalls. El valor está en segundos. Valor: **75** **Restricción:** No se puede utilizar con el parámetro TcpTimeout.
NumberOfPingCalls=	Número de veces que se debe invocar la función ping antes de determinar si el servidor de destino está disponible. Debido a algunas configuraciones de TCP/IP, la primera llamada de ping tras la desconexión del servidor de destino puede devolverse satisfactoriamente. Este parámetro se puede utilizar con los tipos de conexión orientado a conexión o sin conexión. Este parámetro se debe utilizar con PingTimeout. **Restricción:** No se puede utilizar con el parámetro TcpTimeout.
Filter:	Para filtrar clases específicas, utilice esta palabra clave. De forma predeterminada, los sucesos de situación de la clase *ITM_Generic* y los que no envían ningún distintivo de restablecimiento maestro no se formatean. Valor: **Class=ITM_Generic; master_reset_flag='';**

3. Cuando haya terminado de editar `om_tec.config`, guarde el archivo.
4. Debe reiniciar el servidor de supervisión o, alternativamente, puede utilizar el mandato **refreshTECinfo** para completar las actualizaciones sin ten tener que reiniciar el servidor de supervisión. Para utilizar este mandato, inicie la sesión en la interfaz de línea de mandatos con **tacmd login** y, a continuación, ejecute **tacmd refreshTECinfo -t eif** para completar la configuración de EIF.

Resultados

El servidor de supervisión utiliza la configuración de EIF editada para reenviar sucesos al receptor.

Qué hacer a continuación

Si es la primera vez que ha configurado el reenvío de EIF tras una actualización de Tivoli Management Services, también debe reciclar el Tivoli Enterprise Portal Server y los usuarios deben reiniciar Tivoli Enterprise Portal. De lo contrario, el separador EIF no aparecerá en el editor de situaciones.

Un método alternativo para editar la configuración de EIF es a través de la interfaz de línea de mandatos, con **tacmd createEventDest**. Consulte *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) para ver una descripción.

Referencia relacionada:

Consulta del recurso de integración de sucesos de Tivoli
Centro de información de Tivoli Enterprise Console para obtener más información sobre los parámetros y valores.

Tivoli Monitoring: Guía de instalación y configuración
Configure el servidor de supervisión para habilitar el recurso de integración de sucesos de Tivoli

Tivoli Monitoring: Consulta de mandatos
Complete las actualizaciones de configuración de EIF con tacmd refreshTECinfo; realice actualizaciones con tacmd createEventDest

Especificación del reenvío de EIF para un suceso de situación

Cuando se ha configurado el servidor de Tivoli Enterprise Monitoring Server para **Tivoli Event Integration Facility**, los sucesos de situación se pueden reenviar al receptor de sucesos. Utilice el editor de situaciones de Tivoli Enterprise Portal para definir el receptor de sucesos de destino para las situaciones individuales.

Antes de empezar

Una de las opciones de configuración de Tivoli Enterprise Monitoring Server es **Tivoli Event Integration Facility**. Cuando esta opción está habilitada, se especifica el receptor de EIF predeterminado en la ventana Ubicación y número de puerto del servidor de sucesos que se abre (descrita en las publicaciones *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm) y *Consulta del recurso de integración de sucesos de Tivoli Event*). A partir de ese momento, todos los sucesos de situación se reenvían al receptor de EIF de forma predeterminada, utilizando la gravedad derivada del nombre de situación o la gravedad crítica si no se deriva ninguna.

Puede alterar temporalmente este valor predeterminado para situaciones individuales mediante el separador EIF del Editor de situaciones en Tivoli Enterprise Portal.

Se pueden especificar un máximo de ocho destinos de suceso para un suceso de situación reenviado. La asociación de destino de suceso se puede realizar en el

separador EIF del editor de situaciones. Los destinos de sucesos se deben predefinir con el mandato **tacmd createEventDest**. Los cambios en la lista de destinos de suceso no entrarán en vigor hasta que se emita el mandato **tacmd refreshTECinfo** o se reinicie el servidor de supervisión concentrador. Además, si es la primera vez que ha configurado el reenvío de EIF tras una actualización de Tivoli Management Services, también debe reciclar el Tivoli Enterprise Portal Server y los usuarios deben reiniciar Tivoli Enterprise Portal para ver el separador EIF en el editor de situaciones..

Los destinos de suceso alternativos que se han especificado en el archivo tecserver.txt desde release anteriores se definirán automáticamente como destinos de suceso válidos como parte de la migración de archivo tecserver.txt.

Si se han especificado varios destinos de sucesos predeterminados (es decir, varios servidores de destino de sucesos tienen el valor predeterminado establecido en 'Y'), se deben seleccionar todos en Tivoli Enterprise Portal para que los sucesos se reenvíen a todos los destinos predeterminados definidos.

Acerca de esta tarea

Realice estos pasos para especificar el receptor EIF de destino y la gravedad de sucesos reenviados:

Procedimiento

1. En la vista Navigator de Tivoli Enterprise Portal, pulse con el botón derecho del ratón en el elemento de Navigator con el que está asociada la situación y pulse **Situaciones** o pulse **Editor de situaciones** en la barra de herramientas principal.
2. Seleccione la situación a reenviar.
3. Pulse el separador **EIF**.
4. Seleccione **Reenvío de sucesos a un receptor EIF** para especificar que se envía un suceso EIF para cada suceso que se abre para esta situación.
5. Seleccione **Gravedad de EIF** para aplicar los sucesos reenviados para esta situación. <Gravedad de EIF predeterminada> utiliza la misma gravedad que se utiliza para la situación en este elemento Navigator.
6. Para asignar otros receptores de EIF en lugar de o además del <Receptor de EIF predeterminado>, siga uno de los pasos siguientes:
   - Para añadir un destino, selecciónelo en la lista **Receptores EIF disponibles** y muévalo a la lista de asignados. (Después de seleccionar el primer destino, puede utilizar Control+pulsación para seleccionar otros destinos o Mayús+pulsación para seleccionar todos los destinos entre la primera selección y ésta).
   - Para eliminar un destino, selecciónelo en la lista **Receptores EIF asignados** y muévalo a la lista de disponibles.

   La lista **Receptores EIF disponibles** muestra todos los destinos EIF definidos que se han definido mediante Manage Tivoli Monitoring Services o con el mandato **tacmd createEventDest**. Consulte la publicación *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).
7. Guarde la definición de la situación con sus cambios pulsando **Aplicar**, para que el editor de situaciones continúe abierto o pulsando **Aceptar** para cerrar el editor de situaciones.

Referencia relacionada:

Consulta del recurso de integración de sucesos de Tivoli
Centro de información de Tivoli Enterprise Console para obtener más información sobre los parámetros y valores.

Tivoli Monitoring: Guía de instalación y configuración
Configure el servidor de supervisión para habilitar el recurso de integración de sucesos de Tivoli

Tivoli Monitoring: Consulta de mandatos
Complete las actualizaciones de configuración de EIF con tacmd refreshTECinfo; realice actualizaciones con tacmd createEventDest

Personalización del mensaje de suceso

Desde el separador de **EIF** del Editor de situaciones, puede crear definiciones de correlación para sucesos de situación enviados al receptor de EIF. La ventana Personalización de ranura EIF, que se abre desde el separador **EIF**, sirve para personalizar la correlación entre los sucesos de situación y los sucesos de EIF reenviados, alterando temporalmente la correlación predeterminada entre sucesos de situación y sucesos reenviados a Tivoli Enterprise Console event server.

Cuando el nombre de la ranura base es `msg`, se utiliza la columna Valor literal para la plantilla de mensaje. La plantilla de mensajes consta de texto de mensaje fijo y referencias de sustitución variables, o *símbolos*. El símbolo puede hacer referencia a datos comunes o de ranura de sucesos o a una referencia especial a la fórmula de situación. Las ranuras comunes son las que se incluyen en todos los sucesos reenviados, como situation_name; las ranuras de sucesos son las específicas de la situación. Las siguientes reglas de sintaxis se aplican a la definición de ranuras de sucesos:

- Para una ranura de suceso, utilice el nombre de atributo completo ($Attribute_Table.Attribute_Name$)
- Para una ranura común, utilice el nombre de variable que no está completo (sin . puntos) a no ser que sea el símbolo de situación
- Para una fórmula de situación, utilice $formula$

No se da soporte a los caracteres siguientes: < menor que, > mayor que, " comillas dobles, ' comillas y carácter &. Esta columna sólo está disponible si no se ha seleccionado ningún valor en la columna Atributo correlacionado. Consulte la ayuda en línea de Tivoli Enterprise Portal o el manual *Tivoli Enterprise Portal: Guía del usuario* para obtener más información.

Para la ranura `msg`, los usuarios típicos especificar un Valor literal, no un valor de Atributo correlacionado. Si se especifica un valor en la columna atributo correlacionado para la ranura `msg`, se produce lo siguiente:

- Si **Correlacionar todos los atributos** no está seleccionado, el atributo Correlacionado para `msg` no estará presente en el suceso, y se pasará por alto.
- Si **Correlacionar todos los atributos** está seleccionado, el suceso de Tivoli Enterprise Console solo tendrá la plantilla de mensajes predeterminada y no el atributo Correlacionado especificado en la ranura `msg`.

Actualización del XML utilizado por el Servicio de atributos MCS

El archivo XML predeterminado utilizado por el Servicio de atributos MCS (Multiple Console Support) incluye sólo las clases de suceso definidas en los archivos BAROC dentro de la rama TECLIB de la instalación del servidor de supervisión concentrador. Genere un nuevo archivo XML para la Personalización de ranura EIF siempre que se añada un nuevo tipo de agente a la infraestructura de Tivoli Management Services o cuando se ha añadido una nueva clase de suceso al Tivoli Enterprise Console event server.

Antes de empezar

Si una clase de suceso especificada para una regla no se encuentra dentro del conjunto de definiciones de sucesos actual y continúa generando la regla con el conjunto de definiciones actual, todas las clases de suceso no reconocidas se eliminarán de la regla.

El recurso Personalización de sucesos EIF utiliza el servicio de atributos MCS para presentar una lista de clases de sucesos predefinidas en la lista de **Nombres de clases de sucesos** de la ventana Personalización de ranura EIF, que está disponible en el separador EIF del editor de situaciones de Tivoli Enterprise Portal. Sólo las clases de sucesos pertenecientes a los agentes de sistema operativo están predefinidas y se encuentran en el archivo jar del servicio de atributos MCS. Cuando se añade un nuevo tipo de agente a la infraestructura de Tivoli Management Services o se añade una nueva clase de suceso a un agente, debe generar un nuevo archivo XML MCS y dirigir el Tivoli Enterprise Portal Server al nuevo archivo XML para que las nuevas clases de sucesos aparezcan en la lista de **Nombre de clase de suceso**.

Para generar un nuevo archivo XML MCS, instale el programa de utilidad Tivoli Enterprise Console Event Definition Generator (TEDGEN) que se suministra en el DVD de IBM Tivoli Monitoring **Herramientas**. Instale el programa de utilidad TEDGEN en un sistema en el que esté instalado servidor de supervisión concentrador o servidor de portal o en el que esté instalado Tivoli Enterprise Console. El sistema en el que genere el archivo MCS XML debe tener los archivos BAROC necesarios.

Nota: Las definiciones del archivo XML de MCS reemplazan a las del archivo jar de los servicios de atributos MCS (no se fusionan). Para obtener un archivo XML MCS que contenga las definiciones de clases de suceso de los agentes de sistema operativo y el nuevo agente, asegúrese de que todas las definiciones de BAROC para los agentes de sistema operativo y para el nuevo agente se cargan en el servidor de sucesos IBM Tivoli Enterprise Console o se encuentran en el mismo directorio en servidor de supervisión concentrador o servidor de portal antes de ejecutar el programa de utilidad TEDGEN para generar el archivo XML MCS.

Para instalar y configurar la herramienta TEDGEN, siga estos pasos:

1. Instale el programa de utilidad TEDGEN desde el DVD de IBM Tivoli Monitoring **Herramientas** en el servidor de supervisión concentrador, servidor de portal o donde está instalado Tivoli Enterprise Console. El programa de utilidad se encuentra en el directorio `tec/tedgen` del DVD **Herramientas** y las instrucciones de instalación y configuración se encuentran en el archivo `README.txt` en el mismo directorio.

2. Linux UNIX Si ha instalado el programa de utilidad TEDGEN en un sistema servidor de portal en Linux o UNIX, realice también estos pasos de configuración adicionales:
   a. Cree el directorio *dir_instalación*/tables/cicatrsq/TECLIB si no existe, donde *dir_instalación* es el directorio en el que está instalado IBM Tivoli Monitoring.
   b. Copie los archivos om_tec.baroc y kib.baroc del directorio *dir_instalación*/arch/cq/TECLIB en el directorio *dir_instalación*/tables/cicatrsq/TECLIB, donde arch es el directorio de arquitectura para el servidor de portal.

Acerca de esta tarea

En estos pasos se presupone que ha instalado el programa de utilidad TEDGEN en el sistema en el que desea ejecutar la herramienta; en el servidor de sucesos de Tivoli Enterprise Console, el servidor de supervisión concentrador o el servidor de portal.

También debe instalar el soporte de aplicaciones para los agentes cuyos sucesos EIF se personalizan en el servidor de supervisión concentrador o servidor de portal en el que desea ejecutar el programa de utilidad. Si desea ejecutar el programa de utilidad TEDGEN en Tivoli Enterprise Console, también deberá cargar los archivos BAROC del agente en el sistema en el se ha instalado Tivoli Enterprise Console.

Después de instalar el programa de utilidad y el soporte de aplicaciones, ejecute el mandato TEDGEN para crear un nuevo archivo XML para la personalización de ranuras de EIF.

Nota:

- Si ha instalado el programa de utilidad TEDGEN en un servidor de portal instalado en Linux o UNIX, los archivos BAROC no existirán a menos que se haya seleccionado la opción **Instalar el soporte de TEMS para la inicialización remota** durante la instalación del soporte de aplicaciones del agente. Consulte el apartado sobre Instalación de archivos de soporte de aplicaciones en un sistema sin servidor de supervisión en el manual *IBM Tivoli Monitoring: Guía de instalación y configuración*. Esta acción coloca los archivos BAROC en el servidor de portal bajo el directorio *dir_instalación*/tables/ cicatrsq/TECLIB donde *dir_instalación* es el directorio en el que está instalado IBM Tivoli Monitoring.
- Si ha instalado el programa de utilidad TEDGEN en un servidor de portal en Windows, verifique que el directorio TECLIB del servidor de portal contiene los archivos .baroc de los agentes cuyos sucesos desee personalizar. No todos los agentes incluyen sus archivos .baroc en su soporte de aplicaciones de servidor de portal. Si no se encuentra el archivo .baroc de un agente, puede copiarlo del directorio del servidor de supervisión concentrador TECLIB.

Procedimiento

1. Siga uno de estos pasos para ejecutar el mandato TEDGEN:
   - En el sistema en el que se encuentra el servidor de supervisión concentrador o el servidor de portal, emita los mandatos siguientes:

     Windows

     ```
     set CANDLE_HOME=dir_instalación
     cd dir_instalación_TEDGEN\scripts
     tedgen -itmDir dir_instalación\{CMS|CNPS}
     \TECLIB -id id_servidor -xmlPath vía_acceso_archivo_xml_salida
     ```

donde, *dir_instalación* es el directorio en el que está instalado IBM Tivoli Monitoring y *dir_instalación_TEDGEN* es el directorio en el que está instalado el programa de utilidad TEDGEN.

Linux UNIX

```
export CANDLEHOME=dir_instalación
cd dir_instalación:TEDGEN/scripts
tedgen -itmDir
dir_instalación/tables/{nombre_tems|cicatrsq}/
TECLIB -id id_servidor -xmlPath vía_acceso_archivo_xml_salida
```

donde, *dir_instalación* es el directorio en el que está instalado IBM Tivoli Monitoring y *dir_instalación_TEDGEN* es el directorio en el que está instalado el programa de utilidad TEDGEN.

Ejemplo

En el siguiente ejemplo, el servidor de supervisión concentrador llamado **mytems** tiene los archivos BAROC en el directorio TECLIB. El archivo de salida va al mismo directorio y se denomina **tems.xml**.

```
tedgen -itmDir C:\IBM\ITM\CMS\TECLIB -id mytems -xmlPath tems.xml
```

- En el sistema en el que se encuentra el Tivoli Enterprise Console event server, instale el programa de utilidad TEDGEN desde el DVD **Herramientas** que se suministra con el soporte de instalación del servidor de sucesos. Luego cree un nuevo archivo XML:
  a. Emita el mandato **wrb -imprbclass** para importar el archivo BAROC que se instala con el agente recién añadido y los agentes de sistema operativo, si todavía no se han instalado:

     ```
     wrb -imprbclass archivo_clases [ -encoding encoding ]
     [-before archivo_clases | -after archivo_clases] [-force]  base_reglas
     ```

  b. Emita el mandato wrb -loadrb para volver a cargar la base de reglas:

     ```
     wrb -loadrb base_reglas
     ```

  c. Detenga e inicie el servidor de sucesos; para ello, ejecute estos mandatos:

     ```
     wstopesvr
     wstartesvr
     ```

  d. Emita el mandato TEDGEN para generar el archivo XML:

     ```
     tedgen [ -bcDir directorio_clases_baroc | -rbName nombre_base_reglas ]
     -id server_id -xmlPath vía_acceso_archivo_xml_salida
     ```

  Ejemplo

  En el siguiente ejemplo, el archivo XML llamado **tec.xml** se genera a partir de la base de reglas actual en el Tivoli Enterprise Console event server llamado **mytec**.

  ```
  tedgen -id mytec -xmlPath tec.xml
  ```

2. Copie el archivo XML recién generado en el sistema en el que está instalado el servidor de Tivoli Enterprise Portal.
3. Edite el archivo de entorno del servidor de portal para especificar la vía de acceso del archivo XML:
   a. Windows En la ventana Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho del ratón en **Tivoli Enterprise Portal Server** y pulse **Avanzado → Editar archivo ENV** para abrir el archivo `kfwenv` en un editor de texto.

      Linux UNIX Abra *dir_instalación*`/config/cq.ini` en el editor de texto.

   b. Localice la variable de entorno KFW_MCS_XML_FILES y escriba el signo de igual (=) seguido de la vía de acceso del archivo XML de MCS.

c. Guarde y cierre el archivo de entorno.

d. Windows Reinicie el servidor de portal.
Linux UNIX Vuelva a configurar el servidor de portal y luego reinícielo.

Visualización de sucesos desde Universal Agent en Tivoli Enterprise Console

Puesto que todas las aplicaciones de Universal Agent generan dinámicamente sus archivos de catálogo, atributos y ODI, se deben llevar a cabo ciertos pasos manuales para que los sucesos de situación de Universal Agent se visualicen correctamente en Tivoli Enterprise Console.

Antes de empezar

Para que la situación de Universal Agent se pueda convertir correctamente en un suceso de Tivoli Enterprise Console mediante el sistema de reenvío de sucesos de Tivoli Enterprise Console, los archivos de atributos de Universal Agent deben residir en el servidor de Tivoli Enterprise Monitoring concentrador durante la inicialización del concentrador. Si Universal Agent está conectado a un servidor de supervisión remoto, los archivos de catálogo y de atributos de Universal Agent no se propagan al concentrador y la conversión de sucesos de situación de Universal Agent falla.

Acerca de esta tarea

Siga estos pasos para asegurarse de que los archivos de atributos de Universal Agent estén en el servidor de supervisión concentrador y para generar un archivo BAROC con las definiciones de sucesos de situación de Universal Agent, lo que se necesita para analizar y visualizar correctamente los sucesos de Universal Agent en Tivoli Enterprise Console.

Procedimiento

1. Asegúrese de que los archivos de atributos de Universal Agent estén en el concentrador:
   - Conecte temporalmente Universal Agent al servidor de supervisión concentrador para habilitar la carga de los archivos de atributos. Tras establecer una conexión correcta, Universal Agent se puede reconfigurar para que se conecte al servidor de supervisión remoto.
   - Mueva manualmente los archivos de atributos de Universal Agent del servidor de supervisión remoto al concentrador. Ubicación del archivo de atributos:
     Windows *dir_instalación*\CMS\ATTRLIB
     Linux UNIX *dir_instalación*/ tables/tems_name/ATTRLIB.
   - Recicle el servidor de supervisión concentrador.
2. Obtenga los archivos BAROC necesarios para la aplicación Universal Agent
   a. Busque y descargue el *generador de archivos BAROC* desde IBM Integrated Service Management Library.
   b. Ejecute el generador de BAROC, ofreciendo el archivo ODI para la aplicación Universal Agent como entrada. Ubicación de archivo ODI (necesita que Universal Agent se haya conectado correctamente al servidor de supervisión) en el sistema en el que está instalado el servidor de Tivoli Enterprise Portal:

Windows *dir_instalación*\cnps
Linux UNIX *dir_instalación/plataforma*/cq/bin
El formato del nombre del archivo ODI es *xxx*odi*nn*, donde *xxx* es el nombre del agente especificado por la aplicación y *nn* es el número de versión.

c. Después de generar el archivo BAROC, muévalo al servidor de sucesos, luego compílelo y cárguelo.

Utilización de la consola de NetView a través del visor de sucesos de IBM Tivoli Enterprise Console

Puede iniciar la consola IBM Tivoli NetView Java desde las vistas de IBM Tivoli Enterprise Console, navegando de una fila de suceso a los diagnósticos y la topología de red asociados. El suceso seleccionado debe contener un nombre de host o una dirección IP válidos para soportar la visualización de topología del nodo asociado con el suceso. De lo contrario, la vista de topología estándar se visualiza sin un nodo específico seleccionado.

Acerca de esta tarea

Las reglas de IBM Tivoli Enterprise Console sincronizan automáticamente los sucesos reenviados por Tivoli NetView al servidor IBM Tivoli Enterprise Console. Las actualizaciones de estatus de suceso se reflejan en el sistema donde inicia la consola de sucesos de Netview.

Asegúrese de tener los archivos BAROC netview y netview.rls en la base de reglas cargada activamente. Para obtener detalles, consulte la referencia de conjunto de reglas (*Rule Set Reference*) en el Centro de información de Tivoli Enterprise Console (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.itec.doc_3.9/welcome_nd.html).

Si desea utilizar la consola de NetView a través de la vista de IBM Tivoli Enterprise Console de Tivoli Enterprise Portal, debe configurar la variable *NVWC_HOME* en el script shell que inicia el cliente de Tivoli Enterprise Portal de modo que apunte al directorio de instalación de la consola web de NetView.

Para establecer la variable *NVWC_HOME* , siga este procedimiento:

Procedimiento

- Windows *install_dir*\cnp\cnp.bat
- Linux o UNIX *install_dir*/bin/cnp.sh

Qué hacer a continuación

La consola web de NetView debe estar instalada en el sistema en el que se está ejecutando el cliente de Tivoli Enterprise Portal para iniciar la consola de NetView desde la vista de IBM Tivoli Enterprise Console.

Consulte la documentación del producto IBM Tivoli Enterprise Console para ver información más detallada sobre cómo utilizar la consola de NetView.

Capítulo 11. Integración de sucesos de situación con Tivoli Netcool/OMNIbus

Utilice la interfaz del Recurso de integración de sucesos (EIF) de Tivoli para reenviar sucesos de situaciones de empresa a OMNIbus. La prueba Netcool/OMNIbus para Tivoli EIF recibe los sucesos y los correlaciona con los sucesos de OMNIbus y después los inserta en el servidor de OMNIbus.

Las actualizaciones de esos sucesos también se envían a OMNIbus. Cuando un usuario de OMNIbus reconoce, cierra o vuelve a abrir un suceso reenviado, OMNIbus devuelve esos cambios al servidor de supervisión que los ha reenviado.

Los sucesos de situación desde agentes de Tivoli Enterprise Monitoring que se envían como alertas SNMP a la prueba Netcool/OMNIbus SNMP también se pueden utilizar para integrar con Netcool/OMNIbus.

El tema "Configuración del reenvío de sucesos a Tivoli Netcool/OMNIbus" de la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* contiene instrucciones para habilitar el reenvío de sucesos de situación, configurar el servidor OMNIbus para la ejecución de programas a partir de scripts, cargar el esquema de base de datos OMNIbus, configurar la prueba de EIF, habilitar el reenvío de situaciones en el servidor de supervisión concentrador y definir un destino predeterminado del recurso de integración de sucesos (EIF).

© Copyright IBM Corp. 2005, 2013

Capítulo 12. Configuración de conectores para la consola de sucesos comunes

La *consola de sucesos comunes* es una vista de Tivoli Enterprise Portal que proporciona una visualización individual integrada de sucesos de varios sistemas de sucesos. En una tabla, la consola de sucesos comunes presenta sucesos de los sistemas de sucesos y los usuarios pueden clasificar, filtrar y realizar acciones en estos sucesos. Se soportan los siguientes sistemas de sucesos:

- IBM Tivoli Monitoring
- IBM Tivoli Enterprise Console
- IBM Tivoli Netcool/OMNIbus

Un *conector de sucesos comunes* (normalmente denominado *conector*) es software que permite la visualización integrada de sucesos de varios sistemas de sucesos en la consola de sucesos comunes. Un conector recupera datos de sucesos de un sistema de sucesos y envía acciones iniciadas por el usuario que se deben ejecutar en ese sistema de sucesos. Por ejemplo, si realiza una acción en un suceso de Tivoli Enterprise Console o Netcool/OMNIbus en la consola de sucesos comunes, el conector de consola de sucesos comunes asociado envía dicha acción al sistema de sucesos de origen (Tivoli Enterprise Console o Netcool/OMNIbus) para su ejecución. Para que se visualicen los sucesos de un sistema de sucesos específico en la consola de sucesos comunes, debe configurar un conector para dicho sistema de sucesos y establecer una variable en el archivo de entorno del Tivoli Enterprise Portal Server.

Ventana Configuración de la Consola de sucesos comunes

Utilice la ventana Configuración de la consola de sucesos comunes para configurar un conector de consola de sucesos comunes para cada una de las instancias de sistema de sucesos. Dado que el conector para el producto IBM Tivoli Monitoring está configurado previamente cuando se instala el producto, la consola de sucesos comunes incluye de forma predeterminada sucesos de situación. Sin embargo, para que los sucesos de IBM Tivoli Enterprise Console o IBM Tivoli Netcool/OMNIbus se incluyan en la consola de sucesos comunes, debe configurar un conector para cada uno de estos sistemas de sucesos después de instalar el producto IBM Tivoli Monitoring. Esta configuración incluye la especificación de los sistemas de sucesos que se utilizan para obtener sucesos para visualizarlos en la consola de sucesos comunes. Es posible que también desee cambiar algunos de los valores de configuración para el conector de IBM Tivoli Monitoring.

Acerca de esta tarea

Para configurar conectores, abra la ventana Configuración de la consola de sucesos comunes realizando los pasos siguientes en el sistema donde está instalado el Tivoli Enterprise Portal Server y siga este procedimiento:

Procedimiento

- Windows
  1. Seleccione **Inicio** → **Programas** → **IBM Tivoli Monitoring** → Manage Tivoli Enterprise Monitoring Services.

© Copyright IBM Corp. 2005, 2013

2. En la ventana Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho del ratón en **Tivoli Enterprise Portal Server**.
3. En el menú, pulse **Reconfigurar**.
4. En la primera ventana de configuración, pulse **Aceptar**.
5. En la segunda ventana de configuración, pulse **Aceptar**.
6. Pulse **No** como respuesta a la pregunta "¿Desea volver a configurar la información de conexión de almacén para el Tivoli Enterprise Portal Server?"

- Linux o UNIX
  1. En la línea de mandatos, vaya al directorio (cd) *dir_instalación*/bin y entre ./itmcmd manage.
  2. En la ventana Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho del ratón en **Tivoli Enterprise Portal Server**.
  3. En menú emergente, pulse **Configurar**.

Resultados

El servidor de portal se detiene y, después de un momento, se abre la ventana Configuración de consola de sucesos comunes con los separadores siguientes:
- Conector ITM
- Conector TEC
- Conector OMNIbus
- Nombres de las columnas adicionales

Separador Conector ITM

Pulse el separador **Conector ITM** para ver o cambiar la información de un conector IBM Tivoli Monitoring. Dado que el sistema de sucesos de Tivoli Monitoring tiene un solo servidor de Tivoli Enterprise Monitoring concentrador, configure sólo un conector IBM Tivoli Monitoring.

La información siguiente define el conector IBM Tivoli Monitoring:

Habilitar este conector
Puede elegir Sí o No. Un valor de Sí significa que los sucesos de IBM Tivoli Monitoring están disponibles en la consola de sucesos comunes.

Nombre del conector
Nombre que se debe visualizar en la consola de sucesos comunes para este conector.

Número máximo de sucesos para este conector
Número máximo de sucesos que deben estar disponibles en la consola de sucesos comunes para este conector.

Ver sucesos cerrados
Puede elegir Sí o No. Un valor de Sí significa que los sucesos cerrados para este conector están disponibles en la consola de sucesos comunes.

Separador Conector TEC

Pulse el separador **Conector TEC** para ver o cambiar la información de un conector IBM Tivoli Enterprise Console. Para que los sucesos de un servidor de Tivoli Enterprise Console se visualicen en la consola de sucesos comunes, debe configurar un conector IBM Tivoli Enterprise Console.

Para configurar un conector, pulse **Nuevo**. La página Conector TEC resultante contiene la información siguiente que define un conector IBM Tivoli Enterprise Console:

Nombre del conector
Nombre que se debe visualizar en la consola de sucesos comunes para este conector.

Número máximo de sucesos para este conector
Número máximo de sucesos que deben estar disponibles en la consola de sucesos comunes para este conector.

Nombre de la máquina del sistema de sucesos
Nombre de sistema correspondiente al sistema de sucesos que está asociado con este conector.

Número de puerto del sistema de sucesos
Número de puerto de asignador de objetos (oserv), normalmente 94. Es el puerto que el conector utiliza para recuperar sucesos del sistema de sucesos de Tivoli Enterprise Console.

No es el puerto utilizado para conectarse al servidor de sucesos de Tivoli Enterprise Console (de forma predeterminada, 5529).

Nombre de usuario para acceder al sistema de sucesos
Nombre de usuario que se utiliza al acceder al sistema de sucesos que está asociado con este conector.

Contraseña
Contraseña asociada con el nombre de usuario.

Grupo de sucesos que define sucesos para la consola de sucesos comunes
Grupo de sucesos de Tivoli Enterprise Console que define qué sucesos están disponibles en la consola de sucesos comunes.

Si no especifica un grupo de sucesos, todos los sucesos de Tivoli Enterprise Console están disponibles en la consola de sucesos comunes.

Si desea restringir sucesos adicionalmente, también puede definir una cláusula en el campo **Cláusula WHERE de SQL que restringe sucesos para la consola de sucesos comunes**.

Cláusula WHERE de SQL que restringe sucesos para la consola de sucesos comunes
Esta cláusula sólo se puede aplicar a la parte de un suceso que se crea desde la tabla de atributos base de Tivoli Enterprise Console. Por ejemplo, `status <> 30` hace que todos los sucesos con un estatus que no es igual a 30 estén disponibles en la consola de sucesos comunes.

Si no define una cláusula, todos los sucesos de Tivoli Enterprise Console están disponibles en la consola de sucesos comunes, a menos que los excluya un grupo de sucesos que ha especificado en el campo **Grupo de sucesos que define sucesos para la consola de sucesos comunes**.

Ver sucesos cerrados
Puede elegir `Sí` o `No`. Un valor de `Sí` significa que los sucesos cerrados para este conector están disponibles en la consola de sucesos comunes.

Intervalo de tiempo (en minutos) para sondear el sistema de sucesos
Número de minutos entre cada sondeo del sistema de sucesos para sucesos nuevos o cambiados.

Intervalo de tiempo (en minutos) para sincronizar sucesos
Número de minutos entre cada sondeo del sistema de sucesos para determinar qué sucesos se han suprimido.

Intervalo de tiempo (en segundos) entre intentos de reconexión
Número de segundos de retardo entre intentos de reconexión cuando el conector pierde la conexión con el sistema de sucesos.

Número de intentos de reconexión
Número máximo de intentos de reconexión consecutivos a efectuar si el conector pierde la conexión con el sistema de sucesos.

Si este valor se establece en `-1` y el conector pierde la conexión, el conector intenta reconectarse indefinidamente.

Información para columnas de tabla adicionales
La consola de sucesos comunes incluye cinco columnas de tabla adicionales que puede personalizar. En los campos restantes de esta página de Conector TEC, puede definir el tipo de atributo y el nombre de atributo de Tivoli Enterprise Console que identifican el atributo que se debe correlacionar con cada una de estas columnas personalizables.

Para el tipo de atributo, puede elegir uno de los valores siguientes:

- `Base`, que significa que el atributo es de la tabla de atributos base de Tivoli Enterprise Console.
- `Ampliado`, que significa que el atributo es de la tabla de atributos ampliados de Tivoli Enterprise Console.

Separador Conector OMNIbus

Pulse el separador **Conector OMNIbus** para ver o cambiar la información de un conector IBM Tivoli Netcool/OMNIbus. Para que los sucesos de un Tivoli Netcool/OMNIbus ObjectServer se visualicen en la consola de sucesos comunes, debe configurar un conector IBM Tivoli Netcool/OMNIbus.

Para configurar un conector, pulse **Nuevo**. La página Conector OMNIbus resultante contiene la información siguiente que define un conector IBM Tivoli Netcool/OMNIbus:

Nombre del conector
Nombre que se debe visualizar en la consola de sucesos comunes para este conector.

Número máximo de sucesos para este conector
Número máximo de sucesos que deben estar disponibles en la consola de sucesos comunes para este conector.

Nombre de la máquina del sistema de sucesos
Nombre de sistema correspondiente al sistema de sucesos que está asociado con este conector.

Número de puerto del sistema de sucesos
Número de puerto de ObjectServer (normalmente 4100), que este conector utiliza para recuperar sucesos del sistema de sucesos de Tivoli Netcool/OMNIbus.

Nombre de usuario para acceder al sistema de sucesos
Nombre de usuario que se utiliza al acceder al sistema de sucesos que está asociado con este conector.

Contraseña
Contraseña asociada con el nombre de usuario.

Cláusula WHERE de SQL que restringe sucesos para la consola de sucesos comunes
Esta cláusula se puede aplicar sólo a la parte de un suceso que se crea desde la tabla `alerts.status` de Tivoli Netcool/OMNIbus. Por ejemplo, `Severity <>> 0` hace que todos los sucesos con una gravedad que no es igual a 0 estén disponibles en la consola de sucesos comunes.

Si no define una cláusula, todos los sucesos de Tivoli Netcool/OMNIbus están disponibles en la consola de sucesos comunes.

Ver sucesos borrados
Puede elegir `Sí` o `No`. Un valor de `Sí` significa que los sucesos borrados para este conector están disponibles en la consola de sucesos comunes.

Intervalo de tiempo (en minutos) para sondear el sistema de sucesos
Número de minutos entre cada sondeo del sistema de sucesos para sucesos nuevos o cambiados.

Tivoli Netcool/OMNIbus ObjectServer envía automáticamente los sucesos nuevos o cambiados a la consola de sucesos comunes a medida que éstos quedan disponibles. Por consiguiente, la principal finalidad de esta comprobación es asegurar que el servidor y la conexión con el servidor funcionan correctamente.

Intervalo de tiempo (en segundos) entre intentos de reconexión
Número de segundos de retardo entre intentos de reconexión cuando el conector pierde la conexión con el sistema de sucesos.

Número de intentos de reconexión
Número máximo de intentos de reconexión consecutivos a efectuar si el conector pierde la conexión con el sistema de sucesos.

Si este valor se establece en `0` y el conector pierde la conexión, el conector permanece impracticable indefinidamente.

Si este valor se establece en `-1` y el conector pierde la conexión, el conector intenta reconectarse indefinidamente.

Información para columnas de tabla adicionales
La consola de sucesos comunes incluye cinco columnas de tabla adicionales que puede personalizar. En los campos restantes de esta página, puede definir el tipo de campo y el nombre de campo de Tivoli Netcool/OMNIbus que identifican el campo que se debe correlacionar con cada una de estas columnas personalizables.

Para el tipo de campo, puede elegir uno de los valores siguientes:

- `alerts.status`, que significa que el campo contiene datos de la tabla `alerts.status` en Tivoli Netcool/OMNIbus ObjectServer.
- `alerts.details`, que significa que el campo contiene datos de la tabla `alerts.details` de Tivoli Netcool/OMNIbus ObjectServer.
- `Ampliado`, que significa que el campo contiene atributos ampliados de un suceso de Tivoli Enterprise Console que se ha reenviado al sistema de sucesos de Tivoli Netcool/OMNIbus.

Separador Nombres de las columnas adicionales

La consola de sucesos comunes incluye cinco columnas de tabla adicionales que puede personalizar. De forma predeterminada, se utilizan los nombres siguientes para estas columnas:

- Columna adicional 1
- Columna adicional 2
- Columna adicional 3
- Columna adicional 4
- Columna adicional 5

Pulse el separador **Nombres de las columnas adicionales** para ver o cambiar los nombres de estas columnas.

Al definir un conector de Tivoli Enterprise Console o Tivoli Netcool/OMNIbus, puede definir la información que se debe correlacionar con cada una de estas columnas personalizables.

Finalidad de las columnas de tabla adicionales

La consola de sucesos comunes sólo visualiza un conjunto básico de información de la tabla de atributos base de Tivoli Enterprise Console y de las tablas `alerts.status` y `alerts.details` de Tivoli Netcool/OMNIbus.

Si, por ejemplo, desea ver un atributo adicional denominado "origin" de un suceso de Tivoli Enterprise Console, puede realizar los pasos siguientes:

1. En el campo **Tipo de atributo para la columna adicional 1** de la página Conector TEC, elija el tipo de atributo, por ejemplo `base`.
2. En el campo **Nombre de atributo para la columna adicional 1** de la página Conector TEC, entre el nombre de atributo, por ejemplo `origin`.
3. En el campo **Nombre de la columna adicional 1** de la página Nombres de las columnas adicionales, entre el nombre que desee utilizar para la columna que ha personalizado. Por ejemplo, puede entrar `Origin`.

En la columna "Origin" de cada fila que es un suceso de Tivoli Enterprise Console, la consola de sucesos comunes visualiza el valor del atributo de origen.

Separador Conector TEC: definición de información para columnas de tabla adicionales

En los campos siguientes de la página Conector TEC, defina la información que se debe correlacionar con las columnas personalizables:

- Tipo de atributo para la columna adicional 1
- Nombre de atributo para la columna adicional 1
- Tipo de atributo para la columna adicional 2
- Nombre de atributo para la columna adicional 2
- Tipo de atributo para la columna adicional 3
- Nombre de atributo para la columna adicional 3
- Tipo de atributo para la columna adicional 4
- Nombre de atributo para la columna adicional 4
- Tipo de atributo para la columna adicional 5
- Nombre de atributo para la columna adicional 5

Separador Conector OMNIbus: definición de información para columnas de tabla adicionales

En los campos siguientes de la página Conector OMNIbus, defina la información que se debe correlacionar con las columnas personalizables:

- Tipo de campo para la columna adicional 1
- Nombre de campo para la columna adicional 1
- Tipo de campo para la columna adicional 2
- Nombre de campo para la columna adicional 2
- Tipo de campo para la columna adicional 3
- Nombre de campo para la columna adicional 3
- Tipo de campo para la columna adicional 4
- Nombre de campo para la columna adicional 4
- Tipo de campo para la columna adicional 5
- Nombre de campo para la columna adicional 5

Prácticas recomendadas para utilizar la sincronización de sucesos

En el entorno, si se reenvían sucesos de Tivoli Monitoring al sistema de sucesos de Tivoli Enterprise Console o Tivoli Netcool/OMNIbus para la sincronización de sucesos, debe configurar los conectores de sucesos comunes para recuperar sólo una copia del mismo suceso a fin de evitar tener información de sucesos duplicada en la consola de sucesos comunes.

Siga estos métodos recomendados para restringir la consola de sucesos comunes para incluir sólo los sucesos de Tivoli Enterprise Console o Tivoli Netcool/OMNIbus que no se originan como sucesos de Tivoli Monitoring:

Cuando se reenvían sucesos de Tivoli Monitoring al sistema de sucesos de Tivoli Enterprise Console

1. En el servidor de Tivoli Enterprise Console, cree un grupo de sucesos que defina sólo los sucesos de Tivoli Enterprise Console que no se originan como sucesos de Tivoli Monitoring y se denomine, por ejemplo, `All_but_ITM`.
2. Cuando configure un conector TEC, escriba `All_but_ITM` en el campo **Grupo de sucesos que define sucesos para la consola de sucesos comunes**.
3. Cuando configure el Conector ITM, pulse **Sí** en el campo **Habilitar este conector**.

Cuando se reenvían sucesos de Tivoli Monitoring al sistema de sucesos de Tivoli Netcool/OMNIbus

1. Cuando configure un Conector OMNIbus, escriba `ITMStatus = ''` en el campo **Cláusula WHERE de SQL que restringe sucesos para la consola de sucesos comunes**, donde `''` son dos comillas simples sin espacio entre ellas. Esta cláusula restringe los sucesos de Tivoli Netcool/OMNIbus en la consola de sucesos comunes sólo a aquéllos que no se originan como sucesos de Tivoli Monitoring.
2. Cuando configure el Conector ITM, pulse **Sí** en el campo **Habilitar este conector**.

La configuración resultante hace que la consola de sucesos comunes recupere los sucesos de Tivoli Monitoring directamente del sistema de sucesos de Tivoli

Monitoring en lugar del sistema de sucesos de Tivoli Enterprise Console o Tivoli Netcool/OMNIbus, lo que evita que tenga información de sucesos duplicada en la consola de sucesos comunes.

Resolución de problemas con la conexión al servidor de Tivoli Enterprise Console en sistemas Linux

La siguiente información se puede utilizar para solucionar problemas relacionados con la conexión al servidor de Tivoli Enterprise Console en un sistema Linux.

Problema

El conector de Tivoli Enterprise Console no se puede conectar al servidor de Tivoli Enterprise Console. Por consiguiente, los sucesos de Tivoli Enterprise Console no están disponibles en la consola de sucesos comunes.

Explicación

El archivo /etc/hosts del sistema donde está instalado el servidor de Tivoli Enterprise Portal debe incluir el host local con la dirección IP correcta. La línea siguiente muestra aproximadamente cuál es la configuración de Linux predeterminada:

```
127.0.0.1 my_hostname localhost
```

La configuración de Linux predeterminada hace que la solicitud de conexión se envíe al servidor de Tivoli Enterprise Console con la dirección `127.0.0.1`, que no es la dirección IP correcta del sistema donde está instalado el servidor de Tivoli Enterprise Portal. Para que el servidor de Tivoli Enterprise Portal se conecte, debe poder realizar una búsqueda inversa.

Solución

Asegúrese de que el archivo /etc/hosts incluye el host local con la dirección IP correcta. Las dos líneas siguientes muestran aproximadamente cuál es la configuración de Linux correcta, donde *xxx.xxx.xxx.xxx* es la dirección IP del sistema donde está instalado el servidor de Tivoli Enterprise Portal:

```
127.0.0.1 localhost
xxx.xxx.xxx.xxx my_hostname
```

Capítulo 13. Mantenimiento de agentes de supervisión

El mantenimiento de agentes de Tivoli Enterprise Monitoring implica tareas como actualizar al último release, editar variables de entorno para modificar su comportamiento y controlar la visualización en la vista física de Navigator de Tivoli Enterprise Portal.

Los métodos disponibles para el mantenimiento de agentes dependen del tamaño y de la configuración de la red gestionada, del tipo de tareas y de sus preferencias.

Tareas de agente en Tivoli Enterprise Portal

La vista física de Navigator de Tivoli Enterprise Portal muestra los sistemas gestionados de la red supervisada. En el menú de Navigator, puede desplegar y gestionar de forma remota los agentes de Tivoli Enterprise Monitoring que se ejecutan en sistemas operativos distribuidos y que se conectan a un Tivoli Enterprise Monitoring Server que se ejecuta en un sistema operativo distribuido.

Antes de poder instalar y configurar agentes de forma remota, cada sistema de destino debe tener instalado un agente de sistema operativo (SO). Los agentes de supervisión que no soportan la característica de despliegue de agentes remoto no muestran las opciones **Añadir sistema gestionado**, **Configurar** y **Eliminar** en el menú emergente de Navigator. Los tipos de sistemas gestionados que puede añadir a un sistema dependen de los paquetes de agentes que estén en el *depósito de agente* del servidor de supervisión al que está conectado el agente de sistema operativo.

Adición de un agente mediante Tivoli Enterprise Portal

Utilice el cliente de Tivoli Enterprise Portal para añadir sistemas gestionados individuales a la red supervisada.

Antes de empezar

Los tipos de agentes que se pueden instalar de forma remota en un sistema dependen de los paquetes de agentes que estén en el depósito de agente del servidor de supervisión al que está conectado el agente de sistema operativo. Los temas "Despliegue de agentes de supervisión en el entorno" de *IBM Tivoli Monitoring: Guía de instalación y configuración* describen cómo establecer un depósito de agente en el servidor de supervisión y un agente de sistema operativo en cada sistema en el que se desplegarán los agentes.

Una vez instalados los agentes del sistema operativo, la vista física de Navigator añade un elemento para cada sistema gestionado en línea.

Para utilizar esta característica, su ID de usuario debe tener permiso para **Gestionar** para la **Gestión de agentes**.

Acerca de esta tarea

Siga estas instrucciones para instalar y configurar sistemas gestionados mediante Tivoli Enterprise Portal:

© Copyright IBM Corp. 2005, 2013

Procedimiento

1. En la vista física de Navigator, pulse con el botón derecho del ratón en el elemento de Navigator del nivel del sistema donde desea instalar el agente de supervisión. En este ejemplo, están disponibles los sistemas denominados ORANGE, PEAR, CABBAGE y ONION.

   Empresa
   - Sistemas Linux
     - ORANGE
     - PEAR
   - Sistemas Windows
     - CABBAGE
     - ONION

2. Pulse **Añadir sistema gestionado** para abrir la ventana Seleccionar un agente de supervisión. Los agentes mostrados en esta lista son los que existen para el sistema operativo en el que se ejecuta este sistema. El número de versión de dos dígitos va seguido de un número de release de dos dígitos y un número de modificación de hasta cinco dígitos.
3. Resalte el tipo del agente de supervisión a instalar y pulse **Aceptar**. Para algunos tipos de agente, la operación de nuevo sistema gestionado se pone en cola y se muestra el ID de transacción. Para otros tipos de agente, se proporciona un asistenta para configurar el agente en este sistema.
4. Complete los campos para configurar el agente, pulsando **Siguiente** y **Anterior** para moverse entre las páginas.
5. En la página **Agente**, establezca el ID de usuario del sistema operativo bajo el que se ejecutará el agente en el sistema gestionado. *Windows*: Puede aceptar el valor predeterminado para iniciar el sistema gestionado con el ID de usuario (también puede seleccionar el recuadro de selección **Permitir que el servicio interactúe con el escritorio** para permitir el control remoto) o puede seleccionar **Utilizar esta cuenta** y especificar el nombre de usuario y la contraseña bajo los que se ejecutará el agente.

   Sistemas no Windows: Escriba el **Nombre de usuario** bajo el que se ejecutará el agente y el **Nombre de grupo**.
6. Pulse **Finalizar** para completar la configuración del sistema gestionado. Si alguna parte de la información proporcionada no es correcta, recibirá un mensaje de error y se le devolverá a la ventana de configuración. Compruebe las entradas y edite las que sean apropiadas para configurarlas correctamente. La instalación y configuración empiezan y pueden tardar varios minutos en terminarse en función de la configuración de supervisión de Tivoli, la ubicación del sistema gestionado y el tipo de agente de supervisión.
7. Una vez añadido el sistema gestionado a la empresa, pulse **Aplicar actualizaciones pendientes** en la barra de herramientas de la vista de Navigator. El nuevo sistema gestionado (como, por ejemplo, Universal Database) se visualiza debajo del Elemento Sistema de Navigator.

Configuración de un agente mediante Tivoli Enterprise Portal

El cliente de Tivoli Enterprise Portal ofrece una característica muy útil para configurar los sistemas gestionados individuales. Este método de configurar agentes no se aplica a los agentes de sistema operativo porque ya están configurados y en ejecución.

Antes de empezar

Para utilizar esta característica, el ID de usuario debe tener permiso para Gestionar para la gestión de agentes.

Acerca de esta tarea

Para configurar los agentes de supervisión, realice los pasos siguientes.

Procedimiento

1. Pulse con el botón derecho del ratón en el elemento de Navigator correspondiente al agente que desee configurar o actualizar.
2. Pulse **Configurar** para abrir la ventana Configurar sistema gestionado.
3. Edite los campos para configurar un agente, pulsando en **Siguiente** y **Atrás** para moverse entre las páginas. Las otras páginas además de **Agente** son específicas del tipo de agente.
   - Performance Analyzer, Agente de resumen y poda, y Proxy de almacén: Consulte "Soluciones de Tivoli Data Warehouse" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.
   - Universal Agent: Especifique los archivos Metarchivo y Script. Se describen en *IBM Tivoli Monitoring Universal Agent: Guía del usuario*.
   - Agentes no básicos: consulte la guía de instalación del producto en el IBM Tivoli Monitoring Information Center (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/welcome.htm) o en IBM Tivoli Documentation Central (http://www.ibm.com/tivoli/documentation).
4. En la página **Agente**, establezca el ID de usuario que se utilizará para el mantenimiento del agente:

   Windows:
   Acepte el valor predeterminado ◉ **Utilizar cuenta del sistema local** para utilizar su ID de usuario de Tivoli Enterprise Portal. También puede seleccionar ☐ **Permitir que el servicio interactúe con el escritorio** para habilitar el control remoto. O seleccione ○ **Utilizar esta cuenta** y especifique el nombre de usuario y la contraseña bajo los que se controlará el agente.

   No Windows:
   Escriba el **Nombre de usuario** bajo el que se ejecutará el agente y el **Nombre de grupo**.
5. Pulse **Finalizar** para completar la configuración del sistema gestionado. Si alguna parte de la información proporcionada no es correcta, recibirá un mensaje de error y se le devolverá a la ventana de configuración. Compruebe las entradas y edite las que sean apropiadas para configurarlas correctamente.

Inicio, detención y reciclaje de un agente mediante Tivoli Enterprise Portal

Puede iniciar un sistema gestionado fuera de línea o reciclar o detenerlo mediante Tivoli Enterprise Portal.

Antes de empezar

Para utilizar esta característica, su ID de usuario debe tener permiso para **Gestionar** para la **Gestión de agentes**.

Acerca de esta tarea

Todos los mandatos de despliegue se pasan mediante el agente de sistema operativo que está instalado en el sistema de destino. Si un agente de sistema operativo no está instalado, no puede iniciar o detener el agente desplegado.

Procedimiento

- Para iniciar un agente de supervisión desde Tivoli Enterprise Portal:
  1. En la vista física de Navigator, pulse el botón derecho del ratón en el elemento de Navigator del agente fuera de línea.
  2. Pulse **Iniciar**. La solicitud para iniciar el agente se envía al servidor de supervisión al que está conectado. En función de la configuración de supervisión, es posible que transcurran unos segundos antes de que el agente empiece a ejecutarse y de que vea habilitado el elemento de Navigator. Si el agente de supervisión no se inicia y obtiene un mensaje de error, es posible que el sistema no esté disponible.
- Para detener un agente de supervisión desde Tivoli Enterprise Portal:
  1. En la vista física de Navigator, pulse el botón derecho del ratón en el agente que se ha de detener.
  2. Pulse **Detener**. El agente pasa a estar fuera de línea y el elemento de Navigator está sombreado. El agente no entra en línea hasta que se inicia manualmente o, si se establece que se inicie automáticamente, después de que se inicie el servidor de supervisión al que está conectado.
- Para reciclar un agente de supervisión desde Tivoli Enterprise Portal:
  1. En la vista física de Navigator, pulse el botón derecho del ratón en el agente que se ha de detener.
  2. Pulse **Reiniciar** para detener y luego iniciar el agente de supervisión. Esto puede tardar poco tiempo en función del tráfico de red.

Actualización de un agente mediante Tivoli Enterprise Portal

Cuando se entrega una nueva versión de un agente de supervisión distribuido, puede aplicar la nueva versión local o remotamente en un sistema gestionado a la vez o a muchos sistemas simultáneamente. Utilice la ventana Configurar sistema gestionado del cliente de Tivoli Enterprise Portal para aplicar la actualización.

Antes de empezar

Esta posibilidad no se aplica a los agentes de supervisión de sistema operativo, los agentes basados en z/OS o a ningún producto que no soporte la característica de despliegue de agente remoto. Los agentes que se deben actualizar se deben haber instalado originalmente utilizando el despliegue de agente remoto. Los tipos de sistemas gestionados que puede añadir a un sistema dependen de los paquetes de agentes que estén en el depósito de agente del servidor de supervisión al que está conectado el agente de sistema operativo. Consulte los temas “Despliegue de agentes de supervisión en el entorno” del manual *IBM Tivoli Monitoring: Guía de instalación y configuración* para obtener más información.

Antes de iniciar la actualización, debe instalar soporte de aplicación en el Tivoli Enterprise Portal Server para cualquier agente que va a desplegar con el procedimiento indicado a continuación.

Nota: Las actualizaciones de soporte de aplicaciones de agentes son automáticas y este procedimiento no es necesario si el agente de supervisión se está ejecutando

en la infraestructura de IBM Tivoli Monitoring versión 6.2.3 o posterior, a menos que la función de autodescripción esté inhabilitada.

Acerca de esta tarea

Complete estos pasos para aplicar un parche para un agente de supervisión mediante el cliente del portal:

Procedimiento

1. Pulse con el botón derecho del ratón en el elemento de Navigator para el agente que desea actualizar.
2. Pulse **Configurar** para abrir la ventana Configurar sistema gestionado.
3. Pulse el separador **Agente**.
4. Compare la versión instalada del agente de supervisión con cualquiera de las actualizaciones disponibles del producto, luego resalte la fila del agente que se debe actualizar y pulse **Instalar actualizaciones**.

Resultados

La instalación de las actualizaciones empieza y puede tardar unos minutos en completarse. La lista que se muestra refleja el contenido del depósito de despliegue. Si la opción **Instalar actualizaciones** está inhabilitada, significa que cumple una o más de las condiciones siguientes:

- La entrada de depósito no concuerda con el tipo de producto.
- Los campos **VVRR** para el agente y la entrada de depósito son iguales, donde `VV` es el número de versión y `RR` es el número de revisión. Por ejemplo, una entrada de **`0610`** le impide aplicar un fixpack destinado a un agente de la versión 6.2.
- La entrada de depósito pertenece a una versión más antigua que la versión del agente.
- El campo de versión de host contenido en la entrada de depósito no contiene la plataforma de host del agente.
- El campo de requisito previo de la entrada de depósito no contiene un agente del mismo tipo que el propio agente. Por ejemplo, si 6.1 UD (supervisión de DB2) es el agente seleccionado, el campo de requisito previo de la entrada del depósito debe contener una notación de paquete de despliegue como, por ejemplo, ud:061000000, que es un modo de identificar un paquete de despliegue de parches.

Eliminación de un agente mediante Tivoli Enterprise Portal

También puede desinstalar agentes de supervisión de Tivoli Enterprise Portal deteniendo el agente y eliminando los valores de configuración. Después de haber eliminado el agente de la empresa, puede desinstalar completamente el agente del sistema gestionado. Cuando se elimina un agente, se elimina de todos los grupos del sistema gestionado a las que está asignado, de todas las listas de distribución de políticas o situaciones en las que estaba y de todos los elementos personalizados de la vista de Navigator a los que estaba asignado.

Antes de empezar

Para utilizar esta característica, el ID de usuario debe tener permiso para **Gestionar** para la **Gestión de agentes**.

Acerca de esta tarea

Realice los pasos siguientes para eliminar y opcionalmente desinstalar un agente:

Nota: Si el programa de utilidad Manage Tivoli Enterprise Monitoring Services se está ejecutando al desinstalar el agente, el proceso de desinstalación lo cierra automáticamente.

Procedimiento

1. Pulse el botón derecho del ratón en el elemento de Navigator para el agente que desea eliminar.
2. Pulse en **Eliminar**.
3. Pulse **Sí** cuando se le solicite que confirme la eliminación del agente. Si está eliminando un agente que tiene subagentes, otro mensaje le solicitará si desea eliminarlos todos.
4. Cuando se le solicite que confirme si desea desinstalar permanentemente el agente, pulse **Sí** para desinstalar o **No** para dejar el agente instalado en el sistema.

Actualización de un agente mediante la interfaz de línea de mandatos

La actualización de agentes implica la detención de los agentes que están en ejecución, la aplicación de los cambios y el reinicio de los agentes. Después de determinar la información específica sobre los agentes de supervisión que desea actualizar, incluyendo el tipo y la versión, ejecute el mandato **tacmd updateAgent** desde la interfaz de línea de mandatos. Si no se especifica una versión, el agente se actualiza a la versión más reciente.

Acerca de esta tarea

Realice los pasos siguientes en una interfaz de línea de mandatos. Para obtener información de referencia acerca de este mandato y los mandatos relacionados, consulte la publicación *IBM Tivoli Monitoring: Consulta de mandatos*.

Nota: Utilice únicamente mandatos tacmd incluidos con productos Tivoli para procesar paquetes y ejecutar despliegues de agente. La manipulación manual de la estructura de directorio de depósito o de los paquetes y archivos contenidos en ella no se soporta y puede anular la garantía.

Procedimiento

1. Utilice el mandato **tacmd login** para iniciar la sesión en un Tivoli Enterprise Monitoring Server.

   ```
   tacmd login {-s|--server} {[{https|http}://]HOST[:PUERTO]}
   [{-u|--username} NOMBRE_USUARIO]
   [ {-p|--password} CONTRASEÑA]
   [{-t|--timeout} TIEMPOESPERA] [-t TIMEOUT]
   ```

   a. Por ejemplo, para iniciar la sesión en el sistema *ms.austin.ibm.com* con el nombre de usuario *Admin* y la contraseña *log1n*, ejecute el mandato siguiente:

      ```
      tacmd login -s ms.austin.ibm.com -u Admin -p log1n
      ```

2. Después de iniciar la sesión, utilice el mandato **tacmd updateAgent** para instalar una actualización de agente en un nodo especificado.

   ```
   tacmd updateAgent {-t|--type} TYPE {-n|--node} SO-GESTIONADO
    [{-v|--version} VERSIÓN] [{-f|--force}]
   ```

a. Por ejemplo, el siguiente mandato actualiza un agente UNIX (tipo *UX*) en *itmserver*:

```
tacmd updateagent -t UX -n itmserver:KUX -v 6111
```

Borrado de la tabla Estatus de despliegue

Cada vez que emite un mandato **tacmd** de IBM Tivoli Monitoring o utiliza el navegador de Tivoli Enterprise Portal para gestionar de forma remota un Tivoli Enterprise Monitoring Agent, la información sobre la transacción se conserva en la tabla Estatus de despliegue del Tivoli Enterprise Monitoring Server. Para facilitar la gestión del contenido de esta tabla, especialmente en entornos grandes, puede planificar la eliminación periódica de transacciones completadas desde la tabla.

Acerca de esta tarea

Habilite esta característica para revisar las transacciones de despliegue completadas en momentos oportunos y reducir la sobrecarga del servidor de supervisión manteniendo un tamaño de tabla modesto. Para planificar el borrado periódico de transacciones completadas de la tabla Estatus de despliegue, debe especificar la frecuencia con la que desea que se produzca el borrado.

Esta característica la controla la variable de entorno `CLEARDEPLOYSTATUSFREQ=X` del servidor de supervisión, donde *X* es el número de horas entre el borrado automático de la tabla. Si *X* es cero (0) o si no se especifica la variable de entorno, el borrado automático está inhabilitado. Los valores válidos incluyen 0 - 720.

Puede habilitar la característica de dos formas:

- Añada la variable de entorno directamente al archivo de configuración del servidor de supervisión, de forma que el servidor habilite el borrado automático durante el arranque.
- Establezca la variable de entorno en el servidor de supervisión ya en ejecución utilizando la consola de servicio de IBM Tivoli Monitoring.

Cuando el borrado automático está habilitado, el servidor de supervisión busca automáticamente transacciones de despliegue completadas, las elimina de la tabla Estatus de despliegue y a continuación registra la información sobre la transacción suprimida en un archivo de registro para que el usuario la examine posteriormente. El borrado automático se ejecuta con intervalos de una hora que especifica al establecer la variable de entorno.

Procedimiento

- Modifique el archivo de entorno del servidor de supervisión
  1. Abra el archivo de entorno en el sistema donde se ha instalado el servidor de supervisión:
     - Windows Utilice Manage Tivoli Enterprise Monitoring Services (**Inicio** → **Programas** → **IBM Tivoli Monitoring** → **Manage Tivoli Enterprise Monitoring Services**). Pulse con el botón derecho del ratón en el Tivoli Enterprise Monitoring Server y pulse **Avanzado** → **Editar archivo ENV**.
     - Linux UNIX Vaya al directorio *dir_instalación*/config y abra los archivos *<nombrehost>*_ms_*<nombretems>*.config y ms.ini en un editor de texto.
  2. Añada la variable de entorno, especificando el intervalo de hora. Por ejemplo: `CLEARDEPLOYSTATUSFREQ=1`.
  3. Guarde el archivo.

4. Reinicie el servidor de supervisión para implementar los cambios.

- Modifique el archivo de entorno del servidor de supervisión utilizando la consola de servicio de IBM Tivoli Monitoring

  Consulte "Utilización de IBM Tivoli Monitoring Service Console" en la publicación *IBM Tivoli Monitoring: Guía de resolución de problemas* para obtener información detallada.

  1. Abra un navegador web en `http://nombrehost:1920`, donde *nombrehost* es el nombre de host o dirección IP del sistema donde se ejecuta el servidor de supervisión. A continuación, el programa de utilidad se visualiza con información sobre los componentes que se ejecutan actualmente en este sistema.
  2. Seleccione el enlace **ms** para modificar la variable de entorno.
  3. Especifique el ID de usuario y la contraseña.
  4. Especifique el mandato **BSS1 SET CLEARDEPLOYSTATUSFREQ=1**, donde 1 es el intervalo de hora.

Resultados

El archivo de registro `cleardeploystatus.log` del subdirectorio logs del servidor de supervisión (*dir_instalación*`/logs` en Linux y UNIX o *dir_instalación*`\logs` en Windows) contiene una línea de texto para cada transacción de la tabla Estatus de despliegue que se borra. Cada vez que se inicia el servidor de supervisión, registra `---Clear Deploy Status Log---` en el archivo de registro.

Para cada transacción que se borra de la tabla, se graba la siguiente información en el archivo de registro:

- ID de transacción: Identificador de transacción global de la transacción que se ha completado.
- Enviado: Indicación de fecha y hora del envío inicial de la transacción para su proceso.
- Mandato: El mandato de despliegue se ha procesado.
- Estado: El estado de finalización (SUCCESS o FAILURE).
- Reintentos: El número de veces que se ha intentado la transacción antes de que se completara.
- Nombre de servidor de supervisión: El nombre del servidor de supervisión responsable del proceso de la transacción.
- Nombre de host de destino: El nombre de sistema gestionado o identificador de nodo gestionado donde se ha completado el mandato.
- Plataforma: La arquitectura de plataforma notificada del agente de SO en ejecución en el destino.
- Producto: El código de producto del agente para el que se ha procesado la transacción.
- Versión: La versión del producto para el que se ha intentado la transacción.
- Mensaje de finalización: Si el estado devuelto es una anomalía, una explicación de la razón de la anomalía.

Qué hacer a continuación

Puede cambiar la ubicación del archivo de registro donde el servidor de supervisión registra las transacciones que se borran de la tabla Estatus de despliegue añadiendo la variable de entorno `CLEARLOG` al archivo de configuración

del servidor de supervisión especificando un nombre de vía de acceso completo en el sistema local, o cualquier nombre de vía de acceso completo en un sistema de archivos montado.

La utilización de un sistema de archivos montado resulta útil cuando hay un servidor de supervisión y una copia de seguridad del servidor. Mediante un sistema de archivos montado como destino, los registros de ambos sistemas se pueden establecer en el mismo nombre de vía de acceso completo para dar cabida a condiciones de migración tras error.

Nota: El servidor de supervisión concentrador activo realiza el borrado automatizado de la tabla Estatus de despliegue para toda la empresa. Si tiene un servidor de supervisión de copia de seguridad para el concentrador, establezca también la variable de entorno en la copia de seguridad en el mismo valor que se ha especificado en el concentrador, de forma que el proceso de borrado se produzca al mismo tiempo que el suceso de la migración tras error del concentrador.

Cambio del servidor de supervisión con el que se conecta un agente

Un entorno supervisado con varios servidores de Tivoli Enterprise Monitoring puede hacer que todos los agentes o alguno de ellos se conecten a los servidores de supervisión remotos. Puede modificar el servidor de supervisión con el que se conecta un agente reconfigurándolo.

Acerca de esta tarea

Utilice una de estas opciones para reasignar un agente de supervisión a otro servidor de supervisión:

Procedimiento

- Utilice la aplicación Manage Tivoli Enterprise Monitoring Services en el sistema donde está instalado el agente. Pulse el botón derecho del ratón en el agente de supervisión y pulse **Reconfigurar**. Pulse Aceptar en la primera ventana Configuración avanzada de agente y, a continuación, especifique el **Nombre de host** o **Dirección IP** del servidor de supervisión al que desea conectarse. Si el puerto que está utilizando es distinto del valor 1918 predeterminado, especifique el número de **Puerto**.

  Si el agente está instalado en Linux o UNIX, también puede utilizar el mandato **`itmcmd agent -A <código_producto>`** para reconfigurar.
- Utilice el mandato **`tacmd setAgentConnection`** para configurar remotamente el agente. Consulte el manual *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) para ver información detallada sobre este mandato.
- En servidores de supervisión IBM Tivoli Monitoring V6.3 o posteriores, utilice la solución de daemon de inicio de sesión de IBM Tivoli Monitoring disponible en IBM Service Management Connect. El daemon de inicio de sesión es una herramienta que gestiona los agentes de supervisión que pasan a estar en línea y a continuación llama a los siguientes scripts proporcionados por el cliente:

  `Seleccionar TEMS`
  : Este script devuelve una indicación de los servidores de supervisión primarios y secundarios para los que un agente debe reconfigurarse para conectarse a ellos, si el agente se conecta al servidor de supervisión incorrecto.

Después de inicio de sesión

Este script se puede utilizar para realizar la instalación o configuración de un agente después de que se haya conectado a su servidor de supervisión designado. Por ejemplo, este script se puede utilizar para añadir un agente a los grupos de sistemas gestionados o explorar el sistema donde está instalado el agente y desplegar remotamente agentes adicionales según sea necesario.

Para obtener más información sobre la solución del daemon de inicio de sesión y si puede utilizarse o no en el entorno, consulte TEMS login policies for agents o vaya directo a IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) y busque "políticas de inicio de sesión". **Nota**: Esta solución sólo está disponible a través de IBM Service Management Connect.

Qué hacer a continuación

Al reconfigurar un Universal Agent para conectarse a un servidor de supervisión diferente, reinicie todas las situaciones que se distribuyen a dicho sistema gestionado. De lo contrario, las situaciones que están establecidas para iniciarse automáticamente no se podrán iniciar y se producirá un error.

Agentes de supervisión de autodescripción

Los agentes de supervisión de IBM Tivoli Monitoring V6.2.3 que están habilitados para la autodescripción tienen todos los archivos de soporte de aplicación necesarios para actualizar los servidores de Tivoli Management Services. No es necesario que lleve a cabo pasos de instalación de soporte manuales ni que reinicie cada componente del servidor individual que vaya a dar soporte al agente.

Los agentes de supervisión de autodescripción aplican actualizaciones de versión a otros componentes automáticamente cuando el servidor se conecta, sin necesidad de reiniciar los servidores de Tivoli Management Services: servidor de supervisión concentrador, servidor de supervisión remoto y servidor de portal. Esta función de instalación automática de soporte de productos ayuda a eliminar errores que pueden producirse de una instalación incoherente de datos de aplicación en el servidor de IBM Tivoli Monitoring. Para utilizar la función de autodescripción, su Tivoli Management Services debe ser de V6.2.3 o posterior.

Si un agente de supervisión da soporte a la función de autodescripción, el soporte de aplicaciones se instala en el sistema del agente. Si el agente de supervisión incluye la infraestructura del agente de IBM Tivoli Monitoring V6.2.3 o está instalado en un sistema en el que la infraestructura del agente V6.2.3 o posterior ya está instalada, los servidores de supervisión y los servidores de portal recuperan los archivos de soporte de aplicaciones del agente tras el arranque del agente y aplican automáticamente el soporte. Los servidores de infraestructura solo recuperan el soporte de aplicaciones de un agente de autodescripción si aún no ha aplicado el soporte de aplicaciones o si tienen una versión anterior del soporte de aplicaciones.

La actualización de autodescripción se produce una vez por cada versión del agente. Los archivos de actualización se almacenan en el agente de modo que cuando el agente se conecta a un servidor de supervisión, se informa automáticamente al servidor de supervisión de la actualización de soporte de aplicaciones disponible. Si la función de autodescripción está habilitada, el soporte de aplicaciones se recupera del agente y el soporte del servidor de supervisión se actualiza.

Si ha instalado el servidor de supervisión en Linux o UNIX, los archivos de soporte de aplicaciones para todos los agentes de supervisión base y otros agentes soportados se han instalado automáticamente en el servidor de supervisión. Este proceso es distinto a instalar el servidor de supervisión en Windows, ya que en la instalación en Linux o UNIX siempre se lleva a cabo la instalación de manera automática de los archivos de soporte de aplicaciones para agentes de supervisión. Compruebe el servidor de supervisión y el servidor de portal para asegurarse de que se han instalado los productos del agente de autodescripción como se espera.

El componente de Tivoli Enterprise Monitoring Automation Server, proporcionado en IBM Tivoli Monitoring V6.3, contiene el proveedor de servicios de Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM). El proveedor de servidor de Performance Monitoring no da soporte a la renovación dinámica de archivos de soporte de aplicaciones. Esto significa que el Tivoli Enterprise Monitoring Automation Server debe reiniciarse cuando el soporte de aplicaciones nuevo se añade a un sistema, independientemente de si el soporte se ha añadido a través de un agente de autodescripción, una instalación normal, o una copia manual. Sin embargo, si el agente de supervisión no proporciona soporte OSLC, no es necesario reiniciar el servidor de automatización. Normalmente, los agentes anteriores a IBM Tivoli Monitoring V6.3 no proporcionan soporte OSLC. Consulte la documentación del agente para determinar si un agente proporciona soporte OSLC.

Si la característica de agente de autodescripción instala el soporte de aplicación en el Tivoli Enterprise Portal Server y el componente proveedor de datos de panel de instrumentos está habilitado, el servidor de portal se debe reiniciar para que el proveedor de datos de panel de instrumentos pueda seleccionar el soporte de aplicación de nuevo o cambiado y utilizarlo para recuperar los datos para los paneles de control.

Hoja de ruta

Utilice la siguiente hoja de ruta como ayuda para configurar, habilitar y utilizar la función de autodescripción. Dado que esta hoja de ruta está pensada para proporcionar una completa descripción general, donde sea aplicable se proporcionan enlaces a las secciones correspondientes de otras guías de Tivoli Monitoring.

Paso	Descripción e información proporcionada
1	Hay disponibles dos tipos de casos de instalación: una primera instalación y una instalación de actualización. Consulte “Configuración de la inicialización del agente de autodescripción” en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*. **Información adicional:** También se proporciona información de inicialización en “Renovación automática e inicialización de autodescripción” en la página 312. Para obtener más información sobre el mandato **editSdaOptions**, consulte el manual *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).

Paso	Descripción e información proporcionada
2	Configure la autodescripción en el servidor de supervisión concentrador. Consulte “Habilitación de la función del agente de autodescripción en el servidor de supervisión concentrador” en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* para obtener más información sobre esta configuración inicial. Este paso incluye el establecimiento de cada variable de entorno del servidor de supervisión concentrador `KMS_SDA=Y`. **Información adicional:** Para ver futuras referencias y las tareas del administrador posteriores a la configuración inicial, consulte “Habilitación o inhabilitación de la función de autodescripción en el servidor de supervisión” en la página 315.
3	**Nota**: Si no está ejecutando IBM Tivoli Monitoring V6.3, omita este paso. En IBM Tivoli Monitoring V6.3, de forma predeterminada el servidor de supervisión concentrador bloquea todas las instalaciones de agente de autodescripción (incluso si ha activado la autodescripción en el servidor de supervisión concentrador estableciendo `KMS_SDA=Y` en el paso 2) hasta que emite uno de los mandatos siguientes: • **`tacmd addSdaInstallOptions`** para especificar los productos y versiones que se permite instalar al recurso del agente de autodescripción. O BIEN • **`tacmd editSdaInstallOptions -t DEFAULT -i ON`** para permitir instalaciones para todos los productos y versiones sin bloqueos. (Este valor es básicamente el comportamiento predeterminado del agente de autodescripción en V6.2.3 y V6.2.3 FP1.) Esta característica proporciona más control sobre qué productos y versiones el proceso automático del agente de autodescripción instala en el servidor de supervisión y en el servidor de portal. Después de modificar las opciones de instalación, puede utilizar el mandato **`tacmd listSdaInstallOptions`** para visualizar las configuraciones de instalación actuales para el servidor de supervisión concentrador. Para ver información detallada y los mandatos **`tacmd`**, consulte “Gestión de instalaciones de agente de autodescripción” y “Control dinámico de la función del agente de autodescripción del servidor de supervisión concentrador” en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*. **Información adicional:** Para ver completa información de la sintaxis, consulte la publicación *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm). Para futuras referencias, puede actualizar o modificar estas opciones de instalación tras la configuración inicial, consulte “Actualización dinámica de las opciones de instalación de autodescripción” en la página 311.

Paso	Descripción e información proporcionada
4	Utilice el mandato **tacmd listappinstallrecs** para supervisar los registros de instalación del soporte de aplicaciones. Utilice el mandato **tacmd listSdaStatus** para supervisar la habilitación de autodescripción y estado de suspensión para todos los servidores de supervisión del entorno. Consulte el apartado “Instalación del agente de autodescripción” en la página 306. **Información adicional:** Para obtener información sobre los registros de instalación reintentables y los registros de instalación terminales, consulte “Errores de instalación del agente de autodescripción” en la página 309. Para ver completa información de la sintaxis, consulte la publicación *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).
5	Una vez que se haya completado la actualización de la aplicación de autodescripción, puede ver los siguientes nuevos datos del agente en el cliente de portal: • La configuración histórica se actualiza con cada nuevo atributo • Los espacios de trabajo se actualizan • Situaciones, políticas y actualizaciones nuevas o actualizadas (las nuevas situaciones se distribuyen e inician automáticamente mediante las opciones de inicialización configurables por el usuario) • Las consultas se actualizan • Los archivos del servidor de ayuda se actualizan El soporte de aplicaciones no se aplica automáticamente a los clientes de Tivoli Enterprise Portal. Se muestra un indicador en estos clientes que indica al usuario que deben reciclar su cliente para aplicar el soporte de aplicaciones nuevo o modificado. • Si utiliza el cliente de escritorio de Tivoli Enterprise Portal, debe utilizar las imágenes de instalación del agente de supervisión para instalar el soporte de aplicaciones de Tivoli Enterprise Portal en cada uno de los clientes de escritorio. • Si está utilizando el cliente del navegador de Tivoli Enterprise Portal o el cliente de Java WebStart, y tiene los permisos de usuario necesarios para visualizar la aplicación actualizada, una vez que se visualice el indicador puede elegir cerrar y reiniciar estos clientes para ver las nuevas actualizaciones. **Información adicional:** Para obtener más información sobre indicadores de soporte, consulte Respuesta a un suceso de soporte de aplicación en la publicación *Tivoli Enterprise Portal: Guía del usuario*.
6	Para comenzar las pruebas de diagnóstico prelimilares y solucionar los problemas, consulte “Resolución de problemas del agente de supervisión” en la publicación *IBM Tivoli Monitoring: Guía de resolución de problemas*. **Información adicional:** Para ver información detallada de mensajes, consulte la publicación *Mensajes de IBM Tivoli Monitoring* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/messages/itm_messages.htm).

Flujo de sucesos de autodescripción en el servidor de supervisión

El flujo de sucesos automatizados para un agente de autodescripción es distinto si el agente está conectado a un servidor de supervisión concentrador o a un servidor de supervisión remoto.

Agente de autodescripción conectado al servidor de supervisión concentrador

En los pasos siguientes se describe el flujo de sucesos de un agente de autodescripción que se conecta al servidor de supervisión concentrador:

1. El gestor del agente de autodescripción del servidor de supervisión concentrador determina si la versión del soporte de aplicaciones del producto está ya instalada en el servidor de supervisión concentrador. Si la versión del soporte de aplicaciones del producto no se ha instalado todavía, el servidor de supervisión concentrador recupera los archivos de soporte del agente.
2. El servidor de supervisión concentrador empieza la instalación del producto de agente de autodescripción y la renovación dinámica de las estructuras de definición del producto internas del servidor de supervisión. El estado de finalización de la instalación de este agente de autodescripción del servidor de supervisión concentrador se registra en las siguientes ubicaciones:
   - La tabla de propiedades de aplicación de Tivoli Enterprise Monitoring Server local.
   - El recurso de registro de auditoría del Tivoli Enterprise Monitoring Server.
   - El recurso de registro MSG2 del Tivoli Enterprise Monitoring Server.
   - El registro RAS1 del Tivoli Enterprise Monitoring Server.
   - En las plataformas distribuidas del Tivoli Enterprise Monitoring Server, los archivos de registro del programa de instalación del agente de autodescripción son `installsdsupport_*.trc` e `installsdsupport_*.log`. En los sistemas Windows, los registros se encuentran en el directorio *`dir_instalación`*`\logs`. En los sistemas Linux y UNIX, los registros se encuentran en el directorio *`dir_instalación`*`/logs`.
3. Una vez finalizada satisfactoriamente la instalación del producto del servidor de supervisión concentrador, se informa del soporte de producto nuevo o actualizado a los procesos de Tivoli Enterprise Portal Server que se estén ejecutando y estén conectados al servidor de supervisión concentrador.

   En un entorno habilitado para la espera activa (FTO), los datos de configuración de la autodescripción se replican en el servidor de supervisión concentrador en espera. El servidor de supervisión concentrador en espera no da soporte a conexiones directa desde agentes para un servidor de supervisión remoto, lo que significa que las instalaciones de autodescripción no se pueden iniciar directamente en el concentrador en espera. Las instalaciones de autodescripción las inicia en el concentrador en espera el concentrador activo después de que el concentrador activo haya finalizado la instalación de autodescripción. El proceso de instalación de autodescripción en el concentrador en espera recupera los archivos de soporte del producto del concentrador activo. Para obtener más información sobre un entorno FTO, consulte la publicación *IBM Tivoli Monitoring: Guía de alta disponibilidad para sistemas distribuidos*.
4. El Tivoli Enterprise Portal Server realiza los mismos pasos básicos que el servidor de supervisión concentrador. Determina si la versión del producto ya

está instalada en el Tivoli Enterprise Portal Server. No obstante, recupera los archivos de soporte del producto directamente del servidor de supervisión concentrador, no del agente conectado.

5. El Tivoli Enterprise Portal Server empieza la instalación del producto de agente de autodescripción y la renovación dinámica de las estructuras de definición del producto internas del servidor de portal.
6. El Tivoli Enterprise Portal Server informa a los clientes de navegador de Tivoli Enterprise Portal Browser y de escritorio de Tivoli Enterprise Portal en ejecución si hay disponible un soporte de producto nuevo o actualizado. El estado de finalización de esta instalación del producto de agente de autodescripción del Tivoli Enterprise Portal Server se registra en las siguientes ubicaciones:
   - El recurso de registro de auditoría del Tivoli Enterprise Portal Server.
   - El registro RAS1 del Tivoli Enterprise Portal Server.
   - Los archivos de registro del programa de instalación del agente de autodescripción del Tivoli Enterprise Portal Server `installsdsupport_*.trc` e `installsdsupport_*.log`. En los sistemas Windows, los registros se encuentran en el directorio *`dir_instalación`*`\logs`. En los sistemas Linux/UNIX, los registros se encuentran en el directorio *`dir_instalación`*`/logs`.

Agente de autodescripción conectado al servidor de supervisión remoto

En los pasos siguientes se describe el flujo de sucesos de un agente de autodescripción que se conecta al servidor de supervisión remoto:

1. El gestor del agente de autodescripción del servidor de supervisión remoto garantiza que el producto se ha instalado primero en el servidor de supervisión concentrador.
2. Si el producto no se ha instalado primero en el servidor de supervisión concentrador, el servidor de supervisión remoto indica al servidor de supervisión concentrador que debe instalar el producto primero.
3. Cuando finaliza la instalación del servidor de supervisión concentrador, el servidor de supervisión remoto determina si el producto se ha instalado localmente en este servidor de supervisión.
4. La instalación del producto de servidor de supervisión remoto se realiza de la misma forma que se ha descrito para el servidor de supervisión concentrador.
5. Si la instalación del producto de servidor de supervisión concentrador falla por algún motivo, el servidor de supervisión remoto no instalará el producto.

El servidor de supervisión no permite que se vuelvan a intentar las otras solicitudes anómalas de instalación del agente de autodescripción hasta que se haya corregido la condición de error del servidor de supervisión existente y se hayan eliminado los registros de instalación del producto del agente de autodescripción de la tabla de propiedades de aplicación del servidor de supervisión. Para obtener más información, consulte “Errores de instalación del agente de autodescripción” en la página 309.

Nota:

La disponibilidad de la característica del agente de autodescripción en un servidor de supervisión concentrador puede influir en la disponibilidad de la característica en un servidor de supervisión remoto. Aparece un mensaje de error cuando un error del agente de autodescripción en un servidor de

supervisión concentrador hace que la característica de agente de autodescripción se inhabilite en el servidor de supervisión remoto que está conectado al concentrador. Para obtener más información sobre los mensajes de error, consulte la publicación *IBM Tivoli Monitoring: Guía de resolución de problemas*.

Una vez solucionado el error del agente de autodescripción en el servidor de supervisión concentrador, en la siguiente reconexión al concentrador, el servidor de supervisión remoto detecta que la característica de agente de autodescripción está disponible en el concentrador. Como resultado, vuelve a habilitar el agente de autodescripción localmente en el servidor de supervisión remoto.

Cambios detectados por el servidor de supervisión en el inicio

El Tivoli Enterprise Monitoring Server detecta la siguiente información en el inicio:

- Los productos que se han instalado manualmente, por ejemplo, las aplicaciones que no se han instalado utilizando la función de autodescripción.
- Las actualizaciones manuales (cambios en el archivo de catálogos y versiones) en los productos instalados, por ejemplo, los cambios de producto iniciados por el usuario que se producen fuera de una instalación del agente de autodescripción.
- Las instalaciones anómalas del agente de autodescripción.

El Tivoli Enterprise Monitoring Server realiza ajustes y correcciones basándose en los cambios detectados en los productos instalados. En el inicio, sólo se detectan los productos que tengan un archivo de versiones (archivo VER) válido del servidor de supervisión. Este proceso ocurre automáticamente cuando se habilita el gestor de instalación del agente de autodescripción en el servidor de supervisión (**KMS_SDA=Y**). Esta función permite mantener un inventario preciso de los productos y las versiones que se han instalado. Si el gestor de instalación del agente de autodescripción no está habilitado, esta función no se ejecuta.

Instalación del agente de autodescripción

La tabla de propiedades de la aplicación del servidor de supervisión local (TAPPLPROPS) almacena los resultados de las instalaciones de producto del agente de autodescripción del servidor de supervisión. Esta tabla incluye la versión detectada actual de los productos de servidor de supervisión instalados manualmente.

Esta tabla almacena también la información de autodescripción como por ejemplo las opciones de instalación, la distribución de inicios y los registros de suspensión. Para obtener más información sobre los atributos de TAPPLPROPS, consulte Atributos de instalación de las propiedades de aplicación en la publicación *Tivoli Enterprise Portal: Guía del usuario*.

Puede utilizar dos mandatos **tacmd** distintos para comprobar el estado de autodescripción de los servidores de supervisión:

- **tacmd listSdaStatus** para el estado operativo
- **tacmd listappinstallrecs** para el estado de instalación del producto

Utilización del mandato tacmd listSdaStatus

En IBM Tivoli Monitoring V6.3 o posterior, el mandato **tacmd listSdaStatus** visualiza el estado de habilitación de autodescripción para un servidor de supervisión. Puede visualizar el estado de habilitación de autodescripción para una

lista de servidores de supervisión o para todos los servidores de supervisión, lo que es la opción predeterminada. El estado operativo del recurso del agente de autodescripción (suspendido o activo) del servidor de supervisión concentrador también se proporciona si el mandato se emite a un servidor de supervisión concentrador IBM Tivoli Monitoring V6.3 o posterior. El estado operativo de autodescripción (suspendido o activo) del concentrador determina la actividad de autodescripción para todos los servidores de supervisión conectados a ese servidor de supervisión concentrador.

El estado de habilitación de autodescripción se indica mediante los valores `HUB/RTEMS name`, `STATE` y `STATUS`.

En este ejemplo, un mensaje indica que la función de autodescripción está suspendida actualmente. Tanto HUB_A como RTEMS_1 están habilitados para la autodescripción. El código STATUS 0 indica que la autodescripción está habilitada. RTEMS_2 no está habilitado para la autodescripción y se proporciona el código STATUS 16 (`SDA inhabilitado porque KMS_SDA=N`) como explicación.

```
tacmd listSdaStatus

KUILSS203I: Se han suspendido las funciones de SDA.

HUB/RTEMS   STATE   STATUS

HUB_A       ON      0

RTEMS_1     ON      0

RTEMS_2     OFF     16
```

Para obtener más información, ejemplos y descripciones de los códigos `STATUS` del mandato **`tacmd listSdaStatus`**, consulte la publicación *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).

Utilización del mandato `tacmd listappinstallrecs`

Utilice el mandato **`tacmd listappinstallrecs`** para supervisar los registros de instalación del soporte de aplicaciones.

El mandato devuelve los registros de instalación del soporte de aplicaciones y muestra el estado actual de instalación del producto del agente de autodescripción de todos los servidores de supervisión del entorno. Recuerde que este mandato no está disponible cuando el servidor de supervisión no está en ejecución. Si el servidor de supervisión y el servidor de portal están ambos iniciados, puede ver también la información del agente de autodescripción y los valores en el espacio de trabajo Registros de auditoría. Consulte Capítulo 9, “Registro de auditoría”, en la página 243.

El mandato **`tacmd listappinstallrecs`** muestra el estado actual de instalación del producto del agente de autodescripción para todos los servidores de supervisión en el entorno.

```
HUB/RTEMS   PRODUCT     VERSION     GRPID       ID          IDVER       SEEDSTATE   STATE       STATUS

HUB_LZ      A4          06300000    5655        TMS         06300000                            0

HUB_LZ      HD          06300000    5655        TMS         06300000    Y           IC          0

HUB_LZ      HD          06300000    5655        TPW         06300000                IC          0
```

```
HUB_LZ      LZ          06230000    5655        TPS         06230000                IC          0
HUB_LZ      NT          06230000    5655        TMS         06230000                            0
HUB_LZ      TM          06230000    5655        TMS         06230000                            0
HUB_LZ      11          06230000    5655        TMS         06230000                ME          1005
RTEMS_LZ    A4          06230000    5655        TMS         06230000                            0
RTEMS_LZ    LZ          06230000    5655        TMS         06230000    Y           IC          0
RTEMS_LZ    R6          06230000    5655        TMS         06230000                            0
RTEMS_LZ    11          06230000    5655        TMS         06230000    Y           ME          1014
```

La columna HUB/RTEMS muestra el nombre de nodo del servidor de supervisión donde se ha recopilado el registro. Las filas con IC en la columna STATE indican que la instalación del agente de autodescripción se ha completado. También puede ver en este ejemplo que el servidor de supervisión concentrador y el servidor de supervisión remoto tienen una entrada appinstallrecs para el soporte del servidor de supervisión (TMS), pero el servidor de supervisión concentrador tiene dos entradas appinstallrecs adicionales para el soporte del servidor de portal (TPS) y los paquetes de soporte de cliente del navegador de portal (TPW). Estos paquetes adicionales se instalan sólo en el servidor de supervisión concentrador para que estén disponibles para el servidor de portal.

Si la columna STATE está en blanco, significa que el soporte de aplicaciones se ha instalado manualmente. Una columna MANUALINST muestra Y si utiliza la opción -d (detalle). Las afirmaciones del agente de autodescripción appinstallrecs son las siguientes:

IR Solicitud de instalación: Nueva solicitud de instalación en la cola de trabajos.

IM Instalar metadatos: Recupera la solicitud de instalación de la cola de trabajos, e inicia la instalación de metadatos y el trabajo de renovación automática.

MC Metadatos completos: La instalación y la renovación automática de los metadatos se ha completado.

IC Instalación completa: El soporte de aplicaciones SDA se ha completado satisfactoriamente.

ME Error de metadatos: Error de instalación de metadatos. El código STATUS proporciona información adicional.

Consejo: IR, IM y MC appinstallrecords indican todos ellos que la instalación normal del agente de autodescripción está en curso. Para obtener información sobre los registros de instalación del soporte de aplicaciones con un valor de STATE de ME, consulte "Errores de instalación del agente de autodescripción" en la página 309.

Para obtener información detallada sobre los códigos STATUS del mandato **tacmd listappinstallrecs**, consulte la publicación *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).

En IBM Tivoli Monitoring V6.3 o posterior, la opción **listappinstallrecs -t TEMS** ya no está soportada. Utilice en su lugar el mandato **listSdaStatus**.

Errores de instalación del agente de autodescripción

Se notifica un código de error en la columna **STATUS** de la salida de **listappinstallrecs**. Algunos errores se pueden reintentar, otros son terminales.

Errores de instalación del agente de autodescripción que se pueden reintentar

El servicio del agente de autodescripción de los agentes de Tivoli Enterprise Monitoring decide qué tipos de solicitudes de instalación o registro de agente de autodescripción que han fallado anteriormente se intentan de nuevo. Sólo se reintentan los siguientes tipos de códigos de error o anomalía devueltos por el Tivoli Enterprise Monitoring Server, en nombre de una solicitud de registro de agente de autodescripción al servidor de supervisión:

1006 Solicitud de instalación de SDA duplicada

1009 HUB no se encuentra

1017 Error de instalación temporal

1021 El servidor ha excedido el tiempo de espera

Los errores de instalación del agente de autodescripción reintentables son solicitudes de registro o instalación que se han iniciado, pero que no han modificado todavía ninguno de los archivos del Tivoli Enterprise Monitoring Server ni las estructuras internas.

Errores de instalación del agente de autodescripción terminales

Para los registros de errores con un valor de **STATE** de ME, la instalación no se reintentará.

En este ejemplo, el registro de instalación del código de producto 11 visualiza un valor de **STATE** igual a ME:

HUB/RTEMS	PRODUCT	VERSION	GRPID	ID	IDVER	SEEDSTATE	STATE	STATUS
RTEMS_LZ	11	06230000	5655	TMS	06230000	Y	ME	1014

El valor de **STATE** indica que se ha producido un error de instalación de metadatos del agente de autodescripción en el servidor de supervisión. El servidor de supervisión dejará de intentar la instalación del agente de autodescripción para este código de producto hasta que el administrador realice alguna acción para corregir el error. Esta corrección puede implicar al soporte de software de IBM. En este caso de ejemplo, debe utilizar el mandato **tacmd deleteappinstallrecs** para borrar el registro de error del agente de autodescripción una vez solucionado el problema. Para obtener más información, consulte la publicación *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).

Para determinar si una instalación del producto del agente de autodescripción ha fallado con una condición de error terminal, ejecute el mandato **tacmd listappinstallrecs** utilizando la opción **-e** para mostrar sólo los registros de error. Para los registros de errores con un valor de **STATE** de ME, la instalación no se reintentará.

Lleve a cabo los pasos siguientes para reintentar la instalación del agente de autodescripción:

1. Para evitar que se vuelva a producir la misma anomalía, corrija primero la condición que ha impedido la instalación. Asimismo, los recursos de mensajes del servidor de supervisión (mensajes de auditoría, MSG2 y RAS1) proporcionan más información sobre la causa de la anomalía. Realice las acciones correctivas para solucionar la condición o póngase en contacto con el soporte de software de IBM para obtener asistencia.
2. Para cada servidor de supervisión, suprima los registros de instalación anómala en la tabla de propiedades de aplicación ejecutando el mandato **tacmd deleteappinstallrecs**. Este mandato elimina el registro de instalación del producto del agente de autodescripción que genera el bloqueo. Consulte el manual *IBM Tivoli Monitoring: Consulta de mandatos* para obtener más información.
3. Una vez borrados todos los registros de instalación anómala del producto del servidor de supervisión, el recurso del agente de autodescripción del servidor de supervisión notifica inmediatamente al agente de autodescripción en ejecución que puede proporcionar este nivel de soporte del producto para reintentar la instalación del producto. Por ejemplo, si el intento de instalación anterior del producto *pc* y la versión `06230000` ha fallado con **STATE** igual a `ME`, y ejecuta el mandato **deleteappinstallrecs**, todo agente *pc* en ejecución de la versión `06230000` reintenta inmediatamente la instalación.
4. Vuelva a ejecutar **tacmd listappinstallrecs -t <cp>** para el producto *cp* para determinar el estado actual de la instalación.

Si la instalación del producto del agente de autodescripción falla en el servidor de supervisión concentrador primario, el concentrador en espera no intenta instalar el soporte. Corrija la razón del error en el concentrador principal y, a continuación, utilice el mandato **deleteappinstallrecs** para eliminar la entrada de error del concentrador principal. El borrado del error asegura que la instalación del producto del agente de autodescripción se reintentará.

Si la instalación del producto agente de autodescripción falla únicamente en el concentrador en espera, corrija la causa de la anomalía en el concentrador en espera. Mientras está conectado en el concentrador primario, puede utilizar el mandato **deleteappinstallrecs** con la opción **-n <nombre_TEMS_en_esper>** para eliminar la entrada de error en el servidor de supervisión en espera para permitir que se reintente la instalación del agente de autodescripción. La supresión del registro de instalación de la aplicación en el concentrador en espera no desencadena automáticamente que se reintente la instalación del producto del agente de autodescripción como lo hace cuando el registro se suprime del servidor de supervisión primario o un servidor de supervisión remoto. No hay problema si el concentrador en espera no tiene temporalmente soporte de producto del agente.

- Si el concentrador en espera se recicla, el soporte de producto que falta se descubre y la instalación del producto de agente de autodescripción se realiza en ese momento.
- Si el concentrador en espera se promocionan al concentrador activo, la instalación del producto de agente de autodescripción tiene lugar cuando el primer agente de este tipo se conecta con el concentrador ascendido.
- Puede forzar que se reintente la instalación del agente de autodescripción inmediatamente en el concentrador en espera, repitiendo la instalación del agente de autodescripción en el concentrador primario. Después de borrar el registro de instalación de la aplicación de error en el servidor de supervisión, utilice el mandato **deleteappinstallrecs -a** para suprimir el registro de estado

que no es de error del servidor de supervisión principal. Este mandato repite la instalación del agente de autodescripción en el servidor de supervisión en espera, desencadenando la instalación del servidor de supervisión cuando finaliza correctamente.

Actualización dinámica de las opciones de instalación de autodescripción

Puede especificar qué productos y versiones habilitados para la autodescripción el proceso automático del agente de autodescripción puede instalar en el servidor de supervisión y el servidor de portal mientras el servidor de supervisión concentrador está en ejecución.

Acerca de esta tarea

El servidor de supervisión concentrador debe estar iniciado. Se pueden emitir los siguientes mandatos de configuración independientemente de si la función de autodescripción está habilitada o inhabilitada (`KMS_SDA=Y|N`). Los valores de configuración que especifique se almacenan y a continuación se implementan una vez que se activa la autodescripción con la variable `KMS_SDA=Y`. Para obtener más información, consulte "Control dinámico de la función del agente de autodescripción del servidor de supervisión concentrador" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Procedimiento

1. Suspenda la función de autodescripción (sin reiniciar el servidor de supervisión concentrador) mediante el mandato **tacmd suspendSda**. Este mandato garantiza que no tenga lugar ninguna instalación de autodescripción mientras está actualizando las opciones.
2. Ejecute uno de los mandatos siguientes:

   tacmd addSdaInstallOptions
   Especifique los productos y versiones que el recurso del agente de autodescripción puede instalar.

   tacmd editSdaInstallOptions
   Modifique la configuración de versión de producto existente, o cambie el comportamiento predeterminado de la instalación del agente de autodescripción.

   tacmd deleteSdaInstallOptions
   Elimine una configuración de versión específica, o elimine todas las versiones de un producto.

   tacmd listSdaInstallOptions
   Visualice las configuraciones existentes de instalación de agente de autodescripción del servidor de supervisión concentrador.

   Consulte la publicación *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) para ver la sintaxis y ejemplos.
3. Reanude la función de autodescripción (sin reanudar el servidor de supervisión concentrador) mediante el mandato **tacmd resumeSda**.

Resultados

Las instalaciones sólo tienen lugar en los nuevos productos de versiones que ha especificado una vez que la autodescripción se habilita estableciendo la variable KMS_SDA=Y.

Suspensión de la función de autodescripción

Puede suspender y reanudar la función de autodescripción para su entorno mediante los mandatos **tacmd suspendSda** y **tacmd resumeSda** sin necesidad de reiniciar el servidor de supervisión. Puede suspender la función de autodescripción por diversas razones como, por ejemplo, al modificar las opciones de instalación de autodescripción o al pasar a modalidad de mantenimiento.

Antes de empezar

Los mandatos **tacmd suspendSda** y **tacmd resumeSda** cambian dinámicamente el comportamiento de autodescripción sólo cuando el servidor de supervisión concentrador está configurado con KMS_SDA=Y. Si se emiten los mandatos **tacmd suspendSda** y **tacmd resumeSda** no se alterará temporalmente el valor KMS_SDA=N. Si se emite el mandato **tacmd resumeSda** cuando KMS_SDA=N, el mandato se ignora hasta KMS_SDA=Y.

Si se emite el mandato **tacmd suspendSda** o **tacmd resumeSda**, se actualiza la tabla TAPPLPROPS. Este valor se guarda independientemente del valor KMS_SDA. El método recomendado es establecer la variable de entorno del servidor de supervisión concentrador en KMS_SDA=Y y a continuación ejecutar los mandatos **tacmd suspendSda** o **tacmd resumeSda**.

Consulte la publicación *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) para obtener completa información sobre la sintaxis.

Procedimiento

- Para suspender la función de autodescripción, emita el mandato **tacmd suspendSda**.
- Para reanudar la función de autodescripción, emita el mandato **tacmd resumeSda**.

Qué hacer a continuación

Puede ejecutar **tacmd listSdaStatus** para ver el estado de suspensión de los servidores de supervisión. Consulte el apartado "Instalación del agente de autodescripción" en la página 306.

Renovación automática e inicialización de autodescripción

La función de autodescripción le permite supervisar la infraestructura que se va a renovar e iniciar automáticamente con la versión más actualizada del soporte de aplicaciones.

Renovación automática es lo que permite actualizaciones continuas e ininterrumpidas de la infraestructura de supervisión. Tras una renovación automática correcta, la *inicialización* actualiza el entorno con las definiciones de productos más actualizadas.

Renovación automática

Cada producto ofrece soporte de aplicaciones. Antes de IBM Tivoli Monitoring V6.2.3 o posterior, el soporte de aplicación se instalaba en servidor de supervisión, servidor de portal y cliente de portal, y era necesario reciclar cada componente para activar el nuevo soporte de aplicación. Para IBM Tivoli Monitoring V6.2.3, la renovación automática permite al servidor de supervisión y al servidor de portal ofrecer renovación de aplicaciones dinámica tras un suceso de instalación de agente de autodescripción.

La operación de renovación automática no intrusiva se produce cuando un nuevo agente de autodescripción inicia una instalación de aplicación a través de la infraestructura de IBM Tivoli Monitoring. El proceso se activa la primera vez que un agente de autodescripción se conecta a un servidor de supervisión y el soporte de aplicaciones aún no está presente en el servidor de supervisión remoto o el servidor de supervisión concentrador.

El soporte de aplicaciones se instala automáticamente primero en el servidor de supervisión concentrador, seguido del servidor de supervisión remoto con el que está conectado actualmente el agente (que recupera el soporte del agente) y luego en el servidor de portal (que recupera el soporte del servidor de supervisión concentrador). Si un agente conmuta a otro servidor de supervisión remoto en el que no está instalado el soporte, el soporte se actualiza dinámicamente en el nuevo servidor de supervisión remoto de alojamiento.

La renovación automática se produce en un servidor de supervisión inmediatamente tras el despliegue de metadatos. El despliegue de metadatos transfiere y almacena archivos de atributos, archivos de catálogo, archivos de correlación de EIF, archivos de definición del producto inmediatos (archivos de inicialización) y archivos de versión en el servidor de supervisión. Una vez desplegados correctamente los archivos, las memorias caché internas del servidor de supervisión se actualizan y los nuevos metadatos están inmediatamente disponibles para que los componentes del servidor de supervisión los utilicen para la supervisión. La renovación automática también se produce en el servidor de portal, actualizando todos los archivos necesarios.

Si la base de datos del servidor de portal se reinicia mientras el servidor de portal aún se está ejecutando, el servidor de portal se debe reiniciar para que el soporte termine de actualizar el servidor de portal. Para que la renovación automática del servidor de portal funcione correctamente, la base de datos del servidor de portal se debe estar ejecutando.

La renovación automática garantiza que tiene acceso continuo a los metadatos del producto para dar soporte a las actividades de supervisión durante una renovación de agente de autodescripción, utilizando los metadatos existentes y, cuando la renovación automática finaliza, los nuevos metadatos pasan a estar disponibles. Algunos componentes internos del servidor de supervisión ofrecen notificación cuando el usuario tiene nuevos metadatos, por ejemplo para mover las situaciones `en espera pendientes a iniciadas`.

Inicialización

Con el soporte de aplicaciones de un producto se incluyen definiciones de supervisión inmediatas que incluyen dónde se ejecutarán las definiciones. La aplicación de una distribución o "dónde" se denomina generalmente *distribución*. El almacenamiento de las definiciones de supervisión y distribución de productos en

el servidor de supervisión se denomina *inicialización*. La inicialización se produce automáticamente como parte de la instalación del producto del agente de autodescripción de modo que las definiciones de supervisión predeterminadas se habilitan. Puede modificar o inhabilitar este comportamiento a través de la CLI, pero solo debería hacerlo si no desea todas las definiciones de supervisión proporcionadas por el producto. Para obtener más información, consulte "Configuración de la inicialización del agente de autodescripción" en el manual *IBM Tivoli Monitoring: Guía de instalación y configuración* y "tacmd editSdaOptions" en el manual *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).

El mandato **tacmd listappinstallrecs -d** devuelve los registros de instalación del soporte de aplicaciones de la tabla de propiedades de aplicación del servidor de supervisión, incluidos los valores contenidos en la columna SEEDSTATE. Consulte el manual *IBM Tivoli Monitoring: Consulta de mandatos* para obtener más información.Los siguientes valores de la columna SEEDSTATE reflejan el estado de inicialización de los productos instalados por el agente de autodescripción:

`<blanco>` El valor predeterminado. Este valor indica que la inicialización aún no se ha ejecutado o que no se aplica a este producto. El estado SEEDSTATE solo se aplica a los registros del agente de autodescripción que tiene el ID TMS.

`I` Inicialización del producto en curso.

`Y` Producto inicializado.

`N` Producto no inicializado (no se encuentra el archivo SQL)

`E` Error de inicialización.

Durante el arranque del servidor de supervisión, se producen mensajes en el registro `TEMS MSG2` y en el recurso del registro de auditoría cuando se detectan cambios o errores de instalación del agente de autodescripción en productos instalados. Los registros de instalación del soporte de aplicaciones del servidor de supervisión se actualizan según sea necesario para reflejar los cambios indicados por los mensajes MSG2 o el registro de auditoría. El registro `TEMS RAS1` contiene mensajes de rastreo que muestran la realización correcta o error de los cambios en el soporte de aplicaciones. Debe inspeccionar los mensajes MSG2 y los mensajes del registro de auditoría del manual *IBM Tivoli Monitoring: Guía de resolución de problemas* y completar las siguientes acciones:

- Verifique que los cambios detectados en los productos instalados sean los esperados. Si los cambios no son los esperados o son incorrectos, emprenda la acción adecuada para instalar las versiones de producto correctas, a través de una instalación de agente de autodescripción o de una instalación manual.
- Si alguno de los errores se anotan en un producto instalado del agente de autodescripción, limpie los registros de instalación de soporte de aplicaciones, si es necesario. Para ello, suprima los registros de las instalaciones anómalas mediante el mandato **tacmd deleteappinstallrecs** y reinicie las instalaciones del agente de autodescripción, si es necesario. Consulte en la publicación *IBM Tivoli Monitoring: Consulta de mandatos* los mandatos que puede utilizar para llevar a cabo estas tareas.

Nota: La función del agente de autodescripción no automatiza la instalación de paquetes de idiomas del agente. Los procedimientos de instalación de paquetes de idiomas para agentes de autodescripción son los mismos que los de los agentes estándares. Para obtener más información, consulte "Instalación de paquetes de idiomas" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Habilitación o inhabilitación de la función de autodescripción en el servidor de supervisión

Puede habilitar o inhabilitar la función del agente de autodescripción para un servidor de supervisión específico mediante una variable de configuración de entorno en el Tivoli Enterprise Monitoring Server.

Inhabilite la función de autodescripción siempre que no desee la actualización y propagación automática de los metadatos de aplicación del agente de autodescripción se realice para un servidor de supervisión específico. A continuación, el soporte de aplicaciones para el agente debe instalarse y activarse manualmente en cada servidor de supervisión y servidor de portal. De forma predeterminada, la función de autodescripción para los servidores de supervisión remotos está activada, y para los servidores de supervisión concentradores está desactivada.

Acerca de esta tarea

El método recomendado es controlar la función de agente de autodescripción desde el servidor de supervisión concentrador, ya que la habilitación o inhabilitación en el servidor de supervisión concentrador afecta a todos los servidores de supervisión remotos y agentes que se conectan a él.

La habilitación o inhabilitación de la función de autodescripción en un servidor de supervisión remoto específico afecta a todos los agentes que se conectan sólo a ese servidor.

Utilice los pasos siguientes para detener temporalmente la autodescripción en un único servidor de supervisión editando la variable de entorno de servidor de supervisión de destino.

Procedimiento

- Windows
  1. En el sistema donde está instalado el servidor de supervisión, en la aplicación Manage Tivoli Enterprise Monitoring Services pulse con el botón derecho del ratón en el **Tivoli Enterprise Monitoring Server** y seleccione **Avanzado→ Editar archivo ENV**.
  2. Edite la variable de entorno existente: `KMS_SDA=Y | N`
- Linux UNIX
  1. En el sistema donde está instalado el servidor de supervisión, cambie al directorio `<install_dir>/config/`.
  2. Abra el archivo `<nombrehost_tems>_ms_<nombre_tems>.config`.
  3. Edite la variable de entorno existente: `KMS_SDA=Y | N`
- z/OS Consulte `KMS_SDA` en la publicación *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm).

Qué hacer a continuación

Reinicie el servidor de supervisión.

A continuación, puede revisar las versiones de soporte de agente de las formas siguientes:

- Revise los registros de operaciones del agente y el servidor de supervisión para determinar si el agente opera en modalidad estándar o de agente de autodescripción. El Espacio de trabajo Estatus de sistemas gestionados tiene un enlace al registro de operaciones para cada agente de supervisión.
- El mandato **tacmd listappinstallrecs** devuelve los registros de instalación del soporte de aplicaciones y el mandato **tacmd listSdaStatus** visualiza el estado operativo actual del agente de autodescripción para todos los servidores de supervisión del entorno. Recuerde que estos mandatos no están disponibles cuando el servidor de supervisión no está en ejecución. Consulte el apartado "Instalación del agente de autodescripción" en la página 306.

Habilitación o inhabilitación de la función de autodescripción en el agente

Puede habilitar o inhabilitar la función del agente de autodescripción mediante una variable de configuración del entorno del agente de supervisión.

Inhabilite la función de autodescripción siempre que no desee la actualización y propagación automáticas de los metadatos de aplicación del agente de autodescripción para uno o varios agentes individuales. A continuación, el soporte de aplicaciones para el agente debe instalarse y activarse manualmente en el servidor de supervisión y servidor de portal. De forma predeterminada, la capacidad de autodescripción para los agentes está activada.

Antes de empezar

El método recomendado es controlar la función del agente de autodescripción desde el servidor de supervisión concentrador. Para obtener más información, consulte "Habilitación o inhabilitación de la función de autodescripción en el servidor de supervisión" en la página 315.

Procedimiento

- Windows
  1. En el sistema donde está instalado el agente de supervisión, en la aplicación Manage Tivoli Enterprise Monitoring Services pulse con el botón derecho del ratón en el agente y seleccione **Avanzado→ Editar archivo ENV**.
  2. Edite la variable de entorno existente: `TEMA_SDA=Y | N`
- Linux UNIX
  1. En el sistema donde está instalado el agente de supervisión, vaya al directorio `<install_dir>/config/`.
  2. Abra el archivo de coordinación:
     Para agentes de una sola instancia: `<cp>.ini`
     Para agentes de varias instancias: archivo `<cp>_<instancia>.ini`
     Donde *cp* es el código de producto de dos caracteres.
  3. Edite la variable de entorno existente: `TEMA_SDA=Y | N`
- IBM i
  1. Abra `/qautotmp/kmsparm.kbbenv`.
  2. Edite la variable de entorno existente: `TEMA_SDA=Y | N`
- z/OS Consulte `TEMA_SDA` en la publicación *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: Common Planning and Configuration Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm).

Qué hacer a continuación

Reinicie el servidor de supervisión.

Puede revisar las versiones de soporte de agente de las siguientes formas:

- Revise los registros de operaciones del agente y el servidor de supervisión para determinar si el agente opera en modalidad estándar o de agente de autodescripción. El Espacio de trabajo Estatus de sistemas gestionados tiene un enlace al registro de operaciones para cada agente de supervisión.
- El mandato **tacmd listappinstallrecs** devuelve los registros de instalación del soporte de aplicaciones y el mandato **tacmd listSdaStatus** visualiza el estado operativo actual del agente de autodescripción para todos los servidores de supervisión del entorno. Recuerde que estos mandatos no están disponibles cuando el servidor de supervisión no está en ejecución. Consulte el apartado "Instalación del agente de autodescripción" en la página 306.

Determinación de si los agentes están habilitados para la autodescripción

Puede determinar si un agente está habilitado para la autodescripción antes de la instalación o tras la instalación.

Antes de empezar

Los agentes del sistema operativo base de IBM Tivoli Monitoring V6.2.3 están habilitados para la autodescripción, aunque no todos los agentes están habilitados para la autodescripción.

Los agentes de Tivoli Performance Analyzer y Universal Agent no están habilitados para la autodescripción. Para ver una lista completa de agentes habilitados para la autodescripción, consulte el tema Agentes de IBM Tivoli Monitoring habilitados para la autodescripción (SDA) de IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home).

Acerca de esta tarea

Siga los pasos siguientes para determinar qué agentes están habilitados para la autodescripción.

Procedimiento

- Para determinarlo antes de la instalación:

  En la imagen de instalación busque el archivo manifiesto de autodescripción `K<PC>MSMAN.txt`.

  – Windows El archivo se encuentra en el directorio `WINDOWS`. Para los agentes que se ejecutan en Windows Itanium, el archivo se encuentra en el directorio `WIA64`.

  – Linux UNIX El archivo se encuentra en el directorio `unix`.

  – Para agentes creados mediante Agent Builder, el archivo se encuentra en el directorio `K<PC>/support`.
- Para determinarlo tras la instalación:

  – Windows Ejecute el mandato **kincinfo -e**. Mire la columna `SDA STATUS` para ver si el agente está habilitado para la autodescripción.

En este ejemplo, puede ver que Universal Agent tiene Disabled en la columna SDA STATUS, lo que significa que *no* está habilitado para la autodescripción.

```
kincinfo -e

*************** Thursday, July 14, 2011 1:29:36 PM ***************

User: Administrator                         Group: NA

Host Name: ICVW3A03                         Installer: Ver: 062300000

CandleHome : C:\IBM\d1191a\ITM

Installitm : C:\IBM\d1191a\ITM\InstallITM

******************************************************************

...Application support propagation

PC     PRODUCT DESC                         PLAT       VER             BUILD          SDA STATUS

NT     Monitoring Agent for Windows         WINNT      06.23.00.00     11871          Enabled
       OS

R2     Agentless Monitoring for Windows     WINNT      06.23.00.00     201107051647   Enabled
       Operating Sy

R3     Agentless Monitoring for AIX         WINNT      06.23.00.00     201107051650   Enabled
       Operating System

R4     Agentless Monitoring for Linux       WINNT      06.23.00.00     201107051653   Enabled
       Operating Syst

R5     Agentless Monitoring for HP-UX       WINNT      06.23.00.00     201107051655   Enabled
       Operating Syst

R6     Agentless Monitoring for Solaris     WINNT      06.23.00.00     201107051658   Enabled
       Operating Sy

UM     Universal Agent                      WINNT      06.23.00.00     d1184a         Disabled
```

– Linux UNIX Ejecute el mandato ***<dir_instalación>*/bin/cinfo -e**. Mire la columna SDA STATUS para ver si el agente está habilitado para la autodescripción.

En este ejemplo, puede ver que Tivoli Performance Analyzer y Universal Agent tienen Disabled en la columna SDA STATUS, lo que significa que los agentes *no* están habilitados para la autodescripción.

```
<inst_dir>/bin/cinfo -e

*********** Thu Jul 14 13:19:41 EDT 2011 *****************

User: root                                  Groups: root bin daemon sys adm disk wheel

Host name : icvr5d06                        Installer Lvl:06.23.00.00

CandleHome: /data/tmv623-d1191a-201107110121/ITM

Version Format: VV.RM.FF.II (V: Version; R: Release; M: Modification; F: Fix; I: Interim Fix)

******************************************************************

...Application support propagation

PC     PRODUCT DESC                         PLAT       VER             BUILD          SDA STATUS

80     Monitoring Agent for Self Describing lx8266     03.00.00.00     201106281135   Enabled
       Agent

hd     Warehouse Proxy                      lx8266     06.23.00.00     d1191a         Enabled

lz     Monitoring Agent for Linux OS        lx8266     06.23.00.00     11871          Enabled
```

```
pa    Tivoli Performance Analyzer              lx8266    06.23.00.00    11891          Disabled
r2    Agentless Monitoring for Windows         lx8266    06.23.00.00    201107051647   Enabled
      Operating Systems
r3    Agentless Monitoring for AIX             lx8266    06.23.00.00    201107051650   Enabled
      Operating Systems
r4    Agentless Monitoring for Linux           lx8266    06.23.00.00    201107051653   Enabled
      Operating Systems
r5    Agentless Monitoring for HP-UX           lx8266    06.23.00.00    201107051655   Enabled
      Operating Systems
r6    Agentless Monitoring for Solaris         lx8266    06.23.00.00    201107051658   Enabled
      Operating Systems
sy    Summarization and Pruning Agent          lx8266    06.23.00.00    d1177a         Enabled
ul    Monitoring Agent for UNIX Logs           lx8266    06.23.00.00    11751          Enabled
um    Universal Agent                          lx8266    06.23.00.00    d1184a         Disabled
```

Variables de entorno que controlan la función de autodescripción

Algunas variables de entorno activan o desactivan la función de autodescripción en el servidor de supervisión, en el servidor de portal o en el agente.

Finalidad

Las variables de entorno controlan la funcionalidad principal de la función de autodescripción y son los únicos parámetros que los usuarios típicos modifican. Todas las variables de entorno de autodescripción se modifican únicamente bajo la indicación del equipo de soporte de IBM.

Atención: Este tema está pensado sólo para proporcionar una referencia a las principales variables de entorno de autodescripción. Para ver una lista completa de variables de entorno de autodescripción, consulte el tema sobre "Variables de entorno" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Parámetros

No especifique YES o NO; especifique en su lugar Y o N.

Parámetros del servidor de supervisión

KMS_SDA=Y | N
N inhabilita la función del agente de autodescripción en el servidor de supervisión, mientras que Y la habilita. Cuando se inhabilita la autodescripción en el servidor de supervisión concentrador, se inhabilita *toda* la función de autodescripción.

El valor predeterminado es N para los servidores de supervisión concentrador.

El valor predeterminado es Y para los servidores de supervisión remotos.

TEMS_MANIFEST_PATH=*ubic_archivo*
La ubicación donde desea que el servidor de supervisión almacene los archivos JAR y de manifiesto que recopila de los agentes de autodescripción. El cliente debe crear y establecer los permisos correctos para cualquier directorio personalizado o alternativo que se especifique. El directorio no lo crea el

servidor de supervisión. Este parámetro se debe establecer para que la función de autodescripción se habilite; generalmente se establece durante la instalación del componente.

TEMS_JAVA_BINPATH
Esta variable localiza la vía de instalación de Java dentro del entorno z/OS USS. Se puede sustituir dinámicamente con un archivo de configuración local cada vez que el motor de z/OS genera su interfaz de shell de USS. Para obtener más información, consulte *Configuring the Tivoli Enterprise Monitoring Server on z/OS* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/ztemsconfig/ztemsconfig.htm).

Parámetros del servidor de portal

TEPS_SDA=Y | N
N inhabilita la función del agente de autodescripción en el servidor de portal, mientras que Y la habilita.

El valor predeterminado es Y.

TEPS_MANIFEST_PATH=*ubic_archivo*
Se establece de forma predeterminada en la ubicación en la que el servidor de portal grabará y almacenará los archivos JAR de soporte del producto recuperados. Generalmente este parámetro se establece durante la instalación del componente.

Parámetros del agente

TEMA_SDA=Y | N
N inhabilita la función del agente de autodescripción en el agente, mientras que Y la habilita. El valor N impide que el servidor de supervisión recupere archivos de soporte del producto de este agente y ofrece al usuario el control agente a agente sin detener la función del agente de autodescripción en el servidor de supervisión para otros productos.

El valor predeterminado es Y.

Capítulo 14. Servicios de gestión de agentes

Utilice los Servicios de gestión de agentes para supervisar la disponibilidad de los agentes y responder automáticamente (por ejemplo, con un reinicio) si el estado del agente pasa a ser incorrecto o si se cierra de forma imprevista. Con estos servicios puede mejorar la disponibilidad de los agentes.

Características de Tivoli Agent Management Services

Los Servicios de gestión de agentes se basan únicamente en atributos comunes a todos los agentes (como la ubicación de la instalación del sistema de archivos, la ubicación del archivo de registro del sistema de archivos y el nombre de ejecutable) y en las API comunes a los sistemas operativos (como la enumeración de la lista de los procesos en ejecución). Con esta información, los Servicios de gestión de agentes mejoran la disponibilidad de los agentes y proporcionan una interfaz sencilla y unificada para ver y controlar la disponibilidad de los agentes.

Puede poner un agente bajo la gestión de los Servicios de gestión de agentes sin realizar ningún cambio en el agente. A medida que se añaden agentes adicionales a un sistema, se pueden poner fácilmente bajo la gestión de los Servicios de gestión de agentes.

Los Servicios de gestión de agentes constituyen un enfoque estratégico a la gestión de agentes de Tivoli Monitoring que ofrecen estas características:

- Posibilidad de supervisar la disponibilidad de otros agentes y responder automáticamente ante situaciones fuera de lo normal según la política de usuario.
- Un método automatizado mediante valores de políticas y un método manual mediante mandatos de actuación de Tivoli Enterprise Portal para iniciar, detener, *gestionar* y *dejar de gestionar* manualmente un agente.
- Espacios de trabajo de gestión de agentes con vistas de la información que recopilan los Servicios de gestión de agentes. Se suministran espacios de trabajo de gestión de agentes para agentes de Tivoli Enterprise Monitoring básicos y distribuidos.

Relaciones entre los componentes

Los Servicios de gestión de agentes utilizan tres interfaces para comunicarse con otros componentes del proceso del agente del sistema operativo.

© Copyright IBM Corp. 2005, 2013

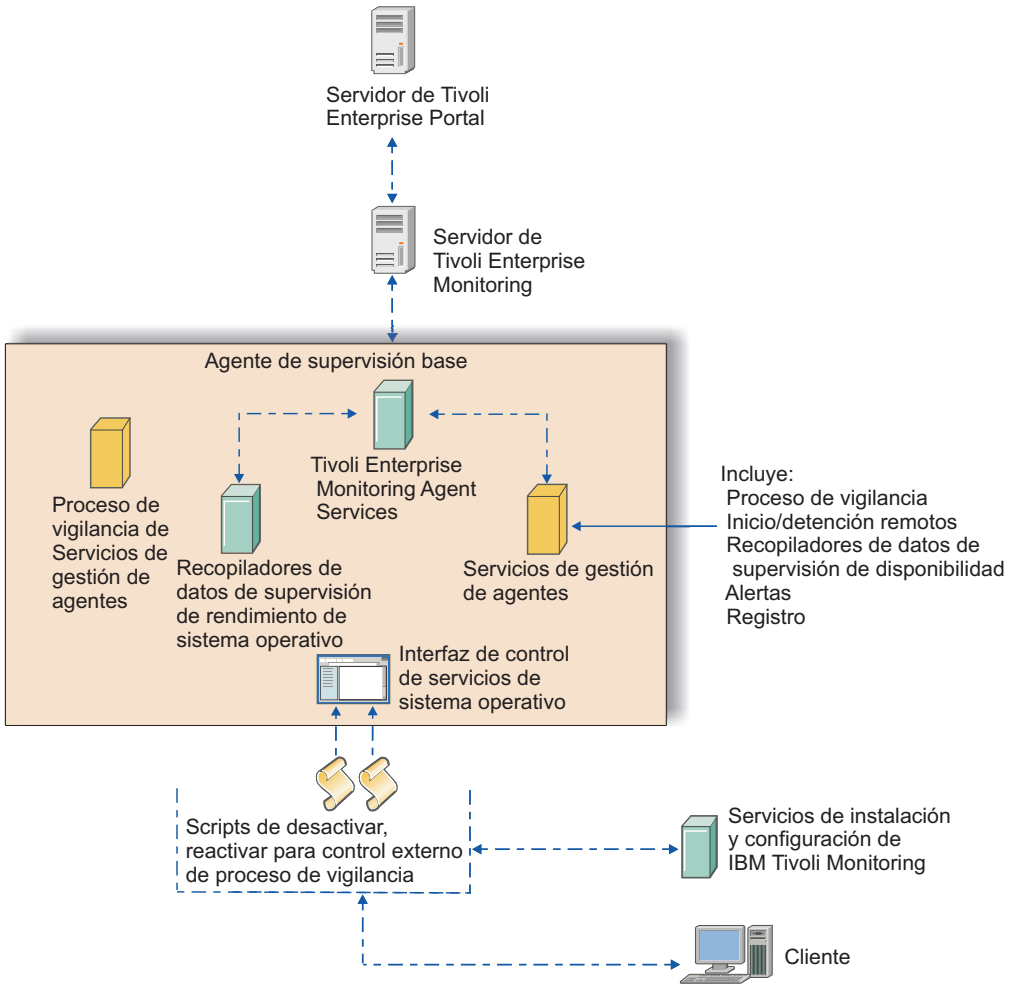

Figura 30. Interacciones de los componentes de los Servicios de gestión de agentes con componentes de IBM Tivoli Monitoring

Descripciones de los componentes

Los servicios de gestión de agentes incluyen dos componentes: proceso de vigilancia del agente y proceso de vigilancia de los servicios de gestión de agentes:

Proceso de vigilancia del agente

El proceso de vigilancia del agente realiza acciones de supervisión de disponibilidad específicas en un agente basándose en la política del archivo CAP (*Common Agent Package*) del agente. Este componente se ejecuta dentro del proceso del agente del sistema operativo como un componente lógico. El proceso de vigilancia no sólo vigila al propio agente del sistema operativo, sino también a cualquier agente de supervisión que tenga un archivo XML en el directorio `CAP` de la instalación del agente del sistema operativo.

Proceso de vigilancia de los Servicios de gestión de agentes

¿Quién vigila el proceso de vigilancia? Es el trabajo de *vigilancia de los Servicios de gestión de agentes*, también denominado *proceso de vigilancia de los servicios del agente de proxy*.. Puede comprobar el estado de este proceso de vigilancia en la vista **Estado de tiempo de ejecución de los agentes** de Tivoli Enterprise Portal. Proporciona supervisión similar al proceso de vigilancia del agente en el agente de sistema operativo, pero se utiliza sólo

para vigilar el agente de sistema operativo. El proceso de vigilancia del agente en el agente de SO proporciona prestaciones adicionales que incluyen la supervisión de otros agentes, la respuesta a consultas de escritorio de Tivoli Enterprise Portal y el manejo de las actuaciones mediante el recurso de comunicación del agente de SO. El proceso de vigilancia de los Servicios de gestión de agentes se incluye como un archivo ejecutable autónomo con los agentes del sistema operativo y se ejecuta como el proceso **kcawd** en Linux y en sistemas operativos como UNIX, y como un proceso **kcawd.exe** en Windows.

Interfaz de usuario de Tivoli Enterprise Portal

Tivoli Enterprise Portal es la interfaz de usuario para los Servicios de gestión de agentes, con mandatos de actuación predefinidos para iniciar o detener manualmente un agente mediante los Servicios de gestión de agentes y para iniciar o detener un agente cuando está gestionado por los Servicios de gestión de agentes. Estos mandatos de actuación están disponibles desde los menús emergentes del espacio de trabajo de Servicios de gestión de agentes y se puede hacer referencia a los mismos en situaciones para la automatización de reflejo.

Nota: También puede continuar utilizando los métodos más familiares para iniciar y detener un agente como, por ejemplo, mediante Manage Tivoli Enterprise Monitoring Services y mediante el menú emergente de Navigator de Tivoli Enterprise Portal.

Instalación y configuración de Tivoli Agent Management Services

Los Servicios de gestión de agentes se instalan automáticamente con el agente del sistema operativo Linux, el agente del sistema operativo UNIX o el agente del sistema operativo Windows, en función de la plataforma del host. Los archivos de soporte de aplicaciones de estos agentes también se instalan en el Tivoli Enterprise Monitoring Server y el Tivoli Enterprise Portal Server.

Con IBM Tivoli Monitoring V6.2.3 Fixpack 1 o posterior, los agentes de sistema operativo se supervisan mediante sockets además del estado del proceso y la comprobación `cinfo`. El socket supervisado es un PIPE utilizado internamente por los servicios del agente de proxy para solicitudes externas. Puede optar por reiniciar el agente del sistema operativo si no responde en el socket en un número consecutivo de intentos especificado por la variable de entorno `KCA_MAX_RETRIES_ON_PIPE`. Cuando la variable se haya modificado en el archivo ENV del agente, debe reiniciar el agente para que los cambios se implementen. De forma predeterminada la variable no está definida, lo que significa que el agente del sistema operativo nunca se reinicia. Debe utilizar un valor para esta variable que sea mayor que 5.

Archivo de paquete del agente común

El comportamiento de supervisión de los Servicios de gestión de agentes en relación con un agente concreto se rige mediante los valores de un archivo de políticas basado en XML, al que se hace referencia como un archivo CAP (*Common Agent Package*). Cada agente que se puede gestionar mediante los Servicios de gestión de agentes instala un archivo CAP llamado, donde *cp* es el código de producto, k*cp*`_default.xml` en un directorio definido por la variable de entorno **KCA_CAP_DIR** en el archivo de configuración del agente de supervisión del sistema operativo para la plataforma relevante. Los agentes que se ejecutan de forma nativa en Windows de 64 bits colocan sus archivos CAP en el directorio del agente

de Tivoli Monitoring de 64 bits; los demás van al directorio de 32 bits:
Windows *install_dir*\TMAITM6[_x64]\CAP
Linux UNIX *install_dir*/config/CAP.

En la plataforma zLinux, Servicios de gestión de agentes tiene los siguientes comportamientos:

- V6.2.3 Fixpack 1 (con una instalación nueva): Habilitado de forma predeterminada
- V6.2.3 Fixpack 1 (para actualizaciones): Habilitado o inhabilitado, en función del estado encontrado antes de la actualización.
- V6.2.2 Fixpack 2 o posterior: Inhabilitado en la instalación o tras una actualización, independientemente de si estaba activo o inactivo antes de la actualización

Para habilitar Servicios de gestión de agentes después de una actualización, establezca la variable de entorno KCA_CAP_DIR en un directorio existente que contenga los archivos CAP.

En Intel Linux y en otras plataformas soportadas, los Servicios de gestión de agentes se habilitan de forma predeterminada.

Elementos que se pueden personalizar del archivo CAP

El archivo CAP instalado por el agente se configura como de sólo lectura y no se debe modificar directamente. Si desea personalizar los valores de política de este archivo, cree una copia del archivo y nómbrelo según el convenio k*pc*.xml. El proceso de vigilancia detecta automáticamente cuando se añade un nuevo archivo CAP o cuando se elimina un archivo CAP del directorio. Los cambios en un archivo CAP existente requieren que se reinicie el agente del sistema operativo para que se apliquen los cambios. Se puede realizar una actualización de un archivo CAP de agente no de sistema operativo sin necesidad de reiniciar el agente de sistema operativo. Para completar esta acción, elimine el archivo CAP del directorio y a continuación, una vez que el proceso de vigilancia ha descubierto que se ha eliminado el archivo, copie el archivo actualizado de nuevo en el directorio. Una actualización de un archivo CAP de agente de SO requiere que se reinicie el agente de SO.

Puede tener un archivo CAP que controle agentes de supervisión de varias instancias o puede crear un archivo CAP separado para cada instancia.

Los elementos definidos en el archivo CAP se pueden visualizar en la vista "Definiciones de gestión de agentes" de Tivoli Enterprise Portal del espacio de trabajo Servicios de gestión del agente. **Nota:** Los atributos no definidos en el archivo CAP no se muestran en la vista "Definiciones de gestión del agente".

El orden de los elementos es importante. Revise kwgcap.xsd para ver una definición formal del esquema del archivo CAP.

<checkFrequency>
El período de tiempo entre las comprobaciones de disponibilidad de los Servicios de gestión de agentes del agente gestionado. Si la carga del sistema es abundante, tenga en cuenta la posibilidad de aumentar el intervalo de checkFrequency junto con el valor de la variable de entorno del agente KCA_CMD_TIMEOUT.

Especifique el valor de frecuencia en múltiplos de 5 segundos, hasta un máximo de 3600 segundos (1 hora). Valor predeterminado: **120**.

<cpuThreshold>
El porcentaje máximo de tiempo de CPU que el proceso del agente puede consumir durante un intervalo de tiempo en segundos igual al valor de "checkFrequency", antes de que los Servicios de gestión de agentes consideren que su estado de salud es incorrecto y lo reinicien.

Especifique el porcentaje de umbral como in entero positivo comprendido entre 1 y 100.

<memoryThreshold>
El promedio máximo de memoria del área de trabajo que el proceso del agente puede consumir durante un intervalo de tiempo en segundos igual al valor de "checkFrequency", antes de que los Servicios de gestión de agentes consideren que su estado de salud es incorrecto y lo reinicien.

Especifique el valor de umbral seguido de la unidad de medida: KB, MB o GB. Ejemplo: 50 MB.

<managerType>
La entidad que realiza la supervisión de disponibilidad del agente.

Especifique un valor enumerado: `NotManaged` o `ProxyAgentServices`. Valor predeterminado: **NotManaged**.

<maxRestarts>
El número de veces por día que se debe reiniciar un agente cuyo estado no es bueno o que se ha detenido de forma anómala. Los agentes que no se han de mantener en ejecución pueden tener el valor 0.

Escriba un entero positivo. Valor predeterminado: **4**.

<subagent id>
Edite este valor *únicamente* si va a crear un archivo CAP específico de la instancia para un determinado agente. Por ejemplo, si desea crear un archivo CAP específicamente para un conjunto de instancias de agente de DB2 donde el archivo `kud_default.xml` tiene un subagente `id="kudagent"`, establézcalo en algo parecido a `<subagent id="kud_instance">`. El valor `<agentName>` para el archivo CAP original del agente y para los archivos CAP específicos de sus instancias deben coincidir.

Especifique un valor de cadena para el ID.

<instance>
Utilice este elemento para proporcionar nombres de instancia específicos a los que se aplican las políticas de archivo CAP. Debe ir tras el elemento `<agentName>` en el archivo CAP. Por ejemplo, para especificar que una instancia de un archivo CAP se debe aplicar a dos instancias específicas del agente de DB2 de Tivoli Monitoring, denominado `test1` y `test2`, especifique esta información:

```
<subagent id="kud_instance">
<agentName>ITCAM Agent for DB2</agentName>
<instancia>
   <name>test1</name>
   <name>test2</name>
</instance>
```

Especifique un valor de cadena para el nombre de la instancia entre un par de etiquetas <name> </name>.

Agentes de supervisión de base de datos y de mensajería en Linux y UNIX

Los agentes de base de datos y mensajería suelen iniciarse como usuarios no root. Para que los Servicios de gestión de agentes den soporte a este comportamiento, puede especificar que un agente se inicie como un usuario determinado en el script de inicio del archivo CAP.

Los Servicios de gestión de agentes se basan en el mismo archivo que los archivos de autoscript, **kcirunas.cfg**, para obtener información de configuración sobre el usuario como el que se debe *ejecutar como* (RunAs) un agente. Esta información se utiliza cuando los Servicios de gestión de agentes inician el agente para garantizar que se ejecute como el usuario correcto. En un entorno en el que los agentes se despliegan de forma remota, utilice el archivo ***nombrehost*_kdyrunas.cfg**. También se comprueba la información de *RunAs* del archivo.

Si desea habilitar este soporte en un archivo CAP anterior, actualice el archivo CAP tal como se muestra en el siguiente ejemplo de Universal Agent (um) en Linux (lz):

```
<startScript>
  <command>$CANDLEHOME/$ITM_BINARCH/lz/bin/agentInstanceCommand.sh
  um START ##INSTANCE##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</startScript>

<startScript>
  <command>$CANDLEHOME/$ITM_BINARCH/lz/bin/agentInstanceCommand.sh
  um START ##INSTANCE## ##USER##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</startScript>
```

Para habilitar este soporte en un archivo CAP anterior, actualice el script de detención:

```
<stopScript>
  <command>$CANDLEHOME/$ITM_BINARCH/lz/bin/agentInstanceCommand.sh
  um STOP ##INSTANCE## ##USER##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</stopScript>
```

Para agentes de una sola instancia en Linux, utilice esta sintaxis:

```
<startScript>
  <command>su -c "$CANDLEHOME/bin/itmcmd agent start ul" -
  ##USER##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</startScript>

<stopScript>
  <command>su -c "$CANDLEHOME/bin/itmcmd agent stop ul" -
  ##USER##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</stopScript>
```

Para agentes de una sola instancia como UNIX Log Agent, utilice esta sintaxis. Es idéntica a la sintaxis de Linux excepto que - ##USER## se coloca después de su en lugar de al final:

```
<startScript>
  <command>su - ##USER## -c "$CANDLEHOME/bin/itmcmd agent start ul"
  </command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</startScript>

<stopScript>
  <command>su - ##USER## -c "$CANDLEHOME/bin/itmcmd agent stop ul"
 </command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</stopScript>
```

Actualice el archivo CAP de Universal Agent de la V6.2.1 a la V6.2.2 o posterior

IBM Tivoli Monitoring V6.2.2 no da soporte a varias instancias del agente cuando <agentType> se establece en el valor **WinService** en lugar de **ITM_Windows** o **ITM_UNIX**, que es necesario para V6.2.2 o posterior.

- Con el valor **ITM_Windows** o **ITM_UNIX** para <agentType>, se utilizan programas de utilidad de instalación `kincinfo/cinfo` estándar de Tivoli Monitoring para descubrir instancias del agente de supervisión.
- Con el valor **WinService** para <agentType> para agentes de supervisión de varias instancias, ya no se visualizan los nombres de instancia de Tivoli Monitoring. El tipo de agente debe ser ahora **ITM_UNIX** o **ITM_Windows**.

Los archivos CAP se han actualizado de V6.2.1 a V6.2.2 o posterior

En V6.2.1, el agente de SO Linux proporcionaba cinco archivos CAP predeterminados en el directorio `$CANDLEHOME/$INTERP_BIN/lz/bin/CAP`. En V6.2.2 o posterior, la ubicación se ha cambiado por `$CANDLEHOME/config/CAP` y los archivos CAP se suministran con cada agente. Cuando un agente de SO Linux se actualiza de V6.2.1 a un release posterior, utilizará los archivos CAP que se encuentran en el directorio `$CANDLEHOME/config/CAP`. Cualquier personalización de los archivos CAP debe basarse en los archivos del directorio `$CANDLEHOME/config/CAP`. Los archivos CAP de la V6.2.1 siguen estando en el sistema en el directorio original si se necesitan.

Referencia relacionada:

Consideraciones sobre la instalación en Linux o UNIX: scripts de inicio automático
La configuración de RunAs del agente está en kcirunas.cfg.

Supervisión de la disponibilidad de los agentes

Los Servicios de gestión de agentes responden a un agente detenido o reconfigurado mediante un reinicio. Los Servicios de gestión de agentes determinan el agente que se detiene en función de su tipo, el mandato especificado en el elemento <availabilityStatusScript> del archivo CAP o ambos.

Para los agentes de tipo *Console*, los Servicios de gestión de agentes determina si el agente se detienen consultando el sistema operativo en busca de aplicaciones en ejecución utilizando el valor del elemento `<agentPath>` del archivo CAP.

Para agentes de tipo *WinService*, la determinación se realiza consultando en el gestor de control de servicios de Windows el estatus del servicio definido en el elemento `<serviceName>` del archivo CAP.

Para agentes e instancias de tipo *ITM_Windows* e *ITM_UNIX*, los Servicios de gestión de agentes determinan si el agente se detiene mediante el mandato especificado en el elemento `<availabilityStatusScript>` del archivo CAP, que puede ser kinconfg o un script que llama a cinfo.

Si el sistema operativo no muestra el proceso en su lista de procesos en ejecución, los Servicios de gestión de agentes saben que el proceso ha concluido e intentarán reiniciarlo mediante el mandato o script definido en el elemento `<startScript>` del archivo del paquete del agente común. Si no existe un archivo CAP, se comprueba el sistema operativo.

Si los agentes gestionados se han configurado pero no se han iniciado, el proceso de vigilancia los iniciará automáticamente 30 minutos después de haber sido configurados. Los agentes gestionados cuyas instancias configuradas las inicia el usuario, se descubrirán inmediatamente y aparecerán en la vista Estatus de disponibilidad del agente.

Si el número de intentos de conexión con el servidor de supervisión supera el valor de CTIRA_MAX_RECONNECT_TRIES (cuyo valor predeterminado es 0), el agente intenta realizar una conclusión. Si el proceso de vigilancia de los Servicios de gestión de agentes se está ejecutando, inmediatamente reinicia el agente. Si desea que se concluya el agente cuando se supera el valor de CTIRA_MAX_RECONNECT_TRIES, se debe inhabilitar este proceso de vigilancia. Utilice la acción AMS Detener gestión para inhabilitar el proceso de vigilancia.

Gestión manual del agente

Desde el espacio de trabajo *Servicios de gestión de agentes* del agente, puede ejecutar estos mandatos de actuación para iniciar, detener, gestionar y dejar de gestionar los agentes.

La acción realizada persistirá hasta que utilice la acción opuesta o hasta que inicie o detenga un agente con otro método (Tivoli Enterprise Portal, Manage Tivoli Monitoring Services o en la línea de mandatos). En la vista de tabla *Estatus de gestión de los agentes*, pulse con el botón derecho del ratón en la fila del agente cuyo estatus desea cambiar y seleccione la acción:

AMS Reiniciar instancia del agente
Utilice esta acción para detener y reiniciar una instancia concreta del agente de supervisión.

AMS Restablecer recuento de reinicios del agente
Utilice este agente para devolver a 0 el recuento de intentos del agente de reiniciarse.

AMS Iniciar agente
Utilice esta acción para iniciar un agente que se encuentre bajo la gestión de los Servicios de gestión de agentes de IBM Tivoli Monitoring. Para un agente de varias instancias utilice **AMS Iniciar instancia del agente**.

AMS Detener agente
Utilice esta acción para detener un agente que se encuentre bajo la gestión de los Servicios de gestión de agentes de IBM Tivoli Monitoring.

AMS Iniciar instancia del agente
Utilice esta acción para iniciar una instancia concreta del agente de supervisión.

AMS Iniciar gestión
Utilice esta acción para colocar un agente bajo la gestión de los Servicios de gestión de agentes de IBM Tivoli Monitoring. Resulta útil cuando el agente se ha puesto fuera de línea intencionadamente y el usuario está listo para reanudar la ejecución del agente y para que este se gestione.

AMS Detener gestión
Utilice esta acción para eliminar un agente de la gestión de los Servicios de gestión de agentes de IBM Tivoli Monitoring. Resulta útil si desea colocar un agente fuera de línea y que no se reinicie automáticamente.

Por ejemplo, para iniciar la gestión del agente universal para Windows (se muestra en el espacio de trabajo Servicios de gestión de agentes, en la vista Estatus de gestión del agente aparece como *No gestionado*), pulse con el botón derecho del ratón la fila y pulse **Actuación > Seleccionar**. Seleccione la acción AMS Iniciar gestión de la lista de acciones posibles. El mandato se muestra como `NT:AMS_Start_Manage "Universal Agent for Windows"`. Pulse **Aceptar** para iniciar la gestión del agente. Tras pulsar **Renovar**, el estatus de Universal Agent cambia a *Gestionado*.

Para obtener más información sobre cada mandatos y sobre los mandatos de actuación en general, consulte el manual *Tivoli Enterprise Portal: Guía del usuario* y la guía del usuario del agente específico.

Referencia relacionada:

Mandatos de actuación
Cómo utilizar y definir mandatos de actuación en Tivoli Enterprise Portal

Capítulo 15. Autonomía del agente

Un Tivoli Enterprise Monitoring Agent puede ejecutarse independientemente del Tivoli Enterprise Monitoring Server. Puede configurar distintos niveles de autonomía en función de la funcionalidad que deba tener el agente de supervisión, las restricciones de recursos y el nivel de dependencia que deba tener el agente del servidor de supervisión. Cualquier agente de supervisión con una infraestructura de IBM Tivoli Monitoring V6.2.2 FP2 o posterior pueden configurarse para que se ejecute de forma autónoma.

Los agentes de supervisión se inician independientemente de su servidor de supervisión y recopilan datos, ejecutan situaciones y registran sucesos cuando se desconectan del servidor de supervisión. Este es el comportamiento predeterminado, que se puede ajustar para una mayor o menor autonomía.

Si configura un Agent Builder o agente de SO para que sea autónomo, éste se convierte en un agente de Tivoli System Monitor. Los agentes de supervisor del sistema se instalan y configuran para que no tengan conexiones o dependencias a un servidor de supervisión. Los agentes del supervisor del sistema son como cualquier otro agente de supervisión, salvo que cualquier proceso que se puede llevar a cabo solamente mediante el servidor de supervisión no está disponible. Asimismo, un agente de supervisor del sistema no se puede instalar en el mismo sistema que el componente Tivoli Management Services o que un agente de supervisión de empresa.

Puede configurar archivos XML especializados para definir y ejecutar situaciones localmente, para recopilar y guardar datos históricos localmente y para emitir alertas SNMP (Simple Network Management Protocol) o sucesos Event Integration Facility (EIF) o ambos a un receptor correspondiente sin conexión con un servidor de supervisión. Estos archivos XML especializados están disponibles para los agentes de supervisión de empresa y para los agentes de supervisión del sistema.

Funciones autónomas

Además de la función autónoma integrada de los agentes de Tivoli Enterprise Monitoring y agentes de Tivoli System Monitor, puede configurar archivos XML especiales que no necesiten conexión con un Tivoli Enterprise Monitoring Server. Con estos archivos XML, puede definir y ejecutar situaciones localmente, emitir sucesos de situación como alertas SNMP o sucesos EIF a un receptor, recopilar y guardar datos históricos localmente, y utilizar configuración centralizada para configurar actualizaciones de archivos XML a determinados agentes de supervisión.

Tivoli Enterprise Monitoring Agent

Los agentes de Tivoli Enterprise Monitoring están configurados de forma predeterminada para un funcionamiento autónomo: el agente se inicia y continúa ejecutándose con o sin conexión con su servidor de supervisión. Sin conexión con el servidor de supervisión, el agente puede continuar ejecutando situaciones de forma autónoma; cuando el agente se vuelve a conectar, cargará los sucesos de situaciones que se han producido mientras ha estado desconectado. Esto hace que se utilice espacio de disco adicional en el agente.

© Copyright IBM Corp. 2005, 2013

Es posible que algunas situaciones no se puedan evaluar por completo únicamente en el agente y que no sea posible ejecutarlas cuando no existe una conexión con el servidor de supervisión. Por ejemplo, las situaciones que utilizan una función de grupo, como COUNT o AVG, se deben evaluar en el servidor de supervisión. Incluso si se reinicia el agente, o el sistema del host, los sucesos se conservan de forma permanente y se transfieren durante la reconexión. Esto sucede de forma automática en todos los agentes que utilizan la infraestructura V6.2.2 o posterior del Tivoli Enterprise Monitoring Agent. No se requieren cambios de configuración.

La *modalidad autónoma* se incorporó en V6.2.1 como un parámetro configurable del agente: IRA_AUTONOMOUS_MODE. A partir de V6.2.2, esté parámetro está habilitado (tiene el valor **Y**) de forma predeterminada. Si no desea que el comportamiento autónomo esté habilitado para un agente, puede inhabilitarlo estableciendo el parámetro en **N**. Independientemente del valor de este parámetro, la recopilación de datos históricos siempre se ejecuta de forma autónoma y se realiza una automatización refleja de una situación cuando esta pasa a ser verdadera. Consulte el apartado "Variables de entorno para comportamiento autónomo" en la página 335.

z/OS Los agentes de OMEGAMON XE for z/OS y OMEGAMON XE for Storage se deben ejecutar conectados porque están configurados en el Tivoli Enterprise Monitoring Server en el RTE local: si el servidor de supervisión deja de estar disponible, estos agentes también. El hecho de que se ejecuten conectados al servidor de supervisión no evita que den soporte a funciones autónomas, como la emisión de condiciones de excepción SNMP y situaciones privadas. (El agente OMEGAMON XE en z/OS se puede configurar de modo que se ejecute de forma autónoma, y por lo tanto sin conexión con el servidor de supervisión, pero esto significa que no hay datos plex disponibles para alertas y situaciones.) OMEGAMON XE para IMS no da soporte actualmente a ninguna de las funciones autónomas.

Tivoli System Monitor Agent

El Tivoli System Monitor Agent está instalado en un sistema que no tiene componentes de Tivoli Management Services ni agentes de Tivoli Enterprise Monitoring instalados que no sean agentes creados con Tivoli Monitoring Agent Builder V6.2.2 o posterior.

El Tivoli System Monitor Agent es un agente de SO que nunca se conecta a un servidor de supervisión. La versión autónoma del agente utiliza el mismo código de agente que se ha instalado para un agente de sistema operativo completo, pero para el proceso de instalación no se utiliza Java y no se proporciona una configuración de interfaz de usuario. La instalación resultante es más rápida y ocupa menos. Los archivos de configuración XML locales que definen estas funciones como situaciones privadas y alertas SNMP se procesan durante el arranque del agente.

Situaciones privadas

Los agentes de supervisión de empresa y los agentes de supervisión del sistema pueden utilizar las situaciones definidas localmente para funcionar por completo de forma autónoma. Estas *situaciones privadas* definidas localmente se crean en el archivo XML de definición de situaciones privadas. Los sucesos de situaciones privadas proceden directamente del agente de supervisión. Debe colocar un archivo de configuración de situaciones privadas en la instalación del agente y reiniciar el agente para habilitar esta función. Si desea enviar una alerta SNMP o un suceso EIF

cuando se abra un suceso de situación privada, el archivo de configuración de condiciones de excepción de SNMP o el archivo de configuración de sucesos EIF también debe estar en la instalación del agente.

Las situaciones privadas en un agente de supervisión de empresa no tienen ninguna interacción con ningún tipo de servidor de supervisión ni envían ninguna notificación al mismo. Las situaciones privadas y las situaciones de empresa se pueden ejecutar simultáneamente.

Importante: Tenga en cuenta que todas las situaciones, ya sean privadas o de empresa, deben tener nombres exclusivos. De lo contrario, las acciones invocadas sobre una situación se aplican a otra situación con el mismo nombre. Puede utilizar el mandato de CLI **tacmd listSit** para obtener una lista de situaciones de empresa en el servidor de supervisión concentrador.

Consulte el apartado “Situaciones privadas” en la página 347.

alertas SNMP y sucesos EIF

Antes de IBM Tivoli Monitoring V.6.2.2, el Tivoli Enterprise Monitoring Server podría reenviar los sucesos de situación correspondientes a un agente de supervisión a un receptor EIF (Event Integration Facility). IBM Tivoli Monitoring V.6.2.2 o posterior le permite configurar alertas SNMP de modo que se envíen para sucesos de situación a un receptor SNMP directamente desde el agente, sin tener que pasar primero por el servidor de supervisión. Paralelamente, con IBM Tivoli Monitoring V.6.2.2 FixPack 1 o posteriores, puede crear un archivo de configuración de sucesos EIF para emitir sucesos de situación privados a un receptor EIF.

Estos métodos de enviar sucesos a OMNIbus pueden coexistir y el entorno supervisado se puede configurar con cualquier combinación de lo siguiente:

- Reenviar sucesos de situación de empresa a través del servidor de supervisión a receptores como el servidores de sucesos IBM Tivoli Enterprise Console y la Netcool/OMNIbus Probe for Tivoli EIF. (Consulte Integración de sucesos de situación con Tivoli Enterprise Console e Integración de sucesos de situación con Tivoli Netcool/OMNIbus.)
- Enviar alertas SNMP para sucesos de situación de empresa, sucesos de situación privada o ambos a receptores como la prueba Netcool/OMNIbus SNMP.
- Emitir sucesos de situación privados directamente a un receptor de EIF según lo definido en un archivo de configuración de sucesos de EIF.

Situaciones de empresa: Puede crear un archivo XML de configuración de condiciones de excepción que permita a un agente emitir alertas SNMP directamente al receptor de sucesos sin tener que direccionar a través del servidor de supervisión. El agente se debe conectar con el servidor de supervisión al menos una vez para poder recibir las definiciones de situaciones de empresa. El usuario debe colocar un archivo de configuración de condiciones de excepción SNMP en la instalación del agente y reiniciar el agente para poder habilitar esta función.

Situaciones privadas: Los agentes de supervisión de empresa y los agentes de supervisión del sistema también pueden enviar alertas SNMP para situaciones privadas directamente a un receptor como la prueba Netcool/OMNIbus SNMP o emitir sucesos de EIF para situaciones privadas a un receptor de EIF como el servidor de sucesos IBM Tivoli Enterprise Console o la Netcool/OMNIbus Probe for Tivoli EIF.

Importante: Si va a reenviar sucesos de situación de empresa a la Netcool/OMNIbus Probe for Tivoli EIF y va a emitir alertas SNMP para sucesos de situación de empresa a la prueba Netcool/OMNIbus SNMP, existe una diferencia en los formatos de los sucesos de situación reenviados por EIF y las alertas SNMP y los datos que contiene cada uno. Tenga en cuenta que la deduplicación de OMNIbus no detectará un suceso correspondiente a una situación que envían ambas pruebas conectadas al mismo Netcool/OMNIbus ObjectServer como el mismo suceso. Esto da lugar a entradas duplicadas para el mismo suceso dentro de ObjectServer que se tratarán individualmente. Generalmente esto no es lo deseado y puede resultar difícil de gestionar.

Consulte el apartado "Alertas SNMP" en la página 378 y el apartado "Sucesos de EIF" en la página 396.

Historial privado

Al igual que puede crear situaciones privadas para los agentes instalados localmente, puede configurar el historial privado para la recopilación de datos históricos a corto plazo en el mismo archivo de configuración de situaciones privadas utilizando el elemento HISTORY. Los archivos binarios de historial privado resultantes se pueden ver con la Interfaz de servicio del agente. Si ha configurado Tivoli Data Warehouse, puede acumular los datos a corto plazo en una base de datos histórica a intervalos.

El elemento HISTORY incluye un atributo para establecer el número de horas que se deben conservar los datos históricos en el sistema antes de que se recorten o se acumulen en el almacén de datos. Aunque el valor predeterminado consiste en conservar datos históricos durante 24 horas, no hay límite en el número de horas que puede conservarlos localmente, aparte de las limitaciones prácticas del almacenamiento del sistema. Si no tiene el parámetro EXPORT configurado, puede utilizar los programas de conversión de archivos que se proporcionan, como por ejemplo krarloff, para mover datos de los archivos históricos a archivos de texto.

El elemento WAREHOUSE especifica la ubicación del agente de proxy de almacén al que se exportan los datos históricos.

Consulte el apartado "Historial privado" en la página 370.

Alteraciones temporales de situación de empresa

Puede configurar alteraciones temporales de situación para el agente de supervisión de empresa instalado localmente utilizando un archivo de configuración *cp*`_thresholds.xml` (donde *cp* es el código de producto de dos caracteres). Y puede gestionar las alteraciones temporales en el agente manualmente o con una configuración centralizada. Los umbrales de la situación actualizada entran en vigor cuando reinicia el agente de supervisión. El agente envía alteraciones temporales de umbral a un archivo local y mantiene los umbrales de situación activos durante reinicios del agente.

Puede aplicar una planificación por días de la semana, días del mes y hora de inicio y de finalización de un día. El agente de supervisión de empresa mantiene los seguimientos de auditoría de alteraciones temporales de umbral de situación dinámica grabando registros de umbral de situación activa en el registro de operaciones del agente, que puede añadir a un espacio de trabajo en Tivoli Enterprise Portal para revisar los umbrales de situación en vigor.

Consulte el apartado "Especificación XML de alteración temporal de situación de empresa" en la página 373.

Interfaz de servicio del agente
El programa de utilidad IBM Tivoli Monitoring Service Index proporciona enlaces a la interfaz de servicio del agente para cada agente de supervisión instalado localmente. Después de iniciar una sesión en el sistema operativo, puede seleccionar uno de estos informes: información del agente, situación, historial o consultas.

Además, puede realizar una solicitud de interfaz de servicio directamente, por ejemplo para iniciar una descarga de configuración inmediata o para reciclar una situación.

Consulte el apartado "Interfaz de servicio del agente" en la página 416.

configuración centralizada
Utilice una configuración centralizada para mantener los archivos XML de configuración del agente de supervisión en una ubicación central que se toman del *servidor de configuración central* a intervalos (el valor predeterminado es cada 60 minutos) o bien bajo demanda. Cada uno de los agentes que participan en una configuración centralizada tiene su propio archivo XML de *lista de carga de configuración* que indica dónde conectarse para obtener las últimas actualizaciones en los archivos de configuración especificados.

Un sistema al que se conecta uno o varios agentes de supervisión para configurar actualizaciones se denomina un *servidor de configuración central*. Un sistema con uno o varios agentes de supervisión que descargan actualizaciones de configuración se denomina un cliente de configuración central.

Consulte Configuración centralizada.

Variables de entorno para comportamiento autónomo

Utilice el archivo de entorno que se proporciona con los servicios de la infraestructura del agente para controlar el comportamiento autónomo del Tivoli System Monitor Agent o del Tivoli Enterprise Monitoring Agent cuando están desconectados del Tivoli Enterprise Monitoring Server.

El manual *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm) proporciona instrucciones para instalar y configurar el Tivoli System Monitor Agent. También tiene una referencia a las variables de entorno del agente común en un apéndice.

Archivo de entorno del Tivoli Enterprise Monitoring Agent

Las variables de entorno se editan en el archivo de entorno de Tivoli Enterprise Monitoring Agent o se añaden al mismo, donde *cp* es el código del producto de dos caracteres:

Windows *dir_instalación*\TMAITM6\k*cp*cma.ini. Vuelva a configurar el agente para implementar los cambios.

Linux UNIX *dir_instalación*/config/*pc*.ini. En los agentes de supervisión del sistema, este archivo es *pc*.environment. Recicle el agente para implementar los cambios.

IBM i /qautotmp/kmsparm.kbbenv

z/OS nombre miembro KPCENV en &hilev.&rte.RKANPARU

Métodos recomendados para z/OS

Utilice el panel "Especificar parámetros no estándares" en la Herramienta de configuración (también denominada Herramienta de ayuda a la instalación y configuración o ICAT) para realizar cambios en miembros. Cualquier cambio que realice con este editor se conserva automáticamente cuando se actualiza el entorno de tiempo de ejecución, lo que significa que los valores no se sobregraban la próxima vez que se actualiza el entorno de tiempo de ejecución. Consulte el tema "Adición, cambio o supresión de un parámetro en un miembro de tiempo de ejecución" en *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Planning and Configuration* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm).

Cualquier parámetro de alteración temporal definido en el miembro KDSENV del conjunto de datos *&hilev.&rte.*RKANPARU se utiliza para todos los agentes que se ejecutan dentro del espacio de direcciones. Esto funciona bien para IRA_EIF_DEST_CONFIG, porque probablemente todos los agentes compartirán el mismo destino de suceso EIF. Los otros parámetros de alteración temporal también se pueden utilizar, pero es posible que los miembros del conjunto de datos identificado tengan que combinar definiciones para varios agentes, lo que no se recomienda. La práctica recomendada consiste en utilizar el convenio de denominación predeterminada para miembros del conjunto de datos de la configuración local cuando se ejecutan varios agentes en el mismo espacio de direcciones.

Para obtener información sobre la utilización de PARMGEN, consulte "Casos de ejemplo de mantenimiento del entorno de ejecución" en la publicación *OMEGAMON XE and Tivoli Management Services on z/OS PARMGEN Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/parmgenref/parmgenref.htm).

Control de autonomía en agentes de Tivoli Enterprise Monitoring

Los siguientes parámetros de configuración inician y controlan el comportamiento autónomo de los agentes de Tivoli Enterprise Monitoring.

IRA_AUTONOMOUS_LIMIT=50

Este parámetro determina el número de sucesos que se pueden almacenar en el agente cuando está en modalidad autónoma o asigna la cantidad de espacio de disco que puede ocupar el agente. Cuando se alcanza el límite de sucesos o el valor máximo de espacio de disco, no se recopilan más sucesos. El valor predeterminado es de **50** sucesos o **2MB**. Especifique el número total de sucesos o el límite de espacio de disco, donde *n* es el valor numérico:

n = número máximo de sucesos (muestreados y puros) que se pueden guardar. Para calcular el espacio de cada sucesos, agregue 1200 al tamaño promedio de fila de aplicación.

nKB = n veces 1024 bytes.

nMB = n veces 1,024,000 bytes.

nGB = n veces 1,024,000,000 bytes

IRA_AUTONOMOUS_MODE=Y

Este parámetro controla la operación autónoma de los agentes de supervisión de empresa. De forma predeterminada, la autonomía está

habilitada. Para inhabilitarla, lo que hace que el agente recupere la dependencia que tenía del servidor de supervisión antes de V6.2.1, establezca este parámetro en **N**.

IRA_EIF_DEST_CONFIG=*nombrearchivo*
Utilice este parámetro en el archivo de entorno del agente para especificar la ubicación del archivo XML de configuración de destino de EIF. Puede especificar la vía de acceso completa o la vía de acceso relativa al directorio de configuración local.

IRA_EIF_MSG_LOCALE=en_US
Este parámetro de los archivos de entorno del agente se establece en inglés americano de forma predeterminada. Para los agentes que dan soporte a texto de mensajes globalizado para la ranura de mensajes en el suceso generado utilizando un archivo de correlación predefinido y paquetes de recursos de idioma, se puede especificar el entorno local de idioma predeterminado.

IRA_EVENT_EXPORT_CHECKUSAGE_INTERVAL=180
Especifica el intervalo preferido en segundos para comprobar si se ha alcanzado IRA_AUTONOMOUS_LIMIT. El valor predeterminado es de **180** segundos (3 minutos). El intervalo mínimo que se puede especificar es de **60** segundos.

IRA_EVENT_EXPORT_EIF=Y
Este parámetro del archivo de entorno del agente se establece para habilitar el recurso de exportación de sucesos de EIF. Cambie el valor por **N** para inhabilitar el recurso.

IRA_EVENT_EXPORT_SIT_STATS=Y
Puede obtener un informe de las estadísticas de operación de la situación mediante la Interfaz de servicio del agente. Este parámetro habilita (Y) o inhabilita (N) la recopilación de datos de estadísticas de operaciones de situaciones:

Nombre de la situación

Tipo de situación: de empresa o privada

Nombre de aplicación

Nombre de tabla

Intervalo de muestreo

Tamaño de datos de fila

Indicación de hora de la primera vez que se ha iniciado la situación

Indicación de hora de la primera vez que la situación ha generado un suceso (filtro pasado)

Indicación de hora de la última vez que se ha iniciado la situación

Indicación de hora de la última vez que se ha detenido la situación

Indicación de hora de la última vez que la situación se ha evaluado en TRUE

Indicación de hora de la última vez que la situación se ha evaluado en FALSE

Número de veces que la situación se ha reciclado

Número de veces que la situación está en operación autónoma

Valor predeterminado: **Y**.

IRA_EVENT_EXPORT_SIT_STATS_DETAIL=N

Cuando se establece en Y, este parámetro habilita la recopilación de las siguientes métricas de sucesos del agente:

- Recuento de muestreo verdadero
- Recuento de muestreo falso
- Índice de muestreo verdadero
- Índice de muestreo falso
- Número de filas de datos contadas en 24 horas
- Número de muestreos verdaderos contados en 24 horas
- Número de muestreos falsos contados en 24 horas

El agente mantiene estas métricas durante ocho días en disco, con un desplazamiento diario durante la medianoche. Valor predeterminado: **N**.

IRA_EVENT_EXPORT_SNMP_TRAP=Y/N

IRA_EVENT_EXPORT_SNMP_TRAP=N inhabilita las alertas SNMP del agente, incluso si está presente el archivo *cp*_trapcnfg.xml. Valor predeterminado: **Y**.

IRA_EVENT_EXPORT_SNMP_TRAP_CONFIG

De forma predeterminada, el agente mira si existe el archivo *dir_instalación*/localconfig/*cp*/*cp*_trapcnfg.xml. Si el archivo de configuración se encuentra en otro sitio o tiene otro nombre, utilice este parámetro para especificar la vía de acceso y el nombre del archivo. Puede especificar la vía de acceso completa o una vía de acceso relativa al directorio de configuración local.

z/OS El agente z/OS busca el nombre de miembro *PC*TRAP predeterminado en el conjunto de datos *&hilev.&rte.*RKANDATV del entorno. Si el miembro de la condición de excepción de SNMP tiene otro nombre, especifique el nombre del miembro con esta variable. Si el miembro está en otro conjunto de datos, especifique el nombre del conjunto de datos y el nombre del miembro, en el formato: *nombre_miembro.nombre_conjuntodatos*.

Por ejemplo, si el nombre del archivo de configuración es MYSNMP y está en RKANDATV, especifique `IRA_EVENT_EXPORT_SNMP_TRAP_CONFIG=MYSNMP`. Si el archivo de configuración está en otro conjunto de datos, por ejemplo, TIVOLI.ITM622.TVT1006.MYFILES(MYSNMP), especifique `IRA_EVENT_EXPORT_SNMP_TRAP_CONFIG=MYSNMP.MYFILES`.

IRA_LOCALCONFIG_DIR

La vía de acceso al directorio de configuración local predeterminada que contiene archivos de configuración personalizados localmente como situaciones privadas, configuración de sucesos de EIF y archivos de configuración de condiciones de excepción de SNMP es el subdirectorio `localconfig` del directorio especificado por la variable de entorno *CANDLE_HOME*; RKANDATV *DD* nombre en sistemas z/OS. Utilice este parámetro para cambiar la vía de acceso.

KHD_REGWITHGLB

Normalmente, el Warehouse Proxy agent se registra con el servidor de supervisión concentrador. Si desea que el proxy de almacén no tenga dependencias del servidor de supervisión, añada KHD_REGWITHGLB=N al archivo de entorno del proxy de almacén (Windows `khdenv`; Linux UNIX `hd.ini`) para que no se registre con el servidor de supervisión.

KHD_WAREHOUSE_LOCATION
Si el Warehouse Proxy agent no se registra con el servidor de supervisión concentrador, debe añadir este parámetro al archivo de entorno en cada agente de supervisión de empresa que tenga autonomía completa. Especifique el nombre calificado al completo de cada proxy de almacén que pueda transferir datos históricos del agente a Tivoli Data Warehouse, separados por un signo de punto y coma (;). La sintaxis es `KHD_WAREHOUSE_LOCATION=`*`protocolo familia`*`:`*`dirección red`*`[`*`número puerto`*`]`, por ejemplo, `KHD_WAREHOUSE_LOCATION=ip.pipe:DEPT-XP[63358];ip:MY-XP[63358];ip.pipe:#9.44.255.253[65538]`.

KSY_AUTONOMOUS
Normalmente, los valores de resumen y poda para grupos de atributos se configuran a través de Tivoli Enterprise Portal o de la interfaz de línea de mandatos **tacmd histconfiguregroups** y se guardan en una tabla WAREHOUSESUMPRUNE en Tivoli Data Warehouse.

Si desea que el agente de resumen y poda no tenga dependencias del Tivoli Enterprise Portal Server, añada KSY_AUTONOMOUS=Y al archivo de entorno del agente de resumen y poda y añada la ubicación de los archivos de descripción del agente mediante la variable KSY_AUTONOMOUS_ODI_DIR.

El agente de resumen y poda necesita los archivos de soporte de aplicaciones del agente que se instalan con el servidor de portal. Si ha establecido KSY_AUTONOMOUS=Y y el agente de resumen y poda no está instalado en el mismo sistema que el servidor de portal, debe copiar los archivos de soporte de aplicaciones necesarios en el mismo sistema. Con la excepción de **dockcj**, que no se utiliza, los archivos de soporte son los archivos **dock*pc*** (donde *pc* es el código de producto de dos caracteres) del directorio servidor de portal: Windows *dir_instalación*`\cnps`; Linux UNIX *dir_instalación*`/`*`arch`*`/cq/data`. Consulte "Ejecución autónoma de agentes de almacén" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

KSY_AUTONOMOUS_ODI_DIR
Aunque el Summarization and Pruning agent se puede configurar para que funcione de forma autónoma desde el servidor de portal, debe tener el servidor de portal instalado y soporte de aplicaciones para todos los agentes configurados para recopilar datos históricos porque el proceso de resumen y poda necesita los archivos de soporte de aplicaciones cuando se ejecuta de forma autónoma. Utilice este parámetro para especificar la vía de acceso a los archivos de soporte de aplicaciones.

Si el agente está configurado para que se ejecute de forma autónoma, los valores de resumen y poda se deben especificar directamente en la tabla WAREHOUSESUMPRUNE de la base de datos de almacén mediante el mandato insert de SQL.

Situaciones privadas

IRA_PRIVATE_SITUATION_CONFIG
Especifica el nombre completo del archivo de configuración de situaciones privadas. Durante la inicialización del agente, se comprueba si existe el archivo de configuración de situaciones privadas: *`dir_instalación`*`/localconfig/`*`cp`*`/`*`cp`*`_situations.xml` donde *cp* es el código de producto de dos caracteres.

z/OS Una vía de acceso completa al archivo de configuración de la situación en z/OS, como 'TIVOLI.ITM622.TVT1006.RKANDATV(MYPSSIT)' donde DDNAME RKANDATV es TIVOLI.ITM622.TVT1006.RKANDATV: `IRA_PRIVATE_SITUATION_CONFIG=MYPSSIT`.
Para un archivo de configuración de situación que no sea miembro de PDS en DDNAME RKANDATV, especifique 'TIVOLI.ITM622.TVT1006.MYFILES(MYPSSIT)' donde DDNAME MYFILES es TIVOLI.ITM622.TVT1006.MYFILES: `IRA_PRIVATE_SITUATION_CONFIG=MYPSSIT.MYFILES`.

Consulte “Situaciones privadas” en la página 347 para obtener más información sobre situaciones privadas.

Historial privado

CTIRA_HIST_DIR
Especifica el directorio en el que se almacenarán los archivos de datos históricos a corto plazo del agente. No se aplica a archivos de datos históricos a corto plazo del servidor de supervisión. Es la ubicación predeterminada de los archivos binarios de historial de empresa o de historial privado.

Windows *dir_instalación*\TMAITM6\logs

Linux UNIX *dir_instalación/arch/pc*/hist

Consulte “Historial privado” en la página 370 para obtener más información sobre la recopilación de datos históricos privados.

Alteraciones temporales de expresiones de situaciones

CTIRA_THRESHOLDS
Especifica el nombre completo del archivo de alteraciones temporales de umbrales (dinámicos) adaptado basado en XML. De forma predeterminada, el agente mira si existe un archivo *dir_instalación*/localconfig/*cp*/*cp*_thresholds.xml (donde *cp* es el código de producto del agente). Puede especificar la vía de acceso completa o la vía de acceso relativa al directorio de configuración local.

z/OS El nombre de archivo predeterminado es ***PC*THRES**. Para especificar la vía de acceso completa, el PDS debe aparecer listado al final (o bien omitido, adoptando como valor predeterminado RKANDATV).

IRA_ADAPTIVE_THRESHOLD_MODE
Especifica la modalidad de operación de umbral (dinámico) adaptado, que puede ser CENTRAL o LOCAL. La modalidad predeterminada es CENTRAL.

En modalidad CENTRAL, las alteraciones temporales de umbrales de situación se crean a través de Tivoli Enterprise Portal o del mandato **tacmd setOverride** de CLI y se distribuyen al agente de destino a través del Tivoli Enterprise Monitoring Server.

Puede establecer un agente en modalidad LOCAL para que el agente utilice XML de configuración de umbral definido localmente en lugar de la distribución de alteración temporal CENTRAL. En la modalidad LOCAL, la distribución central para el agente queda inhibida (su afinidad no se registra) y las alteraciones temporales de umbrales se crean y gestionan

localmente. Utilice la modalidad LOCAL con precaución porque hace que los umbrales del Tivoli Enterprise Monitoring Server y los umbrales del agente se desincronicen.

Si conmuta el agente de la modalidad LOCAL a la modalidad CENTRAL, la especificación de alteración temporal CENTRAL prevalece sobre las definiciones locales y se sincroniza con el repositorio de alteraciones temporales CENTRAL situado en el servidor de supervisión.

Consulte “Especificación XML de alteración temporal de situación de empresa” en la página 373 para obtener más información sobre alteraciones temporales de situaciones locales.

Interfaz de servicio del agente

Estos parámetros de configuración del agente afectan la operación de la interfaz de servicio:

IRA_SERVICE_INTERFACE_NAME
Especifique el nombre de interfaz de servicio de agente preferido para definir un nombre reconocido más funcional para sustituir el nombre predeterminado generado por el agente en el formato de k*cp*agente, donde *cp* es el código de producto de dos caracteres, como por ejemplo kntagent o kmqagent; o *cp*agente, como uagent02 para identificar una segunda instancia de Universal Agent instalada en un sistema.

Valor predeterminado:
Windows system.*nombrehost_cp*
Linux UNIX *nombrehost_cp*

IRA_SERVICE_INTERFACE_DEFAULT_PAGE
Indica al agente que abra la página HTML específica del producto con nombre, en lugar de la página **navigator.htm** predeterminada, después de iniciar la sesión en la interfaz de servicio del agente. De forma predeterminada, el agente busca el archivo específico del producto en *dir_instalación*/localconfig en sistemas distribuidos y el conjunto de datos RKANDATV en sistemas z/OS. Sin embargo, si se ha establecido la variable de entorno IRA_SERVICE_INTERFACE_DIR, el agente busca en el directorio especificado por la variable de entorno.

Si establece IRA_SERVICE_INTERFACE_DEFAULT_PAGE (pero no IRA_SERVICE_INTERFACE_DIR), debe colocar las páginas HTML específicas del producto en el directorio *dir_instalación*/localconfig/html en sistemas distribuidos. Por lo tanto, si crea **myPage.htm** y lo coloca en *dir_instalación*/localconfig/html, debe establecer IRA_SERVICE_INTERFACE_DEFAULT_PAGE=/html/myPage.htm.

IRA_SERVICE_INTERFACE_DIR
Define las especificaciones de vía de acceso del directorio HTML de la interfaz de servicio del agente. Junto con el parámetro IRA_SERVICE_INTERFACE_DEFAULT_PAGE, el agente construye la vía de acceso del archivo a un objeto GET de HTTP específico solicitado. El valor predeterminado es *dir_instalación*/localconfig en sistemas distribuidos.

Ejemplo: Si IRA_SERVICE_INTERFACE_DIR="\mypath\private" y especifica http://localhost:1920///kuxagent/kuxagent/html/myPage.htm en el navegador, se recupera myPage.htm de \mypath\private\html\ en lugar de *dir_ITM*\localconfig\html\.

z/OS No hay ninguna especificación de vía de acceso a directorio, sino un conjunto de datos representado por el nombre JCL DD (Definición de Datos). Por lo tanto, no se utiliza IRA_SERVICE_INTERFACE_DIR pero la especificación IRA_SERVICE_INTERFACE_HTML está en vigor. El valor predeterminado es el nombre RKANDATV DD.

Consulte también las variables de entorno para la configuración centralizada que llevan el prefijo IRA_SERVICE_INTERFACE.

Diagnósticos y resolución de problemas

Estos parámetros se pueden definir en el archivo de entorno del agente para la resolución de problemas. Toda la información de diagnóstico va al registro de rastreo RAS (Reliability, Availability, and Serviceability) del agente.

IRA_DEBUG_AUTONOMOUS=N
Cuando se establece en **Y**, este parámetro habilita el registro de rastreo de todas las operaciones autónomas del agente. El valor predeterminado es **N**.

IRA_DEBUG_EIF=N
Si está establecido en **Y**, este parámetro habilita el registro de rastreo de las operaciones del emisor de EIF. El valor predeterminado es **N**.

IRA_DEBUG_EVENTEXPORT=N
Cuando se establece en **Y**, este parámetro habilita el registro de rastreo de las actividades de exportación de sucesos como, por ejemplo, las condiciones de excepción SNMP. El valor predeterminado es **N**.

IRA_DUMP_DATA=N
Cuando se establece en **Y**, este parámetro habilita el registro de rastreo de todos los datos RPC (llamada de procedimiento remoto). El valor predeterminado es **N**.

IRA_DEBUG_PRIVATE_SITUATION=N
Si tiene el valor **Y**, toda la información de rastreo relacionada con problemas de situaciones privadas se graba en el registro de rastreo RAS. El valor predeterminado es **N**.

IRA_DEBUG_SERVICEAPI=N
Cuando se establece en **Y**, este parámetro habilita el registro rastreo de todos los procesos de la interfaz de servicio del agente. El valor predeterminado es **N**.

KEF_DEBUG=N
Si está establecido en **Y**, este parámetro habilita el registro de rastreo de las operaciones de la biblioteca de EIF. El valor predeterminado es **N**.

Limitaciones de las situaciones

Los tipos de funciones de fórmula que se pueden utilizar en una situación privada son limitados. Asimismo, los tipos de funciones de fórmula de una situación de empresa que puede procesar un agente cuando se desconecta de su Tivoli Enterprise Monitoring Server son limitados.

Tabla 29. Disponibilidad de funciones de fórmula de situación cuando un agente de empresa está conectado o desconectado y cuando la situación es privada.

	Suceso enviado desde el servidor de supervisión	**Suceso enviado desde el agente de supervisión de empresa**		
Función de fórmula	**Soportado en situaciones de empresa**	**Situación de empresa Agente conectado al servidor de supervisión Se evalúa en el servidor de supervisión**	**Situación de empresa Agente desconectado del servidor de supervisión Se evalúa en el agente**	**Soportado en situaciones privadas Se evalúa en el agente[1]**
Funciones de celda				
CHANGE	disponible	disponible	disponible	no disponible
DATE	disponible	disponible	disponible	no disponible
MISSING	disponible	disponible	disponible	disponible
PCTCHANGE	disponible	disponible	disponible	no disponible
SCAN	disponible	disponible	disponible	no disponible
STR	disponible	disponible	disponible	no disponible
TIME	disponible	no disponible	no disponible	no disponible
VALUE	disponible	disponible	disponible	disponible
IN	disponible	disponible	disponible	no disponible
Las **funciones de grupo** se pueden aplicar a grupos de atributos de varias filas y a los configurados para la recopilación de datos históricos. Las vistas de tabla y de diagrama requieren establecer un rango de tiempo para que se muestre un intervalo de muestreos de datos.				
AVG	disponible	no disponible	no disponible	no disponible
COUNT	disponible	no disponible	no disponible	no disponible
MAX	disponible	no disponible	no disponible	no disponible
MIN	disponible	no disponible	no disponible	no disponible
SUM	disponible	no disponible	no disponible	no disponible
Características de la situación				
Incorporada, incluidas situaciones correlacionadas	disponible	no disponible	no disponible	no disponible
Varios grupos de atributos	disponible	no disponible	no disponible	no disponible
Persistencia habilitada	disponible	disponible[2]	disponible[2]	no disponible
Mostrar elemento seleccionado	disponible	disponible	no disponible[3]	no disponible
Utiliza el proceso Duper	disponible	disponible	no disponible[4]	no disponible

Tabla 29. Disponibilidad de funciones de fórmula de situación cuando un agente de empresa está conectado o desconectado y cuando la situación es privada. (continuación)

	Suceso enviado desde el servidor de supervisión	**Suceso enviado desde el agente de supervisión de empresa**		
Función de fórmula	**Soportado en situaciones de empresa**	**Situación de empresa Agente conectado al servidor de supervisión Se evalúa en el servidor de supervisión**	**Situación de empresa Agente desconectado del servidor de supervisión Se evalúa en el agente**	**Soportado en situaciones privadas Se evalúa en el agente[1]**
Distribución al grupo de sistemas gestionados	disponible	disponible	disponible	no disponible

[1] Esta columna también se aplica a los agentes supervisores del sistema.

[2] La persistencia de la situación no se evalúa en el agente. Se pueden emitir condiciones de excepción en dos modalidades: RC (en dos modalidades: RC (Rising Continuous) en la que se emite una condición de excepción cada vez que la situación es verdadera; HY (Hysteresis) en la que se emite una condición de excepción cada vez que la situación es verdadera y se emite una condición de excepción de borrado cuando la situación ya no es verdadera. Asimismo, se puede habilitar la persistencia en el destino de la condición de excepción implementando una regla de persistencia.

[3] Las situaciones que incluyen un elemento de visualización (disponible para varios grupos de atributos de fila) están limitadas a enviar una alerta SNMP para la primera fila que se evalúa como true; no se puede enviar ninguna alerta para las siguientes filas que se evalúan como true.

[4] Se emiten condiciones de excepción pero las situaciones no se evalúan cuando el agente está desconectado del servidor de supervisión.

Restricción: Las situaciones privadas con la función MISSING distribuida a subnodos deben tener una lista de subnodos en la etiqueta DISTRIBUTION. Las situaciones privadas con la función MISSING distribuida a agentes no lo necesitan.

alertas SNMP procedentes de agentes de supervisión de empresa con subnodos

Los agentes de supervisión que utilizan subnodos, como agentes de subnodo creados con Agent Builder, Monitoring for Energy Management y supervisores sin agentes, pueden emitir una alerta SNMP solo para un subnodo por instancia del agente en el que la situación se evalúa como true, no para ningún otro subnodo en el que la misma situación se evalúe como true.

Para cada instancia del agente, se recopilan muestras de datos en una tabla de grupos de atributos. Estas medidas se filtran por subnodo cuando se muestran en Tivoli Enterprise Portal, pero las situaciones que se ejecutan en varios subnodos para una instancia de agente se evalúan realmente en una sola tabla. Si una situación se convierte en verdadera en un subnodo, se emite una alerta SNMP definida para dicha situación, pero no se emite ninguna alerta SNMP para dicha situación en otros subnodos porque no se procesan más filas en la tabla.

A continuación se muestran algunas alternativas a emitir alertas SNMP para agentes con subnodos:

- Reenviar sucesos del servidor de supervisión a un receptor EIF.
- Si configura el agente, definir solo un subnodo por instancia de agente.
- Definir una ubicación distinta para cada subnodo y distribuir dicha situación a un solo subnodo. En el siguiente ejemplo,

  la situación **KAB_Log_Message** se distribuye a los subnodos **ALL LOG** del **agente AB**

  la situación **KAB_Log1only_Message** solo se distribuye al subnodo **AB:uxlog1:LOG**

  la situación **KAB_Log2only_Message** solo se distribuye al subnodo **AB:uxlog2:LOG**

  La instancia 1 del agente de supervisión de registro AB supervisa tres registros (hay un subnodo por cada archivo de registro): **uxlog1**, **uxlog2** y **uxlog3**:

  Si aparece un mensaje en el archivo supervisado por el subnodo **uxlog1**, estas situaciones se convierten en verdaderas: **KAB_Log_Message** y **KAB_Log1only_Message**.

  Si aparece un mensaje en el archivo supervisado por el nodo **uxlog3**, esta situación se convierte en verdadera: **KAB_Log_Message**

  El archivo de configuración de situaciones privadas para el agente:

```
<PRIVATECONFIGURATION>
  <PRIVATESIT>
   <SITUATION>KAB_Log_Message</SITUATION>
    <CRITERIA><![CDATA[ *IF *VALUE KAB_LOGFILE.Message *NE "" ]]>
   </CRITERIA>
   <INTERVAL>000000</INTERVAL>
   <DISTRIBUTION>AB:uxlog:LOG</DISTRIBUTION>
  </PRIVATESIT>
  <PRIVATESIT>
   <SITUATION>KAB_Log1only_Message</SITUATION>
    <CRITERIA><![CDATA[ *IF *VALUE KAB_LOGFILE.Message *NE "" ]]>
   </CRITERIA>
   <INTERVAL>000000</INTERVAL>
   <DISTRIBUTION>AB:uxlog1:LOG</DISTRIBUTION>
  </PRIVATESIT>
  <PRIVATESIT>
   <SITUATION>KAB_Log2only_Message</SITUATION>
    <CRITERIA><![CDATA[ *IF *VALUE KAB_LOGFILE.Message *NE "" ]]>
   </CRITERIA>
   <INTERVAL>000000</INTERVAL>
   <DISTRIBUTION>AB:uxlog2:LOG</DISTRIBUTION>
 </PRIVATESIT>
</PRIVATECONFIGURATION>
```

Archivos XML codificados en UTF-8

El formato de codificación Unicode Transformation Format, de 8 bits está diseñado para facilitar el uso de sistemas basados en ASCII existentes y permite utilizar todos los caracteres del estándar Unicode. Cuando se compone un archivo XML de configuración local en un lenguaje que va más allá del juego de caracteres ASCII, como por ejemplo letras con diacríticos y conjuntos de caracteres de doble byte, utilice un editor que permita guardar el archivo en codificación UTF-8.

Windows Linux UNIX

Los caracteres ASCII utilizan un byte y comprenden los primeros 128 caracteres. Puede escribir el archivo XML con cualquier editor de texto.

Para caracteres no ASCII, como por ejemplo caracteres con diacríticos y caracteres Kanji, se necesita un editor que pueda guardar el archivo como UTF-8.

z/OS

Puesto que UTF-8 no se muestra ni se edita fácilmente con z/OS, el archivo XML se puede codificar en UTF-8 o mediante la página de códigos del agente. La página de códigos se establece en el archivo de entorno del agente con la variable de entorno LANG, como por ejemplo LANG=en_US.IBM-1047. El archivo de entorno se encuentra en *&hilev.&rte.*RKANPARU, con el nombre de miembro KC*P*ENV (donde *CP* es el código de producto de dos caracteres). La variable LANG debe coincidir con el emulador de terminar si utiliza el emulador para editar el archivo. La página de códigos predeterminada para FTP es IBM-1047 si edita el archivo en Windows, Linux o UNIX y luego carga el archivo como texto ASCII en el host.

Consulte "Configuración de los servidores de supervisión concentradores y remotos en z/OS" en el apartado *Configuración de Tivoli Enterprise Monitoring Server en z/OS*.

IBM i

(La configuración de destinos de sucesos de EIF no recibe soporte ni tampoco los informes SNMPv3.) Puesto que UTF-8 no se muestra ni se edita fácilmente con IBM i, el archivo XML se puede codificar en UTF-8 o mediante la página de códigos del agente. La página de códigos se establece en el archivo de entorno del agente con la variable de entorno LANG, como por ejemplo LANG=/QSYS.LIB/EN_US.LOCALE. Es mejor establecer la variable de entorno LANG antes de iniciar **qsh**, el intérprete de Qshell. Algunos programas de utilidad no funcionan correctamente si el entorno local no es válido para el ID de juego de caracteres codificado y el ID de lenguaje del trabajo.

Configuración de los Servicios de gestión de agentes en agentes de Tivoli System Monitor

Configure los Servicios de gestión de agentes para los agentes de Tivoli System Monitor si desea utilizar los servicios para supervisar y controlar la disponibilidad de los agentes.

Antes de empezar

Los Servicios de gestión de agentes está configurado de forma diferente en un entorno de agente supervisor del sistema:

- De forma predeterminada, los Servicios de gestión de agentes gestionan los agentes del supervisor del sistema. Puede suspender la gestión mediante el mandato `disarmWatchdog`, que inhabilita la vigilancia de los Servicios de gestión de agentes para el agente del supervisor del sistema y para cualquier agente creado con Tivoli Monitoring Agent Builder en el mismo sistema. La gestión se reanuda mediante los Servicios de gestión de agentes utilizando el mandato `rearmWatchdog`, que habilita la vigilancia para los agentes autónomos gestionados por los Servicios de gestión de agentes. Estos mandatos se describen en la guía del usuario del agente.

- Los agentes de Agent Builder instalados en un entorno de agente gestor del sistema no los gestiona el proceso de vigilancia de los Servicios de gestión de agentes de forma predeterminada. Puede cambiar si el agente lo gestiona o no el proceso de vigilancia.

Acerca de esta tarea

Después de instalar un agente de Agent Builder en un entorno de agente del supervisor del sistema, siga estos pasos para iniciar o detener la gestión de los Servicios de gestión de agentes.

Procedimiento

1. Mientras se ejecuta el proceso de vigilancia, traslade el archivo CAP (Common Agent Package) con el nombre k*cp*_default.xml (donde *cp* es el código de producto de dos caracteres) desde el directorio CAP a una ubicación temporal. El archivo está situado en el directorio KCA_CAP_DIR.
   Windows *dir_instalación*\TMAITM6[_x64]\CAP\
   Linux UNIX *dir_instalación*/config/CAP
   Si se elimina el archivo del directorio CAP hace que el agente resulte invisible para los Servicios de gestión de agentes.
2. Modifique todas las instancias de <managerType> en el archivo CAP para habilitar o inhabilitar la gestión:
   - <managerType>**ProxyAgentServices**</managerType> para habilitar la gestión.
   - <managerType>**NotManaged**</managerType> para inhabilitar la gestión.

   Una práctica recomendada consiste en cambiar el nombre del archivo modificado por **k*cp*.xml** (donde *cp* es el código del producto de dos caracteres). Todos los archivos CAP situados en KCA_CAP_DIR los procesan los Servicios de gestión de agentes. Si dos o más archivos CAP comparten el mismo valor de "ID de subagente", se procesan en un orden clasificado. Por ejemplo, kca.xml se utiliza antes que kca_default.xml. Asimismo, si cambia el nombre del archivo CAP por *cp*.xml, se asegura de que los cambios no se sobrescriben durante una actualización futura.
3. Guarde el archivo actualizado.
4. Mientras se ejecuta el proceso de vigilancia (kcawd), mueva o copie otra vez el archivo CAP actualizado en KCA_CAP_DIR.

Resultados

Los valores de los Servicios de gestión de agentes se procesan después de que el archivo CAP se coloca en KCA_CAP_DIR.

Situaciones privadas

Defina situaciones privadas para los criterios de supervisión y los sucesos resultantes relevantes para el entorno del agente local o un receptor de sucesos y no relevantes para el entorno de Tivoli Enterprise Monitoring. Las situaciones privadas pueden definirse para agentes de Tivoli Enterprise Monitoring y agentes de System Monitor.

Operación de situaciones privadas

Las situaciones privadas se crean en un archivo con formato XML que no interactúa con el Tivoli Enterprise Monitoring Server. Para utilizar de forma eficaz las situaciones privadas, debe comprender en qué se difieren de las situaciones empresariales.

Infraestructura del agente de Tivoli Management Services

La infraestructura de agentes de la infraestructura de Tivoli Management Services incorpora la capacidad de crear situaciones que se ejecuten localmente y desencadenan sucesos en el sistema en el que ha instalado el Tivoli Enterprise Monitoring Agent o Tivoli System Monitor Agent.

Situaciones de empresa y situaciones privadas

Las *situaciones de empresa* se crean con el Editor de situaciones de Tivoli Enterprise Portal o con el mandato **tacmd createSit** de CLI. Las situaciones de empresa envían sucesos al servidor de supervisión y pueden reenviar sucesos a un receptor del Recurso de integración de sucesos, como por ejemplo el IBM Tivoli Enterprise Console o la Netcool/OMNIbus Probe for Tivoli EIF cuando el servidor de supervisión concentrador se ha configurado para reenviar sucesos. Los sucesos de situaciones de empresa también se pueden enviar como alertas SNMP a un receptor como la prueba Netcool/OMNIbus SNMP

Las *situaciones privadas* se crean en un archivo XML de configuración de situaciones privadas local para el agente. Las definiciones de situaciones aptas que se han exportado de la empresa supervisada también se pueden añadir al archivo para crear situaciones. Los sucesos generados por situaciones privadas pueden permanecer como sucesos locales en la estación de trabajo o se pueden enviar como alertas SNMP a un receptor como la prueba Netcool/OMNIbus SNMP. El archivo de configuración de situaciones privadas reside en el directorio `localconfig/cp` del agente, un archivo por agente, y contiene todas las definiciones de situaciones privadas correspondientes al agente.

Creación de situaciones privadas

Este ejemplo de un archivo XML de configuración de situación privada para el agente de SO Windows tiene dos situaciones definidas. Puede crear situaciones en el archivo especificándolas manualmente.

También puede crear situaciones en este archivo exportando situaciones de empresa existentes del servidor de supervisión, utilizando el mandato de CLI **tacmd bulkExportSit**, y luego copiando las situaciones exportadas aptas para que se utilicen como situaciones privadas del archivo XML al archivo de configuración de situaciones privadas del agente. La última situación (llamada Disk_Queue) del ejemplo procede de un archivo XML de situación exportado.

```
<PRIVATECONFIGURATION>
  <PRIVATESIT>
   <SITUATION>NT_Missing_Scheduler_pr</SITUATION>
    <CRITERIA>
     <![CDATA[ *MISSING NT_Process.Process_Name *EQ ("schedule")]]>
    </CRITERIA>
    <INTERVAL>001000</INTERVAL>
  </PRIVATESIT>
  <PRIVATESIT>
   <SITUATION>NT_Paging_File_Critical_pr</SITUATION>
    <CRITERIA>
```

```
    <![CDATA[  *VALUE NT_Paging_File.%_Usage *GE 80 ]]>
   </CRITERIA>
   <INTERVAL>001500</INTERVAL>
  </PRIVATESIT>
  <PRIVATESIT>
   <SITUATION>Disk_Queue</SITUATION>
    <PDT><![CDATA[ *IF *VALUE NT_Physical_Disk.Avg_Disk_Queue_Length
    *GE 0.004 ]]></PDT>
    <REEV_TIME>003000</REEV_TIME>
  </PRIVATESIT>
</PRIVATECONFIGURATION>
```

El elemento CRITERIA contiene la fórmula:

- Nombre de función ***VALUE** o ***MISSING**. **Valor de expresión** y **Comprobar si faltan elementos** son las únicas funciones de fórmula que se pueden utilizar en situaciones privadas.
- **attribute_group.attribute_name** tal como están escritos en estos lugares:
  - Elemento **name** de archivo .atr del agente, situado en el directorio *<dir_instalación>*/TMAITM6/ATTRLIB/*cp*
  - Elemento **<PDT>** de la salida del archivo *<situation_name>*.xml generado por el mandato de CLI `tacmd bulkExportSit`
  - Elemento **<PREDICATE>** del informe Resumen de la situación que se genera mediante la Interfaz de servicio del agente
  - Columna **Visualización** de la parte de definiciones de atributos del informe Consultas que se genera mediante la Interfaz de servicio del agente
- Operador booleano ***EQ**, ***LT**, ***GT**, ***NE**, ***LE** o ***GE**.
- **Umbral** de la función *VALUE o lista separada por comas de la función *MISSING.
- Se pueden conectar varias expresiones mediante lógica booleana AND u OR, pero no ambas, y solo se puede utilizar un grupo de atributos en la fórmula. Se da soporte a un máximo de nueve expresiones conectadas por AND; y se da soporte a un máximo de diez expresiones conectadas por OR.
- La codificación XML no es sensible a mayúsculas y minúsculas con esta excepción: los valores de atributos de texto deben coincidir con la muestra de datos. Por ejemplo, falta el proceso `notepad` no es válido si se escribe `NOTEPAD`.

Activación

Cuando se inicializa el agente, un analizador de XML examina y valida las definiciones de situaciones privadas. Todos los mensajes de error de análisis XML se registran en el registro de operaciones del agente. (Consulte el manual *IBM Tivoli Monitoring Troubleshooting Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/trouble/itm_trouble.htm).)

Las situaciones privadas continúan ejecutándose hasta que se cierra el agente.

Los sucesos que están abiertos cuando una situación se convierte en verdadera se pueden enviar como condiciones de excepción de SNMPv1/v2 o informes de SNMPv3 cuando se crea un archivo de configuración de condiciones de excepción de SNMP y un receptor como la prueba Netcool/OMNIbus SNMP se ha configurado para recibirlos; o como sucesos EIF cuando se crea el archivo de configuración de sucesos de EIF y un receptor, como el servidor de sucesos de IBM Tivoli Enterprise Console o prueba Netcool/OMNIbus for Tivoli EIF está configurado para recibirlos. Asimismo, la Interfaz de servicio del agente proporciona un informe de resumen de la actividad de las situaciones.

El usuario crea un archivo de situación privada llamado *cp*`_situations.xml` y lo guarda en *`install_dir`*`/localconfig/`*cp* (donde *cp* es el código de producto). Si

prefiere asignar otro nombre al archivo o utilizar otra vía de acceso, se proporcionan las variables de entorno IRA_PRIVATE_SITUATION_CONFIG e IRA_LOCALCONFIG_DIR para que cambie el nombre y la vía de acceso del archivo.

distribuir situaciones privadas local o remotamente

Para editar y suprimir una situación privada, realice los cambios en el archivo XML de la configuración privada en el que se ha definido y luego redistribuya la situación local o remotamente.

Distribución local

Tras editar el archivo de configuración privada y de guardarlo, puede reiniciar el agente para volver a cargar las definiciones de situaciones privadas.

Como alternativa, puede iniciar una sesión en la Interfaz de servicio del agente y especificar solicitudes de situación privada para iniciar, detener o reciclar situaciones privadas individuales. Consulte el apartado "Inicio de la interfaz de servicio del agente" en la página 416 y el apartado "Solicitud de la Interfaz de servicio del agente - Control de situaciones privadas" en la página 438.

Distribución remota

Utilice una lista de carga de configuración para especificar el archivo de configuración privada para que el agente de supervisión lo tome del repositorio de configuración central y lo active. Consulte el apartado Capítulo 16, "configuración centralizada", en la página 447.

Resumen

Las situaciones privadas son solicitudes de supervisión del agente que define un administrador local con el criterio pertinente para el entorno del agente local. Este es un resumen de las características de las situaciones privadas:

- Se crean en el agente localmente a través de un editor sencillo.
- Los resultados y sucesos se emiten con las condiciones de excepción SNMP del agente.
- Se ha de ejecutar desde el momento en que se inicia el agente, independientemente de la conectividad del servidor de supervisión.
- Las expresiones múltiples de una fórmula deben tener conectores lógicos que sean AND conjuntivos u OR disyuntivos. No se da soporte a una combinación de los dos conectores en una fórmula.
- Se da soporte a un máximo de nueve expresiones en la fórmula de situación cuando se conectan mediante la lógica booleana AND y a un máximo de diez expresiones cuando se conectan mediante la lógica booleana OR.
- Todos los operadores de umbral de situación empresarial están soportados: igual a (EQ), no igual a (NE), mayor que (GT), menor que (LT), mayor que o igual a (GE) y menor que o igual a (LE).
- Se incluya soporte para el mandato de acción de automatización de reflejo.
- Se incluye soporte solo para las funciones de fórmula VALUE y MISSING; no se incluye soporte para funciones de grupo ni a otras funciones de celda.
- No se da soporte a caracteres comodín en situaciones privadas ni en alteraciones temporales de situación.
- Un grupo de atributos de una situación. No se da soporte al uso de dos grupos de atributos distintos.

- Se ejecutan simultáneamente con situaciones empresariales cuando el agente está conectado al servidor de supervisión.
- Se pueden ejecutar en un Tivoli Enterprise Monitoring Agent, tanto si está conectado como si es autónomo, o en un Tivoli System Monitor Agent.
- Permanecen desconocidas para la infraestructura gestionada centralmente de IBM Tivoli Monitoring. Tivoli Enterprise Monitoring Server y otro componente de IBM Tivoli Monitoring desconocen su existencia, incluidos los datos y sucesos de supervisión. Por lo tanto, las situaciones privadas no participan en la persistencia o el almacenamiento en memoria caché de sucesos entre los reinicios del agente, cuando el agente está desconectado de su servidor de supervisión.
- Como práctica recomendada, las situaciones de empresa y privadas deben tener nombres de situación exclusivos.

Especificación XML de situaciones privadas

Utilice los elementos de la especificación XML de situaciones privadas para crear situaciones privadas para un agente de su sistema.

Vía de acceso y nombre de archivo de situación privada predeterminada

Windows *dir_instalación*\localconfig*cp**cp*_situations.xml

Linux UNIX *dir_instalación*/localconfig/*cp*/*cp*_situations.xml

z/OS *PC*SICNFG en el conjunto de datos RKANDATV

Si prefiere asignar otro nombre al archivo o utilizar otra vía de acceso, utilice las variables de entorno IRA_PRIVATE_SITUATION_CONFIG e IRA_LOCALCONFIG_DIR para cambiar el nombre y la vía de acceso del archivo. Consulte el apartado “Situaciones privadas” en la página 339 y el apartado “Control de autonomía en agentes de Tivoli Enterprise Monitoring” en la página 336.

Elementos

Las etiquetas XML no son sensibles a mayúsculas y minúsculas. Los demás parámetros son sensibles a mayúsculas y minúsculas. Por ejemplo, puede escribir <PRIVATESIT>, <PrivateSit> o <privatesit>.

<PRIVATECONFIGURATION>

PRIVATECONFIGURATION es el elemento raíz que identifica este XML como un documento de configuración de situación privada de agente.

```
<PRIVATECONFIGURATION>
<PRIVATESIT>
<SITUATION NAME="Check_Process_CPU_Usage"  INTERVAL="000500" />
<CRITERIA>
<![CDATA[ *VALUE NT_Process.%_Processor_Time *GE 65 *AND
  *VALUE NT_Process.Priority_Base *NE 0 *AND
  *VALUE NT_Process.Process_Name *NE _Total]]>
</CRITERIA>
<CMD><![CDATA[netstat >.\logs\netstat.dat]]></CMD>
<AUTOSOPT When="N" Frequency="N" />
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

<PRIVATESIT>

Especifique cada definición de situación entre etiquetas PRIVATESIT inicial y final.

<SITUATION>

Dentro de cada conjunto de etiquetas PRIVATESIT inicial y final, añada un conjunto de etiquetas SITUATION inicial y final. Dentro de cada conjunto de etiquetas SITUATION inicial y final hay una definición de situación completa. Defina la situación con estos atributos:

NAME=

El nombre de la situación, que debe comenzar por una letra y puede tener un máximo de 31 letras números y signo de subrayado, como por ejemplo "Missing_Process_Helper_Harmless". Tenga en cuenta que todas las situaciones, ya sean privadas o de empresa, deben tener nombres exclusivos. De lo contrario, las acciones invocadas sobre una situación se aplican a otra situación con el mismo nombre.

INTERVAL=

A no ser que se trate de una situación de suceso puro, especifique el intervalo de muestreo con el formato HHMMSS. Valor predeterminado: **001500** (15 minutos). De forma opcional, utilice el elemento <INTERVAL>.

CRITERIA=

La fórmula de la situación. Alternativamente, utilice el elemento <CRITERIA>.

```
<SITUATION NAME="High_CPU_Usage" INTERVAL="000500"
CRITERIA="*VALUE NT_Process.%_Processor_Time *GE 65
*AND *VALUE NT_Process.Priority_Base *NE 0
*AND *VALUE NT_Process.Process_Name *NE _Total" />
```

DELETE=

Opcional. Especifique Y para suprimir la situación especificada en el atributo NAME=. Utilice este atributo para eliminar dinámicamente una situación privada sin reiniciar el agente o suprimir el archivo XML de situación privada local. Si especifica un nombre de situación privada no definida o que ya se ha suprimido, no se realiza ninguna acción. Puede especificar varias sentencias de supresión.

Para renovar dinámicamente una situación privada, incluya una sentencia de supresión *antes de* la nueva sentencia add. El orden de las especificaciones en un archivo XML de situaciones privadas afecta a las definiciones y configuración finales de las situaciones privadas de funcionamiento. El orden en el que se leen los archivos XML lo define la lista de carga de configuración centralizada y no sigue un orden alfabético.

Este ejemplo suprime una única situación privada:

```
<privateconfiguration>
<privatesit>
  <situation name="Check_Process_Name" delete="Y" />
</privatesit>
</privateconfiguration>
```

Este ejemplo suprime varias situaciones privadas:

```
<privateconfiguration>
<privatesit>
  <situation name="Check_Process_Name" delete="Y" />
</privatesit>
```

```
<privatesit>
  <situation name="Check_DiskSpace_Low" delete="Y" />
</privatesit>
</privateconfiguration>
```

Este ejemplo renueva una situación privada suprimiendo primero la situación y a continuación añadiendo la situación:

```
<privateconfiguration>
<privatesit>
  <situation name="Check_Process_CPU_Usage" delete="y" >
  </situation>
</privatesit>
<privatesit>
  <situation name="Check_Process_CPU_Usage" interval="000500" >
  </situation>
    <criteria>
    <![CDATA[*VALUE NT_Process_64.%_Processor_Time *GE 10 *AND
             *VALUE NT_Process_64.Priority_Base *NE 1 *AND
             *VALUE NT_Process_64.Process_Name *NE _Total]]>
      </criteria>
</privatesit>
</privateconfiguration>
```

<INTERVAL>

Especifica el intervalo de muestreo de la situación con el formato HHMMSS. Un valor de 000000 (seis ceros) indica que situación de suceso puro. Para situaciones de suceso de muestra, el intervalo mínimo es de 000030 (30 segundos) y el máximo es de 235959 (23 horas, 59 minutos y 59 segundos). Valor predeterminado: **001500** (15 minutos). Este elemento es necesario si no se especifica INTERVAL en el elemento SITUATION.

<CRITERIA>

El criterio de la situación se especifica dentro de este elemento y el elemento `<![CDATA[ ]]>` . Cada expresión tiene tres partes, comenzando por *VALUE o *MISSING, seguido de **atributo-tabla-nombre.atributo-nombre**, el operador lógico (por ejemplo, *EQ), y el valor de umbral de atributo o, para la función MISSING, una lista de nombres separados por comas. Se puede, aunque no es necesario, comenzar la fórmula por *IF, como en la sintaxis de fórmulas de situaciones de empresa.

Para el atributo, utilice el nombre de atributo detallado con el formato atributo-tabla-nombre.atributo-nombre. El archivo de atributos del producto define las tablas de atributos y los atributos asociados, por ejemplo, los archivos **knt.atr** o **kux.atr** que residen en el directorio ATTRLIB para una instalación de agente distribuido.

Otra forma de encontrar nombres de atributos es consultando la tabla a través de la interfaz de servicio del agente. Abra ASI > Consultas y seleccione un nombre de tabla. ASI devuelve un esquema de tabla completa que incluye el nombre de visualización de la tabla y los nombres de visualización de todas las columnas de la tabla.

El operador define el valor del filtro de la operación lógica y los datos. Los operadores soportados son: *EQ para igual a, *NE para no igual a, *GE para mayor que o igual a, *LE para menos que o igual a, *LT para menos que y *GT para mayor que. Dentro del elemento <CRITERIA>, el mandato se especifica entre etiquetas de datos de caracteres para excluirlo del análisis de XML. Este ejemplo muestra una fórmula que activa una alerta cuando el espacio de disco disponible está al 35% o por debajo:

```
<CRITERIA> <![CDATA[*VALUE NT_Logical_Disk.%_Free *LE 35]]> </CRITERIA>
```

Para las expresiones múltiples, utilice el conector *AND o *OR. Todos los conectores de la fórmula deben ser iguales, o bien todos *AND o bien todos *OR. No está soportada la combinación de conectores *AND y *OR. Puede tener hasta un máximo de nueve conectores *AND o hasta un máximo de 10 conectores *OR en una fórmula, .

En una fórmula con varias expresiones, puede haber más de una expresión *MISSING, debe ser la última expresión de la fórmula y solamente se pueden utilizar conectores *AND. (Consulte el manual *Tivoli Enterprise Portal: Guía del usuario* para ver una descripción de **Comprobar si faltan elementos**.)

Los comodines no están soportados. Por ejemplo, *VALUE NT_Process.Process_Name *EQ S* para buscar todos los procesos que comienzan por "S" no es válido en una situación privada. Paralelamente, los caracteres comodín en una lista *MISSING no son válidos, como por ejemplo en NT_Process.Process_Name *EQ ('DB2*') para buscar todos los procesos que comienzan por DB2.

Ejemplos:

```
<CRITERIA>
<![CDATA[ *VALUE NT_Process.%_Processor_Time *GE 65 *AND
  *VALUE NT_Process.Priority_Base *NE 0 *AND
  *VALUE NT_Process.Process_Name *NE _Total]]>
</CRITERIA>
```

```
<CRITERIA>
<![CDATA[ *MISSING NT_Process.Process_Name *EQ ('schedule','notepad')]]>
</CRITERIA>
```

```
<CRITERIA>
<![CDATA[ *VALUE Linux_Process.State *NE Running *AND
*MISSING Linux_Process.Process_Command_Name *EQ ('MyHelp', 'myhelpw')]]>
</CRITERIA>
```

Los atributos enumerados tienen un conjunto predefinido de valores. Puede especificar el símbolo de enumeración o el nombre. Por ejemplo, estas dos expresiones con un estado de ejecución de `Stopped (Detenido)` (`T`) son válidos. Si se envía una alerta SNMP o se emprende una acción, se utiliza el símbolo en lugar del nombre:

```
<CRITERIA><![CDATA[ *VALUE Process.Execution_State *EQ Stopped]]></CRITERIA>
<CRITERIA><![CDATA[ *VALUE Process.Execution_State *EQ T]]></CRITERIA>
```

Si la situación privada utiliza cualquier atributo escalado, sus valores se deben normalizar para una evaluación correcta. Un valor de atributo escalado se utiliza para especificar el número de posiciones de desplazamiento del punto decimal a la izquierda. Por ejemplo, 55.255 es un valor válido para un atributo que se muestra con una escala de 3. Para normalizarlo, debe desplazar el punto decimal a la derecha en tres posiciones para que pase a ser 55255.

SCAL (Escala)	**Valor de comparación de enteros (el ejemplo utilizado es 5000)**
No definido (0)	5000
1	Se ve como 500 ó 500.0, pero representa 5000
2	Se ve como 50 ó 50.00, pero representa 5000
3	Se ve como 5 ó 5.000, pero representa 5000

Los temas de descripción de atributos para su producto deben especificar si se escala el valor. Para los agentes distribuidos, también puede revisar el

archivo de atributos para scal en la definición de atributos. Por ejemplo, khd.atr para el agente de proxy de almacén tiene un atributo de índice de inserción en cola de trabajo con scal 2. Ubicación de archivos k*cp*.atr: Windows *<dir_instalación>*\TMAITM6\ATTRLIB; Linux UNIX *<dir_instalación>*/plataforma/<cp>/tables/ATTRLIB, donde plataforma es el sistema operativo y cp es el código del producto.

En este ejemplo se muestra un entero hexadecimal como el valor de comparación:

```
<CRITERIA><![CDATA[ *VALUE Disk.Mount_Point_U *EQ '/opt' *AND
*VALUE Disk.Space_Used_64 *GT 0x80000000 ]]></CRITERIA>
```

El elemento <CRITERIA> es necesario si no se especifica CRITERIA en el elemento <SITUATION>.

***REGEX**

IBM Tivoli Monitoring con frecuencia requiere exploración de texto y coincidencia de patrón en los datos de ejemplo y sucesos, como nombre, dirección, mensaje y registro. Puede añadir la función de filtro de predicado Expresión regular para mejorar la prestación de agente de supervisión y aplicabilidad. La sintaxis de la especificación de función de predicado *REGEX se define como: **REGEX nombre_atributo operador "Expresión regular"* donde,

nombre_atributo es el nombre de atributo completo de filtro de selección.

operador es la operación lógica del valor y de los datos de filtro. Los operadores soportados son: **EQ* (lo que significa valor igual) y **NE* (lo que significa valor no igual).

" " son delimitadores de expresión regular. También puede utilizar otros caracteres para delimitadores como @ @ si se requiere el carácter " en la expresión. Por ejemplo: **REGEX nombre_atributo operador @Expresión regular@*

Expresión regular especifica la definición de expresión regular deseada.

El ejemplo siguiente muestra el uso de función de predicado *REGEX. En este ejemplo, la compañía ABC desea inspeccionar la entrada del usuario para la información de apartado de correos (P.O. Box), a fin de emitir un suceso porque ABC no puede realizar envíos a apartados de correos.

```
<privateconfiguration>
<privatesit>
<SITUATION NAME="Check_Valid_Address" INTERVAL="000030" >
 </SITUATION>
<criteria>
<![CDATA[*REGEX ABCCUSTOMER_PROFILE00.Address
  *EQ "(?:Post (?:Office )?|P[. ]?O\.? )?[Bb]ox\b"]]>
</criteria>
<DISTRIBUTION>ICVR5A05:ABC00</DISTRIBUTION>
</privatesit>
</privateconfiguration>
```

Se puede utilizar la función de predicado *REGEX en combinación con funciones de predicado adicionales tal como se muestra en el ejemplo siguiente.

```
<privateconfiguration>
<privatesit>
<Situation Name="Check_Valid_Address" Interval="000030" />
```

```
<criteria>
<![CDATA[*VALUE ABCCUSTOMER_PROFILE00.Weight  *GE 5 *AND
  *REGEX ABCCUSTOMER_PROFILE00.Address
  *EQ $(?:Post (?:Office )?|P[. ]?O\.? )?Box\b$ ]]>
</criteria>
<Distribution>ICVR5A05:ABC00</Distribution>
</privatesit>
</privateconfiguration>
```

Como regla general, *REGEX filtra datos de columnas de la aplicación en almacenamiento intermedio de almacenamiento de filas de datos. Por lo tanto, el ancla de entrada de inicio (^ o \A) o ancla de final de línea ($ o \Z) no se aplican y son innecesarias cuando se produce una coincidencia al principio o final de los datos de columna.

Notas de uso:

- No se da soporte a atributos de entero en el predicado de expresión regular.
- No da soporte a atributos enumerados en el predicado de expresión regular. Sin embargo, se debe utilizar el valor de columna real en la propia construcción de la expresión regular. No se da soporte a la sustitución de valores de enumeración en expresiones regulares que requiere modificación automatizada de la propia expresión.

  Por ejemplo, el atributo Day_Of_Week de la tabla Local_Time tiene los valores de cadena de caracteres enumerados de Domingo, Lunes, Martes, Miércoles, Jueves, Sábado, pero el valor de columna real de 00, 01, 02, 03, 04, 05, 06. Se deben utilizar los valores de columna reales en la construcción de expresiones regulares.
- Una expresión regular que contiene atributos de tipos de datos no soportados como, por ejemplo, entero, entero-64, enumeración de enteros y cadena de caracteres hexadecimales, se marca como un error y la definición de situación privada se rechaza.

La implementación de expresión regular varía ligeramente según el motor de soporte. La función de filtro de predicado *REGEX de situación privada utiliza el motor de expresiones regulares de ICU y sus especificaciones. Consulte la publicación *ICU User Guide* para obtener más información.

<CMD>

Opcional. Define el mandato de acción o el script que se ha de invocar cuando una situación es verdadera. Dentro del elemento <CMD>, el mandato se especifica entre etiquetas de datos de caracteres para excluirlo del análisis de XML. Este ejemplo muestra un mandato del sistema que muestra la indicación de fecha y hora en un recuadro de mensaje en el agente cuando la situación pasa a ser verdadera. Sin las etiquetas CDATA, el analizador de XML consideraría el carácter & y las llaves {} como un error.

```
<CMD>
<![CDATA[ net send &{Local_Time.Timestamp}  ]]>
</CMD>
```

tags.

<AUTOSOPT>

Es necesario si se especifica una acción <CMD>. Define las opciones de ejecución de mandatos de acción, WHEN (X), FREQUENCY (Y), WHERE (Z). El valor predeterminado es NNN:

WHEN= Opcional. "Y" para ejecutar el mandato para cada elemento o "N" para ejecutar el mandato solamente en la primera fila de los datos devueltos que cumpla con los criterios de la situación. Si el grupo de atributos devuelve varias filas de datos y más de una fila satisface la condición, puede optar por emitir el mandato sólo sobre la primera fila que cumpla los criterios o una vez para cada fila que cumpla los criterios. Valor predeterminado: **"N"**.

FREQUENCY= Opcional. "Y" para emitir el mandato cada vez que la situación se evalúe como verdadera; o "N" para emitir el mandato cuando la situación sea verdadera, pero no volverlo a emitir hasta que la situación se evalúe como falsa, seguida de otra evaluación como verdadera. Valor predeterminado: **"N"**.

WHERE= "N" para ejecutar el mandato en el agente. Valor predeterminado: **"N"** Puesto que solo hay un valor posible para "where", no es necesario que lo incluya en el elemento AUTOSOPT.

```
<AUTOSOPT When="Y" Frequency="Y" />
```

<DISTRIBUTION>

Es necesario para productos con subnodos (subagentes). Especifica un nombre de sistema gestionado o una lista de nombres de sistemas gestionados separados por un signo de punto y coma (;). No hay valor predeterminado.

Si utiliza el código <HISTORY>, anide el código <DISTRIBUTION> en <HISTORY>.

<LSTDATE>

Opcional. La indicación de la hora de la última actualización del agente. Si no se especifica, se genera automáticamente la hora actual de los datos. El formato es SAAMMDDHHMMSSmmm (como en 1100715074501000 para 15 de Julio, 2010 a las 07:45:01) donde:

S = Siglo (1 para siglo XXI)

A = Año

M = Mes

D = Día

H = Hora

M = Minuto

S = Segundo

m = milisegundo

<LSTUSRPRF>

Opcional. Es el ID del usuario que ha actualizado por última vez la definición de la situación. Si no se especifica, entonces se utiliza el ID de usuario de inicio de sesión actual. Ejemplo:

```
<LSTUSRPRF>SYSADMIN</LSTUSRPRF>
```

<LSTRELEASE>

Opcional. Especifica la versión de la situación. Ejemplo:

```
<LSTRELEASE>V622</LSTRELEASE>
```

<SITINFO>

Opcional. Define los calificadores de situación para sucesos de EIF. Debe

estar encerrado entre el elemento <![CDATA[ ]]>. Alternativamente, define los calificadores para sucesos de EIF mediante parámetros. Varios calificadores quedan delimitados por un signo de punto y coma (;).

ATOM= Opcional. Para grupos de atributos de varias filas. Es el nombre de COLUMNA del catálogo que se va a utilizar como elemento de visualización, lo que hace que se genere un suceso para cada subconjunto de filas con el mismo valor de elemento de visualización.

COUNT= Opcional. Se denomina "permanencia de situación" en Tivoli Enterprise Portal. Especifique el número de intervalos durante los que la situación debe seguir siendo verdadera antes de que se abra un suceso.

SEV= Opcional. La gravedad que se va a asignar al suceso de EIF: Muy grave, Crítico, Aviso, Leve, Inofensivo, Informativo o Desconocido.

TFWD=[Y|N] Opcional. **Y** es el valor predeterminado. Si desea enviar solo alertas SNMP y no sucesos de EIF, establezca este atributo en **N**.

TDST= Opcional. Especifique uno más destinos de receptor de EIF a los que enviar el suceso. Puede especificar un máximo de cinco ID de servidor de destino válidos, separados por una coma (,). Los destinos válidos están definidos en el archivo `pc_eventdest.xml`. Si no se especifica ningún parámetro TDST, el suceso EIF se envía a todos los destinos de sucesos predeterminados definidos (entradas de directorio con el valor default="Y") en el archivo de configuración de destinos.

Ejemplos:

```
<SITINFO><![CDATA[SEV=Fatal;~;]]></SITINFO>
<SITINFO><![CDATA[SEV=Critical;TFWD=Y;TDST=1,3;]]></SITINFO>
```

<HISTORY>

Opcional. Utilice el elemento HISTORY para especificar cada grupo de atributos para el que desea recopilar los datos históricos. El agente no soporta varias especificaciones <HISTORY> para el mismo elemento TABLE.

TABLE= Obligatorio. Este parámetro especifica el nombre del grupo de atributos de la aplicación.

EXPORT= Opcional. Este parámetro especifica el intervalo in minutos para exportar datos históricos a Tivoli Data Warehouse. El intervalo de exportación mínimo es de 15 minuto y el máximo es de 1440 (24 horas). Los intervalos de exportación válidos son 15, 30 y los valores divisibles por 60; un intervalo mayor que 60 puede ser 120, 180, 240, y así sucesivamente, hasta 1440. El intervalo de exportación también debe ser divisible por el valor del parámetro INTERVAL. Si especifica un valor no válido, no se recopilarán ni exportarán datos históricos para el grupo de atributos especificado. Valor predeterminado: **none**.

INTERVAL= Opcional. Este parámetro especifica el intervalo de recopilación de datos históricos en minutos. El intervalo de recopilación mínimo es de 1 minuto y el máximo es de 1440 (24 horas). Los intervalos válidos son los valores que pueden dividirse por 60: un intervalo por debajo de 60 puede ser 1, 2, 3, 4, 5, 6, 10, 12, 15, 20 y 30; un intervalo mayor que 60 puede ser 120, 180, 240, etc. hasta 1440. Si especifica un valor no válido, no se recopilarán datos históricos para el grupo de atributos especificado. Valor predeterminado: **"15"**.

RETAIN= Opcional. RETAIN define el período de retención de datos históricos a corto plazo en horas. El valor predeterminado es de 24 horas y el período de retención mínimo es de una hora. No existe un límite que no sea el que impone el espacio de almacenamiento del

sistema. Cuando se alcanza el límite de retención, las muestras de datos más antiguas se suprimen a medida que llegan nuevas muestras. Valor predeterminado: **"24"**.

Atención: En situaciones privadas utiliza solo nombres externos (igual que nombres de visualización). Las situaciones privadas que utilizan nombres internos fallan.
Ejemplos:

El agente de SO Windows recopila datos de la tabla NT_System cada 15 minutos y mantiene 96 filas de datos (cuatro veces por hora cada 24 horas) en el archivo de historial.

```
<HISTORY TABLE="NT_System" />
```

El agente de SO UNIX recopila datos de tabla del sistema cada 5 minutos y mantiene 3 días de historial a corto plazo.

```
<HISTORY TABLE="System" Interval="5" RETAIN="72"  />
```

El agente de SO Windows recopila datos de la tabla NT_Logical_Disk cada minuto.

```
<HISTORY TABLE="NT_Logical_Disk" INTERVAL="1"  />
```

El elemento <DISTRIBUTION> es necesario para entornos de subnodo. Por ejemplo, el agente universal recopila datos de la tabla TS2TCPIOQ00 cada 10 minutos y mantiene 1 día de historial a corto plazo en el subnodo llamado SYSGTCPIOQ:TS200.

```
<HISTORY TABLE="TS2TCPIOQ00" INTERVAL="10" RETAIN="24" >
<DISTRIBUTION>SYSGTCPIOQ:TS200</DISTRIBUTION>
</HISTORY>
```

El agente de SO Linux recopila datos de la tabla KLZ_Disk cada 5 minutos con los datos exportados cada 15 minutos.

```
<HISTORY TABLE="KLZ_Disk" INTERVAL="5" EXPORT="15" />
```

<WAREHOUSE>

Opcional. Utilice el elemento warehouse para especificar la ubicación de un Warehouse Proxy agent para el que hay que exportar datos. El agente no soporta varias especificaciones <WAREHOUSE>.

LOCATION=

Este parámetro especifica la ubicación de cada Warehouse Proxy agent al que se exportan datos históricos. Se puede especificar una ubicación principal y varias ubicaciones secundarias separadas por un punto y coma (;). Esta ubicación solo la utiliza el agente cuando tenga autonomía completa y no se ha especificado el parámetro KHD_WAREHOUSE_LOCATION.

Especifique una dirección de escucha registrada del Warehouse Proxy agent que va a transferir datos históricos del agente a Tivoli Data Warehouse. La sintaxis es *familia protocolo:red dirección[número puerto]*. Revise el registro de rastreo RAS1 del agente de proxy de almacén para determinar las direcciones registradas.

El siguiente fragmento del registro de RAS1 muestra el agente de proxy de almacén registrando una dirección de escucha:

```
khdxrpcr.cpp,621,"register_interface") Registering
   "Candle_Warehouse_Proxy": ip.pipe:#9.44.255.253 [63358]
```

Nota: Para que los datos históricos se exporten correctamente, el agente de supervisión debe tener el mismo protocolo de comunicaciones habilitado que el especificado para la ubicación del proxy de almacén. Consulte "Supervisión del sistema operativo mediante un agente supervisor del sistema" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* para obtener más información sobre el parámetro KDC_FAMILIES_OVERRIDE.

Ejemplos:

```
<WAREHOUSE LOCATION="ip.pipe:DEPT-XP[63358]" />
<WAREHOUSE LOCATION="ip.pipe:#9.44.255.253[63358]" />
```

Especificación XML de situaciones de empresa exportadas

Utilice las definiciones de situación de los archivos *nombre_situación*.xml que son el resultado de los mandatos **tacmd bulkExportSit** y **tacmd viewSit** de la CLI para llenar el archivo de configuración de situaciones privadas del agente.

Consulte el manual *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) para ver la sintaxis y ejemplos de tacmd.

Si ya tiene situaciones de empresa para un Tivoli Enterprise Monitoring Agent, puede ejecutar el mandato de exportar paquete de situaciones o el mandato ver situación para obtener definiciones de situación para el agente especificado en el formato XML que es aceptable para el archivo de configuración de situaciones privadas. No todas las situaciones exportadas son válidas; solo aquellas que utilizan las funciones de fórmula *VALUE o *MISSING. Consulte "Limitaciones de las situaciones" en la página 342 para ver otras restricciones.

Elementos

Las etiquetas XML no son sensibles a mayúsculas y minúsculas. Los demás parámetros son sensibles a mayúsculas y minúsculas. Por ejemplo, puede escribir <SITNAME>, <SitName> o <sitname>.

<TABLE>
Es el elemento raíz del archivo XML de situaciones exportadas. En el archivo de configuración de situaciones privadas, el etiquetado TABLE (y todo lo comprendido dentro) de la situación exportada se procesa como una definición de situación privada.

<ROW>
Este es el elemento hijo que sigue a TABLE.

<SITNAME>
Nombre de la situación de supervisión. El nombre de la situación, que debe comenzar por una letra y puede tener un máximo de 31 letras números y signo de subrayado. Dentro de cada conjunto de etiquetas SITNAME inicial y final hay una definición de situación completa. Ejemplo:

```
<SITNAME>Free_DiskSpace_Low</SITNAME>
```

Tenga en cuenta que todas las situaciones, ya sean privadas o de empresa, deben tener nombres exclusivos. De lo contrario, las acciones invocadas sobre una situación se aplican a otra situación con el mismo nombre.

<PDT>

Los criterios de la situación se especifican dentro del elemento de predicado <PDT> y el elemento `<![CDATA[ ]]>`. Cada expresión tiene tres partes, comenzando por *IF *VALUE o *IF *MISSING, seguido de **nombre-tabla-atributos.nombre-atributo**, el operador lógico (por ejemplo, *NE), y el valor de umbral de atributo o, para la función MISSING, una lista separada por comas. Las situaciones de empresa exportadas siempre comienzan por *IF y se puede, aunque no es obligatorio, incluir *IF en la fórmula.

Para el atributo, se utiliza el nombre de atributo detallado con el formato nombre-tabla-atributos.nombre-atributo. El archivo de atributos del producto define las tablas de atributos y los atributos asociados, por ejemplo, los archivos **knt.atr** o **kux.atr** que residen en el directorio ATTRIB para una instalación de agente distribuido.

El operador define el valor del filtro de la operación lógica y los datos. Los operadores soportados son: *EQ para igual a, *NE para no igual a, *GE para mayor que o igual a, *LE para menos que o igual a, *LT para menos que y *GT para mayor que. Dentro del elemento <PDT>, el mandato se especifica entre etiquetas de datos de caracteres para excluirlo del análisis de XML. Este ejemplo muestra una fórmula que activa una alerta cuando el espacio de disco disponible está al 35% o por debajo:

```
<PDT> <![CDATA[*IF *VALUE NT_Logical_Disk.%_Free *LE 35]]> </PDT>
```

Para las expresiones múltiples, utilice el conector *AND o *OR. Todos los conectores de la fórmula deben ser iguales, o bien todos *AND o bien todos *OR. No está soportada la combinación de conectores *AND y *OR. Ejemplo:

```
<PDT> <![CDATA[*IF *VALUE NT_Process.%_Processor_Time *GE 65 *AND
*VALUE NT_Process.Priority_Base *NE 0 *AND
*VALUE NT_Process.Process_Name *NE _Total]]> </PDT>
```

No se da soporte a caracteres comodín en situaciones privadas. Por ejemplo, *VALUE NT_Process.Process_Name *EQ DB2* para buscar todos los procesos que comienzan por “DB2” no es válido.Las situaciones de empresa exportadas con atributos escalados no se normalizan cuando se ejecutan como situaciones privadas. Debe normalizar manualmente los valores. Por ejemplo, esta expresión de situación empresarial `Avg Disk Queue Length >= 0.004` es un atributo de punto flotante con una escala de 3. Cuando se exporta la situación con el mandato **tacmd viewSit**, el criterio de supervisión de la exportación se muestra de este modo:

```
<PDT>  <![CDATA[*IF *VALUE NT_Physical_Disk.Avg_Disk_Queue_Length
*GE 0.004]]> < PDT>
```

Cuando se especifica esta misma definición en una situación privada, el valor de comparación de valor se interpreta como un valor cero.

```
<PRIVATECONFIGURATION>
<PRIVATESIT>
<SITUATION>SCALE_TEST</SITUATION>
<CRITERIA><![CDATA[ *IF *VALUE NT_Physical_Disk.Avg_Disk_Queue_Length
*GE 0.004 ]]></CRITERIA>
<INTERVAL>000030</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

Normalice el valor mediante un desplazamiento del punto decimal en tres posiciones a la derecha: 0.004 es 4 o un valor como el que se muestra aquí.

```
<CRITERIA><![CDATA[ *IF *VALUE NT_Physical_Disk.Avg_Disk_Queue_Length
*GE 4.123 ]]></CRITERIA>
```

<CMD>

Opcional. Define el mandato de acción o el script que se ha de invocar cuando una situación es verdadera. Encierre el mandato en la sección <![CDATA[ ]]>. Ejemplo:

```
<CMD><![CDATA[netstat >.\logs\netstat.dat]]></CMD>
```

<AUTOSOPT>

Es necesario si se especifica un mandato de acción <CMD>. Define las opciones de ejecución de mandatos de acciones de automatización de reflejo, en orden XYZ, entre las etiquetas de inicio y fin. El valor predeterminado es NNN:

- **Actuación sólo sobre el primer elemento**
- **No emprender una acción dos veces en una fila (esperar hasta que la situación pase a ser falsa y de nuevo verdadera)**
- **Ejecutar la acción en el sistema gestionado (agente)**

X=Y Ejecutar mandato para cada elemento.

X=N Ejecutar mandato solamente en el primer elemento.

Y=Y Ejecutar mandato para cada intervalo de muestreo.

Y=N No ejecutar el mandato dos veces en una fila.

Z=N Siempre está establecido en N para situaciones privadas y significa ejecutar el mandato en el agente. Si la opción exportada tiene el valor Y, el valor se pasa por alto y se trata como N.

<DISTRIBUTION>

Es necesario para productos con subnodos (subagentes). Especifica un nombre de sistema gestionado o varios nombres de sistemas gestionados separados por una coma (,). El valor predeterminado es el nombre del sistema gestionado del agente o todos los subagentes conocidos.Los grupos de sistemas gestionados no reciben soporte, incluidos los grupos de sistemas gestionados predefinidos, que tienen como prefijo un asterisco (*).

<LSTCCSID>

Opcional. Especifica el ID de juego de caracteres de códigos de IBM. **en_US** es el único valor permitido.

<LSTDATE>

Opcional. La indicación de la hora de la última actualización del agente. Si no se especifica, se genera automáticamente la hora actual de los datos. El formato es SAAMMDDHHMMSSmmm (como en 1090715074501000 para 15 de Julio, 2009 a las 07:45:01) donde:

S = Siglo (1 para siglo XXI)

A = Año

M = Mes

D = Día

H = Hora

M = Minuto

S = Segundo

m = milisegundo

<LSTRELEASE>

Opcional. Especifica la versión de la situación.

<LSTUSRPRF>

Opcional. Es el ID del usuario que ha actualizado por última vez la definición de la situación. Si no se especifica, entonces se utiliza el ID de usuario de inicio de sesión actual.

<SITINFO>

Opcional. Define los calificadores de situación para sucesos de EIF. Dentro del elemento <SITINFO>, encierre la fórmula de situación entre etiquetas `<![CDATA[ ]]>`, como por ejemplo `<![CDATA[ SEV=Critical ]]>`. Alternativamente, define los calificadores mediante parámetros. Varios calificadores quedan delimitados por un signo de punto y coma (;).

ATOM= Opcional. Para grupos de atributos de varias filas. Es el nombre de COLUMNA del catálogo que se va a utilizar como elemento de visualización, lo que hace que se genere un suceso para cada subconjunto de filas con el mismo valor de elemento de visualización.

COUNT= Opcional. Se denomina "permanencia de situación" en Tivoli Enterprise Portal. Especifique el número de intervalos durante los que la situación debe seguir siendo verdadera antes de que se abra un suceso.

SEV= Opcional. La gravedad que se va a asignar al suceso de EIF: Muy grave, Crítico, Aviso, Leve, Inofensivo, Informativo o Desconocido.

TFWD=[Y|N] Opcional. **Y** es el valor predeterminado. Si desea enviar solo alertas SNMP y no sucesos de EIF, establezca este atributo en **N**.

TDST= Opcional. Especifique uno más destinos de receptor de EIF a los que enviar el suceso. Puede especificar un máximo de cinco ID de servidor de destino válidos, separados por una coma (,). Los destinos válidos están definidos en el archivo `pc_eventdest.xml`. Si no se especifica ningún parámetro TDST, el suceso EIF se envía a todos los destinos de sucesos predeterminados definidos (entradas de directorio con el valor default="Y") en el archivo de configuración de destinos.

<TEXT>

La descripción de la situación. Dentro del elemento <TEXT>, encierre la fórmula de situación entre las etiquetas `<![CDATA[ ]]>`.

<REEV_TIME>

Especifica el intervalo de muestreo de la situación con el formato HHMMSS. El valor 0 indica una situación de suceso puro. El intervalo predeterminado es de 15, 001500; el valor mínimo es de 30 segundos, 000030; y el valor máximo es de 23 horas, 59 minutos y 59 segundos, 235959. Ejemplo:

```
<REEV_TIME>000500</REEV_TIME>
```

Elementos que se pasan por alto

Los elementos siguientes de la especificación XML exportada no se utilizan excepto cuando se indica:

<FULLNAME> (procesado para EIF)

<ADVISE>

<AFFINITIES>

<ALERTLIST>

<AUTOSTART>

<DESTNODE />

<HUB />

<LOCFLAG />

<NOTIFYARGS>
<NOTIFYOPTS>
<OBJECTLOCK>
<PRNAMES>
<QIBSCOPE>
<REEV_DAYS> (más de 1 día no soportado)
<REFLEXOK>
<SENDMSGQ>
<SITINFO> (procesado para EIF)
<SOURCE>

Ejemplo de situación de empresa exportada

La situación NT_System_File_Critical exportada con **tacmd bulkExportSit** o **tacmd viewSit** se guarda en el archivo NT_System_File_Critical.xml:

```
<TABLE>
 <ROW>
  <SITNAME>NT_System_File_Critical</SITNAME>
  <FULLNAME>
    <![CDATA[ ]]>
  </FULLNAME>
  <ADVISE>
   <![CDATA[ ADVICE("knt:"+$ISITSTSH.SITNAME$);]]>
  </ADVISE>
  <AFFINITIES>%IBM.STATIC021 01000000000</AFFINITIES>
  <ALERTLIST>*NO</ALERTLIST>
  <AUTOSOPT>NNN</AUTOSOPT>
  <AUTOSTART>*YES</AUTOSTART>
  <CMD>
   <![CDATA[ *NONE  ]]>
  </CMD>
  <DESTNODE />
  <HUB />
  <LOCFLAG />
  <LSTCCSID />
  <LSTDATE>0961009010101000</LSTDATE>
  <LSTRELEASE />
  <LSTUSRPRF>IBM</LSTUSRPRF>
  <NOTIFYARGS />
  <NOTIFYOPTS />
  <OBJECTLOCK />
  <PDT>
    <![CDATA[ *IF *VALUE NT_System.File_Data_Operations/Sec *GE 100000 ]]>
  </PDT>
  <PRNAMES />
  <QIBSCOPE>E</QIBSCOPE>
  <REEV_DAYS>0</REEV_DAYS>
  <REEV_TIME>001500</REEV_TIME>
  <REFLEXOK />
  <SENDMSGQ>*NONE</SENDMSGQ>
  <SITINFO>
   <![CDATA[ SEV=Critical ]]>
  </SITINFO>
  <SOURCE />
  <TEXT>
   <![CDATA[ Knt:KNT1359 ]]>
  </TEXT>
  <DISTRIBUTION>*NT_SYSTEM</DISTRIBUTION>
 </ROW>
</TABLE>
```

En el archivo de configuración de situaciones privadas, se crea un conjunto de etiquetas <PRIVATESIT> y </PRIVATESIT> y luego el contenido de NT_System_File_Critical.xml se pega dentro de las etiquetas. A continuación se muestra un archivo de configuración de situaciones privadas nt_situations.xml después de que se añada la definición de situación exportada NT_System_File_Critical sobre otra definición de situación privada, Check_Process_CPU_Usage. Los elementos redundantes (consulte la sección anterior "Elementos que se pasan por alto") y los elementos no utilizados (AUTOSOPT y CMD, LSTCCSID, LSTRELEASE, DISTRIBUTION) de la situación exportada se han eliminado, aunque dejarlos en el archivo no ocasiona problemas ya que el analizador de XML los pasa por alto:

```
<PRIVATECONFIGURATION>
<TABLE>
 <ROW>
  <SITNAME>NT_System_File_Critical</SITNAME>
  <LSTDATE>09610090101010000</LSTDATE>
  <LSTUSRPRF>IBM</LSTUSRPRF>
  <PDT>
   <![CDATA[ *IF *VALUE NT_System.File_Data_Operations/Sec *GE 100000 ]]>
  </PDT>
  <REEV_TIME>001500</REEV_TIME>
  <SITINFO>
   <![CDATA[ SEV=Critical ]]>
  </SITINFO>
  <TEXT>
   <![CDATA[ Knt:KNT1359 ]]>
  </TEXT>
  </ROW>
</TABLE>
<PRIVATESIT>
  <SITNAME>Check_Process_CPU_Usage</SITNAME>
  <PDT>
   <![CDATA[ *IF *VALUE NT_Process.%_Processor_Time *GE 65 *AND
   *VALUE NT_Process.Priority_Base *NE 0 *AND
   *VALUE NT_Process.Process_Name *NE _Total]]>
  </PDT>
  <REEV_TIME>000300</REEV_TIME>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

Consejo: A cada situación exportada se le asigna su propio archivo XML. Si las situaciones privadas son resultado inicialmente de una exportación de las situaciones de empresa, cree un XML con etiquetas PRIVATECONFIGURATION inicial y final y luego pegue las etiquetas TABLE inicial y final y todo lo contenido entre las mismas en el archivo para cada situación que desee incluir. Para situaciones exportadas, las etiquetas TABLE equivalen a las etiquetas PRIVATESIT.

Ejemplos de situaciones privadas

Defina situaciones privadas para el criterio de supervisión relativo al entorno del agente local y que no dependan ni sean relevantes para el entorno de la empresa. Estos ejemplos se pueden utilizar como plantilla para las situaciones privadas.

Consejo: Se proporcionan archivos de configuración de situaciones privadas de ejemplo en el soporte de instalación de Tivoli Monitoring Agent en el directorio `PrivateConfigSamples`.

lz_situations.xml del sistema operativo Linux

```
<PRIVATECONFIGURATION>
<!--  Situation Description: Percentage of time the processor is busy
is extremely high -->
```

```
<PRIVATESIT>
  <SITUATION>Linux_High_CPU_Overload_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_CPU.Idle_CPU *LT 10  *AND  *VALUE Linux_CPU.CPU_ID
   *EQ Aggregate ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
  </PRIVATESIT>
<!-- Situation Description: Percentage of packet collisions during data
transmission is high -->
<PRIVATESIT>
  <SITUATION>Linux_High_Packet_Collisons_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Network.Collision_Percent *GT 10 ]]>
  </CRITERIA>
  <INTERVAL>000500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Percentage of available i-nodes is low -->
<PRIVATESIT>
  <SITUATION>Linux_Low_Pct_Inodes_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Disk.Inodes_Used_Percent *GT 80 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Percentage of space available on a filesystem
is low -->
<PRIVATESIT>
  <SITUATION>Linux_Low_Pct_Space_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Disk.Space_Available_Percent *LT 15 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Tests if the SSH Daemon, sshd, is up running -->
<PRIVATESIT>
  <SITUATION>Linux_Process_Missing_sshd_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *IF *MISSING Linux_Process.Process_Command_Name
   *EQ ("/usr/sbin/sshd") ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Percentage of Processor time used by
a process high -->
<PRIVATESIT>
  <SITUATION>Linux_Process_High_CPU_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Process.Busy_CPU_Pct *GT 60 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: High number of stopped processes on this system -->
<PRIVATESIT>
  <SITUATION>Linux_Process_Stopped_pr</SITUATION>
  <CRITERIA>
   <![CDATA[ *VALUE Linux_Process.State *NE Running *AND
   *VALUE Linux_Process.State *NE Sleeping  *AND
   *VALUE Linux_Process.State *NE Disk  *AND
   *VALUE Linux_Process.State *NE Trace ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percentage of rejected RPC server or
client calls is high -->
<PRIVATESIT>
  <SITUATION>Linux_RPC_Bad_Calls_pr</SITUATION>
```

```
  <CRITERIA>
   <![CDATA[  *VALUE Linux_RPC_Statistics.RPC_Client_Calls_Retransmitted *GT 30
   *OR  *VALUE Linux_RPC_Statistics.RPC_Server_Calls_Rejected *GT 30 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: The swap space paging activity on this system
is extremely high  -->
<PRIVATESIT>
  <SITUATION>Linux_System_Thrashing_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_System_Statistics.Pages_paged_out_per_sec *GT 400
   *OR  *VALUE Linux_System_Statistics.Pages_paged_in_per_sec *GT 400 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

ux_situations.xml del sistema operativo UNIX

```
<PRIVATECONFIGURATION>
<!--  Situation Description: Reports High CPU processes  -->
<PRIVATESIT>
  <SITUATION>UNIX_CMD_Runaway_Process_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *IF *VALUE Process.CPU_Utilization *GT 95 ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Process CPU utilization is greater than
or equal to 85% -->
<PRIVATESIT>
  <SITUATION>UNIX_CPU_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *IF *VALUE Process.CPU_Utilization *GE 85 *AND *VALUE
   Process.Command *NE kproc *AND *VALUE Process.Command *NE swapper ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Notes typical I/O bound processor (NFS) -->
<PRIVATESIT>
  <SITUATION>UNIX_HD_Exces_IO_Wait_prv</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE System.Wait_I/O *GT 20  ]]>
  </CRITERIA>
  <INTERVAL>000200</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Tests if the Internet Services Daemon, inetd,
is up running -->
<PRIVATESIT>
  <SITUATION>UNIX_Process_Missing_inetd_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *MISSING Process.Command *EQ  ("/usr/sbin/inetd") ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Checks the System CPU, Idle, I/O Wait,
and Load Averages for the Busy state  -->
<PRIVATESIT>
  <SITUATION>UNIX_System_Busy_Warning_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE System.System_CPU *GT 50 *AND
   *VALUE System.Idle_CPU *GT 0 *AND *VALUE System.Wait_I/O *GT 0 *AND
   *VALUE System.Load_Average_5_Min *GT 1 ]]>
```

```
  </CRITERIA>
  <INTERVAL>000200</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

nt_situations.xml del sistema operativo Windows

```
<PRIVATECONFIGURATION>
<!--  Situation Description: One of the NT Logs is close to capacity  -->
<PRIVATESIT>
  <SITUATION>NT_Log_Space_Low_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Monitored_Logs_Report.%_Usage *GE 95 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Test if the NT Scheduler process is running -->
<PRIVATESIT>
  <SITUATION>NT_Missing_Scheduler_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *MISSING NT_Process.Process_Name *EQ ("schedule") ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percent of the Page File in use is too high -->
<PRIVATESIT>
  <SITUATION>NT_Paging_File_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Paging_File.%_Usage *GE 80 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percent of the Page File in use is rising  -->
<PRIVATESIT>
  <SITUATION>NT_Paging_File_Warning_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Paging_File.%_Usage *GE 75 *AND
   *VALUE NT_Paging_File.%_Usage *LT 80  ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percent of the time the disk drive is busy
is too high -->
<PRIVATESIT>
  <SITUATION>NT_Phys_Disk_Busy_Crit_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Physical_Disk.%_Disk_Time *GT 90 *AND
   *VALUE NT_Physical_Disk.Disk_Name *NE _Total ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percent of the time the disk drive is busy
is rising  -->
<PRIVATESIT>
  <SITUATION>NT_Phys_Disk_Busy_Warn_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Physical_Disk.%_Disk_Time *GT 80 *AND
   *VALUE NT_Physical_Disk.%_Disk_Time *LE 90 *AND
   *VALUE NT_Physical_Disk.Disk_Name *NE _Total  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percentage of processor time used is too high  -->
<PRIVATESIT>
  <SITUATION>NT_Proc_CPU_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Process.%_Processor_Time *GE 65 *AND *VALUE
```

```
   NT_Process.Priority_Base *NE 0 *AND *VALUE NT_Process.Process_Name
   *NE _Total  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percentage of processor time used is high  -->
<PRIVATESIT>
  <SITUATION>NT_Proc_CPU_Warn_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Process.%_Processor_Time *GE 50 *AND
   *VALUE NT_Process.%_Processor_Time *LT 65 *AND
   *VALUE NT_Process.Priority_Base *NE 0 *AND
   *VALUE NT_Process.Process_Name *NE _Total]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: A Service Error was reported  -->
<PRIVATESIT>
  <SITUATION>NT_Service_Error_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Event_Log.Source *EQ "Service Control Manager"
   *AND *VALUE NT_Event_Log.Type *EQ Error  ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Rate of operations to file system devices
per second is too high  -->
<PRIVATESIT>
  <SITUATION>NT_System_File_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_System.File_Data_Operations/Sec *GE 100000 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Rate of operations to file system devices per second
 is rising -->
<PRIVATESIT>
  <SITUATION>NT_System_File_Warn_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_System.File_Data_Operations/Sec *GE 10000 *AND
   *VALUE NT_System.File_Data_Operations/Sec *LT 100000  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

sy_situations.xml de Tivoli de resumen y poda de Data Warehouse

```
<PRIVATECONFIGURATION>
<!--  Situation Description: No connectivity to Warehouse database  -->
<PRIVATESIT>
  <SITUATION>KSY_DB_Connectivity_Fail_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KSY_CONNECTIVITY.DB_Connectivity *EQ No ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Failures occurred in pruning  -->
<PRIVATESIT>
  <SITUATION>KSY_Pruning_Failures_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KSY_SUMMARIZATION_STATISTICS.Pruning_Failures *GT 0 ]]>
  </CRITERIA>
  <INTERVAL>000000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Failures occurred in summarization  -->
```

```
<PRIVATESIT>
  <SITUATION>KSY_Summ_Failures_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KSY_SUMMARIZATION_STATISTICS.Summarization_Failures
   *GT 0  ]]>
  </CRITERIA>
  <INTERVAL>000000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: No connectivity to the
Tivoli Enterprise Portal Server  -->
<PRIVATESIT>
  <SITUATION>KSY_TEPS_Conn_Fail_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KSY_CONNECTIVITY.TEPS_Connectivity *EQ No  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

warehouse_situations.xml de Tivoli Data Warehouse

```
<PRIVATECONFIGURATION>
<!--  Situation Description: No connectivity to warehouse database  -->
<PRIVATESIT>
  <SITUATION>KHD_DB_Connectivity_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KHD_DB_INFO.DB_Connectivity *EQ No ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Critical errors during the execution
of the Warehouse Proxy  -->
<PRIVATESIT>
  <SITUATION>KHD_Error_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KHD_LAST_ERROR_DETAILS.Error_Severity *EQ Critical ]]>
  </CRITERIA>
  <INTERVAL>000000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Fatal errors during the execution
of the Warehouse Proxy  -->
<PRIVATESIT>
  <SITUATION>KHD_Error_Fatal_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KHD_LAST_ERROR_DETAILS.Error_Severity *EQ Fatal ]]>
  </CRITERIA>
  <INTERVAL>000000</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

Historial privado

El historial privado es la recopilación y el almacenamiento a corto plazo de los datos de un agente de supervisión local. Defina la recopilación histórica en un archivo de configuración de situaciones privadas para un agente y, a continuación, utilice la interfaz de servicio del agente para ver el historial a corto plazo.

El historial privado se configura en el archivo de configuración de situaciones privadas

La recopilación local de datos históricos se define en el archivo de configuración de situaciones privadas local para cada grupo para el que desea guardar datos históricos. Puede definir un historial privado con o sin situaciones de supervisión privadas. Solamente puede haber una recopilación de datos históricos activa por tabla de aplicaciones (grupo de atributos).

Utilice el código <HISTORY> para especificar cada grupo de atributos para el que desea recopilar datos históricos. Si lo desea, puede utilizar el parámetro EXPORT para especificar un intervalo en minutos para exportar datos a Tivoli Data Warehouse.

Utilice el código <WAREHOUSE> para especificar un Warehouse Proxy agent para el que hay que exportar datos.

Consulte el apartado “Especificación XML de situaciones privadas” en la página 351.

Registro de operaciones del agente
Todos los mensajes de error de validación de XML se guardan en el Registro de operaciones del agente. El historial privado es totalmente independiente y está separado de la recopilación de datos históricos y de la configuración de Tivoli Data Warehouse dentro de IBM Tivoli Management Services. Todos los datos de la tabla del historial a largo plazo residen en su propio archivo binario de historial.

Nombres de archivos históricos a corto plazo
El nombre de tabla de un grupo de atributo también es el nombre de archivo binario del historial con el prefijo **PVTHIST_**; un solo archivo binario de historial por tabla. Como parte de la configuración de historial privado, puede establecer el atributo RETAIN para gestionar el tamaño del archivo de historial. Puede configurar una ubicación de archivo de historial privado alternativo con el parámetro de configuración del agente CTIRA_HIST_DIR.

Directorio de archivos históricos a corto plazo
El agente coloca todos los archivos del historial privado en este subdirectorio:

Windows <dir_instalación> \TMAITM6\logs

Linux UNIX <dir_instalación>/<arch>/<cp>/hist

Puede configurar una ubicación de archivo de historial privado alternativo con el parámetro de configuración del agente CTIRA_HIST_DIR.

Mantenimiento de archivos históricos a corto plazo
Se proporcionan programas de utilidad de conversión de archivos históricos a corto plazo, como **krarloff** (KPDXTRA en z/OS), para mover datos de los archivos históricos a archivos de texto delimitado.

Consideraciones sobre z/OS
El recurso de Almacén de datos permanentes (PDS) del Tivoli Enterprise Monitoring Server en z/OS ofrece un mecanismo para que las aplicaciones de Tivoli Monitoring puedan acceder a datos históricos de la misma forma que a datos de tablas SQL. Los productos OMEGAMON XE aprovechan el recurso PDS para almacenar y recuperar datos históricos a través del componente PDS sin tener que utilizar Tivoli Management Services.

El diccionario de PDS contiene definiciones de tablas de aplicaciones.

- Cada tabla se identifica mediante un nombre de aplicación, generalmente el código de producto de la aplicación, el nombre de tabla y el grupo de archivos asignado.
- Las definiciones de las columnas de la tabla siguen la definición de la tabla e incluyen nombre de columna, tipo de datos, y longitud de datos. Las columnas de la tabla se relacionan con la tabla mediante el mismo identificador.

La siguiente definición de tabla de diccionario PDS de ejemplo procede de la tabla de KN3 KN3BPG del producto Tivoli OMEGAMON XE for Mainframe Network:

```
CREATE ID=N303 APPL=KN3      TABLE=KN3BPG     GROUP=KN3
ADDCOL ID=N303 COL=TMZDIFF    TYP=INTEGER    LEN=4    REQ
ADDCOL ID=N303 COL=WRITETIME  TYP=CHARACTER  LEN=16   BIT=72   REQ
ADDCOL ID=N303 COL=ORIGINNODE TYP=CHARACTER  LEN=32   REQ
ADDCOL ID=N303 COL=SYSID      TYP=CHARACTER  LEN=4    REQ
ADDCOL ID=N303 COL=TIMESTAMP  TYP=CHARACTER  LEN=16   REQ
ADDCOL ID=N303 COL=CATDESC    TYP=INTEGER    LEN=2    REQ
ADDCOL ID=N303 COL=CATPCT     TYP=INTEGER    LEN=4    REQ
ADDCOL ID=N303 COL=POOLNAME   TYP=CHARACTER  LEN=4    REQ
ADDCOL ID=N303 COL=CATEGORY   TYP=INTEGER    LEN=4    REQ
ADDCOL ID=N303 COL=SAMPLES    TYP=INTEGER    LEN=4    REQ
ADDCOL ID=N303 COL=INTERVAL   TYP=INTEGER    LEN=4    REQ
```

Una tabla pertenece a un grupo PDS y se asignan varios archivos VSAM para un grupo de archivos PDS para almacenar datos de la tabla. Se puede utilizar la sentencia OVERRIDE de PDS para modificar la tabla o la asignación de grupos (o ambos) y las propiedades. La especificación del grupo KN3 se ilustra a continuación:

```
OVERRIDE TABLE=KN3BPG APPL=KN3 WRAP=0 GROUP=KN3
GROUP=KN3 FILE=DSN:CCAPI.COMMON.NV.CIDSSP13.RKN3HIS3
GROUP=KN3 FILE=DSN:CCAPI.COMMON.NV.CIDSSP13.RKN3HIS2
GROUP=KN3 FILE=DSN:CCAPI.COMMON.NV.CIDSSP13.RKN3HIS1
```

PDS almacena datos de la tabla utilizando el nombre de aplicación, nombre de tabla, WRITETIME y las columnas indexadas como la clave de archivo de VSAM. Para historial privado, utilizando como ejemplo la tabla KN3BPG – VTAM_Buffer_Usage_By_Category, se necesitan los dos pasos siguientes de configuración:

1. Añada tablas de aplicación que requieran recopilación de datos históricos como tablas nuevas al diccionario PDS, en el conjunto de datos RKANPARU, miembro KN3PDICT:
   a. Haga una copia de la definición de la tabla KN3BPG.
   b. Cambie TABLE=KN3BPG por TABLE=ZN3BPG.
   c. Cambie ID=N303 por un ID exclusivo (por ejemplo, N399).
2. Añada la sentencia OVERRIDE de tablas de aplicación en el conjunto de datos RKANPARU, miembro KN3PG.
   a. Copie la sentencia OVERRIDE de la tabla KN3BPG, si la hay.
   b. Cambie TABLE=KN3BPG por TABLE=ZN3BPG.

Una vez finalizados los dos pasos de configuración, el historial privado se puede configurar y recuperar añadiendo la siguiente información a <cp>_situations.xml, tal como se muestra en este ejemplo:

```
<PRIVATECONFIGURATION>
 <HISTORY TABLE="VTAM_Buffer_Usage_By_Category" Interval="15" Retain="24" />
</PRIVATECONFIGURATION>
```

Ejemplo de solicitud de interfaz de servicio:

```
<HISTREAD>
 <SQLTABLE>
  <TABLENAME>KN3BPG</TABLENAME>
  <FILTER><![CDATA[ *VALUE WRITETIME  *GE 1090728020000000 *AND
   *VALUE WRITETIME  *LE 1090728080000000]]&gt;</FILTER>
  <OUTLIMIT>5000</OUTLIMIT>
 </SQLTABLE>
</HISTREAD>
```

PDS almacena y lee los datos de la tabla histórica de empresa y privada de los mismos conjuntos de datos VSAM utilizando la clave exclusiva. Como alternativa, puede asignar un historial privado a su propio grupo de archivos PDS y asignar conjuntos de datos VSAM separados para el grupo de historial privado.

Especificación XML de alteración temporal de situación de empresa

Puede alterar temporalmente los umbrales establecidos para una situación de empresa bajo demanda o mediante una planificación. Si define alteraciones temporales de situación en la especificación XML de umbrales del Tivoli Enterprise Monitoring Agent, puede gestionarlos localmente.

Atención: Esta información no es aplicable a situaciones privadas. Para obtener más información sobre situaciones privadas, consulte "Especificación XML de situaciones privadas" en la página 351.

Cualquier actualización realizada en el archivo de umbrales XML local entra en vigor cuando se reinicia el agente. Las alteraciones temporales de situación que pasan a través del Tivoli Enterprise Monitoring Server (definidos en Tivoli Enterprise Portal o con el mandato de CLI tacmd setOverride) o aplicados a través de la Interfaz de servicio del agente entran en vigor de inmediato.

Después de leer el documento XML, el agente sincroniza las especificaciones de alteración temporal de umbral definidas con todas las solicitudes de recopilación de datos de todas las definiciones de tablas definidas. Todos los parámetros de umbral, calendario y actualización y supresión de situaciones tienen efecto de forma inmediata. El agente envía todo el documento XML de especificación de alteración temporal de umbral al archivo de umbral local nombrado.

Nombre de archivo y vía de acceso de alteración temporal de situación predeterminada

Windows *dir_instalación*\TMAITM6*pc*_thresholds.xml

Linux UNIX *dir_instalación*/bin/*pc*_thresholds.xml

z/OS *PC*THRESH en el conjunto de datos RKANDATV

IBM i ctira_sit_path/hostname_pc_thresholds.xml

Consulte "Alteraciones temporales de expresiones de situaciones" en la página 340 para ver las variables de entorno del agente que habilitan la operación de alteración temporal de situaciones locales.

Debe crear y escribir manualmente definiciones de alteraciones temporales en el mismo archivo que se crea en modalidad CENTRAL. Los nombres de las columnas que se utilizarán al especificar alteraciones temporales se toman del archivo de atributos (como C:\ibm\ITM\TMAITM6\ATTRLIB\knt.atr para el agente de SO Windows).

Otra forma de buscar los nombres de las columnas que se utilizarán al especificar alteraciones temporales es mediante ASI. Abra ASI > Consultas y seleccione el nombre de la tabla. ASI devuelve un esquema de tabla completa que incluye el nombre de visualización de la tabla y los nombres de visualización de todas las columnas de la tabla.

Elementos

Especifique todos los valores entre comillas, por ejemplo, "NT_Available_Bytes_Warning").

<OVERRIDE>
Las etiquetas <override> de inicio y </override> de fin definen este documento como un documento de configuración de umbral dinámico.

ObjName=
Especifique el nombre del documento de alteración temporal de situación.

<CALENDAR>
Opcional. Especifique la definición del calendario nombrado. Como alternativa, puede especificar una alteración temporal planificada en el elemento <threshold>.

Name=
Especifique el nombre del calendario simbólico.

Action=
Opcional. Especifique la disposición de la definición del calendario. El valor Update crea o sustituye el calendario nombrado. El valor Delete elimina el calendario nombrado existente.

Start= Stop=
Opcional. Utilice estos atributos para aplicar la alteración temporal comenzando por la misma hora y durante la misma duración. Por ejemplo, start="08:15" stop="17:30" hace que la alteración temporal entre en vigor durante el periodo comprendido entre 8:15 AM y 5:30 PM; start="21:45"" stop="05:15" hace que la alteración temporal entre en vigor entre las 9:45 PM y las 5:15 AM al día siguiente. Si calendar= no está definido, se utilizan los valores start=, stop= y cron=.

Cron= Opcional. Especifique una definición de hora en formato **minuto hora día mes día-de-la-semana**, donde **minuto** está comprendido entre 0 y 59, **hora** está comprendido entre 0 y 23, **día** está comprendido entre 1 y 31, **mes** está comprendido entre 1 y 12 y **día-de-la-semana** está comprendido entre 0 y 6 (domingo puede ser 0 ó 7). Separe cada campo por un espacio y utilice cualquier combinación de estos símbolos:

- Utilice un asterisco (*) para indicar cualquier valor válido para el campo. Por ejemplo, * en el campo de mes significa cada mes.
- Especifique varios valores de campo separados por una coma (,).
- Utilice un guión (-) para indicar un rango de valores.
- También se pueden utilizar nombres para los campos **mes** y **día-de-la-semana**. Utilice las tres primeras letras de un día o mes concreto.
- Un valor precedido de una barra inclinada (/) es el número que hay que salta. Por ejemplo, */3 en el campo de hora significa cada tres horas o (0,3,6,9,12,15,18,21). Este tipo de valor no es válido para el campo de minuto.

La definición CRON debe especificar un rango de tiempo (hora de inicio a hora final). Si calendar= no está definido, se utilizan los valores start=, stop= y cron=.

LastUpdate=
Opcional. Indicación de fecha y hora de 16 dígitos de la última actualización. La indicación de fecha y hora se ignora si es anterior a la indicación de fecha y hora establecida existente. Valor predeterminado: **0 0 0 0 0**.

ObjName=
Opcional. Especifique el nombre del documento de alteración temporal.

<SITUATION>
Defina la configuración del umbral de situación.

Name=
Especifique el nombre de la situación.

Table=
Opcional. Especifique el nombre de la tabla de atributos si prefiere utilizar el nombre de atributo para la definición de clave o de umbral, en lugar del nombre de columna de tabla. Utilice el nombre de tabla SQL o el nombre de tabla de atributos.

Action=
Opcional. Especifique la disposición de la definición de la situación. Si la especificación no existe, el valor Update crea la especificación de la situación; de lo contrario, se modifican las alteraciones temporales coincidentes. El valor Delete elimina toda la especificación de la alteración temporal de situación.

LastUpdate=
Opcional. Indicación de fecha y hora de 16 dígitos de la última actualización. Se ignora si es anterior a la indicación de la hora actual.

Calendar=
Opcional. Especifique una definición de calendario con nombre. El calendario se aplica a todos los umbrales de esta situación.

Priority=
Prioridad de la alteración temporal de situación. Un valor numérico menor indica una prioridad mayor. El agente sustituye la alteración temporal de prioridad menor por la actualización de prioridad superior y rechaza una actualización cuya prioridad es igual. Valor predeterminado: 2147483647

ObjName=
Opcional. Especifique el nombre del documento de la alteración temporal.

<KEY> o <TRIGGER>
Opcional. Defina una columna de tabla que contenga un valor de datos que diferencie de forma exclusiva una fila de datos en una muestra de varias filas. Las definiciones <key> anidadas implican una condición AND; las definiciones <key> del mismo nivel implican una condición OR.

Column=
Nombre de la columna. Por ejemplo, *column=USAGE*. Si tiene subagentes sobre los que desea aplicar una alteración temporal, especifique una columna ORIGINNODE como la clave y el nombre del subnodo de sistema gestionado como el valor de la clave.

Attr= Nombre del atributo. Como alternativa a especificar un nombre de columna, puede especificar el nombre del atributo. Si utiliza el nombre del atributo, debe especificar el nombre de la tabla en el elemento

<situation> o especificar el nombre del atributo en el formato **nombre-tabla.nombre-atributo**, como por ejemplo *attr=NT_Paging_File.%_usage*.

Value=
Valor de datos de filtro de atributos o columna. El valor de atributo también se puede especificar entre las etiquetas de inicio y de fin sin utilizar el parámetro Value. No obstante, se prefiere el estilo de parámetro.

<THRESHOLD>
Defina la especificación de umbral.

Column=
Nombre de la columna. Por ejemplo, *column=CONATTMP*.

Attr= Nombre del atributo. Como alternativa a especificar un nombre de columna, puede especificar el nombre del atributo. Si utiliza el nombre del atributo, debe especificar el nombre de la tabla en el elemento <situation> o especificar el nombre del atributo en el formato **nombre-tabla.nombre-atributo**, como por ejemplo *attr=HTTP_Service.Connection_Attempts*.

Position=
Opcional. Posición de la secuencia de atributos en la construcción lógica de la situación. Comienza por el valor 1. El valor cero (0) implica toda la ocurrencia del atributo en la lógica de situación conjuntiva y/o disyuntiva. Este parámetro resulta útil para especificar un atributo de alteración temporal determinado en una lógica que contenga varias ocurrencias del mismo atributo. Por ejemplo A1 > 80% AND A2 < 95%. Valor predeterminado: **0**

Operator=
Opcional. Operador lógico que define de forma exclusiva un atributo en la construcción de una situación que contenga varias ocurrencias del mismo atributo. Los valores de los operadores son: EQ, NE, GE, LE, GT, LT. En el ejemplo anterior, A1 también se puede calificar mediante Operator=GT.

Value=
Valor de columna o de umbral de atributo. El valor de atributo también se puede especificar entre las etiquetas de inicio y de fin sin utilizar el parámetro Value. No obstante, se prefiere el estilo de parámetro.

Calendar=
Opcional. Especifique una definición de calendario con nombre. El calendario altera temporalmente cualquier calendario especificado en el elemento <situation> y en cualquier atributo start=, stop= y cron=.

Start= Stop=
Opcional. Utilice estos atributos para aplicar la alteración temporal comenzando por la misma hora y durante la misma duración. Por ejemplo, start="08:15" stop="17:30" hace que la alteración temporal entre en vigor durante el periodo comprendido entre 8:15 AM y 5:30 PM; start="21:45"" stop="05:15" hace que la alteración temporal entre en vigor entre las 9:45 PM y las 5:15 AM al día siguiente. Si calendar= no está definido, se utilizan los valores start=, stop= y cron=.

Cron= Opcional. Especifique una definición de hora en formato **minuto hora día mes día-de-la-semana**, donde **minuto** está comprendido entre 0 y

59, **hora** está comprendido entre 0 y 23, **día** está comprendido entre 1 y 31, **mes** está comprendido entre 1 y 12 y **día-de-la-semana** está comprendido entre 0 y 6 (domingo puede ser 0 ó 7). Separe cada campo por un espacio y utilice cualquier combinación de estos símbolos:

- Utilice un asterisco (*) para indicar cualquier valor válido para el campo. Por ejemplo, * en el campo de mes significa cada mes.
- Especifique varios valores de campo separados por una coma (,).
- Utilice un guión (-) para indicar un rango de valores.
- También se pueden utilizar nombres para los campos **mes** y **día-de-la-semana**. Utilice las tres primeras letras de un día o mes concreto.
- Un valor precedido de una barra inclinada (/) es el número que hay que salta. Por ejemplo, */3 en el campo de hora significa cada tres horas o (0,3,6,9,12,15,18,21). Este tipo de valor no es válido para el campo de minuto.

La definición CRON debe especificar un rango de tiempo (hora de inicio a hora final). Si calendar= no está definido, se utilizan los valores start=, stop= y cron=.

<DEFAULT>
Opcional. Defina uno o varios umbrales de filtro predeterminados que se aplicarán a varias muestras de filas. Es lo deseable si se han definido etiquetas <key>.

Ejemplo

```
<overrides>
  <situation name="Check_Event" table="NT_Event_Log">
    <threshold attr="Source"
               value="Symantec Antivirus"
               start="08:00" stop="17:00" />
  </situation>
  <situation name="NT_Available_Bytes_Critical" table="NT_Memory">
    <threshold attr="Available_Bytes"
               value="750000"
               start="08:00" stop="17:30"
               cron=" * * * * 1-5" />
  </situation>
  <situation name="NT_Disk_Space_Low">
   <threshold name="FREEMGBTES"
               value="10"
               cron="31-59 8-20 */2 * *"
    </threshold>
  </situation>
  <situation name="NT_Log_Space_Low">
      <threshold name="USAGE"
                 value="75"
                 start="08:00" stop="18:00"
                 cron="* * * * MON,WED,FRI"
     </threshold>
  </situation>
  <situation name="Message_Queue_Warning" table="Queue_Statistics">
    <KEY column="ORIGINNODE" value="SYSG:NETQ3">
      <threshold attr="Queue_Depth"
                 value="10"
                 cron="0-30 8-17 * 3,6,9,12 *"
      </threshold>
    </KEY>
  </situation>
  <situation name="NT_Process_CPU_Critical" table="NT_Process">
```

```
    <KEY attr="Process_Name" value="_Total">
      <threshold attr="%_Processor_Time"
                 value="70"
                 start="06:00" stop="21:30"
                 cron="* * * * 1-5" />
    </KEY>
  </situation>
  <situation name="NT_System_File_Critical" table="NT_System">
      <threshold attr="File_Data_Operations/Sec"
                value="50000"
                cron="* 6-22 * * SAT,SUN"
      </threshold>
  </situation>
  <situation name="DISKFULL">
    <key column="INSTCNAME" value="C:">
      <threshold column="PCFREE">5</threshold>
    </key>
    <key column="INSTCNAME" value="D:">
      <threshold column="PCFREE">10</threshold>
    </key>
    <default>
    <threshold column="PCFREE">0</threshold>
    </default>
  </situation>
  <situation name="Windows_Events">
    <key column="SOURCE" value="MSFTPSVC">
    <key column="EVENTID" value="10">
      <threshold column="SOURCE">MSFTPSVC</threshold>
    </key>
    <key column="EVENTID" value="100">
      <threshold column="SOURCE">MSFTPSVC</threshold>
    </key>
    </key>
    <key column="SOURCE" value="EventLog">
    <key column="EVENTID" value="6005">
      <threshold column="SOURCE">EventLog</threshold>
    </key>
    <key column="EVENTID" value="6009">
      <threshold column="SOURCE">EventLog</threshold>
    </key>
    </key>
    <default>
      <threshold column="SOURCE">NOPASS</threshold>
    </default>
  </situation>
</overrides>
```

Alertas SNMP

Los agentes de Tivoli Enterprise Monitoring y los agentes de Tivoli System Monitor se pueden configurar de modo que envíen alertas a un receptor de SNMP como Netcool/OMNIbus, mediante la prueba Netcool/OMNIbus SNMP o Tivoli NetView. Se proporcionan archivos de reglas OMNIbus de ejemplo para ilustrar ciertas ideas clave de integración.

Configuración de alertas de SNMP

Configuración de un agente de supervisión y de un archivo de configuración de condiciones de excepción SNMP para emitir sucesos de ciclo de vida o sucesos de situación a un receptor de sucesos SNMP.

Archivo de configuración de condiciones de excepción

Debe haber un archivo de configuración de condiciones de excepción cuando se inicia el agente para permitir que el agente emita condiciones de

excepción SNMPv1/v2 o informes SNMPv3 para situaciones configuradas. Si hay un archivo trapcnfg.xml con el nombre correcto en el directorio de configuración local del agente, este emite las condiciones de excepción definidas en el archivo cuando se inicia. El archivo se denomina *cp*_trapcnfg.xml, donde *cp* es el código de producto de 2 caracteres del agente y reside en el directorio *dir_instalación*/localconfig/*cp*. El archivo debe denominarse *pc*_trapcnfg.xml, donde *pc* es el código de producto de dos caracteres, como por ejemplo ux para el agente del SO UNIX.

IBM i El agente IBM i puede enviar condiciones de excepción SNMPv1/v2, pero no puede enviar informes SNMPv3.

z/OS En z/OS, el nombre predeterminado del archivo es *P*CTRAPS en el conjunto de datos RKANDATV.

Parámetros del agente

El parámetro **IRA_EVENT_EXPORT_SNMP_TRAP_CONFIG** del archivo de entorno del agente se puede establecer de modo que especifique otro nombre y vía de acceso para el archivo de configuración de condiciones de excepción. Solo se emiten alertas SNMP para situaciones configuradas en el archivo XML de configuración de condiciones de excepción para dicho tipo de agente. Puede especificar la vía de acceso completa o la vía de acceso relativa al directorio de configuración local.

Para especificar la vía de acceso completa, el PDS debe aparecer listado al final (o bien omitido, adoptando como valor predeterminado RKANDATV).

IRA_EVENT_EXPORT_SNMP_TRAP=N inhabilita las alertas SNMP del agente aunque exista el archivo *cp*_trapcnfg.xml.

Especificación XML

El archivo de configuración de condiciones de excepción puede incluir estos elementos XML:

SNMP

TrapDest

TrapAttrGroup

Situation

StatTrap

SNMP es el elemento XML de nivel superior. TrapDest, TrapAttrGroup y Situation son elementos dentro de las etiquetas SNMP de inicio y fin.

Archivo de configuración de condiciones de excepción de ejemplo

Revise este archivo nt_trapcnfg.xml de ejemplo para un agente de sistema operativo Windows para ver cómo se puede crear un archivo de configuración de condiciones de excepción. Se encuentra en el directorio *dir_instalación*\localconfig\nt para habilitar la emisión de condiciones de excepción para el agente de sistema operativo Windows. El archivo está configurado para enviar condiciones de excepción de estatus a un Tivoli Universal Agent que supervisa condiciones de excepción SNMPv1 en el host nt2003infra y para enviar informes para todos los sucesos de situación definidos individualmente a una prueba SNMP de Netcool/OMNIbus mediante SNMPv3 que se ejecuta en el host 10.21.32.234.

```
<!–C:\IBM\ITM\localconfig\nt\nt_trapcnfg.xml /-->
<SNMP>
   <TrapDest name="UAStatMon" Address=" nt2003infra " Version="v1"
   Community="{AES256:keyfile:a}P0hUrmUhCgfFwimS+Q6w+w==" Stat="Y" />
```

```
<TrapDest name="Probe1" Version="v3" Address="10.21.32.234"
SecLevel="authPriv" User="AuthPrivMD5DES" AuthType="MD5"
AuthPassKey="{AES256:keyfile:a}yifHSbFcTKHBqvORpzxS6A=="
PrivType="DES" PrivPassKey=
"{AES256:keyfile:a}1le2SxljJR1MOIi0EDIvig==" Stat="N" />

<TrapAttrGroup Table="NT_Paging_File" TrapAttrList="Server_Name,
%_Usage" />

<Situation name="NT_Log_Space_Low_pr" sev="2" cat="0"
mode="HY"
target="Probe1" />
<Situation name="NT_Missing_Scheduler_pr" sev="5" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_Paging_File_Critical_pr" sev="5" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_Paging_File_Warning_pr" sev="2" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_Phys_Disk_Busy_Critical_pr" sev="5" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_Phys_Disk_Busy_Warn_pr" sev="2" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_System_File_Warn_pr" sev="2" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_Proc_CPU_Critical_pr" sev="5" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_Proc_CPU_Warn_pr" sev="2" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_Service_Error_pr" sev="2" cat="0"
mode="RC" target="Probe1" />
<Situation name="NT_System_File_Critical_pr" sev="5" cat="0"
mode="HY" target="Probe1" />
<Situation name="NT_System_File_Warn_pr" sev="2" cat="0"
mode="HY" target="Probe1" />

<StatTrap name="EE_HEARTBEAT" sev="1" interval="15" cat="3" />
<StatTrap name="EE_AUTO_ENTER" sev="1" cat="3" />
<StatTrap name="EE_AUTO_EXIT" sev="1" cat="3" />
<StatTrap name="EE_AUTO_USE_LIMIT" sev="5" cat="3" />
<StatTrap name="EE_TEMS_RECONNECT_LIMIT" sev="5" cat="3" />
<StatTrap name="EE_TEMS_CONNECT" sev="1" cat="4" />
<StatTrap name="EE_TEMS_DISCONNECT" sev="1" cat="4" />
<StatTrap name="EE_SIT_STOPPED" sev="1" cat="4" />
</SNMP>
```

Especificación XML del elemento Trap

Utilice los elementos SNMP, TrapDest, TrapAttrGroup, Situation y StatTrap en archivos XML de SNMP para configurar condiciones de excepción para cualquier tipo de agente que desee especificar para el receptor de sucesos.

Las etiquetas XML no son sensibles a mayúsculas y minúsculas. Los demás parámetros son sensibles a mayúsculas y minúsculas. Por ejemplo, puede escribir ADDRESS, Address o address.

Elemento SNMP

El elemento SNMP de la especificación XML de la configuración de la condición de excepción es el elemento XML de nivel superior. TrapDest, TrapAttrGroup y Situation son elementos dentro de las etiquetas SNMP de inicio y fin.

```
<SNMP>
 <TrapDest name="OMNIbus2" Address="nswin21a" Stat="Y" />
 <situation name="*" target="OMNIbus2" />
</SNMP>
```

Elemento TrapDest

Utilice los elementos TrapDest de un archivo XML de configuración de condiciones de excepción para definir un receptor de condiciones de excepción.

El elemento TrapDest requiere los atributos name y address. Para cualquier otro atributo que no se especifiquen se utilizan los valores predeterminados.

```
<TrapDest name="LABEL" Address="HOSTNAME"/>
```

Tabla 30. Especificación XML del elemento TrapDest

Atributo	Descripción	Necesario	Valor predeterm.	SNMPv1/v2 o SNMPv3
Name=	Etiqueta alfanumérica que se utiliza para identificar el destino de la condición de excepción.	Necesario		
Address=	La dirección TCP/IP o el nombre de host del receptor de la condición de excepción.	Necesario		Todos
IP=	Protocolo IP: “4” | “6” 4 es IPv4; 6 es IPv6	Opcional	"4"	Todos
Port=	Puerto de escucha de la condición de excepción de TCP/IP del receptor de condiciones de excepción.	Opcional	"162"	Todos
BindAddress=	Se utiliza para especificar qué interfaz local se ha de utilizar para el tráfico SNMP. La interfaz especificada debe coincidir con el valor IP.	Necesario si el host tiene definidas varias interfaces de red. De lo contrario, el envío de condiciones de excepción puede fallar con el error número 22.	Primero disponible	Todos
Version=	Especifique la versión de la condición de excepción SNMP. Los valores de cadenas válidos son (no distinguen entre mayúsculas y minúsculas): **v1**, **v2**, **v3**.	Opcional	v1	Todos
Type=	Trap | Inform. El tipo debe coincidir con la versión. Version= “v1” | “v2”. El tipo debe ser “Trap”. Version= “3”. El tipo debe ser “Inform”.	Opcional	Coincide con la versión	Todos

Tabla 30. Especificación XML del elemento TrapDest (continuación)

Atributo	Descripción	Necesario	Valor predeterm.	SNMPv1/v2 o SNMPv3
Stat=	Stat se utiliza en un destino para enviar todas las condiciones de excepción a dicho receptor cuando Stat="Y". Establezca Stat en "N" para inhabilitar todas las alertas de estatus para TrapDes. Establézcalo en "N" si solo desea que se envíe un subconjunto de alertas de estatus a TrapDest. Se pueden enviar alertas de estatus individuales a un TrapDest específico utilizando el elemento StatTrap.	Opcional	"Y"	Todos
Community=	Especifique la cadena de nombre de comunidad de la condición de excepción. Se debe cifrar mediante itmpwdsnmp, pero el texto plano también está permitido. (Entre 1-63 caracteres.)	Opcional	public	v1 y v2
SecModel=	Especifique el modelo de seguridad. Sólo está soportado USM.	Opcional	USM	v3
SecLevel=	Especifique los niveles de autenticación y privacidad. Los niveles soportados son: **noAuthNoPriv** – sin autenticación y sin privacidad. **authNoPriv** – autenticación, sin privacidad **authPriv** – autenticación y privacidad (no soportado en agentes de supervisión z/OS)	Necesario para v3.		v3
User=	Especifique el nombre de cuenta	Necesario para v3		v3
AuthType=	Especifique el protocolo de autenticación. Los protocolos soportados son: MD5 y SHA	Necesario para v3; SecLevel= authNoPriv o authPriv		v3

Tabla 30. Especificación XML del elemento TrapDest (continuación)

Atributo	Descripción	Necesario	Valor predeterm.	SNMPv1/v2 o SNMPv3
AuthPassKey=	Especifique la contraseña de autenticación. Se debe cifrar mediante itmpwdsnmp, pero el texto plano también está permitido. (Entre 1-63 caracteres.)	Necesario para v3; SecLevel= authNoPriv o authPriv		v3
PrivType=	Especifique el protocolo de privacidad. El protocolo soportado es DES.	Necesario para v3 SecLevel= authPriv		v3
PrivPassKey=	Especifique la contraseña de privacidad. Se debe cifrar mediante itmpwdsnmp, pero el texto plano también está permitido. (Entre 1-63 caracteres.)	Necesario para v3 SecLevel= authPriv		v3
Timeout=	Especifique el tiempo de espera (en segundos y un entero) para el reconocimiento del mensaje SNMPv3 (mínimo 1).	Opcional	2	v3
Retries=	Especifique el número de retransmisiones cuando se produce un tiempo de espera (mínimo 0 y máximo 5).	Opcional	3	v3

Elemento TrapAttrGroup

Utilice el elemento TrapAttrGroup en un archivo trapcnfg.xml para especificar qué atributos de un grupo de atributos se han de incluir en las condiciones de excepción de los sucesos de situación.

En el ejemplo de sintaxis, las situaciones escritas para el grupo de atributos de archivo de paginación del sistema operativo Windows enviarán al receptor de sucesos una condición de excepción SNMP con los valores de nombre del servidor, porcentaje de uso y punta de uso.

```
<TrapAttrGroup Table="NT_Paging_File" TrapAttrList="Server_Name,
%_Usage,%_Usage_Peak" />
```

Este elemento se puede utilizar para disminuir la cantidad de datos de atributos enviados en cada solicitud de condición de excepción, para reducir la fragmentación de las condiciones de excepción y para reducir los datos de modo que únicamente incluyan lo que es relevante.

El elemento TrapAttrGroup establece los atributos predeterminados que se enviarán para todas las situaciones que se ejecutan en la tabla. Las situaciones

individuales pueden alterar temporalmente los valores TrapAttrGroup especificando un atributo TrapAttrList en el elemento de situación.

Si no se define un elemento TrapAttrGroup para una tabla de atributos, todos los atributos de la fila de datos de la situación se añaden al sitAttributeList varbind de las condiciones de excepción enviadas para las situaciones basadas en esta tabla de atributos. Los atributos utilizados en el predicado situation se añaden en primer lugar y los atributos restantes se van añadiendo hasta que se alcanza la longitud máxima de PDU que es de 1500 bytes.

Tabla 31. Especificación XML del elemento TrapAttrGroup

Atributo	Descripción
Table=	El nombre de la tabla de atributos. Para crear manualmente este archivo, puede consultar el archivo de atributos del agente, *cp*.atr, para identificar los nombres de tablas, donde *cp* es el código de producto de dos caracteres.
TrapAttrList=	Una lista de atributos delimitados por comas que se incluirá en **sitAttributeList varbind** de las condiciones de excepción enviadas para la situación.

Elemento Situation

Utilice los elementos Situation de un archivo XML de configuración de condiciones de excepción para definir la condición de excepción enviada para la situación.

```
<situation name="Situation_ID" target="TrapDest_Name" />
```

El elemento Situation requiere los atributos name y target. Para cualquier otro atributo que no se especifiquen se utilizan los valores predeterminados. El comodín de asterisco, *, se puede especificar para el elemento name, para el elemento target o para ambos elementos:

- Si se especifica el comodín para el nombre de situación representa a todas las situaciones. El siguiente ejemplo envía condiciones de excepción para todas las situaciones verdaderas definidas en el TrapDes definido con el nombre trapProbe1:

  ```
  <situation name="*" target="trapProbe1" />
  ```

  El comportamiento en modalidad Hysteresis no se puede especificar si se utiliza un carácter comodín * para el nombre de la situación.
- Si se especifica el comodín para el parámetro target, se habilita el envío de la situación especificado en el campo de nombre de situación a todos los destinos definidos:

  ```
  <situation name="NT_Disk_Low" target="*" />
  ```
- Si se especifica el comodín para el nombre y el destino de la situación se habilita el envío de todas las condiciones de excepción a todos los receptores de condiciones de excepción definidos.
- Las situaciones con nombre tienen prioridad sobre las definiciones con comodines. Si una definición de situación incluye un comodín y otra definición de situación nombra una situación o el destino, se utilizará la primera aparición de la definición de situación con nombre. Ejemplo:

  ```
  <TrapDest name="MyReceiver" Address="UAHOST1" Version="v1" />
  <TrapDest name="OMNIbus1" Address="OMNIbus1" Version="v2"
   Community="{AES256:keyfile:a}P0hUrmUhCgfFwimS+Q6w+w==" />
  <TrapDest name="OMNIbus2" Version="v3" Address="9.42.10.164"
   SecLevel="authPriv" User="SnmpUser" AuthType="SHA"
   AuthPassKey="{AES256:keyfile:a}vgpNvf5Vx3XbPj1sKRRvYg==" PrivType="DES"
  ```

```
 PrivPassKey="{AES256:keyfile:a}OK5YOWvRIkPOw9k4JRy9ag==" />
<situation name="*" target="OMNIbus2" />
<situation name="My_Missing_Process" target="MyReceiver" />
<situation name="NT_AA_Missing_Test" target="OMNIbus1" />
<situation name="NT_AA_Missing_Test" target="OMNIbus2" />
<situation name="NT_ABC_Missing_Test" target="*" />
```

La situación **My_Missing_Process** envía una condición de excepción a **MyReceiver**, en lugar de a **OMNIbus2**. Y **NT_ABC_Missing_Test** se envía a **MyReceiver**, **OMNIbus1** y **OMNIbus2**, en lugar de únicamente a **OMNIbus2** porque la situación se ha definido de forma explícita y no mediante el uso de comodines.

Si se define una situación más de una vez, la primera aparición de una definición de situación tiene prioridad. Si se vuelve a observar el ejemplo, **NT_AA_Missing_Test** se envía a **OMNIbus1** y no a **OMNIbus2** porque la primera aparición de la definición para la misma situación especifica **OMNIbus1**.

Tabla 32. Especificación XML del elemento Situation

Atributo	Descripción	Necesario	Valor predeterminado
Name=	Este es el ID o nombre corto de la situación.	Necesario	
Target=	Especifique un TrapDest definido previamente. El uso del asterisco, "*", implica el envío de la condición de excepción a todos los destinos definidos.	Necesario	
Sev=	Especifique una gravedad para la condición de excepción. Las gravedades de las condiciones de excepción son: 0 – Borrada 1 – Indeterminada 2 – Aviso 3 – Leve 4 – Grave 5 – Crítica	Opcional	2
Cat=	Especifique la categoría de la condición de excepción. Las categorías estándar de las condiciones de excepción son: 0 - Umbral 1 – Topología de red 2 – Error 3 – Estatus 4 – Configuración de nodo 5 – Alerta de aplicación 6 – Todas las categorías 7 – Sólo registro 8 – Correlación 9 – Ignorar	Opcional	0

Tabla 32. Especificación XML del elemento Situation (continuación)

Atributo	Descripción	Necesario	Valor predeterminado
Mode=	Se utiliza para especificar el comportamiento para la emisión de condiciones de excepción SMNP en situaciones muestreadas. Las modalidades estándar son: RC – (Rising Continuous), en la que se envían condiciones de excepción cada vez que el valor de la evaluación de una situación es true. (Los sucesos puros siempre son RC.) No se enviarán una condición de excepción específica de borrado. HY – (Hysteresis), en la que se envía una condición de excepción la primera vez que la evaluación de una situación muestreada da como resultado true. Una condición de excepción de borrado se enviará cuando el valor muestreado ya no cumpla con el criterio de la situación. La modalidad Hysteresis requiere que la situación tenga un nombre, no que se especifique con un carácter comodín *.	Opcional	RC
Pred=	El predicado (fórmula) de la situación se envía al autoSit-Predicates varbind de la condición de excepción. El atributo Pred le permite omitir el predicado de la situación estableciendo Pred="N". Esto puede resultar útil si no le importa recibir el predicado o si un predicado complejo ocupa demasiado PDU de la condición de excepción, y desea más espacio para enviar los atributos de la situación en el sitAttributeList varbind.	Opcional	Y
Table=	Nombre de tabla del grupo de atributos. Se utiliza con TrapAttrlist para identificar un subconjunto de atributos utilizados para construir **sitAttributeList varbind**.	Solo se necesita si se utiliza **TrapAttrList**.	

Tabla 32. Especificación XML del elemento Situation (continuación)

Atributo	Descripción	Necesario	Valor predeterminado
TrapAttrList=	Una lista de atributos delimitados por comas que se incluirá en el sitAttributeList varbind de las condiciones de excepción enviadas para la situación. Los valores especificados aquí alterarán temporalmente cualquier valor TrapAttrList especificado en un elemento TrapAttrGroup para la tabla en que se está ejecutando la situación.	Opcional	

Nota: Las situaciones para los grupos de atributos de varias filas que incluyen un elemento de visualización están limitados al envío de una condición de excepción para la primera fila que se evalúa en true, pero no para las filas siguientes.

StatTrap

Utilice el elemento StatTrap de un archivo de configuración de condiciones de excepción SNMP para modificar la configuración predeterminada de las condiciones de excepción del ciclo de vida del agente predefinido.

En el ejemplo de sintaxis, la condición de excepción predefinida para EE_HEARTBEAT se ha modificado para que especifique la gravedad 1 (Indeterminada) para el suceso, un intervalo de muestreo de 30 minutos y una categoría de condición de excepción de 3 (Estatus).

```
<StatTrap name="EE_HEARTBEAT" sev="1" interval="30" cat="3" />
```

Estas son ocho condiciones de excepción de ciclo de vida del agente predefinidas y sus valores predeterminados se proporcionan en esta tabla. De forma predeterminada, estas condiciones de excepción se envían a todos los destinos de condición de excepción TrapDest en los que el atributo Stat es `"Y"`. Si se omite el atributo Stat de un elemento TrapDest, el valor predeterminado es `"Y"`.

Tabla 33. Condiciones de excepción de estatus de ciclo de vida del agente

Atributo	Descripción	Gravedad	Categoría
EE_HEARTBEAT	Un latido indica que el agente se está ejecutando y que se emiten sucesos para el destino de la condición de excepción. Esta es la única condición de excepción con un intervalo establecido de 15 minutos.	1 – Indeterminada	3 – Estatus
EE_AUTO_ENTER	El agente ha entrado en modalidad autónoma.	1 – Indeterminada	3 – Estatus
EE_AUTO_EXIT	El agente ha salido de la modalidad autónoma.	1 – Indeterminada	3 – Estatus
EE_AUTO_USE_LIMIT	El agente ha alcanzado el límite de almacenamiento especificado mediante la variable de entorno IRA_AUTONOMOUS_LIMIT. Es posible que durante la reconexión no se carguen los sucesos adicionales generados mientras el agente ha estado desconectado del servidor de supervisión.	1 – Indeterminada	3 – Estatus

Tabla 33. Condiciones de excepción de estatus de ciclo de vida del agente (continuación)

Atributo	Descripción	Gravedad	Categoría
EE_TEMS_RECONNECT _LIMIT	El agente ha alcanzado el límite de reintentos especificado mediante la variable de entorno CTIRA_MAX_TRIES. El agente ya no intentará conectarse a un servidor de supervisión y concluirá. En IBM Tivoli Monitoring 6.2.2 o posteriores, el valor predeterminado de CTIRA_MAX_RECONNECT_TRIES se ha modificado a 0, por lo tanto, el agente no concluirá nunca.	1 – Indeterminada	3 – Estatus
EE_TEMS_CONNECT	El agente se ha conectado correctamente al servidor de supervisión.	1 – Indeterminada	4 – Configuración de nodo
EE_TEMS_DISCONNECT	El agente ha perdido la conexión con el servidor de supervisión.	1 – Indeterminada	4 – Configuración de nodo
EE_SIT_STOPPED	La situación se ha detenido.	1 – Indeterminada	4 – Configuración de nodo

Utilice el elemento StatTrap para configurar las condiciones de excepción del ciclo de vida del agente.

Tabla 34. Especificación XML del elemento StatTrap

Condición de excepción Estatus	Descripción	Necesario	Valor predeterminado
Name=	Este nombre de condición de excepción debe ser el nombre de una condición de excepción Estatus de ciclo de vida. EE_HEARTBEAT EE_AUTO_ENTER EE_AUTO_EXIT EE_AUTO_USE_LIMIT EE_TEMS_RECONNECT_LIMIT EE_TEMS_CONNECT EE_TEMS_DISCONNECT EE_SIT_STOPPED	Opcional	
Target=	Especifique un TrapDest definido previamente. Un asterisco, (*), implica el envío de la condición de excepción a todos los destinos definidos. Si no se define target, todos los TrapDest que tengan Stat=”Y” recibirán la condición de excepción Estatus.	Necesario	
Sev=	Especifique una gravedad para la condición de excepción. Las gravedades de las condiciones de excepción son: 0 – Borrada 1 – Indeterminada 2 – Aviso 3 – Leve 4 – Grave 5 – Crítica	Opcional	Varía

Tabla 34. Especificación XML del elemento StatTrap (continuación)

Condición de excepción Estatus	Descripción	Necesario	Valor predeterminado
Cat=	Especifique la categoría de la condición de excepción. Las categorías estándar de las condiciones de excepción son: 0 - Umbral 1 – Topología de red 2 – Error 3 – Estatus 4 – Configuración de nodo 5 – Alerta de aplicación 6 – Todas las categorías 7 – Sólo registro 8 – Correlación 9 – Ignorar	Opcional	Varía
Interval=	El intervalo especifica la frecuencia en minutos con que se emitirá la condición de excepción de Estatus EE_HEARTBEAT. El intervalo se ignora para las otras condiciones de excepción de estatus debido a que son sucesos puros.	Opcional	15 para EE_HEARTBEAT 0 para todos los demás

Cifrado de claves SNMP: itmpwdsnmp

Utilice el mandato de CLI **itmpwdsnmp** para cifrar de forma interactiva una contraseña o añadirla al archivo XML de configuración de condiciones de excepción SNMP para cifrar todas las contraseñas SNMP.

El mandato **itmpwdsnmp** utiliza GSKIT para cifrar de forma interactiva una cadena o para cifrar todas las cadenas de contraseñas SNMP en un archivo XML de configuración de condiciones de excepción.

itmpwdsnmp [[-b |-n]su_agente_trapcnfg.xml][-?]

donde:
si no hay argumentos se especifica la modalidad interactiva
-b especifica que se ha de crear un archivo de copia de seguridad. No se solicita la supresión del archivo de copia de seguridad.
-n especifica que no se ha de crear ningún archivo de copia de seguridad.
su_agente_trapcnfg.xml] es un archivo XML de configuración de condiciones de excepción que contiene cadenas de contraseñas SNMP en texto plano.
-? muestra el uso

Si no se especifica la opción de copia de seguridad **-b** o **-n** al cifrar un archivo XML de configuración de condiciones de excepción, se le solicitará que suprima la copia de seguridad. La copia de seguridad del archivo XML de configuración de condiciones de excepción de entrada original se crea en el mismo directorio que el original con una indicación de fecha y hora adjuntada al nombre del archivo original.

Windows *dir_instalación*\TMAITM6\itmpwdsnmp.bat
Linux UNIX *dir_instalación*/bin/itmpwdsnmp.sh

Ejemplos de CLI

Este mandato cifra de forma interactiva una cadena de caracteres:

```
itmpwdsnmp
Escriba la cadena de caracteres que desea cifrar: ********
Confirme la cadena de caracteres: ********
{AES256:keyfile:a}GbHOlF7KPYZS80Rripx4QQ==
```

Luego copie la cadena de caracteres cifrada en el archivo de configuración de condiciones de excepción.

Este mandato cifra todas las cadenas de caracteres de contraseñas SNMP del archivo de configuración de condiciones de excepción y luego elimina la copia de seguridad del archivo original:

```
itmpwdsnmp -n nt_trapcnfg.xml
```

Resumen del programa

Cadenas de caracteres de comunidad cifradas 1

Cadenas de caracteres AuthPassKey cifradas 2

Cadenas de caracteres EncryptPassKey cifradas 1

Emisiones del agente y de alertas MIB para SNMP

Los agentes de supervisión de Tivoli emiten tres tipos de mensajes SNMP: **agentStatusEvent** para transmitir el estatus operativo del agente, **agentSitSampledEvent** para situaciones de las que se toman muestras a intervalos y pasan a ser verdaderas, y **agentSitPureEvent** para situaciones que reciben notificaciones no solicitadas.

Están definidos en los archivos canbase.mib y cansyssg.mib disponibles en el soporte de instalación de agentes de IBM Tivoli Monitoring IBM Tivoli Monitoring.

agentStatusEvent

agentStatusEvent es una condición de excepción de información de estatus operativo del agente de supervisión generada por el exportador de sucesos SNMP de agente autónomo de Tivoli que informa y notifica sobre un suceso operativo específico del agente.

agentSitSampledEvent

Se ha detectado un suceso de situación de muestra. Esta condición de excepción la genera el exportador de sucesos SNMP de agente autónomo de Tivoli como respuesta al hecho de que se excediera un umbral de situación en el momento de realizar el muestreo de datos.

agentSitPureEvent

Se ha detectado un suceso de situación puro. Esta condición de excepción la genera el exportador de sucesos SNMP de agente autónomo de Tivoli como respuesta al hecho de que se excediera un umbral de situación. Las variables de una condición de excepción de suceso puro son idénticas a las de una condición de excepción de suceso muestreado, excepto en que no hay agentSit-SampleInterval porque no se toman muestras de sucesos puros; la llegada de datos no solicitados del grupo de atributos supervisado hace que la situación pase a ser verdadera. Una situación creada con un grupo de atributos para un registro del sistema, por ejemplo, abre un suceso puro cuando llega una entrada de registro.

Configuración de OMNIbus para SNMP

Debe configurar el entorno de IBM Tivoli Netcool/OMNIbus para que reciba las alertas SNMP de sucesos de situación de Tivoli Enterprise Monitoring Agent y Tivoli System Monitor Agent. El soporte de instalación de DVD del Tivoli

Monitoring Agent contiene la base de información de gestión (mib) y los archivos de reglas de ejemplo que se añade a la configuración del analizador.

Configuración de OMNIbus para recibir alertas SNMP

Configure la prueba SNMP para que acepte las condiciones de excepción SNMP e informe acerca de sucesos de situación procedentes de agentes de supervisión de Tivoli.

Antes de empezar

Tenga a mano el DVD de agentes de IBM Tivoli Monitoring V6.2.2 o posterior. Compruebe que Tivoli Netcool/OMNIbus V7.x esté instalado y que la prueba SNMP esté instalada.

No configure una situación de empresa para emitir alertas SNMP a la prueba SNMP si el servidor de supervisión concentrador también está configurado para reenviar sucesos correspondientes a la misma situación a la Netcool/OMNIbus Probe for Tivoli EIF porque la deduplicación de OMNIbus no detectará que son el mismo suceso.

Acerca de esta tarea

Complete estos pasos para preparar su entorno OMNIbus para recibir alertas SNMP para los sucesos de situación desde los agentes de supervisión de Tivoli.

Procedimiento

1. Copie el archivo de reglas y el archivo de búsqueda de Tivoli Monitoring.
   a. Localice el directorio `mibs/sample_rules/omnibus` en el soporte de instalación de Tivoli Monitoring V6.2.2 o agentes posteriores.
   b. Copie estos archivos de la base de información de gestión en `$OMNIHOME/probes/arch/` en el sistema en el que está instalada la prueba SNMP:
      ```
      ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules
      ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.lookup
      ```
2. Haga referencia a los archivos en las reglas que está utilizando prueba SNMP.
   a. Abra el archivo de reglas predeterminado en un editor de texto. El archivo de reglas predeterminado es `$OMNIHOME/probes/arch/mttrapd.rules` a menos que se especifique lo contrario en el archivo de propiedades mttrapd (Paso 3).
   b. Añada la referencia de tabla de búsqueda como la primera definición:
      ```
      include "<vía_acceso_archivo_búsqueda>/
      ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.lookup"
      ```

      Las definiciones de tabla deben aparecer al principio del archivo de reglas antes de cualquier sentencia de proceso. Si va a añadir esta sentencia a mttrapd.rules, colóquela después de los comentarios en la cabecera del archivo y antes del primer elemento de proceso. El nombre de archivo completo debe estar encerrado entre comillas dobles. Se pueden utilizar las variables de entorno como %OMNIHOME% o $OMNIHOME. El convenio de nombres de archivo de Linux y UNIX con la barra inclinada / para delimitar la vía de acceso también se utiliza en Windows.
   c. Añada las referencia de reglas en el orden en que se deben procesar.
      ```
      include "<vía_acceso_archivo_reglas>/
      ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules"
      ```

Esta sentencia se debe añadir al archivo de reglas en la ubicación en la que se debe procesar. Por ejemplo, si añade la sentencia include al archivo mttrapd.rules predeterminada, deseará que, en primer lugar, las reglas predeterminadas "Comprueben si existe una condición SNMPv2 y la convierta a símbolos de tipo SNMPv1". El siguiente bloque de código del archivo mttrapd.rules predeterminado maneja las condiciones de excepción genéricas. La sentencia include para el archivo ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules debe ir después de esta, probablemente como la última línea de mttrap.rules. Si está familiarizado con prueba SNMP y con su espacio de sucesos sabrá mejor dónde se han de incluir las reglas.

3. Revise y edite el archivo de propiedades de prueba SNMP:
   a. Abra `$OMNIHOME/probes/arch/mttrapd.props` en un editor de texto.
   b. Establezca la propiedad `Protocol` en `"UDP"` o `"ALL"`. Las alertas SNMP de Tivoli Monitoring se envían utilizando UDP.
   c. Establezca la propiedad `RulesFile` si el archivo de reglas predeterminado para la prueba no es `mttrapd.rules`.
   d. Establezca la propiedad `MIBDirs` en la vía de acceso donde residirán los archivos mib.
4. Haga que los archivos MIB de Tivoli Monitoring estén disponibles para la prueba SNMP:
   a. Localice el directorio `mibs` en el soporte de instalación de Tivoli Monitoring.
   b. Copie `canbase.mib` y `cansyssg.mib` en la ubicación de mib especificada en mttrapd.props por la propiedad MIBDirs.
   c. Los archivos `canbase.mib` y `cansyssg.mib` incluyen algunos mib de SNMP comunes. Estos mib también deben estar disponibles para la prueba de SNMP:
      RFC1155-SMI
      RFC1213-MIB
      SNMPv2-TC
      RFC-1212
      RFC-1215
      Si estos mib no están en la ubicación especificada en `mttrapd.props` por la propiedad `MIBDirs`, están disponibles a nivel público y se pueden descargar de Internet.
5. Si va a integrar Tivoli Monitoring, Tivoli Business Service Manager y Netcool/OMNIbus, las reglas de la prueba Netcool/OMNIbus SNMP también deben incluir un archivo de reglas adicional, `tbsm_snmp_event.rules`, que establece el atributo de OMNIbus **BSM_Identity**. El directorio `mibs/sample_rules/omnibus/tbsm` del soporte de instalación del agente de Tivoli Monitoring (V6.2.2 y superiores) contiene el archivo `tbsm_snmp_event.rules` y el archivo readme que describe cómo utilizarlo con la prueba SNMP y cómo utilizar el archivo `itm_tbsm_update.sql` para añadir el atributo **BSM_Identity** al esquema de base de datos de Netcool/OMNIbus.

Resultados

Ahora debe tener instalados estos archivos en el sistema de prueba:

`ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules`

`ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.lookup`

Archivos `can*.mib` que se proporcionan en el soporte de instalación de Tivoli Monitoring

Qué hacer a continuación

Para activar las nuevas reglas y comenzar a recibir alertas de los agentes de Tivoli Monitoring, reinicie la prueba SNMP.

Reglas de OMNIbus de ejemplo para alertas SNMP

El soporte de instalación de agentes de IBM Tivoli Monitoring V6.2.2 o posterior tiene archivos de reglas de ejemplo que puede añadir a la configuración de la prueba Netcool/OMNIbus SNMP.

MIB de condición de excepción de SNMP de Tivoli Monitoring

El archivo `ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules` contiene una correlación de ejemplo de las variables de condiciones de excepción SNMP de IBM Tivoli Monitoring con los campos alerts.status predeterminados en OMNIbus.

El archivo `ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.lookup` contiene estas tablas:

SituationCategory correlaciona **$autoSit-Category** de Tivoli Monitoring con **@AlertGroup** de OMNIbus.

SituationSeverity correlaciona **$autoSit-Severity** de Tivoli Monitoring con **@Type** de OMNIbus: 1 - Problema; 2 - Resolución; y 13 - Información. También los cambios de LQ gravedad de una condición de excepción de borrado de autoSit-Severity=0 a 1, de modo que la automatización generic_clear de OMNIbus correlacione los sucesos.

SituationSource enumera **$agentSit-Source**, que identifica si la situación es una situación de empresa definida en el servidor de Tivoli Enterprise Monitoring o una situación privada definida en el archivo de configuración de situaciones privadas, situado en el directorio de instalación del agente, *<dir_instalación_tema>*`/localconfig/kpc`. Esta tabla también se utiliza para determinar la clase del suceso.

Notas sobre la creación de @Identifier y @AlertKey

El archivo `ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules` utiliza la función Deduplication Automation and Generic Clear Automation de Tivoli Netcool/OMNIbus. Estas automatizaciones se basan en varios campos de alerta, que incluyen los campos Identifier y AlertKey, cada uno de los cuales puede tener un máximo de 255 caracteres. El estándar del archivo de reglas de Netcool/OMNIbus para establecer el campo de alerta Identifier para una alerta SNMP es:

```
@Identifier = @Node + " " + @AlertKey + " " + @AlertGroup + " " + @Type + " "
+ @Agent + " " + @Manager + " " + $specific-trap
```

Puesto que se incluye AlertKey en la información que se utiliza para construir el identificador, es posible que se encuentre con problemas de truncamiento con valores de AlertKey de 255 caracteres utilizados para crear el identificador.

Tal como está implementado en el archivo ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules:

```
@Identifier = @Node + " " + @AlertKey + " " + $autoSit-Category + " " + @Type  +
" " + @Agent + " " + @Manager + " " + $specific-trap
```

$autoSit-Category es una enumeración de @AlertGroup (24 bytes) y se sustituye por @AlertGroup para que el identificador final tenga 23 bytes menos. Estas son las longitudes máximas de los campos de los componentes utilizados para construir el identificador:

Campo	Tamaño
Longitud máxima de @Node	32
Longitud fija de $autoSit-Category	1
Longitud máxima de @Type	2
Longitud máxima de @Agent	31
Longitud fija de @Manager	13
Longitud fija de $specific-trap	2
6 delimitadores de espacios	6
Total	87

Esto deja 168 caracteres para @AlertKey (255-87=168). Si @AlertKey se ha definido como $agentSit-Name + " (" + $sitDisplayItem + ")", $sitDisplayItem debe tener menos de 133 caracteres (168-35=133).

Campo	Tamaño
agentSit-Name	32
delimitador de espacios	1
paréntesis	2
Total	35

Un método recomendado consiste en limitar $sitDisplayItem a 128 caracteres para mantener la coherencia con las reglas de prueba de EIF de IBM Tivoli Monitoring. Las reglas de ejemplo imponen este límite utilizando

```
$sitDisplayItem=substr($sitDisplayItem, 1, 128)
```

Las situaciones escritas para grupos de atributos (como por ejemplo Registro de sucesos) que generan sucesos puros se pueden deduplicar utilizando $agentSit-Name, pero puede que muchas necesiten información adicional para identificar el suceso de forma exclusiva. Utilice el atributo $sitDisplayItem para construir estos datos adicionales. Luego AlertKey será

```
$agentSit-Name + " (" + $sitDisplayItem + ")"
```

Utilice sentencias case basadas en el campo $agentSit-Table para identificar todos los sucesos basados en una determinada tabla.

Utilice sentencias case basadas en $agentSit-Name si hay situaciones individuales que necesiten $sitDisplayItems exclusivos.

Se puede utilizar el mandato **extract** para extraer el valor de cualquiera de los pares de valores de nombres de $sitAttributeList utilizando la comparación de patrones regex. Se proporciona un ejemplo en las reglas de ejemplo para condiciones de excepción agentSitPureEvent basadas en NTEVTLOG $agentSit-Table.

```
$sitDisplayItem=extract($sitAttributeList,"Description=.(.+).;.*?")
```

Este mandato extrae el valor de la clave de descripción y elimina las comillas.

Notas sobre compatibilidad

@ExtendedAttr

OMNIbus V7.2 y superiores definen la columna `@ExtendedAttr` en ObjectServer. Se proporcionan funciones **nvp** que permiten la manipulación de pares nombre-valor en el campo de alerta `@ExtendedAttr`. La varbin sitAttributeList se formatea de modo que permita una correlación directa en `@ExtendedAttr`, pero esta función está comentada para permitir analizar las reglas cuando la prueba MTTRAPD se conecta a un OMNIbus ObjectServer V7.0 o V7.1. Elimine el comentario de las dos líneas en el archivo ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules que establecen `@ExtendedAttr` si va a reenviar sucesos a OMNIbus V7.2 o superiores.

```
#            @ExtendedAttr = $sitAttributeList
```

@Class

El campo de alerta @Class se utiliza para asociar herramientas de Tivoli Netcool/OMNIbus con sucesos mostrados en EventList de Tivoli Netcool/OMNIbus.

Para Tivoli Netcool/OMNIbus 7.2x e inferiores, consulte la documentación de Netcool/OMNIbus para obtener más información sobre cómo crear y editar clases. De forma predeterminada, estos valores de clase no están definidos en ObjectServer.

El hecho de establecer @Class en un valor que *no* esté definido en ObjectServer de OMNIbus no ocasiona problemas, pero si prefiere no establecer @Class, elimine el comentario de esta línea en el archivo ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules para borrar el campo @Class antes de que el suceso se reenvíe a OMNIbus.`#     @Class = ""`

Habilitación de la automatización de latido de OMNIbus

Para los agentes de Tivoli Enterprise Monitoring que envían sucesos de situación como alertas de SNMP o sucesos de EIF a Netcool/OMNIbus, puede habilitar la automatización de OMNIbus para que se envíe un suceso cuando se omita EE_HEARTBEAT. Se envían sucesos de estatus de ciclo de vida de EE_HEARTBEAT al receptor a intervalos regulares para configurar que el agente de supervisión se está ejecutando y las alertas llegan a su destino.

Acerca de esta tarea

Los sucesos HEARTBEAT procedentes de SNMP y EIF se muestran en la consola de sucesos de OMNIbus a medida que llegan y el recuento se incrementa a medida que llegan nuevos sucesos del agente.

El archivo `itm_heartbeat.sql` contiene automatizaciones de muestra para procesar latidos del agente autónomo tanto para EIF como para SNMP. Ejecute el archivo SQL para habilitar la automatización.

Procedimiento

1. Copie `itm_heartbeat.sql` del directorio DVD del agente de Tivoli Monitoring `mibs/sample_rules/omnibus`.
2. Coloque la copia en la vía de acceso de instalación de Netcool/OMNIbus y ejecute el siguiente mandato:
   - Windows Donde "*usuario*" es un nombre de usuario válido, "*contraseña*" es la contraseña correspondiente y "*servidor*" es el nombre de ObjectServer

```
%NCHOME%\bin\redist\isql.exe -U "usuario" -P "contraseña" -S "servidor"
< itm_heartbeat.sql
```

- Linux UNIX Donde "*nombreservidor*" es el nombre de ObjectServer, "*nombreusuario*" es un nombre de usuario válido y "*contr01*" es la contraseña correspondiente

```
$NCHOME/omnibus/bin/nco_sql -server nombreservidor -user nombreusuario
 -password contrd01 < itm_heartbeat.sql
```

Resultados

Una vez instalada la automatización de OMNIbus, esta registra los latidos procedentes de sistemas gestionados a medida que llegan. Los latidos individuales dejan de mostrarse y de contarse en la consola de sucesos pero, si se omite un latido esperado, la automatización emite una alerta de "falta de latido" con:

```
Summary = 'Heartbeat Missed for:' + heartbeat_missed.Node +
' last received at ' + to_char(heartbeat_missed.LastOccurrence)
```

Qué hacer a continuación

El intervalo predeterminado para enviar el estatus de EE_HEARTBEAT es de 15 minutos. Puede ajustar el valor modificando el atributo de intervalo para el suceso de estatus de latido en el archivo trapcnfg.xml para alertas de SNMP y en el archivo eifdest.xml para el archivo de configuración de sucesos de EIF.

Especialmente con SNMP, un latido omitido no necesariamente indica un problema, ya que el valor predeterminado consiste en emitir una alerta después de que se omita el latido: (2 x intervalo latido) + 2 minutos. Puede editar este valor en itm_heartbeat.sql con la entrada.

```
-- 2 latidos más 2 minutos antes de omitir el agente
    set time_of_expiry = (new.ExpireTime * 2 * 60 + 120) + getdate();
```

Por ejemplo, añada dos minutos más y el valor se parecerá al siguiente:

```
-- 2 latidos más 4 minutos antes de omitir el agente
    set time_of_expiry = (new.ExpireTime * 2 * 60 + 240) + getdate();
```

Sucesos de EIF

Envíe sucesos de situaciones privadas directamente desde un agente de Tivoli Monitoring a un receptor de EIF sin pasar por el Tivoli Enterprise Monitoring Server.

Configuración de sucesos de EIF

Configure un agente de supervisión y un archivo XML de configuración de sucesos de EIF local para emitir sucesos de ciclo de vida o sucesos de situación privada, o ambos, a uno o varios receptores de EIF, como el servidor de sucesos de IBM Tivoli Enterprise Console o Netcool/OMNIbus Probe for Tivoli EIF.

Restricción: EIF no recibe soporte en iSeries para enviar sucesos directamente desde los agentes de iSeries.

Nota sobre uso: En los ejemplos de código siguientes utilice las siguientes sustituciones:

- `<dir_instalación>` es el directorio en el que está instalado IBM Tivoli Monitoring
- `<cp>` es el código de producto de 2 letras del agente en minúsculas

- <CP> es el código de producto de 2 letras del agente en mayúsculas

Configuración de sucesos de EIF

El valor predeterminado de la variable de entorno IRA_EVENT_EXPORT_EIF es Y, lo que hace que el emisor de EIF se inicie durante el arranque del agente. Los siguientes archivos deben estar presentes y configurados en el sistema en el que está instalado el agente de supervisión para que pueda realizarse el reenvío de sucesos de EIF:

- Un archivo de configuración de situaciones privadas para definir las situaciones que generan sucesos cuando los criterios de comparación se evalúan como verdaderos. Las situaciones privadas se inician y se detienen como parte del procedimiento de arranque y cierre del agente.
- Un archivo de configuración de destinos de sucesos para definir las escuchas de sucesos para recibir sucesos emitidos de EIF.

Además, puede tener un archivo de correlación de sucesos para controlar los datos de sucesos que se envían al receptor de EIF.

Parámetros del agente

El parámetro **IRA_EVENT_EXPORT_EIF=Y** del archivo de entorno del agente se establece para habilitar el recurso de exportación de sucesos de EIF. Cambie el valor por **N** para inhabilitar el recurso.

El parámetro **IRA_EIF_DEST_CONFIG=<nombrearchivo>** del archivo de entorno del agente se establece para especificar la ubicación del archivo XML de configuración de destinos de EIF. El valor predeterminado es <dir_instalación>/localconfig/<cp>/<cp>_eventdest.xml.

El parámetro **IRA_LOCALCONFIG_DIR** del archivo de entorno de agente se puede establecer para especificar una vía de acceso a directorio distinta para el destino de EIF o el archivo de correlación de sucesos opcional, o ambos. El valor predeterminado es <dir_instalación>/localconfig/<cp>.

El parámetro **IRA_EIF_MSG_LOCALE=en_US** de los archivos de entorno del agente se establece en inglés americano de forma predeterminada. Para los agentes que dan soporte a texto de mensajes globalizado para la ranura de mensajes en el suceso generado utilizando un archivo de correlación predefinido y paquetes de recursos de idioma, se puede especificar el entorno local de idioma predeterminado.

Especificación XML de configuración de destinos de sucesos de EIF del agente

El archivo XML de destinos de sucesos de EIF se utiliza para especificar el servidor o servidores de destino y sus configuraciones. El elemento raíz es <EventDest> y contiene los elementos <Destination> y <Server>, así como el elemento <StatEvent> opcional para configurar el intervalo de latido de EIF: la frecuencia con la que el agente envía un suceso de latido al receptor de EIF.

El archivo de configuración de destinos de sucesos reside en la siguiente ubicación predeterminada:

Windows <dir_instalación>\localconfig\<cp>\<cp>_eventdest.xml

Linux UNIX <dir_instalación>/localconfig/<cp>/<cp>_eventdest.xml

z/OS RKANDATV, con nombre de miembro <CP>EVDST

Especificación XML de configuración de correlación de sucesos de EIF del agente

El archivo XML de configuración del archivo de correlación de sucesos de EIF opcional se puede utilizar para personalizar los sucesos de EIF que se generan. Si no se proporciona ningún archivo de correlación de sucesos, los

sucesos se formatean mediante correlación genérica. Los archivos de correlación de sucesos pueden ser proporcionados por el producto o definidos por el usuario. Las correlaciones de sucesos definidas por el usuario, si las hay, prevalecen sobre las correlaciones proporcionadas sobre el producto. El nombre y la ubicación del archivo de correlación de sucesos predefinido, si lo hay:

Windows <dir_instalación>\TMAITM6\EIFLIB\k<cp>.map para agentes de 32 bits; <dir_instalación>\TMAITM6_x64\EIFLIB\k<cp>.map para agentes de 64 bits.

Linux UNIX <dir_instalación>/<plataforma>/<cp>/tables/EIFLIB/k<cp>.map

z/OS RKANDATV, con nombre de miembro K<CP>MAP.

Si crea un archivo de correlación de sucesos definida por el usuario, almacénelo en la siguiente ubicación:

Windows <dir_instalación>\localconfig\<cp>\<cp>_eventmap.map

Linux UNIX <dir_instalación>/localconfig/<cp>/<cp>_eventmap.map

z/OS RKANDATV, con nombre de archivo <CP>EVMAP

Archivo de configuración de correlación de sucesos de muestra:

```
<?xml version="1.0" encoding="UTF-8"?>
<itmEventMapping:agent>
   <event_mapping>
      <situation name="Flipper*" mapAllAttributes="Y">
         <class name="ITM_ABC"/>
            <slot slotName="msg">
               <literalString value="The time now is
               $Local_Time.Timestamp.TIMESTAMP$ on $hostname$"/>
            </slot>
      </situation>
   </event_mapping>
</itmEventMapping:agent>
```

Suceso de latido de estatus en línea del agente enviado al receptor de sucesos de EIF El archivo XML de configuración EventDest tiene un elemento opcional para especificar un intervalo de latido. Transcurrido cada intervalo, se prueba el estatus del agente y el resultado se envía como estatus en línea o fuera de línea al receptor o receptores de EIF especificados en el archivo EventDest.

Agentes de Tivoli Enterprise Monitoring instalados antes de la Versión 6.2.2 Fixpack 1

Cuando se ha instalado un agente de sistema operativo de Tivoli Monitoring Versión 6.2.2 Fixpack 1 o posterior, cualquier Tivoli Enterprise Monitoring Agent instalado en dicho sistema es apto para utilizar la función de reenvío de sucesos de EIF autónoma, incluso si se ha instalado antes de la Versión 6.2.2 Fixpack 1. Sin embargo, tenga en cuenta que los agentes de supervisión instalados antes de la Versión 6.2.2 Fixpack 1 necesitan algunos archivos que no están incluidos en el paquete de instalación del agente pero que son parte del soporte de aplicaciones que se proporciona para una instalación del Tivoli Enterprise Monitoring Server: el archivo baroc, el archivo de correlación de sucesos opcional y los archivos de paquetes de recursos. Para que estos agentes de versiones anteriores puedan utilizar el recurso de EIF para reenviar sucesos, se deben seguir los pasos siguientes:

1. Instale el agente de la versión anterior en un entorno de servidor de supervisión para acceder a los archivos baroc y de correlación de sucesos opcional. Los archivos baroc y de correlación de sucesos opcional predefinidos por el agente se encuentran en el directorio <dir_instalación>/CMS/TECLIB o <dir_instalación>/CNPS/teclib.
2. Copie el archivo de correlación de sucesos k<cp>.map proporcionado, si lo hay, en el directorio EIFLIB de la instalación del agente.
3. Si se utiliza el Tivoli Enterprise Console event server como receptor de sucesos, copie el archivo baroc para cada agente en el sistema en el que está instalado el servidor de sucesos. Compile y cargue el archivo baroc en el servidor de sucesos.

Agentes que se ejecutan en el espacio de direcciones del Tivoli Enterprise Monitoring Server concentrador en z/OS

En sistemas z/OS, es posible configurar agentes para que se ejecuten dentro del mismo espacio de direcciones del servidor de supervisión concentrador. Puesto que la función de reenvío de sucesos de EIF (OTEA) también se puede habilitar en el servidor de supervisión concentrador, deben tomarse ciertas precauciones para evitar la interferencia cruzada entre el reenvío de sucesos en el servidor de supervisión concentrador y la exportación de sucesos de EIF directamente desde el agente de supervisión. Un área que puede tener un solapamiento potencial es un archivo de correlación de sucesos personalizado. Actualmente, en el servidor de supervisión concentrador los usuarios pueden codificar su propia correlación de sucesos (además de la que se puede crear con el editor de situaciones de Tivoli Enterprise Portal y almacenar en una tabla del servidor de supervisión). El nombre de estos archivos de correlaciones debe tener el formato **Q<xx>MAP** (donde <xx> es cualquier par de caracteres alfanuméricos) y residir en el conjunto de datos RKANDATV. Para dar soporte a archivos de correlación de sucesos definidos por el usuario para agentes autónomos, que también residen en el conjunto de datos RKANDATV, se debe adoptar un convenio de denominación distinto. Para los archivos de correlación de sucesos definidos por el usuario para agentes autónomos, el convenio de denominación de archivos es **<cp>EVMAP** (donde <cp> es el código de producto del agente de 2 letras).

Especificación XML de correlación de sucesos de EIF

La correlación de sucesos de EIF es un archivo XML que especifica cómo se deben convertir los sucesos correspondientes a una o varias situaciones privadas. Cree un archivo de correlación de sucesos personalizado para modificar los datos que se envían al receptor de EIF.

Formato del archivo de correlación de sucesos

```
<itmEventMapping:agent>
  <id>xx</id>
  <version>n.n</version>
  <event_mapping>
    <situation>
      <slot>
        <mappedAttribute/>
          or
        <mappedAttributeEnum/>
          or
        <literalString/>
      </slot>
      :    one or more slot tags
    </situation>
```

```
or

    <attributeTable>
      <slot>
        <mappedAttribute/>
          or
        <mappedAttributeEnum/>
          or
        <literalString/>
      </slot>
      :    one or more slot tags
    </attributeTable>
  </event_mapping>
</itmEventMapping:agent>
```

Elementos

Las etiquetas XML no son sensibles a mayúsculas y minúsculas. Los demás parámetros son sensibles a mayúsculas y minúsculas.

<itmEventMapping:agent>
itmEventMapping:agent es el elemento raíz que lo identifica como a definición de correlación de sucesos para el agente de supervisión.

<id> Sintaxis:

```
<id>cp</id>
```

ID es el código de producto de dos caracteres, como por ejemplo "UX" para el agente del sistema operativo UNIX. Para correlaciones de sucesos definidas por el usuario, se recomienda utilizar "99" como ID.

<version>
Sintaxis:

```
<version>nnnn</version>
```

Opcional. Utilice este elemento para especificar la versión del archivo de correlación de sucesos.

<valueList>
Sintaxis:

```
<valueList name="nombreListaValores">
```

Opcional. Utilice el elemento valueList para definir una lista de uno o varios elementos de valor, donde *nombreListaValores* es el nombre de la lista.

<valueItem>
Sintaxis:

```
<valueItem name="valor_elemento">
```

Este elemento es obligatorio si se ha definido `valueList`. ValueItem especifica un valor de elemento válido para el elemento `valueList` especificado.

<event_mapping>
Sintaxis:

```
<event_mapping>
```

El elemento event_mapping comprende un grupo de entradas de correlación.

<situation>

Sintaxis:

```
<situation name="nombre_situación" [mapAllAttributes="Y"]
```

El elemento situation especifica una entrada de correlación de DM cuya clave es `nombre_situación`. La cadena de caracteres `nombre_situación` puede contener caracteres comodín (* asterisco y ? signo de interrogación), excepto en la primera posición.

mapAllAttributes="Y" indica al reemisor de sucesos de EIF que construya ranuras de sucesos de EIF como la correlación genérica, excepto las ranuras especificadas de forma explícita mediante la etiqueta <slot> dentro de esta entrada de correlación. Este atributo resulta útil en los casos en los que solo se deben personalizar unas pocas ranuras del suceso (como en el caso de la ranura msg). Esto evita la necesidad de especificar de forma explícita cada ranura para que se incluya en el suceso de EIF.

<attributeTable>

Sintaxis:

```
<attributeTable name="nombre_tabla_atributos"
 [truncated="Y"] [freeSpace="nnnn"]
```

truncated="Y" hace que se asigne "Agente de ITM: Situación privada: Truncado" a la ranura "source" del suceso de EIF en lugar de "Agente de ITM: Situación privada". Esto indica que no todos los atributos de los datos del suceso se pueden ajustar en el suceso de EIF debido a las limitaciones de tamaño, tal como define el generador de correlaciones de sucesos.

freeSpace="*nnnn*" es un valor determinado por el generador de correlaciones de sucesos como tamaño máximo disponible en el almacenamiento intermedio de sucesos de EIF después de que se hayan creado todas las ranuras definidas en la correlación de sucesos. El emisor de sucesos de EIF utiliza su valor para determinad la cantidad de datos de sucesos sin formato que se deben incluir en la ranura `situation_eventdata`.

<class>

Sintaxis:

```
<class name="nombre_clase_eif" [valueList="nombre_listaValores"]
 [defaultClass="nombre_clase_eif_predeterminada"]>
```

name= especifica el nombre de clase de EIF que se utilizará para el suceso de EIF generado. La cadena de caracteres `nombre_clase_eif` puede contener una variable de sustitución (nombre de atributo) para generar nombres de clases de EIF dinámicos, en función del valor del atributo especificado durante la ejecución. Consulte el apartado "Nombre de clase de EIF dinámico" en la página 403.

valueList= especifica un valor de `valueList` que buscar para la generación de nombres de clase de EIF dinámicos.

defaultClass= especifica el nombre de clase de EIF predeterminado que se utilizará para el suceso de EIF si la cadena de caracteres `nombre_clase_eif` contiene una variable de sustitución pero el valor del atributo no tiene ninguna coincidencia en la `valueList` especificada.

<slot> Sintaxis:

```
<slot name="nombre_ranura">
```

Opcional. Define una ranura en el suceso de EIF. El nombre de la ranura es *nombre_ranura*.

<mappedAttribute>

Sintaxis:

```
<mappedAttribute name="nombre_atributo" [multiplier="nnn"]>
```

Opcional. Especifique el origen del valor para la ranura que se va a definir. Es el valor del atributo llamado `nombre_atributo` en los datos del suceso, si está disponible. De lo contrario, se utiliza un valor nulo. Si se especifica el atributo `multiplier=` y el valor del atributo es numérico, el valor asignado para la ranura es el valor del atributo multiplicado por el número especificado.

<mappedAttributeEnum>

Sintaxis:

```
<mappedAttributeEnum name="nombre_atributo">
```

Opcional. MappedAttributeEnum se parece a la etiqueta mappedAttribute, excepto en que si el atributo se define como una enumeración en el archivo de atributos, el texto de visualización enumerado se utiliza como el valor de la ranura en lugar del valor del atributo sin formato. Si no se define ningún texto de visualización enumerado que coincida con el valor del atributo, se utiliza el valor del atributo sin formato.

<literalString>

Sintaxis:

```
<literalString value="texto">
```

Opcional. Utilice el texto como el valor para la ranura que se va a definir. Cuando defina una ranura "msg", puede especificar sustitución de variables dentro del texto (se describe a continuación).

Ranura msg personalizada

Si el valor de la ranura msg se define como una cadena de caracteres literal (elemento <literalString>), puede incluir variables de sustitución. Las variables de sustitución se designan mediante la sintaxis `$variable$`. Cuando se formatea una ranura msg, el reemisor de sucesos de EIF sustituye el símbolo `$variable$` por su valor de sustitución.

Variables válidas:

$AttrGroup.Attribute$

La sustitución de atributos necesita un nombre calificado al completo (es decir, grupo de atributos y nombre de atributo separado por un punto). La señal de la variable ase sustituirá por el valor del atributo mencionado en los datos del suceso. Si el atributo mencionado no se encuentra en los datos del suceso, se utiliza una cadena de caracteres nula.

$AttrGroup.Attribute.TIMESTAMP$

Utiliza la misma sintaxis que $AttrGroup.Attribute$, pero con un calificador de sufijo **.TIMESTAMP**. Esto indica al reemisor de sucesos de EIF que el valor del atributo es una indicación de fecha y hora (definida como tipo timestamp en el archivo de atributos) y debe tener un formato de fecha y hora que se pueda visualizar: MM/DD/AAAA HH:MM:SS. Si el valor del atributo no es una indicación de fecha y hora válida, se utiliza el valor del atributo sin formato.

$slotname$

La sustitución de ranura del suceso sustituye la señal de la variable por el valor de la ranura mencionada una vez realizada la correlación de sucesos.

A continuación se muestra una señal de ejemplo tomada del archivo de correlación de sucesos predefinido en el que ranura msg se ha personalizad para la paridad de DM.

```
<slot slotName="msg">
  <literalString value="Distributed Monitoring $sub_source$/$monitor$
  on host $hostname$ $NT_LogicalDisk.Timestamp$"/>
</slot>
```

Si el valor de las ranuras `sub_source` y `monitor` tienen los valores "tmpdisk" y "Disk Read Bytes/sec", el texto de la ranura msg sería como el del siguiente ejemplo:

```
Distributed Monitoring tmpdisk/Disk Read Bytes/sec on host
 elaix04 08/14/2009 10:23:11
```

Nombre de clase de EIF dinámico

El nombre de clase de sucesos de EIF se define mediante el atributo **name=** del elemento **<class>**. La cadena de caracteres del nombre de la clase de EIF puede contener una variable de sustitución para la generación dinámica del nombre de clase de EIF. La variable de sustitución puede estar en cualquier lugar de la cadena de caracteres de nombre de clase de EIF, excepto al principio. La variable de sustitución tiene la sintaxis `$attributeGroup.attribute$`. En tiempo de ejecución, el reemisor de sucesos de EIF busca en la `valueList` indicada, si existe, el valor del atributo especificado en la variable de sustitución. Si el valor del atributo se encuentra en `valueList`, la variable (y el signo de dólar $ que la delimita) se sustituye por el valor del atributo (después de que se normalice) en la cadena de caracteres del nombre de clase de EIF. Si no se encuentra ninguna coincidencia en `valueList` o si la `valueList` designada no está definida, se utiliza el nombre de clase de EIF definido en el atributo **defaultClass=** como nombre de clase de EIF para el suceso. Si no se especifica **defaultClass=**, la variable del nombre de clase de EIF se sustituye por una cadena de caracteres nula.

Si la variable hace referencia a un atributo numérico, no se realiza ninguna operación de escalado o precisión. La representación de la cadena de caracteres para el campo numérico del registro del suceso de situación se utiliza sin ningún ajuste. Si la variable hace referencia a un atributo enumerado, cualquier representación de texto de la enumeración se utiliza como valor para la variable.

Cuando la situación no es verdadera (el estatus no es "Y"), el registro de estatus de la situación no contiene ningún dato sobre atributos del suceso. Por lo tanto, no hay manera de determinar el valor de ninguna variable de sustitución en el nombre de clase. El reemisor de sucesos de EIF utiliza el atributo **defaultClass=** si hay uno especificado. De lo contrario, utiliza la clase de suceso de EIF del último suceso de EIF enviado para el mismo nombre de situación.

Esta es la parte relevante que una definición de correlación de sucesos de muestra utiliza para correlacionar un suceso de situación "Test_Syslog" con un conjunto de sucesos de EIF en función del valor del atributo "Message_Number".

```
<situation name="Test_Syslog">
  <class name="SAP_Syslog_$R/3_System_Log.Message_Number$"
  valueList="SyslogIDList" defaultClass="SAP_Syslog_Default" />
  :
  :
</situation>
```

Este ejemplo tiene una lista de valores “SyslogIDList” con los valueItems AB0, AB1, A08, BV7, EAS y R45 y una situación “Test_Syslog” que supervisa los ID de mensaje AB0, AB1, AB2, BV7 y BV8. La situación “Test_Syslog” se evalúa como verdadera para cada uno de estos ID de mensaje. Los sucesos de EIF generados son de las siguientes clases:

1. AB0: SAP_Syslog_AB0 x
2. AB1: SAP_Syslog_AB1
3. AB2: SAP_Syslog_Default
4. BV7: SAP_Syslog_BV7
5. BV8: SAP_Syslog_Default

Normalización del valor de atributo
Una variable dentro del nombre de clase de suceso de EIF puede hacer referencia a cualquier atributo válido en el suceso cuyo valor puede contener caracteres que no se puedan utilizar en un nombre de clase de suceso de EIF. Antes de realizar la sustitución de variables en el nombre de clase de suceso, el reemisor de sucesos de EIF sustituye los caracteres UTF-8 multibyte y los caracteres no válidos por un signo de subrayado _. Por ejemplo, los caracteres de espacio en blanco, < > ( ) & /, se sustituye por un carácter de signo de subrayado _.

Ejemplo

```
<itmEventMapping:agent
  xmlns:itmEventMapping="http://www.ibm.com/tivoli/itm/agentEventMapping"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ibm.com/tivoli/itm/agentEventMapping
  agentEventMap.xsd">

  <id>NT</id>
  <version>6.2.0</version>
  <event_mapping>
    <situation name="NT_LDDBPS*">
      <class name="w2k_LogDskDskBytesPerSec"/>
      <slot slotName="source">
        <literalString value="SENTRY"/>
      </slot>
      <slot slotName="probe">
        <literalString value="DskBytesPerSec"/>
      </slot>
      <slot slotName="probe_arg">
        <mappedAttribute name="NT_Logical_Disk.Disk_Name"/>
      </slot>
      <slot slotName="collection">
        <literalString value="w2k_LogicalDisk"/>
      </slot>
      <slot slotName="monitor">
        <literalString value="Disk Bytes/sec"/>
      </slot>
      <slot slotName="units">
        <literalString value="(per second)"/>
      </slot>
      <slot slotName="value">
        <mappedAttribute name="NT_Logical_Disk.Disk_Bytes/Sec"/>
      </slot>
      <slot slotName="effective_value">
```

```
        <mappedAttribute name="NT_Logical_Disk.Disk_Bytes/Sec"/>
      </slot>
      <slot slotName="msg">
        <literalString value="Distributed Monitoring $sub_source$/Disk
        Bytes/sec on host $hostname$ $NT_Logical_Disk.Timestamp.TIMESTAMP$"/>
      </slot>
    </situation>
  </event_mapping>
</itmEventMapping:agent>
```

Se proporcionan archivos de EIF de ejemplo en el soporte de instalación de Tivoli Monitoring Agent en el directorio `PrivateConfigSamples/EIF`.

Especificación XML de configuración de destinos de sucesos de EIF

Utilice los elementos EventDest, Server y Destination del archivo XML de destino de EIF para configurar los servidores de destino para los sucesos de EIF que envía el agente de supervisión.

Elementos

Los elementos y sus atributos no son sensibles a mayúsculas y minúsculas. Por ejemplo, puede especificar EVENTDEST=, EventDest= o eventdest=.

<EventDest>
EVENTDEST es el elemento raíz que lo identifica como a definición de destinos de sucesos para el agente de supervisión.

<Destination>
Inicio de una definición de destinos de sucesos. Especifique el índice del destino. Los atributos opcionales le permiten especificar el tipo de destino, un servidor predeterminado, el tamaño máximo del archivo de memoria caché y la opción de borrar el archivo de memoria caché al reiniciar.

id= Obligatorio. Índice de destino, entre 0 y 999. Valor predeterminado: **0**

type= Opcional. Tipo de destino: T=IBM Tivoli Enterprise Console; M=Netcool/OMNIbus. El tamaño máximo del suceso generado será 4K y 32K para type=T y type=M, respectivamente. Valor predeterminado: **T**

default= Opcional. El servidor que se especifique aquí será el destino predeterminado. Valor predeterminado: **N**

clear_cache= Opcional. Utilice este atributo para especificar si el archivo de memoria caché de EIF existente se debe borrar cuando se cree una instancia del destino. clear_cache="Y" hará que el archivo de memoria caché de sucesos de EIF se borre. En sistemas z/OS, la memoria caché de sucesos de EIF siempre se borra porque EIF de z/OS sólo da soporte a una memoria caché de sucesos principal. Valor predeterminado: **Y**

max_cache_size= Opcional. Especifica el tamaño máximo del archivo físico de memoria caché de sucesos en kilobytes. Valor predeterminado: **4096**

stat= Opcional. Especifique si el destino debe recibir sucesos de ciclo de vida. Valor predeterminado: **N**

master_reset= Opcional. Especifique si se debe enviar un suceso de restablecimiento maestro durante el arranque del agente. Valor predeterminado: **N**

<Server>

Define los servidores de sucesos para el destino: uno principal y un máximo de siete servidores secundarios. Especifique cada nombre de host o dirección IP del servidor de sucesos y el puerto. La primera definición de <server> es la escucha principal. Las demás definiciones de <server> son servidores de reserva.

location= Especifica el nombre de host o dirección IP de la escucha de sucesos.

port= Opcional. Especifica el puerto de escucha del servidor de sucesos de IBM Tivoli Enterprise Console o prueba Netcool/OMNIbus para Tivoli EIF. El número de puerto predeterminado para el servidor de sucesos de IBM Tivoli Enterprise Console es **5529**. Sin embargo, se puede utilizar el valor **port=0** para un IBM Tivoli Enterprise Console en Linux o sistemas operativos como UNIX, lo que indica que el escucha de sucesos está utilizando el correlacionador de puertos. El número de puerto predeterminado para EIF Probe es **9998**. Si no se especifica ningún valor, el valor predeterminado del número de puerto es **0** en la definición de la ubicación del servidor.

SSL= Opcional. Especifique si se enviarán los sucesos cifrados a través de una conexión SSL (Secure Socket Layer) o si los sucesos se enviarán sin cifrar sobre una conexión que no sea SSL. Las conexiones SSL sólo reciben soporte para destinos de sucesos Netcool/OMNIbus (type="M"). Si está habilitado para un destino de sucesos de IBM Tivoli Enterprise Console (type="T"), se utiliza una conexión no SSL predeterminada. Especifique Y para habilitar y N para inhabilitar. Valor predeterminado: **N**.

<StatEvent>

Opcional. Utilice el elemento StatEvent para enviar el estatus en línea o fuera de línea del agente al servidor de sucesos. De forma predeterminada, la supervisión de latido está inhabilitada.

name= especifica el nombre del suceso de latido.

interval= Opcional. El intervalo, expresado en minutos, al que se envía el suceso de latido. Un intervalo de cero significa que no se va a enviar ningún latido. Valor predeterminado: **15**.

Ejemplos: Ambas secciones nombran el suceso de latido, EE_HEARTBEAT. La primera sección especifica un intervalo de 5 minutos y la segunda sección inhabilita el suceso de latido.

```
<StatEvent name="EE_HEARTBEAT" interval="5"/>
<StatEvent name="EE_HEARTBEAT" interval="0"/>
```

El servidor de destino recibe un suceso de EIF con el nombre de clase "ITM_Heartbeat" que contiene una ranura llamada "interval" cuyo valor es el intervalo de latido. Los sucesos de SNMP recibidos contienen un atributo "AlertGroup" cuyo valor es "ITM_Heartbeat" y un atributo "HeartbeatInterval" cuyo valor es el intervalo de latido. Puede personalizar las reglas de latido que se proporcionan o escribir las suyas propias para manejar sucesos de latido.

Nota: No se da soporte a varios sucesos EE_HEARTBEAT. Si se configuran varios destinos para recibir EE_HEARTBEAT, se envía el mismo EE_HEARTBEAT a cada destino.

Ejemplo

El siguiente ejemplo es un archivo de configuración de destinos de sucesos que contiene un destino de sucesos:

```
<EventDest>
 <Destination  id="0" type="M" master_reset="Y" stat="Y" default="Y">
  <Server location="server.ibm.com" port="9998" />
 </Destination>
 <StatEvent name="EE_HEARTBEAT" interval="5" />
</EventDest>
```

El siguiente ejemplo es un archivo de configuración de destinos de sucesos que contiene dos destinos de sucesos:

```
<EventDest>
 <Destination id="0" type="M" default="Y" master_reset="Y" stat="Y">
  <Server location="omniserver.ibm.com" port="9998" />
 </Destination>
 <Destination id="1" type="T" default="Y" master_reset="Y" stat="N">
  <Server location="tecserver.ibm.com" port="5529" />
 </Destination>
 <StatEvent name="EE_HEARTBEAT" />
</EventDest>
```

Aquí, el segundo destino no recibirá sucesos de ciclo de vida porque el parámetro start tiene el valor "N".

El siguiente ejemplo es un archivo de configuración de destinos de sucesos que contiene dos destinos de sucesos definidos para que utilicen una conexión SSL:

```
<EventDest>
    <Destination id="0" type="M" default="Y" master_reset="Y" stat="Y" >
        <Server location="server1.ibm.com" port="9998" SSL="Y" />
     </Destination>
    <Destination id="1" type="M" default="Y" master_reset="Y" stat="Y" >
        <Server location="server2.ibm.com" port="9998" SSL="Y" />
        <Server location="server3.ibm.com" port="9998" SSL="N" />
     </Destination>
</EventDest>
```

Aquí, el segundo destino muestra que no se necesita el mismo valor de SSL cuando hay varias ubicaciones de servidor definidas si se utiliza una conexión SSL para el servidor principal y una conexión no SSL para el servidor secundario.

Consejo: Se proporcionan archivos de EIF de ejemplo en el soporte de instalación de Tivoli Monitoring Agent en el directorio `PrivateConfigSamples/EIF`.

Ranuras comunes para sucesos emitidos de EIF

Revise las descripciones del conjunto de ranuras comunes para comprender la información de sucesos de situación privada en el receptor de EIF.

Todos los sucesos de EIF emitidos tendrán un conjunto común de ranuras, además de las ranuras procedentes de los datos de atributos del suceso. Todos los atributos, excepto los ocultos, definidos en la tabla de atributos que utiliza el suceso se incluyen en el suceso emitido (sujeto a la limitación de tamaño de ranura y de total de sucesos). El conjunto de ranuras comunes se explica en la tabla siguiente.

Tabla 35. Conjunto de ranuras comunes para sucesos de EIF emitidos

Ranuras	Valores y significado
adapter_host	Atributo de clase EVENT base. Igual que hostname (véase más abajo). Son datos específicos de aplicación relacionados con el suceso, si existen.
appl_label	Se utiliza para indicar que el origen del suceso es una situación privada o el estatus en línea del agente. El valor tiene la siguiente sintaxis: **origen : tipo_sit : tipo_suceso** donde **origen** siempre es "A" para agente **tipo_sit** es "P" para una situación privada o "E" para una situación de empresa **tipo_suceso** es "S" para sucesos de situación o "L" para sucesos de estatus de ciclo de vida Por ejemplo, A : P **Nota:** Para sucesos de situación de empresa, el valor appl_label no se establece. Por lo tanto, no hay ningún appl_label="A:E:S".
cms_hostname	No se utiliza o es nulo para un suceso emitido del agente. **Nota:** Puesto que el Tivoli Enterprise Monitoring Server no se utiliza para sucesos emitidos de EIF, el servidor de sucesos de IBM Tivoli Enterprise Console no registra ningún mensaje de error en el archivo synch_trace.log de sincronización de sucesos después de que se cierre un suceso de situación privada.
cms_port	No se utiliza o es nulo para un suceso emitido del agente.
fqhostname	Atributo de clase EVENT base que contiene el nombre de host totalmente calificado, si está disponible.
nombre_host	Atributo de clase EVENT base que contiene el nombre de host TCP/IP del sistema gestionado donde se origina el suceso, si está disponible.
integration_type	Indicador para ayudar al rendimiento de . • N para un suceso nuevo, la primera vez que se genera el suceso • U para el suceso de actualización y los siguientes cambios de estado de sucesos
master_reset_flag	Indicador de restablecimiento maestro establecido para sucesos de restablecimiento maestros. El valor es NULL para todos los demás sucesos: • R para reinicio del agente • De lo contrario, nulo
msg	Atributo de clase EVENT base que contiene el nombre de situación y la fórmula, sin uso de personalización.
origin	Atributo de clase EVENT base contenido en la dirección TCP/IP, si está disponible, del sistema gestionado donde se origina el suceso. La dirección es en formato decimal con puntos.
severity	Atributo de clase EVENT base que contiene la gravedad resuelta.

Tabla 35. Conjunto de ranuras comunes para sucesos de EIF emitidos (continuación)

Ranuras	Valores y significado
situation_displayitem	Elemento de visualización de situación asociada, si está disponible.
situation_eventdata	Datos de suceso de situación sin formato de la segunda fila de datos de suceso, si existen. Los atributos de datos de suceso están en formato de pares de clave-valor. Los datos de sucesos se pueden truncar debido al límite de tamaño total de suceso y tamaño de ranura, que es de 2 KB.
situation_group	Uno o varios nombres de grupos de situaciones (con un máximo de 5) de los que la situación es miembro.
situation_fullname	Nombre de visualización de la situación, si se ha definido una para la situación privada.
situation_name	Identificador exclusivo asignado a la situación.
situation_origin	Nombre de sistema gestionado donde se ha originado el suceso de situación. Tiene el mismo valor que sub_source.
situation_status	Estatus actual del suceso de situación: "Y" la situación es verdadera "N" la situación es falsa "P" la situación se ha detenido
situation_time	Indicación de fecha y hora del suceso de situación.
situation_type	Tipo de suceso de situación: **S** para suceso muestreado, **P** para suceso puro.
situation_thrunode	Nombre del sistema gestionado del agente.
source	Atributo de clase EVENT base que contiene **Agente de ITM: Situación privada** o **Agente de ITM: Situación Privada:Truncada**
sub_origin	Atributo de clase EVENT base que contiene el elemento de visualización, si lo hay.
sub_source	Atributo de clase EVENT base que contiene el nombre de sistema gestionado de origen para la situación asociada.

Suceso de ciclo de vida de EIF

Además de emitir sucesos de inicio o detención y de estatus de situaciones, el emisor de sucesos de Event Integration Facility genera sucesos adicionales de ciclo de vida que no están relacionados con situaciones privadas.

Los sucesos de ciclo de vida se emiten cuando el agente o la situación cambian de estado, tal como se muestra en la *Tabla de sucesos de ciclo de vida de EIF*. El suceso de latido es un suceso de ciclo de vida que no necesita cambio de estatus para que se emita: se envía a intervalos regulares para confirmar que el agente se está ejecutando.

Tabla 36. Sucesos de ciclo de vida de EIF

Suceso	Significado
EE_AUTO_ENTER	La situación ha entrada en operación en modalidad autónoma.
EE_AUTO_EXIT	La situación ha salido de la operación en modalidad autónoma.

Tabla 36. Sucesos de ciclo de vida de EIF (continuación)

Suceso	Significado
EE_CONFIG_UPDATE	Se genera cuando se toma el archivo de configuración de un servidor.
EE_HEARTBEAT	Latido del agente.
EE_TEMS_CONNECT	El agente se ha conectado al servidor de supervisión.
EE_TEMS_DISCONNECT	El agente se ha desconectado del servidor de supervisión.
EE_TEMS_RECONNECT_LIMIT	Se ha superado el límite de reconexiones del agente con el servidor de supervisión.
EE_SIT_STOPPED	La situación se ha detenido. Es opcional. **Nota:** La ranura situation_status para sucesos de EIF envía "P" automáticamente cuando una situación se detiene.

Todos los sucesos de EIF de ciclo de vida son ITM_StatEvent, que es una clase de suceso derivada, con los siguientes valores de ranura:

Tabla 37. Valores de ranura de clase ITM_StatEvent de suceso de ciclo de vida de EIF

Ranura	Valor
source	"Agente de ITM: Suceso de estatus"
appl_label	"A:E:L" para detención de situación de empresa; "A:P:L" para las demás.
hostname	Nombre de host o dirección IP de la máquina agente
fqhostname	Nombre de host completo, si está disponible
origin	La dirección IP del sistema agente
situation_name	Valor de estatus de ciclo de vida, como por ejemplo EE_AUTO_ENTER. Si el suceso de ciclo de vida es EE_SIT_STOP, la ranura situation_displayitem contiene el nombre de la situación que se ha detenido.
situation_time	Fecha y hora a la que se ha producido el suceso de ciclo de vida
date	Fecha del suceso de ciclo de vida
severity	"HARMLESS"
msg	Mensaje que describe el suceso de ciclo de vida

Suceso de latido de EIF

El archivo XML de destino de sucesos de Event Integration Facility puede incluir un elemento StatEvent para enviar el estatus en línea o fuera de línea del agente de supervisión al servidor de sucesos. Puede personalizar las reglas de latido que se proporcionan o escribir las suyas propias para manejar sucesos de latido.

El servidor de destino recibe un suceso de EIF con el nombre de clase "ITM_Heartbeat" que contiene una ranura llamada "interval" cuyo valor es el intervalo de latido. Los sucesos de SNMP recibidos contienen un atributo "AlertGroup" cuyo valor es "ITM_Heartbeat" y un atributo "HeartbeatInterval" cuyo valor es el intervalo de latido. La ranura situation_eventdata también se establece en el intervalo de latido,

La clase **ITM_Heartbeat** de IBM Tivoli Enterprise Console está disponible para personalizar la regla de latido. La clase está en el archivo `om_tec.baroc` que se instala con la sincronización de sucesos en el servidor de sucesos de IBM Tivoli Enterprise Console. Se encuentra en el DVD de herramientas de IBM Tivoli Monitoring. Los sucesos de estatus se guardan aparte de los sucesos de situación de modo que se pueden escribir reglas que solo se apliquen a la clase o tipo específicos.

Ejemplo: El suceso de EIF ITM_Heartbeat tiene un intervalo de 1 minuto (`interval='1';` y `situation_eventdata='1';`) y se caracteriza como un suceso de latido:

```
ITM_Heartbeat;
 interval='1';
 source='ITM Agent: Heartbeat Event';
 sub_source='EE_HEARTBEAT';
 situation_name='**';
 situation_origin='SuperServer:TEST';
 situation_time='09/30/2009 09:03:24.000';
 situation_eventdata='1';
 appl_label='A:P:L';
 hostname='SuperServer.raleigh.ibm.com';
 fqhostname='SuperServer.raleigh.ibm.com';
 origin='9.25.111.201';
 severity='HARMLESS';
 date='09/30/2009';
 msg='Heartbeat Message';END
```

Suceso de restablecimiento maestro

Un restablecimiento maestro se puede configurar para que se envíe cuando se recicla el agente de supervisión. Tras recibir el suceso de restablecimiento maestro, la regla de Netcool/OMNIbus o IBM Tivoli Enterprise Console incluido cierra todos los sucesos abiertos desde este agente en particular y sus subnodos.

Tabla 38. Contenido del suceso de restablecimiento maestro

Ranura	**Valor**
source	"Agente de ITM: Situación privada"
appl_label	"A:P:S"
master_reset_flag	"R"
nombre_host	Nombre de host o dirección IP de la máquina agente
fqhostname	Nombre de host completo, si está disponible
origin	Dirección IP de la máquina agente
situation_name	"**"
situation_origin	Nombre de sistema gestionado del agente
situation_time	Fecha y hora a la que se ha producido el suceso de ciclo de vida
date	Fecha del suceso
situation_status	"N"
severity	"MINOR"
msg	Mensaje que describe que el agente se ha reiniciado. er_reset_flag

Envío de sucesos de situación privada utilizando la comunicación TLS/SSL

Ahora puede enviar sus sucesos de situación privados a un analizador receptor EIF de Netcool/OMNIbus mediante la comunicación TLS/SSL. El EIF de la prueba Netcool/OMNIbus para Tivoli de destino debe ser de la versión 12.0 o posterior.

Complete los pasos siguientes para enviar sucesos de situación privados utilizando la comunicación TLS/SSL:

1. Para cualquier agente de supervisión, defina una o varias situaciones privadas en el archivo XML de situación del agente. Consulte el apartado “Situaciones privadas” en la página 347.
2. Defina uno o más destinos de suceso de Netcool/OMNIbus (type="M") en el archivo XML de destino de suceso del agente de supervisión. especifique SSL="Y" para el elemento <Server> asociado. Consulte el apartado “Especificación XML de configuración de destinos de sucesos de EIF” en la página 405.

   Para obtener más información sobre la configuración de TLS/SSL en Netcool/OMNIbus, consulte "Configuración de una aplicación de receptor de EIF para SSL" en *IBM Tivoli Netcool/OMNIbus Event Integration Facility Reference*.
3. Edite el archivo de entorno del agente de supervisión, donde *cp* es el código de producto de dos caracteres:

   Windows *dir_instalación*\TMAITM6\k*cp*cma.ini.

   Linux UNIX *dir_instalación*/config/cp.ini. Para agentes de supervisión del sistema, el archivo de configuración se *cp*.environment..

   z/OS nombre miembro K*P*CENV en &hilev.&rte.RKANPARU.

   Establezca las variables de entorno siguientes en el archivo de entorno del agente de supervisión:

   Nota: Los valores de las variables de entorno indicadas se aplican a cada conexión segura que el agente establece con todos los destinos de destino (como el servidor de supervisión y el agente de proxy de almacén) y no solo la conexión TLS/SSL establecida con el analizador de EIF de Netcool/OMNIbus de destino.

   - IRA_EVENT_EXPORT_EIF=Y (valor predeterminado)
   - KDEBE_FIPS_MODE_ENABLED=Y o N (valor predeterminado)

     Especifique el valor comparable tal como se define en *nombre_canal*SSLFIPSMode=ON|OFF en el archivo de configuración del análisis EIF. Por ejemplo, si *nombre_canal*SSLFIPSMode=ON, establezca KDEBE_FIPS_MODE_ENABLED=Y.
   - ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y o N (valor predeterminado)

     Especifique el valor comparable tal como se define en *nombre_canal*SSLRequireClientAuthentication=ON|OFF en el archivo de configuración del análisis EIF. Por ejemplo, si *nombre_canal*SSLRequireClientAuthentication=ON, establezca ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y.

     La habilitación de la autenticación de certificado del servidor garantiza que el análisis de EIF es una entidad de confianza porque se necesita presentar un certificado digital firmado por CA.

     Nota: La habilitación de la autenticación de certificado del agente de supervisión significa que cualquier conexión segura iniciada por el agente

requiere que todos los destinos (como, por ejemplo, el servidor de supervisión y el agente de proxy de almacén) presenten un certificado digital firmado por CA para que se establezca la conexión.

4. Las siguientes son las cifras TLS/SSL soportadas por el agente de supervisión de forma predeterminada:
   - TLS_RSA_WITH_AES_256_CBC_SHA
   - TLS_RSA_WITH_AES_128_CBC_SHA
   - SSL_RSA_WITH_3DES_EDE_CBC_SHA

   Asegúrese de que al menos uno de estos cifrados se haya especificado en el parámetro *nombre_canal*SSLcipherList del archivo de configuración del análisis EIF. Si este valor de parámetro no coincide con ninguno de los cifrados TLS y SSL predeterminados, especifique una alteración temporal de cifrado con la variable de entorno KDEBE_V3_CIPHER_SPECS definida en el archivo de entorno del agente.

   De forma predeterminada, el archivo de configuración del analizador de EIF especifica SSL_RSA_WITH_3DES_EDE_CBC_SHA, que coincide con uno de los cifrados de agente de supervisión y, por lo tanto, normalmente no es necesario personalizar la lista de cifrados del agente. Sin embargo, si el parámetro *nombre_canal*SSLCipherList del analizador de EIF no coincide con ninguna de las cifras del agente de supervisión, debe utilizar KDEBE_V3_CIPHER_SPECS para especificar a misma cifra para que se pueda completar el intercambio TLS/SSL. El formato de la variable de entorno es la siguiente:

   KDEBE_V3_CIPHER_SPECS=*nn*

   donde *nn* es el nombre abreviado del cifrado.

   En la tabla siguiente se muestra el nombre abreviado del cifrado y el nombre largo correspondiente que se definiría para el parámetro *nombre_canal*SSLCipherList.

Nombre abreviado	**Nombre largo**
01	SSL_RSA_WITH_NULL_MD5
02	SSL_RSA_WITH_NULL_SHA
03	SSL_RSA_EXPORT_WITH_RC4_40_MD5
04	SSL_RSA_WITH_RC4_128_MD5
05	SSL_RSA_WITH_RC4_128_SHA
06	SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
09	SSL_RSA_WITH_DES_CBC_SHA
0A	SSL_RSA_WITH_3DES_EDE_CBC_SHA
2F	TLS_RSA_WITH_AES_128_CBC_SHA
35	TLS_RSA_WITH_AES_256_CBC_SHA

   Por ejemplo, si *nombre_canal*SSLCipherList=SSL_RSA_WITH_DES_CBC_SHA se define en el archivo de configuración del analizador de EIF, establezca KDEBE_V3_CIPHER_SPECS=09 en el archivo de entorno del agente.

   Nota: La variable KDEBE_V3_CIPHER_SPECS se pasa por alto cuando se define KDEBE_FIPS_MODE_ENABLED=Y. Como resultado, se utilizan los cifrados de TLS y SSL predeterminados.

5. Recicle el agente de supervisión para procesar los cambios en el archivo de entorno del agente, El archivo XML de la situación privada y el archivo XML de destino de sucesos.

Gestión de certificados

Si Netcool/Omnibus EIF Probe utiliza un certificado digital firmado por la entidad emisora (CA) y *nombre_canal*SSLRequireClientAuthentication=YES se especifica en el archivo de configuración del análisis, debe asegurarse de que la base de datos del agente de supervisión haya importando un certificado digital firmado por CA correspondiente.

La configuración de una base de datos de claves del agente de supervisión requiere la utilización de una herramienta de gestión de certificados, que puede ejecutarse en modalidad de CLI o de GUI. Ambas modalidades de funcionamiento requieren un Java Runtime Environment disponible en el sistema local en el que se invoca la herramienta de gestión. Los entornos típicos requieren un mínimo de IBM JRE V6. También debe asegurarse de que la variable de entorno JAVA_HOME apunte a la ubicación de IBM Java. Consulte "Configuración de JRE para GSKit e inicio del gestor de claves" en la página 238.

IBM Tivoli Monitoring y Netcool/OMNIbus se basan en GSKit para su implementaciones de SSL. IBM Tivoli Monitoring V6.3 o posterior instala GSKit V8, que proporciona el programa de utilidad de GUI en el binario `gsk8ikm` y el programa de utilidad de CLI en el binario `<gskittoolcmd>`. Netcool/OMNIbus se basa en GSKit V8, que se ejecuta sólo en la modalidad de CLI; para la modalidad de GUI, debe utilizar el programa de utilidad iKeyman, el cual está incluido en IBM JRE V6, o posterior.

IBM Tivoli Monitoring requiere una base de datos de claves de tipo CMS, mientras que Netcool/OMNIbus requiere una base de datos de Java Key Store (JKS). El archivo de la base de datos de claves de CMS `keyfile.kdb` se instala en el directorio *`dir_instalación`*`\keyfiles`. Sin embargo, no puede utilizar esta base de datos en su formato actual si necesita un certificado digital firmado por CA cuando se envían sucesos a través de una conexión SSL a Netcool/OMNIbus EIF Probe.

Complete las tareas de gestión de certificados del agente utilizando el programa de utilidad iKeyman. Las instrucciones del ejemplo muestran cómo realizar las tareas siguientes:

- Crear una nueva base de datos de claves de CMS, que puede estar ubicada en *`dir_instalación`*`\keyfiles` o en algunos otros directorios
- Importar el certificado digital firmado por CA
- Utilizar la base de datos que se acaba de crear en lugar de la proporcionada por el producto

Ejemplo

El agente de supervisión de ejemplo se ejecuta en un sistema Windows e incluye un archivo de base de datos de claves denominado `omnieif.kdb` con la contraseña `ITMPWD`, un archivo de almacén de claves configurado anteriormente Netcool/OMNIbus denominado `omni.jks` con la contraseña `EIFPWD`, y una etiqueta de certificado denominada `eifca`. Hay una copia del archivo `omni.jks` disponible localmente en el directorio *`dir_instalación`*`\keyfiles`.

Configuración de pulsación de teclas GSKit (modalidad GUI): Para invocar la herramienta de GUI de GSKit en un sistema Windows, siga estos pasos:

1. Ejecute el archivo de mandatos *`dir_instalación`*`\GSK8\bin\gsk8ikm.exe`. Se visualiza la GUI de IBM Key Management. Si se produce un error, compruebe que haya un JRE instalado y que JAVA_HOME esté establecido correctamente.

2. En la barra de menús, pulse **Archivo de base de datos de claves** > **Nuevo**. Especifique la siguiente información en el separador **OK**:

   Tipo de base de datos de claves: `CMS`

   Nombre de archivo: `omnieif.kdb`

   Ubicación: *`dir_instalación`*`\keyfiles\`
3. Especifique la contraseña del almacén de claves y pulse **Aceptar**:

   Contraseña: `ITMPWD`

   Confirmar contraseña: `ITMPWD`

   ☑ Tiempo de caducidad: `366 Days`

   ☑ Guardar contraseña en un archivo
4. Asegúrese de que los **Certificados personales** se muestren en el menú **Contenido de la base de datos de claves**. **Importe** y luego pulse **Aceptar**:

   Tipo de archivo de claves: `JKS`

   Nombre de archivo: `omni.jks`

   Ubicación: *`OMNIbus_keystroke_dir`*`\`
5. Especifique la contraseña para abrir la base de datos de claves de origen: `EIFPWD`. Pulse **Aceptar**.
6. Seleccione claves de la lista de claves de la base de datos de origen. Seleccione la etiqueta `eifca`. Pulse **Aceptar**.
7. Cuando se le solicite `¿Desea cambiar alguna de estas etiquetas antes de llevar a cabo el proceso de importación?` pulse **Aceptar** sin cambiar ninguna etiqueta.
8. Salga de la ventana Gestión de claves de IBM.
9. Edite el archivo de entorno del agente de supervisión y establezca los valores siguientes:

   KDEBE_KEYRING_FILE=*dir_instalación*\keyfiles\omnieif.kdb

   KDEBE_KEYRING_STASH=*dir_instalación*\keyfiles\omnieif.sth

   KDEBE_KEY_LABEL=eifca
10. Reinicie el agente y la nueva base de datos de claves de CMS si se utiliza.

Configuración de almacén de claves de GSKit (modalidad CLI): Si no hay ningún programa de utilidad de GUI de "gestión de claves de IBM" disponible, puede utilizar la herramienta de CLI de GSKit en Windows para realizar la función de importación del certificado. Utilizando los mismos valores elegidos en el ejemplo de interfaz gráfica de usuario, los mandatos son los siguientes:

1. En la línea de mandatos, `cd` al directorio *`dir_instalación`*`\keyfiles` y crear el archivo de base de datos:

   ```
   dir_instalación\GSK8\bin\gsk8cmd.exe -keydb -create -db omnieif.kdb -pw
   ITMPWD -type CMS -stash -expire 366
   ```
2. Ejecute el siguiente mandato para importar el certificado de Netcool/OMNIbus:

   ```
   dir_instalación\GSK8\bin\gsk8cmd.exe -cert -import -file
   OMNIbus_keystore_dir\omni.jks –pw EIFPWD -label eifca -type JKS -target
   omnieif.kdb -target_pw ITMPWD
   ```

   Como en el ejemplo de GUI, debe actualizar estos valores en el archivo de entorno del agente.

   KDEBE_KEYRING_FILE=*dir_instalación*\keyfiles\omnieif.kdb

   KDEBE_KEYRING_STASH=*dir_instalación*\keyfiles\omnieif.sth

   KDEBE_KEY_LABEL=eifca

Interfaz de servicio del agente

Utilice la interfaz de servicio del agente para recuperar información de un agente instalado, tanto si se trata de un Tivoli Enterprise Monitoring Agent como si es un Tivoli System Monitor Agent. Después de iniciar sesión en el sistema operativo local, podrá obtener informes de información del agente, situaciones privadas, historial privado, consultas y atributos y dichas solicitudes como mandatos de lista de carga de configuración.

Se puede acceder a la Interfaz de servicio del agente a través del programa de utilidad IBM Tivoli Monitoring Service Index. La interfaz funciona como un servidor de Internet, acepta y valida las solicitudes, entrega las solicitudes al agente para su proceso y recopila y da formato a los datos de la respuesta utilizando el protocolo de aplicaciones HTTP o HTTPS sobre TCP/IP.

z/OS IBM i La interfaz de servicio del agente no está disponible para su instalación en los sistemas operativos IBM i y z/OS. Sin embargo, puede utilizar las herramientas ITMSUPER incluidas en IBM Support Assistant (ISA), un entorno de servicio de software local gratuito que le ayuda a solucionar dudas y problemas con los productos de software de IBM. Para instalar el software ISA, vaya a IBM Support Assistant (http://www-01.ibm.com/software/support/isa). Como parte del conjunto de herramientas, **itmsa.htm** proporciona acceso directo a informes de agentes en las plataformas IBM i, z/OS, Windows, Linux y UNIX; y **itmsuper.htm** proporciona herramientas de servicios web a los que se puede acceder a través del servidor de supervisión concentrador.

Inicio de la interfaz de servicio del agente

Inicie la interfaz de servicio del agente desde su navegador para ver un menú de opciones para generar informes sobre el agente, obtener el estatus de las situaciones, visualizar el historial a corto plazo y para realizar solicitudes de servicio en XML.

Antes de empezar

Debe tener un ID de usuario administrador para el sistema operativo en el que está instalado el agente de supervisión para poder acceder a la Interfaz de servicio del agente y a sus funciones.

Acerca de esta tarea

Siga estos pasos para iniciar el programa de utilidad IBM Tivoli Monitoring Service Index y luego inicie una sesión en la Interfaz de servicio del agente para el agente sobre el que desea obtener información.

Procedimiento

1. Inicie IBM Tivoli Monitoring Service Index especificando `http://<nombre de host>:1920` o `https//<nombre de host>:3661`, donde nombre de host es el nombre totalmente calificado o la dirección IP del sistema donde está instalado el agente. Se muestra una lista de los servicios iniciados.
2. Pulse el enlace ***cp* Interfaz de servicio del agente** (donde *cp* es el código del componente de dos caracteres) para la aplicación con la que trabajará.
3. Cuando se le solicite, escriba el nombre de usuario y la contraseña de nivel de administrador del sistema operativo.

Resultados

Después de haberse autenticado, se muestra el panel de Navigator de la Interfaz de servicio del agente con enlaces con **Información de agente**, **Situaciones**, **Historial**, **Consultas** y **Solicitudes de interfaz de servicio**. La página Navigator está en el archivo `navigator.htm` que se instala de forma predeterminada en esta ubicación:

Windows *dir_instalación*\localconfig\html

Linux UNIX *dir_instalación*/localconfig/HTML

Los agentes de supervisión que utilizan subnodos, como los supervisores sin agentes, el agente VMware VI y los subnodos creados con Agent Builder, tienen ciertas limitaciones sobre informes en la Interfaz de servicio del agente:

- El enlace Consultas no está disponible
- El listado de situaciones muestra todas las situaciones correspondientes a un agente, incluidos los subnodos; no se puede filtrar por subnodo.
- El historial privado muestra todos los datos históricos recopilados para el atributo seleccionado en el agente, incluidos los subnodos; no se puede filtrar por subnodo.

Perfil de grupo de autorización de acceso

El Perfil de grupo de autorización de acceso (AAGP) contiene las definiciones del grupo de autorización de acceso y las asignaciones de ID de usuario establecidas por el administrador de seguridad.

El administrador de seguridad puede definir cualquier nombre de grupo de autorización de acceso, con la excepción del grupo **Restringido**, que es obligatorio. Cada grupo de autorización de acceso tiene al menos una categoría de componente de agente, como por ejemplo Interfaz de servicio (elemento SIAPI) y servicios publicados por el componente del agente. Cada componente de agente llama al recurso AAGP para obtener el ID de usuario, la categoría del componente y el nombre de servicio solicitado para la autorización de acceso. Tras la autorización, el componente del agente ejecuta el servicio solicitado; de lo contrario, el agente devuelve un estatus de no autorizado.

AAGP no es un servicio de autenticación y da por supuesto que el ID de usuario proporcionado ha sido autenticado. Se realiza el mismo supuesto para la Interfaz de servicio, ya que todos los usuarios primero deben iniciar la sesión en el sistema con un ID y una contraseña válidos. Sin embargo, el agente puede realizar trabajo en nombre de otros agentes o el Tivoli Enterprise Monitoring Server, como por ejemplo acciones de automatización, y el ID de usuario podría ser desconocido para el sistema local. En este caso, el agente considera que el usuario virtual es un miembro fiable de Tivoli Monitoring y por lo tanto auténtico y llama a AAGP para obtener autorización. Como alternativa, AAGP se puede mejorar para que aproveche un servicio de autenticación y autorización en el que dicho recurso esté disponible.

Tipos de grupos de autorización de acceso

Los siguientes grupos predeterminados de AAGP están predefinidos y se cargan automáticamente tras arrancar el agente.

Grupo restringido
: El grupo predeterminado. La categoría Interfaz de servicio de este grupo consta de servicios que ofrecen información del sistema, configuración de

operación, supervisión de carga de trabajo y funciones de notificación de datos históricos. Todos los usuarios están en este grupo obligatorio, incluidos aquellos que no están definidos específicamente.

Grupo de operación
Este grupo incluye los servicios de la categoría de grupo **Restringido** y los servicios de la Interfaz de servicio que ofrecen control de operación, gestión de configuración y funciones de acceso personalizadas de aplicación.

Grupo administrativo
Este grupo tiene acceso a todas las funciones de la Interfaz de servicio, además de Objeto de archivo y actualización dinámica de AAGP.

Tabla 39. Permisos del grupo de autorización de acceso para los mandatos de la interfaz de servicio

API de Interfaz de servicio	Restringido	Operación	Administrativo
AgentInfo	x	x	x
AttrList	x	x	x
ReadAttr	x	x	x
ListSubnode	x	x	x
TableSit	x	x	x
SitStat	x	x	x
SitSummary	x	x	x
HistRead	x	x	x
Informe	x	x	x
PvtControl		x	x
CnfgCommand		x	x
ConfigurationArtifact		x	x
PrivateConfiguration		x	x
Overrides		x	x
AAGP			x
ListAAGP		x	x
FileObj			x

La definición de grupo **Restringido** es obligatoria. Si no se incluye en AAGP, la especificación predeterminada de agente definida en la Tabla 39 entra en vigor.

Si se especifica la palabra clave *NONE para una categoría de componente, se prohíbe a todos los usuarios no explícitos el acceso a dicho servicio de componente. Por ejemplo, `<SIAPI>*NONE</SIAPI>` especificado en el grupo **Restringido** prohíbe el acceso general a la Interfaz de servicio del agente .

FileObj le permite *colocar* o *tomar* archivos de un agente mediante una solicitud HTTP. Para la configuración centralizada, FileObj es la API que se utiliza para permitir que un agente de supervisión actúe como un servidor de configuración central. La Interfaz de servicio del agente está disponible en los servicios básicos del agente de supervisión y se puede utilizar para servir archivos o puede enviar solicitudes HTTP a cualquier agente para colocar o tomar archivos. La función AAGP ofrece seguridad adicional. De forma predeterminada, solo **root** en Linux o

UNIX y **Administrador** en Windows son miembros del grupo AD que tiene permiso para utilizar la API FileObj. Consulte el ejemplo de “Agente de supervisión como servidor de configuración central” en la página 450.

Si AAGP no contiene ninguna especificación <AAGROUP>, la especificación predeterminada de agente que se muestra en la Tabla 39 en la página 418 entra en vigor. Los grupos válidos son RE, OP y AD. No hay necesidad de definir usuarios del grupo R (restringido) porque todos los usuarios se asignan automáticamente al grupo **Restringido** a no ser que AAGP defina lo contrario.

Especificación XML del Perfil de grupo de autorización de acceso

El administrador de seguridad define el Perfil de autorización de grupo de usuarios del agente en formato de especificación XML sencillo:

<AAGP>
Este elemento identifica el archivo XML como un documento de Perfil de grupo de autorización de acceso del agente. Todas las especificaciones de AAGP deben ir entre las etiquetas de elemento de nivel root <AAGP> inicial y </AAGP> final. El contenido del archivo AAGP se fusiona con el AAGP existente que utiliza el agente y puede añadir usuarios a los grupos de autorización de acceso predeterminados. Si prefiere sustituir por completo el AAGP existente, utilice el atributo REFRESH con el elemento AAGP.

REFRESH="Y"
Suprime el AAGP activo actual y lo sustituye por la definición de AAGP de esta especificación de AAGP.

LOCAL="LOCK | UNLOCK"
Opcional, sin valor predeterminado. LOCK y UNLOCK solo se aceptan cuando una actualización de AAGP se originó en ASI.

LOCAL="LOCK" bloquea la configuración de AAGP local, que no se puede actualizar mediante ASI o mediante la descarga del archivo de AAGP del recurso de configuración centralizada.

LOCAL="UNLOCK" desbloquea la configuración de AAGP local y ahora se puede actualizar mediante ASI o la descarga del archivo del recurso de configuración centralizada. UNLOCK solo es válido cuando LOCK está en vigor, de lo contrario, se ignora. Es decir, <AAGP LOCAL="UNLOCK"> debe ir precedido por una operación <AAGP LOCAL="LOCK"> anterior.

<AAGP LOCAL="LOCK"></AAGP> y <AAGP LOCAL="UNLOCK"></AAGP> pueden ser transacciones ASI de AAGP autónomas independientes.

<AAGROUP>
Define un grupo de autorización de acceso. Un conjunto de definiciones de grupo se especifica entre las etiquetas de elemento <AAGROUP> inicial y </AAGroup> final.

<GROUPNAME>
Define el nombre del grupo de autorización de acceso. Especifique el nombre entre las etiquetas de elemento <GROUPNAME> inicial y </GROUPNAME> final. El nombre del grupo puede tener hasta 32 caracteres y los dos primeros caracteres deben ser exclusivos entre todos los nombres de grupos de usuarios.

<INCLUDE>
Opcional. Especifique las definiciones de AAGROUP que se van a incluir en

este AAGROUP. Defina el nombre de AAGROUP entre las etiquetas <INCLUDE> inicial y </INCLUDE> final.

<SIAPI>
Especifica el nombre de la API de la interfaz de servicio del agente y no es sensible a mayúsculas y minúsculas. Solo la categoría de componente se define en este momento. Especifique el nombre entre las etiquetas <SIAPI> inicial y </SIAPI> final.

<other>
El elemento <other> no está disponible en el release actual; está reservado para su futuro uso. Especifica los otros servicios de componentes del agente que se van a gestionar.

<AAUSER>
Define un ID de usuario autorizado y su grupo de autorización de acceso asociado por nombre. Especifique cada definición de usuario entre las etiquetas <AAUSER> inicial y </AAUSER> final.

<ID>
Especifica un ID de inicio de sesión de usuario autorizado y no es sensible a mayúsculas y minúsculas. Especifique el ID de usuario entre las etiquetas <ID> inicial y </ID> final.

<ASSIGN>
Especifica la asignación de grupo de autorización de acceso y no es sensible a mayúsculas y minúsculas. Los tipos de AAGP válidos son RE (**Restringido**), OP (**Operación**) y AD (**Administrativo**). Puede especificar el nombre de grupo completo o el primer carácter. Especifique el tipo de AAGP entre etiquetas <ASSIGN> inicial y </ASSIGN> final.

Ejemplo

```
<AAGP>
 <AAGROUP>
  <GROUPNAME>Restricted</GROUPNAME>
  <SIAPI>AgentInfo</SIAPI>
  <SIAPI>AttrList</SIAPI>
  <SIAPI>ReadAttr</SIAPI>
  <SIAPI>ListSubnode</SIAPI>
  <SIAPI>TableSit</SIAPI>
     <SIAPI>ListTable</SIAPI>
   <SIAPI>SitStats</SIAPI>
  <SIAPI>SitSummary</SIAPI>
  <SIAPI>HistRead</SIAPI>
  <SIAPI>Report</SIAPI>
   <REFLEXAUTO>ExecAction</REFLEXAUTO>
 </AAGROUP>
 <AAGROUP>
  <GROUPNAME>Operation</GROUPNAME>
  <INCLUDE>Restricted</INCLUDE>
  <SIAPI>PvtControl</SIAPI>
  <SIAPI>CnfgControl</SIAPI>
  <SIAPI>CnfgCommand</SIAPI>
   <SIAPI>ConfigurationArtifact</SIAPI>
  <SIAPI>PrivateConfiguration</SIAPI>
  <SIAPI>Overrides</SIAPI>
     <SIAPI>XMSClientSpec</SIAPI>
   <SIAPI>ListAAGP</SIAPI>
     <CLI>ExecCommand</CLI>
   <TAKEACTION>ExecAction</TAKEACTION>
 </AAGROUP>
 <AAGROUP>
  <GROUPNAME>Administrative</GROUPNAME>
```

```
  <INCLUDE>Operation</INCLUDE>
  <SIAPI>FileObj</SIAPI>
  <SIAPI>AAGP</SIAPI>
 </AAGROUP>
 <AAUSER>
   <ID>default</ID>
  <ASSIGN>OP</ASSIGN>
 </AAUSER>
  </AAGP>
```

Metodología del grupo de autorización de acceso

Todos los usuarios del sistema válidos están autorizados automáticamente para el acceso al grupo **Restringido**. El administrador de seguridad de la empresa define los usuarios del grupo autorizado, **administrativo** y otros grupos a través de AAGP. El siguiente procedimiento ilustra la metodología de AAGP.

1. El administrador de seguridad de la empresa crea un AAGP personalizado y lo almacena en un servidor de configuración central seguro. El contenido del grupo de autorización predefinido se puede personalizado y se pueden añadir grupos de autorización personalizados adicionales. Por ejemplo, `<AUTOCMD>KILL</AUTOCMD>` se podrían incluir en el grupo **Operación**.
2. El agente de supervisión inicia y activa el AAGP predeterminado. Un ID administrativo se define como miembro del grupo **Administrativo** de forma predeterminada: *Administrador* en Windows; *root* en Linux o UNIX.
3. El agente de supervisión aprovecha la configuración centralizada y recupera su propio AAGP personalizado de un servidor de configuración central. El agente siempre elige el protocolo HTTPS para esta operación. Si no se incluye ningún AAGP en la lista de carga de configuración del agente o si el AAGP no se puede descargar del servidor de configuración central, el agente funciona en esta modalidad hasta el siguiente reinicio.
4. Los componentes del agente comprueban la autorización de AAGP, que proporciona el ID de usuario, la categoría del componente y el nombre del servicio. El AAGP otorga o deniega el acceso en función del grupo de autorización de acceso y de la asignación de ID de usuario.
5. El agente de supervisión comprueba si hay actualizaciones de AAGP periódicamente según lo especificado en la lista de carga de configuración o cuando se emite el mandato de configuración de la interfaz de servicio.
6. El agente de supervisión no guarda ni almacena el perfil de autorización de usuario localmente.

Configuración persistente de AAGP local

Un administrador puede que necesite realizar cambios de personalización de AAGP para conseguir los objetivos ad-hoc. Por ejemplo, añadir ID de usuario contratista temporal o reorganizar los servicios de categorías por restricciones de acceso de entorno local. Los pasos siguientes describen el procedimiento para implementar cambios de configuración de AAGP local que persistan entre los reinicios del agente:

1. Inicie sesión en el sistema local a través de la interfaz de servicio de agente utilizando un ID de usuario administrador.
2. Utilice la transacción <ListAAGP> para recuperar la especificación de AAGP actual del agente.
3. Edite la salida de ListAAGP para los nuevos requisitos. Por ejemplo, añadir otro ID de usuario autorizado.

4. Enviar las definiciones de AAGP actualizadas al agente a través de la interfaz de servicio de agente.
5. El agente procesa las definiciones de AAGP de entrada que se convierten en la definición de AAGP activa actualmente en vigor. El agente también produce una copia del XML de configuración de AAGP en un archivo local, *ITM_HOME/localconfig/pc/pc*_aagpcnfg.txt en sistemas distribuidos o K*pc*AAGPX.UKANDATV en formato cifrado en sistemas Z/OS.
6. En el siguiente inicio, el agente busca el archivo de configuración de AAGP persistente local, descifra y lee el archivo y, a continuación, procesa todas las sentencias XML de AAGP. Estas acciones restauran las definiciones de AAGP personalizadas anteriormente. Si el agente no puede encontrar el archivo de configuración de AAGP local persistente, las definiciones de AAGP predeterminadas entran en vigor.
7. Mientras que la configuración de AAGP personalizada localmente está en vigor, el agente suspende todas las actualizaciones de AAGP del recurso de configuración centralizada, asegurándose de que los valores de personalización permanecen de AAGP local permanecen sin cambios. El administrador debe enviar una solicitud <AAGP Resume="Y"> a través de la interfaz de servicio de agente para desbloquear la configuración persistente de AAGP local. Esto permite que el recurso de configuración centralizada reanude su soporte a las operaciones de actualización de AAGP.

Control de autorización de AAGP local

Si el administrador desea imponer controles de autorización estrictos en un punto final de agente y no permitir que se ejecuten las solicitudes de automatización, a menos que el ID de usuario esté definido en el sistema local, puede utilizar el procedimiento siguiente para habilitar el control de autorización de AAGP local:

1. Inicie sesión en el sistema local a través de la interfaz de servicio de agente utilizando un ID de usuario administrador.
2. Utilice la transacción <ListAAGP> para recuperar la especificación de AAGP actual del agente.
3. Edite la salida de ListAAGP y suprima la definición de usuario predeterminada.

```
<AAUSER>
   <ID>default</ID>
     <ASSIGN>OP</ASSIGN>
</AAUSER>
```

4. La definición de usuario predeterminada indica a AAGP que cree un ID de usuario secreto interno al que se le otorga autorización para ejecutar la automatización. Sin la definición de ID de usuario predeterminado, AAGP extrae el ID de usuario de cada solicitud de mandato enviado al agente. Si el ID de usuario extraído está sin definir para AAGP, la solicitud de mandato se rechaza con un error de autorización. Esta posibilidad proporciona al administrador local el control total sobre la automatización que está permitido ejecutar en un punto final del agente.
5. Envíe las definiciones de AAGP actualizadas al agente a través de la interfaz de servicio de agente.

Interfaz de servicio del agente - Información de agente

Seleccione **Información de agente** en el menú Interfaz de servicio del agente para recuperar un informe de datos sobre el agente, incluidos los valores de archivos del entorno.

HOSTNAME
Es el nombre completo del sistema, como por ejemplo **myitm.raleigh.ibm.com**.

NODENAME
Es el nombre del sistema gestionado, como por ejemplo **Primary:MYITM:NT**.

SUBSYSID
Si el agente tiene subnodos (subagentes), este es el nombre. De lo contrario, el ID del subsistema es **Primary**.

NODEINFO
Es el tipo de sistema y plataforma operativa, como por ejemplo **Win2003~5.2-SP2**.

PRODUCT
Es el código del producto de dos caracteres del agente, como por ejemplo **NT**.

VERSION
Es la versión instalada del agente, como por ejemplo **06.22.00**.

LEVEL A=00:WINNT C=06.22.00.00:WINNT G=06.22.00.00:WINNT

PATCHLEVEL A=00:WINNT;C=06.22.00.00:WINNT;G=06.22.00.00:WINNT;

AFFINITY
Es el valor que identifica la afinidad del agente con los componentes de Tivoli Management Services. Por ejemplo, **%IBM.STATIC021 000000000A00000u0a4**.

BOOTTIME
Es el día de la semana, la fecha y hora de calendario en que ha finalizado el arranque del agente, como por ejemplo **Wed Jul 29 15:15:33 2009**.

ENVFILE
Es una lista de los valores de parámetros actuales del archivo de entorno del agente. Si tiene que cambiar alguno de los valores, puede abrir el archivo de entorno con Manage Tivoli Monitoring Services o con un editor de texto en sistemas distribuidos.

A continuación se muestra un ejemplo del archivo de entorno del SO Windows tal como se muestra en el informe Información de agente:

```
* CANDLE_HOME=d:\IBM\ITM
* KBB_RAS1=ERROR
* KBB_VARPREFIX=%
* KBB_VARPREFIX=$
* KBB_RAS1_LOG=d:\IBM\ITM\tmaitm6\logs\$(computername)_nt_kntcma_$
(sysutcstart)-.log INVENTORY=d:\IBM\ITM\tmaitm6\logs\$(computername)
_nt_kntcma.inv COUNT=03 LIMIT=5 PRESERVE=1 MAXFILES=9
* TIMEOUT=600
* ITMDEPLOY_AGENTDEPOT=d:\IBM\ITM\tmaitm6\agentdepot
* ICCRTE_DIR=d:\IBM\ITM\GSK8
* CSV1_PATH=d:\IBM\ITM\GSK8\lib
* CSV2_PATH=d:\IBM\ITM\GSK8\bin * KBB_VARPREFIX=$
* PATH!=$(CSV1_PATH);$(CSV2_PATH);$(PATH)
* KEYFILE_DIR=d:\IBM\ITM\keyfiles
* KDEBE_KEYRING_FILE=d:\IBM\ITM\keyfiles\keyfile.kdb
* KDEBE_KEYRING_STASH=d:\IBM\ITM\keyfiles\keyfile.sth
* KDEBE_KEY_LABEL=IBM_Tivoli_Monitoring_Certificate
* KBB_IGNOREHOSTENVIRONMENT=Y
* JAVA_HOME=d:\IBM\ITM\java\java70\jre
* KBB_IGNOREHOSTENVIRONMENT=N
* PATH=d:\IBM\ITM\GSK8\LIB;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\
```

```
System32\Wbem;D:\IBM\SQLLIB\BIN;D:\IBM\SQLLIB\FUNCTION;D:\IBM\SQLLIB\
SAMPLES\REPL;d:\IBM\ITM\bin;d:\IBM\ITM\bin\dll;d:\IBM\ITM\InstallITM;
d:\IBM\ITM\TMAITM6;d:\IBM\ITM\InstallITM
```

Interfaz de servicio del agente - Situaciones

Seleccione la opción **Situaciones** de la Interfaz de servicio del agente para ver el estatus y estadísticas de cada situación, incluidas situaciones privadas y situaciones distribuidas a subnodos, correspondiente al agente de supervisión.

El informe Situaciones ofrece ciertas estadísticas vitales sobre cada situación del agente. El valor de la variable de entorno del agente IRA_EVENT_EXPORT_SIT_STATS determina el nivel de detalle proporcionado.

Nombre de la situación
Sobre cada página de resumen de situación está el nombre de la situación. Si se trata de una situación privada, el nombre irá seguido de **_pr**.

TYPE Muestra o puro. Una situación es de muestra si toma muestras de datos a intervalos regulares. Los sucesos puros son notificaciones no solicitadas. El registro de sucesos de Windows y el atributo Cambio de archivo de Windows son ejemplos de grupos de atributos que notifican sucesos puros.

INTERVAL
El intervalo entre muestras de datos, en segundos. Si las situaciones correspondientes a este grupo de atributos activan sucesos puros, no hay intervalo de muestre y el valor es 0.

ROWSIZE
Es el tamaño de fila.

FIRSTSTARTTIME
Es el día de la semana, día del calendario y hora en que se ha iniciado por primera vez la situación después de que se iniciara el agente.

LASTSTARTTIME
Es el día de la semana, día del calendario y hora del inicio más reciente de la situación.

LASTSTOPTIME
Es el día de la semana, día del calendario y hora de la detención más reciente de la situación.

FIRSTEVENTTIME
Es el día de la semana, día del calendario y hora de la primera vez en que la situación se ha convertido en verdadera y ha abierto un suceso desde que se inició la situación.

LASTTRUETIME
Es el día de la semana, día del calendario y hora de la última vez que la situación se ha convertido en verdadera y ha abierto un suceso.

LASTFALSETIME
Es el día de la semana, día del calendario y hora en que el estado de la situación se ha evaluado como falso después de que un muestreo anterior se evaluara como verdadero.

TIMESRECYCLED
Es el número de veces que la situación se ha detenido e iniciado desde que el agente está en línea.

TIMESAUTONOMOUS
Es el número de veces desde el arranque en que la situación ha entrado en

estado autónomo porque el agente de supervisión de empresa estaba desconectado del servidor de supervisión, seguido de estadísticas DAY:

DAY

DATE (fecha) en que se han recopilado los datos estadísticos más recientes. Si se trata de una situación de empresa, es desde que el agente se conectó por última vez.

TRUESAMPLES es el número de veces que la situación se ha evaluado como verdadera mientras el agente estaba desconectado del servidor de supervisión.

FALSESAMPLES es el número de veces que la situación se ha evaluado como falsa tras una anterior evaluación como verdadera mientras el agente estaba desconectado del servidor de supervisión.

TRUERATIO es el porcentaje del número de veces que la situación se ha evaluado como verdadera en comparación con el estado de falsa.

FALSERATIO es el porcentaje del número de veces que la situación se ha evaluado como falsa en comparación con el estado de verdadera.

HOURROWS es el número de filas de datos que se han incluido en el informe.

HOURTRUE es el número de horas que la situación ha permanecido verdadera mientras el agente estaba desconectado del servidor de supervisión.

HOURFALSE es el número de horas que la situación ha permanecido falsa mientras el agente estaba desconectado del servidor de supervisión.

Se muestran todas las situaciones correspondiente a un agente, incluidos los subnodos. En este agente TestLab de ejemplo con subnodos llamados ComputerA y ComputerB, se listarían diez situaciones:

TestLab

SubNodeA (4 situaciones exclusivas, más 2 situaciones también están en SubNodeB)

SubNodeB (4 situaciones exclusivas, más 2 situaciones que también están en SubNodeA)

Interfaz de servicio del agente - Historial

Seleccione **Historial** en la Interfaz de servicio del agente para ver muestras de datos históricos privados que se han guardados para la tabla del grupo de atributos seleccionado.

Puede filtrar el informe para que solo muestre los atributos en los que está interesado borrando la marca del recuadro de selección que hay junto a los atributos que no desee. Seleccione una fecha y hora iniciales y una fecha y hora finales y pulse **Informe**. El informe se muestra en una tabla bajo los atributos y visualiza muestras de datos históricos para el grupo de tributos, una columna por atributo y una fila por muestra, para el periodo de tiempo especificado, con un máximo de 5000 filas. Si no ve las filas que le interesan dentro de este límite de 5000, puede generar otro informe reduciendo el intervalo de tiempo.

Se muestran todos los datos históricos recopilados para el agente, incluidos los subnodos.

Interfaz de servicio del agente - Consultas

Seleccione la opción **Consultas** de la Interfaz de servicio del agente para consultar en el archivo k*cp*.atr el grupo de atributos seleccionados, que se muestran por nombre de tabla. Un informe es una lista de atributos, su nombre de columna y nombre de visualización y características. El otro informe muestra los valores de muestra actuales de los atributos.

Seleccione un nombre de tabla en la lista para ver los atributos de componente y un informe de los datos de muestra.

Nombre de tabla
Es el nombre de la tabla correspondiente al grupo de atributos tomado del archivo <*dir_instalación*>/ TMAITM6/ATTRLIB/k*cp*.atr (donde *cp* es el código de producto de dos caracteres).

Nombre
Es el nombre de columna del atributo. No se utiliza en situaciones privadas ni en el historial privado, pero es lo que vería si deseara buscar datos almacenados en Tivoli Data Warehouse.

Visualización
Es el nombre detallado del atributo, formateado como *Nombre_Grupo_Atributos.Nombre_Atributo*, y es lo que especifica en definiciones de situaciones privadas y de historiales privados. Por ejemplo, KHD_CONFIG.Connection_Pool_Size o NT_Registry.Server_Name.

Tipo En esta columna se muestra un número que representa el tipo de atributo que es; por ejemplo, 4 indica un atributo enumerado entero. El tipo no se utiliza directamente en una definición de situación privada o de historial de situaciones, pero le informa del formato necesario para el valor del atributo.

Longitud
Es el número de bytes o número máximo de bytes posible para el valor del atributo. Para atributos TIMESTAMP, 16 indica el siguiente formato: SAAMMDDHHMMSSmmm, como por ejemplo 1090819160501000 para siglo XXI, 19 de agosto de 2009 a las 4:05:01 PM

Mínimo
Muestra el valor mínimo posible para el atributo. Si el campo está vacío, significa que no hay valor mínimo para el atributo.

Máximo
Esta columna muestra el valor más alto posible para el atributo. Si el campo está vacío, significa que no hay valor máximo para el atributo.

ENUMS
Es la enumeración y lo que representa para un atributo. Algunos atributos enumerados tienen varias enumeraciones. Cuando componga una situación privada para un atributo enumerado, utilice el valor real de la fórmula y no el valor de visualización (lo que ve en Tivoli Enterprise Portal).

Estos dos informes muestran el resultado de una consulta a un grupo de atributos de Dirección IP de Windows, nombre de tabla NTIPADDR. El primer informe es un listado de los atributos de la tabla, tal como aparecen en el archivo k*cp*.atr. Cuando se cree situaciones privadas o definiciones de historial privadas, tiene que utilizar el nombre que se muestra en la columna **Visualización**.

Tabla 40. Interfaz de servicio del agente - Listado de atributos de muestra de consultas

Nombre	Visualización	Tipo	Longitud	Mínimo	Máximo	ENUMS
ORIGINNODE	NT_IP_Address.System_Name	2	64			
TIMESTAMP	NT_IP_Address.Timestamp	2	16			
INTFNAME	NT_IP_Address.Network_ Interface_Name	3				No está disponible para Windows 2000
IPADDRESS	NT_IP_Address.IP_Address	2	50			
DNSNAME	NT_IP_Address.DNS_Name	10	388			Sin entrada DNS
IPVERSION	NT_IP_Address.IP_Version	4		-2147483648	2147483647	4 IPv4 6 IPv6 10 IPv4_IPv6
MACADDRESS	NT_IP_Address.MAC_Address	2	28			

El segundo informe se muestra con los valores de muestra actuales del grupo de atributos.

Tabla 41. Interfaz de servicio del agente - Informe de muestra de consultas

ORIGINNODE	TIMESTAMP	INTFNAME	IPADDRESS	DNSNAME	IPVERSION	MACADDRESS
Primary:East:NT	1090819142128111	11a_b_g Wireless LAN Mini PCI Adapter	9.52.100.111	East.ibm.com	4	00054e48f5bd
Primary:East:NT	1090819142128111	Interfaz MS TCP Loopback	127.0.0.1	NO_DNS_ ENTRY	4	000d608b2938

Interfaz de servicio del agente - Solicitud de interfaz de servicio

Seleccione **Solicitud de interfaz de servicio** en la Interfaz de servicio del agente para especificar mandatos en formato XML para obtener información sobre el agente, como por ejemplo definiciones de grupos de atributos.

Solicitud de la Interfaz de servicio del agente - Información de agente

Se trata de una solicitud de información de identificación del agente. Los datos recuperados están en tres secciones: ID de agente, que incluye nombre de host del sistema, nombre del sistema gestionado, lista de subnodos e información sobre sistema operativo; ID de producto, que incluye nombre de producto, versión, datos sobre nivel de mantenimiento y de parches, afinidad y características del producto; e ID de entorno, que incluye los valores de las variables de entorno actuales.

Entrada de la solicitud

Tabla 42. Solicitud <AGENTINFO> de la Interfaz de servicio del agente

Etiqueta	Descripción
<AGENTINFO>	Especifique etiquetas AGENTINFO inicial y final para realizar una solicitud de propiedad de agente.

Solicitud de ejemplo:

```
<AGENTINFO>
</AGENTINFO>
```

Salida del informe

Tabla 43. Salida de la solicitud <AGENTINFO> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<HOSTNAME>	Nombre de host del agente
<NODENAME>	Nombre del sistema gestionado del agente
<SUBSYSID>	ID del subsistema del agente
<NODEINFO>	Información sobre el SO del sistema del agente
<PRODUCT>	Nombre del producto ITM
<VERSION>	Versión del agente
<LEVEL>	Nivel de mantenimiento y de instalación del agente
<PATCHLEVEL>	Nivel de parches de mantenimiento del agente
<AFFINITY>	Afinidad del agente en vigor
<BOOTTIME>	Hora de arranque del agente
<ENVFILE>	Archivo de configuración del agente entre etiquetas de datos de control CDATA[]
<STATUS>	Código de estatus de retorno especificado entre etiqueta inicial y final

Salida de ejemplo: El agente devuelve datos sobre propiedades

```
<AGENTINFO>
  <HOSTNAME>dyang7</HOSTNAME>
  <NODENAME>Primary:DYANG7:NT</NODENAME>
  <SUBSYSID>Primary</SUBSYSID>
  <NODEINFO>WinXP~5.1-SP2</NODEINFO>
  <PRODUCT>NT</PRODUCT>
  <VERSION>06.22.00</VERSION>
 <LEVEL>A=00:WINNT C=06.21.00.00:WINNT G=06.21.00.00:WINNT</LEVEL>
 <PATCHLEVEL>A=00:WINNT;C=06.21.00.00:WINNT;G=06.21.00.00:WINNT;
 </PATCHLEVEL>
 <AFFINITY>0008000000000000000000000000000004000000u0a4</AFFINITY>
  <BOOTTIME>Mon Mar 02 22:48:27 2009</BOOTTIME>
  <ENVFILE>
   <![CDATA[
   CANDLE_HOME=C:\IBM\ITM
   KBB_RAS1=ERROR
   KBB_VARPREFIX=%
   TIMEOUT=600
   ITMDEPLOY_AGENTDEPOT=C:\IBM\ITM\tmaitm6\agentdepot
   IRA_AUTONOMOUS_MODE=Y
   CTIRA_HEARTBEAT=1440
   CTIRA_RECONNECT_WAIT=60
   IRA_DUMP_DATA=Y
   IRA_DEBUG_TRANSCON=N
   IRA_DEBUG_EVENTEXPORT=N
   IRA_DEBUG_AUTONOMOUS=Y
   IRA_DEBUG_SERVICEAPI=Y
   IRA_DEBUG_PRIVATE_SITUATION=Y
   IRA_EVENT_EXPORT_LISTSTAT_INTERVAL=300
   IRA_EVENT_EXPORT_SNMP_TRAP=Y
   ICCRTE_DIR=C:\IBM\ITM\GSK8
   CSV1_PATH=C:\IBM\ITM\GSK8\lib
   PATH!=$(CSV1_PATH);$(PATH)
   KEYFILE_DIR=C:\IBM\ITM\keyfiles
```

```
    KDEBE_KEYRING_FILE=C:\IBM\ITM\keyfiles\keyfile.kdb
    KDEBE_KEYRING_STASH=C:\IBM\ITM\keyfiles\keyfile.sth
    KDEBE_KEY_LABEL=IBM_Tivoli_Monitoring_Certificate
    JAVA_HOME=C:\Program Files\IBM\Java70\jre
    PATH=C:\IBM\ITM\GSK8\LIB;\;C:\WINDOWS\system32;C:\WINDOWS;
    C:\WINDOWS\System32\Wbem;c:\perl\bin;C:\Infoprint;
     C:\IBM\ITM\InstallITM ]]>
  </ENVFILE>
</AGENTINFO>
```

Solicitud de la Interfaz de servicio del agente - Lista de subnodos del agente

Utilice la solicitud <LISTSUBNODE> en la solicitud de la Interfaz de servicio para obtener una lista de todos los subnodos conocidos en este sistema.

Entrada de la solicitud

Tabla 44. Solicitud <LISTSUBNODE> de la Interfaz de servicio del agente

Etiqueta	Descripción
<LISTSUBNODE>	Especifique las etiquetas LISTSUBNODE inicial y final para realizar una solicitud de lista de subnodos.

Solicitud de ejemplo:

```
<LISTSUBNODE>
</LISTSUBNODE>
```

Salida del informe

Tabla 45. Salida de la solicitud <LISTSUBNODE> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<SUBNODELIST>	Lista de subnodos.
<NODECOUNT>	Recuento de subnodos.
<NAME>	Nombre de subnodo.

Salida de ejemplo: El agente devuelve una lista de todos los subnodos conocidos del agente

```
<SUBNODELIST>
  <NODECOUNT>3</NODECOUNT>
  <NAME>dyang7ASFSdp:UAGENT00</NAME>
  <NAME>dyang7:TS100</NAME>
  <NAME>dyang7:TS200</NAME>
  </SUBNODELIST>
```

Solicitud de la Interfaz de servicio del agente - Lista de archivos de atributos

Utilice <ATTRLIST> en una solicitud de la Interfaz de servicio para obtener una lista de todos los archivos de atributos (.atr) conocidos que están disponibles en este sistema.

Entrada de la solicitud

Tabla 46. Solicitud <ATTRLIST> de la Interfaz de servicio del agente

Etiqueta	Descripción
<ATTRLIST>	Especifique etiquetas ATTRLIST inicial y final para realizar una solicitud de lista de archivos de atributos.

Solicitud de ejemplo:

```
<ATTRLIST>
</ATTRLIST>
```

Salida del informe

Tabla 47. Salida de la solicitud <ATTRLIST> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<LISTATTRFILE>	Lista de nombres de archivos de atributos disponibles.
<ATTRCOUNT>	El número total de archivos de atributos de la lista.
<NAME>	Nombre del archivo de atributos.

Salida de ejemplo: El agente devuelve una lista de todos los archivos de atributos conocidos que están disponibles en el sistema

```
<LISTATTRFILE>
  <ATTRCOUNT>16</ATTRCOUNT>
  <NAME>DM3ATR00</NAME>
 <NAME>TS1ATR00</NAME>
 <NAME>TS2ATR00</NAME>
 <NAME>UAGATR00</NAME>
 <NAME>kdy.atr</NAME>
 <NAME>khd.atr</NAME>
 <NAME>kib.atr</NAME>
 <NAME>knt.atr</NAME>
 <NAME>kr2.atr</NAME>
 <NAME>kr3.atr</NAME>
 <NAME>kr4.atr</NAME>
 <NAME>kr5.atr</NAME>
 <NAME>kr6.atr</NAME>
 <NAME>ksh.atr</NAME>
 <NAME>ksy.atr</NAME>
 <NAME>kum.atr</NAME>
</LISTATTRFILE>
```

Solicitud de la Interfaz de servicio del agente - Contenido de los archivos de atributos

Utilice <READATTR> en una solicitud de la Interfaz de servicio para obtener un listado del contenido del archivo de atributos (.atr) especificado del sistema.

Entrada de la solicitud

Tabla 48. Solicitud <READATTR> de la Interfaz de servicio del agente

Etiqueta	Descripción
<READATTR>	Especifique etiquetas READATTR inicial y final para realizar una solicitud de archivo de atributos.
<ATTRFILE>	Nombre del archivo de atributos.

Ejemplo de una solicitud para el archivo de atributos TS2ATR00 de Universal Agent:

```
<READATTR>
  <ATTRFILE>TS2ATR00</ATTRFILE>
</READATTR>
```

Salida del informe

Tabla 49. Salida de la solicitud <READATTR> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<ATTRFILE>	Nombre del archivo de atributos.
<ATTRDATA>	Registros del archivo de atributos.

Este ejemplo muestra el contenido del archivo de atributos TS2ATR00:

```
<ATTRFILE>TS2ATR00</ATTRFILE>
  <ATTRDATA>
 <![CDATA[//1090428005244020 TS200/06.00.00
 //Generado por Universal Agent
  //
  entr ATTR
  name TS2TCPIOQ00.Node_Name
  affi 00000000000000080000000000000000000000000000
  acod TS200
  usag I
  appl TS200
  stmp 1090428005244020
  cvrm 06.00.00
  lvrm 06.00.00
  tabl TS24601600
  mult 1
  samp 3
  colu ORIGINNODE
  type 2
  slng 32
  msid KUM0000
  opgr 0
  atid 065535
  //entr ATTR
  name TS2TCPIOQ00.LocalApplAddress
  atom y
  affi 00000000000000080000000000000000000000000000
  acod TS200
  colu UA1
  type 2
  slng 24
  msid KUM0000
  opgr 2
  atid 065535
  //
  entr ATTR
  name TS2TCPIOQ00.TargetApplAddress
  affi 00000000000000080000000000000000000000000000
  acod TS200
  colu UA2
  type 2
  slng 24
  msid KUM0000
  opgr 2
  atid 065535
  //
  entr ATTR
  name TS2TCPIOQ00.SendQueueSize
  affi 00000000000000080000000000000000000000000000
  acod TS200
  colu UA3
  type 1
  msid KUM0000
  opgr 2
  atid 065535
```

```
 mini -2147483648
 maxi 2147483647
 //
 entr ATTR
 name TS2TCPIOQ00.RecvQueueSize
 affi 00000000000000080000000000000000000000000000
 acod TS200
 colu UA4
 type 1
 msid KUM0000
 opgr 2
 atid 065535
 mini -2147483648
 maxi 2147483647
 //
 entr ATTR
 name TS2TCPIOQ00._LocalTimeStamp
 affi 00000000000000080000000000000000000000000000
 acod TS200
 colu UA5
 type 2
 slng 16
 msid KUM0000
 opgr 2
 atid 065535
 //
 entr HIDDEN
 name TS2TCPIOQ00.KUMHELP
 affi 00000000000000080000000000000000000000000000
 colu KUMHELP
 type 3
 opgr 0
 cost 9
 vali ^APPLICATION
 vale "No hay ayuda de aplicación definida"
 vali ^ATTRGROUP[TCPIOQ]
 vale "No hay ayuda de grupo de atributos definida"
 vali LocalApplAddress
 vale "No hay ayuda de atributos definida"
 vali TargetApplAddress
 vale "No hay ayuda de atributos definida"
 vali SendQueueSize
 vale "No hay ayuda de atributos definida"
 vali RecvQueueSize
 vale "No hay ayuda de atributos definida"
 vali _LocalTimeStamp
 vale "Universal Agent ha insertado un atributo para la especificación de la
 palabra clave de metarchivo AddTimeStamp. Es un valor de indicación de fecha
 y hora de 16 bytes que indica cuándo han llegado los datos."
]]></ATTRDATA>
</ATTROUTPUT>
```

Interfaz de servicio del agente - Informe de grupo de atributos

Utilice <REPORT> en una solicitud de la Interfaz de servicio para obtener un informe del grupo de atributos especificado en el atributo TABLENAME, como por ejemplo UNIXOS o NTPROCESS.

Entrada de la solicitud

Tabla 50. Solicitud <REPORT> de la Interfaz de servicio del agente

Etiqueta	Descripción
<REPORT>	Especifique las etiquetas REPORT inicial y final para recuperar datos de la tabla de aplicación correspondiente a la tabla especificada.

Tabla 50. Solicitud <REPORT> de la Interfaz de servicio del agente (continuación)

Etiqueta	Descripción
<SQLTABLE>	El par de etiquetas TABLENAME se especifica entre las etiquetas SQLTABLE inicial y final para identificar el conjunto de la definición de la tabla SQL.
<TABLENAME>	El nombre de la tabla de la que hay que hacer el informe se especifica entre las etiquetas TABLENAME inicial y final. Es el nombre tal como aparece entre las etiquetas inicial y final. Si no está seguro de cómo se escribe el nombre de la tabla, lo encontrará en el campo **tabl** del archivo .atr del agente, situado en el directorio *<dir_instalación>*/TMAITM6/ATTRLIB.
<OUTPUT>	Opcional. Utilice las etiquetas OUTPUT inicial y final y sus etiquetas subordinadas para filtrar y definir mejor el informe. **<COLUMN>** Defina el nombre de columna seleccionado entre las etiquetas inicial y final. **<FILTER>** Defina los criterios de filtro de filas de datos de salida con etiquetas inicial y final. El filtro sigue la misma sintaxis que el elemento <CRITERIA> de la situación privada. Consulte el apartado "Especificación XML de situaciones privadas" en la página 351.

Solicitud de ejemplo 1: Crear un informe de todos los atributos de la tabla del SO UNIX

```
<REPORT>
 <SQLTABLE>
 <TABLENAME>UNIXOS</TABLENAME>
 </SQLTABLE>
</REPORT>
```

Solicitud de ejemplo 2: Informe de resumen del grupo de atributos de proceso de Windows con un filtro y columnas especificadas

La solicitud es para los valores de la fila *_Total*.

```
<REPORT>
 <SQLTABLE>
 <TABLENAME>NTPROCESS</TABLENAME>
   <OUTPUT>
    <COLUMN>ORIGINNODE</COLUMN>
    <COLUMN>TIMESTAMP</COLUMN>
    <COLUMN>INSTCNAME</COLUMN>
    <COLUMN>IDPROCESS</COLUMN>
    <COLUMN>PCTPRCSTME</COLUMN>
    <COLUMN>THREADCNT</COLUMN>
    <COLUMN>WRKINGSET</COLUMN>
   </OUTPUT>
 <FILTER>
 <![CDATA[ *VALUE INSTCNAME  *EQ _Total]]>
 </FILTER>
 </SQLTABLE>
</REPORT>
```

Salida del informe

Tabla 51. Salida de la solicitud <REPORT> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<REPORTDATA>	Identifica el conjunto de datos de salida del informe.
<STATUS>	Código de estatus de retorno especificado entre etiqueta inicial y final
<ROWCOUNT>	Recuento de filas de la tabla de salida.

Tabla 51. Salida de la solicitud <REPORT> de la Interfaz de servicio del agente (continuación)

Etiqueta de salida	Descripción
<ROW>	Identifica datos de una fila de salida.
<NAME>	Define el nombre de columna especificado entre etiqueta inicial y final.
<DATA>	Especifica el valor de datos de columna de salida especificado entre etiquetas inicial y final.

Salida numérica

El informe no formatea los valores numéricos; permanecen sin formatear.

Por ejemplo, si deseara obtener un informe que contuviera un atributo correspondiente a un factor de escala 2, el valor **7** para dicho atributo se mostraría en una vista de tabla en Tivoli Enterprise Portal como **0,07**. Puede buscar el factor de escala, que se muestra en la definición de atributo `scal` en el siguiente archivo de atributos:

Windows *<dir_instalación>*`\TMAITM6\ATTRLIB\k`*cp*`.atr`

Linux UNIX *<dir_instalación>*`/`*plataforma*`/`*<cp>*`/tables/ATTRLIB/k`*cp*`.atr`, donde *plataforma* es el sistema operativo y *cp* es el código del producto.

Los valores enumerados tampoco están formateados, de modo que los valores que se muestran en el informe como **1** y **2**, por ejemplo, mostrarían su texto equivalente (como por ejemplo **Iniciado** y **Detenido**) en el cliente del portal. Los valores enumerados están definidos en el archivo de atributos k*cp*`.atr`: `vale` para el valor de visualización; `vali` para el valor no formateado.

Salida de ejemplo 1: Salida del SO UNIX de una sola solicitud <REPORT>

```
<REPORTDATA><SQLTABLE><TABLENAME>UNIXOS</TABLENAME>
 <ROWCOUNT>1</ROWCOUNT><ROW><COLUMN><NAME>ORIGINNODE</NAME>
 <DATA><![CDATA[fvaix26:KUX]]></DATA></COLUMN><COLUMN>
 <NAME>SAMPLENO</NAME><DATA>0</DATA></COLUMN><COLUMN>
 <NAME>ROWNO</NAME><DATA>0</DATA></COLUMN><COLUMN><NAME>TIMESTAMP</NAME>
 <DATA><![CDATA[1090629105627000]]></DATA></COLUMN><COLUMN>
 <NAME>SYSTEMTYPE</NAME><DATA><![CDATA[AIX]]></DATA> </COLUMN><COLUMN>
 <NAME>SYSTEMVERS</NAME><DATA><![CDATA[5.3]]> </DATA></COLUMN><COLUMN>
 <NAME>TOTREALMEM</NAME><DATA>3915776</DATA> </COLUMN><COLUMN>
 <NAME>TOTVIRTMEM</NAME><DATA>8634368</DATA> </COLUMN><COLUMN>
 <NAME>SYSUPTIME</NAME><DATA>6633819</DATA> </COLUMN><COLUMN>
 <NAME>NOUSRSESS</NAME><DATA>1</DATA> </COLUMN><COLUMN>
 <NAME>NOSYSPROCS</NAME><DATA>112</DATA> </COLUMN><COLUMN>
 <NAME>NETADDR</NAME>
  <DATA><![CDATA[9.42.11.174]]> </DATA></COLUMN><COLUMN>
 <NAME>UNIXUSRCPU</NAME><DATA>1</DATA> </COLUMN><COLUMN>
 <NAME>UNIXSYSCPU</NAME><DATA>1</DATA> </COLUMN><COLUMN>
 <NAME>UNIXIDLCPU</NAME><DATA>98</DATA> </COLUMN><COLUMN>
 <NAME>UNIXWAITIO</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>VMINRUNQ</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>VMINPGWAIT</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>VMPGFAULTS</NAME><DATA>1538</DATA> </COLUMN><COLUMN>
 <NAME>VMPGRCLM</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>VMPGIN</NAME><DATA>2</DATA></COLUMN> <COLUMN>
 <NAME>VMPGOUT</NAME><DATA>1</DATA></COLUMN> <COLUMN>
 <NAME>VMPGSIN</NAME><DATA>1</DATA></COLUMN> <COLUMN>
 <NAME>VMPGSOUT</NAME><DATA>0</DATA></COLUMN> <COLUMN>
 <NAME>VMFREEMEM</NAME><DATA>7614492</DATA></COLUMN> <COLUMN>
 <NAME>VMFREESWAP</NAME><DATA>1019876</DATA> </COLUMN><COLUMN>
 <NAME>PSWITCH</NAME><DATA>5357</DATA> </COLUMN><COLUMN>
 <NAME>SYSCALL</NAME><DATA>42598</DATA> </COLUMN><COLUMN>
```

```
<NAME>SYSFORK</NAME><DATA>337</DATA> </COLUMN><COLUMN>
<NAME>SYSEXEC</NAME><DATA>274</DATA> </COLUMN><COLUMN>
<NAME>BREAD</NAME><DATA>0</DATA></COLUMN> <COLUMN>
<NAME>BWRITE</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>LREAD</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>LWRITE</NAME> <DATA>0</DATA></COLUMN><COLUMN>
<NAME>PHREAD</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>PHWRITE</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>RCVINT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>XMTINT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>MDMINT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>NETCONNECT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>NETSOCKET</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>NETLOAD1</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>NETLOAD2</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>NETLOAD3</NAME><DATA>2</DATA> </COLUMN><COLUMN>
<NAME>MEMFREE</NAME><DATA>108812</DATA> </COLUMN><COLUMN>
<NAME>MEMUSED</NAME><DATA>3806964</DATA> </COLUMN><COLUMN>
<NAME>VMSCAN</NAME><DATA>0</DATA></COLUMN> <COLUMN>
<NAME>VMUSEDPRC</NAME><DATA>119</DATA></COLUMN> <COLUMN>
<NAME>VMFREEPRC</NAME><DATA>881</DATA></COLUMN> <COLUMN>
<NAME>CPUBUSY</NAME><DATA>2</DATA></COLUMN> <COLUMN>
<NAME>SYSREAD</NAME><DATA>5694</DATA></COLUMN> <COLUMN>
<NAME>SYSWRITE</NAME><DATA>749</DATA></COLUMN> <COLUMN>
<NAME>NSYSTHRD</NAME><DATA>-1</DATA></COLUMN> <COLUMN>
<NAME>PRUNABLE</NAME><DATA>112</DATA></COLUMN> <COLUMN>
<NAME>PRUNNING</NAME><DATA>-1</DATA></COLUMN> <COLUMN>
<NAME>PSLEEPING</NAME><DATA>0</DATA></COLUMN> <COLUMN>
<NAME>PIDLE</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>PZOMBIE</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>PSTOPPED</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>THRDRUNQ</NAME><DATA>-1</DATA></COLUMN><COLUMN>
<NAME>THRDWAIT</NAME><DATA>-1</DATA></COLUMN><COLUMN>
<NAME>BOOTTIME</NAME>
 <DATA><![CDATA[1090413161248000]]> </DATA></COLUMN><COLUMN>
<NAME>PENDIOWT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>STARTIO</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>DEVINT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>UPTIME</NAME>
 <DATA><![CDATA[076d18:43:39]]> </DATA></COLUMN><COLUMN>
<NAME>ZATTRIB</NAME><DATA><![CDATA[ ]]> </DATA></COLUMN><COLUMN>
<NAME>ZVALUE</NAME><DATA><![CDATA[ ]]> </DATA></COLUMN><COLUMN>
<NAME>SWAPFREE</NAME><DATA>7436</DATA> </COLUMN><COLUMN>
<NAME>PGINRATE</NAME><DATA>9</DATA> </COLUMN><COLUMN>
<NAME>PGOUTRATE</NAME><DATA>6</DATA> </COLUMN><COLUMN>
<NAME>PGSCANRATE</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGINS1</NAME><DATA>1</DATA> </COLUMN><COLUMN>
<NAME>AVPGINS5</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGINS15</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGINS60</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGOUT1</NAME><DATA>3</DATA> </COLUMN><COLUMN>
<NAME>AVPGOUT5</NAME><DATA>3</DATA> </COLUMN><COLUMN>
<NAME>AVPGOUT15</NAME><DATA>3</DATA> </COLUMN><COLUMN>
<NAME>AVPGOUT60</NAME><DATA>3</DATA> </COLUMN><COLUMN>
<NAME>AVPGSCAN1</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGSCAN5</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGSCAN15</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGSCAN60</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPRRUNQ60</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>NETADDR6</NAME>
 <DATA><![CDATA[No DNS Entry]]> </DATA></COLUMN><COLUMN>
<NAME>ZID</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>ZONE</NAME><DATA><![CDATA[-1]]> </DATA></COLUMN>
</ROW></SQLTABLE>
</REPORTDATA>
```

Salida de ejemplo 2: Informe con un filtro y columnas especificadas

Es la salida de la solicitud de ejemplo de los atributos de proceso de Windows en la fila *_Total*.

```
<REPORTDATA>
 <STATUS>0</STATUS>
 <SQLTABLE>
  <TABLENAME>NTPROCESS</TABLENAME>
  <ROWCOUNT>1</ROWCOUNT>
  <ROW>
   <COLUMN>
    <NAME>ORIGINNODE</NAME>
    <DATA>Primary:DYANG7:NT</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>TIMESTAMP</NAME>
    <DATA>1090303122813634</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>INSTCNAME</NAME>
    <DATA>_Total</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>PCTPRCSTME</NAME>
    <DATA>99</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>IDPROCESS</NAME>
    <DATA>0</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>THREADCNT</NAME>
    <DATA>1057</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>WRKINGSET</NAME>
    <DATA>1088495616</DATA>
   </COLUMN>
  </ROW>
 </SQLTABLE>
</REPORTDATA>
```

Solicitud de la Interfaz de servicio del agente - Lista de tablas y situaciones del agente

Utilice <TABLESIT> en una solicitud de la Interfaz de servicio para obtener un informe del grupo de atributos especificado en el atributo <TABLENAME> y de las situaciones que se están ejecutando para el grupo.

Entrada de la solicitud

Tabla 52. Solicitud <TABLESIT> de la Interfaz de servicio del agente

Etiqueta	Descripción
<TABLESIT>	Especifique las etiquetas TABLESIT inicial y final para recuperar la lista de tablas y situaciones del agente.
<SQLTABLE>	El par de etiquetas TABLENAME se especifica entre las etiquetas SQLTABLE inicial y final para identificar el conjunto de la definición de la tabla SQL.

Tabla 52. Solicitud <TABLESIT> de la Interfaz de servicio del agente (continuación)

Etiqueta	Descripción
<TABLENAME>	El nombre de la tabla de la que hay que hacer el informe se especifica entre las etiquetas TABLENAME inicial y final. Es el nombre tal como aparece entre las etiquetas inicial y final. Si no está seguro de cómo se escribe el nombre de la tabla, lo puede ver en el informe Consultas de la Interfaz de servicio del agente o lo puede encontrar en el campo **tabl** del archivo .atr del agente, situado en el directorio *<dir_instalación>*/TMAITM6/ATTRLIB. El valor ***ALL** significa todas las tablas conocidas del agente.

Solicitud de ejemplo 1: Situaciones activas del SO Windows para proceso y disco lógico

```
<TABLESIT>
 <SQLTABLE>
 <TABLENAME>NTPROCESS</TABLENAME>
 </SQLTABLE>
 <SQLTABLE>
 <TABLENAME>WTLOGCLDSK</TABLENAME>
 </SQLTABLE>
</TABLESIT>
```

Salida del informe

Tabla 53. Salida de la solicitud <TABLESIT> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<SITUATION>	Define el conjunto de situaciones de salida.
<NAME>	Especifica el nombre de la situación.
<TYPE>	E – Situación de empresa ; P – Situación privada
<STATUS>	Devuelve el código de estatus especificado entre etiqueta inicial y final

Salida de ejemplo: El agente del SO Windows devuelve todas las situaciones de proceso y de disco lógico en ejecución

```
<TABLESIT>
 <SQLTABLE>
 <TABLENAME>NTPROCESS</TABLENAME>
  <SITUATION>
   <NAME>Check_Process_CPU_Usage</NAME>
  </SITUATION>
  <TYPE>P</TYPE>
  <SITUATION>
   <NAME>Check_Process_CPU_Usage</NAME>
 </SITUATION>
  <TYPE>P</TYPE>
  <SITUATION>
   <NAME>Is_KFC_Running</NAME>
 </SITUATION>
 <TYPE>E</TYPE>
 </SQLTABLE> <SQLTABLE>
  <TABLENAME>WTLOGCLDSK</TABLENAME>
  <SITUATION>
  <NAME>Check_DiskSpace_Low</NAME>
 </SITUATION>
 <TYPE>P</TYPE>
 </SQLTABLE>
</TABLESIT>
```

Solicitud de la Interfaz de servicio del agente - Control de situaciones privadas

Cree una solicitud <PVTCONTROL> de la Interfaz de servicio para iniciar, detener o reciclar una situación privada en el agente de supervisión.

Las situaciones privadas comienzan a ejecutarse automáticamente cuando se inicia el agente de supervisión para el cual se han escrito, ya sea un agente de Tivoli Enterprise Monitoring o un agente de Tivoli System Monitor. El mandato PVTCONTROL le permite iniciar, detener o reciclar la situación especificada sin tener que detener y reiniciar el agente.

Entrada de la solicitud

Tabla 54. Solicitud <PVTCONTROL> de la Interfaz de servicio del agente

Etiqueta	Descripción
<PVTCONTROL>	Especifique la solicitud de control de situación privada.
<PVTCOMMAND>	Especifique el mandato de situación privada.
<PVTSITNAME>	Especifique un nombre de situación privada.
<PVTACTION>	START – Inicia una solicitud de situación conocida. STOP – Detiene una situación activa. RECYCLE – Detiene y reiniciar una situación activa.

Solicitud de ejemplo 1: Reciclar la situación privada Check_DiskSpace_Low

```
<PVTCONTROL>
 <PVTCOMMAND>
  <PVTSITNAME>Check_DiskSpace_Low</PVTSITNAME>
  <PVTACTION>RECYCLE</PVTACTION>
 </PVTCOMMAND>
</PVTCONTROL>
```

Salida del informe

Tabla 55. Salida de la solicitud <PVTCONTROL> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<STATUS>	Código de estatus de retorno especificado entre etiqueta inicial y final.

Salida de ejemplo 1: Reciclar la situación privada Check_DiskSpace_Low devuelve el estatus del mandato

```
<PVTCONTROL>
 <STATUS>300</STATUS>
<FILOBJ>
```

Solicitud de la Interfaz de servicio del agente - Resumen de situaciones

Utilice el mandato de resumen de situaciones para solicitar un listado de las situaciones privadas que se están ejecutando en el agente de supervisión.

Entrada de la solicitud

Tabla 56. Solicitud <SITSUMMARY> de la Interfaz de servicio del agente

Etiqueta	Descripción
<SITSUMMARY>	Defina la especificación de alteración temporal de umbral dinámico.

```
<SITSUMMARY>
</SITSUMMARY>
```

La salida de la solicitud se parece a los archivos de configuración de situación privada mostrados en el apartado “Ejemplos de situaciones privadas” en la página 365.

Salida del informe

Tabla 57. Salida de la solicitud <SITSUMMARY> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<ROW>	Define una fila de datos de salida.
<DATA>	El contenido del archivo de descarga está especificado entre etiquetas data.
<STATUS>	Código de estatus de retorno especificado entre etiqueta inicial y final.

Salida de ejemplo 1: el agente devuelve el estatus del proceso

```
<SITSUMMARY>
 <STATUS>0</STATUS>
<FILOBJ>
```

Salida de ejemplo 2: El agente devuelve el contenido del archivo de registro de rastreo

```
<SITSUMMARY>
  <STATUS>0</STATUS>
  <ROWCOUNT>5</ROWCOUNT>
 <ROW>
 <DATA><![CDATA[+49BDCB34.001C 00000000 3018060A 2B060106 03010104
 0100060A 0...+..... ]]></DATA>
 </ROW>
 <ROW>
 <DATA><![CDATA[ +49BDCB34.001C 00000010 2B060104 018D0301 0315
 +.........]]></DATA>
 </ROW>
 <ROW>
 <DATA><![CDATA[ (49BDCB34.001D-B90:kraaest1.cpp,92,
 "IRA_ConstructTrapVarBindV1") *TRAP-INFO: IRA_ConstructTrapVarBindV1
 - Entry pPDU<39B4C6A> pTrapWork<3CDA0A8> pTrapSit<2B8F098>
 dataBuffer<39BC948> offset<1363> resetTrap<0>]]> </DATA>
 </ROW>
 <ROW>
 <DATA><![CDATA[ (49BDCB34.001E-B90:kraaesti.cpp,289,
 "addVarBindStringData") <0x39B4C6A,0x16>
 *TRAP-INFO: VarBind 1.3.6.1.4.1.1667.1.2.1.10.1.1 KNT ]]> </DATA>
 </ROW>
 <ROW>
 <DATA><![CDATA[ +49BDCB34.001E 00000000 3014060D 2B060104 018D0301
 02010A01 0...+..... ]]></DATA>
 </ROW>
</SITSUMMARY>
```

Solicitud de la Interfaz de servicio del agente - Estadísticas de supervisión del agente

Utilice el mandato de estadísticas de supervisión del agente para solicitar información sobre la actividad del agente de supervisión.

Entrada de la solicitud

Tabla 58. Solicitud <AGENTSTAT> de la Interfaz de servicio del agente

Etiqueta	Descripción
<AGENTSTAT>	Especifique la solicitud de estadísticas del agente.
<SITUATION>	Defina las propiedades de selección de situaciones.
<NAME>	Especifique el nombre de la situación o *ALL para todas las situaciones conocidas. Valor predeterminado: ***ALL**
<DAYS>	Opcional. Especifique el periodo que desea visualizar, como por ejemplo 1 para los datos de hoy. Se pueden recuperar datos históricos correspondientes a un máximo de 7 días.
<DETAILS>	Opcional. Yes - proporcionar datos detallados cada hora No - proporcionar solo información de estado Valor predeterminado: **No**

Solicitud de ejemplo 1: Recuperar estadísticas de estado de la situación de hoy

```
<AGENTSTAT>
 <SITUATION>
  <NAME>*ALL</NAME>
 </SITUATION>
</AGENTSTAT>
```

Solicitud de ejemplo 2: Recuperar estadísticas de situación NT_Service_Error de hoy

```
<AGENTSTAT>
 <SITUATION>
  <NAME>NT_Service_Error</NAME>
  <DAYS>1</DAYS>
  <DETAILS>Y</DETAILS>
</SITUATION>
</AGENTSTAT>
```

Salida del informe

Tabla 59. Salida de la solicitud <AGENTSTAT> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<TYPE>	Tipo de situación - de muestra (Sample) o suceso puro (Pure-Event).
<INTERVAL>	Intervalo de muestreo de la situación; ó 0 – Pure-Event.
<ROWSIZE>	Tamaño de fila de datos de muestra.
<FIRSTSTARTTIME>	Hora del primer inicio de la situación.
<LASTSTARTTIME>	Hora de inicio más reciente de la situación.
<LAST STOPTIME>	Hora de la última detención de la situación.
<FIRSTEVENTTIME>	La hora en que la situación abrió un suceso por primera vez.
<LASTTRUETIME>	La última vez que la situación se ha evaluado como **True**.
<LASTFALSETIME>	La última vez que la situación se ha evaluado como **False**.
<TIMESRECYCLED>	Número de veces que se ha reiniciado la situación.
<TIMESAUTONOMOUS>	Número de veces que la situación ha entrado en modalidad autónoma.
<DAY>	Medidas diarias de inicio.
<DATE>	Descripción de fecha.

Tabla 59. Salida de la solicitud <AGENTSTAT> de la Interfaz de servicio del agente (continuación)

Etiqueta de salida	Descripción
<TRUESAMPLES>	Recuento de filas de muestra verdaderas.
<FALSESAMPLES>	Recuento de filas de muestra falsas.
<TRUERATIO>	Porcentaje de muestras verdaderas.
<FALSERATIO>	Porcentaje de muestras falsas.
<HOURROWS>	Recuento de filas de muestra por hora.
<HOURTRUE>	Recuento de filas de muestra verdaderas por hora.
<HOURFALSE>	Recuento de filas de muestra falsas por hora.
<STATUS>	Código de estatus de retorno especificado entre etiqueta inicial y final.

Información de salida de ejemplo de la solicitud de ejemplo 2: El agente devuelve las estadísticas de la situación NT_Service_Error de hoy

```
<SITSTATS>
 <SITUATION>
  <NAME>NT_Service_Error</NAME>
  <TYPE>Event</TYPE>
  <INTERVAL>0</INTERVAL>
  <ROWSIZE>3124</ROWSIZE>
  <FIRSTSTARTTIME>Thu Mar 12 23:09:36 2009</FIRSTSTARTTIME>
  <LASTSTARTTIME>NA</LASTSTARTTIME>
  <LASTSTOPTIME>NA</LASTSTOPTIME>
  <FIRSTEVENTTIME>NA</FIRSTEVENTTIME>
  <LASTTRUETIME>NA</LASTTRUETIME>
  <LASTFALSETIME>Fri Mar 13 22:53:31 2009</LASTFALSETIME>
  <TIMESRECYCLED>0</TIMESRECYCLED>
  <TIMESAUTONOMOUS>0</TIMESAUTONOMOUS>
 <DAY>
   <DATE>Fri Mar 13 00:00:00 2009</DATE>
    <TRUESAMPLES>0</TRUESAMPLES>
   <FALSESAMPLES>80</FALSESAMPLES>
   <TRUERATIO>0.00%</TRUERATIO>
   <FALSERATIO>100.00%</FALSERATIO>
    <HOURROWS>0 0 0 0 0 0 0 12 2 2 4 6 0 4 4 6 0 2 5 4 0 15 14 0
     </HOURROWS>
   <HOURTRUE>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     </HOURTRUE>
   <HOURFALSE>0 0 0 0 0 0 0 12 2 2 4 6 0 4 4 6 0 2 5 4 0 15 14 0
   </HOURFALSE>
 </DAY>
 </SITUATION>
</SITSTATS>
```

Interfaz de servicio del agente - Informe histórico

Cree una solicitud <HISTREAD> de la Interfaz de servicio para iniciar, detener o reciclar una situación privada en el agente de supervisión.

Cuando selecciona un intervalo de tiempo para una vista de tabla u otra vista basada en consulta, se muestran datos históricos de los agentes de Tivoli Enterprise Monitoring en Tivoli Enterprise Portal. Fuera del portal puede ver datos históricos de un agente de supervisión de empresa o datos históricos privados de un agente de supervisión de empresa o agente de supervisión del sistema si se obtiene un informa histórico de la Interfaz de servicio del agente o si es crea una solicitud HISTREAD de la Interfaz de servicio.

Entrada de la solicitud

Tabla 60. Solicitud <HISTREAD> de la Interfaz de servicio del agente

Etiqueta	Descripción
<HISTREAD>	Recupera datos históricos de tabla
<SQLTABLE>	Identifica el conjunto de definiciones de tabla SQL.
<TABLENAME>	Define el nombre de la tabla especificado entre etiqueta inicial y final. El nombre de tabla puede tener como máximo 10 caracteres.
<PVTHIST>	Opcional. Especifica lectura de historial privado. No hay agente directo para leer historial a corto plazo de la empresa
<OUTPUT>	Opcional. Define la selección de salida de columnas de tabla.
<COLUMN>	Opcional. Define el nombre de columna seleccionado especificado entre etiqueta inicial y final.
<FILTER>	Opcional. Define criterios de filtro de filas de datos especificados entre etiqueta inicial y final. Consulte la especificación de la situación privada <CRITERIA> para ver detalles. Utilice desde y hasta la columna WRITETIME para especificar el rango de lectura de datos históricos. Utilice la columna ORIGINNODE para seleccionar datos históricos específicos de MSN
<OUTLIMIT>	Opcional. Define el límite de registros de salida especificado entre etiquetas OUTLIMIT inicial y final para protegerse frente a un volumen excesivo de información de salida.

Solicitud de ejemplo 1: Obtener datos históricos del proceso del agente del SO Windows utilizando filtro y selecciones de columna.

```
<HISTREAD>
 <SQLTABLE>
 <TABLENAME>NTPROCESS</TABLENAME>
 <OUTPUT>
  <COLUMN>ORIGINNODE</COLUMN>
  <COLUMN>TIMESTAMP</COLUMN>
  <COLUMN>INSTCNAME</COLUMN>
  <COLUMN>IDPROCESS</COLUMN>
  <COLUMN>PCTPRCSTME</COLUMN>
  <COLUMN>THREADCNT</COLUMN>
  <COLUMN>WRKINGSET</COLUMN>
 </OUTPUT>
 <FILTER>
 <![CDATA[ *VALUE ORIGINNODE *EQ Primary:DYANG3:NT  *AND
   *VALUE WRITETIME  *GE 1090408224500000  *AND
   *VALUE WRITETIME  *LE 1090408234500000]]>
 </FILTER>
 <OUTLIMIT>5000</OUTLIMIT>
 </SQLTABLE>
</HISTREAD>
```

Salida del informe

Tabla 61. Salida de la solicitud <HISTREAD> de la Interfaz de servicio del agente

Etiqueta de salida	Descripción
<HISTREADDATA>	Identifica el conjunto de datos de salida del informe.
<STATUS>	Código de estatus de retorno especificado entre etiqueta inicial y final
<ROWCOUNT>	Recuento de filas de tabla de salida

Tabla 61. Salida de la solicitud <HISTREAD> de la Interfaz de servicio del agente (continuación)

Etiqueta de salida	Descripción
<ROW>	Identifica datos de una fila de salida
<NAME>	Define el nombre de columna especificado entre etiqueta inicial y final.
<DATA>	Especifica el valor de datos de columna de salida especificado entre etiquetas inicial y final.

Salida de ejemplo 1: El agente del SO Windows devuelve datos históricos de proceso correspondientes a los siete atributos especificados el 8 de abril entre la 10:45 PM y las 11:45 PM

```
<HISTREADDATA>
 <SQLTABLE>
  <TABLENAME>NTPROCESS</TABLENAME>
  <ROWCOUNT>212</ROWCOUNT>
  <ROW>
   <COLUMN>
  <NAME>ORIGINNODE</NAME>
    <DATA><![CDATA[Primary:DYANG3:NT]]></DATA>
   </COLUMN>
   <COLUMN>
  <NAME>TIMESTAMP</NAME>
    <DATA><![CDATA[1090408224551430]]></DATA>
   </COLUMN>
   <COLUMN>
   <NAME>INSTCNAME</NAME>
    <DATA>![CDATA[Idle]]> </DATA>
   </COLUMN>
   <COLUMN>
    <NAME>IDPROCESS</NAME>
   <DATA>0</DATA>
   </COLUMN>
   <COLUMN>
   <NAME>PCTPRCSTME</NAME>
   <DATA>74</DATA>
   </COLUMN>
   <COLUMN>
   <NAME>THREADCNT</NAME>
   <DATA>1</DATA>
   </COLUMN>
   <COLUMN>
   <NAME>WRKINGSET</NAME>
   <DATA>16384</DATA>
   </COLUMN>
  </ROW>
  ...
  ...
 </SQLTABLE>
</HISTREADDATA>
```

Interfaz de servicio del agente - Control de configuración

La solicitud de interfaz de servicio se puede utilizar para procesar solicitudes de lista de carga de configuración.

Autorización

La solicitud de interfaz de servicio reconoce la sintaxis XML completa de la lista de carga de configuración. Las solicitudes permitidas dependen de los permisos de grupo:

- Si el ID de usuario es miembro del grupo **Operación** en el Perfil de grupo de autorización de acceso (AAGP), puede utilizar el elemento <CNFGCOMMAND> para renovar archivos utilizando una lista de carga de configuración existente y puede emitir solicitudes de reinicio, recarga y descarga de <CNFGACTION>.
- Si el ID de usuario es miembro del grupo **Administrativo** en AAGP, puede enviar cualquier solicitud de lista de carga de configuración válida utilizando la sintaxis de la Especificación XML de lista de carga de configuración.

Elementos

Los elementos y sus atributos no son sensibles a mayúsculas y minúsculas. Por ejemplo, puede especificar <CNFGCOMMAND>, <CnfgCommand> o <cnfgcommand>.

<CNFGCOMMAND>

Especifique la solicitud del mandato de configuración. El siguiente ejemplo de solicitud de control de configuración vuelve a cargar el contenido de la lista de carga de configuración actual:

```
<CNFGCOMMAND>
  <CNFGACTION>RELOAD</CNFGACTION>
</CNFGCOMMAND>
```

<CNFGACTION>

Especifique la acción del mandato de configuración:

Rearrancar
Este atributo descarga la lista de carga de configuración.

Recargar
Recargar se utiliza para realizar un reenvío inmediato de la lista de carga del agente actual, descargando así todos los artefactos del agente especificado si se han actualizado. Consulte el ejemplo bajo <CnfgCommand>.

Descargar
Descargas se utiliza para especificar el archivo que se va a enviar. Consulte los ejemplos bajo <CnfgFile> y <CnfgDisp>.

<CNFGFILE>

Opcional. Especifique los dos últimos segmentos del nombre del archivo cuando <CNFGACTION> es Download (Descargar).

El nombre del archivo debe existir en la lista de carga. Descargar el archivo alert.txt

```
<CNFGCOMMAND>
  <CNFGACTION>DOWNLOAD</CNFGACTION>
  <CNFGFILE>alert.txt</CNFGFILE>
</CNFGCOMMAND>
```

<CNFGDISP>

Opcional. Especifique la disposición conocida del archivo de configuración como identificación del nombre del archivo cuando <CNFGACTION> es Download (Descargar). La definición del archivo debe existir en la lista de carga. La siguiente solicitud de ejemplo descarga el archivo XML de configuración de situación privada:

```
<CNFGCOMMAND>
  <CNFGACTION>DOWNLOAD</CNFGACTION>
  <CNFGDISP>PVTSIT</CNFGDISP>
</CNFGCOMMAND>
```

<STATUS>

Utilice este elemento para devolver el código de estatus comprendido entre las etiquetas <status> inicial y </status> final. El siguiente ejemplo hace que el agente devuelva el estatus del mandato:

```
<CNFGCOMMAND>
  <STATUS>600 - El mandato de control de configuración ha terminado correctamente
  </STATUS>
</CNFGCOMMAND>
```

Capítulo 16. configuración centralizada

Utilice la función de configuración centralizada para mantener los archivos de configuración de agentes de supervisión en una ubicación central desde la que dichos agentes puedan recopilar la información.

Visión general de la configuración centralizada

La configuración centralizada ofrece la posibilidad de actualizar archivos de configuración local en muchos agentes de supervisión sin conexión con un Tivoli Enterprise Monitoring Server.

Estas son algunas de las ventajas de la configuración centralizada:

- Asegura instalaciones de agente coherentes
- Reduce el soporte de instalación y la complejidad de la configuración
- Mejora la eficacia del despliegue del agente
- Mejora la escalabilidad de Tivoli Monitoring
- Aprovecha los conocimientos de gestión de web de los usuarios

La configuración centralizada implica que un agente de supervisión o (preferiblemente) un servidor web de Tivoli actúa como un repositorio de archivos de configuración del agente que proporcionan los agentes de supervisión en los mismos o en distintos sistemas utilizando su *lista de carga de configuración* local. El repositorio puede contener archivos como XML de configuración para alertas SNMP y sucesos EIF, scripts de automatización y otros archivos operativos pertinente del agente. La lista de carga de configuración especifica la ubicación del servidor central y los archivos de configuración que hay que obtener.

El *servidor de configuración central* puede ser un agente de Tivoli Monitoring de la versión 6.2.2 Fixpack 2 o posterior, o puede ser cualquier servidor web, como por ejemplo WebSphere, IBM HTTP, Microsoft IIS o Apache. Por motivos de seguridad, IBM recomienda elegir un servidor web.

Puede tener varios servidores de configuración central y organizarlos lógicamente como una jerarquía de servidores de configuración central.

Una vez el agente ha iniciado la configuración centralizada, el comportamiento predeterminado consiste en obtener las actualizaciones de archivos del servidor de configuración central designado cada hora. También puede obtener actualizaciones según demanda especificando la lista de carga como una solicitud de la Interfaz de servicios del agente.

Los agentes activan dinámicamente los archivos de configuración conocidos recién descargados, como situaciones privadas y listas de carga de configuración, sin reiniciar el agente. Otros cambios en la configuración que requieren que el agente se reinicie para permitir que los nuevos cambios entren en vigor pueden incluir una especificación de reinicio del agente de modo que dichas actualizaciones en la configuración entren en vigor inmediatamente sin intervención.

Las tareas básicas para implementar la configuración centralizada para agentes existentes son:

© Copyright IBM Corp. 2005, 2013

1. Decidir una estrategia para organizar y distribuir archivos de configuración desde un repositorio central y crear los archivos de configuración.
2. Configurar el servidor de configuración central.
3. Habilitar el agente para que recopile la lista de carga de configuración inicial.
4. Actualizar los archivos de configuración necesarios en el servidor de configuración central.

Diseño de la configuración centralizada

La estructura de la configuración centralizada que defina dependerá del tamaño y de la organización de la empresa supervisada, de los tipos de agentes de supervisión que desee mantener, del tipo de actualizaciones y de su frecuencia.

Lista de carga de configuración

Cualquier agente de supervisión recién instalado o un agente existente puede participar en la configuración centralizada utilizando una lista de carga de configuración. La lista de carga de configuración es un archivo de configuración XML que es exclusivo del agente en ejecución. Indica al agente cómo conectar con uno o más servidores de configuración central y qué archivos debe descargar de dichos servidores.

Los administradores mantienen y actualizan el archivo de configuración en este repositorio centralizado. Los agentes nuevos recopilan archivos de configuración iniciales de esta ubicación y de forma periódica o bajo demandan establecen contacto con el servidor para recopilar actualizaciones o cambios.

Servidor de configuración central

La lista de carga de configuración contiene uno o varios elementos ConfigServer que indican al agente cómo conectar con un servidor de configuración central. Los servidores de configuración central contienen un repositorio de archivos que se sirven a los agentes de supervisión mediante HTTP.

El servidor autentica las solicitudes, examina la indicación de fecha y hora de la última actualización del artículo de configuración (establecido en GMT), y, si la copia del cliente del archivo solicitado es más antigua que la copia del servidor, el servidor devuelve el contenido del artículo de configuración al agente. De lo contrario, devuelve el estatus de HTTP 304 - Objeto no modificado. El servidor devuelve otro estatus de HTTP si se encuentra un error durante el proceso del artículo.

Cuando despliegue un servidor de configuración central, tenga en cuenta estos factores:

Acceso de usuarios
Los administradores necesitan acceso para mantener la lista de carga de configuración que se va a distribuir. Los clientes de configuración central necesitan acceso al servidor de configuración central para recopilar las actualizaciones. Si ya tiene un servidor web y está familiarizado con el acceso y mantenimiento de sus archivos, puede utilizar el servidor web disponible para que actúe como servidor de configuración central. Esto incluye el servidor web correspondiente a la Interfaz de servicio del agente .

Estructura de directorios

Identifique una estructura de directorios en el servidor y el cliente que le permita organizar sus archivos, a fin de minimizar la duplicación en el servidor y de reducir el número de archivos que hay que mantener.

Sustitución de palabras clave

El uso de la sustitución de palabras clave en la lista de carga de configuración puede simplificar la organización de los archivos de configuración.

Por ejemplo, si todos los agentes del sistema operativo Linux se ejecutan en un conjunto de situaciones privadas con sucesos definidos y los agentes del sistema operativo Windows se ejecutan en otro conjunto, se puede utilizar la palabra clave @PRODUCT@ para dirigir los agentes al directorio y archivo correctos en el servidor de configuración central. Coloque los archivos en el directorio *dir_instalación*/localconfig o según se especifique en la variable de entorno IRA_SERVICE_INTERFACE_CONFIG_HOME. Por ejemplo:

- común
  - cnfglist.xml
- lz
  - lz_situations.xml
  - lz_trapcnfg.xml
- nt
  - nt_situations.xml
  - nt_trapcnfg.xml

El archivo cnfglist.xml puede utilizar la palabra clave @PRODUCT@ para dirigir los agentes a los archivos correctos. Ejemplo:

```
<ConfigurationArtifact>
  <ConfigServer
   Name="CENTRAL-CONFIG-SERVER"
   URL="http://icvr5a05.tivlab.raleigh.ibm.com/"
   User="itmuser"
   Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
  <ConfigFile
   Server="CENTRAL-CONFIG-SERVER"
   Name="cnfglist.xml"
   Path="common"
   Disp="CNFGLIST"
   Activate="YES" />
  <ConfigFile
   Server="CENTRAL-CONFIG-SERVER"
   Name="@PRODUCT@_situations.xml"
   Path="@PRODUCT@"
   Disp="PVTSIT"
   Activate="YES" />
  <ConfigFile
   Server="CENTRAL-CONFIG-SERVER"
   Name="@PRODUCT@_trapcnfg.xml"
   Path="@PRODUCT@"
   Disp="TRAPCNFG"
   Activate="RESTART" />
</ConfigurationArtifact>
```

Se pueden utilizar otras palabras clave para crear la granularidad que necesita cada agente para obtener los archivos correctos.

Servidor web como servidor de configuración central

Los agentes de supervisión de Tivoli pueden utilizar los servidores web existentes para recopilar archivos de configuración. Puede utilizar cualquier servidor web al que puedan acceder los agentes con HTTP o HTTPS como servidor de configuración central.

Para utilizar un servidor web, cree un ID de usuario que tenga permiso para acceder a los archivos del servidor de configuración central y haga referencia a dichas credenciales en la lista de carga de configuración. La especificación de URL es ligeramente diferente que cuando el servidor de configuración central es un agente de supervisión, pero esta es la única diferencia en la lista de carga de configuración. El elemento ConfigServer se parece al siguiente:

```
<ConfigServer
   Name="CENTRAL-CONFIG-SERVER"
   URL="http://webserver.domain.com/"
   User="itmuser"
   Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
```

Agente de supervisión como servidor de configuración central

Todos los agentes de supervisión (supervisor del sistema o de empresa) que se ejecutan en las plataformas Windows, Linux y UNIX contienen una interfaz de servicio HTTP que se puede utilizar como servidor de configuración central. Los agentes de supervisión en z/OS e i5 no ofrecen una interfaz de servicio HTTP, de modo que no se pueden utilizar como servidores de configuración central.

La ventaja de utilizar un agente de supervisión como servidor de configuración central en lugar de un servidor web es que no necesita mantener un servidor web y puede utilizar varios agentes para formar un conjunto de servidores de configuración central en cascada para ofrecer equilibrio en la carga de trabajo.

Acceso de usuarios al servidor de configuración central

El acceso a la interfaz de servicio de un agente se controla mediante su Perfil de grupo de autorización de acceso (AAGP). La posibilidad de solicitar o colocar archivos en un agente requiere más derechos de seguridad que la visualización de medidas o datos históricos. De forma predeterminada, cualquier ID válido en el sistema host en el que se está ejecutando el agente puede acceder a la Interfaz de servicio del agente . Estos usuarios pueden ver medidas, situaciones y los datos históricos recopilados por el agente. Sin embargo, el comportamiento predeterminado sólo otorga al ID **Administrativo** del host permiso para acceder a los archivos de configuración central a través de la interfaz de servicio del agente.

Los siguientes ID de usuario son miembros predeterminados del grupo **Administrativo** en la plataforma en la que se está ejecutando el agente:

- Windows: Administrador
- Linux, UNIX: root
- z/OS: ITMUSER
- IBM i: QSECOFR

Puede crear listas de carga de configuración y utilizar las credenciales de **Administrativo** para conectar con el agente de supervisión que actúa como servidor de configuración central. No es necesario que el ID exista en los agentes cliente para que se puedan conectar al servidor de configuración central.

En sistemas Windows, el agente descubre automáticamente todas las cuentas de usuario pertenecientes al grupo Administradores de AAGP; el agente añade dichas cuentas al grupo Administrativo de AAGP durante el arranque. En sistemas UNIX y Linux, el agente descubre automáticamente todos los ID de usuario que tienen autorización de root (superusuario); el agente los añade al grupo Administrativo de AAGP durante el arranque. (El ID de usuario QSECOFR en IBM i e ITMUSER en z/OS no se modifican en este momento.) Como resultado:

- Los clientes no tienen que crear una cuenta de usuario especial para utilizar los servicios del agente.
- Se evita la exposición del ID Administrador/root.
- Cualquier cuenta autorizada en un sistema obtiene acceso automático a los servicios privilegiados del agente como acceso a archivos, personalización de AAGP, etc.

Aunque los ID de usuario se pueden almacenar en formato cifrado, en la mayoría de los casos deseará definir un ID de usuario en el sistema que albergará el servidor de configuración central y añadirá dicho usuario a AAGP del agente.

El siguiente ejemplo muestra los pasos a seguir para crear un usuario en el agente del sistema operativo Linux y otorgar acceso administrativo al servidor de configuración central:

1. Cree el usuario en el sistema: El usuario denominado “itmuser” se crea en el sistema operativo Linux y el agente del sistema operativo Linux (lz) es el servidor de configuración central.
2. Cree un archivo AAGP.xml en el directorio *dir_instalación*/`localconfig` que añada el nuevo ID al grupo **Administrativo**:

   ```
   <AAGP>
     <AAUSER>
       <ID>itmuser</ID>
       <ASSIGN>AD</ASSIGN>
     </AAUSER>
   </AAGP>
   ```

   El directorio de configuración local predeterminado se puede modificar con la variable de entorno IRA_SERVICE_INTERFACE_CONFIG_HOME.

   Consejo: Considere la posibilidad de que cada agente recopile un archivo AAGP para poder contactar con el agente directamente a través de su Interfaz de servicio del agente para realizar las acciones de configuración con un ID que no sea root. Al conectar directamente con la interfaz de servicio de un agente con permiso AD, puede proporcionar las credenciales para conectar con un nuevo servidor de configuración central, colocar u obtener archivos o forzar renovaciones automáticas de archivos de configuración.
3. En el agente de supervisión que funciona como servidor de configuración central, edite la lista de carga de configuración para añadir una entrada DISP="AAGP" ConfigFile para cargar el archivo XML de AAGP.

   Esta lista de carga debe utilizar credenciales (Linux UNIX root; Windows Administrador) para conectarse a fin de añadir el nuevo ID de usuario a AAGP. La lista de carga de configuración editada se parece a la siguiente:

```
<ConfigurationArtifact>
   <ConfigServer
    Name="CENTRAL-CONFIG-SERVER"
    URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
    User="root"
    Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
   <ConfigFile
    Server="CENTRAL-CONFIG-SERVER"
    Name="AAGP.xml"
    Path="/"
    Disp="AAGP" />
</ConfigurationArtifact>
```

4. Guarde la lista de carga en *dir_instalación*/localconfig/lz/lz_cnfglist.xml. Este directorio es la ubicación predeterminada en sistemas Linux y se puede cambiar en la variable de entorno IRA_SERVICE_INTERFACE_CONFIG_LOADLIST.
5. Inicie el agente de SO Linux.

Todos los clientes de configuración central que se conectan a este servidor de configuración central pueden utilizar las credenciales correspondientes a "itmuser" en lugar de las de "root".

```
<ConfigServer
  Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
```

Servidores de configuración central en cascada

Otros agentes de supervisión pueden recopilar una actualización del Perfil de grupo de autorización de acceso (AAGP) de un servidor de configuración central y luego se pueden utilizar para distribuir archivos a otros agentes.

Los servidores en cascada se deben configurar de modo que distribuyan las listas de carga de configuración que especifica su Interfaz de servicio del agente para el URL del elemento ConfigServer.

Los servidores en cascada utilizan los elementos DISP=CUSTOM ConfigFile para descargar el contenido que distribuyen a otros agentes.

Interfaz de servicio del agente

La interfaz de servicio de un agente se puede utilizar para especificar y procesar solicitudes de lista de carga de configuración bajo demanda. Consulte el apartado "Interfaz de servicio del agente - Control de configuración" en la página 443.

Especificación XML de la lista de carga de configuración

Utilice la sintaxis de XML de la especificación XML de la lista de carga de configuración para crear una lista de carga para la configuración centralizada.

Vía de acceso y nombre de archivo predeterminados de la lista de carga de configuración

Los siguientes nombres de archivo de la lista de carga de configuración son los valores predeterminados, donde *cp* es el código de producto de dos caracteres:

Windows *install_dir*\localconfig*cp**cp*_cnfglist.xml

Linux UNIX *install_dir*/localconfig/*cp*/*cp*_cnfglist.xml

z/OS IRA_SERVICE_INTERFACE_CONFIG_LOADLIST=
*CP*CFGLST.RKANDATV

IBM i /QIBM/UserData/IBM/ITM/localconfig/a4/a4_cnfglist.xml

Utilice la variable de entorno del agente IRA_SERVICE_INTERFACE_CONFIG_LOADLIST para modificar la vía de acceso y nombre de archivo predeterminados. Consulte el apartado "Variables de entorno para la configuración centralizada" en la página 462.

Elementos

Las etiquetas de elementos XML y sus atributos **no son sensibles a mayúsculas y minúsculas**, pero los valores **son sensibles a mayúsculas y minúsculas**. Por ejemplo, puede especificar <CONFIGSERVER>, <ConfigServer> o <configserver>.

<ConfigurationArtifact> </ConfigurationArtifact>

ConfigurationArtifact es el elemento raíz que lo identifica como un documento de configuración de lista de carga. Especifique <ConfigurationArtifact> al principio del archivo y </ConfigurationArtifact> al final. Ejemplo de archivo de lista de carga:

```
<ConfigurationArtifact>
 <ConfigServer
    Name="AGOURALAB"
    URL="http://9.55.100.99/"
    User="smith"
    Password="{AES256:keyfile:a}hjZM0YaLzpd5JQC5DeboJg==" />
 <ConfigFile
    Server="AGOURALAB"
    Name="Private_Situations.xml"
    Path="ITM/Config/@HOSTNAME@"
    Disp="PVTSIT"
    Activate="YES" />
 <ConfigFile
    Server="AGOURALAB"
    Name="TRAPCNFG.xml"
    Path="ITM/Config/common"
    Disp="trapcnfg"
    Activate="RESTART" />
  <ConfigFile
    Server="AGOURALAB"
  Name="THRESHOLDS.XML"
    Path="ITM/Config/@PRODUCT@"
    Disp="threshold"
    Activate="YES" />
</ConfigurationArtifact>
```

<ConfigServer>

Defina un servidor de configuración central con los siguientes atributos:

Name=

Define un nombre simbólico de una sentencia SERVER. El nombre puede tener un máximo de 32 caracteres y debe ser exclusivo en la lista de carga. No se permiten nombres duplicados.

URL= Define el URL utilizado para conectar con el servidor de configuración central, que puede ser de cualquiera de los siguientes tipos:

- Una interfaz de servicio del agente que actúe como un servidor de configuración central y especificada como:

  método-HTTP://*Nombrehost*:*puerto*
  ///*PuntoServicio-agente*/*PuntoServicio-agente*

- Un servidor web que actúe como servidor de configuración central y especificado como:

  Método-HTTP://*Nombrehost*:[*puerto*]
  /[*víaacceso*]

donde:

Método-HTTP
: es http o https

Nombrehost
: es el nombre de host del servidor de configuración central. Utilice la dirección IP si no está garantizado que DNS local resuelva el nombre de host.

puerto
: es el puerto de escucha del servidor de configuración central de destino de índice de servicios de Tivoli Monitoring (código de componente KDH) o el servidor web si el puerto no es el predeterminado, 80. El puerto predeterminado de índice de servicios de Tivoli Monitoring es 1920 para HTTP o 3661 para HTTPS; ambos se pueden personalizar con la variable de entorno KDC_FAMILIES en el agente de destino.

PuntoServicio-agente
: es el nombre de la interfaz de servicio del agente registrada por TMS/Engine, como por ejemplo `system.myhost_nt` para el agente del sistema operativo Windows y `myhost_lz` para el agente del sistema operativo Linux. Puede cambiar el nombre de servicio del agente de destino por un nombre reconocible más funcional mediante la variable de entorno del agente IRA_SERVICE_INTERFACE_NAME. Por ejemplo, `https://9.48.123.13:3661///Paris-CSF-A/Paris-CSF-A`. Omita la definición de nombre de instancia del agente si utiliza un repositorio de configuración de servidor web genérico.

Víaacceso
: es una definición de vía de acceso al servidor de configuración central de destino adicional. Por ejemplo, `http://9.48.132.40:80/ITM/config`.

User= Opcional. Especifica el ID de usuario de la cuenta del sistema host del servidor de configuración central.

Password=
: Opcional. Especifique la contraseña del usuario en texto plano o utilice el programa de utilidad itmpwdsnmp para cifrar la contraseña del usuario y especificar aquí la cadena de datos de AES de salida. Consulte el apartado “Cifrado de claves SNMP: itmpwdsnmp” en la página 389.

AltServer=
: Opcional. Especifica un nombre de servidor alternativo. El agente crea el URL de solicitudes de archivos utilizando la definición de servidor alternativo cuando no puede contactar o iniciar la sesión en este servidor. La definición del servidor alternativo no puede incluir una especificación de servidor alternativo adicional.

  Los siguientes códigos de estatus de HTTP hacen que el agente reintente la solicitud mediante la especificación **AltServer**:

401 No autorizado

403 Prohibido

404 No se encuentra el objeto

500 Error de servidor interno

503 Servicio no disponible

Si utiliza el atributo AltServer para especificar un servidor de configuración central alternativo, asegúrese de definir <ConfigServer> alternativo antes de la definición de <ConfigServer> que hace referencia al mismo. Ejemplo:

```
<ConfigServer
 Name="CENTRAL-CONFIG-ALTERNATE"
 URL="http://lnxhostB:1920///lnxhostB_lz/lnxhostB_lz"
 User="itmconfig"
 Password="{AES256:keyfile:a}vHBiEqmmvylNPs90DhQ==" />
<ConfigServer
 Name="CENTRAL-CONFIG-REPOSITORY"
 URL="http://lnxhostA:1920///lnxhostA_lz/lnxhostA_lz"
 User="itmconfig"
 Password="{AES256:keyfile:a}hjZM0YaLzpd5JQC5DJg=="
 AltServer="CENTRAL-CONFIG-ALTERNATE" />
```

Consulte también el ejemplo del apartado ""Variables de entorno de la lista de carga de configuración" en la página 460."

<ConfigFile>

Identifica un <ConfigServer> definido previamente por nombre. El agente envía la solicitud a este **Servidor** para descargar este archivo en particular.

Puede hacer referencia a variables de entorno cuando defina atributos del elemento <ConfigFile>. Dónde se resuelven las variables depende del tipo de servidor de configuración central:

- Si la conexión se realiza a un agente de supervisión que actúa como servidor de configuración central, las variables de entorno utilizadas para definir los atributos ConfigFile, Name y Path se resuelven en el servidor.
- Si la conexión se realiza a un servidor web que actúa como servidor de configuración central, *todas* las variables de entorno se resuelven en el cliente.

Server=

Identifica un <ConfigServer> definido previamente por nombre. El agente envía la solicitud a este **Servidor** para descargar este archivo en particular.

Name=

Especifica el nombre de archivo en la ubicación del servidor. El nombre puede incluir variables de entorno si el agente las puede reconocer y resolver.

Path= Especifica la vía de acceso de la ubicación del archivo en el <ConfigServer> de destino. La vía de acceso puede incluir variables de entorno que se resuelven en el servidor cuando se conecta a un servidor de configuración central. Las variables se resuelven en el cliente de configuración central cuando la conexión se realiza con un servidor web.

La **vía de acceso** es relativa a la raíz de HTTP del servidor de configuración. Cuando se utiliza un agente de supervisión como servidor de configuración, el directorio *dir_instalación*/localconfig es la raíz de HTTP. El ancla del archivo de configuración se puede alterar temporalmente mediante la variable de entorno IRA_SERVICE_INTERFACE_CONFIG_HOME.

Disp= Opcional. Especifica la disposición local de los archivos de configuración del agente conocidos. Cuando se especifica el atributo DISP, el agente coloca el ConfigFile (o ConfigFiles) descargado en la ubicación correcta en el sistema cliente de configuración central en función de los valores de entorno del agente cliente. El atributo DISP también permite la activación de las opciones adecuadas para cada ConfigFile. El agente conoce la ubicación local y el nombre de estos archivos de configuración del agente y, cuando los descarga, los guarda según la especificación del agente.

Si se omite el atributo Disp, se utiliza CUSTOM de forma predeterminada. La colocación de un archivo cuando se utiliza Disp=CUSTOM está restringida a ubicaciones dentro de *dir_instalación* de Tivoli Monitoring. Esta restricción tiene como objetivo mejorar la seguridad. otros tipos de archivos Disp se colocan donde el agente de supervisión espera que esté el archivo, aunque la ubicación especificada esté fuera de la estructura de directorios de *dir_instalación*. Si especifica Disp=CUSTOM, resulta útil utilizar la palabra clave @ITMHOME@ para especificar LocalPath.

Actualmente están definidos los siguientes valores de disposición:

CNFGLIST
Archivo de lista de carga de configuración.

PVTSIT
Archivo XML de configuración de situaciones privadas.

TRAPCNFG
Archivo XML de configuración de condiciones de excepción de SNMP del agente.

THRESHOLD
Archivo XML de configuración de alteraciones temporales de umbral de situación.

EIFCNFG
Archivo de configuración de EIF.

EIFMAP
Archivo de correlación de sucesos de EIF.

UAMETA
Metarchivos de la aplicación Universal Agent.

PASCAP
Archivo de paquete de agente común (CAP) del servicio del agente de proxy (Servicios de gestión de agentes). El valor PASCAP de Disp sólo se puede utilizar en un agente de sistema operativo de Tivoli que dé soporte a los servicios de gestión de agentes. Descarga y activa el archivo CAP si el producto está instalado. Se puede utilizar

Options=NOPRODUCTCHECK para forzar la colocación del archivo CAP aunque el producto que gestiona el archivo CAP no esté instalado. (Consulte el manual Instalación y configuración de los Servicios de gestión de agentes de Tivoli.)

AAGP
Perfil de grupo de autorización de acceso, que contiene las definiciones del grupo de autorización de acceso y las asignaciones de grupo de autorización de acceso de ID de usuario definidas por el administrador de seguridad. (Consulte el apartado "Perfil de grupo de autorización de acceso" en la página 417.)

PERSONALIZADO
CUSTOM es el valor predeterminado que se utiliza si se omite DISP. Se deben especificar los atributos **LocalName** y **LocalPath** para DISP=CUSTOM. Los archivos CUSTOM se pueden descargar sólo a una ubicación dentro de la estructura del directorio de instalación del agente.

Options=
Especifica la opción de manejo de archivos de configuración:

NOPRODUCTCHECK
Sólo es válido con DISP=PASCAP. Omite el requisito de instalación del producto antes de la operación de descarga del archivo CAP. Actualmente este es el único valor definido de la opción.

LocalName=
Especifica el nombre del archivo del sistema local. LocalName sólo se utiliza si se omite DISP o si tiene el valor CUSTOM. Si se omite LocalName cuando Disp=CUSTOM, se utiliza el atributo NAME. LocalName se pasa por alto para los demás valores de Disp porque el agente identifica la ubicación del archivo utilizando valores predeterminados o parámetros de alteración temporal.

LocalPath=
Especifica la vía de acceso al archivo del sistema local. LocalPath sólo se utiliza si se omite DISP o si tiene el valor CUSTOM. Si se omite LocalPATH cuando Disp=CUSTOM, se utiliza el atributo PATH. LocalPath se pasa por alto para los demás valores de Disp porque el agente identifica la ubicación del archivo utilizando valores predeterminados o parámetros de alteración temporal.

Activate=

NO Sustituye el archivo actual por la copia descargada, pero no lo activa. El archivo descargado debe ser más nuevo que el archivo de configuración existente. Este es el valor predeterminado.

RESTART
Reinicia el agente tras una descarga de archivo correcta.

Los siguientes tipos de Disp necesitan que el agente se reinicie para poder leer los archivos de configuración actualizados:

TRAPCNFG

EIFCNFG

EIFMAP

RESTART se puede utilizar con PVTSIT para forzar la sustitución de la definición de situación privada en lugar de fusionar la definición con las situaciones actualmente activas.

RESTART también está disponible para Disp="CUSTOM".

RESTART no recibe soporte en z/OS o i5. El proceso del agente se debe reiniciar de otra manera para activar la nueva configuración.

Servicios de gestión de agentes
El código RESTART utiliza los Servicios de gestión de agentes para reciclar el agente:

- El agente debe estar bajo la gestión de los Servicios de gestión de agentes. Esto se consigue especificando <managerType>ProxyAgentServices</managerType> en el archivo de paquete de agente común (CAP) del agente o utilizando el mandato de actuación MAS Iniciar gestión
- El agente de sistema operativo se debe estar ejecutando en el sistema para que el servicio de vigilancia del agente esté disponible para reciclar el agente.

Cabe esperar los siguientes resultados si el agente no está bajo la gestión de los Servicios de gestión de agentes o si el agente de sistema operativo no se está ejecutando cuando se recupera ConfigFile del servidor de configuración central:

- El agente graba un mensaje en el archivo de registro que indica que se omite el reinicio.
- Si la gestión de sucesos de SNMP o EIF desde el agente de supervisión está habilitada, se genera un suceso de estatus de ciclo de vida autónomo.
- El archivo se activa la siguiente vez que se reinicia el agente.

De forma predeterminada, los Servicios de gestión de agentes están habilitados para todos los agentes de sistema operativo, excepto para el agente del sistema operativo zLinux, que está inhabilitado. El servicio de vigilancia de los Servicios de gestión de agentes para el agente del sistema operativo zLinux se debe habilitar manualmente para poder aprovechar las ventajas de la función RESTART. De lo contrario, el agente del sistema operativo zLinux se debe reiniciar de otra manera para activar la nueva configuración.

Consulte el Capítulo 14, “Servicios de gestión de agentes”, en la página 321 para ver detalles sobre la utilización de los Servicios de gestión de agentes para supervisar la disponibilidad de los agentes.

YES Indica al agente que fusiones el archivo descargado en el archivo actual. Los nuevos cambios entran en vigor dinámicamente sin tener que reiniciar el agente. Esta

opción sólo es válida para los siguientes valores de DISP: CNFGLIST, PVTSIT, threshold y THRESHOLD.

Tabla 62. Elemento <ConfigFile> de la lista de carga de configuración y opciones de activación disponibles para el tipo Disp.

Disp=	**Activate="Yes"**	**Activate="Restart"**	**Activate="NO"**
CNFGLIST	Valor predeterminado	N/D	N/D
PVTSIT	Disponible	Disponible	Valor predeterminado
TRAPCNFG	N/D	Disponible	Valor predeterminado
EIFCNFG	N/D	Disponible	Valor predeterminado
EIFMAP	N/D	Disponible	Valor predeterminado
THRESHOLD	Disponible	Disponible	Valor predeterminado
UAMETA	N/D	Disponible	Valor predeterminado
PASCAP	Los archivos CAP se activan durante la descarga, por lo que el atributo Activate no se aplica.		
AAGP	Valor predeterminado	N/D	N/D
PERSONALIZADO	N/D	Disponible	Valor predeterminado

<ConfigParm>

Opcional. Especifica un valor de alteración temporal de variable de entorno que actualiza los valores del entorno inmediatamente y entra en vigor durante el siguiente intervalo de operación o instancia.

Interval=

Alteración temporal o establecimiento de IRA_SERVICE_INTERFACE_CONFIG_INTERVAL.

Backup=

Alteración temporal o establecimiento de IRA_SERVICE_INTERFACE_CONFIG_BACKUP.

NumbTasks=

Alteración temporal o establecimiento de IRA_SERVICE_INTERFACE_CONFIG_POOL_SIZE.

MaxWait=

Alteración temporal o establecimiento de IRA_SERVICE_INTERFACE_CONFIG_MAX_WAIT.

Sustitución de palabras clave en la lista de carga de configuración

Utilice la sustitución de palabras clave para crear una lista de carga de configuración que se pueda aplicar de forma coherente a distintos agentes y ubicaciones.

Los agentes de supervisión de Tivoli reconocen ciertas palabras clave en los atributos de la lista de carga de configuración y los sustituyen utilizando valores del entorno de ejecución tomados del cliente de configuración central.

Con la excepción de @ITMHOME@, cualquier carácter que no sea alfanumérico se cambia por guiones (-) en la información de salida. Las palabras clave para la lista de carga de configuración son las siguientes:

@PRODUCT@	Es el código de producto de dos caracteres, en minúsculas, del agente de supervisión. Ejemplo: En un agente de SO Windows, @PRODUCT@_trapcnfg.xml se resuelve como nt_trapcnfg.xml
@ITMHOME@	Es la vía de acceso de instalación de IBM Tivoli Monitoring. Ejemplo: si se trata de un sistema Linux y se utiliza la vía de acceso de instalación predeterminada, @ITMHOME@ se resuelve como /opt/IBM/ITM/.
@MSN@	Es el nombre del sistema gestionado (no el nombre del subnodo). Ejemplos_ si el nombre del sistema gestionado del agente es primary:icvw3d62:nt, @MSN@ se resuelve como primary-icvw3d62-nt.
@TASKNAME@	Es el nombre del proceso del agente de supervisión. Ejemplos: klzagent; kntcma.
@VERSION@	Es la versión del producto del agente de supervisión. Ejemplo: si la versión del agente es 6.2.2 Fixpack 2, @VERSION@ se resuelve como 06-22-02.
@HOSTNAME@	Es el nombre del host del sistema. Ejemplo: myhost.
@IPADDRESS@	Es la dirección IP de la interfaz de red del sistema. Ejemplo: si la dirección IP del agente es 9.42.38.333, @IPADDRESS@ se resuelve como 9-42-38-333.
@OSTYPE@	Este es el tipo de sistema operativo. Los valores válidos incluyen: z/OS, Tandem, AS/400, Win98, Win95, WinNT, Win2K, WinXP, Windows, Win2003, WinVista, Windows7 y Win2008. El OSTYPE para todas las demás plataformas se obtiene utilizando el mandato **uname**. También puede encontrar el OSTYPE para un sistema determinado en el registro de RAS1 bajo Tipo de sistema o abriendo la Consola de servicio y buscando en la esquina superior derecha de la pantalla.
@OSVERSION@	Es la versión del sistema operativo. Ejemplos: Red Hat Enterprise Linux Versión 5 (de 64 bits) se resuelve como 2-6-18-128-el5; Windows 2003 (de 32 bits) con ServicePack 2 se resuelve como 5-2-sp2.
@SYSTEMID@	Es el identificador del sistema. Ejemplo: el ID de sistema icvr4a04.mylab.mycity.ibm.com se muestra en la información de salida como icvr4a04-mylab-mycity-ibm-com.

Consulte los ejemplos de sintaxis y organización de palabras clave de “Servidor de configuración central” en la página 448.

Variables de entorno de la lista de carga de configuración

Puede hacer referencia a una variable de entorno en la lista de carga de configuración en lugar de especificar un valor fijo para un atributo. La sustitución de variables le permite aplicar la misma definición de lista de carga en distintos entornos.

Especifique las variables de entorno entre signos de porcentaje (%) cuando haga referencia a las mismas en una lista de carga de configuración. Puede pensar que este requisito es sólo para Windows, puesto que las variables de entorno se especifican entre signos de porcentaje en dicho sistema operativo, pero los delimitadores de signo de porcentaje se utilizan para identificar variables de entorno dentro de la lista de carga de configuración en todas las plataformas.

Las variables de entorno de la lista de carga de configuración se resuelven en el servidor de configuración central o en el cliente de configuración central, en función de si hay un agente de supervisión o un servidor web que actúe como el servidor de configuración central:

- Cuando un agente de supervisión actúa como el servidor de configuración central, las variables de entorno de la lista de carga de configuración se resuelven utilizando el entorno del servidor de configuración central.
- Cuando un servidor web actúa como el servidor de configuración central, las variables de entorno de la lista de carga de configuración se resuelven utilizando el entorno del cliente de configuración central (el agente de supervisión que realiza la solicitud).

Para ilustrar la forma en que se puede utilizar la sustitución de variables en la lista de carga de configuración, supongamos que tenemos un entorno con dos agentes de supervisión que actúan como servidores de configuración central. La variable de entorno SALES_CNFG_FILES se utiliza para identificar el directorio que contiene archivos de configuración que utilizarán los sistemas pertenecientes al departamento de ventas de la empresa. El servidor de configuración central primario es un agente de sistema operativo Windows en un servidor llamado **winhost**

```
IRA_SERVICE_INTERFACE_CONFIG_HOME=C:\IBM\ITM\ConfigFiles
```

y la configuración correspondiente al departamento de ventas está en un directorio llamado `C:\IBM\ITM\ConfigFiles\Sales`, de modo que definimos

```
SALES_CNFG_FILES=Sales
```

El departamento de desarrollo también tiene un servidor de configuración central configurado en un agente de sistema operativo Linux en su servidor **linuxhost**. También conservan una copia actual de los archivos de configuración correspondientes a los sistemas de ventas: su agente se utiliza como servidor de configuración central alternativo si se despliegan nuevos agentes mientras **winhost** no está disponible. Su agente de sistema operativo Linux utiliza el valor predeterminado para IRA_SERVICE_INTERFACE_CONFIG_HOME, que es `/opt/IBM/ITM/localconfig`.

Localizan los archivos de configuración correspondientes al departamento de ventas en `/opt/IBM/ITM/localconfig/eastcoast/sales`, de modo que definen:

```
SALES_CNFG_FILES=eastcoast/sales
```

Esta es la lista de carga de configuración de arranque para el departamento de ventas:

```
<ConfigurationArtifact>
 <ConfigServer Name="BACKUP-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}8wNnAEj6uLMTTOeaC+2rfQ==" />
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://winhost:1920///primary.winhost_nt/primary.winhost_nt/"
  User="itmuser"
  Password="{AES256:keyfile:a}8wNnAEj6uLMTTOeaC+2rfQ=="
  AltServer="BACKUP-CONFIG-SERVER" />
  <ConfigFile Server="CENTRAL-CONFIG-SERVER"
   Name="cnfglist.xml"
   Path="%SALES_CNFG_FILES%"
   Disp="CNFGLIST"
   Activate="YES" />
</ConfigurationArtifact>
```

Cuando los agentes se conectan a **winhost**, recopilan `C:\ibm\ITM\ConfigFiles\Sales\cnfglist.xml`. Si **winhost** no está disponible, los agentes se conectan a **linuxhost** y recopilan `/opt/IBM/ITM/localconfig/eastcoast/sales/cnfglist.xml`.

Mediante la utilización de la variable de entorno en la especificación, se puede realizar una personalización adicional en los servidores de configuración central individuales.

Arranque del lista de carga de configuración

Cuando coloque la lista de carga de configuración inicial, puede colocar un archivo que identifique inmediatamente todos los componentes que el agente de supervisión debe recopilar del servidor de configuración central. Sin embargo, esto significa que debe colocar un archivo de lista de carga de configuración exclusivo en cada agente. Uno de los elementos que un cliente de configuración central siempre debe recopilar del servidor de configuración es la lista de carga. Esto permite modificar la lista de carga desde el servidor de configuración.

Puesto que de todas formas identificará la carga de configuración completa, para iniciar operaciones de configuración centralizada solo tiene que indicar al agente dónde conectarse para obtener la primera lista de carga de configuración. Se puede utilizar una lista de carga de configuración sencilla que contenga un elemento ConfigServer y un elemento ConfigFile para definir el archivo DISP=CNFGLIST para arrancar las operaciones de configuración centralizada.

En este ejemplo, el URL ConfigServer identifica la ubicación del servidor de configuración central y el nombre de usuario y la contraseña para acceder a dicho servidor. El elemento ConfigFile apunta al servidor nombrado en el elemento ConfigServer e identifica el archivo de lista de carga de configuración como cnfglist.xml, que está en la vía de acceso correspondiente al producto.

```
<ConfigurationArtifact>
  <ConfigServer
   Name="CENTRAL-CONFIG-SERVER"
   URL="http://winhost:1920///primary.winhost_nt/primary.winhost_nt/"
   User="Administrator"
   Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
  <ConfigFile
   Server="CENTRAL-CONFIG-SERVER"
   Name="cnfglist.xml"
   Path="@PRODUCT@"
   Disp="CNFGLIST"
   Activate="YES" />
</ConfigurationArtifact>
```

Tras crear una lista de carga de configuración de arranque que identifique la lista de carga correcta para el agente, coloque el archivo y reinicie el agente.

Variables de entorno para la configuración centralizada

Se pueden utilizar variables de entorno para personalizar la variable del agente para la configuración centralizada: para arrancar el servidor de configuración central, para controlar operaciones del cliente de configuración central y, cuando un agente de supervisión actúa como servidor de configuración central, para controlar operaciones.

Para agentes de supervisión de empresa, las variables de entorno se establecen en el archivo de entorno del agente; para agentes supervisores del sistema, las variables de entorno se establecen en el archivo de respuestas *cp*_silent_install.txt.

Para obtener más información sobre la instalación del agente supervisor del sistema, consulte “Supervisión del sistema operativo mediante un agente supervisor del sistema” en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Arranque del servidor de configuración central

Tras el arranque, un agente de supervisión busca en primer lugar sus archivos XML de lista de carga de configuración. Si la lista de carga de configuración no existe, el agente revisa su archivo de entorno en busca de las siguientes variables. El agente construye la lista de carga inicial, o *programa de arranque*, a partir de estos valores de entorno para conectar con un servidor de configuración central y descargar una lista de carga de configuración.

IRA_CONFIG_SERVER_URL
Especifica el URL del servidor. Por ejemplo, http://9.52.111.99.

IRA_CONFIG_SERVER_USERID
Especifica el ID de usuario del servidor. Valor predeterminado: itmuser.

IRA_CONFIG_SERVER_PASSWORD
Especifica la contraseña del usuario en texto plano o como cadena de caracteres de contraseña cifrada de AES.

IRA_CONFIG_SERVER_FILE_PATH
Especifica la vía de acceso a la lista de carga de configuración en el servidor de configuración central. El valor predeterminado es loadlist/@PRODUCT@. Consulte “Sustitución de palabras clave en la lista de carga de configuración” en la página 459 para ver una lista de palabras clave.

IRA_CONFIG_SERVER_FILE_NAME
Especifica el nombre del archivo de lista de carga de configuración en el servidor de configuración central. Valor predeterminado: **cnfglist.xml**.

Operaciones del cliente de configuración central

Las siguientes variables de entorno del agente afectan al modo en que funciona el agente como un cliente para la configuración centralizada. Utilícelas para especificar un archivo de lista de carga de configuración diferente del valor predeterminado, la frecuencia con la que hay que conectar con el servidor de configuración central para comprobar si hay actualizaciones y si hay que descarga solo los archivos de configuración que se han modificado desde la última vez que descargó o todos los archivos.

IRA_SERVICE_INTERFACE_CONFIG_LOADLIST
Utilice esta variable para alterar temporalmente la lista de carga de configuración predeterminada. Especifique la vía de acceso completa y el nombre del archivo de la lista de carga de configuración. Los siguientes nombres de archivo de la lista de carga de configuración son los valores predeterminados, donde *cp* es el código de producto de dos caracteres:

Windows *install_dir*\localconfig*cp**cp*_cnfglist.xml

Linux UNIX *install_dir*/localconfig/*cp*/*cp*_cnfglist.xml

z/OS IRA_SERVICE_INTERFACE_CONFIG_LOADLIST=*CP*CFGLST.RKANDATV

IBM i /QIBM/UserData/IBM/ITM/localconfig/a4/a4_cnfglist.xml

IRA_SERVICE_INTERFACE_CONFIG_INTERVAL
Especifica la frecuencia con la que el agente intenta comprobar con el servidor de configuración central si hay actualizaciones. Especifique el intervalo en minutos. Un día es 1440 minutos; una semana, que también es el máximo, 10080 minutos. Valor predeterminado: **60** minutos.

IRA_SERVICE_INTERFACE_CONFIG_BYPASS_TIMESTAMP
Si tiene el valor N, el agente descarga y sustituye solo los archivos de configuración que tienen una indicación de fecha y hora de UTC posterior a la de la versión local. Valor predeterminado: **N**. Si se establece este parámetro en **Y** se indica al agente que omita la indicación de fecha y hora y descargue siempre el archivo tras cada intervalo.

Como práctica recomendada, sincronice las horas del sistema en la red para asegurarse de que cualquier agente de supervisión que se ejecute con la hora adelantada con respecto a la del servidor de configuración central no se pierda una actualización si el archivo se modifica dentro de la diferencia de tiempo tras la descarga.

IRA_SERVICE_INTERFACE_CONFIG_BACKUP
Cuando se descarga un nuevo archivo de configuración, el agente cambia el nombre del archivo local existente y lo convierte en una copia de seguridad añadiendo el sufijo del 1 al 5 al nombre y moviendo el archivo al directorio de copia de seguridad. Esta variable especifica el número de versiones de copia de seguridad que hay que conservar. El mínimo es 0, para ninguna copia de seguridad y el máximo es 5 copias de seguridad. Valor predeterminado: **2** copias de seguridad.

IRA_SERVICE_INTERFACE_CONFIG_BACKUP_DIR
Utilice esta variable de entorno para establecer un directorio de copia de seguridad distinto del predeterminado. Estos son los directorios de copia de seguridad predeterminados:

Windows *install_dir*\localconfig*cp*\backup

Linux UNIX *install_dir*/localconfig/*cp*/backup

z/OS RKANDATV DD dataset

IBM i /QIBM/UserData/IBM/ITM/localconfig/a4/backup

IRA_SERVICE_INTERFACE_CONFIG_MAX_WAIT
Define el tiempo máximo de espera en segundos para descargar todos los archivos de configuración especificados en la lista de carga del repositorio de configuración central. El rango de tiempo válido es el comprendido entre 15 y 300 segundos. Valor predeterminado: **60** segundos.

IRA_SERVICE_INTERFACE_CONFIG_PASCAP_FACTOR
Linux UNIX cliente de configuración central solo. El factor de multiplicación de tiempo que utiliza el agente de supervisión para calcular el intervalo de retardo de salida del archivo del paquete de agente común (CAP) de los Servicios de gestión de agentes. El intervalo de retardo se deriva de la variable de entorno KCA_DISCOVERY_INTERVAL multiplicada por este factor. El agente impone un valor de factor mínimo de 1. Valor predeterminado: **1.5**.

IRA_SERVICE_INTERFACE_CONFIG_POOL_SIZE
El agente crear una agrupación de hebras de tarea para manejar varios artículos de la lista de carga simultáneamente. El agente coloca una solicitud en una cola FIFO proporcionada por las tareas de la agrupación. Valor predeterminado: **10** tareas.

Operaciones del servidor de configuración central

Los siguientes parámetros de configuración del agente afectan al modo en que funciona el agente como servidor para la configuración centralizada:

IRA_SERVICE_INTERFACE_CONFIG_HOME
Si un agente se utiliza como un servidor de configuración, este valor se puede utilizar para alterar temporalmente la ubicación predeterminada del repositorio de configuración central. La ubicación predeterminada utilizada para colocar archivos que va a ofrecer el servidor de configuración central es: *install_dir*/localconfig.

La raíz del archivo HTTP del servidor web lo define el administrador del servidor web y no se puede modificar. No se pueden utilizar especificaciones de vías de acceso relativas, como ../../, para hacer referencia a artefactos externos a la ubicación del repositorio definido. Además, la nueva ubicación del repositorio no puede ser el directorio raíz.

IRA_SERVICE_INTERFACE_NAME
Especifique el nombre de interfaz de servicio de agente preferido para definir un nombre reconocido más funcional para sustituir el nombre predeterminado generado por el agente en el formato de k*cp*agente, donde *cp* es el código de producto de dos caracteres, como por ejemplo kntagent o kmqagent; o *cp*agente, como uagent02 para identificar una segunda instancia de Universal Agent instalada en un sistema.

Valor predeterminado:
Windows system.*nombrehost_cp*
Linux UNIX *nombrehost_cp*

Ejemplo: el valor predeterminado de agent-ServicePoint para un agente del sistema operativo Windows es: ***nombrehost*_nt**. El URL con el que conectar con un servidor de configuración central en un agente del sistema operativo Windows que se ejecuta en el sistema host winhost1 es: https://winhost1:3661///winhost1_nt/winhost1_nt. Si IRA_SERVICE_INTERFACE_NAME= **ConfigServer-A**, el URL es https://winhost1:3661///ConfigServer-A/ConfigServer-A

KDE_TRANSPORT
Utilice la variable de entorno KDE_TRANSPORT para especificar un puerto distinto del predeterminado, 1920 para HTTP ó 3661 para HTTPS.

No cambie los valores de puerto predeterminados, especialmente en sistemas multifunción UNIX y Linux, ya que muchos componentes pueden estar ubicados en el mismo sistema y algunos de estos componentes pueden depender de los valores predeterminados que se utilizan para los puertos HTTP y HTTPS.

Nota: La variable KDE_TRANSPORT prevalece y altera temporalmente la variable KDC_FAMILIES, Si existe una variable KDC_FAMILIES en el archivo, copie los valores de KDC_FAMILIES que desea conservar en la nueva variable KDE_TRANSPORT. Para obtener más información, consulte el tema sobre "Control de asignaciones de números de puerto" en el servidor de portal en el manual *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Determinación de problemas

Estas opciones de diagnóstico se pueden establecer para el componente del agente. La salida es el archivo de registro ras1.

IRA_DEBUG_SERVICEAPI=Y
Nombre del componente del agente: interfaz de servicio

IRA_DEBUG_PRIVATE_SITUATION=Y
Nombre del componente del agente: situación privada

IRA_DEBUG_TRANSCON=Y
Nombre del componente del agente: Transport Conduit

KDH_DEBUG=D
Nombre del componente del agente: servicio HTTP de índice de servicios de Tivoli Monitoring

Habilitación del cifrado de contraseña en los archivos de configuración en z/OS

Los archivos XML de configuración de autonomía del agente incluyen credenciales de usuario con contraseñas que se pueden especificar en texto plano. La protección del acceso a estos archivos de configuración suele resultar adecuada para asegurar las credenciales. También puede añadir una capa de seguridad almacenando contraseñas en formato cifrado dentro del archivo de configuración.

Antes de empezar

Si habilita alertas de SNMP desde el agente, las cadenas de caracteres de comunidad de SNMP v1 y v2c y las contraseñas de autenticación y privacidad de SNMP v3 se pueden almacenar en formato cifrado en el archivo de configuración de condiciones de excepción *PC*TRAPS.RKANDATV.

Si va ha habilitar la configuración centralizada, los atributos de contraseña de ConfigServer se pueden cifrar cuando se almacenan en un archivo de lista de carga de configuración *PC*CFGLST.RKANDATV o mediante el parámetro IRA_CONFIG_SERVER_PASSWORD en el archivo de entorno K*PC*ENV.

En sistemas Windows, Linux y UNIX, las cadenas de caracteres de contraseñas y de comunidad se cifran y se descifran mediante los programas de utilidad de cifrado de GSKIT proporcionados por la infraestructura de Tivoli Management Services. En z/OS, GSKit se conoce como Integrated Cryptographic Service Facility o ICSF. Si estas cadenas de caracteres se almacenan en formato cifrado en z/OS, el subsistema ICSF debe estar disponible en el sistema z/OS y los módulos ICSF se deben añadir al PROC de arranque del agente de supervisión de z/OS para que las cadenas de caracteres se puedan descifrar y las pueda utilizar el agente.

Procedimiento

1. Compruebe que tiene al menos un coprocesador criptográfico de IBM instalado y que ICSF está instalado.
2. Cree un miembro KAES256 en el conjunto de datos RKANPARU en el entorno de tiempo de ejecución del agente z/OS. Asegúrese de utilizar la misma clave de cifrado que se ha utilizado en el entorno. Si la herramienta de configuración de z/OS ya ha creado un miembro KAES256 con la misma clave de cifrado para un servidor de Tivoli Enterprise Monitoring en z/OS y el agente de z/OS está configurado en el mismo entorno de tiempo de ejecución que el servidor de supervisión, puede saltarse este paso.
   - Copie el miembro KAES256 del conjunto de datos RKANPARU del servidor de supervisión en el conjunto de datos RKANPARU del agente z/OS.

- Como alternativa, puede copiar el archivo KAES256.ser del directorio `keyfiles` del sistema distribuido en el que ejecutará la herramienta itmpwdsnmp para cifrar cadenas de contraseñas y de comunidad. Cargue el archivo KAES256.ser en el miembro KAES256 del conjunto de datos RKANPARU del agente z/OS en modalidad binaria. KAES256.ser es de 48 bytes en sistemas distribuidos y está rellenado con blancos en el miembro KAES256 del conjunto de datos RKANPARU.
- Para obtener instrucciones sobre cómo utilizar la herramienta de configuración de z/OS para crear el miembro KAES256, consulte el tema "Configuración de los servidores de supervisión concentradores y remotos en z/OS" en *Configuración de Tivoli Enterprise Monitoring Server en z/OS*.

3. Concatene módulos ICSF con PROC RKANMODL DDNAME de arranque existente del agente z/OS. Edite el PROC de arranque del agente z/OS y añada soporte de ICSF a RKANMODL DDNAME. A continuación se muestra un ejemplo de RKANMODL donde CSF.SCSFMOD0 es el conjunto de datos que contiene módulos de descifrado de ICSF:

```
//RKANMODL DD DISP=SHR,DSN=my_load_modules
// DD DISP=SHR,DSN=TDOMPT.&LVMLVL..MODL
// DD DISP=SHR,DSN=TDOMPT.&CMSLVL..MODL
// DD DISP=SHR,DSN=CSF.SCSFMOD0
```

4. Reinicie el servidor de supervisión o el agente de supervisión de z/OS o ambos.

Qué hacer a continuación

Utilice el programa de utilidad `itmpwdsnmp` para crear las cadenas de contraseña y de comunidad cifradas. El programa de utilidad solo está disponible en la infraestructura de Tivoli Enterprise Monitoring Agent en plataformas distribuidas. La infraestructura del agente se puede instalar desde el DVD de Tivoli Monitoring base o desde el DVD del agente de Tivoli Monitoring. Ejecute la herramienta `itmpwdsnmp` en modalidad interactiva en el sistema distribuido para cifrar las contraseñas que se colocarán en los archivos de configuración. Para obtener instrucciones, consulte "Cifrado de claves SNMP: itmpwdsnmp" en la página 389.

Configuración de muestra de configuración centralizada

Esta configuración de muestra ilustra las consideraciones sobre planificación y los pasos a seguir para preparar el entorno de Tivoli Monitoring y los archivos para la configuración centralizada.

Cree una estructura de directorios

Decida el tipo de archivos que desea servidor y cree una estructura de directorios en el sistema que permita que se puedan utilizar palabras clave en la lista de carga de configuración para permitir que cada agente cliente recopile los archivos correctos.

El directorio inicial predeterminado en el que se sirven los archivos desde el agente utilizado como servidor de configuración central es *dir_instalación*`/localconfig` en todas las plataformas. Puede reubicar el directorio con la variable de entorno IRA_SERVICE_INTERFACE_CONFIG_HOME en el archivo de entorno del agente.

Para nuestra configuración de muestra, reubicaremos el directorio inicial del servidor de configuración central en

dir_instalación`/configserver`

y crearemos estos subdirectorios:

dir_instalación/configserver/common contiene los archivos que son iguales en todos los agentes.

dir_instalación/configserver/nt contiene los archivos que utilizan los agentes del sistema operativo Windows, que se encuentran con la palabra clave @PRODUCT@.

dir_instalación/configserver/lz contiene los archivos que utilizan los agentes del sistema operativo Linux, que se encuentran utilizando la palabra clave @PRODUCT@.

dir_instalación/configserver/ux contiene los archivos que utilizan los agentes del sistema operativo UNIX, que se encuentran con la palabra clave @PRODUCT@.

dir_instalación/configserver/myfiles contiene otros archivos que quizás desee distribuir

Las palabras clave @OSTYPE@ y @OSVERSION@ resultan útiles para servir distintos archivos a distintos grupos de sistemas. Por ejemplo, en sistemas UNIX, utilice @OSTYPE@ para separar las situaciones de AIX de las situaciones de Solaris. Consulte el apartado "Sustitución de palabras clave en la lista de carga de configuración" en la página 459.

Obtenga la contraseña raíz correspondiente al servidor de configuración central

Para nuestra configuración de muestra, almacene la contraseña en la lista de carga de configuración que utiliza el servidor de configuración central para cargar su archivo AAGP cada vez que se inicia el agente.

Cifre la contraseña mediante el programa de utilidad itmpwdsnmp, disponible en cualquier agente de la V6.2.2 o posterior.

Windows `C:\ibm\ITM\TMAITM6\itmpwdsnmp.bat`

Linux UNIX `/opt/IBM/ITM/bin/itmpwdsnmp.sh`

Este es un ejemplo de lo que se muestra en la línea de mandatos de Linux:

```
itmpwdsnmp.sh

Especifique la contraseña que se va a cifrar:
Confirme la cadena de caracteres:
{AES256:keyfile:a}qNf3u5TzYsiNXRacS4/sXQ==
```

Seleccione el ID que utilizan los agentes para acceder al servidor de configuración central

En nuestra configuración de muestra, es **itmuser**. La contraseña se almacena en la lista de carga de configuración que utilizan los agentes para establecer conexión con el servidor de configuración central.

Cifre la contraseña correspondiente al ID itmuser mediante el programa de utilidad itmpwdsnmp. (Defina este ID en cada agente. El ID se añade al AAGP del agente.)

Windows `C:\ibm\ITM\TMAITM6\itmpwdsnmp.bat`

Linux UNIX `/opt/IBM/ITM/bin/itmpwdsnmp.sh`

Cree el archivo AAGP.xml que añade el ID Administrativo al grupo AD

El ID **Administrativo** que se utiliza para acceder al servidor de configuración central se añade al grupo de autorización de AD predefinido.

Para nuestra configuración de muestra, guardamos el archivo AAGP.xml guardado en el servidor de configuración central en el directorio *dir_instalación*/configserver/common.

```
<AAGP>
 <AAUSER>
  <ID>itmuser</ID>
  <ASSIGN>AD</ASSIGN>
 </AAUSER>
</AAGP>
```

Este archivo AAGP.xml define el AAGP en el servidor de configuración central. Para nuestra configuración de muestra, el servidor de configuración central servirá el mismo archivo a los agentes que se conecten al mismo. Esto simplifica nuestra configuración de muestra. Sin embargo, puede tener distintos conjuntos de agentes que recopilen archivos AAGP exclusivos con distintos conjuntos de ID y grupos de modo que funcionen distintos conjuntos de permisos en la Interfaz de servicio del agente en dichos agentes. El AAGP que descargan se utiliza cuando se conecta *a* su Interfaz de servicio del agente . Los agentes utilizan los ID definidos en el AAGP que ha recopilado el agente para conectar con el servidor de configuración central.

Cree la lista de carga de configuración para el servidor de configuración central

Para nuestra configuración de muestra, utilizamos un agente del sistema operativo Linux como servidor de configuración central, de modo que creamos *dir_instalación*/localconfig/lz_cnfglist.xml, que es la ubicación predeterminada de la lista de carga de configuración del agente. (El hecho de tener el archivo de lista de carga en el directorio localconfig es una de las razones por las que hemos movido la ubicación del repositorio de configuración central predeterminada con IRA_SERVICE_INTERFACE_CONFIG_HOME. El agente podría utilizar los mismos archivos localconfig que sirve a otros agentes, pero puede resultar más cómodo conservar los archivos separados de los que el servidor de configuración central distribuye.) El archivo cnfglist.xml permite que el servidor de configuración central cargue el AAGP en sí mismo:

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="root"
  Password="{AES256:keyfile:a}qNf3u5TzYsiNXRacS4/sXQ==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="AAGP.xml"
  Path="common"
  Disp="AAGP" />
</ConfigurationArtifact>
```

Cree una lista de carga de configuración de arranque genérica

Cree una lista de carga de configuración de arranque genérica que utilizarán los agentes para buscar la lista de carga específica que proporciona la lista completa de archivos que deben recopilar. Este paso no es obligatorio, pero le permite cambiar el modo en que se organizan los archivos en el servidor de configuración central. Hay varias formas de hacerlo.

Para nuestra configuración de muestra, creamos *dir_instalación*/configserver/common/bootstrap_cnfglist.xml con los siguientes valores:

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}2fhfCvELPHKm94/OkbOjyw==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="cnfglist.xml"
```

```
  Path="@PRODUCT@"
  Disp="CNFGLIST"
  Activate="YES" />
</ConfigurationArtifact>
```

No es necesario incluir el AAGP del agente en CNFGLIST de arranque. El agente utiliza este archivo para localizar la lista de configuración exclusiva que debe utilizar el agente. Esta CNFGLIST sólo está en vigor durante unos segundos. En nuestro ejemplo, el agente busca en el directorio identificado por la palabra clave @PRODUCT@ un archivo llamado cnfglist.xml. Constituye una práctica recomendada buscar un CNFGLIST de arranque en el servidor de configuración para permitir que los agentes identifiquen su CNFGLIST modificando este archivo directamente en el servidor de configuración (en lugar de modificando el mecanismo en cada agente para comenzar las operaciones de configuración central).

Cree una CNFGLIST que utilizarán todos los agentes del sistema operativo Windows

En nuestro ejemplo, cree la lista de carga de configuración en *dir_instalación*\configserver\nt\confglist.xml:

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="root"
  Password="{AES256:keyfile:a}qNf3u5TzYsiNXRacS4/sXQ==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="AAGP.xml"
  Path="common"
  Disp="AAGP" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="cnfglist.xml"
  Path="@PRODUCT@"
  Disp="CNFGLIST"
  Activate="YES" />
<ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="@PRODUCT@_situations.xml"
  Path="@PRODUCT@"
  Disp="PVTSIT"
  Activate="YES" />
<ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="@PRODUCT@_trapcnfg.xml"
  Path="@PRODUCT@"
  Disp="TRAPCNFG"
  Activate="RESTART" />
</ConfigurationArtifact>
```

Cree una CNFGLIST que utilizarán todos los agentes del sistema operativo Linux. En nuestro ejemplo, cree la lista de carga de configuración en *dir_instalación*/configserver/lz/cnfglist.xml. Estos son los agentes que deseamos que recopilen todos los archivos en *dir_instalación*/configserver/myfiles.

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}2fhfCvELPHKm94/OkbOjyw==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="AAGP.xml"
  Path="common"
  Disp="AAGP" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="cnfglist.xml"
  Path="@PRODUCT@"
```

```
  Disp="CNFGLIST"
  Activate="YES" />
<ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="myfile1.sh"
  Path="myfiles"
  LocalPath="@ITMHOME@/tmp" />
<ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="myfile2.sh"
  Path="myfiles"
  LocalPath="@ITMHOME@/tmp" />
</ConfigurationArtifact>
```

Cree los otros archivos que desea distribuir

Cree listas de carga de configuración para los otros códigos de producto del agente y otros archivos que desea desplegar y colocar en el servidor de configuración central.

Habilite los agentes de supervisión para que empiecen a utilizar la configuración centralizada

El apartado "Arranque de la configuración centralizada" describe varias formas de empezar a utilizar la configuración centralizada.

Para nuestra configuración de muestra, puede establecer estas variables de entorno en el archivo de entorno del agente cliente:

```
IRA_CONFIG_SERVER_URL=http://linuxhost:1920///linuxhost_lz/linuxhost_lz
IRA_CONFIG_SERVER_USERID=itmuser
IRA_CONFIG_SERVER_PASSWORD={AES256:keyfile:a}2fhfCvELPHKm94/OkbOjyw==
IRA_CONFIG_SERVER_FILE_PATH=common
IRA_CONFIG_SERVER_FILE_NAME=bootstrap_cnfglist.xml
```

También puede crear este archivo *dir_instalación*/localconfig/*pc*/*pc*_confglist.xml:

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}2fhfCvELPHKm94/OkbOjyw==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="bootstrap_cnfglist.xml"
  Path="common"
  Disp="CNFGLIST"
  Activate="YES" />
</ConfigurationArtifact>
```

Arranque de la configuración centralizada

Después de diseñar la lista de carga de configuración para cada agente y de crear el servidor de configuración central, estará listo para que los agentes se conecten y se inicien utilizando una configuración centralizada.

Puede habilitar un agente para que utilice la configuración centralizada editando las variables de entorno del agente para especificar un servidor de configuración central predeterminado, colocando el archivo de lista de carga de configuración en el sistema y reiniciando el agente, o bien enviando una solicitud de interfaz de servicio.

Iniciación de la configuración centralizada con variables de entorno del agente

Puede utilizar las variables de entorno del agente para la configuración centralizada para identificar la ubicación del servidor de configuración central y

descargar la lista de carga de configuración inicial (programa de arranque). Estas variables de entorno solo se utilizan si no existe ninguna lista de carga de configuración local.

Una vez establecido el archivo de la lista de carga de configuración inicial, el agente de supervisión utiliza dicho archivo y ya no intenta utilizar las variables de entorno. Si se suprime la lista de carga de configuración local (en el agente supervisor del sistema también debe ejecutar una instalación silenciosa), el agente vuelve a utilizar las variables de entorno para descargar la lista de carga de configuración del programa de arranque. (Consulte el "Arranque del lista de carga de configuración" en la página 462.)

Iniciación con variables de entorno del agente común de supervisión de empresa

Utilice las variables de entorno de configuración centralizada de Tivoli Enterprise Monitoring Agent para que apunten a servidor de configuración central y descargue la lista de carga de configuración inicial.

Procedimiento

1. En el sistema donde está instalado el agente de supervisión de empresa, abra el archivo de entorno de agente de Manage Tivoli Enterprise Monitoring Services o en la linea de mandatos:
   - Inicie Manage Tivoli Enterprise Monitoring Services:
     Windows Pulse **Inicio → Programas →IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services**
     Linux UNIX Donde *dir_ITM* es el directorio de instalación de IBM Tivoli Monitoring, vaya al directorio *dir_ITM*/bin y ejecute `./itmcmd manage [-h dir_ITM]`.Pulse con el botón derecho en el agente de supervisión y pulse **Avanzado → Editar archivo ENV**.
   - En la línea de mandatos, vaya al directorio de configuración del agente y abra el archivo de entorno en un editor de texto. Donde *cp* es el código de producto de dos caracteres:
     Windows *dir_instalación*\TMAITM6[_x64]\k*cp*env
     Linux UNIX *dir_instalación*/config/*cp*.ini
2. Especifique cómo conectar con un servidor de configuración central y descargar la lista de carga de configuración (programa de arranque) inicial:

   IRA_CONFIG_SERVER_URL
   Especifica el URL del servidor. Por ejemplo, http://9.52.111.99.

   IRA_CONFIG_SERVER_USERID
   Especifica el ID de usuario del servidor. Valor predeterminado: itmuser.

   IRA_CONFIG_SERVER_PASSWORD
   Especifica la contraseña del usuario en texto plano o como cadena de caracteres de contraseña cifrada de AES.

   IRA_CONFIG_SERVER_FILE_PATH
   Especifica la vía de acceso a la lista de carga de configuración en el servidor de configuración central. El valor predeterminado es loadlist/@PRODUCT@. Consulte "Sustitución de palabras clave en la lista de carga de configuración" en la página 459 para ver una lista de palabras clave.

   IRA_CONFIG_SERVER_FILE_NAME
   Especifica el nombre del archivo de lista de carga de configuración en el servidor de configuración central. Valor predeterminado: **cnfglist.xml**.

3. Guarde el archivo de entorno y recicle el agente para aplicar los cambios.

Establecimiento de variables de entorno de la configuración centralizada durante la instalación del agente supervisor del sistema

Puede utilizar variables de entorno de configuración centralizada del agente supervisor del sistema en el archivo de respuestas silencioso para apuntar al servidor de configuración central y descargar la lista de carga de configuración inicial (programa de arranque).

Acerca de esta tarea

Los agentes supervisores del sistema se inician al final de su instalación silenciosa. Sin archivos de configuración locales, los agentes se ejecutan pero no ejecutan situaciones privadas ni envían alertas SNMP ni sucesos EIF. Mediante la configuración centralizada, el agente puede recuperar estos archivos y empezar a utilizarlos de inmediato. La instalación del agente de supervisión del sistema utiliza entradas del archivo de respuestas silencioso para crear entradas en el archivo de entorno del agente.

Para obtener más información sobre el archivo de respuestas silencioso, cómo configurarlo y cómo invocarlo, consulte el tema "Supervisión del sistema operativo mediante un agente supervisor del sistema" de la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Procedimiento

1. Localice el archivo de respuestas *cp*_silent_install.txt (como por ejemplo ux_silent_install.txt) o el soporte de instalación del agente de Tivoli Monitoring y haga una copia del mismo.
2. Abra el archivo de respuestas silencioso en un editor de texto.
3. Especifique cómo conectar con el servidor de configuración central y descargue la lista de carga de configuración inicial.

   SETENV_ IRA_CONFIG_SERVER_URL
   Especifica el URL del servidor. Por ejemplo, http://9.52.111.99.

   SETENV_ IRA_CONFIG_SERVER_USERID
   Especifica el ID de usuario del servidor. Valor predeterminado: itmuser.

   SETENCR_IRA_CONFIG_SERVER_PASSWORD
   Especifica la contraseña del usuario como cadena de caracteres de contraseña cifrada de AES. Si desea especificarla en texto plano, preceda la variable de entorno con SETENV_ en lugar de con SETENCR_.

   SETENV_ IRA_CONFIG_SERVER_FILE_PATH
   Especifica la vía de acceso a la lista de carga de configuración en el servidor de configuración central. El valor predeterminado es loadlist/@PRODUCT@. Consulte "Sustitución de palabras clave en la lista de carga de configuración" en la página 459 para ver una lista de palabras clave.

   SETENV_ IRA_CONFIG_SERVER_FILE_NAME
   Especifica el nombre del archivo de lista de carga de configuración en el servidor de configuración central. Valor predeterminado: **cnfglist.xml**.

Las sentencias *SETENV_parameter=value* crean sentencias *parameter=value* en el archivo de entorno del agente; las sentencias *SETENCR_parameter=value* crean sentencias *parameter={AES256:keyfile:a}encryptedvalue*.

4. Invoque el procedimiento de instalación silenciosa tal como se describe en Ejemplo de un archivo de instalación silenciosa llamado nt_silent_installcc.txt que se invoca en un sistema Windows:

   ```
   silentInstall.cmd -p nt_silent_installcc.txt
   ```

   Ejemplo de un archivo de instalación silenciosa llamado ux_silent_installcc.txt en la vía de acceso /opt/IBM/sma de un sistema UNIX:

   ```
   silentInstall.sh -h /opt/IBM/sma/ -p ux_silent_installcc.txt
   ```

Ejemplo

Este ejemplo muestra una copia de nt_silent_install.txt del soporte de instalación que se puede editar para instalar un agente supervisor del sistema en el sistema local y configurarlo para la configuración centralizada:

Antes

```
;License Agreement=Acepto utilizar el software únicamente de acuerdo con
la licencia instalada.

;SETENV_IRA_CONFIG_SERVER_URL=http://configserver.domain.com:1920
;SETENV_IRA_CONFIG_SERVER_USERID=itmuser
;SETENCR_IRA_CONFIG_SERVER_PASSWORD=plaintext_or_encrypted_using_itmpwdsnmp
;SETENV_IRA_CONFIG_SERVER_FILE_PATH=initloadlist/@PRODUCT@
;SETENV_IRA_CONFIG_SERVER_FILE_NAME=cnfglist.xml
```

Después

```
License Agreement=Acepto utilizar el software únicamente de acuerdo con
la licencia instalada.

SETENV_IRA_CONFIG_SERVER_URL=http://mysystem.mydomain.ibm.com:1920
SETENV_IRA_CONFIG_SERVER_USERID=itmuser
SETENCR_IRA_CONFIG_SERVER_PASSWORD={AES256:keyfile:a}encryptedpassword
SETENV_IRA_CONFIG_SERVER_FILE_PATH=bootstraploadlist
SETENV_IRA_CONFIG_SERVER_FILE_NAME=cnfglist.xml
```

Iniciación de la configuración centralizada con un archivo de lista de carga

Si ha creado un archivo de lista de carga de configuración, inicie la configuración centralizada colocándolo en la ubicación adecuada e iniciando el agente. También puede hacerlo manualmente, utilizando un paquete de despliegue sin agente o mediante la interfaz de línea de mandatos con **tacmd putfile**.

Iniciación colocando manualmente el archivo de lista de carga

Puede iniciar la configuración centralizada colocando el archivo de lista de carga de configuración en el directorio de configuración del agente y reciclando el agente.

Antes de empezar

Cree el archivo de lista de carga de configuración mediante la codificación XML que se describe en "Especificación XML de la lista de carga de configuración" en la página 452.

Procedimiento

1. Acceda al sistema localmente y coloque la lista de carga de configuración *cp*_cnfglist.xml en el directorio *dir_instalación*/localconfig/*cp* del agente, donde *cp* es el código de producto de dos caracteres.
   - Windows *cp*_cnfglist.xml
   - Linux UNIX *cp*_cnfglist.xml
   - z/OS *CP*CFGLST.RKANDATV
   - IBM i a4_cnfglist.xml
2. Recicle el agente.

Resultados

Durante el arranque, el archivo de lista de carga de configuración se lee para el URL del archivo del servidor de configuración central y los archivos se descargan desde ahí.

Iniciación con despliegue remoto de paquetes sin agente

Si el entorno contiene un gran número de agentes existentes que están conectados a un Tivoli Enterprise Monitoring Server, es posible que prefiera utilizar el despliegue remoto para distribuir la lista de carga de configuración a los agentes. Puede utilizar Agent Builder para crear paquetes de despliegue sin agente.

Procedimiento

1. Utilice Agent Builder para crear un paquete de despliegue sin agente. Consulte la publicación *IBM Tivoli Monitoring Agent Builder User's Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/builder/agentbuilder_user.htm) para obtener detalles.
   a. Añada el archivo de programa de arranque común de la lista de carga de configuración confglist.xml al paquete.
   b. Cree su propio mandato de copia que copie el archivo en la ubicación correcta para el agente en el que tiene intención de realizar el despliegue. A continuación se muestra un ejemplo de mandato de instalación para el agente del sistema operativo Linux:
      ```
      cp |DEPLOYDIR|/cnfglist.xml |CANDLEHOME|/localconfig/lz/lz_cnfglist.xml
      ```
   c. Recicle el agente para empezar a utilizar la nueva lista de carga de configuración una vez desplegada.
      - Si lo desea, cree un mandato posterior a la instalación que utilice el servicio de vigilancia de los Servicios de gestión de agentes para reciclar el agente. Cree un mandato para cada plataforma a la que desee dar soporte porque debe especificar la vía de acceso completa al programa de utilidad pasctrl situado en el directorio de la arquitectura binaria del agente.
      - A continuación se muestran algunos de los mandatos posteriores a la instalación que puede utilizar:

        Windows
        ```
        dir_instalación\TMAITM6[_x64]\kcapasctrl.exe recycle nt
        ```

        Linux
        ```
        dir_instalación/lx8266/lz/bin/pasctrl.sh recycle lz
        ```

        UNIX
        ```
        dir_instalación/aix526/ux/bin/pasctrl.sh recycle ux
        ```

- Los agentes sin sistema operativo utilizan el servicio de vigilancia del agente de sistema operativo. Por ejemplo, un agente DB2 de varias instancias en Windows gestionado por Agent Management Services necesita que especifique el nombre de la instancia en el mandato posterior a la instalación. Por lo tanto, puede que la inclusión del reinicio en el paquete de despliegue no sea el mejor método, pero se puede hacer si se utilizan nombres de instancia estándares.

  ```
  dir_instalación\tmaitm6\kcapasctrl.exe recycle –o db2inst1 ud
  ```

- También podría incluir un script en el paquete de despliegue que contenga lógica más avanzada para reciclar instancias del agente y llamar a dicho script en un mandato posterior a la instalación.

  ```
  dir_despliegue/afterscript.sh
  ```

d. Genere el paquete de despliegue remoto.

e. Si el agente no se ha reiniciado mediante un mandato posterior a la instalación en el paquete de despliegue, recicle el agente para activar la lista de carga de configuración.

- Consulte el apartado "Inicio, detención y reciclaje de un agente mediante Tivoli Enterprise Portal" en la página 293.
- Los agentes del sistema operativo se pueden reciclar en el cliente de portal mediante el mandato de actuación AMS Reciclar instancia del agente
- El mandato de actuación AMS Reciclar instancia del agente también se puede ejecutar utilizando el mandato de CLI tacmd executeAction. A continuación se muestran algunos ejemplos para los agentes de sistema operativo:

  Windows

  ```
  tacmd executeaction -n "AMS Recycle Agent Instance" -t nt –m
  Primary:winhost:NT -c value="Monitoring Agent for Windows OS,
  kntcma.exe,,"
  ```

  Linux

  ```
  tacmd executeaction -n "AMS Recycle Agent Instance" -t lz –m
  linuxhost:LZ -c value="Monitoring Agent for Linux OS,klzagent,,"
  ```

  UNIX

  ```
  tacmd executeaction -n "AMS Recycle Agent Instance" -t ux –m
  unixhost:KUX -c value="Monitoring Agent for Unix OS,kuxagent,,"
  ```

2. Añada el paquete al depósito mediante el mandato de CLI **tacmd addbundles**.
3. Despliegue el paquete en los agentes mediante Añadir sistema gestionado en el cliente de portal (consulte "Adición de un agente mediante Tivoli Enterprise Portal" en la página 291) o mediante la CLI utilizando **tacmd addSystem** desde el servidor de supervisión (consulte el manual *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).
4. Si el agente no se ha reiniciado mediante un mandato posterior a la instalación en el paquete de despliegue, recicle el agente para activar la lista de carga de configuración tal como se describe en el paso 1.e.

Iniciación con tacmd putfile

Puede iniciar la configuración centralizada mediante el mandato de CLI **tacmd putfile** para transferir la lista de carga de configuración al agente de supervisión.

Acerca de esta tarea

Siga estos pasos para insertar la lista de carga de configuración en el agente de supervisión en el que desea iniciar la configuración centralizada. El manual *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) describe los mandatos tacmds y su sintaxis e incluye ejemplos.

Procedimiento

1. Inicie una sesión en el servidor de supervisión concentrador:

   ```
   tacmd login –s miservidorconcentrador –u minombreusuario –p micontraseña –t 1440
   ```

   donde *miservidorconcentrador* es el nombre de host completo del servidor de supervisión concentrador y *minombreusuario* y *micontraseña* corresponden a un ID de usuario válido para iniciar una sesión en el sistema operativo del servidor de supervisión.
2. Inerte el archivo: tacmd putfile –m Primary:winhost:NT -s C:\config\cnfglist.xml -d C:\IBM\ITM\localconfig\nt\nt_cnfglist.xml -t text
3. Recicle el agente para activar la lista de carga de configuración. Consulte el apartado Inicio, detención y reciclado de un agente mediante Tivoli Enterprise Portal
   - Los agentes de sistema operativo también se pueden reciclar en el cliente de portal mediante la instancia de actuación del espacio de trabajo AMS Reciclar instancia de agente; abra el espacio de trabajo Servicios de gestión de agentes del agente de sistema operativo, pulse con el botón derecho en el agente de sistema operativo en la vista de tabla “Estatus de entorno de ejecución de agente” y pulse **Actuación - Seleccionar**; luego seleccione **AMS Reciclar instancia de agente**.
   - El mandato de actuación AMS Reciclar instancia de agente también se puede ejecutar mediante el mandato de CLI **tacmd executeAction**. A continuación se muestran algunos ejemplos para los agentes de sistema operativo:

     Windows

     ```
     tacmd executeaction -n "AMS Recycle Agent Instance" -t nt -m
     Primary:winhost:NT -c value="Monitoring Agent for Windows OS,
     kntcma.exe,,"
     ```

     Linux

     ```
     tacmd executeaction -n "AMS Recycle Agent Instance" -t lz -m
     linuxhost:LZ -c value="Monitoring Agent for Linux OS,klzagent,,"
     ```

     UNIX

     ```
     tacmd executeaction -n "AMS Recycle Agent Instance" -t ux -m
     unixhost:KUX -c value="Monitoring Agent for Unix OS,kuxagent,,"
     ```

Iniciación de la configuración centralizada con una solicitud de interfaz de servicio

Puede enviar solicitudes de interfaz de servicio de forma interactiva en un navegador o puede utilizar kshsoap para enviar solicitudes de interfaz de servicio desde un script. Utilice la interfaz de servicio para iniciar la configuración centralizada enviando la lista de carga de configuración como una solicitud.

Iniciación en la Interfaz de servicio del agente

Utilice la Interfaz de servicio del agente para iniciar la configuración centralizada enviando la lista de carga de configuración como una solicitud.

Acerca de esta tarea

Siga estos pasos para especificar la lista de carga de configuración como una solicitud en la Interfaz de servicio del agente .

Procedimiento

1. Abra un navegador y acceda al índice de servicios del agente con el URL `http://nombrehost:1920` o `https://nombrehost:3661`, donde `nombrehost` es el nombre completo o la dirección IP del sistema en el que está instalado el agente de supervisión.
2. Pulse el enlace **IBM Tivoli *cp* Interfaz de servicio del agente** correspondiente al agente, donde *cp* es el código de producto de dos caracteres.
3. Cuando se le solicite, especifique el nombre de usuario y la contraseña. El ID debe ser miembro del grupo **Administrativo** del Perfil de grupo de autorización de acceso en el agente del cliente de configuración central.
4. Seleccione el enlace con la solicitud de interfaz de servicio.
5. Pegue el contenido del archivo XML de la lista de carga de configuración en el recuadro de texto Solicitud de interfaz de servicio del agente y luego envíe la solicitud.

Qué hacer a continuación

Puede utilizar la Interfaz de servicio del agente para enviar la lista de carga de configuración como una solicitud de interfaz de servicio siempre que desee renovar la configuración local bajo demanda.

Iniciación utilizando la API de interfaz de servicio (kshsoap)

La interfaz de servicio es una API que permite crear una interfaz personalizada. Con los agentes se proporcionan archivos HTML de muestra para demostrar la función de la interfaz de servicio. También se puede acceder a la API mediante programación utilizando Java, Visual Basic, Perl, HTML y otros lenguajes. El Tivoli Enterprise Monitoring Server incluye un programa de utilidad de línea de mandatos denominado *kshsoap* que se puede utilizar dentro de un script para enviar estas solicitudes de interfaz de servicio. Puede utilizar kshsoap para iniciar la configuración centralizada.

Procedimiento

1. Cree un archivo llamado **request.xml** con los elementos <UUSER> y <UPASS> para especificar las credenciales que necesita kshsoap para conectar con la interfaz de servicio del agente. Este ID se debe definir en los sistemas de destinos a los que piensa enviar la solicitud. Asimismo, el ID debe ser miembro del grupo **Administrativo** en el Perfil de grupo de autorización de acceso del agente de destino. Ejemplo:

```
<ConfigurationArtifact>
  <UUSER>root</UUSER>
  <UPASS>{AES256:keyfile:a}ENRUCXLW40LpR0RtGSF97w==</UPASS>
    <ConfigServer
        Name="CENTRAL-CONFIG-SERVER"
        URL="http://winhost:1920///system.winhost_nt/system.winhost_nt/"
        User="Administrator"
        Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
    <ConfigFile
        Server="CENTRAL-CONFIG-SERVER"
        Name="cnfglist.xml"
```

```
        Path="@PRODUCT@"
        Disp="CNFGLIST"
        Activate="YES" />
</ConfigurationArtifact>
```

Los elementos <UUSER> y <UPASS> se puede sustituir por <UNAME> y <UWORD> si no desea la contraseña cifrada y prefiere especificarla en texto plano.

2. Cree otro archivo de texto llamado **urls.txt** que contenga los URL de la solicitud de interfaz de servicio del agente. Ejemplo:

```
http://linuxhost:1920///linuxhost_lz/linuxhost_lz
http://unixhost:1920///unixhost_ux/unixhost_ux
```

3. Utilice kshsoap para enviar **request.xml** a las interfaces de servicio mostradas en **urls.txt**. En un servidor de supervisión Windows, kshsoap.exe está en el directorio *dir_instalación*\CMS; en un servidor de supervisión Linux o UNIX, kshsoap.exe se encuentra en el directorio *dir_instalación*/*interp*/ms/bin.

   - Windows

     dir_instalación\CMS\kshsoap
     víaacceso_a_archivo\request.xml *víaacceso_a_archivo*\urls.txt

   - Linux UNIX

     dir_instalación/*interp*/ms/bin/kshsoap
     víaacceso_a_archivo/request.xml *víaacceso_a_archivo*/urls.txt

Autonomía de agente en z/OS

En los temas sobre autonomía del agente hay referencias a archivos y excepciones en agentes de supervisión basados en z/OS. Este tema consolida esta información.

Servidor de configuración central
El servidor de configuración central debe estar en un sistema distribuido; el sistema z/OS no recibe soporte.

Lista de carga de configuración
El agente de supervisión descarga todos los elementos de la lista de carga de configuración al arrancar el agente. El agente utiliza la indicación de fecha y hora de la descarga del archivo inicial como referencia y empieza a llevar un seguimiento de la hora de la última modificación del archivo. Un cambio en la copia del servidor del archivo que se produzca tras esta indicación de fecha y hora se descarga y la indicación de fecha y hora de la última modificación del archivo se actualiza.

Nombres predeterminados para miembros de la configuración local del agente de supervisión z/OS en el conjunto de datos RKANDATV
Donde *CP* es el código de producto de dos caracteres:

*CP***CFGLST**
Nombre de miembro de conjunto de datos de carga de configuración local

*CP***THRES**
Nombre de archivo de alteración temporal de umbral local.

*CP***TRAPS**
Nombre de archivo de configuración de condición de excepción SNMP local

*CP***SICNFG**
Nombre de archivo de configuración de situación privada de agente local

*CP***EIF** Nombre de archivo de configuración de correlación de sucesos de EIF de agente local

*CP***EVMAP**
Nombre de archivo de configuración de destino de EIF de agente local

Activate="RESTART" no recibe soporte en z/OS
La opción RESTART se utiliza para reiniciar el agente tras una descarga de archivo correcta. No recibe soporte en z/OS ni en sistemas operativos i5. El proceso del agente se debe reiniciar de otra forma para activar la nueva configuración.

Varios agentes que se ejecutan en el mismo espacio de direcciones
Cualquier parámetro de alteración temporal definido en el miembro `KDSENV` del conjunto de datos *`&hilev.&rte.`*`RKANPARU` se utiliza para todos los agentes que se ejecutan dentro del espacio de direcciones. Esto funciona bien para `IRA_EIF_DEST_CONFIG`, porque probablemente todos los agentes compartirán el mismo destino de suceso EIF. Los otros parámetros de alteración temporal también se pueden utilizar, pero es posible que los miembros del conjunto de datos identificado tengan que combinar definiciones para varios agentes, lo que no se recomienda. La práctica recomendada consiste en utilizar el convenio de denominación predeterminada para miembros del conjunto de datos de la configuración local cuando se ejecutan varios agentes en el mismo espacio de direcciones.

Cifrado de contraseñas
Los archivos XML de configuración local incluyen credenciales de usuario con contraseñas que se pueden especificar en texto plano. La protección del acceso a estos archivos de configuración suele resultar adecuada para asegurar las credenciales. También puede añadir una capa de seguridad almacenando contraseñas en formato cifrado dentro del archivo de configuración.

Si habilita alertas de SNMP desde el agente, las cadenas de caracteres de comunidad de SNMP v1 y v2c y las contraseñas de autenticación y privacidad de SNMP v3 se pueden almacenar en formato cifrado en el archivo de configuración de condiciones de excepción *CP*TRAPS.RKANDATV.

Si va ha habilitar la configuración centralizada, los atributos de contraseña de ConfigServer se pueden cifrar cuando se almacenan en un archivo de lista de carga de configuración xxCFGLST.RKANDATV o mediante la variable de entorno IRA_CONFIG_SERVER_PASSWORD.

Consulte el tema sobre “Cifrado de contraseñas en archivos de configuración en z/OS” en *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Planning and Configuration* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm) para ver instrucciones.

Capítulo 17. Gestión de datos históricos

Tivoli Management Services proporciona herramientas para recopilar y guardar muestras de datos, mostrar informes históricos, cargar datos en una base de datos relacional para su almacenamiento a largo plazo o convertir archivos históricos a corto plazo en archivos planos delimitados y para la agregación y poda de datos. Estos temas describen los componentes utilizados para la recopilación de datos históricos, cómo almacenan los datos y prácticas recomendadas para configurar la recopilación de datos y mantener la base de datos.

Los temas de "Soluciones de Tivoli Data Warehouse" de la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* describen cómo instalar y configurar un Tivoli Data Warehouse y sus agentes necesarios, el proxy de almacén y el agente de resumen y poda.

Los temas sobre "Configuración de la recopilación de datos históricos" del manual *Tivoli Enterprise Portal: Guía del usuario* describe cómo configurar recopilaciones de datos históricos para grupos de atributos, cómo obtener un informe de datos históricos correspondiente a un intervalo de tiempo especificado, cómo aplicar líneas base históricas a un diagrama para realizar un análisis de tendencia y cómo modelar umbrales de situación utilizando datos históricos.

En el manual *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) se describen los mandatos de historial **tacmd** que se pueden especificar en la línea de mandatos para configurar recopilaciones de datos históricos, visualizar sus definiciones y exportar e importar las definiciones de recopilación de datos históricos.

Acerca de la recopilación de datos históricos

Para que los datos históricos estén disponibles para informes y análisis, debe configurar las recopilaciones de datos históricos. Una o varias de estas recopilaciones se configuran para cada grupo de atributos para los que desea recopilar datos históricos y se distribuyen a los sistemas gestionados que especifique.

Recopilación de datos históricos

Los programas de configuración le permiten especificar la recopilación de datos históricos. Los datos históricos se almacenan en archivos históricos a corto plazo en el servidor de Tivoli Enterprise Monitoring o en el agente de supervisión. Puede elegir especificar que los datos históricos se envíen a la base de datos de Tivoli Data Warehouse para el almacenamiento a largo plazo. El modelo de datos es el mismo en los datos históricos a largo plazo y a corto plazo.

Puede crear otra copia de una definición de recopilación para un grupo de atributos, luego configurar la copia para distintos valores para cualquiera de estos criterios: intervalo de recopilación, intervalo de almacén, distribución de sistemas gestionados o filtrado de atributos. Sin embargo, lo que permanece igual en cada recopilación histórica definida para un grupo de atributos es la Ubicación de recopilación(TEMA o TEMS) y los valores de Resumen y poda.

© Copyright IBM Corp. 2005, 2013

Distribuya a Sistema gestionado (agente) o a Sistema de gestión (TEMS)
Cada recopilación de datos históricos tiene un método de distribución:

Sistema gestionado (agente) es el método predeterminado y requiere que cualquier sistema gestionado de la distribución se conecte a un servidor de Tivoli Enterprise Monitoring V6.2.2 o posterior. La distribución se dirige a un subconjunto de sistemas gestionados: los sistemas gestionados de este tipo de agente que están asignados individualmente o como parte de un grupo de sistemas gestionados. Como alternativa, puede asignar sistemas gestionados para su distribución a un grupo de configuración de historial al que pertenece la recopilación.

Sistema de gestión (TEMS) es el método utilizado para la distribución en IBM Tivoli Monitoring Versión 6.2.1 y anteriores; es el método necesario para la distribución si el sistema gestionado se conecta a un servidor de supervisión V6.2.1 o anterior. La distribución se realiza a los sistemas gestionados de este tipo de agente que están conectados al servidor de Tivoli Enterprise Monitoring. Si se ha elegido el método Sistema de gestión (TEMS) para una definición de recopilación, dicha recopilación pasa a no ser apta como miembro de un grupo de configuración de historial.

Si ha actualizado a Tivoli Management Services Versión 6.2.2 o superior desde un release anterior a la Versión 6.2.2, obtiene una definición de recopilación histórica para cada grupo de atributos configurado y el método de distribución no se modifica: **Sistema de gestión (TEMS)**. Si desea utilizar las técnicas de distribución disponibles cuando la distribución se realiza por sistema gestionado, cambie el método de distribución para cada definición de recopilación por **Sistema gestionado (agente)**.

Grupos de objetos de configuración histórica

Una parte de la definición de la recopilación histórica es la lista de distribución, en la que se especifican los sistemas gestionados que guardarán los muestreos de datos históricos. Puede añadir la distribución directamente a la recopilación histórica, indirectamente mediante un grupo de objetos de configuración histórica o una combinación de ambos.

- La **distribución directa** requiere asignar a la recopilación histórica los sistemas gestionados individuales o los grupos de sistemas gestionados o ambas cosas. La ventaja de este método es que la distribución sólo se aplica a esta recopilación y puede añadir y eliminar fácilmente los sistemas gestionados, según sea necesario.
- La **distribución indirecta** requiere los sistemas gestionados individuales o los grupos de sistemas gestionados, o ambas cosas, al grupo de recopilación histórica del que es miembro la recopilación histórica. La ventaja de este método es que puede establecer una lista de distribución y aplicarla a varias recopilaciones históricas, simplemente añadiendo dichas recopilaciones al miembro del grupo histórico.

Utilice grupos de configuración histórica como método para asignar la misma lista de distribución a varias definiciones de recopilaciones históricas. A continuación, puede controlar la recopilación para el grupo, en lugar de tener que seleccionar las definiciones de recopilaciones históricas de forma individual. Esta función está disponible cuando el servidor de Tivoli Enterprise Portal y el servidor de Tivoli Enterprise Monitoring están a la versión 6.2.2 o posterior y el método de distribución está establecido en **Sistema gestionado (Agente)**.

Esquema de almacén

El almacén de datos tiene una o varias tablas para cada producto, con nombres de columna que están relacionados con el contenido de datos. Esta plataforma sigue un modelo de datos simple que se basa en el concepto de atributos. Un atributo es una característica de un objeto (nodo) gestionado. Por ejemplo, el nombre de disco es un atributo para un disco, que es un objeto gestionado.

Los atributos pueden ser de una sola fila o de varias filas. Los atributos de una sola fila sólo reúnen un conjunto de datos, por ejemplo los atributos de hora local porque sólo hay un conjunto de valores para la hora local en un momento determinado. Los atributos de varias filas pueden reunir varios conjuntos de datos, por ejemplo el atributo Avg_Queue que devuelve un conjunto de datos para cada cola que existe en el sistema. Cada atributo pertenece a un grupo de atributos y cada elemento de atributo almacena datos para una propiedad determinada del grupo de atributos.

Para cada grupo de atributos se genera una tabla y se utilizan los nombres de tabla para la recopilación de datos históricos. Las guías de usuario individuales del agente de supervisión contienen descripciones completas de los grupos de atributos específicos de dicho agente.

Proxy de almacén

Los sistemas gestionados a los que se han distribuido configuraciones de recopilación de datos envían datos a Tivoli Data Warehouse a través del proxy de almacén, un proceso servidor multihebra que puede manejar solicitudes simultáneas de varios agentes de supervisión. Si no es posible alcanzar el proxy de almacén, el agente intenta la transmisión en el siguiente intervalo de almacén (hora siguiente o día siguiente, en función del valor). Si, en el siguiente intervalo, el proxy de almacén no devuelve el estatus durante la transmisión, se reinicia la transacción. Entonces, después de 15 minutos, se reenvían los datos al proxy de almacén. Si el proxy de almacén devuelve un estatus que indica una anomalía, se reiniciará la transacción en el siguiente intervalo de almacén.

Puede tener varios agentes de proxy de almacén en un entorno supervisado. Instale varios agentes de proxy de almacén en un entorno de gran tamaño para abarcar el trabajo de recibir datos históricos de los agentes de supervisión e insertarlos en la base de datos de almacén.

Si no tiene intención de guardar datos históricos en un almacén de datos, no es necesario que instale y configure el proxy de almacén ni el agente de resumen y poda. Si no se utiliza proxy de almacén, es necesario utilizar programas adicionales para recortar los archivos históricos a corto plazo.

Resumen y poda de almacén

El agente de resumen y poda de almacén proporciona la posibilidad de personalizar el tiempo durante el cual se deben guardar datos (poda) y la frecuencia con la que se deben agregar datos (resumen) en el almacén de datos. Con los datos resumidos, el rendimiento de las consultas puede mejorar de forma drástica. Y con el trabajo conjunto del resumen de datos y de la poda de datos, la cantidad de espacio de disco utilizado se puede gestionar mejor.

El resumen de almacén se controla para cada tabla (grupo de atributos). El modo en que se resumen las filas de cada una de las tablas lo determina un conjunto de atributos de cada tabla que han sido designados como *claves primarias*. Siempre hay una clave primaria, ORIGINNODE

(denominado normalmente Nombre de servidor o Nombre de sistema), lo que significa que el recurso gestionado resume dichos datos. Se proporcionan una o más claves primarias adicionales para refinar adicionalmente el nivel de resumen de dicha tabla. Por ejemplo, en una tabla de disco de agente de sistema operativo, es posible que una clave primaria sea el *nombre de disco lógico*, lo que permite proporcionar información histórica para cada disco lógico del sistema.

Solo puede haber un agente de resumen y poda en el entorno gestionado, que se conecta directamente a Tivoli Data Warehouse.

Configuración de la recopilación de datos históricos

Después de que las recopilaciones de datos históricos configurados comiencen a guardar muestreos de datos, tome las medidas necesarias para gestionarlos. Si no se realiza ninguna acción adicional, los archivos de datos históricos crecen sin control y pueden agotar un espacio de disco necesario.

Definición de la recopilación de datos históricos

La ventana Configuración de la recopilación histórica está disponible a través de Tivoli Enterprise Portal. Puede especificar la recopilación y el almacenamiento de datos históricos en el Tivoli Enterprise Monitoring Server o en el sistema remoto donde está instalado el agente de supervisión. Para una mayor flexibilidad en la utilización de la recopilación de datos históricos, puede:

- Configurar varias recopilaciones para el mismo grupo de atributos. Cada recopilación tiene una distribución distinta, puede tener un intervalo de recopilación distinto y puede tener un intervalo de almacenamiento distinto.
- Reducir la cantidad de datos recopilados sólo a los que pasan un filtro creado por el usuario. Por ejemplo, recopilar solo las muestras de datos con tiempo de ocupación de procesador superior al 80%.
- Configurar una recopilación histórica para todos los sistemas gestionados en un servidor de supervisión específico cuando la distribución tenga el valor “Sistema de gestión (TEMS)” y para cualquier sistema gestionado o conjunto de sistemas gestionados cuando la distribución tenga el valor “Sistema gestionado (Agente)”.
- Establecer la **Ubicación de recopilación** para guardar un historial a corto plazo en el servidor de supervisión o en el agente de supervisión para cada recopilación histórica.
- Establecer el **Intervalo de recopilación**, la frecuencia con la que hay que enviar muestras de datos al archivo histórico a corto plazo, con un valor comprendido entre cada minuto y una vez al día para cada recopilación histórica.
- Establecer el **Intervalo de almacén**, la frecuencia con la que hay que guardar datos en el Tivoli Data Warehouse, que va de 15 minutos a una vez al día para cada recopilación histórica.
- Determinar el modo y el momento en que se deben resumir y podar los datos que están almacenados en el almacén de datos. El resumen y poda se configura para cada grupo de atributos que tenga una o varias recopilaciones de datos definidas.
- Iniciar la recopilación en un sistema gestionado añadiéndolo (o un grupo de sistemas gestionados al que pertenezca) a la lista de distribución de una recopilación histórica o a un grupo de configuración histórica de la que la recopilación sea miembro.

- Detener la recopilación en un sistema gestionado eliminándolo (o un grupo de sistemas gestionados al que pertenezca) de la lista de distribución de una recopilación histórica o de un grupo de configuración histórica del que la recopilación sea miembro.
- Crear grupos de configuración histórica con una lista de distribución y asignar recopilaciones al grupo que desee que utilice la distribución.

Definición de recopilaciones de datos históricos desde la línea de mandatos

La recopilación de datos históricos también se puede configurar mediante los mandatos **tacmd hist** de la interfaz de línea de mandatos:

histconfiguregroups

histcreatecollection

histdeletecollection

histeditcollection

histlistattributegroups

histlistcollections

histlistproduct

histstartcollection

histstopcollection

histunconfiguregroups

histviewattributegroup

histviewcollection

bulkExportSit (para exportar recopilaciones de datos históricos)

bulkImportSit (para importar recopilaciones de datos históricos)

Si tiene un entorno de prueba, puede escribir scripts que utilicen tacmds para las recopilaciones de datos históricos y ejecutar el script en otros sistemas de prueba o en el sistema de producción, de modo que no tenga que repetir la misma configuración para cada sistema. Hallará más información sobre estos mandatos en *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm).

Evitar la recopilación de datos redundantes

Es posible que se recopilen datos dos o más veces para el mismo grupo de atributos en un sistema gestionado. Esto sucede si ha configurado varias recopilaciones históricas para el mismo grupo de atributos y las distribuye al mismo sistema gestionado. Esto no solo crea más tráfico de datos y utiliza espacio de almacenamiento innecesario, si no que además los valores de resumen pueden aparecer distorsionados. La distorsión se debe a que se tiene en cuenta el factor de valores adicionales enviados por varias recopilaciones para el mismo grupo de atributos en el cálculo del resumen.

Para una determinada recopilación histórica, no debe preocuparse de asignar inadvertidamente el mismo sistema gestionado a la distribución de recopilación histórica varias veces. La función histórica tiene en cuenta los sistemas gestionados a los que se distribuye la recopilación y recopila una muestra de datos una sola vez por cada sistema gestionado. Un sistema gestionado se incluye en la distribución de una recopilación de datos históricos cuando:

- se hace referencia al mismo directamente en la definición de la recopilación

- está en un grupo de sistemas gestionados al que se hace referencia en la definición de la recopilación
- está en la distribución de un grupo de configuración histórica del que la recopilación histórica es miembro
- está en un grupo de sistemas gestionados que está en la distribución de un grupo de configuración histórica del que la recopilación histórica es miembro

Crear fórmulas de filtro para la recopilación de datos granular

El editor de configuraciones de recopilación de datos históricos tiene un separador **Filtro** con un editor de fórmulas para escribir criterios de filtro que especifiquen los datos que hay que recopilar. La recopilación histórica de una muestra de datos se produce únicamente si los valores de la fila de datos cumplen con los criterios de filtro. Por ejemplo, si el valor del atributo de % de tiempo de escritura en disco es superior al 50%, la muestra de datos se guarda en el histórico a corto plazo; de lo contrario, la muestra no se guarda.

Los criterios de filtro se pueden configurar para cada definición de recopilación. La aplicación de filtros a la recopilación de datos históricos puede ayudar a reducir el tráfico en la red y el espacio de disco malgastado y a mejorar el rendimiento de la función de resumen y poda.

Tenga en cuenta que la recopilación de datos históricos puede afectar a los resultados de cálculos de tendencias realizados con líneas base de diagrama y modelado de situaciones y de vistas basadas en consulta que incluyan datos históricos. Por ejemplo, un filtro para recopilar únicamente filas en las que el proceso utiliza un 80% o más de CPU significa que un cálculo de valores promedios solo se realizará de valores del 80% y superiores, en lugar de hacerlo de todos los valores.

Limitación del crecimiento de archivos históricos a corto plazo

Si ha elegido subir datos mediante el proxy de almacén a Tivoli Data Warehouse, los archivos históricos a corto plazo del servidor de supervisión y del agente de supervisión se recortan automáticamente tras la subida.

Tipo de recopilación Sistema de gestión (TEMS)

La recopilación de datos históricos se puede especificar para servidores de supervisión, productos y grupos de atributos. Sin embargo, todos los agentes del mismo tipo que informan directamente al mismo servidor de supervisión deben tener las mismas opciones de recuperación histórica. Asimismo, para un determinado grupo de atributos, se aplican las mismas opciones de recopilación histórica a todos los servidores de supervisión para los que se ha habilitado actualmente dicha recopilación.

Ubicación de la recopilación

La **Ubicación de recopilación** es donde reside el archivo de datos históricos a corto plazo: en TEMA (Tivoli Enterprise Monitoring Agent) o en TEMS (Tivoli Enterprise Monitoring Server). La ubicación predeterminada es TEMA, que minimiza el impacto de rendimiento sobre el servidor de supervisión desde la gestión de datos históricos. No obstante, hay algunas combinaciones de grupos de productos y atributos que sólo se recopilan en un lugar específico, el servidor de supervisión o el agente de supervisión.

z/OS En productos OMEGAMON XE, el almacén de datos permanentes se utiliza para almacenar historiales a corto plazo, de modo que se debe configurar en la ubicación de la recopilación. Para cualquier

agente proporcionado, no varíe la ubicación de recopilación: recopile todos los datos históricos del producto en el agente de supervisión o en el servidor de supervisión. Para los agentes que están configurados en el mismo espacio de direcciones que los servidores de supervisión (necesario para OMEGAMON XE for z/OS y OMEGAMON XE for Storage en z/OS), configure el almacén de datos permanentes en el mismo espacio de direcciones y especifique TEMS como la ubicación de recopilación.

Agregar y podar datos de almacén

El Agente de resumen y poda es un mecanismo para gestionar los datos de Tivoli Data Warehouse. Los datos del almacén son un registro histórico de actividad y condiciones de la empresa. El resumen de los datos es el proceso mediante el cual se agregan los datos históricos en categorías basadas en el tiempo, por ejemplo por horas, diariamente, semanalmente, etc. El resumen de los datos le permite realizar el análisis histórico de los datos a lo largo del tiempo. La poda de los datos mantiene la base de datos en un tamaño que se puede gestionar y, de este modo, mejora el rendimiento. La poda de la base de datos se debe realizar a intervalos regulares.

Importante: Sólo puede ejecutar un agente de resumen y poda aunque tenga varios servidores de supervisión que compartan una sola base de datos de Tivoli Data Warehouse. La ejecución de varios agentes de resumen y poda causa puntos muertos de la base de datos y conflictos porque las diversas instancias pueden intentar resumir y podar los datos de las tablas simultáneamente.

Conversión de archivos de historial a corto plazo en archivos planos delimitados

Si elige no utilizar Tivoli Data Warehouse, debe establecer trabajos de acumulación para que conviertan y vacíen con regularidad los archivos de datos históricos. Se proporcionan programas de acumulación. Además de cortar los archivos de datos históricos, estos scripts producen archivos planos que se pueden utilizar con herramientas de otros proveedores para producir informes y gráficos de análisis de tendencias. También hay una variable de entorno para establecer el tamaño máximo de los archivos históricos.

Consulte el apartado “Limitación del crecimiento de archivos históricos a corto plazo” en la página 522.

Algunos grupos de atributos no son aptos para la recopilación de datos históricos

Algunos agentes no permiten la recopilación de datos históricos para todos los grupos de atributos. Esto se debe a que el equipo de desarrollo de producto para dicho agente ha determinado que la recopilación de datos históricos para determinados grupos de atributos no es apropiada o puede tener un efecto perjudicial en el rendimiento. Esto se puede deber a la gran cantidad de datos que se generan. Por lo tanto, para cada producto, solo los grupos de atributos que están disponibles para la recopilación histórica se muestran en la ventana Configuración de la recopilación de datos históricos cuando pulsa una Aplicación supervisada.

Cambio del directorio de archivos históricos a corto plazo

Cuando se ha configurado que se recopilen datos históricos en el agente (TEMA; no TEMS), utilice la variable de entorno del agente CTIRA_HIST_DIR para cambiar el directorio en el que se recopilan datos históricos. Por ejemplo, es posible que desee almacenar archivos históricos en un disco que proporcione más capacidad de almacenamiento que el que ofrece la ubicación predeterminada del archivo de datos históricos.

Antes de empezar

El directorio debe estar en un directorio existente, debe especificar la vía de acceso completa y el ID de usuario del sistema operativo debe tener permiso de grabación sobre este directorio. Si el directorio no existe, el agente no recopilará datos históricos.

Acerca de esta tarea

Siga estos pasos para editar la variable de entorno del agente CTIRA_HIST_DIR para establecer otro directorio en el que almacenar los archivos históricos a corto plazo.

Procedimiento

- Windows
  1. En la ventana Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho del ratón en la aplicación supervisada y pulse **Avanzado** → **Editar variables**.
  2. En la ventana Alterar temporalmente valores de variables locales, pulse **Añadir**.
  3. Desplácese por la lista de variables y seleccione **CTIRA_HIST_DIR**
  4. En el campo Valor, sustituya `@LogPath@` por la vía de acceso completa al directorio en el que desea guardar el historial a corto plazo.
  5. Pulse **Aceptar** para ver CTIRA_HIST_DIR en la columna **Variable** y la nueva vía de acceso en la columna **Valor**; vuelva a pulsar **Aceptar** para cerrar la ventana. El valor se graba en el archivo K*cp*ENV, como por ejemplo KNTENV.
  6. Recicle el agente para que los cambios entren en vigor.
- Linux UNIX
  1. Vaya al directorio `<dir_instalación_itm>/config` y abra `cp.ini` en un editor de texto, donde *cp* es el código del producto de dos caracteres. Por ejemplo, `/opt/IBM/ITM/config/ux.ini` para el agente de SO UNIX. Para obtener una lista de códigos de producto, consulte "Códigos de producto, plataforma y componente de IBM Tivoli" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.
  2. En una nueva línea, añada esta variable de entorno seguida de la vía de acceso completa a la ubicación en la que desea guardar el historial a corto plazo:
     ```
     CTIRA_HIST_DIR=
     ```
  3. Guarde y cierre el archivo.
  4. Recicle el agente para que los cambios entren en vigor.

Impacto de rendimiento de las solicitudes de datos históricos

El impacto de la recopilación y del almacenaje de datos históricos en componentes Tivoli Management Services depende de varios factores, incluyendo el intervalo de recopilación, la frecuencia de acumulación en el almacén de datos, el número y el tamaño de las tablas históricas recopiladas, el tamaño del sistema, etc.

Impacto de grandes cantidades de datos históricos en el servidor o agente de supervisión

La ubicación predeterminada para almacenar datos históricos a corto plazo está en el agente de supervisión, aunque en determinadas configuraciones es posible que sea preferible el servidor de supervisión.

Este tema presenta factores a tener en cuenta al determinar

- Los grupos de atributos en los que recopilar los datos históricos
- El lugar donde guardar los archivos de datos de corto plazo
- La frecuencia con la que se deben enviar muestras de datos históricos a la ubicación de recopilación de corto plazo
- Si se deben almacenar datos del grupo de atributos y, en caso afirmativo, la frecuencia con la que se deben enviar los datos de los archivos de histórico a corto plazo al almacén de datos

La ubicación de recopilación puede quedar impactada de forma negativa cuando se procesan grandes cantidades de datos. Esto se produce porque el proceso de almacén del servidor de supervisión o del agente de supervisión debe leer el gran conjunto de filas de los archivos históricos a corto plazo. Entonces el proxy de almacén debe transmitir los datos al almacén de datos. Para conjuntos de datos grandes, esto produce un impacto en la memoria, los recursos de CPU y, especialmente cuando la recopilación es en el servidor de supervisión, el espacio de disco.

Debido a la posibilidad de manejar muchas solicitudes simultáneamente, es posible que el impacto en servidor de supervisión no sea tan grande como el impacto en el agente de supervisión. Sin embargo, cuando la recopilación histórica es en el servidor de supervisión, el archivo de datos históricos para un grupo de atributos puede contener datos para muchos agentes (todos los agentes que almacenan los datos en el servidor de supervisión) creando de este modo un conjunto de datos más grande. Además, las solicitudes en un conjunto de datos grande también producen un impacto en la memoria y en los recursos del Tivoli Enterprise Portal Server.

Cuando se almacenan datos históricos en el agente, el archivo histórico para un grupo de atributos sólo contiene datos para dicho agente y es mucho menor que el que está almacenado en el servidor de supervisión. Los datos de valor de las 24 horas más recientes proceden archivos históricos a corto plazo. Más allá de las 24 horas, los datos se recuperan de Tivoli Data Warehouse. (Puede cambiar el punto de salto con la variable de entorno KFW_REPORT_TERM_BREAK_POINT del servidor de portal.) Esta acción resulta transparente para el usuario; sin embargo, las solicitudes que devuelven gran cantidad de datos pueden afectar de forma negativa al rendimiento de los servidores de supervisión, los agentes de supervisión y la red.

Si una consulta va a un archivo histórico a corto plazo y recupera una gran cantidad de datos, esta recuperación puede consumir una gran cantidad de CPU y memoria y los usuarios pueden ven reducido el rendimiento del sistema mientras se están recuperando datos. Cuando se procesa una gran solicitud de datos, es

posible que se impida que el agente procese otras solicitudes hasta que se haya completado esta solicitud. Esto es importante con muchos agentes de supervisión porque normalmente el agente sólo puede procesar una consulta de vista o una situación a la vez.

Una práctica recomendada que se puede aplicar a la recopilación de datos históricos, a la consulta de vistas o a ambos consiste en utilizar filtros para limitar los datos *antes* de que se recopilen o se notifiquen. Para las recopilaciones de datos históricos, el filtrado previo se realiza en el separador **Filtro** del editor de la configuración de la recopilación de datos históricos o la opción de filtrado de la CLI **tacmd histcreatecollection**, tal como se describe en *IBM Tivoli Monitoring Command Reference* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) y en Creación de una recopilación de datos históricos de *Tivoli Enterprise Portal: Guía del usuario*. Para las vistas de espacios de trabajo, el filtrado previo se realiza en el editor de consultas creando otra consulta a partir de una consulta predefinida y añadiendo un filtro a la especificación, tal como se describe en Creación de otra consulta para el servidor de supervisión de *Tivoli Enterprise Portal: Guía del usuario*.

Solicitudes de datos históricos de tablas grandes

Las solicitudes de datos históricos de tablas que recopilan una gran cantidad de datos tienen un impacto negativo en el rendimiento de los componentes de Tivoli Management Services implicados. Para reducir el impacto de rendimiento en el sistema, establezca un intervalo de recopilación o cree un filtro (o ambos) más largo para las tablas que recopilan una gran cantidad de datos.

Especifique el intervalo de recopilación y los criterios de filtrado en la ventana Configuración de recopilación histórica. Para averiguar los requisitos de espacio de disco para tablas del producto IBM Tivoli Monitoring, consulte la documentación del agente específico.

Al visualizar una vista basada en consulta, puede establecer el intervalo de tiempo para obtener datos de muestreos anteriores. Si se selecciona un intervalo de tiempo largo para el intervalo de tiempo de informe, aumenta la cantidad de datos que se están procesando y esto puede tener un impacto negativo en el rendimiento. El programa debe dedicar más memoria y ciclos de CPU para procesar un gran volumen de datos de informe. En esta instancia, especifique un valor de intervalo de tiempo más corto, especialmente para tablas que recopilan una gran cantidad de datos.

Si un conjunto de filas de informe es demasiado grande, la solicitud de informe puede eliminar la tarea y volver a Tivoli Enterprise Portal sin filas porque el agente ha tardado demasiado tiempo en procesar la solicitud. Sin embargo, el agente continúa procesando los datos de informe hasta completarlos y permanece bloqueado, aunque no se puedan ver los datos de informe.

También pueden existir casos en los que los datos de informe histórico del almacén de datos permanentes de z/OS no estén disponibles. Esto se produce porque el almacén de datos permanentes puede no estar disponible mientras se ejecuta el trabajo de mantenimiento.

Planificación del almacenamiento de datos históricos

Los mismos problemas que se aplican al solicitar conjuntos de filas grandes para informes históricos se aplican al planificar el almacenamiento de datos históricos sólo una vez al día. Cuantos más datos se recopilen y se almacenen, más recursos

se necesitan para leer los datos en la memoria y para transmitirlos al almacén de datos. Si es posible, reduzca el tamaño del conjunto de filas de almacenamiento repartiendo la carga de almacenamiento por horas, es decir, estableciendo el intervalo de almacenaje a uno por hora, en lugar de uno al día.

Utilización de una despensa de datos para mejorar consultas largas o complejas

En esta sección describe cómo se puede utilizar una despensa de datos para aumentar el rendimiento del almacén de datos primario.

En la infraestructura de Tivoli Management Services, el proxy de almacén inserta con regularidad datos nuevos de los archivos históricos a corto plazo en las tablas de almacén de datos. Estos datos detallados se obtienen mediante consultas de vistas históricas para proporcionar esta información y se pueden obtener mediante consultas de una herramienta de informe externa. Los almacenes de datos activos necesitan equilibrar la actividad de lectura y grabación para maximizar el rendimiento del almacén de datos. El almacén de datos tiene una actividad de grabación periódica equilibrada con actividad de lectura frecuente para formatear y crear informes. Bajo determinadas circunstancias (especialmente al formatear informes durante mucho tiempo o al ejecutar consultas complejas), la actividad de lectura y grabación de base de datos puede queda desequilibrada y producir tiempos de espera anormales. Bajo estas circunstancias, puede mejorar de forma significativa el rendimiento añadiendo un almacén de datos secundario, denominado normalmente *despensa de datos*, para informes que producen consultas de datos largas o complejas.

En función de los requisitos de informe, hay dos mecanismos que se pueden utilizar, aprovechando las interfaces abiertas que se incluyen con el almacén:

1. Si se necesita la base de datos completa, utilice los recursos de réplica de base de datos del RDBMS de Tivoli Data Warehouse.
2. Escriba y planifique los scripts de extracción de SQL, similares a los scripts ETL de Tivoli Data Warehouse V1.x, para extraer los elementos de datos deseados a un intervalo planificado de Tivoli Data Warehouse y llenar de datos una base de datos de informe. Esta base de datos de informe se puede optimizar para que la utilice una herramienta de informe externa, igual que se utilizaban las despensas de datos en Tivoli Data Warehouse V1.x. Estos scripts pueden ser scripts SQL, scripts shell o scripts PERL.

Script SQL de despensa de datos de ejemplo para IBM Tivoli Monitoring

El siguiente script SQL es un script de ejemplo de cómo puede crear y llenar una despensa de datos. El script real necesita revisarse para reflejar el entorno.

```
-------------------------------------------------------
-- Script SQL de despensa de datos de ejemplo para TDW 2.1
-------------------------------------------------------
-- Estos scripts muestran la creación y el llenado
-- de una despensa de datos (similares a las despensas de datos de TDW 1.x)
-- empezando en las tablas "planas" de TDW 2.1.
-- Este script se puede ejecutar utilizando CLP de DB2 UDB:
-- db2 -tvf myscript
-------------------------------------------------------
-- 1. Crear la tabla "plana" cada hora desde TDW 2.1 (simulado)
-- Una fila por hora por sistema Windows
drop table itmuser."Win_System_H";
create table itmuser."Win_System_H" (
 WRITETIME                      CHAR( 16 ),
 "Server_Name"                  CHAR( 64 ),
```

```
 "Operating_System_Type"        CHAR( 16 ),
 "Network_Address"              CHAR( 16 ),
 "MIN_%_Total_Privileged_Time"  INTEGER,
 "MAX_%_Total_Privileged_Time"  INTEGER,
 "AVG_%_Total_Privileged_Time"  INTEGER,
 "MIN_%_Total_Processor_Time"   INTEGER,
 "MAX_%_Total_User_Time"        INTEGER,
 "AVG_%_Total_User_Time"        INTEGER );

-- 2. Insertar datos de ejemplo

insert into itmuser."Win_System_H" values (
'1050917030000000', 'Primary:WinServ1:NT', 'Windows_2000', '8.53.24.170',
20, 40, 30, 10, 30, 20 );

insert into itmuser."Win_System_H" values (
'1050917040000000','Primary:WinServ1:NT','Windows_2000','8.53.24.170',
20, 40, 30, 10, 30, 20 );

insert into itmuser."Win_System_H" values (
'1050917030000000','Primary:WinServ2:NT','Windows_2000','8.53.24.171',
20, 40, 30, 10, 30, 20 );

insert into itmuser."Win_System_H" values (
'1050917040000000','Primary:WinServ2:NT','Windows_2000','8.53.24.171',
  20, 40, 30, 10, 30, 20 );

-- 3. Crear una tabla de dimensiones para los hosts
-- la clave primaria es Server_ID, un valor generado
-- la clave alternativa es Server_Name, Network_Address

drop table itmuser."D_Win_System";
create table itmuser."D_Win_System" (
 "Server_ID" INTEGER GENERATED ALWAYS AS IDENTITY
    PRIMARY KEY NOT NULL,
 "Server_Name"                  CHAR( 64 ),
 "Operating_System_Type"        CHAR( 16 ),
 "Network_Address"              CHAR( 16 ) );

-- 4. Crear una tabla de hechos cada hora para los hechos del sistema
-- Server_ID es una clave foránea en D_Win_System

drop table itmuser."F_Win_System_H";
create table itmuser."F_Win_System_H" (
 WRITETIME                      CHAR( 16 ) NOT NULL,
 "Server_ID"                    INTEGER NOT NULL,
 "MIN_%_Total_Privileged_Time"  INTEGER,
 "MAX_%_Total_Privileged_Time"  INTEGER,
 "AVG_%_Total_Privileged_Time"  INTEGER,
 "MIN_%_Total_Processor_Time"   INTEGER,
 "MAX_%_Total_User_Time"        INTEGER,
 "AVG_%_Total_User_Time"        INTEGER,
 constraint SERVID foreign key ("Server_ID")
  references itmuser."D_Win_System" ("Server_ID")
);

-- 5. Insertar en la tabla de dimensiones
-- insertar sólo las filas que aún no existen

insert into itmuser."D_Win_System" (
 "Server_Name",
 "Operating_System_Type",
 "Network_Address" )
select
 "Server_Name",
 min("Operating_System_Type") as "Operating_System_Type",
 "Network_Address"
```

```
from
  itmuser."Win_System_H" h
where
 not exists ( select 1 from
 itmuser."D_Win_System" d
 where d."Server_Name" = h."Server_Name"
 and d."Network_Address" = h."Network_Address"
 )
group by
 "Server_Name",
 "Network_Address"
;

-- 6. Comprobar valores en tabla de dimensiones
select * from itmuser."D_Win_System"
;

-- 7. Insertar en la tabla de hechos
-- insertar sólo las filas que aún no existen
insert into itmuser."F_Win_System_H"
select
 h.WRITETIME   ,
 d."Server_ID" ,
 h."MIN_%_Total_Privileged_Time" ,
 h."MAX_%_Total_Privileged_Time" ,
 h."AVG_%_Total_Privileged_Time" ,
 h."MIN_%_Total_Processor_Time"  ,
 h."MAX_%_Total_User_Time"       ,
 h."AVG_%_Total_User_Time"
from
 itmuser."Win_System_H" h,
 itmuser."D_Win_System" d
where d."Server_Name" = h."Server_Name"
 and d."Network_Address" = h."Network_Address"
 and not exists ( select 1 from
 itmuser."F_Win_System_H" f
  where f.WRITETIME = h.WRITETIME
  and f."Server_ID" = d."Server_ID"
  )
;

-- 8. Comprobar valores de la tabla de hechos
select * from itmuser."F_Win_System_H"
;

-- 9. Repetir "5. Insertar en la tabla de dimensiones"
-- y "7. Insertar en la tabla de hechos" a diario
```

Consulte la publicación IBM Redbooks®, *Introduction to Tivoli Enterprise Data Warehouse* en http://www.redbooks.ibm.com/ para obtener referencias y scripts de extracción de SQL de ejemplo adicionales.

Configuración de historial a corto plazo de Tivoli Data Warehouse

En este apartado se describen algunas de las configuraciones de historial a corto plazo en relación a la base de datos de Tivoli Data Warehouse.

Denominación de las tablas y columnas históricas de Tivoli Data Warehouse

Las tablas históricas de la base de datos de Tivoli Data Warehouse tienen los mismos nombres que los grupos de tablas y columnas históricas. Por ejemplo, el historial de Windows NT para el nombre de grupo NT_System se recopila en un

archivo a corto plazo que tiene el nombre WTSYSTEM. Los datos históricos de este archivo, WTSYSTEM, se almacenan en la base de datos de una tabla denominada NT_System.

El proxy de almacén utiliza el nombre de atributo de producto completo para crear identificadores de tabla y columna DBMS. Esto incluye los caracteres especiales que se encuentran en un nombre de atributo. Cuando la longitud de un nombre de atributo excede la longitud de nombre de tabla o columna máxima soportada por un producto DBMS, el proxy de almacén utiliza los nombres de tabla y columna internos definidos en el archivo de atributos de producto.

La tabla WAREHOUSEID se encuentra en la base de datos de Tivoli Data Warehouse. Contiene registros que describe los nombres de atributo o de tabla que exceden la longitud de nombre máxima de DBMS y que se han convertido a nombres de tabla o columna internos. Puede consultar esta tabla para averiguar el nombre correcto de una tabla o una columna que se ha convertido internamente. Cada nombre de grupo de atributos de esta tabla tiene un valor RECTYPE de "TAB". Sólo los valores de TABLENAME y OBJECTNAME se han rellenado. Cada nombre de columna de atributo tiene un valor RECTYPE de "COL". Todos los demás valores de columna de WAREHOUSEID se han rellenado. La tabla WAREHOUSE ID tiene estas definiciones:

RECTYPE CHAR(3)
Indica el tipo de registro: "TAB" para tabla; "COL" para columna.

TABLENAME CHAR(20)
Indica un nombre de tabla interno.

OBJECTNAME CHAR(140)
Indica un nombre de grupo de atributos.

COLUMNNAME CHAR(20)
Indica un nombre de columna interno.

ATTRNAME CHAR(140)
Indica un nombre de atributo.

El proxy de almacén crea automáticamente un índice asociado para cada tabla de datos de la base de datos de almacén. El índice se basa en las columnas WRITETIME y ORIGINNODE (cuyo nombre de visualización puede ser “Nombre_Servidor,” “Nombre_Sistema," etc., en función de la tabla) y TMZDIFF (diferencia de huso horario). El nombre de índice es el nombre abreviado de la tabla, con un sufijo “_IDX”.

Utilización de comillas dobles para asegurar el acceso correcto a todos los datos

Todos los nombres de tabla y columna del almacén de datos para todos los productos DBMS principales se crean escribiéndolos entre los caracteres de identificador de comillas soportado por DBMS. Al hacer referencia a datos históricos de la base de datos de almacén, debe utilizar el carácter de comillas dobles para asegurar el acceso correcto a dichos datos. Algunos productos de base de datos, por ejemplo Microsoft SQL Server, no necesitan utilizar comillas dobles.

Si ha creado consultas SQL o procedimientos almacenados antes de tener IBM Tivoli Monitoring V6.2.1 para utilizarlos con la versión anterior del programa de recopilación de datos históricos, es posible que ahora sea necesario modificarlos. El SQL necesita tener en cuenta el hecho de que algunos productos de base de datos

relacional (por ejemplo Oracle) necesitan que todos los nombres de tabla y columna se escriban entre comillas dobles para acceder a los datos históricos de IBM, porque es posible que algunos agentes hayan cambiado las caracterizaciones de datos o hayan añadido columnas nuevas.

Directorio ATTRLIB de proxy de almacén

El directorio ATTRLIB del proxy de almacén se crea automáticamente en el momento de instalación del producto. En un sistema Windows, este directorio está ubicado en *dir_ITM*\tmaitm6\attrlib. En un sistema operativo como UNIX, este directorio está ubicado en *dir_ITM*/hd/tables.

Durante la instalación, si se instala el proxy de almacén en el mismo sistema donde están instalados otros agentes, los archivos de atributos de producto de agente que son accesibles para el programa de instalación se añaden al directorio ATTRLIB. El proxy de almacén sólo utiliza el archivo de atributos en una condición específica: cuando la versión de agente de supervisión es anterior a la versión 6.1.0.

El archivo de atributos permite determinar el nombre interno de tabla o columna cuando la longitud de un nombre de atributo excede la longitud de nombre de tabla o columna máxima que un producto DBMS de almacén soporta. Sólo en esa condición, el archivo de atributos debe estar en el directorio ATTRLIB. Si el proxy de almacén se instala en un sistema independiente y tiene un agente de supervisión que no está en el último nivel, debe copiar el archivo de atributos de dicho agente en el directorio ATTRLIB donde está instalado el proxy de almacén.

Si ve un mensaje de error que indica que ha fallado una exportación porque faltaba un archivo de atributos de producto determinado en este directorio, localice el archivo de atributos de producto que falta y cópielo en el directorio ATTRLIB.

Cambios en el conjunto de atributos recopilados

Cuando se detectan cambios en el conjunto de atributos recopilados, por ejemplo cuando se despliega una nueva versión de un agente con atributos añadidos, el programa histórico realiza estas funciones:

- Si se ha especificado el almacén en la solicitud de recopilación de datos históricos actual, se exportan al almacén de datos todos los datos históricos recopilados para la tabla. Si la operación de almacenaje es satisfactoria, se suprimen todos los datos históricos a corto plazo y los archivos de metadatos.

  Si la operación falla (por ejemplo, si el proxy de almacén no está disponible), los archivos de datos y metadatos históricos a corto plazo se renombran. En el entorno de sistema operativo z/OS, si se utiliza una tabla genérica para almacenar los datos, se suprimen los datos históricos a corto plazo para una tabla independientemente de si la operación de almacenaje se ha realizado satisfactoriamente o no.

  – Entornos de sistema operativo Windows y UNIX

    En estos entornos de sistema operativo, los archivos de datos y de metadatos históricos se renombran con los sufijos **.prv** y **.prvhdr** respectivamente.

  – Entorno de sistema operativo IBM i

    En este entorno de sistema operativo, los archivos de datos y metadatos históricos se renombran con los sufijos **P** y **Q** respectivamente.

Si los archivos redenominados ya existen, se suprimen antes de la operación de redenominación (es decir, sólo se conserva una generación de archivos de historial a corto plazo cambiados).

- Si NO se especifica el almacén en la solicitud de recopilación de datos históricos actual, el archivo de datos y metadatos históricos se renombra como se ha descrito más arriba. En z/OS, si se utiliza una tabla genérica para almacenar los datos, se suprimen todos los datos históricos a corto plazo para una tabla junto con el metaregistro.

Migraciones de particiones por rangos de Tivoli Data Warehouse

El particionamiento por rangos es una característica de organización de datos de base de datos que puede mejorar considerablemente el rendimiento de consulta y poda en bases de datos grandes de Tivoli Data Warehouse. Puede migrar las tablas existentes a tablas particionadas para beneficiarse de las mejoras de rendimiento proporcionadas con tablas particionadas.

Para utilizar tablas particionadas, Summarization and Pruning agent y Warehouse Proxy agent deben estar configurados con el particionamiento habilitado y Tivoli Data Warehouse debe permitir el particionamiento.

La migración y la limpieza necesaria se gestionan mediante los scripts generados por la herramienta de publicación de esquemas en modalidad de migración. Los scripts proporcionan las funciones siguientes:

tdw_migrate_setup.sql
Este script crea un procedimiento almacenado para volver a definir la tabla de origen en una tabla particionada nueva y crea las tablas de control necesarias para la migración, como la tabla WAREHOUSE_MIGRATION_STATUS.

tdw_migrate_step1.sql
Este script invoca al procedimiento almacenado creado en el script de configuración. El procedimiento almacenado cambia el nombre de la tabla de origen a MIGRATING_<*nombre abreviado tabla*>, crea la tabla particionada nueva, carga los datos de la tabla de origen a la tabla nueva y, a continuación, cambia el nombre de la tabla de origen a DONE_<*nombre abreviado tabla*>.

tdw_migrate_step2.sql
Este script vuelve a crear los índices en las nuevas tablas particionadas, suprime las tablas de origen y otorga SELECT a PUBLIC en las tablas.

También puede migrar tablas particionadas utilizando un esquema de particionamiento distinto del esquema de particionamiento Tivoli Data Warehouse. Sólo una tabla particionada con el esquema de Tivoli Data Warehouse puede ser gestionada por Summarization and Pruning agent. Si desea continuar utilizando el esquema de particionamiento definido por el usuario, utilice la variable `KSY_TABLE_FILTER` para listar sólo las tablas que desea que se migren.

Las particiones de una tabla migrada se definen en función del periodo de retención de la tabla y el parámetro de reenvío de particiones. El *parámetro de reenvío de particiones* es un parámetro de configuración definido en el archivo de configuración de Resumen y poda utilizando la variable KSY_PARTITIONS_UPWARD. El *periodo de retención* es el parámetro de poda definido en el grupo de atributos que selecciona mediante el diálogo Configuración de historial en Tivoli Enterprise Portal o mediante la línea de mandatos.

Para obtener más información sobre el particionamiento por rangos, consulte "Tivoli Data Warehouse range partitioning" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Las tablas de estado WAREHOUSELOG y WAREHOUSEAGGREGLOG, también pueden migrarse. Estas tablas pueden filtrarse especificándolas en la variable `KSY_TABLE_FILTER` o por código de producto `KHD` para WAREHOUSELOG y `KSY` para el WAREHOUSEAGGREGLOG en la variable `KSY_PRODUCT_FILTER`. Estas tablas se tratan como tablas detalladas si se utiliza `KSY_SUMMARIZATION_FILTER`.

Requisitos previos y métodos recomendados

Antes de empezar, asegúrese de que se cumplen los criterios siguientes:

- Asegúrese de tener suficiente espacio de disco, dado que durante la migración habrá dos copias de los mismos datos hasta que se suprima la tabla de origen. Debe al menos duplicar el espacio de disco de las tablas que se están migrando.
- Defina la poda para todas las tablas que se están migrando *antes de* la migración, de forma que los datos se puedan podar correctamente después de particionadas las tablas.
- Detenga a Summarization and Pruning agent y Warehouse Proxy agent durante el periodo de migración. Además, detenga los informes o usuarios externos de las tablas que se están migrando.
- Asegúrese de que el soporte de aplicaciones de Tivoli Enterprise Portal Server esté actualizado. El servidor de portal y el soporte de aplicación de agente deben coincidir.

El método recomendado es migrar las tablas por lotes. Este método reduce la cantidad de espacio de disco necesaria para la migración y el periodo de tiempo que el Summarization and Pruning agent y el Warehouse Proxy agent deben estar fuera de línea. Se puede migrar un lote de tablas en una ventana de mantenimiento.

Migración de tablas no particionadas a tablas particionadas para DB2 en Linux, UNIX y Windows

Utilice los pasos siguientes para migrar tablas no particionadas si utiliza DB2 en Linux, UNIX o Windows.

Antes de empezar

Revise los "Requisitos previos y métodos recomendados". Debe asegurarse de tener suficiente espacio de disco.

El usuario de Tivoli Data Warehouse debe tener los privilegios siguientes:

- CREATE TABLE
- LOAD
  La migración de DB2 utiliza el programa de utilidad de carga para copiar datos. Para otorgar autorización de carga, inicie sesión en DB2 como un usuario con autorización SYSADM o DBA y emita el mandato de SQL `db2 grant load on database to user <Tivoli Data Warehouse > ID de usuario`.
- Privilegios de ejecución para el procedimiento ADMIN_CMD
  Para otorgar la autorización, inicie sesión en DB2 como un usuario con

autorización SYSADM o DBA y emita el mandato de SQL `db2 grant execute on procedure sysproc.admin_cmd to user <Tivoli Data Warehouse ID de usuario>`.

Los privilegios necesarios para la migración se pueden revocar una vez que se han completado las migraciones que desea.

Acerca de esta tarea

La migración de tablas no particionadas a tablas particionadas en una base de datos de Tivoli Data Warehouse DB2 en Linux, UNIX y Windows utiliza un procedimiento almacenado generado por la herramienta de publicación de esquemas. El procedimiento almacenado utiliza el programa de utilidad LOAD de DB2.

Procedimiento

1. Configure el Summarization and Pruning agent para tablas de partición. Para ver los pasos detallados, consulte "Especificación de tablas particionadas por rangos para el agente de resumen y poda" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.
2. Detenga todas las instancias de Warehouse Proxy agent y Summarization and Pruning agent.
3. Realice una copia de seguridad de la base de datos de Tivoli Data Warehouse.
4. Edite el archivo de respuestas de la herramienta de publicación de esquemas.
   a. Abra el archivo de respuestas:

      Windows *install_dir*\TMAITM6\tdwschema.rsp

      Linux UNIX *install_dir*/*arch*/bin/tdwschema.rsp

   b. Configure las siguientes variables:

      `KSY_PRODUCT_SELECT = migrate`

      `KSY_PRODUCT_FILTER = list of products to migrate`
      Un filtro opcional para indicar que solamente se incluyen ciertos productos específicos. (Si no especifica ningún filtro, todos los productos de la categoría especificada se incluirán de forma predeterminada). Especifique los códigos de producto de tres letras de los productos que desee incluir, separados por comas. Puede encontrar estos códigos utilizando el mandato **tacmd histListProduct** (para obtener más información, consulte *IBM Tivoli Monitoring: Consulta de mandatos*).

      `KSY_TABLE_FILTER = list of tables to migrate`
      Un filtro opcional para indicar sólo tablas específicas. Este filtro se puede utilizar junto con la variable `KSY_PRODUCT_FILTER`. Utilice el siguiente mandato para obtener la lista de tablas que están disponibles para un producto determinado. Sustituya cada espacio en el nombre de grupo de atributos con un carácter de subrayado. Para obtener una lista de nombres de tabla, utilice el siguiente mandato:
      tacmd histListAttributeGroups -t <productcode>

      `KSY_SUMMARIZATION_SELECTION = list of aggregation periods to migrate`
      Un filtro opcional que puede utilizarse además de las variables `KSY_PRODUCT_FILTER` y `KSY_TABLE_FILTER`. Esta variable tiene una opción adicional cuando se utiliza la modalidad de migración. La opción **R** le permite migrar las tablas detalladas. Otras opciones son las siguientes:

      R: Migrar sólo tablas detalladas

      H: Por hora

      D: A diario

W: Semanalmente

M: Mensualmente

Q: Trimestralmente

Y: Anualmente

Los filtros pueden combinarse. Por ejemplo, para migrar las tablas detalladas, por hora y diariamente para el agente de SO Windows:

```
KSY_PRODUCT=KNT
KSY_SUMMARIZATION_SELECTION=R,H,D
```

`KSY_SQL_OUTPUT_FILE_PATH = optional file path for SQL output`
Una vía de acceso opcional al directorio en el que se deben grabar los archivos SQL generados. Si no incluye esta palabra clave, se utilizará el directorio de trabajo actual.

Para obtener más detalles y la sintaxis completa para cada variable, consulte los comentarios en el archivo de respuestas.

5. Asegúrese de que se haya iniciado el Tivoli Enterprise Portal Server.
6. Debe exportar la variable CANDLEHOME, si aún no lo ha hecho. Ejecute los siguientes mandatos:

   Windows

   ```
   set CANDLE_HOME=install_dir
   ```

   Linux UNIX

   ```
   CANDLEHOME=/install_dir
   export CANDLEHOME
   ```

7. Ejecute el script de herramienta de publicación de esquemas para generar los scripts necesarios para la migración.

   Windows `tdwschema -rspfile tdwschema.rsp`

   Linux UNIX `tdwschema.sh -rspfile tdwschema.rsp` Los siguientes scripts se generan para la migración: tdw_migrate_setup.sql, tdw_migrate_step1.sql, y tdw_migrate_step2.sql.
8. Ejecute el script tdw_migrate_setup.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

   ```
   db2 -td# -f tdw_migrate_setup.sql
   ```

   Utilice el script tdw_migrate_setup.sql sólo una vez, incluso al migrar por lotes. Si se ejecuta este script más de una vez la capacidad del proceso de migración de reiniciarse si se produce un error deja de estar disponible.Este script contiene sentencias drop que pueden fallar si los objetos no existen. No tenga en cuenta estas anomalías como errores, pueden pasarse por alto. Las anomalías esperadas pueden devolver los mensajes siguientes: DB21034E y SQL0204N.
9. Ejecute el script tdw_migrate_step1.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

   ```
   db2 -tf tdw_migrate_step1.sql
   ```

   Si se producen errores después de ejecutar este script, los errores deben resolverse antes de ejecutar el script tdw_migrate_step2.sql. Continúe volviendo a ejecutar este script hasta que se resuelvan todos los errores.

   Se aplican los siguientes códigos de retorno:

   - `-2`: La tabla ya está particionada
   - `-1`: Se ha pasado un parámetro no válido
   - `0`: No se han producido errores
   - `1`: Ha fallado el cambio de nombre de la tabla no particionada a MIGRATING_*

- 2: Ha fallado la creación de la tabla particionada
- 3: Ha fallado la carga de datos en la tabla particionada
- 4: Ha fallado el cambio de nombre de la tabla de origen a DONE_*

10. Ejecute el script tdw_migrate_step2.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

    ```
    db2 -tf tdw_migrate_step2.sql
    ```

    Puede ejecutar este script varias veces para resolver los errores. Este script no tiene ningún efecto en las tablas que no se migraron satisfactoriamente.

    Nota: Si está migrando por lotes, se ejecutan los scripts tdw_migrate_step1.sql y tdw_migrate_step2.sql para cada lote.
11. Realice una copia de seguridad de la base de datos. Debe completar este paso dado que se ha utilizado el programa de utilidad de carga en modo no recuperable para mejorar el rendimiento de la migración. Las tablas migradas no se pueden restaurar a partir de una copia de seguridad hasta que se realiza una nueva copia de seguridad.

Resultados

Las tablas que ha especificado ahora están particionadas, y las tablas de origen se han suprimido.

Qué hacer a continuación

Si se han producido errores durante la migración, revise la tabla WAREHOUSE_MIGRATION_STATUS. Para obtener información detallada, consulte *IBM Tivoli Monitoring: Guía de resolución de problemas*.

Migración de tablas no particionadas a tablas particionadas para DB2 en z/OS

Utilice los pasos siguientes para migrar tablas no particionadas si está utilizando DB2 en z/OS.

Antes de empezar

Revise los "Requisitos previos y métodos recomendados" en la página 497. Debe asegurarse de tener suficiente espacio de disco.

Debe tener DB2 en z/OS V9 o posterior para utilizar este procedimiento.

La herramienta de publicación de esquemas sólo puede ejecutarse en una plataforma distribuida, como por ejemplo UNIX o Windows. Los scripts generados deben ejecutarse desde una plataforma distribuida con un cliente de DB2 conectado a la base de datos DB2 z/OS remota.

Los scripts de migración generados deben ejecutarse desde un cliente de DB2.

El usuario de Tivoli Data Warehouse debe tener uno o varios de los privilegios siguientes para poder ejecutar el script tdw_migrate_setup.sql:

- La propiedad y el privilegio EXECUTE para los paquetes, DSNADMJS y DSNADMJF, utilizados en el script de configuración
- Autoridad SYSADM
- Autorización PACKADM para la colección de paquetes

- Autoridad de daemon
  Si el BPX.DAEMON está activo, los procedimientos almacenados cargados en un espacio de direcciones deben estar definidos en el control de programa RACF. De lo contrario, se devuelve el siguiente error: EDC5139I No se permite la operación. Para obtener información detallada sobre este tema, consulte APAR II13698 en el portal de soporte de IBM.

Los privilegios necesarios para la migración se pueden revocar una vez que se han completado las migraciones que desea.

Debe definir los procedimientos almacenados en DB2 utilizando el trabajo de instalación de ejemplo DSNTIJSG. A continuación, asegúrese de que todos los procedimientos almacenados están definidos en el control de programa de RACF. Además, debe definir el entorno de aplicación necesario en WLM para ejecutar estos procedimientos almacenados, y también especificar un valor WLMENV. Para obtener más información sobre cómo definir los procedimientos almacenados en DB2, consulte la publicación *DB2 for z/OS Installation and Migration Guide* y *DB2 for z/OS Administration Guide* para DB2 9 o posterior, en Centro de información de DB2 for z/OS.

Acerca de esta tarea

La migración de tablas no particionadas a tablas particionadas en una base de datos de Tivoli Data Warehouse DB2 on z/OS utiliza un procedimiento almacenado generado por la herramienta de publicación de esquemas. El procedimiento almacenado utiliza un trabajo JCL que utiliza el programa de utilidad LOAD de DB2. Se crea un trabajo JCL y se somete para cada tabla que se está migrando.

Procedimiento

1. Configure el Summarization and Pruning agent para tablas de partición. Para ver los pasos detallados, consulte “Especificación de tablas particionadas por rangos para el agente de resumen y poda” en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.
2. Detenga todas las instancias de Warehouse Proxy agent y Summarization and Pruning agent.
3. Realice una copia de seguridad de la base de datos de Tivoli Data Warehouse.
4. Catalogue la base de datos de z/OS utilizando los mandatos siguientes:
   ```
   db2 catalog tcpip node <node_Name> remote <DB_server_hostname>
     server <port_number> ostype OS390
   db2 catalog dcs database <db_name> as <db_name>
   db2 catalog db <database_name_on_server> as <alias_on_client_database_name>
     at node <node_Name> authentication dcs
   ```
5. Edite el archivo de respuestas de la herramienta de publicación de esquemas.
   a. Abra el archivo de respuestas:

      Windows *install_dir*\TMAITM6\tdwschema.rsp

      Linux UNIX *install_dir/arch*/bin/tdwschema.rsp

   b. Configure las siguientes variables:

      KSY_PRODUCT_SELECT = migrate

      KSY_PRODUCT_FILTER = *list of products to migrate*
      Un filtro opcional para indicar que solamente se incluyen ciertos productos específicos. (Si no especifica ningún filtro, todos los productos de la categoría especificada se incluirán de forma predeterminada). Especifique los códigos de producto de tres letras de los productos que desee incluir,

separados por comas. Puede encontrar estos códigos utilizando el mandato **tacmd histListProduct** (para obtener más información, consulte *IBM Tivoli Monitoring: Consulta de mandatos*).

`KSY_TABLE_FILTER = list of tables to migrate`
Un filtro opcional para indicar sólo tablas específicas. Este filtro se puede utilizar junto con la variable `KSY_PRODUCT_FILTER`. Utilice el siguiente mandato para obtener la lista de tablas que están disponibles para un producto determinado. Sustituya cada espacio en el nombre de grupo de atributos con un carácter de subrayado. Para obtener una lista de nombres de tabla, utilice el siguiente mandato:
tacmd histListAttributeGroups -t <productcode>

`KSY_SUMMARIZATION_SELECTION = list of aggregation periods to migrate`
Un filtro opcional que puede utilizarse además de las variables `KSY_PRODUCT_FILTER` y `KSY_TABLE_FILTER`. Esta variable tiene una opción adicional cuando se utiliza la modalidad de migración. La opción **R** le permite migrar las tablas detalladas. Otras opciones son las siguientes:

R: Migrar sólo tablas detalladas

H: Por hora

D: A diario

W: Semanalmente

M: Mensualmente

Q: Trimestralmente

Y: Anualmente

Los filtros pueden combinarse. Por ejemplo, para migrar las tablas detalladas, por hora y diariamente para el agente de SO Windows:

```
KSY_PRODUCT=KNT
KSY_SUMMARIZATION_SELECTION=R,H,D
```

`KSY_SQL_OUTPUT_FILE_PATH = optional file path for SQL output`
Una vía de acceso opcional al directorio en el que se deben grabar los archivos SQL generados. Si no incluye esta palabra clave, se utilizará el directorio de trabajo actual.

Para obtener más detalles y la sintaxis completa para cada variable, consulte los comentarios en el archivo de respuestas.

6. Debe exportar la variable CANDLEHOME, si aún no lo ha hecho. Ejecute los siguientes mandatos:

   Windows

   ```
   set CANDLE_HOME=install_dir
   ```

   Linux UNIX

   ```
   CANDLEHOME=/install_dir
   export CANDLEHOME
   ```

7. Asegúrese de que se haya iniciado el Tivoli Enterprise Portal Server.
8. Ejecute el script de herramienta de publicación de esquemas para generar los scripts necesarios para la migración.

   Windows `tdwschema -rspfile tdwschema.rsp`

   Linux UNIX `tdwschema.sh -rspfile tdwschema.rsp` Los siguientes scripts se generan para la migración: tdw_migrate_setup.sql, tdw_migrate_step1.sql, y tdw_migrate_step2.sql.
9. Ejecute el script tdw_migrate_setup.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

   ```
   db2 -td# -f tdw_migrate_setup.sql
   ```

Utilice el script tdw_migrate_setup.sql sólo una vez, incluso al migrar por lotes. Si se ejecuta este script más de una vez la capacidad del proceso de migración de reiniciarse si se produce un error deja de estar disponible.Este script contiene sentencias drop que pueden fallar si los objetos no existen. No tenga en cuenta estas anomalías como errores, pueden pasarse por alto. Las anomalías esperadas pueden devolver los mensajes siguientes: DB21034E y SQL0204N.

10. En el script tdw_migrate_step1.sql, actualice la sentencia INSERT INTO WAREHOUSE_MIGRATION_CONFIG con la información siguiente:
    - Especifique el ID de usuario y la contraseña necesaria para ejecutar el procedimiento de migración almacenado. Puede especificar NULL para el ID de usuario y contraseña en las circunstancias siguientes:
      – El sistema operativo es z/OS Versión 1 Release 13 o posterior, y el ID de autorización que está asociado con el espacio de direcciones de procedimiento almacenado tiene autorización daemon.
      – El sistema operativo es z/OS Versión 1 Release 13 o posterior, y el ID de autorización que está asociado con el espacio de direcciones de procedimiento almacenado no tiene autorización daemon, pero está autorizado para el perfil de clase BPX.SRV.*userid* SURROGAT, donde *userid* es el ID de autorización del procedimiento almacenado. En este caso, debe instalar APAR OA36062. Para obtener más información, consulte la publicación *DB2 for z/OS Administration Guide*.
    - Especifique la biblioteca de prefijo de JCL donde se encuentran los programas de utilidad LOAD y UNLOAD del sistema.
11. Ejecute el script tdw_migrate_step1.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

    ```
    db2 -tf tdw_migrate_step1.sql
    ```

    Si se producen errores después de ejecutar este script, los errores deben resolverse antes de ejecutar el script tdw_migrate_step2.sql. Continúe volviendo a ejecutar este script hasta que se resuelvan todos los errores.

    Se aplican los siguientes códigos de retorno:
    - `-5`: Se ha especificado un nombre de sistema no válido
    - `-4`: Se ha especificado una clase de trabajo no válida
    - `-3`: La biblioteca de prefijo es nula
    - `-2`: La tabla ya está particionada
    - `-1`: Se ha pasado un parámetro no válido
    - `0`: No se han producido errores
    - `1`: El cambio de nombre de la tabla de origen ha fallado
    - `2`: La creación de tabla particionada ha fallado
    - `3`: La creación o envío de trabajo JCL de migración ha fallado
    - `4`: El estado de trabajo JCL de consulta de migración ha fallado
    - `5`: La salida del trabajo JCL de captación de migración ha fallado
    - `7`: La carga ha fallado
    - `8`: El cambio de nombre de tabla de origen ha fallado

    El código de retorno 6 se ha dejado en blanco intencionadamente.
12. Ejecute el script tdw_migrate_step2.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

    ```
    db2 -tf tdw_migrate_step2.sql
    ```

Puede ejecutar este script varias veces para resolver los errores. Este script no tiene ningún efecto en las tablas que no se migraron satisfactoriamente.

Nota: Si está migrando por lotes, se ejecutan los scripts tdw_migrate_step1.sql y tdw_migrate_step2.sql para cada lote.

Cuando el script tdw_migrate_step2.sql se ejecuta, las filas de la tabla WAREHOUSE_MIGRATION_CONFIG, WAREHOUSE_JCLJOB_MIGRATION_STATUS y WAREHOUSE_JCLJOB_OUTPUT se suprimen.

13. Realice una copia de seguridad de la base de datos. Debe completar este paso dado que se ha utilizado el programa de utilidad de carga en modo no recuperable para mejorar el rendimiento de la migración. Las tablas migradas no se pueden restaurar a partir de una copia de seguridad hasta que se realiza una nueva copia de seguridad.

Resultados

Las tablas que ha especificado ahora están particionadas, y las tablas de origen se han suprimido.

Qué hacer a continuación

Si se han producido errores durante la migración, revise las tablas WAREHOUSE_MIGRATION_STATUS, WAREHOUSE_JCLJOB_MIGRATION_STATUS y WAREHOUSE_JCLJOB_OUTPUT. Para obtener información detallada, consulte *IBM Tivoli Monitoring: Guía de resolución de problemas*.

Migración de tablas no particionadas a tablas particionadas para Oracle

Utilice los pasos siguientes para migrar tablas no particionadas si está utilizando Oracle.

Antes de empezar

Revise los "Requisitos previos y métodos recomendados" en la página 497. Debe asegurarse de tener suficiente espacio de disco.

Se debe otorgar directamente al usuario de Tivoli Data Warehouse los siguientes privilegios del sistema, no se pueden otorgar mediante un rol:

- ALTER ANY TABLE
- CREATE ANY TABLE
- DROP ANY TABLE
- LOCK ANY TABLE
- SELECT ANY TABLE
- Privilegios de ejecución para el paquete DBMS_REDEFINITION
  Para otorgar autorización, utilice el mandato `grant execute on DBMS_REDEFINITION TO <ID de usuario de Tivoli Data Warehouse>`.

Los privilegios necesarios para la migración se pueden revocar una vez que se han completado las migraciones que desea.

Acerca de esta tarea

La migración de tablas no particionadas a tablas particionadas en una base de datos de Tivoli Data Warehouse Oracle utiliza un procedimiento almacenado generado por la herramienta de publicación de esquemas. El procedimiento almacenado utiliza el paquete DBMS_REDEFINITION para cargar datos de la tabla no particionada en las tablas particionadas.

Procedimiento

1. Configure el Summarization and Pruning agent para tablas de partición. Para ver los pasos detallados, consulte "Especificación de tablas particionadas por rangos para el agente de resumen y poda" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.
2. Detenga todas las instancias de Warehouse Proxy agent y Summarization and Pruning agent.
3. Realice una copia de seguridad de la base de datos de Tivoli Data Warehouse.
4. Edite el archivo de respuestas de la herramienta de publicación de esquemas.
   a. Abra el archivo de respuestas:

      Windows *install_dir*\TMAITM6\tdwschema.rsp

      Linux UNIX *install_dir*/*arch*/bin/tdwschema.rsp

   b. Configure las siguientes variables:

      KSY_PRODUCT_SELECT = migrate

      KSY_PRODUCT_FILTER = *list of products to migrate*
      Un filtro opcional para indicar que solamente se incluyen ciertos productos específicos. (Si no especifica ningún filtro, todos los productos de la categoría especificada se incluirán de forma predeterminada). Especifique los códigos de producto de tres letras de los productos que desee incluir, separados por comas. Puede encontrar estos códigos utilizando el mandato **tacmd histListProduct** (para obtener más información, consulte *IBM Tivoli Monitoring: Consulta de mandatos*).

      KSY_TABLE_FILTER = *list of tables to migrate*
      Un filtro opcional para indicar sólo tablas específicas. Este filtro se puede utilizar junto con la variable KSY_PRODUCT_FILTER. Utilice el siguiente mandato para obtener la lista de tablas que están disponibles para un producto determinado. Sustituya cada espacio en el nombre de grupo de atributos con un carácter de subrayado. Para obtener una lista de nombres de tabla, utilice el siguiente mandato:
      tacmd histListAttributeGroups -t <productcode>

      KSY_SUMMARIZATION_SELECTION = *list of aggregation periods to migrate*
      Un filtro opcional que puede utilizarse además de las variables KSY_PRODUCT_FILTER y KSY_TABLE_FILTER. Esta variable tiene una opción adicional cuando se utiliza la modalidad de migración. La opción **R** le permite migrar las tablas detalladas. Otras opciones son las siguientes:

      R: Migrar sólo tablas detalladas

      H: Por hora

      D: A diario

      W: Semanalmente

      M: Mensualmente

      Q: Trimestralmente

      Y: Anualmente

Los filtros pueden combinarse. Por ejemplo, para migrar las tablas detalladas, por hora y diariamente para el agente de SO Windows:

```
KSY_PRODUCT=KNT
KSY_SUMMARIZATION_SELECTION=R,H,D
```

`KSY_SQL_OUTPUT_FILE_PATH = optional file path for SQL output`
Una vía de acceso opcional al directorio en el que se deben grabar los archivos SQL generados. Si no incluye esta palabra clave, se utilizará el directorio de trabajo actual.

Para obtener más detalles y la sintaxis completa para cada variable, consulte los comentarios en el archivo de respuestas.

5. Asegúrese de que se haya iniciado el Tivoli Enterprise Portal Server.
6. Debe exportar la variable CANDLEHOME, si aún no lo ha hecho. Ejecute los siguientes mandatos:

   Windows

   ```
   set CANDLE_HOME=install_dir
   ```

   Linux UNIX

   ```
   CANDLEHOME=/install_dir
   export CANDLEHOME
   ```

7. Ejecute el script de herramienta de publicación de esquemas para generar los scripts necesarios para la migración.

   Windows `tdwschema -rspfile tdwschema.rsp`

   Linux UNIX `tdwschema.sh -rspfile tdwschema.rsp` Los siguientes scripts se generan para la migración: tdw_migrate_setup.sql, tdw_migrate_step1.sql, y tdw_migrate_step2.sql.
8. Ejecute el script tdw_migrate_setup.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

   ```
   sqlplus <ID de usuario de TDW>/<contraseña>@<SID de Oracle>
   @./tdw_migrate_setup.sql
   ```

   Utilice el script tdw_migrate_setup.sql sólo una vez, incluso al migrar por lotes. Si se ejecuta este script más de una vez la capacidad del proceso de migración de reiniciarse si se produce un error deja de estar disponible.Este script contiene sentencias drop que pueden fallar si los objetos no existen. No tenga en cuenta estas anomalías como errores, pueden pasarse por alto. Las anomalías esperadas pueden devolver los mensajes siguientes: DB21034E y SQL0204N.
9. Ejecute el script tdw_migrate_step1.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

   ```
   sqlplus <ID de usuario de TDW>/<contraseña>@<SID de Oracle>
   @./tdw_migrate_step1.sql
   ```

   Si se producen errores después de ejecutar este script, los errores deben resolverse antes de ejecutar el script tdw_migrate_step2.sql. Continúe volviendo a ejecutar este script hasta que se resuelvan todos los errores.

   Si el script tdw_migrate_step1.sql es satisfactorio, se proporciona un mensaje. Por ejemplo:

   ```
   Particionando tabla "AIXTST"."KSY_TABLE_STATISTICS"

   El procedimiento PL/SQL se ha completado satisfactoriamente.

   La tabla AIXTST.KSY_TABLE_STATISTICS se ha migrado satisfactoriamente.

   El procedimiento PL/SQL se ha completado satisfactoriamente.
   ```

   Si este script encuentra un error, se proporciona un mensaje en la salida estándar. Por ejemplo:

```
Código: -20002 Mensaje: ORA-20002:
La tabla "ITMUSER630"."K4X_USGS_STREAM_FLOW" ya se ha particionado.
```

Se aplican los siguientes mensajes de error:

- 20000: Se ha pasado un parámetro no válido
- 20001: La tabla de origen no existe
- 20002: La tabla ya está particionada
- 20003: Error al determinar si la tabla de origen se puede particionar
- 20004: La creación de una tabla particionada de destino ha fallado
- 20005: No se puede descartar la tabla de destino cuando la redefinición se ha abortado o ha finalizado
- 20006: La migración ha terminado anormalmente
- 20007: Error al finalizar la redefinición de tabla
- 20008: Error durante el cambio de nombre de tabla final

10. Ejecute el script tdw_migrate_step2.sql y vea los resultados para asegurarse de que se ha ejecutado satisfactoriamente.

    ```
    sqlplus <TDW userid>/<contraseña>@<SID de Oracle>
    @./tdw_migrate_step2.sql
    ```

    Puede ejecutar este script varias veces para resolver los errores. Este script no tiene ningún efecto en las tablas que no se migraron satisfactoriamente.

    Nota: Si está migrando por lotes, se ejecutan los scripts tdw_migrate_step1.sql y tdw_migrate_step2.sql para cada lote.
11. De forma opcional, puede hacer una copia de seguridad de la base de datos.

Resultados

Las tablas que ha especificado ahora están particionadas, y las tablas de origen se han suprimido.

Qué hacer a continuación

Si se han producido errores durante la migración, revise los mensajes de error de la ejecución de los scripts.

Configuración del resumen y poda

Después de instalar Tivoli Management Services, una de las tareas de configuración inicial es configurar el agente de resumen y poda para un comportamiento general como, por ejemplo, la planificación y la frecuencia del resumen y poda. Asimismo, debe especificar el resumen y poda de los grupos de atributos para los que se están recopilando datos históricos en su aplicación supervisada.

Acerca del Summarization and Pruning agent

Este tema contiene información relevante que le ayudará a planificar y configurar el Summarization and Pruning agent.

Tivoli Enterprise Portal le permite configurar el resumen y poda para grupos de atributos seleccionados en la ventana **Configuración de la recopilación de historial** o desde la línea de mandatos mediante el mandato `tacmd histconfiguregroups` (consulte el manual *IBM Tivoli Monitoring: Consulta de mandatos*). Para obtener información sobre cómo configurar conexiones de datos

para el proxy de almacén y el agente de Summarization and Pruning agent, consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Planificación para resumir y podar los datos recopilados
El Summarization and Pruning agent no se configura e inicia durante la instalación a fin de darle la oportunidad de configurar la recopilación de historial previamente para todos los agentes de supervisión instalados, una tarea que se debe realizar antes de iniciar el Summarization and Pruning agent por primera vez.

ventana Configuración de la recopilación de historial
La ventana **Configuración de la recopilación de historial** en Tivoli Enterprise Portal tiene opciones para especificar el periodo de tiempo que se agregará y el mismo periodo de tiempo, o uno distinto, que se podará: Anualmente, Trimestralmente, Mensualmente, Semanalmente, Diariamente y Por horas.

Configurar agente de resumen y poda, ventana
Puede configurar el propio Summarization and Pruning agent mediante la ventana Manage Tivoli Enterprise Monitoring Services. Para ver la utilización de recursos o para determinar las horas punta de las cargas, puede definir un conjunto de horas como *turnos*, por ejemplo de 9 AM a 5 PM. Para especificar si un día determinado es un día laborable normal o un día festivo, puede clasificar los días que no son días laborables normales como *días festivos*. Tenga en cuenta que los turnos y días de vacaciones definidos aumentan la cantidad de datos en Tivoli Data Warehouse.

Si Tivoli Data Warehouse y todos los agentes que están recopilando datos no están en el mismo huso horario, el *Indicador de huso horario* identifica el huso horario a utilizar. Si ha elegido utilizar el huso horario de Tivoli Data Warehouse, todos los datos cambian para reflejar el huso horario de Tivoli Data Warehouse. Si elige el huso horario del agente, el día no se modifica, con el huso horario original para ese agente.

Tablas de resumen en Tivoli Data Warehouse
A continuación se proporcionan los nombres de las tablas de resumen. La *x* representa el nombre de tabla original de los datos detallados. El intervalo de resumen que se elige para el grupo de atributos determinado se añade a continuación del nombre de tabla original. Los nombres pueden ser diferentes entre la tabla de datos detallados y la tabla de datos resumidos debido a las restricciones de longitud de nombre de base de datos.

Anual x_Y

Trimestral
x_Q

Mensual
x_M

Semanal
x_W

Diario x_D

Por horas
x_H

La tabla muestra los nombres de las columnas de resumen en las tablas detalladas y lo que significan. La *x* representa el nombre de columna original. Los valores de fórmula los establecen los agentes y pueden ser

diferentes para diferentes grupos de atributos. Los nombres de atributo pueden ser diferentes entre la tabla de datos detallados y la tabla resumida debido a las restricciones de longitud de nombre de base de datos.

Tabla 63. Funciones de resumen

Nombre	**Fórmula**
Promedio	AVG_x
Delta alto	HI_x
Delta bajo	LOW_x
Delta total	TOT_x
Más reciente (basado en la hora a la que se han recopilado los datos históricos en el agente de supervisión)	LAT_x
Máximo	MAX_x
Mínimo	MIN_x
Suma	SUM_x

Los nombres pueden ser diferentes entre la tabla de datos detallados y la tabla de datos resumidos debido a las restricciones de longitud de nombre de base de datos.

Métricas de resumen y poda

El ejemplo siguiente describe cómo calcula el Summarization and Pruning agent las medidas que se acumulan con el tiempo. Puede utilizar los resultados para gestionar los recursos. En este ejemplo, la medida representa los aciertos de memoria caché desde el último reinicio del servidor.

El número total de aciertos de memoria caché durante la última hora se proporciona mediante el valor **Total**. El valor **Bajo** representa el número más bajo de aciertos de memoria caché durante la hora basándose en todos los valores de datos detallados para la hora. El valor **Alto** representa el número más alto de aciertos de memoria caché durante la hora basándose en todos los valores de datos detallados para la hora.

Con estos valores de datos detallados de una hora: 9, 15, 12, 20, 22, el proceso basado en delta tiene las reglas siguientes:

- Si el valor actual es mayor que o igual al valor anterior, la salida es igual al valor anterior menos el valor actual.
- Si el valor actual es menor que el valor anterior, la salida es igual al valor actual.
- Puesto que 15 es mayor que 9, la salida es igual a 6.
- Puesto que 12 es menor que 15, la salida es igual a 12.
- Puesto que 20 es mayor que 12, la salida es igual a 8.
- Puesto que 22 es mayor que 20, la salida es igual a 2.
- El valor TOT_ es 28, que es el total de las salidas.
- El valor LOW_ es 2, que es la más baja de las salidas.
- El valor HI_ es 12, que es la más alta de las salidas.

Valores nulos de tablas y diagramas de datos resumidos y podados

Si ve un valor `nulo` como valor de una celda de tabla o punto de diagrama, significa que no se almacenó ningún dato en Tivoli Data Warehouse. Esto sucede cuando desde un agente de supervisión se proporcionan valores

que se han identificado como no válidos durante un periodo de resumen determinado. Es posible que los archivos de soporte de agente se hayan actualizado o no se pueden calcular algunos datos en las tablas resumidas (por ejemplo, no se pueden calcular valores basados en delta y contador si sólo existe un valor).

Por ejemplo, suponga que un valor no válido para un atributo determinado es -1. Si el agente indica -1 para todos los intervalos de recopilación (1, 5, 15 o 30 minutos; 1 hora; 1 día) hasta el momento en que se realiza el cálculo de resumen y poda durante un periodo de resumen proporcionado (por horas, diariamente, semanalmente, mensualmente, trimestralmente o anualmente), no hay datos en los que realizar los cálculos y se escribe un `null` para el resumen proporcionado.

Sugerencias de planificación de capacidad para la recopilación de datos históricos en Tivoli Data Warehouse

La planificación de capacidad de disco es una predicción de la cantidad de espacio de disco que se va a consumir para cada grupo de atributos cuyos datos históricos se están recopilando. El almacenamiento de disco necesario es un factor importante a tener en cuenta al definir las reglas de recopilación de datos y la estrategia para la recopilación de datos históricos.

Para obtener más información sobre el ajuste de rendimiento para la base de datos DB2, vaya a IBM Integrated Service Management Library y busque esta frase o parte de la misma: Diseño de la base de datos relacional y ajuste del rendimiento para servidores de bases de datos DB2. Para obtener información más detallada sobre la planificación de capacidad y la escala de Tivoli Data Warehouse, consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Resumen después de actualizar el soporte de agente

Después de aplicar soporte en el servidor del portal para un producto actualizado, es posible que después de establecer un intervalo de tiempo seleccionando con ☑ **Utilizar datos resumidos** seleccionado aparezca un mensaje de error de solicitud que indique que en la barra de estado de la vista falta un nombre de columna o éste es desconocido.

La solución es esperar ver los datos de resumen hasta que haya tenido lugar el siguiente procedimiento planificado de resumen y poda. Si es necesario, el resumen y poda se puede volver a planificar para que se ejecute antes. Puede encontrar más información en el manual *IBM Tivoli Monitoring: Guía de instalación y configuración* y en la guía del usuario de Tivoli Enterprise Monitoring Agent de su producto.

Prácticas recomendadas para resumen y poda

Utilice las prácticas recomendadas a la hora de determinar cómo se deben resumir y podar las muestras de datos almacenadas en Tivoli Data Warehouse.

Antes de habilitar la recopilación de datos históricos, tenga en cuenta los requisitos de datos de la empresa. Hay cuatro casos de uso común para datos históricos. Sus requisitos variarán para cada grupo de atributos, de modo que debe tener en cuenta los casos de uso cuando configure la recopilación de datos históricos: determinación y depuración de problemas, creación de informes, planificación de capacidad y alertas predictivas y supervisión adaptativa.

Para ver los métodos recomendados de ajustes de rendimiento para el agente de resumen y poda, así como los otros componentes de supervisión, consulte "Ajuste de rendimiento" en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Cada uno de estos casos de uso tiene distintos requisitos de datos históricos. En las siguientes secciones se describe cada uno de estos casos de uso y los tipos de recopilaciones de datos históricos recomendados.

Determinación y depuración de problemas
Estos tipos de medidas se utilizan para la determinación y depuración de problemas, que tiende a ser un proceso a corto plazo por naturaleza. Es posible que tenga que comparar datos de rendimiento de hace algún tiempo, pero la mayoría de las veces los expertos en el tema solo desean retroceder unos días y evaluar el rendimiento de un servidor o aplicación y compararlo con el rendimiento actual. En este caso, no hay necesidad de resumir los datos.

Creación de informes
Cuando configure la recopilación de datos históricos, debe tener en cuenta la finalidad de los informes. Algunos informes se utilizan para el análisis de tendencia a largo plazo, algunos se utilizan para mostrar como se cumplen con los acuerdos de nivel de servicio y algunos son informes a corto plazo que muestran el estado de un servidor. El principal factor a tener en cuenta para la recopilación de datos históricos es la duración de los informes. Para los informes a corto plazo, puede utilizar datos **Detallados**. Para informes a corto y medio plazo, utilice datos resumidos **Por horas**. Para informes a medio y largo plazo, utilice el resumen **Diario** o **Semanal**.

Tenga en cuenta al configurar el resumen que no es necesario configurar todos los intervalos. Por ejemplo, si desea un resumen **Semanal**, no es necesario que también configure el resumen **Diario** y **Por horas**. Cada intervalo de resumen se puede configurar de forma independiente.

Planificación de capacidad y alertas predictivas
Para la planificación de capacidad y el análisis predictivo, generalmente deberá realizar un análisis de tendencia a largo plazo. Performance Analyzer, por ejemplo, utiliza datos de resumen **Diario** para las funciones de análisis predefinidas. Por lo tanto, en la mayoría de los casos deberá configurar el resumen diario. Puede definir sus propias funciones de análisis y utilizar datos de resumen **Por horas** o **Semanal**.

Para que las funciones de análisis funcionen correctamente, asegúrese de tener el número adecuado de puntos de datos en la tabla resumida. Si no hay suficientes, el análisis estadístico no será muy preciso. Probablemente necesitará como mínimo entre 25 y 50 puntos de datos. Para conseguir 50 puntos de datos utilizando el resumen **Diario**, tiene que conservar los datos durante 50 días antes de realizar la poda. Más puntos de datos harán que las predicciones estadísticas sean más precisas, pero esto afectará al rendimiento del proceso de creación de informes y análisis estadístico. Procure no tener más de algunos ciertos de puntos de datos por recurso que se vaya a evaluar. Si utiliza el resumen **Por horas**, obtiene 336 puntos de datos cada 2 semanas.

Supervisión adaptativa (establecimiento de umbrales dinámicos)
La capacidad de alteración temporal de situación le permite analizar datos históricos para definir un umbral que se basa en características de

rendimiento pasadas. Puede definir la hora del día y turnos en los que analizar datos históricos y realizar recomendaciones sobre umbrales.

Por ejemplo, puede evaluar datos del turno principal durante 2 semanas y establecer el umbral a 1 desviación estándar con respecto a "normal". La supervisión adaptativa utiliza datos **Detallados** para evaluar y realizar recomendaciones sobre umbrales. Por lo tanto, debe mantener una duración razonable de datos **Detallados** para realizar la evaluación. La duración depende de cómo estén definidos los turnos. Si define turnos que incluyen "día de la semana", tiene que conservar los datos durante más tiempo para obtener un análisis eficiente de los datos. Si solo está examinando el "Turno principal" para todos los días de la semana, no es necesario que conserve los datos tanto tiempo.

Conserve datos detallados durante 7 ó 30 días cuando realice comparaciones de todos los días laborables. Si realiza una comparación entre lunes y lunes, tiene que conservar datos detallados más tiempo para poder establecer una tendencia. Cuando compare un día específico de la semana, debe tener al menos 60 días de datos. Antes de continuar la supervisión adaptativa, debe tener en cuenta el uso de los datos. No tiene ninguna ventana realizar una supervisión adaptativa sobre ciertos tipos de datos, como por ejemplo espacio de disco. El objetivo debe ser establecer un umbral estático sobre el % de espacio libre o la cantidad de espacio de disco disponible. Pero la supervisión de CPU es una excelente candidata a la supervisión adaptativa, puesto que puede resultar muy ventajoso saber cuándo un servidor tiene un comportamiento anómalo.

Consideraciones sobre agentes y grupos de atributos

Cada agente y cada grupo de atributos se deben tener en cuenta por separado cuando se define la recopilación de datos históricos. Muchos productos de Tivoli Monitoring han definido un conjunto de recopilaciones de datos históricos con prácticas recomendadas. No incluyen los intervalos de resumen y poda, pero constituyen un buen punto de partida para configurar la recopilación de datos históricos.

Cuando examine estas recomendaciones, tenga en cuenta si desea utilizar una supervisión adaptativa, si desea realizar una determinación de problemas a corto plazo, si desea crear informes a largo plazo o si desea planificar la capacidad y realizar un análisis predictivo. Esto debe tenerse en cuenta al configurar los intervalos de resumen y poda.

Disponibilidad de los datos de resumen y poda

La primera vez que se ejecuta la herramienta de resumen y poda, es posible que no obtenga los resultados previstos. Revise las tareas de instalación y configuración que deben llevarse a cabo antes de poder ejecutar el resumen y poda de datos de Tivoli Data Warehouse.

El procedimiento de resumen y poda depende de tener datos suficientes en el almacén de datos con los que trabajar, el modo en que se establecen los intervalos de recopilación de datos y almacén, y si se han establecido las especificaciones de resumen y poda en la ventana Configuración de la recopilación de datos históricos. Estas tareas de instalación y configuración se deben completar antes de que los datos de resumen y poda estén disponibles en el almacén:

1. Instale el agente de supervisión y luego añada soporte de aplicaciones para el mismo en el servidor de Tivoli Enterprise Monitoring y en el servidor de Tivoli Enterprise Portal.

2. Configure la recopilación de datos históricos para uno o más grupos de atributos del agente.
3. Distribuya la recopilación histórica a los sistemas gestionados para iniciar la recopilación de datos.
4. Para cada grupo de atributos en el que se está realizando la recopilación de datos históricos, configure los intervalos de resumen y poda.
5. Espere como mínimo un intervalo de almacén. Asegúrese de que los datos estén en las tablas detalladas del almacén. No es suficiente consultar los datos históricos de Tivoli Enterprise Portal porque las primeras 24 horas proceden de los archivos históricos a corto plazo y no del almacén de datos.
6. Configure el agente de resumen y poda, asegurándose de que la conexión de prueba a la base de datos funciona y que planifica cuándo deberá realizar el trabajo el agente. Puede configurar el agente con anterioridad, pero debe esperar a que se complete la ejecución planificada para poder ejecutar el resumen y poda de los datos guardados en el almacén.

Después del tiempo de ejecución planificado, tendrá los datos de resumen en el almacén.

Configuración del resumen y poda para los grupos de atributos

Configure el resumen y poda para que Tivoli Data Warehouse agregue los datos y conserve el tamaño de la base de datos en un nivel manejable.

Antes de empezar

El agente de resumen y poda se debe instalar, configurar e iniciar como se describe en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

El ID de usuario debe tener el permiso Configurar historial para abrir la ventana Configuración de la recopilación del historial. Si no tiene este permiso, no verá la opción de menú ni la herramienta para configurar la recogida de datos históricos.

Acerca de esta tarea

Aunque el resumen y poda no es obligatorio para los datos guardados en el almacén, impide que la base de datos crezca de forma exagerada y minimiza la cantidad de datos que se recuperan para Tivoli Enterprise Portal. Incluso si la recopilación de datos de un grupo de atributos no se ha configurado, puede configurar el resumen y poda. Si no se ha creado y distribuido ninguna recopilación para un grupo de atributos, no hay datos para almacenar en el almacén y el resumen y poda no se llevará a cabo.

Procedimiento

1. Si la ventana Configuración de la recopilación de historial no está abierta, pulse **Configuración de historial**.
2. Seleccione una **Aplicación supervisada** en el árbol.
3. Revise los grupos de atributos de la tabla. Si la función de resumen y poda ya se ha configurado para un grupo de atributos, los valores se mostrarán en las celdas de resumen y poda. Contraiga el árbol, arrastre los bordes o desplace la tabla hacia la derecha para ver todas las celdas.
4. Seleccione uno o más grupos de atributos para configurarlos. Puede seleccionar varios grupos con Ctrl+clic o Mayús+clic para seleccionar todos los grupos

desde el primero seleccionado hasta este último. Los valores del primer grupo seleccionado continuarán visualizándose, independientemente de los valores de cualquiera de los otros grupos seleccionados. Esto le permite ajustar los controles de configuración una sola vez y aplicar los mismos valores a todos los grupos de atributos seleccionados. Utilice el botón **Borrar todo** si desea borrar todos los campos y volver a comenzar.

5. En el área **Resumen**, seleccione el recuadro de selección para cada período de tiempo que se va a agregar: Anualmente, Trimestralmente, Mensualmente, Semanalmente, Diariamente y Por horas.
6. En el área **Poda**, seleccione el recuadro de selección para cada período de tiempo que se va a podar: Anualmente, Trimestralmente, Mensualmente, Semanalmente, Diariamente y Por horas. Si también desea conservar los muestreos de datos originales, seleccione el recuadro de selección **Datos detallados**. En los campos correspondientes, especifique el número de días, meses o años que se conservarán los datos.
7. Pulse **Aplicar** para guardar la configuración para los grupos de atributos que se han seleccionado. Las celdas de resumen y poda del grupo de atributos se actualizan para reflejar la nueva configuración.

Qué hacer a continuación

La próxima vez que se lleve a cabo el resumen y poda, el agente de resumen y poda aplicará la configuración para los datos a largo plazo almacenados en el almacén de datos. Espere a que transcurra el siguiente período de tiempo planificado para poder ver cualquier dato resumido.

Cambio de los valores de configuración globales

Utilice la ventana Configurar agente de resumen y poda para cambiar los valores de configuración de todo el sistema para el resumen, la poda o la recopilación de datos.

Acerca de esta tarea

Realice estos pasos para editar la configuración del agente de resumen y poda:

Procedimiento

1. En Manage Tivoli Enterprise Monitoring Services, pulse el botón derecho del ratón en el Summarization and Pruning agent.
2. Pulse **Reconfigurar**.
3. Pulse **Aceptar** en la ventana Agente de resumen y poda de almacén: Configuración avanzada.
4. Pulse **Aceptar** en la siguiente ventana.
5. Pulse **Sí** en la ventana Agente de resumen y poda de almacén para configurar el agente de resumen y poda.
6. Entre la información de base de datos de Tivoli Data Warehouse y de servidor de Tivoli Enterprise Portal en el separador **Orígenes**:
   a. En el campo **Controladores JDBC**, pulse **Añadir** para invocar la ventana del navegador de archivos y seleccionar el controlador JDBC. Pulse **Aceptar** para cerrar el navegador y añadir los controladores JDBC a la lista. También puede resaltar una entrada de la lista de controladores JDBC y pulsar **Suprimir** para suprimir un controlador. Esto le ofrece la posibilidad de recopilar controladores JDBC para comunicarse con la base

de datos de Tivoli Data Warehouse. Los controladores JDBC se instalan por separado y cada base de datos proporciona un conjunto de estos controladores JDBC.

Nota:

- Si la base de datos de Tivoli Data Warehouse está en un sistema operativo como UNIX, busque el directorio donde está instalado DB2 y, en el directorio de controladores jdbc, seleccione los archivos db2jcc.jar y db2jcc_license_cu.jar. Por ejemplo, *<dir_instalación_db2>*/java/db2jcc.jar y *<dir_instalación_db2>*/java/db2jcc_license_cu.jar.
- Si la base de datos de Tivoli Data Warehouse está en un MS SQL Server 2000 ó 2005, instale el controlador JDBC de MS SQL Server 2005 del sitio web de Microsoft SQL Server. Necesitará el archivo sqljbc.jar; consulte las instrucciones de instalación del sistema operativo de Microsoft para localizar el archivo.
- Si la base de datos de Tivoli Data Warehouse utiliza Oracle, utilice el archivo ojdbc14.jar. La ubicación en Windows es *%ORACLE_HOME%*\jdbc\lib; la ubicación en sistemas operativos como UNIX es *$ORACLE_HOME*/jdbc/lib.

b. En la lista desplegable, seleccione el tipo de base de datos para Tivoli Data Warehouse.

c. Si no es correcto, entre el URL, el controlador, el esquema, el ID de usuario y la contraseña de Tivoli Data Warehouse.

Importante: Durante la configuración del proxy de almacén, se crea un usuario de base de datos (denominado ITMUser de forma predeterminada). El ID de usuario que entre aquí debe coincidir con el usuario de base de datos.

d. Pulse **Probar conexión de base de datos** para asegurarse de que puede comunicarse con la base de datos de Tivoli Data Warehouse.

e. Especifique el host y puerto del Tivoli Enterprise Portal Server, si no desea utilizar los valores predeterminados. El campo **Puerto de servidor TEP** es sólo numérico.

7. Seleccione la información de planificación en el separador **Planificación**:
   - Fija – Planifique el agente para que se ejecute cada *x* días y planifique la hora (al menos 5 minutos a partir de ahora si desea ejecutarlo de inmediato). El valor predeterminado es ejecutar cada día a las 2:00 AM.
   - Flexible – Planifique el agente para que se ejecute cada *x* minutos. En el recuadro de texto que hay sobre el botón **Añadir**, puede especificar las horas a las que no se debe ejecutar el agente, con el formato HH:MM-HH:MM (reloj de 24 horas, como por ejemplo 12:00-20:00 para no ejecutar entre las 12:00 PM y las 8:00 PM) y pulse **Añadir** para añadir el rango de horas al recuadro **Excepto**.

   Si selecciona **Fija**, el agente de resumen y poda no realiza inmediatamente ninguna acción de resumen y poda cuando se *inicia*. Efectúa el resumen y poda cuando se *ejecuta*. Se ejecuta según lo establecido en el separador Planificación. Si selecciona **Flexible**, el agente de resumen y poda se ejecuta una vez inmediatamente después de que se inicie y luego en el intervalo **Ejecutar cada**, excepto durante los tiempos de bloqueo.

8. Especifique la información de turnos y los valores de vacaciones en el separador **Días de trabajo**:

   a. Seleccione domingo o lunes en **La semana empieza el**.

b. Si desea especificar turnos, seleccione **Especificar turnos**. Los valores predeterminados para este campo se listan en el recuadro **Horas de turno punta** en el lado derecho de la ventana. Para cambiar estos valores, seleccione las horas que desea en el recuadro **Horas de turno normal** y pulse el botón de flecha derecha para añadirlas al recuadro **Horas de turno punta**.

   Importante: No se recomienda especificar turnos porque aumenta la cantidad de espacio de disco necesaria en el almacén de datos y la cantidad de tiempo de proceso necesario para la acción de resumen y poda.

   Restricción: El cambio de la información de turnos después de haber resumido los datos puede crear una incoherencia en los datos. Los datos anteriores recopilados y resumidos no se pueden volver a calcular con los nuevos valores de turno.

c. Si desea cambiar los valores de vacaciones, seleccione **Especificar días de vacaciones**. Pulse **Sí** o **No** para especificar los fines de semana como días de vacaciones. Seleccione **Añadir** para abrir un calendario y luego seleccione los días de vacaciones que se han de añadir. Los días seleccionados se visualizan en el recuadro bajo el campo **Seleccionar días de vacaciones**. Si desea suprimir días que ha elegido anteriormente, selecciónelos y pulse **Suprimir**.

   Linux UNIX Pulse con el botón derecho para selecciona el mes y el año.

9. Seleccione las opciones que desea en el separador **Parámetros de registro**. este separador define los parámetros para podar las tablas de registro que llena el proxy de almacén y el agente de resumen y poda.
   a. Seleccione □ **Mantener los datos de WAREHOUSEAGGREGLOG para** para podar la tabla WAREHOUSEAGGREGLOG, que llena el agente de resumen y poda. Después de habilitar esta opción, especifique el número de días, meses o años que se deben mantener los datos en la tabla. El agente de resumen y poda de almacén suprimirá los datos que superen la antigüedad del intervalo de tiempo especificado.
   b. Seleccione □ **Mantener los datos de WAREHOUSELOG para** para podar la tabla WAREHOUSELOG, que llena el proxy de almacén. Después de habilitar esta opción, especifique el número de días, meses o años que se deben mantener los datos en la tabla. El agente de resumen y poda suprimirá los datos que superen la antigüedad del intervalo de tiempo especificado.
10. En el separador **Parámetros adicionales** seleccione estas opciones:
   a. Especifique las filas máximas que se pueden suprimir en una sola transacción de base de datos. Los valores son 1 a n. El valor predeterminado es `1000`.
   b. Especifique la antigüedad de los datos que desea resumir en los campos **Resumir por horas los datos anteriores a** y **Resumir por días los datos anteriores a**. Los valores son 0 a n. El valor predeterminado es 1 para datos por horas y `0` para datos diarios.
   c. Elija el huso horario que desea utilizar en la lista desplegable **Utilizar desplazamiento de huso horario**. Si Tivoli Data Warehouse y los agentes que están recopilando datos no están todos en el mismo huso horario y todos los datos se almacenan en la misma base de datos, utilice esta opción para identificar el huso horario que desea utilizar.

d. Especifique el número de hebras de ejecución simultáneas que se utilizarán cuando el agente de resumen y poda esté procesando datos en el campo **Número de hebras de trabajo**. El valor recomendado es dos veces el número de CPU. Un mayor número de hebras permiten que el agente de resumen y poda termine antes, pero se utilizan más recursos en la máquina que ejecuta el agente de resumen y poda y se utilizan más recursos de base de datos, como conexiones y espacio de registro de transacciones.

e. El agente de resumen y poda coloca en memoria caché los errores más recientes que se han producido en memoria. Esta información se proporciona en un grupo de atributos y se puede ver en los espacios de trabajo que se proporcionan con el agente de resumen y poda. El valor **Número máximo de errores de nodos que se deben mostrar** especifica el número máximo de errores que se deben guardar en memoria. Solo se conservan los errores más recientes. Cuando se alcanza el límite, se eliminan los errores más antiguos.

f. El agente de resumen y poda coloca en memoria caché información sobre las ejecuciones más recientes que se han realizado. Esta información se proporciona en un grupo de atributos y se puede ver en los espacios de trabajo que se proporcionan con el agente de resumen y poda. El valor **Número máximo de ejecuciones de resumen y poda que se deben mostrar** especifica el número máximo de ejecuciones que se deben guardar en memoria. Solo se conservan las ejecuciones más recientes. Cuando se alcanza el límite, se eliminan las ejecuciones más antiguas.

g. El agente de resumen y poda comprueba periódicamente que se puede comunicar con la base de datos de almacén de datos. El valor **Tiempo de memoria caché de conectividad de la base de datos** determina la frecuencia con la que se debe realizar esta comprobación.

h. Para mejorar el rendimiento, el agente de resumen y poda procesa por lotes las actualizaciones de la base de datos de almacén de datos. El parámetro **Modalidad de proceso por lotes** especifica cómo se realizará el proceso por lotes. Las dos opciones son **Un solo sistema gestionado** y **Varios sistemas gestionados**.

11. Linux UNIX Pulse en cualquiera de estos botones: **Guardar** después de comprobar que todos los valores sean correctos; **Recargar** para volver a cargas los valores originales; o **Cancelar**, en cualquier momento, para cancelar la ventana Configurar agente de resumen y poda.

Cómo inhabilitar el Summarization and Pruning agent

Puede inhabilitar el agente de resumen y poda para toda la empresa o para determinados productos o conjuntos de grupos de atributos.

Acerca de esta tarea

Si desea inhabilitar el resumen y la poda para toda la empresa:

1. En Manage Tivoli Enterprise Monitoring Services, pulse el botón derecho del ratón en el Summarization and Pruning agent de la columna Servicio/Aplicación.
2. Seleccione **Detener**.

Si desea desactivar el resumen y la poda para un producto determinado o conjunto de grupos de atributos en la ventana **Configuración de la recopilación de historial**:

Procedimiento

1. En Tivoli Enterprise Portal, pulse el botón **Configuración de la recopilación de historial** que está ubicado en la barra de herramientas.
2. Seleccione **Producto**.
3. Seleccione uno o varios **Grupos de atributos**.
4. Pulse el botón **Desconfigurar grupos**.

Registro de errores para datos almacenados

Si el agente de proxy de almacén encuentra errores durante la acumulación de datos en Tivoli Data Warehouse, estos errores se graban en el registro de sucesos. Puede establecer una opción de rastreo para capturar mensajes de error adicionales y luego consultar el registro para ayudar a detectar problemas.

Procedimiento

- Abra el registro de errores en el que aparecen listados los errores del proxy de almacén:
  - Windows Inicie el Visor de sucesos pulsando **Inicio → Programas → Herramientas administrativas → Visor de sucesos**, y luego seleccione **Aplicación** en el menú Registro. Si se produce un error durante la acumulación de datos, se insertan entradas en el registro de sucesos de aplicación de Windows.
  - Linux Abra el archivo *dir_ITM*/logs/*hd*.log.
  - En cualquier plataforma, los errores también se pueden ver en la tabla WAREHOUSELOG de la base de datos del almacén de datos.
- Active la opción de rastreo:
  1. En Manage Tivoli Monitoring Services, pulse con el botón derecho del ratón en **Proxy de almacén** y seleccione **Avanzado Editar parámetros de rastreo**.
  2. Seleccione los filtros RAS1. El valor predeterminado es **ERROR**.
  3. Acepte los valores predeterminados para el resto de campos.
  4. Pulse en **Sí** para reciclar el servicio.
- Para ver el registro de rastreo que contiene los mensajes de error:
  1. En Manage Tivoli Monitoring Services, pulse con el botón derecho del ratón en **Proxy de almacén** y seleccione **Avanzado → Ver registro de rastreo**. La ventana Visor de registro visualiza una lista de archivos de registro para el proxy de almacén.
  2. Seleccione el archivo de registro apropiado en Seleccionar archivo de registro. Todos los registros se listan en esta ventana, ordenados por el archivo más reciente.
  3. Pulse **Aceptar**.

Recopilación del historial de registro de operaciones de agente

El Registro de operaciones de agente recopila los mensajes que se producen en los agentes distribuidos de la empresa. Este registro forma parte de la infraestructura de agente de Tivoli Management Services. En Windows, si la configuración de recopilación de datos históricos incluye el grupo de atributos de Registro de operaciones de agente (tabla OPLOG), debe crear directorios para los datos históricos y editar cada archivo de configuración del agente.

Antes de empezar

Debe crear manualmente los directorios de datos históricos para todos los agentes que están recopilando datos históricos en el mismo sistema y luego editar cada archivo de configuración en el mismo sistema para especificar la nueva vía de acceso para la recopilación de datos a corto plazo. Esto es necesario en Windows porque todos los registros de agente se almacenan de forma predeterminada en el mismo directorio *dir_instalación*\tmaitm6\logs\ y cada agente crea un archivo de registro de operaciones de agente denominado OPLOG para almacenar datos históricos de corto plazo. De este modo, todos los agentes comparten el mismo archivo histórico OPLOG; si más de un proceso de agente intenta almacenar datos históricos del mismo archivo binario histórico de corto plazo, se pueden transferir los mismos datos a Tivoli Data Warehouse más de una vez.

Por ejemplo, se instalan los agentes de supervisión de sistema operativo Windows y Active Directory. Cada proceso creará y almacenará los datos de historial de registro de operaciones en un archivo denominado `C:\IBM\ITM\TMAITM6\logs\OPLOG` . Ahora habrá como mínimo dos procesos que intentarán compartir el mismo archivo de datos históricos. Se pueden grabar en el mismo archivo los datos de varios agentes, pero el proceso de subida de almacén encontrará problemas con esta configuración. Un proceso de agente no está al corriente de que, en un momento determinado, otro proceso de agente pueda estar realizando la misma subida de datos de almacén del mismo archivo histórico de corto plazo. Esto puede producir datos de historial duplicados transferidos a la base de datos de almacén.

Acerca de esta tarea

Para cada agente que recopila datos históricos en Windows, realice estos pasos:

Procedimiento

1. Cree un directorio hijo `history` de *dir_instalación*\tmaitm6\logs\.
2. Cree un directorio hijo `k??` de *dir_instalación*\tmaitm6\logs\history donde `??` es el código de producto de dos caracteres. Por ejemplo, `c:\ibm\itm\tmaitm6\logs\history\k3z` será la vía de acceso a los archivos históricos a corto plazo de *IBM Tivoli Monitoring Agent for Active Directory*. El ID de usuario de sistema para este agente debe tener permiso de lectura y grabación para este directorio.
3. Abra el archivo de configuración de agente *dir_instalación*\tmaitm6\k??cma.ini (donde `??` es el código de producto de dos caracteres) en un editor de texto. Consulte la guía del usuario del producto de supervisión para conocer el nombre del archivo utilizado para la configuración de agente.
4. Localice el parámetro `CTIRA_HIST_DIR=@LogPath@` y añádale al final `\history\k??` (donde `??` es el código de producto de dos caracteres). Por ejemplo, `CTIRA_HIST_DIR=@LogPath@\history\knt` especifica `c:\ibm\itm\tmaitm6\logs\history\knt` para la recopilación de datos históricos de agente de sistema operativo Windows de este sistema.
5. Guarde el archivo de configuración `k??cma.ini`.
6. Copie el archivo de estado de subida de almacén *dir_instalación*\tmaitm6\logs\khdexp.cfg en el directorio `\history\k??`. Si este archivo no se copia en el nuevo directorio de historial de agente, es posible que los datos de historial existentes se pongan en el almacén más de una vez. Es posible que este archivo no exista si la opción de almacén de historial no se ha habilitado nunca.

7. Copie los archivos `.hdr` y sus contrapartidas de nombre base (sin extensión de archivo) del agente en la nueva ubicación. Por ejemplo, el directorio `c:\ibm\itm\tmaitm6\logs\history\knt` puede tener este aspecto:

```
khdexp.cfg
netwrkin
netwrkin.hdr
ntprocssr
ntprocssr.hdr
wtlogcldsk
wtlogcldsk.hdr
wtmemory
wtmemory.hdr
wtphysdsk
wtphysdsk.hdr
wtserver
wtserver.hdr
wtsystem
wtsystem.hdr
```

   Tenga en cuenta que es posible que esté copiando archivos de datos históricos del directorio `tmaitm6\logs` no gestionados por el agente de destino. Por ejemplo, es posible que el directorio contenga datos históricos de base de datos de Oracle, pero que esté copiando los archivos en el nuevo directorio histórico de agente de sistema operativo Windows. Los archivos copiados no utilizados por el agente de sistema operativo Windows no se necesitarán y se pueden suprimir sin problemas.
8. En Manage Tivoli Enterprise Monitoring Services, pulse el botón derecho del ratón en el servicio de agente de supervisión y pulse **Reconfigurar**, pulse dos veces **Aceptar** para aceptar los valores de las ventanas de configuración, a continuación, pulse **Iniciar** el agente.

Proceso de conversión para utilizar archivos planos delimitados

Si elige no almacenar los datos, debe convertir los datos recopilados en archivos planos delimitados. Se puede planificar que los datos se conviertan manual o automáticamente. Si elige continuar convirtiendo los datos en archivos planos delimitados, planifique que la conversión de datos sea automática. Realice la conversión de datos con regularidad incluso aunque esté recopilando datos históricos sólo para soportar el historial a corto plazo que se visualiza en los informes de producto.

Si se utiliza la variable de entorno KHD_TOTAL_HIST_MAXSIZE, el agente no puede grabar datos históricos en los archivos históricos a corto plazo cuando se alcance el límite. Esta variable es un límite para los agentes.

Programas de conversión de datos

La conversión de archivos históricos a corto plazo a archivos planos delimitados se realiza ejecutando un programa de acumulación de datos:

Linux UNIX Windows **krarloff**

z/OS **KPDXTRA**

Columnas añadidas a archivos de datos de historial y a archivos de metadescripción

Se añaden automáticamente cuatro columnas a los archivos de datos de historial y a los archivos de metadescripción:

- **TMZDIFF**. Diferencia de huso horario respecto a la hora media de Greenwich (GMT). Este valor se muestra en segundos.

- **WRITETIME.** Indicación de fecha y hora de CT en que se ha grabado el registro. Es un valor de 16 caracteres con el siguiente formato, donde `S` es el siglo; `aammdd` es el año, mes y día; y `hhmmssttt` son las horas, minutos, segundos y milisegundos: `Saammddhhmmssttt`
- **SAMPLES.** La columna SAMPLES se incrementa para cada valor recopilado durante la misma muestra y, a continuación, se restablece otra vez al valor inicial. Las filas recopiladas en la misma muestra tienen valores de columna SAMPLES diferentes.
- **INTERVAL.** Tiempo entre muestras, mostrado en milisegundos.

Nota: El proceso de almacén de datos solo añade dos columnas, TMZDIFF y WRITETIME, a la base de datos de Tivoli Data Warehouse.

Archivos de metadescripción

Un archivo de metadescripción describe el formato de los datos de los archivos fuente. Los archivos de metadescripción se generan al principio del proceso de recopilación de datos históricos.

Los diversos entornos de sistema operativo utilizan diferentes convenios de denominación de archivo. A continuación se indican las reglas para algunos entornos de sistema operativo:

- IBM i y HP NonStop Kernel: Los archivos de descripción utilizan el nombre del archivo de datos como base. El último carácter del nombre es 'M'. Por ejemplo, para la tabla QMLHB, el nombre de archivo de datos históricos es QMLHB y el nombre de archivo de descripción es QMLHBM.
- z/OS: Los registros de descripción se almacenan en el recurso PDS, junto con los datos.
- UNIX y Linux: Utiliza el convenio de denominación de archivos *.hdr.
- Windows: Utiliza el convenio de denominación de archivos *.hdr.

Archivo de metadescripción *.hdr de ejemplo

```
TMZDIFF(int,0,4) WRITETIME(char,4,16)
QM_APAL.ORIGINNODE(char,20,128) QM_APAL.QMNAME(char,148,48)
QM_APAL.APPLID(char,196,12) QM_APAL.APPLTYPE(int,208,4)
QM_APAL.SDATE_TIME(char,212,16)
QM_APAL.HOST_NAME(char,228,48)
QM_APAL.CNTTRANPGM(int,276,4) QM_APAL.MSGSPUT(int,280,4)
QM_APAL.MSGSREAD(int,284,4) QM_APAL.MSGSBROWSD(int,288,4)
QM_APAL.INSIZEAVG(int,292,4) QM_APAL.OUTSIZEAVG(int,296,4)
QM_APAL.AVGMQTIME(int,300,4) QM_APAL.AVGAPPTIME(int,304,4)
QM_APAL.COUNTOFQS(int,308,4) QM_APAL.AVGMQGTIME(int,312,4)
QM_APAL.AVGMQPTIME(int,316,4) QM_APAL.DEFSTATE(int,320,4)
QM_APAL.INT_TIME(int,324,4) QM_APAL.INT_TIMEC(char,328,8)
QM_APAL.CNTTASKID(int,336,4) SAMPLES(int,340,4)
INTERVAL(int,344,4)
```

Por ejemplo, una entrada puede tener el siguiente formato, donde *int* identifica los datos como un entero, *75* es el desplazamiento de bytes del archivo de datos y *20* es la longitud del campo correspondiente a este atributo en el archivo:

```
attribute_name(int,75,20)
```

Estimación de espacio necesario para contener tablas de datos históricos

Las tablas de datos históricos para un producto se definen en la documentación del producto. Consulte la guía del agente apropiado para obtener ayuda para

determinar los nombres de las tablas donde se almacenan los datos históricos, el tamaño de las mismas y cuáles son las tablas predeterminadas.

Limitación del crecimiento de archivos históricos a corto plazo

tanto si el entorno incluye un almacén de datos como si está configurado para la conversión del histórico a corto plazo en archivos planos delimitados, es recomendable establecer un tamaño máximo para los archivos históricos.

Antes de empezar

El ID de usuario del sistema operativo debe tener permiso de grabación sobre este directorio.

Estas variables de entorno de agente no están disponibles en z/OS.

Acerca de esta tarea

Cuando la configuración incluye acumulación de datos en Tivoli Data Warehouse, el tamaño de los archivos históricos a corto plazo se controla mediante la cantidad de datos que se recopilan, la frecuencia de la recopilación y la frecuencia de acumulación en el almacén de datos. Es posible que el agente de proxy de almacén o que el almacén de datos dejen de estar disponibles, lo que significa que los archivos históricos a corto plazo pueden crecen sin comprobación.

Establezca las variables de entorno KHD_TOTAL_HIST_MAXSIZE y KHD_HISTSIZE_EVAL_INTERVAL en cada Tivoli Enterprise Monitoring Agent en el que se recopilen datos históricos o en el Tivoli Enterprise Monitoring Server si la recopilación de datos se produce en el mismo.

Siga estos pasos para especificar un límite de tamaño para el directorio en el que se guardan los archivos históricos a corto plazo y para establecer la frecuencia con la que se debe realizar una comprobación:

Procedimiento

1. Abra el archivo de entorno del agente:
   - Windows En la ventana Manage Tivoli Monitoring Services, pulse con el botón derecho del ratón en el componente y pulse **Avanzado → Editar archivo EN**. Estos son los archivos *dir_instalación*\TMAITM6\K<pc>ENV donde <pc> es el código de producto de dos caracteres, por ejemplo, C:\IBM\ITM\TMAITM6\KNTENV.
   - Linux UNIX Vaya al directorio *dir_instalación*/config y abra <pc>.ini en un editor de texto, donde <pc> es el código de producto de dos caracteres. Por ejemplo, /opt/IBM/ITM/config/ux.ini para el agente de SO UNIX.

   Para obtener una lista de códigos de producto, consulte "Códigos de producto, plataforma y componente de IBM Tivoli" en *IBM Tivoli Monitoring: Guía de instalación y configuración*.
2. Añada dos líneas nuevas al archivo, donde 5 es el número máximo de megabytes al que puede crecer el directorio en el que se encuentra el archivo histórico a corto plazo y 900 (15 minutos) es el número de segundos entre evaluaciones del tamaño del directorio:

```
KHD_TOTAL_HIST_MAXSIZE =5
KHD_HISTSIZE_EVAL_INTERVAL=900
```

3. Guarde el archivo y ciérrelo.
4. Recicle el componente.

Resultados

Después de establecer un máximo, cuando se alcanza el límite del directorio se dejan de grabar nuevos registros en los archivos históricos a corto plazo, lo que hace que se aparezcan huecos en los datos recopilados. Sin embargo, si los datos se guardan en el almacén, el proxy de almacén recortará los archivos históricos a corto plazo para que contengan solo datos correspondientes a las últimas 24 horas. Esto permitirá que el agente pueda volver a grabar datos históricos; por lo tanto, el límite se puede volver a alcanzar y el proceso se repite. Este proceso también puede ocasionar la aparición de huecos en los datos.

Qué hacer cuando el directorio de archivos históricos a corto plazo alcanza su límite

Cuando las variables de entorno KHD_TOTAL_HIST_MAXSIZE y KHD_HISTSIZE_EVAL_INTERVAL se han establecido para el Tivoli Enterprise Monitoring Agent (o en el Tivoli Enterprise Monitoring Server si la recopilación de datos se produce en el mismo), no se añaden más muestras de datos históricos a los archivos históricos a corto plazo si se ha alcanzado el tamaño máximo del directorio.

Tiene que solucionar la causa del crecimiento no comprobado de los archivos históricos a corto plazo para que se puedan volver a guardar muestras de datos en los archivos históricos. Cuando los datos se recopilan en el agente, puede crear una consulta SQL personalizada o una situación, o ambas, que indique cuándo se produce esta condición.

A continuación se muestra un ejemplo de consulta SQL personalizada que puede ejecutar:

```
SELECT ORIGINNODE, CATEGORY, SEVERITY, TABLE, TIMESTAMP, MESSAGE
FROM O4SRV.KRAMESG WHERE ORIGINNODE = $NODE$
```

Conversión de archivos de historial a corto plazo en archivos planos delimitados

Si ha seleccionado la opción para almacenar datos en una base de datos, esa opción se excluye mutuamente con la ejecución de los programas de conversión de archivos descritos en este apartado. Para utilizar estos procedimientos de conversión, debe haber especificado **Desactivado** para la opción de almacén de la ventana Configuración de la recopilación histórica de Tivoli Enterprise Portal.

El procedimiento de conversión vacía los archivos de acumulación históricos y se debe realizar periódicamente para que los archivos históricos no ocupen cantidades innecesarias de espacio de disco.

Conversión de archivos utilizando el programa krarloff

El programa de acumulación krarloff se puede ejecutar en el Tivoli Enterprise Monitoring Server o en el directorio en el que se ejecuta el agente de supervisión, desde el directorio en el que se almacenan los archivos históricos.

Formato de atributos

Algunos atributos necesitan formatearse para la visualización. Por ejemplo, los números de coma flotante que especifican un determinado número de dígitos de precisión que se deben escribir a la izquierda del separador decimal. Estas consideraciones sobre el formato de visualización se especifican en archivos de atributos de producto.

Cuando utilice el programa de acumulación krarloff para acumular datos históricos en un archivo de texto, se ignoran los atributos que necesitan especificadores de formato como se indica en el archivo de atributos. Únicamente se ve el número solo en el archivo de texto de historial acumulado. De este modo, en lugar de visualizar 45,99% o 45,99, se visualiza el número 4599.

El proxy de almacén inserta datos de acuerdo con el tipo, la longitud y la precisión datos que se especifiquen en los archivos de atributo. Sin embargo, la base de datos de Tivoli Data Warehouse visualiza el formato de atributos correcto *sólo* para los atributos que utilizan enteros con formatos de número de coma flotante.

Puede utilizar el programa de acumulación krarloff para convertir el archivo histórico del Tivoli System Monitor Agent en un archivo de texto en Linux y UNIX. El programa de acumulación krarloff se utiliza porque el Tivoli System Monitor Agent no proporciona el mandato **itmcmd history** en UNIX ni Linux.

Procedimiento

Windows

Ejecute el programa de acumulación krarloff desde el directorio en el que se ejecuta el servidor de supervisión o el agente de supervisión especificando lo siguiente en el indicador de mandatos:

```
krarloff [-h] [-g] [-x] [-d delimiter] [-m metafile] [-r rename-to-file]
[-o output-file] {-s source | source-file name}
```

Donde los corchetes [ ] indican los parámetros opcionales y las llaves { } indican un parámetro obligatorio mostrado abajo.

Linux

1. Establezca las variables de entorno:

   ```
   export PATH=$PATH: $CANDLEHOME/tmaitm6/<interp>/bin/
   export ATTRLIB=$CANDLEHOME/<interp>/lz/tables/ATTRLIB
   export LD_LIBRARY_PATH=$CANDLEHOME/<interp>/gs/lib
   ```

2. Copie la cabecera y el archivo de datos en otro directorio:

   ```
   mkdir $CANDLEHOME/<interp>/lz/hist/tmp
   cp PVTHIST_LNXCPU* $CANDLEHOME/<interp>/lz/hist/tmp
   cd tmp
   ```

3. Ejecute el programa krarloff para convertir el archivo histórico en un archivo de texto. Por ejemplo:

   ```
   krarloff -h -d ";" -m PVTHIST_LNXCPU.hdr -o PVTHIST_LNXCPU.out
   -s PVTHIST_LNXCPU
   ```

UNIX

1. Establezca las variables de entorno:

   ```
   export PATH=$PATH: $CANDLEHOME/tmaitm6/<interp>/bin/
   export ATTRLIB=$CANDLEHOME/<interp>/ux/tables/ATTRLIB
   ```

2. Copie la cabecera y el archivo de datos en otro directorio:

```
mkdir $CANDLEHOME/<interp>/ux/hist/tmp
cp PVTHIST_UNIXDISK* $CANDLEHOME/<interp>/ux/hist/tmp
cd tmp
```

3. Ejecute el programa krarloff para convertir el archivo histórico en un archivo de texto. Por ejemplo:

```
krarloff -h -d ";" -m PVTHIST_UNIXDISK.hdr -o PVTHIST_UNIXDISK.out
-s PVTHIST_UNIXDISK
```

Una vez finalizada la conversión, se cambia el nombre del archivo histórico por `*.old`. Por ejemplo, `PVTHIST_LNXCPU` se convierte en `PVTHIST_LNXCPU.old`.

El agente coloca todos los archivos del historial privado en este subdirectorio:

Windows *install_dir*\TMAITM6\logs

Linux UNIX *install_dir*/<arch>/<pc>/hist

Restricción: El programa de acumulación krarloff no recibe soporte para el agente IBM i en sistemas AS400.

Parámetros de programa de acumulación krarloff

La tabla siguiente muestra los parámetros del programa de acumulación krarloff, su finalidad y sus valores predeterminados.

Tabla 64. Parámetros para el programa de acumulación krarloff

Parámetro	Valor predeterminado	Descripción
-h	off	Controla la presencia o ausencia de la cabecera del archivo de salida. Si existe, la cabecera se imprime como la primera línea. La cabecera identifica el nombre de columna de atributo.
-g	off	Controla la presencia o ausencia del nombre_grupo de producto de la cabecera del archivo de salida. Añada -g a la línea de invocación para el programa de acumulación krarloff para incluir nombre_grupo.nombre_atributo en la cabecera.
-x	off	Excluye los atributos SAMPLES y INTERVAL en el archivo de salida.
-d	tab	Delimitador utilizado para separar campos en el archivo de texto de salida. Los valores válidos son cualquier carácter individual (por ejemplo una coma).
-m	source-file.hdr	Metarchivo que describe el formato de los datos del archivo de origen. Si no se especifica ningún metarchivo en la línea de mandatos, se utiliza el nombre de archivo predeterminado.
-r	source-file.old	Parámetro Rename-to-filename utilizado para renombrar el archivo de origen. Si falla la operación de renombrar, el script espera dos segundos y reintenta la operación.
-o	source-file.*nnn* donde *nnn* es el día del calendario juliano.	Nombre de archivo de salida. Nombre del archivo que contiene el archivo de texto de salida.

Tabla 64. Parámetros para el programa de acumulación krarloff (continuación)

Parámetro	Valor predeterminado	Descripción
-s	ninguno	**Parámetro necesario**. Archivo histórico a corto plazo de origen que contiene los datos que es necesario leer. Entre las llaves, la barra vertical (|) indica que puede utilizar una opción de origen -s o, si se especifica un nombre sin opción, se considera un nombre de archivo de origen. No se suponen valores predeterminados para el archivo de origen.

Conversión de archivos de historial en archivos planos delimitados en sistemas Windows

Los archivos históricos recopilados utilizando las reglas establecidas en el programa de configuración de recopilación de datos históricos se pueden convertir en archivos planos delimitados para utilizarlos en diversas aplicaciones comunes con el fin de manipular fácilmente los datos y crear informes y gráficos. Utilice el mandato **AT** de Windows para planificar la conversión automática de archivos. Utilice el programa de acumulación krarloff para invocar manualmente la conversión de archivo. Para obtener los mejores resultados, planifique que la conversión se ejecute cada día.

Proceso de conversión mediante el mandato AT

Al configurar el proceso que convierte los archivos de historial que ha recopilado en archivos planos delimitados, planifique el proceso automáticamente ejecutando el mandato **AT** de Windows o manualmente ejecutando el programa de acumulación krarloff. La conversión de archivos históricos se puede producir tanto si el Tivoli Enterprise Monitoring Server o el agente está en ejecución como si no lo está.

Nota: Ejecute la conversión de archivo de historial cada 24 horas.

Procedimiento de archivado utilizando el mandato AT de Windows:

Para archivar archivos de datos históricos en servidores de Tivoli Enterprise Monitoring y en sistemas gestionados remotos mediante el mandato **AT**, utilice el procedimiento siguiente. Para saber el formato del mandato, escriba **AT /?** en el indicador de mandatos de MS/DOS.

1. Para que el mandato AT funcione, debe iniciar el servicio Programador de tareas. Para iniciar el servicio de planificación de tareas, seleccione **Configuración > Panel de control > Herramientas administrativas > Servicio**.

   Resultado: Se visualiza la ventana Servicios.
2. En la ventana Servicios, seleccione **Programador de tareas**. Cambie el tipo de inicio de servicio a automático. Pulse **Iniciar**.

   Resultado: Se inicia el servicio Programador de tareas.

   A continuación se muestra un ejemplo de utilización del mandato AT para archivar archivos históricos:

   ```
   AT 23:30 /every:M,T,W,Th,F,S,Su c:\sentinel\cms\archive.bat
   ```

   En este ejemplo, Windows ejecuta el archivo archive.bat situado en c:\sentinel\cms cada día a las 11:30 pm. Un ejemplo del contenido de archive.bat es:

```
krarloff -o memory.txt wtmemory
krarloff -o physdsk.txt wtphysdsk
krarloff -o process.txt wtprocess
krarloff -o system.txt wtsystem
```

Ubicación de los archivos ejecutables y de los archivos de tablas de recopilación de datos históricos de Windows:

En este apartado se muestra la ubicación de los programas de Windows necesarios para convertir datos históricos.

Los programas están en las siguientes ubicaciones:

- Directorio *install_dir*\cms del Tivoli Enterprise Monitoring Server.
- Directorio *install_dir*\tmaitm6 en los sistemas gestionados remotos en los que están instalados los agentes.

Si los datos históricos de agente se han configurado para almacenarse en el sistema de agente y desea almacenar los archivos históricos en un disco que proporciona más capacidad de almacenamiento de la que proporciona la ubicación de archivo de datos históricos predeterminada, se puede alterar temporalmente esta ubicación utilizando la variable de entorno existente *CTIRA_HIST_DIR* para el agente. Esto no se puede realizar cuando los datos históricos están almacenados en el Tivoli Enterprise Monitoring Server.

Si tiene varias instancias de un mismo agente en ejecución en el mismo sistema Windows, el instalador crea un directorio independiente para los archivos históricos de proceso almacenados en el agente. La ubicación predeterminada para los agentes que se ejecutan en el sistema operativo Windows es C:\IBM\ITM\TMAITM6\LOGS. Los directorios nuevos se crean bajo el directorio TMAITM6\LOGS: History\<*código componente 3 caracteres*>*(KUM, KUD, etc.)*\<*nombre de instancia multiproceso especificado*>.

Por ejemplo, si configura una segunda instancia del agente de DB2 Monitoring denominada *UDBINST1* en el mismo sistema Windows, se crea un directorio llamado C:\IBM\ITM\TMAITM6\LOGS\History\KUD\UDBINST1 para almacenar los datos históricos. Esta instancia de la variable de entorno del agente de DB2 CTIRA_HIST_DIR se establece en este valor.

Ubicación de los archivos de tablas de datos históricos de Windows:

En la siguiente sección se describe la ubicación de los archivos de tablas de datos históricos de Windows.

El programa de acumulación krarloff necesita conocer la ubicación de estos archivos.

Si ejecuta el servidor de supervisión y los agentes como procesos o como servicios, los archivos de tabla de datos históricos están ubicados en el:

- Directorio *install_dir*\cms del servidor de supervisión
- Directorio *install_dir*\tmaitm6\logs de los sistemas gestionados

Conversión de archivos de historial en archivos planos delimitados en sistemas IBM i

Los archivos históricos recopilados utilizando las reglas establecidas en el programa de configuración de recopilación de datos históricos se pueden convertir

en archivos planos delimitados para utilizarlos en diversas aplicaciones comunes con el fin de manipular fácilmente los datos y crear informes y gráficos. Utilice el programa de acumulación krarloff para invocar manualmente la conversión de archivo.

Nota: Ejecute la conversión de archivo de historial cada 24 horas.

Almacenamiento de los datos históricos almacenados en un sistema IBM i

Los datos de usuario se almacenan en el directorio IFS establecido para la variable de configuración *CTIRA_HIST_DIR*. El valor predeterminado para esta variable es */qibm/userdata/ibm/itm/hist*. Por cada tabla hay dos archivos almacenados en el sistema IBM i que están asociados a la recopilación de datos históricos.

Por ejemplo, si está recopilando datos para los atributos de estado de sistema, estos dos archivos son:

- KA4SYSTS: Son los datos a corto plazo visualizados como salida por el agente de IBM i.
- KA4SYSTS.hdr: Éste es el metarchivo. El metarchivo contiene una sola fila de nombres de columna.

El contenido de ambos archivos se puede visualizar utilizando el mandato WRKLNK */qibm/userdata/ibm/itm.hist*.

Proceso de conversión en un sistema IBM i

El programa de acumulación krarloff se puede ejecutar en el Tivoli Enterprise Monitoring Server o en el directorio en el que se ejecuta el agente de supervisión desde el directorio en el que se almacenan los archivos históricos.

Ejecute el programa de acumulación krarloff entrando lo siguiente en el indicador de mandatos:

```
call qautomon/krarloff parm (['-h'] ['-g'] ['-x'] ['-d' 'delimiter']
['-m' metafile] ['-r' rename-source-file-to] ['-o' output-file]
{'-s' source-file | source-file )}
```

Donde los corchetes [ ] indican los parámetros opcionales y las llaves { } indican un parámetro obligatorio.

Si ejecuta el programa de acumulación krarloff desde un sistema IBM i en el directorio en el que se ejecuta el agente, sustituya `qautomon` por el nombre del ejecutable para el agente. Por ejemplo, el agente MQ utiliza `kmqlib` en la cadena de mandato.

Nota: Entre el mandato en una sola línea.

Después de ejecutar el programa de acumulación krarloff

Al utiliza el ejemplo de estatus de sistema anterior, después de ejecutar el programa de acumulación krarloff, el archivo KA4SYSTS se convierte en KA4SYSTSO. Se genera un nuevo archivo KA4SYSTS cuando está disponible otra fila de datos.

KA4SYSTSM permanece como está.

KA4SYSTSH es el archivo visualizado como salida por el programa de acumulación krarloff y que contiene los datos en formato de archivo plano

delimitado. Este archivo se puede transferir de IBM i a la estación de trabajo mediante un programa de transferencia de archivos (FTP).

Conversión de archivos de historial en archivos planos delimitados en sistemas UNIX

Este tema explica cómo se utiliza el script **itmcmd history** de UNIX para convertir los datos históricos guardados contenidos en los archivos de datos históricos en archivos planos delimitados. Puede utilizar los archivos planos delimitados en diversas aplicaciones comunes para manipular fácilmente los datos con el fin de crear informes y gráficos.

Visión general de la conversión de datos históricos

En la sección siguiente se describe el procedimiento de conversión de tablas de datos históricos en otros tipos de archivos con el fin de que las utilicen otros productos de software.

En el entorno de UNIX, utilice el script **itmcmd history** para activar y personalizar el procedimiento de conversión utilizado para convertir tablas de datos históricos a corto plazo de Tivoli Monitoring seleccionadas en un formato utilizable por otros productos de software. Los datos históricos que se recopilan están en un formato binario y se deben convertir a ASCII para que lo puedan utilizar productos de otros proveedores. Cada archivo de corto plazo se convierte de forma independiente. Los datos históricos recopilados por el Tivoli Enterprise Monitoring Server pueden estar en la ubicación de host del Tivoli Enterprise Monitoring Server o en la ubicación del agente de informe. La conversión se puede ejecutar en cualquier momento, tanto si el Tivoli Enterprise Monitoring Server o los agentes están activos como si no lo están.

La conversión se aplica a todos los datos históricos recopilados bajo el *dir_instalación* actual asociado con un Tivoli Enterprise Monitoring Server individual, tanto si los datos los ha grabado el Tivoli Enterprise Monitoring Server como si los ha grabado un agente de supervisión.

Cuando entre:

```
itmcmd history -h
```

en la línea de mandatos, se visualizará esta salida:

```
itmcmd history [ -h dir_instalación ] -C [ -L nnn[Kb|Mb] ] [ -t masks*,etc ]
   [ -D delim ] [ -H|+H ] [ -N n ] [ -p cms_name ]
   prod_code itmcmd history -A?itmcmd history [ -h dir_instalación ]
   -A perday|0 [ -W days ] [ -L nnn[Kb|Mb] ] [ -t masks*,etc ]
   [ -D delim ] [ -H|+H ] [ -N n ]
   [ -i instance|-p cms_name ] [ -x ] prod_code
```

Nota: Determinados parámetros son necesarios. Los elementos separados con una barra vertical | indican exclusividad mutua (por ejemplo Kb|Mb significa entrar Kb o Mb, no ambos). Normalmente, los parámetros se entran en una sola línea en la línea de mandatos de UNIX.

Consulte la publicación *IBM Tivoli Monitoring: Consulta de mandatos* para todos los parámetros utilizados con este mandato.

Realización de la conversión de datos históricos

El script **itmcmd history** planifica la conversión de datos históricos en archivos planos delimitados. A continuación, se describen el proceso manual para realizar una conversión de una sola vez y el script de conversión que le permite planificar conversiones automáticas.

Consulte la publicación *IBM Tivoli Monitoring: Consulta de mandatos* para obtener una descripción completa de la sintaxis y las opciones.

Después de que haya tenido lugar la conversión, el archivo plano delimitado resultante tiene el mismo nombre que el archivo histórico de entrada con una extensión que es un dígito numérico individual. Por ejemplo, si el nombre de tabla de archivo histórico de entrada es KOSTABLE, el archivo convertido se denomina KOSTABLE.0. La siguiente conversión se denomina KOSTABLE.1 y así sucesivamente.

Realización de una conversión de una sola vez:

Para realizar un proceso de conversión de una sola vez, cambie a *install_dir*/bin y entre lo siguiente en la línea de mandatos:

```
./itmcmd history -C prod_code
```

Planificación de conversiones de historial automáticas básicas:

Utilice **itmcmd history** para planificar conversiones automáticas mediante el recurso *cron* de UNIX. Para planificar una conversión automática básica, entre lo siguiente en la línea de mandatos:

```
./itmcmd history -A n código_prod
```

donde *n* es un número comprendido entre 1 y 24. Este número especifica el número de veces por día que se ejecuta el programa de conversión de datos, redondeado por exceso al siguiente divisor de 24. El código de producto también es necesario.

Por ejemplo, el siguiente mandato indica que se debe ejecutar la conversión de datos históricos cada tres horas:

```
itmcmd history -A 7 ux
```

Personalización de la conversión de historial:

Puede utilizar el script **itmcmd history** para personalizar adicionalmente la recopilación histórica especificando opciones adicionales. Por ejemplo, puede elegir convertir archivos que están por encima de un límite de tamaño determinado que ha establecido. También puede elegir realizar la conversión de historial durante determinados días de la semana.

Consulte la publicación *Consulta de mandatos* para obtener una descripción de todos los parámetros de conversión de historial.

Conversión de archivos de historial en archivos planos delimitados en sistemas HP NonStop Kernel

Si ha seleccionado la opción para recopilar y almacenar datos en un almacén de datos, esa opción y la ejecución de los programas de conversión de archivos descritos en este capítulo son mutuamente excluyentes. Para utilizar estos

procedimientos de conversión, debe haber especificado **Desactivado** para la opción **Almacén** de la ventana **Configuración de la recopilación de historial** de Tivoli Enterprise Portal.

Los archivos históricos recopilados utilizando las reglas establecidas en el programa de configuración de historial se pueden convertir en archivos planos delimitados para utilizarlos en diversas aplicaciones comunes con el fin de manipular fácilmente los datos y crear informes y gráficos. Utilice el programa de acumulación krarloff para invocar manualmente la conversión de archivo. Para obtener los mejores resultados, planifique que la conversión se ejecute cada día.

Se proporciona soporte para IBM Tivoli Monitoring para WebSphere MQ Configuration y para IBM Tivoli Monitoring para WebSphere MQ Monitoring que se ejecutan en el sistema operativo HP NonStop Kernel (antes llamado Tandem). Si desea obtener información específica de IBM Tivoli Monitoring para WebSphere MQ Monitoring en relación a la recopilación de datos históricos, consulte el tema de personalización de opciones de supervisión que se encuentra en la versión correspondiente de la documentación del producto.

Proceso de conversión en sistemas HP NonStop Kernel

Al configurar el proceso que convierte los archivos de historial que ha recopilado en archivos planos delimitados, planifique el proceso manualmente ejecutando el programa krarloff rolloff. Ejecute la conversión de archivo de historial cada 24 horas.

Utilización del programa de acumulación krarloff en HP NonStop Kernel:

Los archivos de historial se conservan en el subvolumen DATA, bajo el valor predeterminado <$VOL>.CCMQDAT. Sin embargo, la ubicación de los archivos de historial depende del lugar donde se inicie el agente de supervisión. Si ha iniciado el agente de supervisión utilizando STRMQA desde el subvolumen CCMQDAT, los archivos se almacenan en CCMQDAT.

Puede ejecutar el programa de acumulación krarloff desde el subvolumen DATA entrando lo siguiente:

RUN <$VOL>.CCMQEXE.KRARLOFF <parámetros>

Tenga en cuenta que CCMQDAT y CCMQEXE son valores predeterminados. Durante el proceso de instalación, puede asignar sus propios nombres para estos archivos.

Formato de atributos:

Algunos atributos necesitan formatearse para la visualización. Por ejemplo, los números de coma flotante que especifican un determinado número de dígitos de precisión que se deben escribir a la izquierda del separador decimal. Estas consideraciones sobre el formato de visualización se especifican en archivos de atributos de producto.

Cuando utilice el programa de acumulación krarloff para acumular datos históricos en un archivo de texto, se ignoran los atributos que necesitan especificadores de formato como se indica en el archivo de atributos. Únicamente se ve el número solo en el archivo de texto de historial acumulado. De este modo, en lugar de visualizar 45,99% o 45,99, se visualiza el número 4599.

Conversión de archivos de historial en archivos planos delimitados en sistemas z/OS

Puede convertir los archivos históricos a corto plazo en archivos planos delimitados en sistemas z/OS con un procedimiento de archivado manual o como parte de los procedimientos de mantenimiento del almacén de datos permanentes.

Los archivos históricos a corto plazo se pueden convertir en archivos sin formato delimitados automáticamente como parte de los procedimientos de mantenimiento del almacén de datos persistente, o se pueden convertir manualmente con el mandato MODIFY. El archivo plano delimitado sirve como entrada de aplicaciones para la manipulación de datos y la creación de informes.Para obtener más información, consulte *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Planning and Configuration* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm)

Los datos que se han recopilado y almacenado no se pueden extraer puesto que estos datos se han suprimido del almacén de datos permanentes. Para utilizar estos procedimientos de conversión, debe haber establecido el **Intervalo de almacén** en **Desactivado** en la ventana de configuración de la recopilación de historial. Para obtener más detalles sobre la ventana Configuración de la recopilación de historial, consulte la ayuda en línea de Tivoli Enterprise Portal o Creación de una recopilación de datos históricos en *Tivoli Enterprise Portal: Guía del usuario*.

Referencia relacionada:

"Procedimiento de archivado manual" en la página 536
Para convertir manualmente los archivos de datos históricos en el Tivoli Enterprise Monitoring Server y en los sistemas gestionados remotos, emita el siguiente mandato MODIFY:

Proceso automático de conversión y archivado en sistemas z/OS

Esta sección contiene información sobre el proceso de conversión y archivado automático que se realiza en sistemas z/OS.

Al personalizar el entorno de IBM Tivoli Monitoring, se le ha proporcionado la oportunidad de especificar la opción EXTRACT para el mantenimiento. La especificación de la opción EXTRACT asegura que la planificación del proceso para convertir y archivar la información almacenada en las tablas de datos históricos sea automática. No es necesario realizar ninguna acción adicional por su parte. Mientras las aplicaciones graban datos históricos en las tablas de datos históricos, el almacén de datos permanentes detecta cuándo un conjunto de datos determinado está lleno, inicia el proceso KPDXTRA para copiar el conjunto de datos e informa al Tivoli Enterprise Monitoring Server que el conjunto de datos se puede utilizar otra vez para recibir información histórica. Puede encontrar información adicional sobre el almacén de datos permanentes en *IBM Tivoli Management Services en z/OS: Configuración de Tivoli Enterprise Monitoring Server en z/OS*.

Una alternativa a la planificación automática de la conversión es la emisión manual del mandato para convertir los archivos de datos históricos.

Nota: El proceso KPDXTRA no da soporte actualmente a las columnas UTF8.

Conversión de archivos utilizando el programa KPDXTRA:

Los procedimientos de mantenimiento de almacén de datos permanentes llaman al programa de conversión, KPDXTRA, cuando se especifica la opción EXTRACT para mantenimiento. Este programa lee un conjunto de datos que contiene los datos históricos recopilados y graba dos archivos para cada tabla que tiene datos recopilados. El proceso de estos datos no interfiere con la recopilación continua que se está realizando.

Dado que el proceso es automático, aquí se proporciona una visión general breve del uso del programa KPDXTRA. Para obtener información completa sobre el programa KPDXTRA, revise el JCL de ejemplo distribuido con el producto Tivoli Monitoring. El JCL de ejemplo se encuentra como parte del trabajo de ejemplo del programa KPDXTRA contenido en las bibliotecas de ejemplo RKANSAM y TKANSAM.

Formato de atributos:

Algunos atributos necesitan formatearse para la visualización. Por ejemplo, los números de coma flotante que especifican un determinado número de dígitos de precisión que se deben escribir a la izquierda del separador decimal. Estas consideraciones sobre el formato de visualización se especifican en archivos de atributos de producto.

Cuando utilice KPDXTRA para acumular datos históricos en un archivo de texto, se ignoran los atributos que necesitan especificadores de formato como se indica en el archivo de atributos. Únicamente se ve el número solo en el archivo de texto de historial acumulado. De este modo, en lugar de visualizar 45,99% o 45,99, se visualiza el número 4599.

Acerca de KPDXTRA:

El programa KPDXTRA se ejecuta en el entorno de proceso por lotes como parte de los procedimientos de mantenimiento. Es capaz de tomar un parámetro que permite cambiar el separador de columna predeterminado. La sintaxis JCL de z/OS para ejecutar este mandato es:

```
// EXEC PGM=KPDXTRA,PARM='PREF=prefijo-dsn [DELIM=xx] [NOFF]'
```

Se deben asignar varios archivos para que se ejecute este trabajo.

Todos los conjuntos de datos se mantienen con un estado de lectura/grabación, aunque no estén activos. Esto hace que los conjuntos de datos no estén disponibles si se está ejecutando el Tivoli Enterprise Monitoring Server. Por lo tanto, no se pueden ejecutar trabajos en los conjuntos de datos activos y los conjuntos de datos inactivos se deben poner fuera de línea.

Puede eliminar un conjunto de datos del Tivoli Enterprise Monitoring Server emitiendo el siguiente mandato:

```
F stcname,KPDCMD DELFILE FILE=DSN:datastorefile
```

Tenga en cuenta que DELFILE sólo elimina el archivo de PDS; no suprime el archivo. El archivo se puede volver a añadir a PDS GROUP con un mandato RESUME:

```
F stcname,KPDCMD RESUME FILE=DSN:datastorefile
```

Si debe ejecutar un programa de utilidad en un almacén de datos activo, emita un mandato SWITCH antes de emitir este mandato.

nombres DD que es necesario asignar para KPDXTRA:

A continuación se proporciona un resumen de los nombres DD que se deben asignar para el programa KPDXTRA. Consulte el JCL de ejemplo en las bibliotecas de ejemplo distribuidas con el producto para obtener información adicional.

Tabla 65. Nombres DD necesarios

Nombre DD	Descripción
RKPDOUT	Mensajes de registro de KPDXTRA
RKPDLOG	Mensajes de PDS
RKPDIN	Archivo de mandatos de definición de tabla (entrada en subtarea de PDS) configurado por la herramienta de configuración
RKPDIN1	Archivo de PDS del que se deben extraer los datos
RKPDIN2	Archivo de control opcional definido como sentencia DUMMY DD

Parámetros de KPDXTRA:

La tabla siguiente especifica los parámetros de KPDXTRA, junto con sus valores predeterminados y descripciones.

Tabla 66. Parámetros de KPDXTRA

Parámetro	Valor predeterminado	Descripción
PREF=	ninguno	Parámetro necesario. Identifica el calificador de alto nivel donde se graban los archivos de salida.
DELIM=	tab	Especifica el carácter separador a utilizar entre columnas en el archivo de salida. El valor predeterminado es el carácter tabulador X'05'. Para especificar algún otro carácter, especifique un hexadecimal de 2 bytes representativo de dicho carácter. Por ejemplo, para utilizar una coma, especifique DELIM=6B.
QUOTE	NQUOTE	Parámetro opcional que pone todos los campos de tipo carácter entre comillas dobles. Los blancos de cola se eliminan de la salida. Hace que el formato de salida del programa KPDXTRA sea idéntico al formato de salida generada por el programa de acumulación krarloff distribuido.
NOFF	off	Hace que se cree (si se establece en ON) o se omita (si se establece en OFF) un archivo independiente (archivo de cabecera) que contiene el formato de las tablas. También controla la presencia o la ausencia de la cabecera en el archivo de datos de salida que se crea como resultado de la operación de extracción. Si se especifica OFF, el archivo de cabecera no se crea pero se incluye la información de cabecera como la primera línea del archivo de datos. La información de cabecera muestra el formato de los datos extraídos.

Mensajes del programa KPDXTRA:

Estos mensajes se pueden encontrar en los registros sysout de RKPDOUT creados por la ejecución de los procedimientos de mantenimiento:

```
Programa de extracción de almacén de datos permanentes KPDXTRA - Versión V130.00
Utilizando el prefijo de nombre de archivo de salida: CCCHIST.PDSGROUP
Se utilizan los caracteres siguientes para delimitar las señales de archivo de salida:
Valores de columna en archivo de datos.............:  0x05
 Elementos de lista entre paréntesis en archivo de formato:  0x6b
Nota: No se ha encontrado el archivo de control de entrada; se extraen todos los
datos permanentes.

Tabla(s) definida(s) en archivo de almacén de datos permanentes CCCHIST.PDSGROUP.PDS#1:
```

Nombre de aplicación	Nombre de tabla	Estado de extracción
PDSSTATS	PDSCOMM	Excluido
PDSSTATS	PDSDEMO	Incluido
PDSSTATS	PDSLOG	Incluido
PDSSTATS	TABSTATS	Incluido

```
Comprobar la disponibilidad de datos en el archivo de almacén de datos:
  No se han encontrado datos para apl.: PDSSTATS Tabla: PDSDEMO   . Tabla excluida.
  No se han encontrado datos para apl.: PDSSTATS Tabla: TABSTATS  . Tabla excluida.
Se extrae(n) la(s) siguiente(s) 1 tabla(s):
```

Nombre de aplicación	Nombre de tabla	Núm. de filas	Fila más antigua	Fila más reciente
PDSSTATS	PDSLOG	431	1997/01/10 05:51:20	1997/02/04 02:17:54

```
Iniciando operación de extracción.
Iniciando extracción de PDSSTATS.PDSLOG.
El archivo de datos de salida, CCCHIST.PDSGROUP.D70204.PDSLOG, no existe; se crea.
El archivo de formato de salida, CCCHIST.PDSGROUP.F70204.PDSLOG, no existe;
  se crea.
Extracción completada para PDSSTATS.PDSLOG. 431 filas de datos recuperadas, 431 grabadas.
La operación de extracción se ha completado.
```

Ubicación de los archivos ejecutables y de los archivos de la tabla de datos históricos de z/OS

En la siguiente sección se identifica la ubicación de los archivos ejecutables y de los archivos de tablas de datos históricos de z/OS.

Los archivos ejecutables de z/OS se encuentran en la biblioteca *&rhilev.&rte.*RKANMOD o *&thilev.*TKANMOD, donde:

- *&rhilev* es el calificador de alto nivel para el entorno de ejecución.
- *&rte* es el nombre del entorno de ejecución.
- *&thilev* es el calificador de alto nivel de las bibliotecas destino que ha instalado SMP/E.

Los archivos de datos históricos de z/OS que crea el programa de extracción se encuentran en la siguiente estructura de la biblioteca:

- *&hilev.&midlev.&dsnlolev.nombretabla.*D
- *&hilev.&midlev.&dsnlolev.nombretabla.*H

Procedimiento de archivado manual

Para convertir manualmente los archivos de datos históricos en el Tivoli Enterprise Monitoring Server y en los sistemas gestionados remotos, emita el siguiente mandato MODIFY:

```
F stcname,KPDCMD SWITCH GROUP=cccccccc EXTRACT
```

donde:

- *stcname* identifica el nombre de la tarea iniciada que ejecuta el Tivoli Enterprise Monitoring Server o los agentes.
- *cccccccc* identifica el nombre de grupo asociado con las asignaciones de almacén de datos permanentes. Los valores para *cccccccc* pueden variar en función de los productos que se instalen. El nombre de grupo estándar es GENHIST.

Cuando se ejecuta este mandato, sólo se extraen las tablas asociadas con el identificador de grupo. Si se instalan varios productos, se puede controlar cada uno mediante mandatos SWITCH independientes.

Esta conmutación se puede automatizar utilizando un recurso de planificación de instalación o un producto de automatización.

También puede utilizar las características de automatización avanzadas de Tivoli Enterprise Portal para ejecutar el mandato SWITCH. Para ello, defina una situación que, cuando sea verdadera, ejecute el mandato SWITCH como acción.

Mantenimiento del almacén de datos permanentes

Tiene la opción de ejecutar el PDS en el agente o el Tivoli Enterprise Monitoring Server z/OS. Ofrece la posibilidad de registrar y recuperar datos relacionales tabulares durante 24 horas al día mientras se mantienen índices sobre los datos registrados.

Consulte “Configurar el almacén de datos permanentes” in *Configuración de Tivoli Enterprise Monitoring Server en z/OS* para ver instrucciones sobre cómo configurar el almacén de datos permanentes.

Capítulo 18. Tivoli Common Reporting

Los temas de Tivoli Common Reporting tienen información exclusiva de los productos que se ejecutan en Tivoli Enterprise Portal y utilizan Tivoli Data Warehouse como el origen de los datos históricos para generar informes. Esta información va dirigida al administrador que configura Tivoli Common Reporting e instala los paquetes de informes para los usuarios.

Visión general de la Tivoli Common Reporting

La herramienta Tivoli Common Reporting es una característica de generación de informes a disposición de los usuarios de productos Tivoli. Utilice Tivoli Common Reporting para obtener, analizar y notificar tendencias importantes en el entorno gestionado de forma coherente e integrada.

Se proporciona un conjunto de informes predefinidos para los agentes de SO de Tivoli Monitoring y otros productos para supervisar recursos individuales, múltiples y empresariales.

Consumidores de Tivoli Common Reporting

- El programador de sistemas de red que soluciona los problemas de TCP/IP
- El analista de aplicaciones o el gestor de documentación
- El gestor de TI o el asesor de nivel de servicio que valida los acuerdos de nivel de servicio
- El planificador de capacidad
- El gestor de servicios
- El administrador del sistema
- El administrador del almacenamiento

Componentes de Tivoli Common Reporting

Tivoli Common Reporting consta de varios componentes:

- Un *almacén de datos* para almacenar y organizar los diseños de informes, informes y para dar soporte a recursos. El almacén de datos es una ubicación dentro de la infraestructura de Tivoli Common Reporting, en la que se gestionan y mantienen todos los archivos relacionados con informes y los informes.
- Una interfaz de usuario basada en la web para especificar los parámetros de los informes y otras propiedades que permiten generar informes con formato y visualizar los informes.
- Una interfaz de línea de mandatos para trabajar con objetos del almacén de datos y realizar funciones administrativas adicionales.
- *Paquetes de informes*, archivos de archivado que contienen informes, documentación, gráficos y bibliotecas de enlace dinámico.
  - Con el producto Tivoli Common Reporting se incluye un conjunto de informes de ejemplo. Otros conjuntos se pueden descargar e instalar utilizando la función de importar.
  - Dispone de un CD para la versión Cognos de los informes de agente de Tivoli Monitoring.

© Copyright IBM Corp. 2005, 2013

– Se incluyen paquetes de informes BIRT para ciertos agentes de supervisión como archivos .zip en el soporte de instalación del agente de Tivoli Monitoring en el directorio REPORTS/k*cp*, donde *cp* es el código de producto de dos caracteres. Los paquetes de informes están disponibles en IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary) para varios productos Tivoli Monitoring. Puede buscar en "Tivoli Common Reporting" los paquetes de informes en IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary).

Puede encontrar paquetes de informes adicionales generados por otros usuarios no de IBM, plantillas de informes empresariales y la publicación *Tivoli Common Reporting: Development and Style Guide* en Espacio IBM developerWorks Tivoli Common Reporting.

- Eclipse BIRT Report Designer, de código abierto, que puede utilizar para modificar informes o crear sus propios informes. Esta herramienta se puede descargar de Espacio IBM developerWorks Tivoli Common Reporting.

Para obtener más información acerca de Tivoli Common Reporting, incluida la información acerca de cómo instalar y administrar Tivoli Common Reporting y crear informes, consulte el centro de información de Centro de información de IBM Tivoli Common Reporting (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html).

Requisitos previos para Tivoli Common Reporting

Estos son los componentes de requisito previo para instalar y ejecutar paquetes de Tivoli Common Reporting en productos de Tivoli Monitoring.

Para utilizar los informes, necesita los componentes siguientes:

- IBM Tivoli Monitoring
- Tivoli Common Reporting
  - IBM Tivoli Monitoring Versión 6.3 incluye Tivoli Common Reporting 3.1, que es un componente de Jazz for Service Management.
  - IBM Tivoli Monitoring Versión 6.2.3 incluye Tivoli Common Reporting 2.1.1.
  - IBM Tivoli Monitoring 6.2 Fixpack 2 incluye Tivoli Common Reporting for Asset and Performance Management Versión 1.3. Esta versión de Tivoli Common Reporting incluye Cognos Business Intelligence and Reporting Versión 8.4.

  Los informes para los agentes de sistema operativo de IBM Tivoli Monitoring Versión 6.3 se pueden instalar con Tivoli Common Reporting 3.1 ó 2.1.1. Para otros agentes de supervisión, consulte la guía del usuario del agente para determinar las versiones soportadas de Tivoli Common Reporting.

  Si no lo ha hecho, instale y configure Tivoli Common Reporting, utilizando la información que encontrará en Centro de información de IBM Tivoli Common Reporting (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html).

  Para asegurarse de que Tivoli Common Reporting se esté ejecutando, vaya a `http://`*`nombre_sistema`*`:`*`número_puerto`*`/ibm/console/`. El número de puerto predeterminado para http es 16310 y para https es 16311. La vía de acceso predeterminada al servidor es `/ibm/console`. Sin embargo, esta vía de acceso se puede configurar y puede diferir del valor predeterminado en el entorno.

Si ya tiene una versión anterior de Tivoli Common Reporting y ha instalado la versión más nueva en otro directorio, la asignación de puerto es diferente para evitar un conflicto.

- Paquetes de informes

  El producto puede tener un paquete de informes separado que se debe extraer. Consulte la guía del usuario del producto para ver instrucciones. Esto no se aplica a los informes del agente del sistema operativo, que se extraen como parte de su instalación.
- Los datos históricos almacenados en un producto de gestor de base de datos soportado por IBM Tivoli Monitoring Versión 6.2 Fixpack 1 o posterior.
- Los informes BIRT de esta guía son informes históricos, informes de los datos recopilados en Tivoli Data Warehouse 6,2 Fixpack 1 o posterior. Para obtener información sobre las bases de datos soportadas, consulte "Bases de datos soportadas para Tivoli Data Warehouse" en el manual *IBM Tivoli Monitoring: Guía de instalación y configuración*.
- Para el paquete de Cognos de los informes del agente de IBM Tivoli Monitoringconsulte la guía del usuario de su agente de supervisión, que describe cada informe. En concreto, contienen las vistas necesarias para cada informe. Si estas vistas no están presentes, puede que el informe no funcione. Para asegurar que las vistas necesarias estén presentes, ejecute la siguiente consulta en Tivoli Data Warehouse:
  - DB2

    ```
    select distinct "VIEWNAME" from SYSCAT.VIEWS where "VIEWNAME" like '%V'
    ```
  - Oracle

    ```
    select distinct "VIEW_NAME" from USER_VIEWS where "VIEW_NAME" like '%V'
    ```
  - MS SQL Server

    ```
    select distinct "NAME" from SYS.VIEWS where "NAME" like '%V'
    ```

Notas:

1. En Tivoli Common Reporting for Asset and Performance Management, los motores de informes BIRT y Cognos pueden coexistir.
2. Aunque no es necesario, puede instalar Eclipse BIRT Report Designer, Versión 2.2.1. Eclipse BIRT Report Designer, junto con la publicación *Tivoli Common Reporting: Development and Style Guide*, se puede utilizar para editar plantillas de informe o para crear informes nuevos.

Para ver los requisitos de software para ejecutar BIRT Report Designer y para descargarlo, consulte Business Intelligence and Reporting Tools en el sitio web de Eclipse o Espacio IBM developerWorks Tivoli Common Reporting. Descargue la guía de desarrollo y de estilo de Centro de información de IBM Tivoli Common Reporting (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html).

Actualización desde una versión anterior

Los informes del agente de supervisión del sistema operativo BIRT se continúan entregando en IBM Integrated Service Management Library (anteriormente OPAL). Para otros agentes de supervisión (que se han entregado previamente en OPAL y ejecutado bajo Tivoli Common Reporting V1.1.1) puede actualizar Tivoli Common Reporting a la Versión 1.3 o posterior, sin reinstalar los paquetes de informes que se han descargado desde IBM Integrated Service Management Library o desde el soporte del producto.

Los paquetes de informes BIRT están disponibles en IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary) para los agentes de supervisión de sistema operativo base. Dispone de un DVD para la versión de Cognos de los informes de agente de IBM Tivoli Monitoring. Descargue el paquete correspondiente a la versión de la infraestructura de Tivoli Management Services.

Tivoli Common Reporting Versión 1.1.1 se ejecutaba bajo Integrated Solutions Console y se instalaba en una ubicación diferente desde Tivoli Common Reporting Versión 1.2 y superior, que se ejecuta bajo Dashboard Application Services Hub y ahora se basa en dicho producto para dar soporte a la infraestructura. Las versiones 1.1.1 y 1.3 pueden coexistir en el mismo sistema o puede migrar los informes que ha descargado desde IBM Integrated Service Management Library a la Versión 1.3. No es necesario que vuelva a instalar los paquetes de informes. Existen dos opciones para migrar los informes desde la Versión 1.1.1 a la Versión 1.3:

- Durante la instalación de Tivoli Common Reporting Versión 1.3, el programa de instalación detecta si está instalada la Versión 1.1.1 y le pregunta si desea migrar estos informes. Conteste **Yes**.

  Nota: Si ha migrado el paquete de informes que ha descargado desde IBM Integrated Service Management Library a Tivoli Common Reporting Versión 1.3, asegúrese de que los informes previamente instalados se sobrescriben. Cuando importe el paquete de informes, pulse en **Advanced Options** en el recuadro de texto **Import Report Package** y seleccione **Overwrite**.
- Migre los paquetes de informes de forma manual.

Estas dos opciones se describen en la Versión 1.3 *Tivoli Common Reporting User's Guide*.

Nota: Tivoli Common Reporting proporciona una mayor seguridad que le permite asignar una cadena de seguridad a los enlaces de hipertexto de un informe. La publicación *Tivoli Common Reporting User's Guide* proporciona instrucciones para especificar un conjunto de seguridad.

Limitaciones

En esta sección se describen las limitaciones de los informes que genera Tivoli Common Reporting.

- Los informes de Cognos del agente de Tivoli Monitoring están codificados para conectar con una conexión de datos en Tivoli Common Reporting con el nombre "TDW".
- Los informes del agente de Tivoli Monitoring se ejecutan sobre Tivoli Data Warehouse. DB2 limita la longitud de las columnas a 30 caracteres. Dado que Tivoli Data Warehouse utiliza nombre de grupos de atributos como cabeceras de columna, los nombres de atributos con más de 30 caracteres en DB2 Tivoli Data Warehouse se sustituyen por el nombre de columna interno, el nombre de base de datos abreviado para el atributo (por ejemplo, CPU_UTIL o DISK_UTIL en lugar de Utilización de CPU o Utilización de disco).
- Los informes que cubren un largo período de tiempo o que tiene un atributo que requiere muchos procesos pueden provocar un desbordamiento aritmético SQL.
- Algunos de los informes no dan soporte a la definición opcional del Summarization and Pruning agent de Tivoli Data Warehouse de horas de turnos. Los clientes pueden utilizar el soporte de horas de turno para marcar con distintivos los datos recopilados como correspondientes a períodos de horas de

turno de máxima actividad o fuera de horas de turno de máxima actividad. No obstante, algunos informes incluyen todos los datos recopilados entre las horas de inicio y fin de informes seleccionadas por el cliente, si estos datos se han recopilado durante los períodos de horas de turno de máxima actividad o fuera de horas de turno de máxima actividad. Consulte "Acerca del Summarization and Pruning agent" en la página 507 y "Cambio de los valores de configuración globales" en la página 514.

- Si la configuración de horas de turno del Summarization and Pruning agent se modifica, se utiliza la configuración más reciente para los informes. Si especifica un rango de fechas para un informe de disponibilidad de abarca varias configuraciones, puede que las medidas de disponibilidad sean incorrectas. Por ejemplo, si ha editado las horas punta para añadir una hora, el resumen de horas punta y horas no punta es distinto antes y después de la hora a la que se ha reconfigurado el agente. Solo los rangos de horas antes o después de la reconfiguración son válidos y debe evitar especificar un rango de horas que abarque dos configuraciones.

Asegurarse de que se han habilitado los informes históricos

El primer paso para prepararse para ejecutar informes consiste en asegurarse de que los informes históricos estén habilitados.

Acerca de esta tarea

Los informes se ejecutan en datos históricos a largo plazo que se almacenan en Tivoli Data Warehouse. Para poder ejecutar informes, asegúrese de haber instalado los componentes necesarios y de haber configurado la recopilación de datos históricos:

Procedimiento

1. Instale y configure Tivoli Data Warehouse y los agentes de almacén: Warehouse Proxy agent y Summarization and Pruning agent, consulte *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm).
2. Configure la recopilación de datos históricos utilizando la característica Configuración de recopilación de datos históricos en Tivoli Enterprise Portal, consulte Configuración de la recopilación de datos históricos.

   Para agentes de supervisión basados en z/OS, configure el almacén de datos persistentes utilizando la herramienta de configuración, consulte "Configurar el almacén de datos permanentes" en *Configuración de Tivoli Enterprise Monitoring Server en z/OS* y consulte también *IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS Common Planning and Configuration* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm).
3. Opcionalmente, habilite el acceso a los datos resumidos en Tivoli Data Warehouse. El uso de datos resumidos en informes puede simplificar el análisis de los informes visualizados y mejorar el rendimiento de la generación de informes.

Qué hacer a continuación

Después de iniciar Tivoli Data Warehouse, los agentes de almacén y la recopilación de datos, deje pasar suficiente tiempo como para que Tivoli Data Warehouse guarde datos históricos para el periodo de tiempo del informe solicitado o la cantidad de datos adecuada para un informe resumido. Por ejemplo, si desea un

informe mensual, necesita al menos datos almacenados correspondientes a un mes.

Creación y mantenimiento de las tablas de dimensiones

La preparación de Tivoli Data Warehouse para Tivoli Common Reporting incluye la creación de las tablas de dimensiones, que son necesarias para la ejecución de informes de Cognos y la utilización de modelos de datos.

Hay dos formas de crear y mantener las tablas de dimensiones:

- "Utilización del Summarization and Pruning agent para mantener las tablas de dimensiones" en la página 543

  En IBM Tivoli Monitoring V6.3 o posterior, puede crear las tablas aprovechando el Summarization and Pruning agent.

  O BIEN
- "Creación y mantenimiento manual de las tablas de dimensiones" en la página 547

  Antes de IBM Tivoli Monitoring V6.3, tenía que crear y mantener las tablas de dimensiones manualmente. Si desea continuar actualizando manualmente la dimensión, esta opción sigue estando disponible.

Configuración de colección de datos históricos antes de comenzar

Primero debe configurar la colección de datos históricos.

Para crear la tabla de dimensiones de recursos, configure la colección de datos históricos para uno o varios de los siguientes grupos de atributos, en función del sistema operativo para el que esté obteniendo informes:

Tipo	Grupo de atributos	Tabla	Resumen
Linux	Dirección IP de Linux	Linux_IP_Address	Diario
UNIX	Dirección IP de UNIX	UNIX_IP_Address	Diario
Windows	Información del sistema	NT_Computer_Information	Diario
Agente de resumen y poda de almacén	Configuración de resumen de KSY	KSY_Summarization_Config_DV	Diario
IBM i	Información varia	i5OS_Miscellaneous	Diario

Puede configurar la recopilación de datos históricos en Tivoli Enterprise Portal o en la interfaz de línea de mandatos. El siguiente ejemplo muestra cómo se ha creado una recopilación histórica local para NT Computer Information y se ha distribuido desde la CLI:

```
tacmd login -s MyComputer -u MyUser -p MyPassword
tacmd tepslogin -s localhost -u sysadmin
tacmd histconfiguregroups -t knt -o "NT Computer Information" -m -d YQMWDH
  -p Y=2y,Q=2y,M=1y,W=1y,D=6m,H=14d,R=7d
tacmd histcreatecollection -t knt -o "NT Computer Information"
  -a "ComputerInformation" -c 15m -i 15m -l TEMA -e
 "Needed for resource dimension table for TCR."
tacmd histstartcollection -n TEMS_NAME -t "knt" -o "NT Computer Information"
```

Aviso: Cuando el sitio cambia el modelo de datos de IBM Tivoli Monitoring o los informes del agente del sistema operativo, el modelo de datos y los informes

actualizados dejan de recibir soporte. Además, estas actualizaciones se pueden perder si aplica mantenimiento a Tivoli Monitoring o mueve a un release siguiente.

Utilización del Summarization and Pruning agent para mantener las tablas de dimensiones

Summarization and Pruning agent puede configurarse para mantener las tablas de dimensiones que necesita Tivoli Common Reporting.

Hay dos grupos de tablas de dimensiones:

Tablas de dimensiones compartidas
Las tablas de dimensiones compartidas, TIME_DIMENSION, MONTH_LOOKUP y WEEKDAY_LOOKUP, son necesarias para Tivoli Common Reporting.

Estas tablas son creadas y actualizadas utilizando la herramienta de publicación de esquemas durante la tarea de "Creación de tablas de dimensiones utilizando la herramienta de publicación de esquemas" en la página 545.

Tablas de dimensiones de recursos
Las tablas de dimensiones de recursos son MANAGEDSYSTEM, MANAGEDSYSTEMLIST y MANAGEDSYSTEMLISTMEMBERS.

Estas tablas se crean de una de dos maneras:

- Mientras que Summarization and Pruning agent está detenido, utilizando la herramienta de publicación de esquemas durante la tarea de "Creación de tablas de dimensiones utilizando la herramienta de publicación de esquemas" en la página 545.

  O BIEN
- Iniciando Summarization and Pruning agent después de que se configura en la tarea de "Configuración del Summarization and Pruning agent para mantener las tablas de dimensiones".

El método recomendado es el siguiente:

1. Siga los pasos descritos en "Configuración del Summarization and Pruning agent para mantener las tablas de dimensiones".No reinicie el Summarization and Pruning agent después de la configuración.
2. Siga los pasos en "Creación de tablas de dimensiones utilizando la herramienta de publicación de esquemas" en la página 545 para utilizar la herramienta de publicación de esquemas en modalidad de actualización para generar el DDL necesario para crear tanto las tablas de dimensiones compartidas como las tablas de dimensiones de recursos y, a continuación, ejecutar los scripts generados.
3. Reinicie el Summarization and Pruning agent.

Atención: Si está ejecutando Summarization and Pruning agent en modalidad autónoma (`KSY_AUTONOMOUS=YES`), las tablas MANAGEDSYSTEMLIST y MANAGEDSYSTEMLISTMEMBERS no pueden ser mantenidas o creadas por Summarization and Pruning agent.

Configuración del Summarization and Pruning agent para mantener las tablas de dimensiones

Configure Summarization and Pruning agent para mantener las tablas de dimensiones.

Antes de empezar

- Debe tener IBM Tivoli Monitoring V6.3 o posterior.
- Complete esta tarea antes de que se ejecute ningún informe.
- Durante este procedimiento, la tabla MANAGEDSYSTEM se llena utilizando información de la tabla WAREHOUSETCRCONTROL. La tabla WAREHOUSETCRCONTROL se crea en el primer inicio del Summarization and Pruning agent mediante la utilización de la herramienta de publicación de esquemas tal como se documenta en "Creación de tablas de dimensiones utilizando la herramienta de publicación de esquemas" en la página 545, lo que suceda primero.

  Es la responsabilidad de cada agente de supervisión colocar entradas en la tabla WAREHOUSETCRCONTROL. El agente de supervisión puede utilizar scripts o pasos manuales para añadir sus entradas. Para obtener información detallada, consulte la guía del usuario del agente.

  Por ejemplo, el paquete de informes de agentes de SO llena la tabla WAREHOUSETCRCONTROL durante un paso de instalación. Esto significa que debe instalar el paquete de informes de agentes de SO antes de completar esta tarea.

Acerca de esta tarea

Esta tarea configura el Summarization and Pruning agent para mantener las tablas TIME_DIMENSION, MONTH_LOOKUP, WEEKDAY_LOOKUP y MANAGEDSYSTEM. Si las tablas ya existen, el Summarization and Pruning agent se asegura de que las tablas contienen todas las columnas necesarias y a continuación añade las columnas e índices que faltan. Si ya ha personalizado los datos de la tabla, los datos personalizados se mantienen.

Procedimiento

1. Abra el archivo de variables de entorno del Summarization and Pruning agent:

   Windows

   En el sistema donde está instalado el Summarization and Pruning agent, en la aplicación Manage Tivoli Enterprise Monitoring Services, pulse con el botón derecho del ratón en el agente y seleccione **Avanzado → Editar archivo ENV**.

   Linux UNIX

   En el sistema donde está instalado el Summarization and Pruning agent, cambie al directorio *install_dir*/config.

   Abra el archivo sy.ini en un editor de texto.
2. Configure las siguientes variables de entorno:
   - KSY_TRAM_ENABLE=Y

     Controla la funcionalidad de la característica. El valor predeterminado es N.
   - KSY_TRAM_TD_GRANULARITY=*minutos*

     El número de minutos que se insertan los datos en la tabla TIME_DIMENSION. El valor mínimo es 1. El valor predeterminado es 5.
   - KSY_TRAM_TD_INITIAL_LOAD=*meses*

     La cantidad de datos en meses que se cargará en la tabla TIME_DIMENSION cuando está vacía o se crea por primera vez. El valor mínimo es 1. El valor predeterminado es 24 meses.
3. Guarde el archivo.
4. Reinicie el Summarization and Pruning agent.

Resultados

Ahora las tablas de dimensiones las mantiene el Summarization and Pruning agent.

Las tablas siguientes se crean en Tivoli Data Warehouse y le permiten crear informes y consultas basándose en los grupos de sistemas gestionados:

- MANAGEDSYSTEMLIST: Contiene el nombre, el producto y la descripción (que está en blanco de forma predeterminada y se puede personalizar) para el grupo de sistemas gestionados en el servidor de supervisión.
- MANAGEDSYSTEMLISTMEMBERS: Contiene los sistemas gestionados que son miembro de un determinado grupo de sistemas gestionados como se define en la tabla MANAGEDSYSTEMLIST.

Summarization and Pruning agent sólo añade nuevos sistemas a la tabla MANAGEDSYSTEM. Esto significa que si ha personalizado datos, estos se conservan.

Qué hacer a continuación

Compruebe el contenido de las tablas y asegúrese de que tengan datos para el próximo mes. El Summarization and Pruning agent mantiene los datos de un mes antes del mes actual.

Creación de tablas de dimensiones utilizando la herramienta de publicación de esquemas

Utilice la herramienta de publicación de esquemas para crear las tablas de dimensiones que necesitan Tivoli Common Reporting y IBM Tivoli Monitoring.

Las siguientes tablas de dimensiones compartidas son creadas por esta tarea: TIME_DIMENSION, MONTH_LOOKUP y WEEKDAY_LOOKUP. Las siguientes tablas de dimensiones de recursos también son creadas por esta tarea: MANAGEDSYSTEM, MANAGEDSYSTEMLIST, MANAGEDSYSTEMLISTMEMBERS.

Antes de empezar

- Debe tener IBM Tivoli Monitoring V6.3 o posterior.
- Asegúrese de que las recopilaciones históricas y el resumen necesarios para la tabla MANAGEDSYSTEM estén habilitados para cada agente. Para obtener más información, consulte “Configuración de colección de datos históricos antes de comenzar” en la página 542 y la documentación del agente.
- Complete esta tarea antes de que se ejecute ningún informe.
- Debe ser un administrador de base de datos.
- Para usuarios de Oracle, se deben cumplir los requisitos siguientes:
  - El controlador JDBC debe estar en la versión 10.2.3.0 o posterior.
  - Debe crear el usuario IBM_TRAM. Puede crear el usuario mediante la interfaz de usuario de Oracle Enterprise Manager o mediante el siguiente mandato SQL Plus:

```
CREATE USER IBM_TRAM IDENTIFIED BY <password> [DEFAULT TABLESPACE
<deftbsp> TEMPORARY TABLESPACE <temptbsp>];
GRANT CONNECT, CREATE TABLE, CREATE SYNONYM, CREATE VIEW, CREATE
```

```
PROCEDURE TO IBM_TRAM;
GRANT UNLIMITED TABLESPACE TO IBM_TRAM;
GRANT CREATE SEQUENCE TO ITM_USER;
```

donde,

<*contraseña*> es la contraseña del usuario IBM_TRAM

<*deftbsp*> es el espacio de tabla predeterminado para el usuario IBM_TRAM

<*temptbsp*> es el espacio de tabla temporal para el usuario IBM_TRAM

[] indica una parte opcional de la sentencia

- Para Microsoft SQL Server, el esquema debe crearse. Puede crear el esquema a través de Microsoft SQL Management Studio o utilizando la sentencia SQL siguiente:

```
CREATE SCHEMA IBM_TRAM;
```

Acerca de esta tarea

Se da soporte a las siguientes modalidades de herramienta de publicación de esquemas:

- Instalada: Genera el DDL para todas las tablas de Tivoli Reporting and Analytics Model (TRAM) y llena las tablas WAREHOUSEID. Esta modalidad también crea las sentencias para las funciones necesarias, las vistas y los índices.
- Configurada: Genera el DDL para todas las tablas TRAM y llena las tablas WAREHOUSEID sólo para los grupos de atributos que tienen la recopilación de datos históricos y también el resumen configurado. Esta modalidad también crea las sentencias para las funciones necesarias, las vistas y los índices.
- Actualizada: Esta modalidad es el método recomendado. Genera el DDL para las tablas TRAM y llena las tablas WAREHOUSEID analizando las configuraciones actuales de resumen y recopilación de datos históricos y, a continuación, añadiendo atributos y grupos de atributos que no existen aún. Esta modalidad también crea las sentencias para las funciones necesarias, las vistas y los índices.

Para obtener información adicional sobre cómo ejecutar la herramienta de publicación de esquemas, consulte “Generating SQL for data warehouse tables” en la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración*.

Atención: El procedimiento siguiente utiliza la modalidad actualizada.

Procedimiento

1. Abra el archivo de respuestas:

   Windows *install_dir*\TMAITM6\tdwschema.rsp

   Linux UNIX *install_dir*/*arch*/bin/tdwschema.rsp
2. Configure las siguientes variables de entorno:
   - KSY_PRODUCT_SELECT = updated
   - KSY_TABLE_FILTER = TIME_DIMENSION,MONTH_LOOKUP,WEEKDAY_LOOKUP
   - KSY_SQL_OUTPUT_FILE_PATH = *optional file path for SQL output*
3. Asegúrese de que se haya iniciado el Tivoli Enterprise Portal Server.
4. Ejecute el script de la herramienta de publicación de esquemas:

   Windows `tdwschema -rspfile tdwschema.rsp`

Linux UNIX `tdwschema.sh -rspfile tdwschema.rsp`

Los archivos SQL de los productos especificados en el archivo de respuestas se generan y graban en el directorio indicado por la palabra clave KSY_SQL_OUTPUT_FILE_PATH, o en el directorio de trabajo actual, si no se especifica ningún directorio de salida.

5. Ejecute los siguientes scripts en el orden en el que aparecen en la lista.
   - Si utiliza Oracle o Microsoft SQL Server, ejecute los scripts como usuario TRAM `IBM_TRAM`.
   - Si utiliza DB2 en Linux, UNIX y Windows o DB2 en z/OS, ejecute los scripts como un usuario que tiene acceso de administrador a la base de datos de Tivoli Data Warehouse.

```
tdw_schema_table.sql
tdw_schema_index.sql
tdw_schema_view.sql
tdw_schema_function.sql
tdw_schema_insert.sql
```

Ejemplo en DB2:

```
db2 -tvf tdw_schema_table.sql
db2 -tvf tdw_schema_index.sql
db2 -tvf tdw_schema_view.sql
db2 -td# -f tdw_schema_function.sql
db2 -tvf tdw_schema_insert.sql
```

Ejemplo en MSSQL:

```
osql -S <SQL server> -U <user ID> -P <password> -d <database name>
  -I -i tdw_schema_table.sql
osql -S <SQL server> -U <user ID> -P <password> -d <database name>
  -I -i tdw_schema_index.sql
osql -S <SQL server> -U <user ID> -P <password> -d <database name>
  -I -i tdw_schema_view.sql
osql -S <SQL server> -U <user ID> -P <password> -d <database name>
  -I -i tdw_schema_function.sql
osql -S <SQL server> -U <user ID> -P <password> -d <database name>
 -I -i tdw_schema_insert.sql
```

Ejemplo en Oracle:

```
sqlplus <ID de usuario>/<contraseña>@<SID de base de datos TDW> @tdw_schema_table.sql
sqlplus <ID de usuario>/<contraseña>@<SID de base de datos TDW> @tdw_schema_index.sql
sqlplus <ID de usuario>/<contraseña>@<SID de base de datos TDW> @tdw_schema_view.sql
sqlplus <ID de usuario>/<contraseña>@<SID de base de datos TDW> @tdw_schema_function.sql
sqlplus <ID de usuario>/<contraseña>@<SID de base de datos TDW> @tdw_schema_insert.sql
```

Atención: Debe ejecutar los scripts en el orden listado o fallarán.

Resultados

Ahora se crean las tablas de dimensiones.

Qué hacer a continuación

Si ha recibido errores al ejecutar el script tdw_schema_insert.sql, consulte *IBM Tivoli Monitoring: Guía de resolución de problemas*.

Creación y mantenimiento manual de las tablas de dimensiones

Puede crear las tablas de dimensiones creándolas y manteniéndolas manualmente mediante scripts de base de datos.

Creación de tablas de dimensiones compartidas y relleno de la tabla de dimensiones de tiempo

La preparación de Tivoli Data Warehouse para Tivoli Common Reporting incluye la creación de las dimensiones de IBM_TRAM, que se necesitan para ejecutar los informes Cognos y para utilizar los modelos de datos.

Acerca de esta tarea

Este procedimiento crea las siguientes tablas de dimensiones:

Esquema de IBM_TRAM
TRAM indica Tivoli Reporting and Analytics Model, que es el modelo de datos común que utilizan los productos Tivoli.

Aviso: Cuando el sitio cambia el modelo de datos de IBM Tivoli Monitoring o los informes del agente del sistema operativo, el modelo de datos y los informes actualizados dejan de recibir soporte. Además, estas actualizaciones se pueden perder si aplica mantenimiento a Tivoli Monitoring o mueve a un release siguiente.

Tabla TIME_DIMENSION
Incluye años de datos dimensionales de tiempo y granularidad a un número especificado de minutos. Cada fila de esta tabla es una clave de minuto exclusiva con varias dimensiones relacionadas, como horas, día de la semana, día del mes y trimestre.

Tabla MONTH_LOOKUP
Globaliza los nombres de mes para la dimensión de tiempo.

Tabla WEEKDAY_LOOKUP
Globaliza los nombres de la semana para la dimensión de tiempo.

Otras dimensiones
Otras dimensiones compatibles con Tivoli Common Data Model, como ComputerSystem, BusinessService y SiteInfo.

Necesitará los scripts de base de datos incluidos en el paquete de informes extraído bajo el directorio `db_scripts`.

Si los informes se distribuyen con un instalador, los siguientes procedimientos manuales se pueden manejar automáticamente mediante el instalador de informes. Consulte la guía del usuario del agente para obtener información sobre la creación automática de TRAM.

Cuando instale varios paquetes de informes, los pasos siguientes solo se tienen que realizar una vez. Cuando instale varios paquetes de informes, se utilizan las mismas tablas TIME_DIMENSION. Si desea restablecer la granularidad o las horas de inicio y detención, puede repetir el procedimiento.

Procedimiento

- **IBM DB2**
  1. Copie los scripts de base de datos (archivos .db2) del paquete de informes en una ubicación que la que se puedan ejecutar sobre Tivoli Data Warehouse. Los scripts están en la rama db_scripts del directorio en el que se ha extraído el paquete de informes.
  2. Inicie una sesión como db2admin. El ID de usuario debe tener acceso de administrador para crear el esquema IBM_TRAM.

3. Conecte a la base de datos para la que desea crear tablas de dimensiones. Es su Tivoli Data Warehouse.

   ```
   db2 connect to WAREHOUS
   ```

4. Si tiene una versión más antigua de los scripts de base de datos ya instalada, borre la base de datos:

   ```
   db2 -tf clean.db2
   ```

5. Cree el esquema y las tablas:

   ```
   db2 -tf create_schema_IBM_TRAM.db2
   ```

   Cuando el mandato se haya ejecutado correctamente, se muestran varias tablas bajo IBM_TRAM: TIME_DIMENSION, MONTH_LOOKUP, WEEKDAY_LOOKUP, ComputerSystem, BusinessService, SiteInfo, etc.

6. Cree el procedimiento almacenado para generar la dimensión de tiempo:

   ```
   db2 -td@ -vf gen_time_dim_granularity_min.db2
   ```

7. Para llenar la tabla TIME_DIMENSION, llame al procedimiento almacenado de la dimensión de tiempo con fechas y granularidad para generar las indicaciones de fecha y hora. Puede generar un máximo de cinco años de tiempo o hacer que los datos se regeneren cada día.

   ```
   db2 "call IBM_TRAM.CREATE_TIME_DIMENSION('fecha_inicial',
   'fecha_final', granularidad_de_datos)"
   ```

   donde `fecha_inicial` y `fecha_final` tienen el formato AAAA-MM-DD-HH.MM.SS.MILSEC y `granularidad_de_datos` es la frecuencia en minutos. Por ejemplo, el siguiente mandato extrae datos del 1/1/2010 al 1/1/2015 con una granularidad de 60 minutos.

   ```
   db2 "call IBM_TRAM.CREATE_TIME_DIMENSION('2010-01-01-00.00.00.000000',
   '2015-01-01-00.00.00.000000', 60)"
   ```

   Consejo: Cuando llene la dimensión de tiempo, siga estas directrices:

   - Para ver datos anuales, debe especificar el primer día del año, tal como se muestra en el ejemplo anterior.
   - Especifique la fecha final en un futuro suficiente como para que los nuevos datos de entrada se puedan correlacionar y mostrar correctamente en los informes.
   - Una práctica recomendada consiste en utilizar un valor de granularidad de 60 minutos.

- **Microsoft SQL Server**
  1. Copie los scripts de base de datos (archivos .sql) del paquete de informes en una ubicación donde se pueden ejecutar sobre Tivoli Data Warehouse. Los scripts están en la rama db_scripts del directorio en el que se ha extraído el paquete de informes.
  2. Personalice los scripts proporcionados cambiando el nombre de base de datos predeterminado en la sentencia de uso (sustituya USE IBM_TRAM) si no coincide con el valor predeterminado. Si el nombre de Tivoli Data Warehouse es "warehouse", la sentencia es `USE warehouse`:
     a. Si tiene una versión más antigua de los scripts de base de datos ya instalada, borre la base de datos con el mandato **clean.sql**.
     b. Ejecute el mandato **createSchema.sql**.
     c. Ejecute el mandato **createProcedure.sql**.
     d. Ejecute el mandato **populateTimeDimension.sql**. Modifique también los parámetros de límites para la dimensión de tiempo y granularidad, por ejemplo.

```
@startDate    = '2010-01-01 00:00:00',
@endDate      = '2012-12-31 00:00:00',
@granularity  = 60,
```

Si el lunes debe ser el primer día de la semana, añada el cuarto parámetro igual a 1; de lo contrario, libere tres parámetros.

```
@weekday      = 7
```

3. Si tiene una versión más antigua de los scripts de base de datos ya instalada, borre la base de datos:

   `sqlcmd -i clean.sql [-U nombreusuario -P contraseña] [-S nombrehost]`

4. Ejecute los scripts en la línea de mandatos de MS SQL en este orden:

   `sqlcmd -i createSchema.sql [-U nombreusuario -P contraseña] [-S host]`

   `sqlcmd -i createProcedure.sql [-U nombreusuario -P contraseña] [-S host]`

   `sqlcmd -i populateTimeDimension.sql [-U nombreusuario -P contraseña] [-S host]`

- Instalación manual de **Oracle**
  1. Copie los scripts de base de datos (archivos .sql) del paquete de informes en una ubicación donde se pueden ejecutar sobre Tivoli Data Warehouse. Los scripts están en la rama db_scripts del directorio en el que se ha extraído el paquete de informes.
  2. Inicie una sesión de SQL *Plus si aún no se está ejecutando.
  3. Compruebe que dispone de acceso remoto como usuarios sys.
  4. Si tiene una versión más antigua de los scripts de base de datos ya instalada, borre la base de datos (el usuario sys debe llamar el procedimiento):

     `clean.sql`

  5. Siga uno de estos pasos:
     - Si puede acceder de forma remota como usuario sys, ejecute este mandato y especifique toda la información que necesita el script:

       `@MY_PATH\setup_IBM_TRAM.sql`

     - Si no puede acceder de forma remota como usuario sys, ejecute este mandato localmente y especifique toda la información que necesita el script:

       `@MY_PATH\local_setup_IBM_TRAM.sql`

- Instalación por lotes de **Oracle**
  1. Copie los scripts de base de datos (archivos .sql) del paquete de informes en una ubicación donde se pueden ejecutar sobre Tivoli Data Warehouse. Los scripts están en la rama db_scripts del directorio en el que se ha extraído el paquete de informes.
  2. Inicie una sesión de SQL *Plus si aún no se está ejecutando.
  3. Si tiene una versión más antigua de los scripts de base de datos ya instalada, borre la base de datos (el usuario sys debe llamar el procedimiento):

     `clean.sql`

  4. Cree el usuario IBM_TRAM (debe llamar a un usuario con derechos de sistema, como por ejemplo SYS/SYSTEM):

     `@MY_PATH\create_IBM_TRAM.sql TCR_PASS USER_TBSPC TEMPORARY_TBSPC`

     donde TCR_PASS es la contraseña del nuevo usuario, *USER_TBSPC* es el nombre de espacio de tabla de usuario predeterminado (debe existir) y *TEMPORARY_TBSPC* es el nombre de espacio de tabla temporal predeterminado (debe existir)

  5. Cree las tablas IBM_TRAM (el usuario IBM_TRAM creado en el paso anterior debe llamar el script):

```
@MY_PATH\create_schema.sql USER_TBSPC
```

donde *USER_TBSPC* es el nombre de espacio de tabla de usuario predeterminado (debe existir)

6. Otorgue privilegios al usuario, como ITMUSER (el usuario IBM_TRAM debe llamar el script):

```
@MY_PATH\grant_IBM_TRAM.sql USER
```

donde *USER* es el nombre del usuario al que se van a otorgar privilegios.

7. Cree el procedimiento (el usuario IBM_TRAM debe crear el script):

```
@MY_PATH\gen_time_dim_granularity_hr.sql
```

8. Cargue los datos de búsqueda (el usuario IBM_TRAM debe llamar el script):

```
@MY_PATH\populateLookup.sql
```

9. Genere la dimensión de tiempo (el usuario IBM_TRAM debe llamar el procedimiento):

```
@MY_PATH\populateTimeDimension.sql FechaInicial FechaFinal Granularidad
```

donde FechaInicial es la fecha inicial en el formato 'aaaa-mm-dd HH:MM', *FechaFinal* es la fecha final en el formato 'aaaa-mm-dd HH:MM' y *Granularidad* es el número de minutos. Ejemplo:

```
@MY_PATH\populateTimeDimension.sql '2010-01-01 00:00' '2012-
           12-31 00:00' '60'
```

Resultados

Las tablas de dimensiones compartidas y de dimensiones de tiempo están completas.

Resolución de problemas

Si los mandatos de DB2 fallan con el siguiente error:

```
UDA-SQL-0107 Se ha producido una excepción general durante la
operación       "prepare".[IBM][CLI Driver][DB2/NT64] SQL0551N "ITMUSER" no
tiene la autorización o privilegio necesario para realizar la operación
"SELECT" en el objeto "IBM_TRAM......
```

Ejecute los mandatos siguientes para resolver el problema:

1. Conéctese a Tivoli Data Warehouse como usuario con privilegios de DB2.
2. Emita los mandatos grant siguientes:

```
Grant select on IBM_TRAM."ComputerSystem" to ITMUSER
Grant select on IBM_TRAM.MONTH _LOOKUP to ITMUSER
Grant select on IBM_TRAM.TIMEZONE_ DIMENSION to ITMUSER
Grant select on IBM_TRAM.TIME_DIMENSION to ITMUSER
Grant select on IBM_TRAM.WEEKDAY_LOOKUP to ITMUSER
Grant execute on procedure IBM_TRAM.CREATE_TIME_DIMENSION to ITMUSER
```

Qué hacer a continuación

Cree y llene la tabla de dimensiones de recursos.

Cómo crear y rellenar la tabla de dimensiones de recursos

La preparación de Tivoli Data Warehouse para Tivoli Common Reporting incluye la creación y relleno de la tabla de dimensiones de recursos "ManagedSystem", que se necesita para ejecutar los informes Cognos y para utilizar los modelos de datos.

Antes de empezar

Primero debe configurar la colección de datos históricos. Para obtener más información, consulte "Configuración de colección de datos históricos antes de comenzar" en la página 542.

Acerca de esta tarea

Si el sitio ejecuta Tivoli Data Warehouse, cada vez que instale uno o varios agentes de supervisión debe actualizar la tabla ManagedSystem del almacén.

Importante: Los siguientes scripts utilizan esquemas de usuario codificados. Si utiliza otro esquema, debe sustituir cada instancia del esquema codificado por el usuario que especifique.

Procedimiento

- **IBM DB2**
  1. Inicie una sesión como **db2admin**. El ID de usuario debe tener acceso de administrador para crear la dimensión de recursos.
  2. Conecte a la base de datos para la que desea crear la tabla de dimensiones de recursos. Es su Tivoli Data Warehouse.

     ```
     db2 connect to WAREHOUS
     ```
  3. Si ha especificado un usuario distinto del predeterminado, ITMUSER, para conectar con el almacén, personalice los scripts proporcionados `gen_resources.db2`, `populate_resources.db2` y `populate_resources_zos.db2`, sustituyendo cada instancia del esquema "ITMUSER" por el usuario que ha especificado.
  4. Cree las tablas:

     ```
     db2 -tf gen_resources.db2
     ```

     Cuando el mandato se haya ejecutado correctamente, se muestra una nueva tabla bajo el esquema de ITMUSER: ManagedSystem.
     Nota: Si la tabla "ITMUSER.ManagedSystem" ya se ha creado, se muestra el siguiente mensaje cuando se ejecuta el script `gen_resources.db2`, que se puede pasar por alto: `DB21034E El mandato se ha procesado como una sentencia SQL porque no es un mandato válido del procesador de línea de mandatos. Durante el proceso de SQL ha devuelto: SQL0601N El nombre del objeto que se va a crear es idéntico al nombre existente "ITMUSER.MANAGEDSYSTEM" de tipo "TABLE". SQLSTATE=42710"`
  5. Cree el procedimiento almacenado para llenar la tabla ManagedSystem:

     ```
     db2 -td@ -vf populate_resources.db2
     ```
  6. Para llenar la tabla ManagedSystem, llame al procedimiento almacenado:

     ```
     db2 "call ITMUSER.POPULATE_OSAGENTS()"
     ```

     Nota: Si ha especificado un usuario distinto del predeterminado, sustituya `ITMUSER` por el usuario que ha especificado durante la configuración del almacén.

- **Microsoft SQL Server**
  1. Personalice los scripts proporcionados:
     a. En **create_table.sql**, cambie el nombre de la base de datos predeterminada en la sentencia use (sustituya USE WAREHOUS) si difiere del valor predeterminado.
     b. En **create_procedure.sql**, cambie el nombre de la base de datos predeterminada en la sentencia use (sustituya USE WAREHOUS) si difiere del valor predeterminado.
     c. En **populate_agents.sql**, cambie el nombre de la base de datos predeterminada en la sentencia use (sustituya USE WAREHOUS) si difiere del valor predeterminado.
  2. Ejecute los scripts en la línea de mandatos de MS SQL en este orden:

     ```
     sqlcmd -i create_table.sql [-U minombreusuario -P micontraseña] [-H mihost])
     sqlcmd -i create_procedure.sql [-U minombreusuario -P micontraseña] [-H mihost])
     sqlcmd -i populate_agents.sql [-U minombreusuario -P micontraseña] [-H mihost])
     ```

- Instalación manual de **Oracle**
  1. Inicie una sesión de SQL *Plus si aún no se está ejecutando.
  2. Ejecute este mandato (vía de acceso sin espacios) y especifique toda la información que necesita el script:

     ```
     @MY_PATH\setup_populate_agents.sql
     ```

- Instalación por lotes de **Oracle**
  1. Inicie una sesión de SQL *Plus si aún no se está ejecutando.
  2. Cree la tabla ITMUSER.ManagedSystem. El usuario de Tivoli Data Warehouse, que de forma predeterminada es ITMUSER, debe llamar al script. Si ha utilizado otro nombre, modifique el script para que aparezca el nombre correcto.

     ```
     @MY_PATH\create_table.sql USER_TBSPC
     ```

  3. Cree el procedimiento para llenar la tabla:

     ```
     @MY_PATH\create_procedure.sql
     ```

  4. Inicie el procedimiento para llenar la tabla ManagedSystem:

     ```
     begin
     POPULATE_OSAGENTS('ITMUSER');
     end;
     /
     ```

Resultados

La tabla de dimensiones de recursos está completa.

Qué hacer a continuación

Instale y ejecute informes de IBM Cognos.

Importación de informes mediante el instalador de informes

El instalador de informes sólo está disponible para determinados agentes que incluyen informes empaquetados con el instalador. Este método de instalación sólo se puede utilizar cuando está disponible.

Antes de empezar

El instalador de informes da soporte a Tivoli Common Reporting versiones 2.1 y posteriores. Si utiliza Tivoli Common Reporting versión 1.3, no se pueden instalar informes aunque sean compatibles porque el instalador de informes sólo funciona con Tivoli Common Reporting versiones 2.1 y posteriores.

Consulte la guía del usuario específica del agente para ver los pasos adicionales de la instalación y posibles elementos de resolución de problemas para el agente.

Para obtener más in formación sobre Tivoli Common Reporting, consulte Centro de información de IBM Tivoli Common Reporting.

Acerca de esta tarea

Utilice el procedimiento siguiente para importar informes empaquetados mediante el instalador de informes. Este procedimiento se puede utilizar en las versiones 6.2.3 o posteriores de los agentes del sistema operativo y los informes de TivoliPerformance Analyzer.

Procedimiento

- Utilizando la GUI:
  1. Desde el directorio `\osreports` del CD del producto, ejecute el mandato adecuado para su sistema operativo:

     Windows `setup_plataforma.exe`

     Linux UNIX `setup_plataforma.bin`

     Se abrirá la ventana del instalador.
  2. Elija su idioma y pulse **Aceptar**.
  3. En la página de bienvenida, pulse **Siguiente**.
  4. especifique el directorio de instalación de Tivoli Common Reporting, como por ejemplo `tipv2Components\TCRComponents`. (El directorio de instalación puede ser otro, como por ejemplo `tcr21Components`.) Puede utilizar la carpeta predeterminada o utilizar el botón **Elegir** para especificar la vía de acceso. Pulse en **Siguiente**.
  5. Elija los informes que desea instalar. Pulse en **Siguiente**.
  6. Escriba el nombre de usuario y la contraseña de Tivoli Common Reporting. Pulse en **Siguiente**.
  7. Para *cada* origen de datos y script de datos, especifique la información de configuración de orígenes de datos:
     - Si procede, en la ventana de configuración **Orígenes de datos Cognos**, escriba el nombre del usuario de la base de datos de Tivoli Data Warehouse, la contraseña, el tipo de base de datos y el nombre de la base de datos. Para DB2 u Oracle, escriba el nombre de la base de datos. Para SQL, escriba el nombre del origen de datos ODBC.
     - Si procede, en la ventana **Origen de datos BIRT** y en la ventana **Configurar scripts de datos** especifique la información de configuración:

       En el separador **Credenciales de usuario de JDBC**, escriba el nombre de usuario y la contraseña de la base de datos de Tivoli Data Warehouse que desea compartir durante la instalación. Marque el recuadro para saltarse ahora la definición del origen de datos.

       En el separador **Credenciales de base de datos JDBC**, elija el tipo de base de datos en la lista; luego especifique el URL de JDBC de la base

de datos y especifique los archivos del controlador JDBC. Utilice el botón **Examinar** para buscar los archivos JAR. Especifique la clase de JDBC del controlador. Marque el recuadro para saltarse ahora la definición del origen de datos.

Nota: Puede que se necesite más de un archivo JAR para un origen de datos. Para JDBC, los archivos de controlador especificado se copian automáticamente en un directorio de Tivoli Common Reporting desde el que se aprovechan para crear conexiones de base de datos para recopilar datos para informes.

Pulse en **Siguiente**.

8. Se muestra el resumen previo a la instalación. Léalo detenidamente para comprobar si la información es correcta. Si lo es, pulse **Instalar** o utilice el botón **Anterior** para cambiar cualquiera de los parámetros especificados anteriormente.
9. Se muestra una ventana con el progreso de la instalación.
10. Se muestra el informe posterior a la instalación. Compruebe si la instalación ha finalizado correctamente y pulse **Finalizar**.

- Utilizando la línea de mandatos:
  1. Ejecute el mandato `setup_<plataforma>.exe/.bin -i console`.
  2. Elija el idioma de instalación.
  3. Escriba la ubicación del directorio `TCRComponent`.
  4. Elija el tipo de informes que se va a instalar.
  5. Escriba el nombre de usuario y la contraseña de Tivoli Common Reporting.
  6. Configure los scripts de datos y el origen de datos. Puede que algunos paquetes de informes no tengan scripts de datos.
  7. Se proporciona un resumen de la instalación y, a continuación, pulse **Intro** para empezar la instalación.
- Utilizando la modalidad silenciosa:
  1. Cree el archivo de respuestas de instalación silenciosa y dele el nombre `silent_installer.properties`.
  2. Ejecute el mandato `setup_<plataforma>.exe/.bin -i silent -f <vía_acceso_a_archivo_respuestas>`.

Resultados

Los informes de agentes ya están instalados en el servidor de Tivoli Common Reporting.

Qué hacer a continuación

Ahora puede utilizar los informes para visualizar los datos de supervisión obtenidos por lo agentes de supervisión. Para obtener más información sobre cómo ejecutar, administrar y editar informes en Tivoli Common Reporting, consulte los temas Cómo trabajar con informes.

Consulte la guía del usuario específica del agente para obtener más información sobre informes.

Importación y ejecución de informes IBM Cognos

Debe crear y llenar las tablas de dimensiones Cognos y luego importar el paquete de informes para habilitar Tivoli Common Reporting para los agentes de supervisión.

Acerca de esta tarea

Si los informes están incluidos con el instalador de informes, consulte "Importación de informes mediante el instalador de informes" en la página 553.

Si los informes no están incluidos con el instalador de informes, consulte "Importación de informes a través de Dashboard Application Services Hub" en la página 558.

Para ver información detallada sobre la instalación de informes, consulte Centro de información de IBM Tivoli Common Reporting

Ejecución de una exploración de requisitos previos

El informe Explorador de requisitos previos de informes de agentes de SO proporcionado por el paquete de informes de agentes de SO le permite comprobar los requisitos previos del sistema para utilizar la solución de creación de informes del agente de SO de IBM Tivoli Monitoring y Tivoli Common Reporting. Ejecute este informe de comprobación de estado para obtener una descripción general de los requisitos previos y verificar que las tablas de dimensiones compartidas, la tabla de dimensiones de tiempo y dimensiones de recursos de la tabla están disponibles.

Antes de empezar

Para que funcione este informe, debe definirse una conexión de origen de datos en Tivoli Common Reporting para conectar a Tivoli Data Warehouse.

Acerca de esta tarea

El informe de explorador de requisitos previos de informes de agentes de SO devuelve datos en las áreas siguients:

- Requisitos previos para Dimensiones compartidas de Tivoli Common Reporting
- Requisitos previos para Dimensiones compartidas de IBM Tivoli Monitoring
- Requisitos previos por informe

Si el sistema está correctamente configurado, las dimensiones compartidas se notificarán como satisfactorias. Si un conjunto de informes se devuelve como no satisfecho, puede descartarlo si corresponde a un conjunto de informes que no desea recopilar.

Limitación: Al utilizar creación de informes en su idioma nacional, algunas cadenas de texto se visualizan sólo en inglés.

Procedimiento

1. En el árbol de Navigator de Tivoli Common Reporting, seleccione Carpetas públicas → Informes de agentes de SO de IBM Tivoli Monitoring → Validación de requisitos previos → **Informes de explorador de requisitos previos de informes de agentes de SO**.

2. Seleccione entre los dos tipos de informe disponibles:
   - Mostrar todas las secciones: Esta opción muestra todas las secciones, incluyendo anómalas (requisitos previos no satisfechos) y satisfactorias (requisitos previos satisfechos).
   - Mostrar sólo secciones anómalas: Esta opción muestra sólo las secciones anómalas (requisitos previos no satisfechos).
3. Revise la información de informe devuelta. Realice las acciones necesarias para resolver los requisitos previos no satisfechos. Lea la información devuelta en las tablas **Descripción** y busque en las columnas **Estado** y **Detalles** en la información de resumen.

Qué hacer a continuación

Al visualizar el informe, en la columna **Detalles**, puede pulsar en para ver el informe **Detalles de tabla** para obtener información adicional.

Nota: Se puede acceder al informe **Detalles de tabla** pulsando el icono de la columna **Detalles**. Si intenta ejecutar el informe directamente desde Carpetas públicas → Informes de agentes de SO de IBM Tivoli Monitoring → Validación de requisitos previos → **Detalles de tabla**, recibirá un error.

Conexión a Tivoli Data Warehouse utilizando el cliente de base de datos mediante ODBC

Cognos utiliza ODBC para conectarse a la base de datos. Es importante instalar primero un cliente de base de datos en el servidor de Tivoli Common Reporting y conectarlo a Tivoli Data Warehouse. Si la base de datos y el servidor de Tivoli Common Reporting están en el mismo sistema, no se necesita ningún cliente de base de datos.

Procedimiento

- **IBM DB2**
  1. Asegúrese de haber desplegado un cliente de base de datos DB2 en el sistema en el que está instalado el motor de Tivoli Common Reporting basado en Cognos. El cliente debe tener la misma versión que la base de datos que utiliza Tivoli Data Warehouse.
     Linux UNIX Si hay un servidor DB2 instalado donde está instalado el motor de Tivoli Common Reporting basado en Cognos, los archivos del cliente de DB2 ya están disponibles. Sin embargo, tendrá que copiar el archivo de biblioteca de DB2 (libdb2.a) en el directorio *dir_instalación_Cognos_8*/bin para permitir que Cognos se conecte correctamente al servidor de bases de datos en el que reside Tivoli Data Warehouse.
  2. Conecte el cliente de base de datos de DB2 al servidor de bases de datos ejecutando el asistente de configuración de DB2, configurando el nombre de servicio de red local y reiniciando el sistema.
  3. Anote el nombre de la conexión que ha creado porque el instalador de informes lo utilizará en Tivoli Common Reporting.
- **Microsoft SQL Server**
  1. Asegúrese de haber desplegado el cliente de base de datos MS SQL en el sistema en el que está instalado el motor de Tivoli Common Reporting basado en Cognos.

2. Conecte el cliente de MS SQL al servidor de bases de datos ejecutando MS SQL Management Studio Express, configurando el nombre de servicio de red local y reiniciando el sistema.
3. Anote el nombre de la conexión que ha creado porque el instalador de informes lo utilizará en Tivoli Common Reporting.

- **Oracle**
  1. Asegúrese de haber desplegado el cliente de base de datos Oracle en el sistema en el que está instalado el motor de Tivoli Common Reporting basado en Cognos.
  2. Conecte el cliente de base de datos de Oracle al servidor de bases de datos ejecutando el asistente de configuración de red de Oracle, configurando el nombre de servicio de red loca y reiniciando el sistema.
  3. Anote el nombre de la conexión que ha creado porque el instalador de informes lo utilizará en Tivoli Common Reporting.

Resultados

Ahora puede importar y ejecutar informes.

Importación de informes a través de Dashboard Application Services Hub

Utilice la interfaz de usuario de Dashboard Application Services Hub para importar informes para los agentes de sistema operativo de Tivoli Monitoring.

Antes de empezar

Los modelos de informe del agente de supervisión se basan en IBM Cognos. Debe tener Tivoli Common Reporting V1.3 (con el motor Cognos) instalado y en ejecución en el sistema en el que instala los informes. También debe haber creado y llenado las tablas de dimensiones tal como se indica en "Creación de tablas de dimensiones compartidas y relleno de la tabla de dimensiones de tiempo" en la página 548 y "Cómo crear y rellenar la tabla de dimensiones de recursos" en la página 552, y conectado con el almacén de datos tal como se describe en "Conexión a Tivoli Data Warehouse utilizando el cliente de base de datos mediante ODBC" en la página 557.

Restricción: Este método de importación sólo se puede utilizar para informes Cognos.

Acerca de esta tarea

Debe obtener un paquete de informes con el que desee trabajar. Puede descargar paquetes de IBM Integrated Service Management Library, o puede crear uno utilizando la interfaz del administrador de contenido. Todos los paquetes que desea importan se deben almacenar en el directorio `TCR_component_dir\cognos\deployment`.

Procedimiento

1. Inicie la consola de administración de Dashboard Application Services Hub e inicie la sesión.
2. Vaya a **Common Reporting**.
3. En la ventana **Trabajar con informes** a la derecha, pulse **Administración** en la lista desplegable **Iniciar**.

4. Vaya al separador **Configuración** y abra la sección **Administración de contenido**.
5. Cree la importación de un nuevo paquete pulsando **Importar**, que abre un **Asistente para nueva importación**.
6. Siga el asistente para importar un nuevo paquete.

Resultados

Ahora los agentes de sistema operativo están instalado en el servidor de Tivoli Common Reporting.

Qué hacer a continuación

Ahora puede utilizar los informes para visualizar los datos de supervisión recopilados por los agentes de supervisión de sistema operativo. Para obtener más información sobre cómo ejecutar, administrar y editar informes de Cognos en Tivoli Common Reporting, consulte los temas Cómo trabajar con informes.

Consulte la guía del usuario del agente del sistema operativo para obtener más información sobre informes, como el Apéndice Tivoli Common Reporting en el manual *Windows OS Agent: Guía del usuario*.

Si encuentra algún problema al instalar el paquete de informes, consulte la publicación *IBM Tivoli Monitoring: Guía de resolución de problemas*.

Creación de un informe de Dashboard Application Services Hub

Puede crear un informe en Dashboard Application Services Hub.

Acerca de esta tarea

Utilice los pasos siguientes para crear un diagrama de Dashboard Application Services Hub:

Procedimiento

1. Inicie la sesión en Dashboard Application Services Hub como `tipadmin` o como usuario con el rol `chartAdministrator`.
2. Cree una nueva página seleccionado **Valores** > **Gestión de páginas** > **Nueva página**.
3. Seleccione el portlet de diagramas y pulse **Aceptar**.
4. Guarde la página y proporcione un nuevo nombre.
5. En el portlet de diagramas, seleccione **IBM Charts / Tivoli Charts**.
6. Para conectarse al Tivoli Enterprise Portal Server, consulte “Creación de una conexión al proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring” en la página 52.
7. Una vez que la conexión es satisfactoria, puede ver una lista de grupos similares a los espacios de trabajo de IBM Tivoli Monitoring. Para llenar una tabla, seleccione un grupo.
8. Seleccione un diagrama y pulse **Finalizar**. Se visualiza el diagrama.

Importación y ejecución de informes BIRT

Utilice Eclipse BIRT (Business Intelligence and Reporting Tools) Report Designer para desarrollar sus propios informes o editar informes existentes. Eclipse BIRT Report Designer no es necesario para descargar o instalar informes.

Importar un paquete de informes BIRT

Importe el paquete de informes para una aplicación supervisada para obtener los archivos necesarios para definir los informes BIRT.

Antes de empezar

Un *paquete de informes* es un archivo .zip que contiene todos los datos necesarios para definir uno o varios informes, incluidos los diseños y los recursos necesarios y la jerarquía de los conjuntos de informes que contendrán los informes. Los informes del agente de supervisión se incluyen como archivos .zip en la imagen del agente en el directorio REPORTS. Por ejemplo, en un sistema Windows, si la unidad de imagen tiene la etiqueta D:, los informes están en directorios como, por ejemplo, D:\REPORTS\kqb. Consulte el capítulo sobre generación de informes o la *Guía de generación de informes del producto* para obtener la ubicación de los informes.

Acerca de esta tarea

El distintivo del mandato **-import** para el mandato **trcmd** importa paquetes de informes BIRT y Cognos y diseños de informes. El tipo de paquete se reconoce automáticamente. Este mandato se puede utilizar para instalaciones únicas y para el motor de informes. No recibe soporte para otros casos.

Para obtener más información, consulte trcmd -import en el Centro de información de Tivoli Common Reporting.

Para Tivoli Common Reporting V2.1, utilice los siguientes procedimientos:

Procedimiento

1. Utilice la sintaxis para importar un paquete de informes:
   trcmd -import -bulk *pkgFile* [**-reportSetBase** *rsBase*] [**-resourceBase** *resourceBase*] [**-designBase** *designBase*] [**-help**]

   Este ejemplo importa un paquete BIRT llamado avail_skills.zip con su directorio de recursos importado desde C:\download:`trcmd -import -bulk C:\download\sth\report\avail_skills.zip -reportSetBase myReportSetBase -resourceBase myResourceBase -designBase myDesignBase -user tipadmin -password admin`
2. Utilice esta sintaxis para importar un diseño de informe y crear también un nuevo informe asociado al diseño:
   trcmd -import -design *designPath* [**-resourceDir** *resourcePath*] -**reportSetBase** *rsBase*

   Notas de uso:
   - Durante la importación de informes Cognos, los parámetros **-resourceBase**, **-designBase** y **-resourceDir** se pasan por alto.
   - Puede importar un solo informe Cognos desde un archivo .xml con el parámetro **-design**.

Resultados

El árbol de navegación muestra un elemento para los informes y los elementos para los subconjuntos de los informes.

Qué hacer a continuación

Si cambia el origen de datos de un informe cambiará los orígenes de datos para todos los informes. No será necesario que repita el cambio para todos los informes.

Referencia relacionada:

Centro de información de Tivoli Common Reporting - Importación de un paquete de informes
Importar paquete de informes > Descripción de opciones avanzadas.

Configurar el origen de datos

Todos los informes de un paquete de informes BIRT deben apuntar al mismo origen de datos. El puntero del origen de datos se ha de modificar de modo que apunte a Tivoli Data Warehouse.

Acerca de esta tarea

Después de instalar Tivoli Common Reporting e importar el primer conjunto de informes, el usuario con autorización de administrador debe copiar los controladores JDBC desde el gestor de bases de datos local o remoto que está utilizando para ejecutar Tivoli Data Warehouse en el directorio del servidor de Tivoli Common Reporting. Especifique estos archivos en la ventana **Editar origen de datos**. Realice los pasos siguientes para instalar estos controladores.

Procedimiento

1. Localice los archivos de controlador JDBC:

   db2jcc.jar y db2jcc.license_cu.jar de IBM DB2

   Windows `C:\Archivos de programa\IBM\SQLLIB\java`

   Linux UNIX *dirinstalación_db2*`/java`

   Por ejemplo, el directorio de instalación predeterminado de DB2 en estaciones de trabajo de la versión 9 es `/usr/opt/db2_09_01` en AIX y `/opt/IBM/db2/V9.1` en Linux y Solaris.

   Los controladores JDBC se encuentran generalmente en esta vía de instalación de DB2 en el directorio `java` de la vía de acceso alternativa que haya especificado para la instalación de DB2.

   También puede descargar el Controlador IBM DB2 para JDBC y SQLJ del sitio web de IBM.

   sqljdbc.jar de Microsoft SQL Server

   Descargue el Controlador JDBC de Microsoft SQL Server del sitio web de Microsoft. El nombre del archivo JAR de SQL Server 2005 JAR y su ubicación tras la instalación es *mssql2005installdir*`/sqljdbc_1.1/enu/sqljdbc.jar`.

   Oracle oraclethin.jar

   Obtenga el Controlador JDBC Tipo 4 del sitio web de Oracle. El nombre del archivo JAR del controlador JDBC de Oracle y su ubicación tras la instalación es *oracleinstalldir*`/jdbc/lib/oraclethin.jar`.

2. Copie el controlador JDBC al directorio de instalación de Tivoli Common Reporting:
   - *dir_instalación_tcr*TCR_component_dir\lib\birt-runtime-2_2_2\ReportEngine\plugins\org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206\drivers
   - Para un origen de datos DB2, copie los controladores JDBC de DB2 y el archivo JAR de licencia en la misma ubicación. Puede copiar el archivo db2jcc.jar y db2jcc_licence_cu.jar en el servidor DB2 desde la ubicación *dir_instalación_db2*/java (por ejemplo, C:\Archivos de programa\IBM\SQLLIB\java).
3. Ejecute el mandato **trcmd -modify** para configurar el origen de datos. Consulte el tema del mandato trcmd-modify en el Centro de información de Tivoli Common Reporting para obtener instrucciones completas.

Qué hacer a continuación

Para obtener información adicional, consulte la sección de controladores JDBC de la publicación *IBM Tivoli Common Reporting: Development and Style Guide* en Espacio IBM developerWorks Tivoli Common Reporting.

Para obtener más información sobre problemas de conectividad de Tivoli Data Warehouse, consulte la "Parte 5. Configuración del almacenamiento de datos" en el manual *IBM Tivoli Monitoring Installation and Setup Guide* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm).

Generar un informe BIRT de ejemplo

Los paquetes de informes BIRT de Tivoli Common Reporting están organizados por producto. Seleccione un conjunto de informes para generar un informe.

Procedimiento

1. Inicie un navegador compatible con Tivoli Common Reporting y especifique esta dirección: https://<dirección>:16311/ibm/console/logon.jsp, donde <dirección> es la dirección IP o nombre de host del sistema en el que está instalado Tivoli Common Reporting. Si el entorno se ha configurado con un número de puerto distinto del correspondiente al valor predeterminado, especifique ese número en su lugar. La vía de acceso predeterminada al servidor es /ibm/console. Sin embargo, esta vía de acceso se puede configurar y puede diferir del valor predeterminado en el entorno.
2. En el árbol de navegación de la izquierda, expanda el elemento **Informes**.
3. Pulse **Common Reporting**. Se muestran todos los informes disponibles (todos los paquetes de informes que ha importado) en el área de texto de la pantalla.
4. En el separador **Navegación**, expanda el elemento **Productos Tivoli**.
5. En la lista de productos disponibles, seleccione el producto Tivoli cuyos informes desea utilizar.
6. Si esta es la primera vez que ha ejecutado los informes basados en los datos de Tivoli Data Warehouse, realice los pasos siguientes:
   a. Defina Tivoli Data Warehouse como el origen de datos de sus informes; para obtener más información, consulte el apartado "Configurar el origen de datos" en la página 561. Para obtener información acerca de los orígenes de datos, consulte la publicación *IBM Tivoli Common Reporting User's Guide* o la ayuda en línea de Tivoli Common Reporting.

b. Copie los controladores JDBC necesarios desde el gestor de bases de datos local o remoto que está utilizando para ejecutar Tivoli Data Warehouse en el directorio del servidor de Tivoli Common Reporting.

Es posible que para poder iniciar el servidor de Tivoli Common Reporting deba aumentar el tamaño del almacenamiento dinámico predeterminado para la JVM (Java Virtual Machine) en el mandato Java para iniciar el servidor. Si ve estos mensajes cuando crea un informe, es posible que tenga que aumentar el tamaño del almacenamiento dinámico predeterminado:

```
El proceso ha finalizado debido a un error inesperado.
Consulte los archivos de registro de Tivoli Common Reporting para obtener más
información.
```

Consulte *OMEGAMON XE y Tivoli Management Services on z/OS: Informes para Tivoli Common Reporting* para obtener información sobre cómo aumentar el tamaño de almacenamiento dinámico predeterminado.

7. En la columna Acciones, pulse el icono de ejecución para el informe que desea iniciar y a continuación seleccione el tipo de formato de informe: HTML (valor predeterminado), PDF, Microsoft Word, Microsoft Excel o Adobe Postscript.

   Cuando seleccione un informe de Tivoli Common Reporting, se le presentará una ventana **Parámetros de informes** que le solicitará información que se utilizará para generar el informe. El título de la ventana de parámetros indica el tipo de informe que se generará. Para obtener una descripción de los tipos de informes, consulte la guía de usuario del agente o la guía de generación de informes del producto del agente o del producto con el que está trabajando.

   Una ventana Parámetros de informes contiene algunos campos que son comunes para todos los informes, por ejemplo, el intervalo de tiempo. Otros campos son específicos al agente que ejecuta los informes. Para la mayor parte de informes, se selecciona un período de tiempo, los recursos, el nivel de resumen de los datos y los atributos para el gráfico o pulse para aceptar todos los valores predeterminados que se muestran.
8. Pulse **Ejecutar** para generar un informe que coincide con las definiciones de parámetros.

Resultados

Se muestra un reloj mientras Tivoli Common Reporting recopila los datos de informes y crea la salida con formato. Cuando finaliza el proceso, el informe se muestra en Dashboard Application Services Hub.

Qué hacer a continuación

Si no se genera ningún informe o ve un mensaje que indica que los datos solicitados no están disponibles, consulte *IBM Tivoli Common Reporting Guía del usuario* para obtener información sobre cómo definir un origen de datos.

Si está visualizando un informe HTML o PDF, también puede pulsar cualquier enlace incorporado para abrir informes detallados. Si pulsa un enlace incorporado de detalle, el informe se volverá a enlazar consigo mismo con los parámetros recientes o con un informe secundario (detallado o de resumen). Los ejemplos de enlaces detallados incluyen pulsar una barra o diagrama de líneas o una cabecera de tabla.

Capítulo 19. Réplica de la base de datos del Tivoli Enterprise Portal Server

Utilice los programas de utilidad proporcionados con el Tivoli Enterprise Portal Server para migrar las personalizaciones de Tivoli Enterprise Portal que se almacenan en la base de datos de TEPS. Esto incluye ID de usuario, vistas de Navigator, consultas personalizadas, espacios de trabajo personalizados y scripts de terminal local.

También puede utilizar los scripts migrate-import y migrate-export para pasar de un Tivoli Enterprise Portal Server de 32 bits a un Tivoli Enterprise Portal Server de 64 bits en el mismo sistema operativo.

Visión general de la base de datos del Tivoli Enterprise Portal Server

Antes de replicar la base de datos del Tivoli Enterprise Portal Server, debe saber lo que contiene la base de datos y lo necesario antes de empezar.

Personalizaciones de Tivoli Enterprise Portal

Las personalizaciones de Tivoli Enterprise Portal se almacenan en el servidor de portal en la base de datos de TEPS. Esto incluye ID de usuario, vistas de Navigator, consultas personalizadas, espacios de trabajo personalizados y scripts de terminal local. No almacena situaciones, políticas ni grupos de sistemas gestionados.

Durante una actualización de instalación a una nueva versión del servidor de portal, la base de datos de TEPS se actualiza con las vistas de Navigator, consultas y espacios predefinidos nuevos o modificados. Las vistas, consultas y espacios de trabajo personalizados de Navigator que haya creado no se verán afectados.

La replicación de la base de datos de TEPS es necesaria para pasar de un entorno de prueba a un entorno de producción. También puede utilizar el procedimiento para hacer una copia de seguridad de la base de datos como medida de precaución antes de aplicar un fixpack o actualizar a una nueva versión.

Todos los espacios de trabajo creados anteriormente en el entorno de destino se sustituyen por los que se han creado en el entorno de origen. Los cambios de usuario existentes en el entorno de destino también se sustituyen.

Requisitos para la replicación

Antes de migrar el Tivoli Enterprise Portal Server, asegúrese de que el entorno cumpla estos requisitos:

- Los servidores de portal en los sistemas de origen y destino se deben configurar para que se conecten al mismo servidor de supervisión concentrador.
- Los servidores de portal en los sistemas de origen y de destino deben corresponder a la versión 6.2.1 o posterior e, idealmente, haberse instalado desde el mismo DVD de Tivoli Monitoring base.
- Los servidores de portal en los sistemas de origen y destino se deben instalar del mismo modo:

© Copyright IBM Corp. 2005, 2013

- Las aplicaciones seleccionadas son las mismas. Por ejemplo, si el servidor de portal de origen tiene soporte para UNIX, Windows Servers y aplicaciones MQ Series instaladas, el servidor de portal de destino debe tener el mismo soporte de aplicaciones.
- Se utiliza el mismo programa de base de datos para la base de datos del servidor de portal. Por ejemplo, IBM DB2 UDB.

CLI tacmds para la replicación selectiva

La interfaz de línea de mandatos tiene tacmds para exportar e importar objetos específicos de IBM Tivoli Monitoring. Consulte el manual *IBM Tivoli Monitoring: Consulta de mandatos* para ver una descripción de estos mandatos y su sintaxis.

tacmd exportworkspaces
tacmd importworkspaces
Copiar de forma selectiva espacios de trabajo de un servidor de portal a otro.

tacmd exportQueries
tacmd importQueries
Exportar consultas personalizadas a un archivo XML, luego importarlas en un servidor de portal.

tacmd bulkExportSit
tacmd bulkImportSit
Exportar todas las situaciones de empresa de Tivoli Monitoring de un servidor de supervisión concentrador e importarlas en otro.

tacmd bulkExportPcy
tacmd bulkImportPcy
Exportar todas las políticas de Tivoli Monitoring desde un servidor de supervisión concentrador e importarlas en otro. .

tacmd exportNavigator
tacmd importNavigator
Exportar vistas personalizadas de Navigator y sus espacios de trabajo, consultas y asociaciones de situaciones asignados a un archivo XML, luego importarlos en un servidor de portal.

tacmd exportSitAssociations
tacmd importSitAssociations
Exportar todas las asociaciones de situaciones de una vista de Navigator o de un determinado elemento de Navigator a un archivo XML, luego importarlas en un servidor de portal.

tacmd exportSysAssignments
tacmd importSysAssignments
Exportar todas las asignaciones de sistemas gestionados de una vista de Navigator o de un determinado elemento de Navigator a un archivo XML, luego importarlas en un servidor de portal.

Ejecución del script de migración-exportación

Exporte el servidor de Tivoli Enterprise Portal para crear una copia de la base de datos de TEPS para aplicarla a otro sistema o para guardarla como una copia de seguridad.

Antes de empezar

El servidor de portal se puede ejecutar o detener cuando inicia el script de migración-exportación. Si se detiene el servidor, el script lo inicia temporalmente en una modalidad limitada para llevar a cabo la exportación. No inicie manualmente el servidor del portal hasta que se haya completado la migración-exportación.

Acerca de esta tarea

En el sistema donde está instalado el Tivoli Enterprise Portal Server de origen, realice estos pasos para crear una copia de la base de datos de TEPS.

Procedimiento

- Windows
  1. Abra una ventana de indicador de mandatos: **Inicio→ Ejecutar** y entre `CMD`.
  2. Vaya al directorio *dir_instalación*`\CNPS`.
  3. Escriba: `migrate-export`

  El script de migración-exportación genera un archivo denominado **saveexport.sql** en el subdirectorio *dir_instalación*`\CNPS\sqllib`. Contiene todos los datos del servidor de Tivoli Enterprise Portal.
- Linux UNIX
  1. En el sistema de origen, abra una ventana de terminal.
  2. Vaya al subdirectorio bin de su instalación de IBM Tivoli Monitoring, por ejemplo: `cd /opt/IBM/ITM/bin`
  3. Escriba: `./itmcmd execute cq "runscript.sh migrate-export.sh"` Asegúrese de que utiliza el símbolo de comillas dobles y no el de comilla simple.

  El script de migración-exportación genera un archivo denominado **saveexport.sql** en el subdirectorio *dir_instalación*`/$platform/cq/sqllib` . Contiene todos los datos del servidor de Tivoli Enterprise Portal.

Ejecución del script de migración-importación

Cuando tenga una copia de la base de datos del servidor de Tivoli Enterprise Portal, con el nombre `saveexport.sql`, impórtela a cualquier instalación del servidor de portal de la misma versión donde desea valores duplicados.

En función del contenido del archivo saveexport.sql, este proceso puede sustituir por completo la base de datos TEPS existente.

Algunas de las tablas incluidas en el script de importación sólo son aplicables al servidor de CandleNet Portal, el predecesor del Tivoli Enterprise Portal Server. A no ser que no esté importando una base de datos del servidor de Tivoli Enterprise Portal, el archivo de registro de migración-importación contendrá errores de SQL acerca de un nombre sin definir, por ejemplo `SQLExecDirect rc=-1: SQL_ERROR SQLSTATE: 42S02, ERR: -204, MSG: [IBM][CLI Driver][DB2/LINUX] SQL0204N "ITMUSER.TAGGROBJ" es un nombre sin definir. SQLSTATE=42704 RC = -1` (también `ITMUSER.TMANOBJS`, `ITMUSER.TMANTMPL`, `ITMUSER.TTMPLSIT`, `ITMUSER.TTMPLSTA`, `ITMUSER.TSTUSERA`). Ignore estos errores.

Ejecución del script de migración-importación desde Windows de origen a Windows de destino

Ejecute el script de migración-importación para importar una copia de la base de datos del servidor de Tivoli Enterprise Portal desde un sistema Windows a otro sistema Windows.

Antes de empezar

Este procedimiento sobrescribe la base de datos de TEPS en el sistema de destino.

Acerca de esta tarea

En el sistema Windows donde está instalado el servidor de portal de destino, realice estos pasos para importar la base de datos TEPS que se ha copiado desde un sistema Windows utilizando el script de migración-exportación.

Procedimiento

1. Detenga el servidor de portal en el sistema de destino.
2. En el sistema de origen, abra un indicador de mandatos: pulse **Inicio** → **Ejecutar** y escriba `CMD`.
3. Copie el archivo **saveexport.sql** que se ha generado mediante el script de migración-exportación desde el sistema de origen a *dir_instalación*\CNPS\sqllib en el sistema de destino, donde *<unidad correlacionada en sistema destino>* es la unidad de disco del sistema de origen donde reside este archivo. Ejemplo:

   ```
   Copie <unidad correlacionada en sistema destino>:\IBM\ITM\CNPS\sqllib
        \saveexport.sql c:\ibm\itm\cnps\sqllib
   ```

   Si aún no se ha definido una unidad, es necesario correlacionar una unidad en el sistema de origen del sistema de destino con el mandato **net use**.
4. En el sistema de destino, vaya al directorio *dir_instalación*\CNPS y escriba: `migrate-import`. La ejecución del proceso de migración-exportación detiene el servidor de portal si está actualmente en ejecución.
5. Si está utilizando la función de migración-exportación para mover la base de datos de TEPS de un release a otro, realice esta tarea después de migrar la base de datos para añadir soporte de aplicaciones:
   a. Abra *<dir_instalación>*\CNPS\kfwalone en un editor de texto.
   b. Establezca `KFW_MIGRATE_FORCE=Y`, a continuación, guarde y cierre el archivo.
   c. Invoque este script para aplicar el soporte de aplicaciones del servidor del portal a la nueva base de datos TEPS recién migrada: *<dir_instalación>*\CNPS\buildpresentation.bat
6. Reiniciar el servidor de portal.

Ejecución del script de migración-importación desde Windows de origen a Linux o UNIX de destino

Ejecute el script de migración-importación para importar una copia de la base de datos del servidor de Tivoli Enterprise Portal desde un sistema Windows a otro sistema Linux o UNIX.

Antes de empezar

Este procedimiento sobrescribe la base de datos de TEPS en el sistema de destino.

Acerca de esta tarea

En el sistema Linux o UNIX donde está instalado el servidor de portal de destino, realice estos pasos para importar la base de datos TEPS que se ha copiado desde un sistema Windows utilizando el script de migración-exportación.

Procedimiento

1. Detenga el servidor de portal en el sistema de destino.
2. En el sistema de origen, abra un indicador de mandatos: pulse **Inicio → Ejecutar** y escriba `CMD`.
3. Copie el archivo **saveexport.sql** generado por el script migrate-export.bat del sistema Windows de origen en el directorio *dir_instalación*`/`*$platform*`/cq/sqllib` del sistema de destino, donde *$platform* es li6243 para Intel Linux o ls3263 para zSeries Linux en el sistema de destino.
4. Abra una ventana de terminal en el sistema de destino.
5. Vaya al subdirectorio bin de la instalación de Tivoli Monitoring: *dir_instalación*`/bin`. Por ejemplo:

   ```
   cd /opt/IBM/ITM/bin
   ```

6. En la ventana de terminal, escriba `./itmcmd execute cq "runscript.sh migrate-import.sh"`. Asegúrese de que utiliza el símbolo de comillas dobles y no el de comilla simple. El script procesa un archivo llamado **saveexport.sql** en el directorio *dir_instalación*`/`*$platform*`/cq/sqllib`. En función del contenido del archivo saveexport.sql, este proceso puede sustituir completamente los datos del servidor de portal existentes.
7. Si está utilizando la función de migración-exportación para mover la base de datos de TEPS de un release a otro, realice esta tarea después de migrar la base de datos para añadir soporte de aplicaciones:
   a. Abra *dir_instalación*`/cq/bin/lnxnocmsenv` en un editor de texto.
   b. Establezca `KFW_MIGRATE_FORCE=Y`, a continuación, guarde y cierre el archivo.
   c. Invoque este script para aplicar el soporte de aplicación del servidor de portal actual a la base de datos de TEPS recién migrada: *dir_instalación*`/bin/itmcmd execute cq InstallPresentation.sh`. Por ejemplo:

      ```
      /opt/IBM/ITM/bin/itmcmd execute cq InstallPresentation.sh
      ```

8. Reinicie el servidor de portal desde el directorio *dir_instalación*`/bin` con el siguiente mandato:

   ```
   ./itmcmd agent start cq
   ```

Ejecución del script de migración-importación desde Linux o UNIX de origen a Windows de destino

Ejecute el script de migración-importación para importar una copia de la base de datos del servidor de Tivoli Enterprise Portal desde un sistema Linux o UNIX a otro sistema Windows.

Antes de empezar

Este procedimiento sobrescribe la base de datos de TEPS en el sistema de destino.

Acerca de esta tarea

En el sistema Windows donde está instalado el servidor de portal de destino, realice estos pasos para importar la base de datos TEPS que se ha copiado desde

un sistema Linux o UNIX utilizando el script de migración-exportación.

Procedimiento

1. Detenga el servidor de portal en el sistema de destino.
2. Copie el archivo **saveexport.sql** que se ha generado mediante el script de migración-exportación desde el sistema Linux o UNIX de origen (/opt/IBM/ITM/$platform/cq/sqllib) a *dir_instalación*\CNPS\sqllib en el sistema de destino.
3. En el sistema de destino, vaya al directorio *dir_instalación*\CNPS y escriba: migrate-import. La ejecución del proceso de migración-exportación detiene el servidor de portal si está actualmente en ejecución.
4. Si está utilizando la función de migración-exportación para mover la base de datos de TEPS de un release a otro, realice esta tarea después de migrar la base de datos para añadir soporte de aplicaciones:
   a. Abra *<dir_instalación>*\CNPS\kfwalone en un editor de texto.
   b. Establezca KFW_MIGRATE_FORCE=Y, a continuación, guarde y cierre el archivo.
   c. Invoque este script para aplicar el soporte de aplicaciones del servidor del portal a la nueva base de datos TEPS recién migrada: *<dir_instalación>*\CNPS\buildpresentation.bat
5. Reiniciar el servidor de portal.
6. Reinicie el Tivoli Enterprise Portal Server.

Ejecución del script de migración-importación desde Linux o UNIX de origen a Linux o UNIX de destino

Ejecute el script de migración-importación para importar una copia de la base de datos del servidor de Tivoli Enterprise Portal desde un sistema Linux o UNIX a otro sistema Linux o UNIX.

Antes de empezar

Este procedimiento sobrescribe la base de datos de TEPS en el sistema de destino.

Acerca de esta tarea

En el sistema Linux o UNIX donde está instalado el servidor de portal de destino, realice estos pasos para importar la base de datos TEPS que se ha copiado desde otro sistema Linux o UNIX utilizando el script de migración-exportación.

Procedimiento

1. Detenga el servidor de portal en el sistema de destino.
2. Copie el archivo **saveexport.sql** que ha generado el script de migración-exportación del directorio *dir_instalación*/*$platform*/cq/sqllib del sistema Linux o UNIX de origen al mismo directorio en el sistema de destino, donde *dir_instalación* es el directorio de instalación en el sistema de destino, como por ejemplo /opt/IBM/ITM/, y *$platform* es el sistema operativo, como por ejemplo li6243 para Intel Linux o ls3263 para zSeries Linux.
3. Abra una ventana de terminal en el sistema de destino.
4. Vaya al subdirectorio bin de la instalación de Tivoli Monitoring: *dir_instalación*/bin. Por ejemplo:
   ```
   cd /opt/IBM/ITM/bin
   ```
5. En la ventana de terminal, especifique el siguiente mandato.

```
./itmcmd execute cq "runscript.sh migrate-import.sh"
```

Asegúrese de que utiliza el símbolo de comillas dobles y no el de comilla simple. El script procesa un archivo denominado saveexport.sql del subdirectorio IBM/ITM/$platform/cq/sqllib. En función del contenido del archivo saveexport.sql, este proceso puede sustituir completamente los datos del servidor de portal existentes.

6. Si está utilizando la función de migración-exportación para mover la base de datos de TEPS de un release a otro, realice esta tarea después de migrar la base de datos para añadir soporte de aplicaciones:
   a. Abra *dir_instalación*/cq/bin/lnxnocmsenv en un editor de texto.
   b. Establezca KFW_MIGRATE_FORCE=Y, a continuación, guarde y cierre el archivo.
   c. Invoque este script para aplicar el soporte de aplicación del servidor de portal actual a la base de datos de TEPS recién migrada: *dir_instalación*/bin/itmcmd execute cq InstallPresentation.sh. Por ejemplo:

      ```
      /opt/IBM/ITM/bin/itmcmd execute cq InstallPresentation.sh
      ```

7. Reinicie el servidor de portal desde el directorio *dir_instalación*/bin con el siguiente mandato:

   ```
   ./itmcmd agent start cq
   ```

Apéndice A. IBM Tivoli Monitoring Web Services para el servidor SOAP

En este apéndice se describe la característica IBM Tivoli Monitoring Web Services del servidor SOAP. La solución IBM Tivoli Monitoring Web Services le proporciona una interfaz abierta estándar de la industria en soluciones IBM Tivoli Monitoring. Esta interfaz abierta proporciona un acceso fácil a los datos de rendimiento y disponibilidad de Tivoli, y permite utilizar esta información para las posibilidades de automatización e integración.

IBM Tivoli Monitoring Web Services implementa una arquitectura de cliente/servidor. El cliente envía solicitudes de SOAP (Simple Object Access Protocol) al servidor SOAP que se instala con el servidor de supervisión concentrador. El servidor recibe y procesa las solicitudes SOAP del cliente.

Los métodos SOAP predefinidos le permiten realizar muchas funciones en el entorno supervisado. Puede empezar a utilizar los métodos SOAP inmediatamente. También puede utilizar estos métodos SOAP como plantillas al crear sus propios métodos avanzados.

SOAP funciona con cualquier lenguaje de programación o script, cualquier modelo de objeto y cualquier protocolo de cable de Internet. Los métodos SOAP de Tivoli se pueden invocar mediante PERL, Javascript, VBSCRIPT, JSCRIPT, C++, Java y mediante un navegador.

Nota: Web Services no da soporte a la creación de situaciones. Utilice el editor de situaciones de Tivoli Enterprise Portal o la función de CLI **tacmd createSit** para la creación de situaciones. El servidor SOAP sólo puede consultar atributos de sistema gestionado o de agente.

Acerca del cliente SOAP

SOAP (Simple Object Access Protocol - Protocolo de acceso a objetos simple) es un protocolo de comunicaciones basado en XML que permite a las aplicaciones intercambiar información mediante Internet.

SOAP es independiente de la plataforma y del idioma. SOAP utiliza XML para especificar una estructura de solicitudes y respuestas. Utiliza HTTP como mecanismo de transporte para dirigir la solicitud y recibir una respuesta.

Importante: Antes de utilizar la solución de IBM, debe tener unos conocimientos básicos de SOAP, de XML (Extensible Markup Language) y de los espacios de nombres XML, así como de WSDL (Web Services Description Language).

Configuración de Tivoli Monitoring Web Services (servidor SOAP)

De forma predeterminada, el servidor SOAP está instalado en el Tivoli Enterprise Monitoring Server concentrador. Consulte los temas siguientes para establecer las comunicaciones de servidor SOAP entre servidores de supervisión concentradores y para establecer la seguridad en el servidor SOAP.

© Copyright IBM Corp. 2005, 2013

Las instrucciones de este capítulo suponen que se tiene un conocimiento básico de SOAP, XML y espacios de nombres XML así como de Web Services Description Language (WSDL). Para configurar SOAP son necesarios estos pasos:

- Definir los concentradores con los que el servidor SOAP se comunica.
- Crear usuarios y otorgarles acceso.
- Verifique que ha configurado SOAP satisfactoriamente.

Nota: No puede realizar solicitudes SOAP a servidores SOAP de una versión anterior.

Definición de concentradores

En el siguiente procedimiento se describe cómo puede utilizar Manage Tivoli Enterprise Monitoring Services para activar el servidor SOAP y definir los concentradores con los que se comunica el servidor SOAP.

Acerca de esta tarea

Utilice los pasos siguientes para definir concentradores SOAP:

Procedimiento

1. En el sistema donde está instalado el servidor de supervisión concentrador, inicie Manage Tivoli Enterprise Monitoring Services:
   a. Windows Pulse **Inicio → Programas → IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services**.
   b. Linux o UNIX Vaya al directorio *install_dir*/bin y escriba: `./itmcmd manage`
2. Pulse con el botón derecho del ratón en el Tivoli Enterprise Monitoring Server y pulse en **Reconfigurar**.
3. Seleccione o deseleccione el campo ☐ **Seguridad: Validar usuario**.
4. Abra Manage Tivoli Enterprise Monitoring Services.
5. Pulse con el botón derecho del ratón en el **Tivoli Enterprise Monitoring Server**.
6. Pulse en **Avanzado → Configurar concentradores de servidor SOAP**.
7. Pulse **Añadir concentrador**. Aparecerá la ventana Especificación de concentrador.
8. Seleccione el protocolo de comunicaciones a utilizar con el menú **Protocolo**.
9. Especifique un nombre de alias en el campo **Alias** (por ejemplo: HUB2). Los nombres de alias pueden tener un mínimo de 3 caracteres y un máximo de 8 caracteres.
10. Siga uno de estos pasos:
    a. Si está utilizando comunicaciones TCP/IP o de conducto TCP/IP, complete los campos siguientes:

Tabla 67. Campos TCP/IP en diálogo de especificación de concentrador

Campo	Descripción
Nombre de host o dirección IP	Nombre de host o dirección TCP/IP del sistema host.
Puerto	Puerto de escucha TCP/IP para el sistema host.

    b. Si está utilizando comunicaciones SNA, complete los campos siguientes:

Tabla 68. Campos SNA en el diálogo de especificación de concentrador

Campo	Descripción
Nombre de red	Identificador de red SNA de sitio.
Nombre de LU	Nombre de LU para el servidor de supervisión. Este nombre de LU corresponde al alias de LU local del software de comunicaciones SNA.
LU6.2 LOGMODE	Nombre de la modalidad de registro LU6.2. Valor predeterminado: CANCTDCS.
Nombre de TP	Nombre de programa de transacción para el servidor de supervisión.

Nota: Si se está conectando a un servidor de supervisión remoto, la información de protocolo debe ser idéntica a la utilizada para el servidor de supervisión concentrador.

11. Pulse **Aceptar**. Se visualiza el árbol de servidor.

Añadir usuarios

Definición de usuarios en cada concentrador y especificación de los derechos de acceso para cada usuario (consulta o actualización).

Acerca de esta tarea

Siga el siguiente procedimiento para definir usuarios y especificar derechos de acceso:

Procedimiento

1. Seleccione el servidor (pulse en cualquier lugar en el árbol de servidor visualizado), si es necesario.
2. Bajo Añadir datos de usuario, escriba el nombre de usuario. Los ID de usuario deben ser idénticos a los especificados para supervisar la validación de inicio de sesión de servidor. El acceso está restringido sólo al servidor de supervisión al que un usuario tiene acceso.

   Nota: Si no proporciona un ID de usuario, se da permiso a todos los usuarios para actualizar datos.
3. Pulse el tipo de acceso de usuario: **Consulta** o **Actualización**.
4. Pulse en **Añadir usuario**. El árbol de servidor se actualiza, mostrando el usuario y el tipo de acceso.
5. Para suprimir un usuario: Seleccione el nombre de usuario en el árbol y pulse **Suprimir elemento**.
6. Para suprimir un concentrador: pulse en cualquier lugar dentro del árbol del concentrador y pulse en **Borrar árbol**.

Atención: Cuando la seguridad SOAP está habilitada, la **Consulta** del usuario y los permisos de **Actualización** controlan la autorización de los mandatos **tacmd** que envían solicitudes al servidor de supervisión concentrador y solicitudes de otros clientes SOAP. La variable de entorno SOAP_IS_SECURE del servidor de supervisión concentrador también debe estar establecida en YES si desea controlar qué usuarios pueden emitir solicitudes SOAP CT_EMail y CT_Export.

El permiso de consulta impide que el usuario realice operaciones de creación, actualización y supresión, y también mandatos **tacmd** para los mandatos de despliegue remoto y ejecución, como **executeaction** y **executecommand**.

El permiso de actualización otorga permiso para ejecutar todas las operaciones SOAP y se aplica a todos los mandatos de **tacmd** que envían solicitudes al servidor de supervisión concentrador, excepto los mandatos **tacmd getFile** y **tacmd putFile**. El permiso para ejecutar los mandatos **tacmd getFile** y **tacmd putFile** se controla mediante la variable de entorno KT1_TEMS_SECURE del servidor de supervisión concentrador. Para obtener más detalles sobre cómo habilitar el permiso para ejecutar estos dos mandatos, consulte *IBM Tivoli Monitoring: Consulta de mandatos*.

Configuración de IBM Tivoli Monitoring Web Services (SOAP Server) en sistemas UNIX y Linux

Configurar el servidor SOAP en sistemas UNIX y Linux.

Acerca de esta tarea

Utilice los pasos siguientes para definir concentradores SOAP en UNIX o Linux utilizando Manage Tivoli Enterprise Monitoring Services:

Procedimiento

1. Vaya al directorio *install_dir*/bin e inicie Manage Tivoli Enterprise Monitoring Services especificando el siguiente mandato:

   ```
   ./itmcmd manage
   ```

   Se muestra la ventana Manage Tivoli Enterprise Monitoring Services.
2. Pulse con el botón derecho del ratón en el **Tivoli Enterprise Monitoring Server** y seleccione **Configurar** en el menú emergente. Se visualiza la ventana Configurar TEMS.
3. Pulse **Guardar**. Se visualiza la ventana Configuración de concentradores de servidor SOAP. Si el host actual no se visualiza en el árbol de concentradores, defínalo antes de definir los concentradores con los que se comunica.
4. Confirme que el nombre de host o la dirección IP, el número de puerto y el protocolo para el servidor de supervisión concentrador sean correctos. Si no lo son, corríjalos. Si el nombre del concentrador local no aparece en el árbol, defina el concentrador local antes de definir los concentradores con los que él se comunica. El alias para el concentrador local siempre debe ser "SOAP".
5. Para añadir otro concentrador:
   a. Escriba el nombre o la dirección IP y el número de puerto del host en los campos apropiados.
   b. Especifique un nombre de alias en el campo **Alias**. Los nombres de alias pueden tener un mínimo de 3 caracteres y un máximo de 8 caracteres (por ejemplo HUB2).

c. Seleccione el protocolo de comunicaciones a utilizar con el concentrador en el menú **Transporte**.

6. Pulse **Añadir host**. Se visualiza el árbol de servidor, con el concentrador recién definido.

Ajuste del rendimiento de transacción SOAP en sistemas AIX

El rendimiento de transacción SOAP se puede modificar en AIX decidiendo si se deben o no permitir reconocimientos retardados. Ajuste el rendimiento siguiendo este procedimiento.

Acerca de esta tarea

El comportamiento predeterminado en sistemas AIX para conexiones TCP (Transmission Control Protocol) consiste en permitir reconocimientos retardados (paquetes de reconocimientos *Ack*) de hasta 200 ms, lo que se controla mediante la opción de red **tcp_nodelayack**. Este retardo permite combinar los paquetes con una respuesta y minimiza la carga general del sistema. Si establece **tcp_nodelayack** en **1**, el reconocimiento se devuelve inmediatamente al remitente. Con este valor, se genera una sobrecarga de sistema ligeramente superior pero el rendimiento de transferencia de red es mucho mayor cuando el remitente espera el reconocimiento del destinatario. Para ver más información sobre la opción **tcp_nodelayack**, consulte Centro de información de IBM System p y AIX.

Para establecer este parámetro, siga este procedimiento:

Procedimiento

Acceda a una cuenta de usuario que tenga privilegios **root** y emita el mandato siguiente:

```
no -p -o tcp_nodelayack=1
```

Resultados

La salida siguiente es habitual:

```
Setting tcp_nodelayack to 1
Setting tcp_nodelayack to 1 in nextboot file
```

Se trata de un cambio dinámico que entra en vigor inmediatamente. El distintivo **-p** hace que el cambio sea permanente, para que siga estando en vigor la siguiente vez que inicie el sistema operativo.

Habilitación de la seguridad SOAP

Cuando se habilita la opción **Seguridad: Validar usuarios** al configurar el servidor de supervisión concentrador, todas las solicitudes SOAP se autentican excepto las solicitudes de CT_EMail y CT_Export.

Para obtener información sobre cómo configurar el servidor de supervisión concentrador para validad los usuarios SOAP, consulte *IBM Tivoli Monitoring: Guía de instalación y configuración*. Si también desea autenticar los usuarios SOAP que están enviando solicitudes CT_Export o CT_EMail de SOAP, debe habilitar la variable de entorno `SOAP_IS_SECURE` en el servidor de supervisión concentrador.

Acerca de esta tarea

De forma predeterminada, la variable de entorno SOAP_IS_SECURE está inhabilitada. La habilitación de esta variable requiere que todos los usuarios que envían solicitudes CT_EMail y CT_Export conozcan una credencial del servidor de supervisión concentrador. El establecimiento de SOAP_IS_SECURE=YES solo funciona si la validación de usuarios está activada en el servidor de supervisión concentrador.

Procedimiento

1. En el sistema donde está instalado el servidor de supervisión concentrador, abra el archivo KBBENV o ms.ini:

   Windows

   Utilice Manage Tivoli Enterprise Monitoring Services (Inicio → Programas → IBM Tivoli Monitoring → Manage Tivoli Enterprise Monitoring Services) para editar archivos de entorno. Pulse con el botón derecho en el componente que desea modificar y pulse **Avanzado → Editar archivo ENV**. Debe reciclar el componente para implementar los cambios.

   Linux UNIX

   Edite directamente el archivo de entorno. Edite las variables de entorno en el archivo <*install_dir*>/config/ms.ini.
2. Localice la línea y elimine el comentario: # SOAP_IS_SECURE=YES. Por ejemplo: SOAP_IS_SECURE=YES
3. Guarde y cierre el archivo de entorno del servidor de supervisión.
4. Para Windows, debe reiniciar el componente para implementar los cambios. Para Linux o UNIX, debe reconfigurar y reiniciar el servidor de supervisión para implementar los cambios.

Utilización de IBM Tivoli Monitoring Web Services

Se incluyen varios métodos SOAP con IBM Tivoli Monitoring Web Services. Estos métodos permiten consultar y controlar los entornos de IBM Tivoli Monitoring dinámicamente.

Mediante estos métodos SOAP, puede:

- Detener o iniciar políticas y situaciones
- Reenviar mensajes con condiciones de excepción procedentes de System Automation for Integrated Operations Management y mostrarlos en una consola de Mensaje universal
- Recuperar datos de atributo que puede visualizar en gráficos o informes
- Abrir y cerrar sucesos
- Realizar solicitudes de datos en tiempo real
- Emitir solicitudes SOAP como mandatos de sistema en Tivoli Enterprise Portal

También puede utilizar este producto para probar una solicitud a fin de asegurar de que funciona correctamente. Entonces puede crear una política que someta varias solicitudes para procesarlas. Además, puede generar resúmenes de las operaciones diarias.

Puede almacenar en Tivoli Data Warehouse datos recuperados, como se describe en la guía de recopilación de datos históricos.

Nota: IBM Tivoli Monitoring Web Services proporciona filas de datos XML. Utilice los métodos SOAP de IBM en combinación con scripts propios para visualizar los datos en gráficos y tablas.

Puede parecer que las respuestas a las consultas SOAP aparecen ordenadas alfabéticamente, pero algunos atributos no siguen un orden alfabético. Las tareas de automatización deben examinar el contenido sin tener en cuenta el orden.

ID de usuario

En la instalación y configuración, se le solicitará que proporcione los ID de usuario para quienes necesitan acceder a los datos de servidor de supervisión. Si no se proporciona ningún ID de usuario, se da permiso a todos los usuarios para que actualicen datos.

Los ID de usuario deben ser idénticos a los especificados para supervisar la validación de inicio de sesión de servidor. El acceso está restringido sólo al servidor de supervisión al que un usuario tiene acceso.

También puede realizar cambios posteriormente para añadir o eliminar acceso de usuarios a los datos de servidor de supervisión. Consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* para obtener información detallada.

Inicio del cliente SOAP y realización de una solicitud

Inicie el cliente SOAP utilizando Internet Explorer o utilizando el programa de utilidad de línea de mandatos del cliente SOAP (no está disponible en sistemas z/OS).

Acerca de esta tarea

Cuando se utiliza el cliente SOAP conjuntamente con Internet Explorer para emitir solicitudes SOAP, puede modificar las etiquetas o el texto, si es necesario. En cambio, el programa de utilidad de línea de mandatos simplemente visualiza la salida de la solicitud en la línea de mandatos.

Nota: Para poder acceder a objetos de Universal Agent recién creados, se debe reciclar el servidor de supervisión concentrador donde se ejecuta el servidor SOAP. Consulte la publicación *IBM Tivoli Monitoring: Guía de instalación y configuración* para obtener instrucciones sobre cómo configurar el servidor de supervisión concentrador.

Uso del navegador

Utilice Windows Internet Explorer o Mozilla Firefox para escribir el URL de la consola de servicio SOAP.

Acerca de esta tarea

Después de instalar el cliente SOAP de Tivoli Monitoring Web Services, realice estas acciones:

Procedimiento

1. Inicie Internet Explorer versión 5 o posterior o Mozilla Firefox. Asegúrese de habilitar la opción **Acceder a orígenes de datos a través de dominios** en los valores de seguridad de Internet Explorer.

2. En el campo Dirección, escriba el URL del cliente SOAP, donde `localhost` se puede utilizar literalmente al acceder al servidor SOAP que se ejecuta en el mismo sistema o cambiar por el nombre de host apropiado o la dirección de red de un servidor SOAP que se ejecuta en un sistema diferente:
   `http://localhost:1920///cms/soap/kshsoap.htm`

   El número de puerto para el servicio HTTP es 1920.

   Nota: También puede direccionar solicitudes a un concentrador remoto sustituyendo **soap** en el campo Dirección por el nombre de alias del concentrador al que desea acceder (**HUB_localhost** en el ejemplo siguiente). El alias se tiene que haber definido anteriormente en el servidor SOAP (para obtener información sobre cómo definir alias de concentrador, consulte la documentación de instalación). Por ejemplo: `http://localhost:1920///cms/HUB_localhost/kshsoap.htm`
   Se visualiza la página HTML de cliente SOAP.
3. Seleccione un método SOAP en la lista del primer campo. Después de seleccionar un método, los demás campos se actualizan automáticamente.
4. Si es necesario, modifique las etiquetas o el texto del área "Edit Payload (XML)" (Editar carga útil).
5. Pulse **Make SOAP Request** (Realizar solicitud SOAP). La salida de la solicitud se visualiza en el área de carga útil de respuesta de SOAP (Your SOAP Response Payload).

Qué hacer a continuación

Al emitir una solicitud CT_Get para un tipo de agente determinado, el servidor de supervisión donde se ejecuta el servidor SOAP debe estar configurado y tener soporte de aplicación para ese tipo de agente. Por ejemplo, al emitir una solicitud CT_Get para un agente z/OS conectado a un servidor de supervisión z/OS, el servidor de supervisión que ejecuta el servidor SOAP debe estar configurado y tener el soporte de aplicaciones para dicho agente z/OS.

Utilización del programa de utilidad de línea de mandatos de cliente SOAP (kshsoap)

El programa de utilidad de línea de mandatos de cliente SOAP, kshsoap, es un cliente http. Emite solicitudes SOAP directas y muestra la información de salida en la línea de mandatos.

Acerca de esta tarea

Realice estos pasos para crear un archivo de solicitudes SOAP y un archivo receptor de URL de SOAP y para enviar la solicitud.

Procedimiento

- Windows
  1. En el sistema Tivoli Enterprise Monitoring Server donde está instalado el servidor SOAP, cambie al directorio *dir_instalación*\cms.
  2. Cree un archivo de texto con el nombre `SOAPREQ.txt` y escriba la siguiente solicitud SOAP:
     `<CT_Get><object>`*sistemagestionado*`</object></CT_Get>`

     o, si la seguridad está habilitada:

```
<CT_Get><userid>logonid</userid><password>password</password>
<object>ManagedSystem</object></CT_Get>
```

3. Cree otro archivo de texto con el nombre `URLS.txt` que contenga los URL para recibir la solicitud SOAP. En este ejemplo, `affiliatecompanylocalhost` es el nombre del sistema receptor y donde está instalado el servidor de supervisión concentrador: `http://affiliatecompanylocalhost:1920///cms/soap`.
4. En la línea de mandatos, escriba **kshsoap SOAPREQ.txt URLS.txt**

- Linux UNIX Ejecute el script kshsoap situado en el directorio *dir_instalación*/*interp*/ms/bin. Los valores de configuración del servidor de supervisión deben incorporarse en el shell actual antes de invocar al cliente kshsoap. Incorpore los valores especificando el siguiente mandato: . *install_dir*/config/*hostname*_ms_*temsname*.config. Para verificar este paso, puede utilizar el mandato ***env*** para mostrar sus variables de entorno y comparar las entradas de las mismas en el archivo .config.
- Al ejecutar el mandato **kshsoap** en sistemas que tienen instalado APPN, es posible que encuentre un mensaje de error que indique que es necesario configurar un archivo APPN. Para resolver esta situación, modifique la variable de entorno **KDE_WAPPC32** desde la ventana de línea de mandatos en la que va a ejecutar el mandato **kshsoap**:

```
SET KDE_WAPPC32=none
```

Resultados

El programa de utilidad kshsoap procesa el archivo SOAPREQ y visualiza el destino de URL y la solicitud. Envía la solicitud SOAP a cada URL listado en el archivo URLS y, a continuación, visualiza el URL y el mensaje de respuesta recibido.

Emisión de solicitudes SOAP como mandatos de sistema

Puede utilizar la característica Actuación en Tivoli Enterprise Portal para emitir solicitudes SOAP como mandatos de sistema en políticas o en situaciones.

Las solicitudes SOAP se almacenan en un archivo de texto. Para ver detalles, consulte los temas Especificación de una acción y Valores de acción en *Tivoli Enterprise Portal: Guía del usuario*.

El mandato soap es:

```
soap:CT_Execute,filename=SOAPREQ
```

donde:

CT_Execute es el nombre del método SOAP que le permite ejecutar una solicitud SOAP que se almacena en un archivo.

SOAPREQ es el nombre del archivo que ha creado que contiene la solicitud CT_EMail de SOAP

Por ejemplo, SOAPREQ puede contener:

```
<CT_EMail><server>n-smtpmta</server>
<sender>soap@ibm.com</sender>
<receiver>jane_brown@ibm.com</receiver>
<subject>AFDATA no tocado por personas</subject>
<attachmenttitle>AFData.htm</attachmenttitle>
<request><attach>res.pfx</attach></request>
<request id="XMLID">
<CT_Redirect endpoint="http://sp22.ibm.com:18882">
<SOAP-ENV:Envelope xmlns:SOAP-ENV=
```

```
  "http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" >
<SOAP-ENV:Body><AF_Execute><Exec>SOAP0002</Exec></AF_Execute></SOAP-ENV:Body>
  </SOAP-ENV:Envelope></CT_Redirect></request>
<request><attach>res.sfx</attach></request></CT_EMail>
```

Métodos de SOAP

Los métodos SOAP predefinidos se utilizan para componer solicitudes de invocación mediante PERL, Javascript, VBSCRIPT, JSCRIPT, C++, Java y mediante un navegador. Con cada método se muestra una lista de las etiquetas soportadas y ejemplos de uso. Aquí se describe cada método SOAP proporcionado por IBM y sus etiquetas soportadas.

CT_Acknowledge

Enviar un reconocimiento de suceso a la plataforma de IBM Tivoli Monitoring,

<name>
Nombre de la situación. Es necesario.

<source>
El origen del suceso (nombre de agente o nombre de servidor de supervisión). El reconocimiento se aplica a todos los orígenes activos de la alerta mencionada si no se proporciona el origen.

<data>
Si no se proporciona, se inserta "No se han proporcionado datos".

<item>
Elemento de visualización.

<userid>
Opcional. El ID de usuario para acceder al servidor de supervisión concentrador. Si no se proporciona, se inserta "nnn.nnn.nnn.nnn".

<password>
Opcional. La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión/concentrador.

<tipo> Opcional. Especifica el tipo de suceso. El valor puede ser "sampled" o "0", "pure" o "1" y "meta" o "2". Valor predeterminado: “**sampled**”

<hub>
Opcional. Especifica el nombre de alias de un concentrador remoto que se ha configurado en la lista de concentradores. La solicitud SOAP se direcciona a este concentrador.

<expire>
Opcional. Caduca el reconocimiento después del número de minutos entrados aquí.

Ejemplo:

```
<CT_Acknowledge>
  <hub>z/OSPROD</hub>
  <name>situation_from_CT</name>
  <source>CT_supported_system</source>
  <data>Jack is taking care of this failure</data>
  <item>subsystem</item>
  <userid>sysadmin</userid>
```

```
  <password>xxxxxxxx</password>
  <type>pure</type>
  <expire>60</expire>
</CT_Acknowledge>
```

CT_Activate

Iniciar una situación o una política que se ejecuta en la plataforma de IBM Tivoli Monitoring.

Nota: Las situaciones para agentes que se conectan a un Tivoli Enterprise Monitoring Server remoto no se pueden iniciar con este método.

<name>
Nombre de la situación. Es necesario.

<type>
El tipo de objeto que se está activando. Es necesario.

<userid>
Opcional. El ID de usuario para acceder al servidor de supervisión concentrador. Si no se proporciona, se inserta "nnn.nnn.nnn.nnn".

<password>
La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión/concentrador.

<hub>
Opcional. Especifica el nombre de alias de un concentrador remoto que se ha configurado en la lista de concentradores. La solicitud SOAP se direcciona a este concentrador.

Ejemplo:

```
<CT_Activate>
  <hub>z/OSPROD</hub>
  <name>name_of_situation_or_policy</name>
  <type> situation</type>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Activate>
```

CT_Alert

Enviar un suceso a la plataforma de IBM Tivoli Monitoring,

<name>
Nombre de la situación. Es necesario.

<source>
El origen del suceso (nombre de agente o nombre de servidor de supervisión). Esto es obligatorio.

<data>
Si no se proporciona ni se proporciona ninguna etiqueta object.attribute opcional, se inserta "No se han proporcionado datos".

<item>
Elemento de visualización.

<userid>
Opcional. El ID de usuario para acceder al servidor de supervisión concentrador. Si no se proporciona, se inserta "nnn.nnn.nnn.nnn".

<password>
Opcional. La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión/concentrador.

<tipo> Opcional. Especifica el tipo de suceso. El valor puede ser "sampled" o "0", "pure" o "1" y "meta" o "2". Valor predeterminado: "**sampled**"

<hub>
Opcional. Especifica el nombre de alias de un concentrador remoto que se ha configurado en la lista de concentradores. La solicitud SOAP se direcciona a este concentrador.

<data><object.attribute>
Devuelve el valor del atributo o de los atributos especificados en la vista de atributos iniciales del espacio de trabajo de resultados de suceso.

Ejemplo:

```
<CT_Alert>
  <hub>z/OSPROD</hub>
  <name>situation_from_XXX</name>
  <source>XXX_supported_system</source>
  <data><NT_Logical_Disk.Disk_Name>
C:</NT_Logical_Disk.Disk_Name></data>
  <item>subsystem</item>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Alert>
```

Nota: Cuando especifique object.attribute en la etiqueta data, quite los caracteres no alfanuméricos excepto el subrayado (_). Por ejemplo, NT_System. %_Total_Processor_Time se entrada como `NT_System.Total_Processor_Time`.

CT_Deactivate

Detener una situación o política en la plataforma de IBM Tivoli Monitoring.

Nota: Las situaciones para agentes que se conectan a un Tivoli Enterprise Monitoring Server remoto no se pueden detener con este método.

<name>
Nombre de la situación o de la política. Es necesario.

<tipo> El tipo de objeto (situación o política). Es necesario.

<userid>
El ID de usuario para acceder al servidor de supervisión concentrador. Si no se proporciona, se inserta "nnn.nnn.nnn.nnn".

<password>
La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión/concentrador.

<hub>
Opcional. Especifica el nombre de alias de un concentrador remoto que se ha configurado en la lista de concentradores. La solicitud SOAP se direcciona a este concentrador.

Ejemplo:

```
<CT_Deactivate>
  <hub>z/OSPROD</hub>
  <name>name_of_situation_or_policy</name>
  <type> situation</type>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Deactivate>
```

CT_EMail

Envíe la salida de otro método SOAP CT, por ejemplo CT_Get, utilizando correo electrónico mediante un servidor SMTP a una dirección de correo electrónico definida (no disponible en z/OS).

<server>
La dirección nombre/red del servidor smtp es obligatoria.

<sender>
La dirección de correo electrónico del remitente es obligatoria.

<receiver>
La dirección de correo electrónico del receptor es obligatoria.

<subject>
Opcional. Tema del correo electrónico.

<message>
Opcional. Mensaje del correo electrónico.

<attachmenttitle>
Opcional. Título de un documento adjunto.

<request>
Al especificar una solicitud de segundo nivel, por ejemplo CT_Get, se debe incluir cada subsolicitud en una etiqueta <request> </request>.

Opcional: Si se añade un elemento id=" " a la etiqueta <request> se genera un elemento <request id="XMLID"> que encierra la respuesta correspondiente para dicha subsolicitud.

Si la seguridad adicional está habilitada (SOAP_IS_SECURE=YES en las variables de entorno del servidor de supervisión), se requieren también las siguientes etiquetas:

<userid>
El ID de usuario para acceder al servidor de supervisión concentrador.

<password>
La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión.

Ejemplo:

```
<CT_EMail>
  <server>smtp.server</server>
  <sender>myemail@something.com </sender>
  <receiver>youremail@whatever.com </receiver>
  <subject>Estos son sus datos.</subject>
  <message>Datos de tabla suministrados como documento adjunto a continuación. Se presenta
  en formato csv para que se pueda utilizar en MS/Excel.</message>
```

```
  <attachmenttitle>tabledata.csv</attachmenttitle>
  <request id="XMLID">
    <CT_Get>
      <object>NT_Process </object>
      <target>TlPrimary:DCSQLSERVER:NT</target>
      <userid>sysadmin</userid>
      <password>xxxxxxxx</password>
    </CT_Get>
  </request>
</CT_EMail>
```

Ejemplo con seguridad adicional:

```
<CT_EMail>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
  <server>smtp.server</server>
  <sender>myemail@something.com </sender>
  <receiver>youremail@whatever.com </receiver>
  <subject>Estos son sus datos.</subject>
  <message>Datos de tabla suministrados como documento adjunto a continuación. Se presenta
  en formato csv para que se pueda utilizar en MS/Excel.</message>
  <attachmenttitle>tabledata.csv</attachmenttitle>
  <request id="XMLID">
    <CT_Get>
<userid>sysadmin</userid>
<password>xxxxxxxx</password>
<object>NT_Process </object>
<target>TlPrimary:DCSQLSERVER:NT</target>
</CT_Get>
  </request>
</CT_EMail>
```

Con la seguridad adicional, CT_EMail requiere el ID de usuario y la contraseña para la autorización. Si se especifica un CT_Get, se utilizan las mismas credenciales para emitir el CT_Get.

CT_Execute

Ejecuta la solicitud SOAP almacenada en un archivo.

<filename>
Especifica el nombre de archivo que contiene la solicitud SOAP que se debe ejecutar. El archivo debe residir en el directorio \html. En z/OS, debe encontrarse en RKANDATV. Es necesario.

Ejemplo:

```
<CT_Execute>
  <filename>execute1.xml</filename>
</CT_Execute>
```

CT_Export

Envíe la salida de otro método SOAP CT, por ejemplo, CT_Get, a un archivo definido (no disponible en z/OS).

<filename>
Nombre del archivo que debe contener los datos exportados. Es necesario.

Nota: Al insertar la etiqueta de nombre de archivo en un literal de cadena entrecomillada de determinados lenguajes de programación, por ejemplo C++, es necesario doblar las barras inclinadas invertidas.

En la etiqueta <filename>, puede añadir una variable de indicación de fecha/hora opcional. La variable está encerrada entre signos de dólar ($) y puede contener una combinación de aa/mm/dd/hh/mm/ss (para año/mes/día/horas/minutos/segundos). Los atributos de indicación de fecha y hora se pueden especificar en cualquier orden, excepto mm que debe ir precedido de aa o hh para identificarlo como mes (después del año) o minutos (después de las horas). Por ejemplo:

```
<filename>g:\exchange\excel\ntprocess$yymmdd$.htm</filename>
```

<warehouse/>
Especifica que los datos se deben exportar al almacén de datos de Tivoli Enterprise Portal mediante ODBC. <filename> y <warehouse/> son mutuamente excluyentes, pero se debe especificar uno de ellos.

<request>
Al especificar una solicitud de segundo nivel, por ejemplo CT_Get, se debe incluir cada subsolicitud en una etiqueta <request> </request>.

Opcional: Si se añade un elemento id=" " a la etiqueta <request> se genera un elemento <request id="XMLID"> que encierra la respuesta correspondiente para dicha subsolicitud.

Si la seguridad adicional está habilitada (SOAP_IS_SECURE=YES en las variables de entorno del servidor de supervisión), se requieren también las siguientes etiquetas:

<userid>
El ID de usuario para acceder al servidor de supervisión concentrador.

<password>
La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión.

Ejemplo:

```
<CT_Export>
  <filename>g:\exchange\excel\ntprocess$yymmddhhmmss$.htm</filename>
  <request>
    <attach>prefix.xsl</attach>
  </request>
  <request id="XMLID">
    <CT_Get>
      <object>NT_Process</object>
      <target>Primary:DCSQLSE RVER:NT</target>
      <userid>sysadmin</userid>
      <password>xxxxxxxx</password>
    </CT_Get>
  </request>
  <request>
    <attach>suffix.xsl</attach>
  </request>
</CT_Export>
```

Ejemplo con seguridad adicional:

```
<CT_Export>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
  <filename>g:\exchange\excel\ntprocess$yymmddhhmmss$.htm</filename>
  <request>
    <attach>prefix.xsl</attach>
  </request>
```

```
  <request id="XMLID">
    <CT_Get>
<userid>sysadmin</userid>
<password>xxxxxxxx</password>
<object>NT_Process</object>
<target>Primary:DCSQLSE RVER:NT</target>
</CT_Get>
  </request>
  <request>
    <attach>suffix.xsl</attach>
  </request>
</CT_Export>
```

Con la seguridad adicional, CT_Export requiere el ID de usuario y la contraseña para la autorización. Si se especifica un CT_Get, se utilizan las mismas credenciales para emitir el CT_Get.

CT_Get

Recibir un grupo de objetos XML o de objetos XML individuales de un agente de cualquier plataforma de IBM Tivoli Monitoring. Puede utilizarlo para obtener datos en tiempo real.

Importante: Al emitir una solicitud CT_Get en un tipo de agente determinado, el servidor de supervisión donde se ejecuta el servidor SOAP debe estar configurado e inicializado para ese tipo de agente.

<object>
Nombre del objeto que se debe recuperar. Necesario (de forma predeterminada, recupera todos los elementos públicos de un objeto).

<userid>
El ID de usuario para acceder al servidor de supervisión concentrador. Si no se proporciona, se inserta "nnn.nnn.nnn.nnn".

<password>
La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión/concentrador.

<target>
Nombre del agente.

Atención: Toma de forma predeterminada "*ALL". Recupera todos los destinos disponibles.

<history>
Y recupera datos históricos si están disponibles.

<results>
PARSE recupera los atributos de sucesos de historial de estado. Sólo es válido para el objeto Status_History. Múltiple: se puede especificar más de uno.

<attribute>
Nombre de atributo del objeto. Esta etiqueta se puede especificar varias veces.

<hub>
Especifica el nombre de alias de un concentrador remoto que se ha configurado en la lista de concentradores. La solicitud SOAP se direcciona a este concentrador.

<afilter>

Devuelve las filas que satisfacen los criterios de filtro, por ejemplo, atributo, operador, operadores de valor: EQ, NE, GE, GT, LE, LT, LIKE. Como los caracteres de patrón: * ' coincide con uno o muchos caracteres. Sólo se soporta para atributos de carácter. Sólo se soportan varios filtros como conjuntos, por ejemplo utilizando AND para unirlos.

Ejemplo:

```
<CT_Get>
  <hub>z/OSPROD</hub>
  <object>NT_System</object>
  <target>Primary:DCSQLSERVER:NT</target>
  <userid>sysadmin</userid>
  <password></password>
  <history>Y</history>
  <attribute>Server_Name</attribute>
  <attribute>Processor_Queue_Length</attribute>
  <afilter>Write_Time;GT;1020804</afilter>
  <afilter>Write_Time;LT;1020805</afilter>
</CT_Get>
```

Nota: Cuando especifique un atributo en las etiquetas de atributo (attribute), quite los caracteres no alfanuméricos excepto el subrayado (_). Por ejemplo, %_Total_User_Time se entra como `Total_User_Time`.

CT_Redirect

Redireccionar una solicitud SOAP a otro método SOAP registrado fuera del dominio de la plataforma de IBM Tivoli Monitoring.

<request endpoint=" ">

El valor de <request endpoint= " "> debe especificar el destino de la solicitud SOAP redirigida. El XML entero proporcionado como valor del elemento de solicitud se envía a dicho punto final. Cuando se especifica CT_Redirect en una solicitud de segundo nivel, por ejemplo, CT_Export, el atributo <endpoint=" "> *sólo* se especifica en el método CT_Redirect. Es necesario.

Ejemplo:

```
<CT_Redirect>
  <request endpoint= \"http://services.xmethods.net:80/soap/servlet/rpcrouter\">
    <SOAP-ENV:Envelope xmlns:SOAP-ENV=\"http://schemas.xmlsoap.org/soap/envelope/\">
      <SOAP-ENV:Body>
        <ns1:getTemp xmlns:ns1=\"urn:xmethods-Temperature\"SOAP-ENV:
        encodingStyle=\"http://schemas.xmlsoap.org/soap/encoding/\">
          <zipcode>93117</zipcode>
        </ns1:getTemp>
      </SOAP-ENV:Body>
    </SOAP-ENV:Envelope>
  </request>
</CT_Redirect>
```

CT_Reset

Enviar un restablecimiento de suceso (suceso cerrado) a la plataforma de IBM Tivoli Monitoring.

<name>

Nombre de la situación. Es necesario.

<source>
El origen del suceso (nombre de agente o nombre de servidor de supervisión). El restablecimiento se aplica a todos los orígenes activos de la alerta mencionada si no se proporciona el origen.

<item>
Elemento de visualización.

<userid>
Opcional. El ID de usuario para acceder al servidor de supervisión concentrador. Si no se proporciona, se inserta "nnn.nnn.nnn.nnn".

<password>
Opcional. La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión/concentrador.

<hub>
Opcional. Especifica el nombre de alias de un concentrador remoto que se ha configurado en la lista de concentradores. La solicitud SOAP se direcciona a este concentrador.

<tipo> Opcional. Especifica el tipo de suceso. El valor puede ser "sampled" o "0", "pure" o "1" y "meta" o "2". Valor predeterminado: "**sampled**"

Ejemplo:

```
<CT_Reset>
  <hub>z/OSPROD</hub>
  <name>situation_from_CT</name>
  <source>CT_supported_system</source>
  <item>subsystem</item>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Reset>
```

Nota: Los sucesos de muestra se pueden cerrar sólo si la situación se ha detenido o suprimido. Utilice la etiqueta <type> si CT_Reset cerrará un suceso puro.

CT_Resurface

Hacer que resurja un suceso de reconocimiento en la plataforma de IBM Tivoli Monitoring.

<name>
Nombre de la situación. Es necesario.

<source>
El origen del suceso (nombre de agente o nombre de servidor de supervisión). El resurgimiento se aplica a todos los orígenes activos de la alerta mencionada si no se proporciona el origen.

<item>
Elemento de visualización.

<userid>
Opcional. El ID de usuario para acceder al servidor de supervisión concentrador. Si no se proporciona, se inserta "nnn.nnn.nnn.nnn".

<password>
Opcional. La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión/concentrador.

<hub>
Opcional. Especifica el nombre de alias de un concentrador remoto que se ha configurado en la lista de concentradores. La solicitud SOAP se direcciona a este concentrador.

<tipo> Opcional. Especifica el tipo de suceso. El valor puede ser "sampled" o "0", "pure" o "1" y "meta" o "2". Valor predeterminado: "**sampled**"

Ejemplo:

```
<CT_Resurface>
  <hub>z/OSPROD</hub>
  <name>situation_from_CT</name>
  <source>CT_supported_system</source>
  <item>subsystem</item>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Resurface>
```

CT_WTO

Enviar un Mensaje universal a la plataforma de IBM Tivoli Monitoring.

<data>
El mensaje que se debe enviar. Es necesario.

<category>
Opcional. En blanco es el valor predeterminado.

<severity>
Opcional. En blanco es el valor predeterminado.

<userid>
Opcional. El ID de usuario para acceder al servidor de supervisión concentrador. Si no se proporciona, se inserta "nnn.nnn.nnn.nnn".

<password>
Opcional. La contraseña para acceder al servidor de supervisión concentrador. Necesario para la validación de inicio de sesión de servidor de supervisión/concentrador.

<hub>
Opcional. Especifica el nombre de alias de un concentrador remoto que se ha configurado en la lista de concentradores. La solicitud SOAP se direcciona a este concentrador.

Ejemplo:

```
<CT_WTO>
  <hub>z/OSPROD</hub>
  <data>This is Universal Message</data>
  <category>Critical Messages</category>
  <severity>High Severity</severity>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_WTO>
```

Emisión de solicitudes SOAP de segundo nivel

Algunos métodos SOAP de segundo nivel realizan una función determinada con los datos recuperados, utilizando métodos de nivel inferior incorporados. CT_EMail y CT_Export son métodos de segundo nivel que realizan esta función.

Éstos son los métodos de nivel inferior:

- <CT_Get>
- <CT_Redirect>
- <attach>
- <insert>

Las etiquetas **<CT_Get>** y **<CT_Redirect>** se utilizan como se describe en la "Métodos de SOAP" en la página 582. La etiqueta **<attach>** sirve para cargar un archivo. El archivo debe estar en el directorio *<install_dir>*\cms\html en Windows o *<install_dir>*/tables/HUB_Name/HTML en Linux y UNIX. No puede utilizar vías de acceso relativas en la etiqueta <attach>. La etiqueta **<insert>** le permite cargar el texto incorporado en la secuencia de datos (de salida) recuperada en un punto correspondiente a la posición en la solicitud XML.

El siguiente ejemplo muestra cómo se puede utilizar una solicitud de segundo nivel. Este XML crea el archivo tabledata.htm, escrito con los datos de prefix.xls. A continuación, se especifican datos incorporados mediante la etiqueta **<insert>** y se realiza una solicitud utilizando el mandato **<CT_Get>**. Tenga en cuenta que esta solicitud tiene un valor ID de "NTDATA", lo que da lugar a que la etiqueta de datos **<XML id="NTDATA">** se acomode alrededor de estos datos de solicitud en particular. El mandato **<CT_Redirect>** se utiliza para redirigir la solicitud a http://services.xmethods.net:80/soap/servlet/rpcrouter y se realiza una solicitud final para insertar los datos de suffix.xls en tabledata.htm.

```
<CT_Export>
  <filename>tabledata.htm</filename>
  <request>
    <attach>prefix.xls</attach>
  </request>
  <request>
    <insert>
    <insertelement>
      <insertdata>
        Estos datos se han insertado como complementos del servidor SOAP CT.
      </insertdata>
    </insertelement>
    </insert>
  </request>
  <request id="NTDATA">
    <CT_Get>
      <userid>sysadmin</userid>
      <password></password>
      <object>NT_System</object>
      <target>*ALL</target>
    </CT_Get>
  </request>
  <request>
    <CT_Redirect endpoint="http://services.xmethods.net:80/soap/servlet/rpcrouter">
      <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
        <SOAP-ENV:Body>
          <ns1:getTemp xmlns:ns1="urn:xmethods-Temperature" SOAP-
          ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
            <zipcode>93117</zipcode>
          </ns1:getTemp>
        </SOAP-ENV:Body>
      </SOAP-ENV:Envelope>
    </CT_Redirect>
  </request>
  <request>
    <attach>suffix.xls</attach>
  </request>
</CT_Export>
```

Solicitud CT_Get de SOAP de ejemplo

Esta es una solicitud **CT_Get** de SOAP de ejemplo sometida y la respuesta recibida.

Solicitud de SOAP enviada a punto final SOAP, http://esada.ibm.com:19221/SOAP

```
<?xml.version="1.0" encoding="UTF-8" standalone="no"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV=
"http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
   <CT_Get>
    <Object>NT_System</Object>
    <Source>Primary:ESADA:NT</Source>
   </CT_Get>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Respuesta de SOAP de punto final SOAP, http://esada.ibm.com:19221/SOAP

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV=
"http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body>
 <SOAP-CHK:Success xmlns:SOAP-CHK = "http://soaptest1/soaptest/">
 <PARMS> </PARMS>
 <TABLE name="KNT.WTSYSTEM">
  <OBJECT>NT_System</OBJECT>
  <DATA>
   <ROW>
     <Server_Name>Primary:ESADA:NT</Server_Name>
     <Timestamp >1011127123323391</Timestamp>
     <User_Name>SYSTEM</User_Name>
     <Operating_System_Type>Windows_NT</Operating_System_Type>
     <Operating_System_Version>4.0</Operating_System_Version>
     <Network_Address>10.21.2.154</Network_Address>
     <Number_of_Processors  dt:dt="number">1</Number_of_Processors>
     <Processor_Type dt:dt="number">586</Processor_Type>
     <Page_Size dt:dt="number">4096</Page_Size>
     <_Total_Privileged_Time dt:dt="number">1</_Total_Privileged_Time>
     <_Total_Processor_Time dt:dt="number">7</_Total_Processor_Time>
     <_Total_User_Time dt:dt="number">6</_Total_User_Time>
     <Context_Switches_Sec dt:dt="number">1745</Context_Switches_Sec>
     <File_Control_Bytes_Sec dt:dt="number">4500</File_Control_Bytes_Sec>
     <File_Control_Operations_Sec dt:dt="number">98
      </File_Control_Operations_Sec>
     <File_Data_Operations_Sec dt:dt="number">28
      </File_Data_Operations_Sec>
     <File_Read_Bytes_Sec dt:dt="number">800</File_Read_Bytes_Sec>
     <File_Read_Operations_Sec dt:dt="number">27
      </File_Read_Operations_Sec>
     <File_Write_Bytes_Sec dt:dt="number">9772</File_Write_Bytes_Sec>
     <File_Write_Operations_Sec dt:dt="number">1
      </File_Write_Operations_Sec>
     <Processor_Queue_Length dt:dt="number">0</Processor_Queue_Length>
     <System_Calls_Sec dt:dt="number">2368</System_Calls_Sec>
     <System_Up_Time dt:dt="number">956388</System_Up_Time>
     <Total_Interrupts_Sec dt:dt="number">1076</Total_Interrupts_Sec>
    </ROW>
   </DATA>
  </TABLE>
 </SOAP-CHK:Success>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Casos de ejemplo de IBM Tivoli Monitoring Web Services

A continuación se muestran unos ejemplos de cómo se puede utilizar IBM Tivoli Monitoring Web Services. Puede utilizar estos ejemplos como sugerencias para crear aplicaciones propias.

Nota: Estos casos de ejemplo no describen el código real que se ha utilizado para desarrollarlos. Para producir los gráficos y las tablas que se muestran en estos ejemplos, necesita desarrollar scripts propios.

Generación de resúmenes y gráficos de operaciones lógicas diarias

Puede recuperar datos de varios agentes, utilizando el servidor SOAP en un concentrador activo, para generar resúmenes de operaciones lógicas diarias. Puede utilizar el método **CT_EMail** de SOAP para enviar por correo electrónico estos resúmenes a la dirección.

Es posible que desee añadir una etiqueta **<insert>** en **CT_EMail**. Esta etiqueta contiene instrucciones para el formato preferido para los resúmenes. La dirección puede ver estos resúmenes en su escritorio utilizando Internet Explorer. Los resúmenes proporcionan la posibilidad de echar una mirada rápida y eficiente a problemas que se pueden haber producido durante la noche.

Además de las características generales, puede añadir tablas y gráficos:

- Los volúmenes de transacciones, los tiempos de respuesta y el cumplimiento de los niveles de servicio se pueden trazar en relación a las tendencias de recursos y condiciones de error.
- Se pueden trazar gráficos sobre varios segmentos, facilitando su visualización e impresión.
- El eje X puede utilizar una escala de variables para mostrar el turno principal con más detalles.
- Se pueden trazar varios objetos/atributos de varios orígenes y se pueden correlacionar las excepciones por tiempo, proporcionando el foco en las áreas problemáticas.
- Una correlación de estado puede mostrar el estado de las situaciones.

Obtención de instantáneas de datos y de tabla y gráficos fuera de línea

Mediante la utilización del método de SOAP **CT_Get** en un concentrador activo, puede obtener una instantánea de datos de varios agentes para producir gráficos e informes. También puede crear un script AF REXX que solicite una instantánea de los datos.

Además de las características generales, puede añadir tablas y gráficos. Este tipo de solicitud puede contener estas características:

- Se puede trazar el gráfico sobre varios segmentos, facilitando su visualización e impresión.
- Al pulsar en el nombre de atributo del recuadro de descripción es posible que se visualice ese atributo en el eje Y y se muestre el valor de umbral.
- El valor de umbral, cuando se modifica, se puede utilizar como el nuevo valor de umbral.

Los gráficos siguientes representan resúmenes de ejemplo de operaciones empresariales diarias.

Los gráficos siguientes muestran los gráficos/informes de ejemplo generados para este tipo de solicitud.

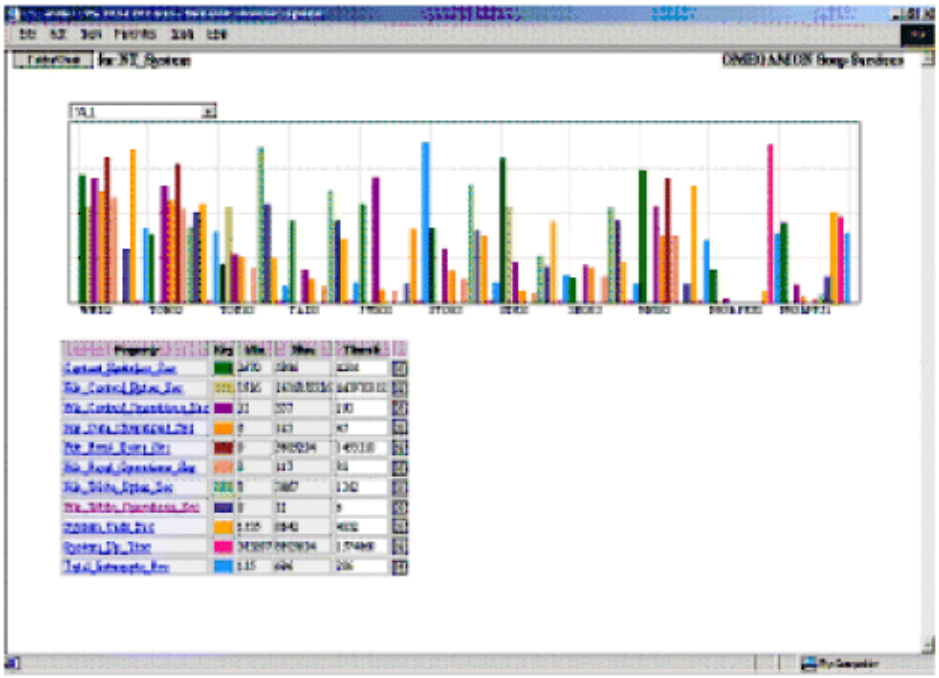

Figura 31. Gráfico y tabla de instantánea de datos

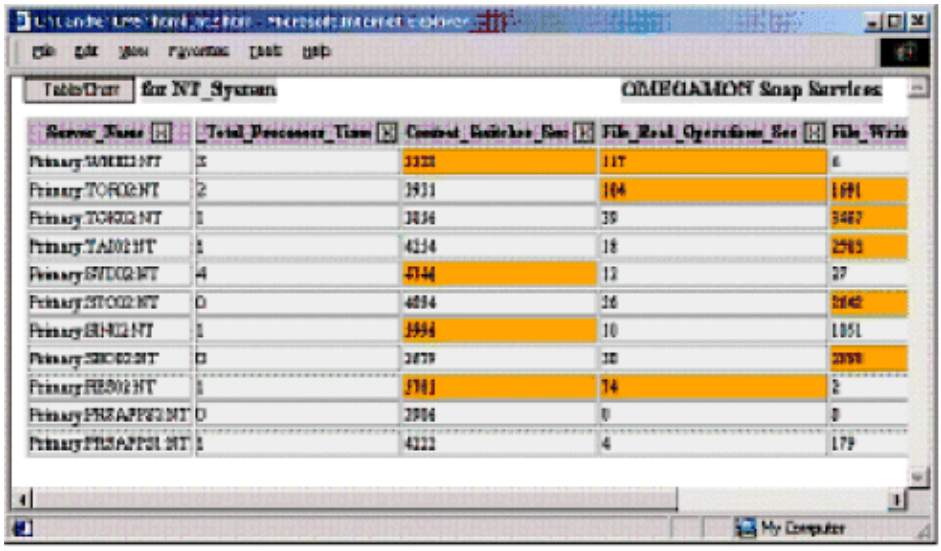

Figura 32. Tabla de instantáneas de datos

Envío de alertas a una plataforma de IBM Tivoli Monitoring

Con el método **CT_Alert** de SOAP, puede enviar una nueva alerta a una plataforma de IBM Tivoli Monitoring.

Por ejemplo, System Automation for Integrated Operations Management detecta un problema en un sistema HP NonStop Kernel y genera una alerte en una plataforma de IBM Tivoli Monitoring. Entonces la plataforma de IBM Tivoli Monitoring visualiza información de alerta de la plataforma de HP NonStop Kernel.

Creación de automatización colaboradora utilizando SA IO

Puede crear una aplicación REXX de System Automation for Integrated Operations Management que llame a las funciones SOAP JSCRIPT para reenviar cualquier mensaje de condición de error de SA IO y mostrarlo en una consola de Mensaje universal. Puede utilizar scripts SA IO para detectar y enviar los mensajes de registro, los mensajes de consola, etc., a IBM Tivoli Monitoring utilizando métodos SOAP.

Puede crear una aplicación que proporcione estas ventajas:

- Puede supervisar dispositivos, como HP NonStop Kernel, detectando mensajes VT100 y generando Mensajes universales.
- Puede enviar mandatos a sesiones Telnet de SA IO supervisadas y devolver las respuestas a esos mandatos.
- Los mensajes de origen se pueden excluir o incluir, basándose en criterios que utilicen expresiones regulares eficientes.
- Un registro local puede mantener información de auditoría sobre el estado de los mensajes recibidos y los mensajes enviados.
- Un registro local puede mantener información sobre el estado de conexión/reintento de concentrador de origen.

Los gráficos siguientes muestran una sesión Telnet de ejemplo, una consola de Mensaje universal que muestra los mensajes recibidos y un registro de mensajes de ejemplo.

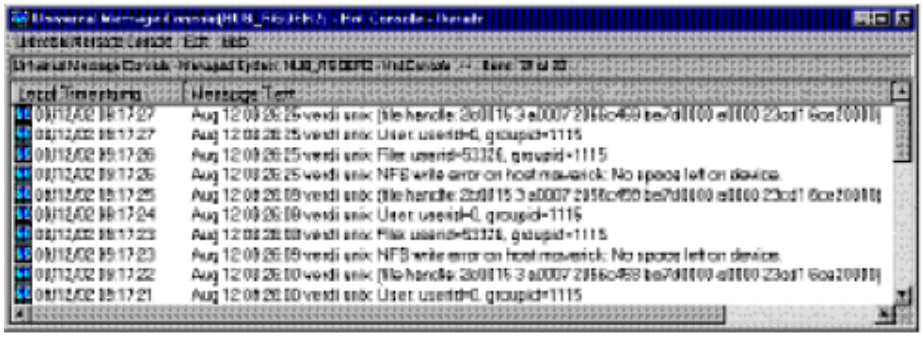

Figura 33. Consola de Mensaje universal que muestra los mensajes recibidos

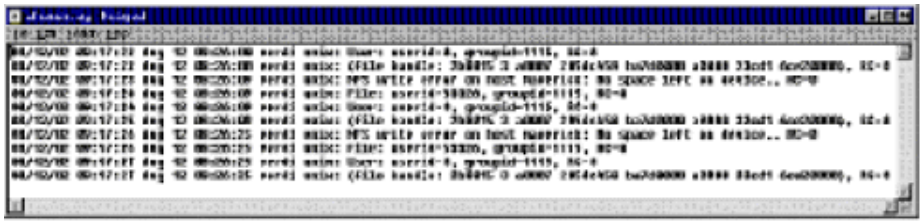

Figura 34. Detalles de registro de mensajes

Reconocimiento de un suceso en una plataforma de IBM Tivoli Monitoring

Puede reconocer un suceso en la plataforma de IBM Tivoli Monitoring.

Por ejemplo, en AF/Operator o System Automation for z/OS V3.2 o posteriores:

1. Un suceso de situación se recibe del Tivoli Enterprise Monitoring Server concentrador
2. Se pagina a una parte responsable que, a su vez, devuelve un reconocimiento
3. El reconocimiento de alerta se reenvía al servidor de supervisión

Para realizar esta tarea, utilice el método SOAP **CT_Acknowledge**. Este método le permite controlar los sucesos del entorno de IBM Tivoli Monitoring según la información obtenida y detectada por las soluciones de automatización de IBM.

Contenido de informe

Puede diseñar un informe para que contenga una tabla y una vista de gráfico. Es posible que desee añadir un botón **Tabla/Gráfico** que le permita conmutar entre el gráfico y la vista de tabla.

Características de vista de gráfico

Los gráficos pueden tener características específicas para permitirle:

- Ver tipos diferentes de gráficos, en función de los datos recuperados
- Elegir el eje Y seleccionando atributos adicionales en la lista de atributos desplegable
- Cambiar el título y las instrucciones del gráfico
- Ver el texto flotante que contiene el nombre y el valor del atributo trazado colocando el ratón sobre cada elemento trazado

Funciones de la vista de tabla

Las tablas pueden tener características específicas. Por ejemplo, puede diseñar tablas que le permiten:

- Ver el texto flotante que contiene el nombre y el valor del atributo trazado colocando el ratón sobre cada elemento trazado
- Modificar la tabla filtrando los atributos que se visualizan
- Eliminar atributos de una tabla pulsando el botón X junto al nombre de atributo

Apéndice B. Habilitación del servicio web de representación gráfica de IBM Tivoli Monitoring

Si tiene un producto basado en la plataforma Tivoli Integrated Portal V2.2, puede utilizar la característica de representación gráfica para visualizar diagramas con los valores consultados del entorno de Tivoli Monitoring. Debe habilitar los servicios web de representación gráfica de IBM Tivoli Monitoring (ITMWebService) en el Tivoli Enterprise Portal Server. El servicio web de representación gráfica también se utiliza con la función de captador de datos basado en política de Tivoli Business Service Manager.

Nota: El proveedor de datos de panel de instrumentos de IBM Tivoli Monitoring se utiliza en lugar del servicio web de representación gráfica al visualizar datos de supervisión en IBM Dashboard Application Services Hub.

Antes de empezar

El inicio de sesión único debe estar habilitado para los usuarios de la consola de Tivoli Integrated Portal y Tivoli Enterprise Portal Server.Los usuarios que visualizan gráficos que contienen datos del servicio web de representación gráfica deben tener un ID de usuario de Tivoli Enterprise Portal que tenga asignada la aplicación de supervisión cuyos datos se visualizan en el gráfico.

Acerca de esta tarea

Complete estos pasos en el sistema en el que el Tivoli Enterprise Portal Server está instalado y en ejecución para habilitar el servicio web de representación gráfica de Tivoli Monitoring.

Procedimiento

1. Copie el archivo **kfwtipewas.properties** en el directorio del servidor del portal:

   Windows De *dir_instalación*\CNPS\SQLLIB\ en *dir_instalación*\CNPS.

   Linux UNIX En *dir_instalación*/*plataforma*/cq/sqllib/ para *dir_instalación*/*plataforma*/cq/.
2. Vuelva a configurar Tivoli Enterprise Portal Server.

Qué hacer a continuación

Como usuario de Tivoli Enterprise Portal tiene autorización para ver ciertos espacios de trabajo pertenecientes a una determinada aplicación supervisada en función de sus permisos. Si tiene autorización para ver, por ejemplo, espacios de trabajo de Linux, las consultas de dichos espacios de trabajo están disponibles en Tivoli Integrated Portal para la generación de diagramas.

Si desea utilizar HTTPS para asegurar la comunicación entre el servicio web de representación gráfica, consulte “Integración de Tivoli Business Service Manager y Tivoli Enterprise Portal Server en SSL” en *IBM Tivoli Monitoring: Guía de instalación y configuración*.

© Copyright IBM Corp. 2005, 2013

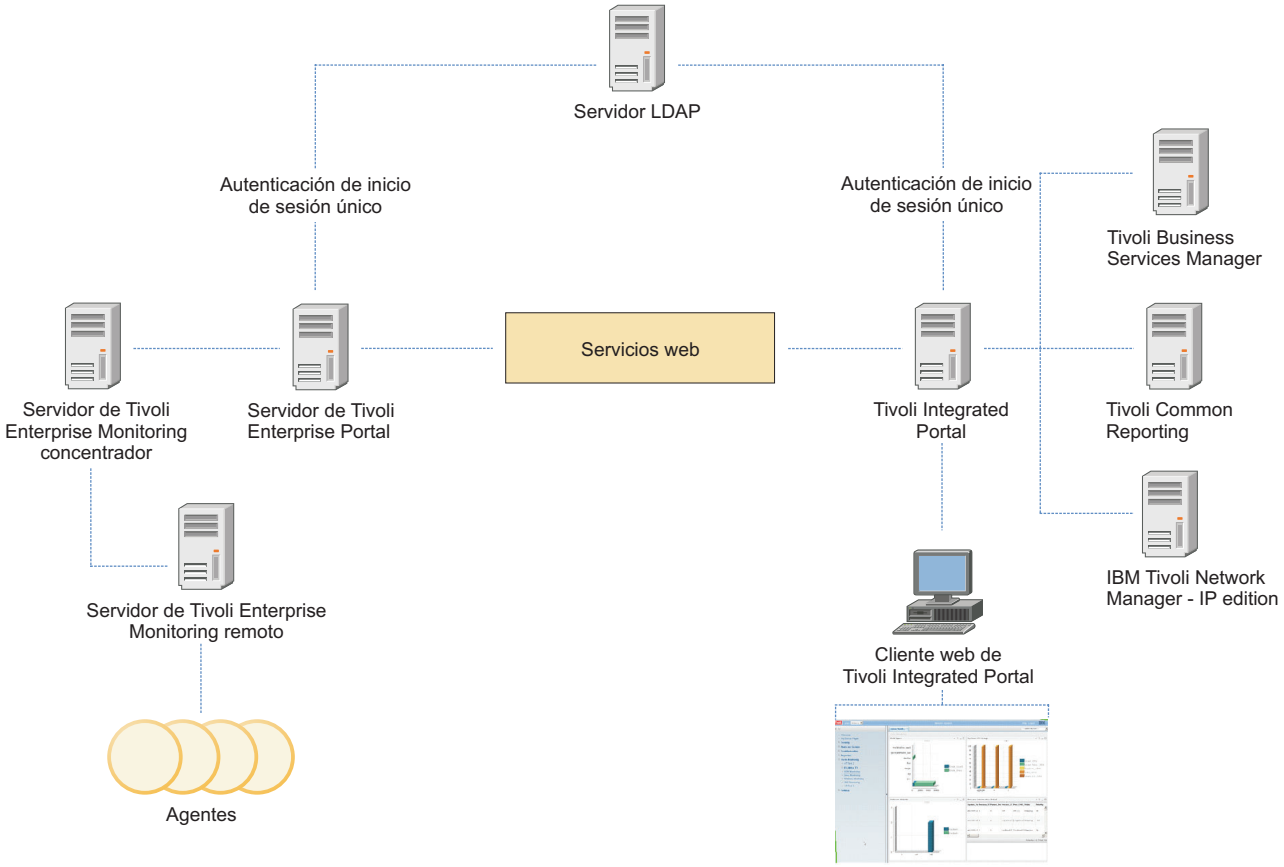

Figura 35. Conexiones entre productos para el servicio web de representación gráfica

Apéndice C. Utilización de Tivoli Management Services Discovery Library Adapter

Utilice el programa Tivoli Management Services Discovery Library Adapter (TMS DLA) para explorar el entorno supervisado a fin de identificar los sistemas gestionados. Luego puede transferir esta información (un archivo de salida XML) a la base de datos de gestión de cambios y configuración (CCMDB), Tivoli Application Dependency Discovery Manager (TADDM) o Tivoli Business Service Manager (TBSM).

El TMS DLA identifica todos los sistemas gestionados distribuidos y z/OS registrados en Tivoli Management Services.

Antes de empezar

Cuando se inicia el script **tmsdla**, TMS DLA obtiene información consultando en el servidor de supervisión concentrador todos los sistemas gestionados y correlacionándolos con los recursos del modelo común de datos según el código de producto y el formato de nombre de sistema gestionado. Las consultas especificadas en el archivo de entrada XML que proporciona cada producto se ejecutan y los resultados se guardan en un solo archivo de salida.

Consulte la guía del usuario específica del agente para determinar si el agente suministra un archivo XML de entrada para el TMS DLS y posible información sobre correlación entre los recursos supervisados del agente y los recursos del modelo de datos común.

Los servidores de supervisión y el Tivoli Enterprise Portal Server se deben estar ejecutando para estas consultas. Además, los agentes gestionados que no estén en línea se pasarán por alto.

Acerca de esta tarea

Ejecute el siguiente script de TMS DLA desde la línea de mandatos del sistema en el que está instalado el servidor de portal:

Procedimiento

- Windows Para crear una publicación IDML de tipo creación, especifique el siguiente mandato:

  ```
  dir_instalación\CNPS\tmsdla.bat
  ```

  Como alternativa, para crear una publicación IDML de tipo renovación, especifique el siguiente mandato. Después de importar en TADDM, los sistemas que están fuera de línea (como por ejemplo para operaciones de mantenimiento) se eliminan de TADDM. Lo mismo se cumple para Tivoli Business Service Manager (TBSM).

  ```
  dir_instalación\CNPS\tmsdla.bat -r
  ```

- Linux UNIX para crear una publicación IDML de tipo creación, especifique el siguiente mandato:

  ```
  dir_instalación/bin/itmcmd execute cq "tmsdla.sh"
  ```

© Copyright IBM Corp. 2005, 2013

Como alternativa, para crear una publicación IDML de tipo renovación, especifique el siguiente mandato. Después de importar en TADDM, los sistemas que están fuera de línea (como por ejemplo para operaciones de mantenimiento) se eliminan de TADDM. Esto también se cumple para TBSM.

```
dir_instalación/bin/itmcmd execute cq "tmsdla.sh -r"
```

Resultados

El TMS DLA genera el archivo de salida XML en el mismo directorio del servidor de portal. El nombre de este archivo sigue el formato estándar de nombres de Discovery Library. Para utilizar la información en CCMDB, TADDM, o TBSM, debe transferir el archivo XML al almacén de archivos de Discovery Library y luego debe utilizar Discovery Library Bulk Loader.

El TMS DLA también crea un archivo de salida con la extensión `.xml.original` que contiene la salida de TMS DLA antes de que se elimine ninguna relación. Las relaciones eliminadas se graban en `tmsdla.log`. Consulte "Dependencia del agente de sistema operativo" en la página 603 para ver ejemplos de casos en los que las relaciones se pueden eliminar del archivo de salida CML del TMS DLA.

Uso

Utilice las siguientes notas de uso como consulta:

```
tmsdla [ [-? | -h] [-d directorio] [-f nombreArchivoSalida] [-l] [-m listaDeSistemasGestionados]
         [-o] [-p númeroPuerto] [-r] [-s] [-t recuentoHebras] [-w tiempoEspera] ]
```

donde:

-? | -h Muestra información de ayuda de sintaxis.

-d Especifique la ubicación del directorio de plantillas.

-f Especifique el nombre del archivo de salida resultante.

-l Descubre vistas lógicas.

-m Especifique la lista de sistemas gestionados.

La lista está delimitado por comillas dobles y sigue esta sintaxis:

```
"os_msys1, os_apptype1, [msys1, apptype1] ~ [os_msys2, os_apptype2,
[msys2, apptype2]] ~ .. ~ [os_msysN, os_apptypeN, [msysN, apptypeN]]"
```

-o Forzar el proceso de los sistemas gestionados fuera de línea.

-p Especifique el número de puerto del servidor de portal si no es el valor predeterminado de 1920. El número de puerto se incluye en el libro de salida y es utilizado por TADDM o TBSM para generar el URL para lanzar al Tivoli Enterprise Portal.

-r Genere un archivo XML de salida de tipo de renovación. Después de importar un archivo de salida de tipo de renovación en TADDM, los objetos para los sistemas gestionados que están fuera de línea, como por ejemplo para las operaciones de mantenimiento, y sus recursos supervisados, se eliminan de la base de datos de TADDM. Lo mismo ocurre cuando se importa un archivo de salida de tipo de renovación en TBSM o CCMDB. Si no especifica esta opción, se genera un archivo XML de salida de tipo de creación que sólo contiene sistemas gestionados en línea y los recursos que están supervisando. Cuando importa un archivo

XML de salida de tipo de creación en TADDM, TBSM, o CCMDB, los sistemas gestionados y los recursos supervisados se añaden o actualizan pero no se producen supresiones.

-s Suprimir la generación del archivo `.original` del proceso de limpieza.

-t Especifique el número de hebras que desea utilizar.

-w Especifique el número de segundos que se debe esperar para que el agente atienda la consulta antes de exceder el tiempo de espera. Utilice esta opción si es posible que los agentes de supervisión no puedan atender las consultas en un plazo de tiempo razonable debido a una alta carga en el sistema consultado. **Valor predeterminado**: 120 segundos.

Valor mínimo: 50 segundos. Los valores inferiores a 50 se pasan por alto y se utiliza el valor predeterminado.

Valor máximo: 600 segundos.

Nota: No se proporcionan códigos de retorno durante la finalización del libro para avisarle si se ha producido un tiempo de espera excedido o faltan datos del agente. Para determinar si tiene que establecer un valor más alto que el valor predeterminado, analice el libro para asegurarse de que todos los agentes han respondido.

Referencia relacionada:

Base de datos de gestión de cambios y de configuración de Tivoli
Busque "Almacén de archivos de Discovery Library" y "Cargador masivo de Discovery Library" en el centro de información de CCMDB

Problemas con el DLA de Tivoli Monitoring
Soluciones para problemas comunes que se producen con el DLA de Tivoli Monitoring

Tivoli Monitoring: Consulta de mandatos
Aquí se describen los mandatos itmcmd, solo disponibles en los servidores de Tivoli Enterprise Monitoring de Linux y UNIX.

Dependencia del agente de sistema operativo

Tivoli Management Services Discovery Library Adapter (TMS DLA) necesita agentes de sistema operativo (SO) para supervisar los mismos sistemas que los agentes de aplicación que proporcionan plantillas de DLA.

Algunos agentes de aplicación (como el agente DB2) se basan en los agentes de sistema operativo para crear los elementos en la publicación de DLA que describen el sistema y los sistemas operativos en los que se están ejecutando los agentes. En sus plantillas de DLA, los agentes de aplicación hacen referencia a los elementos sistema y sistema operativo que crearán los agentes de sistema operativo utilizando un elemento de relación. Por ejemplo, Db2System runsOn a ComputerSystem, donde runsOn es el tipo de relación, Db2System es el elemento de origen y ComputerSystem es el elemento de destino.

Si un agente de sistema operativo no está supervisando el mismo sistema que un agente de aplicación o el agente de sistema operativo y el agente de operación están conectados a distintos entornos de IBM Tivoli Monitoring, es posible que el origen o el destino de un elemento de relación no existan en una publicación de DLA. También es posible que el origen y el destino de una relación con un sistema o sistema operativo no existan si:

- El agente de SO Windows está supervisando un sistema Windows 2000. En este caso, el agente del sistema operativo no puede descubrir la dirección IP del sistema Windows 2000 y, por tanto, no crea elementos del sistema en la publicación de DLA.
- Si utiliza un agente de sistema operativo sin agente para supervisar un sistema que también está supervisando un agente de aplicación, puesto que los agentes de sistema operativo sin agente no ofrecen entrada a las publicaciones de DLA.

Si el origen o el destino de una relación no existen en la publicación de DLA, la publicación no se cargará correctamente en Tivoli Application Dependency Discovery Manager (TADDM) o Tivoli Business Service Manager (TBSM). Por lo tanto, el DLA elimina una relación de una publicación de DLA si el origen o el destino de una relación no existen en la publicación. Esto permite cargar las publicaciones de DLA correctamente. Sin embargo, si se elimina una relación, la publicación de DLA no contendrá la información para correlacionar el recurso afectado (por ejemplo, un sistema de base de datos) con un sistema o sistema operativo en TADDM o TBSM.

El DLA crea dos archivos XML cada vez que se ejecuta el mandato **tmsdla**:

- Una publicación con la extensión `.xml`
- Una publicación con la extensión `.xml.original`

El archivo con la extensión `.xml.original` contiene el contenido de la publicación de DLA antes de que se elimine ninguna relación. Las relaciones eliminadas se graban en `tmsdla.log`.

Si desea que los recursos se correlacionen con los sistemas y sistemas operativos en las publicaciones de DLA cargadas en TADDM y TBSM, instale un agente de sistema operativo en los sistemas supervisados por los agentes de aplicación.

Filtrado de direcciones de red privadas

En entornos en los que las direcciones de red privadas no se duplican, puede cambiar este comportamiento para que Tivoli Management Services Discovery Library Adapter (TMS DLA) llene estos sistemas.

Antes de empezar

El TMS DLA no llena sistemas con datos procedentes de interfaces de red privadas de acuerdo con las normas Internet Engineering Task Force (IETF) RFC 1918 e IETF RFC 4193. Para obtener detalles sobre RFC, consulte el Índice de RCF (http://tools.ietf.org/rfc/index). Este comportamiento evita la fusión incorrecta de sistemas informáticos cuando varias redes privadas utilizan direcciones con rangos que se solapan.

Acerca de esta tarea

Para habilitar el descubrimiento de sistemas con interfaces de red privadas, edite los filtros de direcciones IP de los archivos de plantillas XML que controlan el comportamiento de TMS DLA.

Procedimiento

1. Realice una copia de seguridad de los archivos de plantillas antes de editarlos.
   - Linux UNIX Los archivos de plantillas se guardan en `$ITM_HOME/`*arch*`/cq/tmsdla` en el Tivoli Enterprise Portal Server.

- Windows Los archivos de plantillas se guardan en `%ITM_HOME%\CNPS\tmsdla` en el Tivoli Enterprise Portal Server.

2. Una plantilla para cada agente de supervisión proporciona datos de descubrimiento.
   a. Compruebe cada uno de los archivos de plantillas para determinar si tienen una o más secciones `<tmsdla:filter>`. Por ejemplo, los nombres de archivos de plantillas para los agentes del sistema operativo son:

      `knt_tmsdla.xml` para el agente del SO Windows

      `kux_tmsdla.xml` para el agente del SO UNIX

      `klz_tmsdla.xml` para el agente del SO Linux

   b. Actualice las diversas secciones `<tmsdla:filter>` de cada uno de los archivos de plantillas para que contengan sólo los filtros para direcciones de bucle de retorno (127.0.0.1 para IPv4 y ::1 para IPv6), tal como se muestra en el ejemplo siguiente:

```
<tmsdla:filters>
    <tmsdla:filter name="IF_IP_ADDR" exclude="127\.0\.0\.1"/>
    <tmsdla:filter name="IF_IP_ADDR" exclude="::1"/>
</tmsdla:filters>
```

Qué hacer a continuación

Cuando el soporte de aplicaciones del agente se actualiza en el Tivoli Enterprise Portal Server, se cambia el nombre del archivo de plantillas de DLA actual del agente con las modificaciones para que utilice la extensión `.bak` y la versión más reciente del archivo de plantillas. Después de que finalice la instalación del soporte de aplicaciones, debe actualizar la nueva versión del archivo de plantillas de DLA del agente para que contenga las ediciones que haya realizado en el filtrado de direcciones IP en la versión `*.bak` del archivo de plantillas.

Apéndice D. Utilización de z/OS Tivoli Management Services Discovery Library Adapter

Tivoli Management Services Discovery Library Adapter z/OS (DLA zTMS), disponible desde V6.2.2 Fixpack 7 o posterior y IBM Tivoli Monitoring V6.2.3 Fixpack 1 o posterior, explora el entorno de IBM Tivoli Monitoring y descubre los recursos supervisados por los agentes de OMEGAMON.

DLA zTMS identifica recursos sólo en sistema operativos z/OS. Para descubrir recursos en sistemas distribuidos, también debe ejecutar Tivoli Monitoring Services Discovery Library Adapter.

Antes de empezar

Los datos del libro IDML generado por DLA zTMS se pueden utilizar para complementar los datos recopilados por DLA z/OS, habilitando un inicio según contexto en Tivoli Enterprise Portal desde objetos o sucesos z/OS en Tivoli Business Service Manager (TBSM) o Tivoli Application Dependency Discovery Manager (TADDM).

DLA zTMS crea los siguientes objetos Common Data Model (CDM):

- sys.zOS.Sysplex
- sys.zOS.SysplexGroup
- sys.zOS.ZSeriesComputerSystem
- sys.zOS.ZOS
- sys.zOS.CICSRegion
- sys.zOS.DB2Subsystem
- sys.zOS.IMSSubsystem
- sys.zOS.MQSubsystem
- sys.zOS.AddressSpace

Importante: Para conciliar con el libro de DLA zTMS, la versión de DLA z/OS necesaria es V3.1, con PTF UA61720. El libro IDML generado por DLA zTMS no contiene todos los atributos necesarios para los distintos objetos CDM z/OS. Antes de importar el libro DLA zTMS en una aplicación consumidora, debe ejecutar en primer lugar DLA z/OS en todos los sistemas supervisados por los agentes IBM Tivoli Monitoring OMEGAMON e importar los libros DLA z/OS resultantes en la aplicación consumidora. Luego puede importar el libro DLA zTMS y todos los objetos se reconciliarán con los objetos existentes encontrados en los libros DLA z/OS. Si el libro DLA zTMS se importa sin haber importado primero antes el libro DLA z/OS, es posible que los objetos se muestren en la interfaz de usuario de TBSM como NO_LABEL_SUPPLIED.

Casos de usuarios

1. En LPAR z/OS, ejecute DLA z/OS en todas las LPAR z/OS que desee.
2. En el Tivoli Enterprise Portal Server, ejecute DLA zTMS en servidores de portal con agentes z/OS.
3. Si está utilizando TBSM, complete los campos siguientes:

© Copyright IBM Corp. 2005, 2013

a. En el servidor de datos TBSM, importe los libros DLA z/OS utilizando el kit de herramientas de la biblioteca de descubrimiento de TBSM.
b. En el servidor de datos TBSM, importe el libro DLA zTMS en TBSM utilizando el kit de herramientas de la biblioteca de descubrimiento de TBSM.
c. En la interfaz gráfica de usuario del servidor TBSM, pulse con el botón derecho del ratón en el objeto TBSM para visualizar los elementos del menú de inicio de IBM Tivoli Monitoring.

4. Si está utilizando TADDM, complete los campos siguientes:
   a. En el servidor TADDM, importe los libros DLA z/OS en TADDM utilizando el programa de utilidad de carga masiva.
   b. En el servidor TADDM, importe los libros DLA zTMS en TADDM utilizando el programa de utilidad de carga masiva.

Acerca de esta tarea

Ejecute el siguiente script de DLA desde la línea de mandatos del sistema en el que está instalado el Tivoli Enterprise Portal Server:

Procedimiento

- Windows Para crear un libro IDML, especifique el mandato siguiente:
  dir_instalación\CNPS\ztmsdla.exe

  El archivo de salida se graba en el directorio *dir_instalación*\CNPS\tmsdla.
- Linux UNIX Para crear libro IDML, especifique el siguiente mandato:
  dir_instalación/bin/itmcmd execute cq "ztmsdla"

  El archivo de salida se guarda en el directorio *dir_instalación*/*arch*/cq/bin/tmsdla.

Resultados

El DLA genera el archivo de salida XML en el directorio especificado anteriormente. El nombre de este archivo comienza por ZTMSDISC100-B y sigue el formato estándar de nombres de archivo de Discovery Library, por ejemplo: ZTMSDISC100-B.<*nombrehost*>.<*indicación_fecha_y_hora*>.refresh.xml.

Para importar este libro en TADDM o TBSM, debe transferir el archivo XML al almacén de archivos de Discovery Library y luego debe utilizar Discovery Library Bulk Loader.

Uso

Utilice las siguientes notas de uso como consulta:

```
ztmsdla [/?] [/b] [/d] [/o orgname] [/s] [/p port] [/x outputfile]
```

donde:

/? Muestra información de ayuda de sintaxis.

/b Abre un navegador para ver el archivo de salida de Discovery Library Adapter (sólo en Windows).

/d Crea un archivo de diagnósticos durante el proceso de descubrimiento. Puede utilizar este archivo para realizar la depuración. El archivo está

situado en el mismo directorio que el libro DLA IDML. El nombre del archivo es el mismo que el del libro DLA IDML con la extensión `.log` al final del nombre del archivo, por ejemplo: `ZTMSDISC100-B.<nombrehost>.<indicación_fecha_y_hora>.refresh.log`.

/o orgname
Establece el valor de Organization GlobalName. Si no se especifica este argumento, GlobalName adopta el valor predeterminado `<defaultOrg>`.

/s Cuando se especifica, el URL creado para el atributo sourceContactInfo de la clase ManagementSoftwareSystem se crea utilizando el protocolo HTTPS. TBSM y TADDM utilizan este atributo al realizar un inicio en el contexto del Tivoli Enterprise Portal.

/p port
Establezca el puerto utilizado para el URL creado para el atributo sourceContactInfo. El puerto predeterminado es 1920 para HTTP. Si se especifica la opción /s, el puerto predeterminado es 3661 para HTTPS. Utilice esta opción si el administrador de IBM Tivoli Monitoring ha cambiado los puertos predeterminados del servidor web utilizados para establecer contacto con el servidor de portal.

/x outputfile
Indica el nombre del archivo de salida XML.

Limitaciones conocidas

Existen limitaciones cuando se utiliza una comunicación SNA en lugar de IP.PIPE entre un Tivoli Enterprise Monitoring Server z/OS y agentes OMEGAMON. Dos objetos CICS que representan la misma región de CICS se muestran en TBSM, pero solo se puede pulsar con el botón derecho en uno de los objetos TBSM CICS en el espacio de trabajo de Tivoli Enterprise Portal OMEGAMON CICS.

Apéndice E. Descripciones de sucesos del agente SNMP de MIB

Los agentes de supervisión de Tivoli emiten tres tipos de alertas SNMP para trasmitir el estatus operativo del agente, sucesos de situación muestreados y sucesos de situación puros. Los tipos de alerta están definidos en los archivos canbase.mib y cansyssg.mib, disponibles en el soporte de instalación de IBM Tivoli Monitoring y de agentes de IBM Tivoli Monitoring.

Se envían condiciones de excepción SNMP de estado de situación de agente utilizando 1.3.6.1.4.1.1667.1.3 de empresa (Candle-BASE-MIB::candle-Alert-MIB).

agentStatusEvent

agentStatusEvent es una condición de excepción de información de estatus operativo del agente de supervisión generada por el exportador de sucesos SNMP de agente autónomo de Tivoli que informa y notifica sobre un suceso operativo específico del agente.

Condición de excepción específica: 20

Acceso: solo lectura

Estatus: obligatorio

Tabla 69. Variables de condición de excepción de SNMP para agentStatusEvent

Variable	Descripción	OID
agentSit-Name	El nombre de la situación, de un máximo de 32 bytes, identifica el nombre y la naturaleza del suceso de estatus.	1.3.6.1.4.1.1667.1.2.1.10.1.3
agentSit-OriginNode	El nombre del sistema gestionado en el que se ha evaluado la situación, de un máximo de 32 bytes.	1.3.6.1.4.1.1667.1.2.1.10.1.4
agentSit-LocalTimeStamp	La indicación de fecha y hora en que ha cambiado el estado de la situación. el formato es SAAMMDDHHMMSSmmm (como por ejemplo 1090415094501000 para el 15 de abril de 2009 a las 09:45:01) donde: S = Siglo (1 para siglo XXI) A = Año M = Mes D = Día H = Hora M = Minuto S = Segundo m = milisegundo	1.3.6.1.4.1.1667.1.2.1.10.1.5

© Copyright IBM Corp. 2005, 2013

Tabla 69. Variables de condición de excepción de SNMP para agentStatusEvent (continuación)

Variable	Descripción	OID
autoSit-Category	Categoría de situación asignada. Los valores válidos son: 0 - Umbral 1 – Topología de red 2 - Error 3 - Estatus 4 – Configuración de nodo 5 – Alerta de aplicación 6 – Todas las categorías 7 – Sólo registro 8 - Correlación 9 – Ignorar	1.3.6.1.4.1.1667.1.2.1.6
autoSit-Severity	Gravedad de situación asignada. Los valores válidos son: 0 - Borrada 1 - Indeterminada 2 - Aviso 3 - Leve 4 - Grave 5 - Crítica	1.3.6.1.4.1.1667.1.2.1.7
autoSit-StatusText	El texto del mensaje de descripción de la condición de excepción de estatus del agente, de entre 0 y 256 bytes.	1.3.6.1.4.1.1667.1.2.1.9
autoSit-Interval	El intervalo de condiciones de excepción de estatus del agente; que se suele utilizar para el intervalo de latido. Consulte el "Archivo de configuración de condiciones de excepción de muestra" en "Configuración de alertas de SNMP" en la página 378 para ver un ejemplo de cómo definir el intervalo de latido: `<StatTrap name="EE_HEARTBEAT" sev="1" interval="15" cat="3" />`	1.3.6.1.4.1.1667.1.2.1.11

agentSitSampledEvent

Se ha detectado un suceso de situación de muestra. Esta condición de excepción la genera el exportador de sucesos SNMP de agente autónomo de Tivoli como respuesta al hecho de que se excediera un umbral de situación en el momento de realizar el muestreo de datos.

Condición de excepción específica: 21

Acceso: solo lectura

Estatus: obligatorio

Tabla 70. Variables de condición de excepción de SNMP para agentSitSampledEvent

Atributo	Descripción	OID
agentSit-Application	Es el nombre de la aplicación del producto, de entre 1 y 8 bytes.	1.3.6.1.4.1.1667.1.2.1.10.1.1
agentSit-Table	Es el nombre de la tabla de la aplicación del producto (grupo de atributos), de entre 1 y 12 bytes.	1.3.6.1.4.1.1667.1.2.1.10.1.2

Tabla 70. Variables de condición de excepción de SNMP para agentSitSampledEvent (continuación)

Atributo	Descripción	OID
agentSit-Name	El nombre de la situación, de un máximo de 32 bytes, identifica el nombre y la naturaleza del suceso de estatus.	1.3.6.1.4.1.1667.1.2.1.10.1.3
agentSit-OriginNode	El nombre del sistema gestionado en el que se ha evaluado la situación, de un máximo de 32 bytes.	1.3.6.1.4.1.1667.1.2.1.10.1.4
agentSit-LocalTimeStamp	La indicación de fecha y hora en que ha cambiado el estado de la situación. El formato es SAAMMDDHHMMSSmmm (como por ejemplo 1091031183005000 para el 31 de octubre de 2009 a las 18:30:05) donde: S = Siglo (1 para siglo XXI) A = Año M = Mes D = Día H = Hora M = Minuto S = Segundo m = milisegundo	1.3.6.1.4.1.1667.1.2.1.10.1.5
agentSit-Context	Identificador exclusivo de contexto de la situación, expresado como un entero (comprendido entre -2147483647 y 2147483647). Es el número de descriptor de contexto que identifica una solicitud en ejecución del agente. En un entorno SNMP suele utilizarse un sondeo directo de condiciones de excepción en el que se recibe una condición de excepción y el gestor de red sondea el agente que lo ha originado para obtener información detallada. Este identificador se utiliza para proporcionar el contexto del agente de destino a fin de correlacionar la solicitud con el origen del problema. Aunque se envía agentSit-Context, no se utiliza en este release.	1.3.6.1.4.1.1667.1.2.1.10.1.6
agentSit-SampleInterval	Intervalo de situación muestreada en segundos, entre 0 y 86400.	1.3.6.1.4.1.1667.1.2.1.10.1.7
agentSit-Source	Estatus actual de la situación. Los valores válidos son: 0 - No definido 1 - Empresa, lo que significa que la situación se ha definido en el servidor de Tivoli Enterprise Monitoring 2 - Privada, lo que significa que la situación se ha definido mediante el archivo de configuración local de situaciones privadas.	1.3.6.1.4.1.1667.1.2.1.10.1.20

Tabla 70. Variables de condición de excepción de SNMP para agentSitSampledEvent (continuación)

Atributo	Descripción	OID
autoSit-Category	Categoría de situación asignada. Los valores válidos son: 0 - Umbral 1 – Topología de red 2 - Error 3 - Estatus 4 – Configuración de nodo 5 – Alerta de aplicación 6 – Todas las categorías 7 – Sólo registro 8 - Correlación 9 – Ignorar	1.3.6.1.4.1.1667.1.2.1.6
autoSit-Severity	Gravedad de situación asignada. Los valores válidos son: 0 - Borrada 1 - Indeterminada 2 - Aviso 3 - Leve 4 - Grave 5 - Crítica	1.3.6.1.4.1.1667.1.2.1.7
autoSit-Predicates	Es la fórmula de la situación, de un máximo de 3210 bytes, con el formato nombreAtributo Operador ValorComparación. Cuando la fórmula tiene varias expresiones, se muestran sus conectores booleanos AND u OR.	1.3.6.1.4.1.1667.1.2.1.8
sitAttributeList	Los valores de atributos para la situación asignada al agente de supervisión, de entre 0 y 3200 bytes.	1.3.6.1.4.1.1667.1.2.1.5

agentSitPureEvent

Se ha detectado un suceso de situación puro. Esta condición de excepción la genera el exportador de sucesos SNMP de agente autónomo de Tivoli como respuesta al hecho de que se excediera un umbral de situación. Las variables de una condición de excepción de suceso puro son idénticas a las de una condición de excepción de suceso muestreado, excepto en que no hay agentSit-SampleInterval porque no se toman muestras de sucesos puros; la llegada de datos no solicitados del grupo de atributos supervisado hace que la situación pase a ser verdadera. Una situación creada con un grupo de atributos para un registro del sistema, por ejemplo, abre un suceso puro cuando llega una entrada de registro.

Condición de excepción específica: 22

Acceso: solo lectura

Estatus: obligatorio

Tabla 71. Variables de condición de excepción de SNMP para agentSitPureEvent

Atributo	Descripción	OID
agentSit-Application	Es el nombre de la aplicación del producto, de entre 1 y 8 bytes.	1.3.6.1.4.1.1667.1.2.1.10.1.1

Tabla 71. Variables de condición de excepción de SNMP para agentSitPureEvent (continuación)

Atributo	Descripción	OID
agentSit-Table	Es el nombre de la tabla de la aplicación del producto (grupo de atributos), de entre 1 y 12 bytes.	1.3.6.1.4.1.1667.1.2.1.10.1.2
agentSit-Name	El nombre de la situación, de un máximo de 32 bytes, identifica el nombre y la naturaleza del suceso de estatus.	1.3.6.1.4.1.1667.1.2.1.10.1.3
agentSit-OriginNode	El nombre del sistema gestionado en el que se ha evaluado la situación, de un máximo de 32 bytes.	1.3.6.1.4.1.1667.1.2.1.10.1.4
agentSit-LocalTimeStamp	La indicación de fecha y hora en que ha cambiado el estado de la situación. El formato es SAAMMDDHHMMSSmmm (como por ejemplo 1091031183005000 para el 31 de octubre de 2009 a las 18:30:05) donde: S = Siglo (1 para siglo XXI) A = Año M = Mes D = Día H = Hora M = Minuto S = Segundo m = milisegundo	1.3.6.1.4.1.1667.1.2.1.10.1.5
agentSit-Context	Identificador exclusivo de contexto de la situación, expresado como un entero (comprendido entre -2147483647 y 2147483647). Es el número de descriptor de contexto que identifica una solicitud en ejecución del agente. En un entorno SNMP suele utilizarse un sondeo directo de condiciones de excepción en el que se recibe una condición de excepción y el gestor de red sondea el agente que lo ha originado para obtener información detallada. Este identificador se utiliza para proporcionar el contexto del agente de destino a fin de correlacionar la solicitud con el origen del problema. Aunque se envía agentSit-Context, no se utiliza en este release.	1.3.6.1.4.1.1667.1.2.1.10.1.6
agentSit-Source	Estatus actual de la situación. Los valores válidos son: 0 - No definido 1 - Empresa, lo que significa que la situación se ha definido en el servidor de Tivoli Enterprise Monitoring 2 - Privada, lo que significa que la situación se ha definido mediante el archivo de configuración local de situaciones privadas.	1.3.6.1.4.1.1667.1.2.1.10.1.20

Tabla 71. Variables de condición de excepción de SNMP para agentSitPureEvent (continuación)

Atributo	Descripción	OID
autoSit-Category	Categoría de situación asignada. Los valores válidos son: 0 - Umbral 1 – Topología de red 2 - Error 3 - Estatus 4 – Configuración de nodo 5 – Alerta de aplicación 6 – Todas las categorías 7 – Sólo registro 8 - Correlación 9 – Ignorar	1.3.6.1.4.1.1667.1.2.1.6
autoSit-Severity	Gravedad de situación asignada. Los valores válidos son: 0 - Borrada 1 - Indeterminada 2 - Aviso 3 - Leve 4 - Grave 5 - Crítica	1.3.6.1.4.1.1667.1.2.1.7
autoSit-Predicates	Es la fórmula de la situación, de un máximo de 3210 bytes, con el formato nombreAtributo Operador ValorComparación. Cuando la fórmula tiene varias expresiones, se muestran sus conectores booleanos AND u OR.	1.3.6.1.4.1.1667.1.2.1.8
sitAttributeList	Los valores de atributos para la situación asignada al agente de supervisión, de entre 0 y 3200 bytes.	1.3.6.1.4.1.1667.1.2.1.5

Apéndice F. Registro de operaciones del agente

Un agente de Tivoli Enterprise Monitoring se puede ejecutar de forma autónoma durante un periodo de tiempo indeterminado, tomando muestras de datos y guardando sucesos. Revise el registro de seguimiento de auditoría para examinar y revisar las actividades del agente, incluido el tiempo en que se ejecutaba de forma autónoma.

Cuando un agente se ejecuta de forma autónoma, se graban en el registro de operaciones registros de seguimiento de auditoría para todos los sucesos y filas de datos de aplicaciones de muestra verdaderas. El agente aprovecha el recurso existente Registro de operaciones del agente y graba en el mismo los registros de seguimiento de auditoría. El registro de operaciones del agente puede visualizarse en Tivoli Enterprise Portal mientras el agente está en línea.

- En los sistemas distribuidos, el agente crea el archivo de registro de operaciones de forma automática en el directorio de instalación del agente, lo denomina `Nombre_máquina_producto.LG0` para el archivo de registro en ejecución actual y cambia el nombre del archivo de registro anterior por `Nombre_máquina_producto.LG1` (el archivo de copia de seguridad).
- En los sistemas z/OS, el agente graba los registros del registro de operaciones del agente en una clase `SYSOUT`, guardando parte de los registros en la memoria caché.

El registro de operaciones del agente muestra la actividad de las situaciones privadas.

El registro del registro de actividades autónomas contiene los campos siguientes:

- Nombre del sistema del agente
- ID de mensaje: KRAIRA005
- Indicaciones de fecha y hora globales, mostrando la hora local real de la actividad del suceso
- El mensaje, que muestra el nombre de la situación, el nombre de la tabla de aplicaciones, el nombre del sistema, el nombre de la columna de filtro, el valor de filtro y el valor de muestreo real o el valor de sucesos. Si los criterios de filtro de situación especifican varios pares de nombre y valor de umbral y, por lo tanto, la salida sobrepasa el tamaño de registro del registro de operaciones, entonces el agente genera varios registros de registro.

Para obtener un informe de las actividades de operaciones autónomas del agente, cree una consulta personalizada del registro de operaciones del agente en Tivoli Enterprise Portal que filtre según el mensaje KRAIRA005 y, a continuación, asigne la consulta a una vista de tabla en un espacio de trabajo en el nivel de agente de la vista Física de Navigator. Alternativamente, puede asignar el nombre de consulta predefinido *Registro de operaciones del agente* a una vista de tabla y aplicar un filtro posterior utilizando el separador Filtros del editor de propiedades para filtrar todas las filas salvo las que tienen el mensaje KRAIRA005. La muestra un posible registro de las actividades autónomas que podría generarse a partir de esta consulta.

Este es el resultado de una vista de tabla del registro de operaciones del agente para incluir solamente los mensajes de autonomía del agente: == KRAIRA005

© Copyright IBM Corp. 2005, 2013

Nombre de servidor	Número de mensaje	Indicación de fecha y hora global	Tipo de sistema gestionado
Primary:East:NT	KRAIRA005	02/16/2009 12:35:42	Situation NT_Process_CPU_Critical for KNT.WTPROCESS reset
Primary:East:NT	KRAIRA005	02/16/2009 12:34:43	Situation NT_Process_CPU_Critical for KNT.WTPROCESS triggered (03) Process_Name [_Total] value <kdsmain>
Primary:East:NT	KRAIRA005	02/16/2009 12:34:42	Situation NT_Process_CPU_Critical for KNT.WTPROCESS triggered (02) Priority_Base [0] value <8>
Primary:East:NT	KRAIRA005	02/16/2009 12:34:42	Situation NT_Process_CPU_Critical for KNT.WTPROCESS triggered (01) %_Processor_Time [65] value <66>
Primary:East:NT	KRAIRA005	02/16/2009 12:34:21	Situation NT_Log_Space_Low for KNT.WTPROCESS triggered %_Usage [95] value <100>
Primary:East:NT	KRAIRA005	02/16/2009 12:32:42	Situation NT_Process_Memory_Critical for KNT>WTPROCESS triggered (02) Working_Set [40000000] value <48832512>
Primary:East:NT	KRAIRA005	02/16/2009 12:32:41	Situation NT_Process_Memory_Critical for KNT>WTPROCESS triggered (01) Process_Name [_Total] value <Rtvscan>
Primary:East:NT	KRAIRA005	02/16/2009 12:31:21	Situation NT_System_CPU_Critical for KNT.WTSYSTEM triggered Operating_System_Version [5.0] value <5.1>
Primary:East:NT	KRAIRA005	02/16/2009 12:29:41	Situation CHECK_NETWORK_STAT for KNT.IPSTATS triggered (06) Datagrams_Received_Header_Errors [0] value <0>
Primary:East:NT	KRAIRA005	02/16/2009 12:29:41	Situation CHECK_NETWORK_STAT for KNT.IPSTATS triggered (05) Datagrams_Outbound_Header_Errors [0] value <0>

Nota: La variable de entorno del agente CTIRA_LOG_PATH para agentes de supervisión de empresa distribuidos especifica el directorio en el que se almacena el archivo de registro de operaciones del agente (<*dir_instalación*>\TMAITM6\logs; en Windows y <*dir_instalación*>/config/logs en Linux y UNIX.) Los nombres de archivo utilizan los sufijos .LG0 y .LG1.

Biblioteca de documentación

Este apéndice contiene información acerca de las publicaciones relacionadas con IBM Tivoli Monitoring y con los componentes de Tivoli Management Services que generalmente se comparten.

Estas publicaciones se listan en las siguientes categorías:

- Biblioteca de IBM Tivoli Monitoring
- Publicaciones relacionadas

Para obtener información sobre cómo acceder a las publicaciones y utilizarlas, seleccione **Utilización de las publicaciones** en el panel **Contenido** del Centro de información de IBM Tivoli Monitoring y OMEGAMON XE en http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp.

Para obtener una lista de las publicaciones nuevas y modificadas, pulse **What's new** en la página de bienvenida del centro de información de IBM Tivoli Monitoring y OMEGAMON XE. Para buscar publicaciones de la versión anterior de un producto, pulse **Previous versions** en el nombre del producto del panel **Contents**.

Biblioteca de IBM Tivoli Monitoring

Las publicaciones siguientes proporcionan información acerca de IBM Tivoli Monitoring y acerca de los componentes de Tivoli Management Services que suelen compartirse:

- *Guía de inicio rápido*

  Contiene una introducción a los componentes de IBM Tivoli Monitoring.
- *Guía de instalación y configuración*, SC22-5445

  Proporciona instrucciones para instalar y configurar componentes IBM Tivoli Monitoring en sistemas Windows, Linux y UNIX.
- *Program Directory for IBM Tivoli Management Services on z/OS*, GI11-4105

  Proporciona instrucciones para la instalación de SMP/E de los componentes de Tivoli Management Services en z/OS.
- *Guía de alta disponibilidad para sistemas distribuidos*, SC22-5455

  Proporciona información sobre diferentes métodos para garantizar la disponibilidad de los componentes de IBM Tivoli Monitoring.
- *IBM Tivoli zEnterprise Monitoring Agent: Guía de instalación y configuración*, SC14-7358

  Proporciona instrucciones para instalar y configurar componentes de supervisión de Tivoli zEnterprise en sistemas Windows, Linux y UNIX. También incluye información sobre migración y copia de seguridad, resolución de problemas de Enterprise Common Collector, configuración de Hardware Management Console y el uso de la interfaz de mandatos o API para personalizar el recopilador. Esta guía complementa la publicación *Tivoli zEnterprise Monitoring Agent: Guía del usuario*.
- *Guía del administrador*, SC22-5446

© Copyright IBM Corp. 2005, 2013

Describe las tareas y las funciones de soporte necesarias para el servidor de Tivoli Enterprise Portal y los clientes, incluida la administración de usuarios de Tivoli Enterprise Portal.

- *Consulta de mandatos*, SC22-5448

  Ofrece información detallada sobre sintaxis y parámetros, así como ejemplos, sobre los mandatos que puede utilizar en IBM Tivoli Monitoring.

- *Mensajes*, SC22-5450

  Lista y describe los mensajes que generan todos los componentes de IBM Tivoli Monitoring y los componentes de Tivoli Management Services basados en z/OS como, por ejemplo, el servidor de Tivoli Enterprise Monitoring en z/OS y TMS:Engine.

- *Guía de resolución de problemas*, GC22-5449

  Proporciona información para ayudar a resolver problemas del software.

- Ayuda en línea de Tivoli Enterprise Portal

  Proporciona información de consulta sensible al contexto sobre todas las características y opciones de personalización de Tivoli Enterprise Portal. También proporciona instrucciones para utilizar y administrar Tivoli Enterprise Portal.

- *Tivoli Enterprise Portal: Guía del usuario*, SC22-5447

  Complementa la ayuda en línea de Tivoli Enterprise Portal. La guía proporciona lecciones prácticas e instrucciones detalladas para todas las características de Tivoli Enterprise Portal.

- *Agent Builder: Guía del usuario*, SC11-3772

  Explica cómo utilizar Agent Builder para crear agentes de supervisión y sus paquetes de instalación y para añadir funciones a agentes existentes.

- *Performance Analyzer: Guía del usuario*, SC11-7956

  Explica cómo utilizar Performance Analyzer para comprender las tendencias en el consumo de recursos, identificar problemas, resolver problemas con mayor rapidez y predecir y evitar futuros problemas.

- *IBM Tivoli zEnterprise Monitoring Agent: Guía del usuario*, SC14-7359

  Sirve de complemento a la ayuda en línea del agente de supervisión de Tivoli zEnterprise. La guía proporciona información de consulta sobre la interfaz, casos de ejemplo, información sobre resolución de problemas con agentes así como información sobre informes de Tivoli Common Reporting. Esta guía complementa la publicación *Tivoli zEnterprise Monitoring Agent: Guía de instalación y configuración*.

Documentación para los agentes base

Si ha adquirido IBM Tivoli Monitoring como producto, habrá recibido un conjunto de agentes de supervisión base como parte del producto. Si ha adquirido un producto de agente de supervisión (por ejemplo, un producto OMEGAMON XE) que incluye los componentes compartidos comúnmente de Tivoli Management Services, no habrá recibido los agentes base.

Las publicaciones siguientes proporcionan información sobre el uso de los agentes básicos.

- Agentes del sistema operativo:
  - *Windows OS Agent: Guía del usuario*, SC22-5451
  - *UNIX OS Agent: Guía del usuario*, SC22-5452
  - *Linux OS Agent: Guía del usuario*, SC22-5453
  - *IBM i Agent: Guía del usuario*, SC22-5454

- Supervisores del sistema operativo sin agentes:
  - *Tivoli Monitoring sin agentes para sistemas operativos Windows: Guía del usuario*, SC11-3836
  - *Tivoli Monitoring sin agentes para sistemas operativos AIX: Guía del usuario*, SC11-3838
  - *Tivoli Monitoring sin agentes para sistemas operativos HP-UX: Guía del usuario*, SC11-3839
  - *Tivoli Monitoring sin agentes para sistemas operativos Solaris: Guía del usuario*, SC11-3837
  - *Tivoli Monitoring sin agentes para sistemas operativos Linux: Guía del usuario*, SC11-3835
- Agentes de almacén:
  - *Agente de resumen y poda de almacén: Guía del usuario*, SC22-5457
  - *Agente de proxy de almacén: Guía del usuario*, SC22-5456
- Agentes de System P:
  - *AIX Premium Agent: Guía del usuario*, SA10-5471
  - *CEC Base Agent: Guía del usuario*, SC11-3629
  - *HMC Base Agent: Guía del usuario*, SA10-5473
  - *VIOS Premium Agent: Guía del usuario*, SA10-5472
- Otros agentes base:
  - *Tivoli Log File Agent User's Guide*, SC14-7484
  - *Systems Director base Agent: Guía del usuario*, SC11-7861

Publicaciones relacionadas

Para obtener información sobre los productos y publicaciones relacionados, seleccione **Publicaciones compartidas de OMEGAMON XE** u otras entradas en el panel **Contenido** del Centro de información de IBM Tivoli Monitoring y OMEGAMON XE en http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp .

Otras fuentes de información

También puede obtener documentación técnica acerca de IBM Tivoli Monitoring y de los productos relacionados en las fuentes siguientes:

- Service Management Connect (SMC)

  Para obtener información introductoria sobre SMC, consulte IBM Service Management Connect (http://www.ibm.com/developerworks/servicemanagement).

  Para obtener información sobre los productos de Tivoli, consulte la comunidad de Application Performance Management en SMC en IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm).

  Conecte, aprenda y comparta con profesionales de Service Management. Obtenga acceso a desarrolladores y expertos en soporte técnico de productos que proporcionan sus perspectivas y experiencia. Utilizando SMC, puede:

  - Implicarse en el desarrollo transparente, un compromiso permanente y abierto entre usuarios externos y desarrolladores de productos Tivoli donde se puede acceder a los primeros diseños, demostraciones de velocidad, mapas de ruta de productos y código previo al release.

- Conectarse de manera privada con expertos para colaborar y trabajar con Tivoli and Integrated Service Management.
- Aprovéchese de los conocimientos y la experiencia de otros utilizando los blogs.
- Colabore con la amplia comunidad de usuarios utilizando wikis y foros.

- Wikis de Tivoli

  IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm) incluye una lista de las wikis de Tivoli que ofrecen prácticas recomendadas y casos de ejemplo para utilizar productos Tivoli, libros blancos aportados por empleados de IBM y contenido creado por clientes y business partners.

  Dos de estas wikis tienen una importancia especial para IBM Tivoli Monitoring:

  - IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) proporciona información acerca de IBM Tivoli Monitoring y productos distribuidos relacionados, incluidos los productos de IBM Tivoli Composite Application Management.
  - La Wiki de Tivoli System z Monitoring and Application Management proporciona información sobre de OMEGAMON XE, NetView for z/OS, Tivoli Monitoring Agent para z/TPF y otros productos de gestión de System z y productos de gestión de aplicaciones.

- IBM Integrated Service Management Library

  http://www.ibm.com/software/brandcatalog/ismlibrary/

  IBM Integrated Service Management Library es un catálogo en línea que contiene documentación sobre la integración y otras ampliaciones de productos que se pueden descargar.

- Redbooks

  http://www.redbooks.ibm.com/

  Los IBM Redbooks y Redpapers incluyen información sobre productos desde las perspectivas de la plataforma y la solución.

- Notas técnicas (Technotes)

  Las notas técnicas proporcionan la información más actualizada sobre limitaciones del producto y soluciones temporales. Puede encontrar notas técnicas a través del sitio web de soporte de software de IBM en http://www.ibm.com/software/support/.

Información de soporte

Si tiene un problema con el software de IBM, deseará resolverlo rápidamente. IBM le ofrece varias formas de obtener el soporte que necesita.

En línea

Los siguientes sitios contienen información sobre resolución de problemas:

- Vaya a Portal de soporte de IBM (http://www.ibm.com/support/entry/portal/software) y siga las instrucciones.
- Vaya a IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm) y seleccione la wiki adecuada.

IBM Support Assistant

IBM Support Assistant (ISA) es un entorno de trabajo de servicio de software local y gratuito que le ayuda a resolver preguntas y problemas con productos de software IBM. ISA ofrece acceso rápido a las herramientas de prestación de servicios e información relacionada con el soporte para determinar los problemas. Para instalar el software ISA, vaya a IBM Support Assistant (http://www-01.ibm.com/software/support/isa).

Guía de resolución de problemas

Para obtener más información sobre la resolución de problemas, consulte la guía de resolución de problemas del producto.

Utilización de IBM Support Assistant

IBM Support Assistant es una aplicación autónoma gratuita que puede instalar en cualquier estación de trabajo. A continuación, podrá ampliar la aplicación instalando módulos de plug-ins específicos del producto para los productos IBM que utilice.

IBM Support Assistant ahorra el tiempo que se emplea en la búsqueda de productos, soporte y recursos de formación. IBM Support Assistant le ayuda a recopilar información de soporte cuando necesite abrir un registro de gestión de problemas (PMR), que podrá utilizar para realizar un seguimiento del problema.

Los módulos específicos de un producto le proporcionan los recursos siguientes:

- Enlaces de soporte
- Enlaces de formación
- Posibilidad de enviar informes de gestión de problemas

Para obtener más información y para descargar IBM Support Assistant, consulte http://www.ibm.com/software/support/isa/. Después de descargar y de instalar IBM Support Assistant, siga estos pasos para instalar el plug-in para el producto de Tivoli:

1. Inicie la aplicación IBM Support Assistant.
2. Seleccione **Updater** (Actualizador) en la página de bienvenida.
3. Seleccione **New Properties and Tools** (Nuevas propiedades y herramientas) o seleccione el separador **New Plug-ins** (Nuevos plug-ins), (dependiendo de la versión de IBM Support Assistant que esté instalada.

© Copyright IBM Corp. 2005, 2013

4. Bajo **Tivoli**, seleccione su producto y pulse **Install** (Instalar). Asegúrese de leer la licencia y la descripción.

   Si el producto no está incluido en la lista bajo **Tivoli**, todavía no hay disponible ningún conector para el producto.
5. Lea el acuerdo de licencia y la descripción, y pulse **I agree** (Acepto).
6. Reinicie IBM Support Assistant.

Obtención de arreglos

Es posible que haya un arreglo para el producto para resolver el problema. Para determinar qué arreglos están disponibles para el producto de software de Tivoli, realice estos pasos:

1. Vaya al sitio web de soporte de software de IBM, en http://www.ibm.com/software/support.
2. Bajo **Select a brand and/or product** (Seleccione una marca o producto), seleccione **Tivoli**.

   Si pulsa **Go**, se visualizará la sección **Search within all of Tivoli support**. Si no pulsa **Go**, se muestra la sección **Select a product** (Seleccionar un producto).
3. Seleccione el producto y pulse **Go** (Ir).
4. Bajo **Download** (Descargar), pulse en el nombre de un arreglo para leer su descripción y, opcionalmente, descargarlo.

   Si no hay ninguna cabecera **Descargar** (Descargar) para el producto, suministre un término de búsqueda, un código de error o un número APAR en el campo proporcionado bajo **Search Support (this product)** (Buscar soporte (este producto)) y pulse **Search** (Buscar).

Para obtener más información acerca de los tipos de arreglos que están disponibles, consulte la publicación *IBM Software Support Handbook* en http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

Recepción semanal de actualizaciones de soporte

Para recibir semanalmente notificaciones por correo electrónico acerca de los arreglos y otras noticias de soporte de software, siga estos pasos:

1. Vaya al sitio web de soporte de software de IBM, en http://www.ibm.com/software/support.
2. Pulse **My support** en la esquina superior derecha más lejana de la página bajo **Personalized support**.
3. Si ya se ha registrado en **My support** (Mi soporte), inicie la sesión y vaya al paso siguiente. Si no se ha registrado, pulse en **register now** (registrarse ahora). Complete el formulario de registro utilizando su dirección de correo electrónico como ID de IBM y pulse **Submit**.
4. Se visualizará el separador **Edit profile** (Editar perfil).
5. En la primera lista bajo **Products** (Productos), seleccione **Software**. En la segunda lista, seleccione una categoría de producto (por ejemplo, **Systems and Asset Management** [Gestión de sistemas y activos]). En la tercera lista, seleccione una subcategoría de productos (por ejemplo, **Application Performance & Availability** [Rendimiento y disponibilidad de aplicaciones] o **Systems Performance** [Rendimiento de los sistemas]). Se visualizará una lista de productos aplicables.
6. Seleccione los productos para los que desee recibir actualizaciones.
7. Pulse en **Add products** (Añadir productos).

8. Después de seleccionar todos los productos en los que está interesado, pulse en **Subscribe to email** (Suscribir a correo electrónico) en el separador **Edit profile** (Editar perfil).
9. En la lista **Documents** (Documentos), seleccione **Software**.
10. Seleccione **Please send these documents by weekly email** (Enviar semanalmente estos documentos por correo electrónico).
11. Actualice la dirección de correo electrónico según necesite.
12. Seleccione los tipos de documentos que desea recibir.
13. Pulse en **Update** (Actualizar).

Si experimenta problemas con la característica **My support** (Mi soporte), puede obtener ayuda de una de las maneras siguientes:

En línea
Envíe un mensaje de correo electrónico a erchelp@ca.ibm.com, describiendo el problema.

Por teléfono
En Estados Unidos, llame al 1-800-IBM-4You (1-800-426-4968).

Cómo ponerse en contacto con el soporte de software de IBM

El soporte de software de IBM proporciona asistencia con defectos de producto. El modo más fácil de obtener esta asistencia es abrir un PMR o un ETR directamente desde IBM Support Assistant.

Antes de ponerse en contacto con el soporte de software de IBM, asegúrese de que su empresa tenga un contrato de mantenimiento de software de IBM activo y de disponer de autorización para comunicar problemas a IBM. El tipo de contrato de mantenimiento de software que necesita dependerá del tipo de producto que tenga:

- Para productos de software distribuidos de IBM (incluidos, pero sin limitarse a, los productos Tivoli, Lotus y Rational, así como los productos DB2 y WebSphere que se ejecutan en sistemas operativos Windows o UNIX), regístrese en Passport Advantage de uno de los modos siguientes:

  En línea
  Vaya al sitio web de Passport Advantage en http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.

  Por teléfono
  Para ver el número de teléfono al que debe llamar en su país, vaya al sitio web de soporte de software de IBM en http://techsupport.services.ibm.com/guides/contacts.html y pulse el nombre de su región geográfica.
- Para los clientes con contratos de Suscripción y Soporte (S & S) acceda al sitio web Software Service Request en https://techsupport.services.ibm.com/ssr/login.
- Para los clientes con contratos Linux, iSeries, pSeries, zSeries y otros contratos de soporte, vaya al sitio web de Línea de soporte de IBM en http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- Para los productos de software de IBM eServer (incluidos, aunque sin limitarse a ellos, los productos de DB2 y WebSphere que funcionan en los entornos zSeries, pSeries e iSeries), puede adquirir un contrato de mantenimiento de software dirigiéndose directamente a un representante de ventas de IBM o a un Business Partner de IBM. Para obtener más información sobre el soporte de los productos

de software eServer, vaya el sitio web de IBM Technical Support Advantage en http://www.ibm.com/servers/eserver/techsupport.html.

Si no está seguro de qué tipo de contrato de mantenimiento de software necesita, llame al número 1-800-IBMSERV (1-800-426-7378) desde Estados Unidos. Desde otros países, vaya a la página de contactos de *IBM Software Support Handbook* en la web en http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html y pulse el nombre de su región geográfica para ver los números de teléfono de las personas que ofrecen soporte en su localidad.

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en Estados Unidos. Es posible que IBM no ofrezca en otros países los productos, servicios y características que se describen en este documento. Póngase en contacto con el representante de IBM de su localidad para obtener información acerca de los productos y servicios que están disponibles en su zona. Cualquier referencia a un producto, programa o servicio de IBM no indica ni implica que únicamente se puede utilizar dicho producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de la propiedad intelectual de IBM. No obstante, corresponde al usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal descrito en esta información. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 EE.UU.

Para realizar consultas sobre licencias relacionadas con la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o envíe sus consultas, por escrito, a la dirección siguiente:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde las disposiciones en él expuestas sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, AUNQUE SIN LIMITARSE A, LAS GARANTÍAS DE NO CONTRAVENCIÓN, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO.

Algunos estados no permiten la declaración de limitación de responsabilidad de garantías explícitas o implícitas en determinadas transacciones, por lo que es posible que este párrafo no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incluirán en nuevas ediciones de la publicación. En cualquier momento y sin previo aviso, IBM puede introducir mejoras o efectuar cambios en los productos y/o programas descritos en la presente publicación.

© Copyright IBM Corp. 2005, 2013

Las referencias contenidas en esta información a sitios web no IBM se proporcionan únicamente para su comodidad y de ningún modo constituyen una recomendación de dichos sitios web. El material de estos sitios web no forma parte de los materiales de este producto de IBM y la utilización de estos sitios web la realiza el usuario bajo su propia responsabilidad.

IBM podría utilizar o distribuir la información que se le envía de la forma que considere más adecuada sin incurrir por ello en ninguna obligación con el remitente de la información.

Los propietarios de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido este) y (ii) el uso mutuo de la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones adecuados, incluyendo en algunos casos, el pago de una tarifa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para él lo proporciona IBM, de acuerdo con los términos del contrato con el cliente de IBM, del contrato internacional de programas bajo licencia de IBM o de cualquier acuerdo equivalente entre ambos.

Todos los datos de rendimiento contenidos en el presente documento se han determinado en un entorno controlado. Por consiguiente, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Es posible que algunas medidas se hayan tomado en sistemas que se están desarrollando y no se puede garantizar que dichas medidas serán iguales en los sistemas disponibles en general. Es más, es posible que algunas medidas se hayan estimado efectuando extrapolaciones. Los resultados reales pueden variar. Los usuarios de este documento deberán verificar los datos aplicables a su entorno específico.

La información relativa a productos que no son de IBM la han proporcionado los proveedores de dichos productos, sus anuncios publicados u otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión de su rendimiento, su compatibilidad ni ningún otro aspecto relacionado con los productos que no son de IBM. Las preguntas relativas a las posibilidades de los productos que no son de IBM deberán dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a la dirección o intenciones futuras de IBM están sujetas a cambios o pueden retirarse sin aviso previo y representan únicamente metas y objetivos.

Todos los precios de IBM indicados únicamente son los precios recomendados por IBM para la venta al menor y están sujetos a cambios sin aviso previo. Los precios de los distribuidores pueden variar.

Esta información se proporciona únicamente para fines de planificación. La información contenida en el presente documento está sujeta a cambios antes de que los productos descritos salgan al mercado.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos los nombres son ficticios y cualquier parecido con nombres y direcciones utilizados por una empresa real son simple coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente que ilustran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir dichos programas de ejemplo bajo cualquier forma y sin tener que abonar una cuota a IBM, a fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación adaptados a la interfaz de programación de aplicaciones de la plataforma operativa para la que se han escrito los programas. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por consiguiente, IBM, no puede garantizar ni presuponer la fiabilidad, capacidad de servicio o funcionamiento de dichos programas. Puede copiar, modificar y distribuir libremente estos programas de ejemplo, sin pagar por ello a IBM, con la finalidad de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a las interfaces de programación de aplicación de IBM.

Todas las copias o fragmentos de las copias de estos programas de ejemplo o cualquier trabajo que de ellos se derive, deberán incluir un aviso de copyright como el que se indica a continuación:

© IBM 2013. Partes de este código provienen de Programas de ejemplo de IBM Corp. © Copyright IBM Corp. 2013. Reservados todos los derechos.

Si visualiza esta información en copia software, es posible que las fotografías y las ilustraciones en color no se vean.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas comerciales o marcas registradas de International Business Machines Corp., en muchas jurisdicciones en todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Existe una lista actualizada de las marcas registradas de IBM en la web, en la sección “Copyright and trademark information” en www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript y todas las marcas registradas basadas en Adobe son marcas registradas o comerciales de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

IT Infrastructure Library es una marca registrada de Central Computer and Telecommunications Agency, que ahora forma parte de Office of Government Commerce.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas comerciales o marcas registradas de Intel Corporation o de sus subsidiarias en Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

ITIL es una marca registrada y una marca registrada de comunidad de Minister for the Cabinet Office, registrada en la Oficina de patentes y marcas registradas de EE.UU.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Java y todas las marcas comerciales basadas en Java son marcas comerciales o marcas registradas de Oracle y/o sus filiales.

Cell Broadband Engine es una marca registrada de Sony Computer Entertainment, Inc., en Estados Unidos y/o en otros países y se utiliza bajo la licencia de la misma.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium y el logotipo de Ultrium son marcas registradas de HP, IBM Corp. y Quantum en los Estados Unidos y en otros países.

Índice

Caracteres Especiales

*REGEX 355

A

a Linux 568
a UNIX 568
a Windows 568, 569
AAGP
  Véase Perfil de grupo de autorización de acceso
acerca de esta guía xiii
Active Directory, Microsoft 127
  autenticación de servidor de supervisión
    límites de ID de usuario 142
  Autenticación del usuario LDAP 127
  cuentas de usuarios 148
    scripts de recopilación de datos 132
  esquema de LDAP
    esquema de objetos/atributos de usuario 128
    personalizaciones 127
  herramientas de LDAP 144
    ldapbrowser 146, 149, 153
    ldapsearch 145, 152
    LDP.ex 144
    LDP.exe 153
  IBM Tivoli Monitoring
    jerarquía de OU creada para 128
    sincronización de 132
  repositorio de LDAP
    configuración para comunicaciones de SSL 150
    configurar para comunicaciones TLS/SSL 141
    correlación de nombres distinguidos para 141
    definición 135
actuación
  para solicitudes SOAP 581
actualizar agente 296
Adaptador de Discovery Library 601, 603, 604
  z/OS 607
administración
  ¿Qué hace un administrador del sistema? 5
administración de usuarios 163
  aplicaciones 169
  controles principales 178
  gestión de los ID de usuario 171
  gestionar grupos de usuarios 175
  ID de inicio de sesión SYSADMIN 178
  ID de usuario para Dashboard Application Services Hub 179
administración de usuarios *(continuación)*
  ID de usuario para mandatos de actuación 181
  ID de usuario y grupos 179
  miembros 171
  modalidad de administración de espacios de trabajo 178
  otorgar acceso a usuario 179
  permisos 165
  resolución de mensajes de error de inicio de sesión 182
  usuario predeterminado 179
  validar acceso de usuarios 180
  ventana Usuarios y grupos de usuarios 165
  vistas de Navigator 170
administrador del sistema 10
administrar usuarios 164
AF REXX 594
agente
  instalación 306
  ranura 258
agente de autodescripción
  agentes habilitados para SDA 317
agente de proxy de almacén
  registro de errores 518
Agente de resumen y poda
  limitaciones de Tivoli Common Reporting 540
agente de supervisión 291
  aplicar un parche mediante el portal 294
  asignar mediante el portal 291
  conectar con un servidor de supervisión diferente 299
  detención 293
  inicio 293
  reciclar 293
agentes
  autodescripción
    Véase agentes de autodescripción
agentes autónomos
  proceso duper para situaciones 79
agentes de autodescripción 300, 306
  códigos STATUS 309
  errores de instalación 309
  errores que se pueden reintentar 309
  errores terminales 309
  flujo de sucesos del servidor de supervisión 304
  habilitación en el agente 316
  habilitación en el servidor de supervisión remoto 315
  inhabilitación en el agente 316
  inhabilitación en el servidor de supervisión remoto 315
  inicialización 312
  opciones de instalación 311
  reanudar 312
  renovación automática 312
  suspender 312
agentes de autodescripción *(continuación)*
  variables de entorno 319
agentes de enterprise monitoring 472
agentes de supervisión
  Véase también agentes de enterprise monitoring
  borrar la tabla Estatus de despliegue 297
  configurar mediante el portal 293
  gestión con el cliente de portal 291
  mantener configuración centralizada 447
  supervisar su disponibilidad 328
agentes de Tivoli Enterprise Monitoring
  Véase agentes de enterprise monitoring
agentes del supervisor del sistema
  iniciación de la configuración centralizada 473
  Servicios de gestión de agentes en 346
AIX 577
ajuste
  Tivoli Data Warehouse 510
alertas SNMP 378
  archivo de configuración de condiciones de excepción de ejemplo 378
  configuración 378
  especificación XML de condición de excepción 380
  procedentes de agentes con subnodos 344
  reglas OMNIbus de ejemplo 393
almacén de datos
  ajuste 510
  planificación de capacidad 510
almacén de datos permanentes 536
almacenar datos en base de datos 523
añadir sistema gestionado 291
aplicación REXX de SA IO 596
archivo atr 426
archivo de entorno
  servidor de automatización 81
  servidor de portal 73
  servidor de supervisión 78
archivo de entorno as.ini 81
archivo de entorno ms.ini 78
archivo de entorno qi.ini 73
archivo histórico a corto plazo 523
archivo KASENV 81
archivo KBBENV 78
archivo plano delimitado 523
archivo stash 241
archivos de datos históricos
  en z/OS 535
  tablas predeterminadas 522
archivos de metadescripción 520
arreglos, obtención 624
ASCII y no ASCII
  ID de usuario 171

© Copyright IBM Corp. 2005, 2013

asistente de soporte 623
AT, mandato en un sistema Windows 526
atajo para iniciar el cliente de escritorio 21
atributo de acumulación krarloff 531
atributo KPDXTRA 533
auditar
  política de autorización 204
auditoría
  Actuación 253
  archivo de registro 243
  ejemplo de XML 249
  niveles de rastreo 243
  tacmd executecommand 253
  tipos de registros de sucesos 243
  variables de entorno 251
  XML correlacionado con atributos 245
autenticación
  habilitación 83
  mediante Active Directory 127
  migrar 124
  utilización del registro LDAP externo 127
autenticación de usuarios 86, 89, 90, 91
  hoja de ruta para el inicio de sesión único utilizando LDAP 100
  inicio de sesión único 98
  mediante Active Directory 127
  nuevos usuarios LDAP 123
  servidor de automatización 126
  servidor de portal 94
autonomía
  Véase autonomía del agente
autonomía del agente
  agente
    registro de operaciones 617
  funciones 331
  interfaz de servicio 416
  introducción 331
  prueba SNMP de OMNIbus 391
  registro de actividad 617
  variables de entorno 335
  z/OS 479
ayuda en línea 23

B

BAROC
  generador de archivos 278
base de datos de claves, creación 238
base de datos de TEPS
  poda de sucesos 75

C

cerrar
  suceso 265
certificado
  certificado con firma propia, utilización 240
  creación de una solicitud de certificado de entidad emisora de certificados 239
certificado *(continuación)*
  recepción de un certificado de entidad emisora de certificados 240
  solicitud de un certificado de entidad emisora de certificados 239
certificado autofirmado 240
certificado de entidad emisora de certificados
  recepción 240
  solicitud 239
cifrado asimétrico
  archivo stash 241
  base de datos de claves, creación 238
  certificado con firma propia, utilización 240
  certificado de entidad emisora de certificados, recepción 240
  configuración 215
  contraseña, guardar en archivo stash 241
  par de claves pública-privada, creación 239
  solicitud de certificado de entidad emisora de certificados, creación 239
clase de sucesos BAROC 267
claves de LTPA 121
cleardeploystatus.log 297
CLEARDEPLOYSTATUSFREQ 297
CLI 90, 296
CLI Política de autorización de Tivoli 196
CLI tivcmd 185
cliente
  en un entorno de emulación 67
  escritorio 8
  Java Web Start 8
  navegador 8
  parámetros globales 61
  utilizar SOAP 578
cliente de escritorio 8
  creación de un atajo para iniciar utilizando Web Start 21
  descarga desde el servidor de portal 19
  inicio 16
  múltiples instancias 21
  registros, ubicación de 18
cliente de escritorio de portal
  descarga con IBM Java Web Start 16
  inicio 16
cliente de navegador 8
  establecimiento de propiedades para Linux o UNIX 70
  habilitar varias instancias 22
  inicio 16
  Linux o UNIX
    establecimiento de propiedades del cliente de navegador 70
  paquetes de archivo y cookies 14
  permisos de Windows 15
  personalizar el mensaje de cabecera 15
  valores de seguridad de IE 14
Cliente de navegador 13
cliente de navegador de portal
  inicio 16
cliente de portal
  cliente de portal 62
  parámetros 62
  variables 62
CMS_DUPER 79
componentes 6
comportamiento de agente autónomo
  limitaciones de las situaciones 343
comunicaciones
  factor de interconexión 65
  intervalo de latido 64
  servidor de proxy HTTP 66
condiciones de excepción SNMP
  configuración de la prueba Trapd de múltiples hebras de OMNIbus 391
Conector ITM 284
Conector OMNIbus 286, 289
Conector TEC 285, 288
conexión
  proveedor de datos de panel de instrumentos 53
configuración centralizada 447
  arranque 471
  configuración de muestra 467
  Disp=Custom security 453
  especificación XML 452
  iniciación con despliegue remoto 475
  iniciación con un archivo de lista de carga 474
  iniciación con una solicitud de interfaz de servicio 477
  iniciación con variables de entorno del agente 472
  palabras clave para lista de carga 460
  planificación 448
  seguridad AAGP 417
  variables de entorno 462
  visión general 447
configuración de OMNIbus para recibir alertas SNMP 391
configuración del entorno
  servidor de portal 72
configurar
  conector 283
  consola de sucesos comunes 283
Configurar agente de resumen y poda, ventana 514
configurar autenticación 89, 90, 91
configurar un sistema gestionado 293
conservar 14
consola de administración 111
  configurar servidor LDAP externo 113
Consola de administración de TEPS/e
  detener 115
  habilitar 111
  iniciar 111, 115
  para cambiar DN base 111
  SSL entre el servidor de portal y el servidor LDAP 111
  TEPS/e 115
consola de sucesos 267
consola de sucesos comunes 283
  columna adicional 288
consultas
  copia de seguridad 565

consultas *(continuación)*
de k<cp>.atr en la Interfaz de servicio del agente 426
contraseña, guardar en archivo stash 241
contraseñas
cifrar en archivo de configuración de condiciones de excepción 389
conversión de datos
automática para sistemas z/OS 532
en un sistema UNIX 529
utilización de KPDXTRA en PDS 533
conversión de UNIX 530
conversión en una vez 530
conversión manual 530
convertir
tablas de datos históricos a corto plazo 529
cookie 14
copia de seguridad
consultas 565
correlación
columna personalizable 289
columnas personalizables 288
correlación genérica 258
corto plazo, historial
limitación de tamaño de archivo 522
programas de conversión de datos 520
crear un atajo 21
CT_*, métodos de SOAP 582
CT_Get 594
CTIRA_HIST_DIR 488, 528

D

daemon de inicio de sesión 299
Dashboard Application Services Hub
ID de usuario 179
importación de informes de IBM Cognos 558
paneles de control personalizados 55
datos, conversión
automática para sistemas z/OS 532
datos históricos
gestión 481, 484
impacto de grandes cantidades recopiladas 489
tacmd 484
datos históricos, conversión 520
en HP NSK 531
en IBM i 528
en Linux o UNIX 529
en Windows 526
en z/OS 532
de la sincronización de sucesos 264, 289
cambio de la configuración 264
sitconfig.sh, mandato 264
definir
servidor de supervisión
Véase TEMS
dependencia del agente de sistema operativo 603
descripción de la situación 257
desde Linux 569
desde UNIX 569
desde Windows 568
despensa de datos 491
detención de un agente de supervisión 293
developerWorks 621
diagrama 594
directorio ATTRLIB 495
directorio IFS 528
disableLDAPRepository.sh 123
DLA 601
duplicar información de sucesos 289

E

EIF 274
especificación XML de correlación de sucesos 399
especificación XML de destinos de sucesos 405
XML de configuración de sucesos 396
ejemplo
despensa de datos
script SQL 491
elemento raíz ConfigurationArtifact 453
Elemento SNMP 380
elemento StatTrap 387
elemento TrapDest 381
eliminar agente 295
emisiones del agente y de alertas MIB para SNMP
agentSitPureEvent 390, 611
agentSitSampledEvent 390, 611
agentStatusEvent 390, 611
en el servidor de sucesos
Véase TEC
Enterprise Integration Facility
programa de utilidad TEDGEN 275
Soporte de varias consolas (MCS 275
Entorno 17
entornos de ejecución de IBM
instalación 17
Linux 18
Windows JRE 17
error APPN 580
espacio de trabajo
parámetro de historial 64
especificación XML de condición de excepción 380
Situation 384
SNMP 380
StatTrap 387
TrapAttrGroup 383
TrapDest 381
especificar navegador 23
Event Integration Facility
alteración temporal de los valores predeterminados 272
Event Integration FacilitycreateEventDest
editar la configuración 269
tacmd 269
eWAS
importación de certificados 235
Explorador de requisitos previos de informe de agentes de SO 556
exportación de claves de LTPA 121
exportar
base de datos de servidor de portal 567
expresión regular 355

F

formato de atributos 531, 533
funcionamiento
resumen 594

G

generar 594
gráficos
personalizar mensaje de cabecera del portal 15
Grupos de sistemas gestionados
seguridad 185
grupos de usuarios 175
añadir 176
eliminación 178
revisar y editar 177
ver miembros 175
GSKit
configuración de JRE e inicio del gestor de claves 238

H

habilitación del rastreo para JRE 18
herramienta de programa de utilidad de comprobación de reglas 267
Herramienta de publicación de esquemas
creación de tablas de dimensiones de Tivoli Common Reporting 545
historial
acerca de la recopilación de datos 481
cambiar directorio a corto plazo 488
conversión de corto plazo a archivo plano 524
parámetro de espacio de trabajo 64
prácticas recomendadas 510
privada 370
Véase historial privado
recopilación de datos 9
registro de errores de proxy de almacén 518
registro de operaciones del agente 519
resumen y poda 507
solicitud de interfaz de servicio 441
historial privado 348
Informe de la Interfaz de servicio del agente 425
histórico
ubicación de archivo en Windows 527
HP NonStop Kernel 531
HP NSK
utilización del programa de acumulación krarloff en 531
HTTP
habilitación del servidor proxy 69
habilitar servidor proxy 69

HTTP *(continuación)*
mandato kshsoap 580

I

IBM i
datos históricos, conversión 528
IBM Java Web Start
utilización para descargar el cliente de escritorio 16
IBM JRE
instalación 17
IBM Redbooks 623
IBM Support Assistant 623
IBM Tivoli Enterprise Console
integración de sucesos 255
IBM Tivoli Monitoring
componentes 6
proveedor de servicios de Performance Monitoring 10
ejecutar en sistemas HP NSK 531
integración con 127
para productos WebSphere MQ 531
IBM Tivoli Monitoring Web Services 574
adición de usuarios 575
casos de ejemplo 594
contenido de informe 597
descripción de SOAP y URL 573
ID de usuario 579
inicio del cliente 579
métodos SOAP predefinidos 582
presentación 573
SOAP, cliente 578
solicitud CT_Get de SOAP de ejemplo 593
solicitudes de segundo nivel 591
solicitudes SOAP como mandatos de sistema 581
ID de usuario 118, 171
añadir ID de usuario 171
eliminar un ID de usuario 174
grupo de usuarios de Windows 15
habilitar autenticación 83
IBM Tivoli Monitoring Web Services 579
usuario predeterminado 174
ver y editar un ID de usuario 172
importación de claves de LTPA 121
importar
base de datos de servidor de portal 567
base de datos del servidor de portal de y a un sistema Linux o UNIX 570
información del release 1
informes
Véase informes de IBM Cognos
Informes BIRT 560
configurar origen de datos 561
generar informe 562
importación de un informe 560
instalación de un informe 560
informes de IBM Cognos 556
crear un diagrama de Dashboard Application Services Hub 559
importación 558
informes de IBM Cognos *(continuación)*
importación mediante el instalador de informes 554
informes históricos
impacto de rendimiento de tablas grandes 490
iniciación de la configuración centralizada 472
iniciación de la configuración centralizada colocando el archivo 474
iniciar aplicación 23
inicio de sesión
control del número de intentos 77
inicio de sesión único 98, 120
hoja de ruta para el servidor de portal y el registro LDAP 100
no disponible con autenticación del servidor de supervisión 127, 147
inicio de un agente de supervisión 293
instalación 17
instalador de informes 554
instalar 17
instantánea de datos 594
Integrated Cryptographic Service Facility 71, 72
Integrated Service Management Library 621
Integrated Solutions Console
Véase Consola de administración de TEPS/e
interfaz de servicio del agente
inicio 416
Interfaz de servicio del agente 416
consultas 426
información de agente 423
informe histórico privado 425
iniciación de la configuración centralizada 478
situaciones 424
solicitud AGENTINFO 427
solicitud AGENTSTAT 440
solicitud ATTRLIST 429
solicitud CNFGCONTROL 443
solicitud HISTREAD 441
solicitud LISTSUBNODE 429
solicitud PVTCONTROL 438
solicitud READATTR 430
solicitud REPORT 432
solicitud SITSUMMARY 438
solicitud TABLESIT 436
solicitudes de interfaz de servicio 427
Internet Explorer
Opciones - Seguridad 14
ISA 623
itmc_kdy.properties 297
itmcmd history 529, 530
itmcmd history, ejecución en un sistema UNIX 530

J

Java 17
en un entorno de emulación 67
JRE en Windows para Java Web Start 17
Java Runtime Environment 13
Java Runtime Environment *(continuación)*
para GSKit 238
Java Web Start
descargar el cliente de escritorio 19
utilización para descargar el cliente de escritorio 16
Java Web Start, cliente 8
JRE 17
habilitación del rastreo para 18

K

kcacap.xsd 323
KD8_VM_IMPORT_ID 58
KFW_AUTHORIZATION_MAX_INVALID_LOGIN 77
KFW_MCS_XML_FILES 275
KFWENV, archivo 73
KHD_HISTSIZE_EVAL_INTERVAL 522, 523
KHD_TOTAL_HIST_MAXSIZE 522, 523
KMS_EVAL_REFLEX_AT_TEMS 79
KMS_OMTEC_GLOBALIZATION_LOC 259
KPDXTRA 533
DDNAMES a asignar 534
parámetros 534
KPDXTRA, programa
acerca de 533
mensajes 535
krarloff 524
kshsoap 580
KSY_Summarization_Config_DV 552
KSY_TRAM_ENABLE 544
KSY_TRAM_TD_GRANULARITY 544
KSY_TRAM_TD_INITIAL_LOAD 544
kwgcap.xsd 323

L

latido
XML de destino de EIF 405
LDAP 118
configuración de servidor de portal 105
configuración del servidor de portal 109
configurar un servidor externo 113
inhabilitar la autenticación del servidor de portal 123
nuevos usuarios 123
SSL para servidor de portal 116
ldapsearch 91
mandato de ejemplo (no TLS/SSL) 93
mandato de ejemplo con SSL 93
Lightweight Directory Access Protocol
Active Directory, Microsoft 127
línea de mandatos 90
Linux 290, 576
Linux_IP_Addres 552
Linux o UNIX
datos históricos, conversión 529
lista de carga de configuración 462, 474
especificación XML 452

lista de carga de configuración *(continuación)*
iniciación de la configuración centralizada con tacmd putfile 477
mandato kshsoap 478
palabras clave 460
variables de entorno 460
listas de control de accesos
seguridad 185
lz_situations.xml del sistema operativo Linux 365

M

Manage Tivoli Enterprise Monitoring Services 91
definir concentradores de SOAP 574
parámetros globales 61
MANAGEDSYSTEMLIST 544
MANAGEDSYSTEMLISTMEMBERS 544
mandato itmpwdsnmp 389
mandatos
sitconfig.sh 264
mandatos de actuación
ID de usuario para 181
memoria caché de sucesos 263
mensaje de cabecera en modalidad de navegador 15
mensaje de suceso 257, 274
mensajes de error de inicio de sesión 574
Método SOAP
CT_Acknowledge 582, 597
CT_Activate 583
CT_Alert 583, 596
CT_Deactivate 584
CT_EMail 585
CT_Execute 586
CT_Export 586
CT_Get 588, 593
CT_Redirect 589
CT_Reset 589
CT_Resurface 590
CT_WTO 591
Microsoft Management Console 133
conector ADSI Edit para 144
migración-importación 568, 569
de Linux o UNIX a Linux o UNIX 570
migrar
autenticación 124
modalidad de escritorio
parámetro databus 65
modalidad de navegador
retardo de conmutación de espacio de trabajo 65

N

Netcool/OMNIbus
certificado 414
EIF utilizando SSL 412
NetView
consola 279
nombre distinguido
correlacionar con ID de usuario TEP 172
nombres DD para KPDXTRA
en z/OS 534
nombres distinguidos 118
Consola de administración de TEPS/e 111
Notas técnicas (Technotes) 621
novedades de este release 1
NT_Computer_Information 552
nt_situations.xml del sistema operativo Windows 368

O

OMNIbus
alertas SNMP
automatización de latido de OMNIbus 395
automatización de latido 395
habilitación de la automatización de latido 395
integración de sucesos de situaciones de empresa 281
reglas de ejemplo para alertas SNMP 393
sucesos de EIF
automatización de latido de OMNIbus 395
sucesos de estatus de EE_HEARTBEAT 395
opciones de línea de mandatos de ldapsearch 92
OSLC-PM 10

P

palabras clave para lista de carga de configuración 460
panel de control 27
configurar
SSL, para el servidor de Dashboard Application Services Hub 222
SSL, utilización de certificados de terceros 220
crear paneles personalizados 55
hoja de ruta
migración a SSO y políticas 45
sin SSO ni políticas 27
SSO y políticas 32
KD8_VM_IMPORT_ID 58
SSL 219
UISolutions 58
paneles de instrumentos de gestión de infraestructura 27
paquete de agente común 323
par de claves pública-privada
creación 239
parámetro
barra de tareas de Windows 65
conjunto de códigos de codificación 64
databus para modalidad de escritorio en un servidor HTTP externo 65
despliegue de agente 62
parámetro *(continuación)*
edición global 61
factor de interconexión 65
historial de espacio de trabajo 64
host local de emulador de terminal 65
identificador de cliente de rastreo 63, 66
intervalo de latido 64
llamadas de rastreo con hebras 67
máximo de script de terminal 65
nombre de archivo de rastreo 66
opción de rastreo 67
pausa de sonido de suceso 65
profundidad de cola de hebras de rastreo 67
puerto de emulador de terminal 65
rastreo local o remoto 67
retardo de conmutación de espacio de trabajo 65, 66
sensibilidad de arrastre de ratón 64
servidor de proxy HTTP 66
sesiones de terminal activas 65
solicitud de aviso de cambio de vista 66
tamaño de adjunto 62
tamaño de página de vista 63
tipo de emulador de terminal 65
user.language 67
user.region 68
parámetro de ajuste 267
parámetro de integración 267
parámetros
Véase variables de entorno
parámetros globales 61
PDS 536
Perfil de grupo de autorización de acceso 417, 453
personalización de la conversión de historial 530
planificación
conversión de datos históricos 530
planificación de capacidad
Tivoli Data Warehouse 510
PolicyDistributor 195
política
solicitudes SOAP 581
procedimientos de archivado
utilización de mandato AT de Windows 526
proceso
kfwServices 73
proceso de conversión
en sistemas HP NonStop Kernel 531
Proceso de vigilancia de los Servicios de gestión de agentes 322
proceso de vigilancia de los servicios del agente de proxy 322
Proceso de vigilancia del agente 322
proceso duper 79
programa de acumulación krarloff
conversión de archivos en HP NSK 531
en HP NSK 531
en Linux o UNIX 529
en Windows 526
en z/OS 532

programa de acumulación krarloff *(continuación)*
IBM i 528
sistemas HP NonStop Kernel
datos históricos, conversión 531
Windows
datos históricos, conversión 526
z/OS
datos históricos, conversión 532
programa de arranque 462
programa de utilidad TEDGEN 275
proveedor de datos de panel de instrumentos
creación de una conexión 53
proveedor de servicios de Open Services Lifecycle Collaboration Performance Monitoring 10
proveedor de servicios de Performance Monitoring 10
proxy
parámetro de servidor HTTP 66
proxy de almacén
directorio ATTRLIB 495
putfile 477

R

rastreo
parámetros 67
reciclar un agente de supervisión 293
reconfigurar
cliente de navegador 120
reconocimientos retardados 577
recopilación de datos históricos
configurar resumen y poda 513
establecer límite de tamaño de archivo a corto plazo 522
impacto de rendimiento en solicitudes de datos grandes 489
recopilar el servidor de portal 565
requisitos previos 565
recurso de integración de sucesos
habilitar globalización 259
red privada 604
Redbooks 621, 623
REGEX 355
registro de auditoría de ITM 243
registro de operaciones 617
registro de operaciones del agente
recopilar historial 519
registros de auditoría 243
rendimiento, impacto
almacén 491
solicitudes de datos históricos de tablas grandes 490
requisitos previos
configurar autenticación 95
resolución de mensajes de error de inicio de sesión 182
resolución de problemas 623
applets java 13
cliente en un entorno de emulación 67
conexión 290
excepción Java 15
parámetros de rastreo 67
resumen y poda 483, 513
resumen y poda *(continuación)*
configuración 507
configuración global 514
descripción 507
disponibilidad de los datos 512
inhabilitar 517
Resumen y poda de sy_situations.xml 369
RoleAdministrator 194, 196
Runtime 17

S

script
máximo de terminal 65
script de migración-exportación 567
script de migración-importación 567
script enableISCLite.sh 154
script updateTEPSEPass.sh 154
seguridad
Véase también Perfil de grupo de autorización de acceso
basada en roles 185
Grupos de sistemas gestionados 185
listas de control de accesos 185
Servidor de políticas de autorización 185
servidor de portal para LDAP y SSO 94
seguridad de usuarios
configuración de un servidor de supervisión concentrador en Linux o UNIX 90
configuración para un servidor de supervisión concentrador en Windows 89
Service Management Connect 621, 623
Servicio de atributos MCS 275
Servicio web de representación gráfica de IBM Tivoli Monitoring 599
Servicios de gestión de agentes 321
características 321
en agentes del supervisor del sistema 346
gestión manual del agente 328
instalación y configuración 323
mandatos de actuación 328
supervisar la disponibilidad de agentes 328
Servicios web
configurar 576
Servicios web de Tivoli Monitoring
inicio del navegador 579
programa de utilidad de línea de mandatos 580
SOAP
programa de utilidad de línea de mandatos 580
servidor de configuración central
servidor web
como servidor de configuración central 448
servidor web como 448
Servidor de políticas de autorización 185
auditoría 204
Servidor de políticas de autorización *(continuación)*
casos de ejemplo
despliegue 208
despliegue, varios dominios con políticas independientes 210
despliegue, varios dominios con roles y políticas compartidas 209
gestión de políticas 192
gestión de políticas, basado en dominios 210
gestión de políticas, PolicyDistributor 195
gestión de políticas, RoleAdministrator 194
conceptos 186
configurar
SSL 223
SSL, preparación de la CLI política de autorización de Tivoli 227
SSL, preparación del servidor de portal 229
SSL, utilización de certificados de terceros 225
SSL, utilización de certificados de WebSphere 224
crear políticas, prácticas recomendadas 192
dominios, varios 207
grupos de roles 207
Interfaz de línea de mandatos (CLI) 196
prácticas recomendadas 192
preparación para habilitar 190
requisitos previos 207
roles, gestionar 196
roles, predefinidos 189
servidor de portal
Véase también Servidor de Tivoli Enterprise Portal
Véase también TEPS
autenticación de usuario mediante Active Directory 127
autenticación de usuarios 161
caso de usuario 152
correlación de ID de usuario con nombres distinguidos de LDAP 141
creación de ID de usuario y de permisos 133
habilitación de la autenticación de LDAP 141, 152
habilitar y configurar para Active Directory 134
conectar a uno diferente 21
copia de seguridad 565
exportar base de datos 567
habilitación de FIPS 230
importar base de datos 567
inhabilitación de la autenticación de LDAP 123
inicie la sesión en dos desde el mismo sistema 22
línea de mandatos de Linux o UNIX para configurar LDAP 109

servidor de portal *(continuación)*
Manage Tivoli Enterprise Monitoring Services para configurar LDAP 105
migrar autenticación 124
replicar 565
requisitos previos de replicación 565
servidor de portal 73
SSL para LDAP 116
variables 73
variables de entorno 73
servidor de supervisión
Véase también TEMS
autenticación de usuarios
caso de usuario 147
desventajas frente a la autenticación del servidor de portal 127, 147
habilitación y configuración 142
límites de ID de usuario 142, 147
mediante Active Directory 127
conectar el agente a uno diferente 299
migrar autenticación 124
servidor de supervisión concentrador 86, 89
configuración de la autenticación de usuarios en Linux o UNIX 90
configuración de la seguridad de usuarios en Windows 89
SSL con el servidor LDAP 218
Servidor de Tivoli Enterprise Portal
Véase servidor de portal
servidor HTTP
parámetro databus para especificar externo 65
servidor SOAP 594
adición de usuarios 575
configuración 574
definición de concentradores 574
seguridad 578
sincronización de sucesos de situación
IBM Tivoli Enterprise Console 263
sincronización de sucesos TEC 255
sistema gestionado
añadir mediante el portal 291
aplicar un parche mediante el portal 294
descripción 6
sistemas gestionados
configurar mediante el portal 293
sitconfig.sh, mandato 264
situación
parámetro de sonido 65
solicitudes SOAP 581
situación de muestra 265
situaciones
comportamiento de agente autónomo 343
estatus en Interfaz de servicio del agente 424
integración de sucesos con OMNIbus 281
privada
Véase situaciones privadas
proceso duper 79
situaciones de empresa exportadas 360
situaciones de empresa y situaciones privadas 348
situaciones privadas 348
características 348
de situaciones de empresa exportadas 360
ejemplos 365
especificación XML 351
iniciar, detener, reciclar 438
limitaciones 343
SMC 621, 623
SNMP
cifrado de claves 389
Elemento Situation 384
elemento XML TrapAttrGroup 383
tipos de sucesos de agente MIB 390, 611
SOAP 573, 577
inicio del navegador 579
servidor 576
SOAP (Simple Object Access Protocol - Protocolo de acceso a objetos simple), solicitudes de cliente 573
SOAP_IS_SECURE 578
solicitudes de cliente de SOAP 573
soporte de cliente 625
soporte de FIPS 230
Soporte de software 623
ponerse en contacto 625
recepción semanal de actualizaciones 624
SSL 222
archivo stash 241
base de datos de claves, creación 238
certificado con firma propia, utilización 240
certificado de entidad emisora de certificados, recepción 240
con proveedor de datos de panel de instrumentos 219
con Servidor de políticas de autorización 223
configuración de cifrado asimétrico 215
contraseña, guardar en archivo stash 241
entre el servidor de portal y el servidor LDAP 116
entre el servidor de supervisión concentrador y el servidor LDAP 218
gestión de certificados para Netcool/OMNIbus 414
par de claves pública-privada, creación 239
solicitud de certificado de entidad emisora de certificados, creación 239
sucesos de EIF 412
SSL entre el servidor de portal y el servidor LDAP 111
SSO 120
subnodos de agente
distribución de historial privado 351
limitaciones de las situaciones 344
suceso de situación 274
sucesos
control del tamaño de adjuntos 76
sincronización de IBM Tivoli Enterprise Console 263
sucesos de EIF
ciclo de vida 409
enviar directamente de agente a receptor 396
latido 410
ranuras comunes 407
restablecimiento maestro 411
SSL 412
sucesos de latido 410
sucesos de situación
correlación 255
Summarization and Pruning agent
automatización de la tabla de informes 543
supervisión
Servicios de gestión de agentes 321
Support Assistant 623
sysadmin 83
SYSADMIN 178

T

tabla Estatus de despliegue 297
tacmd 477
bulkExportPcy 565
bulkExportSit 348, 360, 565
bulkImportPcy 565
bulkImportSit 565
createSit 348, 573
exportNavigator 565
exportQueries 565
exportSitAssociations 565
exportSysAssignments 565
exportworkspaces 565
histconfiguregroups 335, 507
importNavigator 565
importQueries 565
importSitAssociations 565
importSysAssignments 565
importworkspaces 565
setOverride 335, 373
updateAgent 296
viewSit 360
z/OS
variables de entorno del agente 335
tacmd addSdaInstallOptions 311
tacmd deleteSdaInstallOptions 311
tacmd editSdaInstallOptions 311
tacmd listappinstallrecs 306
tacmd listSdaInstallOptions 311
tacmd listSdaStatus 306
tacmd refreshTECinfo
createEventDest 272
tacmd resumeSda 311, 312
tacmd setAgentConnection 299
tacmd suspendSda 311, 312
tamaño de página de vista de gráfico 63
tamaño de página de vista de tabla 63
tamaño máximo de directorio 523
TCP 577
TEP
Véase Tivoli Enterprise Portal

TEPS/e
  detener 115
  iniciar 115
Tivoli Common Reporting 537
  Actualización desde un release anterior 540
  cliente de base de datos sobre ODBC 557
  comprobación de estado para creación de informes 556
  conexión con Tivoli Data Warehouse 557
  crear un diagrama de Dashboard Application Services Hub 559
  Explorador de requisitos previos de informe de agentes de SO 556
  información relevante 537
  Informes BIRT 560
  informes de IBM Cognos 556
  instalador de informes 554
  limitaciones 540
  requisitos previos 538
  tablas de dimensiones 542
    automatización 543
    configure Summarization and Pruning agent 544
    tabla de dimensiones de recursos 552
    tabla de dimensiones de tiempo 548
    tablas de dimensiones compartidas 548
    utilización de la herramienta de publicación de esquemas 545
Tivoli Data Warehouse
  ajuste 510
  configuración de historial a corto plazo 493
  configurar para Tivoli Common Reporting 542
  historial
    configuración del archivo a corto plazo 493
  migraciones de particiones por rangos 496
    para DB2 en Linux, UNIX y Windows 497
    para DB2 en z/OS 500
    para Oracle 504
  planificación de capacidad 510
Tivoli Enterprise Console
  estatus de suceso de situación 260
  gravedad de suceso 259
  vista 279
Tivoli Enterprise Monitoring Automation Server
  variables de entorno 81
    editar 81
Tivoli Enterprise Portal 295
  cliente 6
  descripción 6, 8
  novedades de este release 1
  tipos de cliente 8
Tivoli Management Services
  componentes 6
Tivoli Monitoring Service Index
  Interfaz de servicio del agente 416
Tivoli Servidor de políticas de autorización
  Véase Servidor de políticas de autorización
TLS
  Véase SSL
TMS DLA 601
tmsdla 601

U

UISolutions
  importar 58
Universal Agent
  sucesos en Tivoli Enterprise Console 278
UNIX 576
UNIX_IP_Address 552
UNIX o Linux
  datos históricos, conversión 529
URL 14
URL ior 65
USE_EGG1_FLAG 71
user.language 67
user.region 68
Usuarios, privilegios de grupo 15
ux_situations.xml del sistema operativo UNIX 367

V

validación de usuarios 86
  Véase autenticación de usuarios
valores de seguridad 14
variable de entorno de servidor de portal
  KFW_ATTACHMENT_SEGMENT_MAX 76
  KFW_ATTACHMENT_MAX 76
  KFW_EVENT_RETENTION 75
  KFW_PRUNE_END 75
  KFW_PRUNE_START 75
variables de entorno
  agente 527
  autonomía del agente 335
  CMS_DUPER 79
  KCA_CAP_DIR 323
  KCA_CMD_TIMEOUT 323
  KCA_MAX_RETRIES_ON_PIPE 323
  KMS_EVAL_REFLEX_AT_TEMS 79
  lista de carga de configuración 460
  servidor y cliente de configuración central 462
  SOAP_IS_SECURE 578
variables de entorno de servidor de portal
  KFW_AUTHORIZATION_MAX_INVALID_LOGIN 77
ventana
  Editar parámetros de Tivoli Enterprise Portal 61
ventana de configuración 283
vista de terminal
  parámetros 65
vista física de Navigator 291

W

warehouse_situations.xml de Tivoli Data Warehouse 370
WAREHOUSEID 493
Web Services 573
  definición de concentradores 574
Web Start 21
WebSphere Application Server incorporado 235
Windows
  grupo de usuarios 15
  ubicación de archivos de tabla de datos históricos 527
  ubicación de archivos ejecutables 527
Windows, mandato AT de sistemas 526

X

XML
  Véase también archivos de configuración locales
  AGENTINFO 427
  AGENTSTAT 440
  ATTRLIST 429
  CNFGLIST 452
  codificación UTF-8 345
  EVENTDEST 396
  EVENTMAP 396
  historial privado 351
  HISTREAD 441
  LISTSUBNODE 429
  PVTCONTROL 438
  READATTR 430
  REPORT 427, 432
  SITSUMMARY 427, 438
  situaciones privadas 351
  situation_name (exportado) 360
  TABLESIT 436
  THRESHOLDS 373
  TRAPCNFG 378, 380
  z/OS
    XML codificado en UTF-8 345
XML codificado en UTF-8 345
XML de alteraciones de umbral 373
XML de alteraciones temporales 373

Z

z/OS
  alertas SNMP en PCTRAPS 378
  autonomía del agente 331, 479
  conversión de datos mediante KPDXTRA 533
  historial privado y PDS 370
  Integrated Cryptographic Service Facility 71, 72
  LDAP no soportado en concentrador 83
  procedimiento de archivado manual 536
  RACF o ACF/2 para validación de usuarios 180
  ubicación de archivos de datos históricos 535

Impreso en España

SC22-5446-00