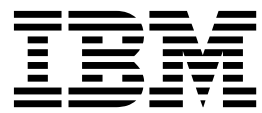


IBM Cognos Analytics
Versión 11.0

Guía de administración y seguridad



©

Información sobre el producto

Este documento se aplica a IBM Cognos Analytics Versión 11.0.0 y puede aplicarse también a las versiones posteriores.

Copyright

Licensed Materials - Property of IBM

© Copyright IBM Corp. 2005, 2018.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, el logotipo de IBM y ibm.com son marcas comerciales o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de otras compañías. Hay disponible una lista actual de marcas registradas de IBM en la web en “Información de copyright y marcas registradas” en www.ibm.com/legal/copytrade.shtml.

Los términos siguientes son marcas registradas de otras empresas:

- Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos o en otros países.
- Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos o en otros países.
- Linux es una marca registrada de Linus Torvalds en los Estados Unidos o en otros países.
- UNIX es una marca registrada de The Open Group en los Estados Unidos o en otros países.
- Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle o sus filiales.

Captura(s) de pantalla de producto de Microsoft utilizadas con permiso de Microsoft.

Contenido

Introducción	xiii

Capítulo 1. Administración del software de IBM Cognos	1

IBM Cognos Administration	1
Habilitación de la salida de informe accesible en todo el sistema	2
Tareas automatizadas	3
Configuración de un entorno de creación de informes multilingüe	4
Configuración de la base de datos para la creación de informes multilingüe	6
Instalación de fuentes	6
Fuente predeterminada de IBM Cognos	7
Fuentes de Creación de informes	7
Configuración de impresoras	7
Configuración de navegadores web	8
Concesión de acceso de usuario a informes de Series 7	12
Restricción de acceso al software de IBM Cognos	13

Capítulo 2. Compilación de aplicaciones de IBM Cognos Analytics	15

Capítulo 3. Configuración del registro	17

Mensajes de registro	18
Niveles de registro	18
Establecimiento de niveles de registro	21
Informes de auditoría	22
Configuración de la creación de informes de auditoría	22
Visualización detallada de los mensajes de error de protección	23
Inhabilitación de la creación de archivos principales de volcado	24
Utilización del registro para diagnosticar un problema para un usuario específico	24
Ejecución del registro para un usuario específico mediante la edición de archivos ipf específicos del componente	25
Ejecución del registro para un usuario específico mediante la utilización de categorías seleccionadas	26
Inhabilitación del registro para un usuario específico	27

Capítulo 4. Métricas de rendimiento del sistema	29

Cómo recopilar datos de métricas	29
Métricas del sistema	30
Paneles de la página de estado del sistema	42
Evaluación del rendimiento del sistema	44
Visualización de atributos de las puntuaciones de métrica	45
Establecimiento de los valores del umbral de la métrica	45
Restablecimiento de métricas	46
Restablecimiento de las métricas del sistema	47
Renovación de las conexiones de servicio de informes	47

Capítulo 5. Administración del servidor	49

Asignadores y servicios	49
Detención e inicio de asignadores y servicios	52
Servicio de Content Manager activo	54
Eliminación de asignadores del entorno	55
Agrupación de asignadores en carpetas de configuración	57
Direccionamiento avanzado de asignadores	58
Especificación de correlaciones de pasarela para datos de PowerPlay de IBM Cognos Series 7	61
Cambio de nombre de asignadores	61
Prueba de los asignadores	62
Migración tras error para varios asignadores	63

Protección de asignadores	64
Especificación de los asignadores para albergar el servidor proxy JMX.	65
Ubicaciones de Content Manager	66
Establecimiento de parámetros avanzados de Content Manager	66
Establecimiento del límite de tamaño de caché para el caché de Content Manager.	69
Reducción de la carga de Content Manager almacenando los archivos de sesión de usuario localmente.	69
Anular el procesamiento local predeterminado en el caché de solicitud	70
Tareas de mantenimiento del almacén de contenido	71
Antes de iniciar el mantenimiento interno del almacén de contenido	71
Mantenimiento del almacén de contenido en espacios de nombres externos	72
Creación de una tarea de mantenimiento del almacén de contenido	73
Ejecución de una tarea de mantenimiento del almacén de contenido	73
Inicio y detención de actividades en segundo plano	74
Ajuste del rendimiento de servidor	74
Establecer grupos de servidores para direccionamiento avanzado de asignadores	75
Equilibrado de las solicitudes entre los asignadores	75
Equilibrio de la carga de los asignadores con factor de solicitudes en curso	76
Establecimiento de la propiedad de equilibrio de la carga de los asignadores en el modo compatible con clúster	78
Establecimiento de periodos de máxima actividad de uso	79
Número máximo de procesos y conexiones	80
Cómo especificar límites de tiempo en cola	82
Valores de archivos PDF	83
Establecimiento del tiempo máximo de ejecución	87
Cómo especificar el tiempo que se deben guardar las salidas de informe de la lista de observación	88
Cómo limitar zonas activas generadas en un gráfico de Analysis Studio o Creación de informes	89
Cómo establecer el límite de tamaño de informe para el servicio de datos de informes	89
Excluyendo el ID de contexto para un agente de las tareas de servicio web IBM WebSphere	90
Ajuste de memoria caché para el servicio de repositorio	90
Limpieza masiva de tablas NC	91
Ejecución simultánea de consultas	92
Establecer parámetros para la ejecución simultánea de consultas.	94
Establecimiento de la prioridad de consultas	94
La conversión de claves de búsqueda numérica a cadenas en consultas	96
Almacenamiento de la sesión en la memoria caché	97
Inhabilitar la memoria caché de la sesión a nivel del servidor	98
Cómo inhabilitar el almacenamiento de la sesión en la caché en el nivel del paquete o el informe	98
Habilitación del parámetro HTTPOnly para asegurar la cookie del pasaporte CAM	99
Reducción de la precisión decimal.	99
Almacén de objetos externos para almacenar la salida de informe localmente	100
Resultado del informe guardado	100
Guardar archivos de resultados de informes fuera del software IBM Cognos	101
Guardar archivos de resultado de informes en el software IBM Cognos	102
Configuración del informe y los servicios de informe por lotes para usar las hojas de trabajo grandes.	103
Cambio de nombre de forma dinámica de las pestañas de la hoja de trabajo en los informes en Excel 2007	104
Configuración de la solución de linaje	104
Configuración del URI de InfoSphere Business Glossary	106
Configuración del URI de descubrimiento de colaboración	106
Habilitación de métricas de cola de tareas, trabajos y SMTP	107
Establecimiento de la duración de las tareas humanas y las anotaciones terminadas (comentarios)	108
Cambiar el comportamiento del filtro de acceso a detalles	109
Control sobre si los parámetros URL se envían a Content Manager	110
Impresión desde sistemas operativos UNIX	110
Añadir los dominios de Cognos Workspace a la lista de dominio válida	111
Cómo evitar el bloqueo del almacén de contenido al añadir o actualizar un gran número de planificaciones.	111

Capítulo 6. Orígenes de datos y conexiones 113

Tipos de orígenes de datos	114
Orígenes de datos de IBM Db2	114
Cubos de IBM Cognos	116
Origen de datos Oracle Essbase	120
IBM InfoSphere Warehouse Cubing Services	124

Orígenes de datos Informix	124
Orígenes de datos de Microsoft Analysis Services	125
Orígenes de datos de Microsoft SQL Server	130
Conexiones con orígenes de datos ODBC	133
Orígenes de datos Oracle	135
Conexiones de origen de datos del repositorio externo	136
Orígenes de datos SAP Business Information Warehouse (SAP BW)	138
Orígenes de datos de Sybase Adaptive Server Enterprise	141
Orígenes de datos de TM1	142
Orígenes de datos XML	144
Conexiones de origen de datos	146
Creación de una conexión de origen de datos	147
Añadir una conexión nueva	153
Modificación de una conexión existente	153
Cambio de los valores de conexión	154
Parámetros de conexión dinámica en las conexiones JDBC	155
Inicios de sesión de orígenes de datos	156
Creación de un inicio de sesión	156
Modificación de un inicio de sesión	157
Niveles de aislamiento	158
Transferencia de contexto de IBM Cognos a una base de datos	160
Bloques de comandos	161
Uso de atributos de conexión de IBM Db2 CLI para Db2	167
Uso de contexto de aplicación en SQL dinámico	169
Despliegue de PowerCubes actualizados	171
Protección de orígenes de datos	172
Capítulo 7. Administración de Query Service	175
Configuración de las propiedades de servicio de consultas	175
Administración de almacenamiento en caché de Query Service	178
Borrar todo lo almacenado en la memoria caché	178
Análisis del uso de la memoria caché	178
Creación y planificación de tareas de administración del servicio de consultas	179
API de línea de comandos de Query Service	181
Capítulo 8. Cómo hacer una copia de seguridad de los datos	183
Copia de seguridad del almacén de contenido	183
Copia de seguridad de los proyectos y modelos de Framework Manager	184
Capítulo 9. Archivado de contenido de IBM Cognos	185
Configurar el archivado de contenido	187
Creación de una ubicación de archivo para un repositorio del sistema de archivos	187
Importación de definiciones de clases personalizadas y propiedades en IBM FileNet Content Manager	188
Importación de definiciones y propiedades de clases personalizadas en IBM Content Manager 8	188
Especificación de una hora disponible para ejecutar el proceso de archivado	190
Especificación del tiempo de ejecución de subprocessos	190
Archivado de formatos seleccionados de salidas de informe	191
Indicación de que las especificaciones de informe no han de archivar	192
Administrar el archivado de contenido	192
Especificación de un repositorio externo para la salida de informe	193
Creación de tareas de mantenimiento de archivado de contenido	193
Creación de una tarea de mantenimiento de actualización de regla de conservación	194
Creación de una tarea de mantenimiento de eliminación de contenido	195
Búsqueda de contenido en el repositorio externo	196
Búsqueda de contenido archivado	197
Capítulo 10. Modelo de seguridad	199
Proveedores de autenticación	199
Supresión o restauración de espacios de nombres no configurados	201
Autorización	202

Espacio de nombres de Cognos	202
IBM Cognos Application Firewall	203
Validación y protección de datos	203
Registro y supervisión	204
Capítulo 11. Usuarios, grupos y roles	207
Usuarios	207
Entornos locales del usuario	208
Grupos y roles	208
Creación de un grupo o un rol de Cognos	210
Adición o eliminación de miembros de un grupo o un rol de Cognos	211
Capítulo 12. Permisos de acceso y credenciales	213
Establecimiento de permisos de acceso para una entrada	220
Credenciales de confianza	222
Creación de credenciales de confianza	223
Administración de sus propias credenciales de origen de datos	224
Cómo guardar credenciales de origen de datos	224
Visualización y eliminación de sus credenciales de origen de datos	225
Capítulo 13. Funciones y características protegidas.	227
Establecimiento del acceso a funciones o características seguras	235
Capítulo 14. Capacidades de objetos	239
Configuración de las capacidades de objeto de un paquete	241
Capítulo 15. Seguridad inicial	243
Entradas incorporadas	243
Roles predefinidos.	244
Roles no de licencia	245
Roles de licencia	246
Permisos predeterminados basados en licencias	247
Asignación de capacidades según roles de licencia	254
Escenario de actualización: Si los roles personalizados tienen los mismos nombres que los roles de licencia más recientes	254
Valores de seguridad después de la instalación	254
Protección de Administradores del sistema y roles predefinidos	255
Protección del espacio de nombres de Cognos	255
Protección del almacén de contenido	256
Capítulo 16. Propiedades de la entrada	257
Propiedades generales	257
Propiedades de informe de Report, Query, Analysis y PowerPlay	259
Propiedades del trabajo	261
Propiedades del agente	261
Propiedades de reglas	262
Capítulo 17. Gestión de actividades.	263
Gestión de actividades actuales	263
Gestión de actividades pasadas	265
Gestionar las próximas actividades para un día específico	265
Actividades suspendidas	267
Suspensión de entradas	267
Visualización de las entradas suspendidas de un día determinado.	268
Gestión de actividades planificadas	269
Gestión de la prioridad de ejecución de entradas	270
Visualización del historial de ejecución de las entradas	271
Especificación del tiempo que se deben guardar los historiales de ejecución	273
Volver a ejecutar una tarea de entrada anómala	274

Capítulo 18. Administración de planificaciones	277
Planificación de una entrada	279
Ejemplo: Cambio de credenciales para una planificación	281
Utilizar trabajos para planificar varias entradas	281
Datos de la solicitud en memoria caché	284
Planificación de entradas basada en activadores	284
Configuración de planificación basada en activadores	284
Planificación de una entrada basada en una aparición	285
 Capítulo 19. Despliegue	 287
Especificaciones de despliegue.	288
Archivos de despliegue	288
Planificación de despliegue.	288
Seguridad y despliegue	288
Mantener nombres de objetos localizados al importar archivos más antiguos	290
Despliegue de todo el almacén de contenido	291
Despliegue del contenido de directorio y de las carpetas públicas seleccionadas	293
Valores avanzados del despliegue	297
Especificación de si la salida del informe forma parte del despliegue	297
Inclusión de los objetos de configuración y sus hijos en los despliegues	298
Reglas para la resolución de conflictos de despliegue al importar y exportar	298
Reglas de resolución de conflictos	299
Reglas para la resolución de conflictos en el despliegue de todo el almacén de contenido	300
Reglas para la resolución de conflictos en el despliegue parcial	301
Despliegue de las entradas de IBM Cognos	303
Exportar de un entorno de origen	304
Cómo mover el archivo de despliegue	308
Importación en un entorno de destino	308
Inclusión de los objetos de configuración en la importación de todo el almacén de contenido.	311
Comprobación de las aplicaciones desplegadas	312
Actualización de las especificaciones de informes	312
Asignación de ID de contenido	313
Despliegue de Human Task and Annotation Services	314
Despliegue de comentarios de IBM Cognos Workspace	315
Almacenamiento y creación de informes de los comentarios de IBM Cognos Workspace	316
 Capítulo 20. Paquetes	 319
Creación de un paquete para un PowerCube	319
Paquetes SAP BW	319
Creación de un paquete SAP BW	320
Edición de un paquete SAP BW	320
Establecimiento del número máximo de objetos utilizados en los paquetes de SAP BW	320
 Capítulo 21. Administración de perfiles de usuario	 323
Edición del perfil de usuario predeterminado.	323
Visualización o modificación de un perfil de usuario	324
Visualización o modificación de un perfil de usuario	324
Suprimir contenido	324
Supresión de un perfil de usuario	325
Copia de perfiles de usuario	326
 Capítulo 22. Entornos de varios arrendatarios	 327
Configuración de arrendamiento múltiple	328
Configuración de un arrendamiento múltiple basado en un nodo de jerarquía.	329
Configuración de un arrendamiento múltiple basado en un atributo de cuenta de usuario.	331
Configuración de un arrendamiento múltiple basado en un proveedor de arrendatario personalizado	332
Características avanzadas de arrendamiento múltiple	333
Configuración de la propiedad Correlación de conjunto delimitador de arrendatario	334
Inhabilitación del arrendamiento múltiple	338
Administración de arrendatarios	338

Reglas de contención para arrendamiento múltiple	339
Creación de arrendatarios	340
Asignación de ID de arrendatario a contenido existente	340
Establecimiento de un ID de arrendatario para un objeto público	341
Suplantación de un arrendatario	341
Administración delegada de arrendatarios.	342
Configuración de arrendatarios virtuales para habilitar el uso compartido del contenido entre los arrendatarios	344
Visualización del nombre de arrendatario en la interfaz de usuario de Cognos Analytics	345
Administrar perfiles de usuario arrendatario	345
Despliegue de contenido de arrendatario	346
Terminación de las sesiones de usuario activo para arrendatarios	350
Inhabilitar y habilitar arrendatarios	351
Supresión de arrendatarios	351
Crear y ejecutar las tareas de utilización del almacén de contenido	352
Crear y ejecutar una verificación de consistencia del almacén de contenidos	353
Acceso a actividades interactivas en un entorno de inquilinos múltiples	354
Capítulo 23. Biblioteca de recursos	357
Visualizaciones	357
Cómo importar visualizaciones a la biblioteca	357
Gestión de visualizaciones	358
Capítulo 24. Informes y cubos	361
Informes activos de IBM Cognos	361
Vistas de informes.	362
Visualización de la información de linaje de un elemento de datos	362
Acceso a InfoSphere Business Glossary	363
Formatos de informe	363
Formatos HTML	364
Formato PDF	364
Formatos Microsoft Excel	365
Formato CSV	365
Idiomas del informe	366
Especificar el idioma para un informe	366
Cómo especificar los valores de la solicitud predeterminados para un informe	366
Especificación del tiempo que se deben mantener las versiones de las salidas de informe	367
Especificación del tiempo que se deben guardar los historiales de salida de informe.	367
Los orígenes de datos con conjuntos con nombre pueden producir resultados imprevisibles	367
Informes de Series 7 en IBM Cognos Analytics	368
Informes y cubos de Series 7 PowerPlay	368
Inicio de sesión único	368
Cambio de los valores predeterminados para un informe de Series 7 PowerPlay	369
Propiedades multilingües de los informes y cubos de Series 7	369
Capítulo 25. Administración de tareas humanas	371
Solicitudes de aprobación y tareas ad-hoc	371
Visualización de comentarios	371
Suscripción a las notificaciones de correo electrónico	372
Creación de una tarea ad-hoc	372
Acciones que se pueden efectuar en las solicitudes de aprobación y las tareas ad-hoc	374
Reclamación de una tarea	375
Cambio de los destinatarios de una tarea	375
Cambio del propietario actual	375
Cambio de los posibles propietarios y las partes interesadas.	376
Revocación de la propiedad de una tarea	376
Establecimiento de fechas límite para una tarea	376
Cómo cambiar la prioridad de una tarea	377
Cómo añadir comentarios a una tarea	377
Inicio o detención de una tarea	377

Finalización de una tarea	378
Cancelación de una tarea	379
Solicitudes de notificación	379
Creación de una solicitud de notificación	380
Lectura y confirmación de una solicitud de notificación	381
Archivado de tareas	381
Visualización del archivo de tareas	382

Capítulo 26. Acceso a detalles 383

Introducción a los conceptos de acceso a los detalles	384
Rutas de acceso a los detalles	384
Contextos de la selección	385
Acceso a detalles en distintos formatos de informe	385
Acceso a los detalles entre paquetes	386
Referencias de marcador.	386
Miembros y valores	387
Dimensiones compatibles	388
Claves de empresa	388
Ámbito	389
Parámetros correlacionados.	390
Fechas de acceso a los detalles entre PowerCubes y paquetes relacionales	391
Configuración del acceso a detalles en los paquetes	391
Edición de las definiciones de acceso a los detalles existentes	393
Configuración de parámetros para un informe de acceso a detalles	394
Depuración de una definición para acceso a detalles	396
Acceso al ayudante para acceso a detalles	398
Ejemplo: depurar una definición para acceso a detalles	398
Configuración del acceso a detalles en un informe	399
Especificar texto de acceso a detalles	400

Capítulo 27. IBM Cognos Workspace 403

Eliminación de la marcación HTML de los detalles de entrada RSS	403

Capítulo 28. Administración de IBM Cognos Mobile 405

Configuración previa de las aplicaciones de Cognos Mobile nativas para los usuarios	405
Especificación de valores avanzados de Cognos Mobile	408
Configuración de un tema de Mobile	408
Creación de un tema de Mobile personalizado	410
Configuración de los servicios de Cognos Mobile	411
Valores de configuración del servicio de Cognos Mobile	411
La configuración de notificaciones push de Apple para la aplicación nativa de iOS	415
Gestión del certificado SSL para notificaciones push de Apple	416
Habilitación de notificaciones push de Apple.	416
Gestión de informes en un dispositivo móvil	418
Atajos de Cognos Mobile en un dispositivo móvil	418
Prestaciones de registro de Cognos Mobile	419
Registro de Cognos Mobile.	419
Habilitación del registro de Cognos Analytics para el servidor Mobile	420
Diagnóstico para el usuario.	422
Ejemplos de Cognos Mobile	423
Seguridad de Cognos Mobile	425
Prestaciones de Cognos Mobile	426
Protección de contraseña	427
Soporte HTML y HTTP durante el inicio de sesión	427
Autenticación de certificados	428
Seguridad de aplicaciones en Cognos Mobile.	429
Seguridad de los datos de informes en dispositivos móviles.	430
Borrado del contenido de un dispositivo	430
Establecimiento de una clave de contrato	430
Establecimiento de políticas de autenticación de usuario para un dispositivo móvil	431

Apéndice A. Características de accesibilidad.	433
Habilitación de la salida de informe accesible en todo el sistema	433
Características de accesibilidad de Cognos Mobile	434
Atajos del teclado en Cognos Mobile	434
Problemas conocidos	437
Apéndice B. Round Trip Safety Configuration de caracteres Shift-JIS	439
Ejemplo: Conversión segura de Shift-JIS	440
Programa de utilidad Round Trip Safety Configuration	440
Especificación de conversiones	441
Especificación de sustituciones	442
Aplicación de las conversiones y las sustituciones	443
Restauración de los valores predeterminados de conversión	443
Especificación de conversiones para informes de Series 7 PowerPlay Web	444
Apéndice C. Permisos de acceso iniciales	445
Permisos de acceso iniciales a los objetos raíz y de nivel superior de Content Manager	446
Permisos de acceso iniciales a las prestaciones	447
Apéndice D. Localización de bases de datos de ejemplos	473
Una columna por idioma	473
Determinación del idioma (columnas) en el modelo	473
Consulta de ejemplo	473
Una fila por idioma	474
Determinación del idioma (filas) en el modelo	474
Consulta de ejemplo	475
Transcripciones y extensiones multialfabeto	475
Transcripciones en el modelo	476
Extensiones multialfabeto	476
Uso de extensiones multialfabeto para el formateo condicional	476
Apéndice E. Esquema para los comandos de orígenes de datos	479
commandBlock	480
comandos	480
sessionStartCommand	481
sessionEndCommand	481
arguments	482
argument	482
setCommand	482
sqlCommand	483
sql	483
name	483
value	484
Apéndice F. Esquema de datos para mensajes de registro	485
Definiciones de tablas	485
Tabla COGIPF_ACTION	485
Tabla COGIPF_AGENTBUILD	487
Tabla COGIPF_AGENTRUN	488
Tabla COGIPF_ANNOTATIONSERVICE	490
Tabla COGIPF_EDITQUERY	491
Tabla COGIPF_HUMANTASKSERVICE	493
Tabla COGIPF_HUMANTASKSERVICE_DETAIL	496
Tabla COGIPF_NATIVEQUERY	497
Tabla COGIPF_PARAMETER	499
Tabla COGIPF_RUNJOB	499
Tabla COGIPF_RUNJOBSTEP	501
Tabla COGIPF_RUNREPORT	502
Tabla COGIPF_THRESHOLD_VIOLATIONS	504

Tabla COGIPF_USERLOGON	507
Tabla COGIPF_VIEWREPORT	509
Apéndice G. Configuración de valores avanzados	513
Configuración de valores avanzados globalmente	513
Configuración de valores avanzados para asignadores específicos	514
Configuración de valores avanzados para servicios específicos	515
Referencia de valores avanzados	515
Valores avanzados del servicio de agente	515
Valores avanzados del servicio de Content Manager	517
Valores comunes de configuración	522
Valores avanzados de Portal Services (servicio de presentación)	524
Valores avanzados del servicio de entrega	526
Valores avanzados del servicio de asignador	528
Valores avanzados del servicio de gestión de eventos	528
Valores avanzados del servicio de trabajos	531
Valores avanzados del Metrics Manager Service	531
Valores avanzados del servicio de control	532
Valores avanzados de servicio de informes y servicio de informes por lotes	537
Valores avanzados del servicio de repositorio	546
Valores avanzados de UDA	547
Índice.	551

Introducción

Esta información se ha concebido para su utilización con IBM® Cognos Administration, el componente administrativo del software de IBM Cognos.

Esta información incluye procedimientos detallados e información general que le ayudarán a administrar el software de IBM Cognos.

Búsqueda de información

Para buscar documentación de productos en la web, incluida toda la documentación traducida, acceda al Knowledge Center de IBM (<http://www.ibm.com/support/knowledgecenter>).

Características de accesibilidad

IBM Cognos Administration dispone de características de accesibilidad que ayudan a los usuarios que tienen una discapacidad física, por ejemplo movilidad restringida o visión limitada, a utilizar los productos de tecnología de la información. La disponibilidad de las características de accesibilidad puede variar, sin embargo, si se añaden a la interfaz de usuario de Cognos Administration otras páginas y componentes que no den soporte a la accesibilidad.

Para obtener información sobre las características de accesibilidad que están disponibles en IBM Cognos Administration, consulte: Apéndice A, “Características de accesibilidad”, en la página 433.

La documentación HTML de IBM Cognos tiene características de accesibilidad. Los documentos PDF son suplementarios y, como tales, no incluyen características de accesibilidad adicionales.

Proyecciones futuras

En esta documentación se describe la funcionalidad actual del producto. Puede que se incluyan referencias a elementos que actualmente no están disponibles. Sin embargo, no deberá deducirse su futura disponibilidad real. Estas referencias no constituyen un compromiso, promesa ni obligación legal que implique la entrega de ningún tipo de material, código o funcionalidad. El desarrollo, entrega y comercialización de las características o funcionalidad son aspectos que quedan a la entera discreción de IBM.

Declaración de limitación de responsabilidad de los ejemplos

Los nombres Sample Outdoors Company, Great Outdoors Company, GO Sales, cualquier variación de Sample Outdoors o Great Outdoors y Planning Sample describen operaciones comerciales ficticias con datos de muestra utilizados para desarrollar aplicaciones de muestra para los clientes de IBM e IBM. Estos registros ficticios incluyen datos de ejemplo para las transacciones de ventas, la distribución de productos, la gestión financiera y los recursos humanos. Cualquier parecido con nombres, direcciones, números de contacto o valores de transacciones reales es pura coincidencia. Otros archivos de ejemplo pueden contener datos ficticios generados manual o informáticamente, datos relativos a hechos procedentes de fuentes públicas o académicas, o datos utilizados con el permiso del poseedor del

copyright, para utilizarlos como datos de ejemplo para desarrollar las aplicaciones de ejemplo. Los nombres de productos a los que se hace referencia pueden ser marcas registradas de sus respectivos propietarios. Está prohibido realizar cualquier tipo de duplicación no autorizada.

Capítulo 1. Administración del software de IBM Cognos

Tras la instalación y la configuración del software de IBM Cognos, puede llevar a cabo la administración del servidor, los datos, la seguridad y los contenidos, así como de las actividades y los servicios de administración.

También puede realizar las tareas administrativas siguientes:

- tareas automatizadas
- Configuración del entorno y de la base de datos para la creación de informes multilingüe
- Instalación de fuentes
- Configuración de impresoras
- Configuración de navegadores web
- Concesión de acceso de usuario a informes de Series 7
- Restricción de acceso al software de IBM Cognos

Además de las tareas administrativas típicas, también puede personalizar la apariencia y la funcionalidad de los distintos componentes de IBM Cognos.

Para obtener información sobre problemas potenciales, consulte la publicación *IBM Cognos Analytics Guía de resolución de problemas*.

IBM Cognos Administration

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration**.

Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Tabla 1. Tipos de herramientas de administración

Área administrativa	Pestaña	Uso
Actividades	Estado	Para gestionar entradas actuales, pasadas, próximas y planificadas de IBM Cognos.
Sistemas de Content Manager	Estado	Para administrar sistemas de Content Manager
Almacén de contenido	Configuración	Para realizar tareas de mantenimiento del almacén de contenido
Orígenes de datos	Configuración	Para crear y administrar conexiones de orígenes de datos.

Tabla 1. Tipos de herramientas de administración (continuación)

Área administrativa	Pestaña	Uso
Despliegue	Configuración	Para desplegar IBM Cognos , exportar desde un entorno de origen y, a continuación, importar en un entorno de destino
Asignadores y servicios	Estado	Para administrar asignadores y servicios.
Impresoras	Configuración	Para crear y administrar impresoras
Seguridad	Seguridad	Para controlar el acceso a determinadas funciones del producto, como administración y creación de informes, y a características de las funciones, como separación y SQL definido por el usuario
Administración del servicio, el sistema, el asignador y el servidor	Estado	Para supervisar el rendimiento del sistema mediante métricas del sistema y administrar servidores
Ajuste del servidor	Estado	Para optimizar la velocidad y la eficacia del software de IBM Cognos.
Usuarios, grupos y roles	Seguridad	Para crear y administrar usuarios, grupos y roles

Habilitación de la salida de informe accesible en todo el sistema

Puede especificar valores que afecten a todo el sistema para la salida de informe accesible que se aplican a todas las entradas, incluidos los informes, los trabajos y las entradas planificadas.

Los informes accesibles contienen características, como el texto alternativo, que permiten que los usuarios con discapacidades accedan al contenido de los informes mediante el uso de tecnología asistencial, como los lectores de pantalla.

Los valores de accesibilidad existentes en las preferencias de usuario y las propiedades de informe pueden reemplazar los valores que se aplican a todo el sistema en IBM Cognos Administration.

Los informes accesibles requieren más procesamiento y tienen un tamaño de archivo mayor que los informes no accesibles. Por lo tanto, los informes accesibles afectan al rendimiento. De forma predeterminada, el soporte para salida de informe accesible está inhabilitado.

La salida de informe accesible está disponible en los siguientes formatos: PDF, HTML y Microsoft Excel.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios**.
2. En la barra de herramientas de la página **Configuración**, pulse el botón Establecer propiedades .
3. Pulse la pestaña **Valores**.
4. En la lista desplegable **Categoría**, pulse **Reemplazo de administrador**.
5. En la categoría **Reemplazo de administrador**, situada junto a **Soporte de accesibilidad para informes**, en la columna **Valor**, pulse **Editar**.
6. En la página **Soporte de accesibilidad para informes**, seleccione una de las opciones siguientes:

Opción	Descripción
Inhabilitar	La salida de informe accesible no está disponible para los usuarios.
Hacer obligatoria	La salida de informe accesible siempre se crea.
Dejar que decida el usuario	El usuario especifica la salida de informe accesible. Si establece esta opción en No seleccionado , la salida de informe accesible no se crea automáticamente. Esta es la opción predeterminada. Si establece esta opción en Seleccionado , la salida de informe accesible no se crea de forma predeterminada.

Tareas automatizadas

Prácticamente todo lo que se puede hacer con el producto, se puede llevar a cabo mediante la interfaz API o URL correspondiente o la herramienta de línea de comandos, tal como se ilustra en la tabla siguiente.

Tabla 2. Tareas automatizadas

Objetivo	Interfaz de automatización	Información
Modificar un modelo o volver a publicarlo en los sistemas operativos UNIX o Microsoft Windows.	Herramienta Script Player	<i>IBM Cognos Framework Manager Developer Guide e IBM Cognos Framework Manager Guía del usuario</i>
Modificar un modelo no publicado con los métodos <code>updateMetadata</code> y <code>queryMetadata</code> .	API de bus de BI	<i>IBM Cognos Software Development Kit Developer Guide</i>

Tabla 2. Tareas automatizadas (continuación)

Objetivo	Interfaz de automatización	Información
Recuperar los elementos de consulta disponibles en el paquete publicado con el método getMetadata.	API de bus de BI	IBM Cognos Software Development Kit Developer Guide
Otorgar privilegios a los usuarios.	API de bus de BI	IBM Cognos Software Development Kit Developer Guide
Administrar e implementar la seguridad.	API de bus de BI	IBM Cognos Software Development Kit Developer Guide
Ejecutar, ver y editar informes a través de un hipervínculo de una página HTML. Utilizar URL para ver, editar y ejecutar informes.	Interfaz URL	IBM Cognos Software Development Kit Developer Guide
Manipular objetos del almacén de contenido. Administrar Content Manager.	API de bus de BI	IBM Cognos Software Development Kit Developer Guide
Administrar informes.	API de bus de BI	IBM Cognos Software Development Kit Developer Guide
Administrar servidores y asignadores.	API de bus de BI	IBM Cognos Software Development Kit Developer Guide
Modificar o crear informes.	API de bus de BI y especificación de informe	IBM Cognos Software Development Kit Developer Guide

Configuración de un entorno de creación de informes multilingüe

Puede configurar un entorno de creación de informes multilingüe.

Puede crear informes que muestren datos en más de un idioma y utilizar distintas configuraciones regionales. Esto significa que puede crear un informe que pueden utilizar consumidores de informes de todo el mundo.

Las bases de datos de ejemplo que se proporcionan con el software de IBM Cognos almacenan una selección de campos de texto, como nombres y descripciones, en más de 25 idiomas, lo que da prueba de un entorno de creación de informes multilingüe.

A continuación se indica el proceso para crear un entorno de creación de informes multilingüe:

- Utilice metadatos multilingües.

El administrador de orígenes de datos puede almacenar datos multilingües en columnas, filas o tablas individuales.

- Cree un modelo multilingüe.

Los modeladores utilizan Framework Manager para añadir metadatos multilingües al modelo desde cualquier tipo de origen de datos, excepto OLAP. Añaden metadatos multilingües mediante la definición de los idiomas que soporta el modelo, la traducción de cadenas de texto en el modelo para elementos como descripciones y nombres de objetos, y la definición de los idiomas que se exportan en cada paquete. Si el origen de datos contiene datos multilingües, los modeladores pueden definir consultas que recuperen datos en el idioma predeterminado para el usuario del informe.

Para obtener más información, consulte la publicación *IBM Cognos Framework Manager Guía del usuario*.

- Cree mapas multilingües.

Los administradores y los modeladores emplean un programa de utilidad del sistema operativo Microsoft Windows denominado Map Manager para importar mapas y actualizar etiquetas de mapas en Creación de informes. Para las características de mapa como los nombres de ciudades y países o regiones, los administradores y los modeladores pueden definir nombres alternativos para ofrecer versiones multilingües del texto que aparece en el mapa.

Para obtener más información, consulte la publicación *IBM Cognos Map Manager Installation and User Guide*.

- Cree un informe multilingüe.

El autor de informes utiliza Creación de informes para crear un informe que se pueda visualizar en distintos idiomas. Por ejemplo, puede especificar que el texto, como por ejemplo el título, aparezca en alemán cuando el informe lo abra un usuario alemán. También puede añadir traducciones para objetos de texto y crear otros objetos dependientes del idioma.

Para obtener más información, consulte la publicación *IBM Cognos Analytics - Reporting User Guide*.

- Especifique el idioma en el que se visualiza un informe.

- Definir propiedades multilingües, como un nombre, una sugerencia y una descripción, para cada entrada en el portal.
- Especificar el idioma predeterminado que desea que se emplee cuando se ejecute un informe.

Sugerencia: Puede especificar el idioma predeterminado en la página de opciones de ejecución, en las propiedades de informe o en sus preferencias.

- Especificar un idioma, distinto del predeterminado, que desee que se emplee cuando se ejecute un informe.

Los datos aparecerán en el idioma y con la configuración regional especificados en

- las opciones del navegador web del usuario
- las opciones de ejecución
- las preferencias de IBM Cognos Analytics

Cualquier texto que añadan los usuarios o los autores aparecerá en el idioma en el que lo hayan escrito.

Configuración de la base de datos para la creación de informes multilingüe

IBM Cognos Analytics es un producto Unicode capaz de consultar datos en numerosos idiomas y codificaciones.

IBM Cognos Analytics generalmente consulta la base de datos utilizando la codificación de datos nativa de la base de datos (Latin-1, Shift-JIS, Unicode, etc.). IBM Cognos Analytics traduce estos datos a Unicode según sea necesario.

Al consultar bases de datos con dos o más codificaciones de datos, Creación de informes solicita los datos en Unicode. Algunas bases de datos requieren una configuración específica del software cliente o servidor para habilitar esta función. Para obtener más información, consulte la documentación del distribuidor de la base de datos.

Nota: Para obtener información sobre problemas de seguridad de recorrido de ida y vuelta al convertir caracteres de Unicode a Shift-JIS y viceversa, consulte la información sobre el programa de utilidad Round Trip Safety Configuration en Apéndice B, "Round Trip Safety Configuration de caracteres Shift-JIS", en la página 439.

Instalación de fuentes

El software de IBM Cognos utiliza fuentes para mostrar informes y páginas HTML en navegadores, para representar informes PDF en el servidor IBM Cognos y para representar los gráficos utilizados en los informes PDF y HTML.

Para mostrar la salida correctamente, las fuentes deben estar disponibles donde se representa el informe o el gráfico. En el caso de gráficos e informes PDF, las fuentes deben estar instaladas en el servidor de IBM Cognos. Por ejemplo, si un usuario de Creación de informes selecciona la fuente Arial para un informe, dicha fuente debe estar instalada en el servidor de IBM Cognos para representar correctamente los gráficos y los archivos PDF. Si una fuente solicitada no está disponible, el software de IBM Cognos la sustituye por una fuente distinta.

Dado que los informes HTML se representan en un navegador, las fuentes necesarias deben estar instaladas en el sistema personal de cada uno de los usuarios del software de IBM Cognos que vayan a leer el informe HTML. Si una fuente solicitada no está disponible, el navegador la sustituirá por una fuente distinta.

Al crear informes, debe seleccionar fuentes que tengan instaladas los usuarios o el servidor de IBM Cognos. Microsoft ofrece una amplia selección de fuentes con distintos paquetes de idioma, por lo que es poco probable que suponga un problema en el sistema operativo Microsoft Windows. Sin embargo, los servidores UNIX rara vez disponen de fuentes instaladas. Debe estar dispuesto a adquirir e instalar las fuentes necesarias en los clientes del navegador y del servidor.

Para obtener más información acerca de los valores del archivo en PDF, consulte "Valores de archivos PDF" en la página 83. Para obtener información sobre el uso del formato PDF en los informes, consulte "Formatos de informe" en la página 363. Para obtener información sobre la configuración de fuentes y sobre la correlación de fuentes sustitutas, consulte la *IBM Cognos Analytics Guía de instalación y configuración*.

Fuente predeterminada de IBM Cognos

Si no se encuentra una fuente solicitada, el servidor de IBM Cognos representará los archivos PDF y los gráficos con una fuente predeterminada.

Andale WT, parte de la familia de fuentes Sans Serif, es la fuente predeterminada por su amplio soporte de caracteres Unicode. Sin embargo, es posible que no esté completa para todos los idiomas y que no sea tan atractiva como las fuentes adquiridas. Asimismo, esta fuente no soporta la sustitución de glifos (GSUB) y las ligaduras en la mayoría de idiomas.

Fuentes de Creación de informes

Creación de informes es una aplicación HTML y JavaScript que se ejecuta en un navegador.

Debido al diseño del navegador, Creación de informes funciona en el recinto de pruebas de seguridad del navegador y no tiene acceso a la lista de fuentes instaladas en el sistema local. En lugar de ello, Creación de informes utiliza fuentes configuradas en la configuración global de IBM Cognos.

Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Configuración de impresoras

Para que las impresoras estén disponibles para los usuarios al distribuir informes, puede crear entradas para impresoras y guardarlas en el almacén de contenido de IBM Cognos.

Cuando los usuarios deseen imprimir un informe, pueden seleccionar una impresora que se haya configurado sin necesidad de conocer la información de dirección de red.

Al crear una entrada de impresora, asegúrese de que la impresora que defina esté configurada en el sistema en el que esté instalado IBM Cognos.

Para configurar impresoras, debe disponer de las capacidades necesarias para acceder a la funcionalidad **IBM Cognos Administration**. Debe tener permisos de escritura en el espacio de nombres de Cognos, consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Para evitar posibles errores, asegúrese de que se cumplan las condiciones siguientes antes de intentar imprimir:

- Asegúrese de que en todos los sistemas que tengan servidores de IBM Cognos esté instalado Adobe Reader.
- Compruebe que el servidor IBM Cognos se inicia con una cuenta que tenga acceso a la impresora de red.
A veces, las cuentas del sistema pueden no tener acceso a la impresora de red.
- Si IBM Cognos está instalado en un sistema operativo UNIX, compruebe que el comando **lpstat -v** devuelva una impresora configurada y que haya definida una variable de impresora.
- Al definir la dirección de red de la impresora, use la siguiente sintaxis:
Para el sistema operativo Microsoft Windows utilice `\\nombre_servidor\\nombre_impresora`.

Para un sistema operativo UNIX, utilice *nombre_impresora*, que es el nombre de la cola de impresión que muestra el comando `lpstat -v`.

- El nombre de red debe coincidir con el nombre de cola de impresión en lp.
- Asegúrese de que los usuarios de IBM Cognos cuentan con los permisos de acceso correctos para la impresora.

El rol Administradores del directorio debe tener todos otorgados los permisos de acceso, y el grupo Todos debe disponer de permisos de lectura, ejecución y visita.

Consejo: Para comprobar o asignar permisos de acceso para una impresora, en la columna **Acciones**, pulse el botón Establecer propiedades  para la impresora y, a continuación, pulse la pestaña **Permisos**.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Impresoras**.

Aparecerá una lista de impresoras.

Consejo: Para eliminar una impresora, seleccione la casilla de verificación para la impresora y pulse el botón de supresión.

2. En la barra de herramientas, pulse el botón Nueva impresora .
3. Escriba un nombre y, si lo desea, una descripción para la impresora.

Consejo: Utilice un nombre que proporcione información sobre la impresora, como Impresora en color - 4º piso.

4. Escriba la dirección de red de la impresora con el formato `\\nombre_servidor\nombre_impresora` para una impresora de red en una instalación del sistema operativo Windows y *nombre_impresora* para una instalación del sistema operativo UNIX o para una impresora local en Windows.
5. Pulse **Finalizar**.

Configuración de navegadores web

Los componentes de IBM Cognos Analytics utilizan configuraciones de navegador predeterminadas. Se necesitan valores adicionales para el navegador.

Configuración del navegador necesaria en Cognos Analytics

En la tabla siguiente se muestran los valores que deben habilitarse.

Tabla 3. Configuración del navegador habilitada

Navegador	Valor
Internet Explorer	Permitir cookies Secuencias de comandos ActiveX Permitir META REFRESH Ejecutar controles y conectores de ActiveX Activar script de los controles de ActiveX marcados como seguros Comportamientos binarios y script Permitir el acceso al portapapeles por programa Persistencia de los datos del usuario
Firefox	Permitir cookies Habilitar Java™ Habilitar JavaScript Cargar imágenes
Safari 5	Habilitar Java Habilitar JavaScript Bloquear cookies: Nunca
Google Chrome	Cookies: Permitir la configuración de datos locales Imágenes: Mostrar todas las imágenes JavaScript: Permitir que todos los sitios ejecuten JavaScript

Creación de informes y Query Studio utilizan el soporte nativo XML de Microsoft Internet Explorer, que es un componente del navegador. El soporte ActiveX debe habilitarse, ya que las aplicaciones de Microsoft implementan XML mediante ActiveX. Cognos Analytics no proporciona ni descarga controles de ActiveX. Sólo los controles de ActiveX que están instalados como parte de Internet Explorer se habilitan con esta configuración.

Si utiliza Microsoft Internet Explorer, podrá añadir la dirección URL de las pasarelas a la lista de Sitios de confianza. Por ejemplo, `http://<nombre_servidor>:<número_puerto>/ibmcognos`. De este modo, se habilita Preguntar automáticamente si se debe descargar un archivo.

Permita menús emergentes en todas las páginas de Cognos Analytics y en todos los navegadores.

Cookies utilizadas por los componentes de Cognos Analytics

Cognos Analytics de instalación y configuración.

Tabla 4. Cookies utilizadas por los componentes de Cognos Analytics

Cookie	Tipo	Función
AS_TICKET	Temporal por sesión	Creado si Cognos Analytics está configurado para usar un espacio de nombres de IBM Cognos Series 7
caf	Temporal por sesión	Contiene información sobre el estado de seguridad.
Cam_passport	Temporal por sesión	Almacena una referencia a una sesión de usuario almacenada en el servidor de Content Manager. Los administradores pueden establecer el atributo HTTPOnly para que los scripts no puedan leer ni manipular la cookie de pasaporte CAM durante la sesión de un usuario con su navegador web.
cc_session	Temporal por sesión	Contiene información de la sesión
cc_state	Temporal por sesión	Mantiene información durante las operaciones de edición, como cortar, copiar y pegar.
CRN	Temporal por sesión	Contiene la información de contenido y de entorno local del producto y está configurado para todos los usuarios de IBM Cognos.
CRN_RS	Permanente	Almacena la elección realizada por el usuario para Ver carpeta de miembros en Creación de informes
PAT_CURRENT_FOLDER	Permanente	Almacena la ruta de la carpeta actual si se utiliza el acceso del archivo local, y si éste se ha actualizado después de que se hayan usado los cuadros de diálogo Abrir o Guardar.
pp_session	Temporal por sesión	Almacena la información de la sesión específica de PowerPlay Studio.
qs	Permanente	Almacena los valores que el usuario ha llevado a cabo para elementos de la interfaz de usuario como menús y barras de herramientas.

Tabla 4. Cookies utilizadas por los componentes de Cognos Analytics (continuación)

Cookie	Tipo	Función
userCapabilities	Temporal por sesión	Contiene todas las funciones y la firma del usuario actual.
usersessionid	Temporal por sesión	Contiene un identificador de sesión de usuario exclusivo, válido para la duración de la sesión del navegador.
FrameBorder PageOrientation PageSize PDFLayerDimension PDFOPTS	Temporal por sesión	Estas cookies almacenan las preferencias de exportación a PDF.
DimTreeToolbarVisible	Permanente	Almacena el valor que determina si debe mostrarse u ocultarse la barra de herramientas del visor de dimensiones.
cea-ssa	Temporal por sesión	Almacena el valor que determina si la información de la sesión del usuario se comparte con otros componentes de Cognos Analytics.
BRes	Temporal por sesión	Almacena información que sirve para determinar la resolución de pantalla que debe utilizarse en la representación de gráficos.

Tabla 4. Cookies utilizadas por los componentes de Cognos Analytics (continuación)

Cookie	Tipo	Función
XSRF (Cross-Site Request Forgery)	Temporal por sesión	XSRF engaña a un navegador web para que ejecute una acción malintencionada en un sitio de confianza en el que el usuario está autenticado actualmente. XSRF abusa de la confianza en el navegador de un usuario que tiene un sitio. Impide que una página que se ha cargado desde el dominio X realice solicitudes al dominio Y, presuponiendo que el usuario ya esté autenticado en el dominio Y. Cuando se autentica por primera vez en Cognos Analytics, se establece la cookie XSRF. A partir de este punto, todas las solicitudes necesitarán la cookie XSRF-TOKEN, así como una cabecera HTTP denominada X-XSRF-TOKEN.

Después de actualizar o de instalar software nuevo, reinicie el navegador web y aconseje a los usuarios que borren la memoria caché del navegador.

Concesión de acceso de usuario a informes de Series 7

Si el software de IBM Cognos está configurado correctamente para utilizar el espacio de nombres de IBM Cognos Series 7, puede permitir que los usuarios accedan a NewsIndexes y NewsBoxes de la versión Series 7 de IBM Cognos Upfront.

Se recomienda que IBM Cognos Analytics y IBM Cognos Series 7 utilicen el mismo servidor web si Upfront está configurado para utilizar URL relativas. Si IBM Cognos Analytics e IBM Cognos Series 7 utilizan servidores web distintos, configure Series 7 para que utilice URL completos. De esta forma, los usuarios pueden utilizar el botón Atrás del navegador web para navegar de Upfront de vuelta a IBM Cognos Analytics.

Para obtener información sobre el modo de configurar Series 7, consulte la publicación *IBM Cognos Series 7 Configuration Manager User Guide*.

Procedimiento

1. En IBM Cognos Configuration, configure IBM Cognos para que utilice el espacio de nombres de IBM Cognos Series 7. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.
2. En la ventana **Propiedades**, en **Valores de cookies**, asegúrese de que la propiedad **Distintivo de protección activado** esté establecida en **falso**.
3. En el menú **Archivo**, pulse **Guardar** y cierre IBM Cognos Configuration.

4. Asegúrese de que se esté ejecutando el servidor de tiquets para el espacio de nombres de IBM Cognos Series 7.
5. Asegúrese de que el valor de tiempo de espera del servidor de tiquets de Series 7 esté establecido en el mismo valor o en un valor superior que el valor de tiempo de espera de pasaporte de IBM Cognos.
6. En el sistema en el que esté instalado el software de IBM Cognos, abra el archivo *install_location/templates/ps/system.xml* en un editor.
Asegúrese de que su editor permita guardar archivos en formato UTF-8.
7. Busque y edite (con un editor XML) el parámetro *series7* de la manera siguiente:

```
<!-- Series 7 Integration parameters -->
<param name="series7">
  <enabled>true</enabled>
  <!-- character encoding used by series7 -->
  <encoding>series7_character_encoding</encoding>
  <!-- host and port to connect to Upfront server -->
  <host>Upfront_host_name</host>
  <port>Upfront_dispatcher_port_number</port>
  <!-- Upfront gateway location -->
  <gateway>Upfront_gateway_location</gateway>
  <!-- If required, specify the prefix for IBM Cognos
back URLs when linking to Series 7 content. (eg. http://ibmcognos_computer)
otherwise relative URL's will be used -->
  <back-prefix>http://Series_7_server</back-prefix>
</param>
```

Para ver la codificación de caracteres utilizada por Series 7, en Series 7 Configuration Manager, en la pestaña **Propiedades**, pulse **IBM Cognos Shared**, a continuación, en **Entorno local** y, por último, en la propiedad **Codificación**.

8. Guarde al archivo *system.xml* en formato UTF-8.
9. Mediante IBM Cognos Configuration, detenga y, a continuación, reinicie IBM Cognos Analytics.

Para obtener más información sobre la detención de IBM Cognos Analytics, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Restricción de acceso al software de IBM Cognos

Es posible que no quiera que todos los usuarios de un origen de autenticación tengan acceso al software de IBM Cognos.

Para proteger el software de IBM Cognos, configure el producto de modo que únicamente los usuarios que pertenezcan a un grupo o rol determinados del origen de autenticación, o del espacio de nombres de Cognos, puedan acceder a él.

Se recomienda utilizar el espacio de nombres de Cognos, puesto que contiene grupos y roles preconfigurados que ayudan a proteger el software de IBM Cognos rápidamente. Uno de los grupos preconfigurados es Todos. De manera predeterminada, el grupo Todos pertenece a varios grupos y roles incorporados del espacio de nombres de Cognos. Si decide utilizar el espacio de nombres de Cognos, deberá eliminar el grupo Todos de todos los roles y grupos incorporados, y reemplazarlo por grupos, roles o usuarios que tengan permiso de acceso al software de IBM Cognos.

Para restringir el acceso al software de IBM Cognos, realice lo siguiente:

- En IBM Cognos Configuration, habilite las propiedades necesarias para restringir el acceso.

Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

- En **IBM Cognos Administration**, elimine el grupo Todos de todos los roles y grupos incorporados.

Sustitúyalo por grupos, roles o usuarios autorizados para acceder a las distintas áreas funcionales del software de IBM Cognos. Para obtener más información, consulte Capítulo 15, “Seguridad inicial”, en la página 243.

- Configure permisos de acceso para entradas individuales, como carpetas, paquetes, informes, páginas, etc. Para obtener más información, consulte Capítulo 12, “Permisos de acceso y credenciales”, en la página 213.

Para obtener más información sobre los conceptos de seguridad implementados en el software de IBM Cognos, consulte: Capítulo 10, “Modelo de seguridad”, en la página 199.

Capítulo 2. Compilación de aplicaciones de IBM Cognos Analytics

Puede utilizar los componentes de IBM Cognos Analytics para crear aplicaciones de creación de informes y análisis.

La duración de una aplicación de IBM Cognos Analytics puede ser de meses o incluso de años. Durante ese periodo, los datos pueden cambiar y aparecer nuevos requisitos. Conforme los datos subyacentes cambian, los autores deben modificar el contenido existente y desarrollar contenido nuevo. Con el tiempo, los administradores también deben actualizar los modelos y los orígenes de datos. Para obtener más información sobre el uso de los orígenes de datos, consulte *IBM Cognos Analytics Guía de administración y seguridad* e *IBM Cognos Framework Manager Guía del usuario*.

Antes de empezar

En una aplicación en funcionamiento, la infraestructura técnica y de seguridad y el portal se encuentran en el lugar adecuado, igual que los procesos para la gestión de cambios, el control de datos, etc. Para obtener información adicional, consulte el kit de herramientas IBM Cognos Solutions Implementation Methodology, que incluye guías orientativas y documentos de soporte. La información sobre el kit de herramientas está disponible en IBM Support Portal (www.ibm.com/support/entry/portal/support).

Cuando utilice IBM Cognos Analytics para crear aplicaciones en todos los componentes de IBM Cognos Analytics, localice y prepare orígenes de datos y modelos, cree y publique el contenido y, a continuación, entregue la información. El siguiente gráfico ofrece una descripción general del flujo de trabajo.

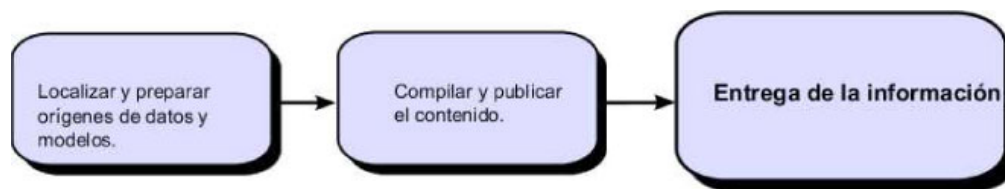


Figura 1. Uso de Cognos Analytics para crear aplicaciones

Procedimiento

1. Localizar y preparar orígenes de datos y modelos.

IBM Cognos Analytics puede crear informes a partir de una amplia variedad de orígenes de datos, tanto relacionales como dimensionales. Las conexiones de base de datos se crean en la interfaz de administración Web, y se utilizan para modelar, para crear informes y para ejecutar la aplicación.

Para utilizar los datos de creación y visualización de informes, los estudios requieren un subconjunto de un modelo de metadatos (llamado paquete). Es posible que los metadatos requieran un modelado amplio en Framework Manager.

2. Compilar y publicar el contenido.

Los informes, las tablas de puntuación, los análisis, los espacios de trabajo, etc. se crean en los estudios de IBM Cognos Analytics. El estudio que deba utilizar dependerá del contenido, la vida útil y el público del informe, así como de si el modelado de los datos es dimensional o relacional. Por ejemplo, los análisis y los informes automáticos se hacen mediante IBM Cognos Query Studio e IBM Cognos Analysis Studio, y los informes planificados se crean en IBM Cognos Analytics - Reporting. Los informes y las tablas de puntuación de Creación de informes suelen prepararse para un público más amplio, publicarse y planificarse para la separación, distribución, etc. También se puede utilizar Creación de informes para preparar plantillas para crear informes automáticos.

3. Entregar y visualizar la información.

El contenido se entrega desde el portal de IBM Cognos y se visualiza la información que se ha grabado o que se ha entregado mediante otros mecanismos. También es posible ejecutar informes, análisis, tablas de puntuación, etc. desde el estudio en el que se crean.

Para obtener información sobre el ajuste y el rendimiento, consulte *IBM Cognos Analytics Guía de administración y seguridad* e IBM Support Portal (www.ibm.com/support/entry/portal/support).

Capítulo 3. Configuración del registro

Además de los mensajes de error, los mensajes de registro proporcionan información sobre el estado de los componentes y una visión de alto nivel de los eventos importantes. Por ejemplo, los mensajes de registro pueden proporcionar información sobre los intentos de inicio y detención de servicios, la finalización de solicitudes de procesamiento y los indicadores de errores muy graves. Los registros de auditoría, disponibles a partir de una base de datos de registro, ofrecen información sobre la actividad de informe y usuario.

Los servicios de IBM Cognos de cada sistema envían información sobre los errores y eventos a un servidor de registro local. Hay un servidor de registro local instalado en la carpeta *install_location/logs* en cada sistema con IBM Cognos Analytics que contiene Content Manager o componentes de nivel de aplicación. Dado que el servidor de registro utiliza un puerto diferente del de otros componentes de IBM Cognos Analytics, sigue procesando eventos aunque se hayan inhabilitado otros servicios en el sistema local como, por ejemplo, el asignador.

En el flujo de trabajo siguiente se muestran las tareas necesarias para preparar el registro.

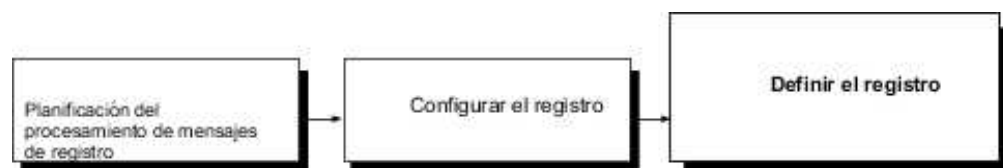


Figura 2. El flujo de trabajo para implementar el registro

- Durante la planificación, determine la configuración de registro adecuada para su entorno. Por ejemplo, evalúe los diversos repositorios de mensajes de registro, como los servidores y archivos de registro remotos, el syslog de UNIX o Linux o el registro de eventos de Windows NT, además del archivo de registro local. También puede enviar solamente información de registro de auditoría a una base de datos. Tenga en cuenta la seguridad, por ejemplo, los métodos disponibles para proteger los archivos de registro frente a fallos del sistema y la modificación por parte del usuario.
- Durante la configuración, defina las propiedades de inicio del registro, como, por ejemplo, los valores de conexión de las bases de datos. Si desea recopilar los registros de auditoría, deberá crear también una base de datos de registro. Si debe protegerse la comunicación entre un servidor de registro local y un servidor de registro remoto, realice los cambios de configuración adecuados en los dos sistemas con IBM Cognos Analytics. También puede habilitar algunas características de registro, como el registro específico del usuario.
- Al configurar el registro, especifique el nivel de detalle que se debe registrar para que los mensajes se centren en la información relevante para su organización. Los informes de auditoría también pueden configurarse para hacer un seguimiento de la actividad de informes y usuarios.

Para obtener más información sobre el uso de los mensajes de registro para resolver problemas y sobre la resolución de problemas relacionados con el registro, consulte la *IBM Cognos Analytics Guía de resolución de problemas*.

Mensajes de registro

Puede especificar la ubicación de los mensajes de registro y el tamaño y el número de los archivos de registro. También puede configurar las propiedades del servidor de registros.

De forma predeterminada, los mensajes de registro se guardan en el archivo `cogaudit.log` situado en el directorio `ubicación_instalación\logs`. Los mensajes de registro también se pueden almacenar en una base de datos. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Utilice los mensajes de registro para la resolución de problemas solamente. Si desea hacer un seguimiento de informes, paneles o uso de historial, utilice los informes de auditoría. Para obtener más información, consulte “Informes de auditoría” en la página 22.

Para obtener más información acerca del servicio de registro, consulte: “Asignadores y servicios” en la página 49.

Niveles de registro

Establezca los niveles de registro especificando los eventos y los mensajes que se deben registrar en el archivo de registro o en la base de datos de registro.

Un evento es una aparición en el entorno de IBM Cognos lo suficientemente importante como para realizar un seguimiento, por ejemplo, iniciar o detener un servicio.

Puede establecer un nivel de registro diferente para cada servicio de asignador. Es posible realizarlo para cada asignador o para todos los asignadores de la misma carpeta. Si establece diferentes niveles de registro para servicios diferentes, puede reducir la cantidad de información de registro irrelevante. Por ejemplo, si debe solucionar problemas para el servicio de informes por lotes, puede seleccionar un nivel de registro detallado sólo para ese servicio y mantener al mínimo los mensajes de registro. El nivel de registro para un servicio se aplica a todos sus componentes.

Consejo: El servicio de registro no posee niveles de registro asociados.

La siguiente tabla indica los detalles que registra cada registro de nivel.

Tabla 5. Niveles de registro

Detalles	Mínimo	Básico	Solicitud	Rastreo	Completo
Inicio y apagado del servicio y el sistema, error en tiempo de ejecución	X	X	X	X	X

Tabla 5. Niveles de registro (continuación)

Detalles	Mínimo	Básico	Solicitud	Rastreo	Completo
Administración de la cuenta de usuario y uso en tiempo de ejecución		X	X	X	X
Solicitudes de uso		X	X	X	X
Solicitudes y respuestas de servicio			X		X
Todas las solicitudes a todos los componentes con los valores de los parámetros				X	X
Otras consultas a componentes de IBM Cognos (consulta nativa)				X	X

Puede mantener el rendimiento del sistema si administra la cantidad de registro realizada por el servidor. Dado que un registro amplio afecta al rendimiento de servidor, el incremento del nivel de registro puede repercutir de forma negativa en el rendimiento del software de IBM Cognos.

El nivel de registro predeterminado es Mínimo. Utilice los niveles de registro Completo y Rastreo solo para solucionar problemas detalladamente, bajo la supervisión del soporte al cliente. Pueden reducir el rendimiento de servidor de forma significativa.

Si utiliza informes de auditoría, consulte “Configuración de la creación de informes de auditoría” en la página 22 para ver las directrices de establecimiento del nivel de registro. Para obtener más información acerca de cómo establecer los niveles de registro para los informes de auditoría, consulte “Informes de auditoría” en la página 22.

Niveles de validación del informe y niveles de registro

Puede recopilar información sobre los niveles de validación del informe si establece el nivel de registro correspondiente. Los mensajes de validación del informe se pueden incluir en los mensajes de registro del sistema.

Es posible utilizar la información de validación de varias formas. Si el sistema ofrece generalmente una respuesta insuficiente, puede establecer el registro en un nivel superior. La información adicional puede ayudarle a determinar qué informes fallan y por qué. Si aparecen mensajes de aviso en los registros, puede significar que los usuarios reciben resultados dudosos. Puede alertar a los propietarios sobre los informes ofensivos.

Existen cuatro niveles de validación del informe y cinco niveles de registro. En la tabla siguiente se muestra la correspondencia entre ellos.

Tabla 6. Niveles de validación del informe y niveles de registro

Nivel de validación del informe	Nivel de registro
Error	Mínimo, Básico
Aviso	Solicitud
Transformación de clave	Rastreo
Información	Completo

Cuanto mayor sea el nivel de registro, más se reducirá el rendimiento del sistema. Normalmente, establezca el nivel en Mínimo o Básico para recopilar errores, o en Solicitud para recopilar errores y avisos.

Para obtener más información sobre informes y la validación de informes, consulte *IBM Cognos Analytics - Reporting Guía del usuario*.

Registro de consultas nativas

Si desea crear informes de auditoría que incluyan las consultas que se ejecuten para el origen de datos de creación de informes, deberá habilitar el registro de consultas nativas. Puede utilizar el registro de consultas nativas para conocer qué tipos de información desean los usuarios o si un informe se ejecuta de forma eficaz. Para obtener información sobre la creación de informes de auditoría, consulte “Informes de auditoría” en la página 22.

Para habilitar el registro de consultas nativas en DQM (Dynamic Query Mode), establezca **Auditar nivel de registro para el servicio de consulta** en **Solicitud** o en un valor superior cuando configure el informe de auditoría. Sin embargo, si utiliza informes de auditoría, puede habilitar el registro de consultas nativas independientemente del registro de nivel de solicitud, tal y como se describe en “Establecimiento de niveles de registro” en la página 21.

Registro de opciones de ejecución de informes

Puede registrar las opciones de ejecución de informes en el sistema de registro. Las opciones de ejecución de informes son: parámetros de solicitud, opciones de ejecución y especificaciones de informe.

Esta funcionalidad está inhabilitada de forma predeterminada. Puede habilitar esta funcionalidad mediante los parámetros avanzados siguientes del servicio de informes y del servicio de informes por lotes:

RSVP.PARAMETERS.LOG

Cuando este parámetro tiene el valor true, se registran las opciones de ejecución y los parámetros de solicitud.

Valor predeterminado: false

RSVP.REPORTSPEC.LOG

Cuando este parámetro tiene el valor true, se registran las especificaciones de informe.

Valor predeterminado: false

Para obtener información sobre el establecimiento de estos parámetros para el servicio de informes y el servicio de informes por lotes, consulte: “Configuración de valores avanzados para servicios específicos” en la página 515.

Establecimiento de niveles de registro

Establezca los niveles de registro especificando los eventos y los mensajes que se deben registrar en el archivo de registro o en la base de datos de registro.

Un evento es una aparición en el entorno de IBM Cognos lo suficientemente importante como para realizar un seguimiento, por ejemplo, iniciar o detener un servicio.

Los niveles de registro que establezca para el sistema se aplicarán a todos los asignadores y servicios. Los niveles de registro que establezca en el nivel del asignador se aplicarán a todos los servicios asociados con el asignador. Los niveles de registro que establezca para los servicios individuales se aplicarán al servicio a través de todos los asignadores.

Los niveles de registro establecidos para los asignadores reemplazarán los niveles de registro establecidos para el sistema. Los niveles de registro establecidos para los servicios reemplazarán los niveles de registro establecidos para los asignadores o el sistema.

Si utiliza el registro para solucionar problemas, consulte “Niveles de registro” en la página 18 para ver las directrices de establecimiento de los niveles de registro. Si utiliza informes de auditoría, consulte “Configuración de la creación de informes de auditoría” en la página 22.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Todos los asignadores** o **Servicios**, en función de dónde desee establecer los niveles de registro.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** del elemento cuyos niveles de registro desea establecer, pulse **Establecer propiedades**.

4. Pulse la pestaña **Valores**.
5. Para filtrar la lista, en el menú **Categoría**, pulse **Registro**.
6. En la lista, busque el servicio que desea y, en el menú **Valor**, seleccione el nivel de registro que desee para el servicio.
7. Si el registro de consultas nativas está disponible para el servicio y desea utilizarlo, seleccione la casilla de verificación **Auditar consulta nativa para el servicio de informe por lotes**. Para obtener más información, consulte “Registro de consultas nativas” en la página 20.
8. Pulse **Aceptar**.

Informes de auditoría

Utilice los informes de auditoría para ver la información sobre el informe, los paneles, y las actividades de histórico en la base de datos de registro.

Los informes de auditoría proporcionan información sobre el acceso a informes, paneles e historias. Esta información se graba en la base de datos de registro cuando se crea, ejecuta o modifica un informe, panel o historia. Incluye el nombre y la ubicación del informe, panel o historia, el nombre del usuario que lo ejecutó o modificó, y la hora y la fecha en que tuvo lugar.

Los usos posibles de la información de auditoría incluyen:

- Planificación de capacidades
- Conformidad con las licencias
- Supervisión de rendimiento
- Identificación del contenido no utilizado

Los ejemplos ampliados de IBM Cognos Analytics incluyen informes de auditoría de muestra. Para obtener más información, consulte *Samples for IBM Cognos Analytics Guide*.

Configuración de la creación de informes de auditoría

Debe configurar la creación de informes de auditoría antes de generar informes de auditoría o utilizar los informes de auditoría de ejemplo que se incluyen en el software de IBM Cognos.

Para permitir la creación de informes de auditoría, establezca el nivel de registro para todos los servicios o solo los servicios de IBM Cognos seleccionados en **Básico** (auditoría habilitada) o **Solicitud**. Si establece el nivel de registro en **Mínimo**, la auditoría estará inhabilitada. Utilice los niveles de registro **Completo** y **Rastreo** solamente para solucionar problemas detalladamente, bajo la supervisión del servicio de soporte al cliente. Pueden reducir el rendimiento del servidor de forma significativa.

Procedimiento

1. Configurar una base de datos de registro en el sistema de bases de datos que utilice su organización.
Para obtener más información, consulte las directrices para crear una base de datos de registro en la publicación *IBM Cognos Analytics Guía de instalación y configuración*.
2. En IBM Cognos Configuration, en **Entorno > Registros**, configure los mensajes de registro que se enviarán a la base de datos que creó en el paso 1.

3. En **Cognos Administration**, defina los niveles de registro apropiados para los servicios de Cognos.
 - a. Vaya a **Gestionar > Consola de administración**.
 - b. En la pestaña **Estado**, seleccione **Sistema**.
 - c. En el panel **Tarjeta de puntuación**, seleccione la vista **Todos los asignadores**.
 - d. En el menú Acciones del asignador, pulse **Establecer propiedades**, y luego pulse en la pestaña **Configuración**.
 - e. En la lista desplegable **Categoría**, seleccione **Registros**.
 - f. Defina el nivel de registro en **Básico** para los servicios siguientes: Content Manager Cache service, Content Manager Service, Query Service. Puede habilitar el registro de auditoría para otros servicios, en función de los requisitos de su organización, o incluso para todos los servicios, si el impacto sobre el rendimiento del servidor no ha de ser un problema para usted.
 - g. Para habilitar el registro de consultas nativas en CQM (Compatible Query Mode), seleccione estos dos recuadros de selección:
 - **Auditar consulta nativa para el servicio de informe por lotes**
 - **Auditar consulta nativa para el servicio de informe**
 - h. Para habilitar el registro de consultas nativas en DQM (Dynamic Query Mode), establezca **Auditar nivel de registro para el servicio de consulta** en **Solicitud** o en un valor superior.
 - i. Pulse **Aceptar**.
4. En Cognos Configuration, reinicie el servicio **IBM Cognos**.

Visualización detallada de los mensajes de error de protección

Puede ver detalles de error completos, que puedan contener información confidencial.

Algunos mensajes de error de IBM Cognos pueden contener información confidencial, como los nombres de servidor. De forma predeterminada, la opción de mensajes de error de protección de IBM Cognos Application Firewall está habilitada. Los usuarios reciben información que sólo indica que se ha producido un error.

Si posee los permisos adecuados, es posible recuperar los detalles de error completos. Es posible que desee ver los mensajes de registro; consulte “Mensajes de registro” en la página 18.

Procedimiento

1. Busque el identificador de código de error en el mensaje de error de usuario. Por ejemplo, el número de error en el siguiente mensaje es `secureErrorID:2004-05-25-15:44:11.296-#9`:

Se ha producido un error. Póngase en contacto con el administrador. CAF ha registrado el error completo con `SecureErrorID:2004-05-25-15:44:11.296-#9`
2. Abra el archivo `cogaudit.log` en el directorio `ubicación_instalación/logs`.
3. Busque el identificador de código de error para localizar el mensaje de error aplicable.

Inhabilitación de la creación de archivos principales de volcado

Los archivos principales de volcado se crean cuando existen problemas graves, como una excepción no controlada o cuando un proceso de IBM Cognos termina de forma anómala.

Si se produce un problema de este tipo, recibirá el siguiente mensaje de error:

Report
Server no responde.

Dado que los archivos principales de volcado son de gran tamaño y se crea uno de nuevo cada vez que se produce un problema, es posible que desee inhabilitarlos. Puede habilitar de nuevo los archivos principales de volcado si encuentra problemas que lo requieran.

También puede ser aconsejable suprimir los archivos principales de volcado existentes en el directorio `\bin` de la instalación de servidor de IBM Cognos, si no son necesarios para la solución de problemas. En un entorno de Microsoft Windows, los archivos principales de volcado tienen la extensión `.dmp` y el nombre de archivo `IDproceso.dmp`, como por ejemplo `BIBusTKServerMain_seh_3524_3208.dmp`. En un entorno de UNIX, los archivos se denominan "core". En un entorno de Linux, los archivos se denominan `core.IDproceso`.

Procedimiento

1. En el servidor donde está instalado IBM Cognos Analytics, abra el archivo `cclWinSEHConfig.xml` desde el directorio `ubicación_instalación\configuration`.
2. En el elemento de configuración, cambie el valor de la variable de entorno a 0 (cero) para que se lea

```
<env_var name="CCL_HWE_ABORT" value="0"/>
```
3. Guarde el archivo.

Utilización del registro para diagnosticar un problema para un usuario específico

Puede utilizar registros para diagnosticar un problema que se produce para un usuario o para varios usuarios concretos.

Establezca temporalmente que el registro sólo se efectúe para ese usuario. Una vez resuelto el problema, inhabilite el registro específico del usuario y reanude el registro normal sin interferir en los valores de registro existente.

Habilite e inhabilite el registro para usuarios concretos con el servicio de proceso remoto para Java Management Extensions (JMX), una tecnología que suministra herramientas para administrar y supervisar aplicaciones y redes orientadas a servicios. Puede conectar con el servicio de proceso remoto JMX con el ejecutable `jconsole` que se proporciona con el Java JDK. De forma predeterminada, la salida del registro específico del usuario se guarda en el directorio `install_location\logs`.

Antes de empezar

Primero debe habilitar el registro específico del usuario para IBM Cognos Analytics. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Procedimiento

1. Conecte con el servicio de proceso remoto de JMX; para ello, lance el ejecutable `jconsole` y especifique la información siguiente:
 - El URL para conectarse a los datos. Por ejemplo:
`service:jmx:rmi://servidor_Content_Manager/jndi/rmi://servidor_supervisión:<puerto_JMX>/proxyservlet`
siendo `puerto_JMX` el valor que ha configurado en **Puerto JMX externo** en IBM Cognos Configuration, y `servidor_Content_Manager` y `servidor_supervisión` nombres de sistemas. No utilice el nombre `localhost`, ni siquiera si se conecta de forma local.
 - El ID de usuario y la contraseña para que la conexión sea segura.
 - Los valores de **Credencial JMX externa** en IBM Cognos Configuration.
2. En la ventana de conexión de servidor de proceso remoto, expanda **com.cognos**, **Metrics**, **camAsyncAA**, `http://nombre_servidor:número_puerto/p2pd` y seleccione el nodo **Operations**.
3. Copie el CAMID del usuario en el campo **enableDyeTrace** y pulse el botón **enableDyeTrace**.

Consejo: En IBM Cognos Administration, para encontrar el CAMID, realice lo siguiente:

- Pulse la pestaña **Seguridad** y, a continuación, pulse **Usuarios, grupos y roles**.
- Pulse **Establecer propiedades** para el usuario y luego pulse **Ver ruta de búsqueda, ID y URL**

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration**. Para obtener más información, consulte: Capítulo 13, "Funciones y características protegidas", en la página 227.

4. Para verificar que ha habilitado el usuario correctamente, navegue hacia arriba hasta **Atributos** y vea el contenido del valor **DyeTracedUsers**.

Ejecución del registro para un usuario específico mediante la edición de archivos ipf específicos del componente

Puede iniciar el registro para un usuario especificado e implementar el rastreo hasta el originador ("dye tracing") mediante la edición de archivos ipf específicos del componente.

Procedimiento

1. Añada un elemento `<filter>` a una definición `<appender>` existente o añada una nueva definición `<appender>`.
Debe asegurarse de que las categorías hacen referencia a una definición `<appender>` que utiliza el elemento `<filter>`.
2. Cuando una definición `<appender>` especifique un servidor de registro, cambie los valores de puerto por los valores del puerto de servidor de registro configurado que utiliza.

Ejecución del registro para un usuario específico mediante la utilización de categorías seleccionadas

Para iniciar el registro para un usuario especificado, implemente el rastreo hasta el originador ("dye tracing") y personalice la salida utilizando categorías seleccionadas y distribuyendo la salida a una o varias definiciones de adicionador.

Procedimiento

1. En el directorio *ubicación_instalación*\configuration, localice el archivo de rastreo ipf para el componente que desea rastrear. Los archivos se denominan *ipfcomponenteclientconfig.xml.sample*. Por ejemplo, *ipfAAAclientconfig.xml*.
2. Cree una copia del archivo *ipfcomponenteclientconfig.xml.sample* especificado utilizando el nombre *ipfclientconfig.xml.off*.
3. Mediante un editor de texto, abra el archivo *ipfclientconfig.xml.off* y realice los cambios siguientes:

- Añada o modifique el nivel de registro del <categories> que necesite.
- Realice una de las dos acciones siguientes:

Añada una nueva sección <appender> bajo el último elemento <appender> existente, como se indica a continuación:

```
<appender name="DyeTraceOutput" class="org.apache.log4j.RollingFileAppender">
  <param name="File" value="../logs/dyetrace_output.log"/>
  <param name="MaxBackupIndex" value="1"/>
  <param name="MaximumFileSize" value="10485760"/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="%m%n"/>
  </layout>
  <filter class="com.cognos.indications.LogIPFDyeTraceFilter"/>
</appender>
```

O modifique una de las definiciones de adicionador existentes añadiendo la línea

```
<filter class="com.cognos.indications.LogIPFDyeTraceFilter"/>
```

before closing the </appender> tag.

4. Para las secciones de <category> a las que desea aplicar el filtro de rastreo hasta el originador, edite la propiedad <appender-ref> para que ésta haga referencia al adicionador DyeTraceOutput o al adicionador al que se ha añadido el filtro. Por ejemplo:

```
<category name="Audit.RTUsage.CAM.AAA" class="com.cognos.indications.
LogTypedLogger" additivity="false">
  <level value="debug"/>
  <appender-ref ref="DyeTraceOutput"/>
</category>
```

5. Guarde el archivo *ipfclientconfig.xml.off*.
6. Para activar este archivo, cambie su nombre por *ipfclientconfig.xml*.
7. Puede inhabilitar el registro específico de usuario y reanudar el registro normal cambiando el nombre del archivo *ipfclientconfig.xml* nuevamente por *ipfclientconfig.xml.off*. Restablezca los usuarios a los que ha aplicado DyeTracing después de reiniciar el producto.

Resultados

En 60 segundos, el registro específico de usuario se activa automáticamente y se genera salida. Para el adicionador descrito aquí, la salida se almacena en el archivo *install_location*\logs\dyetrace_output.log. Para otros adicionadores, será el

destino configurado para ese adicionador. Cuando se establece una sesión autenticada con IBM Cognos, sólo se registran las acciones del usuario especificado.

Puede que reciba alguna indicación no relacionada con el usuario especificado. Por ejemplo, esto podría producirse cuando inicia el producto o cuando se registran indicaciones antes de haberse completado la autenticación del usuario. Puede cambiar el nivel de registro de las categorías para que no se genere un número excesivo de indicaciones.

Inhabilitación del registro para un usuario específico

Puede inhabilitar el registro para un usuario específico.

Procedimiento

Suprima el archivo `ipfclientconfig.xml` que ha creado en “Utilización del registro para diagnosticar un problema para un usuario específico” en la página 24.

Resultados

Se reanuda el registro normal de todos los usuarios. El registro de un usuario concreto puede tardar 30 segundos en detenerse.

Capítulo 4. Métricas de rendimiento del sistema

Puede supervisar el rendimiento del sistema mediante métricas en IBM Cognos Administration, lo que permite diagnosticar y corregir problemas rápidamente.

Por ejemplo, es posible que desee saber si hay más de 50 elementos en una cola o si algún elemento ha estado esperando en una cola más tiempo del especificado.

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration** Capítulo 13, “Funciones y características protegidas”, en la página 227.

Mediante métricas, puede evaluar el estado del sistema en conjunto, además del estado de cada uno de los servidores, los asignadores y los servicios. Es posible visualizar los atributos de cada puntuación de métrica, establecer los valores de umbral que se utilizan para calcular métricas y restablecer métricas. Si lo desea, puede renovar las conexiones del servicio de informes en el caso de que se haya reconstruido un PowerCube.

También es posible realizar funciones tales como iniciar y detener asignadores o servicios “Detención e inicio de asignadores y servicios” en la página 52 y anular el registro de asignadores “Eliminación de asignadores del entorno” en la página 55.

Se pueden utilizar archivos de registro para analizar el rendimiento y la utilización a largo plazo Capítulo 3, “Configuración del registro”, en la página 17.

Se puede crear un archivo dump de métricas para tareas de resolución de problemas .

Cómo recopilar datos de métricas

Los datos de las métricas se recopilan de forma diferente dependiendo del tipo de cambio de la métrica, el ámbito temporal y el tiempo de recopilación asociado con la métrica.

Para obtener más información sobre cómo se aplican a las métricas individuales, consulte “Métricas del sistema” en la página 30.

Tipo de cambio de métrica

El valor que muestra una métrica depende del tipo de cambio, según se muestra en la tabla siguiente.

Tabla 7. Tipos de cambio de métrica

Tipo de cambio	Descripción
Contador	El valor es una suma que aumenta con cada cambio. Por ejemplo, número de peticiones es un tipo de cambio de contador.

Tabla 7. Tipos de cambio de métrica (continuación)

Tipo de cambio	Descripción
Indicador	El valor puede aumentar o disminuir con el tiempo, dependiendo de los eventos. Por ejemplo, el número de procesos que se ejecutan en un determinado momento es un tipo de cambio de indicador.

Ámbito temporal de la métrica

El intervalo en el que se recopila el valor de una métrica difiere de una métrica a otra, según se muestra en la tabla siguiente.

Tabla 8. Alcances de tiempo de métrica

Ámbito temporal	Descripción
Momento determinado	El valor se recopila en un punto específico del tiempo como, por ejemplo, al restablecer un grupo de métricas o reiniciar un servicio.
Desde restablecimiento	El valor se recopila en el intervalo después del último restablecimiento de la métrica.

Tiempo de recopilación de la métrica

El tiempo en el que se recopila el valor de una métrica difiere de una métrica a otra, según se muestra en la tabla siguiente.

Tabla 9. Tiempos de recopilación de la métrica

Tiempo de recopilación	Descripción
Al cambiar	El valor se recopila cuando se produce un cambio como, por ejemplo, cuando cambia el número de solicitudes.
A petición	El valor se recopila al seleccionar un artículo nuevo en el panel Tabla de puntuación o al restablecer un grupo de métricas. Para obtener más información, consulte: "Paneles de la página de estado del sistema" en la página 42 y "Restablecimiento de métricas" en la página 46.
Desconocido	El tiempo de recopilación se desconoce.

Métricas del sistema

Existe una amplia variedad de métricas disponibles que ayudan a supervisar el rendimiento de la instalación del software de IBM Cognos.

Para obtener más información, consulte “Cómo recopilar datos de métricas” en la página 29.

Algunas métricas se restablecen cuando se reinicia el servicio. Otras métricas también se pueden restablecer manualmente “Restablecimiento de métricas” en la página 46.

En el nivel del sistema y del servidor, las métricas incluyen todos los asignadores asociados. En el nivel del asignador, las métricas incluyen todos los servicios asociados. En los grupos de servidores, las métricas se refieren a todos los asignadores del grupo.

Métricas de sesión

Puede utilizar las métricas de sesión para supervisar las sesiones de usuario. Esto es útil para supervisar tendencias del sistema, como modelos de utilización por hora del día y día de la semana. Las métricas de sesión también son útiles para comprender el contexto de otras métricas. Por ejemplo, si el número de sesiones es extraordinariamente elevado, podría representar que las métricas de longitud de cola son más altas de lo normal. Para obtener más información, consulte “Métricas de cola” en la página 32.

Están disponibles las siguientes métricas de sesión:

- **Número de sesiones**

Especifica el número de sesiones de usuario activas.

Tabla 10. Número de sesiones

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema	Indicador	Momento determinado	A petición

- **Marca de límite superior de sesiones**

Especifica el número máximo de sesiones de usuario activas desde el último restablecimiento.

Tabla 11. Marca de límite superior de sesiones

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema	Indicador	Desde restablecimiento	Al cambiar

- **Marca de límite inferior de sesiones**

Especifica el número mínimo de sesiones de usuario activas desde el último restablecimiento.

Tabla 12. Marca de límite inferior de sesiones

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema	Indicador	Desde restablecimiento	Al cambiar

Métricas de cola

Puede utilizar métricas de cola para determinar si el sistema es capaz de satisfacer la demanda. Por ejemplo, si las solicitudes pasan demasiado tiempo en una cola, es posible que no se disponga de recursos suficientes para satisfacer la demanda.

Las métricas de cola están disponibles para servicios que utilizan colas, como el servicio de informes y el servicio de datos de informes.

En el nivel del sistema, las métricas de cola están disponibles para las siguientes entradas:

- Trabajo
Cola de trabajos contiene métricas relacionadas con la cola interna que utilizan todos los servicios de gestión de eventos.
- Tarea
Cola de tareas contiene métricas relacionadas con la cola interna que utilizan todos los servicios de control. Esta cola contiene las tareas hasta que se completan correctamente.
- SMTP
Cola SMTP contiene métricas relacionadas con la cola interna que utilizan todos los servicios de entrega. Esta cola contiene los correos electrónicos hasta que se envían.

Algunos de las métricas disponibles para esos grupos de métricas de cola deben estar habilitados para que se muestren. Para obtener más información, consulte “Habilitación de métricas de cola de tareas, trabajos y SMTP” en la página 107.

Están disponibles las siguientes métricas de cola:

- **Latencia**
Especifica la duración media de tiempo que las solicitudes han pasado en la cola (en segundos).

Tabla 13. Latencia

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Número de solicitudes de cola**
Especifica el número de solicitudes que han pasado a través de la cola.

Tabla 14. Número de solicitudes de cola

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio	Contador	Desde restablecimiento	Al cambiar

- **Longitud de la cola**

Especifica el número de elementos incluidos en la cola.

Tabla 15. Longitud de la cola

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio	Indicador	Momento determinado	A petición

- **Marca de límite superior de longitud de la cola**

Especifica el número máximo de elementos en la cola desde el último restablecimiento.

Tabla 16. Marca de límite superior de longitud de la cola

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Marca de límite inferior de longitud de la cola**

Especifica el número mínimo de elementos en la cola desde el último restablecimiento.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Tiempo en cola**

Especifica la duración acumulada de tiempo que las solicitudes han pasado en la cola (en días, horas, minutos y segundos).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio	Contador	Desde restablecimiento	Al cambiar

- **Marca de límite superior de tiempo en cola**

Especifica el periodo máximo de tiempo que una solicitud ha esperado en la cola (en días, horas, minutos y segundos).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Marca de límite inferior de tiempo en cola**

Especifica el periodo mínimo de tiempo en días, horas, minutos o segundos que una solicitud ha esperado en la cola.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio	Indicador	Desde restablecimiento	Al cambiar

Métricas JVM

Las métricas JVM se pueden utilizar para supervisar la Máquina virtual Java y su tamaño de montón asociado, que especifica la cantidad de memoria que está en uso actualmente. Por ejemplo, si un asignador se ha estado ejecutando durante un tiempo prolongado y el índice de utilización del montón es alto, puede ser conveniente reiniciar el asignador. La métrica de tamaño máximo del montón indica si se ha asignado una cantidad adecuada de memoria a la JVM en función de la cantidad de memoria hardware disponible. El tamaño actual del montón, con relación al tamaño máximo del montón, indica si se está utilizando la memoria disponible. Si el tamaño actual del montón está próximo al tamaño máximo del montón, es posible modificar los valores de ajuste para reducir la carga en una JVM determinada. El tamaño actual del montón puede variar ampliamente dependiendo de la carga actual del sistema.

Para obtener más información sobre ajuste, consulte “Ajuste del rendimiento de servidor” en la página 74.

Están disponibles las siguientes métricas JVM:

- **Tamaño de montón actual (bytes)**

Especifica el tamaño actual del montón de JVM (en bytes).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Asignador	Indicador	Momento determinado	A petición

- **Tamaño de montón solicitado inicialmente (bytes)**

Especifica la cantidad inicial de memoria que la JVM solicita al sistema operativo durante el inicio (en bytes).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Asignador	Indicador	Momento determinado	A petición

- **Tamaño de montón máximo (bytes)**

Especifica la cantidad máxima de memoria que puede utilizar la JVM (en bytes).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Asignador	Indicador	Momento determinado	A petición

- **Tiempo activo**

Periodo de tiempo durante el que la JVM ha estado en ejecución (en días, horas, minutos y segundos).

En los niveles del sistema, el servidor y el grupo de servidores, éste es el valor más alto de todos los asignadores asociados.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador	Contador	Momento determinado	A petición

- **Tamaño de montón confirmado**

Especifica la cantidad de memoria cuya disponibilidad está garantizada para su uso por parte de JVM (en bytes).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Asignador	Indicador	Momento determinado	A petición

Métricas de solicitud

Las métricas de solicitud se pueden utilizar para supervisar el volumen de las solicitudes, el estado operativo de los servicios, los tiempos de respuesta y los tiempos de procesamiento. Las métricas generales de solicitud incluyen datos para todos los servicios y son una consolidación de las métricas para todos los asignadores. Las métricas de solicitud específicos de un servicio sólo incluyen datos para ese servicio.

En los niveles del sistema, el servidor y el grupo de servidores, las métricas incluyen datos de todos los asignadores asociados. En el nivel del asignador, las métricas incluyen todos los servicios asociados.

Están disponibles las siguientes métricas de solicitud:

- **Hora actual**

Especifica la hora y fecha actuales utilizadas por el servicio para interpretar los valores de tiempo.

Utilícelo sólo si el servicio no tiene ningún mecanismo de sincronización de reloj.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Servicio	Contador	Momento determinado	A petición

- **Último tiempo de respuesta**

Especifica el tiempo de procesamiento de la solicitud correcta o errónea más reciente (en días, horas, minutos y segundos).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Indicador	Momento determinado	Al cambiar

- **Número de solicitudes con error**

Especifica el número de solicitudes de servicio que han fallado (se ha devuelto un error).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Contador	Desde restablecimiento	Al cambiar

- **Número de solicitudes procesadas**

Especifica el número de solicitudes procesadas.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Contador	Desde restablecimiento	Al cambiar

- **Número de solicitudes correctas**

Especifica el número de solicitudes de servicio que se han realizado correctamente (no se ha devuelto un error).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Contador	Desde restablecimiento	Al cambiar

- **Porcentaje de solicitudes con error**

Especifica el porcentaje de solicitudes procesadas que han devuelto un error.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Porcentaje de solicitudes correctas**

Especifica el porcentaje de solicitudes procesadas que se han realizado correctamente.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Marca de agua máxima de tiempo de respuesta**

Especifica el periodo máximo de tiempo empleado en procesar una solicitud correcta o con error (en días, horas, minutos y segundos).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Marca de agua mínima de tiempo de respuesta**

Especifica el periodo mínimo de tiempo empleado en procesar una solicitud correcta o con error (en días, horas, minutos y segundos).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Segundos por solicitud correcta**

Especifica el periodo medio de tiempo empleado en procesar una solicitud correcta (en segundos).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Indicador	Desde restablecimiento	Al cambiar

- **Tiempo de servicio**

Especifica el tiempo empleado en procesar todas las solicitudes (en días, horas, minutos y segundos).

Entrada	Hora de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Contador	Desde restablecimiento	Al cambiar

- **Tiempo de servicio empleado con solicitudes con error**

Especifica el tiempo empleado en procesar todas las solicitudes de servicio con error (en días, horas, minutos y segundos).

Entrada	Hora de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Contador	Desde restablecimiento	Al cambiar

- **Tiempo de servicio empleado con solicitudes correctas**

Especifica el tiempo empleado en procesar todas las solicitudes de servicio correctas (en días, horas, minutos y segundos).

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Contador	Desde restablecimiento	Al cambiar

- **Solicitudes correctas por minuto**

Especifica el número medio de solicitudes correctas procesadas en un minuto.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Asignador Servicio	Indicador	Desde restablecimiento	Al cambiar

Métricas de proceso para el servicio de informes, de informes por lotes y de metadatos

Las siguientes métricas de proceso están disponibles para servicios de informes, servicios de informes por lotes y servicios de metadatos:

- **Número de procesos**

Especifica el número de procesos actualmente en ejecución.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio de informes y servicio de informes por lotes Servicio de metadatos	Indicador	Momento determinado	A petición

- **Número de procesos configurados**

Especifica el mismo valor que se configuró para las siguientes propiedades de servicios afectados:

- “Número máximo de procesos para el [nombre_servicio] durante el periodo de máxima actividad”
- “Número máximo de procesos para el [nombre_servicio] durante el periodo que no es de máxima actividad” es un valor no predeterminado

Este valor no se puede restablecer.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio de informes y servicio de informes por lotes Servicio de metadatos	Indicador	Momento determinado	A petición

- **Marca de agua máxima de procesos**

Para sistema, servidor y grupo de servidores, se especifica el número total de todas las métricas de marca de agua máxima de procesos para todos los recursos asociados.

Para servicios, se especifica el número máximo de procesos que se ejecutan en un momento dado después del último restablecimiento.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio de informes y servicio de informes por lotes Servicio de metadatos	Indicador	Desde restablecimiento	Al cambiar

- **Marca de agua mínima de procesos**

Para sistema, servidor y grupo de servidores, se especifica el número total de todas las métricas de marca de agua mínima de procesos para todos los recursos asociados.

Para servicios, se especifica el número mínimo de procesos que se ejecutan en un momento dado después del último restablecimiento.

Entrada	Tipo de cambio	Ámbito temporal	Tiempo de recopilación
Sistema Servidor/grupo de servidores Servicio de informes y servicio de informes por lotes Servicio de metadatos	Indicador	Desde restablecimiento	Al cambiar

Paneles de la página de estado del sistema

La página Sistema tiene tres paneles, Tabla de puntuación, Métricas y Valores, que se utilizan para evaluar el estado del sistema.

Al pulsar el título se puede ordenar por determinadas columnas. De forma predeterminada, las columnas están ordenadas en orden ascendente. Para ordenar en orden ascendente, pulse el botón del ratón una vez. Para ordenar en orden descendente, vuelva a pulsar el botón del ratón. Para volver al orden predeterminado, pulse el botón del ratón una tercera vez. Cada panel se puede renovar de forma independiente.

Panel Tabla de puntuación

El panel **Tabla de puntuación** enumera las entradas: sistema, servidores, grupos de servidores, asignadores y servicios. Para cada entrada, se muestra una puntuación

de métrica y el estado operativo, de manera que se pueda evaluar el rendimiento del sistema. Para obtener más información, consulte “Evaluación del rendimiento del sistema” en la página 44.

Cada puntuación de métrica se representa mediante uno de los siguientes iconos:

- Un círculo verde indica que es buena .
- Un rombo amarillo indica que está en el promedio .
- Un cuadrado rojo indica que es insuficiente .

Es necesario establecer los umbrales antes de que aparezcan las puntuaciones de métrica. Para obtener más información, consulte “Establecimiento de los valores del umbral de la métrica” en la página 45.

Si un servicio está inhabilitado en IBM Cognos Configuration, no aparecerá en la lista.

La puntuación de métrica de cada entrada se basa en el rendimiento de entradas hijo individuales. El estado que se muestra para cada entrada es el estado más bajo de las entradas hijo. Por ejemplo, si todas las métricas de un asignador son buenas, pero un servicio de ese asignador tiene una métrica insuficiente, la puntuación de métrica que se mostrará para el asignador será insuficiente.

El estado es uno de los siguientes:

- **Disponible** si todos los componentes están disponibles.
- **Parcialmente disponible** si al menos un componente está disponible y otro componente no está disponible o está parcialmente no disponible.
- **No disponible** si ningún componente está disponible.

El menú Acciones para grupos permite realizar funciones tales como iniciar y detener asignadores o servicios “Detención e inicio de asignadores y servicios” en la página 52, anular el registro de asignadores “Eliminación de asignadores del entorno” en la página 55 y probar asignadores “Prueba de los asignadores” en la página 62. Además, cada entrada tiene un menú Acciones asociado, al que se accede pulsando la flecha situada junto a la entrada.

Puede utilizar el panel **Tabla de puntuación** para dirigirse hasta la entrada que desee ver. Puede seleccionar la vista que desee desde el menú Cambiar vista situado en la esquina superior izquierda. Es posible pulsar las entradas para seleccionarlasy mostrar el siguiente nivel de entradas. Por ejemplo, pulse un servidor para ver los asignadores asociados o pulse un asignador para ver los servicios asociados.

El panel **Tabla de puntuación** se puede maximizar para ver una vista consolidada de información que se muestra en el panel **Tabla de puntuación** y métricas importantes del panel **Métricas**. La vista consolidada incluye la siguiente información:

- Para los servidores y los grupos de servidores: puntuación de métrica, estado operativo, tiempo activo, tiempo de servicio, número de solicitudes procesadas y porcentaje de solicitudes correctas.

- Para los asignadores: puntuación de métrica, estado operativo, número de procesos, tiempo de servicio, tamaño de montón actual (bytes), número de solicitudes procesadas y porcentaje de solicitudes correctas.
- Para los servicios, la información depende del servicio.

Panel Métricas

El panel **Métricas** muestra las métricas de la entrada seleccionada. Los grupos de métricas se pueden ampliar para mostrar valores y puntuaciones de métrica individuales. Cada grupo de métricas se puede restablecer de forma independiente “Restablecimiento de métricas” en la página 46.

Para seleccionar las métricas que desea mostrar, seleccione una o varias casillas de verificación para los valores bueno, promedio o malo o **Sin puntuación de métrica**. De forma predeterminada, se muestran todas las métricas. Las métricas sin puntuación incluyen aquellos para los que no se pueden establecer umbrales y aquellos para los que aún no se han establecido. Para mostrar los últimos, pulse la casilla de verificación **Sin puntuación de métrica** antes de poder establecerlos.

Panel Valores

El panel **Valores** muestra la configuración asociada con la entrada seleccionada en el modo de sólo visualización. Para cambiar los valores, pulse el botón Establecer propiedades .

Para obtener más información sobre los valores del panel **Valores**, consulte: Capítulo 5, “Administración del servidor”, en la página 49.

Evaluación del rendimiento del sistema

Para evaluar el rendimiento del software de IBM Cognos, se pueden ver las puntuaciones de métrica que se basan en los umbrales que haya establecido. También puede ver el estado operativo de los componentes del sistema.

Es necesario establecer los umbrales antes de que aparezcan las puntuaciones de métrica. Para obtener más información, consulte “Establecimiento de los valores del umbral de la métrica” en la página 45. Si los asignadores y los servicios no funcionan como deberían, puede perfeccionar el rendimiento del servidor “Ajuste del rendimiento de servidor” en la página 74. Para obtener más información sobre los valores del registro, consulte: Capítulo 3, “Configuración del registro”, en la página 17.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
El icono de la puntuación de métrica correspondiente a la entrada **Sistema** muestra el estado general del sistema. El icono de la puntuación de métrica de cada servidor muestra el estado de ese servidor. En el panel **Métricas** se muestran las métricas individuales.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.
Si selecciona **Todos los grupos de servidores**, puede ver los asignadores que no estén agrupados por servidor pulsando **Grupo de servidores predeterminado**.
3. Para ver las métricas de un elemento mostrado, pulse la entrada.

4. Para ver los hijos de una entrada mostrada, pulse la entrada.

Consejo: Los paneles individuales se pueden renovar pulsando el botón Renovar del panel.

5. Para ver o cambiar las propiedades de una entrada, pulse el botón del menú Acciones situado junto a la entrada y, a continuación, en **Establecer propiedades**.
6. Para ver la vista consolidada, pulse el botón Maximizar del panel **Tabla de puntuación**.

Consejo: Para volver a la vista anterior, pulse el botón Restaurar.

Visualización de atributos de las puntuaciones de métrica

Puede ver la última vez que una métrica se restableció y se actualizó. También puede ver el valor actual del umbral de cada puntuación de métrica para el que se haya establecido un umbral. En el caso de las métricas que se recopilan a intervalos regulares, también puede ver el periodo de tiempo al que se aplica el valor.

Antes de empezar

Para obtener más información sobre los valores de umbral, consulte “Establecimiento de los valores del umbral de la métrica”.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse la vista que desea.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el panel **Métricas**, expanda  el grupo de métricas que desee ver.
4. En la columna **Valor** del panel **Métricas**, pase el puntero sobre el valor de la métrica que desee ver.
Se mostrará el nombre de la métrica.
5. Para ver más información sobre alguna métrica, pulse **Más**.

Establecimiento de los valores del umbral de la métrica

Se pueden establecer valores de umbral para utilizarlos con algunas puntuaciones de métrica.

Los valores aceptables de umbral dependen del entorno operativo. Cuando se cruza un umbral, cambia el estado de las puntuaciones de métricas.

Por ejemplo, puede determinar que la longitud máxima aceptable de una cola sea de 50 elementos. Seleccione **Los valores bajos son buenos**. Establezca el valor superior en 50 y el valor inferior en 40. Si la cola permanece por debajo de 40 elementos de longitud, la puntuación de métrica estará en verde (bueno). Si la longitud de la cola supera los 40 elementos, la puntuación de métrica estará en amarillo (promedio). Si la longitud de la cola supera los 50 elementos, la puntuación de métrica estará en rojo (insuficiente).

O para el porcentaje de solicitudes correctas, puede seleccionar **Los valores elevados son buenos**. Establezca el valor superior en 98 y el valor inferior en 95. Si el porcentaje de solicitudes correctas cae por debajo del 95 por ciento, la puntuación de métrica estará en rojo (insuficiente). Si el porcentaje de solicitudes correctas está entre el 95 y el 98 por ciento, la puntuación de métrica estará en amarillo (promedio). Si el porcentaje de solicitudes correctas permanece por encima de 98, la puntuación de métrica estará en verde (bueno).

Los cambios en los umbrales surten efecto de forma inmediata.

No existen valores predeterminados para los umbrales. Debe establecerlos para que se muestren las puntuaciones de métrica.

Antes de empezar

Las entradas del registro Capítulo 3, “Configuración del registro”, en la página 17 se realizan en las circunstancias siguientes:

- Cuando hay infracciones de los umbrales de la métrica.
- Cuando cambian las métricas enumeradas, como el estado operativo.

No se generan registros cuando cambian los valores de la métrica pero permanecen en el mismo rango.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse la vista que desea.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. Para cambiar el umbral de una métrica, en el panel **Métricas**, pulse el botón Editar umbrales  correspondiente a la métrica.
4. Pulse el modelo de rendimiento que desee: **Los valores elevados son buenos**, **Los valores medios son buenos** o **Los valores bajos son buenos**.
5. Para especificar un valor de umbral, pulse el cuadro de umbral e introduzca el número de umbral que desee.
6. Pulse la flecha del valor de umbral para especificar el rango en el que está incluido el valor.
Por ejemplo, si el valor máximo es de 50 y desea que los valores de 50 se incluyan en la categoría promedio antes que en la categoría insuficiente, pulse la flecha para mover el valor del umbral a la categoría promedio.
7. Pulse en **Aceptar**.

Restablecimiento de métricas

Un grupo de métricas se puede restablecer en cualquier momento.

Al restablecer un grupo de métricas, se restablecen todas las métricas del grupo. Por ejemplo, puede restablecer el grupo de métricas Cola - Servicio de informes de un servidor.

Algunas métricas no se pueden restablecer. Por ejemplo, las métricas de JVM no se pueden restablecer porque se recalcularon después del último restablecimiento.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse la vista que desea.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el panel **Métricas**, pulse el botón Restablecer  para el grupo de métricas que desee restablecer.

Restablecimiento de las métricas del sistema

Se pueden restablecer todas las métricas del sistema al mismo tiempo.

Algunas métricas no se pueden restablecer. Por ejemplo, las métricas de JVM no se pueden restablecer por que se recalcularon después del último restablecimiento.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, pulse **Acciones**, **Restablecer todas las métricas del sistema**.

Renovación de las conexiones de servicio de informes

Si se ha reconstruido un PowerCube, puede actualizar la información de conexión sin que los usuarios actuales se vean afectados.

En primer lugar debe renovar la información de conexión con el PowerCube reconstruido y, a continuación, renovar los servidores de informes para utilizar el PowerCube reconstruido para las conexiones nuevas.

Para obtener más información, consulte “Despliegue de PowerCubes actualizados” en la página 171.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. Con todos los servidores mostrados, pulse la casilla de verificación de los servidores que desee y, en el menú **Acciones para grupos**, pulse **Renovar las conexiones de servicio de informes**.

Consejo: También puede realizar esta tarea desde el menú **Acciones** situado junto al sistema, los servidores y los asignadores. También puede pulsar la pestaña **Configuración**, después en **Asignadores y servicios** y después en el botón **Renovar las conexiones de servicio de informes - Configuración**.

3. Cuando aparezca la página **Ver los resultados**, asegúrese de que la operación se ha realizado correctamente y pulse **Cerrar**.

Capítulo 5. Administración del servidor

La administración del servidor incluye la gestión y el mantenimiento del sistema IBM Cognos, y el ajuste del rendimiento del sistema.

Debe estar familiarizado con los componentes de IBM Cognos y con el modo de instalarlos y configurarlos. Si ha instalado componentes o servidores de IBM Cognos en más de un sistema, toda la funcionalidad se puede controlar a través de la administración del sistema. Para obtener información sobre el entorno de IBM Cognos, consulte la *IBM Cognos Analytics Guía de de instalación y configuración*.

Para realizar determinadas tareas de administración, puede utilizar los componentes de administración y debe tener los permisos necesarios para acceder a la función de administración Capítulo 13, “Funciones y características protegidas”, en la página 227.

Asignadores y servicios

El asignador es el punto de entrada de las solicitudes de servicio de IBM Cognos enviadas por una pasarela de un servidor web u otro software. El asignador controla las solicitudes de direccionamiento y equilibra la carga de solicitudes del usuario a los distintos servicios de IBM Cognos.

En el entorno de IBM Cognos dispone de más de un asignador. En estas instalaciones distribuidas, un asignador se configura para cada instancia del Content Manager o de Componentes de nivel de aplicación que están instalados y configurados en el entorno.

Después de instalar y configurar el software de IBM Cognos habrá un asignador en cada sistema de forma predeterminada. Cada asignador tiene una serie de servicios asociados, los cuales se enumeran en la siguiente tabla.

Servicios de IBM Cognos

Después de instalar y configurar IBM Cognos Analytics, habrá un asignador en cada sistema de forma predeterminada. Cada asignador tiene una serie de servicios asociados, los cuales se enumeran en la siguiente tabla.

Tabla 17. Servicios de IBM Cognos

Servicio	Función
Servicio de agente	Ejecuta agentes. Si las condiciones de un agente se cumplen al ejecutarlo, el servicio de agente pide al servicio de control que ejecute las tareas.
Servicio de anotaciones	Permite la adición de comentarios a los informes por medio del espacio de trabajo de IBM Cognos. Estos comentarios se conservan en todas las versiones del informe.
Servicio de informes por lotes	Gestiona las peticiones de segundo plano de ejecutar informes y ofrece informes de salida en nombre del servicio de control.

Tabla 17. Servicios de IBM Cognos (continuación)

Servicio	Función
Servicio de memoria caché de Content Manager	Aumenta el rendimiento global del sistema y la escalabilidad de Content Manager mediante el almacenamiento en la caché de los resultados de las consultas frecuentes en cada asignador.
Servicio de Content Manager	- Desempeña funciones de manipulación de objetos en el almacén de contenido, como añadir, consultar, actualizar, suprimir, mover y copiar. - Realiza funciones de gestión del almacén de contenido, como importar y exportar.
Servicio de entrega	Envía correos electrónicos a un servidor SMTP externo en nombre de otros servicios, tales como los servicios de informes, los servicios de trabajos o de agentes
Servicio de gestión de eventos	Crea, planifica y gestiona objetos de eventos que representan informes, trabajos, agentes, mantenimiento del almacén de contenido y despliegue de importaciones y exportaciones.
Servicio Graphics	Produce gráficos en nombre del servicio de informes. Los gráficos se pueden generar en cuatro formatos distintos: Barrido, Vector, Microsoft Excel XML o PDF.
Human Task Service	Permite la creación y la administración de tareas humanas. Una tarea humana, como la aprobación de un informe, se puede asignar a una persona o a un grupo ad hoc o mediante cualquiera de los otros servicios.
Servicio de visualización de descubrimiento interactivo	Lo utiliza Cognos Workspace para proporcionar recomendaciones de visualización.
Servicio de trabajos	Ejecuta trabajos indicando al servicio de control que ejecute los pasos del trabajo en segundo plano. Los pasos incluyen informes, otros trabajos, importaciones, exportaciones, etc.
Servicio de registro	Graba los mensajes de registro generados por el asignador y otros servicios. El servicio de registro puede configurarse para grabar información de registro en un archivo, una base de datos, un servidor de registro remoto, el visor de sucesos de Windows o un registro del sistema UNIX. Los clientes o Cognos Software Services pueden entonces analizar la información de registro, como la que se indica a continuación: - Eventos de seguridad - Información de error del sistema y de aplicación - Información de diagnóstico seleccionada

Tabla 17. Servicios de IBM Cognos (continuación)

Servicio	Función
Servicio de metadatos	Ofrece soporte para la información de linaje de datos en Cognos Viewer, Creación de informes, Query Studio y Analysis Studio. La información de linaje incluye información como, por ejemplo, el origen de datos y expresiones de cálculo.
Servicio de migración	Gestiona la migración de IBM Cognos Series 7 a IBM Cognos Analytics.
Servicio móvil	Gestiona las actividades relacionadas con el cliente de IBM Cognos Mobile: • Transforma los informes y análisis para consumo móvil. • Comprime el contenido de informes y análisis para una rápida distribución sin cables a dispositivos móviles y disponer de acceso desde esos dispositivos. • Lleva el contenido de informes y análisis a los dispositivos móviles. • Facilita las solicitudes relacionadas con informes y análisis de entrada y salida entre el dispositivo móvil y el entorno en el que se debe buscar, examinar o ejecutar informes. • Sincroniza el almacén de contenido móvil en el servidor con la base de datos móvil del dispositivo móvil. • Traduce mensajes SOAP (Simple Object Access Protocol) en mensajes aptos para dispositivos inalámbricos. • Se comunica con el dispositivo móvil.
Servicio de control	• Gestiona la supervisión y la ejecución de tareas planificadas, enviadas para su ejecución posterior o ejecutadas como tareas de segundo plano. • Asigna un servicio de destino para que se haga cargo de una tarea planificada. Por ejemplo, el servicio de control puede pedir al servicio de informes por lotes que ejecute un informe, al servicio de trabajos que ejecute un trabajo o al servicio de agente que ejecute un agente. • Crea objetos de historial en Content Manager y gestiona la migración tras error y la recuperación de entradas de ejecución.
Servicio de consola de administración de Planning	Gestiona la comunicación con la consola de Contributor Administration.
Servicio de datos Planning	Gestiona comunicaciones para la creación de informes en tiempo real a partir de datos del plan de Contributor.

Tabla 17. Servicios de IBM Cognos (continuación)

Servicio	Función
Servicio de trabajos Planning	Gestiona la comunicación con el subsistema del servidor de trabajo Planning.
Servicio web de Planning	Se ocupa de la comunicación con Web de Contributor y el complemento de Contributor de los usuarios de <i>Excel</i> .
Servicio de PowerPlay	Gestiona las solicitudes de ejecución de informes de PowerPlay.
Servicio de presentación	- Transforma las respuestas genéricas XML de otro servicio en formatos de salida como HTML o PDF. - Ofrece funciones de visualización, navegación y administración.
Query Service	Gestiona las solicitudes de consulta dinámica y devuelve el resultado al servicio por lotes o de informes que las ha enviado.
Servicio de metadatos relacionales	Lo utilizan Framework Manager y CubeDesigner para importar metadatos desde bases de datos relacionales. También lo puede utilizar Dynamic Query Analyzer durante la ejecución.
Servicio de datos de informes	Gestiona la transferencia de datos de informe entre IBM Cognos Analytics y las aplicaciones que utilizan los datos, como IBM Cognos for Microsoft Office e IBM Cognos Mobile.
Servicio de informes	Se encarga de las peticiones interactivas de ejecución de informes y ofrece informes de salida a los usuarios.
Servicio de repositorio	Gestiona solicitudes para recuperar la salida del informe archivado de un repositorio de archivos o almacén de objetos.
Servicio del sistema	Define el servicio de Business Intelligence compatible con Bus API empleado para obtener los parámetros de configuración de toda la aplicación. También ofrece métodos para normalizar y validar cadenas de entorno local y correlacionar cadenas de entorno local a los entornos locales soportados por su aplicación.
Servicio de la galería de visualización	Se utiliza para cargar y recuperar visualizaciones RAVE1 en la galería de visualizaciones de Creación de informes. Lo requiere el servicio de informes.

Detención e inicio de asignadores y servicios

Puede detener e iniciar asignadores y servicios manualmente. Si un servicio deja de responder, debe detenerlo y reiniciarlo.

Cada asignador y servicio se puede:

- Iniciar.

- Detener inmediatamente y suprimir todas las solicitudes en ejecución o en cola, sin terminar esas solicitudes.
- Detener después de que se procesen las solicitudes en ejecución y en cola.

Puede detener o iniciar a la vez todos los asignadores y servicios del entorno de IBM Cognos.

Al iniciar el software de IBM Cognos mediante la herramienta de configuración, se inician todos los asignadores y servicios a menos que estén inhabilitados en la herramienta de configuración. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

De forma predeterminada, todos los servicios se inician cuando se reinicia el sistema en el que están instalados.

Antes de empezar

Al detener un servicio también se detienen todos sus procesos. Al detener un asignador, se detienen todos sus servicios. Si el asignador suspendido tiene un Content Manager activo, se bloquean todos los usuarios excepto los administradores.

Cuando un servicio se detiene, su estado pasa a ser suspendido Capítulo 4, “Métricas de rendimiento del sistema”, en la página 29.

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse los asignadores o los servicios que desea.
Pulse **Todos los servidores**, **Todos los grupos de servidores** o **Todos los asignadores**. Para seleccionar un servicio, detenga el puntero sobre **Servicios** y pulse el servicio necesario.
3. Pulse la flecha del menú Acciones correspondiente al asignador o al servicio y elija la acción que desee realizar.
Dependiendo del asignador o el servicio, puede realizar las acciones siguientes:

Tabla 18. Detención e inicio de asignadores y servicios: objetivos, vistas y acciones

Objetivo	Vista del panel Tabla de puntuación	Acción
Iniciar todos los asignadores del sistema	Todos los servidores	En el menú Acciones para grupos, pulse Iniciar los asignadores . Consejo: Para aplicar una acción solamente a algunas entradas, seleccione las casillas de verificación de una o varias entradas y, a continuación, pulse la acción que desee.

Tabla 18. Detención e inicio de asignadores y servicios: objetivos, vistas y acciones (continuación)

Objetivo	Vista del panel Tabla de puntuación	Acción
Iniciar todos los asignadores para un grupo de servidores	Todos los grupos de servidores	En el menú Acciones del grupo de servidores, pulse Iniciar los asignadores .
Iniciar todos los asignadores para un servidor	Todos los servidores	En el menú Acciones del servidor, pulse Iniciar los asignadores .
Iniciar un asignador específico	Todos los asignadores	En el menú Acciones del asignador, pulse Iniciar .
Iniciar un servicio específico	Todos los servicios	En el menú Acciones del servicio, pulse Iniciar .
Detener todos los asignadores del sistema	Todos los servidores	En el menú Acciones para grupos, pulse Detener inmediatamente los asignadores o Detener los asignadores después de completar la ejecución y la cola .
Detener todos los asignadores para un grupo de servidores	Todos los grupos de servidores	En el menú Acciones del grupo de servidores, pulse Detener inmediatamente los asignadores o Detener los asignadores después de completar la ejecución y la cola .
Detener todos los asignadores para un servidor	Todos los servidores	En el menú Acciones del servidor, pulse Detener inmediatamente los asignadores o Detener los asignadores después de completar la ejecución y la cola .
Detener un asignador específico	Todos los asignadores	En el menú Acciones del asignador, pulse Detener inmediatamente o Detener después de completar la ejecución y la cola .
Detener un servicio específico	Todos los servicios	En el menú Acciones del servicio, pulse Detener inmediatamente o Detener después de completar la ejecución y la cola .

Aparecerá un cuadro de diálogo para confirmar la acción.

4. Pulse **Cerrar**.

Servicio de Content Manager activo

Un servicio de Content Manager que está en modo en espera se puede activar manualmente.

Un servicio de Content Manager está diseñado para activarse al inicio. Los demás servicios de Content Manager se inician en modo en espera. Sólo puede haber un

servicio de Content Manager activo en un momento determinado. Al activar un servicio, el servicio que esté activo cambia a modo en espera.

También se puede especificar un servicio de Content Manager que esté en espera como el servicio activo predeterminado al inicio.

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Especificación de un servicio de Content Manager predeterminado

Puede especificar un servicio de Content Manager predeterminado.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Content Manager**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** de **ContentManagerService**, pulse **Establecer como activo de forma predeterminada**.

Consejo: Solamente los servicios de Content Manager que no sean el servicio predeterminado mostrarán la opción **Establecer como activo de forma predeterminada** en el menú **Acciones**.

Activar un servicio de Content Manager

Puede activar un servicio de Content Manager específico.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Content Manager**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** de **ContentManagerService**, pulse **Iniciar**.

Eliminación de asignadores del entorno

Es posible eliminar un asignador que ya no se necesite en el entorno de IBM Cognos.

Puede detener el servicio de IBM Cognos mediante IBM Cognos Configuration. Con esta acción también se detendrá el asignador. Si suprime un asignador sin detener antes el servicio de IBM Cognos, el asignador se reiniciará automáticamente al cabo de 30 segundos.

Antes de empezar

Para eliminar un asignador, primero se debe detener el asignador del sistema en el que esté instalado. Después de detener el asignador, debe eliminarlo del almacén de contenido; para ello, anule el registro correspondiente en IBM Cognos Administration.

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. Detenga el servicio de IBM Cognos mediante IBM Cognos Configuration.
Con esto también se detiene el asignador. Para obtener información acerca de la detención del servicio de IBM Cognos, consulte la *IBM Cognos Analytics Guía de instalación y configuración*.
2. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
3. Determine los asignadores de los que desee anular el registro. Puede anular el registro de todos los asignadores del sistema, de un servidor o de un grupo de servidores.
4. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Todos los servidores**, **Todos los grupos de servidores** o **Todos los asignadores**. La vista que elija depende de los asignadores cuyo registro desee anular.

Tabla 19. Acciones necesarias para lograr los objetivos de anulación de registro para los asignadores

Objetivo	Acción
Anular el registro de todos los asignadores del sistema	En la vista Tabla de puntuación , Todos los asignadores , pulse la flecha para ver el menú Acciones para grupos y, a continuación, pulse Anular el registro de los asignadores . Consejo: Para aplicar una acción solamente a algunas entradas, seleccione las casillas de verificación de una o varias entradas y, a continuación, pulse la acción que desee.
Anular el registro de todos los asignadores para un servidor	En la vista Tabla de puntuación , Todos los servidores , en el menú Acciones de un servidor, pulse Anular el registro de los asignadores .
Anular el registro de todos los asignadores para un grupo de servidores	En la vista Tabla de puntuación , Todos los grupos de servidores , en el menú Acciones de un asignador, pulse Anular el registro de los asignadores .
Anular el registro de un asignador específico	En la vista Tabla de puntuación , Todos los asignadores , en el menú Acciones de un asignador, pulse Anular registro .

Aparecerá un cuadro de diálogo para confirmar la acción.

5. Pulse **Aceptar**.

La información del asignador se eliminará del almacén de contenido.

Agrupación de asignadores en carpetas de configuración

Las carpetas de configuración son útiles para organizar asignadores si la instalación incluye muchos de ellos. Puede agrupar asignadores de tal forma que pueda aplicar los mismos valores de configuración de una vez a todos los asignadores y servicios de la carpeta.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Acerca de esta tarea

Al añadir un asignador a una carpeta de configuración, hereda automáticamente los valores de configuración de la carpeta. Sin embargo, si ha cambiado anteriormente los valores predeterminados de ese asignador o servicio, se guardarán los valores cambiados.

Al cambiar los valores de configuración de un asignador o una carpeta de configuración, los servicios del asignador y las entradas hijo de la carpeta adquieren automáticamente los nuevos valores. Sin embargo, si cambia los valores de los servicios, se mantienen los valores cambiados.

Puede crear una nueva carpeta de configuración en la raíz del área de Configuración o en una carpeta de configuración existente.

Consejo:

- Para ver y editar las propiedades de configuración del elemento padre de una entrada mostrada en la ruta de la barra de herramientas, pulse el botón

Establecer propiedades - Configuración . Puede cambiar y aplicar valores de configuración a todos los asignadores y los servicios del área de Configuración cuando se encuentre en la raíz del área Configuración.

- Utilice la ruta de la barra de herramientas para explorar los distintos niveles de su configuración. La ruta se inicia con Configuración y, si se hace demasiado larga, se ajusta.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios**.
2. Pulse el botón Nueva carpeta.
3. Escriba un nombre y, si lo desea, una descripción, y especifique dónde guardar la carpeta de configuración.
4. Pulse **Finalizar**.

Ahora puede añadir asignadores a la carpeta de configuración cortándolos de su ubicación original y pegándolos en el interior de la carpeta. También puede cambiar los valores en el nivel de la carpeta de configuración.

Consejo: Para mover un asignador a otra carpeta, pulse **Más** junto al asignador y, a continuación, pulse **Mover**.

Direccionamiento avanzado de asignadores

Dependiendo de la configuración del sistema, es posible controlar el modo de distribuir los informes entre los servidores.

Por ejemplo, si hay distintos departamentos que mantienen sus propios servidores, o si hay servidores configurados para accesos a datos específicos, como servidores Microsoft Windows para bases de datos de Microsoft SQL Server y servidores Linux configurados para acceso a IBM Db2. Es posible configurar el software de IBM Cognos para que servidores específicos procesen las solicitudes de informes mediante la aplicación de reglas de direccionamiento.

Los valores de afinidad tienen prioridad sobre los valores de direccionamiento avanzado. Para obtener más información, consulte “Número máximo de procesos y conexiones” en la página 80.

Al definir las reglas de direccionamiento se debe seleccionar un grupo de servidores. Los nombres de grupos de servidores son una propiedad de un asignador o de las carpetas de configuración en las que se organizan los asignadores. Para obtener más información para establecer nombres de grupo de servidores, consulte “Establecer grupos de servidores para direccionamiento avanzado de asignadores” en la página 75.

Para determinar qué grupos de servidores procesan determinados informes, debe asociar los grupos de servidores a etiquetas de direccionamiento para objetos de datos, tales como paquetes, módulos de datos o archivos cargados y para los grupos o roles de usuario. A continuación, necesita especificar cómo se distribuyen las etiquetas de direccionamiento entre los asignadores de su entorno. La distribución se controla mediante las reglas de direccionamiento que crea para las etiquetas de direccionamiento. La solicitud de informe la procesará un servidor específico, en función de las etiquetas de direccionamiento asociadas al objeto de datos desde el que se ha creado el informe y/o el usuario o grupo que ejecuta el informe.

Consejo: Una etiqueta de direccionamiento puede ser cualquier palabra o frase, pero como método recomendado, especifique una etiqueta que sea descriptiva en su entorno. Puede tener etiquetas, como Informes de ventas, Datos de Db2, Europa.

Al crear las reglas de direccionamiento, se pueden crear condiciones que determinan los grupos de servidores mediante los cuales se van a procesar los informes. Por ejemplo, se pueden establecer reglas de direccionamiento de tal forma que los informes de un paquete de finanzas creados por un usuario del grupo de finanzas se procesen mediante los servidores de finanzas. También se pueden establecer reglas de direccionamiento, de modo que los informes creados por cualquier usuario de ventas, independientemente del objeto de datos utilizado para crear el informe, se procesen mediante los servidores de ventas. En el primer ejemplo, debe especificar etiquetas de direccionamiento para el grupo o rol y el paquete, pero en el segundo ejemplo solo debe especificar una etiqueta de direccionamiento para el grupo o rol y dejar en blanco la etiqueta de direccionamiento del paquete. No tiene que especificar una etiqueta de direccionamiento para el objeto de datos y el grupo o rol en las reglas de direccionamiento.

Debe disponer de los permisos necesarios para acceder a la función **IBM Cognos Administration**. Para obtener más información, consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Establecimiento de etiquetas de direccionamiento para objetos de datos

Las etiquetas de direccionamiento de objeto de datos se utilizan para configurar reglas de direccionamiento para los asignadores. Puede especificar etiquetas de direccionamiento para los siguientes objetos de datos: paquetes, módulos de datos y archivos cargados.

Procedimiento

1. En **Contenido del equipo** o **Mi contenido**, localice el paquete, módulo de datos o archivo descargado necesario y abra su panel de propiedades. En la pestaña **General**, expanda la sección de propiedades **Avanzado**.
2. En **Direccionamiento avanzado**, pulse **Establecer**.
3. Especifique las etiquetas de direccionamiento de este modo:
 - Seleccione el botón **Nuevo** para especificar una o varias etiquetas de direccionamiento nuevas.
 - Seleccione el botón **Seleccionar** para seleccionar entre las etiquetas de direccionamiento existentes.

Nota: Una etiqueta de direccionamiento puede ser cualquier palabra o frase, pero como método recomendado, especifique una etiqueta que sea descriptiva en su entorno. Puede tener etiquetas, como Informes de ventas, Datos de Db2, Europa.

Resultados

Las etiquetas de direccionamiento se utilizan cuando “Establecimiento de reglas de direccionamiento para asignadores” en la página 60.

Establecimiento de etiquetas de direccionamiento para grupos o roles

Puede establecer etiquetas de direccionamiento para grupos o roles. Las etiquetas de direccionamiento se utilizan para especificar reglas de direccionamiento para asignadores.

Procedimiento

1. En **Gestionar > Consola de administración**, abra **IBM Cognos Administration**.
2. En la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
3. Pulse el espacio de nombres **Cognos** para visualizar los grupos y roles.
4. Pulse el botón Establecer propiedades  para un grupo o rol.
5. En **Direccionamiento avanzado > Conjuntos de direccionamiento**, pulse **Establecer**.

Aparecerá la página **Asignar conjuntos de direccionamiento**.
6. Seleccione una etiqueta de direccionamiento para el rol o grupo de usuarios en **Conjuntos de direccionamiento disponibles**, o escríbala en **Introducir conjuntos de direccionamiento** y pulse el botón **Añadir** para añadir la etiqueta al recuadro **Conjuntos de direccionamiento asignados**. Cuando escribe varias etiquetas, separe cada etiqueta con un signo de punto y coma. Por ejemplo, Sales groups;Marketing;Development.

7. Repita el paso 5 para añadir otras palabras clave de direccionamiento que desee aplicar al paquete.
El orden en que se añaden las etiquetas de direccionamiento no importa.
8. Pulse **Aceptar**.
Las etiquetas de direccionamiento se muestran bajo **Direccionamiento avanzado** en la página de propiedades de grupo o rol.
9. En la página **Establecer propiedades**, pulse **Aceptar**.

Resultados

Las etiquetas de direccionamiento se utilizan cuando “Establecimiento de reglas de direccionamiento para asignadores”.

Establecimiento de reglas de direccionamiento para asignadores

Puede establecer reglas de direccionamiento para asignadores o carpetas de configuración.

Los grupos de servidores son una propiedad de los asignadores o las carpetas de configuración, y se deben configurar previamente para establecer las reglas de direccionamiento para grupos de servidores. Para obtener más información, consulte: “Establecer grupos de servidores para direccionamiento avanzado de asignadores” en la página 75.

Procedimiento

1. En **Gestionar > Consola de administración**, abra **IBM Cognos Administration**.
2. En la pestaña **Configuración**, pulse **Asignadores y servicios**.
Se muestran los asignadores y las carpetas de configuración que se han creado.

Consejo: Los grupos de servidores ya deben estar configurados. Para obtener más información, consulte: “Establecer grupos de servidores para direccionamiento avanzado de asignadores” en la página 75.

3. En la barra de herramientas, seleccione el botón Especificar reglas de direccionamiento .
Aparecerá la página **Especificar reglas de direccionamiento**.
4. Pulse **Agregar regla**.
5. Especifique las reglas de direccionamiento haciendo coincidir las etiquetas de direccionamiento con grupos de servidores. Una regla de direccionamiento puede ser una combinación de las etiquetas y grupos de servidores siguientes:
 - **Etiqueta de direccionamiento de datos y Grupo de servidores**
 - **Etiqueta de direccionamiento de grupos o Etiqueta de direccionamiento de roles y Grupo de servidores**
 - **Etiqueta de direccionamiento de datos y Etiqueta de direccionamiento de grupos o Etiqueta de direccionamiento de roles y Grupo de servidores**
6. En la columna **Acciones**, pulse el botón Ver los miembros para ver una descripción general de los miembros.
7. Para cambiar el orden de las reglas de direccionamiento, seleccione **Modificar la secuencia**. Seleccione la regla que desee mover y pulse **Arriba**, **Abajo**, **A la parte superior** o **A la parte inferior**.

Importante: A diferencia de las etiquetas de direccionamiento, el orden en el que se enumeran las reglas de direccionamiento influye en el modo en que se aplican.

Una regla se cumple cuando las propiedades asociadas con el objeto de datos o grupo o rol implicados en la solicitud cumplen con los criterios de la regla. Las reglas se evalúan en orden hasta que se cumple la primera y la solicitud se encamina al grupo de servidores nombrado por la primera regla que se haya cumplido.

8. Pulse **Aceptar**.

Especificación de correlaciones de pasarela para datos de PowerPlay de IBM Cognos Series 7

Puede especificar la ubicación de un servidor de PowerPlay de Series 7.

Los usuarios de IBM Cognos for Microsoft Office pueden enviar solicitudes al servicio de datos de informes (RDS) de datos que residan en un servidor PowerPlay de Series 7. El servicio de datos de informes (que funciona en el servidor de aplicaciones de IBM Cognos) se comunica con PowerPlay de Series 7 a través de la pasarela de PowerPlay Enterprise Server de Series 7.

Si la configuración de la red prohíbe el acceso del servidor de aplicaciones al servidor de nivel Web que alberga la pasarela de PowerPlay Enterprise Server de Series 7, se debe instalar una segunda pasarela interna de PowerPlay Enterprise Server de Series 7 en el nivel del servidor de aplicaciones. En este tipo de configuración, se puede especificar la ubicación del servidor PowerPlay de Series 7.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Datos de informes**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** de **reportDataService**, pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. En la columna **Valor**, pulse **Editar** para Correlaciones de pasarelas.
6. Pulse la casilla de verificación **Reemplazar los valores adquiridos de la entrada padre**.
7. Pulse **Agregar correlación**.
8. En **Pasarela de la aplicación (externa)**, escriba la dirección del servidor web.
9. En **Pasarela de la aplicación (interna)**, escriba la dirección del servidor PowerPlay Series 7.
10. Pulse **Aceptar**.

Cambio de nombre de asignadores

Como medida de seguridad, puede cambiar el nombre de los asignadores si no se desea revelar el nombre del sistema host, el número de puerto, el servlet o la ruta del asignador.

Para obtener más información, consulte: “Protección de asignadores” en la página 64.

Normalmente, los administradores del servidor pueden ver y cambiar el nombre de los asignadores.

Es recomendable que, al cambiar el nombre de un asignador, no se utilice ninguna información que revele el nombre o el puerto del sistema host, ni información de rutas o de otros sistemas. Sin embargo, es importante recordar dónde está instalado el asignador para tareas de supervisión.

Consejo: Si se cambia el nombre de un asignador y es necesario acceder a la información de host, puerto y ruta, se pueden utilizar los métodos de Software Development Kit para buscar esta información en la propiedad dispatcherPath del objeto Asignador.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Todos los asignadores**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** de un asignador, pulse **Establecer propiedades**.
4. En el cuadro **Nombre**, introduzca un nombre nuevo para el asignador.
Utilice un nombre significativo que le ayude a distinguir los asignadores. No revele información del sistema en el nombre.
5. Si lo desea, añada una sugerencia e información descriptiva.
6. Pulse **Aceptar**.

Prueba de los asignadores

Para evaluar el rendimiento del software de IBM Cognos, se puede probar el estado de los asignadores.

También se puede asegurar de que los asignadores están respondiendo y ver el tiempo de actividad, que es el tiempo en segundos durante el que los asignadores trabajan sin fallos.

Puede ver el estado de los asignadores y del servicio, y revisar mensajes de registro.

Antes de empezar

Al probar un asignador también se prueban los servicios que pertenecen a ese asignador.

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration** Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.

- Determine los asignadores que desea probar y, a continuación, siga las instrucciones de esta tabla. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse los elementos que desea visualizar.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

Tabla 20. Objetivos, vistas y acciones para probar los asignadores

Objetivo	Vista del panel Tabla de puntuación	Acción
Probar todos los asignadores del sistema	Todos los servidores	En el menú Acciones para grupos, pulse Probar . Consejo: Para aplicar una acción solamente a algunas entradas, seleccione las casillas de verificación de una o varias entradas y, a continuación, pulse la acción que desee.
Probar todos los asignadores para un grupo de servidores	Todos los servidores	En el menú Acciones para grupos, pulse Probar los asignadores .
Probar todos los asignadores para un servidor	Todos los servidores	Localice el servidor que desea probar. En el menú Acciones del servidor, pulse Probar .
Probar un asignador específico	Todos los asignadores	Localice el asignador que desea probar. En el menú Acciones del asignador, pulse Probar .

Aparecerá un cuadro de diálogo para confirmar la acción.

- Pulse **Aceptar**.

Si los asignadores no se comportan como se espera, puede ajustar el rendimiento del servidor mediante la modificación de sus valores de configuración. Para obtener más información, consulte “Ajuste del rendimiento de servidor” en la página 74.

Migración tras error para varios asignadores

En una instalación distribuida del software de IBM Cognos, puede configurar cada uno de los componentes de pasarela para que se comuniquen con más de un asignador con fines de migración tras error.

Los componentes de pasarela buscan sus asignadores asociados para asegurarse de que las solicitudes se enruten a los asignadores que estén en servicio y que respondan correctamente. Se puede establecer la frecuencia de ejecución de estas búsquedas.

Para obtener más información sobre la configuración de varios asignadores, consulte el tema “Configuración de sistemas pasarela” en *IBM Cognos Analytics Guía de instalación y configuración*.

Cómo establecer la frecuencia de las búsquedas de estado del asignador

Se puede especificar la frecuencia de búsqueda de los asignadores con el fin de determinar su estado actual para tareas de migración tras error.

Use los parámetros siguientes:

- **ConnectionCheckingSleepTime**

Especifica el intervalo en segundos entre búsquedas del estado de los asignadores.

El rango de valores válidos es de 1 a 2147483647. Los valores inferiores a 5 consumen demasiados recursos (tiempo de la CPU y ancho de banda de red). El valor predeterminado es 30.

- **ConnectionCheckingQuickSleepTime**

Especifica el intervalo en segundos entre búsquedas cuando no se encuentran asignadores operativos. El valor de este parámetro debe ser menor que **ConnectionCheckingSleepTime**.

El rango de valores válidos es de 1 a 2147483647. Los valores inferiores a 5 consumen demasiados recursos (tiempo de la CPU y ancho de banda de red). El valor predeterminado es 5.

Procedimiento

1. Copie el archivo *install_location/cgi-bin/cognoscgi.conf.sample* en *install_location/bin* y cambie el nombre por *cognoscgi.conf*.
2. Abra el archivo *cognoscgi.conf* en un editor que pueda guardar archivos en formato UTF-8.
3. Añada las siguientes líneas al archivo:
`ConnectionCheckingSleepTime=time in seconds`
`ConnectionCheckingQuickSleepTime=time in seconds`
4. Guarde el archivo *cognoscgi.conf* en formato UTF-8.

Protección de asignadores

Puede cambiar el nombre de asignador predeterminado para evitar riesgos de seguridad.

Los usuarios del software de IBM Cognos pueden introducir rutas de búsqueda de XPath en el campo de dirección de un navegador web, o en hiperenlaces. Los usuarios pueden introducir cualquier sintaxis de ruta de búsqueda contra parámetros de ruta de búsqueda en la interfaz de usuario. El software de IBM Cognos utiliza la lista de control de acceso (ACL) de Content Manager para comprobar los objetos que se devuelven al usuario.

En algunos casos, los usuarios malintencionados podrían ver el nombre del asignador. Esta práctica supone un riesgo para la seguridad, incluso a pesar de que los usuarios no pueden pulsar el nombre del asignador ni realizar acciones sobre él.

Para evitar este tipo de riesgos en la seguridad, cambie el nombre del asignador predeterminado. El nombre de asignador predeterminado es *nombre_sistema:9300* y se puede cambiar a *servidor1*, por ejemplo, para ocultar el número de puerto y el nombre de host. Para obtener más información, consulte “Cambio de nombre de asignadores” en la página 61.

Especificación de los asignadores para albergar el servidor proxy JMX

Los administradores pueden crear una lista de uno o más asignadores como candidatos para albergar el servidor proxy JMX (Java Management Extensions). Esto contribuye a reducir el número de subprocesos necesarios para recopilar las métricas JMX y aumenta el número de subprocesos que están disponibles para el gestor de contenidos.

El servidor proxy JMX se comunica con los asignadores y recopila sus métricas JMX. Esta comunicación requiere aproximadamente cuatro subprocesos por asignador. Una instalación distribuida con un elevado número de asignadores necesita un gran volumen de subprocesos, que afectan al rendimiento del gestor de contenidos. Para resolver este asunto y mejorar el rendimiento del gestor de contenidos, los administradores pueden elegir uno o más asignadores como candidatos para albergar el servidor proxy JMX (Java Management Extensions).

Elección de los asignadores

Puesto que IBM Cognos Administration utiliza el servicio de presentación y tiene conexión con el servidor proxy, puede elegir asignadores que ejecutan el servicio de presentación. Esto proporciona llamadas locales al servidor proxy.

Utilice IBM Cognos Administration para crear una lista de uno o más asignadores para albergar el servidor proxy JMX (Java Management Extensions). El asignador que se encuentra en la parte superior de la lista y que se está ejecutando es el asignador elegido para albergar el servidor proxy JMX.

Si no se ejecuta ninguno de los asignadores de la lista de preferidos, se elegirá un asignador disponible al azar para albergar el servidor proxy JMX. Tenga en cuenta que este es el comportamiento predeterminado si no crea una lista de asignadores.

Edición de asignadores de host de JMX

Utilice IBM Cognos Administration para añadir uno o más asignadores a la lista de asignadores candidatos para actuar como host para albergar el servidor proxy JMX (Java Management Extensions).

Procedimiento

1. Lance IBM Cognos Administration.
2. En la pestaña **Estado**, pulse **Sistema**.
3. En el panel **Tabla de puntuación**, pulse la flecha del menú Acciones correspondiente a la entrada **Sistema** y pulse **Establecer propiedades**.
4. En la página Establecer propiedades - Configuración, pulse la pestaña **Valores**.
5. Pulse **Editar** para definir los **Asignadores de host proxy JMX**. Aparece la página **Establecer asignadores de host proxy JMX**.
6. Pulse **Añadir** para añadir un asignador.
7. Seleccione los asignadores que desee añadir.
8. Pulse el botón de flecha a la derecha y, cuando aparezcan las entradas que desea en el cuadro **Entradas seleccionadas**, pulse **Aceptar**.
9. Pulse **Aceptar**.
10. Pulse **Arriba**, **Abajo**, **Al principio** o **Al final** para ordenar los asignadores.
11. Pulse **Aceptar**.

Resultados

El asignador que se encuentra en la parte superior de la lista y que se está ejecutando es el asignador elegido para ejecutar el servidor proxy JMX. Puede cambiar el orden de los asignadores en cualquier momento. Si no se ejecuta ninguno de los asignadores de esta lista, se elegirá un asignador disponible al azar para albergar el servidor proxy JMX.

Ubicaciones de Content Manager

La instalación puede incluir más de un Content Manager, cada uno en una ubicación distinta. Un sistema de Content Manager está activo y uno o varios componentes de Content Manager están en espera.

Asegúrese de que están sincronizados los relojes de cada sistema en el que esté instalado Content Manager. De no ser así, se pueden producir comportamientos extraños si ocurre una migración tras error. Por ejemplo, puede haber un retraso antes de que el estado de un servidor recién inhabilitado se actualice en IBM Cognos Administration. Para obtener más información sobre Content Manager, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Para obtener más información sobre el establecimiento de parámetros de Content Manager, consulte “Establecimiento de parámetros avanzados de Content Manager”.

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration** Capítulo 13, “Funciones y características protegidas”, en la página 227.

Establecimiento de parámetros avanzados de Content Manager

Es posible establecer parámetros avanzados de Content Manager.

Los parámetros avanzados de Content Manager incluyen valores para la agrupación de conexiones de base de datos, entradas ordenadas para entornos locales no ingleses, sincronización y examen de espacios de nombres externos.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Content Manager**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones de ContentManagerService**, pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. Pulse **Editar** junto a **Valores avanzados**.
6. Seleccione **Reemplazar los valores adquiridos de la entrada padre**.
7. En la columna **Parámetro**, introduzca el nombre del parámetro.
Por ejemplo, escriba `CM.DbConnectPoolCleanupPeriod`.
8. En la columna **Valor**, escriba el valor asociado a esta configuración.
9. Continúe escribiendo nombres y valores de parámetros según sea necesario.

10. Pulse **Aceptar**.

11. En la página **Establecer propiedades**, pulse **Aceptar**.

Administración de los valores de agrupación de conexiones de base de datos para Content Manager

Content Manager utiliza conexiones de base de datos para acceder al almacén de contenido. Puede cambiar los valores de la agrupación de conexiones para Content Manager con el fin de aumentar el rendimiento.

Gracias a las conexiones conjuntas, Content Manager no tiene que crear ni abrir conexiones para nuevas solicitudes. Esto proporciona tiempos de respuesta más rápidos. Sin embargo, como las conexiones conjuntas reservan recursos de la base de datos, las conexiones inactivas deben cerrarse si no se necesitan.

Se puede gestionar el número de conexiones con el almacén de contenido mediante la limitación del número máximo de conexiones y la especificación del tiempo que permanecen las conexiones en la agrupación antes de que se cierren automáticamente.

Están disponibles los parámetros siguientes:

- **CM.DbConnectPoolMax**

Especifica el número máximo de conexiones de base de datos simultáneas que permite el almacén de contenido.

Este parámetro sólo se aplica a los valores de agrupación de conexiones de Content Manager. Si hay otros servicios que accedan al mismo almacén de contenido, es posible que haya más conexiones de base de datos simultáneas que las especificadas en este parámetro.

Los valores válidos son -1, cualquier valor del rango entre 5 y 2147483647 o el valor de base de datos, el valor que sea menor. El valor predeterminado es -1 (ilimitado).

- **CM.DbConnectPoolTimeout**

Especifica el periodo de tiempo máximo en milisegundos que espera un subproceso a que esté disponible una conexión de la agrupación.

El rango de valores válidos es de -1 a 2147483627. Un valor de 0 especifica que los subprocesos nunca esperan una conexión si no hay una disponible inmediatamente. El valor predeterminado es -1 (ilimitado).

- **CM.DbConnectPoolIdleTime**

Especifica el periodo de tiempo mínimo en milisegundos que una conexión permanece inactiva en la agrupación. Este parámetro sólo se utiliza si el valor del parámetro DbConnectPoolCleanUpPeriod es positivo.

El rango de valores válidos es de -1 a 2147483647. Un valor de 0 o -1 especifica que las conexiones inactivas se cierran cuando Content Manager se reinicia. El valor predeterminado es 300.000 (5 minutos).

- **CM.DbConnectPoolCleanUp Period**

Especifica el periodo de tiempo en milisegundos entre invocaciones de un subproceso de limpieza que cierra aquellas conexiones inactivas en la agrupación que superan el valor de DbConnectPoolIdleTime.

El rango de valores válidos es de -1 a 2147483647. El valor predeterminado es 300.000 (5 minutos).

Cómo ordenar entradas para entornos locales no ingleses

Puede corregir los problemas de ordenación en entornos locales no ingleses para un almacén de contenido Oracle o Microsoft SQL.

Para corregir un problema de ordenación, utilice el parámetro CM.SortCollation. Por ejemplo, para ordenar las entradas de una base de datos Oracle mediante una ordenación fonética china, se puede establecer el parámetro CM.SortCollation en SCHINESE_PINYIN_M.

Para obtener más información sobre las ordenaciones soportadas, consulte la documentación de Oracle y de SQL Server. La configuración del valor CM.SortCollation no tiene ningún efecto en los administradores de contenido que se ejecutan en las bases de datos Sybase o IBM Db2.

Administración de la sincronización de Content Manager

Si una instalación incluye sistemas con Content Manager en espera, se pueden configurar los parámetros que especifiquen las actividades de espera de Content Manager.

Se puede especificar la frecuencia de las comprobaciones para asegurarse de que el asignador activo no haya fallado, el tiempo que se tarda en determinar que Content Manager está activo cuando se produce una migración tras error y al inicio, la frecuencia de envío de una respuesta por parte de un Content Manager cuando está ocupado y cuánto tiempo puede durar una interrupción de red breve sin que se produzca una migración tras error.

Están disponibles los parámetros siguientes:

- **CM.CMSync_NegotiationTime**
Especifica el periodo de tiempo en milisegundos necesario para determinar el Content Manager activo cuando se produce una migración tras error.
El rango de valores válidos es de 1 a 9223372036854775807. El valor predeterminado es 2000.
- **CM.CMSync_NegotiationTimeForStartUp**
Especifica el periodo de tiempo en milisegundos necesario para determinar el Content Manager activo al inicio.
El rango de valores válidos es de 1 a 9223372036854775807. El valor predeterminado es 60000.
- **CM.CMSync_CheckActive Time**
Especifica el periodo de tiempo en milisegundos necesario para que un Content Manager activo pase a estado en espera cuando otro Content Manager se active.
El valor predeterminado es 10000.
- **CM.CMSync_PingTimeout**
Especifica el periodo de tiempo en milisegundos necesario para que un Content Manager envíe una respuesta si está en ejecución.
El rango de valores válidos es de 1 a 9223372036854775807. El valor predeterminado es 120000.
- **CM.CMSync_ShortNetworkInterruptionTime**
Especifica el periodo de tiempo en milisegundos que puede durar una interrupción de red breve sin que se produzca una migración tras error.
El rango de valores válidos es de 1 a 9223372036854775807. El valor predeterminado es 3000.

Control de examen de espacios de nombres externos

Puede controlar si los usuarios pueden examinar espacios de nombres externos.

Cuando el parámetro `CM.SecurityQueryRequiresRead` está establecido en `true`, el Content Manager impide el examen de espacios de nombres externos si la política de espacios de nombres externos se ha actualizado para denegar permisos de lectura a usuarios o grupos. Este valor controla si el Content Manager fuerza un filtro de permiso de lectura para resultados de consultas de espacios de nombres externos. El valor predeterminado es `false`.

Establecimiento del límite de tamaño de caché para el caché de Content Manager

Puede especificar el límite superior del tamaño de la memoria caché como porcentaje del tamaño de montón de JVM.

El valor predeterminado es 10%. Los valores válidos van del 0 al 100. El incremento del tamaño de la memoria caché puede reducir la carga en Content Manager, lo que permite que éste dé servicio a más nodos distribuidos. Sin embargo, si este valor es demasiado alto, pueden aparecer errores de memoria agotada en el asignador.

Si se asigna el valor 0 (cero), se inhabilita la memoria caché en todo el sistema, con lo que todas las solicitudes de consulta se enviarán directamente a Content Manager, lo cual puede reducir el rendimiento del sistema. Sin embargo, esto es útil para comparar el rendimiento con y sin la memoria caché.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Memoria caché de Content Manager**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** de **ContentManagerCacheService**, pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. En la columna **Valor**, cambie el número de **Límite de montón para el servicio de memoria caché de Content Manager**.
6. Escriba el valor que desea y pulse **Aceptar**.

Reducción de la carga de Content Manager almacenando los archivos de sesión de usuario localmente

Puede cambiar la ubicación en la que se almacenan los archivos de sesión de usuario.

Cuando un usuario ejecuta un informe interactivo, el servidor de informes envía una solicitud a Content Manager en la que se solicita almacenar la salida de informe en la memoria caché de la sesión del usuario. La salida de informe puede tener uno de los formatos siguientes: PDF, HTML con imágenes, software de hoja de cálculo Microsoft Excel, CSV o XML.

Para reducir la carga de procesamiento en Content Manager, los archivos de sesión de usuario se almacenan en el sistema de archivos local del servidor de informes. De forma predeterminada, esta ubicación se encuentra en el servidor de informes. Puede cambiar la ubicación a un sistema remoto, como un directorio compartido en el sistema operativo Microsoft Windows o un directorio común montado en el

sistema operativo UNIX. Para obtener más información, consulte el tema sobre el cambio de la ubicación de la salida de informe temporal en la *IBM Cognos Analytics* Guía de instalación y configuración.

Si está realizando una actualización, los archivos de sesión de usuario se almacenan en Content Manager. Deberá cambiar el sistema de archivos local del servidor de informes si desea reducir la carga de Content Manager.

El almacenamiento de archivos temporales puede aumentar el uso de disco. Asegúrese de asignar suficiente espacio para los archivos.

Esto no interferirá con las versiones anteriores de las aplicaciones, como Software Development Kit, que sigue enviando solicitudes a Content Manager.

Están disponibles los parámetros siguientes:

- **Ubicación de objetos temporales**

Especifica la ubicación de los archivos de memoria caché temporales. Para almacenar los archivos de memoria caché temporales en el servidor de informes, seleccione **Sistema de archivos del servidor**. Para almacenar los archivos de memoria caché temporales en Content Manager, seleccione **Almacén de contenido**.

El valor predeterminado es **Sistema de archivos del servidor**.

- **Duración de los objetos temporales**

Especifica la cantidad de tiempo, en horas, que se conservarán los archivos de memoria caché temporales. Si establece este valor en cero, los archivos se conservarán hasta que se supriman manualmente.

Este valor solamente lo utiliza el asignador. El servidor de informes suprime los archivos de memoria caché temporales cuando el navegador se cierra o cuando el usuario pulsa el botón Atrás del navegador. Si el servidor de informes no suprime los archivos, el asignador utiliza este valor para suprimir los archivos.

El valor predeterminado es 4 horas.

También existe un valor en Cognos Configuration para cifrar archivos temporales, que no se ve afectado por los valores de **Duración de los objetos temporales** o **Ubicación de objetos temporales**. Para obtener más información, consulte *IBM Cognos Analytics* Guía de instalación y configuración.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios**.
2. Pulse el botón **Establecer propiedades - Configuración**  y pulse **Valores**.
3. En el menú **Categoría**, pulse **Ajuste**.
4. Cambie los valores de **Ubicación de objetos temporales** y **Duración de los objetos temporales** según convenga.
5. Pulse **Aceptar**.

Anular el procesamiento local predeterminado en el caché de solicitud

Puede reemplazar el procesamiento de entorno local en la memoria caché de solicitud para todos los informes.

Esto se puede hacer utilizando el valor avanzado `RSVP.PROMPTCACHE.LOCALE`. Cuando este valor se configura, el entorno local especificado se utiliza en lugar del entorno local especificado en el informe cada vez que se crea, actualiza o utilizan datos de caché de solicitud. Esto significa que se utiliza una única memoria caché de solicitud para cada informe independientemente del entorno local del usuario del informe.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para **ReportService**, en la columna **Parámetro**, escriba **RSVP.PROMPTCACHE.LOCALE**.
3. En la columna **Valor**, escriba el valor asociado para el parámetro y haga clic en **Aceptar**.

Tareas de mantenimiento del almacén de contenido

Se pueden crear tareas de mantenimiento de contenidos y ejecutarlas a petición, a la hora planificada o según un activador.

Por ejemplo, una renovación de la base de datos o un correo electrónico. Se pueden planificar las tareas de mantenimiento de contenido como parte de un trabajo o como parte de un agente. También puede ver el historial de ejecución de tareas de mantenimiento de contenido .

Se pueden buscar y corregir inconsistencias dentro del almacén de contenido o entre el almacén de contenido y los espacios de nombres externos.

Las tareas de mantenimiento de contenido pueden comprobar inconsistencias en el almacén de contenido debidas a datos que faltan o están obsoletos, o entre el almacén de contenido y los espacios de nombres externos.

En caso necesario, también puede iniciar y detener tareas que se ejecutan en segundo plano en el almacén de contenido.

Para obtener información acerca del uso de las tareas de mantenimiento del almacén de contenido en un entorno de arrendatarios múltiples, consulte “Crear y ejecutar una verificación de consistencia del almacén de contenidos” en la página 353.

Antes de iniciar el mantenimiento interno del almacén de contenido

Para garantizar que no se pierdan los datos que desee conservar, debe elegir, en primer lugar, el modo de búsqueda y comprobar los resultados antes de corregir el almacén de contenido.

Si faltan datos en el almacén de contenido pueden producirse errores en las actualizaciones. Los datos obsoletos pueden impedir la creación de nuevos objetos. Cuando una tarea de mantenimiento corrige el almacén de contenido, añade valores predeterminados para los datos que faltan que se pueden actualizar más adelante. También suprime permanentemente los datos obsoletos.

Cuando se buscan y se corrigen los datos, el almacén de contenido no se corrige mientras la tarea de mantenimiento de contenido se está ejecutando. En lugar de eso, Content Manager corrige las inconsistencias del almacén de contenido la próxima vez que se inicia.

Importante: Tras ejecutar una tarea de mantenimiento de contenido para buscar y corregir el almacén de contenido, haga una copia de seguridad del almacén de contenido antes de reiniciar Content Manager.

Se recomienda realizar comprobaciones de mantenimiento internas con regularidad, pero sobre todo antes de realizar una actualización para garantizar la consistencia de los almacenes de contenido.

Mantenimiento del almacén de contenido en espacios de nombres externos

Puede utilizar IBM Cognos Administration para el mantenimiento del almacén de contenido en los espacios de nombres externos.

Al suprimir usuarios del proveedor de autenticación, la información de la cuenta del usuario permanece en el almacén de contenido. Se puede utilizar IBM Cognos Administration para encontrar la información de usuario que aún exista en el almacén de contenido y corregir el almacén de contenido suprimiendo los usuarios que no existan en los espacios de nombres externos. También puede suprimir perfiles de usuarios individuales de los almacenes de contenido.

Si desea ejecutar una tarea de mantenimiento de contenido en más de un espacio de nombres, realice una de las siguientes acciones:

- Si desea ejecutarla ahora, sólo tiene que iniciar sesión en los espacios de nombres y crear la tarea de mantenimiento de contenido.
- Si desea planificarla para que se ejecute más adelante o forma periódica, tenga en cuenta que una tarea planificada de mantenimiento de contenido funciona con los espacios de nombres que seleccione al crear esta tarea. Antes de planificar una tarea de mantenimiento de contenido, asegúrese de que sus credenciales contengan información de inicio de sesión de cada espacio de nombres mediante la renovación de las credenciales después de iniciar sesión en cada espacio de nombres que seleccione para ejecutar la tarea de mantenimiento de contenido.

Sugerencia: Pulse **Opciones de Mi área**, **Mis preferencias**, en la pestaña **Personal** y, a continuación, en **Renovar las credenciales**.

Debe tener permisos de acceso en cada espacio de nombres externo seleccionado y permisos de lectura en todas las cuentas de usuario de cada espacio de nombres externo. Si no tiene permisos de lectura en una cuenta de usuario, se asume que el usuario se ha suprimido del espacio de nombres. Al ejecutar un trabajo de mantenimiento de contenido, la información del usuario del almacén de contenido se muestra como inconsistente (para **Buscar**) o suprimida automáticamente (para **Buscar y corregir**).

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration**. Para obtener más información, consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Creación de una tarea de mantenimiento del almacén de contenido

Puede crear una tarea de mantenimiento del almacén de contenido.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Administración de contenidos**.
2. Pulse la flecha del botón Mantenimiento de nuevo contenido  de la barra de herramientas y, a continuación, en **Nueva comprobación de consistencia**.
3. Introduzca un nombre y, si lo desea, una descripción y una sugerencia, y pulse **Siguiente**.
4. Elija la comprobación de consistencia que desee:
 - Para comprobar las incoherencias del almacén de contenido, pulse **Referencias internas**.
 - Para ejecutar el mantenimiento de contenido en espacios de nombres, pulse **Referencias a espacios de nombres externos** y seleccione los espacios de nombres que desee.
5. Pulse **Siguiente**.
6. Elija la acción que desee:
 - Para ejecutar la tarea ahora o más adelante, pulse **Guardar y ejecutar una vez** y en **Finalizar**. Especifique la hora y la fecha de la ejecución. Pulse **Buscar** o en **Buscar y corregir** y, a continuación, en **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - Para planificar la ejecución de la tarea de forma periódica, pulse **Guardar y planificar** y a continuación en **Finalizar**. A continuación, seleccione la frecuencia y las fechas de comienzo y de final. Pulse **Buscar** o en **Buscar y corregir** y, a continuación, en **Aceptar**.

Consejo: Para inhabilitar temporalmente la planificación, seleccione la casilla de verificación **Inhabilitar la planificación**. Para visualizar el estado de la planificación, consulte “Gestión de actividades planificadas” en la página 269.

- Para guardar la tarea sin planificar o ejecutar, pulse **Sólo guardar** y en **Finalizar**.

Ejecución de una tarea de mantenimiento del almacén de contenido

Puede ejecutar una tarea de mantenimiento del almacén de contenido.

Procedimiento

1. En la pestaña **Configuración**, pulse **Administración de contenidos**.
2. Pulse **Ejecutar con opciones** junto a la tarea de mantenimiento de contenido.
3. Active la casilla de verificación **Ahora** para ejecutar inmediatamente la tarea de mantenimiento de contenido o la casilla de verificación **Más adelante** para definir una fecha y una hora.
4. Pulse **Buscar** o en **Buscar y corregir**.
5. Pulse **Ejecutar**.

Inicio y detención de actividades en segundo plano

Puede iniciar y detener las actividades en segundo plano que se están ejecutando en el Gestor de contenidos.

Acerca de esta tarea

Detener las actividades en segundo plano disminuye la carga de procesamiento en el Gestor de contenidos, permitiendo que aumente el rendimiento. Puede iniciar las actividades en segundo plano después de que el Gestor de contenidos completa el trabajo que requería de un volumen mayor de recursos.

Procedimiento

1. Lance IBM Cognos Administration.
2. En la pestaña **Estado**, pulse **Sistema**.
3. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Content Manager**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

4. Pulse la flecha para ver el menú Acciones situado junto al servicio de Content Manager y luego pulse **Iniciar actividades en segundo plano** o **Detener actividades en segundo plano**.

Ajuste del rendimiento de servidor

Debe incluir el ajuste del rendimiento como parte habitual de la administración de servidores.

Al ajustar los valores de configuración de los asignadores y los servicios, se puede optimizar la velocidad y la eficacia del software de IBM Cognos. Para los usuarios, un rendimiento óptimo implica que sus informes se ejecuten con más rapidez y sin errores. Para usted, implica que el software de IBM Cognos es estable y que los usuarios están satisfechos.

Normalmente, desea ajustar los servidores para satisfacer la demanda de los usuarios en los momentos de máxima utilización.

Es posible que tenga que añadir asignadores a la instalación para satisfacer las necesidades de los usuarios. O bien, puede que tenga que distribuir la instalación o actualizar el sistema en el que está instalado el software de IBM Cognos. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

El nivel de registro "Establecimiento de niveles de registro" en la página 21 puede afectar al rendimiento. Cuando el software de IBM Cognos registra más detalles, se asignan más recursos al registro y hay menos recursos disponibles para ejecutar informes.

Antes de cambiar cualquier valor, asegúrese de comprobar los asignadores y de revisar los mensajes de registro pertinentes "Mensajes de registro" en la página 18. Para obtener más información sobre cómo probar los asignadores, consulte "Prueba de los asignadores" en la página 62. También debe conocer los requisitos de rendimiento.

Modelos

Asegúrese de que sus modelos estén optimizados para la creación de informes. Para obtener más información, consulte la publicación *IBM Cognos Framework Manager Guía del usuario*.

Sistemas operativos

El rendimiento del software de IBM Cognos está estrechamente relacionado con el rendimiento del sistema operativo del sistema en el que está instalado el software de IBM Cognos. Por lo tanto, asegúrese de que el sistema operativo esté ajustado.

Establecer grupos de servidores para direccionamiento avanzado de asignadores

Si desea definir reglas de direccionamiento para informes, debe establecer grupos de servidores para los asignadores o las carpetas de configuración a los que desee que se direccionen los informes.

Para obtener información sobre cómo definir reglas de direccionamiento, consulte “Direccionamiento avanzado de asignadores” en la página 58.

Consejo: Si está configurando el direccionamiento del asignador avanzado mediante PowerPlay, debe asegurarse de que el grupo de servidores incluya al menos un servidor PowerPlay para gestionar las solicitudes de PowerPlay.

Procedimiento

1. En **Gestionar > Consola de administración**, abra **IBM Cognos Administration**.
2. En la pestaña **Estado**, pulse **Sistema**.
3. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Todos los asignadores**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

4. En el menú **Acciones** del asignador, pulse **Establecer propiedades**.
5. Pulse la pestaña **Valores**.
6. Seleccione **Ajuste** en la lista **Categoría**.
7. Escriba un nombre en la columna **Valor** para la propiedad **Grupo de servidores**.

Importante: El nombre puede contener un máximo de 40 caracteres.

8. Pulse **Aceptar**.

Puede utilizar este grupo de servidores cuando define reglas de direccionamiento, como se describe en el tema “Establecimiento de reglas de direccionamiento para asignadores” en la página 60.

Equilibrado de las solicitudes entre los asignadores

Si su instalación incluye más de un asignador, puede especificar la proporción de solicitudes que cada asignador gestiona mediante la modificación de su capacidad de procesamiento.

Esto se conoce habitualmente como equilibrio de carga. Normalmente la capacidad de un asignador se ajusta en función de la velocidad de la CPU del sistema en el que está instalado.

Por ejemplo, se instala un primer asignador en un sistema a 2 GHz y un segundo asignador en un sistema a 1 GHz. Se establece la capacidad de procesamiento del primer asignador en 2.0 y la del segundo en 1.0. El primer asignador gestiona dos tercios de las solicitudes mientras que el segundo gestiona un tercio de las solicitudes. Si establece la capacidad de ambos asignadores en 1.0, las solicitudes se envían alternativamente a cada asignador.

La capacidad de procesamiento predeterminada de cada asignador es de 1.0.

Los valores de afinidad tienen prioridad sobre los valores de solicitud de equilibrio. Para obtener más información, consulte “Número máximo de procesos y conexiones” en la página 80.

También puede controlar el equilibrio de carga de los asignadores mediante el establecimiento del factor de solicitudes en curso. Consulte “Equilibrio de la carga de los asignadores con factor de solicitudes en curso”. También puede desactivar el formato de ronda recíproca ponderada en el asignador. Consulte “Establecimiento de la propiedad de equilibrio de la carga de los asignadores en el modo compatible con clúster” en la página 78.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. Pulse la flecha del menú Acciones situada junto a **Sistema** y pulse **Establecer propiedades**.
3. Pulse la pestaña **Valores**.
4. Seleccione **Ajuste** en la lista **Categoría**.
5. En la columna **Valor**, escriba el nuevo valor de **Capacidad de procesamiento** y, a continuación, pulse **Aceptar**.

El nuevo valor surte efecto de forma inmediata.

Equilibrio de la carga de los asignadores con factor de solicitudes en curso

Puede establecer el factor de solicitudes en curso para proporcionar información al algoritmo de ronda recíproca, que indicará a éste cómo está funcionando el asignador.

El formato de ronda recíproca ponderada del equilibrio de carga trata todas las solicitudes como iguales, y todos los asignadores como igualmente capaces de manejar el número de solicitudes que reciben. Sin embargo, las diferentes solicitudes requieren más o menos potencia de procesamiento. Los asignadores también se ejecutan en servidores diferentes, con distintas capacidades de procesamiento. Por ejemplo, si un asignador sufre una demora porque se ejecuta en un servidor más lento o porque recibe muchas solicitudes que requieren mucha potencia de procesamiento, el formato de ronda recíproca sigue tratando todos los

asignadores de la misma manera. Los asignadores que sufran demoras tendrán más solicitudes en curso en sus colas. El algoritmo de ronda recíproca puede utilizar esta información para evitar el envío de nuevas solicitudes a esos asignadores hasta que dejen de estar sobrecargados.

El valor avanzado `inProgressRequestFactor` controla cuánta información se envía al algoritmo de ronda recíproca. Cuanto más alto sea el valor, menos probable será que se utilice un nodo con más solicitudes en curso. Nuestra investigación muestra que la cantidad de información ideal es el valor predeterminado 2,0. Para utilizar un formato simple de ronda recíproca, debe establecerlo en 0,0 a nivel de sistema.

Puede establecer el valor en el nivel de sistema o en el nivel de servicio. Se utiliza el valor del nivel de sistema como valor predeterminado para todos los servicios. Los valores de servicio tienen prioridad sobre el valor del nivel del sistema.

También puede controlar el equilibrio de la carga de los asignadores mediante el establecimiento de la capacidad de procesamiento. Consulte “Equilibrado de las solicitudes entre los asignadores” en la página 75. También puede desactivar el formato de ronda recíproca ponderada en el asignador. Consulte “Establecimiento de la propiedad de equilibrio de la carga de los asignadores en el modo compatible con clúster” en la página 78. Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Establecimiento de la propiedad del factor de solicitud en progreso en todo el sistema

Puede especificar la propiedad del factor de solicitud en progreso para todos los servicios.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados globalmente” en la página 513.
2. En la columna **Parámetro**, escriba **`DISP.default.inProgressRequestFactor`**.
3. En la columna **Valor**, escriba el valor que se utilizará como valor predeterminado para todos los servicios. Para obtener información acerca de los valores que se pueden especificar, consulte “Equilibrio de la carga de los asignadores con factor de solicitudes en curso” en la página 76.
4. Pulse **Aceptar**.

El nuevo valor se aplica inmediatamente.

Establezca la propiedad Factor de solicitud en progreso para un servicio específico

Puede especificar la propiedad de factor de solicitud en progreso para un servicio específico.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para el servicio que desea configurar, en la columna **Parámetro**, escriba **`DISP.service_name.inProgressRequestFactor`**, donde `service_name` es el nombre del servicio.

Por ejemplo, para el servicio de informes, escriba **`DISP.reportService.inProgressRequestFactor`**.

3. En la columna **Valor**, escriba el valor asociado que se utilizará como predeterminado para el servicio. Para obtener información acerca de los valores que se pueden especificar, consulte “Equilibrio de la carga de los asignadores con factor de solicitudes en curso” en la página 76.
4. Pulse **Aceptar**.
El nuevo valor se aplica inmediatamente.

Establecimiento de la propiedad de equilibrio de la carga de los asignadores en el modo compatible con clúster

Si los servidores IBM Cognos funcionan dentro de una infraestructura de equilibrio de carga, podrá desactivar el formato de ronda recíproca ponderada de equilibrio de carga para el asignador.

Si no establece este parámetro, el equilibrio de carga se puede duplicar por el clúster y el software de IBM Cognos, lo que puede reducir el rendimiento.

Se puede establecer una propiedad del asignador llamada `loadBalancingMode` en `weightedRoundRobin` o `clusterCompatible`.

En el modo `weightedRoundRobin`, el asignador realiza solicitudes en forma de ronda ponderada, según los valores de configuración del asignador. Para obtener más información, consulte “Equilibrado de las solicitudes entre los asignadores” en la página 75. Éste es el modo predeterminado.

En modo `clusterCompatible`, las solicitudes que no son de afinidad se procesan localmente si es posible. Si no hay ningún servicio en el asignador local, la solicitud falla. Esto garantiza que el software de IBM Cognos respete los equilibrios de carga realizados por la propia infraestructura de equilibrio de carga.

Se puede establecer la propiedad `loadBalancingMode` para asignadores individuales o para un grupo de asignadores en una carpeta de configuración. Para obtener más información, consulte “Agrupación de asignadores en carpetas de configuración” en la página 57. Como es una propiedad heredada, se pueden mover asignadores a una carpeta de configuración y establecer la propiedad `loadBalancingMode` para la carpeta con el objetivo de establecer rápidamente la propiedad para un grupo de asignadores.

También puede controlar el equilibrio de carga de los asignadores mediante el establecimiento del factor de solicitudes en curso (consulte “Equilibrio de la carga de los asignadores con factor de solicitudes en curso” en la página 76) o mediante el establecimiento de la capacidad de procesamiento (consulte “Equilibrado de las solicitudes entre los asignadores” en la página 75).

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. Pulse la flecha del menú Acciones situada junto a **Sistema** y pulse **Establecer propiedades**.

Consejo: También puede cambiar el valor del equilibrio de carga en el nivel del asignador.

3. Pulse la pestaña **Valores**.
4. Seleccione **Ajuste** en la lista **Categoría**.
5. En la columna **Valor**, seleccione el valor del **Modo de equilibrio de carga**, que puede ser Ronda recíproca ponderada o Compatible con clúster y, a continuación, pulse **Aceptar**.

El nuevo valor surte efecto de forma inmediata.

Establecimiento de periodos de máxima actividad de uso

Puede especificar las horas de inicio y de fin del periodo de demanda máxima de la organización.

La mayoría de las organizaciones tienen un periodo de demanda máxima. Este periodo suele ser normalmente durante las horas de oficina, cuando los empleados están trabajando y ejecutan informes interactivos.

Durante ese periodo de máxima actividad, es posible que desee establecer un número de conexiones y procesos suficientemente bajo como para que los trabajos se puedan ejecutar con más rapidez y los recursos del sistema puedan procesar solicitudes interactivas de los usuarios. Para obtener más información, consulte “Número máximo de procesos y conexiones” en la página 80. Durante el periodo que no es de máxima actividad, se puede establecer un número de conexiones y procesos más alto porque la demanda del sistema es menor.

El periodo predeterminado de máxima actividad es de 07:00 a 18:00. El número predeterminado de conexiones para cada servicio durante el periodo de máxima actividad y durante el periodo que no es de demanda máxima es de cuatro.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Todos los asignadores**.

Consejo: En el panel **Tabla de puntuación**, la vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** del asignador, pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. Seleccione **Ajuste** en la lista **Categoría**.
6. En la columna **Valor**, escriba los nuevos valores de las configuraciones siguientes:
 - **Hora de inicio del periodo de máxima actividad**
 - **Hora de inicio del periodo que no es de máxima actividad**

Consejo: Si desea restablecer un valor de configuración a su valor predeterminado, seleccione su casilla de verificación y pulse **Restablecer valor predeterminado**.

7. Pulse **Aceptar**.

Número máximo de procesos y conexiones

Puede establecer el número máximo de procesos y conexiones.

Para el servicio de informes y el servicio de informes por lotes, se puede establecer el número máximo de procesos y el número máximo de conexiones de alta y baja afinidad que el asignador puede abrir para gestionar solicitudes. Para los servicios de agente, Content Manager, entrega, trabajo y datos de informes, se puede establecer el número máximo de conexiones.

Hay valores distintos para horas de demanda máxima y horas que no son de demanda máxima. Para obtener más información, consulte “Establecimiento de periodos de máxima actividad de uso” en la página 79.

Número máximo de conexiones

Hay un máximo de uno de cada uno de estos servicios por asignador: agente, Content Manager, entrega, trabajo, datos de informes. Las conexiones gestionan una solicitud de un servicio cada vez.

Se puede especificar el número máximo de conexiones para cada servicio durante periodos de máxima actividad y periodos que no son de demanda máxima con los valores siguientes:

- **Conexiones máximas para el servicio <nombre_servicio> durante el periodo que no es de máxima actividad**
- **Conexiones máximas para el servicio de <nombre_servicio> durante el periodo de máxima actividad**

El número predeterminado de conexiones es de cuatro.

Número máximo de procesos

En cada asignador puede haber varios servicios de informes y servicios de informes por lotes. Se puede especificar el número máximo de procesos durante los periodos de máxima actividad utilizando los valores siguientes:

- **Número máximo de procesos para el <nombre_servicio> durante el periodo de máxima actividad**
- **Número máximo de procesos para <service_name> durante el periodo no pico**

El número predeterminado de procesos para cada servicio es de dos.

Conexiones de afinidad

Los servidores de informes aceptan conexiones de baja y alta afinidad para solicitudes de proceso de los servicios de informes y de informes por lotes.

Las solicitudes de baja afinidad se pueden gestionar mediante cualquier servidor de informes. Normalmente, las solicitudes de baja afinidad se utilizan cuando se solicita inicialmente la ejecución de un informe.

Las solicitudes de alta afinidad se deben gestionar mediante un servidor de informes específico. Lo habitual es que las solicitudes de alta afinidad sean de informes que ya se solicitaron, y pueden incluir acciones, como ir a la página siguiente de un informe. Si el servidor de informes específico no está disponible o está ocupado, el informe se volverá a ejecutar (solicitud de baja afinidad) en cualquier servidor de informes y la página siguiente (solicitud de alta afinidad) se dirigirá a ese servidor.

Los valores de afinidad tienen prioridad sobre los valores de solicitud de equilibrio y los valores de direccionamiento avanzado. Para obtener más información, consulte: “Equilibrado de las solicitudes entre los asignadores” en la página 75 y “Direccionamiento avanzado de asignadores” en la página 58.

Si los valores de afinidad cambian para un servicio mientras se están ejecutando las entradas, el número de procesos del servidor se podría duplicar. El número de procesos puede exceder temporalmente el valor máx. mientras surte efecto el cambio. Esto puede provocar problemas si el sistema no tiene suficiente memoria para el periodo provisional.

Puede especificar el número de conexiones de baja y alta afinidad para el servicio de informes y el servicio de informes por lotes utilizando el valor siguiente:

Número de conexiones de <baja | alta> afinidad para <nombre_servicio> durante un periodo que no es de alta actividad

Nota: Aunque la descripción de este valor implica que se aplica únicamente a periodos que no son de alta actividad, se aplica a periodos de alta actividad y a periodos que no son de alta actividad.

Para el servicio de informes por lotes, el número predeterminado de conexiones de baja afinidad es de dos. Para el servicio de informes, el número predeterminado de conexiones de baja afinidad es de cuatro. El número predeterminado de conexiones de alta afinidad para todos los servicios es de uno.

Establecimiento del número máximo de procesos y conexiones

Puede establecer el número máximo de procesos y conexiones.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios** y después pulse el servicio que desea.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** del servicio, pulse **Establecer propiedades**.

Consejo: Para el servicio de informes y el servicio de informes por lotes, también puede establecer algunos valores en el nivel del sistema o del asignador.

4. Pulse la pestaña **Valores**.
5. Seleccione **Ajuste** en la lista **Categoría**.
6. En la columna **Valor**, escriba valores nuevos para los procesos y las conexiones que desee cambiar.

Consejo: Si desea restablecer un valor de configuración a su valor predeterminado, seleccione su casilla de verificación y pulse **Restablecer valor padre**.

7. Pulse **Aceptar**.

Cómo especificar límites de tiempo en cola

Se puede especificar el número máximo de segundos que las solicitudes interactivas realizadas por los usuarios esperan en la cola una conexión del servicio de informes disponible.

Si una solicitud no se puede procesar dentro del límite de tiempo, la solicitud fallará y los usuarios recibirán un mensaje de error. Si el sistema operativo tiene los recursos adecuados y el software de IBM Cognos está configurado correctamente, las solicitudes no superarán el límite de tiempo.

Al especificar un límite de tiempo, hay que considerar el número máximo de segundos que se desea que los usuarios esperen una respuesta. El límite predeterminado de tiempo en cola es de 240 segundos.

Las solicitudes de servicio de informes por lotes permanecen en la cola de forma indefinida.

Si hay una carga de usuarios elevada (más de 165 usuarios) y los informes interactivos están funcionando continuamente en una instalación distribuida, se puede aumentar el límite de tiempo en cola a 360 para no recibir mensajes de error. También se puede aumentar el valor de tiempo de espera asíncrono para no recibir mensajes de error. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En la pestaña **Estado**, pulse **Sistema**.
2. Pulse la flecha del menú Acciones situada junto a **Sistema** y pulse **Establecer propiedades**.

Sugerencia: También puede cambiar los valores del límite de tiempo en cola en el nivel del servicio o del asignador.

3. Pulse la pestaña **Valores**.
4. Seleccione **Ajuste** en la lista **Categoría**.
5. En la columna **Valor**, escriba un nuevo valor de configuración del **Límite de tiempo del servicio de informes en la cola (segundos)**.

Sugerencia: Si desea restablecer un valor de configuración a su valor predeterminado, seleccione su casilla de verificación y pulse **Restablecer valor predeterminado**.

6. Pulse **Aceptar**.

Valores de archivos PDF

Hay cuatro valores de configuración para archivos PDF que determinan juntos la velocidad a la que se crean los archivos PDF y el tamaño de dichos archivos.

Los valores ideales son diferentes para cada entorno. Por ejemplo, si crea archivos PDF como parte de trabajos por lotes por la noche, es posible que no le preocupe la velocidad. Puede elegir unos valores que creen archivos pequeños que se puedan distribuir fácilmente pero que tarden más tiempo en generarse. Si crea archivos PDF ad hoc o archivos PDF complejos con muchos gráficos, es posible que le preocupe más la velocidad que el tamaño del archivo.

Puede utilizar diferentes valores de archivos PDF para el servicio de informes y para el servicio de informes por lotes.

Codificación de caracteres de PDF

La codificación de caracteres de PDF determina el juego de caracteres que se utiliza para crear archivos PDF. Se puede elegir entre codificación Windows1252, codificación estándar de un solo byte del sistema operativo Microsoft Windows para texto latino en sistemas de escritura occidentales o la codificación Unicode (UTF-16). De forma predeterminada, la codificación de caracteres de PDF se determina de forma automática en función de los caracteres que se encuentren en el archivo.

Los nombres de los valores son los siguientes:

- **Codificación de caracteres de PDF para el servicio de informes**
- **Codificación de caracteres de PDF para el servicio de informes por lotes.**

Valor	Función
Windows1252	Si sabe que los archivos sólo contienen caracteres Windows1252, utilice este valor para que la creación de archivos PDF sea más rápida. Cualquier carácter unicode (UTF-16) sin equivalente en Windows1252 se convierte a un carácter Windows1252 indeterminado.

Valor	Función
Fuente	Si sabe que los archivos contienen caracteres que no son Windows1252 (por ejemplo, caracteres chinos), utilice este valor para que los PDF se generen con más rapidez que con el valor Auto. Todas las fuentes incorporadas en el PDF tienen codificación de caracteres Windows1252. Casi todas las demás fuentes utilizan el juego de caracteres UTF-16. Este valor suele crear archivos PDF más grandes que el valor Windows1252. Es posible que los archivos codificados con UTF-16 ofrezcan una mayor compresión (consulte “Tipo de compresión de contenido” en la página 86).
Automático	Utilice este valor para determinar automáticamente si se debe utilizar Windows1252 o UTF-16 para codificar el texto en el documento. Si se deben analizar grandes cantidades de texto, ésta será el valor más lento de los tres. Si le preocupa la velocidad, puede probar otros valores con varios informes para determinar la mejor configuración para su entorno. Esta es la opción predeterminada.

Inclusión de fuentes

Para garantizar que las fuentes utilizadas en un informe estén disponibles para todos los lectores, las fuentes se pueden incluir en los archivos PDF. En IBM Cognos Configuration, hay dos listas de inclusión de fuentes, una para el servicio de informes y otra para el servicio de informes por lotes.

Las fuentes se pueden especificar como siempre incluidas o nunca incluidas. Por ejemplo, las fuentes de las que no se dispone de derechos legales para redistribuirlas se pueden especificar como nunca incluidas. Las fuentes que no están disponibles en oficinas comerciales remotas pero son necesarias para leer informes PDF, se pueden especificar como siempre incluidas.

Para obtener más información sobre las listas de inclusión de fuentes, consulte la *IBM Cognos Analytics Guía de instalación y configuración*.

En **IBM Cognos Administration**, se puede permitir o rechazar la inclusión de fuentes en los archivos PDF del servicio de informes y del servicio de informes por lotes. También se puede elegir inclusión automática de fuentes. Tenga en cuenta que los archivos con fuentes incluidas son más grandes y tardan más tiempo en generarse. Las fuentes incluidas pueden exigir demasiado de los recursos de la red. La utilización de pocas fuentes incluidas puede reducir el consumo de recursos de la red.

No obstante, la licencia de algunas fuentes prohíbe su inclusión. Asegúrese de que dispone del permiso del proveedor para incluir fuentes con licencia.

Los nombres de los valores son los siguientes:

- **Opción que permite al servicio de informes incluir fuentes en documentos PDF generados**
- **Opción que permite al servicio de informes por lotes incluir fuentes en documentos PDF generados.**

Existen fuentes especializadas, como fuentes de códigos de barras, que siempre se incluyen cuando se utilizan. Estos valores no controlan la inclusión de las fuentes especializadas. Las fuentes incorporadas en el PDF nunca se incluyen.

Valor	Función
Permitir	Utilice este valor si sabe que el público no dispone de las fuentes que necesita para ver los informes PDF. Los archivos son más grandes y la salida del PDF se genera más lentamente. Las fuentes que aparecen en la lista de nunca incluir de IBM Cognos Configuration no se incluyen. Esta es la opción predeterminada.
No permitir	Utilice este valor si sabe que el público dispone de todas las fuentes que necesita para ver los informes PDF. Los archivos son más pequeños y se generan con más rapidez. Las fuentes no se incluyen a menos que estén en la lista de incluir siempre de IBM Cognos Configuration.
Automático	Determina automáticamente las fuentes que se incluyen. Este valor es el que tarda más tiempo en generar informes PDF. Si los datos sólo contienen caracteres Windows1252, se utilizarán las listas de incluir siempre y nunca incluir de IBM Cognos Configuration. Si se produce un conflicto, se utilizará la lista de nunca incluir. Excepto para las fuentes especializadas, las fuentes que no están en la lista sólo se suelen incluir si se utilizan en el archivo los caracteres UTF-16 de esa fuente.

Tipo de compresión de contenido

Se puede establecer el tipo de compresión que se utilizará al crear informes PDF. La creación de archivos PDF con un tipo de compresión mayor tarda más tiempo, pero los archivos resultantes son más pequeños.

El tipo de compresión de contenido especifica los datos que se comprimen. El “Especificación de valores de archivos PDF” especifica el grado de compresión de los datos. La combinación de los dos valores determinan el tamaño final del archivo.

Los nombres de los valores son los siguientes:

- **Tipo de compresión de los documentos PDF creados mediante el servicio de informes**
- **Tipo de compresión de los documentos PDF creados mediante el servicio de informes por lotes.**

Los valores de esta configuración, de menor a mayor compresión, son: **Clásico, Básico, Mejorado, Avanzado y Completo**. Clásico es el valor predeterminado.

El tipo de compresión se refiere a la cantidad de datos que se comprimen dentro de un informe PDF. Normalmente, menos compresión implica una compresión más rápida y un documento más grande. Las versiones de Adobe PDF Acrobat Reader anteriores a la 6.0 no soportan los tipos de compresión superiores a Clásico.

En casos excepcionales, la compresión provoca que los archivos pequeños se vuelvan ligeramente más grandes.

Nivel del algoritmo de compresión

El tipo de compresión de contenido especifica los datos que se comprimen. El “Tipo de compresión de contenido” especifica el grado de compresión de los datos. La combinación de los dos valores determinan el tamaño final del archivo.

Los nombres de los valores son los siguientes:

- **Nivel de compresión de contenido de los documentos PDF creados mediante el servicio de informes**
- **Nivel de compresión de contenido de los documentos PDF creados mediante el servicio de informes por lotes.**

Los valores válidos del nivel del algoritmo de compresión están comprendidos entre 0 (sin compresión) y 9 (compresión máxima). El valor predeterminado es 9.

Especificación de valores de archivos PDF

Puede especificar valores de archivos PDF.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios** y pulse el servicio que desea.

Consejo: La vista actual es **Todos los servidores, Todos los grupos de servidores, Todos los asignadores o Servicios**.

3. En el menú **Acciones** del servicio, pulse **Establecer propiedades**.

4. Pulse la pestaña **Valores**.
5. Seleccione **Ajuste** en la lista **Categoría**.
6. En la columna **Valor**, escriba el valor que desee para cada uno de los valores del archivo PDF.

Consejo: Si desea restablecer un valor de configuración a su valor predeterminado, seleccione su casilla de verificación y pulse **Restablecer valor predeterminado**.

7. Pulse **Aceptar**.

Establecimiento del tiempo máximo de ejecución

Puede establecer el tiempo máximo de ejecución del servicio de informes y el servicio de informes por lotes.

Por ejemplo, puede limitar el tiempo de ejecución si sabe que algo no funciona porque las tareas tardan más tiempo en ejecutarse. También puede servir para garantizar que ninguna tarea monopolice el tiempo del servidor en detrimento de las demás.

Si se supera el límite de tiempo, la ejecución se cancela. El valor predeterminado es cero, que no especifica ningún límite de tiempo de ejecución.

Este valor tiene prioridad sobre el valor del límite del regulador. Para obtener más información, consulte “Cómo establecer el límite de tamaño de informe para el servicio de datos de informes” en la página 89.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Acerca de esta tarea

Este valor se puede cambiar en el nivel de sistema, asignador o servicio.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios** y después pulse el servicio que desee.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** del servicio, pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. Seleccione **Ajuste** en la lista **Categoría**.
6. En la columna **Valor**, escriba un nuevo valor para **Tiempo máximo de ejecución para el nombre_servicio (segundos)**.
7. Pulse **Aceptar**.

Cómo especificar el tiempo que se deben guardar las salidas de informe de la lista de observación

La salida de informe de la lista de observación se puede guardar durante un número de ejecuciones o un número de días o meses concretos.

Por ejemplo, se pueden guardar hasta 10 versiones o se pueden guardar las versiones de la salida de informe durante un periodo comprendido entre 2 días y 6 meses.

Existen dos valores:

- Si desea especificar la duración máxima de tiempo para mantener la salida de informe de la lista de observación, utilice el valor **Antigüedad de conservación de versión de documento periódico**. El valor predeterminado es 1 día. En el panel **Valores**, aparece como 1 Día(s).
- Si desea especificar el número máximo de copias que se deben conservar, utilice el valor **Recuento de conservación de versión en un documento periódico**. No existe ningún valor predeterminado.

Si se especifican ambos valores, el que se cumpla en primer lugar determinará el número de versiones que se guardarán.

Los valores que se elijan dependerán de la frecuencia de generación de la salida de informe de la lista de observación y de los recursos de sistema. Por ejemplo, si un informe se ejecuta por la noche para proporcionar salidas durante el día a petición a través del portal y las listas de observación se actualizan semanalmente, se podrán guardar cuatro versiones cada mes pero no más de 5 versiones durante ese tiempo. Si un trabajo se utiliza para ejecutar informes y las listas de observación sólo se actualizan cuando el trabajo se ejecuta, sólo se podrá guardar 1 versión cada día.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En la pestaña **Estado**, pulse **Sistema**.
2. Pulse la flecha del menú Acciones situada junto a **Sistema** y pulse **Establecer propiedades**.
3. Pulse la pestaña **Valores**.
4. Seleccione **Ajuste** en la lista **Categoría**.
5. En la columna **Valor**, escriba el nuevo valor de la configuración **Antigüedad de conservación de versión de documento periódico** y seleccione **Día(s)** o **Mes(es)** en el menú desplegable.
6. En la columna **Valor**, escriba un nuevo valor para la configuración **Recuento de conservación de versión en un documento periódico**.
7. Pulse **Aceptar**.

Cómo limitar zonas activas generadas en un gráfico de Analysis Studio o Creación de informes

Para mejorar el rendimiento, puede limitar el número de zonas activas que generan los gráficos de Analysis Studio y Creación de informes.

Una zona activa aparece en un gráfico cuando se pasa el puntero sobre él. Por ejemplo, una zona activa en un símbolo de obtención de detalles de nivel inferior o en una ayuda contextual ofrece información sobre la columna, la línea o la sección circular. El tiempo de respuesta del navegador aumenta con el número de zonas activas. Cuando se generan los gráficos con muchos miembros, las zonas activas se pueden convertir en una carga adicional para los recursos de sistema, que puede bloquear el navegador.

Al limitar el número de zonas activas, se da prioridad a elementos como etiquetas de eje y etiquetas de leyenda antes que a los elementos gráficos individuales, como barras, secciones circulares, etc. Dependiendo del número de elementos de un gráfico y del valor del número máximo de zonas activas, algunos elementos del eje pueden tener zonas activas mientras que otros elementos del eje y elementos gráficos no, o todos los elementos de eje y algunos elementos gráficos pueden tener zonas activas mientras que otros elementos gráficos no.

El valor de máximo de zonas activas en Creación de informes anula este valor. Para obtener más información, consulte la publicación *IBM Cognos Analytics - Reporting.User Guide*.

El valor predeterminado es un número ilimitado de zonas activas.

Procedimiento

1. En la pestaña **Estado**, pulse **Sistema**.
2. Pulse la flecha del menú Acciones situada junto a **Sistema** y pulse **Establecer propiedades**.
Sugerencia: También se puede cambiar el valor de zonas activas en el nivel del servicio o del asignador.
3. Pulse la pestaña **Valores**.
4. Seleccione **Ajuste** en la lista **Categoría**.
5. Localice el valor **Número de zonas activas generadas en un gráfico mediante el servicio de informes por lotes** o el valor **Número de zonas activas generadas en un gráfico mediante el servicio de informes**. En la columna **Valor**, pulse la flecha situada junto a **Ilimitado** y, a continuación, pulse **<Number>**. Escriba un nuevo valor para el número máximo de zonas activas.
6. Pulse **Aceptar**.

Cómo establecer el límite de tamaño de informe para el servicio de datos de informes

Puede aumentar el límite de tamaño para datos de informe.

Para limitar los recursos, como la memoria, que el servicio de datos de informes utiliza, el software de IBM Cognos limita el tamaño de los datos de informe que se pueden enviar. Si se reciben errores en IBM Cognos for Microsoft Office que indican que el tamaño de los resultados de un informe es demasiado grande, puede aumentar el límite del tamaño de datos de informe cambiando el valor de Límite del regulador.

El valor de tiempo máximo de ejecución tiene prioridad sobre este valor. Para obtener más información, consulte “Establecimiento del tiempo máximo de ejecución” en la página 87.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Datos de informes**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** de **ReportDataService**, pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. En la columna **Valor**, cambie el número de **Límite del regulador (MB)**.
6. Pulse **Aceptar**.

Excluyendo el ID de contexto para un agente de las tareas de servicio web IBM WebSphere

De forma predeterminada, cuando el servicio de agente interactúa con un servicio web, se incluye el ID de contexto del agente.

Si está ejecutando un agente que incluye una tarea de servicio web en IBM WebSphere, debe excluir este ID de contexto para impedir que se produzcan conflictos con los ID de contexto propios de WebSphere.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para **AgentService**, en la columna **Parámetro**, escriba **asv.webservice.useRunContext**.
Debe especificar este valor en cada instancia de **AgentService** que está ejecutando.
3. Escriba **verdadero** como un valor para este parámetro y haga clic en **Aceptar**.
4. Reinicie los servicios IBM Cognos.

Ajuste de memoria caché para el servicio de repositorio

Puede ajustar la memoria caché del servicio de repositorio. Existen varias propiedades de dimensionamiento que se pueden establecer para memoria local y recursos de disco. Los valores pueden ser exclusivos en cada asignador.

En la tabla siguiente se proporciona una descripción de los tipos de memoria caché que se pueden ajustar para el servicio de repositorio.

Tabla 21. Tipos de memoria caché disponibles en el servicio de repositorio

Parámetro	Descripción
Número máximo de segundos que los informes y los elementos de informe pueden existir en la memoria caché.	Número máximo de segundos que un informe puede existir en la memoria caché, independientemente de la frecuencia con la que se utilice. Una vez que caduca un informe, se recupera del repositorio y no de la memoria caché. El valor predeterminado es de 1200 segundos (20 minutos). Un valor de 0 significa que el informe no se guarda en la memoria caché.
Número máximo de informes y elementos de informe que pueden desbordarse al disco.	Número máximo de entradas de memoria caché que pueden mantenerse en la memoria local. El valor predeterminado es 1000 entradas. Un valor de 0 significa que no hay ningún límite para el número de elementos que se mantienen en la memoria local.
Número máximo de informes y elementos de informe que se pueden almacenar en memoria.	Número máximo de entradas de memoria caché que se pueden grabar en el disco local. Cuando la memoria caché llega al límite, los elementos se desbordan en el disco local. El valor predeterminado es 100 informes y elementos de informe. Un valor de 0 significa que no hay ningún límite en el número de elementos grabados en el disco. Las entradas se graban en la ubicación de los archivos de datos definida en IBM Cognos Configuration.

El servicio de repositorio utiliza el valor avanzado **repository.maxCacheDocSize** para especificar el tamaño máximo, en megabytes, de cada salida de informe que se puede almacenar en la memoria caché. Las salidas con un tamaño mayor al tamaño especificado no se guardan en la memoria caché y se deben recuperar siempre del repositorio o de Content Manager. El valor predeterminado es 10. Puede especificar este valor avanzado de forma individual para un servicio de repositorio o un asignador concreto o bien globalmente para todo el entorno de IBM Cognos. Para obtener más información, consulte Apéndice G, "Configuración de valores avanzados", en la página 513.

Limpieza masiva de tablas NC

Utilice el proceso de limpieza masiva para eliminar tareas finalizadas de las tablas NC en el almacén de contenido.

Se da soporte al proceso por lotes para varias tareas y objetos. Un ejemplo habitual podría ser un trabajo planificado que contiene ejecuciones de informes. El servicio de supervisión almacena el trabajo y los comandos de ejecución del informe en una cola de tareas en las tablas NC. En circunstancias idóneas, las tareas finalizadas se eliminan una a una en un proceso en segundo plano. No obstante, en servidores ocupados o si la tasa de ejecución planificada sobrepasa la capacidad del sistema, podría no haber suficiente tiempo para eliminar las tareas finalizadas de esta forma. La cola de tareas seguiría creciendo y podría provocar problemas de rendimiento en el servidor. El problema se manifiesta al crecer la lista de ejecuciones de informe pendientes, al consultar las actividades actuales en el componente de administración.

Estas son las tablas NC que se verían afectadas:

- NC_TASK_ANCESTOR_STOREIDS

- NC_TASK_HISTORY_DETAIL
- NC_TASK_QUEUE
- NC_TSE_STATE_MAP
- NC_TASK_PROPERTY

El proceso de limpieza masiva utiliza un script `BulkFinishedTaskCleanerThread` dependiente de la base de datos. Este script lo inicia el servicio de supervisión durante el inicio del servicio IBM Cognos. Cuando está habilitado, el script primero comprueba si existe un determinado número (configurable) de tareas completadas en las tablas NC. Si se encuentran este tipo de tareas, se trasladan a una tabla provisional y las tablas NC se borran en una única transacción. No es necesario eliminar ninguna tabla ni volverlas a crear desde el esquema de NC. Tampoco es necesario detener los servicios de IBM Cognos.

El proceso de limpieza se habilita y se configura utilizando la siguiente configuración avanzada del servicio de supervisión:

- `event.finished.check.active`
- `event.finished.check.interval`
- `event.finished.check.threshold`

Para obtener más información sobre estos ajustes, consulte el tema “Valores avanzados del servicio de control” en la página 532.

Para obtener información sobre la configuración avanzada, consulte Apéndice G, “Configuración de valores avanzados”, en la página 513.

Importante: Asegúrese de tener siempre una copia de seguridad actual y válida del almacén de contenido.

Ejecución simultánea de consultas

Dependiendo del entorno, se puede mejorar el rendimiento de la ejecución de informes habilitando la ejecución simultánea de consultas.

De forma predeterminada, el software de IBM Cognos ejecuta secuencialmente las consultas de un informe. Esto se puede hacer estableciendo propiedades avanzadas del servidor para el servicio de informes, el servicio de informes por lotes o ambos. Cuando está habilitada la ejecución simultánea de consultas, el servidor de informes determina las consultas del informe que se pueden ejecutar simultáneamente.

El autor de informes debe especificar las consultas del informe que son candidatas a la ejecución simultánea. Para obtener más información, consulte la publicación *IBM Cognos Analytics - Reporting.User Guide*.

RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS

Utilice este parámetro para habilitar la ejecución simultánea de consultas y establecer el número máximo de ayudantes de ejecución de consultas para cada proceso del servicio de informes o del servicio de informes por lotes.

El valor predeterminado es 0, que indica que la ejecución simultánea de consultas está inhabilitada.

Cada ayudante de ejecución de consulta produce una conexión de origen de datos adicional. Por ejemplo, un servicio de informes que tenga cuatro procesos con dos conexiones de alta afinidad y dos conexiones de baja afinidad:

- Si el número máximo de ayudantes de ejecución de consultas se establece en 0 (inhabilitado), el número máximo de conexiones al origen de datos creado por el servicio de informes será de 16 (dos conexiones de baja afinidad más dos conexiones de alta afinidad más cero ayudantes de ejecución de consultas para cuatro procesos).
- Si el número máximo de ayudantes de ejecución de consultas se establece en 2, el número máximo de conexiones al origen de datos creado por el servicio de informes es de 24 (dos conexiones de baja afinidad más dos conexiones de alta afinidad más dos ayudantes de ejecución de consultas para cuatro procesos).

RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT

Utilice este parámetro para especificar el número máximo de ayudantes de ejecución de consultas para cada informe. Este parámetro se utiliza para impedir que un único informe consuma todos los ayudantes de ejecución de consultas disponibles.

Por ejemplo, un informe tiene ocho consultas que se pueden ejecutar simultáneamente:

- Si RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS y RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT están establecidos ambos en cuatro, el informe consume todos los ayudantes de consultas cuando se ejecutan. Ningún otro informe puede ejecutar consultas simultáneamente hasta que el informe se haya terminado de ejecutar.
- Si RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT está establecido en dos en su lugar, el informe consume dos ayudantes de consulta, dejando dos para uso de los otros informes.

El valor predeterminado de este parámetro es 1.

Este valor no tiene efecto a menos que RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS esté ajustado en más de 0.

RSVP.CONCURRENTQUERY.ENABLEDFORINTERACTIVEOUTPUT

Utilice este parámetro para habilitar la ejecución simultánea de consultas cuando el servicio de informes genere salidas interactivas.

En los informes interactivos, si está activada la ejecución simultánea de consultas, es posible que algunas se ejecuten de forma innecesaria porque los resultados no se utilizan. Por ejemplo, todas las consultas de un informe multipágina se pueden ejecutar con una consulta en cada página como mínimo, pero el usuario sólo puede ver la primera página. Si no desea utilizar recursos para resultados que no se emplearán en los informes interactivos, puede inhabilitar este parámetro.

Las páginas de solicitud creadas no son salidas interactivas y no se ven afectadas por este valor.

El valor predeterminado de este parámetro es false, que indica que está inhabilitado.

RSVP.PROMPT.EFFECTIVEPROMPTINFO.IGNORE

Utilice este parámetro para inhabilitar el envío del atributo `effectivePromptInfo` en las solicitudes de metadatos e inhabilitar el movimiento de la información de solicitud desde el nivel inferior del atributo de título de un nivel hasta el propio nivel.

El valor predeterminado de este parámetro es `false`, que indica que está inhabilitado.

Establecer parámetros para la ejecución simultánea de consultas

Utilice el procedimiento siguiente para establecer los parámetros para la ejecución simultánea de consultas.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para **ReportService** o **BatchReportService**, en la columna **Parámetro**, escriba uno de los nombres de parámetros que se describen en la sección “Ejecución simultánea de consultas” en la página 92.
3. En la columna **Valor**, escriba el valor correspondiente para el parámetro.
4. Pulse **Aceptar**.

Establecimiento de la prioridad de consultas

Puede establecer parámetros que especifican como funciona la priorización de las consultas.

Cuando se ejecuta un informe con los controles de solicitud definidos, se recupera toda la información de los parámetros, incluida la información de parámetros definida en el informe, el modelo y el origen de datos. Esto es necesario para introducir los datos y para alinear funciones de controles de solicitud con las de su parámetro asociado. Esta operación puede influir en el rendimiento, especialmente cuando hay muchas consultas o son complejas. Desde la perspectiva del usuario, puede tardar demasiado tiempo en presentar la primera página de solicitud o la página del informe.

Para aumentar la velocidad, los autores de informes pueden establecer una sugerencia de consulta en Creación de informes con el fin de otorgar prioridad a una consulta al determinar la información del parámetro. Las consultas se priorizan en función de donde se utilizan y de si contienen filtros. Un grupo de prioridad es el conjunto de consultas que comparten atributos similares, como un filtro. En lugar de recuperar los parámetros para todas las consultas al mismo tiempo, se recuperan primero los parámetros para las consultas con prioridad definida por el autor, independientemente de como se haya establecido la priorización de consultas automatizada. Para obtener más información acerca de parámetros, filtros y controles de solicitud, consulte la publicación *IBM Cognos Analytics - Reporting Guía del usuario*.

Las consultas se agrupan por prioridad según se muestra en la tabla siguiente. Cuando un grupo de consultas tiene subgrupos, el primer subgrupo tiene prioridad sobre el segundo.

Grupo de consultas	Prioridad
Consultas con la propiedad Utilizar para información del parámetro establecida en Sí en Creación de informes	1
Consultas con filtros definidos que no se utilizan para rellenar controles de solicitud • Primera referencia a esas consultas • Referencias posteriores a esas consultas	2
Consultas con filtros definidos que se utilizan para rellenar controles de solicitud • Primera referencia a esas consultas • Referencias posteriores a esas consultas	3
Consultas sin filtros definidos que no se utilizan para rellenar controles de solicitud • Primera referencia a esas consultas • Referencias posteriores a esas consultas	4
Consultas sin filtros definidos que se utilizan para rellenar controles de solicitud • Primera referencia a esas consultas • Referencias posteriores a esas consultas	5

Para especificar una configuración para todo el sistema que defina el modo de procesar las consultas y los grupos de consultas, se puede asignar un nombre o un valor de configuración a la configuración avanzada del servidor de informes, RSVP.PROMPT.RECONCILIATION. Esto permite especificar el grado de conciliación entre las funciones de control de solicitud y el tipo de datos, y los del parámetro asociado. El valor elegido determina si es más importante la velocidad o la precisión de la conciliación. Por ejemplo, si el autor de informes garantiza que los parámetros se definan con el mismo tipo de datos y funciones (p.ej., opcionalidad, cardinalidad y discreción), en todas las consultas, al especificar CHUNKED o 3, es probable que se consiga el mejor rendimiento en la mayoría de las situaciones.

RSVP.PROMPT.RECONCILIATION.CHUNKSIZE permite especificar el tamaño del trozo. Este valor se puede aplicar al utilizar CHUNKED GROUPED y CHUNKED. El tamaño de trozo predeterminado es 5.

Las propiedades avanzadas del servidor de informes y las sugerencias de consulta de Creación de informes trabajan conjuntamente para ofrecer el mejor rendimiento.

Se pueden utilizar los valores que se muestran en la tabla siguiente para configurar RSVP.PROMPT.RECONCILIATION.

Valor	Nombre	Función
0	COMPLETE	Todas las consultas se envían a la vez. Se trata de la forma de conciliación más lenta y precisa. Éste es el valor predeterminado.
1	GROUPED	Las consultas se envían por grupo de prioridad. Este valor funciona mejor para informes que tienen muchas consultas sin filtrar y pocas consultas filtradas. Ofrece una velocidad media y una alta precisión de conciliación.
2	CHUNKED GROUPED	Las consultas se envían por grupo de prioridad con un número máximo por solicitud. Las consultas no se desglosan en grupos. Este valor es mejor para informes que tienen muchas consultas con expresiones de filtro similares. Ofrece una velocidad máxima y una baja precisión de conciliación.
3	CHUNKED	Las consultas se envían por grupo de prioridad con un número máximo por solicitud. Las consultas se pueden desglosar en grupos.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration** Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para el servicio **Informe**, en la columna **Parámetro**, escriba uno de los nombres de parámetro descritas en esta sección.
3. En la columna **Valor**, escriba un valor asociado con la configuración.
4. Opcional: Si es necesario, continúe escribiendo otras configuraciones y valores.
5. Pulse **Aceptar**.
6. Repita los mismos pasos para **BatchReportService**.

La conversión de claves de búsqueda numérica a cadenas en consultas

Se puede producir un error si el origen de datos no convierte los elementos de datos numéricos en cadenas.

Una solicitud de búsqueda está asociada a una consulta que no se ejecuta cuando se representa la solicitud de búsqueda la primera vez. Al escribir una cadena de búsqueda se filtra la consulta y los resultados se muestran en un cuadro de lista. El servidor de informes no comprueba el tipo de datos del elemento de consulta filtrado porque la mayoría de los orígenes de datos convierten el elemento de datos en una cadena (varchar) y el filtro es válido. Sin embargo, algunos orígenes de datos, como Teradata, no realizan la conversión, lo que genera un error.

El siguiente mensaje de error se muestra cuando se ejecuta un informe Creación de informes o Query Studio:

RQP-DEF-0177 Se ha producido un error al realizar la operación 'sqlPrepareWithOptions' status='-69' UDA-SQL-0043 La base de datos subyacente ha detectado un error durante el procesamiento de la solicitud SQL.[NCR][ODBC Teradata Driver][Teradata Database] La coincidencia parcial de cadenas requiere operandos de caracteres.

Para evitar este error, asegúrese de que el valor avanzado **RSVP.PROMPT.CASTNUMERICSEARCHKEYTOSTRING** esté establecido en true (valor predeterminado) para **ReportService** y **BatchReportService**. Este valor avanzado se utiliza para convertir los elementos de datos numéricos a un formato de cadena (varchar). Para obtener más información acerca de la configuración de los valores avanzados, consulte: "Configuración de valores avanzados para servicios específicos" en la página 515.

Ejemplo de elementos de datos sin convertir

[data item] starts with '20'

[data item] contains '123'

O una combinación booleana:

[data item] starts with '2' AND [data item] contains '009' OR [data item] contains '119'

Ejemplo de un elemento de datos sin convertir con una función inferior

Si la búsqueda no distingue entre mayúsculas y minúsculas, estas expresiones contendrán la función lower, que tiene más sentido al buscar en elementos de datos de cadena que en numéricos.

lower([data item]) starts with lower('20')

lower([data item]) contains ('123')lower

([data item]) starts with lower('2') AND lower([data item]) contains lower('009') OR lower([data item]) contains lower('119')

Ejemplo de elemento de datos convertidos en una cadena

cast([data item], varchar(128)) starts with '20'

cast([data item], varchar(128)) contains '123'

cast([data item], varchar(128)) starts with '2' AND cast([data item], varchar(128)) contains '009' OR cast([data item], varchar(128)) contains '119'

Almacenamiento de la sesión en la memoria caché

En Creación de informes, Query Studio e IBM Cognos Viewer si está habilitado el almacenamiento de la sesión en la memoria caché, los resultados de las solicitudes anteriores enviadas a la base de datos se almacenan en la memoria caché durante la sesión.

Para aumentar el rendimiento en sucesivas consultas, el software de IBM Cognos utiliza resultados almacenados en la memoria caché para algunas acciones en lugar de acceder a la base de datos. Esta opción se aplica si se pueden utilizar los mismos resultados o si los resultados son un subconjunto de los almacenados en la memoria caché. Se puede inhabilitar el almacenamiento de la sesión en la caché en el nivel del servidor o en el nivel del paquete o el informe.

Como el rendimiento se puede ver afectado, es preferible inhabilitar el almacenamiento de la sesión en la caché en el nivel del servidor en las siguientes situaciones:

- Los usuarios esperan resultados actualizados directamente de la base de datos en cada consulta, por ejemplo, nuevos registros que se añadieron a la base de datos de forma provisional.
- Si se desea limitar el número de veces que se accede a la memoria caché durante una sesión.

Se puede inhabilitar el almacenamiento de la sesión en la caché para informes individuales debido a su elevado consumo de recursos, por ejemplo, en informes que utilizan separación.

También se puede habilitar e inhabilitar el almacenamiento de la sesión en la caché para consultas específicas de informes de Creación de informes (consulte la publicación *IBM Cognos Analytics - Reporting Guía del usuario*) y para modelos de Framework Manager (consulte la publicación *IBM Cognos Framework Manager Guía del usuario*).

El almacenamiento de la sesión en la caché está habilitado de forma predeterminada para nuevos modelos e informes. Los paquetes e informes existentes conservan los valores de almacenamiento de la sesión en la caché.

Inhabilitar la memoria caché de la sesión a nivel del servidor

Se puede inhabilitar el almacenamiento de la sesión en la caché en el nivel del servidor.

Procedimiento

1. En el directorio *install_location/configuration*, haga una copia del archivo *CQEConfig.xml.sample* y cámbiele el nombre a *CQEConfig.xml*.
2. Abra el archivo *install_location/configuration/CQEConfig.xml* en un editor. Asegúrese de que su editor permita guardar archivos en formato UTF-8.
3. Busque el parámetro *queryReuse* en el archivo *CQEConfig.xml* y cambie el valor por 0.
4. Guarde el archivo *CQEConfig.xml*.
5. Con IBM Cognos Configuration, detenga y luego reinicie el servicio IBM Cognos. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Cómo inhabilitar el almacenamiento de la sesión en la caché en el nivel del paquete o el informe

Se puede inhabilitar el almacenamiento de la sesión en la caché en el nivel del paquete o el informe.

Procedimiento

1. Copie el archivo *install_location/configuration/CQEConfig.xml.sample* en *install_location/bin* y cámbiele el nombre por *CQEConfig.xml*.
2. Abra el archivo *install_location/bin/CQEConfig.xml* con un editor.
3. Asegúrese de que su editor permita guardar archivos en formato UTF-8.
4. Busque el parámetro *queryReuse* y elimínelo.
5. Guarde el archivo *CQEConfig.xml*.
6. Con IBM Cognos Configuration, detenga y reinicie el software de IBM Cognos. Para obtener información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Habilitación del parámetro HTTPOnly para asegurar la cookie del pasaporte CAM

El pasaporte CAM identifica la sesión del navegador web del usuario con el servidor. Los administradores pueden establecer el atributo HTTPOnly para que los scripts no puedan leer ni manipular la cookie de pasaporte CAM durante la sesión de un usuario con su navegador web.

Acerca de esta tarea

La habilitación del atributo HTTPOnly evita que scripts maliciosos roben la identidad de sesión del usuario. Cuando un administrador establece este atributo, el navegador web puede utilizar la cookie de la sesión solo para enviar solicitudes de HTTP al servidor.

Si desea habilitar el atributo HTTPOnly, asegúrese de que los usuarios tienen un navegador web que admite este atributo.

Procedimiento

1. Diríjase a IBM Cognos Administration.
2. En la pestaña **Estado**, pulse **Sistema**.
3. En el panel **Scorecard** del menú desplegable **Sistema**, haga clic en **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. Desde la lista **Categorías**, seleccione **Entorno**.
6. Para el parámetro **HTTPOnly Cookie Support**, seleccione la casilla de verificación correspondiente en la columna **Valor**.
7. Pulse **Aceptar**.

Reducción de la precisión decimal

Puede establecer precisión decimal en los informes de tabla de referencias cruzadas.

En un informe de tabla de referencias cruzadas, los valores soportan un máximo de 18 dígitos, más el separador decimal. La precisión decimal determina el número de dígitos reservados para expresar el componente decimal de un número. Los dígitos restantes están reservados para expresar el componente entero del número. La precisión decimal predeterminada es de 7 dígitos, lo que limita la longitud de los enteros a 11 dígitos.

Si desea reservar más de 11 enteros para expresar el componente entero de un número, debe reducir la precisión decimal. Por ejemplo, puede establecer la precisión decimal en 2, lo que le permite reservar hasta 16 dígitos para el componente entero de un número.

Procedimiento

1. En el directorio *install_location*\configuration, ubique el archivo qfs_config.xml.
2. Copie el archivo qfs_config.xml y cambie el nombre del archivo copiado a qfs_config.xml.backup.
3. Abra el archivo qfs_config.xml original y busque la línea de código siguiente:

```
<provider name="CubeBuildProvider"libraryName="qfsCubeBuildProvider"
serviceProvider="true">
  <providerDetails>
```
4. Para el elemento providerDetails, añada la siguiente línea:

```
<scaleOfFloatDouble value="n"/>
```

donde "n" representa el valor de la precisión decimal que desea especificar. El valor predeterminado es 7.
5. Guarde el archivo qfs_config.xml.
6. Reinicie el servicio de IBM Cognos.

Almacén de objetos externos para almacenar la salida de informe localmente

Puede configurar Content Manager para almacenar las salidas de informe en una unidad local o en una unidad compartida de red mediante la definición de un almacén de objetos externos.

Mediante el uso del almacén de objetos para reportar resultados reduce el tamaño del almacén de contenido y proporciona mejoras de rendimiento para el Gestor de contenido.

Para obtener más información acerca de la configuración de un almacén de objetos externos, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Resultado del informe guardado

Puede especificar dónde guardar copias de los archivos de resultado del informe.

Se pueden guardar los formatos de salida de informe siguientes: PDF, CSV, XML, datos de Microsoft Excel 2002, 2007 y Datos de Excel 2007, y HTML que no tenga gráficos incluidos.

Puede compartir los archivos de resultado del informe guardado con aplicaciones externas o con usuarios que no tienen acceso al software IBM Cognos.

Tiene las opciones siguientes para guardar los archivos de resultados de informes:

- Una ubicación fuera del software de IBM Cognos
Con esta opción, los usuarios pueden controlar qué archivos de resultados de informes se guardan en el sistema de archivos. Para obtener más información, consulte “Guardar archivos de resultados de informes fuera del software IBM Cognos” en la página 101.
- Una ubicación en el software IBM Cognos

Con esta opción, todos los archivos de resultados de informes se guardan en la misma ubicación del sistema de archivos definido en Content Manager. Esto hace que esta opción sea útil para propósitos de implementación. Un archivo de descripción con una extensión `_desc` que se crea con esta opción, contiene información útil para el software de archivo de terceros o de IBM.

Esta opción también permite ejecutar un script predeterminado para cada archivo de resultados que ayuda con la integración de terceros.

Para obtener más información, consulte: “Guardar archivos de resultado de informes en el software IBM Cognos” en la página 102.

Ambas opciones para guardar los archivos de resultados del informe son independientes uno del otro, pero se pueden utilizar al mismo tiempo.

Guardar archivos de resultados de informes fuera del software IBM Cognos

Los archivos de resultados de informes se pueden guardar en un sistema de archivos fuera del software IBM Cognos. Los usuarios pueden elegir cuáles archivos de resultados guardar.

Antes de empezar

Antes de utilizar esta funcionalidad, configure el directorio raíz que está representado mediante la propiedad **Archive Location File System Root** en IBM Cognos Configuration. Para obtener más información, consulte la sección sobre cómo guardar la salida de informe fuera de IBM Cognos Analytics en *IBM Cognos Analytics Guía de instalación y configuración*.

Acerca de esta tarea

Esta opción es útil cuando los usuarios desean compartir informes con aplicaciones externas como un sitio web. Los informes se guardan en esta ubicación cada vez que se actualizan de manera que el contenido actual siempre está disponible. Esta opción también permite guardar informes en una red local para los usuarios que no tienen acceso al software IBM Cognos.

Múltiples ubicaciones se pueden especificar para los asignadores y servicios.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios**.
2. En la barra de herramientas, pulse el icono **Definir ubicaciones del sistema de archivos** .
3. Haga clic en **Nuevo** y escriba un nombre, descripción y sugerencia en pantalla.
4. En el cuadro **Ubicación del sistema de archivos**, escriba la ubicación en la que desee guardar los archivos de salida de informe.
5. Pulse **Finalizar**.

Resultados

La ubicación que ha especificado se adjunta a la **Ubicación raíz del sistema de archivos** que se configuró en IBM Cognos Configuration.

Consejo: En IBM Cognos Configuration, la **Ubicación raíz del sistema de archivos** se representa mediante la propiedad **Archive Location File System Root**.

Qué hacer a continuación

Cuando los usuarios seleccionan **Guardar informe como archivo externo** como el método de entrega de informes cuando ejecutan o programan un informe, los archivos de resultado del informe se guardan en esta ubicación cada vez que se ejecuta el informe.

Guardar archivos de resultado de informes en el software IBM Cognos

Los usuarios pueden guardar copias de archivos de resultado de informes en el software IBM Cognos. Todos los archivos de resultados de informes se guardan en una ubicación especificada en el Gestor de contenidos.

Antes de empezar

Antes de utilizar esta funcionalidad, configure la propiedad **Guardar los resultados del informe en un sistema de archivos** en IBM Cognos Configuration to true. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Acerca de esta tarea

Debe especificar una ubicación en el Gestor de contenidos donde se guardarán copias de los archivos de resultados del informe. La ubicación aplica a resultados guardados originados del servicio de Gestor de contenidos seleccionado. Esta ubicación está representada por el parámetro **CM.OutPutLocation**.

Cuando guarda el resultado del informe de esta manera, también se crea un archivo descriptor XML para el archivo de resultado. El archivo descriptor contiene información acerca del resultado del informe, como el nombre, localización, hora de creación, clave de separación, ruta de búsqueda para el informe asociado y contacto de la versión del informe. El archivo descriptor toma el nombre del archivo de resultado con el sufijo añadido _desc. Por ejemplo, un informe en PDF guardado con el nombre 158_1075940415360.pdf tendrá un archivo descriptor con el nombre 158_1075940415360_desc.xml.

También puede especificar un script de manera que los comandos posteriores al procesamiento se pueden ejecutar cada vez que se copia un resultado del informe al sistema de archivos.

Las salidas de informe siempre se escriben en el directorio configurado para cada instancia del servicio de entrega. Para evitar que se escriban salidas de informes en varias ubicaciones, asegúrese de que se está ejecutando solamente una instancia del servicio de entrega o bien configure todas las instancias de servicio para que utilicen una ubicación de archivo de red compartida. Todos los asignadores que ejecuten el servicio de entrega deben tener acceso al sistema de archivos o estar inhabilitados en todos los sistemas en los que no está previsto que se guarde la salida de informe.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.

2. Para **ContentManagerService**, defina los parámetros siguientes:

- **CM.OutPutLocation**

Especifica una ubicación en el software IBM Cognos donde se guardan los archivos de resultados del informe. Las versiones de informes anteriores no se suprimen de esta ubicación cuando se guardan nuevas versiones. Esta ubicación se debe gestionar adecuadamente de manera que solo se guarden las versiones seleccionadas del informe.

Este parámetro es obligatorio si desea guardar archivos de resultado de informe en el software IBM Cognos.

- **CM.OutputScript**

Especifica la ubicación y nombre del script de shell, como un archivo .bat o .sh que se ejecuta después de guardar el resultado del informe en el directorio de destino. Los nombres completos del archivo de resultado del informe y el archivo descriptor asociado se transfieren al script. Este parámetro es opcional.

- **CM.OutputByBurstKey**

Este parámetro es aplicable cuando el resultado del informe se distribuye por separación. Especifica si debe almacenar los archivos de resultado del informe en un subdirectorío con el mismo nombre que la clave de separación. El valor predeterminado es falso lo que significa que las claves de separación no almacenan el resultado.

Configuración del informe y los servicios de informe por lotes para usar las hojas de trabajo grandes

Los administradores pueden habilitar la compatibilidad de hojas de trabajo Microsoft Excel 2007 grandes. Cuando se hace esto, las hojas de trabajo con hasta 1 048 576 filas son compatibles.

Para habilitar la compatibilidad con hojas de trabajo grandes, especifique la configuración avanzada **RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET** para **ReportService** y **BatchReportService**. Cuando se especifica el valor **RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET**, los valores siguientes también se pueden especificar:

- **RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS**

Especifica el número de filas para el resultado antes de moverlo a una nueva hoja de trabajo.

- **RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE**

Ajusta el tamaño de fragmentos de la memoria interna, en filas, que el servidor IBM Cognos Analytics genera antes de vaciarlo a un disco. Si este valor no se especifica, el valor predeterminado es de aproximadamente 45 000 filas. Esta propiedad puede ser útil cuando hay problemas, como agotar la memoria al generar informes con el valor predeterminado. Es posible que sea necesario disminuir los valores para permitir que el informe se ejecute correctamente.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para **ReportService**, en la columna **Parámetro**, escriba **RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET**.
3. En la columna **Valor**, escriba verdadero.

4. Especifique los valores **RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS** y **RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE** de forma parecida y escriba los valores necesarios para los mismos.
5. Pulse **Aceptar**.
6. Repita los mismos pasos para **BatchReportService**.

Cambio de nombre de forma dinámica de las pestañas de la hoja de trabajo en los informes en Excel 2007

En IBM Cognos Analytics, si la propiedad avanzada **RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE** está establecida en **true**, las pestañas de la salida de Excel 2007 cambian de nombre de forma dinámica según los saltos de página que se hayan especificado.

Nota: Esta propiedad no se aplica a Analysis Studio.

Acerca de esta tarea

Si se especifican saltos de página por línea de producto, las pestañas de la hoja de trabajo tendrán el mismo nombre. Por ejemplo, las páginas que tienen saltos de página por las líneas de producto Equipo de acampada, Equipo de montañismo, Accesorios personales, Protección aire libre y Equipo de golf tendrán pestañas con el mismo nombre.

Para obtener información sobre los nombres de las pestañas cuando los informes contienen dos conjuntos de páginas que utilizan la línea de producto como elemento de agrupación o que contienen conjuntos de páginas anidados, consulte la publicación *IBM Cognos Creación de informes Guía del usuario*.

Procedimiento

1. Siga los pasos del tema “Configuración de valores avanzados para servicios específicos” en la página 515.
2. En la página Establecer valores avanzados - ReportService, en la columna **Parámetro**, escriba **RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE**.
3. En la columna **Valor**, escriba **true**.

Configuración de la solución de linaje

El linaje proporciona detalles sobre los datos de un informe, como el origen de datos y las expresiones de cálculo. Puede configurar la solución de linaje predeterminada del software de IBM Cognos, la herramienta de linaje IBM InfoSphere Information Governance Catalog o una solución de linaje personalizada.

Puede acceder a la información de linaje en IBM Cognos Viewer, Creación de informes, Query Studio y Analysis Studio. Para utilizar la solución predeterminada o IBM InfoSphere Information Governance Catalog, asegúrese de que el valor del parámetro **URI del servicio de información de metadatos** de la categoría **Entorno** esté configurado de la forma especificada en los pasos de esta sección.

Para implementar una solución de linaje personalizada, deberá:

- Crear una interfaz Web que convierta los parámetros de las solicitudes de linaje del software de IBM Cognos e invoque la solución de linaje personalizada.

Para obtener más información, consulte la sección que trata sobre la integración de una solución de linaje personalizada en la publicación *IBM Cognos Software Development Kit Developer Guide*.

- Cambiar el valor del parámetro **URI del servicio de información de metadatos** de la categoría **Entorno** a la dirección URL del servidor de linaje.

Antes de empezar

Debe estar habilitada la función de **linaje**. Para obtener más información, consulte Capítulo 13, "Funciones y características protegidas", en la página 227 y Capítulo 14, "Capacidades de objetos", en la página 239.

Nota: Para ver una lista de las versiones soportadas de InfoSphere Information Server, consulte la sección Informes de compatibilidad de productos de software de Cognos Analytics.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el menú Acciones de **Sistema**, pulse **Establecer propiedades**.
3. Pulse la pestaña **Valores**.
4. En la categoría **Entorno**, **URI del servicio de información de metadatos**, escriba uno de los siguientes valores.
 - Si desea configurar la solución de linaje predeterminada del software de IBM Cognos, escriba **/lineageUIService**.
Si este valor ya se ha especificado, pulse **Cancelar**. No es necesario que cambie ningún valor.
 - Si desea configurar IBM InfoSphere Information Governance Catalog como solución de linaje, escriba el URL como se indica a continuación:
`/lineageUIService?iis=https://nombre_servidor_igc:9080/ibm/iis/igc#cognosLineage/cognos_server_name`
donde `nombre_servidor_igc:9080/ibm/iis/igc#cognosLineage/`
`cognos_server_name` es el URL de acceso a IBM InfoSphere Information Governance Catalog en la red.
`nombre_servidor_igc` representa el nombre del servidor donde está instalado IBM InfoSphere Information Governance Catalog.
 - Para beneficiarse de una combinación de linaje de Cognos y linaje de InfoSphere Information Governance Catalog, se debe configurar un parámetro adicional. Un parámetro "launchPoint" establecido en el valor "indirect" indicará que se debe utilizar el linaje Cognos para el linaje a nivel de Cognos (por ejemplo, información a nivel de informe y modelo) y se puede utilizar Information Governance Catalog para explorar el linaje del origen de datos. Si pulsa el objeto de origen de datos en el visor de linaje de Cognos, se invoca IBM InfoSphere Information Governance Catalog para explorar la información de linaje detallada a nivel de origen de datos.
`/lineageUIService?launchPoint=indirect`
`&iis=URL_Information_Governance_Catalog`
Por ejemplo, `/lineageUIService?launchPoint=indirect&iis=https://nombre_servidor_igc:9080/ibm/iis/igc#cognosLineage/nombre_servidor_cognos`
`nombre_servidor_igc` representa el nombre del servidor donde está instalado IBM InfoSphere Information Governance Catalog.

- Si desea configurar una solución de linaje personalizada, sustituya el valor existente por el URI que representa la interfaz Web de linaje.

Por ejemplo, escriba `https://miempresa.com/ourLineageService.cgi`

5. Pulse **Aceptar**.

Configuración del URI de InfoSphere Business Glossary

Para acceder a IBM InfoSphere Business Glossary desde el visor en IBM Cognos Analytics, y desde el árbol de metadatos de Reporting, Query Studio y Analysis Studio, debe especificar el URI de la página web del Glosario.

De forma predeterminada, los resultados de búsqueda del Glosario en el software de Cognos devuelven únicamente términos que contengan la palabra clave especificada en la búsqueda. No se devuelven otros tipos de activos.

Para obtener más información, consulte “Acceso a InfoSphere Business Glossary” en la página 363.

Antes de empezar

Para acceder a InfoSphere Business Glossary, los usuarios deben tener permisos para la función **Glosario**. Para obtener más información, consulte Capítulo 13, “Funciones y características protegidas”, en la página 227 y Capítulo 14, “Capacidades de objetos”, en la página 239.

Procedimiento

1. En **Gestionar > Consola de administración**, abra **IBM Cognos Administration**.
2. En la pestaña **Estado**, pulse **Sistema**.
3. En **Sistema**, pulse el menú **Acciones** y después pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. En la categoría **Entorno**, **URI de IBM Business Glossary**, escriba el siguiente URI: `https://nombre_servidor_igc:número_puerto/ibm/iis/igc/popup/popupSearch.do?exactMatch=1`
Por ejemplo, escriba `https://nombre_servidor_igc:9080/ibm/iis/igc/popup/popupSearch.do?exactMatch=1`
6. Pulse **Aceptar**.

Configuración del URI de descubrimiento de colaboración

Puede configurar IBM Cognos Analytics y IBM Cognos Workspace para utilizar IBM Connections para la toma de decisiones colaborativa. La integración con IBM Connections permite a los usuarios empresariales colaborar durante la creación o la visualización de informes, la realización de análisis o la supervisión de espacios de trabajo. Los usuarios disponen de acceso a las actividades de IBM Connections desde IBM Cognos Workspace y a la página principal de IBM Connections desde IBM Cognos Analytics e IBM Cognos Workspace.

El URI de descubrimiento de colaboración especifica el servidor de IBM Connections que ha de utilizarse como proveedor de colaboración. Cuando se especifica un URI, se añade soporte relacionado con la colaboración a IBM Cognos Analytics tal como se indica a continuación:

- Se añade un enlace a la página de bienvenida del portal de IBM Cognos Analytics. Si el usuario tiene acceso a la página principal de IBM Connections, el

enlace se denomina **Acceder a mi red social** y enlaza al usuario con la página principal. Si el usuario tiene acceso a las actividades de IBM Connections, pero no a la página principal, el enlace se denomina **Mis actividades** y enlaza al usuario con la página de actividades.

- Se añade un enlace con la página principal de IBM Connections al menú Lanzar del portal.
- Se añade un enlace con la página principal de IBM Connections al menú Acciones de IBM Cognos Workspace
- Se añade el botón de menú **Colaborar** en la aplicación del espacio de trabajo en IBM Cognos Workspace. Esto permite al usuario crear o ver una actividad de espacio de trabajo en IBM Connections.

Para acceder a la página principal y a la página de actividades de IBM Connections, el administrador debe habilitar la función **Colaborar**. Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios** para ver la lista de asignadores.
2. En la barra de herramientas, pulse el botón Establecer propiedades - Configuración.
3. Pulse la pestaña **Valores**.
4. Para la categoría **Entorno, URI de descubrimiento de colaboración**, especifique el URI, tal y como se indica a continuación:
`http://nombre_servidor:numero_puerto/activities/serviceconfigs`
Por ejemplo, `http://nombre_servidor:9080/activities/serviceconfigs`
donde *nombre_servidor* representa el nombre del servidor en el que se ha instalado IBM Connections.
5. Pulse **Aceptar**.

Habilitación de métricas de cola de tareas, trabajos y SMTP

De forma predeterminada, sólo está habilitado la métrica de longitud de cola para las métricas de cola de tareas, trabajos y SMTP. Hay otras métricas disponibles para cada uno, pero se establecen en cero y no aparecen en la interfaz de usuario a menos que se habiliten.

- **Marca de agua máxima de tiempo en cola**
- **Marca de agua mínima de tiempo en cola**
- **Tiempo en cola**
- **Número de solicitudes de cola**
- **Marca de agua máxima de longitud de la cola**
- **Marca de límite inferior de longitud de la cola**

Para obtener más información sobre estas métricas, consulte: Capítulo 4, “Métricas de rendimiento del sistema”, en la página 29. Tenga en cuenta que habilitar estos valores puede afectar al rendimiento.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el menú Acciones de **Sistema**, pulse **Establecer propiedades**.
3. Pulse la pestaña **Valores**.
4. En la categoría **Entorno**, situada junto a **Valores avanzados**, pulse el enlace **Editar**.
5. Si aparece, seleccione la casilla de verificación **Reemplazar los valores adquiridos de la entrada padre**. De lo contrario, continúe con el paso siguiente.
6. En la columna **Parámetro**, escriba los siguientes valores:
enable.tide.metrics.smtpqueue, **enable.tide.metrics.jobqueue** y **enable.tide.metrics.taskqueue**.
7. Junto a cada parámetro, en la columna **Valor**, escriba **Verdadero** para habilitar la métrica.
8. Pulse **Aceptar**.
9. Abra el archivo `install_location/webapps/p2pd/WEB-INF/classes/iManage-metadata.xml` en un editor.
Asegúrese de que su editor permita guardar archivos en formato UTF-8.
Para realizar una instalación distribuida, debe editar el archivo `iManage-metadata.xml` en cada sistema, de lo contrario, es posible que las métricas globales aparezcan inicialmente pero dejen de hacerlo cuando navegue fuera de la página.
10. Elimine el comentario de las secciones que empiezan por `<!-- These metrics have been explicitly disabled. Please consult documentation on how to enable them. -->`
11. Guarde el archivo.
12. Con **IBM Cognos Configuration**, detenga y reinicie el software de **IBM Cognos**.
Para obtener información acerca de la detención del software de **IBM Cognos**, consulte la *IBM Cognos Analytics Guía de instalación y configuración*.

Establecimiento de la duración de las tareas humanas y las anotaciones terminadas (comentarios)

Puede establecer la duración de las anotaciones y de las tareas humanas terminadas.

La duración es la cantidad de tiempo transcurrido el cual la entrada asociada se suprime. Por ejemplo, si la duración de una anotación está establecida en 60 días, la anotación se suprime 60 días después de suprimir el informe asociado. Si la duración de una tarea humana está establecida en 120, dicha tarea puede suprimirse 120 días después si se suprimen todos los paneles de control o los informes enlazados.

La duración predeterminada es de 90 días para las tareas humanas terminadas y de 180 para las anotaciones terminadas.

Para obtener más información acerca de las tareas humanas, consulte: Capítulo 25, “Administración de tareas humanas”, en la página 371. Para obtener más información sobre las anotaciones (comentarios), consulte la Guía de usuario de *IBM Cognos Workspace*.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Human Task Service** o **Servicios > Servicio de anotaciones**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones** del servicio, pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. En el caso de las anotaciones, localice el valor **Duración de la anotación terminada**. En el caso de **Servicio de tareas humanas**, encuentre el valor **Duración de la tarea humana terminada**. Establezca la duración en días o en meses y pulse **Aceptar**.

Resultados

Las anotaciones o las tareas humanas terminadas se suprimirán una vez transcurrido el número de días que haya especificado.

Cambiar el comportamiento del filtro de acceso a detalles

Puede cambiar el comportamiento del filtro de acceso a detalles dinámico si desea obtener detalles para generar un filtro mediante la utilización de la clave de empresa de miembro en lugar del título de miembro predeterminado.

Establezca el parámetro `RSVP.DRILL.DynamicFilterUsesBusinessKey` en 0 para utilizar Título de miembro. Establezca éste en 1 para utilizar Clave de empresa.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a la funcionalidad **IBM Cognos Administration**. Consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Informe** o **Servicios > Informe por lotes**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En **Servicio de informe** o **Servicio de informe por lotes**, pulse el menú **Acciones** y pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. Pulse **Editar** junto a **Valores avanzados**.
6. Seleccione **Reemplazar los valores adquiridos de la entrada padre**.
7. En la columna **Parámetro**, escriba `RSVP.DRILL.DynamicFilterUsesBusinessKey`.
8. En la columna **Valor**, escriba el valor asociado a esta configuración.

9. Pulse **Aceptar**.
10. En la página **Establecer propiedades**, pulse **Aceptar**.

Control sobre si los parámetros URL se envían a Content Manager

Para las cuestiones de rendimiento, los parámetros de URL no se incluyen con las consultas a Content Manager.

Sin embargo, es posible que se requieran los parámetros de URL; por ejemplo, para evitar errores de inicio de sesión único con los proveedores de autenticación. Si se necesitan parámetros de URL, puede incluirlos al ajustar **forwardURLParamsToCM** en **true**.

El valor predeterminado de este parámetro es **false**.

Procedimiento

1. En IBM Cognos Administration, pulse en **Configuración > Asignadores y servicios**.
2. Para especificar el valor **forwardURLParamsToCM** para un único asignador, realice lo siguiente:
 - a. En la columna **Nombre**, pulse en un asignador y pulse en **Establecer propiedades**.
 - b. Vaya a **Servicio de presentación**, y pulse en **Establecer propiedades**.
 - c. Pulse en la pestaña **Valores** y, en **Entorno, Valores avanzados**, pulse en **Editar**.
 - d. Pulse **Reemplazar los valores adquiridos de la entrada padre**. Ahora, continúe con el paso 4.
3. Para especificar el parámetro **forwardURLParamsToCM** de forma global, para varios asignadores, realice lo siguiente:
 - a. En la barra de herramientas **Configuración**, pulse en **Establecer propiedades - Configuración**.
 - b. Pulse en la pestaña **Valores** y, en **Entorno, Valores avanzados**, pulse en **Editar**.
4. En el campo **Parámetro**, escriba **forwardURLParamsToCM** y, en el campo **Valor**, escriba **verdadero**.
5. Pulse **Aceptar**.

Impresión desde sistemas operativos UNIX

La propiedad **RSVP.PRINT.POSTSCRIPT** controla cuál interfaz utilizar para imprimir documentos en PDF desde un sistema operativo UNIX. Si desea continuar utilizando la interfaz Adobe Acrobat PDF, establezca el valor de esta propiedad en **falso**.

La propiedad **RSVP.PRINT.POSTSCRIPT** aplica solo para los sistemas operativos UNIX y su valor predeterminado es **verdadero**. Mantener el valor predeterminado proporciona usuarios con la capacidad para imprimir PDF utilizando la interfaz de postscript interna de un sistema operativo UNIX.

Antes de cambiar el valor de la propiedad **RSVP.PRINT.POSTSCRIPT** en **falso**, asegúrese de que ha instalado la última versión de Adobe Acrobat Reader para su sistema operativo.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para **BatchReportService**, en la columna **Parámetro**, escriba **RSVP.PRINT.POSTSCRIPT**.
3. En la columna **Valor**, escriba false.
4. Pulse **Aceptar**.

Añadir los dominios de Cognos Workspace a la lista de dominio válida

Debe utilizar todos los dominios válidos para los URL en los widgets de caja de herramientas en IBM Cognos Workspace. Añada los dominios que utilizarán los usuarios de Cognos Workspace para la lista de dominios válidos.

Procedimiento

1. En IBM Cognos Administration, pulse en **Configuración > Asignadores y servicios**.
2. Pulse el icono **Establecer propiedades** .
3. Abra la pestaña **Valores**.
4. Seleccione **Valores avanzados** y pulse **Editar**.
5. Añada el parámetro **BUXClientValidDomainList**.
6. En la columna **Valor**, añada los dominios en una lista separada por comas.

Cómo evitar el bloqueo del almacén de contenido al añadir o actualizar un gran número de planificaciones

En IBM Cognos Analytics, cuando se añaden o se actualizan muchas planificaciones, la base de datos del almacén de contenido puede bloquearse si las planificaciones contienen datos no válidos. Si experimenta este problema, puede establecer una propiedad avanzada que valide las propiedades de las planificaciones e inhabilite las planificaciones no válidas.

Acerca de esta tarea

Las planificaciones que contienen datos no válidos pueden bloquear la base de datos del almacén de contenido. Por ejemplo, una planificación puede contener credenciales de cuenta de usuario no válidas. Si añade o actualiza planificaciones y la propiedad de credencial hace referencia a credenciales de cuenta de usuario no válidas, Content Manager intenta actualizar las planificaciones no válidas repetidamente sin éxito.

Si la propiedad `emf.schedule.validation.enabled` tiene el valor `true`, se validan las propiedades de planificación tales como la fecha de inicio, la fecha de finalización, los tipos de datos y las credenciales de cuenta de usuario. Las planificaciones no válidas que se encuentren se inhabilitan y los detalles de las planificaciones inhabilitadas se registran en los archivos de registro.

El valor predeterminado de esta propiedad es `false`. Para habilitar la validación de las planificaciones, establezca la propiedad en `true`.

Procedimiento

1. Siga los pasos del tema “Configuración de valores avanzados para servicios específicos” en la página 515.
2. En la lista de servicios de asignador, seleccione **EventManagerService**.
3. En el valor de configuración **Entorno**, en la columna **Valor**, pulse **Editar**.
4. Para añadir el nombre del parámetro, escriba
`emf.schedule.validation.enabled`.
5. Para añadir el valor, escriba `true`.

Capítulo 6. Orígenes de datos y conexiones

Un origen de datos define la conexión física con una base de datos. IBM Cognos Analytics da soporte a varios orígenes de datos relacionales, OLAP y DMR.

En la conexión de origen de datos se especifican los parámetros necesarios para conectarse a la base de datos, por ejemplo, la ubicación de la base de datos y la duración del tiempo de espera. Una conexión de origen de datos puede incluir información de credenciales y de inicio de sesión. Un origen de datos puede tener varias conexiones.

Puede hacer que más de una conexión de origen de datos esté disponible combinándolas, junto con otros elementos, en paquetes creados y publicados con Framework Manager. Para obtener más información sobre cómo crear el paquete, consulte la publicación *IBM Cognos Framework Manager Guía del usuario*. También puede crear y editar paquetes en el software de IBM Cognos para algunos orígenes de datos. Para obtener más información, consulte Capítulo 20, “Paquetes”, en la página 319.

Puede proteger los orígenes de datos mediante la seguridad de IBM Cognos. El software de IBM Cognos también respeta la seguridad definida en el origen de datos. Para obtener más información, consulte: “Protección de orígenes de datos” en la página 172.

Para mover los orígenes de datos de un entorno a otro, despliegue todo el almacén de contenido. Para obtener más información, consulte Capítulo 19, “Despliegue”, en la página 287.

Modo de consulta compatible

Este tipo de proceso de consulta se utiliza en IBM Cognos Analytics versión 10.2.2 y anteriores. Para ejecutar informes que utilizan el modo de consulta compatible, debe utilizar bibliotecas de cliente de origen de datos de 32 bits y configurar el servidor de informes para que sea de 32 bits. El modo de consulta compatible utiliza conexiones ODBC y de cliente nativo para la comunicación con orígenes de datos.

Si el origen de datos es de 64 bits, asegúrese de que utiliza las bibliotecas de cliente de 32 bits para la conexión al origen de datos para utilizar el modo de consulta de compatibilidad.

Modo de consulta dinámica

El modo de consulta dinámica proporciona comunicación con los orígenes de datos mediante conexiones Java o XMLA.

Para bases de datos relacionales soportadas, se requiere una conexión JDBC de tipo 4. Un controlador JDBC de tipo 4 convierte las llamadas JDBC directamente en el protocolo de base de datos específico del proveedor. Está escrito en Java puro y es independiente de la plataforma. En el caso de las bases de datos relacionales, los controladores JDBC se deben copiar en el directorio *ubicación_instalación\drivers* de IBM Cognos Analytics. Para obtener más información, consulte el tema

sobre cómo configurar la conectividad de base de datos para bases de datos de creación de informes en la publicación *IBM Cognos Analytics Guía de instalación y configuración*.

En el caso de los orígenes de datos OLAP soportados, la conectividad XMLA mejora el acceso al proporcionar un MDX personalizado y mejorado para el origen y la versión específicos de la tecnología OLAP y utiliza la inteligencia del origen de datos OLAP.

Para obtener más información, consulte: “Uso de conexiones JDBC para orígenes de datos” en la página 146.

Tipos de orígenes de datos

IBM Cognos Analytics da soporte a muchos tipos diferentes de orígenes de datos, incluidos los orígenes de datos relacionales, OLAP y XML.

La lista de tipos de orígenes de datos soportados puede cambiar de un release a otro. Para obtener información acerca de los orígenes de datos soportados actualmente, consulte el sitio web Entornos de software soportados (www.ibm.com/support/docview.wss?uid=swg27047186). Para obtener información adicional, consulte la lista de Problemas críticos (www.ibm.com/support/docview.wss?uid=swg27047185) que también puede incluir información acerca de los orígenes de datos.

La información de conexión de los orígenes de datos de cada tipo de origen de datos puede ser diferente. Para obtener información acerca de los parámetros que necesita especificar para conectar con su origen de datos, consulte la documentación del proveedor.

Orígenes de datos de IBM Db2

IBM Cognos Analytics da soporte a orígenes de datos de Db2.

Pueden utilizarse conexiones JDBC para conectarse a los sistemas operativos Db2 for Linux, UNIX y Microsoft Windows, y Db2 for z/OS.

Conexiones de base de datos IBM Db2 de confianza

Puede establecer una conexión entre la base de datos IBM Db2 y el software de IBM Cognos en la que varios usuarios se conecten a la base de datos mediante la característica de conexión de confianza con la base de datos.

Un origen de datos que se utilice para conexiones de aplicaciones de confianza debe definir bloques Abrir sesión para cualquier estado de base de datos específico del usuario que deba definirse antes de que se emitan las consultas de los usuarios proxy. El bloque Abrir conexión asociado sólo se ejecuta una vez cuando se intenta establecer la conexión de confianza, mientras que los bloques Abrir sesión se pueden ejecutar muchas veces para usuarios diferentes.

La información que indica que una conexión va a realizar una solicitud en nombre de un usuario, quien tiene autorización para utilizar inicios de sesión proxy, se proporciona a la base de datos utilizando el siguiente bloque de comandos de sesión asociado a la conexión de base de datos de confianza. El valor que se utiliza para la variable de sesión, OCI_ATTR_USERNAME, debe coincidir con el nombre de usuario de Db2.


```

<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>#${account.defaultName}</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>

```

Para obtener información sobre cómo añadir un bloque de comandos para una conexión de origen de datos, consulte: “Añadir bloques de comandos al crear un origen de datos” en la página 166.

Requisitos previos para utilizar las conexiones de confianza

Existen algunos requisitos previos para considerar si tiene previsto utilizar conexiones de confianza.

- Utilice el cliente Db2 versión 9.5 o superior en todas las plataformas.
- Utilice una Db2 Call Level Interface (Db2 CLI) para crear una conexión fiable.
- Debe crear un inicio de sesión para la conexión de origen de datos para especificar las credenciales de Db2 del usuario de Db2 de confianza.
- El contexto de confianza que ha definido en la base de datos Db2 no debe solicitar credenciales para el usuario a través de proxy.

IBM Db2 Parámetros de conexión

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos.

Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 22. Db2 parámetros de conexión

Parámetro	Descripción
Db2 nombre de base de datos	Introduzca el nombre (alias) de la base de datos Db2 que se utilizó al configurar el cliente Db2.
Db2 cadena de conexión	Opcional. Introduzca la pareja nombre/valor de nombre que los distribuidores de Db2 CLI o ODBC pueden aceptar.
Secuencia de ordenación	Introduzca la secuencia de ordenación que se incluirá en la cadena de conexión de base de datos. Las secuencias de ordenación sólo son necesarias en los casos excepcionales en los que puede haber discrepancias de ordenación entre IBM Cognos Analytics y una base de datos. El motor de consulta de Cognos puede detectar determinados tipos de secuencias de ordenación en una base de datos Db2, incluidas 1252-IDENTITY y 1252-UNIQUE. La ordenación entre el procesamiento local y el procesamiento de la base de datos es la misma si la base de datos Db2 tiene establecida una de estas secuencias de ordenación.
Abrir de forma asíncrona	No se utiliza.

Tabla 22. Db2 parámetros de conexión (continuación)

Parámetro	Descripción
Contexto de confianza	Seleccione esta casilla de verificación para permitir que IBM Cognos Analytics intente una conexión de confianza con un servidor Db2 configurado de forma apropiada. Para obtener más información, consulte la documentación de administración Db2. Si selecciona esta casilla de verificación con un cliente o un servidor que no soporte la característica, puede recibir un error de conexión o un error de ejecución de informe.
Tiempos de espera	Especifique el tiempo en segundos en el que desea que la base de datos se conecte o espere respuesta antes de que se agote el tiempo de espera. El rango de entradas válidas es de 0 a 32.767. Para que la base de datos espere de forma indefinida, introduzca cero, que es el valor predeterminado.
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: "Protección de orígenes de datos" en la página 172. Si no es necesaria la autenticación, pulse Sin autenticación. Si se necesita autenticación, pulse Inicios de sesión. Si se necesita un ID de usuario y una contraseña en la cadena de conexión, seleccione la casilla de verificación Identificador de usuario. Si se necesita una contraseña, seleccione la casilla de verificación Contraseña y especifique la contraseña en los cuadros Contraseña y Confirmar contraseña. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, pulse Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

IBM Db2Parámetros de conexión JDBC

Si ha seleccionado la casilla de verificación **Configurar conexión JDBC**, puede especificar parámetros de conexión JDBC al crear un origen de datos.

Para obtener más información, consulte "Conexiones de origen de datos" en la página 146.

Cubos de IBM Cognos

Los cubos de IBM Cognos que se pueden utilizar como orígenes de datos en IBM Cognos Analytics son IBM Cognos Planning Contributor e IBM Cognos PowerCubes.

Si tiene problemas para crear conexiones con orígenes de datos en cubos de Cognos, consulte *IBM Cognos Analytics Guía de resolución de problemas*.

Para obtener más información sobre el modo de conectar datos no publicados (en tiempo real) a IBM Cognos Planning - Contributor, consulte la *Guía de instalación* de IBM Cognos Planning.

IBM Cognos Planning Contributor

IBM Cognos Analytics soporta IBM Cognos Planning Contributor como origen de datos.

Puede utilizar IBM Cognos Analytics para realizar informes y analizar datos de Contributor en tiempo real.

Puede crear un paquete de IBM Cognos Contributor de una de las maneras siguientes:

- Mediante la consola de Contributor Administration, que le permite crear un paquete que contenga todos los cubos de la aplicación. Cuando un usuario abre el paquete en un estudio, se le presentan los metadatos de todos los cubos de la aplicación y puede elegir entre varios cubos para crear informes. Sin embargo, los usuarios pueden correr el riesgo de crear accidentalmente consultas que intenten utilizar valores de más de un cubo, las cuales producirían informes sin datos. Para obtener más información, consulte la publicación *IBM Cognos Planning Contributor Administration Guide*.
- Mediante Framework Manager, que le permite determinar cuántos cubos se exponen en un paquete. De forma predeterminada, se obtiene un cubo en cada paquete. Sin embargo, así se pueden generar un gran número de paquetes, que pueden resultar difíciles de gestionar. Para obtener más información, consulte la publicación *IBM Cognos Framework Manager Guía del usuario*.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 23. Parámetros de conexión de origen de datos de Planning Contributor

Parámetro	Descripción
Espacio de nombres externo	Seleccione el espacio de nombres externo.

IBM Cognos PowerCubes

IBM Cognos Analytics soporta PowerCubes generados por Transformer 7.3 y versiones posteriores.

Puede habilitar un PowerCube para los usuarios finales creando un paquete y publicándolo desde Transformer o Framework Manager. También puede crear paquetes PowerCube en IBM Cognos Analytics (consulte Capítulo 20, “Paquetes”, en la página 319. Se crea una conexión de origen de datos a un PowerCube en Transformer o en Framework Manager mientras se publica el cubo, o en IBM Cognos Administration una vez el cubo se ha publicado.

Los PowerCubes se pueden crear en el sistema operativo Linux y en los entornos de HP-UX Itanium mediante el uso de Transformer. Puede utilizar la seguridad de IBM Cognos con esos tipos de cubos, pero no la seguridad de Series 7. Sin embargo, puede desplegar PowerCubes de Series 7 protegidos en sistemas con Linux y HP-UX Itanium que funcionen como servidores de informes en el entorno de IBM Cognos si el almacén de contenido de Cognos se está ejecutando en un servidor compatible con Series 7.

No se pueden crear cubos en Linux o HP-UX Itanium si se están utilizando archivos de definición de consulta de Impromptu (.iqd) como orígenes de datos, ya que Series 7 IQD Bridge no recibe soporte en estas plataformas.

Tras crearse una conexión con un PowerCube, puede:

- Crear un paquete para un PowerCube; consulte “Creación de un paquete para un PowerCube” en la página 319.
- Desplegar PowerCubes actualizados; consulte “Despliegue de PowerCubes actualizados” en la página 171.

Para obtener más información sobre PowerCubes, consulte la publicación *IBM Cognos Transformer User Guide*.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 24. Parámetros de conexión de origen de datos de PowerCubes

Parámetro	Descripción
Tamaño de la memoria caché de lectura	Nota: El valor predeterminado de este parámetro es de 80 MB. Puede establecer este parámetro en un valor entre 1 MB y 1 GB, según se necesite para lograr un rendimiento óptimo de las consultas. El tamaño óptimo de la memoria caché de lectura puede ser mayor o menor que el valor predeterminado de 80 MB. Esto es lo habitual, puesto que los PowerCubes en producción varían ampliamente en tipo y características de las consultas. Tenga en cuenta que el tamaño de la memoria caché de lectura no influye en el tiempo inicial necesario para abrir un cubo. El perfil típico para el rendimiento de las consultas o el tiempo de procesamiento sigue un modelo, según el cual el rendimiento aumenta con el tamaño de la memoria caché de lectura y posteriormente se estabiliza por encima del valor óptimo. Para determinar la configuración óptima, es recomendable que baje el valor predeterminado en 10 MB (o 5 MB, o 1 MB, dependiendo del nivel de ajuste fino deseado) y que utilice los resultados del rendimiento de las consultas como guía para establecer si son necesarios reducciones o aumentos adicionales. El tamaño óptimo de la memoria caché de lectura cambiará a medida que el cubo crezca y cambie en el entorno de producción. En consecuencia, tendrá que revisar el tamaño óptimo de la memoria caché de lectura cuando se produzcan cambios en el modelo de rendimiento de las consultas del usuario o en las características de PowerCube.

Tabla 24. Parámetros de conexión de origen de datos de PowerCubes (continuación)

Parámetro	Descripción
Ubicación	Si todos los servidores de informes están instalados en sistemas con el sistema operativo Microsoft Windows, especifique la Ubicación en Windows. Si todos los servidores de informes están instalados en sistemas con el sistema operativo UNIX, especifique la Ubicación en Unix o Linux. Escriba la ruta de acceso completa y el nombre de archivo del cubo. Por ejemplo, para un cubo local, escriba C:\cubes\sales_and_marketing.mdc. Para un cubo de red, escriba \\nombre_servidor\cubes\sales_and_marketing.mdc. Nota: Para cubos que residan en sistemas UNIX, especifique la ubicación correcta en UNIX y escriba algunos caracteres en la ubicación en Windows porque la ubicación de Windows no puede estar vacía. Nota: Si los servidores de informes están instalados en sistemas Windows y UNIX, y desea que el servidor de informes ejecute una solicitud para acceder al PowerCube en ambos entornos, especifique las ubicaciones en Windows y UNIX. Para asegurarse de que se devuelvan los mismos datos independientemente del entorno en el que el servidor de informes acceda al cubo, el mismo archivo de cubo debe estar guardado en ambas ubicaciones.
Inicio de sesión	Si utiliza la seguridad de IBM Cognos, pulse Restringir la autenticación de PowerCubes a un único espacio de nombres y seleccione un espacio de nombres de la lista. Si se conecta a un PowerCube protegido con contraseña, pulse Contraseña del cubo y escriba la contraseña en los cuadros Contraseña y Confirmar contraseña. Nota: Seleccione Todos los espacios de nombres aplicables (incluidos PowerCubes no seguros) sólo si migra de Series 7 PowerCubes a IBM Cognos Analytics en el entorno de desarrollo o de prueba. Este valor también se puede utilizar para PowerCubes no seguros en un entorno de producción. Si se necesita una contraseña del cubo, pulse Contraseña del cubo y, a continuación, introduzca la contraseña en los cuadros Contraseña y Confirmar contraseña. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, pulse Crear un inicio de sesión que pueda utilizar el grupo Todos. Para obtener más información, consulte “Protección de orígenes de datos” en la página 172.

Recomendación: uso de PowerCubes en el software de IBM Cognos

Existen algunas recomendaciones si se utilizan PowerCubes en el software de IBM Cognos.

En concreto:

- Al comprobar la migración de PowerCubes Series 7, puede seleccionar la opción de inicio de sesión para autenticar con **Todos los espacios de nombres aplicables**.

Esta opción sólo se utiliza para la migración de espacios de nombres en modelos de Transformer. No cambia el hecho de que no se soporten varios espacios de nombres en un entorno de producción.

- Cuando utilice PowerCubes Series 7 como orígenes de datos, es recomendable que se optimicen para IBM Cognos Analytics.

Los PowerCubes optimizados proporcionan una recuperación de datos más rápida en tiempo de ejecución. Los PowerCubes se optimizan con un programa de utilidad de línea de comandos denominado pcoptimizer que se proporciona con el software de IBM Cognos.

Para obtener más información sobre la optimización de PowerCubes, consulte la publicación *IBM Cognos Analytics Guía de resolución de problemas*.

- Si publica un PowerCube y el cubo contiene vistas personalizadas, deberá estar autenticado en el software de IBM Cognos con un identificador de usuario y una contraseña válidos.

El acceso anónimo no se soporta en esta situación.

Protección de PowerCubes

Los PowerCubes soportados por el software de IBM Cognos pueden protegerse con los espacios de nombres de seguridad de IBM Cognos. La seguridad se puede aplicar a un cubo completo o a las vistas personalizadas. Antes de acceder a un cubo protegido con un espacio de nombres de IBM Cognos, debe iniciar sesión en el espacio de nombres aplicable.

En los entornos de producción, el software de IBM Cognos sólo soporta los PowerCubes protegidos en un espacio de nombres único. Por lo tanto, cuando se despliegan PowerCubes para utilizarlos en un entorno de producción, debe seleccionar la opción de iniciar sesión **Restringir la autenticación de PowerCubes a un único espacio de nombres**.

Nota: En lugar de utilizar la seguridad de IBM Cognos, puede añadir protección con contraseña a un PowerCube o decidir no utilizar seguridad.

Origen de datos Oracle Essbase

Antes de conectarse al origen de datos Oracle Essbase, es necesario realizar algunas configuraciones si el origen de datos utiliza dimensiones de escenario, jerarquías o medidas.

Cuando se configura un origen de datos Oracle Essbase System 9 con un espacio de nombres LDAP, se soporta el inicio de sesión único. El identificador de usuario y la contraseña utilizados para iniciar sesión en el espacio de nombres LDAP se conectan de forma automática al origen de datos. Para obtener más información sobre la configuración de un espacio de nombres LDAP, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 25. Parámetros de origen de datos de Oracle Essbase

Parámetro	Descripción
Nombre de servidor	Especifique el nombre del servidor donde se encuentra la base de datos. En el sistema operativo UNIX, puede ser la dirección TCP/IP del servidor.
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: “Protección de orígenes de datos” en la página 172. Si no es necesaria la autenticación, pulse Sin autenticación. Para Essbase Server System 9 e IBM 8.4, se soporta el inicio de sesión único si su servidor de Essbase está configurado para un espacio de nombres de LDAP. • Seleccione Un espacio de nombres externo y seleccione LDAP en la lista. • El identificador de usuario y la contraseña utilizados para iniciar sesión en el espacio de nombres LDAP se conectan de forma automática al origen de datos. Si es necesario un identificador de usuario y una contraseña en la cadena de conexión, pulse Inicios de sesión. • Si se necesita una contraseña, seleccione la casilla de verificación Contraseña y especifique la contraseña en los cuadros Contraseña y Confirmar contraseña. • Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, pulse Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Configuración de dimensiones de escenario

Si se conecta a un origen de datos Oracle Essbase que contenga una dimensión de escenario, deberá configurar de forma manual la dimensión de escenario para que IBM Cognos Analytics la reconozca. De lo contrario, IBM Cognos Analytics trata la dimensión de escenario como una dimensión regular.

Procedimiento

En Oracle Essbase, asigne un atributo definido por el usuario (UDA) denominado COGNOS_SCENARIO_DIMENSION a la dimensión de escenario.

Especificación de jerarquías equilibradas

El proveedor de Oracle Essbase no determina si una jerarquía está equilibrada o desequilibrada. Considera todas las jerarquías como desequilibradas de forma predeterminada.

En una jerarquía equilibrada, cada ruta desciende a la misma profundidad mientras que las ramas de una jerarquía desequilibrada descienden a niveles diferentes.

Procedimiento

1. En la herramienta Hyperion Solutions Essbase Administration Services, cree un atributo definido por el usuario (UDA) denominado COGNOS_HIERARCHY_BALANCED en la estructura de la base de datos de Essbase. El miembro raíz de la dimensión correspondiente que contiene una jerarquía equilibrada es el que crea el UDA.
2. Establezca el atributo en 1.

Especificación de formatos de medida

Para mejorar la legibilidad de los valores notificados, puede especificar una cadena de formato alternativa para las medidas.

Defina un UDA para los miembros apropiados en la dimensión de cuenta:

COGNOS_FORMAT=*format_string*

El valor *format_string* puede ser cualquier formato numérico predefinido de la tabla siguiente. Puede utilizar un formato numérico preestablecido para que los valores se indiquen en millones (M) o millares (K). Por ejemplo, 1.801.791 puede indicarse como 1,8 M o como 1.801,8 K.

Las cadenas de formato predefinidas son:

Tabla 26. Cadenas predefinidas de orígenes de datos de Oracle Essbase

Opciones de formato	Valor de ejemplo	Ejemplo
General	1000000	1000000
0	1000000	1000000
#,##0	1000000	1,000,000
\$0	1000000	\$1000000
\$\$,##0	1000000	\$1,000,000
0%	1000000	100000000%
%0	1000000	%100000000
0E+000	1000000	1E+006
0K	1000000	1000K
#,##0K	1000000	1,000K

Tabla 26. Cadenas predefinidas de orígenes de datos de Oracle Essbase (continuación)

Opciones de formato	Valor de ejemplo	Ejemplo
K0	1000000	K1000
K#,##0	1000000	K1,000
\$0K	1000000	\$1000K
\$\$,##0K	1000000	\$1,000K
0M	1000000000	1000M
#,##0M	1000000000	1,000M
M0	1000000000	M1000
M#,##0	1000000000	M1,000
\$0M	1000000000	\$1000M
\$\$,##0M	1000000000	\$1,000M

Con la excepción de la cadena de formato General, también puede predefinir que se muestre el número de decimales, utilizando la cadena de formato `format_string ~n`, donde `n` es el número de decimales. Por ejemplo, 1.801.791 puede indicarse como \$1.801.791,00 utilizando la cadena de formato `$$,##0~2`. Si no desea números decimales, finalice la cadena de formato con `~0`.

Si la aplicación cliente utiliza un entorno local diferente, deberá reemplazar los símbolos de moneda (\$), miles (.) y decimales (,) en el valor `format_string` para `COGNOS_FORMAT UDA` con los símbolos regionales correspondientes en vigor para la aplicación cliente.

Si no especifica que se muestre el número de decimales, o si la cadena de formato no coincide con uno de los valores predefinidos (incluidos los símbolos regionales), se utilizará de forma predeterminada la cadena de formato General.

Puede aplicar un formato diferente para cada medida. En la tabla siguiente se muestran algunos ejemplos del modo de aplicar diferentes formateos a medidas diferentes:

Tabla 27. Formatos de origen de datos de Oracle Essbase para medidas

Medida	Formato aplicado
Medidas (dimensión de cuenta)	<code>COGNOS_FORMAT=#,##0</code>
Unidades	<code>COGNOS_FORMAT=#,##K</code>
Costes	<code>COGNOS_FORMAT=\$\$,###</code>
Beneficios	<code>COGNOS_FORMAT=0%</code>

IBM InfoSphere Warehouse Cubing Services

El software de IBM Cognos proporciona ayuda para acceder a la tecnología Cubing Services de IBM InfoSphere Warehouse para la versión 9.5.2 y posteriores. No es necesario instalar componentes de IBM Cognos en el servidor de Cubing Services.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 28. Parámetros de conexión de origen de datos de servicios de cubo de almacén de InfoSphere

Parámetro	Descripción
URL del servidor	Especifique la dirección URL del servidor con el formato <code>http://<nombre_host>:<puerto xmla servidor cube>/IBMXmlAnalysis/</code> o <code>https://<nombre_host>:<puerto xmla servidor cube>/IBMXmlAnalysis/</code>. Un ejemplo de <code><nombre_host>:<puerto xmla servidor cube></code> es <code>wottcub1:80</code>.
Conexión Open SSL	Para utilizar sockets seguros, seleccione esta casilla de verificación. Para utilizar sockets no seguros, no la seleccione. El valor debe ser el mismo que el valor del servidor.
Inicio de sesión	Si se necesita un ID de usuario y una contraseña en la cadena de conexión, seleccione la casilla de verificación Identificador de usuario. Si se necesita una contraseña, seleccione la casilla de verificación Contraseña e introduzca la contraseña en los cuadros Contraseña y confirmar contraseña.

Orígenes de datos Informix

El software de IBM Cognos proporciona soporte para orígenes de datos Informix.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 29. Parámetros de conexión de origen de datos de Informix

Parámetro	Descripción
Nombre de la base de datos Informix	Introduzca el nombre de la base de datos.
Nombre de host	Introduzca el nombre de host.

Tabla 29. Parámetros de conexión de origen de datos de Informix (continuación)

Parámetro	Descripción
Nombre de servidor	Introduzca el nombre de servidor.
Secuencia de ordenación	Introduzca la secuencia de ordenación que se incluirá en la cadena de conexión de base de datos. Las secuencias de ordenación sólo son necesarias en los casos excepcionales en los que puede haber discrepancias de ordenación entre el software de IBM Cognos y una base de datos.
Servicio	Seleccione o introduzca el nombre del servicio que utiliza el servidor de bases de datos remota para las solicitudes entrantes.
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: "Protección de orígenes de datos" en la página 172. Si se necesitan un ID de usuario o una contraseña en la cadena de conexión, seleccione la casilla de verificación Identificador de usuario. Si se necesita una contraseña, seleccione la casilla de verificación Contraseña y especifique la contraseña en los cuadros Contraseña y Confirmar contraseña. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, seleccione Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Orígenes de datos de Microsoft Analysis Services

El software de IBM Cognos soporta conectividad con Microsoft Analysis Services desde una plataforma del sistema operativo Microsoft Windows.

Al instalar Microsoft SQL Server, puede optar por añadir Analysis Services. Para hacer posible la conectividad se necesitan las bibliotecas cliente de Microsoft Pivot Table, que se instalan con los componentes de cliente de Microsoft SQL Server.

Debe instalar una versión coincidente del software de cliente de SQL Server en cada sistema en el que se ejecuten los componentes de nivel de aplicación de IBM Cognos Analytics Server o IBM Cognos Framework Manager.

Debe habilitar el protocolo TCP para Microsoft SQL Server y los componentes de cliente de Microsoft SQL Server.

El servidor de IBM Cognos Analytics soporta tres tipos diferentes de autenticación para los orígenes de datos de Analysis Services:

- “Autenticación mediante inicios de sesión” en la página 127
- “Autenticación mediante credenciales del servicio” en la página 128
- “Autenticación con un espacio de nombres externo” en la página 128

Para conocer algunas consideraciones especiales si va a utilizar Framework Manager, consulte “Consideraciones sobre Framework Manager ” en la página 130, y para obtener información sobre consultas de expresiones multidimensionales (MDX), consulte “Consultas de expresiones multidimensionales (MDX)” en la página 130.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Puede seleccionar los siguientes orígenes de datos:

- Microsoft Analysis Services 2012 (ODBO)
- Microsoft Analysis Services 2014 (ODBO)
- Microsoft Analysis Services 2016 (ODBO)
- Microsoft Analysis Services (HTTP XMLA)

Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 30. Parámetros de conexión de origen de datos de servicios de análisis de Microsoft

Parámetro	Descripción
Nombre de servidor	Nota: Introduzca el nombre del servidor en el que se encuentran las bases de datos.
Instancia con nombre	Introduzca la instancia con nombre si se especificó una durante la instalación. Nota: Este parámetro sólo se aplica a Microsoft Analysis Services 2005 y 2008.
Idioma	Seleccione el idioma. En Microsoft Analysis Services 2005 y 2008, el autor de informes utiliza este entorno local como entorno local de diseño para recuperar metadatos del cubo con el fin de mostrarlos en los informes. Una vez creados los informes, se pueden ejecutar en cualquier entorno local.

Tabla 30. Parámetros de conexión de origen de datos de servicios de análisis de Microsoft (continuación)

Parámetro	Descripción
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: “Protección de orígenes de datos” en la página 172. Para realizar la autenticación con las credenciales de la cuenta de dominio de Windows que ejecuta el servicio IBM Cognos, seleccione Credenciales de servicio del software de IBM Cognos. Para obtener más información, consulte: “Autenticación mediante credenciales del servicio” en la página 128. Para utilizar un espacio de nombres externo, seleccione Un espacio de nombres externo y seleccione un espacio de nombres. Para obtener más información, consulte “Autenticación con un espacio de nombres externo” en la página 128. Cuando modifique un origen de datos existente que utilizaba inicios de sesión anteriormente, suprima los inicios de sesión después de cambiar a un espacio de nombres externo. De lo contrario, tendrán prioridad los inicios de sesión. Para crear un inicio de sesión estático que pueda utilizar cualquier usuario, seleccione Inicios de sesión y Cree un inicio de sesión que pueda utilizar el grupo Todos. Seleccione la casilla de verificación Contraseña e introduzca un Identificador de usuario de un dominio de Windows válido y, a continuación, especifique la contraseña en las casillas Contraseña y Confirmar contraseña. Para obtener más información, consulte “Autenticación mediante inicios de sesión”.

Autenticación mediante inicios de sesión

Cuando desee guardar y mantener las credenciales para autenticarse en los orígenes de datos de Microsoft Analysis Services en el software de IBM Cognos, utilice un inicio de sesión cuando cree el origen de datos. Puede definir un inicio de sesión que puedan utilizar todos los usuarios (predeterminado) o otorgar acceso a usuarios específicos. También puede crear inicios de sesión múltiples y utilizar los permisos para otorgar acceso a usuarios, grupos o roles específicos.

El inicio de sesión guarda las credenciales del dominio de Windows válido, que se utilizan para autenticación en Analysis Services. Se deben especificar en la siguiente sintaxis:

<DOMINIO>\<NOMBRE_USUARIO>

Para Microsoft Analysis Services 2005 y 2008, los usuarios con credenciales deben formar parte del grupo de usuarios OLAP local que existe en el sistema en el que se ejecuta Analysis Services. Este grupo, que se crea al instalar Analysis Services, se llama SQLServerMSASUser\$<NOMBRE_SERVIDOR>\$MSSQLSERVER.

En cada instalación de un componente de nivel de aplicación de IBM Cognos, asegúrese de que el software de IBM Cognos se ejecute como una cuenta incorporada de LocalSystem o de que el software de IBM Cognos se ejecute como una cuenta de dominio válida que a la que se le haya otorgado el privilegio **Actuar como parte del sistema operativo** en la política de seguridad local.

A los usuarios de IBM Cognos se les debe otorgar permiso de lectura y ejecución para ese inicio de sesión.

Autenticación mediante credenciales del servicio

Utilice las credenciales del servicio cuando desee utilizar las credenciales de la cuenta que esté ejecutando el servicio IBM Cognos para autenticarse en Microsoft Analysis Services. Cada conexión a los orígenes de datos de Microsoft Analysis Services utiliza las credenciales del servicio independientemente del usuario que ejecute la solicitud.

Para utilizar las credenciales del servicio, el software de IBM Cognos deberá iniciarse como un servicio de Windows. El servicio debe ejecutarse como un usuario del dominio de Windows válido. Las cuentas incorporadas de LocalSystem o NetworkService no son aplicables. Para obtener más información sobre el modo de iniciar el servicio IBM Cognos bajo una cuenta, consulte la información sobre cómo configurar una cuenta de usuario o una cuenta de servicio de red en la *IBM Cognos Analytics Guía de instalación y configuración*.

La cuenta desde la que se ejecuta el servicio IBM Cognos debe satisfacer los siguientes requisitos:

- La cuenta debe ser miembro del mismo bosque de Active Directory que Analysis Services o debe establecerse la confianza del bosque para configuraciones de bosques cruzados.
- Se debe haber otorgado a la cuenta el privilegio **Iniciar sesión como servicio** en la política de seguridad local de todos los sistemas de Windows que ejecuten los componentes de nivel de aplicación de IBM Cognos.
- En las configuraciones de varios nodos, se debe utilizar la misma cuenta en todos los sistemas que ejecuten componentes de nivel de aplicación de IBM Cognos.
- Para Microsoft Analysis Services 2005 y 2008, se deben haber otorgado a la cuenta de servicio privilegios suficientes en la seguridad de SSAS para adjuntar a los cubos deseados y recuperar los datos.
- Para Microsoft Analysis Services 2005 y 2008, la cuenta debe formar parte del grupo de usuarios OLAP local que existe en el sistema en el que se ejecuta Analysis Services. Este grupo, que se crea al instalar Analysis Services, se llama SQLServerMSASUser\$<NOMBRE_SERVIDOR>\$MSSQLSERVER.

Autenticación con un espacio de nombres externo

Si desea que los usuarios de IBM Cognos accedan a orígenes de datos de Microsoft Analysis Services con sus propias credenciales (autenticación pass-through del

usuario, inicio de sesión), utilice un espacio de nombres externo. Las credenciales que se utilizan para autenticación en Analysis Services se toman del espacio de nombres especificado en el que se haya autenticado previamente el usuario.

Las credenciales proporcionadas por un usuario que ha iniciado sesión en el espacio de nombres se transmiten a Analysis Services. Debido a los métodos de autenticación soportados por Analysis Services, sólo puede seleccionar un espacio de nombres del tipo Microsoft Active Directory.

Dependiendo de cómo se haya autenticado el usuario en el espacio de nombres de Active Directory especificado para la autenticación de espacio de nombres externo, puede disponer de las siguientes configuraciones de inicio de sesión que proporcionan una experiencia de usuario sin problemas:

- Si un usuario se ha autenticado de forma explícita mediante un nombre de usuario de dominio y una contraseña, se puede realizar la autenticación pass-through. Las credenciales de dominio proporcionadas se transmiten a Analysis Services.
- Si un usuario se ha autenticado en el espacio de nombres de Active Directory mediante un inicio de sesión que no esté basado en Kerberos, no se podrá realizar la autenticación pass-through del usuario. Esto se aplica a las configuraciones en las que el espacio de nombres de Active Directory está configurado para el modo de correlación de identidad.

Para configurar la autenticación pass-through del usuario en Analysis Services, asegúrese de que se cumplan las siguientes condiciones:

- Todos los sistemas que ejecutan componentes de nivel de aplicación de IBM Cognos deben ejecutar IBM Cognos Analytics como un servicio de Windows bajo una cuenta de dominio válida o LocalSystem.
- Todos los sistemas que ejecutan el software de IBM Cognos deben tener un sistema operativo Microsoft Windows Server. (Windows XP no soporta la autenticación pass-through.)
- Los sistemas que ejecutan Analysis Services y el software de IBM Cognos deben formar parte del mismo bosque de Active Directory.
- La cuenta de dominio (cuenta de usuario) o la cuenta del sistema (LocalSystem) deben ser de confianza para delegación.
- Todas las cuentas de usuario de Windows que requieran acceso a Analysis Services a través del software de IBM Cognos no deben tener activada la propiedad **La cuenta es sensible y no se puede delegar**.

Analysis Services está configurado para autenticación Kerberos. Para obtener más información, póngase en contacto con su administrador de Analysis Services.

Para SSAS 2005 y SSAS 2008, las cuentas de Windows de todos los usuarios deben formar parte del grupo de usuarios OLAP local en el sistema en que se esté ejecutando Analysis Services. Este grupo, que se crea al instalar Analysis Services, se llama `SQLServerMSASUser$<NOMBRE_SERVIDOR>$MSSQLSERVER`.

Tenga en cuenta que existe un problema de Microsoft que repercute negativamente en la autenticación pass-through del usuario cuando Analysis Services y los clientes que acceden a él se ejecutan en sistemas operativos que utilizan AES (Windows 2008, Microsoft Vista, Windows 7). Para obtener más información, consulte la documentación de Microsoft.

Tenga en cuenta que no se puede probar un origen de datos que esté configurado para autenticación de espacios de nombres externos. Para comprobar que funciona, acceda al origen de datos mediante una consulta.

Consideraciones sobre Framework Manager

IBM Cognos Framework Manager accede directamente a los orígenes de datos de Analysis Services sin utilizar los servicios de informes o metadatos. Esto tiene unas implicaciones importantes, especialmente en las configuraciones con autenticación pass-through del usuario para Analysis Services.

Si el inicio de sesión basado en Kerberos está habilitado para el espacio de nombres de Active Directory que se ha configurado, como un origen de autenticación de espacios de nombres externos para el origen de datos de Analysis Services, asegúrese de que los usuarios que ejecuten Framework Manager cumplan el siguiente criterio:

- Tener establecido el privilegio **Actuar como parte del sistema operativo** en la política de seguridad local del sistema que ejecute Framework Manager o ser miembro del grupo Administradores locales del sistema de Framework Manager con el privilegio **Iniciar sesión localmente**.
- Ser de confianza para delegación.

Consultas de expresiones multidimensionales (MDX)

Para realizar consultas de MDX, debe instalar los siguientes componentes de Microsoft Office para las funciones de Microsoft Excel Visual Basic for Applications (VBA), tales como ROUNDDOWN:

- Office Excel
- Microsoft Visual Basic for Applications (una característica compartida en Office)

Instale esos componentes en el servidor de IBM Cognos para MSAS y en el sistema servidor de Analysis Services para SSAS 2005 o SSAS 2008 y, a continuación, reinicie la máquina servidor.

Orígenes de datos de Microsoft SQL Server

El software de IBM Cognos soporta los siguientes tipos de orígenes de datos de Microsoft SQL Server: ODBC, cliente nativo de SQL 2012 y cliente nativo de SQL 2014.

En función de los tipos de orígenes de datos de Microsoft SQL Server que utilice, deberá tener en cuenta algunas consideraciones al definir determinados tipos de autenticación.

Autenticación con las credenciales del servicio IBM Cognos

No debe utilizar una cuenta del sistema local de Microsoft Windows para iniciar sesión en el servidor de IBM Cognos con un origen de datos de Microsoft SQL Server OLE DB.

Autenticación con un espacio de nombres externo

Puede configurar el software de IBM Cognos para que utilice un espacio de nombres de Microsoft Active Directory, en el que se soliciten a los usuarios credenciales como parte del proceso de inicio de sesión de IBM Cognos. Puede

configurar el software de IBM Cognos para que utilice estas mismas credenciales de forma automática al acceder al origen de datos de Microsoft SQL Server. La conexión de origen de datos de Microsoft SQL Server debe estar configurada para **Un espacio de nombres externo** y ese espacio de nombres debe ser el espacio de nombres de Active Directory.

Puede configurar el software de IBM Cognos para que utilice un espacio de nombres de Microsoft Active Directory y autentique a los usuarios para el software de IBM Cognos mediante delegación y autenticación Kerberos. Puede configurar el software de IBM Cognos para que autentique de forma automática a los usuarios al acceder al origen de datos de Microsoft SQL Server. Se necesita la configuración siguiente:

- La pasarela de IBM Cognos debe estar instalada en un servidor web de IIS que esté configurado para la autenticación integrada de Windows.
- Content Manager, el servidor de informes (Componentes de nivel de aplicación), el servidor web de IIS y el servidor de origen de datos (Microsoft SQL Server) deben pertenecer al mismo dominio de Active Directory.
- La conexión de origen de datos de Microsoft SQL Server debe estar configurada para **Un espacio de nombres externo** y ese espacio de nombres debe ser el espacio de nombres de Active Directory.
- Los servidores de informes son de confianza para delegación.

Restricción: Si utiliza la autenticación de Kerberos para un solo inicio de sesión, cada fuente de datos solo puede tener una conexión. Para múltiples conexiones al SQL Server con un solo inicio de sesión habilitado, debe crear múltiples fuentes de datos o una conexión para cada fuente de datos.

Para obtener más información acerca de las opciones de instalación para la pasarela y Content Manager, así como sobre el modo de configurar el espacio de nombres y delegar confianza, consulte la publicación *Guía de instalación y configuración*.

Parámetros de conexión de Microsoft SQL Server

Los siguientes parámetros se utilizan en los orígenes de datos de Microsoft SQL Server.

Tabla 31. Parámetros de conexión de Microsoft SQL Server

Parámetro	Descripción
Nombre de servidor	Introduzca el nombre de servidor. Si hay varias instancias de Microsoft SQL Server, especifique <i>nombre_servidor\nombre_instancia</i> .
Nombre de base de datos	Introduzca el nombre de la base de datos.
Nombre de la aplicación	Introduzca el nombre de la aplicación.
Secuencia de ordenación	Introduzca la secuencia de ordenación que se incluirá en la cadena de conexión de base de datos. Las secuencias de ordenación sólo son necesarias en los casos excepcionales en los que puede haber discrepancias de ordenación entre el software de IBM Cognos y una base de datos.

Tabla 31. Parámetros de conexión de Microsoft SQL Server (continuación)

Parámetro	Descripción
Conexión MARS	Seleccione la conexión MARS (Multiple Active Results Set). Este parámetro sólo se usa en Microsoft SQL Server (Cliente nativo SQL 2005 o superior). Pulse Sí para permitir que las aplicaciones dispongan de más de una solicitud pendiente por conexión y más de un conjunto de resultados predeterminado activo por conexión.
Parámetros de conexión opcionales	Introduzca un tipo opcional de valor de clave de un parámetro utilizando la siguiente sintaxis: <i>param1=value1</i>. Los distintos parámetros deben delimitarse con punto y coma, como se muestra en el siguiente ejemplo: <i>param1=value1;param2=value2</i> Todo lo que escriba para este parámetro se agrega a la parte de base de datos de la cadena de conexión. Consejo: La primera aparición del carácter @ separa la parte de base de datos de la cadena de conexión y la parte de IBM Cognos de la cadena de conexión, excepto si el carácter @ forma una parte de la ID de usuario o la contraseña. Esta no es aplicable para el modo de consulta dinámica.
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: "Protección de orígenes de datos" en la página 172. Si no es necesaria la autenticación, seleccione Sin autenticación. Para obtener más información sobre IBM Cognos Analytics, consulte el manual "Autenticación con las credenciales del servicio IBM Cognos" en la página 130. Si utiliza un espacio de nombres de Microsoft Active Directory y desea soportar el inicio de sesión único, seleccione Un espacio de nombres externo, y seleccione el espacio de nombres de Active Directory. Para obtener más información, consulte "Autenticación con un espacio de nombres externo" en la página 130. Si se necesita autenticación, seleccione Inicios de sesión. Si se necesita un ID de usuario y una contraseña en la cadena de conexión, seleccione la casilla de verificación Identificador de usuario. Si se necesita una contraseña, seleccione la casilla de verificación Contraseña y especifique la contraseña en los cuadros Contraseña y Confirmar contraseña.

Puede incluir comandos de base de datos en la información de conexión de este tipo de origen de datos. Para obtener más información, consulte "Transferencia de contexto de IBM Cognos a una base de datos" en la página 160.

Para obtener más información sobre los parámetros de conexión de Microsoft SQL Server (ODBC), consulte “Conexiones con orígenes de datos ODBC”.

Conexiones con orígenes de datos ODBC

El software de IBM Cognos soporta orígenes de datos ODBC.

El software de IBM Cognos divide las conexiones ODBC en dos categorías: conexiones de orígenes de datos ODBC específicas de proveedor, que utilizan prestaciones específicas de controlador para la creación de consultas y conexiones de orígenes de datos ODBC genéricas, que utilizan prestaciones generales.

El software de IBM Cognos soporta los orígenes de datos ODBC enumerados en la tabla siguiente. El código de base de datos aparece en la cadena de conexión, pero no se puede editar.

Tabla 32. Orígenes de datos ODBC y código de base de datos

Origen de datos ODBC	Código de base de datos
ODBC	OD
Microsoft SQL Server (ODBC)	SS
Netezza (ODBC)	NZ
Sybase IQ (ODBC)	IQ
Teradata (ODBC)	HF

Cualquier conexión de origen de datos ODBC no indicada se creará mediante el origen de datos ODBC genérico, código de base de datos OD.

Parámetros de conexión de ODBC

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos.

Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 33. Parámetros de conexión de ODBC

Parámetro	Descripción
Origen de datos ODBC	Introduzca el nombre del origen de datos (DSN) según se define en el archivo ODBC.ini. Para obtener más información sobre el archivo ODBC.ini, consulte la publicación IBM Cognos Analytics <i>Guía de instalación y configuración</i>.

Tabla 33. Parámetros de conexión de ODBC (continuación)

Parámetro	Descripción
Cadena de conexión ODBC	Introduzca cualquier texto que deba añadirse a la cadena de conexión. Este parámetro se suele dejar en blanco.
Secuencia de ordenación	Introduzca la secuencia de ordenación que se incluirá en la cadena de conexión de base de datos. Las secuencias de ordenación sólo son necesarias en los casos excepcionales en los que puede haber discrepancias de ordenación entre el software de IBM Cognos y una base de datos.
Abrir de forma asíncrona	Seleccione la opción si desea que la conexión procese las solicitudes de forma independiente entre sí. No la seleccione si desea que la conexión termine la solicitud actual antes de empezar otra.
ODBC Unicode	Seleccione la opción si desea que el software de IBM Cognos utilice el estándar de datos Unicode para interpretar los datos. Déjela sin seleccionar si desea que el software de IBM Cognos utilice ANSI para interpretar los datos. Esta selección sólo se aplica a las conexiones de orígenes de datos de Teradata y ODBC genérico.
Tiempos de espera	Especifique el tiempo en segundos en el que desea que la base de datos se conecte o espere respuesta antes de que se agote el tiempo de espera. El rango de entradas válidas es de 0 a 32.767. Para que la base de datos espere de forma indefinida, introduzca cero, que es el valor predeterminado.

Tabla 33. Parámetros de conexión de ODBC (continuación)

Parámetro	Descripción
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: “Protección de orígenes de datos” en la página 172. Para Teradata, Microsoft SQL y ODBC genérico: • Si no es necesaria la autenticación, seleccione Sin autenticación. • Si las credenciales en la base de datos coinciden con las credenciales utilizadas para iniciar sesión en el entorno de IBM Cognos, para un inicio de sesión único, seleccione Un espacio de nombres externo y luego el espacio de nombres apropiado. • Si se necesita autenticación, seleccione Inicios de sesión. Si se necesita una contraseña, seleccione la casilla de verificación Contraseña y especifique la contraseña en los cuadros Contraseña y Confirmar contraseña. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, seleccione Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Orígenes de datos Oracle

El software de IBM Cognos soporta orígenes de datos de Oracle.

Parámetros de conexión de Oracle

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos.

Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 34. Parámetros de conexión de Oracle

Parámetro	Descripción
Cadena de conexión SQL*Net	Escriba el nombre de instancia de la base de datos de Oracle tal como se ha especificado en el archivo tnsnames.ora.

Tabla 34. Parámetros de conexión de Oracle (continuación)

Parámetro	Descripción
Secuencia de ordenación	Introduzca la secuencia de ordenación que se incluirá en la cadena de conexión de base de datos. Las secuencias de ordenación sólo son necesarias en los casos excepcionales en los que puede haber discrepancias de ordenación entre el software de IBM Cognos y una base de datos.
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: “Protección de orígenes de datos” en la página 172. Si se necesita un ID de usuario en la cadena de conexión, escríbalo en el cuadro ID de usuario. Si se necesita una contraseña, seleccione la casilla de verificación Contraseña y especifique la contraseña en los cuadros Contraseña y Confirmar contraseña. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, seleccione Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Conexiones de origen de datos del repositorio externo

El software de IBM Cognos da soporte a conexiones de origen de datos para repositorios informes externos. Puede utilizar la conexión de repositorio de informes para conectarse a un sistema de archivos o a un repositorio IBM FileNet Content Manager.

Debe instalar, configurar y establecer el repositorio de IBM FileNet Content Manager antes de crear una conexión de origen de datos de repositorio externo.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Conexiones de IBM FileNet Content Manager

Utilice la información de la tabla siguiente para especificar los parámetros necesarios para crear una conexión al repositorio IBM FileNet Content Manager.

Para obtener información sobre cómo crear orígenes de datos, consulte: “Creación de una conexión de origen de datos” en la página 147.

Tabla 35. Parámetros de conexión utilizados para conectarse a un repositorio FileNet

Parámetro	Descripción
Tipo de repositorio	Seleccione IBM FileNet Content Manager para conectar con el repositorio externo FileNet.
URL de repositorio de CMIS	Especifique el URL de la ubicación de FileNet utilizando el formato: http://<nombre_servidor>:nombre_puerto/<nombre_CMIS FileNet>/resources/<nombre_almacén objeto_FileNet>/ Por ejemplo: http://server1:9080/fncmis/resources/archive/
Ruta raíz	Escriba la ubicación de la carpeta en la que ha de almacenarse el contenido archivado en FileNet. Esta ubicación ya debe existir en FileNet. Por ejemplo, podría tener una ubicación de carpeta en FileNet denominada repositorio_informes.
Parámetros de conexión de repositorio	Opcionalmente, especifique los parámetros que han de añadirse al URL para el nombre de clase de controlador.
Inicio de sesión	Seleccione la casilla de verificación ID de usuario . Seleccione la casilla de verificación Contraseña . Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, pulse Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Conexiones del sistema de archivos

Puede crear una conexión de origen de datos en un sistema de archivos después de configurar la raíz de alias en IBM Cognos Configuration. La raíz de alias apunta a una ubicación de archivo en una unidad local o una unidad compartida de red.

Utilice la información de la tabla siguiente para especificar los parámetros necesarios al crear una conexión de origen de datos en el repositorio del sistema de archivos.

Tabla 36. Parámetros de conexión utilizados para conectarse a un repositorio de sistema de archivos

Parámetro	Descripción
Raíz del sistema de archivos de repositorio	Seleccione la raíz de alias.
Ruta raíz	Este es un parámetro opcional, que es una subcarpeta de la raíz de alias. Para especificar la ruta raíz, especifique la ubicación de la subcarpeta para almacenar el contenido archivado en la ubicación del sistema de archivos. Esta ubicación ya debe existir. Por ejemplo, /sales.
Parámetros de conexión de repositorio	Opcionalmente, especifique los parámetros que han de añadirse al URL para el nombre de clase de controlador.

Orígenes de datos SAP Business Information Warehouse (SAP BW)

El software de IBM Cognos soporta el acceso a orígenes de datos SAP BW.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146. Los tipos de parámetro que especifique serán diferentes en función del tipo de inicio de sesión en SAP BW que escoja:

- Tipo de inicio de sesión Servidor de aplicaciones
- Tipo de inicio de sesión Destino
- Tipo de inicio de sesión Servidor de Mensajería

Parámetros de conexión del tipo de inicio de sesión Servidor de aplicaciones

Si selecciona **Servidor de aplicaciones** para **Tipo de inicio de sesión de SAP**, especifique los parámetros de la tabla siguiente.

Tabla 37. Parámetros de conexión de tipo de inicio de sesión en el servidor de aplicaciones

Parámetro	Descripción
Servidor de aplicaciones	Escriba el nombre del servidor de aplicaciones SAP. Para obtener más información, consulte a su administrador del sistema SAP.
Número del sistema	Introduzca el número del sistema. Para obtener más información, consulte a su administrador del sistema SAP.
Número de cliente	Introduzca el número del cliente. Para obtener más información, consulte a su administrador del sistema SAP.
Página de códigos del servidor SAP	Seleccione la página de códigos del servidor SAP. El software de IBM Cognos sigue las reglas de internacionalización de SAP, ofreciendo una aplicación compatible que soporta varias secuencias de comandos e idiomas sin modificar SAP BW en el software de IBM Cognos. Para obtener más información, consulte a su administrador del sistema SAP.
Cadena del direccionador SAP	Escriba la cadena del direccionador SAP. La cadena del direccionador describe las estaciones de una conexión necesarias entre dos hosts. Para obtener más información, consulte a su administrador del sistema SAP.

Tabla 37. Parámetros de conexión de tipo de inicio de sesión en el servidor de aplicaciones (continuación)

Parámetro	Descripción
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: “Protección de orígenes de datos” en la página 172. Si se configura un espacio de nombres de inicio de sesión de confianza mediante IBM Cognos Configuration, puede seleccionar Un espacio de nombres externo y seleccionar el espacio de nombres que desea utilizar. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, seleccione Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Parámetros de conexión del tipo de inicio de sesión Destino

Si selecciona **Destino** para **Tipo de inicio de sesión SAP**, especifique los parámetros de la tabla siguiente.

Tabla 38. Parámetros de conexión de tipo de inicio de sesión de destino

Parámetro	Descripción
Número de cliente	Introduzca el número del cliente. Para obtener más información, consulte a su administrador del sistema SAP.
Página de códigos del servidor SAP	Seleccione la página de códigos del servidor SAP. El software de IBM Cognos sigue las reglas de internacionalización de SAP, ofreciendo una aplicación compatible que soporta varias secuencias de comandos e idiomas sin modificar SAP BW en el software de IBM Cognos. Para obtener más información, consulte a su administrador del sistema SAP.

Tabla 38. Parámetros de conexión de tipo de inicio de sesión de destino (continuación)

Parámetro	Descripción
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: “Protección de orígenes de datos” en la página 172. Si se configura un espacio de nombres de inicio de sesión de confianza mediante IBM Cognos Configuration, puede seleccionar Un espacio de nombres externo y seleccionar el espacio de nombres que desea utilizar. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, seleccione Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Parámetros de conexión del tipo de inicio de sesión Servidor de Mensajería

Si selecciona **Servidor de Mensajería** para **Tipo de inicio de sesión de SAP**, especifique los parámetros de la tabla siguiente.

Tabla 39. Parámetros de conexión de tipo de inicio de sesión en Message Server

Parámetro	Descripción
Identificador del sistema	Escriba el identificador del sistema SAP al que desea conectarse. Para obtener más información, consulte a su administrador del sistema SAP.
Grupo de inicio de sesión	Especifique el grupo de SAP. Para obtener más información, consulte a su administrador del sistema SAP.
Número de cliente	Introduzca el número del cliente. Para obtener más información, consulte a su administrador del sistema SAP.

Tabla 39. Parámetros de conexión de tipo de inicio de sesión en Message Server (continuación)

Parámetro	Descripción
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: “Protección de orígenes de datos” en la página 172. Si se configura un espacio de nombres de inicio de sesión de confianza mediante IBM Cognos Configuration, puede seleccionar Un espacio de nombres externo y seleccionar el espacio de nombres que desea utilizar. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, seleccione Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Orígenes de datos de Sybase Adaptive Server Enterprise

El software de IBM Cognos soporta Sybase Adaptive Server Enterprise CT-15.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos.

Tabla 40. Parámetros de orígenes de datos de Sybase Adaptive Server Enterprise

Parámetro	Descripción
Nombre de servidor	Introduzca el nombre del servidor.
Nombre de base de datos	Introduzca el nombre de la base de datos. Selecione Maestro si desea que el servidor Sybase determine la base de datos predeterminada. Para reemplazar la predeterminada, introduzca un nombre de base de datos válido.
Nombre de la aplicación	Introduzca el nombre de la aplicación. Si deja este campo en blanco, el valor predeterminado será el nombre del ejecutable de Cognos, por ejemplo, BiBustksrvermain o DataBuild.
Secuencia de ordenación	Introduzca la secuencia de ordenación que se incluirá en la cadena de conexión de base de datos. Las secuencias de ordenación sólo son necesarias en los casos excepcionales en los que puede haber discrepancias de ordenación entre el software de IBM Cognos y una base de datos.

Tabla 40. Parámetros de orígenes de datos de Sybase Adaptive Server Enterprise (continuación)

Parámetro	Descripción
Tamaño del paquete	Introduzca el tamaño del paquete. El valor predeterminado es 2048. Aumente el tamaño del paquete para reducir el número de paquetes que deben enviarse. Disminuya el tamaño del paquete si un tamaño de paquete más grande supone un problema. El tamaño que puede solicitar no puede ser mayor que lo que permite el servidor Sybase. Póngase en contacto con el administrador de la base de datos para obtener más información.
Nivel asíncrono	Seleccione el nivel asíncrono.
Intervalo del sondeo	Introduzca el intervalo del sondeo. El valor predeterminado es 100.
Tiempos de espera	Especifique el tiempo en segundos en el que desea que la base de datos se conecte o espere respuesta antes de que se agote el tiempo de espera. El rango de entradas válidas es de 0 a 32.767. Para que la base de datos espere de forma indefinida, introduzca cero, que es el valor predeterminado.
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte “Inicios de sesión de orígenes de datos” en la página 156. Si se necesitan un ID de usuario o una contraseña en la cadena de conexión, seleccione la casilla de verificación Identificador de usuario. Si se necesita una contraseña, seleccione la casilla de verificación Contraseña y especifique la contraseña en los cuadros Contraseña y Confirmar contraseña. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, seleccione Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Orígenes de datos de TM1

El software de IBM Cognos proporciona ayuda para acceder a servidores y cubos de TM1.

Debe instalar el cliente de TM1 en el mismo sistema en el que esté instalado IBM Cognos Analytics. Cuando cree una conexión de origen de datos de TM1, tenga en cuenta cómo le gustaría configurar la autenticación.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 41. Parámetros de origen de datos de TM1

Parámetro	Descripción
Host de administración	Introduzca el nombre de una máquina que la red pueda identificar.
Nombre de servidor	Introduzca el nombre de servidor según se ha configurado en el archivo TM1S.cfg. Para obtener más información, consulte la documentación de TM1.
Inicio de sesión	Para obtener más información sobre el inicio de sesión, consulte: “Protección de orígenes de datos” en la página 172. Si no es necesaria la autenticación, seleccione Sin autenticación. Si se utiliza un espacio de nombres externo, seleccione Un espacio de nombres externo y, a continuación, seleccione el espacio de nombres. Si se necesita autenticación, seleccione Inicios de sesión. Si se necesita un ID de usuario y en la cadena de conexión, seleccione la casilla de verificación Identificador de usuario. Si se necesita una contraseña, seleccione la casilla de verificación Contraseña y especifique la contraseña en los cuadros Contraseña y Confirmar contraseña. Para crear un identificador de usuario y una contraseña que se conecten automáticamente al origen de datos, seleccione Crear un inicio de sesión que pueda utilizar el grupo Todos. Introduzca el Identificador de usuario y la contraseña en los cuadros Contraseña y Confirmar contraseña.

Autenticación

Su elección debe cumplir el requisito de autenticación del servidor de TM1. Por ejemplo, si no crea un identificador de usuario y una contraseña, pero el servidor de TM1 requiere un inicio de sesión, se solicitará al usuario que inicie sesión.

Puede utilizar un espacio de nombres externo (proveedor de servicios de directorio de terceros) como método de autenticación. El servidor de TM1 debe configurarse

para autenticarse con IBM Cognos Analytics. Para obtener más información, consulte la documentación de TM1 sobre Cognos Access Manager Authentication.

Nota: En el modo de seguridad 5 (CAM), TM1 espera un cam_passport de un usuario autenticado. TM1 necesita este cam_passport para la autenticación. Cuando el cam_passport de un usuario no tiene derechos para ver cubos de TM1 detrás de TM1 Server, se produce un error de autenticación.

Resultados inesperados cuando se usa la agregación con orígenes de datos de TM1

Los orígenes de datos de TM1 pueden incluir celdas derivadas de reglas. IBM Cognos Analytics no puede identificar estas celdas derivadas de reglas antes de tiempo, por lo que realizar una agregación en estas celdas puede producir resultados inesperados. Por ejemplo, agregar un conjunto que contiene un valor derivado de reglas puede producir resultados inesperados en Creación de informes y Analysis Studio.

Nota: Las operaciones de agregación explícita (suma, promedio, recuento, mínimo y máximo) no se verán afectadas.

Si utiliza cubos de datos de TM1 con celdas derivadas de reglas en IBM Cognos Analytics, le recomendamos que instale el número de compilación de TM1 9.4.00001.576, que identifica los errores de agregación marcando las celdas de error con guiones (--).

El host de administración debe cumplir todos los requisitos para soportar los orígenes de datos de TM1

La instalación incluye IBM Cognos Analytics y orígenes de datos de TM1. Tras una actualización, o al crear o modificar una conexión con un origen de datos de TM1, puede recibir el siguiente mensaje de error:

COGCQ00223094 - TM1-ERR-0060 el servidor TM1 está configurado con un modo de seguridad no soportado.

Para resolver el problema, cambie el nombre de host de administración por un nombre de dominio completo en el asistente de Conexiones con orígenes de datos.

Orígenes de datos XML

Al crear un origen de datos XML, debe utilizar XML como tipo de conexión y especificar la ubicación del documento XML en la cadena de conexión.

Puede especificar la cadena de conexión para un origen de datos XML como:

- Un URL de HTTP que identifique el almacén de contenido necesario para la conexión al documento XML.

Por ejemplo, `HTTP://xmltestserver.cognos.com/XML/countryregion.xml`.

Asegúrese de crear un alias web para el directorio que contenga el archivo XML y de habilitar el examen de directorios.

- Una ruta de archivo

Un ejemplo de ruta de archivo del sistema operativo Microsoft Windows sería `\\nombreservidor\XML\countryregion.xml`.

Un ejemplo de ruta de archivo del sistema operativo UNIX sería `/nombre montaje/XML/countryregion.xml`.

- Un archivo local

Por ejemplo, C:\XML\countryregion.xml;VALIDATE=ON.

Para acceder a un archivo local, utilice una ruta de archivo que emplee una sintaxis específica de la plataforma.

Para comprobar una cadena de conexión XML, debe escribir el siguiente código al final de la cadena:

```
;VALIDATE=ON
```

El texto de este código no distingue mayúsculas y minúsculas.

Debe especificar los parámetros de conexión al crear un origen de datos o al modificar una conexión de origen de datos. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Tabla 42. Parámetros de origen de datos XML

Parámetro	Descripción
Cadena de conexión	Introduzca la cadena de conexión.

Cadenas de conexión XML con parámetros

En una cadena de conexión URL de HTTP para un origen de datos XML, puede utilizar parámetros para enviar información adicional. Puede incluir una cadena de definición de solicitud en el componente de parámetro.

Si la definición de solicitud está especificada en el informe, se utiliza este valor. De lo contrario, se solicita al usuario que proporcione un valor. La solicitud no recibe soporte para otros tipos de cadenas de conexión.

Un ejemplo de componente URL es `addressing_scheme://ubicación_red/path;parameters?query#fragment_identifier`

Codifique el componente de parámetro con la cadena de definición entre dos conjuntos de signos de interrogación. Una solicitud no puede cruzar un límite de componente.

Un ejemplo de una cadena XML con parámetros es `http://Mi_ubicación_red/Mi_ruta/myxml.asp?countryregionsid=??CanadaPrompt??`

Las cadenas de conexión XML con parámetros tienen estas restricciones:

- Cuando un componente URL es una solicitud, no puede contener otros datos.
- Las solicitudes incluidas en las cadenas de conexión XML no funcionan en Framework Manager. No se pueden importar datos de una cadena de conexión XML con parámetros.
- Al configurar una cadena de conexión XML con parámetros, el botón de prueba no funciona.
- La validación de la especificación de consulta en Creación de informes no funciona si está conectada a una cadena de conexión XML con parámetros.

Conexiones de origen de datos

La conexión de origen de datos especifica los parámetros necesarios para conectarse a una base de datos, como la ubicación de la base de datos y la duración del tiempo de espera. Estos parámetros forman una cadena de conexión para el origen de datos.

Si es un administrador, puede configurar todos los orígenes de datos necesarios antes de que se creen los modelos en Framework Manager para que todas las conexiones estén disponibles en el asistente de Framework Manager Metadata.

Los orígenes de datos se almacenan en el espacio de nombres de **Cognos** y deben tener nombres exclusivos. Por ejemplo, no puede utilizar el mismo nombre para un origen de datos y un grupo.

Uso de conexiones JDBC para orígenes de datos

Para algunas conexiones de origen de datos, puede proporcionar información adicional de conexión de origen de datos de conectividad de base de datos Java (JDBC). La información de conexión de origen de datos JDBC es opcional. Las conexiones con orígenes de datos JDBC son necesarias si los paquetes se publican desde Framework Manager con la opción **Utilizar modo de consulta dinámica** habilitada.

Las cadenas de conexión JDBC para orígenes de datos relacionales tienen el formato siguiente:

```
^User ID:^?Password:;LOCAL;JD;URL=<urlspec>;  
DRIVER_NAME=<driver class name spec>[;CognosProperty=value[;...]]
```

Por ejemplo, la cadena de conexión JDBC para un origen de datos de Microsoft SQL Server podría tener la siguiente apariencia:

```
^UserID:^?Password:;LOCAL;JD-SS;URL=jdbc:sqlserver://sotaimpqc05:1433;  
databaseName=dmsqc1;DRIVER_NAME=com.microsoft.sqlserver.jdbc.SQLServerDriver;  
LOCALSORT=us_us_ASCII;LEVEL=PRIMARY
```

En el caso de las bases de datos relacionales, los controladores JDBC se deben copiar en el directorio *ubicación_instalación\drivers* de Cognos Analytics. Para obtener más información, consulte el tema sobre cómo configurar la conectividad de base de datos para bases de datos de creación de informes en la publicación *IBM Cognos Analytics Guía de instalación y configuración*.

Para obtener más información sobre los valores del servicio de consulta, consulte Capítulo 7, “Administración de Query Service”, en la página 175.

Tenga en cuenta que no se implementan niveles de aislamiento para conexiones JDBC. Puede observar un comportamiento diferente si el nivel de aislamiento que seleccione para la conexión de cliente nativo es diferente del nivel predeterminado utilizado por el controlador JDBC. Para obtener información sobre los valores predeterminados del controlador, consulte la documentación del controlador JDBC.

Para obtener más información sobre los niveles de aislamiento, consulte “Niveles de aislamiento” en la página 158.

Utilización de vías de acceso de red para orígenes de datos basados en archivos

Si tiene una instalación distribuida en varios servidores, se recomienda utilizar rutas de red para todos los orígenes de datos basados en archivos en lugar de rutas locales. De este modo, se asegurará de que los orígenes de datos estén accesibles para los servicios que los necesiten, independientemente de qué servidor necesite los datos.

Al crear una conexión con un origen de datos basado en archivos, como un PowerCube, debe introducir una ruta y un nombre de archivo. Para apuntar al archivo, utilice una ruta local, como C:\cubes\Great Outdoors Company.mdc, o una ruta de red, como \\nombre_servidor\cubes\Great Outdoors Company.mdc.

En una instalación distribuida, en la que los servidores de informes se ejecutan en diferentes sistemas, para utilizar una ruta local es necesario que el archivo y la ruta sean válidos en todos los sistemas en los que se ejecute el servidor de informes. Como alternativa, si utiliza una ruta de red para señalar un archivo, cada servidor de informes señala el mismo archivo en la red sin que el archivo esté disponible localmente. También, para asegurar que el archivo esté siempre disponible, es recomendable que lo guarde en un directorio compartido al que se pueda acceder desde la red.

Si ha instalado componentes de IBM Cognos Analytics en servidores del sistema operativo UNIX, se recomienda que también localice el origen de datos basado en archivo en un servidor UNIX. A continuación, debe utilizar una vía de acceso de UNIX, tal como servername/cubes/Great Outdoors Company.mdc, para acceder al archivo.

Si ha instalado todos los componentes en un solo sistema, puede utilizar rutas locales, pero debe asegurarse de que los servicios que necesiten los datos tengan el acceso apropiado a los archivos de datos del sistema.

Para las instalaciones distribuidas del sistema operativo Microsoft Windows, se recomienda utilizar rutas UNC para directorios compartidos de los orígenes de datos basados en archivos, como los archivos PowerCubes o XML.

Creación de una conexión de origen de datos

La conexión de origen de datos especifica los parámetros necesarios para conectarse a una base de datos, como la ubicación de la base de datos y la duración del tiempo de espera. Estos parámetros forman una cadena de conexión para el origen de datos.

Puede incluir información de autenticación para la base de datos en la conexión de origen de datos mediante la creación de un inicio de sesión. Los usuarios no necesitan introducir información de autenticación de la base de datos cada vez que se utilice la conexión porque la información de autenticación se cifra y se guarda en el servidor. El inicio de sesión producido cuando se crea un origen de datos está disponible para el grupo Todos. Más adelante, se podrá modificar quién puede utilizar el inicio de sesión o crear más inicios de sesión.

Antes de empezar

Debe disponer de permisos de escritura para la carpeta en la que desea guardar el origen de datos y para el espacio de nombres de **Cognos**. También debe tener

permisos de ejecución para la característica protegida **Conexiones con orígenes de datos**. Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Acerca de esta tarea

Las conexiones de orígenes de datos existentes no se pueden editar en Framework Manager.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, seleccione **Conexiones con orígenes de datos**.

Consejo: Para eliminar un origen de datos, seleccione la casilla de verificación para el origen de datos y luego seleccione el botón de supresión.

2. Seleccione el botón **Nuevo origen de datos**.
3. En la página de nombre y descripción, escriba un nombre exclusivo para el origen de datos y, si lo desea, una descripción y una sugerencia y, a continuación, seleccione **Siguiente**.
4. En la página de conexión, en la lista desplegable **Tipo**, seleccione el tipo de origen de datos que desea crear.

La casilla de verificación **Configurar conexión JDBC** se activa para los orígenes de datos relacionales. Si no desea crear una conexión JDBC, desactive la casilla de verificación. Para obtener más información acerca de las conexiones JDBC, consulte “Uso de conexiones JDBC para orígenes de datos” en la página 146.

Si no aparece su origen de datos, pulse **Otro tipo**.

5. Especifique el nivel de aislamiento:
 - Si **Nivel de aislamiento** no aparece, seleccione **Siguiente**.
 - Si **Nivel de aislamiento** también aparece, seleccione la pasarela de objetos predeterminada o especifique un valor y, a continuación, seleccione **Siguiente**.
6. Especifique los parámetros de conexión para el origen de datos.

Para obtener información acerca de los parámetros de conexión del tipo de origen de datos que está usando, pulse el elemento asociado de la lista siguiente:

 - “IBM Cognos Planning Contributor” en la página 117
 - “IBM Cognos PowerCubes” en la página 117
 - “Conexiones con orígenes de datos ODBC” en la página 133
 - “Orígenes de datos de IBM Db2” en la página 114
 - “IBM InfoSphere Warehouse Cubing Services” en la página 124
 - “Orígenes de datos Informix” en la página 124
 - “Orígenes de datos de Microsoft SQL Server” en la página 130
 - “Orígenes de datos de Microsoft Analysis Services” en la página 125
 - “Orígenes de datos Oracle” en la página 135
 - “Orígenes de datos SAP Business Information Warehouse (SAP BW)” en la página 138
 - “Orígenes de datos de Sybase Adaptive Server Enterprise” en la página 141
 - “Orígenes de datos de TM1” en la página 142
 - “Orígenes de datos XML” en la página 144

- “Conexiones de origen de datos del repositorio externo” en la página 136
7. Seleccione **Probar la conexión** y, a continuación, **Probar** para comprobar si los parámetros son correctos.

En la columna **Estado** puede ver si la conexión se ha realizado correctamente. Si no se ha realizado correctamente, seleccione **Cerrar**, vuelva a los pasos anteriores y verifique sus parámetros de conexión. Si se ha realizado correctamente, vaya al paso siguiente.

8. Pulse **Finalizar**.

Si ha seleccionado un origen de datos diferente de IBM Cognos PowerCube o SAP BW, el nuevo origen de datos aparecerá en **Conexiones con orígenes de datos**, en la pestaña **Configuración** que se puede seleccionar cuando se utilice el asistente de metadatos en Framework Manager.

Si ha seleccionado IBM Cognos PowerCube o SAP BW, vaya al paso siguiente.

9. Pulse **Aceptar** para volver a **Conexiones con orígenes de datos**; con algunos orígenes de datos, puede pulsar **Crear un paquete** y en **Aceptar**.

Nota: Ya puede crear un paquete con el nuevo origen de datos, o hacerlo posteriormente. La casilla de verificación **Crear un paquete** solamente está disponible si tiene las características necesarias.

10. **11.0.6** Para que la conexión del origen de datos esté disponible en la nueva interfaz de administración en **Gestionar > Conexiones de servidor de datos**, pulse el botón Establecer propiedades  para la conexión, y en la pestaña **Conexión**, seleccione el recuadro de selección **Permitir modelado basado en web**.

Qué hacer a continuación

Si ha creado un inicio de sesión, ahora puede modificarlo o añadir más inicios de sesión. Para obtener más información, consulte “Inicios de sesión de orígenes de datos” en la página 156. También puede añadir más conexiones; consulte “Inicios de sesión de orígenes de datos” en la página 156.

Parámetros de conexión específicos de Cognos

Puede especificar algunos parámetros opcionales específicos de Cognos para las conexiones JDBC.

Estos parámetros los puede especificar cuando crea o actualiza conexiones JDBC para orígenes de datos en IBM Cognos Administration o IBM Cognos Framework Manager, o cuando crea o actualiza las conexiones del servidor de datos en **Gestionar > Conexiones del servidor de datos** en la interfaz de administración de IBM Cognos Analytics versión 11.0.x.

En los diferentes editores de conexiones, estos parámetros se pueden especificar como **Propiedades de conexión** o **Parámetros de conexión JDBC**.

ibmcognos.fetchBufferSize

Este parámetro se utiliza para establecer el tamaño de captura del controlador JDBC para las conexiones de orígenes de datos en IBM Cognos Analytics.

Cuando el modo de consulta dinámica de IBM Cognos Analytics ejecuta consultas utilizando JDBC, el valor de tamaño de captura que se pasa a un controlador JDBC se calcula de forma dinámica. El soporte de los tamaños de captura depende de los proveedores de base de datos. Los proveedores también deciden qué significa el

tamaño de captura, y cuál es el tamaño de captura cuando se utiliza internamente en el controlador y el servidor. Para obtener más detalles, consulte la documentación de JDBC del proveedor.

El modo de consulta dinámica calcula un valor para una consulta utilizando la fórmula siguiente: `maximum( (bufferSize / 'row-size'), 10)`

El valor predeterminado del tamaño de almacenamiento intermedio es de 100 kilobytes (KB). El tamaño de fila se calcula a partir del tamaño de las columnas proyectadas mediante el conjunto de resultados de una consulta. Las consultas que proyectan columnas de gran precisión o que proyectan muchas columnas utilizan un tamaño de captura más pequeño que las que proyectan un número menor de columnas o columnas con una precisión menor.

Si la recuperación de un conjunto de resultado se puede mejorar de forma importante utilizando un tamaño de almacenamiento intermedio más grande, el administrador puede especificar la propiedad de conexión **`ibmcognos.fetchBufferSize`**. El modo de consulta dinámica ajusta automáticamente el valor, si éste está por debajo de 10 kilobytes o por encima de 10 megabytes.

Si `ibmcognos.fetchBufferSize > 1024 * 10240`, entonces `bufferSize = 1024 * 10240`

Si `ibmcognos.fetchBufferSize < 10240`, entonces `bufferSize = 10240`

No siempre se recomiendan tamaños mayores porque pueden aumentar potencialmente el consumo de memoria por el controlador JDBC y no permitir mejorar el rendimiento. Revise siempre la documentación del proveedor de base de datos y los métodos recomendados, antes de utilizar valores de gran tamaño para la propiedad **`ibmcognos.fetchBufferSize`**.

`ibmcognos.decfloat`

Cuando se especifica este parámetro, la modalidad de consulta dinámica se dirige de modo que utilice un tipo flotante decimal, DECFLOAT 128, que representa con exactitud los valores con una precisión de hasta 34 dígitos. Cuando se detecta una columna con una precisión mayor, se modifica internamente a DECFLOAT y el tipo de datos del modelo o informe se describe como DECIMAL(0,0).

Para habilitar esta característica, especifique el parámetro de conexión **`ibmcognos.decfloat=true`** para la conexión de base de datos que ha de utilizar la modalidad de consulta dinámica. En los modelos existentes, las columnas se deben volver a correlacionar con DECIMAL(0,0), en lugar de con doble.

Para que la modalidad de consulta dinámica lea las filas que devuelve una consulta, el controlador JDBC debe devolver los valores de columnas utilizando un tipo de datos Java específico. En los releases anteriores, una base de datos, tal como ORACLE, podía devolver una columna numérica en la que la precisión hacía que una consulta dinámica utilizara el tipo de datos doble. Cuando los valores devueltos por una consulta tenían una precisión superior a los 16 dígitos, el resultado de la conversión podía ser un valor no preciso.

Por ejemplo, si se ha definido una columna ORACLE como NUMBER (sin indicar la precisión), o si se ha calculado un agregado como SUM que ORACLE ha devuelto como NUMBER, es posible que el valor 1234567890123456789 devuelto se convierta en el valor 1.23456789012345677E18. Los dos valores no son iguales.

Si la base de datos no devuelve valores de gran tamaño, no utilice este parámetro y asegúrese de que los modelos no incluyen columnas con el tipo de datos DECIMAL(0,0). Esto permite a la modalidad de consulta directa utilizar un tipo de datos que requiere menos memoria que el tipo DECFLOAT.

ibmcognos.qualifier_list

Este parámetro se utiliza para eliminar la ambigüedad de los metadatos cuando se ejecutan consultas dinámicas. Asigna una lista de uno o varios calificadores a los orígenes de datos definidos en IBM Cognos Analytics.

Los siguientes ejemplos muestran la sintaxis que se ha de utilizar cuando se especifica el parámetro **ibmcognos.qualifier_list** y los valores que se pueden asignar al mismo:

- **ibmcognos.qualifier_list=CATALOG1.SCHEMA1, CATALOG2.SCHEMA2**
- **ibmcognos.qualifier_list=SCHEMA1, SCHEMA2**
- **ibmcognos.qualifier_list=CATALOG1.SCHEMA1, SCHEMA2**
- **ibmcognos.qualifier_list=CATALOG1, CATALOG2**

Se utiliza un punto en el calificador para separar los componentes catálogo y esquema. Si no está presente un punto y la base de datos da soporte a los esquemas, el valor se trata como un esquema. De lo contrario, el valor se trata como un catálogo, si la base de datos da soporte a catálogos.

El servicio de consultas busca la lista en el orden especificado y utiliza los metadatos de columnas que encuentra para el primer calificador coincidente. Si no se encuentra ninguna coincidencia, se genera un error de metadatos ambiguos.

El administrador debe confirmar que la lista de calificadores proporcionada para este parámetro es idéntica, tanto en orden como en contenido, a cualquier lista de búsqueda que pueda haber definido la sesión de base de datos del usuario. La lista de calificadores solo se aplica cuando la sesión intenta anular la ambigüedad de los metadatos devueltos por un controlador JDBC. Los nombres cualificados de las sentencias SQL reflejan los valores asignados a las propiedades de catálogo o de esquema del origen de datos de paquete utilizado durante la planificación de la consulta.

ibmcognos.authentication

Este parámetro se utiliza para configurar las conexiones de origen de datos cuando se utiliza la autenticación de Kerberos.

Para diferentes tipos de conexiones de orígenes de datos, especifique **ibmcognos.authentication=java_krb5** y, a continuación, añada las propiedades que requiere el controlador JDBC para la autenticación Kerberos, si son necesarias. El ejemplo siguiente muestra cómo especificar este parámetro para algunas conexiones de origen de datos:

- Para las conexiones de teradatos, especifique
ibmcognos.authentication=java_krb5;LOGMECH=KRB5;
- Para las conexiones de SAP-HANA, especifique
ibmcognos.authentication=java_krb5;
- Para las conexiones de Microsoft SQL Server, especifique
ibmcognos.authentication=java_krb5;authenticationScheme=JavaKerberos;

ibmcognos.maxvarcharsize

La consulta dinámica puede utilizar un valor de precisión VARCHAR mayor que el valor predeterminado soportado por la base de datos. Este parámetro se utiliza para reemplazar el valor de precisión VARCHAR predeterminado de base de datos para el modo de consulta dinámica.

Para especificar este parámetro, utilice la sintaxis siguiente, donde N es un valor entero mayor que cero soportado por el proveedor de base de datos:

```
ibmcognos.maxvarcharsize=N
```

El estándar SQL utiliza el tipo de datos CLOB y NCLBO (National Character Large Object) para contener los valores de caracteres elevados. Las diferentes bases de datos dan soporte al tipo de datos CLOB o a sus propias versiones de este tipo con características similares. El tipo de datos CLOB impone varias restricciones en los tipos de construcciones SQL que se pueden utilizar en las consultas. Asimismo, los proveedores de base de datos pueden imponer restricciones adicionales en el modo de manejar las columnas CLOB en las interfaces de cliente, tales como JDBC. Para evitar las restricciones relacionadas con CLOB, el modo de consulta dinámica convierte automáticamente las columnas CLOB en columnas VARCHAR utilizando la función CAST. Como resultado, los primeros N caracteres del tipo CLOB se devuelven como VARCHAR en la consulta dinámica.

Consejo: No se realiza el CAST automático cuando un controlador JDBC describe la columna como VARCHAR y no como CLOB y cuando la referencia de columna está encerrada entre un CAST especificado por el usuario.

Si la longitud de un CLOB de una fila es mayor que los datos de precisión de CAST, se trunca.

En algunos casos, el proveedor de base de datos puede dar soporte a una especificación mayor si se cumplen valores de configuración de base de datos específicos, tales como los valores de tamaño de fila, página o servidor. Si se cumplen estas condiciones previas, se puede especificar un valor mayor en una conexión de servidor de datos. Si no se cumplen las condiciones previas, cuando utiliza un valor mayor que el valor soportado por la base de datos, las sentencias SQL no se ejecutan correctamente. Antes de utilizar valores de VARCHAR mayores, consulte la documentación del proveedor de base de datos y verifique el valor con el administrador de base de datos.

La consulta dinámica utiliza los siguientes valores de precisión VARCHAR para las diferentes bases de datos:

Tabla 43. Valores de precisión VARCHAR en modo de consulta dinámica

Base de datos	Precisión VARCHAR predeterminada
Db2 iSeries	32739
Db2 ZSeries	4096
Db2 LUW	8168
Exasol	2000000
Informix Dynamic Server	255
MariaDB	21845
MemSQL	21845
MySQL	65535

Tabla 43. Valores de precisión VARCHAR en modo de consulta dinámica (continuación)

Base de datos	Precisión VARCHAR predeterminada
Oracle	4000
Pivotal Greenplum	2000000
PostgreSQL	2000000
SAP Hana	5000
SQL Server	varchar(max)
Teradata	32000
Otros proveedores	1024

Si el valor de `ibmcognos.maxvarcharsize` es mayor que el valor máximo de Java (2147483647), o no es un entero, se omite el valor.

Si el valor de `ibmcognos.maxvarcharsize` es inferior al valor predeterminado 1024 y al tamaño de VARCHAR del proveedor, se utiliza el valor más bajo de estos 2 valores, en lugar del valor `ibmcognos.maxvarcharsize`.

Añadir una conexión nueva

Puede crear una conexión nueva para un origen de datos existente.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Conexiones con orígenes de datos**.
2. Pulse el origen de datos en el que quiera añadir una nueva conexión.

Consejo: Para eliminar una conexión de origen de datos, seleccione la casilla de verificación y pulse el botón de supresión.

3. Pulse el botón Nueva conexión .
4. En la página de nombre y descripción, escriba un nombre exclusivo para la conexión y, si lo desea, una descripción y una sugerencia y, a continuación, pulse **Siguiente**.
5. Continúe con los pasos 5 al 10 en “Creación de una conexión de origen de datos” en la página 147.

Resultados

Si ha creado un inicio de sesión, ahora puede modificarlo o añadir más inicios de sesión. Para obtener más información, consulte “Inicios de sesión de orígenes de datos” en la página 156.

Modificación de una conexión existente

Puede añadir nuevas conexiones de orígenes de datos o editar las conexiones existentes.

Puede añadir varias conexiones a un origen de datos existente. Por ejemplo, quiere que un origen de datos tenga dos o más conexiones en la misma base de datos que tengan propiedades diferentes, como valores de tiempo de espera o permisos de acceso diferentes. También puede añadir conexiones al origen de datos que señale a diferentes bases de datos, pero éstas deben contener el mismo esquema.

En el momento de crear una conexión de origen de datos, puede crear un inicio de sesión que el grupo Todos puede utilizar para acceder a la base de datos. Más adelante, se podrá modificar quién puede utilizar este inicio de sesión o crear más inicios de sesión. Por ejemplo, puede controlar el acceso a los datos si se establecen los permisos para cada conexión de origen de datos. Para obtener más información, consulte “Establecimiento de permisos de acceso para una entrada” en la página 220.

Para añadir o modificar una conexión de origen de datos, debe tener acceso a las prestaciones obligatorias a fin de administrar orígenes de datos; consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Si está creando un origen de datos de Oracle, IBM Db2, o Microsoft SQL Server, puede incluir comandos de base de datos en la información de conexión. Para obtener más información, consulte “Transferencia de contexto de IBM Cognos a una base de datos” en la página 160.

Para obtener información acerca del establecimiento del número máximo de conexiones con orígenes de datos disponibles en el servidor de informes, consulte “Cambio de los valores de conexión”.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Conexiones con orígenes de datos**.
2. Pulse el origen de datos en el que quiera modificar la conexión.
3. Pulse el botón Establecer propiedades  correspondiente a la conexión que desea modificar.
4. Pulse la pestaña **Conexión**.
5. Si desea cambiar el tipo de origen de datos, pulse un elemento de la lista desplegable **Tipo**.
6. Pulse el icono Editar  para modificar la cadena de conexión.
7. Continúe con los pasos 5 al 10 en “Creación de una conexión de origen de datos” en la página 147.

Cambio de los valores de conexión

Puede establecer el número máximo de conexiones de origen de datos disponibles, la duración de la retención de conexiones y cómo se reutilizan las conexiones de origen de datos.

Cada instancia del servidor de informes tiene una agrupación de conexiones de base de datos establecidas. Las conexiones se reutilizan para nuevas solicitudes que tengan la misma base de datos, usuario y contraseña. Las entradas permanecen en la agrupación hasta que están inactivas durante un periodo de tiempo de espera y, a continuación, se cierran. Cuando la agrupación está llena, no se añaden más conexiones. lo que provoca un error de solicitud.

Tamaño de agrupación

Especifica el número máximo de conexiones con orígenes de datos disponibles en el servidor de informes.

Tiempo de espera

Especifica el periodo de retención de conexiones. Las conexiones se examinan una vez por minuto y se eliminan las aquellas que hayan estado inactivas durante más tiempo que el valor de tiempo de espera.

Valor predeterminado: 900

Conexiones de datos reutilizables

Las conexiones con orígenes de datos sólo se pueden reutilizar si las credenciales de la base de datos de la conexión coinciden con las de la nueva solicitud. Una nueva solicitud puede reclamar las conexiones con orígenes de datos inactivas. Esto sucede cuando se alcanza el número máximo de conexiones y la nueva solicitud no puede utilizar las conexiones inactivas. En este caso, la conexión inactiva más antigua termina y se crea una nueva conexión.

Cuando se alcanza el número máximo de conexiones y todas están activas, las solicitudes adicionales generan un error. El servidor se debe configurar para garantizar que las solicitudes de informes simultáneas no excedan el tamaño de agrupación de solicitudes.

Para obtener más información sobre las solicitudes del servicio de informes, consulte “Número máximo de procesos y conexiones” en la página 80.

Procedimiento

1. En cada sistema en donde esté instalado IBM Cognos Analytics, abra el archivo *install_location/configuration/CQEConfig.xml.sample* en un editor de texto.

Asegúrese de que su editor permita guardar archivos en formato UTF-8.

2. Busque los parámetros Timeout y PoolSize y edítelos de la siguiente manera:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration company="Cognos" version="#.#"
rendition="###">
  <component name="CQE">
    <section name="DBConnectionPool">
      <!-- Description: Database connection timeout.
      Default is 900 seconds (15minutes) -->
      <entry name="Timeout" value="number_of_seconds"/>
      <!-- -->
      <!-- Description: Database connection pool size. -->
      <!-- Maximum number of connections managed by the report
      server. Default=50 -->
      <entry name="PoolSize" value="number_of_connections"/>
    </section>
  </component>
</configuration>
```

3. Guarde el archivo como CQEConfig.xml en el directorio *install_location/configuration*.

4. Con la configuración de IBM Cognos, detenga y luego reinicie el servicio IBM Cognos.

Para obtener información sobre la detención de servicios, consulte la *IBM Cognos Analytics Guía de instalación y configuración*.

Parámetros de conexión dinámica en las conexiones JDBC

Una conexión JDBC a un origen de datos especifica un conjunto estático de valores que el motor de consultas pasa al controlador JDBC.

En los entornos como Apache Hive o Cloudera Impala pueden utilizarse características como la delegación de identidad, que requiere pasar los valores dinámicos mediante el motor de consultas. Puede especificar variables de sesión en

los campos **JDBC URL** y en **Propiedades de conexión**. Por ejemplo, el campo **JDBC URL** puede incluir el siguiente par de nombre-valor:

```
hive.server2.proxy.user=#$account.defaultName#
```

Cuando el motor de consultas crea una nueva conexión de base de datos, sustituye las variables de sesión por su valor correspondiente. Si no existe una variable de sesión, el nombre de la variable se elimina sin haber especificado ningún valor, lo que puede provocar que el controlador rechace la conexión.

Nota: No pueden utilizarse funciones macro. Solo se pueden usar variables de referencia a sesión.

Inicios de sesión de orígenes de datos

Puede añadir inicios de sesión a las conexiones con orígenes de datos existentes para que los usuarios no necesiten especificar las credenciales de la base de datos cuando ejecuten informes.

Cuando cree un inicio de sesión, especifique los usuarios y los grupos que pueden acceder al inicio de sesión. El identificador de usuario y la contraseña que componen el inicio de sesión deben estar definidos en la base de datos.

Puede modificar un inicio de sesión existente si las credenciales utilizadas para iniciar sesión en la base de datos cambian o si desea cambiar quién puede utilizar el inicio de sesión.

En el caso de las configuraciones de orígenes de datos que requieran que cada usuario disponga de su propio inicio de sesión, la administración puede resultar poco práctica. Para obtener información sobre el modo en que los usuarios pueden administrar sus propias credenciales de origen de datos, consulte “Administración de sus propias credenciales de origen de datos” en la página 224.

Creación de un inicio de sesión

El inicio de sesión de conexión de la fuente de datos se debe definir de manera que el servicio de consultas pueda acceder de forma automática a los datos.

Acerca de esta tarea

Una conexión de origen de datos debe tener al menos un inicio de sesión que el servicio de consulta pueda utilizar para conectarse al origen de datos. Si la conexión de origen de datos tiene dos o más inicios de sesión, uno de los inicios de sesión debe denominarse Cubos dinámicos. Este inicio de sesión será utilizado por el servicio de consulta para conectarse al origen de datos.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Conexiones con orígenes de datos**.
2. Pulse el origen de datos y, a continuación, en la conexión a la que desee añadir un inicio de sesión nuevo.
3. Pulse el botón Nuevo inicio de sesión .
4. En la página de nombre y descripción, escriba un nombre exclusivo para el inicio de sesión de origen de datos y, si lo desea, una descripción y una sugerencia y, a continuación, pulse **Siguiente**.

5. Escriba el **Identificador de usuario** y la **Contraseña** para conectarse a la base de datos y, a continuación, pulse **Siguiente**.
Aparecerá la página **Seleccionar los usuarios**.
6. Para añadir usuarios y grupos que puedan utilizar el inicio de sesión, pulse **Añadir**.
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, grupos o roles.
 - Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
 - Para escribir el nombre de las entradas que desea añadir, pulse **Tipo** y escriba los nombres de grupos, roles o usuarios mediante el siguiente formato, en donde un punto y coma (;) separa cada entrada.
`espacio_nombres/nombre_grupo/nombre_rol;espacio_nombres/nombre_usuario;`
 A continuación se incluye un ejemplo:
`Cognos/Authors;LDAP/scarter;`
7. Pulse el botón de flecha a la derecha y, cuando aparezcan las entradas que desea en el cuadro **Entradas seleccionadas**, pulse **Aceptar**.

Consejo: Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de una lista, seleccione la casilla de verificación en la barra de título correspondiente a la lista **Nombre**. Para hacer visibles las entradas del usuario, pulse **Mostrar usuarios en la lista**.
8. Pulse **Finalizar**.
Debajo de la conexión aparecerá el nuevo inicio de sesión de origen de datos.

Modificación de un inicio de sesión

Puede modificar un inicio de sesión existente.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Conexiones con orígenes de datos**.
2. Pulse el origen de datos y, a continuación, en la conexión para la que desee modificar el inicio de sesión.
Sugerencia: Para eliminar un inicio de sesión, seleccione la casilla de verificación y pulse el botón de supresión.
3. Pulse el botón Establecer propiedades  correspondiente al inicio de sesión que desea modificar.
4. Pulse la pestaña **Inicio de sesión**.
Aparecerá una lista de usuarios y grupos que puedan utilizar el inicio de sesión.
5. Si desea cambiar el identificador de usuario y la contraseña que componen el inicio de sesión, pulse **Editar el inicio de sesión**, escriba las nuevas credenciales y, a continuación, pulse **Aceptar**.
6. Si desea añadir usuarios o grupos a la lista de inicio de sesión, pulse **Añadir** y elija el modo de seleccionar usuarios y grupos:

- Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, grupos o roles.
 - Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
 - Para introducir el nombre de las entradas que desea añadir, pulse **Tipo** e introduzca los nombres de grupos, roles o usuarios mediante el siguiente formato, en donde un punto y coma (;) separa cada entrada.
`espacio_nombres/nombre_grupo;espacio_nombres/
nombre_rol;espacio_nombres/nombre_usuario;`
A continuación se incluye un ejemplo:
Cognos/Authors;LDAP/scarter;
7. Pulse el botón de flecha a la derecha y, cuando aparezcan las entradas que desea en el cuadro **Entradas seleccionadas**, pulse **Aceptar**.
- Consejo:** Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista. Para hacer visibles las entradas del usuario, pulse **Mostrar usuarios en la lista**.
8. Pulse **Aceptar**.

Niveles de aislamiento

Puede especificar niveles de aislamiento para los orígenes de datos.

El nivel de aislamiento especifica cómo se gestionan las transacciones que modifican la base de datos. De forma predeterminada, se utiliza la pasarela de objetos predeterminada. No todos los tipos de bases de datos soportan cada nivel de aislamiento. Algunos proveedores de base de datos utilizan diferentes nombres para los niveles de aislamiento.

Las consultas que sean ejecutadas por informes y análisis están destinadas a ser operaciones de sólo lectura. Las consultas se ejecutan con una unidad de trabajo en el origen de datos como una transacción con un nivel de aislamiento predeterminado o definido por el administrador. Los autores de informes no deben suponer que las consultas que ejecutan procedimientos almacenados confirman todos los datos escritos por el procedimiento. En algunos entornos, los cambios realizados por un procedimiento pueden quedar confirmados por las características de la base de datos. Un procedimiento almacenado marcado con acceso de escritura en Framework Manager confirma los cambios pero sólo se puede usar con Event Studio.

Si necesita ejecutar consultas específicas con distintos niveles de aislamiento, debe definir distintas conexiones de base de datos.

Para los orígenes de datos OLAP, incluido SAP BW, la unidad de trabajo de transacciones es de sólo lectura.

Los siguientes niveles se encuentran en orden creciente de aislamiento:

- Lectura no confirmada
Los cambios efectuados por otras transacciones están disponibles inmediatamente para una transacción.

Tabla 44. Tipos de base de datos de lectura no confirmada y niveles de aislamiento equivalentes

Tipo de base de datos	Nivel de aislamiento equivalente
Oracle	No aplicable
Db2	Lectura no confirmada
Microsoft SQL Server	Lectura no confirmada
Sybase Adaptive Server Enterprise	Lectura no confirmada
Informix	Lectura sucia

- Lectura confirmada

Una transacción puede acceder sólo a filas confirmadas por otras transacciones.

Tabla 45. Tipos de base de datos de lectura confirmada y niveles de aislamiento equivalentes

Tipo de base de datos	Nivel de aislamiento equivalente
Oracle	Lectura confirmada
Db2	Estabilidad del cursor
Microsoft SQL Server	Lectura confirmada
Sybase Adaptive Server Enterprise	Lectura confirmada
Informix	Lectura confirmada

- Estabilidad del cursor

Otras transacciones no pueden actualizar la fila en la que se posiciona una transacción.

Tabla 46. Tipos de base de datos de estabilidad del cursor y niveles de aislamiento equivalentes

Tipo de base de datos	Nivel de aislamiento equivalente
Oracle	No aplicable
Db2	No aplicable
Microsoft SQL Server	No aplicable
Sybase Adaptive Server Enterprise	No aplicable
Informix	Estabilidad del cursor

- Lectura reproducible

Las filas seleccionadas o actualizadas por una transacción no se pueden cambiar por otra transacción hasta que ésta se complete.

Tabla 47. Tipos de base de datos de lectura reproducible y niveles de aislamiento equivalentes

Tipo de base de datos	Nivel de aislamiento equivalente
Oracle	No aplicable
Db2	Estabilidad de lectura
Microsoft SQL Server	Lectura repetible
Sybase Adaptive Server Enterprise	Lectura repetible
Informix	Lectura repetible

- Protección fantasma

Una transacción no puede acceder a las filas insertadas o suprimidas desde el inicio de la transacción.

Tabla 48. Tipos de base de datos de protección fantasma y niveles de aislamiento equivalentes

Tipo de base de datos	Nivel de aislamiento equivalente
Oracle	No aplicable
Db2	No aplicable
Microsoft SQL Server	No aplicable
Sybase Adaptive Server Enterprise	No aplicable
Informix	No aplicable

- **Serializable**

Un conjunto de transacciones ejecutado simultáneamente produce el mismo resultado que si se hubiese efectuado de manera secuencial.

Tabla 49. Tipos de base de datos de serializable y niveles de aislamiento equivalentes

Tipo de base de datos	Nivel de aislamiento equivalente
Oracle	Serializable
Db2	Lectura repetida
Microsoft SQL Server	Serializable
Sybase Adaptive Server Enterprise	Serializable
Informix	No aplicable

Transferencia de contexto de IBM Cognos a una base de datos

Los administradores de base de datos desean conocer detalles sobre las aplicaciones que se conectan a sus sistemas de bases de datos. Esta información puede utilizarse para realizar auditorías, gestionar la carga de trabajo y solucionar problemas.

La información sobre las aplicaciones de IBM Cognos se puede transferir a las bases de datos mediante los bloques de comandos de conexión de origen de datos. Los bloques de comando son compatibles con las siguientes conexiones de origen de datos: ORACLE (OR), IBM Db2 (D2), Teradata (TD), SQL Server (SS) y Netezza (NZ). Para obtener más información, consulte “Bloques de comandos” en la página 161.

En Db2, los atributos de conexión también se pueden utilizar como un método de transferencia de información sobre las aplicaciones Cognos. Para obtener más información, consulte “Uso de atributos de conexión de IBM Db2 CLI para Db2” en la página 167.

El software de IBM Cognos puede proporcionar información sobre sus aplicaciones de elaboración de informes y los usuarios que acceden a las aplicaciones, incluido el conjunto predeterminado de información sobre los usuarios autenticados que se recupera de los proveedores de autenticación. La información se puede ampliar especificando correlaciones de espacios de nombres personalizados en IBM Cognos Configuration. Para obtener más información acerca de las correlaciones, consulte la guía *IBM Cognos Analytics Installation and Configuration Guide*.

Bloques de comandos

Los bloques de comandos de conexión están pensados para cambiar el estado de sesión de una conexión que se abre en un origen de datos. Las sentencias que se pueden utilizar en los bloques de comandos dependen de las sentencias que admitan los proveedores de bases de datos y los permisos del usuario en relación con esas sentencias. Las sentencias de los bloques de comandos se pueden parametrizar utilizando variables de sesión y funciones macro de IBM Cognos.

Los bloques de comandos se ejecutan mientras el software de IBM Cognos abre y cierra conexiones de base de datos o sesiones en conexiones. Puede utilizar bloques de comandos para ejecutar comandos SQL nativos, por ejemplo, para ejecutar un procedimiento almacenado cuando se abre una sesión.

Están disponibles los siguientes tipos de bloque de comandos:

- **Comandos para abrir conexión**
- **Comandos para abrir sesión**
- **Comandos para cerrar sesión**
- **Comandos para cerrar conexión**

Como administrador, debe saber cuándo debe ejecutarse un bloque de comandos para una conexión de base de datos. Se recomienda definir las sentencias de base de datos en un bloque de comandos para abrir sesión. Las conexiones abiertas con bases de datos se ejecutan con menor frecuencia dado que IBM Cognos agrupa y reutiliza las conexiones de base de datos. Utilice bloques de comandos para abrir sesión si el contexto de aplicación de una conexión de base de datos cambia con frecuencia.

Los bloques de comandos no deben incluir variables de sesión o macros de Cognos cuyos valores cambien con frecuencia. Estos tipos de variables de sesión o macros incrementan la frecuencia de ejecución de los bloques de comandos y el número de cachés de orígenes de datos y reducen la reutilización de la caché de los conjuntos de datos.

Cuando cree bloques de comandos, plantéese configurar los siguientes parámetros de conexión de base de datos:

- ¿Cuáles son los valores de la agrupación de conexiones de base de datos especificados para los servidores de informes en el archivo CQEConfig.xml?
- ¿Cuenta la base de datos con unos valores de tiempo de espera de conexión inactiva agresivos?
- ¿Cuenta el motor de consulta con unos valores de tiempo de espera de conexión inactiva agresivos?
- ¿El periodo entre solicitudes es mayor que los valores de tiempo de espera?
- ¿Se ha enrutado alguna solicitud a distintos servidores de informes que deben crear nuevas conexiones?

El diagrama siguiente muestra un ejemplo de la interacción entre los cuatro bloques de comandos. La interacción comienza cuando llega la consulta del usuario 1. Se presupone que no existe una conexión con la base de datos.

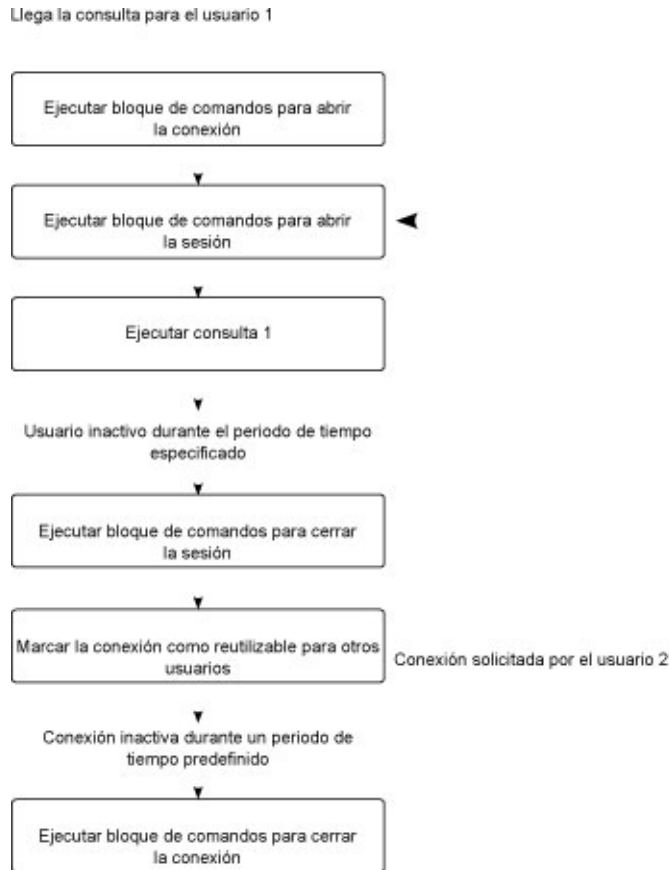


Figura 3. Ejemplo de interacción entre bloques de comandos

Funciones de macro

Las funciones de macro disponibles en el software de IBM Cognos pueden proporcionar información en un bloque de comandos sobre los usuarios y los objetos de aplicaciones de creación de informes, como paquetes, informes o consultas. Todas las funciones de macro pueden devolver valores cuando se les hace referencia en un bloque de comandos, lo que permite que el contexto de aplicación se transmita a la base de datos desde un bloque de comandos. También se pueden utilizar funciones de macro que hacen referencia a mapas de parámetros en un modelo.

Consideraciones

- No se pueden probar los bloques de comandos con conexiones que utilicen el enlace **Probar la conexión** de la página de propiedades de la conexión. Si tiene instalado Software Development Kit, asegúrese de que el código XML se valide en el archivo de esquema `c10_location/webapps/p2pd/WEB-INF/classes/DataSource.xsd`.
- La estructura de los comandos es la misma para todos los orígenes de datos. Sin embargo, los comandos de base de datos específicos pueden variar en función de la base de datos que se utilice. En esta sección, en los ejemplos se utilizan comandos de Oracle y IBM Db2.
- Los comandos en los bloques son específicos de proveedor y deben incluirse en la etiqueta `<sqlCommand>`.
- En función de los valores, puede que el motor de consulta abra nuevas conexiones con mayor rapidez que en una aplicación cargada normalmente, lo

que puede dar la impresión equivocada de que la información se restablece para cada solicitud ejecutada. Para controlar este comportamiento, plantéese utilizar el regulador (DQM) **La caché es sensible a bloques de comandos de conexión**. Para obtener más información, consulte el tema relacionado con los reguladores de Framework Manager para el modo de consultas dinámicas en la publicación *IBM Cognos Framework Manager Guía del usuario*.

Ejemplo: bloque de comandos de apertura de conexión

A continuación se muestra un ejemplo de utilización de un bloque de comandos de apertura de conexión

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql>ALTER SESSION SET NLS_LANGUAGE = FRENCH</sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Ejemplo: bloque de comandos de cierre de conexión

A continuación se muestra un ejemplo de utilización de un bloque de comandos de cierre de conexión para restablecer el idioma en inglés antes de desconectarse de una base de datos Oracle.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql>ALTER SESSION SET NLS_LANGUAGE = ENGLISH</sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Ejemplo: transmisión de información de solicitud

A continuación se muestra un ejemplo de un bloque de comandos para abrir sesión de IBM Db2 que, cuando se ejecuta, genera un conjunto de parámetros que se deben pasar a un procedimiento definido por el usuario.

El ejemplo combina funciones de macro para garantizar que los valores se generan como literales de cadena válidos y concatenaciones de cadena con algunos literales. La variable `modelPath` es un ejemplo de cómo acceder a propiedades de una solicitud procesada al ejecutarse el bloque.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> CALL myproc(#sq($current_timestamp) + ',' +
        sq($machine) + ',' +
        sq(#$modelPath)#) + 'Constant1'')
    </sql>
  </sqlCommand>
</commands>
</commandBlock>
```

Una vez expandida la macro, el administrador de base de datos obtiene la información siguiente sobre la consulta:

```
CALL myproc('2009-05-27 08:13:33.425-05:00','USERCOMPUTERNAME','/content/
package[@name="EAPPS"]'/model[@name="model"], 'Constant1', '')
```

Ejemplo: uso de mapas de parámetros

Este ejemplo de IBM Db2 muestra cómo un administrador de base de datos puede obtener información del modelo.

Un estándar de aplicación podría consistir en definir un mapa de parámetros que aparezca en todos los modelos. El mapa de parámetros define información de contexto sobre la aplicación IBM Cognos. Este enfoque requiere que cualquier aplicación que utilice la conexión deba proporcionar esta información para evitar errores.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> CALL myproc(#sq($APP_INFO{APPNAME}) + ',' +
        sq($APP_INFO{'APPMAJOR'}) + ',' +
        sq($APP_INFO{'APPMINOR'}) + ',' +
        sq($APP_INFO{'APPCONTACT'}) + ', ''Constant1'' '#))
      </sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Una vez expandida la macro, el administrador de base de datos obtiene la información siguiente sobre la consulta:

```
CALL myproc('ApplicationName','10','1','TradingApp@email.com',
'Constant' )
```

Ejemplo: transmisión de detalles del proveedor de autenticación

Este ejemplo de IBM Db2 muestra cómo incluir la información de sesión, cuyo origen es un proveedor de autenticación, en la información transmitida a la base de datos.

El bloque de comandos invoca el procedimiento de Db2 SYSPROC.WLM_SET_CLIENT y transmite los valores obtenidos de las variables de sesión disponibles. Esta información la pueden utilizar los administradores de base de datos al definir reglas de gestión de carga de trabajo en la base de datos que aportan mayor prioridad a grupos de usuarios específicos cuando varios grupos de usuarios comparten una conexión de base de datos.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> CALL SYSPROC.WLM_SET_CLIENT_INFO
        (#$account.personalInfo.userName#,
        'UserComputerName',
        #$account.parameters.var1#, 'ApplicationName', 'AUTOMATIC')
      </sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Ejemplo: utilizar bloques de comandos para conexiones proxy

Si utiliza conexiones proxy, puede emplear una conexión inactiva existente con inicios de sesión para conexiones proxy.

Más de un usuario puede utilizar la conexión física. Se necesitan menos conexiones físicas, ya que las conexiones proxy se ejecutan sobre la conexión física existente.

Para crear una conexión proxy, cree bloques de comandos para abrir sesión en XML.

A continuación se muestra un ejemplo sencillo de un bloque de comandos para abrir sesión que crea una conexión proxy para User1 (Oracle) o cambia a User1 (Db2). Tenga en cuenta que sessionStartCommand solo puede utilizarse con Oracle y Db2.

```

<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>

```

Otro ejemplo es una macro que se puede sustituir si los nombres de usuario de autenticación son equivalentes al identificador de usuario proxy o al usuario de contexto de confianza.

```

<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>#${account.personalInfo.userName}</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>

```

En el siguiente ejemplo se muestra un bloque de comandos para cerrar sesión para una sesión proxy. La conexión proxy actual ha finalizado. Tenga en cuenta que sessionEndCommand finaliza un OCI_session en Oracle y vuelve a cambiar el usuario por el propietario de contexto de confianza para Db2.

```

<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>

```

Ejemplo: utilizar bloques de comandos para bases de datos privadas virtuales de Oracle

Normalmente, Oracle utiliza inicios de sesión para determinar la información de la base de datos a la que pueden acceder los usuarios. Una base de datos privada virtual determina los usuarios que pueden acceder a determinada información, sin que se necesite más información de inicio de sesión.

Cree un bloque de comandos para la conexión mediante el uso de macros que sustituye el usuario que ha iniciado sesión en tiempo de ejecución. Las macros identifican el usuario, de manera que no es necesario que vuelva a introducir la información de inicio de sesión.

Si todos los usuarios que acceden a la base de datos están definidos como usuarios de la base de datos y las cuentas de usuario se utilizan para las conexiones, podrá configurar de forma automática el contexto cuando se establezca la conexión. Por ejemplo, se puede sustituir la macro por el nombre de usuario.

El bloque de comandos XML almacena una serie de comandos que se ejecuta en la secuencia definida. Esto puede incluir los comandos que se describen en Apéndice E, “Esquema para los comandos de orígenes de datos”, en la página 479.

El siguiente ejemplo muestra un bloque de comandos XML para una base de datos privada virtual.

Este bloque de comandos configura un contexto (base de datos privada virtual) en la conexión basada en el parámetro transmitido. El parámetro transmitido se recupera del entorno que se relaciona con el inicio de sesión del usuario en el nivel de portal. Estas variables se pueden modificar en la herramienta de configuración. Sus valores son específicos del usuario y se obtienen mediante el mecanismo de control de seguridad (CAM).

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql>BEGIN PKG_COUNTRY_CONTEXT.SP_SET_COUNTRY1
        (#$account.parameters.var1#);
      END;</sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Este ejemplo muestra la sustitución de parámetros de cuenta. Debe especificar la información de cuenta como propiedades personalizadas. Para obtener información acerca de las propiedades de sesión, consulte la *Guía del usuario* de Framework Manager.

Nota: Los bloques de comandos para las conexiones proxy de Oracle y las bases de datos privadas virtuales en el nivel de origen de datos afectan a todas las conexiones a ese origen de datos.

Añadir bloques de comandos al crear un origen de datos

Puede añadir bloques de comandos cuando cree orígenes de datos.

De forma predeterminada, las conexiones adquieren las propiedades del origen de datos padre. Podrá modificar las conexiones individuales posteriormente.

Procedimiento

1. En la pestaña **Configuración** de Administración de Cognos, comience por crear un origen de datos para una base de datos que admita bloques de comandos.
2. En la página de especificación de comandos, pulse **Establecer** junto a la cadena de comandos que desee especificar.
3. En la página de establecimiento de comandos, añada el código XML del bloque de comandos y, a continuación, pulse **Aceptar**.

Consejo: Para IBM Db2 o Microsoft SQL Server, puede añadir un bloque de comandos solo para abrir una sesión.

4. Siga añadiendo bloques de comandos según sea necesario y haga clic en **Finalizar**.

Añadir o modificar bloques de comandos para una conexión

Puede añadir, modificar o eliminar bloques de comandos para conexiones de orígenes de datos específicas.

Las conexiones adquieren las propiedades del origen de datos padre. Si añade un bloque de comandos de un origen de datos, ese bloque estará disponible para todas las conexiones del origen.

Procedimiento

1. En la pestaña **Configuración** de Administración de Cognos, seleccione una de estas opciones:
 - Acceda a las propiedades de origen de datos si desea modificar los bloques de comandos de todas las conexiones que tiene este origen de datos.
 - Acceda a las propiedades de conexión del origen de datos si desea modificar los bloques de comandos de una conexión.
2. Haga clic en la pestaña **Conexión** y en la sección **Comandos**, realice una de estas tareas:
 - Para añadir el bloque de comandos, haga clic en **Establecer** en uno de los tipos de comando disponibles y pegue el código XML del bloque de comandos en el cuadro **Comandos de base de datos XML**.
 - Para modificar un bloque de comandos, haga clic en **Editar** para el tipo de comando seleccionado y modifique o elimine el código XML del bloque de comandos en el cuadro **Comandos de base de datos XML**.

Puede restablecer los bloques de comandos activando las casillas de verificación **Restablecer valor padre** o **Borrar**.

Consejo: En IBM Db2 o Microsoft SQL Server, puede añadir bloques de comandos solo para abrir una sesión.

3. Siga añadiendo o modificando los bloques de comandos según sea necesario y haga clic en **Finalizar**.

Uso de atributos de conexión de IBM Db2 CLI para Db2

Db2 Call Level Interface (Db2 CLI) es una interfaz SQL invocable de Db2 LUW, Db2 for z/OS y Db2for I). IBM Cognos Analytics puede modificar algunos de los atributos de conexión de Db2 CLI para pasar contexto de aplicación a Db2 en un formato aceptable para los componentes de IBM Optim Integrated Data Management.

Esta información se puede recuperar posteriormente desde registros especiales de Db2 mediante sentencias SQL.

Para habilitar esta funcionalidad, debe modificar un archivo de configuración en cada sistema servidor de informes de IBM Cognos configurado para su entorno de IBM Cognos. Dado que esta funcionalidad se configura a nivel de consulta, la información asociada a los atributos de conexión se actualiza automáticamente cada vez que se ejecuta el informe.

En la lista siguiente se muestran los atributos de conexión de Db2 CLI que IBM Cognos Analytics puede modificar y el tipo de información que dichos atributos pueden transmitir a Db2:

- **SQL_ATTR_INFO_USERID**
Especifica el nombre del usuario que ejecuta un informe.
- **SQL_ATTR_INFO_WRKSTNNAME**
Especifica la dirección del sistema en el que está instalado el navegador del usuario.
- **SQL_ATTR_INFO_APPLNAME**

Especifica el nombre de paquete asociado a la consulta. Si la longitud de la cadena es superior a 32 caracteres, se desborda a \$SLOT2 en la cadena de contabilidad.

- **SQL_ATTR_INFO_ACCTSTR**

Especifica el prefijo o cadena que asocia la solicitud a IBM Cognos Analytics. Los valores son:

Tabla 50. Uso de atributos de conexión de Db2 CLI para Db2

Valor	Descripción
COG	Asocia la solicitud a productos de IBM Cognos en IBM Optim Integrated Data Management.
ccc	Asocia la solicitud a una solución IBM Cognos.
vr	Especifica la versión del producto IBM Cognos
Información de contabilidad adicional	Esta información se divide en los campos siguientes (ranuras): • \$SLOT2 - \$packageName (sección de desbordamiento para \$SLOT1) • \$SLOT3 - \$reportName • \$SLOT4 - \$queryName • \$SLOT5 - \$reportPath Cada ranura cuenta con una longitud fija que acepta cadenas que no contengan más de 46 bytes, con espacios añadidos si es necesario. Dado que las rutas de informes, las rutas de modelos, etc., a menudo son largas, es posible acortar las cadenas para ajustarse a las limitaciones de espacio. Nota: En Db2, los valores transmitidos a la API no pueden contener caracteres de comillas simples, que se convierten en espacios. Si la codificación del juego de caracteres utiliza varios bytes por carácter, el carácter se convierte en "?" para evitar el desbordamiento. Esto es importante cuando se utiliza Unicode y un carácter podría necesitar más de 2 bytes.

Procedimiento

1. Si se conecta a la base de datos con el modo de consulta compatible, realice los siguientes pasos:

- a. En el directorio *install_location/configuration*, haga una copia del archivo *CQEConfig.xml.sample* y cámbiele el nombre a *CQEConfig.xml*.

Consejo: Si se utilizó el archivo *CQEConfig.xml* para otros propósitos, por ejemplo para inhabilitar la memoria caché de una sesión, es posible que exista en el directorio *install_location/configuration*. En ese caso, utilice el archivo *CQEConfig.xml* para realizar los pasos restantes.

- b. Abra el archivo *install_location/configuration/CQEConfig.xml* en un editor.

Asegúrese de que su editor permita guardar archivos en formato UTF-8.

- c. Localice el elemento `<section name="QueryEngine">` y añada la entrada DB2WFM con un valor de 1, como se muestra en el siguiente ejemplo:

```
<section name="QueryEngine">
  <entry name=" DB2WFM" value="1"/>
</section>
```

Para inhabilitar esta funcionalidad, establezca el valor en cero.

2. Si se conecta a la base de datos con la modalidad de consulta dinámica, realice los siguientes pasos:
 - a. En el directorio *install_location/configuration*, realice una copia del archivo *xqe.config.xml* y cámbiele el nombre por *xqe.config.xml.backup*.
 - b. Abra el archivo *install_location/configuration/xqe.config.xml* en un editor.
Asegúrese de que su editor permita guardar archivos en formato UTF-8.
 - c. Localice el elemento `<setConnectionAttributes enabled="false">` y cambie su valor por "true", tal como se muestra en el siguiente ejemplo:
`<setConnectionAttributes enabled="true">`
 Para inhabilitar esta funcionalidad, establezca el valor en "false".
3. Guarde el archivo.
4. Repita los pasos para cada sistema servidor de informes configurado para el entorno IBM Cognos.
5. Reinicie el servicio de IBM Cognos.

Uso de contexto de aplicación en SQL dinámico

Los administradores de servidores de bases de datos pueden registrar y analizar la carga de trabajo de SQL dinámico generada por el software de IBM Cognos.

Como administrador de IBM Cognos, puede definir una cadena personalizada que incluya un contexto de aplicación que se añada entre marcadores de comentario al SQL generado por la aplicación. Puede utilizar literales, macros y variables de sesión, por ejemplo nombres de usuario, nombres de servidor, rutas de acceso completas del informe, etc., para personalizar el comentario generado por el software de Cognos.

El administrador de la base de datos debe comprobar si su cliente de base de datos quita comentarios de las sentencias antes del envío al servidor. Esta opción probablemente puede configurarse; consulte al proveedor del cliente de base de datos.

Al utilizar las variables de sesión aplicables, puede configurar el formato de la cadena para productos y herramientas específicos que pueden extraer comentarios del SQL dinámico. El software de IBM Cognos incluye comentarios en cualquier SQL dinámico generado para un sistema de gestión de base de datos relacional (RDBMS), siempre que el proveedor soporte esta funcionalidad.

Utilice el archivo *CQEConfig.xml.sample* incluido junto con el producto para personalizar las especificaciones de la cadena. La macro de este archivo muestra las entradas predeterminadas que el software de IBM Cognos utiliza para generar los comentarios. No obstante, usted también puede añadir entradas adicionales.

En el siguiente ejemplo se muestran los tipos de variables de sesión que puede especificar en la macro en el archivo *CQEConfig.xml.sample*:

```
<configuration company="Cognos" version="0.1" rendition="cer2">
  <component name="CQE">
    <section name="QueryEngine">
      <entry name="GenerateCommentInNativeSQL" value="1"/>
      <!-- ( default(off)=0, on=1) -->
      <entry name="GenerateCommentInCognosSQL" value="1"/>
      <!-- ( default(off)=0, on=1) -->
      <!-- The content of the comments is controlled with two entries, their
      defaults are specified in the value attribute -->
      <entry name="NativeCommentMacro" value="# 'NC user=' + $account.defaultName
```

```

+ 'report=' + $report + 'start=' + $startTime + 'modelPath=' +
$modelPath + 'reportPath=' + $reportPath + ' queryName=' + $queryName
+ ' REMOTE_ADDR=' + $REMOTE_ADDR + 'HTTP_HOST=' + $HTTP_HOST + 'SERVER_NAME='
+ $SERVER_NAME + ' requestID=' + $requestID + 'sessionID=' + $sessionID
#"/>
<entry name="CognosCommentMacro" value="# 'CC user=' + $account.defaultName
+ 'report=' + $report + 'start=' + $startTime + 'modelPath=' +
$modelPath + 'reportPath=' + $reportPath + ' queryName=' + $queryName
+ ' REMOTE_ADDR=' + $REMOTE_ADDR + 'HTTP_HOST=' + $HTTP_HOST + 'SERVER_NAME='
+ $SERVER_NAME + ' requestID=' + $requestID + 'sessionID=' + $sessionID
#"/>
</section>
</component>
</configuration>

```

En tiempo de ejecución, la macro utilizada en el ejemplo anterior añadiría el siguiente comentario al SQL generado automáticamente, o al SQL nativo:

```

/* CC user=Anonymous report=REPORT1
start=2008-08-28T01:59:35.403Z modelPath=/content/package
[@name='New Package']/model[@name='model']
reportPath=/content/package[@name='New Package']/report[@name='REPORT1']
queryName=Query1 REMOTE_ADDR=127.0.0.1 HTTP_HOST=localhost
SERVER_NAME=localhost
requestID=wq21shM9jGhqdmj9h92Mq1qvdm1hyM1Gq9lyG9sq
sessionID=010:0d159165-745a-11dd-ac9f-b741aeca4631:2789499633
*/
select distinct
    ALL_TIME.CALENDAR_WEEKDAY as CALENDAR_WEEKDAY
from
    EAPPS..EAPPS.ALL_TIME ALL_TIME

```

No toda la información contenida en el comentario generado es significativa en todas las situaciones. La información de identificador de sesión y solicitud proporciona un enlace con el recurso de auditoría, información de rendimiento de perfQFS, y otros rastreos en IBM Cognos. Sin embargo, el nombre de una consulta en un informe y el propio informe pueden ser significativos, por ejemplo, cuando un usuario está realizando un análisis o consulta aleatorios en contraposición a la ejecución de un informe, análisis o consulta guardados.

De forma predeterminada, un usuario anónimo no puede ver todas las variables de sesión en los comentarios generados.

Adición de contexto de aplicación para el modo de consulta dinámica

Para utilizar comentarios en SQL para la modalidad de consulta dinámica puede configurar el archivo xqe.config.xml, ubicado en install_location/configuration.

Se editan los elementos siguientes en el elemento <queryPlanning>.

```

<generateCommentsInNativeSQL enabled="true"/>
<NativeCommentMacro value="#'user=' + $account.defaultName + ' reportPath='
+ $reportPath + ' queryName=' + $queryName + ' REMOTE_ADDR=' + $REMOTE_ADDR
+ ' SERVER_NAME=' + $SERVER_NAME + ' requestID=' + $requestID#"/>

```

Cómo añadir contexto de aplicación a SQL dinámico

Los administradores de servidores de bases de datos pueden configurar el archivo CQEConfig.xml.sample para registrar y analizar la carga de trabajo SQL dinámica generada por el software IBM Cognos. Para el modo de consulta dinámica, los administradores configuran el archivo xqe.config.xml.

Procedimiento

1. En el directorio *install_location/configuration*, haga una copia del archivo CQEConfig.xml.sample y cámbiele el nombre a CQEConfig.xml.

Consejo: Si el archivo CQEConfig.xml se ha utilizado para otros fines, por ejemplo para inhabilitar la memoria caché de una sesión, es posible que exista ya en el directorio *install_location/configuration*. En ese caso, utilice el archivo CQEConfig.xml para realizar los pasos restantes.

2. Abra el archivo *install_location/configuration/CQEConfig.xml* en un editor. Asegúrese de que su editor permita guardar archivos en formato UTF-8.
3. Localice y elimine el comentario de las líneas de código que empiezan por:
entry name="GenerateCommentInNativeSQL"...
entry name="GenerateCommentInCognosSQL"...
entry name="NativeCommentMacro"...
entry name="CognosCommentMacro"...
4. Si lo desea, puede modificar NativeCommentMacro y CognosCommentMacro especificando los valores de parámetros necesarios y eliminando los parámetros que no necesite.
Si deja un valor de parámetro vacío, el parámetro no aparecerá en el comentario generado.
5. Guarde el archivo CQEConfig.xml.
6. Reinicie el servicio de IBM Cognos.

Despliegue de PowerCubes actualizados

Después de reconstruir o actualizar un PowerCube, puede utilizar varios métodos para desplegar el cubo en el entorno de producción.

Para desplegar un IBM Cognos Transformer PowerCube actualizado, utilice el método de copiar y activar en IBM Cognos Transformer (el método recomendado), o el PowerCube usted mismo y utilice el programa de utilidad de línea de comandos pactivate.

Para desplegar un PowerCube de Series 7 Transformer actualizado, debe copiar primero el PowerCube. A continuación, use el programa de utilidad de línea de comandos pactivate para activar el cubo.

Para obtener más información, consulte la sección Copiar y activar una versión más reciente del PowerCube publicado en IBM Cognos Analytics Transformer *Guía del usuario*.

Procedimiento

1. Copie el PowerCube de Transformer al entorno de producción.
 - El nombre del directorio de destino en el entorno de producción debe ser el mismo que el del PowerCube. Por ejemplo, si el cubo se denomina production.mdc, el directorio de destino deberá denominarse production.
 - El directorio de destino debe encontrarse en el mismo directorio que el del PowerCube. Por ejemplo, si una conexión de origen de datos especifica que el PowerCube se encuentra en D:\Cubes\production.mdc, el directorio de destino, denominado production, deberá ser D:\Cubes\production.Por ejemplo, copie el PowerCube en D:\Cubes\production\production.mdc.

2. En la solicitud de línea de comandos, escriba el comando `pcactivate` utilizando la siguiente sintaxis:

```
pcactivate nombre_cubo.mdc  
ubicación_destino ubicación_destino
```

Puede escribir más de una ubicación de destino.

Por ejemplo, escriba

- `pcactivate TheCube.mdc d:\deploy\cubes`
- `pcactivate production.mdc D:\Cubes`
- `pcactivate sales.mdc \\server_1\cubes \\server_2\cubes`
- `pcactivate "Production Cube.mdc" "install_location\webcontent\cubes"`

Nota: Si incluye una ruta en el parámetro `cube_name`, se eliminará y se omitirá.

Protección de orígenes de datos

Puede proteger los orígenes de datos con la seguridad específica del origen de datos o la seguridad de IBM Cognos.

La seguridad de IBM Cognos para un origen de datos no reemplaza las políticas de seguridad que ya existan para el origen de datos. Por ejemplo, en los cubos de IBM Cognos, la seguridad puede establecerse en el nivel de cubo. Para los orígenes de datos de Microsoft Analysis Server, la seguridad puede establecerse mediante el uso de roles de cubo.

En función del origen de datos, están disponibles uno o más de los siguientes métodos de autenticación:

- Sin autenticación

El software de IBM Cognos inicia sesión en el origen de datos sin proporcionar credenciales de inicio de sesión.

- Credenciales del servicio IBM Cognos

El software de IBM Cognos inicia sesión en el origen de datos utilizando el inicio de sesión especificado para el servicio de IBM Cognos. Los usuarios no necesitan inicios de sesión de base de datos individuales. Sin embargo, en los entornos de producción, generalmente los inicios de sesión de la base de datos individuales son más apropiados.

- Un espacio de nombres externo

El software de IBM Cognos inicia sesión en el origen de datos con las credenciales utilizadas para autenticar el espacio de nombres de autenticación especificado. El espacio de nombres debe estar activo, los usuarios deben iniciar sesión antes de acceder al origen de datos y las credenciales de autenticación utilizadas para el espacio de nombres deben ser relevantes para la autenticación del origen de datos.

Si selecciona la casilla de verificación **Transformar identificador de usuario**, el servidor de Cognos Analytics elimina el nombre de dominio del ID de usuario devuelto por el espacio de nombres externo antes de establecer la conexión de base de datos. La implementación actual da soporte a la transformación del ID de usuario para los siguientes formatos únicamente:

- `nombre_dominio\ID_usuario` - Después de la transformación, el ID de usuario sería `ID_usuario`
- `ID_usuario@nombre_dominio` - Después de la transformación, el ID de usuario sería `ID_usuario`

Si desea conservar el nombre de dominio como parte del ID de usuario, asegúrese de que esta casilla de verificación está deseleccionada.

Todos los orígenes de datos también soportan los inicios de sesión de origen de datos definidos para el grupo Todos o para los usuarios individuales, grupos o roles; consulte: Capítulo 11, “Usuarios, grupos y roles”, en la página 207. Si el origen de datos necesita un inicio de sesión, pero el usuario no tiene acceso a un inicio de sesión para este origen de datos, se le solicitará la autenticación cada vez que acceda al origen de datos.

Capítulo 7. Administración de Query Service

El servicio de consulta soporta la modalidad de consulta dinámica de IBM Cognos Analytics.

Para obtener más información, consulte Capítulo 6, “Orígenes de datos y conexiones”, en la página 113.

Mediante Cognos Administration, puede realizar las siguientes tareas de administración de Query Service:

- Configurar propiedades de Query Service
- Administrar el almacenamiento en memoria caché de Query Service

Asimismo, también puede configurar el nivel de registro de auditoría para Query Service. Para obtener más información, consulte “Configuración de la creación de informes de auditoría” en la página 22.

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration**. Para obtener más información, consulte Capítulo 12, “Permisos de acceso y credenciales”, en la página 213. También debe disponer de la función de administración de Query Service. Para obtener más información, consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Configuración de las propiedades de servicio de consultas

El servicio de consultas utiliza un número de valores de configuración de entorno, registro y ajuste.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, seleccione **Cubos dinámicos**.
2. En la sección **Scorecard**, seleccione la vista **Todos los grupos de servidores**.

Consejo: Para seleccionar una vista diferente, en la sección **Scorecard**, haga clic en el menú desplegable para la vista actual.

3. Haga clic en el grupo de servidores bajo **Sistema**.
4. Desde el menú **Acciones** para **QueryService - dispatcher_name**, haga clic en **Establecer propiedades**
5. Pulse la pestaña **Valores**.
6. En la columna **Valor**, escriba o seleccione los valores de las propiedades que desea cambiar. La siguiente lista describe las propiedades que puede establecer para el servicio de consultas.

Valores avanzados

Pulse **Editar** para especificar valores de configuración avanzada. Dado que una entrada adquiere valores avanzados de un padre, al editar estos valores se reemplazan los valores avanzados adquiridos. Para obtener información sobre los tipos de valores avanzados, consulte la publicación *IBM Cognos Analytics Guía de administración y seguridad*.

Configuraciones de cubos dinámicos

Pulse **Editar** para añadir cubos dinámicos a Query Service.

Nivel de registro de auditoría para Query Service

Seleccione el nivel de registro que quiere utilizar para Query Service.

Habilitar rastreo de ejecución de consultas

Un rastreo de ejecución de consulta (ejecutar rastreo de árbol) muestra las consultas que se ejecutan para un origen de datos. Puede utilizar el rastreo para localizar y resolver problemas relacionados con consultas.

Puede encontrar registros de identificación de planificación en la ubicación siguiente: *install_location/logs/XQE/reportName/runtreeLog.xml*

Puede ver y analizar estos archivos de registro con IBM Cognos Dynamic Query Analyzer. Para obtener más información, consulte la publicación *IBM Cognos Dynamic Query Analyzer Guía del usuario*.

Habilitar rastreo de planificación de consultas

El rastreo del plan de consultas (árbol del plan) captura el proceso de transformación de una consulta. Esta información se puede utilizar para obtener un conocimiento avanzado de las decisiones y las reglas que se ejecutan para crear un árbol de ejecución.

El rastreo de planificación de consultas se registra para cada consulta que se ejecuta mediante el modo de consulta dinámica. Puede encontrar registros cronológicos de rastreo en la siguiente ubicación: *install_location/logs/XQE/reportName/plantreeLog.xml*

Como los registros de planificación son grandes, repercuten en el rendimiento de la consulta cuando se habilita este valor.

Generar comentarios en SQL activo

Especifica qué informes generan las consultas SQL en la base de datos.

Escribir modelo en archivo

Especifica si Query Service escribirá el modelo en un archivo cuando se ejecuta una consulta. El archivo sólo se utiliza para la resolución de problemas. Modifique esta propiedad sólo bajo la orientación del soporte de software de IBM.

Puede encontrar el archivo en la ubicación siguiente: *install_location\logs\model\packageName.txt*

Tiempo de espera de conexión inactiva

Especifica el número de segundos que se mantendrá una conexión de origen de datos inactiva para que se pueda reutilizar.

El valor predeterminado es 300. Las entradas válidas son valores comprendidos entre 0 y 65535.

Los valores más bajos reducen el número de conexiones a costa del rendimiento. Los valores más altos pueden mejorar el rendimiento pero aumentan el número de conexiones con el origen de datos.

No iniciar los cubos dinámicos al iniciarse el servicio

Evita que se inicien los cubos dinámicos cuando se inicia Query Service.

Tiempo de espera de comando de administración de cubos dinámicos

Especifique el tiempo que se debe esperar a que un recurso esté disponible para una acción de administración de cubos dinámicos. Esta acción se cancelará si se sobrepasa el periodo de tiempo.

Consejo: Si se establece este valor en cero, el comando esperará indefinidamente.

Tiempo mínimo de ejecución de consultas antes de que se considere la posibilidad de almacenar un conjunto de resultados en memoria caché (milisegundos)

Especifique el tiempo mínimo que esperará una consulta antes de almacenar los resultados en la memoria caché.

Este valor se aplica solamente a los cubos dinámicos.

Tamaño de montón de JVM inicial para Query Service (MB)

Especifica el tamaño inicial, en MB, del montón de Java Virtual Machine (JVM).

Límite de tamaño de montón de JVM para Query Service (MB)

Especifica el tamaño máximo, en MB, del montón de JVM.

Tamaño inicial de la nursery de JVM

Especifica el tamaño inicial, en MB, que JVM asigna a nuevos objetos. El tamaño de la nursery se calcula automáticamente. No necesita cambiar el entorno a menos que el soporte del cliente de IBM Cognos recomiende un cambio.

Límite de tamaño de JVM nursery

Especifica el tamaño máximo en MB, que JVM asigna a objetos nuevos. El tamaño de la nursery se calcula automáticamente. No necesita cambiar el entorno a menos que el soporte del cliente de IBM Cognos recomiende un cambio.

Política de recolección de elementos no utilizados de JVM

Especifica la política de recolección de elementos no utilizados utilizada por JVM. No necesita cambiar el entorno a menos que el soporte del cliente de IBM Cognos recomiende un cambio.

Argumentos de JVM adicionales para Query Service

Especifica otros argumentos que controlan la Java Virtual Machine (JVM). Los argumentos pueden variar para distintas JVM.

Número de salida de ciclos de recolección de elementos no utilizados al registro detallado

Especifica el número de ciclos de recolección de elementos no utilizados que se incluirán en la recolección de elementos no utilizados detallados. Esto controla el tamaño máximo del archivo de registro. Consulte con soporte al cliente de IBM Cognos para aumentar el entorno y recopilar más registros.

Deshabilite el registro de recopilación de elementos no utilizados detallados de JVM

Controla el registro de recolección de elementos no utilizados detallados de JVM. No necesita cambiar el entorno a menos que el soporte al cliente de IBM Cognos recomiende un cambio especializado.

7. Inicie o reinicie el servicio de consultas.

Resultados

Un resumen de las propiedades del servicio de consultas se muestra en el panel **Valores - Servicio de consultas**.

Administración de almacenamiento en caché de Query Service

El almacenamiento en caché reutiliza los resultados ejecutados anteriormente y, cuando es posible, evita el envío de nuevas consultas a la base de datos.

El almacenamiento en caché puede mejorar el rendimiento cuando vuelven a ejecutarse informes con pequeñas modificaciones, cuando se realizan análisis dentro del mismo cubo y cuando se realizan solicitudes maestro-detalle repetitivas para informes de gran tamaño. La memoria caché mantiene los permisos de seguridad del usuario que ejecuta la solicitud.

Para obtener más información sobre cómo funciona la memoria caché, consulte la publicación *IBM Cognos 10 Dynamic Query Cookbook* en la sección Cognos Proven Practices (www.ibm.com/developerworks/data/library/cognos/cognosprovenpractices.html) del sitio web de IBM.

Borrar todo lo almacenado en la memoria caché

Puede borrar la memoria caché para evitar el uso de datos no actualizados que podría haber almacenados en la memoria caché.

Es posible que desee borrar la memoria caché manualmente si los metadatos de origen de datos cambian con poca frecuencia o si desea borrar la memoria caché entre las operaciones de borrado de memoria caché planificadas automáticamente. Si borra la memoria caché mediante los pasos siguientes, se borrará todo lo que haya en la memoria caché.

Si desea borrar un origen de datos, catálogo o cubo específicos de la memoria caché, cree una tarea de administración de Query Service. También puede crear una tarea de administración de Query Service si sus metadatos de origen de datos cambian con regularidad. Por ejemplo, es posible que desee establecer una planificación para borrar la memoria caché cada hora, cada día o cada semana. Para obtener más información, consulte “Creación y planificación de tareas de administración del servicio de consultas” en la página 179.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Almacenamiento en caché de Query Service**.
2. Seleccione los grupos de servidores para limpieza de memoria caché.
3. Pulse **Borrar memoria caché**.

Se mostrará el estado del comando **Borrar memoria caché**.

Si una o varias consultas o informes pendientes están utilizando una memoria caché, este comando aplica internamente el distintivo "obsoleto" a ésta, y se borra automáticamente en cuanto se completa esta utilización.

4. Pulse **Cerrar**.

Análisis del uso de la memoria caché

Puede analizar el uso de la memoria caché mediante la creación de un archivo XML con marca de hora que muestre el estado de las cachés de los cubos especificados (número de accesos y errores de acceso a la memoria caché para distintos niveles de un cubo).

Esto resulta útil para saber los cubos que se encuentran en la memoria caché en cualquier momento. El archivo incluye una lista con el nombre del origen de datos,

el nombre del catálogo y el nombre de cubo de los cubos que se están almacenando en la memoria caché. Esto le puede ayudar a decidir cuándo debe borrar la memoria caché.

El informe se almacena en el directorio *ubicación_c8/logs*. El nombre de archivo tiene el formato *SALDump_prefijo_nombre origen de datos_nombre categoría_nombre cubo_indicación fecha hora.xml*.

También se puede planificar la ejecución automática de la escritura del estado de la memoria caché. Para obtener más información, consulte “Creación y planificación de tareas de administración del servicio de consultas”.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Almacenamiento en caché de Query Service**.
2. Seleccione los grupos de servidores para limpieza de memoria caché.
3. Pulse **Escribir estado de la memoria caché**.
Se mostrará el estado del comando **Escribir estado de la memoria caché**.
4. Pulse **Cerrar**.

Creación y planificación de tareas de administración del servicio de consultas

Los administradores pueden crear y planificar tareas de Query Service para orígenes de datos. Las tareas de Query Service controlan uno o más cubos borrando, escribiendo en, o renovando su memoria caché. Para cubos dinámicos, también puede planificar cuándo los cubos se iniciarán, detendrán o reiniciarán, y cuándo renovarán la seguridad.

- Planificar el borrado de la memoria caché y borrar la memoria caché para controlar la utilización de la memoria por parte de un cubo u origen de datos específico.
- Planificar la generación de un informe con marca de hora (escribir el estado de la memoria caché).

También puede borrar manualmente toda la memoria caché y escribir el estado de la memoria caché en un informe, también manualmente.

Para obtener más información, consulte: “Borrar todo lo almacenado en la memoria caché” en la página 178 y “Análisis del uso de la memoria caché” en la página 178.

Puede crear tareas de administración de Query Service y ejecutarlas a petición. Se pueden ejecutar a la hora planificada Capítulo 18, “Administración de planificaciones”, en la página 277 o según un activador, como la renovación de una base de datos o un correo electrónico “Planificación de entradas basada en activadores” en la página 284. También se pueden planificar como parte de un trabajo “Utilizar trabajos para planificar varias entradas” en la página 281. Del mismo modo, se puede ver el historial de ejecución de las tareas de administración de Query Service “Visualización del historial de ejecución de las entradas” en la página 271.

Antes de empezar

Cuando cree y planifique tareas para cubos dinámico, ha de planificar tareas de inicio y detención para los cubos de origen y los cubos virtuales por separado. Existen otros factores que han de tenerse en cuenta al planificar tareas de inicio y detención para cubos dinámicos:

- Los cubos de origen que forman una parte de un cubo virtual deben planificarse para que se inicien primero.
- Si los cubos de origen forman parte de un cubo virtual, el cubo virtual debe planificarse para que se detenga antes que los cubos de origen.
- Debe proporcionar tiempo suficiente para que los cubos de origen puedan iniciarse antes de la planificación del inicio de un cubo virtual. La misma consideración debe tomarse al planificar la detención de los cubos virtuales y de origen.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Administración de contenidos**.
2. Pulse el botón Nueva tarea de administración de Query Service .
3. Especifique un nombre, una descripción, una sugerencia y una ubicación. Pulse **Siguiente**.
4. Seleccione una operación: **Borrar memoria caché** o **Escribir estado de la memoria caché**.
5. Para orígenes de datos Oracle Essbase y SAP BW, especifique el origen de datos, el catálogo y el cubo. Pulse **Siguiente**.
Introduzca un asterisco (*) como comodín para especificar todos.
6. Para los orígenes de datos relacionales modelados dimensionalmente (DMR), especifique el nombre de un paquete o el nombre de un origen de datos. Si especifica un nombre de origen de datos y selecciona la operación **Borrar memoria caché**, la memoria caché se borra para todos los paquetes que implican ese origen de datos.
7. Para las tareas de cubo dinámico, seleccione el **Grupo de servidores**, **Asignador** y **Cubos** y, a continuación, pulse **Siguiente**.
8. Elija la acción que desee:
 - Para ejecutar la tarea ahora o más adelante, pulse **Guardar y ejecutar una vez** y en **Finalizar**. Especifique una hora y una fecha para la ejecución y, a continuación, pulse **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - Para planificar la ejecución de la tarea de forma periódica, pulse **Guardar y planificar** y a continuación en **Finalizar**. A continuación, seleccione la frecuencia y las fechas de comienzo y de final. Pulse **Aceptar**.

Consejo: Para inhabilitar temporalmente la planificación, seleccione la casilla de verificación **Inhabilitar la planificación**.

Nota: Para ver el estado de la planificación, consulte: “Gestión de actividades planificadas” en la página 269.

- Para guardar la tarea sin planificar o ejecutar, pulse **Sólo guardar** y en **Finalizar**.

Qué hacer a continuación

Debe recordar suprimir una tarea planificada si suprime el cubo asociado de Query Service. De lo contrario, las tareas planificadas apuntarán a cubos inexistentes.

API de línea de comandos de Query Service

Puede gestionar la memoria caché manual o automáticamente con una API de línea de comandos además de utilizar IBM Cognos Administration.

El programa de utilidad de línea de comandos está en el directorio *install_location\bin* y se denomina **QueryServiceAdminTask.sh** o **QueryServiceAdminTask.bat**, en función del sistema operativo.

Escriba `QueryServiceAdminTask -help` en una shell de comandos para visualizar instrucciones sobre cómo utilizar el programa de utilidad.

El programa de utilidad de línea de comandos realiza una solicitud de tarea inmediata y no utiliza el planificador de trabajos ni el servicio de control. Como resultado, los comandos afectan sólo al servidor de IBM Cognos Analytics en el que se ejecutan.

Capítulo 8. Cómo hacer una copia de seguridad de los datos

Se recomienda hacer con regularidad una copia de seguridad de los valores de configuración y de los datos del software de IBM Cognos, así como de los modelos y los proyectos de Framework Manager. Esto evita la pérdida de datos en caso de robo o de daños en el sistema. Una vez que el sistema esté operativo, podrá restaurar los datos.

Dado que la realización de copias de seguridad consume recursos del sistema, si se ejecuta el software de IBM Cognos mientras se efectúa una copia de seguridad de la base de datos, el rendimiento se verá afectado.

Si ha modificado la ubicación de los valores de claves de firma y cifrado de la ubicación predeterminada, asegúrese de realizar una copia de seguridad del directorio que las contenga. Asimismo, si los almacenes de claves están protegidos con contraseñas, asegúrese de conservar dichas contraseñas.

Los datos de los que realiza una copia de seguridad se deben restaurar en el mismo sistema. Para obtener información sobre el traslado de datos de un sistema a otro, consulte: Capítulo 19, “Despliegue”, en la página 287.

Para obtener información sobre la realización de copias de seguridad de datos antes de actualizar el software, consulte el tema sobre actualizaciones en IBM Cognos Analytics *Guía de instalación y configuración*.

Si utiliza un sistema de control del código fuente para almacenar los proyectos de Framework Manager, no será necesario que realice una copia de seguridad de los proyectos.

Si ha personalizado información en IBM Cognos Configuration o en el almacén de contenido, asegúrese de que la copia de seguridad se realice correctamente.

Copia de seguridad del almacén de contenido

Puede realizar una copia de seguridad del almacén de contenido.

Procedimiento

1. Realice una copia de seguridad del almacén de contenido.

Para obtener más información, consulte la documentación de la base de datos.

2. Copie el directorio `install_location/configuration` en la ubicación de copia de seguridad.

Este directorio contiene los valores de configuración.

Resultados

Si en algún momento debe restaurar los valores de configuración, puede copiar el directorio del que se haya realizado una copia de seguridad en la ubicación correcta.

Para obtener información sobre la restauración del almacén de contenido, consulte la documentación de la base de datos.

Copia de seguridad de los proyectos y modelos de Framework Manager

Puede realizar una copia de seguridad de los proyectos y modelos de Framework Manager.

Procedimiento

Copie el directorio del proyecto de Framework Manager y sus subdirectorios en la ubicación de copia de seguridad.

De manera predeterminada, los proyectos y los modelos se encuentran en Mis documentos/My Projects.

Resultados

Si en algún momento debe restaurar los proyectos y modelos de Framework Manager, puede copiar los directorios de los que haya realizado una copia de seguridad en la ubicación correcta.

Capítulo 9. Archivado de contenido de IBM Cognos

El almacenamiento del contenido archivado en el repositorio externo contribuye a garantizar el cumplimiento de los estrictos requisitos relacionados con la normativa y puede mejorar la escalabilidad y el rendimiento de los productos de IBM Cognos, pues reduce el tamaño del contenido del almacén de contenido.

El software da soporte a un IBM FileNet Content Manager con el repositorio externo de IBM FileNet CMIS. Si ya ha instalado la versión 1 del software de IBM FileNet CMIS, debe actualizar este software con el fixpack, versión 2. El archivado de contenido también puede configurarse para utilizar el sistema de archivos.

Los administradores crean una conexión de origen de datos con un repositorio externo para permitir que el contenido pueda moverse desde el almacén de contenido hasta el repositorio. Los usuarios pueden ver el contenido archivado en el repositorio externo. Mediante la obtención de resultados de búsqueda de contenido reciente y archivado, los usuarios pueden realizar comparaciones críticas entre los datos actuales y los datos históricos. Este eficiente mecanismo permite a la compañía satisfacer los requisitos corporativos y gubernamentales a la vez que se obtiene una experiencia de usuario carente de complejidades.

El contenido archivado en el repositorio externo no es gestionado en el entorno IBM Cognos. Por ejemplo, si borra informes en IBM Cognos Analytics, los resultados archivados no se borran en su repositorio externo.

Existen dos tipos de escenario de flujo de trabajo para el archivado del contenido. El primer flujo de trabajo permite a los administradores archivar paquetes y carpetas tras la instalación del software de IBM Cognos Content Archival. El segundo flujo de trabajo permite a los administradores crear conexiones de repositorio para nuevos paquetes y carpetas.

Flujo de trabajo 1: archivar el contenido tras la instalación del software de conectividad

Los administradores pueden archivar la salida guardada del informe para paquetes y carpetas específicos o para todos los paquetes y carpetas tras la instalación o actualización de IBM Cognos Analytics. Este flujo de trabajo sólo debe realizarse una vez, pues todo el contenido se encuentra actualmente en el almacén de contenido.

- Cree una conexión de origen de datos con el repositorio externo.
- Seleccione conexiones de repositorio para los paquetes y carpetas que han de archiversse.
- Cree y ejecute una tarea de mantenimiento de archivado de contenido para seleccionar las carpetas y paquetes que han de archiversse en el repositorio externo.

Después de haber establecido una conexión de repositorio para los paquetes y carpetas, toda nueva salida de informe se archivará automáticamente, lo que significa que no será necesario volver a ejecutar la tarea de mantenimiento de archivado de contenido.

Flujo de trabajo 2: crear conexiones de repositorio para nuevos paquetes y carpetas

Los administradores pueden crear conexiones de repositorio para los nuevos paquetes y carpetas realizando estas tareas:

- Cree una conexión de origen de datos con el repositorio externo.
- Seleccione conexiones de repositorio para los paquetes y carpetas que han de archivarse.

Utilización de tareas de mantenimiento de contenido de archivado de contenido

La tarea de mantenimiento de contenido de archivado de contenido se utiliza para crear una referencia a las versiones de informe de las carpetas y paquetes que selecciona y configura. La selección de carpetas y paquetes marca el contenido y permite que éste permanezca en el almacén de contenido hasta que se archiva en el repositorio externo.

Es importante tener en cuenta que esta tarea no mueve el contenido desde el almacén de contenido hasta el repositorio externo. Primero debe seleccionar las conexiones de repositorio para los paquetes y carpetas. Las versiones de informe de las carpetas y paquetes que no se marcan para el archivado están disponibles para suprimirse del almacén de contenido.

Después de haber marcado el contenido, la tarea de archivado de contenido se ha completado. Una tarea que se ejecuta en segundo plano de Content Manager busca los elementos marcados y, a continuación, los copia y guarda en el repositorio externo.

La importación de contenido a una carpeta o paquete que se ha configurado para el archivado en un repositorio externo no mueve y archiva automáticamente el contenido importado al repositorio. Un administrador debe ejecutar una tarea de mantenimiento de contenido de archivado de contenido para esta carpeta o paquete para poder archivar el contenido importado.

Tareas que se ejecutan en segundo plano

Las tareas XML que se ejecutan en segundo plano y que se utilizan para mover el contenido desde el almacén de contenido hasta el repositorio externo son `archiveTask.xml` y `deleteTask.xml`. El archivo `archiveTask.xml` mueve el contenido marcado a un repositorio externo. Puede utilizar este archivo para establecer tiempos de ejecución de subproceso y archivar salidas de formatos seleccionados. El archivo `deleteTask.xml` es un archivo de configuración que recupera y suprime los objetos de versión marcados de la cola. No debe modificar este archivo.

Preserve los ID de contenido antes de archivar

Si lo desea, puede preservar los ID de contenido antes de archivar la salida del informe.

Los objetos del almacén de contenido tienen ID de contenido que se suprimen y sustituyen por nuevos ID de forma predeterminada cuando ejecuta un despliegue de importación y mueve contenido a un entorno de destino. Sin embargo, puede que existan situaciones en las que deberá preservar los identificadores de

contenido, por ejemplo, al mover la salida de informe a un repositorio de informes externo.

Configurar el archivado de contenido

Debe configurar el entorno para el archivado de contenido. Para que los cambios de configuración entren en vigor, debe detener e iniciar los servicios de IBM Cognos.

Creación de una ubicación de archivo para un repositorio del sistema de archivos

Para archivar informes o especificaciones de informe en un repositorio de sistema de archivos de archivado de contenido IBM Cognos, debe crear una raíz de alias que apunte a una ubicación de archivo de una unidad local o una unidad compartida de red.

Antes de empezar

Debe ser un administrador y tener acceso a la ubicación del archivo. Content Manager y los componentes de nivel de aplicación deben poder acceder a esta ubicación utilizando un URI de archivo.

Procedimiento

1. Si se está ejecutando, detenga el servicio de IBM Cognos.
2. Inicie IBM Cognos Configuration.
3. Pulse **Acciones > Editar la configuración global**.
4. En la pestaña **General**, seleccione **Raíces de alias**, pulse dentro del campo de valor, pulse el botón de edición y cuando aparezca el recuadro de diálogo **Valor - Raíces de alias**, pulse **Añadir**.
5. En la columna **Nombre de raíz de alias**, especifique un nombre exclusivo para el repositorio del sistema de archivos.

Nota: No se ha establecido ningún límite para el número de alias que se pueden crear.

6. Especifique la ruta a la ubicación del sistema de archivos, donde la ruta del sistema de archivos es la ruta completa a una ubicación de archivo existente:
 - En Windows, en la columna **URI de Windows**, escriba file:/// seguido de la ruta local, por ejemplo, file:///c:/ruta-sistema-archivos, o escriba file:// seguido del nombre del servidor y de la ruta de la unidad compartida, por ejemplo file://servidor/unidad-compartida.
 - En UNIX o Linux, en la columna **unixURI**, especifique file:/// seguido por la ruta local, por ejemplo, file:///ruta-sistema-archivos.

Nota: Las rutas relativas como file:///../ruta-sistema-archivos, no se soportan.

En una instalación distribuida, tanto el sistema de Content Manager como el sistema de los componentes del nivel de aplicación deben tener acceso a la ubicación del archivo. Utilice ambos URI solo en una instalación distribuida. El URI de UNIX y el URI de Windows de una raíz de alias deben apuntar a la misma ubicación en el sistema de archivos.

7. Pulse **Aceptar**.
8. Reinicie el servicio de IBM Cognos. Esto podría requerir unos minutos.

Importación de definiciones de clases personalizadas y propiedades en IBM FileNet Content Manager

Para utilizar el archivado de contenido de IBM Cognos, debe importar un conjunto de archivos de propiedades y clases personalizadas en IBM FileNet Content Manager.

Las propiedades y definiciones de clases personalizadas incluyen metadatos específicos de FileNet. Puede instalar los archivos de propiedades y clases personalizadas en cualquier momento.

Procedimiento

1. Si se ha configurado el archivado de FileNet, vaya al directorio `install_location/configuration/repository/filenet/upgrade/`.
2. Si todavía no se ha configurado el archivado de FileNet, vaya al directorio `install_location/configuration/repository/filenet/new/`.
3. Copie los archivos `CMECMIntegrationObjects_CEEExport._xxx.xml` a una carpeta local en el servidor FileNet.
4. Abra la herramienta de administración de FileNet Enterprise Manager y conéctese al dominio del repositorio externo de FileNet.
5. Seleccione un almacén de objetos de destino y pulse **Importar todos los elementos** para importar las definiciones en el almacén de objetos.
6. En el panel Opciones de importación, pulse **Importar archivo de manifiesto** y vaya hasta la ubicación de los archivos `CMECMIntegrationObjects_CEEExport._xxx.xml`.
7. Seleccione el archivo `CMECMIntegrationObjects_CEEExport_Manifest.xml` y pulse **Importar**.
8. Reinicie FileNet Content Engine y la aplicación FileNet CMIS para aplicar los cambios en el entorno.

Nota: La actualización de los cambios en todos los nodos FileNet podría requerir mucho tiempo.

Importación de definiciones y propiedades de clases personalizadas en IBM Content Manager 8

Para utilizar el archivo de contenido de IBM Cognos con IBM Content Manager 8, debe importar un conjunto de archivos de clases y propiedades personalizadas. También debe actualizar el archivo de configuración CMIS con los tipos de carpeta IBM Cognos.

Las definiciones y propiedades de clases personalizadas incluyen metadatos específicos de IBM Content Manager 8. Puede instalar los archivos de propiedades y clases personalizadas en cualquier momento.

Debido a que no hay un gestor de recursos definido durante el proceso de instalación, no hay mensajes de error de conflicto durante el proceso de importación.

Antes de empezar

Debe tener IBM Content Manager 8 instalado con un repositorio externo de IBM Content Manager 8 CMIS versión 1.1.

Procedimiento

1. Abra el Content Manager 8 **System Administration Client**.
2. En el menú principal, pulse en **Herramientas > Importar XML**.
3. En la ventana **Importar opciones de XML**, sección **Archivo a importar**:
 - En el campo **Archivo del modelo de datos**, haga clic en **Navegar** y seleccione el archivo `CMECMIntegrationTypes_RMImport_Manifest.xsd` desde el cual desea importar los objetos.
 - En el campo **Archivo de objetos administrativos**, haga clic en **Navegar** y seleccione el archivo `CMECMIntegrationTypes_RMImport_MimeTypes.xml` para importar el archivo de objetos administrativos.

La ubicación predeterminada es el directorio `install_location/configuration/repository/contentManager8/New`.
4. Para ver los conflictos, en la ventana **Importar opciones de XML**, bajo **Opciones de procesamiento**, seleccione **Procesar de manera interactiva**.
5. Haga clic en **Importar** para comenzar el proceso de importación.
 - a. En la ventana **Importar resultados de preprocesador**, amplíe **Tipos de elementos** y haga doble clic en un tipo de elemento que indique un conflicto.
 - b. En la ventana **Detalles de la definición de importación y definición de destino**, en la columna **Destino resultante**, seleccione los nombres para el **Gestor de recursos** y **Colección** creado cuando instaló Content Manager 8 y haga clic en **Aceptar**.
 - c. Repita los pasos a y b para cada tipo de elemento que indica un conflicto.
6. Después de resolver todos los conflictos, desde la ventana **Importar resultados del preprocesador**, haga clic en **Continuar**.
7. En la ventana **Confirmar selección de importación**, haga clic en **Importar**.
8. Después de finalizar la importación, haga clic en **Aceptar**.
9. Para actualizar el archivo de configuración de CMIS para detectar los tipos de carpeta de IBM Cognos, ejecute CMIS para el programa de configuración Content Manager 8 para crear un perfil.
10. Abra el archivo `cmpathsrvservice.properties` en la carpeta de perfiles de configuración IBM CMIS for Content Manager.

Para UNIX, la ruta de archivo predeterminado es: `/opt/IBM/CM_CMIS/profiles/profile1`

Para Windows, la ruta de archivo predeterminada es: `C:\Program Files\IBM\CM_CMIS\profiles\profile1`

 - a. Localice la línea `folderTypes`.
 - b. Añada los tipos de carpeta IBM Cognos `COGNOSREPORT` y `REPORTVERSION` en mayúsculas. Separe cada tipo de carpeta por una coma.

Por ejemplo:
`folderTypes = C1bFolder,COGNOSREPORT,REPORTVERSION`
 - c. Guarde y cierre el archivo.
11. Ejecute CMIS para el programa de configuración de Content Manager 8 y seleccione la opción para volver a implementar el archivo de configuración de CMIS automáticamente.

Nota: Para obtener más información acerca de la implementación manual de CMIS, consulte Implementación manual de IBM CMIS for Content Manager

(<http://pic.dhe.ibm.com/infocenter/cmgt/v8r4m0/topic/com.ibm.installingcmcmis.doc/cmsde001.htm>).

12. Desde la consola administrativa de WebSphere Application Server, reinicie **CMIS for Content Manager Application**.

Especificación de una hora disponible para ejecutar el proceso de archivado

Para mantener el rendimiento alto del sistema durante las horas punta, puede configurar un periodo de inactividad para especificar cuándo se deben ejecutar las tareas de supresión o archivado.

Un periodo de inactividad es un periodo temporal en el que se deniega el movimiento de datos. De forma predeterminada, no se define un periodo de inactividad cuando el software está instalado.

Procedimiento

1. Vaya al directorio *install_location/webapps/p2pd/WEB-INF/cm/tasks/manager*.
2. Utilizando un editor de texto XML, abra el archivo *tasksManager.xml*.
3. Por ejemplo, para especificar un periodo de inactividad semanal de 8 de la mañana a 5 de la tarde, de martes a viernes, añada el siguiente elemento `<blackoutPeriods>` como elemento hijo del elemento `backgroundTasksManager`.
 - hora de inicio = `<hour>08</hour>`
 - hora de detención = `<hour>17</hour>`
 - días =

```
<day>Tuesday</day>
<day>Wednesday</day>
<day>Thursday</day>
<day>Friday</day>
```
4. Si es necesario, reduzca el número de subprocesos disponibles para los procesos de archivado y supresión. El número máximo de subprocesos es 7.
5. Guarde y cierre el archivo.
6. Reinicie las actividades en segundo plano del servicio de Content Manager.

Especificación del tiempo de ejecución de subprocesos

Puede utilizar subprocesos para planificar el tiempo de procesamiento del sistema operativo.

Las tareas en segundo plano de archivado y supresión utilizan subprocesos para mover el contenido. Los subprocesos son unidades de tiempo de procesamiento que el sistema operativo planifica.

Procedimiento

1. Vaya al directorio *install_location/webapps/p2pd/WEB-INF/cm/tasks/config*.
2. Mediante un editor de texto XML, abra el archivo *archiveTask.xml*.
3. Por ejemplo, para configurar que tres subprocesos se ejecuten desde la media noche a las 8 de la mañana, que un subproceso se ejecute desde las 8 de la mañana a las 5 de la tarde, que ningún subproceso se ejecute de las 5 de la tarde a la medianoche y que todos los subprocesos se ejecuten cada día de la semana, añada el siguiente elemento XML `<executionPeriods>` como elemento hijo del elemento `backgroundTask`.

```

    <executionPeriods>
  <executionPeriod>
    <threads>3</threads>
    <startTime>
      <hour>00</hour>
      <minute>00</minute>
    </startTime>
    <stopTime>
      <hour>08</hour>
      <minute>00</minute>
    </stopTime>
    <days>
      <day>Monday</day>
      <day>Tuesday</day>
      <day>Wednesday</day>
      <day>Thursday</day>
      <day>Friday</day>
      <day>Saturday</day>
      <day>Sunday</day>
    </days>
  </executionPeriod>
  <executionPeriod>
    <startTime>
      <hour>08</hour>
      <minute>00</minute>
    </startTime>
    <stopTime>
      <hour>17</hour>
      <minute>00</minute>
    </stopTime>
    <days>
      <day>Monday</day>
      <day>Tuesday</day>
      <day>Wednesday</day>
      <day>Thursday</day>
      <day>Friday</day>
      <day>Saturday</day>
      <day>Sunday</day>
    </days>
  </executionPeriod>
</executionPeriods>

```

4. Guarde y cierre el archivo.

Archivado de formatos seleccionados de salidas de informe

Puede limitar el archivado para limitar el archivado a formatos de salida específicos. De forma predeterminada, se archivan las salidas de cualquier formato determinado, incluidos PDF, XML, HTML y Excel.

Puede limitar el archivado de formatos de salida específicos en el repositorio.

Procedimiento

1. Vaya al directorio *install_location/webapps/p2pd/WEB-INF/cm/tasks/config*.
2. Mediante un editor de texto XML, abra el archivo *archiveTask.xml*.
3. Por ejemplo, para definir el archivado de solo versiones de salida de informes en PDF, añada el siguiente elemento XML *<outputFormats>* como elemento hijo del elemento XML *runOptions*.

```

<outputFormats>
  <outputFormat>PDF</outputFormat>
</outputFormats>

```

Puede utilizar el elemento *outputFormats* de ejemplo existente y modificar la lista para especificar los formatos de salida que se archivarán.

No puede archivar selectivamente varias versiones de salida de informe de archivo, por ejemplo, HTML con gráficos.

Guarde y cierre el archivo.

Indicación de que las especificaciones de informe no han de archivarse

De forma predeterminada, se archiva la salida de la especificación de informe. Las especificaciones de informe describen cómo se han generado los datos dentro de un informe.

Para desactivar el archivo de las especificaciones del informe, debe modificar dos archivos: CM.xml y ningún CM_FILENET.xml o CM_CM8.xml, dependiendo de si archiva su contenido en un repositorio de IBM FileNetContent Manager o un repositorio de IBM Content Manager 8.

Procedimiento

1. Vaya al directorio *install_location/webapps/p2pd/WEB-INF/repositories/config*.
2. Mediante un editor de texto XML, abra el archivo CM.xml.
3. Elimine el comentario o elimine la siguiente línea: `<property name="specifications" metadataPropertyName="specification" useTempFile="true"`
4. Guarde y cierre el archivo.
5. Vaya al directorio *install_location/webapps/p2pd/WEB-INF/repositories/config*.
6. Lleve a cabo uno de los pasos siguientes:
 - Si archiva su contenido en FileNet, abra el archivo con el nombre CM.FILENET.xml en el editor de texto.
 - Si archiva su contenido en IBM Content Manager 8, abra el archivo con el nombre CM.xml en un editor de texto.

7. Comente o elimine el elemento siguiente:

```
<property repositoryName="REPORTEXECUTIONSPECIFICATION" repositoryType="ASSOCIATED"
metadataPropertyName="specification">
  <associatedObjectTypes>
    <objectType name="VERSIONSPECIFICATION">
      <properties>
        <property repositoryName="cmis:name" repositoryType="STRING"
metadataPropertyName="reportVersionDefaultName" valueHandler="com.cognos.cm.
repositoryPluginFramework.
PropertyValueAppendStringHandler" valueHandlerArgument="_specification"/>
      </properties>
    </objectType>
  </associatedObjectTypes>
</property>
```

Nota: En el archivo CM.xml, el valor objectType name es `<objectType name="$t!-2_VERSIONSPECIFICATIONv-1">`.

8. Reinicie las actividades en segundo plano del servicio de Content Manager. Para obtener más información, consulte la *IBM Cognos Analytics Guía de administración y seguridad*.

Administrar el archivado de contenido

La administración del archivado de contenido incluye la creación de tareas de archivado y la especificación de ubicaciones de archivado.

La salida de informe puede archivarse en un repositorio de informes externo para su almacenamiento a largo plazo. Para obtener más información, consulte “Conexiones de origen de datos del repositorio externo” en la página 136.

Especificación de un repositorio externo para la salida de informe

Debe especificar un repositorio en el nivel de carpeta y de paquete para que pueda archivarse contenido en el repositorio.

Para especificar un repositorio, debe existir una conexión con el repositorio, y debe disponer de privilegios suficientes para seleccionar el repositorio. Debe disponer de permiso de ejecución para la característica protegida **Administrar conexiones de repositorios** para la prestación **Repositorios externos**. Cuando se especifica una conexión, todas las versiones de la salida de informe nuevas se copian en el repositorio externo.

Si ya se ha especificado una conexión de origen de datos con un repositorio externo, éste puede sobrescribirse y seleccionarse otro repositorio. Si ya no desea archivar contenido en el paquete o carpeta, puede eliminar la referencia a la conexión mediante la opción **Borrar**. A continuación se incluye un ejemplo. Una subcarpeta adquiere de manera predeterminada una conexión de repositorio desde la carpeta padre. No obstante, es posible que no quiera archivar el contenido de la subcarpeta, o no desee que dicho contenido se archive en el repositorio especificado para la carpeta padre. Para que el contenido de una subcarpeta no se archive, utilice la opción **Borrar**. Si desea utilizar un repositorio diferente desde la carpeta padre, especifique una conexión para la subcarpeta.

También puede crear una conexión de origen de datos con un repositorio externo para una carpeta o paquete si el repositorio existe y si dispone de permiso suficiente para crear una conexión de repositorio. Para obtener más información, consulte “Conexiones de origen de datos del repositorio externo” en la página 136.

Procedimiento

1. Seleccione una carpeta o paquete y pulse en el icono Establecer propiedades.
2. En la pestaña **General**, vaya a la sección **Repositorio de informes**.
3. Para especificar un origen de datos o cambiar un origen de datos existente, seleccione **Reemplazar el repositorio de informes adquirido de la entrada padre**.
4. En **Conexión**, pulse en **Seleccionar una conexión**.
5. En la ventana **Seleccionar el origen de datos (Navegar)**, seleccione el origen de datos.

Creación de tareas de mantenimiento de archivado de contenido

Puede crear una tarea de mantenimiento de contenido de archivado de contenido para mover la salida de informe de las carpetas y paquetes para su archivado en el repositorio externo.

Acerca de esta tarea

Puede crear y planificar una tarea de archivado de contenido para marcar las versiones de la salida de informe, que se encuentran en las carpetas y paquetes, para su archivado. El contenido que se marca para el archivado se copia y se guarda en el repositorio externo.

Las carpetas y paquetes que se marcan para el archivado no pueden suprimirse del almacén de contenido hasta que se han movido y guardado correctamente en el repositorio externo.

Procedimiento

1. Lance IBM Cognos Administration.
2. En la pestaña **Configuración**, pulse **Administración de contenidos**.
3. En la barra de herramientas, pulse el icono de mantenimiento de nuevo contenido y, a continuación, pulse en **Archivado de contenido**.
4. Escriba un nombre para la tarea de archivado de contenido y, opcionalmente, una descripción y una sugerencia. Pulse **Siguiente**.
5. Seleccione el nivel de grabación.
6. Haga clic en **Agregar**
7. Seleccione carpetas, paquetes, espacios de nombre o carpetas de espacio de nombre que desea marcar para archivar y haga clic en **Agregar**.
8. Pulse **Aceptar**.
9. Pulse **Siguiente**.
10. Seleccione una de las siguientes opciones:
 - Para ejecutarla ahora o posteriormente, pulse **Guardar y ejecutar una vez**. Pulse **Finalizar**, especifique la hora y la fecha de la ejecución y, a continuación, pulse **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - Para planificar la ejecución de forma periódica, pulse **Guardar y planificar**. Pulse **Finalizar** y seleccione la frecuencia y las fechas de inicio y finalización. Pulse **Aceptar**.
 - Para guardar sin planificar o ejecutar, pulse **Sólo guardar** y en **Finalizar**.

Creación de una tarea de mantenimiento de actualización de regla de conservación

Puede crear una tarea de mantenimiento de actualización de regla de conservación para modificar globalmente el número de versiones de la salida de informe, versiones de contenido de documentos e historial de informes que actualmente se conservan en el almacén de contenido.

Acerca de esta tarea

Los administradores utilizan la tarea de actualización de la regla de retención para especificar el número de informes, consultas, análisis y objetos del documento para mantener en el almacén de contenido. Puede especificar durante cuánto tiempo han de conservarse el historial y las versiones de salida en el almacén de contenido. Cualquier elemento más antiguo que la fecha que especifique se suprimirá del almacén de contenido. Esta tarea de actualización marca las versiones de la salida que han de suprimirse del almacén de contenido si las versiones de la salida no cumplen la regla de conservación definida. Una tarea que se ejecuta en segundo plano en Content Manager suprime los objetos marcados del almacén de contenido. Para reducir el contenido del almacén de contenido,

considere la posibilidad de conservar un máximo de dos versiones en el almacén de contenido y de archivar las versiones más antiguas en el repositorio externo.

Importante: Ejecute esta tarea sólo después de haber creado y ejecutado la tarea de archivado de contenido. Si la ejecuta antes, el contenido que no se ha marcado para el archivado se suprimirá permanentemente del almacén de contenido.

Procedimiento

1. Lance IBM Cognos Administration.
2. En la pestaña **Configuración**, pulse **Administración de contenidos**.
3. En la barra de herramientas, pulse el icono de mantenimiento de nuevo contenido y, a continuación, pulse en **Actualización de regla de conservación**.
4. Escriba un nombre para la tarea de actualización de regla de conservación y, opcionalmente, una descripción y una sugerencia. Pulse **Siguiente**.
5. Seleccione las carpetas y paquetes que desea incluir.
6. Para los valores de conservación de **Historial de ejecución**, realice una de las acciones siguientes:
 - Para conservar el historial de ejecución durante un número específico de apariciones, pulse en **Número de apariciones** y especifique el número. Para guardar un número ilimitado de salidas de informes, escriba el valor 0.
 - Para conservar el historial de ejecución durante un periodo de tiempo específico, pulse en **Duración** y pulse en **Días** o en **Meses**. Introduzca el valor adecuado en el cuadro.
7. Para los valores de conservación de **Versiones de salida**, realice una de las acciones siguientes:
 - Para mantener la salida de informe para un determinado número de apariciones, pulse **Número de apariciones** e introduzca el número. Para guardar un número ilimitado de salidas de informes, escriba el valor 0.
 - Para conservar salidas de informes durante un determinado periodo de tiempo, pulse **Duración** y luego en **Días** o en **Meses**. Introduzca el valor adecuado en el cuadro.
8. Seleccione el nivel de grabación y pulse en **Aceptar**.
9. Seleccione una de las siguientes opciones:
 - Para ejecutarla ahora o posteriormente, pulse **Guardar y ejecutar una vez**. Pulse **Finalizar**, especifique la hora y la fecha de la ejecución y, a continuación, pulse **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - Para planificar la ejecución de forma periódica, pulse **Guardar y planificar**. Pulse **Finalizar** y seleccione la frecuencia y las fechas de inicio y finalización. Pulse **Aceptar**.
 - Para guardar sin planificar o ejecutar, pulse **Sólo guardar** y en **Finalizar**.

Creación de una tarea de mantenimiento de eliminación de contenido

Puede crear una nueva tarea de mantenimiento de eliminación de contenido para marcar objetos de historial y versiones de la salida de informe, que se encuentran en las carpetas y paquetes, para su supresión.

Acerca de esta tarea

Puede especificar durante cuánto tiempo han de conservarse el historial y las versiones de salida en el almacén de contenido. Cualquier elemento más antiguo que la fecha que especifique se suprimirá del almacén de contenido.

Importante: Considere las circunstancias siguientes al ejecutar las tareas de mantenimiento de contenido de eliminación de contenido:

- Ejecute esta tarea sólo después de haber creado y ejecutado la tarea de archivado de contenido. Si la ejecuta antes, el contenido que no se ha marcado para el archivado se suprimirá permanentemente del almacén de contenido.
- El contenido marcado para supresión se suprime solo en IBM Cognos Analytics. El contenido no se suprime en su repositorio externo.

Procedimiento

1. Lance IBM Cognos Administration.
2. En la pestaña **Configuración**, pulse **Administración de contenidos**.
3. En la barra de herramientas, pulse el icono de mantenimiento de nuevo contenido y, a continuación, pulse en **Eliminación de contenido**.
4. Escriba un nombre para la tarea de eliminación de contenido y, opcionalmente, una descripción y una sugerencia.
5. Pulse en **Seleccionar otra ubicación** si desea editar la ubicación. Busque y seleccione la carpeta o pulse en **Nueva carpeta** para añadir una nueva ubicación. Pulse **Aceptar**.
6. Pulse **Siguiente**.
7. Seleccione las carpetas y paquetes que desea incluir.
8. Para los valores de **Historial de ejecución**, pulse en la casilla de verificación **Historial de ejecución**, especifique el valor adecuado en el cuadro y, a continuación, seleccione **Días** o bien **Meses**.
9. Para los valores de **Versiones de salida**, pulse en la casilla de verificación **Versiones de salida**, especifique el valor adecuado en el cuadro y, a continuación, seleccione **Días** o bien **Meses**.
10. Seleccione el nivel de grabación y pulse en **Aceptar**.
11. Seleccione una de las siguientes opciones:
 - Para ejecutarla ahora o posteriormente, pulse **Guardar y ejecutar una vez**. Pulse **Finalizar**, especifique la hora y la fecha de la ejecución y, a continuación, pulse **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - Para planificar la ejecución de forma periódica, pulse **Guardar y planificar**. Pulse **Finalizar** y seleccione la frecuencia y las fechas de inicio y finalización. Pulse **Aceptar**.
 - Para guardar sin planificar o ejecutar, pulse **Sólo guardar** y en **Finalizar**.

Búsqueda de contenido en el repositorio externo

El contenido archivado puede verse en IBM Cognos Analytics o en el repositorio externo.

Después de haber movido y archivado el contenido, éste se almacena en la ubicación que se ha especificado al crear la conexión de origen de datos con el repositorio externo.

Búsqueda de contenido archivado

Puede acceder al contenido almacenado en el almacén de contenido de IBM Cognos y en un repositorio externo. Si ven los resultados de búsqueda de contenido reciente y archivado, los usuarios pueden realizar comparaciones críticas entre los datos actuales y los datos históricos.

Al realizar búsquedas de contenido archivado, los usuarios pueden buscar un elemento en un nombre de informe o un elemento de datos en un informe. El contenido archivado puede verse pulsando en los enlaces de los resultados de la búsqueda.

El contenido que se almacena en un repositorio de informes no está disponible para IBM Cognos Workspace. Cuando se realiza una búsqueda en IBM Cognos Workspace, la salida de informe archivada no se notifica.

Capítulo 10. Modelo de seguridad

La seguridad del software IBM Cognos está diseñada para cumplir con la necesidad de seguridad en diferentes entornos. Puede utilizarla en cualquier contexto, desde una prueba de aplicación de conceptos, en la que la seguridad no suele estar habilitada, hasta un despliegue empresarial a gran escala.

El modelo de seguridad se puede integrar fácilmente en la infraestructura de seguridad existente de la organización. Se basa en uno o más proveedores de autenticación. Los proveedores se utilizan para definir y mantener usuarios, grupos y roles, así como para controlar el proceso de autenticación. Cada uno de los proveedores de autenticación admitidos en el software de IBM Cognos se conoce como espacio de nombres .

Además de los espacios de nombres que representan a los proveedores de autenticación, el software de IBM Cognos cuenta con un espacio de nombres incorporado denominado “Espacio de nombres de Cognos” en la página 202. El espacio de nombres de Cognos mejora las políticas de seguridad de la organización y la capacidad de despliegue de las aplicaciones.

La seguridad en el software de IBM Cognos es opcional. Si la seguridad no está habilitada, significa que no hay configurado ningún proveedor de autenticación y, por lo tanto, todos los accesos de usuario son anónimos. Normalmente los usuarios anónimos suelen tener un acceso limitado de sólo lectura.

Documentación de seguridad en las prácticas recomendables de Cognos

La publicación *IBM Cognos Analytics Guía de administración y seguridad* Guía de administración y seguridad IBM Cognos Analytics. Si necesita información sobre implementaciones específicas, con distintos proveedores de seguridad, puede utilizar los recursos disponibles en IBM Cognos Proven Practices (<http://www.ibm.com/developerworks/data/library/cognos/cognosprovenpractices.html>). Pulse el enlace **Seguridad** de la página y siga los enlaces a distintos tipos de artículos sobre seguridad.

Proveedores de autenticación

Los proveedores de autenticación son los encargados de llevar a cabo la autenticación de usuarios en el software de IBM Cognos. Estos proveedores de autenticación definen los usuarios, los grupos y los roles que se utilizan para la autenticación. Los nombres de usuarios, los identificadores, las contraseñas, la configuración regional y las preferencias personales son algunos ejemplos del tipo de información que se almacena en los proveedores.

Si se configura la autenticación para el software de IBM Cognos, los usuarios deben proporcionar, en el momento de iniciar sesión, credenciales válidas, como el identificador de usuario y la contraseña. En el entorno del software de IBM Cognos, a los proveedores de autenticación también se les conoce como espacios de nombres, y se representan mediante entradas de espacios de nombres  en la interfaz de usuario.

El software de IBM Cognos no replica los usuarios, grupos y roles definidos en el proveedor de autenticación correspondiente. Sin embargo, se puede hacer referencia a ellos en el software de IBM Cognos cuando se establezcan los permisos de acceso a informes y otro tipo de contenido. También se pueden convertir en miembros de grupos y roles de Cognos.

En esta versión se soportan los siguientes proveedores de autenticación:

- Active Directory
- OpenID Connect
- Proveedor Java personalizado
- Proxy de autenticación de OpenID Connect
- IBM Cognos Series 7
- LDAP
- SAP
- SiteMinder

Los proveedores de autenticación se configuran mediante IBM Cognos Configuration. Para obtener más información, consulte *Guía de instalación y configuración*.

Varios espacios de nombres

Si en el sistema hay varios espacios de nombres configurados, al iniciar sesión debe seleccionar el que desea utilizar. Sin embargo, esto no le impide iniciar sesión posteriormente con otros espacios de nombres. Por ejemplo, si establece permisos de acceso, es posible que desee hacer referencia a las entradas de otros espacios de nombres. Para iniciar sesión en otro espacio de nombres, no es necesario que cierre sesión en el espacio de nombres que esté utilizando. Puede haber iniciado sesión en varios espacios de nombres a la vez.

Su inicio de sesión principal es el espacio de nombres y las credenciales que utiliza para iniciar sesión. Los espacios de nombres en los que inicie sesión posteriormente y las credenciales que utilice se convertirán en los inicios de sesión secundarios.

Cuando suprima uno de los espacios de nombres, podrá iniciar sesión mediante otro espacio de nombres. Si suprime todos los espacios de nombres excepto el espacio de nombres de Cognos, no se le solicitará que inicie sesión. Si está habilitado el acceso anónimo, iniciará sesión automáticamente como usuario anónimo. Si el acceso anónimo no está habilitado, no podrá acceder a la página de inicio de sesión. En este caso, utilice IBM Cognos Configuration para habilitar el acceso anónimo.

Cómo ocultar espacios de nombres

Puede ocultar espacios de nombres a los usuarios durante el inicio de sesión. Esto le permite tener espacios de nombres de inicio de sesión de confianza sin mostrarlos en la lista de selección de espacios de nombres que se presenta cuando los usuarios inician la sesión.

Por ejemplo, puede que desee integrar el inicio de sesión único en los sistemas, pero que los clientes puedan seguir realizando la autenticación directamente en el software de IBM Cognos sin que se les solicite que elijan un espacio de nombres.

Puede ocultar los espacios de nombres Proveedor Java personalizado e eTrust SiteMinder que haya configurado.

Para obtener más información, consulte *Guía de instalación y configuración*.

Supresión o restauración de espacios de nombres no configurados

Puede conservar los espacios de nombres y todo su contenido en el almacén de contenido, aunque ya no estén configurados para utilizarlos en el software de IBM Cognos. Cuando un espacio de nombres no está configurado, aparece como inactivo en la herramienta del directorio.

Un espacio de nombres inactivo es aquel que se ha configurado pero que, posteriormente, se ha suprimido en IBM Cognos Configuration. Los miembros del rol Administradores del sistema pueden suprimir el espacio de nombres del almacén de contenido. No se puede iniciar sesión en un espacio de nombres inactivo.

Si una versión nueva del software de IBM Cognos detecta un espacio de nombres previamente configurado y que ya no se utiliza, el espacio de nombres aparecerá en la herramienta del directorio como inactivo. Si sigue necesitando los datos del espacio de nombres, puede volverlo a configurar. Si no necesita el espacio de nombres, puede suprimirlo.

Cuando suprime un espacio de nombres, también suprime todas las entradas de Mis carpetas que tenga asociadas, así como su contenido.

Un espacio de nombres activo no se puede suprimir, pero se puede actualizar.

Para volver a crear un espacio de nombres en IBM Cognos Configuration, debe utilizar el ID original del mismo. Para obtener más información sobre configuración y nueva creación de espacios de nombres, consulte la *Guía de instalación y configuración*.

Supresión de un espacio de nombres inactivo

Si se ha eliminado un espacio de nombres de IBM Cognos Configuration y ya no se necesita, un miembro del rol Administradores del sistema podrá suprimirlo de forma permanente en la herramienta del directorio. Al suprimir un espacio de nombres, también se suprimen todas las entradas de Mis carpetas que tenga asociadas.

Para acceder a la herramienta de administración del directorio, debe contar con permisos de ejecución para la característica protegida **Conexiones con orígenes de datos** y permisos de visita para la función protegida de administración.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
Si el espacio de nombres que desea suprimir no tiene una marca de selección en la columna **Activo**, está inactivo y se puede suprimir.
2. En la columna **Acciones**, pulse el botón **Suprimir**.
Si el espacio de nombres está activo, el botón **Suprimir** no estará disponible.

Resultados

El espacio de nombres se suprimirá de forma permanente. Para volver a utilizar el espacio de nombres en el software de IBM Cognos, deberá añadirlo mediante IBM Cognos Configuration.

Autorización

La autorización es el proceso de otorgar o denegar el acceso a los datos, así como de especificar las acciones que se pueden realizar con esos datos, según la identidad del usuario.

La autorización del software de IBM Cognos asigna permisos a usuarios, grupos y roles que les permiten realizar acciones, como leer o escribir, en objetos del almacén de contenido, como carpetas e informes. El almacén de contenido se puede ver como una jerarquía de objetos de datos, que incluye no sólo carpetas e informes, sino paquetes para creación de informes, directorios y servidores.

Cuando los administradores de IBM Cognos distribuyen informes a los usuarios, pueden configurar carpetas en las que se pueden almacenar tanto informes como otros objetos. A continuación, estas carpetas se pueden proteger para que sólo el personal autorizado pueda ver, cambiar o realizar otras tareas con su contenido.

Para obtener información sobre el establecimiento de permisos de acceso para las entradas de IBM Cognos, consulte: Capítulo 12, “Permisos de acceso y credenciales”, en la página 213. Para obtener información sobre la jerarquía de Content Manager de objetos y los permisos de acceso iniciales, consulte: Apéndice C, “Permisos de acceso iniciales”, en la página 445.

Espacio de nombres de Cognos

El espacio de nombres de Cognos es el espacio de nombres incorporado en el software de IBM Cognos. Contiene objetos de IBM Cognos, como grupos, roles, orígenes de datos, listas de distribución y contactos.

Durante la inicialización del almacén de contenido, se crean las entradas de seguridad predefinidas e incorporadas en este espacio de nombres Capítulo 15, “Seguridad inicial”, en la página 243. Debe modificar los valores de seguridad iniciales de esas entradas y del espacio de nombres de Cognos inmediatamente después de instalar y configurar el software de IBM Cognos “Valores de seguridad después de la instalación” en la página 254.

Puede cambiar el nombre del espacio de nombres de Cognos mediante IBM Cognos, pero no puede suprimirlo, ya que el espacio de nombres está siempre activo.

Cuando establezca la seguridad en el software de IBM Cognos, puede utilizar, si lo desea, el espacio de nombres de Cognos para crear grupos y roles específicos del software de IBM Cognos. En este espacio de nombres, también puede crear políticas de seguridad que hagan referencia de forma indirecta a las entradas de seguridad de los proveedores de autenticación, de forma que el software de IBM Cognos se pueda desplegar más fácilmente de una instalación a otra “Seguridad y despliegue” en la página 288.

El espacio de nombres de Cognos siempre existe en el software de IBM Cognos, pero el uso de los grupos y roles de Cognos que contiene es opcional. Los grupos

y roles creados en el espacio de nombres de Cognos vuelven a crear un paquete con los usuarios, los grupos y los roles existentes en los proveedores de autenticación, con el fin de optimizar su uso en el entorno IBM Cognos. Por ejemplo, en el espacio de nombres de Cognos, puede crear un grupo denominado Directores de recursos humanos y añadir usuarios y grupos concretos del departamento de TI de su empresa y de las organizaciones de recursos humanos definidas en su proveedor de autenticación. Posteriormente, puede establecer permisos de acceso al grupo Directores de recursos humanos para las entradas del software de IBM Cognos.

IBM Cognos Application Firewall

IBM Cognos Application Firewall (CAF) es una herramienta de seguridad que se utiliza para complementar la infraestructura de seguridad existente del software de IBM Cognos en el nivel de la aplicación. IBM Cognos Application Firewall analiza, modifica y valida las solicitudes HTTP y XML antes de que las pasarelas o los asignadores las procesen, y antes de su envío al servicio o al cliente que las solicite. Actúa como un proxy inteligente para las pasarelas y los asignadores del producto de IBM Cognos e impide que se entren datos malintencionados en los componentes de IBM Cognos. Las formas más habituales de datos malintencionados son los desbordamientos del búfer y los ataques cross-site scripting (XSS), ya sea mediante la inyección de scripts en páginas válidas o la redirección a otros sitios web.

IBM Cognos Application Firewall proporciona a los componentes de IBM Cognos características de seguridad, que incluyen validación y protección de datos, registro y supervisión y protección de la salida. Para obtener más información, consulte: “Validación y protección de datos” y “Registro y supervisión” en la página 204.

IBM Cognos Application Firewall está habilitado de forma predeterminada y no se debe inhabilitar.

Puede actualizar IBM Cognos Application Firewall de forma independiente al resto de componentes de IBM Cognos.

Para obtener más información sobre el cortafuegos de la aplicación IBM Cognos, consulte la *Guía de instalación y configuración*.

Validación y protección de datos

La validación de los datos de entrada garantiza que éstos se encuentren en el formato esperado, según un conjunto de reglas variables predefinidas. Las variables HTML, los datos XML, los valores de cookies y los parámetros se comprueban con este conjunto de reglas.

IBM Cognos Application Firewall (CAF) realiza una validación positiva de los parámetros, en lugar de sólo buscar las etiquetas conocidas de inyección de scripts o las firmas de inyección SQL habituales. Cada uno de los parámetros se valida en relación a una regla que espera un determinado tipo de datos en un determinado formato. Si los datos no coinciden con la regla de CAF, éstos se rechazarán.

Para proporcionar una validación aún más sólida, CAF busca la coincidencia con patrones de expresiones regulares, con el fin de proteger las entradas de datos que utilicen formatos complicados.

Un tipo habitual de ataque consiste en engañar a un usuario para que acceda a un sitio peligroso mediante la modificación de los parámetros del formulario. El botón Atrás y las características de URL de error de un producto constituyen el objetivo principal de este tipo de ataque.

CAF limita la lista de hosts y dominios a los que un URL de retorno puede acceder. CAF se puede configurar con una lista de nombres de host, incluidos los números de puerto y los dominios. Si un URL de retorno contiene un host o un dominio que no aparece en la lista, la solicitud se rechazará. De forma predeterminada, el nombre de host del asignador se añadirá a la lista. Puede configurar esta lista mediante IBM Cognos Configuration.

Para obtener más información, consulte *Guía de instalación y configuración*.

Registro y supervisión

IBM Cognos Application Firewall (CAF) puede supervisar y registrar todo el acceso a las pasarelas y los asignadores de IBM Cognos. Utilice el registro para realizar un seguimiento de los posibles ataques o del uso incorrecto de las aplicaciones de IBM Cognos.

Puede configurar CAF para registrar el acceso a un archivo específico o para utilizar el registro de la aplicación de registro de IBM Cognos (IPF). Si el registro está habilitado, se registrarán todas las solicitudes que no superen la validación de CAF.

Para obtener más información, consulte *Guía de instalación y configuración*.

Puede utilizar el registro de solicitudes del servidor web para obtener información detallada sobre la dirección IP del cliente de origen en un ataque sospechoso.

Codificación cross-site scripting (XSS)

Muchos clientes utilizan otras aplicaciones, como eTrust SiteMinder, para comprobar las vulnerabilidades de cross-site scripting. Estos productos bloquean las solicitudes de obtención de HTTP que contengan caracteres específicos.

CAF codifica los caracteres en CSS (hojas de estilo en cascada) con URL para impedir que otras herramientas de cross-site scripting bloqueen los caracteres.

La característica de codificación XSS de CAF sólo se aplica a los clientes que utilicen el portal de IBM Cognos Analytics.

De forma predeterminada, la codificación XSS de CAF está inhabilitada. Para habilitar esta característica, utilice IBM Cognos Configuration.

Para obtener más información, consulte *Guía de instalación y configuración*.

Filtrado de mensajes de error

Algunos mensajes de error pueden contener información confidencial, como nombres de servidor. De forma predeterminada, los detalles de los mensajes de error del software de IBM Cognos se enrutan hacia archivos de registro de IPF; además, se habilita la opción de mensajes de error de protección. La información que ven los usuarios solamente indica la aparición de un error, pero ningún detalle adicional.

Para especificar quién puede recuperar todos los detalles del error, entre los que se puede incluir información confidencial, cambie la función **Errores detallados** en la administración de IBM Cognos. Normalmente esta función se asigna a los administradores de directorios, pero también se puede asignar a otros usuarios. Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Para obtener información sobre la recuperación de todos los detalles del error, consulte “Visualización detallada de los mensajes de error de protección” en la página 23.

Firma de parámetros

La firma de parámetros protege los valores de los parámetros frente a modificaciones cuando se envían a un navegador web. CAF puede firmar parámetros o partes específicas de los datos. La firma sólo se utiliza en situaciones concretas. Está habilitada siempre que lo esté CAF.

Capítulo 11. Usuarios, grupos y roles

Los usuarios, grupos y roles se crean con fines de autenticación y autorización.

Puede utilizar grupos y roles creados en el software de IBM Cognos, así como usuarios, grupos y roles creados en proveedores de autenticación. Los grupos y roles creados en el software de IBM Cognos se conocen como grupos de Cognos y roles de Cognos.

Usuarios

Las entradas de usuarios se crean y se mantienen en un proveedor de autenticación con el fin de identificar de forma exclusiva una cuenta humana o informática. No puede crear entradas de usuario en el software de IBM Cognos.

En los proveedores se almacena la información relacionada con los usuarios, como nombres y apellidos, contraseñas, identificadores, entornos locales y direcciones de correo electrónico. Sin embargo, puede que esta información no incluya todo lo que necesite el software de IBM Cognos. Por ejemplo, no especifica la ubicación de las carpetas personales de los usuarios, ni las preferencias de formato para la visualización de informes. Esta información adicional sobre los usuarios se almacena en el software de IBM Cognos, pero, cuando se procesa en el software de IBM Cognos, la información aparece como parte del espacio de nombres externo.

Usuarios de Series 7

Si ha configurado el proveedor de autenticación de IBM Cognos Series 7, un usuario de ese espacio de nombres deberá pertenecer al menos a una clase de usuario de Access Manager para que el usuario se pueda utilizar en el software de IBM Cognos. Para obtener más información, consulte “Proveedores de autenticación” en la página 199.

Por ejemplo, si crea un usuario en Series 7 Access Manager y lo asigna a una clase de usuario pero, a continuación, elimina al usuario de esa clase, no podrá iniciar sesión como ese usuario en el software de IBM Cognos.

Supresión y nueva creación de usuarios

En los proveedores de autenticación Series 7, no se pueden mantener propiedades ni elementos asociados al suprimir y volver a crear un usuario. Por ejemplo, si un usuario crea un objeto en **Mis carpetas** y, a continuación, se suprime ese usuario, el objeto **Mis carpetas** dejará de estar asociado a ese usuario. Si se vuelve a crear un usuario con el mismo nombre, no se volverán a crear instancias de los objetos.

Si utiliza un servidor LDAP, la estabilidad de los objetos **Mis carpetas** dependerá de cómo se utilicen los identificadores. Si en la configuración del proveedor LDAP se utiliza el atributo predeterminado dn para el parámetro Identificador exclusivo, una instancia del usuario creada nuevamente con el mismo nombre conserva los objetos **Mis carpetas** del usuario original. Si cambia el parámetro Identificador exclusivo por un atributo exclusivo establecido mediante el servidor LDAP, por ejemplo, nsuniqueid en Sun Java System, se perderá la asociación de los objetos **Mis carpetas** para un usuario suprimido, además de crearse un nuevo objeto **Mis carpetas** para un usuario con el mismo nombre.

Los perfiles de usuario se pueden suprimir, copiar y cambiar. Para obtener más información, consulte Capítulo 21, “Administración de perfiles de usuario”, en la página 323.

Entornos locales del usuario

Un entorno local especifica la información lingüística y las convenciones culturales para el tipo de carácter, ordenación, formato de fecha y hora, unidad de moneda y mensajes. Puede especificar entornos locales para distintos productos, contenidos, servidores, autores y usuarios del software de IBM Cognos.

El entorno local del usuario hace referencia al entorno local del contenido y producto de cada usuario de IBM Cognos. Las solicitudes de los usuarios se reciben con un entorno local asociada. El software de IBM Cognos debe determinar las preferencias de entorno local y de idioma de los usuarios, además de aplicar un entorno local de respuesta adecuada al distribuir los informes en distintos idiomas.

Los entornos locales del usuario especifican los valores predeterminados que el usuario desea para el formateo de fecha, hora, moneda y número. El software de IBM Cognos utiliza esta información para presentar los datos al usuario.

El software de IBM Cognos obtiene el valor del entorno local del usuario mediante la comprobación de estos orígenes, en el orden indicado:

- Valores de preferencias del usuario
Si el usuario establece los valores de preferencias de usuario correspondientes, el software de IBM Cognos utilizará estos valores para el entorno local del contenido y de producto del usuario, así como para las opciones de formateo predeterminadas. Los valores de preferencias del usuario reemplazan los valores obtenidos del proveedor de autenticación.
- Proveedor de autenticación
Si el proveedor de autenticación tiene ya establecido un entorno local, el software de IBM Cognos utilizará esos valores para el entorno local del contenido y de producto del usuario.
- Valor del navegador
Los usuarios anónimos e invitados no pueden establecer los valores de preferencias. En el caso de esos usuarios, el software de IBM Cognos obtiene un entorno local de usuario del navegador almacenado en el sistema del usuario.

Grupos y roles

Los grupos y los roles se pueden definir como se indica a continuación.

Los grupos  y los roles representan colecciones de usuarios que realizan funciones similares o que tienen un estado similar en una organización. Entre los ejemplos de grupos se encuentran los empleados, los desarrolladores o los vendedores. Los miembros de los grupos pueden ser usuarios y otros grupos. Cuando los usuarios inician sesión, no pueden seleccionar el grupo que desean utilizar para una sesión. Siempre inician sesión con todos los permisos asociados a los grupos a los que pertenecen.

Los roles  del software de IBM Cognos tiene una función similar a los grupos. Los miembros de los roles pueden ser usuarios, grupos y otros roles.

En el diagrama siguiente se muestra la estructura de los grupos y los roles.

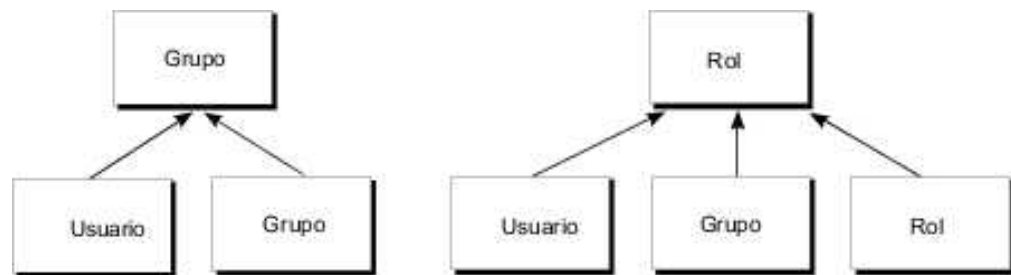


Figura 4. Estructura de grupos y roles

Los usuarios pueden convertirse en miembros de grupos y roles definidos en el software de IBM Cognos, así como en grupos y roles definidos en los proveedores de autenticación. Un usuario puede pertenecer a uno o más grupos o roles. Si los usuarios son miembros de más de un grupo, sus permisos de acceso se fusionan.

Los grupos y los roles de Cognos se crean cuando

- No se pueden crear grupos ni roles en el proveedor de autenticación.
- Se necesitan grupos o roles que incluyan varios espacios de nombres.
- Se necesitan grupos o roles portátiles que se puedan desplegar.

Cree los grupos y roles necesarios en el proveedor de autenticación y añádalos a los grupos y los roles adecuados de Cognos.

- Desea responder a necesidades concretas de administración de IBM Cognos.
- Desea evitar que se abarrotan los sistemas de seguridad de la organización con la información utilizada exclusivamente en el software de IBM Cognos.

Roles de Series 7

Si ha configurado el proveedor de autenticación de IBM Cognos Series 7, las colecciones de usuarios, conocidas como clases de usuarios en Series 7, aparecerán como roles en el software de IBM Cognos. Puede acceder a Series 7 y al software de IBM Cognos mediante un solo inicio de sesión. Si inicia la sesión mediante Series 7 y, a continuación, accede al software de IBM Cognos, asumirá automáticamente los roles que se aplicaban en Series 7 al iniciar sesión por primera vez. No se pueden asumir distintos roles de Series 7. Para obtener más información sobre la configuración del proveedor de autenticación, consulte "Proveedores de autenticación" en la página 199.

Los usuarios pueden asumir distintos roles en Series 7 después de acceder al software de IBM Cognos.

Roles utilizados para ejecutar informes y trabajos

Los roles utilizados para ejecutar informes y trabajos están asociados a los usuarios que ejecutan los informes de forma interactiva, que son los propietarios de los informes, y cuyas credenciales se utilizan para ejecutar informes y trabajos planificados. El proceso puede asumir distintos roles en función de las opciones seleccionadas para ejecutar los informes.

- Cuando se ejecuta un informe que tiene seleccionada la opción Ejecutar como propietario, el proceso asume todos los roles asociados al propietario del informe.

- Cuando se ejecuta un informe o un trabajo planificado, la sesión asume todos los roles asociados al usuario cuyas credenciales se utilizaron para procesar la solicitud “Credenciales de confianza” en la página 222.

Listas de distribución como miembros de grupos y roles

En algunos espacios de nombres, como Microsoft Active Directory, una lista de distribución puede aparecer en la pestaña **Miembros** de la página **Establecer propiedades** de un grupo o un rol. Sin embargo, no puede añadir listas de distribución a los miembros de un grupo o un rol, ni tampoco puede utilizarlos para establecer permisos de acceso a entradas de la interfaz de usuario de IBM Cognos.

Puede añadir una lista de distribución de IBM Cognos como miembro de un grupo o un rol de Cognos mediante Software Development Kit. Sin embargo, el Software Development Kit no se puede utilizar para añadir una lista de distribución de Active Directory a un grupo de Active Directory. Para realizar este proceso se deben utilizar las herramientas de administración de Active Directory.

Grupos y roles de IBM Cognos Controller

Para el software de IBM Cognos, utilice los grupos y roles de IBM Cognos Controller para configurar la seguridad. Para obtener información sobre el uso de estos grupos y roles para configurar la seguridad, consulte IBM Cognos Controller *Installation and Configuration Guide*.

Creación de un grupo o un rol de Cognos

Puede añadir entradas de varios espacios de nombres, creadas tanto en los proveedores de autenticación como en el software de IBM Cognos, como miembros de grupos de Cognos. También puede crear grupos vacíos sin ningún miembro.

Los miembros de grupos de Cognos pueden ser usuarios u otros grupos. Los miembros de roles de Cognos pueden ser usuarios, grupos u otros roles.

Si desea crear grupos o roles que hagan referencia a entradas de varios espacios de nombres, deberá iniciar una sesión en cada uno de los espacios de nombres antes de comenzar su tarea. De otro modo, no contará con todos los derechos administrativos para las entradas a las que desee hacer referencia.

Se recomienda utilizar los grupos y los roles de Cognos para configurar los permisos de acceso a las entradas del software de IBM Cognos, ya que simplifican el proceso de despliegue. Para obtener más información, consulte “Seguridad y despliegue” en la página 288.

Al suprimir un grupo o un rol de Cognos, los permisos de acceso de los usuarios basados en él dejan de estar activos. No se pueden restaurar los permisos de acceso creando un grupo o un rol con el mismo nombre.

Para administrar usuarios, grupos y roles, debe tener permisos de ejecución para la característica protegida **Usuarios, grupos y roles**, así como permisos de visita para la función protegida **Administración**. Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
2. Pulse el espacio de nombres **Cognos**.

Consejo: Si desea suprimir un grupo o un rol de Cognos, seleccione la casilla de verificación situada junto a él y pulse el botón **Suprimir**.

3. En la barra de herramientas, pulse el botón **Nuevo grupo**  o **Nuevo rol** .
4. En la página **Especificar un nombre y una descripción**, escriba un nombre y, si lo desea, una descripción para el nuevo grupo o rol y, a continuación, seleccione una carpeta de destino y pulse **Siguiente**.
5. Si desea crear un grupo sin miembros, pulse **Finalizar**.
6. Si desea añadir miembros al nuevo grupo o rol, pulse **Añadir** y elija cómo seleccionar usuarios, grupos o roles:
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, grupos o roles.
 - Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
 - Para escribir el nombre de las entradas que desea añadir, pulse **Tipo** y escriba los nombres de grupos, roles o usuarios mediante el formato siguiente, donde un punto y coma (;) separa cada entrada:
`espacio_nombres/nombre_grupo;espacio_nombres/nombre_rol;espacio_nombres/nombre_usuario;;`
A continuación se incluye un ejemplo:
`Cognos/Authors;LDAP/scarter;`
7. Pulse el botón de flecha a la derecha y, cuando aparezcan las entradas que desea en el cuadro **Entradas seleccionadas**, pulse **Aceptar**.

Consejo: Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista. Para hacer visibles las entradas del usuario, pulse **Mostrar usuarios en la lista**.

8. Pulse **Finalizar**.

Adición o eliminación de miembros de un grupo o un rol de Cognos

Para modificar los miembros de un grupo o un rol de Cognos, añada o elimine miembros.

Al suprimir usuarios, grupos o roles de un grupo o un rol de Cognos, no se suprimen del proveedor de autenticación ni del software de IBM Cognos.

Si desea modificar grupos o roles que hagan referencia a entradas de varios espacios de nombres, deberá iniciar una sesión en cada uno de los espacios de nombres antes de comenzar su tarea. De otro modo, no contará con todos los derechos administrativos para las entradas que desee modificar.

Para administrar usuarios, grupos y roles, debe tener permisos de ejecución para la característica protegida **Usuarios, grupos y roles**, así como permisos de visita para

la función protegida **Administración**. Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
2. Pulse el espacio de nombres **Cognos**.
3. En la columna **Acciones**, pulse el botón **Propiedades** del grupo o el rol cuyos miembros desee modificar.
4. Pulse la pestaña **Miembros**.
5. Si desea añadir miembros, pulse **Añadir** y elija cómo seleccionar los miembros:
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, grupos o roles.
 - Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
 - Para escribir el nombre de las entradas que desea añadir, pulse **Tipo** y escriba los nombres de grupos, roles o usuarios mediante el siguiente formato, en donde un punto y coma (;) separa cada entrada.
espacio_nombres/nombre_grupo;espacio_nombres/nombre_rol;espacio_nombres/nombre_usuario;
A continuación se incluye un ejemplo:
Cognos/Authors;LDAP/scarter;
6. Pulse el botón de flecha a la derecha y, cuando aparezcan las entradas que desea en el cuadro **Entradas seleccionadas**, pulse **Aceptar**.

Consejo: Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista. Para hacer visibles las entradas del usuario, pulse **Mostrar usuarios en la lista**.
7. Para eliminar los miembros de un grupo o un rol de Cognos, en la página **Establecer propiedades** especifique los usuarios, los grupos o los roles que desee eliminar y pulse **Eliminar**.
8. Pulse **Aceptar**.

Capítulo 12. Permisos de acceso y credenciales

Los permisos de acceso y las credenciales se utilizan para proteger los datos de la organización. Especifique los usuarios y los grupos que tienen acceso a un informe específico o a otro contenido del software de IBM Cognos. También puede especificar las acciones que pueden llevar a cabo en el contenido.

Al establecer los permisos de acceso, puede hacer referencia tanto a usuarios, grupos y roles de proveedor de autenticación como a grupos y roles de Cognos. Sin embargo, si piensa desplegar su aplicación en el futuro, le recomendamos que utilice únicamente los grupos y los roles de Cognos para configurar el acceso a las entradas del software de IBM Cognos y así simplificar el proceso.

Permisos y acciones permitidas

En la tabla siguiente se describen los permisos de acceso que puede otorgar o denegar.

Tabla 51. Permisos y acciones permitidas

Permisos	Iconos	Acciones permitidas
Lectura	  	Visualizar todas las propiedades de una entrada, incluida la especificación de informe, la salida de informe, etc. que son propiedades de un informe.
Escritura	  	Modificar las propiedades de una entrada. Suprimir una entrada. Crear entradas en un contenedor, como un paquete o una carpeta. Modificar la especificación de informe para los informes creados en Creación de informes y Query Studio. Crear nuevas salidas para un informe.

Tabla 51. Permisos y acciones permitidas (continuación)

Permisos	Iconos	Acciones permitidas
Ejecución	  	Procesar una entrada Para entradas como informes, agentes y métricas, el usuario puede ejecutar la entrada. Para orígenes de datos, conexiones e inicios de sesión, las entradas se pueden utilizar para recuperar datos del proveedor de datos. El usuario no puede leer la información de la base de datos directamente. El servidor de informes puede acceder, en nombre del usuario, a la información de la base de datos para procesar una solicitud. Antes de que un usuario pueda utilizar una entrada, el software de IBM Cognos verifica si posee permisos de ejecución para la misma. En lo que a las credenciales se refiere, los usuarios pueden permitir que otra persona utilice las suyas. Nota: Los usuarios deben contar con permisos de ejecución para la cuenta que utilicen con la ejecución como opción de informe de propietario.
Estable- cimiento de políticas	  	Leer y modificar los valores de seguridad para una entrada.
Visita	  	Visualice los contenidos de una entrada de contenedor, como un paquete o una carpeta, y las propiedades generales del propio contenedor sin acceso completo al contenido. Nota: Los usuarios pueden visualizar las propiedades generales de las entradas para las que posean cualquier tipo de acceso. Las propiedades generales incluyen nombre, descripción, fecha de creación, etc., que son comunes a todas las entradas.

Permisos de acceso para los usuarios

Los usuarios deben contar al menos con permisos de visita para las entradas padre de las entradas a las que desean acceder. Las entradas padre incluyen objetos contenedor como carpetas, paquetes, grupos, roles y espacios de nombres.

Los permisos para los usuarios se basan en conjuntos de permisos para cuentas de usuario individuales y para los espacios de nombres, grupos y roles a los que pertenecen los usuarios. Los permisos también se ven afectados por las propiedades de miembro y propietario de la entrada.

El software de IBM Cognos soporta permisos de acceso combinados. Cuando los usuarios que pertenecen a más de un grupo inician una sesión, cuentan con permisos combinados para todos los grupos a los que pertenecen. Es importante que recuerde esto, especialmente si va a denegar algún acceso.

Sugerencia: Para garantizar que un usuario o un grupo pueda ejecutar informes desde un paquete, pero no pueda abrir el paquete en un estudio de IBM Cognos, otorgue al usuario o al grupo permisos de ejecución y visita para el paquete. Los usuarios también necesitan permisos de lectura para el paquete con el fin de lanzar estudios.

Permisos de acceso necesarios para las acciones

Para realizar acciones específicas, cada usuario, grupo o rol necesita que se le otorgue la combinación de permisos de acceso adecuada para la entrada, su entrada padre y su entrada de origen y de destino. La siguiente tabla incluye los permisos necesarios para acciones específicas.

Tabla 52. Permisos de acceso necesarios para las acciones

Acción	Permisos necesarios
Añadir una entrada	Permisos de escritura para una entrada padre
Solicitar las propiedades de una entrada	Permisos de lectura para una entrada
Ver los hijos de una entrada	Permisos de visita para una entrada
Actualizar una entrada	Permisos de escritura para una entrada
Suprimir una entrada	Permisos de escritura para una entrada y permisos de escritura para una entrada padre
Copiar una entrada	Permisos de escritura para una entrada y cualquier entrada hijo, permisos de visita para todos los hijos y permisos de escritura y de visita para la entrada padre destino
Mover una entrada	Permisos de lectura y escritura para una entrada, permisos de escritura tanto para la entrada padre origen y la entrada padre destino y permisos de visita para la entrada padre destino

Permisos y acciones permitidas para los informes de Cognos Workspace

Los usuarios de Cognos Workspace pueden realizar o no acciones en función de sus permisos y combinaciones de permisos para los objetos de informe, parte de informe, carpeta de informe o espacio de trabajo. Al propietario de un objeto se le otorga automáticamente permisos de lectura, escritura, visita y ejecución. Si un objeto está inhabilitado, debe tener otorgado acceso de escritura para verlo y editarlo.

En el caso de los informes, los usuarios con los permisos de acceso y las combinaciones de permisos siguientes pueden realizar las acciones siguientes:

Tabla 53. Permisos de acceso y acciones permitidas con los informes

Permisos	Acciones permitidas
Lectura	Los usuarios pueden ver el informe en el panel de contenido. Los usuarios no pueden expandir el informe para mostrar las partes del informe. Los usuarios no pueden arrastrar el informe.
Lectura y visita	Los usuarios pueden ver el informe en el panel de contenido. Los usuarios no pueden expandir el informe para mostrar las partes del informe. Si existe salida guardada, los usuarios pueden arrastrar el informe al lienzo y ver la salida guardada. Si no hay salida guardada, los usuarios no pueden arrastrar el informe. Si intentan esta acción, los usuarios ven en el widget el mensaje de error: No se puede mostrar el contenido. Es posible que se haya suprimido o que no cuente con los privilegios suficientes. Los usuarios pueden ver la salida guardada en el espacio de trabajo. Los usuarios no pueden ejecutar un informe dinámico en un espacio de trabajo. Si intentan esta acción, los usuarios ven el mensaje de error: RSV-CM-0006. El usuario no dispone de permiso de ejecución para este informe.
Ejecución	Los usuarios pueden ver el informe en el panel de contenido. Los usuarios no pueden expandir el informe para mostrar las partes del informe. Los usuarios pueden ejecutar el informe, pero las interacciones no están disponibles. Las interacciones no están disponibles si: • Se arrastra un informe al lienzo. • Un usuario con permisos de ejecución guarda un informe y otros usuarios lo abren. • Un usuario con permisos de ejecución abre un espacio de trabajo creado por otros usuarios. Cuando la salida guardada no se puede ver en un espacio de trabajo, los usuarios ven el mensaje de error: No se puede mostrar el contenido. Es posible que se haya suprimido o que no cuente con los privilegios suficientes.

Tabla 53. Permisos de acceso y acciones permitidas con los informes (continuación)

Permisos	Acciones permitidas
Lectura y ejecución	Los usuarios pueden ver el informe en el panel de contenido. Los usuarios pueden expandir el informe para mostrar las partes del informe. Los usuarios pueden ejecutar el informe y las interacciones están disponibles. En el panel de contenido, los usuarios no pueden guardar los cambios del informe. Si los usuarios añaden el informe al espacio de trabajo y lo guardan, los cambios del informe pueden guardarse. Si otra persona distinta del propietario del informe añade el informe al espacio de trabajo, ese usuario no puede guardar los cambios. El usuario ve el mensaje de error: El contenido no se puede guardar. No dispone de derechos suficientes.
Lectura, ejecución, visita	Los usuarios pueden ver el informe en el panel de contenido. Los usuarios pueden expandir el informe para mostrar las partes del informe. En el panel de contenido, los usuarios pueden ejecutar el informe y las interacciones están disponibles. Los usuarios pueden añadir el informe al lienzo como salida dinámica o guardada. El tipo de informe que se añade depende de la acción predeterminada especificada en las propiedades del informe.
Lectura, escritura, ejecución, visita	Los usuarios pueden ver el informe en el panel de contenido. Los usuarios pueden expandir el informe para mostrar las partes del informe. Los usuarios pueden añadir el informe al espacio de trabajo. Los usuarios pueden ejecutar el informe y las interacciones están disponibles. Los usuarios pueden cambiar y guardar el informe. Los usuarios pueden añadir el informe al lienzo como salida dinámica o guardada. El tipo de informe que se añade depende de la acción predeterminada especificada en las propiedades del informe.
Lectura, ejecución, establecimiento de política	Los usuarios pueden ver el informe en el panel de contenido. Los usuarios pueden expandir el informe para mostrar las partes del informe. Los usuarios pueden ejecutar el informe y las interacciones están disponibles. En el panel de contenido, los usuarios no pueden guardar los cambios del informe. Si los usuarios arrastran el informe al espacio de trabajo y lo guardan, los cambios del informe pueden guardarse. Esta acción crea una copia del informe. El informe del espacio de trabajo copiado hereda los permisos del informe original si el usuario tiene permiso para establecer políticas.

En el caso de las partes de informe, los usuarios con los permisos de acceso y las combinaciones de permisos siguientes pueden realizar las acciones siguientes:

Tabla 54. Permisos de acceso y acciones permitidas con las partes de informe

Permisos	Acciones permitidas
Lectura y ejecución	Los usuarios pueden ver el informe. Los usuarios pueden expandir el informe para mostrar las partes del informe. Los usuarios pueden arrastrar la parte de informe al lienzo y pueden ejecutar la parte de informe.

En el caso de las carpetas, los usuarios con los permisos de acceso y las combinaciones de permisos siguientes pueden realizar las acciones siguientes:

Tabla 55. Permisos de acceso y acciones permitidas con las carpetas

Permisos	Acciones permitidas
Lectura	Los usuarios pueden ver la carpeta en el panel de contenido y pueden leer las propiedades de la carpeta. Los usuarios no pueden arrastrar la carpeta al lienzo. Los usuarios no pueden expandir la carpeta para mostrar el contenido. Los usuarios no pueden guardar objetos de espacio de trabajo en esta carpeta.
Visita	Los usuarios pueden arrastrar la carpeta al lienzo. Los usuarios pueden expandir la carpeta para mostrar el contenido. Los usuarios no pueden guardar objetos de espacio de trabajo en esta carpeta.
Escritura y visita	Los usuarios pueden arrastrar la carpeta al lienzo. Los usuarios pueden expandir la carpeta para mostrar el contenido. Los usuarios pueden guardar objetos de espacio de trabajo en esta carpeta.

En el caso de los espacios de trabajo, los usuarios con los permisos de acceso y las combinaciones de permisos siguientes pueden realizar las acciones siguientes:

Tabla 56. Permisos de acceso y acciones permitidas con los espacios de trabajo

Permisos	Acciones permitidas
Lectura	Los usuarios pueden ver el espacio de trabajo. Los usuarios no pueden abrir el espacio de trabajo.
Lectura y visita	Los usuarios pueden abrir el espacio de trabajo. Con el permiso de visita, los usuarios pueden ver los widgets del espacio de trabajo.

Tabla 56. Permisos de acceso y acciones permitidas con los espacios de trabajo (continuación)

Permisos	Acciones permitidas
Lectura, escritura y visita	Los usuarios pueden ver, abrir y guardar el espacio de trabajo.

Propiedad de entradas

Si el usuario es propietario de una entrada, éste contará con permisos de acceso completo para la entrada. Esto garantiza que los usuarios siempre pueden acceder a las entradas que poseen y modificarlas. De forma predeterminada, el propietario de una entrada es el usuario que la crea. Sin embargo, cualquier otro usuario que cuente con permisos para establecer política para la entrada puede hacerse con la propiedad de la entrada.

Acceso otorgado y denegado

Puede otorgar o denegar el acceso a las entradas. Un icono que representa el tipo de acceso aparece junto al nombre de la entrada en la pestaña **Permisos**. Por ejemplo, cuando un grupo dispone de permisos de ejecución para un informe, aparece este icono  junto al nombre del grupo en la pestaña **Permisos** del informe. Cuando un grupo no dispone de permisos de ejecución para un informe, aparece este icono  junto al nombre del grupo.

El acceso denegado tiene prioridad sobre el acceso otorgado. Al denegar a determinados usuarios o grupos el acceso a una entrada, se sustituyen otras políticas de seguridad que otorgan el acceso a la entrada.

Si los permisos otorgados y denegados entran en conflicto, el acceso a la entrada siempre se deniega. Por ejemplo, un usuario pertenece a dos grupos. Un grupo tiene otorgado el acceso a un informe y el otro grupo tiene denegado el acceso al mismo informe. El usuario tendrá denegado el acceso a este informe.

Deniegue el acceso únicamente cuando sea realmente necesario. Por lo general, resulta una mejor práctica administrativa otorgar permisos que denegarlos.

Permisos de elementos padre e hijo

Los permisos de acceso se adquieren de las entradas padre. Si los permisos de acceso no están definidos, la entrada adquiere los permisos de su entrada padre. Puede sustituir los permisos de elementos padre definiendo permisos para la entrada hijo.

Los objetos que únicamente existen como hijos de otros objetos siempre adquieren permisos de sus elementos padre. Un ejemplo de este tipo de objeto son las especificaciones de informe y las salidas de informe. Se pueden visualizar mediante el Software Development Kit. No puede establecer permisos específicamente para dichos objetos.

Permisos y despliegue

Si es un administrador que está desplegando en un entorno de destino, consulte: Capítulo 19, “Despliegue”, en la página 287.

Permisos de funciones

Si es un administrador, puede establecer el acceso a las funciones y las características protegidas otorgando permisos de ejecución para espacios de nombres, usuarios, grupos o roles específicos. Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Supresión de grupos y roles de Cognos

Cuando se suprime un grupo o un rol de Cognos, los permisos de acceso basados en ese grupo o rol también se suprimen. No podrá restablecerlos mediante la creación de un nuevo grupo o rol con el mismo nombre, puesto que esta entrada posee un ID interno diferente.

Si los proveedores de autenticación crean los grupos o roles, compruebe que su proveedor de autenticación sepa manejar dichas situaciones. Por lo general, no se pueden crear permisos de acceso si éstos están basados en los ID; por el contrario, pueden crearse si se basan en nombres.

Acceso a entradas asociadas con orígenes de datos protegidos frente a múltiples espacios de nombres

Los orígenes de datos en el software de IBM Cognos pueden protegerse contra múltiples espacios de nombres. En algunos entornos, el espacio de nombres utilizado para proteger el origen de datos no es el espacio de nombres principal utilizado para acceder a IBM Cognos Analytics. Cuando intente acceder a una entrada, como un informe, una consulta o un análisis que esté asociado a un origen de datos protegido frente a múltiples espacios de nombres y no se haya iniciado sesión en todos los espacios de nombres necesarios, se mostrará una solicitud de autenticación. Debe iniciar una sesión en el espacio de nombres para poder acceder a la entrada.

Cuando el inicio de sesión único (SSO) está habilitado, la solicitud de autenticación no aparece. Se iniciará la sesión automáticamente en el espacio de nombres.

Esta funcionalidad se aplica únicamente a IBM Cognos Viewer. Si se produce una situación similar en un estudio de IBM Cognos, debe salir de la tarea e iniciar sesión en todos los espacios de nombres que desee utilizar en la sesión actual.

Establecimiento de permisos de acceso para una entrada

El establecimiento de los permisos de accesos para una entrada incluye la creación de nuevos permisos o la actualización de los existentes. Puede especificar permisos de acceso para todas las entradas del software de IBM Cognos. Algunos ejemplos de dichas entradas son los informes, consultas, análisis, paquetes, agentes, métricas, espacios de nombres, grupos, usuarios o asignadores. Puede hacer referencia a usuarios, grupos y roles desde espacios de nombres diferentes en una política de seguridad de una entrada.

Si tiene previsto hacer referencia a entradas desde varios espacios de nombres, inicie sesión en cada espacio de nombres antes de empezar a establecer los

permisos de acceso. De lo contrario, las entradas de los espacios de nombres en los que no haya iniciado sesión aparecerán como **No disponible**.

Las entradas a las que hace referencia una política de seguridad también pueden aparecer como **No disponible** cuando

- Se han suprimido recientemente desde un espacio de nombres externo.
El software de IBM Cognos no tiene control alguno sobre el contenido de los proveedores de seguridad.
- Las entradas están asociadas a un espacio de nombres externo que se ha suprimido recientemente.

Para evitar este problema, ejecute el tipo de comprobación de consistencia de la tarea de mantenimiento de contenido seleccionando la opción **Referencias a espacios de nombres externos**. Content Manager suprime las entradas asociadas a los espacios de nombres suprimidos de las políticas de seguridad.

Para obtener más información, consulte “Tareas de mantenimiento del almacén de contenido” en la página 71.

Para administrar la seguridad, debe tener permisos para establecer política. Para obtener más información, consulte Capítulo 12, “Permisos de acceso y credenciales”, en la página 213.

Procedimiento

1. En el software de IBM Cognos, localice la entrada para la que desee establecer los permisos de acceso.
2. En la columna **Acciones**, pulse el botón Establecer propiedades  para la entrada.
3. En la página **Establecer propiedades**, pulse la pestaña **Permisos**.
4. Seleccione si desea utilizar los permisos de la entrada padre o especificar permisos específicamente para la entrada:
 - Para utilizar los permisos de la entrada padre, desactive la casilla de verificación **Reemplazar los permisos de acceso adquiridos de la entrada padre**, luego pulse Aceptar si se le solicita que utilice los permisos de elementos principales. Pulse **Aceptar**.
 - Para establecer los permisos de acceso para la entrada, seleccione la casilla de verificación **Reemplazar los permisos de acceso adquiridos de la entrada padre**, luego continúe con el paso 5.
5. Si desea eliminar una entrada de la lista, seleccione su casilla de verificación y pulse **Eliminar**.

Consejo: Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

6. Para especificar las entradas para las que desea otorgar o denegar accesos, pulse **Añadir** y luego escoja cómo seleccionar las entradas:
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, grupos o roles.
 - Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.

- Para introducir el nombre de las entradas que desea añadir, pulse **Tipo** e introduzca los nombres de grupos, roles o usuarios mediante el siguiente formato, en donde un punto y coma (;) separa cada entrada.

*espacio_nombres/nombre_grupo;espacio_nombres/
nombre_rol;espacio_nombres/nombre_usuario;*

A continuación se incluye un ejemplo:

Cognos/Authors;LDAP/scarter;

7. Pulse el botón de flecha a la derecha y, cuando aparezcan las entradas que desea en el cuadro **Entradas seleccionadas**, pulse **Aceptar**.

Consejo: Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista. Para hacer visibles las entradas del usuario, pulse **Mostrar usuarios en la lista**.

8. Para cada entrada de la lista, en el cuadro situado junto a la lista, seleccione o desactive casillas de verificación para especificar qué tipo de acceso desea otorgar o denegar.

9. Pulse **Aceptar**.

En la columna **Permisos**, aparecerá un icono junto al usuario, el grupo o el rol. Este icono representa el tipo de acceso otorgado o denegado a la entrada.

10. Si desea eliminar permisos de acceso que se establecieron anteriormente para las entradas hijo, de forma que éstas puedan obtener permisos configurados para esta entrada, en la sección **Opción**, seleccione la casilla de verificación **Suprimir los permisos de acceso de todas las entradas hijo**.

Esta opción sólo aparece con entradas que sean contenedores. Puede utilizarla para restringir el acceso a una jerarquía de entradas.

Aviso: Seleccione esta opción únicamente cuando tenga la certeza de que es seguro cambiar los permisos de acceso de las entradas hijo.

11. Pulse **Aceptar**.

Credenciales de confianza

Las credenciales de confianza se utilizan para los usuarios que deben llevar a cabo una tarea o proceso pero que no poseen los suficientes permisos de acceso para las entradas que contienen datos sensibles, como inicios de sesión en la base de datos y miembros de grupo. Los usuarios con permisos de acceso más amplios, que poseen las entradas, pueden autorizar a otros usuarios de confianza a que utilicen sus credenciales para acceder a dichas entradas.

Las credenciales de confianza también se utilizan para ejecutar solicitudes planificadas para cuando los usuarios no han iniciado sesión en el software de IBM Cognos, por ejemplo por la noche. Cuando se ejecuta la solicitud, se crea una sesión de usuario. La credencial de confianza se utiliza para iniciar una sesión en el software de IBM Cognos con el usuario que represente la credencial de confianza, y los permisos de acceso del usuario se utilizan para ejecutar el informe o el trabajo.

Las credenciales de confianza se almacenan como parte del objeto de la cuenta en el espacio de nombre.

De manera predeterminada, las credenciales de confianza se renuevan automáticamente una vez al día. Un administrador puede cambiar la frecuencia de renovación al especificar la propiedad **expiryRenewedTC** en IBM Cognos

Configuration, bajo las propiedades **Seguridad > Autenticación > Propiedades avanzadas**. Solo enteros que representan la cantidad de sías se pueden utilizar como valores para esta propiedad. El valor mínimo es 1.

Cuando cambia su contraseña debe renovar sus credenciales manualmente. De lo contrario, si se utilizan las credenciales antes de renovarlas automáticamente, es posible que no funcionen. Por ejemplo, un trabajo programado que utiliza estas credenciales puede fallar. Para obtener información acerca de cómo renovar las credenciales de confianza manualmente, consulte “Creación de credenciales de confianza”.

Creación de credenciales de confianza

Puede crear credenciales de confianza cuando desee autorizar a otros usuarios a utilizar sus credenciales cuando dichos usuarios no tengan permisos de acceso suficientes para realizar determinadas tareas.

Para que los usuarios utilicen las credenciales de confianza se deben otorgar permisos de visita para el espacio de nombres.

Procedimiento

1. Pulse el botón Opciones de Mi área , **Mis preferencias**.
2. Si todavía no ha creado credenciales, en la pestaña **Personal**, en **Credenciales**, pulse **Crear credenciales**.

Consejo: Si las credenciales de confianza se ha creado, puede que solamente debe renovar la lista; para ello, pulse **Renovar credenciales**.

3. Seleccione los usuarios, grupos o roles que desea autorizar para el uso de sus credenciales.

Si se le solicitan sus credenciales, introduzca su identificador de usuario y contraseña.

4. Si desea añadir entradas, pulse **Añadir** y elija cómo seleccionar las entradas:
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, grupos o roles.
 - Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
 - Para introducir el nombre de las entradas que desea añadir, pulse **Tipo** e introduzca los nombres de grupos, roles o usuarios mediante el siguiente formato, en donde un punto y coma (;) separa cada entrada.
`namespace/group_name;namespace/role_name;namespace/user_name;`
A continuación se incluye un ejemplo:
`Cognos/Authors;LDAP/scarter;`
5. Si desea eliminar una entrada de la lista, seleccione la casilla de verificación que se encuentra junto a ella y pulse **Eliminar**.

Resultados

Los usuarios, grupos o roles que pueden utilizar sus credenciales se enumeran ahora en la sección **Credenciales**.

Administración de sus propias credenciales de origen de datos

Es importante administrar las credenciales de origen de datos para sus usuarios, porque estas credenciales son necesarias para determinadas tareas.

Las credenciales de origen de datos se le pueden solicitar cuando realice las acciones siguientes:

- Ver, ejecutar o abrir una entrada
- Utilizar una planificación o un trabajo
- Seleccionar los orígenes de datos que se pueden utilizar para crear un paquete

También se le pueden solicitar las credenciales de origen de datos cuando utilice Framework Manager (consulte Framework Manager *User Guide*).

Si es administrador, también puede crear o modificar inicios de sesión de origen de datos “Inicios de sesión de orígenes de datos” en la página 156. Sin embargo, si tiene un gran número de usuarios, esto puede resultar poco manejable para las configuraciones de orígenes de datos que requieren que cada usuario tenga su propio inicio de sesión, puesto que las credenciales de cada usuario deben crearse individualmente. También puede ver las credenciales de origen de datos de otros usuarios.

Tenga en cuenta que las credenciales se comprueban en el orden siguiente:

- En primer lugar, se comprueban los inicios de sesión que crea como administrador.
- Si no se encuentran credenciales para el usuario, se consulta el perfil del usuario para ver si tiene almacenadas sus propias credenciales.
- Si no se encuentran las credenciales del usuario en ninguno de estos lugares, se le solicitan al usuario.

Esto es importante porque, si crea credenciales después de que un usuario haya guardado sus propias credenciales, dicho usuario puede obtener datos relacionados con las credenciales que haya creado para él, y esto podría no ser lo que el usuario espera.

Antes de empezar

Si es un usuario, su administrador debe concederle permisos de ejecución para la función **Administrar inicios de sesión de origen de datos propios** y permisos de visita para sus ancestros. También debe tener permisos de lectura y visita sobre su propia cuenta. A continuación, puede guardar las credenciales en su perfil personal, siempre y cuando no tenga acceso a ningún inicio de sesión predefinido para el origen de datos. No se le pedirán las credenciales si tiene permiso para acceder a una credencial de origen de datos existente y ha guardado la credencial personal en su perfil. Puede ver y suprimir sus credenciales de origen de datos en la página **Mis preferencias**.

Para ver las credenciales de otro usuario, debe tener permisos de lectura y visita para la cuenta del usuario. Para eliminar las credenciales del origen de datos, debe tener permisos de lectura, escritura y visita para la cuenta del usuario.

Cómo guardar credenciales de origen de datos

Puede guardar sus credenciales de origen de datos para que no se le soliciten cada vez que sean necesarias.

Procedimiento

1. Cuando se le pida que escriba sus credenciales de origen de datos, especifique su identificador de usuario y su contraseña.
2. Seleccione la casilla de verificación **Recordar mi identificador de usuario y contraseña al conectarme a este origen de datos**.
3. Pulse **Aceptar**.

Resultados

La próxima vez que realice una acción que requiera esas credenciales de origen de datos, no se le solicitarán a menos que se hayan suprimido o hayan caducado.

Visualización y eliminación de sus credenciales de origen de datos

Puede ver y suprimir sus credenciales de origen de datos.

Procedimiento

1. Pulse **Opciones de Mi área, Mis preferencias**.
2. Pulse la pestaña **Personal**.
Sus credenciales de origen de datos aparecerán en **Credenciales del origen de datos**. Puede ordenar la lista por **Nombre del origen de datos** o por **Nombre de la conexión de origen de datos**.
3. Para eliminar una credencial de origen de datos, seleccione la casilla de verificación correspondiente y pulse **Eliminar**.

Capítulo 13. Funciones y características protegidas

Las funciones y las características protegidas existentes en las funciones, también conocidas como capacidades, controlan el acceso a distintas tareas de administración y áreas funcionales de la interfaz de usuario en el software de IBM Cognos.

Algunos ejemplos de funciones protegidas son **Administración** y **Creación de informes**. Algunos ejemplos de características protegidas son **SQL definido por el usuario** y **Separación**.

Content Manager lee los permisos del usuario al iniciar sesión. En función de los permisos de las funciones y las características protegidas, los usuarios pueden acceder a componentes específicos y realizar tareas concretas en el software de IBM Cognos.

Cuando se inicializa un almacén de contenido, se crean los permisos iniciales de las funciones y las características protegidas. Los permisos definen qué grupos y roles predefinidos e incorporados de Cognos tienen acceso a qué funciones y características protegidas, y el tipo de acceso que ostentan. Los permisos iniciales otorgan acceso ilimitado al software de IBM Cognos, ya que el rol incorporado Administradores del sistema incluye al grupo Todos entre sus miembros. Debe eliminar dicho grupo de los miembros de Administradores del sistema antes de empezar a establecer acceso a las funciones. Para obtener más información, consulte Capítulo 15, “Seguridad inicial”, en la página 243.

Al ejecutar un informe con la opción **Ejecutar como el propietario**, se utilizan las funciones del propietario para las propiedades de diseño de informe y de separación en formato HTML. El resto de funciones dependen del usuario que ejecute el informe.

Los administradores configuran el acceso a las funciones y las características protegidas mediante la página **Funciones** de la pestaña **Seguridad** de **IBM Cognos Administration**. Para obtener más información, consulte “Establecimiento del acceso a funciones o características seguras” en la página 235.

Los usuarios pueden ver una lista de las funciones y las características protegidas disponibles en **Mis preferencias** en la pestaña **Personal**.

Para obtener más información, consulte “Permisos de acceso iniciales a las prestaciones” en la página 447.

Adaptive Analytics

Esta función protegida controla el acceso a los informes empaquetados mediante Adaptive Analytics.

Administración

Esta función protegida contiene las características protegidas que controlan el acceso a las páginas de administración que se utilizan para administrar el software de IBM Cognos. Los administradores del sistema pueden utilizar esta función para delegar tareas de administración a otros administradores.

Las características protegidas siguientes están asociadas a esta función:

- **Administración de Adaptive Analytics**
Los usuarios pueden acceder a Adaptive Analytics para realizar tareas administrativas.
- **Tareas de administración**
Los usuarios pueden acceder a la opción **Administración de contenidos** de la pestaña **Configuración** de **IBM Cognos Administration** para administrar las exportaciones, las importaciones, las comprobaciones de consistencia y las actualizaciones de informes.
- **Configurar y administrar el sistema**
Los usuarios pueden acceder a la opción **Sistema** de la pestaña **Estado** y a **Asignadores y servicios** de la pestaña **Configuración** de **IBM Cognos Administration** para configurar los asignadores y los servicios, así como para administrar el sistema.
- **Administración de Controller**
Los usuarios pueden utilizar las funciones administrativas de IBM Cognos Controller.
- **Conexiones con orígenes de datos**
Los usuarios pueden acceder a la opción **Conexiones con orígenes de datos** de la pestaña **Configuración** de **IBM Cognos Administration** para definir los orígenes de datos, las conexiones y los inicios de sesión.
- **Listas de distribución y contactos**
Los usuarios pueden acceder a la opción **Listas de distribución y contactos** de la pestaña **Configuración** de **IBM Cognos Administration** para administrar las listas de distribución y los contactos.
- **Administración de Mobile**
Los usuarios pueden administrar los servicios y las aplicaciones de IBM Cognos Mobile.
- **Administración de Planning**
Los usuarios pueden acceder a la consola de IBM Cognos Planning Contributor Administration e IBM Cognos Planning Analyst para realizar tareas de administración.
- **Servidores PowerPlay**
Al usuario se le otorga acceso limitado a las páginas de IBM Cognos Administration. Esto incluye el acceso a la página de PowerPlay y la capacidad para configurar propiedades de PowerPlay.
- **Impresoras**
Los usuarios pueden acceder a la opción **Impresoras** de la pestaña **Configuración** de **IBM Cognos Administration** para administrar las impresoras.
- **Administración de Query Service**
Los usuarios pueden acceder a la página **Estado > Almacenes de datos** de **IBM Cognos Administration** para gestionar los cubos dinámicos. Los usuarios pueden realizar operaciones en los cubos, como iniciar y detener cubos, renovar la memoria caché de datos y crear y planificar tareas de Query Service.
- **Ejecutar actividades y planificaciones**
Los usuarios pueden acceder a las opciones **Actividades actuales**, **Actividades pasadas**, **Próximas actividades** y **Planificaciones** de la pestaña **Estado** de **IBM Cognos Administration** para supervisar las actividades del servidor y

administrar las planificaciones. Para otorgar acceso a la funcionalidad de planificación con independencia de la funcionalidad de supervisión, utilice la función Planificación.

- **Definir las funciones y administrar los perfiles de la IU**

Los usuarios pueden acceder a las opciones **Funciones** y **Perfiles de interfaces de usuario** de la pestaña **Seguridad** de **IBM Cognos Administration** para administrar las funciones y las características protegidas, así como los perfiles de la interfaz de usuario de Creación de informes.

- **Estilos y portlets**

Los usuarios pueden acceder a las opciones **Estilos** y **Portlets** de la pestaña **Configuración** de **IBM Cognos Administration** para administrar los estilos y los portlets.

- **Usuarios, grupos y roles**

Los usuarios pueden acceder a la opción **Usuarios, grupos y roles** de la pestaña **Seguridad** de **IBM Cognos Administration** para administrar espacios de nombres, usuarios, grupos y roles.

Analysis Studio

Esta función protegida controla el acceso a IBM Cognos Analysis Studio. Los usuarios con acceso a este estudio exploran, analizan y comparan datos dimensionales, buscan información significativa en orígenes de datos de gran tamaño y responden las preguntas de negocio.

Cognos Viewer

Esta función protegida controla el acceso a IBM Cognos Viewer, que se utiliza para ver los informes.

Las características protegidas asociadas a esta función son

- **Menú contextual**

Los usuarios pueden utilizar el menú contextual de IBM Cognos Viewer.

Nota: Para ver el menú contextual, los usuarios deben tener acceso tanto a la característica protegida **Selección** como a **Menú contextual**.

- **Ejecutar con opciones**

Los usuarios pueden cambiar las opciones de ejecución predeterminadas. Si los usuarios no tienen permisos de ejecución sobre esta característica, no pueden ver el icono **Ejecutar con opciones**  para los informes.

- **Selección**

Los usuarios pueden seleccionar texto de listas y tablas de referencias cruzadas.

- **Barra de herramientas**

Los usuarios pueden ver la barra de herramientas de IBM Cognos Viewer.

Colaborar

Esta función protegida controla el acceso a IBM Connections desde IBM Cognos.

Las características protegidas asociadas a esta función son:

- **Lanzar herramientas de colaboración**

La característica protegida permite a los usuarios lanzar IBM Connections desde cualquier menú de inicio del entorno de IBM Cognos Analytics, incluidos la

página de inicio de Cognos Workspace y el menú Acciones. Los enlaces remitirán a la página principal de IBM Connections del usuario, si está configurada, o a Actividades.

- **Permitir características de colaboración**

Esta característica protegida controla el acceso al icono **Colaborar** y a los resultados de la búsqueda de IBM Connections Search dentro de Cognos Workspace. Los usuarios deben disponer de acceso para poder crear o ver actividades desde Cognos Workspace.

Controller Studio

Esta función protegida controla el acceso a IBM Cognos Controller.

Panel de control

Esta función protegida controla el acceso a las funciones **Nuevo > Panel de control** y **Nuevo > Historia**. Los usuarios necesitan permisos de ejecución en el panel de control para crear o ver paneles de control e historias. De forma predeterminada, se listan los roles asignados con permisos de ejecución en la sección “Prestación Panel de control” en la página 454.

Data Manager

Esta función protegida controla el acceso a Data Manager.

Conjuntos de datos

Esta función protegida controla el acceso al menú **Crear conjunto de datos** que está disponible desde el paquete y desde los menús contextuales del módulo de datos.

Herramientas de escritorio

Esta función protegida controla el acceso a los productos de Cognos Desktop Tools. Los usuarios con esta función son miembros del rol Exploradores de Analytics. Esto les permite acceder a Cognos Analysis For Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer y Dynamic Query Analyzer, Transformer y TM1 Writeback para el servidor FLBI TM1 empaquetado.

Errores detallados

Esta función protegida controla el acceso para la visualización de los mensajes de error detallados en el navegador web.

Ayudante para acceso a detalles

Esta función protegida controla el acceso a la funcionalidad de depuración de acceso a detalles en la página **Ir a** correspondiente y las definiciones para acceso a detalles. Los usuarios que cuenten con esta función podrán ver información adicional en la página **Ir a** de cada destino de acceso a detalles. Esta información puede resultar útil para depurar una definición de acceso a detalles, o bien se puede reenviar al representante de Cognos Software Services.

Event Studio

Esta función protegida controla el acceso a Event Studio.

Panel de control ejecutivo

Esta función protegida controla el acceso a IBM Cognos Workspace. Los usuarios que tienen acceso a esta función tienen asignados permisos básicos para los espacios de trabajo en Cognos Workspace. Con este tipo de permisos, los usuarios pueden ver los espacios de trabajo, detallar más y menos en los datos del espacio de trabajo, añadir comentarios, imprimir los espacios de trabajo, utilizar filtros de deslizador y seleccionar filtros de valor si están incluidos en el espacio de trabajo.

Las características protegidas siguientes, asociadas a la función **Panel de control ejecutivo**, conceden permisos más amplios para el espacio de trabajo:

- **Utilizar características avanzadas de panel de control**

Utilice esta característica para conceder a los usuarios los permisos más altos para el espacio de trabajo.

- **Utilizar características interactivas de panel de control**

Utilice esta característica para conceder a los usuarios permisos para acceder a las funciones del espacio de trabajo que permiten la interacción con los datos de widget. Esto incluye el acceso a la barra de herramientas a petición del widget que proporciona opciones para interactuar con los datos de informe, por ejemplo opciones de ordenación, supresión, restablecimiento, intercambio de filas y columnas y cambio del tipo de visualización de informes.

Repositorios externos

Esta función protegida controla el acceso a los repositorios externos. Los repositorios externos proporcionan almacenamiento a largo plazo para el contenido de informe. Cuando se especifica una conexión con un repositorio externo para un paquete o carpeta, las versiones de la salida de informe se copian en el repositorio automáticamente.

Las características protegidas asociadas a esta función son

- **Administrar conexiones del repositorio**

Los usuarios pueden establecer una conexión de repositorio en un paquete o carpeta si ya existe una conexión de origen de datos.

- **Ver documentos externos**

Los usuarios pueden ver la salida de informe almacenada en un repositorio externo.

Generar salida CSV

Con permisos para esta función protegida, los usuarios pueden generar salidas de informe en formato de texto delimitado (CSV). Sin esta función, los usuarios no verán una opción en la interfaz de usuario para ejecutar informes en el formato CSV.

Generar salida PDF

Con permisos para esta función protegida, los usuarios pueden generar salidas de informe en formato PDF. Sin esta función, los usuarios no verán una opción en la interfaz de usuario para ejecutar informes en el formato PDF.

Generar salida XLS

Con permisos para esta función protegida, los usuarios pueden generar salidas de informe en formato de hoja de cálculo de Microsoft Excel (XLS). Sin esta función, los usuarios no verán una opción en la interfaz de usuario para ejecutar informes en el formato XLS.

Generar salida XML

Con permisos para esta función protegida, los usuarios pueden generar salida de informe en formato XML. Sin esta función, los usuarios no verán una opción en la interfaz de usuario para ejecutar informes en el formato XML.

Glosario

Esta función protegida controla el acceso a IBM InfoSphere Business Glossary.

Ocultar entradas

Esta función protegida especifica que un usuario puede ocultar entradas y ver entradas ocultas en el software de IBM Cognos.

La casilla de verificación **Ocultar esta entrada** aparece en la pestaña **General** de las páginas de propiedades de entradas. La casilla de verificación **Mostrar entradas ocultas** aparece en la pestaña **Preferencias** en los perfiles de usuario y en la pestaña **General** en Opciones de Mi área , **Mis preferencias**.

Importar metadatos relacionales

Especifica que un grupo puede importar metadatos relacionales en un proyecto de Framework Manager o Dynamic Cube Designer con el modo de consulta dinámica.

De manera predeterminada, los grupos Administrador del sistema, Administrador de directorio y Administradores de informes pertenecen a esta función protegida.

Si otros grupos necesitan la capacidad de importar metadatos relacionales a un proyecto de modo de consulta dinámica, deberán añadirse a la función. Por ejemplo, si crea un grupo de usuarios de Framework Manager y añade en él a sus usuarios de Framework Manager, también deberá añadir el grupo a la función protegida Importar metadatos relacionales.

Linaje

Esta función protegida controla el acceso a la acción **Linaje**. Utilícela para ver información sobre los elementos de datos o de metadatos de IBM Cognos Viewer, o del árbol de origen en Creación de informes, Query Studio y Analysis Studio.

Gestionar contenido

Esta función protegida controla el acceso a la pestaña **Contenido** en **Gestionar**.

Administración de los propios inicios de sesión de origen de datos

Esta función protegida controla la capacidad de gestionar las credenciales del origen de datos en la pestaña **Personal** de **Mis preferencias**.

Mobile

Esta función protegida controla el acceso a IBM Cognos Mobile.

Planning Contributor

Esta función protegida controla el acceso a IBM Cognos Planning Contributor e IBM Cognos Planning Analyst.

PowerPlay Studio

Esta función protegida controla el acceso a PowerPlay Studio.

Query Studio

Esta función protegida controla el acceso a Query Studio, que se puede utilizar para crear sencillos informes ad hoc.

La característica protegida asociada a esta función es

- **Crear**
Cree informes y utilice la opción Guardar como para los informes nuevos y las vistas personalizadas.
- **Avanzado**
Utilice características de creación avanzadas, como la creación de filtros complejos, el estilo de formateo y el soporte multilingüe.

Report Studio

Esta función asegurada controla el acceso a la interfaz del usuario Creación de informes y a la funcionalidad de ejecución del informe subyacente. Los usuarios deben ejecutar permisos en la función asegurada para obtener acceso a la interfaz del usuario de Creación de informes. Los permisos de trayecto o de lectura en esta función asegurada puede ser necesario para utilizar las funciones aseguradas asociadas; por ejemplo, para ejecutar informes creados con SQL personalizados o HTML incrustado.

Las características protegidas asociadas a esta función son:

- **Permitir datos externos**
Los usuarios pueden utilizar datos externos en los informes.
- **Separación**
Los usuarios pueden crear y ejecutar informes de separación.
- **Crear/Suprimir**
Los usuarios pueden crear informes, utilizar la opción Guardar como para informes y vistas de informes nuevos, así como cambiar los modelos.
- **Elementos HTML en informe**
Los usuarios pueden utilizar el botón HTMLItem y los elementos del hiper enlace de la especificación del informe al autorizar informes.

- **SQL definido por el usuario**

Los usuarios pueden editar las sentencias SQL directamente en la especificación de consulta y ejecutar las especificaciones de consulta que contengan las sentencias SQL editadas.

Consejo: En Framework Manager no se aplican restricciones sobre quién puede utilizar esta característica. Por ejemplo, un usuario de Framework Manager que no tenga derechos **SQL definido por el usuario** en **IBM Cognos Administration** puede crear un asunto de consulta y utilizar consultas SQL creadas manualmente para buscar en una base de datos.

Planificación

Esta función protegida controla el acceso a la funcionalidad de planificación de elementos que se pueden ejecutar, como informes.

Las características protegidas asociadas a esta función son

- **Planificación por día**

Los usuarios pueden planificar las entradas con una frecuencia diaria.

- **Planificación por hora**

Los usuarios pueden planificar las entradas por horas.

- **Planificación por minuto**

Los usuarios pueden planificar las entradas por minutos.

Si a un usuario se le deniega el acceso a la función **Planificación por minuto**, la planificación por minuto también se le denegará para otras funciones que la permiten, como por ejemplo, la función **Planificación por mes**.

- **Planificación por mes**

Los usuarios pueden planificar las entradas con una frecuencia mensual.

- **Planificación por activador**

Los usuarios pueden planificar las entradas en función de un activador.

- **Planificación por semana**

Los usuarios pueden planificar las entradas con una frecuencia semanal.

- **Planificación por año**

Los usuarios pueden planificar las entradas con una frecuencia anual.

- **Planificar prioridad**

Los usuarios pueden configurar y cambiar la prioridad de procesamiento de las entradas planificadas.

Asistente para paquetes de autoservicio

Esta función protegida controla la capacidad de seleccionar qué orígenes de datos se pueden utilizar para crear un paquete.

Establecer funciones específicas de entradas

Esta función protegida especifica que un usuario puede configurar funciones en el nivel de entrada.

La pestaña **Funciones** aparecerá en las páginas **Establecer propiedades** de los paquetes y las carpetas de usuarios que tengan esta función y que tengan permisos de política configurados para la entrada o propietarios de la entrada.

Ejecución de especificaciones

Esta función protegida especifica que un usuario o una aplicación de Software Development Kit pueda utilizar una especificación en línea.

Los estudios de IBM Cognos Analytics y algunos servicios utilizan las especificaciones en línea de forma interna para realizar tareas. El servicio que ejecuta la especificación prueba una serie de funciones para garantizar que el usuario pueda utilizar esa especificación en línea. Para obtener más información, consulte el método `runSpecification` de la *Guía del desarrollador*.

Cargar archivos

Esta función protegida controla el acceso a la función **Cargar archivos**. Los usuarios que tienen esta función puede cargar archivos de datos.

Reglas de observación

Esta función protegida controla el acceso a la pestaña **Reglas de Elementos de mi lista de observación**. Use esta función protegida para crear y ejecutar reglas de observación.

Modelado basado en web

Esta función protegida controla el acceso a la función de modelado basado en web. Los usuarios que tienen esta función pueden crear módulos de datos desde el menú **Nuevo > Módulo de datos**.

Establecimiento del acceso a funciones o características seguras

Para establecer el acceso a las funciones y las características protegidas, debe otorgar permisos de ejecución para los mismos a espacios de nombres, usuarios, grupos o roles especificados.

Regularmente, otorga permisos de ejecución para la característica y permisos cruzados para su función segura principal. Por ejemplo, para otorgar acceso a Creación de informes y a toda su funcionalidad, debe otorgar permisos de ejecución para la función protegida de **Creación de informes**. Si desea otorgar sólo acceso a la característica protegida **Crear/Suprimir** de Creación de informes, conceda permisos de visita a la función protegida **Creación de informes** y de ejecución a la característica protegida **Crear/Suprimir**.

Antes de empezar

Para administrar las funciones y las características protegidas, debe haber establecido permisos de política. Normalmente este proceso lo realizan los administradores del directorio.

Para poder empezar a establecer permisos sobre funciones, asegúrese de que ya se haya cambiado los valores de seguridad iniciales.

Procedimiento

1. En **Gestionar > Consola de administración**, abra **IBM Cognos Administration**.
2. En la pestaña **Seguridad**, pulse **Funciones**.

Aparecerá una lista con todas las funciones protegidas disponibles.

3. Seleccione si desea establecer acceso para una función o para una característica:

- Para establecer el acceso para una función, pulse el botón Acciones  correspondiente al nombre de la función y pulse **Establecer propiedades**.
- Para establecer acceso para una función, pulse el botón Acciones correspondiente al nombre de característica y pulse **Establecer propiedades**.

Consejo: Las funciones que tienen funciones seguras tienen enlaces.

4. Pulse la pestaña **Permisos**.
5. Seleccione si desea utilizar los permisos de la entrada padre o especifique otros permisos:
 - Para utilizar los permisos de la entrada padre, desactive la casilla de verificación **Reemplazar los permisos de acceso adquiridos de la entrada padre** y pulse **Aceptar**.
 - Para establecer los permisos explícitamente para la entrada, seleccione la casilla de verificación **Reemplazar los permisos de acceso adquiridos de la entrada padre** y realice los pasos restantes.
6. Si desea eliminar una entrada de la lista, seleccione su casilla de verificación y pulse **Eliminar**.

Consejo: Para seleccionar o anular la selección de todas las entradas de una página, pulse **Seleccionar todo** o **Deseleccionar todo**.

7. Si desea añadir entradas a la lista, pulse **Añadir** y elija el modo de seleccionar las entradas:
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación correspondientes a los usuarios, grupos o roles que desee.
 - Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
 - Para escribir el nombre de las entradas que desea añadir, pulse **Tipo** y escriba los nombres de grupos, roles o usuarios mediante el siguiente formato, en donde un punto y coma (;) separa cada entrada.
espacio_nombres/nombre_grupo;espacio_nombres/nombre_rol;espacio_nombres/nombre_usuario;
A continuación se incluye un ejemplo:
Cognos/Authors;LDAP/scarter;
8. Pulse el botón de flecha a la derecha y, cuando aparezcan las entradas que desea en el cuadro **Entradas seleccionadas**, pulse **Aceptar**.

Consejo: Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, seleccione la casilla de verificación de la lista. Para hacer visibles las entradas del usuario, pulse **Mostrar usuarios en la lista**.

9. Seleccione la casilla de verificación situada junto a la entrada para la que desee establecer acceso a la función o la característica.
10. En el cuadro situado junto a la lista, seleccione las casillas de verificación adecuadas para otorgar permisos de ejecución  para la entrada.
11. Pulse **Aplicar**.

En la columna **Permisos**, aparece un icono que denota los permisos de ejecución otorgados junto al espacio de nombres, usuario, grupo o rol.

12. Repita los pasos del 8 al 10 para cada entrada.
13. Pulse **Aceptar**.

Capítulo 14. Capacidades de objetos

Las capacidades de objeto especifican las funciones y las características protegidas que pueden utilizar los usuarios, los grupos o los roles con los distintos paquetes. Por ejemplo, las funciones definen el estudio en el que se va a abrir un paquete, así como las características del estudio disponibles mientras se trabaja con ese paquete.

Las funciones protegidas y sus características, también conocidas como funcionalidad global, controlan el acceso a los distintos componentes y la funcionalidad del software de IBM Cognos. Para que las capacidades de objeto funcionen, debe combinarlas con funciones globales aplicables. Por ejemplo, al configurar capacidades de objeto de un paquete que contenga informes de Creación de informes y Query Studio, asegúrese de que el usuario también tenga acceso a las funciones protegidas de **Creación de informes** y **Query Studio** así como a sus características protegidas aplicables.

Al volver a publicar un paquete existente de una herramienta de cliente, como Framework Manager, no se sobrescriben ni se modifican las capacidades de objeto previamente especificadas.

Las prestaciones de objeto pueden controlarse con la función protegida **Establecer funciones específicas de entradas** “Establecer funciones específicas de entradas ” en la página 234.

Puede configurar las siguientes capacidades de objeto para paquetes individuales “Configuración de las capacidades de objeto de un paquete” en la página 241:

Adaptive Analytics

Esta función protegida controla el acceso a los informes empaquetados mediante Adaptive Analytics.

Administración

Esta función protegida controla el acceso a las páginas administrativas del software de IBM Cognos. Puede especificar las capacidades de objeto de las siguientes características protegidas en **Administración**.

- **Administración de Adaptive Analytics**

Los usuarios pueden acceder a Adaptive Analytics para realizar tareas administrativas.

- **Administración de Planning**

Los usuarios pueden acceder a la consola de IBM Cognos Planning Contributor Administration e IBM Cognos Planning Analyst para realizar tareas de administración.

Event Studio

Esta función protegida controla el acceso a Event Studio.

Glosario

Esta función protegida controla el acceso a IBM InfoSphere Business Glossary.

Planning Contributor

Esta función protegida controla el acceso a IBM Cognos Planning Contributor e IBM Cognos Planning Analyst.

PowerPlay Studio

Esta función protegida controla el acceso a PowerPlay Studio.

Query Studio

Esta función protegida controla el acceso a Query Studio, que se puede utilizar para crear sencillos informes ad hoc.

La característica protegida asociada a esta función es

- **Crear**
Cree informes y utilice la opción Guardar como para los informes nuevos y las vistas personalizadas.
- **Avanzado**
Utilice características de creación avanzadas, como la creación de filtros complejos, el estilo de formateo y el soporte multilingüe.

Report Studio

Esta función asegurada controla el acceso a la interfaz del usuario Creación de informes y a la funcionalidad de ejecución del informe subyacente. Los usuarios deben ejecutar permisos en la función asegurada para obtener acceso a la interfaz del usuario de Creación de informes. Los permisos de trayecto o de lectura en esta función asegurada puede ser necesario para utilizar las funciones aseguradas asociadas; por ejemplo, para ejecutar informes creados con SQL personalizados o HTML incrustado.

Las características protegidas asociadas a esta función son:

- **Permitir datos externos**
Los usuarios pueden utilizar datos externos en los informes.
- **Separación**
Los usuarios pueden crear y ejecutar informes de separación.
- **Crear/Suprimir**
Los usuarios pueden crear informes, utilizar la opción Guardar como para informes y vistas de informes nuevos, así como cambiar los modelos.
- **Elementos HTML en informe**
Los usuarios pueden utilizar el botón HTMLItem y los elementos del hiper enlace de la especificación del informe al autorizar informes.
- **SQL definido por el usuario**
Los usuarios pueden editar las sentencias SQL directamente en la especificación de consulta y ejecutar las especificaciones de consulta que contengan las sentencias SQL editadas.

Consejo: En Framework Manager no se aplican restricciones sobre quién puede utilizar esta característica. Por ejemplo, un usuario de Framework Manager que no tenga derechos **SQL definido por el usuario** en **IBM Cognos Administration** puede crear un asunto de consulta y utilizar consultas SQL creadas manualmente para buscar en una base de datos.

Linaje

Esta función protegida controla el acceso a la acción **Linaje**. Utilícela para ver información sobre los elementos de datos o de metadatos de IBM Cognos Viewer, o del árbol de origen en Creación de informes, Query Studio y Analysis Studio.

Ejecución de especificaciones

Esta función protegida especifica que un usuario o una aplicación de Software Development Kit pueda utilizar una especificación en línea.

Los estudios de IBM Cognos Analytics y algunos servicios utilizan las especificaciones en línea de forma interna para realizar tareas. El servicio que ejecuta la especificación prueba una serie de funciones para garantizar que el usuario pueda utilizar esa especificación en línea. Para obtener más información, consulte el método `runSpecification` de la *Guía del desarrollador*.

Reglas de observación

Esta función protegida controla el acceso a la pestaña **Reglas de Elementos de mi lista de observación**. Use esta función protegida para crear y ejecutar reglas de observación.

Configuración de las capacidades de objeto de un paquete

Utilice esta funcionalidad para especificar las funciones y las características protegidas que pueden utilizar los usuarios, los grupos o los roles con paquetes específicos.

Puede especificar capacidades de objeto en el nivel del paquete o, si el paquete está almacenado en una carpeta, en el nivel de la carpeta. Las funciones especificadas en el nivel de la carpeta sólo se aplican a los paquetes de esa carpeta y a sus subcarpetas, pero a ninguna otra entrada, incluidos los informes. Por ejemplo, si una carpeta contiene paquetes, informes y una subcarpeta que contiene otros paquetes e informes, sólo se verán afectados por los valores de las funciones los paquetes de la carpeta y de la subcarpeta.

Las funciones siguientes se aplican de manera global; no pueden definirse por carpetas individuales:

- Generar salida CSV
- Generar salida PDF
- Generar salida XLS
- Generar salida XML

Antes de empezar

Para utilizar las capacidades de objeto, los usuarios deben

- Tener acceso a las funciones y las características protegidas asociadas al paquete (Capítulo 13, “Funciones y características protegidas”, en la página 227).

- Tener acceso a la función protegida **Capacidades de objetos** (“Establecer funciones específicas de entradas ” en la página 234).
- Tener permisos para establecer política para el paquete Capítulo 12, “Permisos de acceso y credenciales”, en la página 213 o ser propietarios del paquete.

Al configurar capacidades de objeto por primera vez después de instalar el software de IBM Cognos, recomendamos que empiece con **Carpetas públicas**, y que las funciones de **Carpetas públicas** dupliquen las funciones globales. De esta forma se proporciona una línea base precisa sobre las capacidades de objeto que se pueden ajustar aún más.

Procedimiento

1. Abra el paquete o la página de propiedades de la carpeta.

Consejo: Al configurar capacidades de objeto para **Carpetas públicas**, pulse el botón Propiedades  en la barra de herramientas del producto. Se ha sustituido **Carpetas públicas** por **Contenido del equipo** en Cognos Analytics versión 11.0.x.

2. Pulse la pestaña **Funciones**.
3. Seleccione la casilla de verificación **Reemplazar las funciones adquiridas de la entrada padre**.
4. En la lista **Nombre y Funciones**, seleccione la casilla de verificación situada junto al usuario, el grupo o el rol para el que desee especificar capacidades de objeto.

Si el usuario, el grupo o el rol no está en la lista, pulse **Añadir**. Si desea eliminar el usuario, el grupo o el rol de la lista, seleccione su casilla de verificación y pulse **Eliminar**.

Para obtener más información sobre la adición o la eliminación de entradas de esta lista, consulte los pasos de “Establecimiento de permisos de acceso para una entrada” en la página 220.

5. En la lista **Otorgar y Denegar**, active o desactive las casillas de verificación aplicables para otorgar o denegar las capacidades de objeto necesarias para los usuarios, los grupos o los roles.

Junto al nombre del usuario, el grupo o el rol aparece un icono que representa una función otorgada o denegada. Cuando deniega acceso a una función protegida, lo deniega automáticamente para todas sus características protegidas.

6. Cuando proceda, seleccione la casilla de verificación **Suprimir las funciones de todas las entradas hijo**.

Utilice esta opción para especificar las capacidades de objeto de una jerarquía de entradas como, por ejemplo, para todos los paquetes de una carpeta.

7. Pulse **Aceptar**.

Capítulo 15. Seguridad inicial

Cuando se inicializa un almacén de contenido, se crea un conjunto de objetos de seguridad que se almacena en el espacio de nombres de Cognos. Estos objetos tienen como objetivo simplificar la administración de IBM Cognos.

Las políticas de seguridad iniciales otorgan un acceso ilimitado a los usuarios a todos los objetos del almacén de contenido. El administrador de seguridad debe modificar los valores de seguridad iniciales para proteger el almacén de contenido. Para obtener más información, consulte “Valores de seguridad después de la instalación” en la página 254.

Para ver un resumen de los permisos de acceso iniciales para los objetos de Content Manager, consulte: Apéndice C, “Permisos de acceso iniciales”, en la página 445.

Entradas incorporadas

Las entradas incorporadas incluyen la cuenta de usuario Anónimo, los grupos Todos los usuarios autenticados y Todos, así como los roles Administradores del sistema y Administradores de arrendatarios. Las entradas incorporadas no se pueden suprimir. Éstas aparecen tanto en los entornos protegidos como en los no protegidos.

Anónimo

Esta entrada representa una cuenta de usuario que comparten los miembros del público general que pueden acceder al software de IBM Cognos sin que se les pida autenticarse. Por ejemplo, este tipo de acceso resulta útil cuando se distribuye un catálogo en línea.

Los usuarios anónimos sólo pueden ver las entradas para las que no se hayan establecido permisos de acceso, o que no se hayan configurado de forma específica para esa cuenta o para el grupo Todos.

Para inhabilitar la cuenta de usuario Anónimo, cambie los parámetros de configuración en la herramienta de configuración.

Todos los usuarios autenticados

Este grupo representa a los usuarios que han autenticado los proveedores de autenticación. La pertenencia a este grupo viene determinada por el producto y no se puede ver ni modificar.

Este grupo no se puede desplegar. Para obtener más información, consulte “Cómo incluir grupos y roles de Cognos” en la página 295.

Todos

Este grupo representa a todos los usuarios autenticados y a la cuenta de usuario Anónimo. La pertenencia a este grupo viene determinada por el producto y no se puede ver ni modificar.

Puede utilizar el grupo Todos para establecer rápidamente la seguridad predeterminada. Por ejemplo, para proteger un informe, puede otorgar al grupo Todos permisos de lectura, escritura o ejecución del informe. Una vez activada esta seguridad, puede otorgar acceso al informe a otros usuarios, grupos o roles, así como eliminar el grupo Todos de la política de seguridad de este informe. A continuación, sólo se otorgará acceso al informe a los usuarios, los grupos y los roles que especifique.

Puede utilizar el grupo Todos para aplicar seguridad durante el despliegue (consulte “Seguridad y despliegue” en la página 288), pero no puede desplegar el propio grupo. Para obtener más información, consulte “Cómo incluir grupos y roles de Cognos” en la página 295.

Administradores del sistema

Se trata de un rol especial del software de IBM Cognos. Los miembros de este rol se consideran usuarios root o usuarios avanzados. Pueden acceder y modificar cualquier objeto del almacén de contenido, con independencia de cualquier política de seguridad configurada para el objeto. Sólo los miembros del rol Administradores del sistema pueden modificar la pertenencia a este rol.

Este rol no puede estar vacío. Si no desea utilizar el rol Administradores del sistema, puede crear un grupo vacío en el espacio de nombres de Cognos o en su proveedor de autenticación, así como añadir este grupo a los miembros del rol Administradores del sistema.

Cuando se crea este rol durante la inicialización del almacén de contenido, el grupo Todos está incluido entre sus miembros, lo que significa que todos los usuarios tienen un acceso ilimitado al almacén de contenido. Justo después de instalar y configurar el software de IBM Cognos, debe modificar los valores de seguridad iniciales de este rol y eliminar el grupo Todos de sus miembros. Para obtener más información, consulte “Valores de seguridad después de la instalación” en la página 254.

Puede desplegar este rol, incluidos los grupos y roles de Cognos. Para obtener más información, consulte “Cómo incluir grupos y roles de Cognos” en la página 295.

Administradores de arrendatarios

Este rol se utiliza en un entorno de varios arrendatarios IBM Cognos. Los miembros de este rol pueden administrar varios arrendatarios.

Cuando se crea este rol durante la inicialización del almacén de contenido, no tiene miembros ni prestaciones. Solamente los administradores del sistema pueden añadir miembros y asignar prestaciones y permisos de acceso para este rol.

Roles predefinidos

Los roles predefinidos incluyen varios roles de IBM Cognos. Cada rol tiene un conjunto específico de permisos de acceso y se puede utilizar para proteger distintos componentes y funciones del software de IBM Cognos. Puede utilizar los roles predefinidos o suprimirlos.

Cuando se crean los roles predefinidos durante la inicialización del almacén de contenido, el grupo Todos forma parte del rol Administradores del sistema. Algunos de estos roles son: Consumidores, Usuarios de consultas, Usuarios del

análisis y Autores. Si desea utilizar los roles predefinidos, debe modificar su pertenencia a grupo inicial inmediatamente después de instalar y configurar el software de IBM Cognos. Para obtener más información, consulte “Valores de seguridad después de la instalación” en la página 254.

Existen dos tipos de roles predefinidos de Cognos: roles sin licencia y roles de licencia.

Roles no de licencia

En la tabla siguiente se enumeran los roles predefinidos de Cognos que no están basados en requisitos de licencia.

Tabla 57. Roles predefinidos Cognos sin licencia

Rol sin licencia	Descripción
Administradores de Adaptive Analytics	Los miembros pueden administrar informes empaquetados con Adaptive Analytics.
Usuarios de Adaptive Analytics	Los miembros pueden utilizar informes empaquetados con Adaptive Analytics.
Usuarios del análisis	Los miembros tienen los mismos permisos de acceso que el rol Consumidores. También pueden utilizar IBM Cognos Analysis Studio.
Autores	Los miembros tienen los mismos permisos de acceso que Usuarios de consultas y Usuarios del análisis. Pueden utilizar Creación de informes, Query Studio y Analysis Studio, así como guardar contenido público, como informes y salidas de informes.
Consumidores	Los miembros pueden leer y ejecutar contenido público, como informes.
Administradores de Controller	Los miembros cuentan con acceso completo a los menús de IBM Cognos Controller y pueden crear distintos usuarios de IBM Cognos Controller, así como definir sus limitaciones.
Usuarios de Controller	Los miembros tienen acceso general a los menús de IBM Cognos Controller.
Autores de Data Manager	Los miembros tienen acceso general a los menús de IBM Data Manager.
Admin. del directorio	Los miembros pueden administrar el contenido de los espacios de nombres. En el espacio de nombres de Cognos, administran grupos, cuentas, contactos, listas de distribución, orígenes de datos e impresoras.
Autores de Express	Los miembros pueden recibir salidas de separación, incluidos informes activos y ver informes programados. También pueden acceder a IBM Cognos Portal y a las aplicaciones de IBM Cognos Mobile.
Administradores de biblioteca	Los miembros pueden acceder, importar y administrar el contenido de la pestaña Biblioteca en IBM Cognos Administration.
Administradores de métrica	Los miembros pueden administrar las tareas y los paquetes de métricas.
Usuarios de Mobile	Los miembros pueden acceder al contenido de IBM Cognos, como los informes, a través de las aplicaciones de IBM Cognos Mobile.
Administradores de Mobile	Los miembros pueden administrar las aplicaciones de IBM Cognos Mobile.

Tabla 57. Roles predefinidos Cognos sin licencia (continuación)

Rol sin licencia	Descripción
Modeladores	Los miembros pueden utilizar la interfaz de usuario de modelado para crear y gestionar módulos de datos.
Administradores de portales	Los miembros pueden administrar los portlets de Cognos y otros portlets. Esta administración incluye la personalización de portlets, la definición de estilos de portlets y el establecimiento de permisos de acceso a portlets. Los administradores del portal también pueden cargar extensiones que permite a los usuarios, por ejemplo, añadir imágenes a informes o paneles de control.
Usuarios de Planning Contributor	Los miembros pueden acceder al cliente Web de Contributor, al complemento Contributor para Microsoft Excel o a Analyst.
Administradores de permisos de Planning	Los miembros pueden acceder a la consola de Contributor Administration, a Analyst y a todos los objetos asociados de la aplicación.
Usuarios de consultas	Los miembros tienen los mismos permisos de acceso que el rol Consumidores. También pueden utilizar IBM Cognos Query Studio.
Lectores	Los miembros tienen acceso de sólo lectura al software de IBM Cognos. Pueden explorar algunas partes del almacén de contenido, ver salidas de informes guardadas en el portal, seleccionar celdas de salidas de informes guardadas en Cognos Viewer y utilizar el menú contextual de Cognos Viewer para realizar acciones, como acceder a detalles.
Admin. de informes	Los miembros pueden administrar el contenido público, para el que tengan acceso completo. También pueden utilizar IBM Cognos Analytics - Reporting y IBM Cognos Query Studio.
Administradores del servidor	Los miembros pueden administrar servidores, asignadores y trabajos.

Roles de licencia

Para ayudarle a correlacionar las capacidades según los requisitos de licencias, Cognos Analytics también proporciona roles predefinidos que se basan en titularidades de licencia.

En la tabla siguiente se enumeran los roles predefinidos de licencia.

Tabla 58. Roles predefinidos Cognos de licencia

Rol de licencia	Descripción
Administradores de Analytics	Los miembros tienen los mismos permisos de acceso que los exploradores de Analytics. También puede acceder a IBM Software Development Kit.
Exploradores de Analytics	Los miembros tienen los mismos permisos de acceso que los usuarios de Analytics. También pueden acceder a Planning Analytics para Microsoft Excel, Cognos Framework Manager, Cognos Cube Designer, Dynamic Query Analyzer y Transformer.

Tabla 58. Roles predefinidos Cognos de licencia (continuación)

Rol de licencia	Descripción
Usuarios de Analytics	Los miembros pueden crear nuevos informes, paneles de control, historias, nuevos trabajos, conexiones de servidor de datos y orígenes o módulos de datos. Pueden ejecutar informes, responder a solicitudes y cargar archivos. También pueden acceder a Cognos para Microsoft Office, Cognos Workspace, Cognos Event Studio, Cognos Query Studio y Cognos Analysis Studio.
Usuarios de distribución de información	Los miembros pueden leer contenido público, como informes. No obstante, los miembros no pueden ejecutar contenido público.

Permisos predeterminados basados en licencias

En IBM Cognos Analytics, el contador de licencias de **Gestionar > Licencias** lo controlan las funciones concedidas a un usuario, grupo o rol.

Nota: Si realiza cambios en los permisos predeterminados, un usuario puede ascender a una licencia diferente a la que se le ha concedido de forma predeterminada.

La tabla siguiente correlaciona las funciones concedidas a cada licencia. Las funciones están divididas en funciones protegidas. La letra X indica que se ha otorgado permiso para una función protegida específica.

Tabla 59. Funciones de Cognos Analytics 11 por roles de licencia

Función	Característica protegida	Distribución de información	Usuario de Analytics	Explorador de Analytics	Administrador de Analytics	Comentarios
Adaptive Analytics		No aplicable	No aplicable	No aplicable	No aplicable	
Administración			X	X	X	
	Administración de Adaptive Analytics	No aplicable	No aplicable	No aplicable	No aplicable	
	Tareas de administración				X	
	Configurar y gestionar el sistema				X	
	Administración de Controller	No aplicable	No aplicable	No aplicable	No aplicable	Es necesaria una titularidad de IBM Connections separada
	Conexiones de orígenes de datos		X	X	X	

Tabla 59. Funciones de Cognos Analytics 11 por roles de licencia (continuación)

Función	Característica protegida	Distribución de información	Usuario de Analytics	Explorador de Analytics	Administrador de Analytics	Comentarios
	Listas de distribución y contactos				X	
	Administración de Metric Studio				X	
	Administración de Mobile				X	
	Administración de Planning	No aplicable	No aplicable	No aplicable	No aplicable	Es necesaria una titularidad de IBM Planning Contributor separada
	Servidores de PowerPlay		X	X	X	Es necesaria una licencia de IBM Connections separada
	Impresoras				X	
	Administración de Query Service				X	
	Ejecutar actividades y planificaciones				X	
	Establecer prestaciones y gestionar perfiles de IU				X	
	Estilos y portlets				X	
	Usuarios, grupos y roles				X	
Analysis Studio			X	X	X	
Cognos Insight		No aplicable	No aplicable	No aplicable	No aplicable	
Cognos Viewer		X	X	X	X	

Tabla 59. Funciones de Cognos Analytics 11 por roles de licencia (continuación)

Función	Característica protegida	Distribución de información	Usuario de Analytics	Explorador de Analytics	Administrador de Analytics	Comentarios
	Menú contextual	X	X	X	X	
	Ejecutar con opciones		X	X	X	
	Selección	X	X	X	X	
	Barra de herramientas	X	X	X	X	
Colaborar			X	X	X	Es necesaria una titularidad de IBM Connections separada
	Permitir características de colaboración		X	X	X	Es necesaria una titularidad de IBM Connections separada
	Lanzar herramientas de colaboración		X	X	X	Es necesaria una titularidad de IBM Connections separada
Controller Studio		No aplicable	No aplicable	No aplicable	No aplicable	Es necesaria una titularidad de IBM Connections separada
Panel de control			X	X	X	
Data Manager		No aplicable	No aplicable	No aplicable	No aplicable	
Herramientas de escritorio				X	X	
Conjuntos de datos		X	X	X	X	

Tabla 59. Funciones de Cognos Analytics 11 por roles de licencia (continuación)

Función	Característica protegida	Distribución de información	Usuario de Analytics	Explorador de Analytics	Administrador de Analytics	Comentarios
Errores detallados		X	X	X	X	Cuando el administrador otorga este permisos, el usuario puede ver mensajes de error detallados en el visor y el informe
Ayudante para acceso a detalles			X	X	X	Cuando el administrador concede este permiso, el usuario puede ver los parámetros que se han pasado desde el origen y cómo éstos se correlacionan en el objeto de destino desde la página Ir a, utilizando el asistente de acceso a detalles.
Event Studio			X	X	X	
Ejecutar búsqueda con índice		X	X	X	X	
Panel de control ejecutivo			X	X	X	
	Utilizar características avanzadas de panel de control		X	X	X	

Tabla 59. Funciones de Cognos Analytics 11 por roles de licencia (continuación)

Función	Característica protegida	Distribución de información	Usuario de Analytics	Explorador de Analytics	Administrador de Analytics	Comentarios
	Utilizar características interactivas de panel de control		X	X	X	
Repositorios externos		X	X	X	X	El administrador debe activar los permisos establecidos para que los usuarios puedan acceder a los archivos archivados
	Administrar conexiones de repositorios				X	
	Ver documentos externos	X	X	X	X	
Generar salida CSV		X	X	X	X	
Generar salida PDF		X	X	X	X	
Generar salida XLS		X	X	X	X	
Generar salida XML		X	X	X	X	
Glosario		X	X	X	X	Integración con el glosario de IBM InfoSphere Business. Se puede utilizar directamente desde el visor
Ocultar entradas		X	X	X	X	
Importar metadatos relacionales					X	

Tabla 59. Funciones de Cognos Analytics 11 por roles de licencia (continuación)

Función	Característica protegida	Distribución de información	Usuario de Analytics	Explorador de Analytics	Administrador de Analytics	Comentarios
Linaje		X	X	X	X	Una vez habilitado, el usuario tiene acceso desde el visor
Gestionar contenido					X	
Administrar inicios de sesión de origen de datos propios			X	X	X	
Metric Studio				X	X	
	Editar vista			X	X	
Mobile		X	X	X	X	
Planning Contributor		No aplicable	No aplicable	No aplicable	No aplicable	Es necesaria una titularidad de IBM Planning Contributor separada
PowerPlay Studio			X	X	X	Es necesaria una licencia de IBM Connections separada
Query Studio			X	X	X	
	Advanced		X	X	X	
	Crear		X	X	X	
Report Studio			X	X	X	
	Permitir datos externos				X	
	Separación		X	X	X	
	Crear/Suprimir		X	X	X	
	Elementos HTML en informe		X	X	X	

Tabla 59. Funciones de Cognos Analytics 11 por roles de licencia (continuación)

Función	Característica protegida	Distribución de información	Usuario de Analytics	Explorador de Analytics	Administrador de Analytics	Comentarios
	SQL definido por el usuario		X	X	X	
Planificación			X	X	X	
	Planificación por día		X	X	X	
	Planificación por hora		X	X	X	
	Planificación por minuto		X	X	X	
	Planificación por mes		X	X	X	
	Planificación por activador		X	X	X	
	Planificación por semana		X	X	X	
	Planificación por año		X	X	X	
	Planificación por prioridad				X	
Asistente para paquetes de autoservicio					X	
Establecer funciones específicas de entradas					X	
Instantáneas		X	X	X	X	
Ejecución de especificaciones					X	
Cargar archivos			X	X	X	
Reglas de observación			X	X	X	
Modelado basado en web			X	X	X	

Asignación de capacidades según roles de licencia

Puede asignar funciones, basándose en la titularidad de roles de licencia.

- Para utilizar los roles predefinidos que se configuran automáticamente durante la instalación, siga los pasos de la sección **Cómo restringir usuarios en función de sus roles de licencia en Cognos Analytics (versión 11.0.7 +)**.
- Para configurar manualmente estos roles, siga los pasos que se indican en **Cómo restringir usuarios en función de sus roles de licencia en Cognos Analytics (versiones 11.0.0 a 11.0.6)**.

Escenario de actualización: Si los roles personalizados tienen los mismos nombres que los roles de licencia más recientes

Si anteriormente ha creado roles con los mismos nombres de licencia que los roles de licencia de Cognos más reciente y está planificando una actualización, tenga en cuenta qué funciones desea aplicar a los roles después de la actualización.

Para obtener más información, consulte “Roles de licencia” en la página 246.

- Si desea seguir utilizando las capacidades que ya había asignado a dichos roles con anterioridad, puede realizar la actualización sin perderlas.
- No obstante, si desea adoptar las capacidades de los nuevos roles de licencia, primero debe eliminar o cambiar los nombres de los roles actuales **antes de la actualización**.

Valores de seguridad después de la instalación

La instalación del software de IBM Cognos software installation ya debe estar configurada para utilizar un proveedor de autenticación, lo que se documenta en la IBM Cognos Analytics Guía de instalación y configuración.

Cuando se crean los roles predefinidos durante la inicialización del almacén de contenido, el grupo **Todos** forma parte del rol **Administradores del sistema**, lo que significa que todos los usuarios tienen un acceso completo al almacén de contenido. Para limitarlo, debe añadir los usuarios de confianza como miembros de este rol y, a continuación, eliminar el grupo **Todo** de éste.

También debe modificar la lista de miembros de los roles predefinidos, que incluyen el grupo **Todos**, como **Consumidores**, **Usuarios de consultas** y **Autores**. Realice modificaciones similares en ellos, como haría con el rol **Administradores del sistema**. Estas modificaciones también deben tener en cuenta los términos de licencia.

Si no desea utilizar los roles predefinidos, puede suprimirlos.

Para proteger el espacio de nombres de **Cognos**, modifique sus permisos de acceso iniciales. Para ello, otorgue acceso a los usuarios necesarios.

Cuando establezca los permisos de acceso, no debe denegar explícitamente el acceso a las entradas del grupo **Todos**, ya que, si lo hace, reemplazará las demás políticas de seguridad de la entrada. Si deniega el acceso a la entrada de **Todos**, dicha entrada no se podrá utilizar.

Para mantener una instalación segura, solamente se les debe otorgar a los usuarios los permisos y las funciones necesarias para que puedan realizar las tareas que se les asignan. Por ejemplo, normalmente los **Lectores** solamente tendrían permisos

de lectura y visita para **Carpetas públicas** y no tendrían permiso para crear informes utilizando ningún estudio. Los consumidores generalmente solo tienen permisos de lectura, visita y ejecución.

Determinadas funciones, como **Elementos HTML en informe** y **SQL definido por el usuario**, deben administrarse con sumo cuidado. Estas funciones se comprueban durante el proceso de creación, así como al ejecutar informes. Si un consumidor necesita ejecutar un informe que precisa estas características, puede utilizar la característica **Ejecutar como propietario** para limitar el número de usuarios del sistema que necesitan estas características. La característica **Ejecutar como propietario** utiliza las credenciales del propietario del informe para realizar comprobaciones de funciones y para acceder a los datos.

Para obtener información acerca de cómo se otorgan las capacidades para los paquetes, consulte: Capacidades de objeto.

Protección de Administradores del sistema y roles predefinidos

Como uno de los primeros pasos de la configuración de la seguridad para el entorno de IBM Cognos, modifique la pertenencia inicial del rol Administradores del sistema y otros roles predefinidos.

Si el grupo **Todos** es miembro de un rol predefinido, elimine el grupo de la pertenencia a roles.

Procedimiento

1. En **Gestionar > Consola de administración**, abra **IBM Cognos Administration**.
2. En la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
3. Pulse el espacio de nombres **Cognos**.
4. En la columna **Acciones** del rol que desea modificar, pulse el botón **Establecer propiedades**.
5. En la pestaña **Miembros**, modifique la pertenencia de rol:
 - Asegúrese de que uno o más usuarios definidos en su proveedor de autenticación sean miembros.
 - Elimine el grupo **Todos** si este grupo es miembro del rol.
 - Pulse **Aceptar**.
6. En la pestaña **Permisos**, establezca los permisos de acceso para este rol, con el fin de evitar que los usuarios no autorizados puedan crear, actualizar o suprimir el contenido y, a continuación, pulse **Aceptar**.
7. Con cada rol que desee modificar, repita los pasos del 3 al 6.

Protección del espacio de nombres de Cognos

También puede configurar el espacio de nombres de Cognos como sigue.

Procedimiento

1. En **Gestionar > Consola de administración**, abra **IBM Cognos Administration**.
2. En la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
3. En la columna **Acciones** situada junto al espacio de nombres de Cognos, pulse el botón **Establecer propiedades**.

4. En la pestaña **Permisos**, establezca los permisos de acceso para el espacio de nombres de **Cognos**, con el fin de evitar que los usuarios no autorizados puedan crear, actualizar o suprimir el contenido.
Se recomienda eliminar el grupo Todos. Sin embargo, puede conservarlo, según sus necesidades.
5. Si lo desea, seleccione la casilla de verificación **Suprimir los permisos de acceso de todas las entradas hijo**.
6. Pulse **Aceptar**.

Protección del almacén de contenido

Para garantizar la seguridad y la integridad del almacén de contenido, el servicio de Content Manager accede a él a través del inicio de sesión único de base de datos especificado en IBM Cognos Configuration. El inicio de sesión de base de datos está cifrado según los estándares de cifrado del usuario. No obstante, la seguridad del almacén de contenido no depende solamente de la de IBM Cognos Analytics sino también de la seguridad de la base de datos nativa, la del sistema operativo y la de la red.

Para proteger la base de datos, siga estas directrices:

- Proteja la base de datos y la API de la base de datos mediante los mecanismos que proporciona la propia base de datos, la red y el sistema operativo.
- Asigne un número limitado de usuarios para el mantenimiento de la base de datos.
- Use del siguiente modo la seguridad nativa de la base de datos para otorgar el mínimo de permisos a las cuentas de usuario que tienen acceso a la base de datos:
 - Microsoft SQL Server
Los usuarios deben tener permisos para crear y descartar tablas en la base de datos. Asegúrese de que la cuenta de usuario sea miembro de los roles db_ddladmin, db_datareader y db_datawriter, y también propietaria de su propio esquema predeterminado.
 - ORACLE
Los usuarios deben tener permiso para conectarse a la base de datos. También deben ser capaces de crear, modificar y descartar tablas, activadores, vistas, procedimientos y secuencias, además de insertar, actualizar y suprimir datos de las tablas de base de datos. Los permisos deben otorgarse directamente a la cuenta de usuario, y no a través de la pertenencia a un grupo o rol.
 - IBM Db2
Los usuarios deben tener permisos para crear, descartar tablas, CREATETAB, CONNECT e IMPLICITSCHEMA en relación con la base de datos. También deben tener permisos USE para el espacio de tabla USER TEMPORARY y otros espacios de tabla apropiados asociados a la base de datos.
 - Sybase Adaptive Server Enterprise
Los usuarios deben tener permiso para crear, descartar tabla, crear valor predeterminado, crear procedimiento, crear regla, crear tabla y crear vista en la base de datos.
- Limite el número de usuarios que tienen acceso de lectura o escritura a las tablas de Content Manager.
- Siga otras recomendaciones para proteger la base de datos. Para obtener información, consulte la documentación de la base de datos.

Capítulo 16. Propiedades de la entrada

Puede controlar la forma en que aparece y se comporta una entrada modificando sus propiedades. Las propiedades de las entradas varían según el tipo de entrada y sus privilegios. Por ejemplo, los informes tienen propiedades para controlar las opciones de ejecución, mientras que las carpetas no las tienen. Si una propiedad no es aplicable al tipo de entrada que está personalizando, no aparecerá en la página **Establecer propiedades**.

Propiedades generales

Las propiedades generales aparecen en la pestaña **General** de la página **Establecer propiedades**.

En la tabla siguiente se describen las propiedades generales disponibles.

Tabla 60. Propiedades de entrada general

Propiedad	Descripción
Tipo	El tipo de entrada.
Propietario	El propietario de la entrada. De forma predeterminada, el propietario es la persona que creó la entrada. Cuando ya no existe ningún propietario en el espacio de nombres, o es un espacio de nombres distinto al del usuario actual, el propietario se muestra como No disponible. Si dispone de permisos de establecimiento de políticas, pulse Convertir al usuario en propietario para convertirse en el propietario de la entrada.
Contacto	La persona responsable de la entrada. Pulse Establecer contacto y luego en Seleccionar el contacto para establecer el contacto para la entrada, o bien pulse Introducir una dirección de correo electrónico para introducir la dirección de correo electrónico del contacto.
Ubicación	La ubicación de la entrada en el portal y su ID. Pulse Ver ruta de búsqueda, ID y URL para ver la ubicación completa y el identificador de la entrada en el almacén de contenido. A las entradas se les asigna un número de identificación (IID) exclusivo.
Creado	La fecha en la que se creó la entrada.
Modificado	La fecha más reciente en la que se modificó la entrada.
Icono	El icono para la entrada. Pulse Editar para especificar un icono alternativo.

Tabla 60. Propiedades de entrada general (continuación)

Propiedad	Descripción
Con índice	La indicación de fecha y hora que indica cuándo se ha indexado la entrada por última vez. La propiedad no aparece si la entrada no se ha indexado.
Inhabilitar esta entrada	Una vez seleccionada esta opción, los usuarios sin permisos de escritura para esta entrada no podrán acceder a ella. La entrada ha dejado de estar visible en el portal. Si tiene acceso de escritura a una entrada que está inhabilitada, el icono de inhabilitado aparecerá junto a la entrada.
Ocultar esta entrada	Seleccione esta propiedad para ocultar informes, paquetes, páginas, carpetas, trabajos y otros tipos de entradas. Puede ocultar una entrada para evitar que se utilice de forma innecesaria o para organizar la vista. Las demás entradas podrán seguir accediendo a la entrada oculta. Por ejemplo, se podrá acceder a un informe oculto como destino de acceso a detalles. La entrada oculta se seguirá viendo, si bien su icono estará atenuado. Si desactiva la casilla de verificación Mostrar entradas ocultas en las opciones de Mi área , Mis preferencias, dejará de ver la entrada. Para ver esta propiedad, el administrador debe haberle otorgado la función Ocultar entradas.
Idioma	Una lista de los idiomas que están disponibles para el nombre de entrada, la sugerencia y la descripción según la configuración que estableció su administrador. Pulse Eliminar valores de este idioma para eliminar el nombre de la entrada, la sugerencia y la descripción de un idioma especificado.
Nombre	El nombre de la entrada del idioma seleccionado.
Sugerencia	Una descripción opcional de la entrada. La sugerencia aparece al detener el puntero sobre el icono de la entrada del portal. Se pueden utilizar más de 100 caracteres para una sugerencia.
Descripción	Una descripción opcional de la entrada. Aparece en el portal cuando establece sus preferencias para utilizar la vista de detalles. La vista de detalles aparece únicamente en las Carpetas públicas y en Mis carpetas.
Historial de ejecución	El número de apariciones o el periodo de tiempo que hay que conservar los historiales de ejecución de la entrada.
Versiones de salida de informe	El número de apariciones o el periodo de tiempo que hay que conservar las salidas de informe. Al establecer este valor a cero (0), se guarda un número ilimitado de versiones.

Tabla 60. Propiedades de entrada general (continuación)

Propiedad	Descripción
Paquete	El paquete que está asociado con la entrada. Si movió o suprimió el paquete de origen, el texto indica No disponible. Pulse Enlace a un paquete para vincular la entrada a un paquete diferente.
URL	Un URL a un archivo o a una dirección de sitio web. Este campo sólo es visible si dispone de permisos de lectura para la entrada. Si dispone de permisos de escritura sin permisos de lectura, esta propiedad no estará visible.
Informe origen	Una ruta de acceso a la entrada origen de una vista de informe. Si movió o suprimió la entrada de origen, el texto indica No disponible. Pulse Propiedades del informe para visualizar las propiedades de informe de origen. Pulse Enlace a un informe para vincular la entrada a un paquete diferente.
Agente de origen	Una ruta de acceso a la entrada origen de una vista de agente. Si movió o suprimió la entrada de origen, el texto indica No disponible. Pulse Propiedades del agente para visualizar las propiedades del informe de origen. Pulse Enlace a un agente para vincular la entrada a un paquete diferente.
Direccionamiento avanzado	Las etiquetas de direccionamiento se pueden aplicar a los objetos de datos, tales como paquetes, módulos de datos y archivos cargados y a los grupos de usuarios y roles. Estas etiquetas, junto con los grupos de servidores, se utilizan para especificar reglas de direccionamiento para los asignadores.
Pasarela	La ubicación del servidor web en donde reside el producto de IBM Cognos original. Se aplica únicamente a los informes PowerPlay de Series 7.

Propiedades de informe de Report, Query, Analysis y PowerPlay

Las propiedades de informe aparecen en las siguientes pestañas de la página **Establecer propiedades**:

- La pestaña **Informe** de los informes de Creación de informes
- La pestaña **Consulta** de los informes de Query Studio
- La pestaña **Análisis** de los informes de Analysis Studio
- La pestaña **PowerPlay Report** de los importes de PowerPlay de Series 7

Puede seleccionar los tamaños de papel disponibles. En **IBM Cognos Administration**, pulse **Configuración > Asignadores y servicios**. Pulse el botón para definir los tamaños del papel . Para añadir nuevos tamaños de papel, pulse **Nuevo**. Para suprimir tamaños de papel, pulse **Suprimir**.

En la tabla siguiente se describen las propiedades de informe disponibles.

Tabla 61. Propiedades de Report, Query, Analysis y PowerPlay Report

Propiedad	Descripción
Acción predeterminada	La acción predeterminada cuando se ejecuta el informe.
Formatos	El formato de salida que se ha de utilizar cuando se ejecuta el informe.
Opciones de PDF	Las opciones, tales como la orientación, el tamaño del papel y la contraseña para abrir el informe, que se han de utilizar para generar la salida en PDF.
Habilitar el soporte de accesibilidad	Especifica si se crearán salidas de informes que den soporte a la accesibilidad. Al habilitar este soporte, se crean salidas de informes legibles por un lector de pantalla.
Idiomas	El idioma predeterminado que se utiliza para los datos del informe cuando se ejecuta el informe.
Valores de la solicitud	Cuando el recuadro de selección está seleccionado, se solicita a los usuarios que seleccionen valores para filtrar los datos cuando se ejecuta el informe.
Valores actuales	Los valores que se utilizan para filtrar los datos cuando se ejecuta un informe. Para obtener más información, consulte “Cómo especificar los valores de la solicitud predeterminados para un informe” en la página 366.
Historial de ejecución	Especifica durante cuánto tiempo se han de conservar los historiales de ejecución. Puede guardar los historiales de ejecución durante un número de ejecuciones o un número de días o meses específicos.
Versiones de salida de informe	Especifica durante cuánto tiempo se han de conservar los historiales de salida de informes. Puede guardar la salida de informe durante un número de ejecuciones o un número de días o meses específicos.
Filas por página en informes HTML	El número de filas que desea que aparezcan por página web en los informes HTML
Ejecutar como el propietario	Permite utilizar las credenciales del propietario cuando se ejecuta el informe. Para obtener más información, consulte “Credenciales de confianza” en la página 222.
Ejecutar como el propietario: Funciones solamente	Permite utilizar únicamente las credenciales del propietario cuando se ejecuta el informe.
Opciones de HTML: Abrir en modo de diseño	Si se ha de abrir el informe Series 7 PowerPlay de formato HTML en modo de diseño.

Propiedades del trabajo

Las propiedades del trabajo aparecen en la pestaña **Trabajo** de la página **Establecer propiedades**.

En la tabla siguiente se describen las propiedades de trabajo disponibles.

Tabla 62. Propiedades del trabajo

Propiedad	Descripción
Pasos	Una lista de pasos en el trabajo.
Envío de pasos	Permite ejecutar tareas de trabajo a la vez o de forma secuencial.
Valores predeterminados para todos los pasos	Establece valores predeterminados en el nivel del trabajo. Pulse Establecer y especifique los valores predeterminados de todos los pasos del trabajo. Si no se establecen valores predeterminados, se utilizarán los valores predeterminados de los pasos individuales.
Nivel de detalles del historial de ejecución	Pulse Todos para guardar todos los detalles del historial de los pasos del trabajo una vez que la actividad de ejecución finalice correctamente. El historial completo de los pasos del trabajo incluye los campos Nombre, Tiempo de la solicitud, Hora de inicio, Hora de finalización y Estado. Pulse Limitados para guardar sólo determinados detalles del historial de ejecución del trabajo. Entre los determinados detalles del historial de ejecución del trabajo se incluyen: la hora de inicio, la de finalización, el estado y los mensajes del trabajo. Si la ejecución del trabajo falla, se guardan todos los detalles del historial. El valor predeterminado es Todos. El valor del nivel de detalles del historial de ejecución del trabajo reemplaza los valores de los pasos del trabajo.

Propiedades del agente

Las propiedades del agente aparecen en la pestaña **Agente** de la página **Establecer propiedades**.

En la tabla siguiente se describen las propiedades de agente disponibles.

Tabla 63. Propiedades del agente

Propiedad	Descripción
Tareas	Una lista de tareas en el agente.
Acción predeterminada	La acción predeterminada cuando se ejecuta el agente.
Valores de la solicitud	Los valores que se utilizan para filtrar los datos cuando se ejecuta un agente.

Tabla 63. Propiedades del agente (continuación)

Propiedad	Descripción
Ejecutar como el propietario	Permite utilizar las credenciales de propietario cuando se ejecuta el agente. Para obtener más información, "Credenciales de confianza" en la página 222.
Ejecutar como el propietario: Funciones solamente	Permite utilizar únicamente las credenciales del propietario cuando se ejecuta el informe.
Lista de alertas	Permite a los usuarios agregarse a la lista de alertas para un agente.

Propiedades de reglas

Utilice las propiedades de reglas para definir o modificar una regla de observación. Puede acceder a las propiedades de reglas desde la pestaña **Reglas** de **Elementos de mi lista de observación** pulsando el icono Establecer propiedades de una entrada de regla de observación. Las propiedades se encuentran en la pestaña **Regla** de la página **Establecer propiedades**.

Las propiedades de reglas especifican condiciones en la salida de informes HTML guardados de modo que cuando se guarda el informe y se cumplen las condiciones, el usuario reciba una alerta.

La siguiente tabla describe las propiedades de reglas disponibles.

Tabla 64. Propiedades de regla

Propiedad	Descripción
Inhabilitar la regla	Permite inhabilitar la regla de observación. Cuando se inhabilita, la regla de observación no se aplica cuando se genera la salida de informe.
Enviar una alerta cuando el informe <i>nombre de informe</i> contenga:	El nombre del informe y la regla definida para la regla de observación. Para editar la definición, pulse la condición de filtro existente, como mayor que (>), y, en la lista que aparezca, pulse otra condición. Especifique un valor distinto en el cuadro.
Para el contexto seleccionado	Los objetos del informe al que afecta la regla.
Tipo de alerta	El tipo de alerta que se recibe cuando se cumpla la regla. Puede recibir una alerta por correo electrónico o como elemento de noticias.

Capítulo 17. Gestión de actividades

Puede ver una lista de las actividades planificadas que son actividades actuales, actividades pasadas o próximas actividades para un día específico.

Puede filtrar la lista para que aparezcan sólo las entradas que desee. Un gráfico de barras muestra una descripción general de las actividades diarias, por hora. Puede utilizar el gráfico como ayuda para elegir la fecha idónea para volver a planificar actividades. Puede establecer prioridades de ejecución para las entradas. También puede ver el historial de ejecución de las entradas, indicar cuánto tiempo se deben guardar los historiales de ejecución y volver a ejecutar entradas fallidas.

Puede ver quién ha ejecutado cada entrada y realizar acciones en entradas según sea necesario. Por ejemplo, puede que desee cancelar o suspender un trabajo de gran tamaño de un usuario si está retrasando entradas importantes en la cola. También puede reemplazar la prioridad de una instancia de entrada o cambiarla de forma permanente para la propia entrada.

Si cambia de una vista a otra, deberá renovar para ver los datos actuales. Por ejemplo, si cambia de **Actividades pasadas** a **Próximias actividades**, deberá renovar para ver los datos actuales en los paneles.

Los administradores pueden utilizar las funciones de administración **Gestionar > Actividades** o **IBM Cognos Administration** para gestionar actividades para todas las entradas de usuario.

Gestión de actividades actuales

Las actividades actuales son entradas que se están procesando ahora en el software de IBM Cognos.

Cada entrada se enumera por nombre y muestra la hora de solicitud, el estado y la prioridad para las actividades en segundo plano. El gráfico de barras muestra el número total de entradas, desglosadas por número de entradas pendientes, en ejecución, en espera y suspendidas. Cuando la actividad se está procesando, se muestra el número de proceso.

Puede ordenar las columnas **Tiempo de la solicitud**, **Estado** y **Prioridad**. Puede seleccionar ver una lista de actividades en segundo plano o actividades interactivas. El usuario que ha ejecutado la entrada también figura en la lista. Puede ordenar por usuario.

Puede suspender entradas en segundo plano y liberarlas más tarde cuando desee que se ejecuten. Puede cancelar permanentemente ejecuciones para entradas que tengan uno de los siguientes estados:

- Pendiente en cola
- En ejecución
- suspendidas
- A la espera de que se complete un proceso externo al software de IBM Cognos

Puede filtrar las entradas para mostrar sólo las que desee. Puede seleccionar mostrar sólo las entradas con un estado o prioridad específico, o bien entradas de un tipo o ámbito determinado.

Para las entradas interactivas actuales, puede filtrar por estado y por el asignador en el que se ejecuta la actividad. En el caso de entradas actuales de fondo, puede filtrar por estado, prioridad, tipo, ámbito, usuario que ha ejecutado la entrada, usuario propietario de la entrada y asignador.

Cuando una entrada está actualmente en ejecución, se muestra el asignador, el ID de proceso y la hora de inicio. Tenga en cuenta que el identificador de proceso y el asignador de las entradas en segundo plano actuales pueden no estar disponibles al aparecer la actividad inicialmente. Renueve la página para ver el identificador de proceso y el asignador actualizados.

Si cancela una entrada que contiene otras entradas, como un trabajo o un agente, se cancelarán los pasos o las tareas que aún no se hayan completado. Sin embargo, los pasos o las tareas que ya se han completado permanecerán completados.

Puede modificar la prioridad de las entradas “Visualización del historial de ejecución de las entradas” en la página 271 “Gestión de la prioridad de ejecución de entradas” en la página 270 y ver el historial de ejecución.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Actividades actuales**.
3. En la sección **Filtro**, pulse **Actividades en segundo plano** o **Actividades interactivas** y especifique las opciones de filtro que desea utilizar.

Consejo: Si desea utilizar opciones avanzadas de filtro, pulse **Opciones avanzadas**. Para restablecer los valores predeterminados de todas las selecciones, pulse **Restablecer valores predeterminados**.

4. Pulse **Aplicar**.
La lista muestra las entradas seleccionadas.
5. Para realizar una acción en una entrada individual, pulse la flecha de **Acciones** correspondiente a la entrada y seleccione la acción. Para realizar una acción en varias entradas, seleccione la casilla de verificación de las entradas que desee y pulse uno de los siguientes botones de la barra de herramientas.

En la tabla siguiente se especifican las acciones disponibles para las entradas y los iconos asociados:

Tabla 65. Administrar las acciones e iconos de las actividades actuales

Acción	Icono
Mostrar detalles (esquina superior derecha)	
Ocultar detalles (esquina superior derecha)	
Cancelar la ejecución (menú Acciones junto a la entrada)	
Suspender la ejecución (menú Acciones junto a la entrada)	
Ejecutar las entradas suspendidas (menú Acciones junto a la entrada)	

Tabla 65. Administrar las acciones e iconos de las actividades actuales (continuación)

Acción	Icono
Establecer prioridad (menú Acciones junto a la entrada)	

Consejo: Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

Gestión de actividades pasadas

Las actividades pasadas son entradas que han terminado de procesarse en el software de IBM Cognos.

Cada entrada se enumera por nombre y muestra la hora de solicitud y el estado. Puede ordenar las columnas **Tiempo de la solicitud** y **Estado**. El gráfico de barras muestra el número total de entradas desglosado por estado. Si una entrada ha resultado fallida, aparecerá un botón que mostrará la gravedad del error. El usuario que ha ejecutado la entrada también figura en la lista.

Puede filtrar las entradas para mostrar sólo las que desee. Puede optar por ver una lista de actividades que pasaron en un periodo de tiempo especificado, por ejemplo las cuatro últimas horas o el último día, o bien puede especificar un intervalo de fechas u horas. Puede filtrar por estado, tipo o ámbito. Puede filtrar por el usuario que ha ejecutado la entrada, el usuario que es el propietario de la entrada y el asignador en el que se ha ejecutado la actividad.

Puede ver el historial de ejecución “Visualización del historial de ejecución de las entradas” en la página 271.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Actividades pasadas**.
3. Sitúese sobre el botón de error junto al estado para ver la gravedad del error.
4. Para realizar una acción en una entrada individual, pulse la flecha de **Acciones** correspondiente a la entrada y seleccione la acción.

Para realizar una acción en varias entradas, pulse el icono **Mostrar detalles**  o el icono **Ocultar detalles**  de la barra de herramientas.

Gestionar las próximas actividades para un día específico

Puede seleccionar ver una lista de todas las próximas actividades planificadas para un día específico.

Cada entrada se enumera por nombre y muestra la hora de solicitud y la prioridad. Un gráfico de barras muestra el número total de entradas planificadas y canceladas para cada hora del día. La leyenda del gráfico muestra el número total de entradas planificadas y canceladas del día.

Puede ordenar las columnas **Tiempo de la solicitud**, **Estado** y **Prioridad**. Puede seleccionar ver una lista de actividades en segundo plano o actividades interactivas.

Cada entrada muestra el usuario que la ha planificado. Puede ordenar por usuario.

Puede cancelar ejecuciones planificadas de entradas, volver a planificar ejecuciones de entradas que se han cancelado y establecer prioridades. Puede suspender las entradas indefinidamente o hasta una fecha determinada. Para obtener más información, consulte “Actividades suspendidas” en la página 267

Puede pulsar el icono **Mostrar detalles**  para ver más información. Para cada entrada, se muestran los valores de **Tiempo de respuesta de la última ejecución** y **Ruta de acceso**.

Puede filtrar las entradas para mostrar sólo las que desee. Puede seleccionar el día y la hora para los que desee ver las próximas actividades. Puede filtrar por estado, prioridad, tipo y ámbito.

También puede filtrar por el usuario que ha planificado la entrada y por el propietario de la entrada.

Puede aplicar un filtro para determinar cuántas entradas planificadas están suspendidas actualmente. Para obtener más información, consulte “Actividades suspendidas” en la página 267.

Puede cambiar la prioridad de una entrada en la cola “Gestión de la prioridad de ejecución de entradas” en la página 270.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Próximas actividades**.
3. En la sección **Filtro**, pulse las opciones de filtro que desee utilizar.

Consejo: Si desea utilizar opciones avanzadas de filtro, pulse **Opciones avanzadas**. Para restablecer los valores predeterminados de todas las selecciones, pulse **Restablecer valores predeterminados**.

4. Pulse **Aplicar**.
 - La lista muestra las entradas seleccionadas.
 - La línea de estado del filtro muestra los criterios utilizados para generar la lista.
 - El gráfico de barras muestra las entradas planificadas y canceladas por hora del día especificado.

La lista de entradas, la línea de estado del filtro y el gráfico se actualizan cada vez que se vuelve a definir el filtro y se pulsa **Aplicar**. La lista de entradas y la línea de estado del filtro no cambian cuando se examina el gráfico con una fecha diferente.

5. Para realizar una acción en una entrada individual, pulse la flecha de **Acciones** correspondiente a la entrada y seleccione la acción. Para realizar una acción en varias entradas, seleccione la casilla de verificación de las entradas que desee y pulse uno de los siguientes botones de la barra de herramientas.

En la tabla siguiente se especifican las acciones disponibles para las entradas y los iconos asociados:

Tabla 66. Administrar las acciones e iconos de las próximas actividades para un día específico

Acción	Icono
Mostrar detalles (esquina superior derecha)	
Ocultar detalles (esquina superior derecha)	
Cancelar la ejecución (menú Acciones junto a la entrada)	
Suspender entradas (menú Acciones junto a la entrada)	
Ejecutar las entradas suspendidas (menú Acciones junto a la entrada)	
Volver a planificar una ejecución cancelada (menú Acciones junto a la entrada)	
Establecer prioridad (menú Acciones junto a la entrada)	

Consejo: Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

Actividades suspendidas

Puede suspender entradas para cumplir requisitos del sistema y retomarlas más adelante.

Después de suspender entradas, puede ver una lista de las entradas que están suspendidas indefinidamente.

Puede reanudar las entradas suspendidas incluso después de que haya transcurrido el tiempo de ejecución original. Por ejemplo, si planifica un informe para las 9:00 AM y, a continuación, lo suspende, podrá reiniciarlo a las 9:30 AM.

El gráfico de barras de próximas actividades le servirá de ayuda para determinar cuándo volver a planificar las entradas. Si explora las fechas próximas en el gráfico, podrá ver el número de entradas de un día determinado. Si detiene el puntero sobre una hora concreta del día, podrá ver el número de entradas de esa hora. Utilice esta función para localizar una fecha en que la demanda sea baja y volver a planificar la entrada en esa fecha. Las columnas del gráfico muestran el número total de entradas planificadas y canceladas para cada hora del día. La leyenda del gráfico muestra el número total de entradas planificadas, canceladas y suspendidas del día.

Suspensión de entradas

Puede suspender actividades.

Por ejemplo, si el sistema tiende a sobrecargarse a determinadas horas del día, puede reducir la carga de trabajo y evitar cuellos de botella durante estos picos de actividad suspendiendo entradas indefinidamente o volviéndolas a planificar para más adelante.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Próximamente**.
3. En la sección **Filtro**, seleccione una fecha en **Día**, y en **Estado** pulse **Planificado**.
4. Pulse **Aplicar**.

La lista muestra las entradas planificadas correspondientes a la fecha seleccionada. Puesto que hay entradas atrasadas en esa fecha, puede que sea conveniente suspender determinadas entradas indefinidamente y volver a planificar otras. Desea examinar las próximas fechas en el gráfico y seleccionar otra fecha para las entradas suspendidas.

5. En el gráfico, pulse los iconos Siguiente y Anterior para examinar las próximas fechas. El gráfico muestra las entradas planificadas y canceladas por hora de cada día.

Importante: La lista de entradas que aparece no cambia para corresponderse con la fecha que seleccione en el gráfico. La lista de entradas corresponde al criterio de filtro especificado y no cambiará hasta que especifique y aplique un nuevo filtro.

6. En la lista de entradas planificadas, seleccione la casilla de verificación correspondiente a las entradas que desea suspender y pulse el botón Suspend de la barra de herramientas. En el cuadro de diálogo **Suspender actividad**:

- Para suspender entradas indefinidamente, pulse **Indefinidamente**.
- Para volver a planificar entradas en otra fecha, pulse **Hasta** y seleccione una fecha y una hora.

Observe que se renuevan tanto el gráfico como la lista de entradas, y las entradas suspendidas dejan de aparecer en la lista de entradas.

Consejo: Para suspender una entrada determinada, pulse la flecha del menú **Acciones** de la entrada y pulse **Suspender**.

Visualización de las entradas suspendidas de un día determinado

Puede visualizar una lista de las entradas suspendidas de un día determinado.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Próximamente**.
3. En la sección **Filtro**, bajo **Día** seleccione una fecha, y en **Estado** pulse **Suspendido**.
4. Pulse **Aplicar**.

La lista muestra las entradas suspendidas de ese día.

Puede ejecutar, cancelar o volver a planificar las entradas suspendidas. Para realizar una acción en una entrada concreta, pulse la flecha situada a la derecha de la entrada y seleccione la acción que desea realizar. Para realizar una acción en varias entradas, seleccione la casilla de verificación de las entradas que desee y pulse el botón que corresponda de la barra de herramientas.

En la tabla siguiente se especifican las acciones disponibles para las entradas y los iconos asociados:

Tabla 67. Ver una lista de entradas suspendidas para las acciones e iconos de un día específico

Acción	Icono
Mostrar detalles (esquina superior derecha)	
Ocultar detalles (esquina superior derecha)	
Cancelar la ejecución (menú Acciones junto a la entrada)	
Suspender entradas (menú Acciones junto a la entrada)	
Ejecutar las entradas suspendidas (menú Acciones junto a la entrada)	
Volver a planificar una ejecución cancelada (menú Acciones junto a la entrada)	
Establecer prioridad (menú Acciones junto a la entrada)	

Consejo: Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

Gestión de actividades planificadas

Puede ver una lista de entradas planificadas para todos los usuarios.

Cada entrada se enumera por nombre, estado y prioridad. Un gráfico de barras muestra una descripción general de actividades desglosado por planificaciones habilitadas e inhabilitadas.

Se muestra la fecha y la hora de modificación de la planificación y el usuario que la ha planificado.

Puede filtrar las entradas para mostrar sólo las que desee. Puede optar por mostrar únicamente las entradas con un estado o prioridad específico, o bien las entradas de un determinado tipo o ámbito. También puede filtrar por el usuario que ha planificado la entrada y por el propietario de la entrada.

Puede establecer propiedades, ejecutar la planificación una vez, inhabilitar y habilitar entradas planificadas, modificar la planificación, eliminar la planificación, establecer la prioridad “Gestión de la prioridad de ejecución de entradas” en la página 270 y ver el historial de ejecución “Visualización del historial de ejecución de las entradas” en la página 271. Según la entrada también puede realizar otras funciones, como las entradas de vistas o las listas de eventos.

Para obtener más información sobre planificaciones, consulte: Capítulo 18, “Administración de planificaciones”, en la página 277.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Planificaciones**.
3. En la sección **Filtro**, pulse las opciones de filtro que desee utilizar.

Consejo: Si desea utilizar opciones avanzadas de filtro, pulse **Opciones avanzadas**. Para restablecer los valores predeterminados de todas las selecciones, pulse **Restablecer valores predeterminados**.

4. Pulse **Aplicar**.

La lista muestra las entradas seleccionadas.

5. Para realizar una acción en una entrada individual, pulse la flecha del menú Acción, junto a la entrada y seleccione la acción. Para realizar una acción en varias entradas, seleccione la casilla de verificación de las entradas que desee y pulse uno de los siguientes botones de la barra de herramientas.

En la tabla siguiente se especifican las acciones disponibles para las entradas y los iconos asociados:

Tabla 68. Acciones e iconos de actividades planificadas

Acción	Icono
Mostrar detalles (esquina superior derecha)	
Ocultar detalles (esquina superior derecha)	
Habilitar la planificación (menú Acciones junto a la entrada)	
Inhabilitar la planificación (menú Acciones junto a la entrada)	
Establecer prioridad (menú Acciones junto a la entrada)	

Consejo: Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

Gestión de la prioridad de ejecución de entradas

Puede asignar una prioridad de 1 a 5 a entradas planificadas.

Por ejemplo, una entrada con una prioridad 1 se ejecuta antes que una entrada con prioridad 5. Si hay más de una entrada con la misma prioridad, se ejecutará primero la que llegó antes a la cola. La prioridad predeterminada es 3.

Las entradas interactivas siempre se ejecutan inmediatamente y la prioridad no se puede cambiar una vez que se están ejecutando.

La prioridad de una entrada se establece al planificarla Capítulo 18, “Administración de planificaciones”, en la página 277. Cuando una entrada se encuentra en la cola actual, próxima o planificada, se puede cambiar la prioridad.

Es posible que desee establecer una prioridad baja para las entradas que tardan en ejecutarse de modo que otras entradas de la cola no se retrasen.

Cuando se ejecuta un trabajo “Utilizar trabajos para planificar varias entradas” en la página 281, se establece la prioridad de todo el trabajo, no de cada una de las

entradas del trabajo. Es posible que desee establecer una prioridad baja para un trabajo con muchas entradas de modo que las otras entradas de la cola no se retrasen.

Planifique la prioridad para el trabajo padre. Cuando se ejecute el trabajo, todas las entradas hijo heredarán la prioridad del trabajo padre. Si el trabajo está en la cola sin ejecutarse todavía, se puede actualizar su prioridad. Esto no puede hacerse para las entradas individuales del trabajo. Cambiar la prioridad del trabajo cambia la prioridad de todas sus entradas hijo. Puede ver el historial de ejecución de un trabajo “Visualización del historial de ejecución de las entradas” mientras se está ejecutando y comprobar cuáles de sus entradas se han completado, se están ejecutando o están pendientes.

La prioridad de las entradas que están en la cola no afecta a la entrada que ya se esté ejecutando. Esa entrada se completa y, a continuación, se revisa la prioridad de la cola para ver cuál es la próxima entrada que debe ejecutarse.

Consejo: En IBM Cognos Administration, puede cambiar la prioridad de las entradas en función de las opciones filtradas. Por ejemplo, para cambiar la prioridad de todas las entradas ejecutadas por Joan Jackson, seleccione este nombre en **Ejecutado por** en **Filtro**. A continuación, puede seleccionar todas las entradas visualizadas y cambiar la prioridad de todas ellas a la vez.

Antes de empezar

Debe disponer de la función **Ejecutar actividades y planificaciones** para administrar la prioridad de ejecución de las entradas.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Actividades actuales, Próximas actividades o Planificaciones**.
3. Para cambiar la prioridad de una entrada, haga clic en la flecha del menú Acción junto a la entrada y seleccione **Establecer prioridad**. Para modificar la prioridad de más de una entrada, seleccione la casilla de verificación de las entradas que desee y pulse el botón Establecer prioridad  de la barra de herramientas.

Consejo: Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

4. Desde el menú, pulse la prioridad que desee y, a continuación, en **Aceptar**.

Resultados

La nueva prioridad aparecerá en la columna **Prioridad** situada junto a las entradas que seleccionó.

Visualización del historial de ejecución de las entradas

Puede ver el historial de ejecución de entradas planificadas para su ejecución en segundo plano, sin que nadie espere para visualizarlas.

Esto incluye las entradas planificadas que se ejecutan una vez y se guardan y las entradas interactivas que se guardan o se envían por correo. Las entradas interactivas no tienen historiales de ejecución.

El software de IBM Cognos mantiene la información de historial cada vez que se ejecuta una entrada en segundo plano. El historial de ejecución de una entrada incluye información como la hora de solicitud, la hora de inicio, la hora de finalización y si el informe se ejecutó correctamente.

Puede ver un historial de ejecución más detallado para la entrada, que incluye mensajes generales, de error y de aviso relacionados con la entrada y las acciones que se pueden llevar a cabo. Si hay mensajes de correo electrónico asociados con la entrada, se incluye el estado de entrega del correo electrónico.

Algunos tipos de entradas muestran información adicional en la página de historial de ejecución detallada:

- Para los informes, se conserva una versión de salida de informe cada vez que un informe se ejecuta según una planificación. Puede ver la versión de salida de informe en el historial de ejecución detallado.
- Para los trabajos y agentes, puede ver una lista de pasos y un historial detallado de ejecución para cada uno. También puede ver las partes del trabajo o el agente que aún no se han completado. Si la entrada es parte de una entrada padre, puede ver la entrada padre que inició la ejecución.
- Para las tareas humanas contenidas en un agente, puede ver una lista de pasos y un historial detallado de ejecución para cada una.
- Para las entradas de exportación e importación del despliegue, puede ver el contenido público en **IBM Cognos Administration**.

Puede que vea el mensaje siguiente: *Sólo está disponible actualmente la información del progreso. La información se actualizará después de la finalización de la actividad padre.*

Esto significa que el despliegue ha finalizado, pero la actividad padre sigue en ejecución. Una vez obtenida de Content Manager la información final de terminación, ya no aparecerá el mensaje.

Puede volver a ejecutar las entradas fallidas “Volver a ejecutar una tarea de entrada anómala” en la página 274 desde la página detallada del historial de ejecución. Puede ver una lista de ejecuciones relacionadas que forman parte de la serie de repeticiones y ver un historial detallado de ejecución para cada una. Puede especificar cuántas apariciones del historial de ejecución desea mantener y durante cuánto tiempo “Especificación del tiempo que se deben guardar los historiales de ejecución” en la página 273.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Planificaciones** o **Actividades pasadas**.
3. Junto a la entrada, pulse la flecha y, a continuación, en **Ver historial de ejecución** .
4. Si lo desea, seleccione el **Estado** de las entradas que desee ver.
Aparecerá una lista de entradas seleccionadas.

5. Si desea ver los detalles del historial de ejecución, en la columna **Acciones**, pulse el botón Ver detalles del historial de ejecución  situado junto a la entrada que desee. Después, si lo desea, seleccione de la lista **Gravedad** la gravedad de las entradas.
Debajo de los pasos del trabajo aparecen todos los detalles del historial de ejecución. Si el nivel de detalles de dicho historial de ejecución está establecido en **Limitados**, no se registrarán detalles de historial para los pasos del trabajo.
6. Si hay una versión de salida de informe, en la columna **Acciones**, pulse el botón Ver salidas  de la entrada que desee. A continuación, en la lista **Versiones**, pulse la versión que desee. Para suprimir una versión, pulse **Administrar versiones** y en la casilla de verificación de la versión y, a continuación, en **Suprimir**.
7. Si desea ver mensajes, pulse un elemento con un enlace en la columna **Mensajes**.
Los mensajes se anidan. Puede ver mensajes hijo dentro de los mensajes hijo. Si se muestra un mensaje como un enlace, puede seguir detallando más a través de los mensajes hijo.

Especificación del tiempo que se deben guardar los historiales de ejecución

Puede guardar los historiales de ejecución durante un número de ejecuciones o un número de días o meses específicos.

Por ejemplo, puede guardar los historiales de ejecución de las últimas diez ejecuciones (apariciones), los dos últimos días o los últimos seis meses. También puede optar por guardar todos los historiales de ejecución.

Antes de empezar

Debe contar con permisos de lectura y escritura para la entrada y permisos de lectura o visita para la carpeta que contiene la entrada.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Actividades actuales**, **Próximas actividades** o **Planificaciones**.
3. Junto a la entrada, pulse la flecha y, a continuación, pulse **Establecer propiedades**.
Aparecerá la página Propiedades de la entrada.
4. En la pestaña **General**, en **Historial de ejecución**, seleccione el método de retención y escriba el valor:
 - Para conservar los historiales de ejecución durante un determinado número de apariciones, pulse **Número de apariciones** e introduzca el número. Para guardar un número ilimitado de historiales de ejecución escriba el valor 0.
 - Para conservar historiales de ejecución durante un determinado periodo de tiempo, pulse **Duración** y luego en **Días** o en **Meses**. Introduzca el valor adecuado en el cuadro.
5. Pulse **Aceptar**.

Volver a ejecutar una tarea de entrada anómala

Puede volver a enviar una entrada anómala.

Cuando una entrada, como por ejemplo un informe, una tarea de agente o un trabajo, se ejecuta según una planificación o en segundo plano y resulta fallida, puede volver a enviar la entrada fallida con las mismas opciones indicadas en la ejecución original.

En el caso de un trabajo que contienen pasos que se ejecutaron correctamente y pasos que no se ejecutaron correctamente, no es necesario volver a ejecutar todo el trabajo, sino sólo los pasos del trabajo pertinentes. Si los pasos de los trabajos se ejecutan en secuencia, puede volver a ejecutar el trabajo comenzando por el paso fallido del trabajo. Si lo desea, puede seleccionar los pasos que desee volver a ejecutar y saltarse los fallidos. Sin embargo, los pasos de trabajo seleccionados se ejecutan en secuencia y, si uno de ellos resulta fallido, los pasos que tienen lugar después del paso fallido no se ejecutan.

Cuando vuelve a ejecutar un paso de trabajo individual, se crea un nuevo historial de ejecución que incluye sólo el paso de trabajo para el trabajo padre. Para obtener más información sobre los historiales de ejecución, consulte “Visualización del historial de ejecución de las entradas” en la página 271.

Cuando se vuelve a ejecutar una entrada de agente, también se vuelven a ejecutar las tareas asociadas, por ejemplo un correo electrónico que envía la salida de informe a una lista de destinatarios, si resultaron fallidas inicialmente. Si hay dos tareas asociadas ejecutándose en paralelo y una tarea resulta fallida y la otra finaliza correctamente, repetir la ejecución del agente supone volver a ejecutar sólo la tarea fallida. Sin embargo, si las tareas se seleccionan para ejecutarse en caso de error, se vuelven a ejecutar cuando falla la repetición.

Aunque el historial de ejecución muestra las entradas que se ejecutaron correctamente, éstas no se pueden volver a ejecutar. Las opciones de ejecución no se guardan para estas entradas.

Una repetición puede resultar fallida cuando se suprime o actualiza una tarea asociada a una entrada fallida.

Antes de empezar

Debe tener permisos de ejecución para volver a ejecutar una tarea fallida.

Procedimiento

1. En el menú **Gestionar**, pulse **Consola de administración**.
2. En la pestaña **Estado**, pulse **Actividades pasadas**.
3. Junto a la entrada, pulse la flecha y, a continuación, en **Ver detalles del historial de ejecución** .

La página **Ver detalles del historial de ejecución** muestra detalles de ejecución, como la hora de inicio y de finalización, el estado de la ejecución y los mensajes de error de una ejecución fallida. Otra información que aparece en la página depende de si la entrada es para una sola tarea, un trabajo con varios pasos o un agente con tareas. Por ejemplo, si es una sola tarea, aparecen las

opciones del informe y las salidas del informe. Si es un trabajo con varios pasos, aparecerá una sección **Trabajo** con los detalles de ejecución de los pasos del trabajo.

4. En **Estado**, junto a **Error**, pulse **Volver a ejecutar**.

- Si la tarea de repetición de ejecución es una sola tarea, recibirá un mensaje para confirmar la nueva ejecución.
- Si la tarea de repetición de la ejecución es un trabajo con varios pasos de trabajo o un agente con tareas, aparecerá la página **Volver a ejecutar**. Seleccione la casilla de verificación situada junto a las entradas que desee volver a ejecutar.

Consejo: También puede volver a ejecutar entradas erróneas pulsando **Volver a ejecutar** en la sección Pendiente de completarse. Para volver a ejecutar un paso de un trabajo concreto, en la sección Trabajo, en la columna Acciones, pulse el botón Ver detalles del historial de ejecución  del paso fallido.

Capítulo 18. Administración de planificaciones

Puede planificar las entradas de IBM Cognos para que se ejecuten a la hora que usted desee. Por ejemplo, puede que desee ejecutar informes o agentes durante las horas en las que las solicitudes al sistema se reducen. O puede que desee ejecutarlos de forma regular en intervalos semanales o mensuales.

Para utilizar esta funcionalidad, debe tener los permisos necesarios para la función protegida **Planificación en IBM Cognos Administration**.

Para planificar informes para ejecutar con el formato de texto delimitado (CSV), PDF, hoja de cálculo de Microsoft Excel (XLS) o XML, necesita tener la capacidad de generar salidas en el formato específico. Para obtener más información, consulte: “Formatos de informe” en la página 363. Puede actualizar una planificación existente en la que se especifiquen formatos que no puede ejecutar, pero no puede incluir en la planificación formatos que no pueda ejecutar.

En **IBM Cognos Administration**, puede controlar el acceso a la planificación por día, semana, mes, año y activador utilizando la capacidad de planificación adecuada. También puede restringir la planificación intradía utilizando las funciones **Planificación por minuto** y **Planificación por hora** (Capítulo 13, “Funciones y características protegidas”, en la página 227).

Si posee privilegios de administrador también podrá planificar tareas que le permitan:

- Mantener su almacén de contenido (“Tareas de mantenimiento del almacén de contenido” en la página 71)
- Planificar tareas de almacenamiento en caché de Query Service (“Creación y planificación de tareas de administración del servicio de consultas” en la página 179)
- Importar o exportar entradas desde un archivo de despliegue (Capítulo 19, “Despliegue”, en la página 287)
- Ejecutar trabajos (“Utilizar trabajos para planificar varias entradas” en la página 281)
- Ejecutar el mantenimiento de métricas Capítulo 4, “Métricas de rendimiento del sistema”, en la página 29

Puede planificar las entradas para que se ejecuten a intervalos determinados. Puede planificar entradas de forma individual o utilizar trabajos para planificar múltiples entradas de una sola vez. Los trabajos poseen su propia planificación, independientemente de las planificaciones de informes.

Puede planificar entradas para que se ejecuten el último día de cada mes. También puede planificar entradas para que se activen por apariciones, como renovaciones de bases de datos o correos electrónicos.

Puede ejecutar informes para producir salidas basadas en las opciones definidas, como el formato, el idioma y la accesibilidad.

Únicamente se puede asociar una planificación a cada entrada. Si necesita múltiples planificaciones para una entrada de informe o de agente, puede crear vistas de informe o vistas de agente y, a continuación, crear una planificación para cada vista.

Una vez que haya creado una planificación, la entrada o el trabajo se ejecuta en la fecha y la hora especificada. Entonces puede ver las entradas planificadas y administrarlas. Para obtener más información, consulte Capítulo 17, “Gestión de actividades”, en la página 263.

Credenciales para entradas planificadas

Cuando se abre una entrada planificada, las credenciales muestran el propietario de la planificación actual. Si no es ya el propietario de la planificación, puede nombrarse propietario “Ejemplo: Cambio de credenciales para una planificación” en la página 281.

Las credenciales para una planificación no cambian automáticamente al modificar ésta. Debe cambiar explícitamente las credenciales.

Para obtener información sobre las credenciales de origen de datos, consulte “Credenciales de confianza” en la página 222.

Solicitudes en entradas planificadas

Si se planifica una entrada que contiene solicitudes, debe guardar los valores de la solicitud o especificar los valores predeterminados “Cómo especificar los valores de la solicitud predeterminados para un informe” en la página 366 para garantizar que exista un valor cuando el informe se ejecute según la planificación.

En un trabajo puede especificar valores de solicitud para los pasos de trabajos. Si se ejecuta una entrada como parte de un trabajo, se utilizan los valores de solicitud de la definición del trabajo en lugar de los valores guardados con la entrada. Si no se especifican valores en la definición del trabajo, el software de IBM Cognos utilizará los valores guardados en la entrada.

Prioridad de las entradas planificadas

Cuando planifica una entrada, puede seleccionar una prioridad de 1 a 5. Por ejemplo, una entrada con prioridad 1 se ejecuta antes que una entrada con prioridad 5. Si hay más de una entrada con una misma prioridad, se ejecuta primero la que llegó primero a la cola. El valor predeterminado es 3. Si no tiene permisos para las prioridades de las entradas, se mostrará la prioridad, pero no podrá cambiarla.

Cuando se planifica un trabajo, sólo puede definir la prioridad para todo el trabajo, no para entradas individuales dentro de un mismo trabajo. No obstante, puede cambiar la prioridad de entradas individuales cuando están pendientes en la cola.

La prioridad de las entradas que están en la cola no afecta a la entrada que ya se esté ejecutando. La entrada en ejecución finaliza y a continuación se comprueba la prioridad de la cola para determinar la siguiente entrada que debe ejecutarse.

Para obtener más información, consulte “Gestión de la prioridad de ejecución de entradas” en la página 270.

Historiales de ejecución para entradas planificadas

El software de IBM Cognos mantiene la información de historial cada vez que se ejecuta una entrada planificada. Puede utilizar el historial de ejecución para una entrada para ver cuándo se ejecutó y si la ejecución fue correcta. Para obtener más información, consulte “Visualización del historial de ejecución de las entradas” en la página 271.

Planificación de una entrada

Una entrada se planifica para ejecutarla más adelante o para hacerlo en una fecha y hora periódica. Por ejemplo, puede planificar un informe o un agente.

Si ya no necesita una planificación, puede suprimirla. También puede inhabilitarla sin perder ninguno de los detalles de planificación. Podrá habilitar la planificación más adelante. Para obtener más información, consulte Capítulo 17, “Gestión de actividades”, en la página 263.

Puede planificar una entrada para que se ejecute el último día de cada mes o como parte de un trabajo. Puede planificar informes basados en apariciones de activador “Planificación de entradas basada en activadores” en la página 284.

Para utilizar esta funcionalidad, debe tener los permisos necesarios para la función protegida **Planificación** en **IBM Cognos Administration**.

Para planificar una entrada necesita los permisos necesarios para ejecutarla. Por ejemplo, para planificar un informe o una vista de informe debe contar con permisos de lectura, escritura, ejecución y visita. Para planificar una vista de informe hijo, debe contar con permisos de ejecución para el informe padre. También son necesarios los siguientes permisos de acceso para cualquier origen de datos utilizado por el informe:

- dataSource: ejecución y visita
- dataSourceConnection: ejecución y visita

Si únicamente posee el acceso de ejecución, se le solicitará que inicie una sesión en la base de datos.

- dataSourceSignon: ejecución

Para planificar informes que se ejecuten con los formatos de salida CSV, PDF o XML, necesita tener la capacidad de generar salidas en el formato específico. Para obtener más información, consulte: “Formatos de informe” en la página 363.

Para establecer la prioridad de una entrada, debe disponer de los permisos necesarios para la característica protegida **Prioridad de planificación**. Para obtener más información, consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Si lo desea, puede cambiar el propietario de la planificación actual cambiando las credenciales para una entrada planificada. Para obtener más información, consulte “Ejemplo: Cambio de credenciales para una planificación” en la página 281.

Procedimiento

1. Pulse el botón Planificación  para la entrada que desee planificar.
2. Establezca la prioridad de la entrada planificada.

Seleccione un número menor para aumentar la prioridad. El valor predeterminado es 3.

3. En **Frecuencia**, seleccione la frecuencia con la que desea que se ejecute la planificación.

La sección **Frecuencia** es dinámica y cambia en función de la selección. Antes de seleccionar la frecuencia, espere hasta que la página se actualice.

Si especifica la planificación intradía en la sección **Frecuencia**, también puede seleccionar una frecuencia diaria para las entradas planificadas. Para ello, continúe con el paso 4.

Si no especifica la planificación intradía, siga en el paso 5.

4. En **Frecuencia diaria**, especifique la frecuencia con la que un informe se ejecuta durante el día a partir de la hora de inicio seleccionada en el paso 5. Puede optar por planificar una entrada por minuto o por hora.

Cuando se especifica una frecuencia diaria, también existe la opción de seleccionar un periodo de tiempo durante el cual desee ejecutar la entrada, por ejemplo, entre las 9:00 AM y las 5:00 PM. De este modo, puede restringir la ejecución de las entradas a los periodos del día en los que se requieren actualizaciones.

Consejo: Cuando especifique una frecuencia por horas y un período de tiempo, si selecciona una frecuencia por horas que divida de forma equitativa el reloj de 24 horas, la entrada planificada se ejecutará todos los días a la misma hora. Si selecciona una frecuencia que no divida de forma equitativa el reloj de 24 horas, la entrada planificada se ejecutará a horas diferentes los siguientes días.

Tabla 69. Ejemplo de horas de ejecución para el día 1 y el día 2 para entradas programadas por horas dentro de un período de tiempo

Frecuencia diaria	Período de tiempo especificado	Hora a la que se ejecuta la entrada el día 1	Hora a la que se ejecuta la entrada el día 2
Cada 3 horas	9:00 a 18:00	9:00	9:00
		12:00	12:00
		15:00	15:00
		18:00	18:00
Cada 5 horas	9:00 a 18:00	9:00	10:00
		14:00	15:00

5. En **Inicio**, seleccione la fecha en la que desea que se inicie la planificación.
6. En **Fin**, seleccione cuándo desea que finalice la planificación.
Si desea crear una planificación pero no quiere aplicarla en ese momento, seleccione la casilla de verificación **Inhabilitar la planificación**. Para habilitar la planificación más adelante, elimine la selección de la casilla de verificación.
7. Si dispone de opciones adicionales en la página **Planificación**, especifique la que desee.
Por ejemplo, para los informes, puede seleccionar formatos, idiomas, métodos de entrega (incluido cómo se deben guardar los archivos de salida de informe) y valores de solicitud.
8. Pulse **Aceptar**.

Resultados

Se crea una planificación y el informe se ejecuta en la siguiente hora planificada.

Ejemplo: Cambio de credenciales para una planificación

Desea cambiar las credenciales de una planificación para que se le identifique como propietario de la planificación actual.

Procedimiento

1. Pulse el botón Planificación  correspondiente a la entrada cuyas credenciales desee cambiar.

En **Credenciales**, aparecerá el nombre del propietario de la planificación actual.

2. Pulse el enlace **Utilizar mis credenciales** para convertirse en el propietario de la planificación. Guarde los cambios.

La próxima vez que abra la planificación, sus credenciales le identificarán como el propietario de ésta; por ejemplo, Sam Carter (scarter).

Nota: Si ha iniciado la sesión como usuario anónimo, la información acerca del propietario de la planificación actual no está disponible.

Utilizar trabajos para planificar varias entradas

Creando un trabajo puede establecer la misma planificación para múltiples entradas. Un trabajo identifica un conjunto de informes, vistas de informe y otros trabajos que se planifican juntos y comparten los mismos valores de planificación. Al ejecutar un trabajo planificado, se ejecutan todas las entradas del trabajo.

Si no está disponible un elemento de trabajo, puede seleccionar un enlace diferente pulsando **Enlace a una entrada**.

Los trabajos contienen pasos, que son referencias a informes individuales, trabajos y vistas de informe. Puede especificar si desea ejecutar los pasos a la vez o de forma secuencial.

- Si los pasos se ejecutan a la vez, todos los pasos se envían al mismo tiempo. Si el trabajo es correcto, todos los pasos se ejecutarán correctamente. Si un paso falla, el resto de pasos del trabajo no se verá afectado y seguirá ejecutándose pero el trabajo tendrá el estado **Error**.
- Si los pasos se ejecutan de forma secuencial, puede especificar el orden en el que desea ejecutarlos. Un paso sólo se envía una vez que el paso anterior se haya ejecutado correctamente. Si un paso falla, puede seleccionar si desea detener el trabajo o si desea continuar con el resto de los pasos.

Puede planificar un trabajo para ejecutarlo a una hora determinada, de forma periódica o en función de un activador, como la renovación de una base de datos o un correo electrónico. Para obtener más información, consulte “Planificación de entradas basada en activadores” en la página 284.

Los informes individuales, trabajos y vistas de informe de los pasos también poseen planificaciones individuales. Las opciones de ejecución de las entradas de pasos individuales sobrescriben las opciones de ejecución establecidas para el trabajo. Puede establecer opciones de ejecución para el trabajo que sirvan como predeterminadas para las entradas de pasos que no poseen sus propias opciones de ejecución.

Puede ejecutar informes para producir salidas basadas en las opciones definidas, como el formato, el idioma y la accesibilidad.

También puede incluir importaciones y exportaciones de despliegue y mantenimiento de almacén de contenido en un trabajo. Para obtener más información, consulte: “Tareas de mantenimiento del almacén de contenido” en la página 71 y Capítulo 19, “Despliegue”, en la página 287.

Los permisos necesarios para incluir una entrada como parte de un trabajo varían en función del tipo de entrada. Los permisos son los mismos que para planificar una entrada. Para obtener más información, consulte “Planificación de una entrada” en la página 279.

Procedimiento

1. En el portal de IBM Cognos Analytics, seleccione  **Nuevo** y, a continuación, seleccione  **Trabajo**.
2. Escriba un nombre y, si lo desea, una descripción y una sugerencia de pantalla. A continuación, seleccione la ubicación en la que desee guardar el trabajo y pulse **Siguiente**.
Aparecerá la página **Seleccionar los pasos**.
3. Pulse **Añadir**.
4. Seleccione las casillas de verificación de las entradas que desea añadir y pulse el botón de flecha . Cuando las entradas que desee aparezcan en el cuadro **Entradas seleccionadas**, pulse **Aceptar**.
También puede pulsar **Buscar** y, en el cuadro **Cadena de búsqueda**, introducir la frase que desee buscar. Para las opciones de búsqueda, pulse **Editar**. Cuando haya encontrado la entrada, pulse el botón de flecha derecha para incluirla en el cuadro **Entradas seleccionadas** y pulse **Aceptar**.
Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista. Para hacer visibles las entradas del usuario, pulse **Mostrar usuarios en la lista**.
5. Si desea modificar las opciones de ejecución de una entrada individual cuando se ejecute como parte del trabajo, pulse el icono Establecer , pulse **Generar salidas de informes**, seleccione la casilla **Reemplazar valores predeterminados**, realice los cambios y pulse **Aceptar**.
Para enviar el informe a destinatarios móviles, seleccione **Enviar el informe a destinatarios móviles** y pulse **Seleccionar destinatarios**.

Consejo: Para regresar a las opciones predeterminadas de las entradas individuales, pulse el botón para suprimir.
6. Si desea renovar la memoria caché para un informe cuando se ejecute el trabajo, pulse el icono de edición junto al informe y, a continuación, en el menú **Ejecutar el informe en**, pulse **Renovar el informe en memoria caché**. Pulse **Reemplazar valores predeterminados**. Para aceptar el idioma que se mostrará, pulse **Aceptar**. Para cambiar el idioma, pulse **Seleccionar los idiomas**, seleccione los idiomas que desee y pulse **Aceptar**. Pulse **Aceptar** para aceptar los idiomas que se mostrarán.

Consejo: Para borrar la memoria caché, pulse el botón de supresión.

7. Si desea crear o renovar la memoria caché, pulse el icono Establecer, pulse **Renovar el informe en memoria caché**, seleccione la casilla **Reemplazar valores predeterminados**, añada otros idiomas si lo desea y pulse **Aceptar**.

Consejo: Para borrar la memoria caché, pulse **Más** junto al informe cuya memoria caché desee borrar, pulse **Borrar memoria caché** y pulse **Aceptar** dos veces.

8. En **Envío de pasos**, seleccione si desea enviar los pasos **Todos a la vez** o **Secuencialmente**.

Si selecciona **Secuencialmente**, los pasos se ejecutarán en el orden en que aparezcan en la lista **Pasos**. Si desea que el trabajo continúe ejecutándose aunque uno de los pasos contenga errores, seleccione la casilla de verificación **Continuar en error**.

Consejo: Para modificar el orden, pulse **Modificar la secuencia**, realice los cambios y pulse **Aceptar**.

9. Si desea especificar las opciones de ejecución predeterminadas en el nivel de trabajo, en **Valores predeterminados para todos los pasos**, pulse **Establecer**.

Tenga en cuenta que es posible que las opciones de ejecución que están disponibles para un trabajo con varias entradas no se apliquen a todas las entradas. Si la opción no se aplica a una entrada, se ignora.

10. Si desea reemplazar las opciones predeterminadas, seleccione la categoría y la casilla de verificación **Reemplazar valores predeterminados**, seleccione las opciones predeterminadas que desee para el trabajo y pulse **Aceptar**.

11. Para guardar todos los detalles del historial de los pasos del trabajo una vez que la actividad de ejecución finalice correctamente, pulse la opción **Todos** de la lista de niveles de detalles del historial de ejecución. Pulse **Limitados** para guardar sólo determinados detalles del historial de ejecución del trabajo. Si la ejecución del trabajo falla, se guardan todos los detalles del historial.

El valor predeterminado es **Todos**.

12. Seleccione la acción que desee:

- Para ejecutarlo ahora o más adelante, pulse **Ejecutar ahora o más adelante** y en **Finalizar**. Especifique la hora y la fecha de la ejecución. Pulse **Buscar** o **Buscar y corregir** y, a continuación, pulse **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
- Para planificarlo de forma periódica, pulse **Planificar ejecución periódicamente** y pulse **Finalizar**. A continuación, seleccione la frecuencia y las fechas de comienzo y de final. Pulse **Buscar** o **Buscar y corregir** y, a continuación, pulse **Aceptar**.

Consejo: Para inhabilitar temporalmente la planificación, seleccione la casilla de verificación **Inhabilitar la planificación**. Para obtener más información, consulte: Capítulo 17, “Gestión de actividades”, en la página 263..

- Para guardar sin planificar o ejecutar, pulse **Sólo guardar** y en **Finalizar**.

Resultados

Se crea un trabajo y se ejecutará en la siguiente hora planificada.

Datos de la solicitud en memoria caché

Para los informes que soliciten valores cada vez que se ejecuta el informe, puede que desee utilizar datos de la solicitud en memoria caché. Los informes se ejecutan más rápido porque los datos se recuperan de la memoria caché en lugar de hacerlo de la base de datos.

La memoria caché sólo se utiliza cuando un idioma solicitado es el mismo que uno de la memoria caché. Por ejemplo, la memoria caché contiene datos para inglés, inglés (Estados Unidos) y alemán (Alemania). Cuando se lo solicite, indicará inglés (Estados Unidos) para el informe. Hay una coincidencia exacta y se utilizan los datos de la memoria caché. Los datos de la memoria caché también se utilizan si hay una coincidencia parcial. Si solicita inglés (Canadá), se utilizan los datos de la memoria caché para inglés. Si solicita alemán (Austria), no hay ninguna coincidencia y no se utilizan los datos de la memoria caché.

Puede utilizar memorias caché para informes o para vistas de informe. Para vistas de informe, se utiliza en primer lugar la memoria caché de la vista de informe. Si no se encuentra ninguna memoria caché de la vista de informe, se utiliza la memoria caché del informe asociado.

Debe utilizar un trabajo para crear o renovar una memoria caché. Puede renovar la memoria caché automáticamente planificando el trabajo para que se ejecute periódicamente. Si desea utilizar datos activos la próxima vez que ejecute el informe, puede borrar la memoria caché.

Planificación de entradas basada en activadores

Puede planificar entradas en función de una aparición, como la renovación de una base de datos o un correo electrónico. La aparición actúa como un activador y provoca la ejecución de la entrada. Por ejemplo, puede que desee ejecutar un informe siempre que se renueva una base de datos.

La planificación basada en activadores se puede utilizar para ejecutar, de forma automática, entradas basadas en una aparición. También se puede utilizar para limitar el momento en que los usuarios pueden ejecutar entradas. Por ejemplo, en un entorno de almacén en el que la base de datos sólo se renueva una vez a la semana, no es necesario ejecutar informes con mayor frecuencia.

Puede decidir planificar el informe basándose en la renovación de la base de datos; de este modo los informes sólo se ejecutarán una vez a la semana.

La planificación basada en activadores sólo se aplica a la entrada, pero no a cualquier entrada asociada a ella. Por ejemplo, si a un informe se le aplica una planificación basada en activadores, ésta no se aplica a las vistas de informe asociadas a él. Sin embargo, puede planificar una vista de informe utilizando un activador.

En **IBM Cognos Administration**, puede controlar el acceso a la planificación por activador utilizando la función **Planificación por activador**.

Configuración de planificación basada en activadores

Para planificar una entrada basada en una aparición y confirmar la planificación basada en activadores debe contar con permisos de lectura, escritura y de visita.

Para planificar informes para ejecutar con el formato de texto delimitado (CSV), PDF, hoja de cálculo de Microsoft Excel (XLS) o XML, necesita tener la capacidad de generar salidas en el formato específico. Para obtener más información, consulte: “Formatos de informe” en la página 363.

También son necesarios los siguientes permisos de acceso para todos los orígenes de datos utilizados por la entrada:

Tabla 70. Orígenes de datos y permisos necesarios para la planificación basada en activadores

Origen de datos	Permisos
dataSource	Ejecución y visita
dataSourceConnection	Ejecución y visita Si únicamente posee el acceso de ejecución, se le solicitará que inicie una sesión en la base de datos.
dataSourceSignon	Ejecución

Antes de configurar la planificación basada en activadores, asegúrese de que sus credenciales existen y están actualizadas.

Sugerencia: Pulse el botón Opciones de Mi área , **Mis preferencias** y, en la pestaña **Personal**, pulse **Renovar credenciales**.

Lleve a cabo este proceso para configurar la planificación basada en activadores:

- Planifique una entrada basada en la aparición “Planificación de una entrada basada en una aparición”.
- Pida a su administrador que configure la aparición de activador en un servidor.

Las apariciones de activador también las puede configurar un desarrollador de Software Development Kit mediante el uso de IBM Cognos Software Development Kit. Para obtener más información, consulte *Software Development Kit Developer Guide*.

Planificación de una entrada basada en una aparición

Como parte de la configuración de la planificación basada en activadores, debe planificar una entrada basada en una aparición.

La planificación basada en activadores estará activada si el usuario que ha disparado el activador tiene:

- Permisos de lectura y visita para la entrada de planificación
- Permisos de visita para todos los ancestros de la entrada de planificación
- Acceso a IBM Cognos Administration

Para planificar informes para ejecutar con el formato de texto delimitado (CSV), PDF, hoja de cálculo de Microsoft Excel (XLS) o XML, necesita tener la capacidad de generar salidas en el formato específico. Para obtener más información, consulte: “Formatos de informe” en la página 363.

Procedimiento

1. Pulse el botón Planificación  junto a la entrada que desea planificar.
2. En Frecuencia, pulse la pestaña **Por activador**.
3. En **Nombre del activador**, escriba el nombre de la aparición de activación.
Nota: El nombre del activador que vaya a introducir se lo puede proporcionar el administrador o el programador. Si no es así, debe comunicar a su administrador o programador el nombre de activador que utilice.
4. La fecha de inicio predeterminada es "ahora" y la fecha de finalización predeterminada es "por siempre", lo que quiere decir que la planificación por activador se ejecutará cuando se dispare el activador (ya sea desde trigger.bat o desde una aplicación de Software Development Kit). Si especifica una fecha de inicio y finalización válidas, la planificación por activador únicamente se podrá disparar entre dichas fechas.
5. Pulse **Aceptar**.

Capítulo 19. Despliegue

El despliegue supone mover aplicaciones de una instalación a otra. Puede desplegar el contenido de IBM Cognos desde un entorno de origen a un entorno de destino.

Puede desplegar todo el almacén de contenido o solo contenido específico, como paquetes, carpetas, espacios de nombres, cuentas de usuario o visualizaciones.

Normalmente, el despliegue transfiere entradas de un entorno de desarrollo a un entorno de prueba y luego a un entorno de producción. También puede desplegar entre sistemas operativos.

Es importante planificar el despliegue para asegurarse de que despliega la información correcta y de que no interrumpe el entorno de destino. También es importante tener en cuenta la seguridad en los entornos de origen y de destino.

Puede actualizar las entradas de versiones anteriores si ejecuta el asistente para importación de despliegue. Para obtener más información, “Importación en un entorno de destino” en la página 308.

Puede utilizar un sistema operativo o un mecanismo de programación para realizar el despliegue desde una línea de comandos. Puede utilizar el IBM Cognos Software Development Kit para automatizar el proceso de despliegue con el fin de realizar las acciones siguientes:

- Crear, actualizar y suprimir una especificación de despliegue
- Crear una especificación de despliegue desde un archivo de despliegue
- Enviar solicitudes de exportación e importación del despliegue
- Acceder al historial de despliegue

Para obtener más información, consulte IBM Cognos Software Development Kit *Developer Guide*.

Para obtener información sobre el despliegue de contenido en un entorno de varios inquilinos IBM Cognos Analytics, consulte “Despliegue de contenido de arrendatario” en la página 346.

El despliegue del servicio de tareas humanas es una tarea independiente. Para obtener más información, consulte “Despliegue de Human Task and Annotation Services” en la página 314.

El despliegue de contenido de IBM Cognos Analytics de un entorno a otro es un proceso complejo que requiere un enfoque global. El documento de prácticas recomendables IBM Cognos Analytics – Deploy Content Between Environments (http://www.ibm.com/developerworks/data/library/cognos/infrastructure/cognos_specific/page581.html) proporciona directrices y ejemplos de gran utilidad para ayudarle a realizar un despliegue satisfactorio.

Especificaciones de despliegue

Una especificación de despliegue es una entrada en el almacén de contenido que define las entradas que se deben desplegar, las preferencias de despliegue y el nombre del archivo de despliegue.

Hay dos tipos de especificaciones de despliegue. Las especificaciones de exportación se crean en el entorno de origen y controlan la creación de los archivos de despliegue. Las especificaciones de importación se crean en el entorno de destino y controlan las entradas de importación del archivo de despliegue.

Puede ver el historial de despliegue de cada especificación de despliegue para ver la fecha, la hora y los detalles de la importación o la exportación.

Archivos de despliegue

Un archivo de despliegue es un archivo comprimido que contiene entradas reales y que se crea al exportar del entorno de origen.

Mueva el archivo de despliegue del entorno de origen al entorno de destino. A continuación, importe desde el archivo de despliegue al entorno de destino.

Para mover un archivo de despliegue, necesita tener acceso a los directorios de instalación del sistema en el que esté instalado el software de IBM Cognos. Esta ubicación se establece en la herramienta de configuración. La ubicación predeterminada es *install_location/deployment*. Para obtener información acerca del cambio de ubicación, consulte IBM Cognos *Guía de instalación y configuración*.

Al exportar a un archivo de despliegue existente, el contenido del archivo se sobrescribe.

Planificación de despliegue

Al realizar un despliegue, debe considerar cómo gestionar la seguridad y el método de despliegue que va a seleccionar.

Para no interrumpir las referencias del entorno de destino, debe desplegar todas las entradas que hagan referencia a las entradas en otro paquete u otra carpeta. Entre las entradas que se deben tener en cuenta, se incluyen las siguientes:

- vistas de informes y trabajos
- Pertenencias y permisos de entrada

Seguridad y despliegue

Antes de realizar el despliegue, debe tener en cuenta los permisos de acceso, la seguridad de los archivos de despliegue y las referencias a los espacios de nombres que no sean **Cognos**.

Permisos de acceso

Las entradas que despliegue pueden tener seguridad asociada, como los permisos de acceso Capítulo 12, “Permisos de acceso y credenciales”, en la página 213 que especifican los usuarios y los grupos que pueden tener acceso. Si despliega todo el almacén de contenido “Despliegue de todo el almacén de contenido” en la página 291, se desplegarán todos los permisos de acceso. Si despliega los paquetes, las carpetas públicas y el contenido de directorio seleccionados, podrá elegir si desea

desplegar los permisos de acceso “Despliegue del contenido de directorio y de las carpetas públicas seleccionadas” en la página 293.

Tenga en cuenta lo siguiente:

- Usuarios y grupos a los que se hace referencia
Si despliega permisos de acceso en un entorno de destino, deben existir usuarios y grupos a los que se hace referencia en el entorno de destino.
- Reglas de permisos de acceso
Para que los permisos de acceso funcionen después de que se desplieguen las entradas, el entorno de origen y el de destino deberán utilizar el mismo proveedor de autenticación con la misma configuración. De lo contrario, es posible que los permisos no funcionen después del despliegue.
Utilice el espacio de nombres de Cognos para asegurarse de que los permisos del entorno de origen funcionen en el entorno de destino. Por ejemplo, en el entorno de origen cree grupos de Cognos con el grupo Todos como miembro y, a continuación, establezca los permisos de acceso para los grupos. Después del despliegue, en el entorno de destino, correlacione grupos de Cognos con los usuarios y grupos apropiados del proveedor de autenticación y, a continuación, elimine Todos de la pertenencia al grupo.

Para obtener más información sobre cómo desplegar grupos y roles de Cognos, consulte “Cómo incluir grupos y roles de Cognos” en la página 295.

Protección de los archivos de despliegue

Un archivo de despliegue “Archivos de despliegue” en la página 288 puede contener información confidencial, como inicios de sesión y cuentas confidenciales o números de tarjetas de crédito en salidas de informes. Al exportar, puede cifrar el archivo de despliegue con una contraseña. Más adelante, al importar, deberá escribir la contraseña de cifrado. La contraseña debe contener ocho caracteres como mínimo.

Debe cifrar el archivo de despliegue cuando contenga inicios de sesión de origen de datos “Inicios de sesión de orígenes de datos” en la página 156 o cuando despliegue todo el almacén de contenido “Despliegue de todo el almacén de contenido” en la página 291.

Los valores de cifrado se configuran en la herramienta de configuración. Para obtener más información, consulte IBM Cognos *Guía de instalación y configuración*.

Cómo incluir referencias a otros espacios de nombres

Algunas entradas, como grupos, roles, listas de distribución, contactos, inicios de sesión de origen de datos y algunas propiedades de informe, como los destinatarios de correo electrónico y los contactos del informe, pueden hacer referencia a entidades en espacios de nombres distintos del espacio de nombres de **Cognos**. Cuando despliegue carpetas públicas y contenido de directorio, puede desplegar estas entradas con referencias o sin ellas a estos espacios de nombres.

Tenga en cuenta lo siguiente:

- Referencias incluidas
Si incluye las referencias en otros espacios de nombres, el sistema verificará que cada una de las entidades de referencia exista en los espacios de nombres aplicables. Por lo tanto, debe asegurarse de que ha iniciado sesión en cada

espacio de nombres y de que posee los permisos necesarios para acceder a las entidades requeridas en los espacios de nombres. Si no puede acceder a los espacios de nombres, encontrará errores durante el despliegue.

- Referencias no incluidas

Si no incluye las referencias en otros espacios de nombres, las entidades de referencia se eliminarán de la lista de pertenencia de grupos, roles, listas de distribución e inicios de sesión de origen de datos y de otras propiedades donde puedan existir.

Al desplegar todo el almacén de contenido “Despliegue de todo el almacén de contenido” en la página 291, las referencias se incluyen en todos los espacios de nombres.

Mantener nombres de objetos localizados al importar archivos más antiguos

Las nuevas versiones del software de IBM Cognos software introducen compatibilidad con nuevos entornos locales. Importar archivos antiguos a las versiones nuevas puede ocasionar que falten traducciones de nombres de objetos en algunos entornos locales. Para evitar este problema, establezca la propiedad avanzada **CM.UpdateInitialContentNamesAfterImport** antes de la importación.

Acerca de esta tarea

Por ejemplo, se han añadido los idiomas catalán, croata, danés, griego, kazakstán, noruego, eslovaco, eslovenio y tailandés a IBM Cognos Business Intelligence versiones 10.1.1 y 10.2. Los archivos creados con versiones anteriores no admiten estos entornos locales. Al planificar la importación de estos tipos de archivos, configure la propiedad **CM.UpdateInitialContentNamesAfterImport** antes de iniciar la importación. Esto garantizará que los nombres de objetos, como **Carpetas públicas** o **Mis carpetas**, en estos idiomas adicionales se traduzcan y muestren correctamente.

Si observa que los nombres de objetos no se muestran en el idioma especificado después de importar un archivo más antiguo, consulte la *IBM Cognos Analytics Guía de resolución de problemas*.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para **ContentManagerService**, escriba el nombre de parámetro **CM.UpdateInitialContentNamesAfterImport**.
3. En la columna **Valor**, escriba los idiomas afectados y separe cada uno con una coma.

Por ejemplo, para los idiomas de contenido eslovaco y croata, escriba la siguiente cadena de texto:

sl,hr

Resultados

Eliminar este valor avanzado cuando ya no necesita el soporte para el archivo antiguo debido a que hay un impacto de rendimiento asociado con tener este valor habilitado.

Despliegue de todo el almacén de contenido

El despliegue de todo el almacén de contenido garantiza que todos los paquetes, carpetas y contenido de directorio se copian en la nueva ubicación.

Por ejemplo, si cambia el sistema en el que está instalado el software de IBM Cognos, puede mover todo el almacén de contenido del antiguo entorno al nuevo, y mantener todos los informes y otras entradas creadas por los administradores y los usuarios.

Otras razones para desplegar todo el almacén de contenido son las siguientes:

- Mover una aplicación completa a un entorno vacío y nuevo, como un sistema nuevo, desde un entorno de desarrollo.
- Renovar una aplicación completa en un entorno existente, como un sistema existente, desde un entorno de desarrollo.
- Mover una aplicación desde un entorno existente que utilice una tecnología subyacente diferente, como un tipo de base de datos diferente para el almacén de contenido o un sistema operativo diferente.
- Actualizar el contenido del almacén de contenido.

Al mover un almacén de contenido de un entorno a otro, debe utilizar los mismos espacios de nombres para que las políticas, los usuarios, los roles y los grupos funcionen correctamente.

Cuando despliegue todo el almacén de contenido, si no hay conflictos, se eliminará el contenido del almacén de contenido de destino y se sustituirá por el contenido del almacén de contenido de origen, excepto los datos de configuración. Las entradas importadas conservan los propietarios del almacén de contenido de origen. Para obtener más información sobre la resolución de conflictos, consulte “Reglas de resolución de conflictos” en la página 299.

Una vez finalizada el despliegue, es posible que algunos enlaces de los paquetes asociados con los informes no funcionen. Puede que sea necesario volver a enlazar los paquetes a los informes. Para obtener más información sobre cómo enlazar paquetes a los informes, consulte la documentación de los estudios.

Sugerencia: En lugar de desplegar todo el almacén de contenido, puede desplegar sólo las carpetas públicas específicas y el contenido de directorio “Despliegue del contenido de directorio y de las carpetas públicas seleccionadas” en la página 293.

Almacén de contenido

El almacén de contenido incluye todas las entradas en el portal, como:

- Carpetas públicas
- Paquetes
- informes
- orígenes de datos
- Listas de distribución y contactos
- Impresoras
- Espacio de nombres de Cognos
- Especificaciones de despliegue

No incluye el historial de despliegue “Historial de despliegue”. Los objetos de configuración “Información de configuración” como asignadores, se incluyen en las exportaciones de forma predeterminada, pero se excluyen en las importaciones.

Si desea desplegar las páginas y las carpetas personales de los usuarios, deberá incluir la información de cuenta de usuario al exportar e importar.

Historial de despliegue

Cuando exporte un almacén de contenido completo, se exportarán las especificaciones de despliegue de exportación e importación que existan en el almacén de contenido de origen. Los historiales de despliegue no se exportan.

Más adelante, cuando importe todo el almacén de contenido, también importará las especificaciones de despliegue de exportación e importación. Las entradas de las especificaciones importadas no aparecen en la página **Ver historial de despliegue** para las especificaciones importadas.

Si se utilizan algunas de las especificaciones de despliegue importadas para un archivo de despliegue cifrado, puede suprimirlas. Para importar por primera vez un almacén de contenido completo, debe crear una especificación de despliegue de importación nueva.

De forma predeterminada, la información guardada en los registros de despliegue incluye sólo los informes de progreso y de resumen. Si desea incluir información detallada, cambie el nivel de grabación con el valor avanzado CM.DEPLOYMENTDETAILENTIRECONTENT. Utilice los pasos de “Establecimiento de parámetros avanzados de Content Manager” en la página 66. Hay más niveles de grabación disponibles en el despliegue parcial “Grabación de detalles de despliegue” en la página 296.

Información de configuración

Al importar todo un almacén de contenido, los datos de configuración se incluyen en la exportación, pero quedan excluidos de la importación de forma predeterminada. Es recomendable que no cambie este valor. Sin embargo, si debe importar los valores de configuración, puede cambiar el valor predeterminado en Valores avanzados “Inclusión de los objetos de configuración en la importación de todo el almacén de contenido” en la página 311.

Si importa los datos de configuración, especialmente en un entorno distribuido con varios Content Managers, los datos importados pueden sobrescribir la información actual sobre el estado de Content Manager.

Sugerencia: Si importa la configuración, reinicie el servicio en el entorno de destino para actualizar la información de estado correctamente.

Para obtener más información acerca de cómo incluir datos de configuración en la importación, consulte “Inclusión de los objetos de configuración en la importación de todo el almacén de contenido” en la página 311.

Para obtener más información acerca del modo de importar objetos específicos del almacén de contenido, consulte “Reglas para la resolución de conflictos en el despliegue de todo el almacén de contenido” en la página 300.

Despliegue del contenido de directorio y de las carpetas públicas seleccionadas

Puede realizar un despliegue parcial, sólo del contenido de directorio y de las carpetas públicas seleccionadas, en lugar de todo el almacén de contenido.

Puede desplegar paquetes y carpetas en Carpetas públicas. Examine la jerarquía de carpetas públicas y seleccione un paquete o una carpeta. Esto desplegará todo el contenido. No se pueden seleccionar entradas concretas en los paquetes ni en las carpetas. Durante la exportación, los paquetes y las carpetas padre no se exportan y Content Manager no crea ubicaciones de marcadores de posición en el entorno de destino. Tanto durante la exportación como durante la importación, puede especificar una nueva ubicación de destino en la jerarquía de Content Manager para cada paquete y carpeta desplegados.

El contenido de directorio que se puede desplegar incluye el espacio de nombres de Cognos, las listas de distribución y los contactos, así como los orígenes de datos y sus conexiones, y los inicios de sesión.

Al desplegar carpetas públicas y contenido de directorio, no puede incluir objetos de las áreas de configuración, función, exportDeploymentFolder e importDeploymentFolder del almacén de contenido “Opciones de despliegue parcial” en la página 294. Para obtener más información, consulte “Cómo incluir referencias a otros espacios de nombres” en la página 289.

Para obtener más información acerca del modo de importar objetos específicos del almacén de contenido, consulte “Reglas para la resolución de conflictos de despliegue al importar y exportar” en la página 298.

Una vez que haya finalizado el despliegue, es posible que algunos enlaces para los paquetes asociados con los informes no funcionen, incluso si se han incluido los paquetes y sus informes en el despliegue. Puede que sea necesario volver a enlazar los paquetes a los informes. Para obtener más información sobre cómo enlazar paquetes a los informes, consulte la documentación de los estudios.

Sugerencia: Si desea desplegar entradas específicas, puede crear una carpeta en el nivel raíz de Carpetas públicas, copiar las entradas específicas en esa carpeta y seleccionarla cuando realice el despliegue.

Despliegue de paquetes

Durante un despliegue parcial, puede desplegar uno o varios paquetes a la vez.

Un paquete puede hacer referencia a objetos que se encuentran fuera del paquete, tales como objetos de seguridad, orígenes de datos y listas de distribución. Sin embargo, los objetos con referencias no se despliegan con el paquete.

Mientras esté realizando la importación, puede anular la selección de paquetes del archivo de despliegue que no desee importar.

Cambio de nombre de los paquetes y las carpetas

Durante un despliegue parcial, puede cambiar el nombre de los paquetes y de las carpetas para que tengan un nuevo nombre en el entorno de destino.

Esto es útil si no desea sobrescribir un paquete o una carpeta que tenga el mismo nombre en el entorno de destino. El paquete o la carpeta original permanece intacto, y se cambia el nombre del desplegado.

También es posible que desee añadir nombres multilingües para paquetes y carpetas, de manera que los usuarios puedan ver nombres adecuados para su entorno local. Un entorno local especifica la información lingüística y las convenciones culturales para el tipo de carácter, ordenación, formato de fecha y hora, unidad de moneda y mensajes.

Inhabilitación de los paquetes y las carpetas

Durante un despliegue parcial, puede inhabilitar los paquetes y las carpetas en el entorno de destino para que los usuarios no puedan acceder a ellos.

La inhabilitación de paquetes y carpetas es útil si desea probarlos en el entorno de destino antes de que estén disponibles para los usuarios.

Puede inhabilitar los paquetes y las carpetas en el momento de la exportación o la importación.

Al inhabilitar un paquete o una carpeta, las entradas que contiene no están accesibles en el entorno de destino después de la importación. Los usuarios no pueden ejecutar, ver ni editar las entradas. Sólo los usuarios que tienen privilegios de escritura en las entradas inhabilitadas pueden acceder a ellas.

Opciones de despliegue parcial

Durante un despliegue parcial, al exportar o importar, puede elegir las siguientes opciones.

Si no selecciona ninguna opción al exportar, no estará disponible durante la importación.

Cómo incluir versiones de salida de informe

Si lo desea, puede incluir las versiones de salida de informe en el despliegue. Si selecciona esta opción, puede decidir la acción que se debe realizar si se produce un conflicto. Puede reemplazar las versiones de salida de informe existentes en el entorno de destino por las del archivo de despliegue o conservar las versiones del entorno de destino.

Cómo incluir el historial de ejecución

El historial de ejecución de un informe muestra las estadísticas sobre el estado y la hora en que se ejecutó el informe “Visualización del historial de ejecución de las entradas” en la página 271 en el despliegue. Puede elegir si desea incluir el historial de ejecución de los informes.

Si selecciona esta opción, puede decidir la acción que se debe realizar si se produce un conflicto. Puede reemplazar los historiales de ejecución de un informe existentes en el entorno de destino por los del archivo de despliegue o conservar los historiales del entorno de destino.

Cómo incluir planificaciones

Puede elegir si desea incluir planificaciones Capítulo 18, “Administración de planificaciones”, en la página 277 en el despliegue. Si no despliega las planificaciones, se eliminarán de los trabajos y los informes del entorno de destino.

Si selecciona esta opción, puede decidir la acción que se debe realizar si se produce un conflicto. Puede reemplazar las planificaciones existentes en el entorno de destino por las del archivo de despliegue o conservar las planificaciones del entorno de destino.

Cuando elige importar planificaciones en el despliegue, puede cambiar las credenciales de planificación importadas por sus credenciales. La credencial de una planificación es la credencial que se utiliza para ejecutar el informe en la planificación. Esta credencial determina los permisos en el informe, así como las funciones que se aplican en la ejecución de informe. Si el informe no tiene la propiedad **Ejecutar como el propietario** establecida como true, la credencial también se utilizará para acceder al origen de datos, a la conexión de datos y a los objetos de inicio de sesión. El cambio de credencial puede afectar a la operación de las siguientes formas:

- Sin impacto
- El informe produce diferentes datos como resultado de la selección de una conexión o inicio de sesión diferente en el origen de datos.
- El informe no se puede ejecutar porque el usuario no tiene las funciones o los permisos necesarios.

Para cambiar las credenciales de planificación importadas a las credenciales de la persona que realiza la importación, haga lo siguiente:

- Añada la configuración avanzada CM.DeploymentUpdateScheduleCredential y establezca el valor en **True**. Consulte el procedimiento, “Establecimiento de parámetros avanzados de Content Manager” en la página 66.
- Cuando realice la importación en el entorno de destino con el Asistente para nueva importación “Importación en un entorno de destino” en la página 308, asegúrese de pulsar **Incluir planificaciones** y seleccione **Sustituir entradas existentes** en **Resolución de conflictos**. A continuación, en **Propiedad de entrada**, seleccione **El usuario que realiza la importación**.

Cómo incluir grupos y roles de Cognos

Puede elegir si desea incluir grupos y roles de Cognos Capítulo 11, “Usuarios, grupos y roles”, en la página 207 en el despliegue.

Al desplegar los grupos y los roles de Cognos, debe desplegarlos todos. Sin embargo, los siguientes grupos incorporados no se despliegan:

- Anónimo
- Todos los usuarios autenticados
- Todos

Al desplegar grupos, los miembros del grupo Administradores del sistema se fusionan con los miembros de este grupo que ya está en el entorno de destino. De este modo se garantiza que el entorno de destino esté accesible en caso de que los miembros desplegados no sean válidos. Sin embargo, puede ser que necesite modificar la lista de pertenencias cuando finalice el despliegue.

Si selecciona esta opción, puede decidir la acción que se debe realizar si se produce un conflicto. Puede sustituir los grupos y roles del entorno de destino por los del archivo de despliegue o para conservar los grupos y roles del entorno de destino.

Cómo incluir listas de distribución y contactos

Puede elegir si desea incluir listas de distribución y contactos en el despliegue. Si decide desplegar las listas de distribución y los contactos, deberá desplegarlos todos.

Si selecciona esta opción, puede decidir la acción que se debe realizar si se produce un conflicto. Puede especificar si desea sustituir las listas de distribución y los contactos en el entorno de destino por los del archivo de despliegue o conservar las listas de distribución y los contactos del destino.

Cómo incluir orígenes de datos

Puede elegir que se incluyan orígenes de datos y sus conexiones asociadas Capítulo 6, “Orígenes de datos y conexiones”, en la página 113 en el despliegue. Si decide desplegar orígenes de datos, deberá desplegarlos todos.

Puede desplegar los orígenes de datos con o sin sus inicios de sesión. Si no despliega los inicios de sesión, deberá configurar los orígenes de datos de acuerdo con ello en el entorno de destino. Si despliega los inicios de sesión, deberá cifrar el archivo de despliegue.

Si selecciona esta opción, puede decidir la acción que se debe realizar si se produce un conflicto. Puede especificar si desea sustituir los orígenes de datos en el entorno de destino por los del archivo de despliegue o conservar los orígenes de datos del entorno de destino.

Si sustituye los orígenes de datos de destino, y no coinciden las conexiones de orígenes de datos en los entornos de origen y de destino, podrá perder las conexiones de base de datos. En este caso, deberá reconectar de forma manual los orígenes de datos en el entorno de destino después de la importación con el software de cliente de base de datos.

Cómo incluir permisos de acceso

Puede elegir si desea incluir permisos de acceso “Permisos de acceso” en la página 288 en el despliegue.

Si selecciona esta opción, puede decidir la acción que se debe realizar si se produce un conflicto. Puede especificar si desea sustituir los permisos de acceso en el entorno de destino por los del archivo de despliegue o conservar los permisos de acceso del entorno de destino.

Grabación de detalles de despliegue

Puede especificar el tipo de información que desea guardar en los registros de despliegue mediante el establecimiento del **nivel de grabación** para el despliegue. La cantidad de información guardada en los registros tiene impacto en el rendimiento.

Puede definir los niveles de grabación siguientes:

- **Básico**
Guarda el progreso de despliegue y la información de resumen. Ésta es la opción predeterminada.
- **Mínimo**

Guarda sólo la información de resumen de despliegue. Esta opción necesita muy poca memoria.

- **Rastreo**

Guarda todos los detalles del despliegue. Esta opción necesita mucha memoria.

Para obtener más información acerca del modo de grabar los detalles de despliegue al desplegar un almacén de contenido completo, consulte “Historial de despliegue” en la página 292.

Consideraciones sobre la propiedad

Puede cambiar la propiedad de las entradas importadas al usuario que realiza la importación. Es posible seleccionar esta opción en el momento de la exportación o la importación. Si utiliza los propietarios del origen, se importarán los propietarios junto con las entradas. Puede aplicar las opciones de propiedad a las nuevas entradas, o a las entradas existentes o nuevas.

Valores avanzados del despliegue

Puede utilizar los valores avanzados para especificar el modo en que funciona el despliegue en el entorno.

Si utiliza los valores avanzados podrá:

- Especificar si la salida del informe forma parte del despliegue
- Especificar si los objetos de configuración y los hijos forman parte del despliegue

Especificación de si la salida del informe forma parte del despliegue

Puede especificar si la salida del informe forma parte del despliegue.

Hay dos valores avanzados que puede utilizar:

- CM.DEPLOYMENTSKIPALLREPORTOUTPUT para incluir toda la salida de informe de **Mis carpetas** y **Carpetas públicas** u omitirla.
- CM.DEPLOYMENTSKIPUSERREPORTOUTPUT para incluir la salida de informe de usuario únicamente en **Mis carpetas** u omitirla.

De forma predeterminada, se establecen en True (incluir). Para cambiar el valor predeterminado que se excluirá, establézcalas en False.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration** Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el menú Acciones de **Sistemas**, pulse **Establecer propiedades**.
3. Pulse la pestaña **Valores**.
4. Pulse **Editar** junto a **Valores avanzados**.
5. Seleccione **Reemplazar los valores adquiridos de la entrada padre**.

6. En la columna **Parámetro**, escriba
CM.DEPLOYMENTSKIPALLREPORTOUTPUT o
CM.DEPLOYMENTSKIPUSERREPORTOUTPUT.
7. En la columna **Valor**, escriba la configuración que desee utilizar.
8. Pulse **Aceptar**.
9. En la página **Establecer propiedades**, pulse **Aceptar**.

Inclusión de los objetos de configuración y sus hijos en los despliegues

Para incluir los objetos de configuración y sus hijos como parte de los despliegues, establezca la propiedad avanzada CM.DEPLOYMENTINCLUDECONFIGURATION en true. De forma predeterminada, en IBM Cognos Analytics, el valor de la propiedad es false.

Antes de empezar

Debe disponer de los permisos necesarios para acceder a **IBM Cognos Administration** Capítulo 13, “Funciones y características protegidas”, en la página 227.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. Pulse la flecha del menú Acciones situada junto a **Sistemas** y pulse **Establecer propiedades**.
3. Pulse la pestaña **Valores**.
4. Pulse **Editar** junto a **Valores avanzados**.
5. Seleccione **Reemplazar los valores adquiridos de la entrada padre**.
6. En la columna **Parámetro**, escriba
CM.DEPLOYMENTINCLUDECONFIGURATION.
7. En la columna **Valor**, escriba la configuración que desee utilizar.
8. Pulse **Aceptar**.
9. En la página **Establecer propiedades**, pulse **Aceptar**.

Reglas para la resolución de conflictos de despliegue al importar y exportar

Las reglas de resolución de conflictos son aplicables cuando se importa o se exporta en un entorno de destino.

Las reglas son diferentes dependiendo de si despliega todo el almacén de contenido o las carpetas públicas y el contenido de directorio seleccionados. El método que elija determinará los objetos que se incluirán en la importación y en el modo de resolver los conflictos cuando un objeto ya exista en el entorno de destino.

Los objetos del almacén de contenido representan las entradas en el portal y las propiedades de esas entradas. Por ejemplo, el objeto reportView representa una entrada de vista de informe en el portal y el objeto runHistory representa el historial de ejecución de una entrada. Para obtener más información sobre los objetos, consulte IBM Cognos Software Development Kit *Developer Guide*.

Los objetos de las **Carpetas públicas** heredan las reglas de despliegue de forma predeterminada dependiendo de si despliega todo el almacén de contenido o si sólo selecciona **Carpetas públicas** y el contenido del directorio.

Aunque sólo se puedan producir conflictos durante la importación, y no durante la exportación, se utilizan las mismas reglas para procesar objetos en el archivo durante la exportación. Durante una operación de exportación, si la regla para un objeto es KEEP, no se incluye en el archivo. Para cualquier otro valor, se incluye en el archivo.

Reglas de resolución de conflictos

Un conflicto se puede producir cuando la entrada que desea importar del archivo de despliegue ya existe en el almacén de contenido de destino.

Cuando ocurre esto, se utiliza una de las siguientes reglas de resolución de conflictos, según la entrada y los valores avanzados que haya utilizado.

Tabla 71. Reglas de resolución de conflictos

Regla	Descripción
Sustituir	Sustituye la entrada y sus hijos. Se eliminan la entrada y todos los hijos del almacén de contenido de origen. Se añaden la nueva entrada y todos los hijos al almacén de contenido de origen.
Mantener	Mantiene la entrada. No se actualizan las propiedades de la entrada ni todos sus hijos. Se mantienen los hijos existentes de la entrada. Se pueden añadir nuevos hijos.
Actualizar	Actualiza la entrada. Se actualizan las propiedades de la entrada y todos sus hijos. Se mantienen los hijos existentes de la entrada. Se pueden añadir nuevos hijos.
Combinar	Combina las propiedades de las entradas con las entradas existentes.

Si una entrada no tiene hijos, la sustitución y la actualización tienen el mismo resultado final.

Contenido

Todos los objetos del área de contenido del almacén de contenido se incluyen y se sustituyen al importar todo el almacén de contenido.

Directorio

Si incluye los orígenes de datos, las conexiones y los inicios de sesión y conserva las entradas existentes, los objetos asociados del archivo se fusionarán con los objetos del entorno de destino. Aunque los objetos se fusionen, las reglas de conservación seguirán aplicándose. No es posible que se produzca una fusión completa porque se pueden haber descartado algunos objetos.

Tenga en cuenta que si desea incluir grupos y roles, así como listas de distribución y contactos de Cognos, estos elementos deberán estar almacenados en una carpeta del espacio de nombres para poder desplegarlos.

Los miembros de las listas de distribución, los grupos y los roles del archivo no se fusionan con el contenido del entorno de destino. Sin embargo, el conjunto de listas de distribución, grupos y roles se fusiona con el conjunto existente del entorno de destino. No obstante, los miembros del grupo Administradores del sistema siempre se fusionan cuando se importa este grupo. Para obtener más información, consulte “Cómo incluir grupos y roles de Cognos” en la página 295.

Reglas para la resolución de conflictos en el despliegue de todo el almacén de contenido

La regla para la resolución de conflictos predeterminada en el despliegue de todo el almacén de contenido es sustituir.

Las excepciones a la regla para la resolución de conflictos predeterminada se indican en la tabla siguiente:

Tabla 72. Despliegue completo, excepciones a la regla de resolución de conflictos predeterminada

Nombre del objeto	Regla de resolución de conflictos
OUTPUT, GRAPHIC, PAGE	Mantener si • El valor avanzado CM.DEPLOYMENTSKIPALLREPORTOUTPUT se ha establecido en True • El objeto se encuentra bajo cuentas de usuario y el valor avanzado CM.DEPLOYMENTSKIPUSERREPORTOUTPUT se ha establecido en True Para obtener más información sobre los valores, consulte “Especificación de si la salida del informe forma parte del despliegue” en la página 297.
ACCOUNT	Actualizar si Incluir información de cuenta de usuario se selecciona durante el despliegue, mantener si no es así. Para obtener más información sobre la inclusión de la información de cuenta de usuario, consulte “Despliegue de todo el almacén de contenido” en la página 291.

Tabla 72. Despliegue completo, excepciones a la regla de resolución de conflictos predeterminada (continuación)

Nombre del objeto	Regla de resolución de conflictos
SESSION, CACHEOUTPUT, REPORTCACHE, REPORTMETADATACACHE, DEPLOYMENTDETAIL	Mantener
FOLDER, MRUFOLDER, SUBSCRIPTIONFOLDER	Sustituir si se encuentra directamente bajo un objeto de cuenta de usuario de espacio de nombres de Cognos (carpeta Mis carpetas) o directamente bajo el objeto de cuenta de usuario de espacio de nombres de terceros (carpeta Mis carpetas).
CAPABILITY, SECUREDFUNCTION, CONFIGURATION, CONFIGURATIONFOLDER, DISPATCHER, DIRECTORY, NAMESPACE, NAMESPACEFOLDER, PORTAL, PORTALPACKAGE, PORTALSKINFOLDER, PORTLETFOLDER, PORTLETPRODUCER, PORTLET, PAGELETFOLDER, PAGELET, PAGELETINSTANCE, PORTLETINSTANCE	Actualizar
ROLE, GROUP	Sustituir (pero conservar identificador de objeto).
CONTENT, ADMINFOLDER, TRANSIENTSTATEFOLDER	Sustituir. Tenga en cuenta que la opción de despliegue <code>entireContentStoreReplace</code> sólo se puede cambiar por <code>False</code> (actualizar) con una aplicación de Software Development Kit. Para obtener más información, consulte la documentación del Software Development Kit.
HISTORY, HISTORYDETAIL, HISTORYDETAILREQUEST, ARGUMENTS	Mantener si se encuentra bajo el objeto ADMINFOLDER.

Reglas para la resolución de conflictos en el despliegue parcial

Al desplegar carpetas públicas y el contenido del directorio en lugar de todo el almacén de contenido, puede seleccionar el contenido que desee desplegar.

Algunas reglas para la resolución de conflictos dependen de las selecciones que realice.

Al actualizar un objeto padre, se añaden los hijos nuevos del archivo de despliegue y se unen al grupo existente de hijos del entorno de destino. Si se produce un conflicto, la regla de resolución de conflictos consistirá en sustituir los hijos.

Al no sustituirse todos los pasos del trabajo, no es posible que se produzca un conflicto cuando se importen objetos jobStepDefinition.

Si incluye las versiones de salida de informe y los historiales de ejecución, y conserva las entradas existentes, los objetos asociados del archivo se fusionarán con los objetos del entorno de destino. Aunque los objetos se fusionen, las reglas de conservación seguirán aplicándose. No es posible que se produzca una fusión completa porque se pueden haber descartado algunos objetos.

La regla para la resolución de conflictos predeterminada para despliegues parciales es sustituir.

Las excepciones a la regla para la resolución de conflictos predeterminada se indican en la tabla siguiente:

Tabla 73. Despliegue parcial, excepciones a la regla de resolución de conflictos predeterminada

Nombre del objeto	Regla de resolución de conflictos
REPORTVERSIONSQL	Depende de si Incluir versiones de salida de informe se establece en sustituir o en mantener “Cómo incluir versiones de salida de informe” en la página 294.
OUTPUT	Mantener si el valor avanzado DEPLOYMENTSKIPREPORTOUTPUT se establece en True “Especificación de si la salida del informe forma parte del despliegue” en la página 297. De lo contrario, depende de si Incluir versiones de salida de informe se establece en sustituir o en mantener “Cómo incluir versiones de salida de informe” en la página 294.
GRAPHICPAGE	Mantener si el valor avanzado DEPLOYMENTSKIPREPORTOUTPUT se establece en True “Especificación de si la salida del informe forma parte del despliegue” en la página 297. De lo contrario, depende de si Incluir versiones de salida de informe se establece en sustituir o en mantener “Cómo incluir versiones de salida de informe” en la página 294.
HISTORY	Depende de si Incluir historial de ejecución se establece en sustituir o en mantener “Cómo incluir el historial de ejecución” en la página 294.

Tabla 73. Despliegue parcial, excepciones a la regla de resolución de conflictos predeterminada (continuación)

Nombre del objeto	Regla de resolución de conflictos
SCHEDULE	Depende de si Incluir planificaciones se establece en sustituir o en mantener “Cómo incluir planificaciones” en la página 294.
JOBSTEPDEFINITION	Sustituir.
JOBDEFINITION	Actualizar y eliminar los hijos JOBSTEPDEFINITION. Si se especifica PackageHistories y packageHistoriesConflictResolution se establece en sustituir, eliminar también los objetos HISTORY.
DATASOURCE, DATASOURCECONNECTION, DATASOURCENAMEBINDING	Depende de si Incluir orígenes de datos y conexiones se establece en mantener o en sustituir “Cómo incluir orígenes de datos” en la página 296.
DATASOURCESIGNON	Depende de si Incluir orígenes de datos y conexiones e Incluir inicios de sesión se establecen en mantener o en sustituir “Cómo incluir orígenes de datos” en la página 296.
DISTRIBUTIONLIST, CONTACT	Depende de si Incluir listas de distribución y contactos se establece en mantener o en sustituir “Cómo incluir listas de distribución y contactos” en la página 296.
ROLE, GROUP	Depende de si Incluir grupos y roles de Cognos se establece en mantener o en sustituir “Cómo incluir grupos y roles de Cognos” en la página 295. (Si se establece en sustituir, se conserva el identificador del objeto.)
CACHEOUTPUT, REPORTCACHE, REPORTMETADATACACHE	Mantener

Despliegue de las entradas de IBM Cognos

Para desplegar el software de IBM Cognos, debe exportar el archivo de despliegue en el entorno de origen y, a continuación, mueva el archivo al entorno de destino e impórtelo allí.

Puede organizar la especificación de despliegue en carpetas de la misma forma que organiza todas las entradas.

Despliegue y agentes

El despliegue puede formar parte de un agente.

Planificaciones de despliegue e historial de ejecución

Puede planificar el despliegue para que se ejecute de forma automática a una hora en concreto o como parte de un trabajo. El software de IBM Cognos guarda el historial de ejecución para cada especificación de despliegue. Después de exportar o importar, puede ver la fecha y la hora, y el estado del despliegue. También puede ver los mensajes de error creados por el despliegue y la lista de entradas que se han exportado o importado. Para obtener más información, consulte: Capítulo 17, “Gestión de actividades”, en la página 263.

Permisos

Para desplegar entradas de IBM Cognos, debe tener permisos de ejecución para la característica protegida **Tareas de administración** y permisos de visita para la función protegida **Administración**. Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

También debe pertenecer al grupo Administradores del sistema y tener acceso de lectura y escritura al espacio de nombres de Cognos para poder desplegar el grupo Administradores del sistema. Para obtener más información, consulte “Establecimiento de permisos de acceso para una entrada” en la página 220.

Cuando realice una exportación parcial de las carpetas públicas y del contenido de directorio “Despliegue del contenido de directorio y de las carpetas públicas seleccionadas” en la página 293 en lugar de exportar todo el almacén de contenido “Despliegue de todo el almacén de contenido” en la página 291, deberá poseer permisos de visita y de lectura para las entradas que exporte. También es necesario tener permisos de escritura porque al exportar se crea una especificación y un historial de despliegue. Al importar, debe poseer permisos de escritura y permisos para establecer política para las entradas que importe.

Requisitos previos

El software de IBM Cognos y otros productos deben instalarse y configurarse en los entornos de origen y de destino. Para obtener más información, consulte IBM Cognos *Guía de instalación y configuración*.

Es recomendable que detenga el servicio de Content Manager antes de exportar e importar. Esto impide a los usuarios recibir resultados imprevisibles si ejecutan operaciones durante el despliegue. Por ejemplo, si los usuarios ven informes en un paquete mientras se está importando el paquete, pueden encontrar errores cuando se sustituyan las salidas de informe. Para obtener más información, consulte: “Detención e inicio de asignadores y servicios” en la página 52.

Antes de empezar, debe planificar el despliegue para determinar las opciones de despliegue que va a utilizar y las entradas que va a desplegar “Planificación de despliegue” en la página 288. Tal vez desee realizar una copia de seguridad antes del despliegue Capítulo 8, “Cómo hacer una copia de seguridad de los datos”, en la página 183.

Exportar de un entorno de origen

Para exportar entradas de IBM Cognos, cree una especificación de despliegue de exportación y, a continuación, ejecute la exportación.

También puede utilizar una especificación de despliegue guardada anteriormente para exportar o para volver a desplegar entradas.

Las entradas se exportan a un archivo de despliegue de exportación “Archivos de despliegue” en la página 288 del entorno de origen. Posteriormente, las entradas del archivo se importan al entorno de destino. Puede actualizar las entradas del entorno de destino mediante las entradas del archivo de despliegue.

Para obtener información sobre la resolución de conflictos durante los despliegues, consulte “Reglas para la resolución de conflictos de despliegue al importar y exportar” en la página 298.

Cuando exporte, seleccione las entradas que vaya a desplegar y cuando importe, establezca las opciones que se utilizarán como predeterminadas.

Creación de una nueva especificación de implementación de exportación

Una especificación de implementación de exportación define el contenido que se debe exportar.

Para obtener información acerca de cómo exportar el contenido en un entorno de varios inquilinos de IBM Cognos Analytics, consulte “Despliegue de contenido de arrendatario” en la página 346.

Antes de empezar

Si desea conservar cuentas de acceso a origen de datos al exportar un almacén de contenido, debe seleccionar **Incluir información de cuenta de usuario**. Si desea conservar la información de configuración al exportar, puede establecer el valor avanzado CM.DEPLOYMENTINCLUDECONFIGURATION en TRUE. Para obtener más información, consulte “Inclusión de los objetos de configuración y sus hijos en los despliegues” en la página 298.

Procedimiento

1. En el entorno de origen, abra **IBM Cognos Administration**.
2. En la pestaña **Configuración**, pulse **Administración de contenidos**.
3. En la barra de herramientas, pulse el icono **Nueva exportación** . Aparecerá el asistente para **Nueva exportación**.
4. Escriba un nombre exclusivo, y una descripción y sugerencia opcionales para la especificación de despliegue. Seleccione la carpeta en la que desee guardarla y pulse **Siguiente**.
5. Elija si desea exportar todo el almacén de contenido o para realizar una exportación parcial de contenido específico:
 - Para exportar el contenido específico, pulse **Seleccionar carpetas públicas, directorio y contenido de biblioteca**. Pulse **Siguiente** y proceda al paso 7.
 - Para exportar todo el almacén de contenido, pulse **Seleccionar todo el almacén de contenido** y seleccione si desea incluir información de cuenta de usuario. Pulse **Siguiente** y proceda al paso 15.
6. En la página **Seleccionar el contenido de las carpetas públicas**, pulse **Añadir**.
7. En la página **Seleccionar entradas**, en el cuadro **Entradas disponibles**, seleccione una de las siguientes entradas o su contenido:
 - **Carpetas públicas**

Contiene paquetes y carpetas. Seleccione los paquetes y carpetas que desea exportar.

- **Directorio**

Contiene espacios de nombres, carpetas de espacios de nombres, grupos y roles, así como cuentas de usuario individuales. Cuando selecciona una cuenta de usuario, todo el contenido asociado con el usuario, incluyendo el contenido de **Mis carpetas** del usuario, se incluye en la exportación.

- **Biblioteca**

Contiene recursos de biblioteca, como visualizaciones.

8. Pulse en el icono de flecha  para mover los elementos seleccionados al cuadro **Entradas seleccionadas** y pulse **Aceptar**.
9. Para cada entrada que esté exportando, realice una de las acciones siguientes:
 - Si desea que la entrada tenga un nombre distinto en el entorno de destino, o si desea cambiar la ubicación de destino o añadir nombres multilingües, pulse el icono **Editar** , realice los cambios y pulse **Aceptar**.
 - Si no desea que los usuarios accedan a las entradas y a su contenido, seleccione la casilla de verificación en la columna **Deshabilitar después de importar**. Esto es útil, por ejemplo, cuando desea probar los informes antes de ponerlos a disposición en el entorno de destino.
10. En **Opciones**, seleccione si desea incluir las versiones de salida de informe, el historial de ejecución y las planificaciones, y lo que debe hacer con las entradas en caso de conflicto.
11. En la página **Seleccionar el contenido de directorio**, seleccione si desea exportar los grupos y los roles, las listas de distribución y contactos, los orígenes de datos y conexiones de Cognos y lo que se debe hacer con las entradas en caso de conflicto.
12. En la página **Especificar las opciones generales**, seleccione si desea incluir permisos de acceso y referencias a los espacios de nombres que no sean **IBM Cognos** y a quién deberían pertenecer las entradas después de importarlas en el entorno de destino.
13. Especifique el **Nivel de grabación** del histórico de implementación. Para obtener más información, consulte “Grabación de detalles de despliegue” en la página 296.
14. En la página **Especificar un archivo de despliegue**, en **Archivo de despliegue**, seleccione un archivo de despliegue existente en la lista o bien escriba un nuevo nombre para crear uno.

Si escribe un nuevo nombre para el archivo de despliegue, el nombre no deberá contener espacios en blanco. Si el nombre de la especificación de despliegue nueva coincide con el nombre del archivo de despliegue existente, se añadirán los caracteres **_#** al final del nombre, donde **#** es un número como 1.
15. En **Cifrado**, pulse **Establecer la contraseña de cifrado**, escriba una contraseña y pulse **Aceptar**.
16. Pulse **Siguiente**. Aparecerá la información de resumen.
17. Revise la información de resumen y pulse **Siguiente**. Si desea cambiar la información, haga clic en **Atrás** y siga las instrucciones.
18. Especifique cómo ejecutar la especificación de implementación de la exportación:

- Para ejecutarla ahora o más adelante, pulse **Guardar y ejecutar una vez** y en **Finalizar**. Especifique la hora y la fecha de la ejecución. A continuación, pulse **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
- Para planificar su ejecución de forma periódica, pulse **Guardar y planificar** y, a continuación, en **Finalizar**. A continuación, seleccione la frecuencia, las fechas de inicio y finalización, y pulse **Aceptar**.

Consejo:

Para inhabilitar temporalmente la planificación, seleccione la casilla de verificación **Inhabilitar la planificación**. Para visualizar el estado de la planificación, consulte “Gestión de actividades planificadas” en la página 269.

- Para guardar sin planificar o ejecutar, pulse **Solo guardar**, y pulse **Finalizar**.

Resultados

Después de ejecutar la exportación, puede mover el archivo de despliegue. También puede visualizar el historial de ejecución de exportación “Visualización del historial de ejecución de las entradas” en la página 271.

Modificación de una especificación de despliegue existente

Puede reutilizar una especificación de despliegue guardada anteriormente para exportar o para volver a desplegar sus entradas.

Procedimiento

1. En el entorno de destino, abra **Lanzar IBM Cognos Administration**.
2. En la pestaña **Configuración**, pulse **Administración de contenidos**.
3. En la columna **Acciones** pulse el botón Propiedades  de la especificación de despliegue que desee modificar y, a continuación, pulse la pestaña **Exportar**.
4. Modifique las opciones de despliegue según sea necesario.

Consejo: Si desea cambiar la ubicación de destino de la exportación, pulse el botón Editar  situado junto al nombre de exportación, en la columna **Nombre de destino**, sección **Carpetas públicas**, y seleccione el paquete o la carpeta que desee.

5. Pulse **Aceptar**.

Resultados

De este modo, se guardarán las opciones y se podrá ejecutar la exportación ahora o más tarde. Para obtener más información, consulte “Ejecución de una exportación”.

Ejecución de una exportación

Después de crear un nuevo archivo de despliegue de exportación o de modificar uno existente, puede ejecutarlo.

Procedimiento

1. En la columna **Acciones**, pulse el botón Ejecutar con opciones .
2. Pulse **Ahora** para ejecutar la exportación inmediatamente o en **Más adelante**, e introduzca la hora a la que desee ejecutarla.

También puede planificar una tarea para que se ejecute periódicamente y ver una lista de las tareas planificadas. Para obtener más información, consulte: Capítulo 18, “Administración de planificaciones”, en la página 277.

Para evitar los mensajes de aviso al iniciar sesión en varios espacios de nombres, antes de ejecutar la exportación de nuevo, renueve las credenciales.

Resultados

Ahora puede mover el archivo de despliegue.

Cómo mover el archivo de despliegue

Mueva el archivo de despliegue que creó en el entorno de origen al entorno de destino.

Si los entornos de origen y de destino utilizan el mismo almacén de contenido, podrá importar sin mover el archivo de despliegue.

La ubicación en la que se guardan los archivos de despliegue está establecida en la herramienta de configuración. La ubicación predeterminada es *install_location/deployment*.

Antes de empezar

Si tiene previsto mover el archivo de despliegue a una ubicación de una LAN, asegúrese de que hay suficiente espacio de disco. Si no cifró el archivo de despliegue, es recomendable que lo copie en una ubicación segura.

Procedimiento

1. Copie el archivo de despliegue del entorno de origen a una ubicación en la LAN o en un CD.
2. Copie el archivo de despliegue de la LAN o el CD al entorno de destino de la ubicación establecida en la herramienta de configuración.

Resultados

Ahora puede incluir objetos de configuración si importa un almacén de contenido completo o importa a un entorno de destino.

Importación en un entorno de destino

Cree una especificación de despliegue de importación nueva o modifique una existente y, a continuación, ejecute la importación.

Puede importar mediante el uso de una especificación de despliegue existente si anteriormente la guardó sin importar, o si desea volver a desplegar las entradas de IBM Cognos. Puede actualizar las entradas en el entorno de destino con las entradas del archivo de despliegue.

Para obtener información sobre la resolución de conflictos durante los despliegues, consulte “Reglas para la resolución de conflictos de despliegue al importar y exportar” en la página 298.

Al importar, selecciona de entre las entradas que se exportaron. Puede aceptar las opciones predeterminadas establecidas durante la exportación o cambiarlas. No puede seleccionar las opciones que no se incluyeron en el archivo de despliegue

durante la exportación. Para obtener más información acerca del modo de importar objetos específicos del almacén de contenido, consulte “Reglas para la resolución de conflictos de despliegue al importar y exportar” en la página 298.

También puede utilizar el Asistente para nueva importación para actualizar las entradas de las versiones anteriores del producto. Es posible actualizar las especificaciones de informe durante la importación o actualizarlas más adelante con el asistente Nueva actualización de informe. Para obtener más información, consulte “Actualización de las especificaciones de informes” en la página 312.

Cuando ejecuta una importación, los identificadores de almacén de contenido se suprimen y se asignan nuevos identificadores. Si los identificadores de almacén deben retenerse porque una funcionalidad de IBM Cognos determinada los utiliza, tiene la opción de preservar los identificadores de almacén. Para obtener más información, consulte “Asignación de ID de contenido” en la página 313.

Para utilizar una especificación de despliegue de importación existente, consulte “Modificación de una especificación de despliegue de importación existente” en la página 310.

Si realiza un despliegue parcial de carpetas públicas y contenido de directorio específicos, el asistente de importación muestra si los paquetes y las carpetas ya existen en el entorno de destino, así como la fecha y la hora de su última modificación. Puede utilizar esta información para decidir cómo resolver los conflictos. Al desplegar de nuevo, el asistente también muestra si los paquetes y las carpetas estaban en el despliegue original.

Creación de una nueva especificación de implementación de importación

Una especificación de implementación de importación define el contenido que se debe importar.

Para obtener información acerca de cómo importar el contenido en un entorno de varios inquilinos de IBM Cognos Analytics, consulte “Despliegue de contenido de arrendatario” en la página 346.

Procedimiento

1. En el entorno de destino, abra **IBM Cognos Administration**.
2. En la pestaña **Configuración**, pulse **Administración de contenidos**.
3. En la barra de herramientas, pulse el icono **Nueva importación** . Aparecerá el asistente para **Nueva importación**.
4. En el cuadro **Archivo de despliegue**, pulse el archivo de despliegue que desee importar.
5. Escriba la contraseña que se utilizó para cifrar el contenido, y pulse **Aceptar** y luego **Siguiente**.
6. Escriba un nombre único y una descripción opcional y una sugerencia en pantalla para la especificación de implementación, seleccione la carpeta en donde desea guardarlo, y pulse **Siguiente**.
7. Seleccione el contenido que desee incluir en la importación.

Consejo: Para asegurarse de que las entradas objetivo requeridas existen en el almacén de contenido objetivo, pulse el botón de edición  al lado del paquete y verifique la ubicación. Si lo desea, en este momento puede cambiar la ubicación de destino.

8. Seleccione las opciones que desea, junto con su opción de resolución de conflictos para las opciones que seleccione.
9. En la página **Especificar las opciones generales**, seleccione si desea incluir permisos de acceso y referencias a los espacios de nombres que no sean **IBM Cognos** y a quién deberían pertenecer las entradas después de importarlas en el entorno de destino.
10. Especifique el **Nivel de grabación** del histórico de implementación. Para obtener más información, consulte “Grabación de detalles de despliegue” en la página 296.
11. Pulse **Siguiente**.
12. Revise la información de resumen y pulse **Siguiente**.
13. Seleccione cómo ejecutar la especificación de implementación de importación:
 - Para ejecutarla ahora o más adelante, pulse **Guardar y ejecutar una vez** y en **Finalizar**. Especifique la hora y la fecha de la ejecución. A continuación, pulse **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - Para planificar su ejecución de forma periódica, pulse **Guardar y planificar** y, a continuación, en **Finalizar**. A continuación, seleccione la frecuencia, las fechas de inicio y finalización, y pulse **Aceptar**.

Consejo: Para inhabilitar temporalmente la planificación, seleccione la casilla de verificación **Inhabilitar la planificación**. Para visualizar el estado de la planificación, consulte “Gestión de actividades planificadas” en la página 269.

- Para guardar sin planificar o ejecutar, pulse **Sólo guardar** y, a continuación, en **Finalizar**.

Cuando ejecute la importación, tendrá la opción de seleccionar para actualizar la especificación de informe. Si decide no actualizar la especificación de despliegue en este momento, lo puede hacer más tarde. Para obtener más información, consulte “Actualización de las especificaciones de informes” en la página 312.

Resultados

Después de ejecutar la importación, puede probar el despliegue. También puede visualizar el historial de ejecución de importación “Visualización del historial de ejecución de las entradas” en la página 271.

Modificación de una especificación de despliegue de importación existente

Puede modificar una especificación de despliegue existente.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Administración de contenidos**.
2. En la columna **Acciones** pulse el botón Propiedades  de la especificación de despliegue que desee modificar y, a continuación, pulse la pestaña **Importar**.
3. Modifique las opciones de despliegue según sea necesario.

Consejo: Si desea cambiar la ubicación de destino de la importación, pulse el botón Editar  situado junto al nombre de importación, en la columna **Nombre de destino**, sección **Carpetas públicas**, y seleccione el paquete o la carpeta que desee.

4. Pulse **Aceptar**.

Resultados

De este modo, se guardarán las opciones y se podrá ejecutar la importación ahora o más tarde. Para obtener más información, consulte “Ejecutar importación”.

Ejecutar importación

Después de crear o modificar una especificación de despliegue de importación, ejecute el informe.

Procedimiento

1. En la columna **Acciones**, pulse el botón Ejecutar con opciones .
2. Pulse **Ahora** para ejecutar la importación inmediatamente o en **Más adelante**, e introduzca la hora a la que desee ejecutarla.
3. Si desea actualizar las especificaciones de informe, pulse **Actualizar todas las especificaciones de informe a la última versión**.

También puede planificar una tarea para que se ejecute periódicamente y ver una lista de las tareas planificadas. Para obtener más información, consulte: Capítulo 18, “Administración de planificaciones”, en la página 277.

4. Para especificar cómo han de asignarlos los identificadores de contenido, en **ID de contenido**, seleccione
 - **Asignar ID nuevos durante la importación** para sustituir los identificadores de contenido existentes por nuevos identificadores
 - **No asignar ID nuevos durante la importación** para conservar los identificadores de contenido existente al realizar la importación

Resultados

Ahora puede probar el despliegue.

Inclusión de los objetos de configuración en la importación de todo el almacén de contenido

Puede incluir objetos de configuración al importar un almacén de contenido completo.

Antes de empezar

De forma predeterminada, los objetos de configuración se excluyen cuando se importa un almacén de contenido completo, aunque se incluyen en la exportación. Los objetos de configuración incluyen asignadores y carpetas de configuración, que se utilizan para agrupar los asignadores. Para obtener más información, consulte “Reglas para la resolución de conflictos en el despliegue de todo el almacén de contenido” en la página 300.

No es recomendable importar los objetos de configuración. Los asignadores deben configurarse en el entorno de destino antes de importar los datos de un entorno de

origen. Si debe importar objetos de configuración, deberá detener los servicios de asignador de origen antes de la importación o reiniciar el software de IBM Cognos en el entorno de destino después de la importación. De lo contrario, es posible que se produzcan errores con el estado de los asignadores. Si desea importar objetos de configuración, deberá estar preparado para una breve interrupción del servicio.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para asignadores específicos” en la página 514.
2. Para **ContentManagerService**, escriba **CM.DEPLOYMENTINCLUDECONFIGURATION** como nombre del **Parámetro**.
3. Escriba **verdadero** como un valor para este parámetro y haga clic en **Aceptar**.

Comprobación de las aplicaciones desplegadas

Después de importar los paquetes del archivo de despliegue, verifique que todas las entradas se hayan desplegado correctamente en el entorno de destino.

Puede comprobar el despliegue

- Revisando el historial de ejecución para un despliegue.
- Asegurándose de que los paquetes y carpetas correctas se han importando junto con el contenido.
- Asegurándose de que se han importado los orígenes de datos, las listas de distribución y los contactos, así como los grupos y los roles de Cognos.
- Verificando los permisos para las entradas importadas.
- Asegurándose de que se han importado las planificaciones.
- Asegurándose de que se han actualizado las referencias para paquetes cuyo nombre se haya cambiado.
- Ejecutando los informes importados y las vistas de informe.

Actualización de las especificaciones de informes

Si no actualizó las especificaciones de informe cuando ejecutó el asistente de importación, puede actualizarlas con el asistente Nueva actualización de informe.

Antes de empezar

Importante: No actualice las especificaciones de informe si tiene aplicaciones de Software Development Kit que crean, modifican o guardan especificaciones de informe. Primero debe actualizar las aplicaciones de Software Development Kit para que sean compatibles con el esquema de especificaciones de informe de IBM Cognos BI. De lo contrario, es posible que las aplicaciones de Software Development Kit no puedan acceder a las especificaciones de informe actualizadas. Para obtener más información acerca de la actualización de especificaciones de informe, consulte la publicación *IBM Cognos Software Development Kit Developer Guide*.

Procedimiento

1. Inicie sesión como administrador con permisos de ejecución para la característica **Administración de contenidos**.
2. Abra **IBM Cognos Administration**.
3. En la pestaña **Configuración**, pulse **Administración de contenidos**.

4. Pulse la flecha del botón Mantenimiento de nuevo contenido  de la barra de herramientas y, a continuación, en **Nueva actualización de informe**.
5. Escriba un nombre para la tarea de actualización y, si lo desea, una descripción y una sugerencia. Pulse **Siguiente**.
6. Seleccione los paquetes y las ubicaciones para la especificación de informe que desee actualizar. Pulse **Siguiente**.

Si actualiza las especificaciones de informe por paquete, se actualizarán todos los informes del almacén de contenido basados en el modelo del paquete. Si actualiza las especificaciones de informe por carpeta, se actualizarán todos los informes de la carpeta.
7. Seleccione una de las siguientes opciones:
 - **Guardar y ejecutar una vez** abre la página Ejecutar con opciones.
 - **Guardar y planificar** abre la herramienta de planificación.
 - **Sólo guardar** permite guardar la actualización para que pueda ejecutarla más adelante.

Asignación de ID de contenido

Cuando ejecuta un despliegue de importación, puede seleccionar cómo han de asignarse los ID de contenido para los objetos del almacén de contenido.

Los objetos del almacén de contenido tienen ID de contenido que se suprimen y sustituyen por nuevos ID de forma predeterminada cuando ejecuta un despliegue de importación y mueve contenido a un entorno de destino. Sin embargo, puede que existan situaciones en las que deberá preservar los ID de contenido, por ejemplo, al archivar salidas de informes a un repositorio de informes externo. En este caso, puede optar por preservar los ID de contenido al ejecutar la importación. Para obtener más información sobre cómo asignar ID al importar objetos, consulte: “Ejecutar importación” en la página 311.

La preservación de los ID de contenido puede aplicarse a un despliegue parcial o a un despliegue de la totalidad del almacén de contenido.

Conflictos de ID de contenido

Cuando se retienen ID de contenido existentes, pueden producirse conflictos durante la importación. A continuación se detallan las situaciones de conflicto que se pueden producir.

Tabla 74. Conflicto con ID de contenido coincidente

Información	Detalles
Descripción	Cuando en el entorno de destino existe un objeto importado en una ubicación distinta, pero con un ID de contenido coincidente, el ID no se preserva durante la importación sino que se sustituye por un ID de reciente generación. El objeto que existe en el entorno de destino puede ser otra versión del mismo objeto o puede ser un objeto completamente distinto.
Aviso	Un mensaje de aviso describirá que el contenido no se ha preservado y, si los privilegios de seguridad lo permiten, identificará qué objeto del entorno de destino está en conflicto. No se emitirá ninguna información acerca de la resolución del conflicto.

Tabla 74. Conflicto con ID de contenido coincidente (continuación)

Información	Detalles
Solución	Para solucionar cualquier conflicto de ID de contenido, tiene las opciones siguientes: • No realizar ningún cambio en los ID de contenido tras la importación y conservar los ID tal como están. Ahora, los enlaces para el objeto importado apuntarían al objeto de entorno de destino que con más probabilidad es una versión más antigua del mismo objeto. Si no se hace referencia fuera del almacén de contenido al ID de contenido para el objeto importado, no existirá ninguna referencia externa rota tras la importación. El objeto importado seguirá existiendo como un objeto separado. • Suprimir el objeto importado y el objeto del entorno de destino. Si el objeto vuelve a importarse, el objeto se añadirá a la misma ubicación con su ID de contenido. • Actualizar manualmente el objeto de destino con propiedades del objeto importado. Los enlaces para el objeto se preservarán, pues el ID de contenido no habrá cambiado. El objeto importado podrá entonces suprimirse.

Tabla 75. Conflicto con ID de contenido diferente

Información	Detalles
Descripción	Cuando en el entorno de destino exista un objeto importado en la misma ubicación, pero con un ID de contenido distinto, el ID se preservará durante la importación y sustituirá al ID existente en el entorno de destino.
Aviso	No se emiten mensajes de aviso.
Solución	Tenga en cuenta que todas las referencias externas al ID de contenido de destino, si existen, se perderán permanentemente al sustituirse el ID de contenido.

Despliegue de Human Task and Annotation Services

El contenido para Human Task and Annotation Services se almacena por separado del almacén de contenido principal. Este contenido podría almacenarse en la misma base de datos que el almacén de contenido, como tablas distintas o en una base de datos por separado. Para desplegar este contenido se utilizan scripts, en lugar de la herramienta de despliegue.

En el procedimiento de este tema se describe la utilización de scripts para desplegar contenido de Human Task and Annotation Service. Para obtener información acerca de los scripts para desplegar comentarios de IBM Cognos Workspace, consulte “Despliegue de comentarios de IBM Cognos Workspace” en la página 315.

Desplíéguelos ejecutando un archivo de proceso por lotes, que recupera las tareas humanas o las anotaciones de una base de datos de origen. A continuación, ejecute otro archivo de proceso por lotes para instalarlos en un servidor de destino.

Procedimiento

1. Cree los datos de la tarea en la base de datos creando una selección de tareas que apunte a informes válidos.

Para obtener más información, consulte IBM Cognos Event Studio *User Guide*.
Para obtener más información sobre las anotaciones (comentarios), consulte la Guía de usuario de *IBM Cognos Workspace*.

2. En el servidor de origen, abra un indicador de comandos en *install_location/bin*.
3. Ejecute el archivo *htsDeployTool* con los argumentos siguientes:

```
htsDeployTool -camUsername nombre_usuario_cam -camPassword contraseña_cam  
-camNamespace espacio_nombres_cam -exportFile nombre_archivo_exportación  
-password contraseña_archivo_exportación
```

siendo:

- *nombre_usuario_cam* el nombre de usuario para el espacio de nombres.
- *contraseña_cam* la contraseña del usuario para el espacio de nombres.
- *espacio_nombres_cam* el nombre del espacio de nombres.
- *nombre_archivo_exportación* el nombre del archivo de exportación que se creará; por ejemplo, *ArchivoExportTareaHumana1*.
- *contraseña_archivo_exportación* la contraseña del archivo de exportación.

Escriba entre comillas los argumentos que contienen espacios. Escriba una barra inclinada invertida delante de los caracteres especiales. Por ejemplo:

```
htsDeployTool -exportFile "jan\'s file" -password test2Password  
-camNamespace default -camUsername myId -camPassword myPassword
```

Para permitir el acceso anónimo, omita los argumentos *-cam*.

Para exportar anotaciones, añada el argumento *-persistenceUnit annotations*.

Por ejemplo:

```
-camPassword <camPassword> -camNameSpace <camNamespace> -exportfile  
AnnotationExportFile1 -password <exportFilePassword> -persistenceUnit  
annotations.
```

4. Asegúrese de que se haya creado el *<nombre_archivo_exportación>.xml.gz* en *install_location/deployment*. Por ejemplo, *HumanTaskExportFile1.xml.gz*. Cópielo.
5. En el servidor de destino, pegue el archivo *<nombre_archivo_exportación>.xml.gz* en *install_location/deployment*.
6. En el servidor de destino, abra un indicador de comandos en *install_location/bin* y ejecute el archivo *htsDeployTool* con los argumentos siguientes:

```
htsDeployTool -camUsername nombre_usuario_cam contraseña_cam -camNamespace  
espacio_nombres_cam -importFile nombre_archivo_exportación -password  
contraseña_archivo_importación
```

siendo:

- *nombre_usuario_cam* el nombre de usuario para el espacio de nombres.
- *contraseña_cam* la contraseña del usuario para el espacio de nombres.
- *espacio_nombres_cam* el nombre del espacio de nombres.
- *nombre_archivo_importación* el nombre del archivo que ha creado en el paso 3.
- *contraseña_archivo_importación* la contraseña del archivo que ha creado en el paso 3.

Vea más sugerencias de sintaxis en el paso 3.

Despliegue de comentarios de IBM Cognos Workspace

Puede desplegar comentarios de IBM Cognos Workspace mediante el procedimiento siguiente.

Procedimiento

1. En el sistema que tiene las anotaciones que desea desplegar, exporte el almacén de contenido. Para obtener información acerca de la exportación de un almacén de contenido, consulte: “Creación de una nueva especificación de implementación de exportación” en la página 305.
2. En el servidor de origen, en un indicador de comandos abra la carpeta `install_location/bin`.
3. En la carpeta `bin`, ejecute el archivo denominado `htsDeployTool` con los argumentos siguientes:

```
htsDeployTool -persistenceUnit annotations -camUsername camUsername  
-camPassword camPassword -camNamespace camNamespace -exportFile  
exportFileName -password exportFilePassword
```

donde

camUsername es el nombre de usuario del espacio de nombres.

camPassword es la contraseña de usuario para el espacio de nombres.

camNamespace es el nombre del espacio de nombres.

exportFileName es el nombre del archivo de exportación que se creará; por ejemplo, `HumanTaskExportFile1`. Ejemplo: `htsDeployTool -persistenceUnit annotations -exportFile myFile -password test2Password -camNamespace default -camUsername myId -camPassword myPassword`

Para permitir el acceso anónimo, omita los argumentos `-cam`.
4. Asegúrese de que se ha creado el archivo *nombre_archivo_exportación.xml.gz* en `install_location/deployment`. Por ejemplo, `HumanTaskExportFile1.xml.gz`. Cópielo.
5. En el servidor de destino, importe un despliegue. Para obtener información acerca de las especificaciones de despliegue e importación, consulte: “Especificaciones de despliegue” en la página 288.
6. En el servidor de destino, pegue el archivo *nombre_archivo_exportación.xml.gz* en `install_location/deployment`.
7. En el servidor de destino, abra un indicador de comandos en `install_location/bin` y ejecute `htsDeployTool` con los argumentos siguientes:

```
htsDeployTool -persistenceUnit annotations -camUsername camUsername  
-camPassword camPassword -camNamespace camNamespace -importFile  
importFileName -password importFilePassword
```

donde

camUsername es el nombre de usuario del espacio de nombres.

camPassword es la contraseña de usuario para el espacio de nombres.

camNamespace es el nombre del espacio de nombres.

importFileName es el nombre del archivo de exportación que ha creado en el paso 3.

importFilePassword es la contraseña del archivo que ha creado en el paso 3.

Almacenamiento y creación de informes de los comentarios de IBM Cognos Workspace

En este tema se proporciona información acerca del almacenamiento y creación de informes de los comentarios de Cognos Workspace.

Almacenamiento de comentarios

Los comentarios se almacenan dentro de sus propias tablas de base de datos, que pueden ser la misma base de datos que la del almacén de contenido o bien una base de datos por separado. La propiedad Human Task and Annotation Services de IBM Cognos Configuration define la conexión de base de datos con la base de datos en la que se almacenan las tablas de anotaciones. Si no se especifica una conexión de base de datos para la propiedad Human task service and Annotation service, las tablas de anotaciones se crean en la base de datos del almacén de contenido.

La propiedad Human Task and Annotation Services también define la conexión de base de datos para las tablas de Human task service. Sin embargo, aunque Human Task Service and Annotation Service comparten una conexión de base de datos, las tablas de anotaciones y de tareas humanas están separadas. Las tablas de anotaciones tienen el prefijo ANS_ y las tablas de Human Task Service tienen el prefijo HTS_.

Los usuarios reciben scripts para exportar e importar datos de Human Task and Annotation de las tablas al servidor de IBM Cognos de destino. Los scripts facilitan la realización de actividades tales como la copia de seguridad y restauración de comentarios y el despliegue de comentarios entre servidores.

Creación de informes de comentarios

En IBM Cognos Analytics, no existe ninguna vista ni representación del modelo de IBM Cognos Framework Manager de comentarios de Cognos Workspace lista para utilizarse. Sin embargo, puede crear un modelo basado en las tablas de base de datos del servicio de anotaciones en Framework Manager. Las tablas, que son simples, pueden utilizarse para buscar el comentario o texto de la anotación, la persona que ha creado el comentario, la fecha en la que se ha creado el comentario y el informe al que se asocia el comentario. También puede crear informes del contexto de un comentario creando un modelo o consulta de informe para el esquema en el que se almacenan los comentarios. Las dimensiones, los miembros de la dimensión, los elementos de metadatos y los elementos de datos constituyen el contexto de la anotación en el informe.

Para obtener más información acerca de la creación de un informe desde la base de datos de anotaciones, puede especificar las palabras clave de búsqueda, informes de la base de datos de anotaciones, en Cognos Proven Practices (<http://www.ibm.com/developerworks/data/library/cognos/cognosprovenpractices.html>).

Capítulo 20. Paquetes

Puede crear paquetes para los orígenes de datos de SAP BW y Cognos PowerCube en IBM Cognos Administration.

Un modelador puede crear un paquete al publicar PowerCubes desde Transformer. Para obtener más información, consulte *Transformer User Guide*.

Un modelador también puede crear y publicar paquetes mediante Framework Manager. Para obtener información, consulte *Framework Manager User Guide*.

Creación de un paquete para un PowerCube

Antes de poder utilizar un origen de datos de PowerCube en cualquiera de los estudios de IBM Cognos, debe crear un paquete.

Al crear un origen de datos de PowerCube, se le da la opción de crear un paquete con el nuevo origen de datos. También puede crear un paquete para un origen de datos PowerCube existente.

Para realizar estas tareas, debe poseer permisos de ejecución para la característica protegida Conexiones con orígenes de datos.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Conexiones con orígenes de datos**.
2. Seleccione el botón **Nuevo origen de datos**.
3. Siga los pasos del **Asistente para nuevo origen de datos**.
 - En la página **Especificar la conexión**, en la lista **Tipo**, seleccione **IBM Cognos PowerCube**.
 - En la página **Finalizar**, seleccione **Crear un paquete**.

Paquetes SAP BW

Antes de poder utilizar un origen de datos de SAP BW en cualquiera de los estudios de IBM Cognos, debe crear un paquete.

Al crear un origen de datos SAP BW en IBM Cognos Administration, se le da la opción de crear un paquete con el nuevo origen de datos. También puede crear un paquete para un origen de datos SAP BW existente. Para obtener más información, consulte “Conexiones de origen de datos” en la página 146.

Para editar un paquete de SAP BW una vez creado, consulte “Edición de un paquete SAP BW” en la página 320.

Para establecer el número máximo de objetos utilizados en los paquetes de SAP BW, consulte “Establecimiento del número máximo de objetos utilizados en los paquetes de SAP BW” en la página 320.

Para realizar estas tareas, debe poseer permisos de ejecución para la característica protegida Conexiones con orígenes de datos; consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Puede establecer la cantidad de objetos que se pueden utilizar en un paquete de SAP BW. Para obtener información sobre la creación y la publicación de paquetes en Framework Manager, consulte *Framework Manager User Guide*.

Creación de un paquete SAP BW

El procedimiento para crear un paquete de SAP BW es el siguiente.

Acerca de esta tarea

Para obtener más información, consulte “Orígenes de datos SAP Business Information Warehouse (SAP BW)” en la página 138.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Conexiones con orígenes de datos**.
2. Seleccione el botón **Nuevo origen de datos**.
3. Siga los pasos del **Asistente para nuevo origen de datos**.
 - En la página **Especificar la conexión**, en la lista **Tipo**, seleccione **SAP BW**.
 - En la página **Finalizar**, seleccione **Crear un paquete**.

Edición de un paquete SAP BW

El procedimiento para editar un paquete de SAP BW es el siguiente.

Procedimiento

1. Pulse **Más** junto al paquete y después pulse **Editar paquete**.
2. Seleccione una de las opciones siguientes:
 - Para modificar las selecciones de metadatos, pulse **Modificar selecciones de metadatos**. Vuelva al paso 5 de “Creación de un paquete SAP BW”.
 - Para editar las variables del paquete, pulse **Editar variables**. Pulse el valor que desea editar y, a continuación, seleccione o escriba la variable nueva. Pulse **Aceptar**.
 - Para modificar los valores del paquete, pulse **Modificar valores del paquete** y seleccione **Utilizar modo de consulta dinámica**.

Establecimiento del número máximo de objetos utilizados en los paquetes de SAP BW

Puede establecer el número máximo de cubos y consultas de información que se pueden incluir cuando se crea un paquete de SAP BW.

Cuanto más tiempo tarde en realizarse una importación de SAP BW, más tiempo dedicará el servidor a procesar la solicitud, lo que puede tener un impacto negativo sobre el rendimiento y afectar a otras aplicaciones. Encuentre el equilibrio entre el número de cubos y las consultas de información que los usuarios necesitan normalmente y el posible impacto en el rendimiento del servidor.

Están disponibles los siguientes parámetros (con distinción entre mayúsculas y minúsculas):

- **com.ibm.cognos.metadatauiservice.sap.maxcubes**

Número máximo de cubos que se pueden utilizar en un paquete de SAP BW. Los valores válidos son 0 y valores superiores a 0. El valor predeterminado es 2.

- **com.ibm.cognos.metadatauiservice.sap.maxInfoQueries**

Número máximo de consultas de información que se pueden utilizar en un paquete de SAP BW. Los valores válidos son 0 y valores superiores a 0. El valor predeterminado es 5.

Para obtener más información acerca de los orígenes de datos SAP BW y la creación de paquetes de SAP BW, consulte: Capítulo 6, “Orígenes de datos y conexiones”, en la página 113.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Estado**, pulse **Sistema**.
2. En el panel **Tabla de puntuación**, en el menú Cambiar vista de la vista actual, pulse **Servicios > Metadatos**.

Consejo: La vista actual es **Todos los servidores**, **Todos los grupos de servidores**, **Todos los asignadores** o **Servicios**.

3. En el menú **Acciones de Servicio de metadatos**, pulse **Establecer propiedades**.
4. Pulse la pestaña **Valores**.
5. Junto a **Valores avanzados**, pulse **Editar**.
6. Seleccione **Reemplazar los valores adquiridos de la entrada padre**.
7. En la columna **Parámetro**, introduzca el nombre del parámetro.
Por ejemplo, escriba `com.ibm.cognos.metadatauiservice.sap.maxcubes`.
8. En la columna **Valor**, escriba el valor asociado a esta configuración.
9. Continúe escribiendo nombres y valores de parámetros según sea necesario.
10. Pulse **Aceptar**.
11. En la página **Establecer propiedades**, pulse **Aceptar**.

Capítulo 21. Administración de perfiles de usuario

Un perfil de usuario define las pestañas del portal a las que el usuario puede acceder y especifica las preferencias del usuario, como el idioma del producto, el formato de salida preferido de los informes y el estilo utilizado en la interfaz de usuario.

Cuando el usuario inicia sesión en el software de IBM Cognos por primera vez se crea un perfil de usuario. También puede crearlo un administrador. Inicialmente, el perfil se basa en el perfil de usuario predeterminado.

Los usuarios pueden visualizar y cambiar las preferencias asociadas con su perfil.

Para copiar, editar o suprimir perfiles de usuario, un administrador debe poseer permisos de escritura para el espacio de nombres que contiene los usuarios aplicables. El rol predefinido de IBM Cognos, **Administradores del directorio**, no posee permisos de escritura en espacios de nombres que no sean el espacio de nombres **Cognos**. Los **Administradores del sistema** deben otorgar permisos a los **Administradores del directorio** para que puedan administrar perfiles de usuario para el espacio de nombres.

Para administrar los perfiles de usuario, debe tener los permisos de acceso requeridos para **IBM Cognos Administration**.

Para obtener más información sobre la gestión de las cuentas, consulte: Capítulo 11, “Usuarios, grupos y roles”, en la página 207.

Conceptos relacionados:

Capítulo 5, “Administración del servidor”, en la página 49

La administración del servidor incluye la gestión y el mantenimiento del sistema IBM Cognos, y el ajuste del rendimiento del sistema.

Edición del perfil de usuario predeterminado

El perfil de usuario predeterminado se define en el espacio de nombres **Cognos**. Contiene valores que se aplican a todos los nuevos usuarios. Puede editar el perfil de usuario predeterminado para sus usuarios a fin de minimizar el número de cambios que es necesario hacer en los perfiles de usuario individuales.

Los cambios realizados en el perfil de usuario predeterminado se aplican solamente a los usuarios que inicien sesión en el software de IBM Cognos por primera vez. Los perfiles de usuario ya existentes no se verán afectados.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
2. Pulse el espacio de nombres **Cognos**.
3. En la barra de herramientas, pulse el botón Editar perfil de usuario predeterminado .
4. Configure el perfil de usuario predeterminado y pulse **Aceptar**.

Resultados

Cada usuario que inicie sesión en el software de IBM Cognos por primera vez heredará automáticamente esos valores, aunque los podrá cambiar posteriormente.

Visualización o modificación de un perfil de usuario

Puede ver o modificar los perfiles de usuario.

Puede suprimir elementos específicos del perfil del usuario. Esto puede resultar útil en las siguientes situaciones:

- El contenido del usuario está ocupando tanto espacio que el rendimiento se ve afectado. Desea suprimir una parte o todo el contenido.
- Desea ver un perfil de usuario antes de suprimirlo para asegurarse de que no suprime ningún contenido importante.

Si se suprimió un usuario en su proveedor de autenticación, el usuario ya no aparecerá en el software de IBM Cognos y no podrá modificar el perfil de usuario.

Sólo puede ver los perfiles de los usuarios que hayan iniciado sesión al menos una vez. Cuando los usuarios inicien sesión, se mostrará una fecha en la columna **Modificado**.

Para ver un perfil de usuario y suprimir o modificar el contenido, debe tener permisos de visita sobre la cuenta de usuario y sobre cualquier otra carpeta que tenga contenido propiedad del usuario. Debe poseer permisos de escritura sobre la entrada y el padre de la entrada que desee suprimir.

Puede cambiar el perfil de usuario para usuarios individuales, pero no para grupos o roles.

Visualización o modificación de un perfil de usuario

Puede ver o modificar el perfil de un usuario.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
2. Pulse el espacio de nombres que contenga el usuario.
3. Busque el usuario cuyas preferencias desee ver o modificar.
4. En la columna **Acciones**, pulse **Más**.
5. Pulse **Establecer preferencias**.
6. Pulse las distintas pestañas para ver o modificar los valores.
7. Pulse **Cancelar** para salir sin realizar cambios o realice los cambios y pulse **Aceptar**.

Suprimir contenido

Puede suprimir elementos específicos del perfil del usuario, como el contenido de Mis carpetas o páginas.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.

2. Seleccione el espacio de nombres que contenga el usuario.
3. Busque el usuario.
4. En la columna **Nombre**, pulse el nombre de usuario.

Sugerencia: Si el nombre del usuario no es un enlace, quiere decir que el perfil de usuario no se ha creado. Para crear el perfil, en la columna **Acciones**, pulse el botón Crear perfil de este usuario  y siga con el resto de los pasos.

Aparecerá una lista de las carpetas del usuario.

5. Pulse una carpeta para ver su contenido.
6. Pulse el elemento que desee suprimir de la carpeta y, a continuación, en el botón Suprimir de la barra de herramientas.

No puede suprimir las carpetas.

Supresión de un perfil de usuario

Puede suprimir perfiles de usuario desde el almacén de contenido.

Cuando suprima un usuario en el proveedor de autenticación, es posible que antes desee suprimir el perfil de usuario del almacén de contenido para que deje de utilizar espacio de almacenamiento.

Debe suprimir el perfil de usuario del software de IBM Cognos antes de suprimir el usuario en el espacio de nombres asociado. Una vez suprimido el usuario, la información del mismo ya no aparecerá en el software de IBM Cognos y no podrá administrar el perfil del usuario en **IBM Cognos Administration**.

Si la cuenta de usuario ya estaba suprimida del espacio de nombres asociado, puede utilizar el mantenimiento de almacén de contenido para buscar y, si lo desea, eliminar toda la información de la cuenta de usuario asociada al software de IBM Cognos.

Si un usuario con un perfil de usuario suprimido entra en el sistema, se crea una cuenta con los valores predeterminados. Si un usuario tiene iniciada una sesión mientras se está suprimiendo el perfil de usuario asociado, el pasaporte del usuario caducará y aparecerá la página de inicio de sesión.

Antes de suprimir un perfil de usuario, es posible que desee ver su contenido para asegurarse de que no suprime nada importante.

Sólo puede trabajar con perfiles de usuario que hayan iniciado una sesión al menos una vez.

Antes de empezar

Para suprimir un perfil de usuario, debe tener permisos de escritura para el objeto padre.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
2. Pulse el espacio de nombres que contenga el usuario.
3. Busque el usuario cuyo perfil de usuario desee suprimir. Puede utilizar la característica Buscar para buscar un usuario.
4. En la columna **Acciones**, pulse **Más**.

5. Pulse **Suprimir perfil de este usuario**.
6. Pulse **Aceptar**.

Copia de perfiles de usuario

Quizá desee copiar un perfil de usuario.

Copiar un perfil de usuario resulta útil en las siguientes situaciones:

- Cuando un usuario cambia de nombre y está configurando la cuenta con el nombre nuevo.
- Cuando un usuario se mueve a otro espacio de nombres o la organización cambia los espacios de nombres y debe configurar cuentas nuevas.
- Cuando crea numerosas cuentas de usuario nuevas que son parecidas.

Si prevé suprimir el usuario de origen en el proveedor de autenticación, copie la información de la cuenta del usuario antes de suprimirla. Una vez suprimido el usuario, éste ya no aparecerá en el software de IBM Cognos y no podrá copiar la información de la cuenta del usuario.

Sólo puede trabajar con perfiles de usuarios que hayan iniciado una sesión al menos una vez. Cuando los usuarios inician sesión, se muestra una fecha en la columna **Modificado** y el nombre de usuario se convierte en un enlace.

Antes de empezar

Para copiar perfiles de usuario, debe disponer de permisos de escritura en los espacios de nombres de los usuarios de origen y de destino.

Consejo: Al copiar un perfil de usuario, no se copian las credenciales de confianza.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Seguridad**, pulse **Usuarios, grupos y roles**.
2. Pulse el espacio de nombres que contenga el usuario de origen (el usuario desde el que desea realizar la copia).

Consejo: Puede seleccionar solamente los espacios de nombres a los que tiene acceso de escritura.
3. Busque el usuario de origen.
4. En la columna **Acciones** del usuario de origen, pulse **Más**.
5. En la página **Ejecutar una acción**, pulse **Copiar perfil de este usuario**.
6. En la página **Copiar perfil de usuario**, pulse **Seleccionar usuario de destino** y navegue para buscar el usuario de destino.
7. Después de seleccionar el usuario de destino, en la página **Copiar perfil de usuario**, seleccione uno o varios de los valores de perfil siguientes que desee copiar: **Preferencias**, **Pestañas del portal y contenido de las carpetas personales** o **Contenido de las carpetas personales**.
8. Si es necesario, seleccione la casilla de verificación **Suprimir perfil del usuario de origen cuando finalice la copia**.
9. Pulse **Copiar**.

Capítulo 22. Entornos de varios arrendatarios

Los entornos de varios arrendatarios constan de diversos clientes u organizaciones, denominados arrendatarios. El arrendamiento múltiple (o multiarrendamiento) es la capacidad de una aplicación de dar soporte a varios arrendamientos en un mismo despliegue. Garantiza que, en cada arrendatario, los usuarios solo pueden acceder a los datos que tienen autorización para usar. El arrendamiento múltiple puede reducir los costes de mantenimiento de las aplicaciones.

IBM Cognos Analytics proporciona prestaciones integradas de arrendamiento múltiple. Los despliegues existentes se pueden migrar de forma incremental para implementar las prestaciones de arrendamiento múltiple. Los despliegues existentes que no utilicen las prestaciones de arrendamiento múltiple no se ven afectados si el arrendamiento múltiple está habilitado.

Todos los objetos de Content Manager pueden tener un único ID de arrendatario opcional. Todos los usuarios de Cognos, incluidos los administradores, pueden tener un ID de arrendatario opcional. Los usuarios de Cognos no pueden, independientemente de las políticas de seguridad de Cognos Analytics, acceder a un objeto de Content Manager si no tienen un ID de arrendatario que se corresponda con el ID de arrendatario de objeto de Content Manager. Los objetos de Content Manager que no tienen un ID de arrendatario se consideran públicos y cualquier usuario puede acceder a ellos. Los usuarios que no tienen un ID de arrendatario pueden acceder únicamente a los objetos públicos.

Consejo: El ID de arrendatario es una cadena simple. No hay restricciones en cuanto a la longitud del ID de arrendatario; sin embargo, no debe sobrepasar los 255 caracteres, que es el límite de la columna tenantID en el esquema de base de datos.

El diagrama siguiente muestra un ejemplo de cómo las prestaciones de arrendamiento múltiple de Cognos Analytics aíslan el acceso a objetos del almacén de contenido. Los usuarios solo pueden acceder a los objetos a los que están autorizados a acceder en cada agrupación de arrendatarios.

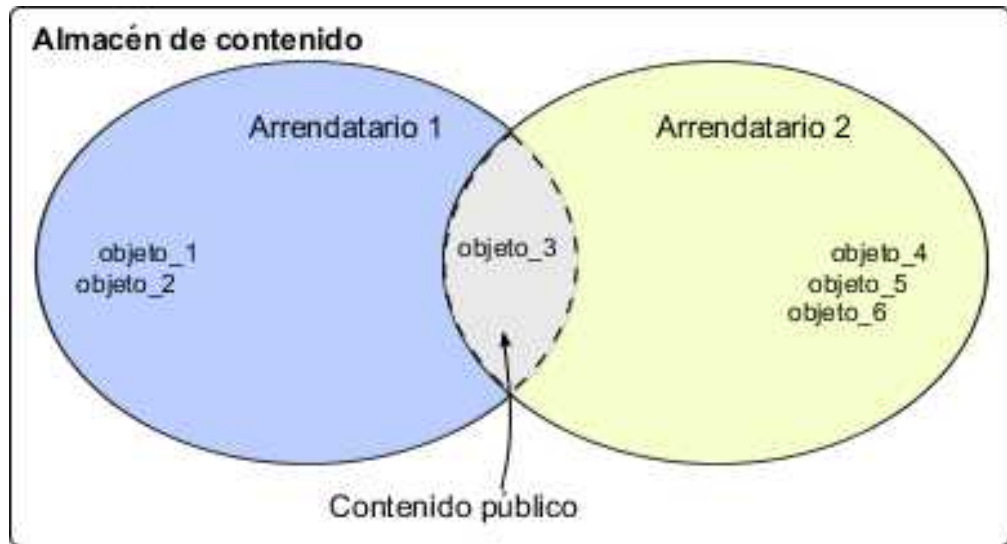


Figura 5. Almacén de contenido configurado para utilizar las prestaciones de arrendamiento múltiple de Cognos Analytics

En este ejemplo, los usuarios tienen acceso a los siguientes objetos:

- Los usuarios que pertenecen a Arrendatario 1 pueden acceder a objeto_1, objeto_2 y objeto_3.
- Los usuarios que pertenecen a Arrendatario 2 pueden acceder a objeto_3, objeto_4, objeto_5 y objeto_6.

Consejo: El administrador del sistema puede acceder a todos los objetos del almacén de contenido.

Al acceder a los objetos, el arrendamiento de objetos se evalúa antes que los permisos de acceso a objeto. Por lo tanto, los usuarios en una aplicación habilitada para el arrendamiento múltiple solo verán siempre los objetos asociados a su arrendatario y los objetos categorizados como públicos.

Después de que el múltiple arrendamiento se activa, puede registrar actividades de arrendamiento utilizando una base de datos de inicio de sesión de auditoría. IBM Cognos Analytics proporciona informes de auditoría de ejemplo que muestran cómo utilizar la información de arrendamiento para supervisar determinadas actividades de usuario. Para obtener información acerca de cómo utilizar IBM Cognos Configuration para configurar una base de datos de inicio de sesión, consulte *IBM Cognos Analytics Guía de configuración e instalación*. Para obtener información acerca de la configuración de los informes de auditoría de ejemplo, consulte https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ig_smples.doc/c_sampleauditreports.html#SampleAuditReports.

Configuración de arrendamiento múltiple

Para configurar el arrendamiento múltiple en su instalación de IBM Cognos Analytics, debe especificar las propiedades de arrendamiento múltiple en IBM Cognos Configuration.

Los valores para las propiedades de arrendamiento múltiple son diferentes para cada entorno y dependen de cómo correlacione la información de arrendamiento con los usuarios individuales del entorno.

Importante: No necesita modificar nada del proveedor de autenticación para configurar el arrendamiento múltiple.

Antes de configurar el arrendamiento múltiple en IBM Cognos Configuration, debe decidir cómo correlacionar la cuenta de usuario en el proveedor de autenticación con el arrendatario. Para este fin, puede utilizar la posición de un usuario dentro de la jerarquía de su proveedor de autenticación o las propiedades de cuenta de usuario de su proveedor de autenticación. También puede implementar un proveedor de arrendatarios personalizado. Para esta última opción, debe utilizar el kit de desarrollo de software de IBM Cognos. La elección del método de implementación idóneo para su entorno requiere una planificación minuciosa y conocimientos sobre el proveedor de autenticación.

En función de la decisión que tome sobre cómo correlacionar la cuenta de usuario con el arrendatario, elija uno de los siguientes métodos para configurar el arrendamiento múltiple.

- “Configuración de un arrendamiento múltiple basado en un nodo de jerarquía”
- “Configuración de un arrendamiento múltiple basado en un atributo de cuenta de usuario” en la página 331
- “Configuración de un arrendamiento múltiple basado en un proveedor de arrendatario personalizado” en la página 332

Puede configurar el arrendamiento múltiple globalmente, en el nivel **Autenticación** en IBM Cognos Configuration, o para espacios de nombres específicos. Las propiedades de arrendamiento múltiple de un espacio de nombres especificado reemplazan las propiedades de arrendamiento múltiple establecidas globalmente.

Configuración de un arrendamiento múltiple basado en un nodo de jerarquía

Puede reutilizar la información de estructura de nodo dentro de una jerarquía de su proveedor de autenticación al configurar el arrendatario.

Necesita correlacionar la información de jerarquía con la propiedad **Correlación de ID de arrendatario > Patrón** en IBM Cognos Configuration.

Antes de empezar

Puede utilizar el atributo de cuenta de usuario `ancestors` a este fin. El atributo `ancestors` representa la ruta jerárquica a una cuenta de usuario en forma de matriz. En la siguiente tabla se muestra cómo podría correlacionar el atributo `ancestors` a una jerarquía para identificar la información de arrendamiento:

Tabla 76. Atributo de ancestros correlacionado con la información de jerarquía

Información de ancestros	Jerarquía	Ejemplo de LDAP
<code>ancestors[0]</code>	Nodo de directorio	
<code>ancestors[1]</code>	ID de espacio de nombres	base DN

Tabla 76. Atributo de ancestros correlacionado con la información de jerarquía (continuación)

Información de ancestros	Jerarquía	Ejemplo de LDAP
ancestors[2]	Agrupación de arrendatarios, por ejemplo, una carpeta	organizational units

Por ejemplo, si los usuarios se almacenan en un directorio LDAP y los arrendatarios se encuentran directamente en el nombre distinguido (DN) base como unidades organizativas, puede establecer el tipo **Patrón** con el siguiente valor: `~/ancestors[2]/defaultName`.

Además de `defaultName`, los siguientes calificadores `ancestors` pueden devolver información de tenencia:

- `name/locale`

El parámetro de entorno local de este ejemplo se basa en la correlación de la configuración de espacio de nombres. Si no se proporciona ningún entorno local, el nombre es el título del objeto. Por ejemplo, puede especificar:

`~/ancestors[2]/name/EN-ca`

- `searchPath/objectID`

Por ejemplo, puede especificar: `~/ancestors[2]/searchPath/objectID`

Procedimiento

1. Abra IBM Cognos Configuration.
2. Elija si se configurarán los valores de arrendamiento múltiple globalmente para todos los espacios de nombres o para un espacio de nombres concreto.
 - Para configurar el arrendamiento múltiple para todos los espacios de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador.
 - Para configurar el arrendamiento múltiple para un único espacio de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador. A continuación, pulse el espacio de nombres que desea configurar.
3. En el grupo de propiedades **Arrendamiento múltiple**, pulse el botón de edición de la propiedad **Correlación de ID de arrendatario**.
4. En la ventana **Correlación de ID de arrendatario** que se muestra, especifique la correlación del siguiente modo:
 - a. En **Tipo**, seleccione **Patrón**.
 - b. En **Valor**, escriba la cadena que ha creado siguiendo las instrucciones indicadas anteriormente en este tema. Por ejemplo, puede especificar el siguiente valor: `~/ancestors[2]/defaultName`.
 - c. Pulse **Aceptar**.
5. Solo para un espacio de nombres de Active Directory, pulse la columna **Valor** de **Propiedades personalizadas** y pulse el botón de edición. Añada la propiedad `MultiDomainTree` y establezca su valor en `true`.
6. Pruebe la configuración de arrendamiento múltiple.
 - a. Pulse con el botón secundario sobre **Autenticación** o el espacio de nombres (en función de lo que haya elegido en el paso 2) y pulse **Probar**.

- b. Inicie sesión utilizando las credenciales de administrador del sistema y pulse **Aceptar**.
 - c. Pulse el botón **Detalles** y lea la información que aparece.
- Si el arrendamiento múltiple está configurado correctamente, en los detalles se muestra el ID de arrendatario. Si el ID de arrendatario no se muestra, actualice y corrija los valores; a continuación, pruebe de nuevo.
7. Si la prueba ha sido satisfactoria, en el menú **Archivo**, pulse **Guardar**.
 8. Reinicie el servicio de IBM Cognos para que los cambios entren en vigor.

Configuración de un arrendamiento múltiple basado en un atributo de cuenta de usuario

Puede designar un atributo de cuenta de usuario específico en su proveedor de autenticación para correlacionar con el arrendatario. Después de seleccionar el atributo de cuenta de usuario que desee correlacionar con el arrendatario, deberá crear una propiedad personalizada y correlacionarla con ese atributo.

Necesita correlacionar el atributo de cuenta de usuario con la propiedad **Correlación de ID de arrendatario > Patrón** en IBM Cognos Configuration.

Antes de empezar

El atributo de cuenta de usuario que elija para identificar al arrendatario del usuario solo debe utilizarse con este fin.

Por ejemplo, puede decidir que el atributo `businessUnit` de una cuenta de usuario de LDAP identifique el arrendatario del usuario. En este caso, debe establecer la propiedad de tipo **Patrón** como se indica en el ejemplo siguiente: `~/parameters/parameter_name`. A continuación, especifique una propiedad personalizada denominada `parameter_name` y asocie esta propiedad con el atributo de cuenta de usuario `businessUnit`.

Procedimiento

1. Abra IBM Cognos Configuration.
2. Elija si se configurarán los valores de arrendamiento múltiple globalmente para todos los espacios de nombres o para un espacio de nombres concreto.
 - Para configurar el arrendamiento múltiple para todos los espacios de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador.
 - Para configurar el arrendamiento múltiple para un único espacio de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador. A continuación, pulse el espacio de nombres que desea configurar.
3. En el grupo de propiedades **Arrendamiento múltiple**, pulse el botón de edición de la propiedad **Correlación de ID de arrendatario**.
4. En el campo **Correlación de ID de arrendatario** que se muestra, especifique la correlación del siguiente modo:
 - a. En **Tipo**, seleccione **Patrón**.
 - b. En **Valor**, escriba la cadena que ha creado siguiendo las instrucciones indicadas anteriormente en este tema.

Por ejemplo, escriba `~/parameters/nombre_parámetro`, donde `~/parameters` es una parte constante de la sintaxis y `nombre_parámetro` es el nombre de la propiedad personalizada.

- c. Pulse **Aceptar**.
5. En el grupo de propiedades **Correlaciones de cuenta (Avanzado)**, especifique la propiedad personalizada y correlaciónela con el atributo de cuenta del siguiente modo:
 - a. Pulse la columna **Valor** de **Propiedades personalizadas** y pulse el botón de edición.
 - b. En la ventana **Valor: Propiedades personalizadas**, pulse **Añadir**.
 - c. En la columna **Nombre**, escriba el nombre de la propiedad personalizada. En la columna **Valor**, escriba el nombre del atributo. Para el ejemplo que se utiliza en el paso 4, la propiedad personalizada debe ser: `parameter_name` para **Nombre** y `businessUnit` para **Valor**.
 - d. Pulse **Aceptar**.
6. Pruebe la configuración de arrendamiento múltiple.
 - a. Pulse con el botón secundario sobre **Autenticación** o el espacio de nombres (en función de lo que haya elegido en el paso 2) y pulse **Probar**.
 - b. Inicie sesión utilizando las credenciales de administrador del sistema y pulse **Aceptar**.
 - c. Pulse el botón **Detalles** y lea la información que aparece.

Si el arrendamiento múltiple está configurado correctamente, en los detalles se muestra el ID de arrendatario. Si el ID de arrendatario no se muestra, actualice y corrija los valores; a continuación, pruebe de nuevo.
7. Si la prueba ha sido satisfactoria, en el menú **Archivo**, pulse **Guardar**.
8. Reinicie el servicio de IBM Cognos para que los cambios entren en vigor.

Configuración de un arrendamiento múltiple basado en un proveedor de arrendatario personalizado

Puede crear una clase Java personalizada y hacer referencia a ella al configurar el arrendamiento múltiple. Puede utilizar este método cuando necesite unir datos de varios proveedores de autenticación, o desde un proveedor de autenticación y una base de datos relacional. Debe utilizar el kit de desarrollo de software de IBM Cognos para este método.

Cuando utilice este método, correlacione la propiedad **Correlación de ID de arrendatario > Clase de proveedor** de IBM Cognos Configuration con una clase Java personalizada.

Antes de empezar

Para poder configurar el arrendamiento múltiple con este método, debe llevar a cabo las siguientes tareas:

- Compile los archivos de clase Java personalizada necesarios en archivos JAR y colóquelos en el directorio `install_location/webapps/p2pd/WEB-INF/lib` con los archivos que tengan asociados, o bien actualice la variable de entorno `CLASSPATH` para que incluya la ruta a estos archivos.
- Implemente la interfaz de `ITenantProvider` utilizando IBM Cognos Custom Authentication Provider y defina la clase Java personalizada en dicha interfaz. Por ejemplo, el nombre de clase Java personalizada puede ser `com.ejemplo.clase`. Para obtener más información, consulte la publicación *IBM Cognos Software Development Kit Custom Authentication Provider Developer Guide*.

Consejo: IBM Cognos Custom Authentication Provider incluye una clase Java personalizada de ejemplo que puede utilizar. Puede encontrar los archivos de ejemplo en el directorio *install_location\sdk\java\AuthenticationProvider\MultiTenancyTenantProviderSample*.

Procedimiento

1. Abra IBM Cognos Configuration.
2. Elija si se configurarán los valores de arrendamiento múltiple globalmente para todos los espacios de nombres o para un espacio de nombres concreto.
 - Para configurar el arrendamiento múltiple para todos los espacios de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador.
 - Para configurar el arrendamiento múltiple para un único espacio de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador. A continuación, pulse el espacio de nombres que desea configurar.
3. En el grupo de propiedades **Arrendamiento múltiple**, pulse el botón de edición de la propiedad **Correlación de ID de arrendatario**.
4. En la ventana **Correlación de ID de arrendatario** que se muestra, especifique la correlación del siguiente modo:
 - a. En **Tipo**, seleccione **Clase de proveedor**.
 - b. Para **Valor**, escriba el nombre de la clase Java personalizada que se define en la interfaz `IBoundingSetProvider` que se ha implementado utilizando IBM Cognos Custom Authentication Provider. Por ejemplo, escriba `com.ejemplo.nombre_clase`.
 - c. Pulse **Aceptar**.
5. Si necesita especificar una propiedad personalizada, en el grupo de propiedades **Correlaciones de cuenta (Avanzado)**, pulse el botón de edición de la columna **Valor** de la **Propiedad personalizada** y añada el nombre de propiedad y el valor según se necesite.
6. Pruebe la configuración de arrendamiento múltiple.
 - a. Pulse con el botón secundario sobre **Autenticación** o el espacio de nombres (en función de lo que haya elegido en el paso 2) y pulse **Probar**.
 - b. Inicie sesión utilizando las credenciales de administrador del sistema y pulse **Aceptar**.
 - c. Pulse el botón **Detalles** y lea la información que aparece.

Si el arrendamiento múltiple está configurado correctamente, en los detalles se muestra el ID de arrendatario. Si el ID de arrendatario no se muestra, actualice y corrija los valores; a continuación, pruebe de nuevo.
7. Si la prueba ha sido satisfactoria, en el menú **Archivo**, pulse **Guardar**.
8. Reinicie el servicio de IBM Cognos para que los cambios entren en vigor.

Características avanzadas de arrendamiento múltiple

Las características avanzadas de arrendamiento múltiple se pueden utilizar para configurar la administración delegada de arrendatarios y el uso compartido de contenido entre arrendatarios.

Un usuario de Cognos puede tener un único ID de arrendatario asociado con la propiedad **Correlación de ID de arrendatario**. Si se define la propiedad

Correlación de ID de arrendatario, se pueden asignar ID de arrendatario adicionales a un usuario de Cognos mediante la propiedad **Correlación de conjunto delimitador de arrendatario**.

Los objetos de Content Manager pueden tener asignado como su ID de arrendatario un ID de arrendatario virtual, que puede contener varios ID de arrendatario. Esto permite a los usuarios de varios arrendatarios acceder al contenido común, como carpetas o informes.

Se pueden utilizar al mismo tiempo los ID de arrendatario virtual para los objetos de Content Manager y los diversos ID de arrendatario que se implementan para los usuarios mediante las propiedades **Correlación de ID de arrendatario** y **Correlación de conjunto delimitador de arrendatario**. Estas características se pueden utilizar para permitir a los administradores de arrendatarios administrar varios arrendatarios, lo que se conoce como administración delegada de arrendatarios; también permiten a los usuarios de Cognos acceder a objetos de Content Manager para varios arrendatarios, lo que se conoce como uso compartido del contenido entre arrendatarios.

Cuando se implementa la administración delegada de arrendatarios, el administrador del sistema puede delegar determinadas tareas, como la administración de seguridad, planificaciones, actividades y eventos de algunos arrendatarios a los miembros con el rol **Administradores de arrendatarios**. Los administradores de arrendatarios pueden administrar un conjunto de arrendatarios, tal como se define en el conjunto delimitador del administrador de arrendatarios, además de sus propios arrendatarios. El administrador del sistema conserva el control total sobre los permisos de los administradores de arrendatarios. Para obtener más información, consulte “Administración delegada de arrendatarios” en la página 342.

Cuando se implementa el uso compartido del contenido entre los arrendatarios, los usuarios pueden acceder al contenido de diferentes arrendatarios, además de su propio contenido de arrendatario. El uso compartido del contenido para los usuarios se activa con las características de arrendamiento múltiple siguientes:

- La propiedad **Correlación de conjunto delimitador de arrendatario**
Un usuario puede acceder a cualquier objeto de Content Manager cuyo ID de arrendatario esté incluido en el conjunto delimitador de arrendatario del usuario.
- ID de arrendatario virtual
A un objeto de Content Manager que tenga asignado un ID de arrendatario virtual pueden acceder los usuarios de cualquier arrendatario cuyo ID de arrendatario esté incluido en el ID de arrendatario virtual del objeto.

Para obtener más información, consulte el tema “Configuración de arrendatarios virtuales para habilitar el uso compartido del contenido entre los arrendatarios” en la página 344.

Configuración de la propiedad Correlación de conjunto delimitador de arrendatario

El conjunto delimitador de arrendatario es una propiedad que puede tener varios valores y que puede incluir diversos ID de arrendatario.

Configure esta propiedad en IBM Cognos Configuration mediante uno de estos métodos:

- “Configuración del conjunto delimitador de arrendatario basado en un atributo de cuenta de usuario”
- “Configuración del conjunto delimitador de arrendatario basado en un proveedor personalizado” en la página 336

En el conjunto delimitador habrá arrendatarios inhabilitados si el usuario es administrador del sistema. Los arrendatarios suprimidos se eliminan automáticamente del conjunto delimitador.

Puede aplicar este valor globalmente, para todos los espacios de nombres configurados o para espacios de nombres individuales. Las propiedades de arrendamiento múltiple de un espacio de nombres específico reemplazarán las propiedades de arrendamiento múltiple que establezca globalmente en el nivel **Autenticación** en IBM Cognos Configuration.

Consejo: Las propiedades **Correlación de ID de arrendatario** y **Correlación de conjunto delimitador de arrendatario** se pueden implementar de forma independiente. Por ejemplo, puede utilizar la posición de un usuario dentro de una jerarquía para determinar la propiedad **Correlación de ID de arrendatario** y utilizar un proveedor personalizado para determinar la propiedad **Correlación de conjunto delimitador de arrendatario**. Sin embargo, en la mayoría de las implementaciones, ambas propiedades deben contener unos ID de arrendatario del mismo tipo; por ejemplo, número de departamento.

Configuración del conjunto delimitador de arrendatario basado en un atributo de cuenta de usuario

Puede designar un atributo de cuenta de usuario específico en su proveedor de autenticación para correlacionar con el conjunto delimitador de arrendatario. Debe estar habilitado el arrendamiento múltiple.

Necesita correlacionar el atributo de cuenta de usuario con la propiedad **Correlación de conjunto delimitador de arrendatario** > **Patrón** en IBM Cognos Configuration.

Antes de empezar

Después de seleccionar en el proveedor de autenticación un atributo de cuenta de usuario que desea correlacionar con el conjunto delimitador de arrendatario, debe crear una propiedad personalizada y correlacionarla con el atributo de cuenta de usuario.

Puede utilizar el atributo departmentNumber de una cuenta de usuario de LDAP para identificar el conjunto delimitador del usuario. En este caso, puede establecer la propiedad **Correlación de conjunto delimitador de arrendatario**, **Patrón** como se indica en el ejemplo siguiente: ~/parameters/bounding_set. A continuación, especifique una propiedad personalizada denominada bounding_set y asocie esta propiedad con el atributo de cuenta de usuario departmentNumber

Procedimiento

1. Abra IBM Cognos Configuration.
2. Elija si se configurará este valor globalmente para todos los espacios de nombres o para un espacio de nombres concreto.
 - Para configurar este valor para todos los espacios de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador.

- Para configurar este valor para un único espacio de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador. A continuación, pulse el espacio de nombres que desea configurar.
- 3. En el grupo de propiedades **Arrendamiento múltiple**, pulse el botón de edición de la propiedad **Correlación de conjunto delimitador de arrendatario**.
- 4. En el campo **Correlación de conjunto delimitador de arrendatario** que se muestra, especifique la correlación del siguiente modo:
 - a. En **Tipo**, seleccione **Patrón**.
 - b. En **Valor**, escriba la cadena que ha creado siguiendo las instrucciones indicadas anteriormente en este tema.
Por ejemplo, escriba `~/parameters/boundingSet`, donde `~/parameters` es una parte constante de la sintaxis y `boundingSet` es el nombre de la propiedad personalizada.
 - c. Pulse **Aceptar**.
- 5. En el grupo de propiedades **Correlaciones de cuenta (Avanzado)**, especifique la propiedad personalizada y correlaciónela con el atributo de cuenta del siguiente modo:
 - a. Pulse la columna **Valor** de **Propiedades personalizadas** y pulse el botón de edición.
 - b. En la ventana **Valor: Propiedades personalizadas**, pulse **Añadir**.
 - c. En la columna **Nombre**, escriba el nombre de la propiedad personalizada. En la columna **Valor**, escriba el nombre del atributo. Para el ejemplo que se utiliza en el paso 4, la propiedad personalizada debe ser: `boundingSet` para **Nombre** y `departmentNumber` para **Valor**.
 - d. Pulse **Aceptar**.
- 6. Pruebe la configuración de arrendamiento múltiple.
 - a. Pulse con el botón secundario sobre **Autenticación** o el espacio de nombres (en función de lo que haya elegido en el paso 2) y pulse **Probar**.
 - b. Inicie sesión utilizando las credenciales de administrador del sistema y pulse **Aceptar**.
 - c. Pulse el botón **Detalles** y lea la información que aparece.
Si el valor se ha configurado de forma correcta, el valor de propiedad **Conjunto delimitador de arrendatario** se muestra en los detalles. Si este valor no se muestra, asegúrese de que sea correcto y pruebe de nuevo.
- 7. Si la prueba ha sido satisfactoria, en el menú **Archivo**, pulse **Guardar**.
- 8. Reinicie el servicio de IBM Cognos para que los cambios entren en vigor.

Configuración del conjunto delimitador de arrendatario basado en un proveedor personalizado

Puede crear una clase Java personalizada que se inicie durante el proceso de autenticación de usuario para determinar el conjunto delimitador de arrendatario. Debe utilizar el kit de desarrollo de software de IBM Cognos para este método.

Cuando utilice este método, debe correlacionar la propiedad **Correlación de conjunto delimitador de arrendatario** > **Clase de proveedor** de IBM Cognos Configuration con una clase Java personalizada.

Antes de empezar

Antes de configurar el conjunto delimitador de arrendatario mediante el uso de este método, debe llevar a cabo las siguientes tareas:

- Compile los archivos de clase Java personalizada necesarios en archivos JAR y colóquelos en el directorio *install_location/webapps/p2pd/WEB-INF/lib* con los archivos que tengan asociados, o bien actualice la variable de entorno CLASSPATH para que incluya la ruta a estos archivos.
- Implemente la interfaz IBoundingSetProvider utilizando IBM Cognos Custom Authentication Provider. En esta interfaz, defina una clase Java personalizada que podrá utilizar más tarde cuando configure la propiedad **Correlación de conjunto delimitador de arrendatario > Clase de proveedor**. Por ejemplo, el nombre puede ser *com.ejemplo.clase*. Para obtener más información, consulte la publicación *IBM Cognos Software Development Kit Custom Authentication Provider Developer Guide*.

Procedimiento

1. Abra IBM Cognos Configuration.
2. Elija si se configurará este valor globalmente para todos los espacios de nombres o para un espacio de nombres concreto.
 - Para configurar este valor para todos los espacios de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador.
 - Para configurar este valor para un único espacio de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador. A continuación, pulse el espacio de nombres que desea configurar.
3. En el grupo de propiedades **Arrendamiento múltiple**, pulse el botón de edición de la propiedad **Correlación de ID de arrendatario**.
4. En el campo **Correlación de conjunto delimitador de arrendatario** que se muestra, especifique la correlación del siguiente modo:
 - a. En **Tipo**, seleccione **Clase de proveedor**.
 - b. Para **Valor**, escriba el nombre de la clase Java que ha definido en la interfaz IBoundingSetProvider utilizando IBM Cognos Custom Authentication Provider.
 Por ejemplo, escriba *~/parameters/boundingSet*, donde *~/parameters* es una parte constante de la sintaxis y *boundingSet* es el nombre de la propiedad personalizada.
 - c. Pulse **Aceptar**.
5. Si necesita especificar una propiedad personalizada, en el grupo de propiedades **Correlaciones de cuenta (Avanzado)** lleve a cabo las siguientes acciones:
 - a. Pulse la columna **Valor** de **Propiedades personalizadas** y pulse el botón de edición.
 - b. En la ventana **Valor: Propiedades personalizadas**, pulse **Añadir**.
 - c. Especifique la propiedad **Nombre** y **Valor** según resulte necesario.
 - d. Pulse **Aceptar**.
6. Pruebe la configuración de arrendamiento múltiple.
 - a. Pulse con el botón secundario sobre **Autenticación** o el espacio de nombres (en función de lo que haya elegido en el paso 2) y pulse **Probar**.
 - b. Inicie sesión utilizando las credenciales de administrador del sistema y pulse **Aceptar**.
 - c. Pulse el botón **Detalles** y lea la información que aparece.

Si el valor se ha configurado de forma correcta, el valor de propiedad **Conjunto delimitador de arrendatario** se muestra en los detalles. Si este valor no se muestra, asegúrese de que sea correcto y pruebe de nuevo.

7. Si la prueba ha sido satisfactoria, en el menú **Archivo**, pulse **Guardar**.
8. Reinicie el servicio de IBM Cognos para que los cambios entren en vigor.

Inhabilitación del arrendamiento múltiple

Para inhabilitar el arrendamiento múltiple, debe eliminar las propiedades de autenticación de arrendamiento múltiple en todos los sistemas de Content Manager en los que se hayan configurado.

Todos los ID de arrendatario se deben eliminar de todos los objetos en el almacén de contenido. Si todos los ID de arrendatario no se eliminan después de inhabilitar el arrendamiento múltiple, el comportamiento de la aplicación podría ser impredecible.

Procedimiento

1. Abra IBM Cognos Configuration.
2. Elija si se inhabilitarán los valores de arrendamiento múltiple globalmente para todos los espacios de nombres o para un espacio de nombres concreto.
 - Para inhabilitar el arrendamiento múltiple para todos los espacios de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador.
 - Para inhabilitar el arrendamiento múltiple para un único espacio de nombres, pulse **Autenticación** en la categoría **Seguridad** en la ventana Explorador. A continuación, pulse el espacio de nombres que desea configurar.
3. En **Multiarrendamiento**, pulse el botón de edición de la propiedad **Correlación de ID de arrendatario**.

Se muestra el cuadro **Correlación de ID de arrendatario**.
4. Suprima los valores de la propiedad **Modelo** o **Clase de proveedor**.

Si se han especificado propiedades personalizadas para el espacio de nombres, deberá eliminarlas también.
5. Pruebe la configuración para comprobar si las propiedades de arrendamiento múltiple se han eliminado.
 - a. Pulse con el botón secundario sobre **Autenticación** o el espacio de nombres (en función de lo que haya elegido en el paso 2) y pulse **Probar**.
 - b. Inicie sesión utilizando las credenciales de administrador del sistema y pulse **Aceptar**.
 - c. Pulse el botón **Detalles** y lea la información que aparece.

El ID de arrendatario no debe mostrarse.
6. En el menú **Archivo**, pulse **Guardar**.
7. Reinicie el servicio de IBM Cognos.

Qué hacer a continuación

Una vez que se haya inhabilitado el arrendamiento múltiple, el administrador del sistema debe revisar y actualizar las políticas de los objetos y a continuación actualizar el arrendamiento a público.

Administración de arrendatarios

Los administradores del sistema y los administradores de arrendatarios delegados realizan las tareas de administración de arrendatarios.

Los administradores del sistema deben ser miembros del rol **Administradores del sistema** en el espacio de nombres de **Cognos**. Los administradores del sistema pueden ver y modificar todos los objetos en el almacén de contenido. También pueden delegar tareas de administración de arrendatarios a otros administradores que pertenezcan al rol **Administradores de arrendatarios** en el espacio de nombres de **Cognos**.

Los miembros del rol **Administradores del sistema** pueden realizar las tareas siguientes en un entorno de IBM Cognos Analytics de varios arrendatarios:

- Crear, cambiar y suprimir objetos de arrendatario
- Cambiar las propiedades de arrendamiento de cualquier objeto del almacén de contenido
- Mover arrendatarios
- Terminar las sesiones de los arrendatarios

La pestaña **Multiarrendamiento** de la sección **Gestionar** es el área central de la administración de arrendatarios. En esta pestaña, el administrador puede añadir nuevos arrendatarios y gestionar todos los arrendatarios registrados en el entorno de Cognos Analytics actual. Solamente los miembros del rol **Administradores del sistema** pueden acceder a la pestaña **Multiarrendamiento**.

Consejo: La pestaña **Multiarrendamiento** en IBM Cognos Administration también se puede utilizar para la administración de arrendatarios.

Reglas de contención para arrendamiento múltiple

Varios arrendatarios pueden coexistir en un único almacén de contenido. Las reglas de contención de arrendatarios mantienen la seguridad y el aislamiento entre arrendatarios. Estas reglas dictan cómo se crea el contenido y dónde se puede localizar.

Cada objeto del almacén de contenido tiene un valor de ID de arrendatario que indica a qué arrendatario pertenece el objeto. Para obtener información sobre cómo crear los ID de arrendatario, consulte “Creación de arrendatarios” en la página 340.

El ID de arrendatario de un objeto debe ser el mismo que el ID de arrendatario de su padre, a menos que el ID de arrendatario padre sea público. Si el ID de arrendatario padre es público, el ID de arrendatario del hijo se puede cambiar a cualquier valor. Para obtener más información, consulte “Establecimiento de un ID de arrendatario para un objeto público” en la página 341.

Si el usuario que ha iniciado la sesión actualmente crea un objeto, el ID de arrendatario de objeto es el mismo que el ID de arrendatario del usuario.

Los objetos de modelo y vista de modelo heredan sus ID de arrendatario del paquete. Por ejemplo, los modelos publicados en un paquete público son siempre públicos.

Los administradores del sistema pueden ejecutar una verificación de consistencia del almacén de contenido para detectar instancias de violación de las reglas de contención del arrendatario. Para obtener más información, consulte “Crear y ejecutar una verificación de consistencia del almacén de contenidos” en la página 353.

Creación de arrendatarios

Los administradores del sistema deben crear y habilitar un objeto de arrendatario antes de que los usuarios arrendatarios puedan acceder a IBM Cognos Analytics.

Antes de empezar

El arrendatario múltiple debe estar habilitado en IBM Cognos Configuration.

Acerca de esta tarea

El administrador del sistema crea el objeto de arrendatario en el componente **Gestionar** de Cognos Analytics, en la pestaña **Multiarrendamiento** y asigna un ID de arrendatario exclusivo a dicho objeto.

Los ID de arrendatario se definen en el proveedor de autenticación como LDAP, Active Directory o un proveedor de autenticación personalizado. Para obtener más información, consulte “Configuración de arrendamiento múltiple” en la página 328.

Procedimiento

1. En **Gestionar**, seleccione la pestaña **Multiarrendamiento**.
2. Seleccione el icono **Añadir un arrendatario** .
3. Especifique los parámetros **Nombre** e **ID de arrendatario**.
Asegúrese de que especifica un ID de arrendatario válido que se haya configurado previamente en el proveedor de autenticación.
Otros parámetros de esta página son opcionales.
4. Seleccione **Añadir**.

Resultados

El nombre del arrendatario se muestra en la pestaña **Arrendamiento múltiple**. De forma predeterminada, el arrendatario está inhabilitado . Puede habilitar al arrendatario después de que se haya configurado por completo.

Asignación de ID de arrendatario a contenido existente

Una vez que el arrendamiento múltiple está habilitado, el administrador del sistema asigna ID de arrendatario a los objetos de almacén de contenido existentes. Todos los objetos que pertenecen a un arrendatario tienen el mismo ID de arrendatario.

Cuando un usuario de un arrendatario específico inicia sesión en IBM Cognos Analytics, o cuando el administrador del sistema suplanta al arrendatario, el sistema busca el ID de arrendatario y filtra el contenido.

Se pueden crear los arrendatarios y se pueden asignar los ID de arrendatario utilizando SDK (Software Development Kit).

Acerca de esta tarea

En un entorno de arrendatario múltiple, todos los objetos del almacén de contenido son públicos o pertenecen a un único arrendatario. Como administrador del sistema, debe asegurarse de que los objetos existentes tengan un ID de

arrendamiento adecuado o estén pensados para continuar siendo públicos. Por ejemplo, puede asignar los ID de arrendatario al contenido de una carpeta, pero dejar que la carpeta sea pública.

Si el contenido de arrendatario no está organizado en carpetas individuales, puede crear una carpeta raíz para cada arrendatario. Esto ayuda a conservar la exclusividad de los nombres en el entorno Cognos Analytics.

También puede asignar los ID de arrendatario a objetos individuales, tales como informes, paneles de control, conexiones de servidor de datos, grupos de usuarios y roles, etc.

Procedimiento

1. Inicie sesión en IBM Cognos Analytics como administrador del sistema.
2. En **Contenido del equipo**, localice las entradas del contenedor, como carpetas o paquetes cuyos descendientes se deben asignar al mismo ID de arrendatario.
Cuando asigne los ID de arrendatario para objetos, como las conexiones de servidor de datos o grupos o roles, localice los objetos en el área adecuada de la interfaz de administración.
3. Abra el panel **Propiedades** para el objeto al que desea asignar el ID de arrendatario.
4. En la pestaña **General**, sección **Avanzada**, pulse el enlace junto a **Arrendatario**.
5. Seleccione un ID de arrendatario en la lista de ID disponibles y pulse **Aplicar**.

Resultados

El ID de arrendatario se aplica a la entrada. Si la entrada es un contener, por ejemplo, una carpeta o un paquete, el ID de arrendatario se aplica a la entrada y a sus descendientes.

El nombre del arrendatario se muestra en la pestaña **General**, sección **Avanzado**, de la página de propiedades del objeto.

Establecimiento de un ID de arrendatario para un objeto público

Puede asignar un ID de arrendatario para objetos cuyo padre es público.

Procedimiento

1. Abra el panel **Propiedades** para el objeto, tal como una conexión de servidor de datos, para el que desee especificar el ID de arrendatario.
2. En la pestaña **General**, sección **Avanzada**, seleccione el enlace junto a **Arrendatario**.
3. Elija un ID de arrendatario de la lista de ID disponibles
4. Pulse **Aplicar**.

Suplantación de un arrendatario

Como administrador del sistema o administrador de arrendatarios, puede suplantar a un arrendatario para ver el contenido e interactuar con él desde la perspectiva del arrendatario. Al suplantar a un arrendatario, puede realizar todas las tareas que este arrendatario puede realizar y permanecer conectado al sistema.

Los administradores del sistema pueden suplantar a todos los arrendatarios que están definidos en el almacén de contenido. Los administradores de arrendatarios pueden suplantar solamente a aquellos arrendatarios que pueden administrar.

Procedimiento

1. Inicie sesión en IBM Cognos Analytics como administrador del sistema o como administrador de arrendatarios. Para obtener más información, consulte “Administración de arrendatarios” en la página 338.

2. En la cabecera principal, pulse el icono **Suplantar arrendatario** .

Consejo: En IBM Cognos Administration, los administradores del sistema también pueden iniciar la suplantación de arrendatarios desde la pestaña **Arrendamiento múltiple**. En el menú desplegable **Acciones** de cualquier arrendatario, pulse **Suplantar**.

Se muestra la cabecera **Suplantación de arrendatario**.

3. En el cuadro de selección de arrendatarios, pulse el icono desplegable y seleccione el arrendatario al que desea suplantar.

El nombre del arrendatario se muestra en el cuadro de selección. Si la casilla de verificación **Mostrar solo contenido del arrendatario** está seleccionada (que es el valor predeterminado), los administradores del sistema o los administradores de arrendatarios solamente pueden ver el contenido asociado con el arrendatario seleccionado. Si la casilla de verificación **Mostrar solo contenido del arrendatario** no está seleccionada, los administradores del sistema pueden ver el contenido de todos los arrendatarios del almacén de contenido y los administradores de arrendatarios pueden ver el contenido de todos los arrendatarios que pueden administrar.

4. Realice las tareas que tenía planificadas para el arrendatario seleccionado.
Si desea modificar o crear contenido de otro arrendatario, seleccione el arrendatario en el cuadro de selección.

5. Pulse el icono **Cerrar**  en la cabecera **Suplantación de arrendatario** para finalizar la sesión de suplantación de arrendatario.

Administración delegada de arrendatarios

Los administradores del sistema pueden delegar tareas de administración de arrendatarios a los miembros del rol **Administradores de arrendatarios**.

Si la propiedad **Correlación de conjunto delimitador de arrendatario** está configurada, los **administradores de arrendatarios** pueden acceder solamente a los arrendatarios que estén definidos en su conjunto delimitador correspondiente. También están limitados por las políticas de seguridad de Cognos Analytics que los administradores del sistema asignen al contenido. En estas circunstancias, los **administradores de arrendatarios** se consideran administradores de arrendatarios limitados.

Si la propiedad **Correlación de conjunto delimitador de arrendatario** no está configurada, los **administradores de arrendatarios** omiten la comprobación de arrendamiento y están limitados solamente por las políticas de seguridad de Cognos Analytics que los administradores del sistema asignen al contenido. En estas circunstancias, los **administradores de arrendatarios** se consideran administradores de arrendatarios sin límites.

Para obtener más información acerca de la propiedad **Correlación del conjunto delimitador de arrendatario**, consulte las Características de arrendamiento múltiple avanzadas en la *IBM Cognos Analytics Guía de administración y seguridad*.

Los **Administradores de arrendatarios** pueden realizar las tareas de administración de arrendatario que les asigna el sistema.

Los **Administradores de arrendatarios** no pueden realizar las siguientes tareas:

- Acceder a la pestaña **Multiarrendamiento** en **Gestionar** y en IBM Cognos Administration.
- Crear, eliminar, desplegar e inhabilitar arrendatarios
- Gestionar perfiles de usuario arrendatarioTerminar las sesiones de usuario y personalizar los arrendatarios.
- Cambiar el arrendamiento de cualquier objeto del almacén de contenido
- Realizar tareas de administración de servidores, como el ajuste y la ejecución de tareas de utilización y verificaciones de consistencia del almacén de contenido.

Consejo: El rol de **Administradores de arrendatarios** es una de las entradas incluidas en el Espacio de nombres de Cognos.

Para obtener información acerca del rol **Administradores del sistema** en un entorno de varios arrendatarios, consulte: “Administración de arrendatarios” en la página 338.

Configuración del rol Administradores de arrendatarios

En el almacén de contenido inicial, el rol **Administradores de arrendatarios** no tiene ningún miembro; solamente los **administradores del sistema** tienen permiso de acceso sobre este rol. Los administradores del sistema deben añadir miembros y cambiar los permisos de acceso iniciales de este rol para utilizarlo en la administración delegada de arrendatarios.

Acerca de esta tarea

Al añadir miembros al rol **Administradores de arrendatarios**, seleccione los usuarios, los grupos o los roles de los arrendatarios pertinentes.

Procedimiento

Utilice el procedimiento siguiente para añadir o eliminar miembros del rol **Administradores de arrendatarios**.

1. Inicie sesión en IBM Cognos Analytics como un administrador del sistema que sea miembro del rol **Administradores del sistema**.
2. En **Gestionar > Cuentas > Espacios de nombres**, seleccione el espacio de nombres **Cognos**.
3. En la lista de entradas, localice el rol de **Administradores de arrendatarios** y en su menú contextual , pulse **Ver miembros**.
4. En la pestaña **Miembros**, seleccione el icono para añadir miembros  y explore la jerarquía de su espacio de nombres de seguridad para seleccionar los usuarios, grupos o roles que desea que sean miembros de este rol.

Resultados

Después de añadir los usuarios, grupos o roles pertinentes al rol **Administradores de arrendatarios**, puede utilizar este rol para configurar las políticas de seguridad y las prestaciones de los objetos del almacén de contenido.

Para obtener información sobre cómo establecer los permisos de acceso, consulte: “Establecimiento de permisos de acceso para una entrada” en la página 220. Para obtener información sobre cómo establecer las prestaciones, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227.

Configuración de arrendatarios virtuales para habilitar el uso compartido del contenido entre los arrendatarios

Cuando se configuran arrendatarios virtuales, los usuarios que pertenecen a diferentes arrendatarios pueden acceder a los objetos del almacén de contenido.

Los arrendatarios virtuales incluyen los arrendatarios reales que ya están configurados en Cognos Analytics.

Antes de empezar

El arrendamiento múltiple está habilitado para IBM Cognos Analytics y los arrendatarios se crean en **Gestionar > Multiarrendamiento**. Para obtener más información, consulte “Creación de arrendatarios” en la página 340.

Acerca de esta tarea

Las entradas de los arrendatarios virtuales y los reales se ven de forma idéntica en la pestaña **Multiarrendamiento**. Para que resulte más fácil identificar a los arrendatarios virtuales, utilice nombres descriptivos cuando los cree y especifique descripciones.

Por ejemplo, desea configurar el uso compartido de contenido para los arrendatarios denominados América del Norte, América Central y América del Sur. Crea un arrendatario virtual llamado América y le añade los tres arrendatarios. Los usuarios que pertenezcan a cualquiera de los tres arrendatarios pueden acceder al contenido de su propio arrendatario, al contenido de los otros dos arrendatarios y al contenido público.

Si suprime un arrendatario virtual, también se suprime todo el contenido asociado con él.

Para obtener más información, consulte Características de arrendamiento múltiple avanzadas (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_config_mt_advanced.html).

Procedimiento

Realice los siguientes pasos para crear un arrendatario virtual y una carpeta para el contenido del arrendatario virtual.

1. Inicie sesión en IBM Cognos Analytics como miembro del rol **Administradores del sistema**.
2. En **Gestionar**, seleccione la pestaña **Multiarrendamiento**.
3. Seleccione el icono **Añadir un arrendatario** .

4. Especifique los parámetros **Nombre** e **ID de arrendatario**.
No es necesario que el ID de arrendatario virtual esté configurado previamente. Puede ser cualquier valor.
Para obtener una descripción, escriba una serie, tal como Arrendatario virtual, que le ayude a identificar al arrendatario entre los demás arrendatarios de Cognos Analytics.
5. Seleccione **Añadir**. El nombre del arrendatario virtual se muestra en la lista de arrendatarios y el arrendatario está inhabilitado de forma predeterminada. Puede habilitar el arrendatario después de finalizar su configuración.
6. Para el arrendatario virtual que ha creado, desde su menú contextual, , seleccione **Ver miembros**.
7. En la pestaña **Miembros**, seleccione el icono para añadir miembros .
8. Seleccione los arrendatarios que desee añadir al arrendatario virtual y pulse **Añadir**.

Consejo: Puede añadir arrendatarios inhabilitados. Sin embargo, los usuarios no podrán acceder al contenido de los arrendatarios inhabilitados hasta que se habiliten.

9. Cree una nueva carpeta. El nombre de la carpeta debería ser parecido al nombre del arrendatario virtual para que la identificación resulte más fácil.
10. En la página de propiedades de la carpeta, en la pestaña **General**, sección **Avanzado**, cambie el valor de **ID de arrendatario** por el ID de arrendatario del arrendatario virtual seleccionando el ID de la lista de los ID disponibles. Por ejemplo, si el ID de arrendatario virtual es América, seleccione este ID en la lista y asígnelo a la carpeta.

Visualización del nombre de arrendatario en la interfaz de usuario de Cognos Analytics

Puede especificar si los usuarios sin permisos administrativos pueden ver el nombre del arrendatario en la interfaz de usuario de Cognos Analytics.

De forma predeterminada, solo los administradores del sistema y los administradores de arrendatarios pueden ver el nombre de arrendatario asociado con los objetos. Si desea que los usuarios no administrativos tengan el mismo privilegio, cambie el valor avanzado **portal.showTenantInfoForAllUsers** correspondiente al servicio de presentación por true.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para el servicio de presentación, especifique la propiedad **portal.showTenantInfoForAllUsers** y asígnele el valor true.

Administrar perfiles de usuario arrendatario

Cada arrendatario puede tener su propio perfil de usuario predeterminado que se comparte por parte de los usuarios arrendatarios.

Acerca de esta tarea

El administrador del sistema crea el perfil de usuario del arrendatario. Este perfil se basa en el perfil de usuario predeterminado que se define en el espacio de

nombre **Cognos**. El perfil de usuario predeterminado se puede cambiar para que sea relevante para el arrendatario. Por ejemplo, el perfil puede reflejar el idioma del producto, pestañas del portal y el estilo de la interfaz del usuario de IBM Cognos asociada con el arrendatario.

Cuando un usuario arrendatario inicia sesión en el software de IBM Cognos por primera vez, el perfil del usuario se crea automáticamente para el usuario. El perfil se basa en el perfil de usuario del arrendatario, si existe uno. Si un perfil de arrendatario no existe, el perfil de usuario predeterminado se aplica al usuario.

Los administradores del sistema pueden modificar o suprimir el perfil de usuario arrendatario. El perfil también se puede implementar con otros objetos de arrendatarios del entorno de origen al entorno de destino. Al implementar al arrendatario, aplican las mismas reglas de resolución de conflicto a los perfiles de usuario de arrendatario como otros objetos de arrendatario.

Para obtener más información acerca de los perfiles del usuario en IBM Cognos Analytics, consulte Capítulo 21, “Administración de perfiles de usuario”, en la página 323.

Procedimiento

1. En **IBM Cognos Administration**, pulse la pestaña **Arrendatarios múltiples**.
2. Elija la acción aplicable:
 - Para crear el perfil del usuario para uno o más arrendatarios, seleccione las casillas de verificación de arrendatario y pulse el icono **Editar perfil de usuario predeterminado**  en la barra de herramientas. Si es necesario, haga cambios en las pestañas diferentes.
 - Para cambiar un perfil de usuario existente para un arrendatario, desde el menú desplegable **Acciones** del arrendatario, haga clic en **Editar perfil de usuario del arrendatario** y haga los cambios requeridos en las diferentes pestañas.
 - Para suprimir el perfil del usuario para uno o más arrendatarios, seleccione las casillas de verificación del arrendatario y haga clic en el icono **Suprimir perfil del usuario arrendatario** en la barra de herramientas. Para suprimir el perfil del usuario para un arrendatario, desde el menú desplegable **Acciones**, haga clic en **Suprimir perfil del usuario arrendatario**.

Despliegue de contenido de arrendatario

Puede exportar e importar el contenido de arrendatarios.

El contenido de arrendatarios se puede implementar solo o con el contenido público. El contenido público también se puede implementar por sí mismo.

Para obtener información sobre el despliegue en IBM Cognos Analytics, consulte Capítulo 19, “Despliegue”, en la página 287.

Exportación de contenido de arrendatarios a un archivo de implementación

Puede exportar el contenido de arrendatario desde el entorno de origen en un archivo de despliegue. Más adelante, puede importar el archivo al entorno de destino.

Antes de empezar

Solo se exporta contenido público y objetos que pertenecen a los arrendatarios seleccionados. Antes de iniciar la exportación, debe completar la asignación de arrendamiento en el almacén de contenido.

Acerca de esta tarea

Puede exportar el contenido de la siguiente manera:

- El contenido que pertenece a los arrendatarios seleccionados y el contenido público
- El contenido que pertenece solo a los arrendatarios seleccionados.
- Solo contenido público

Información de la cuenta del usuario, incluyendo cuentas de usuarios públicos, se pueden incluir o excluir de la exportación. Al exportar arrendatarios con contenido público incluido, la información de la cuenta de usuario público también se incluye de manera predeterminada. Si desea excluir la información de cuenta pública de este tipo de exportación, utilice la configuración avanzada

CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS. Para obtener más información, consulte “Excluir información de cuenta de usuario público al implementar contenido público” en la página 350.

Cuando se excluye el contenido público de la exportación de arrendatarios y un objeto de arrendatarios tiene ancestros públicos, los ancestros públicos se incluyen en la exportación de manera que las referencias de contenido se puedan conservar en el sistema de destino. Por ejemplo, en una situación donde la conexión de la fuente de datos pertenece a un arrendatario, pero la fuente de datos en sí es pública, se exporta la fuente de datos.

Procedimiento

1. En **IBM Cognos Administration**, pulse la pestaña **Arrendatarios múltiples**.
2. Pulse el icono **Nueva exportación**  en la barra de herramientas. Se abrirá el asistente **Nueva exportación**.
3. Escriba un nombre exclusivo, y una descripción y sugerencia opcionales para la especificación de despliegue. Seleccione la carpeta en la que desee guardarla y pulse **Siguiente**.
4. En la página **Elegir un método de implementación**, seleccione **Seleccionar arrendatarios**. Si aplica, seleccione la casilla de verificación **Incluir información de la cuenta del usuario** también y haga clic en **Siguiente**.
5. En la página **Seleccionar arrendatarios**, realice los pasos siguientes:
 - a. Con los iconos de flechas, mueva los arrendatarios aplicables del cuadro **Disponible** al cuadro **Seleccionado**. Asegúrese de que los nombres correctos de arrendatarios están en el cuadro **Seleccionado**.

Importante: Al exportar solo contenido público, el cuadro **Seleccionado** debe estar vacío.

- b. Si desea incluir contenido público en la exportación, seleccione la casilla de verificación **Incluir contenido público**.
- c. Elija una de las opciones **Resolución de conflictos**. Estas opciones se utilizan cuando el archivo de implementación se importa al entorno de destino. La opción **Reemplazar entradas existentes** reemplace objetos en el entorno de destino con objetos en el archivo de implementación. La opción

Mantener entradas existentes combina objetos del archivo de implementación con objetos asociados en el entorno de destino.

d. Pulse **Siguiente**.

6. En la página **Especificar un archivo de despliegue**, en **Archivo de despliegue**, seleccione un archivo de despliegue existente en la lista o bien escriba un nuevo nombre para crear uno.

Si escribe un nuevo nombre para el archivo de despliegue, el nombre no deberá contener espacios en blanco. Si el nombre de la especificación de despliegue nueva coincide con el nombre del archivo de despliegue existente, se añadirán los caracteres **_#** al final del nombre, donde **#** es un número como 1.

7. En **Cifrado**, pulse **Establecer la contraseña de cifrado**, escriba la contraseña y pulse **Aceptar**.
8. Revise la información de resumen y pulse **Siguiente**. Si desea cambiar la información, haga clic en **Atrás** y siga las instrucciones.
9. Decida lo que debe hacer con la especificación de implementación:
 - a. Para ejecutarla ahora o después, haga clic en **Guardar y ejecutar una vez** y haga clic en **Finalizar**. Especifique la hora y la fecha de la ejecución. A continuación, pulse en **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - b. Para planificarlo a una hora recurrente, haga clic en **Guardar y programar** y haga clic en **Finalizar**. A continuación, seleccione la frecuencia y las fechas de comienzo y de final. A continuación, pulse **Aceptar**.

Consejo: Para inhabilitar temporalmente la planificación, seleccione la casilla de verificación **Inhabilitar la planificación**.

- c. Para guardar sin programar o ejecutar, haga clic en **Guardar solamente** y haga clic en **Finalizar**.

Resultados

La especificación de implementación se guarda en IBM Cognos Administration, en la pestaña **Configuración**, en **Administración de contenido**. Desde esta ubicación, puede actualizar y ejecutar la especificación de implementación y mover el archivo de implementación a un almacén de contenido diferente.

Importación de contenido de arrendatarios a un entorno de destino

El contenido de arrendatarios se puede importar desde el archivo de implementación al entorno de destino.

Acerca de esta tarea

Cuando importa desde el archivo de implementación, selecciona de entradas que se exportaron. Si se ha incluido la información de la cuenta del usuario con el contenido público, puede guardar esta información o excluirla.

Cuando importa el contenido, puede reemplazar el contenido en el entorno de destino con el contenido del archivo de implementación.

No se sustituye todo el contenido de arrendatario en el entorno de destino, pero se sustituye el contenido del entorno de destino que esté en conflicto con el contenido del archivo.

Algunas entradas en el almacén de contenido de destino pueden contener referencias a contenido público que se ha excluido de la implementación del arrendatario. Si el contenido público no está en el almacén de contenido de destino, esto resulta en referencias divididas entre las entradas. Los administradores reciben una notificación sobre las referencias divididas a través de los detalles de implementación. Para reparar las referencias divididas, puede implementar el contenido público por separado o volver a exportar el contenido de arrendatarios con el contenido público incluido.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Administración de contenidos**.
2. En la barra de herramientas, haga clic en el icono Nueva importación . Aparecerá el asistente para **Nueva importación**.
3. En la sección **Archivo de implementación**, seleccione el archivo de implementación que desea importar.
4. Escriba la contraseña que se utilizó para cifrar el archivo y pulse **Aceptar**.
5. Escriba un nombre exclusivo, una descripción opcional y una sugerencia para la especificación de despliegue, seleccione la carpeta en la que desea guardarla y pulse **Siguiente**.
6. Verifique que el ID del arrendatario es correcto.
7. Si la información de cuenta del usuario se incluye con el contenido público en el archivo de implementación, puede decidir incluir o excluir esta información ahora al seleccionar o desmarcar la casilla de verificación **Incluir información de la cuenta del usuario**. Esta selección no está disponible cuando la información de la cuenta del usuario no se incluye en el archivo.
8. Elija una de las opciones **Resolución de conflictos**. La opción **Reemplazar entradas existentes** reemplaza objetos en el entorno de destino con objetos en el archivo de implementación. La opción **Mantener entradas existentes** combina objetos del archivo de implementación con objetos asociados en el entorno de destino.
9. Pulse **Siguiente**.
10. Revise la información de resumen y pulse **Siguiente**.
11. Decida qué hacer con la especificación de implementación de importación:
 - Para ejecutarla ahora o después, haga clic en **Guardar y ejecutar una vez** y haga clic en **Finalizar**. Especifique la hora y la fecha de la ejecución. A continuación, pulse **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - Para planificarlo a una hora recurrente, haga clic en **Guardar y programar** y haga clic en **Finalizar**. A continuación, seleccione la frecuencia y las fechas de inicio y finalización y haga clic en **Aceptar**.

Consejo: Para inhabilitar temporalmente la planificación, seleccione la casilla de verificación **Inhabilitar la planificación**. Para visualizar el estado de la planificación, consulte “Gestión de actividades planificadas” en la página 269.

- Para guardarlo sin planificar o ejecutar, haga clic en **Solo guardar** y haga clic en **Finalizar**.

Cuando ejecute la importación, tendrá la opción de seleccionar para actualizar la especificación de informe. Si decide no actualizar la especificación de despliegue en este momento, lo puede hacer más tarde. Para obtener más información, consulte “Actualización de las

especificaciones de informes” en la página 312. También tiene la opción de seleccionar el ID de almacén. Elija **Asignar nuevos ID durante la importación**.

12. Cuando ejecute la importación, tendrá la opción de seleccionar para actualizar la especificación de informe. Si decide no actualizar la especificación de despliegue en este momento, lo puede hacer más tarde. Para obtener más información, consulte “Actualización de las especificaciones de informes” en la página 312. también tiene la opción de seleccionar **ID de almacén**. Cuando ejecuta una importación, los ID de almacén de contenido se suprimen y se asignan nuevos ID. Si el ID de almacén de contenido se debe retener, puede elegir conservarlo. Para obtener más información, consulte “Asignación de ID de contenido” en la página 313.

Resultados

La especificación de implementación de importación se guarda en IBM Cognos Administration, en la pestaña **Configuración**, en **Administración de contenido**. Desde esta ubicación puede actualizar y ejecutar la especificación de implementación.

Excluir información de cuenta de usuario público al implementar contenido público

En el software IBM Cognos versión 10.2.0 no hubo opción para excluir la información de la cuenta del usuario cuando se implementó el contenido público. Esta opción existe en el producto a partir de la versión 10.2.1.

Acerca de esta tarea

Al exportar arrendatarios de Gestor de contenido 10.2.0, antes de actualizar el Gestor de contenido a la versión 10.2.1, es posible que aún tenga un gran número de cuentas de usuarios sin ID de arrendatarios. Si desea excluir esas cuentas de su despliegue, utilice el valor avanzado

CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para servicios específicos” en la página 515.
2. Para **ContentManagerService**, escriba el siguiente nombre de parámetro:
CM.TENANTS_DEPLOYMENT_EXCLUDE_PUBLIC_USER_ACCOUNTS.
3. Escriba **true** como un valor para este parámetro y haga clic en **Aceptar**.

Terminación de las sesiones de usuario activo para arrendatarios

Debe terminar las sesiones de usuarios activos de arrendatario antes de borrar a un arrendatario o antes de realizar algunas operaciones de mantenimiento de arrendatarios.

Antes de empezar

Antes de terminar sus sesiones de usuario activo, inhabilite el arrendatario para que las sesiones de usuarios nuevos no se puedan iniciar. Para obtener más información, consulte: “Inhabilitar y habilitar arrendatarios” en la página 351.

Acerca de esta tarea

Utilice esta acción para terminar todas las sesiones de usuarios activos para los arrendatarios especificados. El acceso para todos los arrendatarios no está afectado.

Procedimiento

1. En **Gestionar > Multiarrendamiento**, localice el arrendatario adecuado.
2. En el menú contextual del arrendatario , pulse **Terminar sesiones**.

Resultados

Se muestra un mensaje que especifica el número de sesiones de usuario finalizadas.

Inhabilitar y habilitar arrendatarios

Puede inhabilitar un arrendatario cuando desea prevenir el acceso de los usuarios a IBM Cognos Analytics y modificar el contenido del arrendatario.

Acerca de esta tarea

De forma predeterminada, un arrendatario recién creado está inhabilitado y deberá habilitarlo una vez configurado.

Debe inhabilitar un arrendatario antes de desplegar el arrendatario y su contenido. Para obtener más información, consulte Despliegue del contenido del arrendatario (www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_mt_deployment.html).

Como método recomendado, también debe inhabilitar el arrendatario antes de finalizar sus sesiones de usuario activas. Para obtener más información, consulte: “Terminación de las sesiones de usuario activo para arrendatarios” en la página 350.

Procedimiento

1. En **Gestionar > Multiarrendamiento**, localice el arrendatario que requiera.
2. En el menú contextual del arrendatario , pulse **Inhabilitar**.
Se añade un icono que indica el estado de inhabilitado al icono del arrendatario



Puede habilitar el arrendatario seleccionando **Habilitar**.

Supresión de arrendatarios

Puede suprimir un arrendatario de IBM Cognos Analytics. Esto puede ser necesario si el arrendatario se ha movido permanentemente a una instancia diferente de IBM Cognos Analytics.

Antes de empezar

Antes de suprimir un arrendatario, debe terminar las sesiones de usuarios activas arrendatarios. De otra manera, no podrá suprimir el arrendatario. Para obtener más información, consulte: “Terminación de las sesiones de usuario activo para arrendatarios” en la página 350.

Acerca de esta tarea

Cuando elimina un arrendatario, también elimina todo el contenido asociado con el arrendatario, como los informes o paneles de control.

Procedimiento

1. En **Gestionar > Multiarrendatario**, localice el arrendatario que desee suprimir.
2. En el menú contextual del arrendatario , pulse **Suprimir**.

Crear y ejecutar las tareas de utilización del almacén de contenido

Las tareas de utilización del almacén de contenido proporcionan una perspectiva del uso del almacén de contenidos.

Puede determinar cuántas instancias de cada tipo de objeto los usuarios de sus arrendatarios tienen en el almacén de contenidos y la cantidad de espacio que esas instancias ocupan. También puede determinar información más detallada, como el tamaño de cada objeto.

Acerca de esta tarea

Esta información se puede utilizar con fines de facturación y aprovisionamiento. Por ejemplo, las decisiones de facturación se pueden basar en el conteo de instancia de tipos de objetos específicos, como informes. Las decisiones de aprovisionamiento se pueden realizar al determinar qué arrendatarios se deben mover a una instancia diferente de IBM Cognos debido a la cantidad de espacio que utilizan.

Después de crear las tareas de utilización del almacén de contenidos, puede ejecutarlas a solicitud, a la hora programada o basándose en un activador. Los archivos .csv resultantes se pueden utilizar como fuentes de datos para crear informes en IBM Cognos Analytics.

Procedimiento

1. En **IBM Cognos Administration**, pulse la pestaña **Arrendatarios múltiples**.
2. Haga clic en el icono crear utilización de contenido  en la barra de herramientas.
3. Especifique el nombre de la tarea y opcionalmente una descripción y sugerencia en pantalla.
4. Para la propiedad de **Arrendatario**, pulse **Establecer** para seleccionar el ID del arrendatario que desea asociar con esta tarea. Si no selecciona el arrendatario en este punto, la tarea se creará con el ID de arrendatario de sesión actual.
5. Seleccione el arrendatario o arrendatarios que desea incluir en esta tarea de utilización de contenido al utilizar los iconos de flechas para mover los arrendatarios del cuadro **Disponible** al cuadro **Seleccionado**.
6. En la sección **Opciones**, especifique cómo guardar la información en los archivos de registro después de ejecutar esta tarea:
 - Bajo **Archivo**, si selecciona **Uno para todos los arrendatarios**, la información para todos los arrendatarios se guarda en un solo archivo. Si selecciona **Uno por arrendatario**, la información para cada arrendatario se guarda en un archivo separado.

- Bajo **Granularidad**, si selecciona **Por tipo de objeto y arrendatario**, un resumen de información de alto nivel de cada arrendatario se guarda. El resumen incluye un conteo de instancias y el tamaño total de cada tipo de objeto en el almacén de contenido agrupado por arrendatario. Si selecciona **Todos los objetos**, se guarda un resumen de información detallado acerca de cada objeto en el almacén de contenidos. El resumen incluye el ID de arrendatario de objeto, nombre, ID de almacén, ID de almacén principal y tamaño.
7. Elija cómo ejecutar la tarea:
- Para ejecutar la tarea ahora o más adelante, pulse **Guardar y ejecutar una vez**. Especifique la hora y fecha para la ejecución y pulse **Ejecutar**.
 - Para programar la tarea a una hora recurrente, pulse **Guardar y programar**. Entonces, seleccione la frecuencia, fecha de inicio y finalización, y pulse **Aceptar**.
- Consejo:** Para inhabilitar temporalmente la planificación, seleccione la casilla de verificación **Inhabilitar la planificación**. Para visualizar el estado de la planificación, consulte “Gestión de actividades planificadas” en la página 269.
- Para guardar la tarea sin programar o ejecutar, pulse **Solo guardar**.

Resultados

La nueva tarea aparece en la pestaña **Configuración**, en **Administración de contenido**. Puede modificar o ejecutar la tarea más adelante.

Los archivos de registro que resultan de ejecutar las tareas de utilización del almacén de contenidos se guardan en el directorio registros que se especifica en la configuración de IBM Cognos con los siguientes nombres:

- `cmUtilization_date_stamp.csv` cuando se ha utilizado la opción **Uno para todos los arrendatarios**.
- `cmUtilization_date_stamp_tenant_ID.csv` cuando se ha utilizado la opción **Uno por arrendatario**.

Crear y ejecutar una verificación de consistencia del almacén de contenidos

Puede ejecutar una verificación de consistencia para detectar instancias de objetos que violan las reglas de restricción para los arrendatarios múltiples. El contenido que no sigue las reglas de restricción de arrendatarios posiblemente no serán accesibles para los usuarios previstos o posiblemente no se seleccionarán cuando el arrendatario al que pertenece se elimina.

Las reglas de restricción de arrendatarios requieren que el ID del arrendatario de un objeto sea el mismo que el ID del arrendatario de su principal, a menos que el ID del arrendatario principal sea público. Para obtener más información, consulte “Reglas de contención para arrendamiento múltiple” en la página 339.

Antes de empezar

Haga una copia de seguridad del almacén de contenidos antes de ejecutar una verificación de consistencia del almacén de contenidos.

Acerca de esta tarea

Instancias en las que el objeto viola las reglas de restricción de arrendatario se resuelven automáticamente si utiliza la opción **Buscar y reparar** al ejecutar la tarea de verificación de consistencia del almacén de contenidos. Las inconsistencias relacionadas con los arrendatarios se reparan al asignar el ID del arrendatario principal al objeto secundario que ocasiona el error. No necesita iniciar el servicio IBM Cognos para reparar estos tipos de errores. Sin embargo, otros tipos de inconsistencias del almacén de contenidos no se reparan hasta que se inicia el servicio IBM Cognos. Un resumen de cada reparación se crea bajo el historial de ejecución de la tarea.

Si desea revisar y resolver manualmente las instancias de las reglas de restricción de arrendatarios puede utilizar la opción **Buscar solo** al ejecutar la verificación de consistencia del almacén de contenidos. Se crea un resumen de cada error bajo el historial de ejecución de la tarea, asumiendo que el usuario que ejecuta la tarea es un administrador del sistema. Esta opción puede ser más segura ya que le da el tiempo para investigar cada objeto individualmente y asignar el ID de arrendatario correcto al objeto.

Procedimiento

1. En IBM Cognos Administration, en la pestaña **Configuración**, pulse **Administración del contenido**.
2. Pulse el icono de mantenimiento de nuevo contenido  en la barra de herramientas y luego pulse **Verificación de consistencia**.
3. Escriba el nombre de la tarea y opcionalmente una descripción y sugerencia en pantalla.
4. Pulse **Referencias internas** para verificar si el almacén de contenidos tiene inconsistencias.
5. Elija cómo ejecutar la tarea:
 - Para ejecutar la tarea ahora o más adelante, pulse **Guardar y ejecutar una vez**. Especifique la hora y la fecha de la ejecución. Pulse **Buscar** o en **Buscar y corregir** y, a continuación, en **Ejecutar**. Revise la hora de ejecución y pulse **Aceptar**.
 - Para programar la tarea a una hora recurrente, pulse **Guardar y programar**. Seleccione la frecuencia y las fechas de inicio y finalización. Pulse **Buscar** o en **Buscar y corregir** y, a continuación, en **Aceptar**.
 - Para guardar la tarea sin programar o ejecutar, pulse **Solo guardar**.

Resultados

La nueva tarea aparece en la pestaña **Configuración**, bajo **Administración de contenido**. Puede modificar o ejecutar la tarea más adelante. Para obtener más información acerca del uso de estos tipos de tareas en un entorno de IBM Cognos, consulte “Tareas de mantenimiento del almacén de contenido” en la página 71.

Acceso a actividades interactivas en un entorno de inquilinos múltiples

El contenido de actividades interactivas en IBM Cognos Analytics no se filtra por ID de arrendatario. Por lo tanto, se requieren medidas adicionales para restringir el acceso a las actividades interactivas para los usuarios.

El contenido de las actividades en segundo plano se filtra por el ID de inquilino de manera que todos los usuarios puedan ver estas actividades.

Se puede acceder a las actividades en segundo plano y las actividades interactivas en **Mis actividades y planificaciones**. Los administradores pueden ver también las actividades en la pestaña **Estado** en IBM Cognos Administration. Para obtener más información, consulte Capítulo 17, “Gestión de actividades”, en la página 263.

Restricción del acceso a actividades interactivas para los usuarios

Para evitar el riesgo de exponer el contenido de inquilino a usuarios a los que no está destinado, los administradores del sistema pueden restringir el acceso a actividades interactivas.

Acerca de esta tarea

Utilice el valor avanzado

COGADMIN.restrictInteractiveActivitiesToSystemAdministrators para restringir el acceso a las actividades interactivas para los usuarios de manera que solo los administradores del sistema puedan ver este tipo de actividades.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para asignadores específicos” en la página 514.
2. Para el asignador especificado, en la columna **Parámetro**, escriba el siguiente nombre: **COGADMIN.restrictInteractiveActivitiesToSystemAdministrators**
3. Especifique un valor de true para este parámetro y haga clic en **Aceptar**.
4. Reinicie el servicio de IBM Cognos.

Resultados

Solo los administradores del sistema pueden ver ahora las actividades interactivas en el entorno de IBM Cognos.

Ocultación de las actividades interactivas de usuarios desconocidos

Es posible que los administradores de arrendatarios no tengan permisos para visualizar todos los usuarios en el entorno de IBM Cognos. Sin embargo, los administradores aún pueden ver las actividades interactivas de todos los usuarios porque estos tipos de actividades no se filtran por la ID de inquilino.

Acerca de esta tarea

El administrador del sistema puede ocultar las actividades interactivas de los usuarios que el administrador de inquilinos no puede ver desde su vista.

Procedimiento

1. Siga los pasos en la sección “Configuración de valores avanzados para asignadores específicos” en la página 514.
2. Como el nombre del **Parámetro**, escriba el siguiente nombre: **COGADMIN.filterInteractiveActivitiesOfUnknownUsers**
3. Especifique un valor de true para este parámetro y haga clic en **Aceptar**.
4. Reinicie el servicio de IBM Cognos.

Resultados

Los administradores de inquilinos pueden ver ahora las actividades interactivas solamente de usuarios inquilinos específicos.

Capítulo 23. Biblioteca de recursos

Los administradores importan, almacenan y gestionan recursos reutilizables, como visualizaciones y perfiles de interfaces de usuario, en la pestaña **Biblioteca** en IBM Cognos Administration.

La pestaña **Biblioteca** proporciona una ubicación central para administrar los recursos.

Para acceder y gestionar el contenido en la pestaña **Biblioteca**, debe ser miembro del rol **Administradores de biblioteca**. Para obtener más información, consulte “Roles predefinidos” en la página 244.

Los administradores deben importar los recursos y establecer los permisos de acceso para los recursos en la biblioteca. Los usuarios con los permisos correspondientes pueden entonces utilizar los recursos en los informes de IBM Cognos.

Los administradores también pueden eliminar recursos de la biblioteca.

Visualizaciones

Las visualizaciones ayudan a los consumidores de informes a identificar patrones y valores atípicos y a comprender los datos. Utilice las herramientas de visualización de IBM Cognos Analytics para incorporar diversos tipos de visualizaciones y mayor interactividad a los informes de IBM Cognos.

Los administradores deben importar las visualizaciones de sistemas locales y compartimientos de archivos a IBM Cognos Analytics.

Encontrará una amplia gama de visualizaciones personalizables y listas para usar en IBM Cognos Analytics Community (www.ibm.com/communities/analytics/cognos-analytics-blog/cognos-business-intelligence-cognos-analytics-all-visualizations). Puede elegir las visualizaciones que se correspondan con sus datos y respondan a sus preguntas de negocio, y descargarlas en el sistema de archivos o en las unidades de red. A continuación, utilice la pestaña **Biblioteca** para importar las visualizaciones a la biblioteca y ponerlas a disposición de los autores de informes.

Las visualizaciones se incluyen en un despliegue de almacén de contenido completo. Al realizar un despliegue de almacén de contenido parcial, los administradores pueden optar por incluir visualizaciones. Para obtener más información, consulte: Capítulo 19, “Despliegue”, en la página 287.

Cómo importar visualizaciones a la biblioteca

Los administradores deben importar las visualizaciones de sistemas locales y compartimientos de archivos al entorno de IBM Cognos Analytics. Las visualizaciones importadas se mencionan luego en la pestaña **Biblioteca** y están disponibles para usarlas en informes de IBM Cognos.

Acerca de esta tarea

Las visualizaciones existentes se pueden volver a importar si han cambiado. Puesto que los cambios en las visualizaciones no se pueden revertir, debe comprender cuál es el impacto sobre los informes asociados antes de sustituir las visualizaciones. En caso contrario, esta acción puede provocar que se hagan cambios no deseados en los informes o impedir que se ejecuten los informes.

Al volver a importar visualizaciones, los autores de informes deben actualizar los informes que contienen las visualizaciones en IBM Cognos Analytics - Reporting para que los cambios entren en vigor. Con la mayoría de los cambios, es suficiente volver a abrir los informes en una ventana nueva en Creación de informes. Sin embargo, en algunos casos es necesario realizar modificaciones en el informe. Por ejemplo, si la visualización nueva ha modificado elementos de la estructura del conjunto de datos del informe o les ha cambiado el nombre, el informe debe modificarse en Creación de informes.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Biblioteca**, pulse **Visualizaciones**.
2. En la barra de herramientas, pulse el icono **Importar** . Se abre **Seleccionar Visualizaciones - Nueva página Importar visualizaciones**.
3. Pulse **Examinar** para navegar al archivo de visualización que desea seleccionar. Vuelva a examinar si desea seleccionar archivos de visualización adicionales.

Consejo: Para eliminar un archivo de visualización de la lista de

visualizaciones seleccionadas, pulse el icono **Eliminar selección** .

4. Para sustituir una visualización existente, seleccione la casilla de verificación **Sustituir entradas existentes**.
Si desmarca esta casilla de verificación mientras intenta importar una visualización existente, la importación fallará. Esto es así para garantizar que una visualización existente no se sobrescribe accidentalmente, lo que puede provocar errores en los informes que utilizan esa visualización. Si decide sustituir una visualización concreta, seleccione la casilla de verificación **Sustituir entradas existentes** para importar la visualización. A continuación, en Creación de informes, actualice los informes que contienen esa visualización.
5. Para importar las visualizaciones seleccionadas pulse **Importar**.

Resultados

Las visualizaciones importadas ahora se enumeran en la página **Visualizaciones**. Las visualizaciones tienen permisos de acceso predeterminados que los administradores pueden cambiar.

Gestión de visualizaciones

Después de importar visualizaciones a IBM Cognos Administration, los administradores pueden gestionarlas en la pestaña **Biblioteca**.

Acerca de esta tarea

Puede realizar una de las acciones siguientes para la gestión de recursos de visualización:

- **Establecer propiedades**

Las visualizaciones son propiedades que se asignan de forma predeterminada, incluyendo el acceso a permisos, cuando se importan. Los administradores de la biblioteca pueden cambiar los valores predeterminados, incluyendo los permisos de acceso, de un recurso de visualización.

Para obtener más información, consulte Capítulo 16, “Propiedades de la entrada”, en la página 257 y “Establecimiento de permisos de acceso para una entrada” en la página 220.

Importante: el icono Establecer propiedades  de la barra de herramientas se utiliza para establecer las propiedades, incluyendo los permisos de acceso, de la página de **Visualizaciones** en la **Biblioteca**.

- **Ver mis permisos**

Los administradores pueden ver sus propios permisos para cada visualización.

- **Suprimir**

Puede eliminar visualizaciones individuales o múltiples de la base de datos del almacén de contenido.

- **Descargar**

Puede descargar una visualización existente al disco duro o a la unidad compartida de red para modificar la visualización.

Procedimiento

1. En IBM Cognos Administration, en la pestaña **Biblioteca**, pulse la página **Visualizaciones**.
2. En la lista de visualizaciones puede realizar las siguientes tareas:
 - Para administrar una visualización, pulse en el menú desplegable y luego pulse en la acción seleccionada.
 - Para suprimir varias visualizaciones, seleccione las casillas de verificación que están asociadas a las visualizaciones elegidas y, en la barra de herramientas, pulse el icono **Suprimir** .

Capítulo 24. Informes y cubos

Puede utilizar los informes y los cubos para analizar datos y para que le ayuden a tomar decisiones documentadas y a tiempo.

En IBM Cognos Analytics, los informes y los cubos se pueden publicar en el portal para garantizar que todas las personas de la organización dispongan de información precisa y pertinente siempre que la necesiten.

Cómo trabajar con informes y cubos

Un informe puede hacer referencia a la especificación que indica qué información se debe incluir en un informe o a los propios resultados. Las especificaciones de informe pueden contener resultados almacenados, o bien se puede ejecutar un nuevo informe para producir nuevos resultados.

Una vez que se haya publicado un informe en el portal, podrá verlo, ejecutarlo, abrirlo o ver sus versiones de salida. También podrá ver el informe en diversos formatos.

Puede distribuir los informes guardándolos, enviándolos por correo electrónico, enviándolos a un dispositivo móvil, imprimiéndolos o separándolos. También puede establecer opciones estándar y opciones avanzadas para la ejecución actual.

Puede planificar un informe para que se ejecute más adelante o de forma periódica. Puede planificar un informe como parte de un trabajo o basado en un activador. Puede ver el historial de ejecución de un informe. También puede incluir un informe en un agente.

Puede añadirse a la lista de alertas de un informe con el fin de recibir notificaciones siempre que se creen versiones nuevas de dicho informe. También puede especificar reglas de observación en las salidas de informe HTML guardadas para recibir una alerta cada vez que se cumplan los eventos especificados por las reglas de observación.

Puede inhabilitar características basadas en la selección, tales como detallar menos o detallar más y acceder a detalles.

Monedas mixtas

Los valores de moneda mixta se producen cuando se calculan valores con diferentes monedas. Al utilizar un origen de datos OLAP, los valores de moneda mixta utilizan el asterisco (*) como unidad de medida.

Informes activos de IBM Cognos

Puede utilizar IBM Cognos Analytics - Reporting para crear informes activos. IBM Cognos Active Report es un tipo de salida de informe que proporciona informes administrados altamente interactivos y fáciles de utilizar. Los informes activos se crean para usuarios empresariales con la finalidad de que puedan explorar sus datos y obtener información adicional.

Los autores de informes generan informes destinados a las necesidades de los usuarios, lo que permite que la experiencia sea sencilla y participativa. Los informes activos se pueden utilizar por usuarios que no están conectados, lo que les convierte en la solución idónea para los usuarios remotos, como el personal de ventas.

Los informes activos son una extensión del informe tradicional de IBM Cognos. Puede aprovechar los informes existentes y convertirlos para que sean informes activos añadiendo comportamiento interactivo, y así proporcionar a los usuarios finales una interfaz fácil de utilizar.

Vistas de informes

Una vista de informe utiliza la misma especificación de informe que el informe de origen pero posee propiedades diferentes, como, por ejemplo, valores de solicitud, planificaciones, métodos de entrega, opciones de ejecución, idiomas y formatos de salida.

Acerca de esta tarea

La creación de una vista de informe no modifica el informe original. Puede determinar el informe de origen para una vista de informe visualizando sus propiedades. Las propiedades de la vista de informe también proporcionan un enlace a las propiedades del informe de origen.

Si el informe de origen se mueve a otra ubicación, el enlace de la vista de informe no se rompe. Si se suprime el informe de origen, el enlace de vista de informe se rompe y se elimina el enlace de propiedades al informe de origen.

Si desea utilizar un informe genérico como estructura subyacente para informes adicionales, realice una copia del informe.

La vista de informe posee las mismas opciones y propiedades de ejecución que la entrada original.

Visualización de la información de linaje de un elemento de datos

La información de linaje rastrea los metadatos de un elemento de datos de un informe HTML o de una vista de informe hasta el paquete y los orígenes de datos utilizados por el paquete.

El linaje también muestra cualquier filtro del elemento de datos añadido por el autor de informes, o definido en el modelo de datos. Por ejemplo, puede pulsar una celda de una tabla de referencias cruzadas para ver cómo se ha calculado el valor de la celda.

No es posible ver la información de linaje cuando se ejecuta un informe desde un dispositivo móvil.

IBM Cognos Analytics se puede configurar para que utilice la solución de linaje predeterminada que se suministra con el producto o bien una solución de linaje personalizada. IBM InfoSphere Information Governance Catalog también está soportado.

Para acceder a la información de linaje de un informe, el administrador debe configurar la solución de linaje, habilitar la función **Linaje** y otorgar permisos de lectura en el informe.

Para obtener más información, consulte: “Configuración de la solución de linaje” en la página 104, Capítulo 13, “Funciones y características protegidas”, en la página 227 y Capítulo 14, “Capacidades de objetos”, en la página 239.

La solución de linaje de IBM Cognos muestra el linaje de informes en su nivel más alto. El linaje no cambia tras detallar más en un informe. Puesto que el contexto de selección utilizado para lanzar el linaje se puede ver afectado por las acciones de detallar más, se recomienda lanzar siempre el linaje en el nivel de informe más alto antes de detallar más en el informe. De lo contrario, es posible que la solución de linaje no se lance correctamente.

Procedimiento

1. Abra un informe HTML o una vista de informe.
2. Pulse con el botón derecho del ratón en el elemento de datos que desee y en **Linaje**.
Aparecerán las vistas de linaje.

Acceso a InfoSphere Business Glossary

Si su organización utiliza IBM InfoSphere Business Glossary, también puede acceder al Glosario en el software de Cognos desde IBM Cognos Analytics Viewer y desde el árbol de metadatos de Reporting, Query Studio y Analysis Studio.

Antes de empezar

Para poder acceder a InfoSphere Business Glossary, debe tener permisos para la función **Glosario** y el administrador debe haber configurado el URI del Glosario.

Para obtener más información, consulte: Capítulo 13, “Funciones y características protegidas”, en la página 227, Capítulo 14, “Capacidades de objetos”, en la página 239 y “Configuración del URI de InfoSphere Business Glossary” en la página 106.

Procedimiento

1. Abra un informe HTML o una vista de informe en Cognos Analytics Viewer.
2. Pulse con el botón derecho del ratón en el elemento de datos que desee y en **Glosario**.

Resultados

De forma predeterminada, los resultados de búsqueda del Glosario en el software de Cognos devuelven únicamente términos que contengan la palabra clave especificada en la búsqueda. No se devuelven otros tipos de activos.

Formatos de informe

En IBM Cognos Analytics, puede visualizar informes en un navegador, o en función de sus permisos, puede generar informes en formatos que se pueden importar a otras aplicaciones. Los administradores pueden restringir el acceso a las capacidades necesarias para ejecutar informes con formatos de texto delimitado (CSV), PDF, hoja de cálculo de Microsoft Excel (XLS) o XML.

Todos los usuarios tienen, de forma predeterminada, permisos para las siguientes capacidades:

- Generar salida CSV
- Generar salida PDF
- Generar salida XLS
- Generar salida XML

Estas funciones protegidas de forma independiente pueden dar soporte a la gestión de recursos de sistema. Para controlar las opciones de formato que los usuarios pueden ver y ejecutar en la interfaz de usuario, establezca permisos de acceso para estas capacidades.

Si su acceso a un formato está restringido, podrá ver el contenido en el formato restringido y especificar el formato restringido en las propiedades de un informe.

Para realizar las acciones siguientes, debe tener permisos de ejecución y de visita para la capacidad correspondiente:

- Ejecutar informes en un formato restringido.
- Establecer planificaciones o trabajos para los informes que se ejecutan en un formato restringido.
- Profundizar en destinos que se ejecutan con un formato restringido.
- Imprimir un informe PDF en un widget de Cognos Workspace.

Al ejecutar un informe, solo verá las opciones de formato para las que tenga la capacidad de generar salidas. El formato HTML no es una función protegida.

La capacidad de generar salidas no se aplica a PowerPlay o a los informes activos.

Para especificar el formato de informe, debe contar también con permisos de lectura y de escritura para el informe y permisos de visita para la carpeta que contiene el informe.

Puede especificar el formato que desea que se emplee de forma predeterminada cuando se ejecute un informe.

Puede especificar el formato de informe en la página de opciones de ejecución, en las propiedades de informe o en sus preferencias.

Formatos HTML

En IBM Cognos Analytics, puede elegir el formato de salida HTML para un informe.

Formato PDF

Utilice el formato PDF para ver y distribuir informes en formato de libros en línea. En IBM Cognos Analytics, para generar la salida de informe en formato PDF, debe tener permisos de ejecución y visita para la prestación **Generar salida PDF**.

Debe tener privilegios de administrador para especificar las opciones avanzadas de PDF.

Formatos Microsoft Excel

Puede exportar la salida de informe a varios formatos distintos de software de hoja de cálculo de Microsoft Excel.

En IBM Cognos Analytics, para generar salida de informe en los formatos Microsoft Excel, debe tener permisos de ejecución y visita para la prestación **Generar salida XLS**.

Los formatos de Excel representan la salida de informe en formato XML de Excel nativo, también denominado XLSX.

El formato **Excel** proporciona informes con formato completo. El resultado es parecido al de otros formatos de Excel, con las excepciones siguientes:

- Los gráficos se procesan como imágenes estáticas.
- La altura de las filas puede cambiar en el informe generado para conseguir una mayor fidelidad.
- Microsoft Excel 2007 ignora las anchuras de columna especificadas explícitamente en los informes.
- Las celdas fusionadas se utilizan para mejorar el aspecto de los informes.
- El tamaño predeterminado de las hojas de trabajo es de 65.536 filas por 256 columnas.

El administrador de IBM Cognos puede habilitar hojas de trabajo más grandes y cambiar el número máximo de filas de una hoja de trabajo, hasta un máximo de 16.384 columnas por 1.048.576 filas, utilizando las propiedades avanzadas del servidor.

Datos de Excel proporciona los datos con un formateo mínimo. El formateo de datos predeterminado se aplica a los datos en función del tipo de datos y se da por supuesto que cada columna tiene un solo tipo de datos.

El resultado es parecido al de otros formatos de Excel, con las excepciones siguientes:

- La salida generada solamente incluye la primera consulta de lista del informe. Si un informe contiene varias consultas y la primera consulta es una consulta multidimensional para una tabla de referencias cruzadas o para un gráfico, se visualiza un mensaje de error cuando se ejecuta el informe.
- No se da soporte a marcos anidados ni a enlaces maestro-detalle.
- Las celdas del archivo de Microsoft Excel tienen una anchura y altura predeterminadas. Debe ajustar la anchura y la altura de las columnas si los datos superan el tamaño predeterminado.
- No se representan las especificaciones de estilo, incluidos el color, el color de fondo y las fuentes.
- No se representan los bordes.
- No se aplica el formateo de datos especificado por el usuario en la especificación de informe, incluidos el resaltado de excepciones y las reglas de color para números negativos.

Formato CSV

Los informes guardados en formato de texto delimitado (CSV) se abren en la aplicación asociada al tipo de archivo .csv.

Debe tener permisos de ejecución y visita para la prestación **Generar salida CSV** para generar la salida de informe en formato CSV.

Los informes guardados en formato CSV

- Están diseñados para soportar datos Unicode en diversos sistemas operativos cliente.
- Están codificados en UTF-16 Little Endian.
- Incluyen una BOM (marca de orden de bytes) al comienzo del archivo.
- Están delimitados por pestañas.
- No incluyen las cadenas entre comillas.
- Utilizan un carácter de nueva línea para delimitar las filas.
- Muestran solo los resultados de una consulta de informe. Los elementos de diseño de página, como los títulos, las imágenes y los valores paramDisplay, no aparecen en la salida CSV.

Idiomas del informe

Puede seleccionar el idioma de un informe.

Puede especificar el idioma del informe en las propiedades de informe o en sus preferencias. Al ejecutar un informe, se utiliza el idioma especificado en las propiedades de informe. Si no se especifica en las propiedades de informe, se utiliza el idioma especificado en sus preferencias.

La selección de un idioma para su informe no modifica el idioma utilizado en el portal. Puede modificar el idioma empleado en la interfaz del portal en sus preferencias.

Al ejecutar un informe, el servidor de informes se conecta con el origen de datos subyacente para obtener los datos. Al utilizar un origen de datos SAP BW, si el servidor SAP BW no soporta el idioma asociado con su entorno local del contenido, IBM Cognos Analytics busca una correlación de entorno local para el entorno local correspondiente. Si el servidor SAP BW soporta el idioma del entorno local, se utilizará este idioma. De lo contrario, el informe se ejecuta utilizando el idioma predeterminado instalado en el servidor SAP BW.

Para especificar el idioma del informe, debe contar con permisos de lectura y de escritura sobre dicho informe y permisos de visita sobre la carpeta en el que está incluido.

El paquete empleado para crear el informe debe contener datos multilingües para que las salidas del informe se muestren en los idiomas seleccionados.

Especificar el idioma para un informe

Para especificar el idioma de un informe, modifique las propiedades de informe.

Cómo especificar los valores de la solicitud predeterminados para un informe

De forma predeterminada, si un informe contiene solicitudes, debe seleccionar valores cada vez que se ejecuta el informe. Puede cambiar el comportamiento de las solicitudes en las propiedades de informe.

Acerca de esta tarea

Para establecer los valores de solicitud predeterminados, debe contar con permisos de lectura y de escritura para el informe y permisos de lectura o de visita para la carpeta en el que está incluido.

Si el autor de informes es usted, puede crear valores de solicitud predeterminados para un informe. Cuando el informe se ejecuta, los datos se filtran automáticamente basándose en los valores de solicitud que especifique. El usuario no tiene que especificar valores de solicitud cuando el informe se ejecuta. Esto puede resultarle útil si la mayoría de los usuarios utilizan los mismos valores de solicitud cada vez que ejecutan un informe.

Si posee acceso de escritura a un informe y modifica los valores de solicitud, dichos valores se almacenan para cualquier persona que ejecute el informe después de usted. Si utiliza repetidamente valores de solicitud que difieren de la mayoría de los usuarios, cree una vista de ese informe.

Especificación del tiempo que se deben mantener las versiones de las salidas de informe

En las propiedades de un informe puede especificar el número de versiones de salida de informe que se conservarán y el número de días o meses que deben conservarse.

Especificación del tiempo que se deben guardar los historiales de salida de informe

Puede guardar la salida de informe durante un número de ejecuciones o un número de días o meses específicos.

Por ejemplo, puede guardar la salida de informe durante las diez últimas apariciones o durante 2 días o 6 meses.

Acerca de esta tarea

Debe contar con permisos de lectura y escritura para la entrada y permisos de lectura o visita para la carpeta que contiene la entrada.

Los orígenes de datos con conjuntos con nombre pueden producir resultados imprevisibles

Si los orígenes de datos dimensionales incluyen conjuntos con nombre, que son conjuntos de miembros o expresiones de conjunto creadas para su reutilización, los resultados de datos son imprevisibles en Query Studio si están combinados con el filtrado y el anidado de niveles.

Además, si los orígenes de datos incluyen conjuntos con nombre de varios niveles, los resultados de datos son imprevisibles en Analysis Studio cuando se añaden.

Por tanto, se recomienda evitar la exposición de conjuntos con nombre de uno o varios niveles a los usuarios de Query Studio y Analysis Studio.

El trabajo con conjuntos con nombre puede también ocasionar resultados imprevisibles en Creación de informes. Para obtener más información, consulte la publicación IBM Cognos Analytics - Reporting *Guía del usuario*.

Informes de Series 7 en IBM Cognos Analytics

PowerPlay 7.3 o posterior puede configurarse para utilizar IBM Cognos Analytics como portal en lugar de Upfront. Sin embargo, si accede a los contenidos de otras aplicaciones o versiones de IBM Cognos anteriores a PowerPlay 7.3, el administrador puede seguir dependiendo del portal Upfront.

Informes y cubos de Series 7 PowerPlay

Una vez publicados los informes y los cubos de Series 7 PowerPlay en el portal de IBM Cognos Analytics, podrá utilizar las herramientas de creación de PowerPlay para crear y editar informes de Series 7 PowerPlay.

Para obtener más información acerca de las herramientas de creación de PowerPlay, consulte *PowerPlay Web User's Guide*.

Puede cambiar las opciones de ejecución predeterminadas de los informes y cubos de Series 7 PowerPlay y seleccionar propiedades multilingües.

Los informes y cubos de Series 7 PowerPlay funcionan de forma distinta al resto de informes. Las siguientes acciones no se aplican a los informes y cubos de Series 7 PowerPlay:

- Visualización del historial de ejecución y las versiones de salida de informe.
- Especificación del tiempo que se deben mantener las salidas del informe y los historiales.
- Cancelación y suspensión de informes.
- Especificación de valores de solicitud para formatos de informe que no sean PDF.
- Especificación de idioma para el contenido de los informes.
- Ejecución de un informe como el propietario.
- Planificación de informes.
- Distribución de informes.

Inicio de sesión único

El inicio de sesión único asegura que no se pida a los usuarios que estén conectados a una aplicación de IBM Cognos que se autenticuen cuando ejecuten otra aplicación de IBM Cognos.

Podrá asegurarse de que los usuarios se beneficien de un inicio de sesión único garantizando que tanto IBM Cognos Analytics como PowerPlay utilicen el mismo espacio de nombres de Series 7 que su origen de autenticación. De forma alternativa, puede asegurarse de que los espacios de nombres de autenticación que se utilicen tanto para IBM Cognos Analytics como PowerPlay se configuran para que utilicen un mecanismo externo de inicio de sesión único para la autenticación; como por ejemplo los inicios de sesión en el sistema operativo para proveedores de Series 7 PowerPlay o LDAP con correlación de identidad externa en IBM Cognos Analytics.

Para obtener instrucciones acerca de la configuración del inicio de sesión único de Series 7, consulte la publicación *Access Manager Administrator Guide*.

Para obtener instrucciones sobre la configuración de un inicio de sesión único para el producto de creación de informes de IBM Cognos, consulte la *Guía de instalación y configuración*.

Cambio de los valores predeterminados para un informe de Series 7 PowerPlay

Puede cambiar las opciones predeterminadas de los informes de Series 7 PowerPlay.

Puede seleccionar una de las siguientes acciones predeterminada al ejecutar un informe:

- Ejecutar el informe en formato PDF (valor predeterminado)
- Abrir el informe con PowerPlay Web Explorer

Para los informes con formato HTML, puede seleccionar abrir el informe en el modo de diseño (sin datos). La apertura de un informe en el modo de diseño resulta útil para ver rápidamente la estructura del informe.

Para los informes en formato PDF, puede seleccionar que se soliciten los valores que filtran el rango de datos incluidos en un informe. Por ejemplo, puede especificar un rango de fechas que sea un subconjunto de fechas disponibles en el informe. Si el informe de Series 7 PowerPlay se creó con valores de solicitud, se le pedirá que especifique valores cuando se ejecute el informe.

Propiedades multilingües de los informes y cubos de Series 7

En IBM Cognos Analytics, puede seleccionar las propiedades multilingües de un informe o cubo de Series 7.

Los valores de IBM Cognos Analytics no afectan al contenido, los datos, las etiquetas de categoría y otras etiquetas. El idioma para estos elementos lo establece el administrador de PowerPlay que crea el informe o el cubo.

Capítulo 25. Administración de tareas humanas

Existen tres tipos de tareas humanas que pueden verse en **Mi bandeja de entrada**: solicitudes de aprobación, tareas ad-hoc y solicitudes de notificación.

Abra **Mi bandeja de entrada** desde el **Menú personal** de la página de bienvenida.

Se pueden crear tareas desde

- Event Studio (solicitudes de notificación y de aprobación)
Para obtener más información, consulte *Event Studio User Guide*.
- **Mi bandeja de entrada** (solicitudes de notificación y tareas ad-hoc).
- Una regla de observación configurada para un informe (solamente solicitudes de notificación).

Solicitudes de aprobación y tareas ad-hoc

Puede crear solicitudes de aprobación con Event Studio.

Para obtener más información, consulte *Event Studio User Guide*.

Puede crear tareas ad-hoc desde la bandeja de entrada de tareas. Para obtener más información, consulte “Creación de una tarea ad-hoc” en la página 372.

Las solicitudes de aprobación o las tareas ad-hoc pueden tener varios destinatarios:

- Un propietario de la tarea: un usuario determinado
- Posibles propietarios: varios usuarios, grupos, roles o listas de distribución
- Partes interesadas: una o varias partes interesadas, que no son posibles propietarios

Si una tarea solamente tiene un posible propietario, ese usuario se convierte automáticamente en el propietario de la tarea. Si una tarea tiene varios propietarios, el usuario que reclama la tarea se convierte en su propietario.

Es posible crear una tarea con una o varias partes interesadas, pero sin propietarios ni posibles propietarios. En este caso, las partes interesadas pueden asignar posibles propietarios después de la creación.

Estado de la tarea

El estado de una solicitud de aprobación o una tarea ad-hoc puede ser uno de los siguientes:

- No iniciado: la tarea está en espera de iniciarse.
- Iniciado: la tarea tiene un propietario y está en progreso.
- Finalizado: el propietario ha finalizado la tarea.
- Cancelado: la tarea se ha cancelado por un destinatario.

Visualización de comentarios

Puede ver los comentarios que hayan añadido otros destinatarios, así como los comentarios del historial de auditoría, registrados por el sistema.

También puede añadir sus propios comentarios a una tarea. Para obtener más información, consulte “Cómo añadir comentarios a una tarea” en la página 377.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea cuyos comentarios desee ver y, a continuación, pulse la pestaña **Debate** en el panel de lectura.
De forma predeterminada, sólo aparecen los comentarios del usuario.
3. Seleccione el tipo de comentarios que desee ver de la lista desplegable de comentarios.
Puede ver todos los comentarios del usuario y de auditoría, o puede filtrar la visualización por tipo de comentario.

Suscripción a las notificaciones de correo electrónico

Las opciones de notificación predeterminadas se configuran al crear la tarea. Puede cambiar las suscripciones de cualquier tarea con el estado No iniciado o Iniciado.

Puede decidir si desea recibir o dejar de recibir notificaciones cuando

- Una tarea no se inicia en la fecha de inicio
- Una tarea no se ha completado en la fecha límite
- El estado de una tarea cambia (iniciado, finalizado o cancelado)
- El propietario de una tarea cambia
- Un comentario de usuario se añade a la tarea

Nota:

- Las notificaciones se envían al propietario de la tarea con copia a todas las partes interesadas.
- El destinatario que cambia el estado o el propietario de una tarea, o añade un comentario de usuario, no recibe la notificación asociada.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea cuyas suscripciones a las notificaciones desee cambiar y, a continuación, pulse la pestaña **Opciones de notificación** en el panel de lectura.
3. Seleccione las casillas de verificación adecuadas para todas las notificaciones que desee recibir y desactive aquellas casillas que no necesite.
4. Pulse **Guardar**.

Creación de una tarea ad-hoc

Cree una tarea ad-hoc para enviar una tarea a la bandeja de entrada de tareas de los destinatarios que especifique.

Puede añadir fechas límite a una tarea ad-hoc al crearla. Otra posibilidad es que los posibles propietarios o las partes interesadas añadan las fechas límite posteriormente, actualizando la tarea desde la bandeja de entrada de tareas.

Puede configurar opciones de notificación para que el propietario de la tarea reciba correos electrónicos cuando:

- Una tarea ad-hoc no se haya completado al llegar la fecha límite.
- Una tarea ad-hoc no se haya iniciado en la fecha de inicio.

Nota: También se envía una copia del correo electrónico a las partes interesadas.

Además, puede configurar opciones de notificación para que el propietario de la tarea y todas las partes interesadas reciban mensajes de correo electrónico cuando:

- El estado de una tarea ad-hoc cambie (iniciado, finalizado o cancelado).
- El propietario de una tarea ad-hoc cambie.
- Se añada un comentario a la tarea ad-hoc.

Nota: Los posibles propietarios y las partes interesadas pueden anular la suscripción a notificaciones específicas actualizando la tarea desde la bandeja de entrada de tareas.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. En la lista desplegable de tareas, seleccione Nueva tarea **Nueva tarea** .
3. En el panel de lectura, pulse **Agregar o eliminar destinatarios**. Aparecerá la página **Seleccionar destinatarios**.
4. Seleccione los usuarios, grupos, roles y listas de distribución necesarios para añadir posibles propietarios y partes interesadas.
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, los grupos, los roles o las listas de distribución.

Consejo: Para que se muestren las entradas del usuario, pulse **Mostrar usuarios en la lista**.

- Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
- Para escribir el nombre de las entradas que desea añadir, pulse **Tipo** y escriba los nombres de los grupos, roles o usuarios utilizando el siguiente formato, donde un punto y coma (;) separa cada entrada:
*espacio_nombres/nombre_grupo;espacio_nombres/
nombre_rol;espacio_nombres/nombre_usuario;;*

A continuación se incluye un ejemplo:

Cognos/Authors;LDAP/scarter;

5. Pulse el botón de flecha de **Posible propietario** o **Parte interesada** para actualizar la lista **Entradas seleccionadas** y, a continuación, pulse **Aceptar**.

Consejo: Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

6. Pulse **Aceptar**.
7. En el campo **Asunto**, escriba el asunto de la tarea.
8. Si es necesario, añada una fecha límite para la finalización de la tarea en el cuadro **Fecha límite**.
9. Si es necesario, añada una fecha límite para el inicio de la tarea en el cuadro **Empezar en**.
10. Seleccione la prioridad en la lista **Prioridad**.
11. En el cuadro **Mensaje**, escriba el texto directamente.

12. Para añadir enlaces, pulse **Añadir enlaces**, seleccione las entradas que desee, pulse el botón de flecha para actualizar la lista **Entradas seleccionadas** y pulse **Aceptar**.

Consejo: Para eliminar enlaces, selecciónelos y pulse **Eliminar enlaces**.

13. Si desea configurar opciones de notificación, pulse **Avanzado**; de lo contrario, diríjase al paso 16.
14. Seleccione las opciones de notificación de fecha límite y creación de tarea según sea necesario:
- **Enviar notificación si no se ha empezado en la fecha de inicio**
 - **Enviar notificación si no se ha completado en la fecha límite**
15. Seleccione las opciones de notificación de cambio de solicitud de aprobación según sea necesario:
- **Iniciado**
 - **Comentario**
 - **Propietario cambiado**
 - **Finalizado**
 - **Cancelado**
16. Pulse **Guardar**.

Acciones que se pueden efectuar en las solicitudes de aprobación y las tareas ad-hoc

Las acciones que puede realizar en una solicitud de aprobación o una tarea ad-hoc difieren según el tipo de destinatario.

En la tabla siguiente se resumen las acciones que puede realizar cada tipo de destinatario.

Tabla 77. Solicitud de aprobación y acciones ad hoc por tipo de destinatario

Acción	Posible propietario	Propietario	Parte interesada
Reclamar la propiedad de una tarea	X		
Cambio de los destinatarios de una tarea	X	X	X
Revocar la propiedad de una tarea		X	
Establecer fechas límite para una tarea	X	X	X
Cambiar la prioridad de una tarea	X	X	X
Añadir comentarios a una tarea	X	X	X

Tabla 77. Solicitud de aprobación y acciones ad hoc por tipo de destinatario (continuación)

Acción	Posible propietario	Propietario	Parte interesada
Iniciar o detener una tarea		X	
Finalizar una tarea		X	
Cancelar una tarea		X	X

Reclamación de una tarea

Si es un posible propietario de una tarea no reclamada, puede reclamarla. A continuación, la tarea será de su propiedad.

Si es el único posible propietario de una tarea, la propiedad de ésta se le asignará de forma automática. En este caso, no es necesario reclamar la tarea.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea que desea reclamar y pulse **Convertir al usuario en propietario** en el panel de lectura.

Cambio de los destinatarios de una tarea

Todos los destinatarios de una tarea pueden cambiar el propietario actual de dicha tarea.

También pueden añadir o eliminar posibles propietarios y partes interesadas de una tarea. El estado de la tarea debe ser No iniciado o Iniciado.

Nota: Si es el propietario de una tarea, puede revocar la propiedad de ésta “Revocación de la propiedad de una tarea” en la página 376.

Cambio del propietario actual

Puede cambiar el propietario actual.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea cuyo propietario actual desea cambiar y pulse **Cambiar propietario** en el panel de lectura.
Aparecerá la página **Seleccionar el usuario**.
3. Seleccione el usuario.
 - Para realizar una selección en las entradas de la lista, pulse el espacio de nombres correspondiente y después seleccione el usuario necesario.
 - Para buscar una entrada, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
4. Pulse **Aceptar**.
5. Pulse **Guardar**.

Cambio de los posibles propietarios y las partes interesadas

Puede cambiar los posibles propietarios y las partes interesadas.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea cuyos posibles propietarios y partes interesadas desea cambiar y pulse **Agregar o eliminar destinatarios** en el panel de lectura. Aparecerá la página **Seleccionar destinatarios**.
3. Seleccione los usuarios, los grupos, los roles y las listas de distribución necesarios.
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, los grupos, los roles o las listas de distribución.

Consejo: Para que se muestren las entradas del usuario, pulse **Mostrar usuarios en la lista**.

- Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
- Para introducir el nombre de las entradas que desea añadir, pulse **Tipo** e introduzca los nombres de grupos, roles o usuarios mediante el siguiente formato, en donde un punto y coma (;) separa cada entrada.

*espacio_nombres/nombre_grupo;espacio_nombres/
nombre_rol;espacio_nombres/nombre_usuario;*

A continuación se incluye un ejemplo:

Cognos/Authors;LDAP/scarter;

4. Pulse el botón de flecha de **Posible propietario** o **Parte interesada** para actualizar la lista **Entradas seleccionadas** y, a continuación, pulse **Aceptar**.

Consejo: Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

5. Pulse **Aceptar**.
6. Pulse **Guardar**.

Revocación de la propiedad de una tarea

Si es el propietario de una tarea, puede revocar la propiedad y dejar de ser el propietario de dicha tarea.

Esto cambia el propietario por Sin reclamar y el estado de la tarea por No iniciado.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea que desee revocar y pulse **Eliminar al usuario como propietario** en el panel de lectura.

Establecimiento de fechas límite para una tarea

Cualquier destinatario puede añadir una fecha de inicio o una fecha límite para una solicitud de aprobación o una tarea ad-hoc con un estado No iniciado o Iniciado. También pueden modificar las fechas límite existentes.

Cuando hay notificaciones configuradas, si una tarea no se inicia o finaliza en el plazo necesario, se envían notificaciones de correo electrónico a todos los posibles propietarios y partes interesadas suscritos. Para obtener más información sobre las notificaciones, consulte “Suscripción a las notificaciones de correo electrónico” en la página 372.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea para la que desee actualizar las fechas límite.
3. Si es necesario, añada una fecha límite para la finalización de la tarea en el cuadro **Fecha límite**.
4. Si es necesario, añada una fecha límite para el inicio de la tarea en el cuadro **Empezar en**.
5. Pulse **Guardar**.

Cómo cambiar la prioridad de una tarea

La prioridad de una tarea se configura cuando se crea la tarea. Cualquier destinatario de la tarea puede cambiar la prioridad de una tarea con un estado No iniciado o Iniciado.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea cuya prioridad desea cambiar y, a continuación, seleccione la prioridad en la lista **Prioridad** en el panel de lectura.
3. Pulse **Guardar**.

Cómo añadir comentarios a una tarea

Todos los destinatarios de una tarea pueden añadir comentarios.

Para obtener información sobre la visualización de comentarios añadidos a una tarea, consulte “Visualización de comentarios” en la página 371.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea a la que desea añadir comentarios y, a continuación, pulse la pestaña **Debate** en el panel de lectura.

3. Pulse **Añadir comentario** , escriba los comentarios en la ventana que aparezca y, a continuación, pulse **Aceptar**.
4. Pulse **Guardar**.

Inicio o detención de una tarea

Si es el propietario de una tarea que no se ha iniciado, puede iniciarla.

De este modo el estado pasará a ser Iniciado, y los demás destinatarios podrán ver el progreso de la tarea.

Un posible propietario también puede iniciar una tarea no reclamada. El usuario se convertirá en el propietario de la tarea.

Si es el propietario de una tarea que ya se ha iniciado, puede detenerla. De este modo el estado pasará a ser No iniciado.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea que desee iniciar y, a continuación, seleccione **Iniciar tarea** en la lista desplegable **Estado** del panel de lectura.

Sugerencia: Para detener una tarea que se haya iniciado, seleccione **No iniciado** en la lista desplegable **Estado**.

3. Pulse **Guardar**.

Finalización de una tarea

Si es el propietario de una tarea que tiene el estado No iniciado o Iniciado, puede finalizar la tarea llevando a cabo la acción necesaria.

La acción necesaria difiere según el tipo de tarea. Para tareas ad-hoc, debe marcar la tarea como finalizada.

Para tareas de solicitud de aprobación, la acción depende de cómo la ha configurado el creador de la tarea. Debe realizar una de las acciones siguientes:

- Aprobar o rechazar la solicitud

Para este tipo de solicitud de aprobación, debe aprobar o rechazar la solicitud desde la bandeja de entrada de tareas para finalizar la tarea.

Dependiendo de la configuración de la tarea, su finalización puede tener como resultado la realización de otra acción. Por ejemplo, si aprueba una solicitud para distribuir un informe, cuando la tarea finalice el informe se podrá distribuir de forma automática. Si la solicitud se rechaza, no habrá más acciones.

- Especificar el resto de tareas que se deben aprobar y ejecutar

Este tipo de solicitud de aprobación contiene una o varias tareas planificadas para que se ejecuten después de que finalice la tarea. Debe seleccionar las tareas cuya ejecución aprueba.

Finalización de una tarea ad-hoc

El procedimiento para finalizar una tarea ad-hoc es el siguiente.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea que desee completar y luego pulse **Marcar como terminado**.
El estado de la tarea cambia a Finalizada.

Aprobación o rechazo de una solicitud

El procedimiento para aprobar o rechazar una solicitud es el siguiente.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea que desee finalizar y visualice los detalles en el panel de lectura.
3. Si es necesario, añada un comentario para explicar la decisión en el cuadro **Comentario**.
4. Pulse **Aprobar** o **Rechazar** para finalizar la tarea.

Nota: **Aprobar** y **Rechazar** son nombres de botones predeterminados. El usuario que ha creado la tarea puede haber utilizado nombres de botones personalizados, que pueden diferir de los predeterminados.
El estado de la tarea cambia a Finalizada.

Especificación de la aprobación y ejecución del resto de tareas

Puede especificar la aprobación y ejecución del resto de tareas.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea que desee finalizar y visualice los detalles en el panel de lectura.
3. Seleccione el resto de tareas que desee aprobar y luego pulse **Enviar**.

Nota: **Enviar** es el nombre predeterminado del botón. El usuario que ha creado la tarea puede haber utilizado un nombre de botón personalizado, que difiera del predeterminado.

El estado de la tarea cambia a Finalizada.

Cancelación de una tarea

Un propietario de tarea o parte interesada pueden cancelar una solicitud de aprobación o una tarea ad-hoc con un estado No iniciado o Iniciado.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la tarea que desee cancelar y pulse **Marcar como cancelada** en el panel de lectura.

El estado de la tarea cambia a Cancelada.

Solicitudes de notificación

Puede crear una solicitud de notificación con una opción para que los destinatarios confirmen la solicitud. También puede especificar fechas límite para las confirmaciones.

Una solicitud de notificación puede tener varios destinatarios.

- Usuarios, grupos, roles y listas de distribución a quienes se envía la solicitud (destinatarios de la lista Para)
- Partes interesadas a quienes se envía una copia de la solicitud (destinatarios de la lista CC)

El estado de una solicitud de notificación puede ser:

- No leído: el destinatario no ha abierto la solicitud.
- Leído: el destinatario ha abierto la solicitud.
- Confirmado: un destinatario incluido en la lista Para al que se ha enviado la solicitud la ha confirmado.

También se pueden crear notificaciones en IBM Cognos Event Studio. Para obtener más información, consulte *Event Studio User Guide*.

Confirmaciones

Cuando se crea una solicitud de notificación, puede solicitar una confirmación de cada destinatario incluido en la lista Para.

Nota: Las partes interesadas (destinatarios de lista CC) no tienen la opción de confirmar las solicitudes de notificación.

Fechas límite

Al crear una solicitud de notificación, es posible incluir una fecha límite de confirmación. También puede especificar que se envía un correo electrónico a cada destinatario de la lista Para que no confirme una solicitud de notificación en la fecha límite. En la fecha límite, se envía un correo electrónico independiente a los interesados de la lista CC para informarles de que algunos destinatarios de la lista Para no han confirmado la solicitud de notificación.

Consejo: Una parte interesada puede verificar quién ha confirmado una solicitud de notificación comprobando los correos electrónicos o las tablas de auditoría.

Cuando todos los destinatarios de la lista Para han confirmado la solicitud, se cancela la fecha límite.

Creación de una solicitud de notificación

Añada una solicitud de notificación a un agente para enviar una notificación segura sobre un evento a la bandeja de entrada de los destinatarios que especifique.

Puede solicitar una confirmación y añadir una fecha límite de confirmación.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione **Nueva notificación**  en la lista desplegable de tareas.
3. Pulse **Agregar o eliminar destinatarios** en el panel de lectura.
Aparecerá la página **Seleccionar destinatarios**.
4. Seleccione los usuarios, los grupos, los roles y las listas de distribución necesarios para añadir como destinatarios.
 - Para seleccionar entradas de la lista, pulse el espacio de nombres adecuado y, a continuación, seleccione las casillas de verificación situadas junto a los usuarios, los grupos, los roles o las listas de distribución.

Consejo: Para que se muestren las entradas del usuario, pulse **Mostrar usuarios en la lista**.

- Para buscar entradas, pulse **Buscar** e introduzca la frase que desee buscar en el cuadro **Cadena de búsqueda**. Para las opciones de búsqueda, pulse **Editar**. Busque la entrada que desee y pulse en ella.
- Para introducir el nombre de las entradas que desea añadir, pulse **Tipo** e introduzca los nombres de grupos, roles o usuarios mediante el siguiente formato, en donde un punto y coma (;) separa cada entrada.

*espacio_nombres/nombre_grupo;espacio_nombres/
nombre_rol;espacio_nombres/nombre_usuario;*

A continuación se incluye un ejemplo:

Cognos/Authors;LDAP/scarter;

5. Pulse el botón de flecha de **Para** o **CC** para actualizar la lista **Entradas seleccionadas** y, a continuación, pulse **Aceptar**.

Consejo: Para eliminar entradas de la lista **Entradas seleccionadas**, selecciónelas y pulse **Eliminar**. Para seleccionar todas las entradas de la lista, pulse la casilla de verificación de la lista.

6. Pulse **Aceptar**.
7. En el campo **Asunto**, escriba el asunto de la solicitud de notificación.
8. En el cuadro **Mensaje**, escriba el texto directamente.
9. Para añadir enlaces, pulse **Añadir enlaces**, seleccione las entradas que desee, pulse el botón de flecha para actualizar la lista **Entradas seleccionadas** y pulse **Aceptar**.

Consejo: Para eliminar enlaces, selecciónelos y pulse **Eliminar enlaces**.

10. Si desea configurar opciones de notificación, pulse **Avanzado**; de lo contrario, dirijase al paso 13.
11. Para solicitar una confirmación de cada destinatario de la lista **Para**, seleccione el cuadro **Solicitar acuse de recibo**.
12. Para enviar una notificación de correo electrónico a los destinatarios que no hayan confirmado la solicitud en una fecha especificada, seleccione el cuadro **Enviar notificación si no se ha confirmado en la fecha**, y luego seleccione la fecha necesaria.
13. Pulse **Guardar**.

Lectura y confirmación de una solicitud de notificación

Las solicitudes de notificación nuevas de la bandeja de entrada de tareas tienen el estado No leído.

Puede leer la solicitud de notificación y confirmarla si tiene esta opción disponible.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione la solicitud de notificación no leída que desee leer y visualice los detalles en el panel de lectura.
El estado de la solicitud de notificación cambia a Leído.
3. Si el nombre de usuario aparece en la lista **Para**, y se necesita una confirmación, pulse **Confirmar**.
El estado de la solicitud de notificación cambia a Confirmado.

Nota: Si el nombre de usuario aparece en la lista **Para**, es un destinatario de la solicitud de notificación. Si aparece en la lista **CC**, es una parte interesada a la que se envía una copia de la solicitud. Si hay una fecha límite configurada para la solicitud de notificación, aparece en el cuadro **Fecha límite**.

Archivado de tareas

El archivado es un método para eliminar tareas no deseadas de la bandeja de entrada.

Cuando se archiva una tarea, permanece activa en IBM Cognos Analytics y otros destinatarios de la tarea pueden continuar trabajando con ella. Cualquier notificación asociada a una tarea archivada también permanece activa.

Las tareas que se suprimen del archivado también permanecen activas, pero ya no puede verlas.

Procedimiento

1. Visualice la bandeja de entrada de tareas.
2. Seleccione las tareas que desee archivar y, a continuación, pulse **Archivar**  en la lista desplegable **Mover a**.

Visualización del archivo de tareas

Puede ver una lista de tareas que ha archivado.

Procedimiento

Visualice la bandeja de entrada de tareas, y luego pulse la pestaña **Archivar**.

Qué hacer a continuación

Para ver los detalles de una tarea, selecciónela. Los detalles de la tarea aparecen en el panel de lectura. Si la tarea contiene archivos adjuntos, como un informe, puede efectuar una doble pulsación en él para verlo.

Consejo:

- Para ver la fecha límite para las tareas en lugar de la fecha de recepción, seleccione **Mostrar fecha límite** en la lista desplegable **Mostrar fecha de recepción**.
- Para volver a la bandeja de entrada de tareas, pulse la pestaña **Bandeja de entrada**.
- Para suprimir las tareas no deseadas, selecciónelas y, a continuación, pulse

Suprimir



Capítulo 26. Acceso a detalles

Las aplicaciones de acceso a detalles son una red de informes enlazados por los que pueden navegar los usuarios, manteniendo su contexto y enfoque, para explorar y analizar información.

El acceso a los detalles le ayudará a crear aplicaciones de mayor tamaño que un solo informe.

Por ejemplo, tiene un informe de Analysis Studio que muestra los ingresos y desea poder acceder a los detalles de un informe de Creación de informes en el que se muestra información detallada de los ingresos planificados y reales.

Otro ejemplo: tiene un informe de Analysis Studio en el que se enumeran las diez promociones más importantes por minorista y desea poder acceder a los detalles de un informe de Creación de informes en el que se muestran los ingresos del plan de promoción.

El acceso a detalles funciona transmitiendo información del objeto de origen al de destino, que generalmente es un informe. Se define lo que se transmite del informe de origen mediante el establecimiento de correspondencias por parte del sistema entre la información del contexto de la selección del informe de origen en el contenido del destino (acceso a detalles dinámico) o mediante la definición de parámetros en el destino (acceso a detalles con parámetros). Se define el acceso a detalles para el origen, en el nivel del paquete o en el nivel del informe. Dentro de un paquete, se controla el ámbito de los datos para los que está disponible el acceso a detalles en la definición para acceder a detalles. En un informe, se define el acceso a detalles en un elemento del informe.

Qué debe saber

Para que un enlace de acceso a detalles funcione, debe conocer lo siguiente:

- Qué es o qué será el informe de origen
- Qué es o qué será el informe de destino
- Si los usuarios del enlace de acceso a detalles del informe de origen tienen los permisos pertinentes para ver o ejecutar el informe de destino
- Qué relación tienen los datos de los dos informes

En función de los datos subyacentes, puede crear una definición de acceso a los detalles (acceso a los detalles dinámico) o bien que correlacione los metadatos de origen con parámetros definidos en el informe o el paquete de destino (acceso a los detalles con parámetros).

- Si se ejecutará o se abrirá el informe de destino

El destino del acceso a detalles generalmente es una definición de informe guardado. El informe se puede crear en Creación de informes, PowerPlay Studio, Query Studio o Analysis Studio. El destino de acceso a detalles también puede ser un paquete que contiene un PowerCube, en cuyo caso se crea una vista predeterminada del PowerCube.

- Si se ejecuta el destino, en qué formato y con qué filtros

Si no desea ejecutar el informe de destino a petición, puede crear en su lugar un enlace a un marcador de la salida guardada.

Orígenes y destinos

Existen numerosas combinaciones distintas de origen y destino. Así, puede acceder a detalles

- Entre informes creados en paquetes diferentes en tipos de origen de datos diferentes, como, por ejemplo, de un análisis creado a partir de un cubo a un informe detallado creado a partir de un origen de datos relacionales. Para obtener más información sobre la creación de acceso a detalles en los paquetes, consulte “Configuración del acceso a detalles en los paquetes” en la página 391.
- De un informe existente a otro informe mediante Creación de informes. Para obtener información sobre la creación de acceso a datos en un informe, consulte: “Configuración del acceso a detalles en un informe” en la página 399
- Entre informes de IBM Cognos Viewer creados en Creación de informes, Query Studio, PowerPlay Studio y Analysis Studio
- De cubos Series 7 PowerPlay Web a informes de IBM Cognos Analytics.

Introducción a los conceptos de acceso a los detalles

Antes de configurar el acceso a detalles, debe comprender los conceptos clave. El conocimiento de los mismos le ayudará a evitar errores de tal modo que los consumidores de informes puedan acceder a los detalles de la forma más eficaz posible.

Rutas de acceso a los detalles

Se puede crear una ruta de acceso a los detalles en un informe de origen o mediante Definiciones de acceso a los detalles. Una ruta de acceso a detalles es la definición de la ruta que se utiliza el moverse de un informe a otro, incluido el modo en el que se transmiten los valores de datos entre los informes.

Utilizando **Definiciones de acceso a los detalles**, puede crear una ruta de acceso a los detalles desde cualquier informe del paquete de origen en cualquier informe de destino de otro paquete. Este tipo de definición para acceso a detalles se almacena en el paquete de origen.

Para cualquier informe de destino que contenga parámetros, los parámetros de destino se deben correlacionar a los metadatos correctos de la ruta de acceso a detalles. De este modo, se garantiza que los valores del informe de origen se transmiten a los valores de parámetros correctos y que el informe de destino se filtra correctamente. Si no se correlacionan los parámetros, se solicitarán los valores a los usuarios cuando se ejecute el informe de destino.

Una ruta de acceso a los detalles basada en informes hace referencia a una ruta creada y almacenada en un informe de origen. Este tipo de ruta de acceso a detalles también se denomina acceso a detalles creado. La ruta está asociada a una columna de datos, un gráfico o una tabla de referencias cruzadas determinados en el informe de origen y solo está disponible cuando los usuarios seleccionan dicha área del informe. Si hay disponible una definición para acceso a detalles creada, aparece un hipervínculo en el informe de origen cuando se ejecuta.

El acceso a los detalles basado en informes se limita a los informes de origen y a cualquier informe de destino. Utilice este tipo de acceso a los detalles cuando desee transmitir los valores de elemento de datos o los resultados de parámetros

de un informe de origen a uno de destino, los resultados de una expresión de informe a un informe de destino o utilizar un enlace de URL como parte de la definición para acceso a detalles.

Contextos de la selección

El contexto de la selección representa la estructura de los valores seleccionados por el usuario en el origen.

En IBM Cognos Analysis Studio, incluye el área de contexto. Cuando se utiliza una definición para acceso a detalles del paquete, el contexto de la selección se utiliza para ofrecer valores de parámetros correlacionados (acceso a detalles con parámetros) o para correlacionar los valores y los elementos de datos correspondientes.

También se pueden definir enlaces para acceso a detalles para abrir el objeto de destino en un marcador. El contexto de la selección también puede especificar el contenido de este marcador.

El acceso a los detalles es posible entre la mayoría de las combinaciones de los estudios de IBM Cognos Analytics. Cada estudio está optimizado para los objetivos y las aptitudes del público que lo utiliza y, en algunos casos, para el tipo de origen de datos para el que está diseñado. Por tanto, es posible que tenga que tener en cuenta cómo administran el contexto de la selección los distintos estudios al acceder a detalles entre objetos creados en estudios diferentes y la compatibilidad de los orígenes de datos. Al probar o depurar, puede ver cómo se correlacionan los valores de origen en distintos contextos mediante el ayudante para acceso a detalles.

Acceso a detalles en distintos formatos de informe

Los valores de la definición para acceso a detalles determinan el formato en el que los usuarios ven los resultados de los informes.

Por ejemplo, los usuarios pueden ver los informes de IBM Cognos Viewer como una página web HTML o bien abrirlos en IBM Cognos Query Studio, IBM Cognos PowerPlay Studio o IBM Cognos Analysis Studio. Si los usuarios disponen de PowerPlay Studio, puede que también vean la vista predeterminada de un PowerCube.

Los informes se pueden abrir como páginas HTML, o con formato de software PDF, XML, CSV o de hoja de cálculo Microsoft Excel. Cuando se define una ruta de acceso a detalles, es posible elegir el formato de salida. Esto puede resultar útil si el uso previsto del informe de destino no es la visualización en línea. Si se va a imprimir el informe, elija una salida como PDF; si se va a exportar a Excel para seguir procesándolo, opte por una salida como Excel o CSV, etc.

Para ejecutar informes o profundizar en destinos que ejecutan informes con el formato de texto delimitado (CSV), PDF, hoja de cálculo de Microsoft Excel (XLS) o XML, necesita tener la capacidad de generar salidas en el formato específico.

Nota: Solo se da soporte a PDF de obtención de detalles en Internet Explorer si se utiliza el plugin de Adobe PDF.

Si se define una ruta de acceso a detalles a un informe creado en Analysis Studio, PowerPlay Studio o Query Studio, los consumidores podrán abrir el informe en su estudio en lugar de en IBM Cognos Viewer. Esto puede resultar útil si prevé que

un consumidor utilice el informe de destino de acceso a detalles a modo de inicio de una sesión de análisis o consulta para buscar más información.

Por ejemplo, si una aplicación contiene un informe de tipo panel de control de datos de alto nivel, puede definir un enlace para acceso a detalles a Analysis Studio para investigar elementos de interés. A continuación, se puede acceder a detalles de la vista de Analysis Studio en un informe PDF para imprimirlo.

Nota: IBM Cognos Analytics - Reporting no muestra resultados de datos.

Conceptos relacionados:

“Formatos de informe” en la página 363

En IBM Cognos Analytics, puede visualizar informes en un navegador, o en función de sus permisos, puede generar informes en formatos que se pueden importar a otras aplicaciones. Los administradores pueden restringir el acceso a las capacidades necesarias para ejecutar informes con formatos de texto delimitado (CSV), PDF, hoja de cálculo de Microsoft Excel (XLS) o XML.

Acceso a los detalles entre paquetes

Es posible configurar el acceso a detalles entre paquetes.

Los dos paquetes pueden estar basados en distintos tipos de origen de datos, pero existen algunos límites. En la tabla siguiente se muestran las correlaciones de orígenes de datos que soportan el acceso a detalles.

Tabla 78. Correlaciones de orígenes de datos que soportan el acceso a detalles

Origen de datos de origen	Origen de datos de destino
OLAP	OLAP Nota: El acceso a detalles de OLAP a OLAP solo se soporta si los tipos de origen de datos son el mismo, por ejemplo, de SSAS a SSAS.
OLAP	Relacionales modelados dimensionalmente
OLAP	Datos relacionales Nota: Para obtener más información, consulte “Claves de empresa” en la página 388.
Relacionales modelados dimensionalmente	Relacionales modelados dimensionalmente
Relacionales modelados dimensionalmente	Relacionales
Relacionales	Relacionales

Referencias de marcador

Al acceder a los detalles, los valores que se transmiten se suelen utilizar para filtrar el informe, aunque no siempre.

IBM Cognos Analytics soporta marcadores en informes PDF y HTML guardados, de modo que el usuario pueda desplazarse por un informe para ver la parte relevante en función de un parámetro de URL.

Por ejemplo, imagine que tiene un informe de inventario de gran tamaño planificado para que se ejecute de forma diaria o semanal durante las horas de inactividad con el fin de no afectar a los recursos. Los usuarios pueden ver este

informe como un destino porque contiene información detallada, pero usted desea que vean la salida guardada en lugar de ejecutar este informe de gran tamaño. Gracias a esta opción de Acción y a los valores de los marcadores, los usuarios pueden acceder a los detalles desde otra ubicación de origen en función de los productos para abrir el informe guardado en la página en la que se muestra el producto en el que desean centrarse.

Cuando se utiliza un marcador del informe de origen en una definición para acceso a detalles, el marcador proporciona el valor del parámetro de URL. Cuando los consumidores del informe accedan a los detalles mediante esta definición, verán la sección relevante del informe de destino.

Nota: Solo se da soporte a PDF de obtención de detalles en Internet Explorer si se utiliza el plugin de Adobe PDF.

Las referencias de marcador se limitan a informes previamente ejecutados con una salida en formato PDF o HTML que contienen objetos de marcador.

Miembros y valores

Los datos modelados dimensionalmente, tanto si se almacenan en cubos o como si se almacenan como datos relacionales modelados dimensionalmente (DMR), organizan los datos en dimensiones. Estas dimensiones contienen jerarquías, jerarquías que contienen niveles, niveles que, a su vez, contienen miembros.

Un ejemplo de dimensión es Ubicaciones. Una dimensión Ubicaciones puede contener dos jerarquías: ubicaciones por estructura organizativa y ubicaciones por geografía. Cualquiera de estas jerarquías puede contener niveles como País, Región y Ciudad.

Los miembros son las instancias de un nivel. Por ejemplo, Nueva York y Londres son miembros del nivel Ciudad. Un miembro puede tener varias propiedades, como Población, Latitud y Longitud. Internamente, un miembro se identifica mediante un nombre exclusivo de miembro (MUN). El método por el cual se deriva un MUN depende del proveedor de cubos.

Los modelos de datos relacionales están formados por asuntos de datos, como Empleados, que, a su vez, están formados por elementos de datos, como Nombre o Extensión. Estos elementos de datos tienen valores, como Pedro Rodríguez.

En IBM Cognos Analytics, los métodos de acceso a detalles disponibles son los siguientes

- De dimensional (miembro) a dimensional (miembro)
- De dimensional (miembro) a relacional (valor de elemento de datos)
- De relacional (valor de elemento de datos) a relacional (valor de elemento de datos)

Si el parámetro de destino es un miembro, el origen deberá ser un miembro. Normalmente, el origen y el destino deben pertenecer a una dimensión compatible. Sin embargo, si los datos lo soportan, también puede optar por definir una correlación mediante propiedades diferentes del elemento de metadatos de origen.

Si el parámetro de destino es un valor, el origen puede ser un valor o un miembro. Si el origen es un miembro dimensional, debe asegurarse de que el nivel o la dimensión están correlacionados correctamente al elemento de datos de destino en la definición para acceso a detalles. La clave de empresa del origen del miembro

normalmente coincidirá con el valor de destino relacional que, la mayoría de los casos, es la clave de empresa. Sin embargo, si los datos lo soportan, también puede optar por definir una correlación a partir del título del elemento de metadatos de origen.

Dimensiones compatibles

Si trabaja con varios orígenes de datos dimensionales, observará que algunas dimensiones tienen la misma estructura y otras no.

El motivo de esta diferencia en la estructura de las dimensiones es que los orígenes de datos pueden tener finalidades distintas.

Por ejemplo, una dimensión Cliente aparece en un almacén de datos Ingresos pero no en un almacén de datos Inventario. Sin embargo, las dimensiones Productos y Hora aparecen en ambos almacenes de datos.

Las dimensiones que aparecen en varios almacenes de datos son compatibles si su estructura es idéntica en todos los aspectos siguientes:

- Nombres de jerarquía
- Nombres de nivel
- Orden de nivel
- Claves internas

El acceso a detalles entre distintos almacenes de datos dimensionales sólo es posible si las dimensiones son compatibles y el almacén de datos de dimensión es del mismo tipo de proveedor, por ejemplo, IBM Cognos PowerCube, que el origen y el destino. Por ejemplo, en dos almacenes de datos para Ingresos e Inventario que contengan dimensiones Productos y Hora, se pueden definir las dimensiones Productos y Hora de forma diferente para cada almacén de datos. Sin embargo, para que el acceso a detalles entre las dimensiones Productos y Hora funcione, sus estructuras deben ser idénticas en cada almacén de datos.

Si no está seguro de si sus dimensiones son compatibles, debería comprobarlo con el modelador de datos para garantizar que el acceso a detalles produzca resultados significativos.

IBM Cognos Analytics no soporta las dimensiones compatibles generadas por IBM Cognos Framework Manager para orígenes de datos de SAP BW.

Orígenes de datos relacionales modelados dimensionalmente

Asegúrese de que cada nivel contiene una clave de empresa con valores que coinciden con el PowerCube u otros modelos DMR. Asimismo, debe asegurarse de que la propiedad **Clave de empresa raíz** está configurada y utiliza la clave de empresa del primer nivel de la jerarquía. De este modo, se asegurará de que tiene un nombre exclusivo de miembro compatible cuando intente acceder a los detalles con miembros de esta dimensión.

Claves de empresa

Cuando se define el acceso a detalles de un miembro en un valor relacional, se transmite la clave de empresa del miembro de forma predeterminada.

Esto implica que el parámetro de destino relacional debe configurarse utilizando el elemento de datos con un valor coincidente, el cual, la mayoría de las veces, es el elemento de datos de clave de empresa. También se puede optar por pasar el título del elemento de metadatos de origen.

Por ejemplo, los empleados se suelen identificar de forma exclusiva con un número de empleado, no con su nombre, porque puede que no sea exclusivo. Cuando se accede a los detalles de un miembro dimensional en un elemento de datos relacionales, el valor proporcionado es la clave de empresa. Por lo tanto, se debe definir el parámetro del informe de destino para que acepte un valor de clave de empresa. La lógica exacta utilizada para definir el valor de clave de empresa proporcionado depende del proveedor de cubos. En el caso de los PowerCubes de IBM Cognos, el valor de clave de empresa es la propiedad **Origen** definida para el nivel en IBM Cognos Transformer. Los PowerCube de IBM Cognos Series 7 Transformer pasan el valor de origen si se ha habilitado el distintivo de acceso a detalles antes de crear el cubo. De lo contrario, se utiliza el código de categoría.

En IBM Cognos Analytics - Reporting, puede determinar la clave de empresa de miembro utilizando una expresión como `roleValue('_businessKey',[Equipo de acampada])`. Esta expresión distingue entre mayúsculas y minúsculas.

Las claves de empresa SSAS 2005 de varias partes no tienen soporte en las operaciones de acceso a detalles.

Consejo: Cuando otros usuarios ejecuten el informe de acceso a detalles, puede optar por no solicitarles una clave de empresa. En Creación de informes, se puede crear una página de solicitud con un texto que sea familiar para los usuarios, pero que filtre la clave de empresa. El modelador de IBM Cognos Framework Manager permite asimismo configurar la opción **Referencia de elemento de visualización** de la propiedad **Información de solicitud** para utilizar la clave de empresa cuando se utilice el elemento de datos en una solicitud.

Ámbito

El ámbito es específico de las definiciones para acceso a los detalles creadas mediante Definiciones para acceso a los detalles (definiciones para acceso a los detalles del paquete). Define cuándo se muestra el informe de destino a los usuarios en función de los elementos que incluye el informe de origen.

Por lo general, el ámbito de una ruta de acceso a detalles se define de tal modo que coincida con un parámetro transmitido. Por ejemplo, en el caso de un informe de destino que contiene una lista de empleados, normalmente se desea mostrar el informe como una opción de acceso a detalles disponible sólo cuando un usuario visualiza nombres de empleado en un informe de origen. Si los nombres de empleado no se encuentran en el informe de origen, y se ha configurado el ámbito en el nombre de empleado de la definición para acceso a detalles, el informe de empleados no aparecerá en la lista de informes de destino de acceso a detalles disponibles de la página **Ir a**. Puede establecer el ámbito como medida o elemento del informe.

En el acceso a detalles basado en informes, en aquellos casos en los que la ruta de acceso a detalles está asociada a una columna de informe específica, la columna sirve de ámbito.

Parámetros correlacionados

Los destinos de acceso a detalles pueden contener parámetros existentes o puede añadir parámetros al destino para tener un mayor control del enlace de acceso a detalles.

Normalmente se correlacionan todos los parámetros de un destino de acceso a detalles a elementos desde el origen.

Al correlacionar elementos de origen que son miembros de OLAP o DMR a parámetros de destino, puede escoger entre un conjunto de propiedades de miembro relacionadas para satisfacer los requisitos del parámetro de destino. Para un destino dimensional, un elemento de origen dimensional utiliza el nombre exclusivo de miembro de forma predeterminada. Para un destino relacional, un elemento de origen dimensional utiliza la clave de empresa de forma predeterminada.

Por ejemplo, podría modificar la propiedad de miembro de origen que se utiliza para una correlación al título de miembro en lugar de a la clave de empresa para que coincida con el parámetro en un destino relacional. Para un destino dimensional, puede definir un parámetro que acepte una propiedad particular (por ejemplo, una clave de empresa o nombre exclusivo padre) y, a continuación, transferir la propiedad de origen apropiada para satisfacer ese destino.

Nota: Si define el acceso a detalles entre dimensiones no compatibles, debe probarlo con cuidado para garantizar que los resultados tengan el comportamiento esperado.

Si no especifica correlaciones de parámetro, se le solicitarán de manera predeterminada los parámetros necesarios en el destino cuando utilice el enlace de acceso a detalles. Para personalizar este comportamiento, utilice el valor Mostrar páginas de solicitud.

Cuando la acción está establecida en **Ejecutar el informe con filtro dinámico**, se aplica un filtro adicional si los nombres del contexto del informe de origen coinciden con los nombres de los elementos del destino. Utilice también esta acción cuando no haya parámetros definidos en el destino.

Si los parámetros no están correlacionados correctamente, es posible que reciba un informe vacío, resultados incorrectos o un mensaje de error.

El origen y el destino no pueden contener nombres de parámetros idénticos cuando son de paquetes diferentes, aunque la estructura de datos sea compatible. Si el origen y el destino son del mismo paquete, no habrá restricciones.

Si tiene los permisos necesarios, puede utilizar el ayudante para acceso a detalles para comprobar los parámetros de origen que se han pasado y los parámetros de destino que se correlacionan para un enlace de acceso a detalles determinado.

Puede cambiar el comportamiento del filtro de acceso a detalles dinámico si desea obtener detalles para generar un filtro mediante la utilización de la clave de empresa de miembro en lugar del título de miembro predeterminado. Para obtener más información acerca del cambio del comportamiento del filtro de acceso a detalles, consulte *IBM CognosGuía de administración y seguridad*.

Fechas de acceso a los detalles entre PowerCubes y paquetes relacionales

El método habitual de acceso a detalles de OLAP a paquetes relaciones exige que el parámetro de informe de destino se establezca mediante la clave de empresa en los datos relacionales, lo que no funciona bien en el caso de las fechas.

Las fuentes de datos de OLAP regularmente ven las fechas como miembros, como 1 Trimestre de 2012, mientras que las fuentes de datos de relación ven las fechas como rangos, como 1/enero/2012 a 31/marzo/2012.

Existe una característica especial para acceder a detalles entre PowerCubes y paquetes relacionales. Asegúrese de que el parámetro de informe de destino está configurado con `in_range`. El parámetro debe ser de tipo fecha-hora y no entero.

A continuación encontrará un ejemplo:

```
[gosales_goretailers].[Orders].[Order date] in_range ?Date?
```

Asegúrese asimismo de que la definición para acceso a detalles se correlaciona al parámetro en el nivel de dimensión y de que el nivel de fecha de PowerCube no está configurado para suprimir las categorías en blanco. Si habilita la opción para suprimir las categorías en blanco del modelo de Transformer antes de crear el cubo, puede que el acceso a detalles de fechas no sea correcto. Esto se debe a que faltan valores en el rango.

Configuración del acceso a detalles en los paquetes

Una definición para acceso a detalles especifica un destino para el acceso a detalles, las condiciones en las que está disponible el destino (como el ámbito) y cómo ejecutar, abrir y filtrar el destino.

En IBM Cognos Analytics, una definición para acceso a los detalles se asocia a un paquete de origen. La ruta de acceso a detalles incluida en la definición para acceso a detalles está disponible para todos los informes basados en el paquete de origen con el que está asociada. El destino se puede basar en cualquier paquete de destino y se puede almacenar en cualquier lugar. Por ejemplo, todos los informes creados en el paquete de ejemplo Almacén de datos VA (análisis) o en una carpeta enlazada a este paquete pueden acceder a cualquier definición para acceso a detalles.

Nota: Puede definir el acceso a los detalles en determinados informes configurando la definición de acceso a los detalles en el informe en lugar de en el paquete, o restringir el acceso a los detalles modificando los valores del informe de manera que éste no esté disponible como destino de acceso a los detalles.

Se pueden generar definiciones de acceso a los detalles entre los informes creados en los distintos estudios y los informes basados en distintos paquetes y orígenes de datos.

El informe de destino se debe crear antes de comenzar a crear la definición de acceso a los detalles. Los destinos de acceso a detalles pueden ser informes, análisis, vistas de informe, paquetes PowerCube y consultas.

Las definiciones de acceso a los detalles soporta los paquetes dimensionales y relacionales.

Antes de empezar

Para ejecutar informes o profundizar en destinos que ejecutan informes con el formato de texto delimitado (CSV), PDF, hoja de cálculo de Microsoft Excel (XLS) o XML, necesita tener la capacidad de generar salidas en el formato específico.

Procedimiento

1. Compruebe el destino de acceso a detalles:
 - Confirme que los usuarios de acceso a detalles tengan acceso al destino.
 - Si lo desea, oculte el destino para el acceso directo.
 - Si es necesario, compruebe qué parámetros existen en el destino.
Cuando una definición para acceso a detalles enlaza objetos de distintos paquetes, debe tener en cuenta los tipos de datos utilizados tanto en el objeto de origen como en el de destino. Revise la estructura y los valores de los datos que tiene previsto transmitir en el acceso a detalles y asegúrese de crear parámetros apropiados para el escenario, si ha definido parámetros, o de que el acceso a detalles dinámico funcione correctamente.
2. Inicie **Definiciones de acceso a los detalles**.
3. Desplácese hasta el paquete para el que desea crear la definición para acceso a detalles.
4. Pulse el icono **Definición para nuevo acceso a detalles** de la barra de herramientas.

Consejo: Si no aparece el icono **Definición para nuevo acceso a detalles**, asegúrese de que está en el nivel del paquete y no en una carpeta de dicho paquete. Las definiciones para acceso a detalles se deben almacenar en el nivel de paquete.

5. Escriba un nombre para la definición para acceso a detalles.
6. Si lo desea, escriba una descripción y una sugerencia, y pulse **Siguiente**.
7. Siga las instrucciones que aparecen en pantalla:
 - Si lo desea, restrinja el ámbito a un elemento de consulta o a una medida en el origen.
Si el destino contiene parámetros, deberá establecer el ámbito para los parámetros que se correlacionen con el informe de destino.
 - Seleccione el destino desde cualquier paquete.
Si los destinos de PowerPlay están disponibles, deberá seleccionar si establecerá el destino como informe o como PowerCube.
 - Pulse **Siguiente**.
8. En la sección **Acción**, especifique cómo abrir el objeto de destino al ejecutar el enlace de acceso a detalles y, si ha seleccionado ejecutar el informe, en la sección **Formato**, especifique el formato para ejecutar el informe.

Nota: Los usuarios pueden modificar los valores de **Acción** cuando utilicen el enlace al acceso a detalles. Si utiliza marcadores en el destino, entonces debe seleccionar la acción **Ver informe más reciente**.

9. En la tabla **Valores de los parámetros**, especifique cómo correlacionar los metadatos de origen a los parámetros que existan en el objeto o el informe de destino.

Por ejemplo, si accede a detalles entre orígenes de datos OLAP, los miembros se correlacionan entre sí. Si accede a detalles de un origen de datos OLAP a

un origen de datos relacionales, el valor de origen (miembro) se correlacionará con el nombre del elemento de consulta (valor).

Normalmente, cada parámetro que existe en el destino debe estar correlacionado con los metadatos de origen. Si no es así, al usuario del informe se le solicitarán los valores que falten cuando se utilice el enlace de acceso a detalles.

10. Pulse **Correlacionar con metadatos** o pulse el botón Editar .

- En la pantalla que aparece, seleccione los metadatos del origen que se van a correlacionar con el parámetro de destino.
- Si el paquete de origen es dimensional, puede seleccionar la propiedad del elemento de metadatos de origen que se vaya a utilizar en la correlación. De forma predeterminada, la clave de empresa se utiliza para un destino relacional, y el nombre exclusivo de miembro se utiliza para un destino dimensional.
- Repita esto para cada parámetro de la lista.

11. En la sección **Mostrar páginas de solicitud**, especifique cuándo aparecerán las páginas de solicitud.

- En la pantalla que aparece, seleccione los metadatos del origen que se van a correlacionar con el parámetro de destino.
- Si el paquete de origen es dimensional, puede seleccionar la propiedad del elemento de metadatos de origen que se vaya a utilizar en la correlación. De forma predeterminada, la clave de empresa se utiliza para un destino relacional, y el nombre exclusivo de miembro se utiliza para un destino dimensional.
- Repita esto para cada parámetro de la lista.

Puede establecer esta acción sólo cuando haya parámetros en el informe de destino y se vaya a ejecutar. Si modifica la acción a **Ver informe más reciente**, por ejemplo, para referencias de marcador, la propiedad **Mostrar páginas de solicitud** se inhabilitará porque utilizará un informe ejecutado previamente. Si opta por abrir el informe directamente en Analysis Studio, entonces la propiedad **Mostrar páginas de solicitud** también estará inhabilitada.

Especifique los valores de solicitud en **Propiedades de informe, Solicitar valores**.

12. Pulse **Finalizar**.

13. Ejecute un informe del paquete de origen y pruebe el enlace de acceso a detalles.

Nota: La definición para acceso a detalles se asocia y se guarda con el origen. Los errores relacionados con el destino sólo se generan cuando se ejecutan los enlaces de acceso a detalles, no cuando se guarda la definición para acceso a detalles.

Conceptos relacionados:

“Formatos de informe” en la página 363

En IBM Cognos Analytics, puede visualizar informes en un navegador, o en función de sus permisos, puede generar informes en formatos que se pueden importar a otras aplicaciones. Los administradores pueden restringir el acceso a las capacidades necesarias para ejecutar informes con formatos de texto delimitado (CSV), PDF, hoja de cálculo de Microsoft Excel (XLS) o XML.

Edición de las definiciones de acceso a los detalles existentes

Puede editar las definiciones de acceso a los detalles existentes.

Procedimiento

1. En la página de bienvenida de IBM Cognos Analytics, pulse **Nuevo > Otros > Definiciones de acceso a los detalles**.
2. Pulse el nombre de un paquete para ver sus definiciones para acceso a detalles.
3. Para la definición para acceso a detalles que desea modificar, pulse el icono **Establecer propiedades**  en la columna **Acciones**.

Consejo: Si no ve las definiciones para acceso a detalles, compruebe que no se encuentra en una carpeta del paquete. Todas las definiciones para acceso a detalles se almacenan en el nivel raíz del paquete. Si no ve una definición para acceso a detalles específica, verifique que dispone de los permisos correctos.

4. Pulse la pestaña **Destino**.
5. Realice las modificaciones necesarias y pulse **Aceptar**.
6. Ejecute un informe del paquete de origen y pruebe el enlace de acceso a detalles.

Nota: La definición para acceso a detalles se asocia y se guarda con el origen. Los errores relacionados con el destino sólo se generan cuando se ejecutan los enlaces de acceso a detalles, no cuando se guarda la definición para acceso a detalles.

Configuración de parámetros para un informe de acceso a detalles

Para obtener mayor control sobre el acceso a detalles, puede definir parámetros en el informe de destino.

Configuración de parámetros para un destino de acceso a los detalles

Para obtener mayor control sobre el acceso a detalles, puede definir parámetros en el informe de destino.

Procedimiento

1. Abra el informe de destino.
2. Asegúrese de que el informe está disponible para el acceso a detalles:
 - En el menú **Datos**, seleccione **Comportamiento de detalle**.
 - En la pestaña **Básico**, seleccione **Aceptar filtros dinámicos cuando este informe sea un destino de acceso a detalles** y pulse **Aceptar**.
3. Cree un parámetro que servirá como columna de acceso a detalles o que se utilizará para filtrar el informe. (Menú **Datos, Filtros**).

Por ejemplo, para acceder a los detalles de la línea de producto o utilizarla como filtro, cree un parámetro como el siguiente:

[Línea de producto]=?prodline_p?

Consejo: Utilice los operadores **in** o **in_range** si desea que el informe de destino acepte varios valores o un rango de valores.

4. En el cuadro **Uso**, especifique lo que se hará cuando un valor del parámetro de destino no se transmita como parte de un acceso a detalles:
 - Para especificar que los usuarios deben pulsar un valor del informe de origen, pulse **Requerido**.

Si un valor del parámetro de destino no se transmite, a los usuarios se les solicitará que seleccionen un valor.

- Para especificar que no es necesario que los usuarios pulsen un valor del informe de origen, pulse **Opcional**.
A los usuarios no se les solicitará que seleccionen un valor y el valor no estará filtrado.
- Para especificar que no se utilice el parámetro, pulse **Desactivado**.
El parámetro no se utiliza en el informe y, por tanto, no está disponible para las definiciones para acceso a detalles. Para obtener más información sobre cómo definir parámetros de informe, consulte Creación de informes *Guía del usuario*.

Consejo: Si se necesita el parámetro en el informe por otros motivos, también puede especificar no utilizarlo en la definición para acceso a detalles (tabla **Parámetros, Método, No usar parámetro**).

Resultados

La definición para acceso a detalles controla cuándo se muestran las páginas o los parámetros de solicitud.

Configuración de parámetros para un destino de acceso a detalles en Query Studio

Para obtener mayor control sobre el acceso a detalles, puede definir parámetros en el informe de destino en Query Studio.

Procedimiento

1. Abra el informe de destino en Query Studio.
2. Asegúrese de que el informe está disponible para el acceso a detalles:
 - En el menú, seleccione **Ejecutar informe, Opciones avanzadas**.
 - Seleccione **Habilitar acceso a detalles de un paquete en la salida de informe** y pulse Aceptar.
3. Cree un filtro que servirá como parámetro de acceso a detalles o que se utilizará para filtrar el informe.
 - Seleccione la columna por la que desea filtrar y pulse el botón de filtrado.
 - Cambie los valores según sea necesario y pulse Aceptar.

Configuración de parámetros para un destino de acceso a detalles en Analysis Studio

Es posible crear un análisis de destino de acceso a detalles y añadirle parámetros de destino estableciendo una dimensión como parámetro de destino.

Al crear una definición para acceso a detalles para el análisis, este parámetro aparece en la lista de parámetros de destino.

Para soportar la obtención de detalles de nivel inferior en la dimensión y posteriormente el acceso a detalles, correlacione la dimensión de los metadatos de origen con la dimensión de destino. El miembro o los miembros que actualmente se encuentran en la vista se transmiten al análisis de destino como valores de filtro. Esta acción se aplica a cualquier consulta, informe o análisis utilizado en acciones de acceso a los detalles. Para soportar el acceso a detalles directamente de un nivel particular, correlacione dicho nivel de los metadatos de origen con la dimensión de destino.

Se pueden establecer varios parámetros en un destino de análisis. Sin embargo, no se pueden transmitir miembros en una selección configurada en Analysis Studio.

Procedimiento

1. En Analysis Studio, cree un análisis de referencias cruzadas mediante el paquete configurado para análisis de acceso a detalles.
2. Si lo desea, añada como fila o columna el elemento de datos que desee que sea la solicitud.
3. Mueva o añada la dimensión o el nivel que desee que sea un parámetro de destino al área **Contexto**.

Nota: No se pueden transmitir miembros en una selección configurada en Analysis Studio.

4. Visualice la lista para el elemento en el área **Contexto** y pulse **Usar como parámetro "Ir a"**.
5. Guarde este análisis como informe de destino.
Ahora puede crear la definición para acceso a detalles en un paquete de origen.

Resultados

Cuando cree la definición para acceso a detalles y utilice el análisis de referencias cruzadas como destino, el elemento de parámetro **Ir a** del análisis aparecerá como parámetro de acceso a detalles.

Depuración de una definición para acceso a detalles

IBM Cognos Analytics incluye una funcionalidad de depuración que se puede utilizar para detectar problemas con las definiciones de acceso a los detalles y para corregir los errores de acceso a los detalles.

También le puede ayudar a entender cómo funciona el acceso a detalles, especialmente a través de diferentes tipos de orígenes de datos. A esta funcionalidad también se la denomina ayudante para acceso a detalles. También puede depurar definiciones para acceso a detalles que se hayan creado en un PowerCube y se hayan migrado a IBM Cognos Analytics.

Si el informe de destino no recibe ningún parámetro, compruebe la correlación de la definición para acceso a detalles y asegúrese de que se crearon los parámetros en relación con el tipo de datos correcto para el escenario de acceso a detalles. Por ejemplo, si desea crear una definición para acceso a detalles desde un paquete OLAP hasta un informe de destino basado en un paquete relacional, deberá configurar los parámetros de destino en un elemento de consulta que tenga el mismo valor que título de miembro o la clave de empresa OLAP. Para obtener más información, consulte "Miembros y valores" en la página 387.

Si el informe de destino se filtra con los valores incorrectos, compruebe los valores que se hayan correlacionado del informe de origen al informe de destino.

Debe tener los permisos necesarios para utilizar el ayudante para acceso a detalles. La información que proporciona el ayudante para acceso a detalles estará disponible en la página **Ir a** cuando ejecute el acceso a detalles. El ayudante para acceso a detalles proporciona la siguiente información.

Valores de origen transmitidos

Los valores de origen son los valores del contexto de la selección disponibles para transmitirse al informe de destino cuando el usuario desee acceder a los detalles

del informe o el objeto de destino. Por ejemplo, si accede a detalles desde un origen en Analysis Studio, verá los valores en la intersección que seleccionó antes de la acción de acceso a detalles y los valores en el área de contexto.

Los valores de la lista de depuración son los valores del informe de origen que se transformaron a través de una operación de acceso a detalles.

- Valor de visualización

Muestra el valor que ven los usuarios cuando utilizan este elemento de datos o este miembro. Para los miembros de OLAP, éste es el título o la etiqueta de miembro. Por ejemplo: Telephone es un miembro de la dimensión Order Method.

- Usar valor

Muestra el valor que utilizan los informes y los análisis de IBM Cognos cuando recuperan el elemento de datos o el miembro. Para los miembros de OLAP, éste es el nombre exclusivo de miembro (MUN). Por ejemplo:

[great_outdoors_company].[Order Method].[Order Method].[Order Method1]->:[PC].[@MEMBER].[2] es el MUM del miembro Telephone en la dimensión Order Method.

Correlación de destino

Si decide utilizar parámetros en el informe de destino, la correlación de destino mostrará el nombre de cada parámetro que se asignó en la definición para acceso a detalles y los valores que el informe de origen intenta transmitir a ese parámetro.

- Nombre de parámetro

Muestra una lista de parámetros de destino válidos correlacionados en la definición para acceso a detalles para recibir información de la jerarquía, el nivel o el elemento de consulta en el que realizó la acción de acceso a detalles.

Puede ver sólo los parámetros en los que hay una correlación válida y sólo los nombres de los parámetros. Por ejemplo, si el informe de destino contiene un parámetro para Product Type y la definición para acceso a detalles correlaciona ese parámetro de destino con los metadatos de nivel Product Type, verá este parámetro de destino sólo si intenta acceder a detalles en el nivel Product Type en el informe de origen. Con el acceso a detalles en el nivel Product Line no se muestra este parámetro de destino.

Asegúrese de que los parámetros de destino de las definiciones para acceso a detalles estén correlacionados correctamente. Los parámetros que no están correlacionados correctamente pueden recibir información de los metadatos de origen incorrectos, especialmente donde están los valores de datos que no son únicos. Si no puede ver los parámetros de destino o los parámetros que esperaba ver en la lista **Ver correlación de destino**, compruebe la correlación de parámetros en la definición de acceso a detalles.

- Valor de visualización

Muestra el valor que ven los usuarios cuando utilizan un elemento o un miembro de datos. Para los miembros de OLAP, éste es el título o la etiqueta de miembro. Por ejemplo: Telephone es un miembro de la dimensión Order Method.

- Usar valor

Muestra el valor transformado que utiliza la definición para acceso a detalles cuando se transmite un miembro o un valor de elemento de datos al parámetro de destino.

Los miembros de OLAP transmitidos a parámetros de destino relacionales obtienen la clave de empresa de los miembros MUN y sólo transmiten la clave de empresa. Si se utiliza el ejemplo del miembro Telephone en Order Methods, la clave de empresa será 2. Si no está seguro de cuál es la clave de empresa de un

miembro, puede escribir una expresión como `roleValue('_businessKey',[member])`. Este valor se transmite al parámetro de destino.

Los miembros de OLAP transmitidos a un parámetro de destino basado en otro paquete OLAP del mismo tipo de OLAP muestran un MUN transformado. Si se utiliza el ejemplo *Order Methods*, ahora el MUN se transforma y la definición para acceso a detalles utiliza el valor `[great_outdoors_company].[Order Method].[Order Method].[Order Method1]-> [Order Method1]`.

`[2]:[PC].[@MEMBER].[2]`. La porción media de `[Order Method1][2]` es donde la definición para acceso a detalles busca el miembro correcto en el informe de destino cuando los informes de orígenes de datos OLAP son diferentes. Para ver el MUM de un número específico, puede buscar en las propiedades del miembro en Creación de informes y buscar en la propiedad *Member Unique Name*.

Acceso al ayudante para acceso a detalles

Puede utilizar el ayudante para acceso a detalles con fines de depuración cuando trabaje con definiciones de acceso a los detalles.

Antes de empezar

Para utilizar esta funcionalidad, debe tener los permisos necesarios para la función protegida **Ayudante para acceso a detalles** en IBM Cognos Administration.

Procedimiento

1. Seleccione un enlace en el informe de origen, pulse con el botón derecho en el enlace y seleccione **Ir a** o, desde PowerPlay Studio, pulse el botón de acceso a detalles.

Aparecerá la página **Enlaces relacionados** que muestra la lista de los informes de destino disponibles. Si no se muestra el informe de destino, revise los valores de ámbito en la definición para acceso a detalles.

Sugerencia: Si sólo hay un destino disponible, cuando seleccione **Enlaces relacionados**, el destino se abrirá sin mostrar la página **Ir a**.

2. Pulse **Ver valores de origen transmitidos** para ver los valores que puede pasar el informe de origen.
3. Junto al informe de destino, pulse la flecha abajo y seleccione **Ver correlación de destino**.

Aparecerá una lista de datos correlacionados válidos que muestra los valores de origen disponibles, y los valores de uso y de visualización.

4. Para cualquier conjunto de valores, pulse **Más información** para ver el XML para el contexto de la selección (origen transmitido) o la especificación de acceso a detalles (correlación de destino).

Ejemplo: depurar una definición para acceso a detalles

A continuación se muestra un ejemplo de depuración de definición para acceso a detalles.

El origen OLAP tiene una dimensión *Productos* con los niveles *Línea*, *Tipo* y *Nombre*. Ha definido un parámetro en el destino relacional para que coincida con cada nivel de esa dimensión de origen OLAP. Es posible que vea todos los parámetros de una única dimensión en la lista *Ver correlación de destino*. Esto sucede porque los parámetros de destino individuales se correlacionan con una única dimensión en la definición para acceso a detalles, en este caso a la dimensión

Productos. En el origen de datos OLAP tiene un valor de clave de empresa, o el valor de origen utilizado para crear los miembros, que se duplica en los tres niveles, como se muestra en la tabla siguiente.

Tabla 79. Ejemplo de correlación de parámetro problemática para la definición de acceso a los detalles

Nombre de parámetro	Valor de visualización	Usar valor
Parámetro de línea de producto	Equipo de acampada	1
Parámetro de tipo de producto	Material de cocina	1
Parámetro de nombre de producto	Cantimplora flexible Cocinero Viajero	1

La correlación de los tres parámetros a la dimensión Productos es correcta si los valores de uso no están duplicados en la dimensión. En la tabla anterior, los miembros de los tres niveles tienen el mismo valor de uso. En este caso, la operación de acceso a detalles no puede determinar qué nivel es el correcto porque el escenario indica que todos los niveles son válidos. En esta situación, el primer nivel encontrado con una clave de empresa o un valor de uso válido se cumplimenta mediante la definición para acceso a detalles. Esto puede producir un comportamiento inesperado.

Este ejemplo muestra los motivos por los que es importante asegurarse siempre de que los almacenes de datos y los orígenes OLAP estén diseñados con claves de empresa o valores de origen únicos. Para corregir esta situación, la definición para acceso a detalles debe tener correlacionado cada parámetro de destino a cada nivel asociado en los metadatos de origen antes que en la dimensión.

Configuración del acceso a detalles en un informe

Utilice Creación de informes para crear un informe de acceso a detalles de origen para enlazar dos informes con información relacionada. A continuación, puede acceder a información relacionada o más detallada de un informe seleccionando un valor o varios valores del informe de origen. También puede acceder a los detalles en el mismo informe si se crean marcadores.

Antes de empezar

Sugerencia: Para utilizar un informe como origen en una definición de acceso a los detalles, debe estar seleccionada la opción **Permitir paquete basado en el acceso a detalles** (menú **Datos, Comportamiento de detalle**). Ésta es la opción predeterminada.

Procedimiento

1. Abra el informe de destino.
2. Cree un parámetro que servirá como columna de acceso a detalles o para filtrar el informe.

Por ejemplo, para acceder a detalles o filtrar por Línea de producto, cree el siguiente parámetro:

[Línea de producto]=?prodline_p?

Consejo: Utilice los operadores **in** o **in_range** para que el informe de destino acepte varios valores o un rango de valores.

3. En el cuadro **Uso**, especifique lo que se hará cuando un valor del parámetro de destino no se pase como parte de un acceso a detalles:

- Para especificar qué usuarios deben seleccionar un valor, pulse **Requerido**.

Si un valor del parámetro de destino no se transmite, a los usuarios se les solicitará que seleccionen un valor.

- Para especificar qué usuarios no tienen que seleccionar un valor, pulse **Opcional**.

A los usuarios no se les solicitará que seleccionen un valor y el valor no estará filtrado.

- Para especificar que no se utilice el parámetro, pulse **Desactivado**.

No se utilizará el parámetro durante el acceso a detalles. Tampoco se utilizará en el informe con ninguna otra finalidad.

Sugerencia: Si se necesita el parámetro en el informe por otros motivos, también puede especificar no utilizarlo en la definición para acceso a detalles (tabla **Parámetros, Método, No usar parámetro**).

Resultados

El texto de acceso a detalles aparecerá como un hipervínculo azul en los elementos de texto en las áreas del informe que no contengan gráficos. Los consumidores del informe también pueden iniciar una acción de acceso a detalles pulsando el botón **Ir a** o pulsando con el botón derecho del ratón en el elemento y en **Ir a, Enlaces relacionados**. Si dispone de los permisos necesarios, podrá ver los parámetros que se han pasado del origen y cómo se han correlacionado en el objeto de destino utilizando el Ayudante para acceso a detalles en la página **Ir a**.

Especificar texto de acceso a detalles

Puede especificar el texto de acceso a detalles que aparecerá cuando los usuarios puedan acceder a los detalles de varios destinos.

Por ejemplo, si el informe lo ven usuarios de regiones diferentes, puede mostrar el texto en un idioma diferente para cada región.

Procedimiento

1. Haga clic en el objeto de acceso a los detalles y en el panel **Propiedades**, haga clic en **Definiciones de acceso a los detalles**.
2. Si existe más de una definición de acceso a detalles para el objeto, en el cuadro **Definiciones de acceso a los detalles**, pulse una definición.
3. Pulse la pestaña **Etiqueta**.
4. Para enlazar la etiqueta a una condición, en el cuadro **Condición** realice lo siguiente:
 - Pulse **Variable** y en una variable existente, o cree una nueva.
 - Pulse **Valor** y en uno de los valores posibles de la variable.
5. En el cuadro **Tipo de origen**, pulse el tipo de origen que desea utilizar.
6. Si el tipo de origen es **Texto**, pulse el botón de puntos suspensivos correspondiente al cuadro **Texto** y escriba el texto.

7. Si el tipo de origen es **Valor de elemento de datos** o **Etiqueta de elemento de datos**, pulse **Elemento de datos** y en un elemento de datos.
8. Si el tipo de origen es **Expresión de informe**, pulse el botón de puntos suspensivos correspondiente al cuadro **Expresión de informe** y defina la expresión.
9. Si la etiqueta está enlazada a una condición, repita los pasos del 5 al 8 para el resto de los valores posibles.

Resultados

Cuando los usuarios ejecuten el informe de origen y pulsen el enlace de acceso a detalles, aparecerá la página **Ir a**. El texto de acceso a detalles especificado aparecerá en cada destino. Si no ha especificado el texto de acceso a detalles en un destino, se utilizará el nombre de acceso a detalles.

Capítulo 27. IBM Cognos Workspace

IBM Cognos Workspace es una herramienta basada en web que le permite utilizar el contenido de IBM Cognos y orígenes de datos externos para crear sofisticados espacios de trabajo interactivos. Para obtener más información sobre IBM Cognos Workspace, consulte IBM Cognos Workspace *Guía del usuario*.

Para iniciar Cognos Workspace, en la página **Bienvenida**, pulse **Nuevo > Otros > Espacio de trabajo**.

Eliminación de la marcación HTML de los detalles de entrada RSS

En IBM Cognos Workspace, un usuario puede insertar un widget RSS desde la caja de herramientas. Una vez configurada la entrada RSS, el widget de entrada RSS muestra la marcación HTML cuando están habilitados los detalles de la entrada.

Se puede ocultar la marcación HTML cuando la opción **Mostrar detalles de la entrada** se ha habilitado especificando el valor avanzado, **CPSRssAllowUnsafeCharacters** en el asignador. Debe establecer el parámetro para cada asignador. Si hay varios asignadores, puede definir el parámetro globalmente.

Procedimiento

1. En IBM Cognos Administration, pulse en **Configuración > Asignadores y servicios**.
2. Para especificar el valor **CPSRssAllowUnsafeCharacters** para un único asignador, realice lo siguiente:
 - a. En la columna **Nombre**, pulse en un asignador y pulse en **Establecer propiedades**.
 - b. Vaya a **Servicio de presentación**, y pulse en **Establecer propiedades**.
 - c. Pulse en la pestaña **Valores** y, en **Entorno, Valores avanzados**, pulse en **Editar**.
 - d. Pulse **Reemplazar los valores adquiridos de la entrada padre**. Ahora, continúe con el paso 4.
3. Para especificar el parámetro **CPSRssAllowUnsafeCharacters** de forma global, para varios asignadores, realice lo siguiente:
 - a. En la barra de herramientas **Configuración**, pulse en **Establecer propiedades - Configuración**.
 - b. Pulse en la pestaña **Valores** y, en **Entorno, Valores avanzados**, pulse en **Editar**.
4. En el campo **Parámetro**, escriba **CPSRssAllowUnsafeCharacters** y, en el campo **Valor**, escriba **verdadero**.
5. Pulse **Aceptar**.

Resultados

La marcación HTML no se muestra en los detalles de entrada RSS.

Capítulo 28. Administración de IBM Cognos Mobile

IBM Cognos Mobile amplía la funcionalidad de la instalación existente de IBM Cognos Analytics a los dispositivos móviles de forma que los usuarios puedan ver e interactuar con el contenido de Cognos Analytics en sus tabletas o smartphones.

Con el Rich Client de Cognos Mobile, los usuarios pueden ver en sus dispositivos móviles los informes activos de Cognos Analytics - Reporting y los espacios de trabajo de Cognos Workspace. Los informes activos deben existir en el servidor como salidas guardadas o haberse enviado al usuario móvil. Los informes activos deben ejecutarse en el servidor, no en el cliente.

Se utiliza la funcionalidad de solicitudes y el mecanismo de planificación de Cognos Analytics para ofrecer informes personalizados en un tiempo razonable. Cognos Analytics incluída la seguridad basada en dispositivo y basada en servidor, para proteger el contenido de los informes y de los espacios de trabajo.

Muchos servidores de gestión y herramientas de administración específicos de dispositivos que Cognos Mobile utiliza ofrecen la posibilidad de eliminar contenido de forma remota desde un dispositivo o inhabilitar el dispositivo por completo. Por ejemplo, si se pierde o se roba un dispositivo, el administrador de Cognos Analytics administrador puede utilizar esta funcionalidad para proteger el contenido sensible del dispositivo. El administrador de Cognos Analytics también puede establecer una fecha de caducidad para un informe después de la cual dejaría de estar accesible hasta que el usuario volviera a autenticarse.

Cognos Mobile da soporte a las solicitudes entre el dispositivo móvil y el entorno de servidor para las siguientes funciones del producto:

- Buscar
- Examinar
- Ejecutar

La pestaña **Mobile** de IBM Cognos Administration proporciona prestaciones de administración centralizada para Cognos Mobile. Para acceder a esta pestaña, el administrador debe tener los permisos de acceso necesarios para la prestación **Administración de Mobile**. Se puede utilizar **Administradores de Mobile**, uno de los roles predefinidos en el espacio de nombres de **Cognos**, para especificar permisos de acceso sobre esta prestación.

Cognos Mobile utiliza el mismo conjunto de usuarios que Cognos Analytics. Para obtener información sobre la administración de Cognos Analytics, consulte otras secciones de *IBM Cognos Analytics Guía de administración y seguridad*.

Configuración previa de las aplicaciones de Cognos Mobile nativas para los usuarios

Configure la aplicación IBM Cognos Mobile para agilizar la configuración para los usuarios y controlar el funcionamiento de la aplicación en los dispositivos iOS y Android.

Acerca de esta tarea

Puede codificar y generar valores de configuración en un URL para distribuirlo a los usuarios de aplicación de Cognos Mobile en un mensaje de correo electrónico, una conversación o mediante otros métodos. Con este URL, los usuarios pueden configurar automáticamente la aplicación en los dispositivos móviles.

Se incluye el URL de servidor Cognos en la configuración para que los usuarios no necesiten escribir el URL en sus dispositivos móviles al configurar la aplicación.

Como medida de seguridad adicional, también se puede incluir una contraseña en la configuración. La contraseña de configuración de dispositivo móvil proporciona un sello de evidencia de falsificación para asegurar la integridad del URL de configuración y confirma que el origen del URL es válido. El URL de configuración y la contraseña no se deben transmitir nunca juntos utilizando el mismo medio, por ejemplo correo electrónico o conversación, al mismo tiempo. Los usuarios sólo deben entrar esta contraseña una vez cuando abren el URL de configuración.

Procedimiento

1. En **IBM Cognos Administration**, pulse la pestaña **Mobile**.
2. Pulse **Configuración remota**.
3. Para **URL del servidor de IBM Cognos**, escriba el URL de servidor de IBM Cognos Analytics: `http://nombre_servidor:número_puerto/bi/v1/disp`.
4. Habilite o inhabilite los valores siguientes:

Autenticación pass-through

Habilite este valor para que los usuarios puedan navegar al servidor de Cognos Analytics a través de las diferentes páginas web relacionadas que se les muestra.

De forma predeterminada, IBM Cognos Mobile necesita conectividad directa con el servidor de IBM Cognos Analytics. Si la conectividad directa no es posible porque intervienen productos de seguridad, este valor se debe habilitar. Los productos que intervienen pueden incluir CA SiteMinder, Tivoli Access Manager, Microsoft ISA Server o páginas de destino en redes WiFi públicas.

Descargas automáticas

Habilite este valor para que las aplicaciones de Cognos Mobile descarguen automáticamente las salidas de informe nuevas de la bandeja de entrada del usuario, así como los informes enviados al usuario. Este valor se debe habilitar, a menos que el ancho de banda pueda representar un problema.

Mostrar servidor de ejemplo

Habilite este valor para que las aplicaciones de Cognos Mobile accedan al servidor de ejemplo de Cognos Mobile. El servidor de ejemplos contiene informes de IBM Cognos de ejemplo que ilustran las prestaciones del software IBM Cognos. Los informes de ejemplo están optimizados para utilizarlos en dispositivos móviles.

Mantener estado de la aplicación

Habilite este valor para que la aplicación pueda restaurar el espacio de contenido más reciente después de reiniciarse. Por ejemplo, si la aplicación se cierra mientras se estaba viendo un informe en el espacio de contenido "Mis informes", la aplicación vuelve a abrir el espacio de

contenido "Mis informes" después de un reinicio. Si este valor está inhabilitado, la aplicación muestra el panel principal tras un reinicio.

Valor predeterminado: **Desactivado**

5. Opcional: Seleccione el recuadro de selección **Mobile Configuration Password** (Contraseña de configuración de dispositivo móvil) y escriba la contraseña que desee. La contraseña puede contener un máximo de 20 caracteres alfanuméricos y no puede contener espacios.

Si decide especificar esta contraseña, asegúrese de proporcionarla por separado del URL de configuración a los usuarios.

6. Opcional: Seleccione la casilla de verificación **Determinación del certificado SSL/TLS** y pegue la huella digital SHA-1 del certificado SSL o TLS que protege el punto de entrada al servidor de Cognos Analytics server. Un ejemplo de punto de entrada al servidor de Cognos Analytics sería un servidor web, un servidor proxy o un equilibrador de carga.

Habilite este valor para garantizar el que el cliente se comunica solamente con los servidores que están configurados con el certificado X.509v3 y que tienen la misma huella digital SHA-1.

Este valor es una secuencia de 40 caracteres hexadecimales (de la a a la f y del 0 al 9) sin signos de puntuación. Elimine los signos de puntuación del valor antes de pegarlo en este campo. Puede especificar varios valores de huella digital SHA-1 si los separa mediante un signo de dos puntos (:).

Consejo: En Firefox, para obtener la huella digital SHA-1, pulse el icono de candado de la barra de URL del navegador y luego pulse **Más información > Ver certificado**.

7. Pulse **Generar código de configuración móvil**. Se genera un URL codificado en base64 que incluye los valores de configuración especificados.

A continuación se muestra un ejemplo del URL generado:

```
cmug://aHR0cDovL3ZvdHRtb2IxL2NzcDI-dmVyc2lvdj0xLjAmcGFzc2lvZmYmYXV0b
2R3bj1vZmYmZG1zcHNhbXA9b24mcHdkPW9uJnNhbkQ9UW1zQVJoTTNPaFVfJmhhc2g9Q
VFhQUFBQklvOZqVTBoQk1vV2U3SEJiUjhkc2JBV2wrKzI0Y2d6cWxLMi8.
```

8. Copie el URL de configuración y proporciónelo a los usuarios de la aplicación Cognos Mobile por correo electrónico, conversación o por otros métodos.

Asegúrese de que se cumplen las condiciones siguientes al copiar y transmitir el URL:

- Todos los caracteres del URL, incluidos los guiones bajos (_), se seleccionan al copiar el URL.
- La aplicación que utiliza para transmitir el URL de configuración mantiene las mayúsculas y minúsculas del URL. El URL es sensible a las mayúsculas y minúsculas.

Resultados

Cuando los usuarios tocan el URL de configuración desde el administrador, la aplicación Cognos Mobile se abre en sus dispositivos iOS o Android. Los usuarios deben confirmar si desean continuar con la configuración automática. Si se ha especificado la contraseña de configuración de dispositivo móvil en el paso 5, los usuarios deben entrar la contraseña cuando se les solicite. Entonces la aplicación se configura con los valores especificados en el URL.

Si los usuarios entran una contraseña incorrecta o tocan el botón **Cancelar**, la aplicación se abre sin aplicar los valores de configuración.

Consejo: Algunas aplicaciones de correo electrónico proporcionan el URL de configuración a los usuarios como texto sin formato. En esta situación, los administradores puede colocar el URL en una página web accesible para los usuarios. En iOS, los usuarios pueden copiar y pegar el URL en el navegador y abrirlo desde allí.

Especificación de valores avanzados de Cognos Mobile

Puede configurar los valores avanzados de IBM Cognos Mobile globalmente para todos los servicios, para un asignador concreto o para un servicio de Mobile en particular.

Cuando se configuran globalmente, los valores que especifique los adquieren todas las instancias del servicio de Mobile. Puede reemplazar los valores globales especificando valores personalizados en el nivel de asignador o de servicio de Mobile.

Si la entrada de configuración contiene entradas hijo con valores que reemplazan a los valores globales, se pueden restablecer los valores personalizados de las entradas hijo para que utilicen los valores predeterminados. Para restablecer el valor por su valor predeterminado, suprimalo.

Procedimiento

1. En IBM Cognos Administration, en la pestaña **Configuración**, pulse **Asignadores y servicios** y realice una de las siguientes acciones:
 - Para configurar los valores avanzados globalmente, en la barra de herramientas de la página **Configuración**, pulse el icono **Establecer propiedades – Configuración**  y vaya al paso 3.
 - Para configurar los valores avanzados para un asignador concreto, localice el asignador y, en la columna **Acciones**, pulse el icono **Establecer propiedades** . A continuación, vaya al paso 3.
 - Para configurar los valores avanzados para un servicio de Mobile en concreto, pulse el asignador que incluye este servicio. En la lista de servicios de asignador, busque **MobileService**. En la columna **Acciones**, pulse el icono **Establecer propiedades**  asociado con el servicio y vaya al paso 3.
2. Pulse la pestaña **Valores**.
3. Para **Valores avanzados**, pulse **Editar**.
Si no aparece el parámetro en la lista, escriba el nombre.
4. Especifique el valor adecuado y pulse **Aceptar**.

Consejo: Para suprimir un valor avanzado, seleccione la casilla de verificación correspondiente y pulse **Suprimir**.

Configuración de un tema de Mobile

El tema de Mobile define el aspecto de la página de bienvenida de la aplicación IBM Cognos Mobile. De forma predeterminada, las aplicaciones cliente utilizan el tema predeterminado incluido en el producto. Puede crear su propio tema de Mobile para personalizar el aspecto de la aplicación y configurar el tema para ponerlo a disposición de los grupos de usuarios y roles que elija. Los administradores pueden volver al tema predeterminado en cualquier momento.

Acerca de esta tarea

Las tareas de configuración incluyen la habilitación del soporte para temas de Mobile, la adición, edición o supresión de los temas y la definición de los grupos y roles que pueden utilizar los temas.

Un mismo usuario puede pertenecer a diferentes grupos y roles y, por lo tanto, puede tener acceso a diferentes temas. Para asegurarse de que se aplican los temas correctos a los usuarios, los administradores deben pensar detenidamente qué grupos y roles pueden elegir al configurar el tema.

El tema predeterminado de Cognos Mobile se define en la plantilla defaultTheme.zip que se instala con el producto. Los administradores pueden utilizar esta plantilla como punto de partida al crear un tema personalizado. Aparte de eso, esta plantilla no es necesaria para que el producto funcione correctamente. Para obtener más información, consulte: "Creación de un tema de Mobile personalizado" en la página 410.

Procedimiento

1. Desde un navegador de escritorio, inicie la sesión en IBM Cognos Analytics con privilegios de administrador de Mobile.
2. Vaya a IBM Cognos Administration y pulse la pestaña **Mobile**.
3. Siga estos pasos para asegurarse de que el soporte de temas está habilitado para el servicio de Mobile:
 - a. Pulse **Configuración de servidor**.
 - b. En el grupo de valores **Política**, localice el valor **Soporte de temas de Mobile** y asegúrese de que tiene especificado el valor **themesOn**.
 - c. Pulse el botón **Aplique la configuración de Mobile** para guardar la configuración.
4. Abra la página **Configuración de la interfaz de usuario de Mobile**.

5. Para añadir un tema nuevo, pulse el icono **Nuevo tema** .
6. En la página **Configuración del tema de Mobile**, siga estos pasos:
 - a. En el cuadro **Especifique un nombre para el tema**, escriba el nombre del tema. Puede especificar cualquier nombre que sea comprensible en su entorno.
 - b. En el cuadro **Especifique un archivo de tema para cargarlo**, busque el archivo zip que contiene los recursos del tema.
 - c. En el cuadro **Especifique un grupo o rol**, pulse el botón **Elegir grupo** y elija los grupos o roles que necesitan utilizar el tema. Puede elegir grupos y roles del espacio de nombres de Cognos o de otros espacios de nombres activos.
 - d. Pulse **Aceptar** cuando todos los parámetros estén especificados correctamente.

El nombre del tema aparece en la página **Configuración de la interfaz de usuario de Mobile**.

7. Si desea editar el tema, pulse el icono **Establecer propiedades** correspondiente en la columna **Acciones**. Puede editar cualquier parámetro del tema.
8. Si desea suprimir el tema, seleccione la casilla de verificación correspondiente y

pulse el icono **Suprimir**  en la barra de herramientas.

Para volver al tema predeterminado de Cognos Mobile, suprima el tema que esté configurado en este momento. Los usuarios que utilizaban este tema volverán a utilizar automáticamente el tema predeterminado la próxima vez que se conecten al servidor de Cognos Analytics.

9. Con los dispositivos iOS y Android, conéctese al servidor para el que se ha configurado el tema para comprobar si los cambios se han aplicado correctamente.

Resultados

Los usuarios pueden utilizar la aplicación mientras los recursos del tema se descargan en sus dispositivos. El tema se aplica la siguiente vez que los usuarios se conecten al servidor de Cognos Analytics o al renovar la aplicación.

Cuando un usuario desea conectarse a varios servidores que puedan tener configurados temas diferentes, el tema que se aplica a ese usuario es el tema que está configurado para el servidor al que el cliente se conectó correctamente la primera vez. La conexión a otros servidores no cambia el tema del usuario aunque los servidores utilicen temas diferentes. Para cambiar el tema por el que está configurado para otro servidor, elimine la conexión con el servidor que tiene el tema actual. Después el usuario puede conectarse al servidor que utiliza el tema necesario.

Creación de un tema de Mobile personalizado

Puede crear un tema de Mobile personalizado para sustituir el tema predeterminado que se suministra con IBM Cognos Mobile.

Antes de empezar

Planifique el diseño del tema personalizado y prepare los recursos necesarios, como los archivos de imagen.

Acerca de esta tarea

Cuando se instala Cognos Mobile, el directorio de instalación *install_location/templates/mobile* contiene el archivo *defaultTheme.zip*. Esta es la plantilla de temas predeterminada. Puede utilizar esta plantilla como punto de partida al crear su propio tema personalizado.

El archivo *defaultTheme.zip* contiene diferentes directorios y archivos. El archivo *main_panel\index.html* es el único que se necesita para el tema personalizado. En este archivo definirá todos los recursos, como las imágenes, que desea utilizar en el tema personalizado, y modificará el esquema de color y los estilos de fuente.

El directorio *nls* de la plantilla de temas predeterminada contiene una estructura de directorios para los temas de idiomas concretos. Puede imitar esta estructura o implementar su propio mecanismo para crear temas en un idioma concreto.

Puede utilizar el procedimiento siguiente a modo de guía al crear un tema de Mobile personalizado basado en el tema predeterminado.

Procedimiento

1. Vaya al directorio *install_location/templates/mobile*, haga una copia del archivo *defaultTheme.zip* y guárdelo con otro nombre.
2. Extraiga los archivos del archivo .zip que ha creado en el paso anterior.

3. Edite el archivo `main_panel\index.html` según sea necesario. Este archivo debe contener referencias a todos los recursos que se incluyen con el tema.
4. Comprima todos los recursos del tema en un solo archivo .zip. Como mínimo, el archivo .zip debe contener el archivo `main_panel\index.html` modificado.
5. Guarde el archivo .zip del tema en el directorio que desee.

Ahora puede configurar IBM Cognos Mobile para que utilice el tema personalizado. Para obtener más información, consulte: “Configuración de un tema de Mobile” en la página 408.

Configuración de los servicios de Cognos Mobile

Puede configurar globalmente todas las instancias del servicio de IBM Cognos Mobile.

Acerca de esta tarea

Al aplicar globalmente los valores de configuración se garantiza que todas las instancias del servicio de Mobile están sincronizadas, lo que ayuda a evitar errores.

Importante: Los valores no se pueden personalizar para diferentes arrendatarios en un entorno de varios arrendatarios.

Procedimiento

1. Desde un navegador de escritorio, inicie la sesión en IBM Cognos Analytics con privilegios de administrador de Mobile.
2. Vaya a IBM Cognos Administration y pulse la pestaña **Mobile**.
3. Pulse la página **Configuración de servidor**.
4. Localice el valor que desea configurar y asígnele el valor que corresponda.
Puede configurar varios valores. Para ver una lista de valores, consulte: “Valores de configuración del servicio de Cognos Mobile”.
5. Pulse el botón **Aplique la configuración de Mobile**.

Valores de configuración del servicio de Cognos Mobile

Estos valores se utilizan para administrar la entrega del contenido de IBM Cognos Analytics a las aplicaciones móviles.

Valores de política

Estos valores definen cómo se entrega el contenido de Cognos Analytics a las aplicaciones móviles.

Número máximo de páginas a almacenar para cada informe

Las páginas que superen el límite especificado se descartan del dispositivo.

Este valor es aplicable a los informes de destino de acceso a detalles que se inician desde IBM Cognos Workspace.

Valor predeterminado: 5

Consejo: Si su entorno Cognos Mobile incluye solamente clientes nativos, configure el valor predeterminado en 50 páginas. De lo contrario, utilice el valor predeterminado sugerido, que es 5.

Número máximo de días para almacenar un informe

Especifica la duración máxima, en días, que un informe se almacena en la base de datos. Los informes que superan este límite se eliminan automáticamente del dispositivo.

Valor: de 1 a 999.

Valor predeterminado: 30

Número máximo de horas entre ejecuciones de informes de origen y de destino

Especifica, en horas, la cantidad máxima de tiempo permitido entre las ejecuciones de los informes de origen y de destino cuando se utiliza la característica de acceso a los detalles con informes activos en la aplicación nativa de iOS. Cuando la diferencia entre las dos ejecuciones sobrepasa esta cantidad, el destino de acceso a los detalles de la aplicación no se utiliza.

El valor predeterminado 1 significa que siempre que el informe de destino se haya ejecutado en un plazo de 1 hora después de la ejecución del informe de origen, el informe de destino se podrá abrir correctamente.

Un valor de 0 inhabilita la funcionalidad de acceso a los detalles de la aplicación. Al ejecutar el informe de origen después del informe de destino utilizando este valor, el informe de destino no se abre y se muestra un mensaje de error. El mensaje de error indica que el informe de destino no existe y que primero debe ejecutarse.

Este valor no se aplica a la aplicación nativa de Android.

Permiso para compartir capturas de pantalla de informe

Permite o impide que los usuarios de un cliente nativo compartan capturas de pantalla de los informes que estén viendo. Los usuarios pueden compartir capturas de pantalla de informe por correo electrónico o por otros métodos.

Valor: True o False.

Valor predeterminado: True.

Carpeta raíz de Mobile

Especifica el nombre la carpeta raíz desde la que se deben iniciar los usuarios de Cognos Mobile cuando exploren o busquen contenido de un dispositivo móvil.

Valor predeterminado: en blanco

El valor de este parámetro debe ser la ruta de búsqueda de Content Manager con el formato siguiente: `/content/package[@name='<nombre_carpeta_raíz>']`.

Si el valor está en blanco Cognos Mobile utiliza la carpeta de contenido raíz o la carpeta raíz que se haya especificado en el archivo `system.xml` de portal en el directorio `install_location/templates/ps`. Si añade una carpeta raíz, utilice la sintaxis del valor `consumer-root` en el archivo `system.xml`.

Consejo: Para encontrar la ruta de búsqueda en IBM Cognos Analytics, consulte las propiedades del paquete o de la carpeta que desee utilizar como carpeta raíz de Cognos Mobile. A continuación, pulse **Ver ruta de búsqueda, ID y URL**.

Soporte de temas de Mobile

Indica si se da soporte a los temas de Mobile personalizados para la aplicación web de IBM Cognos Mobile.

Valores: **themesOn** y **themesOff**

Valor predeterminado: **themesOff**

Número máximo de horas para acceder a los datos locales de Mobile almacenados en un dispositivo

Especifica el número máximo de horas si los usuarios de dispositivos móviles pueden acceder a los datos locales de Cognos Mobile almacenados en un dispositivo.

Valor: de 0 a 8760.

Valor predeterminado: 36.

Un valor de 0 inhabilita el mecanismo de la clave de contrato.

Número máximo de horas para almacenar las credenciales almacenadas en memoria caché

Si no desea almacenar credenciales en un dispositivo, escriba 0. Para almacenar las credenciales en un dispositivo, escriba un valor que sea mayor que el valor de tiempo de espera actual de IBM Cognos Analytics. Siempre que los usuarios inician la sesión, disponen de acceso a sus credenciales almacenadas en la memoria caché.

Valor: de 0 a 8760.

Valor predeterminado: 0

Número de horas máximo que el cliente puede permanecer no actualizado con informes planificados

Este valor se aplica a los casos en que un administrador planifica informes para un usuario en el servidor y el usuario no se comunica con el servidor antes de la fecha de caducidad, por ejemplo, para recuperar otros informes o para navegar por el portal de IBM Cognos Analytics portal. En la mayoría de los casos como, por ejemplo, cuando los informes se originan a partir de planificaciones existentes o de acciones iniciadas por el usuario, este valor no se tendrá en cuenta porque, normalmente, el dispositivo se retrasa respecto al servidor solamente unos segundos.

Valor: de 0 a 999.

Valor predeterminado: 24

El valor 0 envía informes para que se descarguen en dispositivos inmediatamente.

Valores de seguridad

Estos valores se utilizan para proteger la aplicación Cognos Mobile.

Nivel de cifrado de almacenamiento local para aplicaciones IBM Cognos Mobile

Especifica el método con el que se cifran los datos almacenados en los dispositivos iOS o Android.

Valores: NONE, AES128, AES256

Valor predeterminado: AES128

Consejo: La aplicación web no almacena datos localmente y no se ve afectada por este valor.

Tiempo de espera de sesión del código de seguridad en segundos

Especifica la necesidad de proporcionar un código de seguridad al acceder a la aplicación Mobile y el número máximo de segundos que la aplicación puede permanecer inactiva. El código de seguridad no puede repetir números ni contener números consecutivos.

Valor: de 1 a 8760.

Valor predeterminado: -1.

Un valor de -1 significa que no se necesita ningún código de seguridad. Un valor de 0 significa que el usuario debe crear un código de seguridad e introducirlo cada vez que accede a la aplicación.

Un valor mayor que 0 significa que el usuario debe crear un código de seguridad y puede dejar la aplicación inactiva durante el número de segundos que se especifique en el valor antes de tener que volver a especificar el código para usar la aplicación. Por ejemplo, si el valor se establece en 60, el usuario debe entrar un código de seguridad y puede dejar la aplicación Mobile inactiva durante 60 segundos.

Número máximo de intentos para entrar un código de seguridad al acceder a la aplicación IBM Cognos Mobile

Especifica el número máximo de veces que los usuarios pueden intentar entrar su código de seguridad al acceder a la aplicación Mobile.

Valor: de 1 a 99.

Valor predeterminado: 10.

Valores de notificación

Estos valores se utilizan para configurar las notificaciones push de Apple.

Notificaciones de correo electrónico para notificaciones push de Apple

Especifica la dirección o direcciones de correo electrónico de los administradores a los que debe notificarse acerca de la fecha de caducidad del certificado de notificaciones push de Apple.

El valor es una dirección de correo electrónico válida con el formato siguiente: *admin@dominio.com*. Si se especifican varias direcciones de correo electrónico, deben separarse con un punto y coma (;). Por ejemplo, *admin1@dominio.com;admin2@dominio.com*

Soporte para las notificaciones push de Apple

Habilita las notificaciones push de Apple para la aplicación nativa de iOS y especifica el texto del mensaje que se mostrará a los usuarios de dispositivos iOS. Los valores son:

- Ninguno: Las notificaciones push de Apple están inhabilitadas y no se envían mensajes desde el servidor al servicio de alertas Apple Push Notification Service.
- Nombre: Las notificaciones push de Apple están habilitadas. Los mensajes enviados desde el servidor al servicio de alertas Apple Push Notification Service incluyen el nombre del informe.
- Genérico: Las notificaciones push de Apple están habilitadas. Los mensajes enviados desde el servidor al servicio de alertas Apple Push Notification Service no incluyen el nombre del informe. En su lugar, se muestra un mensaje genérico.

Valor predeterminado: Nombre.

Comprobación de frecuencia para la fecha de caducidad del certificado de notificaciones push de Apple en horas

Especifica, en horas, la frecuencia con la que el servicio de Cognos Mobile comprueba la fecha de caducidad del certificado de las notificaciones push de Apple. La primera comprobación se lleva a cabo cuando el servicio de Cognos Mobile se inicia.

Valor: de 1 a 8760.

Valor predeterminado: 24

Intervalo de feedback para notificaciones push de Apple en horas

Especifica el intervalo de tiempo, en horas, tras el cual el servidor de Cognos Mobile comprueba si hay notificaciones fallidas en el servicio de información de las notificaciones push de Apple. El servicio de información conserva una lista de los dispositivos que tienen intentos repetidos o fallidos de la entrega de las notificaciones. El servidor de Cognos Mobile dejará de enviar notificaciones a los dispositivos indicados por el servicio de información.

Valores: 1 a 720

Valor predeterminado: 24

Umbral de caducidad para las notificaciones push de Apple en días

Especifica el número de días antes de la fecha de caducidad del certificado de notificaciones push de Apple en que los administradores empezarán a recibir mensajes de correo electrónico acerca de proximidad de la fecha de caducidad.

Valor: de 1 a 365

Valor predeterminado: 14

La configuración de notificaciones push de Apple para la aplicación nativa de iOS

Las notificaciones push de Apple avisan a los usuarios de las aplicaciones nativas de iOS acerca de la disponibilidad de nuevos informes de IBM Cognos Analytics.

Para enviar notificaciones push, el servidor de Cognos Mobile necesita un certificado SSL de Apple. El certificado SSL se incluye en todas las versiones comercializadas de IBM Cognos Mobile y es válido durante 12 meses desde la fecha en la que Apple lo emitió. El administrador debe supervisar la fecha de caducidad del certificado y actualizarlo antes de que caduque. De lo contrario, los usuarios dejan de recibir notificaciones push. Para obtener más información, consulte: “Gestión del certificado SSL para notificaciones push de Apple” en la página 416.

Los siguientes puertos TCP se utilizan para la comunicación entre el servidor de Cognos Mobile, el dispositivo iOS de Apple y el servicio de alertas Apple Push Notification Service (APNS):

- Cognos Mobile utiliza el puerto 2195 para enviar notificaciones a APNS.
- El servidor de Cognos Mobile utiliza el puerto 2196 para contactar con el servicio de información de APNS.
- En el dispositivo iOS, el puerto 5223 se utiliza para conectar con APNS a través de Wi-Fi.

Deje abiertos estos puertos en el cortafuegos de conexión a Internet.

Gestión del certificado SSL para notificaciones push de Apple

El administrador supervisa los archivos de registro y los mensajes de correo electrónico por si contienen mensajes sobre la proximidad de la fecha de caducidad del certificado y actualiza el certificado si es necesario.

Acerca de esta tarea

El certificado SSL para las notificaciones push de Apple es válido durante 12 meses desde la fecha en la que Apple lo emitió. Catorce días antes de la fecha de caducidad de certificado, el servidor Cognos Mobile empieza a registrar avisos en el archivo *install_location\logs\mob.log* acerca de la proximidad de la fecha de caducidad del certificado. Para asegurarse de que los avisos acerca de la fecha de caducidad de certificado se registran, el registro del servidor debe establecerse en el nivel Warn como mínimo. Cuando el nivel de registro está establecido en Error, los mensajes de caducidad de certificado no se registran.

Además de los avisos del archivo de registro, el servidor Cognos Mobile también se puede configurar para enviar mensajes de correo electrónico a los administradores acerca de la proximidad de la fecha de caducidad del certificado.

El texto del aviso en el archivo de registro o en el cuerpo del mensaje de correo electrónico, en inglés solamente, especifica la fecha de caducidad del certificado y el URL del sitio web de soporte de IBM (<http://www.ibm.com/support/>) donde se encuentra el fixpack de IBM Cognos Mobile más reciente con el certificado SSL de Apple.

Procedimiento

1. Asegúrese de que los siguientes valores de configuración están especificados en IBM Cognos Administration. Estos valores se utilizan para configurar el servidor Cognos Mobile para que se envíen mensajes de correo electrónico a los administradores acerca de la fecha de caducidad del certificado.
 - **Notificaciones de correo electrónico para notificaciones push de Apple**
 - **Comprobación de frecuencia para la fecha de caducidad del certificado de notificaciones push de Apple en horas**
 - **Umbral de caducidad para las notificaciones push de Apple en días**Para obtener más información, consulte: “Habilitación de notificaciones push de Apple”.
2. Supervise los mensajes del registro y los mensajes de correo electrónico para ver si contienen información sobre la fecha de caducidad del certificado.
3. Para actualizar el certificado, vaya al sitio web de IBM Support (<http://www.ibm.com/support>) y descargue el último fixpack de Cognos Mobile, que incluye un certificado válido para las notificaciones de envío de Apple.
4. Instale el nuevo certificado en todos los servidores afectados.

Habilitación de notificaciones push de Apple

El administrador debe configurar los valores del servicio de Mobile asociados a las notificaciones push de Apple para que los usuarios puedan recibir notificaciones push.

Acerca de esta tarea

La primera vez que una aplicación habilitada para operaciones se registre para las notificaciones push, los usuarios recibirán una alerta que les pregunta si desean recibir notificaciones. Después de responder a esta alerta, los usuarios no ven la alerta de nuevo a menos que se restaure su dispositivo o que la aplicación esté desinstalada durante al menos un día. Posteriormente, una alerta de texto envía una notificación al usuario del dispositivo iOS siempre que hay un informe nuevo disponible y el icono de aplicación se actualiza con el número de informes nuevos. El usuario puede abrir la aplicación desde la notificación.

La aplicación de iOS nativa para IBM Cognos Mobile puede recibir notificaciones push de varios servidores Cognos Analytics. Si los usuarios ya no desean que se visualicen las notificaciones, deben desactivar los valores de notificación de la aplicación en los valores de iOS.

Procedimiento

1. En IBM Cognos Administration, pulse la pestaña **Mobile**.
2. Pulse **Configuración de servidor**.
3. Especifique los valores de **Notificación** siguientes:

Soporte para las notificaciones push de Apple

Habilita las notificaciones push de Apple para la aplicación nativa de iOS y especifica el texto del mensaje que se mostrará a los usuarios de dispositivos iOS. Los valores son:

- Ninguno: Las notificaciones push de Apple están inhabilitadas y no se envían mensajes desde el servidor al servicio de alertas Apple Push Notification Service.
- Nombre: Las notificaciones push de Apple están habilitadas. Los mensajes enviados desde el servidor al servicio de alertas Apple Push Notification Service incluyen el nombre del informe.
- Genérico: Las notificaciones push de Apple están habilitadas. Los mensajes enviados desde el servidor al servicio de alertas Apple Push Notification Service no incluyen el nombre del informe. En su lugar, se muestra un mensaje genérico.

Valor predeterminado: Nombre.

Notificaciones de correo electrónico para notificaciones push de Apple

Especifica la dirección o direcciones de correo electrónico de los administradores a los que debe notificarse acerca de la fecha de caducidad del certificado de notificaciones push de Apple.

El valor es una dirección de correo electrónico válida con el formato siguiente: *admin@dominio.com*. Si se especifican varias direcciones de correo electrónico, deben separarse con un punto y coma (;). Por ejemplo, *admin1@dominio.com;admin2@dominio.com*

Umbral de caducidad para las notificaciones push de Apple en días

Especifica el número de días antes de la fecha de caducidad del certificado de notificaciones push de Apple en que los administradores empezarán a recibir mensajes de correo electrónico acerca de proximidad de la fecha de caducidad.

Valor: de 1 a 365

Valor predeterminado: 14

Intervalo de feedback para notificaciones push de Apple en horas

Especifica el intervalo de tiempo, en horas, tras el cual el servidor de Cognos Mobile comprueba si hay notificaciones fallidas en el servicio de información de las notificaciones push de Apple. El servicio de información conserva una lista de los dispositivos que tienen intentos repetidos o fallidos de la entrega de las notificaciones. El servidor de Cognos Mobile dejará de enviar notificaciones a los dispositivos indicados por el servicio de información.

Valores: 1 a 720

Valor predeterminado: 24

Comprobación de frecuencia para la fecha de caducidad del certificado de notificaciones push de Apple en horas

Especifica, en horas, la frecuencia con la que el servicio de Cognos Mobile comprueba la fecha de caducidad del certificado de las notificaciones push de Apple. La primera comprobación se lleva a cabo cuando el servicio de Cognos Mobile se inicia.

Valor: de 1 a 8760.

Valor predeterminado: 24

4. Pulse el botón **Aplique la configuración de Mobile**.
5. Especifique el valor avanzado **Database.DeviceExpiryIntervalDays** para el servicio de Mobile. Para obtener más información, consulte: "Especificación de valores avanzados de Cognos Mobile" en la página 408.

Gestión de informes en un dispositivo móvil

Los usuarios de IBM Cognos Mobile pueden abrir informes activos guardados o enviados en sus dispositivos móviles. Los usuarios pueden ejecutar los espacios de trabajo de IBM Cognos.

Los informes activos se pueden enviar a los usuarios con estos métodos:

- Planificando que los informes se envíen a los dispositivos de los usuarios a intervalos especificados.
- Enviando informes de separación a los dispositivos a los usuarios.
- Ejecutando una cantidad de informes diversos como un trabajo y enviándolos a los dispositivos de los usuarios.
- Definiendo eventos que hacen que se ejecute un informe y, a continuación, se entregue a los dispositivos de los usuarios.

Los usuarios pueden suprimir informes de sus dispositivos. Si lo hacen, solamente se suprime la copia del dispositivo, no el informe real.

Atajos de Cognos Mobile en un dispositivo móvil

Mientras se trabaja con IBM Cognos Mobile en el dispositivo, puede utilizar una cantidad de atajos para navegar y llevar a cabo otras acciones.

Tabla 80. Atajos de Cognos Mobile en un dispositivo móvil

Acción	Atajo
Inicio	1
Fin	9
Arriba	2

Tabla 80. Atajos de Cognos Mobile en un dispositivo móvil (continuación)

Acción	Atajo
Abajo	8
Izquierda	4
Derecha	6
Intro	Abrir
Acercar	Q
Alejar	A
Zoom	Z
Página	P
Marcar celda	5

Prestaciones de registro de Cognos Mobile

El registro de IBM Cognos Mobile se proporciona mediante las prestaciones de registro del propio producto y las de IBM Cognos Analytics.

Ambos métodos de registro generan archivos de registro que se utilizan para supervisar las actividades y resolver problemas. Estos archivos se encuentran en el directorio *install_location/logs*. Los archivos de configuración ubicados en el directorio *install_location/configuration*, con los componentes de nivel de aplicación, se utilizan para modificar las prestaciones de registro de Cognos Mobile.

Ambos métodos de registro pueden coexistir. Por ejemplo, se puede utilizar el mecanismo de registro de Mobile predeterminado para hacer un seguimiento de la actividad de servicio de Mobile y el mecanismo de registro de Cognos Analytics para habilitar el rastreo de depuración. El registro de auditoría solamente está disponible mediante las prestaciones de registro de Cognos Analytics.

Los sucesos asociados al inicio y la detención del servicio de Cognos Mobile se registran en el archivo de Cognos Analytics *install_location/logs/cogaudit.log*.

Además de las prestaciones de registro de Cognos Mobile y Cognos Analytics, puede utilizar las prestaciones de registro de iOS y Android para registrar los eventos asociados con las aplicaciones nativas de Cognos Mobile.

Registro de Cognos Mobile

IBM Cognos Mobile registra las actividades relacionadas con el inicio del servicio, la configuración y la ejecución de informes en el archivo *mob.log* en el directorio *ubicación_instalación/logs*. Este es el tipo predeterminado de registro en Cognos Mobile.

La información de registro que aparece en el archivo *mob.log* viene determinada por el archivo *ubicación_instalación/configuration/mob.log4j.xml*.

Cuando se utiliza el archivo *mob.log4j.xml* predeterminado, un administrador puede supervisar el servicio de Mobile para eventos tales como actualizaciones de esquema de base de datos, cambios en los valores de configuración y en los valores avanzados del servicio de Mobile, y avisos y errores. Sin embargo, el archivo *mob.log4j.xml* predeterminado no incluye el nivel de registro Debug. Si necesita

este nivel de registro en el archivo `mob.log`, debe habilitar la depuración. Para obtener más información, consulte: “Aumento de las prestaciones del registro de Cognos Mobile predeterminadas a los niveles de depuración”.

La tabla siguiente especifica los niveles de registro en el archivo `mob.log`, desde el nivel más alto hasta el más bajo:

Tabla 81. Niveles de registro en mob.log

Nivel de registro	Descripción
Debug	Proporciona información de depuración. Este nivel normalmente se utiliza para depurar problemas específicos. Este nivel no está disponible de forma predeterminada y debe estar habilitado. Para obtener más información, consulte: “Aumento de las prestaciones del registro de Cognos Mobile predeterminadas a los niveles de depuración”.
Información	Proporciona información sobre IBM Cognos Mobile.
Warn	Indica una aparición sospechosa que podría justificar una investigación en más profundidad.
Error	Indica una condición de error grave que requiere intervención.

El nivel de registro que el usuario elige incluye todos los niveles por debajo del mismo. Por ejemplo, si el usuario elige Info, los mensajes de aviso e información también se escriben en el archivo de registro.

Aumento de las prestaciones del registro de Cognos Mobile predeterminadas a los niveles de depuración

Puede habilitar el nivel de registro Depurar para el archivo `mob.log`.

Acerca de esta tarea

El archivo `mob.log4j.xml` predeterminado no incluye el registro del nivel Debug. Para habilitar la depuración, utilice el archivo `ubicación_instalación/configuration/mob.log4j.xml.DEBUG.sample`.

Procedimiento

1. Detenga el servicio de Mobile en IBM Cognos Configuration.
2. En el directorio `ubicación_instalación/configuration`, realice los cambios siguientes:
 - a. Cambie el nombre de `mob.log4j.xml` por `mob.log4j.xml.original`.
 - b. Cambie el nombre de `mob.log4j.xml.DEBUG.sample` por `mob.log4j.xml`.
3. Inicie el servicio de Mobile.

Resultados

El registro de depuración completo ahora está habilitado para IBM Cognos Mobile.

Habilitación del registro de Cognos Analytics para el servidor Mobile

IBM Cognos Mobile registra las actividades y la información de depuración, así como la información acerca de la actividades de informes y de los usuarios.

Acerca de esta tarea

El tipo de información que se registra en los archivos de registro de Cognos Mobile lo determina el nivel de registro definido en el archivo `ipfclientconfig.xml` del directorio `install_location/configuration`. El mismo directorio contiene el archivo `ipfMOBclientconfig.xml.sample`. Para habilitar el registro, solamente tiene que cambiar el nombre de `ipfMOBclientconfig.xml.sample` por `ipfclientconfig.xml`.

Se pueden definir los niveles de registro siguientes para Cognos Mobile:

Tabla 82. Niveles de registro de Cognos Mobile

Nivel de registro	Descripción
Debug	Proporciona información de depuración. Este nivel de registro normalmente se utiliza para depurar problemas específicos.
Info	Proporciona información sobre los servicios de IBM Cognos.
Warn	Indica una aparición sospechosa que podría justificar una investigación en más profundidad.
Error	Indica una condición de error grave que requiere intervención.

El nivel de registro que el usuario elige incluye todos los niveles por debajo del mismo. Por ejemplo, si el usuario elige Info, los mensajes de aviso e información también se escriben en el archivo de registro.

También puede habilitar el registro en IBM Cognos Administration. Para obtener más información, consulte: “Configuración del registro de auditoría en IBM Cognos Administration” en la página 422.

Procedimiento

1. Detenga el servicio de Mobile en IBM Cognos Configuration.
2. En el directorio `install_location/configuration`, cambie el nombre de `ipfMOBclientconfig.xml.sample` por `ipfclientconfig.xml`.
3. Abra el archivo `ipfclientconfig.xml`, especifique los niveles de registro que desea y guarde el archivo.
4. Inicie el servicio de IBM Cognos.

Resultados

En función de los niveles de registro especificados en el archivo `ipfclientconfig.xml`, se generan los archivos de registro siguientes en el directorio `install_location/logs`.

- `ipf-MOB_xxxx.log`

Este archivo registra la información de eventos de auditoría de Cognos Mobile. Si hay una base de datos de registro definida en IBM Cognos Configuration en **Entorno, Registro**, los eventos de auditoría también se registran en esta base de datos. Este tipo de registro está habilitado de forma predeterminada en el archivo `ipfMOBclientconfig.xml.sample`.

Para obtener información sobre la configuración de una base de datos de registro, consulte *IBM Cognos Analytics Guía de instalación y configuración*

- `ipfMOBtrace_xxxx.log`

Este archivo registra los datos de rastreo y depuración de Cognos Mobile. El tipo de datos capturado en este archivo es el mismo que el de los datos del archivo `mob.log`. Sin embargo, este archivo se puede configurar con un nivel de registro diferente para registrar más o menos información. Este tipo de registro está habilitado de forma predeterminada en el archivo `ipfMOBclientconfig.xml.sample`.

- `ipfMOBperf_XXXX.log`

Este archivo registra los datos de rendimiento de Cognos Mobile. Este tipo de registro está inhabilitado de forma predeterminada en el archivo `ipfMOBclientconfig.xml.sample`.

Configuración del registro de auditoría en IBM Cognos Administration

Utilice los registros de auditoría para ver información acerca de la actividad de los informes y de los usuarios de IBM Cognos Mobile.

Acerca de esta tarea

Como ejemplos de acciones registradas en los registros de auditoría, podemos citar las horas de inicio y fin de sesión de los usuarios, las sesiones de usuarios caducadas, la entrega de informes planificada, la salida guardada, etc.

También puede habilitar el registro de auditoría en el archivo `install_location/configuration/ipfclientconfig.xml`. Para obtener más información, consulte: “Habilitación del registro de Cognos Analytics para el servidor Mobile” en la página 420.

Para obtener más información sobre la creación de informes de auditoría, consulte *IBM Cognos Analytics Guía de administración y seguridad*. Este documento también contiene información acerca de los informes de auditoría de Cognos Mobile de ejemplo.

Procedimiento

1. Abra Cognos Administration.
2. En la pestaña **Configuración**, pulse **Asignadores y servicios**.
3. Pulse el nombre del asignador.
4. En la lista de servicios de asignador, busque **MobileService** y, en la columna **Acciones**, pulse el icono **Establecer propiedades**.
5. Pulse la pestaña **Valores** y, en **Categoría**, seleccione **Registro**.
6. En **Nivel de registro de auditoría para el servicio móvil**, seleccione cualquier valor excepto **Mínimo**.
Se pueden especificar los niveles de registro siguientes para habilitar el registro de auditoría: **Básico**, **Solicitud**, **Rastreo** y **Completo**. El nivel de registro **Mínimo** inhabilita el registro de auditoría.
7. Pulse **Aceptar**.
8. Para aplicar el valor, detenga y reinicie el servicio de IBM Cognos.

Diagnóstico para el usuario

Los usuarios pueden activar y desactivar el registro en sus aplicaciones nativas de iOS y Android y elegir el nivel de detalles de registro que se capturan.

La lista siguiente muestra los niveles soportados de registro cronológico, desde el nivel más alto hasta el más bajo:

- Red
- Depuración
- Información
- Aviso
- Error

El nivel de registro que el usuario elige incluye todos los niveles por debajo del mismo. Por ejemplo, si el usuario elige Información, los mensajes de Aviso y Error también se escriben en el archivo de registro.

El tamaño máximo de un mensaje registrado es 2 KB. Si un mensaje excede este tamaño, se trunca.

Aplicaciones de iOS

Si el registro está activado, se crea un directorio con el nombre `SupportArtifacts` en el directorio de los documentos de las aplicaciones. Se creará un archivo llamado `mobile_ios.log` en el directorio `SupportArtifacts`. En este archivo se escriben todos los eventos registrados.

El tamaño máximo de un archivo de registro activo es 1 MB. Cuando se alcanza este tamaño, el contenido del archivo de registro activo se mueve a un archivo llamado `mobile_ios.log.old`. Si ya existe un archivo `mobile_ios.log.old`, primero se eliminará. Se crea un archivo `mobile_ios.log` nuevo y pasa a ser el archivo de registro activo.

Si el registro se ha inhabilitado, el directorio y todo su contenido se elimina del directorio de los documentos de las aplicaciones.

Aplicaciones de Android

Si el registro está activado, se crea un directorio con el nombre `SupportArtifacts` en el directorio `/Android/data/com.ibm.cognob.artoo/files`. Se creará un archivo llamado `cognob.log` en el directorio `SupportArtifacts`. En este archivo se escriben todos los eventos registrados.

El tamaño máximo de un archivo de registro activo es 1 MB. Cuando se alcanza este tamaño, el contenido del archivo de registro activo se mueve a un archivo llamado `cognob.log.old`. Si el archivo `cognob.log.old` ya existe, primero se eliminará. Se crea un archivo `cognob.log` nuevo y pasa a ser el archivo de registro activo.

Si el registro se ha inhabilitado, el directorio y todo su contenido se elimina del directorio de los documentos de las aplicaciones.

Ejemplos de Cognos Mobile

Los ejemplos de IBM Cognos Analytics incluyen informes activos que se han optimizado para utilizar con el cliente enriquecido de IBM Cognos Mobile en un dispositivo móvil.

Los usuarios de dispositivos móviles pueden probar la funcionalidad interactiva de los informes activos. Estos informes permiten que los usuarios comparen distintas

áreas de sus empresas para determinar tendencias, por ejemplo, a lo largo del tiempo, por región, por departamentos o una combinación, o para comparar métodos empresariales y estadísticas.

Los informes activos de ejemplo de Cognos Mobile muestran las siguientes características del producto.

- Un comportamiento interactivo entre controles.
- Acceso a Detalles bajo demanda optimizando la funcionalidad detallada.
- Una paleta condicional y un desglose detallado de los gráficos.
- Un diseño específico según los movimientos típicos, como deslizar y desplazar.
- Un diseño de una interfaz de usuario personalizada, como la portada y la paleta de colores.
- Un tipo distinto de elementos de informe activo, como unidad, control de pestañas, gráfico, botones, lista desplegable, iterador y control deslizante

paquete Almacén de datos VA (análisis)

El paquete GO Data Warehouse (análisis) incluye los siguientes informes activos.

Resultados de los productos principales

Este informe activo muestra los datos de ingresos de los productos principales Equipo de acampada y Equipo de golf.

Informe financiero

Este informe activo muestra el rendimiento actual y los cambios en la posición financiera de una empresa. Este tipo de información es útil para todos los usuarios implicados en la toma de decisiones empresariales. Sin embargo, es más probable que pueda beneficiarse de esta información el departamento de finanzas al implementar comprobaciones y controles en el sistema para cumplir los requisitos y las normativas legales, impositivas y contables, y cuando se proporciona asesoramiento acerca de directrices futuras, del rendimiento y de las oportunidades para la empresa. Este informe se ha optimizado para tabletas.

Informe de rotación de inventario

Este informe activo muestra información acerca de la rotación de inventario de productos regional, basada en datos comparativos de dos años. El informe proporciona métricas de inventario clave que una empresa puede utilizar para gestionar su inventario. Puede detallar más en cada categoría de producto para ver la información de inventario detallada y el número de errores de pedido relacionados con el inventario. Este informe se ha optimizado para tabletas.

Objetivo de ventas por región

Este informe activo muestra el objetivo de ventas por región, incluidas las diferencias de porcentaje entre los ingresos planificador y los ingresos reales.

paquete Almacén de datos VA (consulta)

El paquete GO Data Warehouse (consulta) incluye los siguientes informes activos.

Costes de publicidad con respecto a ingresos

Este informe activo muestra los costes de publicidad con respecto a los ingresos por año. Los controles de pestañas se utilizan para agrupar elementos de informe similares.

Satisfacción del cliente

Este informe activo compara el número de devoluciones por clientes, por método de pedido y región. El informe proporciona información adicional sobre el método de pedido con el número máximo de devoluciones. También muestra los resultados de la encuesta de cliente para distintas regiones. Este informe se ha optimizado para tabletas.

Contratación de empleados

Este informe activo compara la eficacia de los diversos métodos de contratación para cada departamento y país o región. Muestra los nombres de empresas, puestos cubiertos, puestos planificados y un gráfico con viñetas de los puestos cubiertos respecto a los puestos planificados. Este informe se ha optimizado para tabletas.

Ingresos por producto

Este informe activo muestra los ingresos por producto seleccionado. Este informe se ha optimizado para los teléfonos móviles.

Seguridad de Cognos Mobile

IBM Cognos Mobile combina las medidas de seguridad de IBM Cognos Analytics con medidas extraordinarias necesarias para dispositivos móviles.

Las medidas de seguridad ofrecen protección contra la pérdida o robo y contra accesos no autorizados en la red inalámbrica. La seguridad se aplica tanto si el dispositivo está en modo conectado o desconectado.

La solución de Cognos Mobile comprende las siguientes medidas de seguridad que se implementan en IBM Cognos y en entornos específicos de dispositivos:

- Cifrado de datos estándar de IBM Cognos
- Autenticación estándar de IBM Cognos, incluido el soporte para proveedores de autenticación personalizada de IBM Cognos.
- Certificados PKCS12.
- Tecnología de clave de contrato.
- Políticas de autenticación de usuarios de dispositivos.
- Base de datos cifrada de móvil basada en el dispositivo.
- Transmisión y cifrado protegido de datos estándar específico del dispositivo.
- Protección de contraseña basada en el dispositivo.
- Limpieza remota del dispositivo.

Cognos Mobile da soporte a servidores web que se hayan configurado para utilizar la autenticación básica, como Microsoft Windows NTLM, Microsoft Active Directory y algunas configuraciones de CA SiteMinder. Con estos tipos de autenticación, la aplicación puede colocar en la memoria caché las credenciales del usuario si el administrador ha habilitado esta opción. Para todos los demás tipos de autenticación, como la página de respuesta del servidor HTML, la aplicación mostrará la página que permite al usuario interactuar con la página del modo previsto por el proveedor de autenticación.

Cognos Mobile da soporte a configuraciones de seguridad de inicio de sesión único. Sin embargo, normalmente, los usuarios de dispositivos móviles no se autentican previamente en el dominio de seguridad del mismo modo que lo hacen los usuarios de escritorio. Por tanto, los usuarios de dispositivos móviles suelen proporcionar sus propias credenciales de inicio de sesión único la primera vez que acceden al servidor de Cognos Analytics server.

Importante: La aplicación de IBM Cognos Mobile para iPad también da soporte a configuraciones de seguridad de inicio de sesión único. Los usuarios pueden habilitar el inicio de sesión único desde las opciones de **Ajustes** de sus iPad al activar el parámetro **Autenticación pass-through** para la aplicación IBM Cognos. Si este valor está habilitado, se solicitará a los usuarios de iPad las credenciales de inicio de sesión único la primera vez que accedan al servidor de Cognos Analytics.

Opcionalmente, las credenciales de inicio de sesión se pueden almacenar en la memoria caché del dispositivo móvil de forma que el usuario tenga que iniciar sesión solamente una vez para acceder al dispositivo y a Cognos Mobile. Cognos Mobile ofrece tecnología de base de datos cifrada y almacén de contenido en el dispositivo. El acceso al almacenamiento local del dispositivo lo controla la clave de contrato otorgada de forma central que se debe renovar periódicamente. Puede configurar la duración del contrato de forma que si le roban o pierde el dispositivo, los datos no estén accesibles.

Puede disponer de diferentes niveles de seguridad, dependiendo de las necesidades de su organización. Además de almacenar credenciales de inicio de sesión en el dispositivo, puede permitir el inicio de sesión anónimo o fiarse de las características de seguridad de la red del dispositivo móvil.

Si desea un nivel de seguridad mayor, puede utilizar la seguridad de Cognos para todas las comunicaciones o utilizar la tecnología de clave de contrato para controlar el acceso a datos.

Para obtener información sobre la seguridad de Cognos Analytics, consulte Capítulo 10, “Modelo de seguridad”, en la página 199. Para obtener información acerca de la seguridad de dispositivos, consulte la documentación de ese dispositivo.

Prestaciones de Cognos Mobile

Las prestaciones de IBM Cognos Mobile en IBM Cognos Administration permiten restringir el acceso a IBM Cognos Mobile a los usuarios y los administradores.

Consejo: Las prestaciones de IBM Cognos Analytics también se conocen como funciones y características protegidas.

Las prestaciones de Cognos Mobile son las siguientes:

- **Mobile**

Esta función protegida se utiliza para restringir el acceso a Cognos Mobile a los usuarios. Solamente los usuarios, grupos o roles que tienen permisos para ejecutar esta función protegida pueden iniciar la sesión en Cognos Mobile. Si los usuarios que no tienen los permisos necesarios intentan iniciar sesión, verán un mensaje de error que les solicitará que se pongan en contacto con un administrador de Cognos Analytics.

- **Administración de Mobile**

Esta característica protegida de la función protegida **Administración** se utiliza para restringir el acceso a las páginas de administración de la pestaña **Mobile** en Cognos Administration. Solamente los usuarios, grupos o roles que tienen permisos para ejecutar esta característica protegida pueden acceder a esta pestaña para realizar tareas de administración, como la configuración del servicio de Mobile, en Cognos Mobile.

Para simplificar el proceso de establecer permisos de acceso a las prestaciones **Mobile** y **Administración de Mobile**, puede utilizar los roles predefinidos **Usuarios de Mobile** y **Administradores de Mobile** que existen en el espacio de nombres de **Cognos** en Cognos Administration. El rol **Usuarios de Mobile** contiene permisos que son necesarios para que los usuarios normales puedan acceder a Cognos Mobile. El rol **Administradores de Mobile** contiene permisos que son necesarios para acceder a las funciones de administración de Cognos Mobile de la pestaña **Mobile** de Cognos Administration. Puede añadir usuarios, grupos o roles del directorio de su organización a estos roles e incluir los roles en las políticas de seguridad de Cognos Analytics. También puede ignorar estos roles, o suprimirlos, y crear sus propios grupos o roles de seguridad que se utilizarán para establecer permisos de acceso a Cognos Mobile.

Establecer permisos de acceso a las prestaciones **Mobile** y **Administración de Mobile** es una de las primeras tareas que el administrador debe realizar cuando configura Cognos Mobile. Para obtener más información, consulte Capítulo 13, “Funciones y características protegidas”, en la página 227.

Protección de contraseña

Normalmente, las empresas desean disponer de una protección de contraseña en los dispositivos móviles.

Tras un periodo especificado de inactividad, se solicita a los usuarios que vuelvan a especificar su contraseña de dispositivo y puede que exista un límite en la cantidad de veces que pueden realizar el intento de especificar una contraseña. Cuando se alcanza el límite, el dispositivo móvil se restablece y se eliminan todos los datos del dispositivo. A continuación, el usuario debe llevar a cabo las acciones adecuadas para restaurar los datos en el dispositivo.

Puede almacenar las credenciales de los usuarios de IBM Cognos en sus dispositivos móviles, de forma que solamente tengan que especificarse las credenciales la primera vez que se accedan a Cognos Mobile. Después, se seguirán solicitando las credenciales cada vez que se inicie la sesión, pero Cognos Mobile rellena las contraseñas de forma automática. Solamente cuando se alcance el límite de tiempo en las credenciales almacenadas, los usuarios tendrán que volver a especificar sus credenciales.

Si se ha configurado un PIN en un dispositivo iOS, la aplicación IBM Cognos Mobile cifra los informes activos de Cognos importados manualmente que están almacenados en el dispositivo. Esta característica se aplica a los informes activos que se importan manualmente a través del correo electrónico, iTunes o un servidor de archivos.

Para obtener información acerca de cómo habilitar o establecer políticas de contraseña para un dispositivo móvil, consulte la documentación del dispositivo.

Soporte HTML y HTTP durante el inicio de sesión

El producto IBM Cognos Mobile que se utiliza en dispositivos móviles es una aplicación nativa, en contraposición a una aplicación web. Para visualizar informes en dispositivos móviles, no se utiliza ningún navegador web y no se utiliza HTML.

Sin embargo, IBM Cognos Mobile utiliza HTTP para comunicarse con el servidor de IBM Cognos Analytics y debe interoperar con mecanismos de seguridad basados en la web que controlan el acceso al servidor de Cognos Analytics server. Para permitir que los usuarios autenticuen y naveguen a través de estos

mecanismos de seguridad, IBM Cognos Mobile muestra los elementos de formato HTML básicos y permite que el usuario lleve a cabo las acciones que tengan asociadas.

En la tabla siguiente se muestran las funciones HTTP y HTML a las que IBM Cognos Mobile da soporte.

Tabla 83. Funciones HTTP y HTML soportadas por Cognos Mobile

Función	Descripción
Redirecciones HTTP	Soporta HTTP 301 movido de forma permanente y HTTP 302 movido de forma temporal. Después seguirá los URL relativos y absolutos indicados en la cabecera Ubicación.
Redirecciones HTML	Da soporte al HTML equivalente a una redirección HTTP, por ejemplo, <meta http-equiv="Refresh" content="3;URL=http://...">.
Autenticación HTTP	Da soporte a HTTP 401 sin autorización tanto con el esquema básico como NTLM. NTLM predominantemente es un esquema de autenticación de Microsoft, conocido también como Windows Integrated Authentication.
Formularios HTML	Muestra el texto de una página HTML (incluido el texto con códigos de ancla), botones y el texto de tipos de campos de entrada, contraseña y ocultos. También muestra el tipo de entrada de selección, que se utiliza para mostrar una lista de elementos que se pueden elegir como, por ejemplo, una lista de espacios de nombre de seguridad.

Autenticación de certificados

Si el servidor web se ha configurado para que requiera la autenticación de certificado de cliente, puede utilizar un certificado SSL de cliente (certificado de cliente X509v3) para proporcionar un inicio de sesión transparente y una comunicación segura entre el servidor de IBM Cognos Analytics y las aplicaciones nativas.

Consejo: Este tipo de autenticación también se conoce como autenticación SSL bidireccional o autenticación mutua.

El archivo de certificado debe tener el formato PKCS12 (extensión .pkcs12) y contener la identidad del cliente, en forma de certificado y clave privada. Un administrador debe configurar un mecanismo seguro para importar el archivo de certificado en las aplicaciones nativas y proporcionar la contraseña del certificado a los usuarios para que puedan escribirla al importar el certificado.

Un administrador puede proporcionar los mecanismos siguientes para importar el certificado SSL de cliente para las aplicaciones iOS y Android de Cognos Mobile:

- Un enlace al archivo de certificado desde un sitio web.

Un administrador debe dirigir los usuarios a un sitio web que contiene un enlace al archivo .pkcs12. Los usuarios tocan el enlace para importar el archivo a la aplicación. En los dispositivos Android, a los usuarios se les solicita que guarden el archivo.

- Un correo electrónico con el archivo de certificado adjunto.

Los usuarios deben descargar el archivo .pkcs12 adjunto. En los dispositivos Android, a los usuarios se les solicita que guarden el archivo.

- Copiando el archivo de certificado al dispositivo.

En este escenario, el dispositivo móvil está conectado a un sistema personal. En Android, el archivo .pkcs12 se puede copiar manualmente del sistema personal, en el que el administrador proporciona el archivo de forma segura, al dispositivo móvil. En iOS, el administrador o el usuario pueden proporcionar el archivo .pkcs12 a través de iTunes, colocándolo en la carpeta **IBM Cognos Documents**.

Este método no es escalable y solamente resulta de utilidad para resolver problemas puntuales o realizar configuraciones puntuales.

Al seleccionar el archivo .pkcs12 en sus dispositivos móviles, los usuarios deben seleccionar **IBM Cognos Mobile** en el cuadro de diálogo **Abrir con**. A continuación, se pide a los usuarios la contraseña asociada con el archivo .pkcs12 en el cuadro de diálogo **Certificado de cliente**. Una vez que se abre la aplicación, el certificado se almacena en el sistema de almacenamiento de contraseñas, como Keychain en los dispositivos iOS, en el dispositivo móvil del usuario.

Consejo: En Android, si la aplicación Gmail no puede abrir un certificado PKCS12, una solución temporal sería utilizar otro cliente de correo, como la aplicación de correo electrónico predeterminada. Si esto no es posible, el uso de la extensión .p12 del certificado podría permitir a la aplicación importarlo correctamente. Al importar un certificado a través de un hipervínculo debe utilizarse la extensión .pkcs12.

Seguridad de aplicaciones en Cognos Mobile

Se puede utilizar un código de seguridad para restringir el acceso a la aplicación IBM Cognos Mobile para los usuarios de iOS y Android.

El administrador de Cognos puede especificar que el usuario del dispositivo móvil deba especificar un código de seguridad para acceder a la aplicación IBM Cognos Mobile y la cantidad de tiempo que la aplicación móvil puede permanecer inactiva antes de que el usuario tenga que volver a especificar el código para usar la aplicación. Esta funcionalidad está controlada por el valor de configuración **Tiempo de espera de sesión del código de seguridad**.

Si el valor de este parámetro indica que el usuario necesita un código de seguridad, este valor también representa el número de segundos que la aplicación Mobile puede permanecer inactiva antes de que se solicite al usuario que vuelva a especificar el código de seguridad para acceder a la aplicación Mobile.

Además de este valor, también hay un valor de tiempo de espera predeterminado que se incluye con las aplicaciones nativas de Mobile. El valor que se especifica para el parámetro del servidor anula el valor predeterminado en la aplicación.

Los usuarios pueden desactivar el parámetro del servidor en sus dispositivos móviles, pero no pueden cambiar su valor. Si el parámetro se ha desactivado, pero la configuración del servidor requiere que el usuario utilice un código de seguridad, la próxima vez que el usuario intente ejecutar la aplicación deberá volver a autenticarse con el servidor y se le solicitará que cree un código de seguridad. Sin ese código, los usuarios no pueden ver el contenido local.

El administrador de Cognos también puede establecer un límite en el número de intentos incorrectos al especificar el código de seguridad para iniciar la sesión en las aplicaciones de Cognos Mobile. Esto está controlado por el valor de configuración **Número de intentos máximo para entrar un código de seguridad al acceder a la aplicación de IBM Cognos Mobile**. Si el usuario supera el número

máximo de intentos, todo el contenido de Cognos de sus dispositivos móviles se destruirá. Si el usuario necesita un PIN para acceder al servidor, el número de reintentos especificado por el servidor prevalece sobre el valor de reintentos del dispositivo móvil.

Para obtener más información, consulte los valores de seguridad en: “Valores de configuración del servicio de Cognos Mobile” en la página 411.

Seguridad de los datos de informes en dispositivos móviles

Todas las versiones compiladas y comprimidas de informes de IBM Cognos Analytics se cifran y se almacenan localmente en la base de datos cifrada móvil del dispositivo móvil. Estos informes se pueden leer o interpretar solamente mediante la aplicación cliente de IBM Cognos Mobile.

Puede utilizar la tecnología de clave de contrato para establecer una fecha de caducidad para los datos de informes que se almacenan en el dispositivo móvil. Cuando se supera la fecha de caducidad, no se puede acceder a los datos de informe del dispositivo hasta que el dispositivo pueda restablecer comunicaciones con el servidor y el usuario pueda volverse a autenticar en el servidor.

Si se ha configurado un PIN en un dispositivo iOS, la aplicación IBM Cognos Mobile cifra los informes activos de Cognos importados manualmente que están almacenados en el dispositivo. Esta característica se aplica a los informes activos que se importan manualmente a través del correo electrónico, iTunes o un servidor de archivos.

Borrado del contenido de un dispositivo

Puede que tenga que borrar todo el contenido de un dispositivo móvil. Esta acción puede ser necesaria si se pierde o se roba un dispositivo o si un empleado cambia los roles o abandona la compañía.

Las contraseñas de dispositivos y la tecnología de clave de contrato garantizan que el contenido sólo está disponible para los usuarios autorizados. En todos los dispositivos, la seguridad y la gestión se administran mediante soluciones de gestión de dispositivos móviles de terceros.

Si el dispositivo móvil no está conectado al servidor durante un periodo de tiempo predeterminado, basado en las horas especificadas en el valor de configuración

Número máximo de horas para acceder a los datos locales de Mobile almacenados en un dispositivo, los datos de IBM Cognos dejarán de estar accesibles desde el dispositivo. Para obtener más información sobre los valores de configuración, consulte: “Valores de configuración del servicio de Cognos Mobile” en la página 411.

Establecimiento de una clave de contrato

IBM Cognos Mobile utiliza el concepto de contrato para controlar el acceso a los datos que están almacenados en dispositivos móviles.

Los datos se toman del servidor durante un periodo de tiempo que el administrador de IBM Cognos controla a través del valor del servidor **Número máximo de horas para acceder a los datos locales de Mobile almacenados en un dispositivo**. Este valor indica la cantidad máxima de tiempo que el usuario podrá acceder a los datos de un dispositivo móvil mientras permanezca sin contacto con el servidor. Por ejemplo, el dispositivo está fuera de línea o fuera del alcance de la

conexión inalámbrica. Si el dispositivo no consigue renovar el contrato dentro del periodo de tiempo especificado, los datos del dispositivo dejarán de estar accesibles. El rango válido de valores para esta opción, en horas, es de 0 a 8760. El valor predeterminado es de 36 horas. Un valor de 0 inhabilita el mecanismo de la clave de contrato. Para obtener información sobre cómo especificar este valor, consulte: “Configuración de los servicios de Cognos Mobile” en la página 411.

Establecimiento de políticas de autenticación de usuario para un dispositivo móvil

Las políticas de autenticación de usuarios de dispositivos IBM Cognos Mobile definen si las credenciales de autenticación de IBM Cognos Analytics se almacenan en la memoria caché del dispositivo móvil y la frecuencia en que los usuarios deben volver a escribir esas credenciales. Los usuarios deben especificar sus credenciales al menos una vez.

Todos los tiempos de espera de IBM Cognos Analytics se aplican al usuario del dispositivo móvil. Las políticas de autenticación de usuarios de dispositivos están por encima de los tiempos de espera asociados a IBM Cognos Analytics.

Para simplificar el proceso de autenticación del usuario, el administrador de IBM Cognos puede permitir que las credenciales se almacenen en la memoria caché del dispositivo móvil mediante el valor **Número máximo de horas para almacenar las credenciales almacenadas en memoria caché**. El rango de valores para esta opción, en horas, es de 0 a 8760. El valor predeterminado 0 significa que no desea almacenar las credenciales en un dispositivo. Para obtener información sobre cómo especificar este valor, consulte: “Configuración de los servicios de Cognos Mobile” en la página 411.

El valor de pasaporte CAM (mecanismo de control de la seguridad de IBM Cognos) de IBM Cognos Analytics se aplica a todos los dispositivos. Si caduca el límite del valor del pasaporte, la sesión del usuario termina. Sin embargo, si el límite de tiempo de la autorización de dispositivos supera el tiempo de espera que ha finalizado la sesión, el límite de tiempo de la autorización de dispositivos permanece vigente tras finalizar la sesión del usuario. Solamente cuando se alcance el límite de tiempo de autenticación de dispositivos, los usuarios tendrán que volver a especificar sus credenciales.

Procedimiento

Utilice el procedimiento siguiente para establecer el tiempo de espera del pasaporte CAM.

1. Abra **IBM Cognos Configuration** en el sistema donde se ha instalado IBM Cognos Content Manager.
2. En el panel **Explorador**, pulse **Explorador > Autenticación**.
3. En el panel **Propiedades**, para **Tiempo de espera de inactividad en segundos**, escriba el valor que desee.

Para obtener más información sobre IBM Cognos Configuration, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Apéndice A. Características de accesibilidad

IBM Cognos Administration dispone de características de accesibilidad que ayudan a los usuarios que tienen una discapacidad física, por ejemplo movilidad restringida o visión limitada, a utilizar los productos de tecnología de la información.

La disponibilidad de las características de accesibilidad puede variar, sin embargo, si se añaden a la interfaz de usuario de Cognos Administration otras páginas y componentes que no den soporte a la accesibilidad.

Para obtener más información sobre el compromiso de IBM respecto a la accesibilidad, consulte: IBM Accessibility Center (<http://www.ibm.com/able>).

Las características siguientes dan soporte a la accesibilidad en Cognos Administration:

- Para oír la información que se visualiza en pantalla, las personas con visión limitada pueden utilizar software lector de pantalla, junto con un sintetizador de voz digital. Cognos Administration utiliza Web Accessibility Initiative-Accessible Rich Internet Applications (WAI-ARIA).
- Para desplazarse por el software y emitir comandos mediante un teclado solamente, puede utilizar los atajos de teclado habituales de Microsoft Windows. No hay atajos de teclado exclusivos.
- Para omitir los enlaces de las cabeceras y los menús e ir directamente al contenido principal de la página, los usuarios de JAWS pueden seleccionar el enlace **Omitir hasta contenido principal** en la lista de la ventana de enlaces. Los usuarios del teclado ven la opción **Omitir hasta contenido principal** si se desplazan hasta él.
- Los administradores pueden especificar valores que afecten a todo el sistema para la salida de informe accesible que se aplican a todas las entradas.
- También se puede crear salida accesible para los informes, los trabajos, los pasos de los trabajos y las entradas planificadas en formato PDF, HTML y del software Microsoft Excel 2007.

Habilitación de la salida de informe accesible en todo el sistema

Puede especificar valores que afecten a todo el sistema para la salida de informe accesible que se aplican a todas las entradas, incluidos los informes, los trabajos y las entradas planificadas.

Los informes accesibles contienen características, como el texto alternativo, que permiten que los usuarios con discapacidades accedan al contenido de los informes mediante el uso de tecnología asistencial, como los lectores de pantalla.

Los valores de accesibilidad existentes en las preferencias de usuario y las propiedades de informe pueden reemplazar los valores que se aplican a todo el sistema en IBM Cognos Administration.

Los informes accesibles requieren más procesamiento y tienen un tamaño de archivo mayor que los informes no accesibles. Por lo tanto, los informes accesibles afectan al rendimiento. De forma predeterminada, el soporte para salida de informe accesible está inhabilitado.

La salida de informe accesible está disponible en los siguientes formatos: PDF, HTML y Microsoft Excel.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios**.
2. En la barra de herramientas de la página **Configuración**, pulse el botón Establecer propiedades .
3. Pulse la pestaña **Valores**.
4. En la lista desplegable **Categoría**, pulse **Reemplazo de administrador**.
5. En la categoría **Reemplazo de administrador**, situada junto a **Soporte de accesibilidad para informes**, en la columna **Valor**, pulse **Editar**.
6. En la página **Soporte de accesibilidad para informes**, seleccione una de las opciones siguientes:

Opción	Descripción
Inhabilitar	La salida de informe accesible no está disponible para los usuarios.
Hacer obligatoria	La salida de informe accesible siempre se crea.
Dejar que decida el usuario	El usuario especifica la salida de informe accesible. Si establece esta opción en No seleccionado , la salida de informe accesible no se crea automáticamente. Esta es la opción predeterminada. Si establece esta opción en Seleccionado , la salida de informe accesible no se crea de forma predeterminada.

Características de accesibilidad de Cognos Mobile

La aplicación IBM Cognos Mobile es totalmente accesible en los dispositivos iOS 7 y superiores. En estos dispositivos, si la característica **VoiceOver** está habilitada, actúa como un lector de pantalla. Los usuarios pueden desplazarse con un teclado Bluetooth o con gestos de pantalla utilizando los comandos de atajo del teclado de Apple estándares. Para obtener más información, consulte la documentación de su dispositivo.

La aplicación Cognos Mobile incluye atajos del teclado adicionales para facilitarle el desplazamiento en diferentes vistas.

Atajos del teclado en Cognos Mobile

Existen atajos del teclado para las diferentes vistas de la aplicación Cognos Mobile.

Se han definido atajos del teclado para las pantallas, los espacios y las vistas siguientes:

- Pantalla de inicio de IBM Cognos Mobile
- Espacios Mis informes, Contenido importado y Ejemplos
- Vistas Examinar y Búsqueda
- Report Viewer
- Ventana **Escribir código de seguridad**

Pantalla de inicio de IBM Cognos Mobile

Si la característica **VoiceOver** está habilitada en su dispositivo móvil iOS, puede utilizar los atajos del teclado de Cognos Mobile para desplazarse por IBM Cognos Analytics en la pantalla de inicio de Cognos Mobile.

En la pantalla de inicio de IBM Cognos Mobile, utilice el atajo del teclado siguiente para realizar la acción que se indica a continuación:

Tabla 84. Atajos del teclado de la pantalla de inicio de IBM Cognos Mobile

Acción	Atajo del teclado
Si el foco está en una conexión de espacio, abrir la ventana Suprimir.	Ctrl+D

Espacios Mis informes, Contenido importado y Ejemplos

Si la característica **VoiceOver** está habilitada en su dispositivo móvil iOS, puede utilizar los atajos del teclado de Cognos Mobile para desplazarse por IBM Cognos Analytics en los espacios Mis informes, Contenido importado y Ejemplos.

Los atajos del teclado activan acciones diferentes que dependen del modo en el que esté trabajando. Los modos son el modo predeterminado y el modo de edición.

Modo predeterminado

En el modo predeterminado, utilice estos atajos del teclado para realizar las acciones siguientes:

Tabla 85. Atajos del teclado del modo predeterminado de los espacios Mis informes, Contenido importado y Ejemplos

Acción	Atajo del teclado
Salir o minimizar un espacio.	Ctrl+X
Abrir las vistas Examinar y Búsqueda (espacio Mis informes solamente).	Ctrl+B
Renovar la lista de informes.	Ctrl+R
Editar el título del espacio.	Ctrl+T
Abrir o cerrar los valores de autenticación de usuario (espacio Mis informes solamente).	Ctrl+A
Abrir o cerrar los valores de fondo de pantalla.	Ctrl+W
Entrar en el modo de vista previa de informe o salir de él.	Ctrl+P
Entrar en el modo de edición.	Ctrl+D

Modo de edición

En el modo de edición, utilice estos atajos del teclado para realizar las acciones siguientes:

Tabla 86. Atajos del teclado del modo de edición de los espacios Mis informes, Contenido importado y Ejemplos

Acción	Atajo del teclado
Volver al modo predeterminado cuando haya terminado la edición.	Ctrl+D
Seleccionar todo si no hay nada seleccionado o no seleccionar nada si todo está seleccionado.	Ctrl+A
Intercambiar un informe que tiene el foco por el informe siguiente (el foco permanece en el informe movido).	Ctrl+S
Suprimir los informes seleccionados y volver al modo predeterminado.	Suprimir

Vistas Examinar y Búsqueda

Si la característica **VoiceOver** está habilitada en su dispositivo móvil iOS, puede utilizar los atajos del teclado de Cognos Mobile para desplazarse por IBM Cognos Analytics en las vistas Examinar y Búsqueda.

En el espacio Mis informes, puede examinar el contenido y realizar búsquedas. En las vistas Examinar y Búsqueda, utilice estos atajos del teclado para realizar las acciones siguientes:

Tabla 87. Atajos del teclado de las vistas Examinar y Búsqueda

Acción	Atajo del teclado
Cerrar la vista Examinar o Búsqueda.	Ctrl+X
Renovar la página Examinar o Búsqueda actual.	Ctrl+R
Ir a la página siguiente.	Opc+ flecha izquierda o derecha
Cerrar la ventana Salida guardada si está abierta.	Retorno o Intro

Report Viewer

Si la característica **VoiceOver** está habilitada en su dispositivo móvil iOS, puede utilizar los atajos del teclado de Cognos Mobile para desplazarse por IBM Cognos Analytics en el visor de informes.

En el espacio Mis informes, puede ver informes en Report Viewer. Los atajos del teclado activan acciones diferentes que dependen del modo en el que esté trabajando. Los modos son el modo predeterminado y el modo de dibujo.

Modo predeterminado

En el modo predeterminado, utilice estos atajos del teclado para realizar las acciones siguientes:

Tabla 88. Report Viewer, atajos del teclado del modo predeterminado

Acción	Atajo del teclado
Cerrar o minimizar Report Viewer. Al acceder a los detalles, volver al origen.	Ctrl+X

Tabla 88. Report Viewer, atajos del teclado del modo predeterminado (continuación)

Acción	Atajo del teclado
Abrir o cerrar el selector de páginas.	Ctrl+P
Abrir o cerrar el menú Acciones.	Ctrl+A
Entrar en el modo de dibujo.	Ctrl+D
Ir a la página siguiente.	Ctrl+. (>)
Ir a la página anterior.	Ctrl+, (<)

Modo de dibujo

En el modo de dibujo, utilice estos atajos del teclado para realizar las acciones siguientes:

Tabla 89. Report Viewer, atajos del teclado del modo de dibujo

Acción	Atajo del teclado
Descartar cambios y salir del modo de dibujo.	Ctrl+D
Compartir un informe con anotaciones.	Ctrl+M
Cuando el menú Dibujar cuadro está abierto, incrementar la anchura de Dibujar cuadro en 10 píxeles.	Ctrl+W
Cuando el menú Dibujar cuadro está abierto, reducir la anchura de Dibujar cuadro en 10 píxeles.	Ctrl+Mayús+W
Cuando el menú Dibujar cuadro está abierto, incrementar la altura de Dibujar cuadro en 10 píxeles.	Ctrl+H
Cuando el menú Dibujar cuadro está abierto, reducir la altura de Dibujar cuadro en 10 píxeles.	Ctrl+Mayús+H
Cuando el menú Dibujar cuadro está abierto, salir del menú Dibujar cuadro.	Ctrl+X

Ventana Escribir código de seguridad

Si la característica **VoiceOver** está habilitada en su dispositivo móvil iOS, puede utilizar los atajos del teclado de Cognos Mobile para desplazarse por IBM Cognos Analytics en la ventana **Entre código de seguridad**.

Utilice estos atajos del teclado para realizar las acciones siguientes:

Tabla 90. Atajos del teclado de la ventana Escribir código de seguridad

Acción	Atajo del teclado
Especificar el PIN	Números del teclado
Borrar el último número que se ha escrito	Suprimir

Problemas conocidos

Cognos Mobile incluye atajos del teclado para facilitar el desplazamiento y la realización de tareas en IBM Cognos Analytics si solamente se utiliza un teclado. Sin embargo, puede experimentar problemas ya conocidos con la característica **VoiceOver** de iOS.

Al visualizar el contenido de un informe, los atajos del teclado de Cognos no funcionan

Cuando la característica **VoiceOver** está habilitada y se visualiza el contenido de un informe en Report Viewer o en la pantalla de inicio de Cognos Mobile, los comandos de teclado de Cognos Mobile no funcionan. Para resolver este problema, vuelva a colocar el foco en el área de la barra de herramientas.

La escucha del teclado deja de funcionar cuando se toca un elemento

Al visualizar el contenido de un informe en la aplicación Cognos Mobile, si toca un elemento, la característica **VoiceOver** deja de funcionar. La solución temporal es desactivar la característica **VoiceOver** y volverla a activar o bien desplazarse a otra vista y volver a la vista original para restablecer la característica **VoiceOver**.

La tecla Suprimir no funciona en los campos de entrada de texto

Si está en modo **VoiceOver**, la tecla Suprimir no funciona en los campos de entrada de texto en la aplicación Cognos Mobile. Si se equivoca y desea retroceder para suprimir un carácter, utilice el atajo del teclado Ctrl+Suprimir.

Apéndice B. Round Trip Safety Configuration de caracteres Shift-JIS

Shift-JIS es un sistema de codificación para caracteres japoneses. Es el equivalente a ASCII, un sistema de codificación para caracteres ingleses.

Codificación nativa y Unicode

Dado que Shift-JIS y ASCII definen los caracteres para un idioma, los podemos considerar como sistemas de codificación nativa. Unicode es un sistema de codificación de caracteres que define los caracteres para todos los idiomas. Debido a que el software se utiliza en un entorno multilingüe global, los caracteres que utilizan los sistemas para procesamiento deben convertirse a menudo entre sistemas de codificación nativa y Unicode.

Seguridad de recorrido de ida y vuelta

Los problemas asociados con las conversiones entre los sistemas de codificación nativa y Unicode se conocen como problemas de seguridad de recorrido de ida y vuelta.

Mediante Unicode, se desarrollan aplicaciones que pueden admitir la entrada simultánea de caracteres en distintos idiomas. Los datos de entrada, introducidos por los usuarios o recuperados de las bases de datos, pueden contener caracteres codificados en un sistema de codificación nativa. Por ejemplo, en el sistema operativo Microsoft Windows, los caracteres ingleses introducidos por un usuario se codifican mediante Windows-1252.

Cuando una aplicación recibe caracteres en un sistema de codificación nativa, los convierte a Unicode para procesarlos. Una vez que ha finalizado el procesamiento, los caracteres se pueden volver a convertir en el sistema de codificación nativa.

En la mayoría de los casos, los caracteres se convierten sin ambigüedad, ya que cada carácter nativo se correlaciona con un solo carácter Unicode. Si la conversión de un carácter de idioma nativo a y desde Unicode genera el carácter original, el carácter se considerará seguro para un recorrido de ida y vuelta.

Por ejemplo, el carácter "A" es seguro para un recorrido de ida y vuelta en Windows-1252, de la forma siguiente:

- El carácter de Windows-1252 para "A" es 0x41.
- Se convierte en el carácter correspondiente de Unicode U+0041.
- Ningún otro carácter de Windows-1252 se convierte en el mismo carácter Unicode, por lo que siempre se vuelve a convertir en 0x41.

Problemas específicos de Shift-JIS

Si bien los caracteres de la mayoría de los sistemas de codificación de caracteres nativos son seguros para un recorrido de ida y vuelta, el sistema de codificación Shift-JIS supone una excepción. Aproximadamente 400 caracteres de Shift-JIS no son seguros para un recorrido de ida y vuelta, porque varios caracteres de este grupo se pueden correlacionar al mismo carácter Unicode. Por ejemplo, los dos caracteres Shift-JIS 0x8790 y 0x81e0 se convierten en el carácter Unicode U+2252.

IBM Cognos Analytics y Shift-JIS

IBM Cognos Analytics utiliza Unicode. La seguridad de recorrido de ida y vuelta de los caracteres es fundamental para garantizar la precisión de los datos en los informes generados.

El programa de utilidad Round Trip Safety Configuration garantiza la seguridad del recorrido de ida y vuelta de los caracteres Shift-JIS sólo cuando se utilizan ambos para convertir los caracteres:

- De Shift-JIS en Unicode
- De Unicode en Shift-JIS

Si los datos se solicitan a una base de datos con su propio mecanismo automático para realizar la conversión de Shift-JIS a Unicode, IBM Cognos Analytics no llamará al programa de utilidad Round Trip Safety Configuration para convertir los caracteres de Unicode a Shift-JIS. d. No se puede garantizar la seguridad de recorrido de ida y vuelta de los caracteres de los datos.

Para obtener más información sobre el programa de utilidad Round Trip Safety Configuration, consulte “Programa de utilidad Round Trip Safety Configuration”.

Ejemplo: Conversión segura de Shift-JIS

En el siguiente ejemplo se ilustra el problema que se produce en la conversión de Shift-JIS a Unicode:

- Una base de datos contiene caracteres codificados en Shift-JIS.
- Un registro de la base de datos contiene el carácter Shift-JIS 0x8790.
- Un usuario introduce el carácter Shift-JIS 0x8790 en un formulario de entrada de datos de un navegador.
- La aplicación recibe el formulario de entrada y convierte el carácter Shift-JIS 0x8790 en el carácter Unicode U+2252.
- Debido a que la base de datos contiene caracteres con codificación Shift-JIS, el carácter Unicode U+2252 no se puede especificar como parte de la consulta.
- La aplicación debe volver a convertir el carácter U+2252 en un carácter Shift-JIS. Tanto 0x8790 como 0x81e0 se convierten en U+2252. Si el proceso de conversión selecciona 0x81e0, la consulta no devolverá registros.

Para resolver este problema, puede usar el programa de utilidad Round Trip Safety Configuration para garantizar que la conversión se realice al carácter 0x8790 y que se encuentre el registro.

Programa de utilidad Round Trip Safety Configuration

Puede usar el programa de utilidad Round Trip Safety Configuration para configurar el proceso de conversión de caracteres Shift-JIS, de forma que IBM Cognos Analytics siempre devuelva los registros correctos.

Este programa de utilidad le permite controlar las dos situaciones siguientes:

- Hay más de un carácter Shift-JIS que se convierte en el mismo carácter Unicode.

Si los datos contienen este tipo de caracteres Shift-JIS, puede usar el programa de utilidad para especificar que el carácter Unicode siempre se convierta en el carácter Shift-JIS necesario. Para obtener más información, consulte “Especificación de conversiones” en la página 441.

- Hay más de un carácter Unicode que representa el mismo carácter o un carácter similar después de la conversión.
Estos caracteres Unicode se pueden considerar idénticos cuando los sistemas los procesan y se pueden sustituir entre sí. Puede usar el programa de utilidad para garantizar que se realice la sustitución correcta. Para obtener más información, consulte “Especificación de sustituciones” en la página 442.

Especificación de conversiones

Si los datos contienen más de un carácter Shift-JIS que convierte el mismo carácter Unicode, use el programa de utilidad Round Trip Safety Configuration para especificar que el carácter Unicode siempre se convierta en el carácter Shift-JIS necesario.

Antes de seleccionar el carácter Shift-JIS que se utilizará en una conversión, decida el carácter Shift-JIS que se está usando actualmente en el entorno. Sólo se puede utilizar un carácter Unicode de los equivalentes posibles de Shift-JIS en un entorno específico.

En la pestaña Conversión, los caracteres de codificación nativa aparecen con el formato 0xYYYY, mientras que los caracteres Unicode aparecen con el formato U+YYYY, donde YYYY representa el valor hexadecimal del carácter Unicode.

Por ejemplo, el carácter "A" aparece de la forma siguiente:

- En la codificación nativa, 0x41
- En Unicode, U+0041

Cada fila representa una regla de correlación que asocia dos o tres caracteres Shift-JIS al carácter Unicode de la primera columna.

De manera predeterminada, todos los caracteres Shift-JIS de una fila se convierten en el carácter Unicode asociado. Por ejemplo, los dos caracteres Shift-JIS 0x8782 y 0xFA59 se convierten en el carácter Unicode U+2116.

Puede configurar más de un carácter a la vez.

Procedimiento

1. Inicie el programa de utilidad Round Trip Safety Configuration en *install_location/bin*:
 - Para el sistema operativo Microsoft Windows, `rtsconfig.exe`
 - Para el sistema operativo UNIX, `rtsconfig`
2. Pulse la pestaña **Conversión**.
Sugerencia: Para ver el glifo situado junto al carácter Unicode, en el menú **Ver**, pulse **Glifos**. Es posible que algunos glifos no se vean, según el tipo y el tamaño de las fuentes que utilice.
3. En el menú **Editar**, pulse **Buscar un carácter** y, a continuación, introduzca el valor hexadecimal del carácter Shift-JIS.
4. Pulse **Aceptar**.
5. En la columna **Primer carácter Shift-JIS**, **Segundo carácter Shift-JIS** o **Tercer carácter Shift-JIS**, seleccione el carácter Shift-JIS al que desee convertir el carácter Unicode.
6. Repita los pasos del 3 al 5 con cada carácter Shift-JIS que desee configurar.
7. Guarde las especificaciones mediante uno de los métodos siguientes:

- Para guardar solamente las especificaciones, en el menú **Archivo**, pulse **Guardar**.
- Para guardar y aplicar las especificaciones, en el menú **Herramientas**, pulse **Configurar**.

Si sólo guarda la especificación, podrá aplicarla posteriormente. Para obtener más información, consulte “Aplicación de las conversiones y las sustituciones” en la página 443. También puede restaurar los valores predeterminados. Para obtener más información, consulte “Restauración de los valores predeterminados de conversión” en la página 443.

Las especificaciones se guardan en el archivo `shift-jis.xml`, en el directorio `install_location/bin`.

Especificación de sustituciones

Después de la conversión, los datos Unicode pueden contener caracteres con el mismo significado pero con distinto aspecto. Por ejemplo, una tilde de anchura completa (~) y una de anchura media tienen valores distintos en Unicode, pero se pueden considerar idénticas durante el procesamiento.

Puede usar el programa de utilidad Round Trip Safety Configuration para especificar que se pueden sustituir pares específicos de caracteres similares mediante un solo carácter. Por ejemplo, puede especificar que los dos tipos de tilde se sustituyan por una tilde de anchura completa.

En la pestaña Sustitución, la primera columna contiene pares de caracteres que normalmente significan lo mismo, pero que se representan con distintos valores en Unicode. Cada fila representa una regla de sustitución. En la primera columna aparecen los datos antes de la conversión. En la segunda columna aparecen los posibles caracteres de sustitución.

Procedimiento

1. Inicie el programa de utilidad Round Trip Safety Configuration en `install_location/bin`:
 - Para el sistema operativo Microsoft Windows, `rtsconfig.exe`
 - Para el sistema operativo UNIX, `rtsconfig`
2. Pulse la pestaña **Sustitución**.

Sugerencia: Para ver el glifo situado junto al carácter Unicode, en el menú **Ver**, pulse **Glifos**. Es posible que algunos glifos no se vean, según el tipo y el tamaño de las fuentes que utilice.
3. En la columna **Código original**, pulse el carácter que desee sustituir.
4. En la columna **Código de sustitución**, pulse el carácter equivalente.

Aparecerá una lista con las posibles opciones de sustitución.
5. En la lista, pulse el carácter Unicode que desee utilizar o pulse **No sustituir**.
6. Repita los pasos del 3 al 5 con cada carácter Unicode que desee sustituir.
7. Guarde las especificaciones mediante uno de los métodos siguientes:
 - Para guardar solamente las especificaciones, en el menú **Archivo**, pulse **Guardar**.
 - Para guardar y aplicar las especificaciones, en el menú **Herramientas**, pulse **Configurar**.

Si sólo guarda la especificación, podrá aplicarla posteriormente. Para obtener más información, consulte “Especificación de conversiones” en la página 441.

También puede restaurar los valores predeterminados. Para obtener más información, consulte “Restauración de los valores predeterminados de conversión”.

Las especificaciones se guardan en el archivo `shift-jis.xml`, en el directorio `install_location/bin`.

Aplicación de las conversiones y las sustituciones

Si no desea aplicar cambios al guardar, puede aplicar los datos posteriormente. Según la información guardada en el archivo `install_location/bin/shift-jis.xml`, se generan dos archivos:

- En el caso de datos de sustitución, `i18n_res.xml`
- En el caso de datos de conversión, `ibm-943_P14A-2000.cnv`

Acerca de esta tarea

De forma predeterminada, al aplicar los datos no se comprueba la seguridad de recorrido de ida y vuelta de los caracteres. Al establecer el modo de configuración, puede determinar que se compruebe la seguridad de recorrido de ida y vuelta. Para ello, debe seleccionar la opción que devuelve un error de conversión en tiempo de ejecución en el caso de los caracteres que no sean seguros en dicho sentido. Esto puede resultar útil para detectar inicialmente los caracteres Shift-JIS que se deben configurar.

Procedimiento

1. Detenga la IBM Cognos Analytics.
2. En el programa de utilidad Round Trip Safety Configuration, en el menú **Herramientas**, pulse **Establecer modo de configuración**.
3. Especifique si desea que se compruebe la seguridad de recorrido de ida y vuelta de los caracteres.
4. En el menú **Herramientas**, pulse **Configurar**.
5. Inicie IBM Cognos Analytics.

Restauración de los valores predeterminados de conversión

En cualquier momento puede restaurar rápidamente los valores predeterminados de los datos de configuración y sustitución. Por ejemplo, puede que desee restaurar la configuración en las siguientes situaciones:

- Después de establecer que la aplicación utilice un origen de datos distinto en el que sea necesaria otra configuración.
- Después de realizar un prototipo.

Procedimiento

1. Detenga la IBM Cognos Analytics.
2. En el programa de utilidad Round Trip Safety Configuration, en el menú **Herramientas**, pulse **Restaurar valores predeterminados**.
El proceso de conversión se establece para que utilice los valores predeterminados.
3. Inicie IBM Cognos Analytics.

Especificación de conversiones para informes de Series 7 PowerPlay Web

IBM Cognos Series 7 proporciona una solución limitada para los caracteres japoneses definidos por el proveedor (VDC) en codificación Shift-JIS. Para garantizar la integridad y la coherencia de los datos al utilizar informes de PowerPlay con IBM Cognos Analytics, debe establecer los valores predeterminados en la correlación de caracteres.

Procedimiento

1. Detenga la IBM Cognos Analytics.
2. Inicie el programa de utilidad Round Trip Safety Configuration, consulte “Programa de utilidad Round Trip Safety Configuration” en la página 440.
3. En el menú **Herramientas**, pulse **Restaurar valores predeterminados**.
4. En el menú **Herramientas**, pulse **Configurar**.

Las tablas de conversión se establecen para que utilicen los valores predeterminados en segundo plano.

5. Cierre el programa de utilidad Round Trip Safety Configuration.
6. Inicie IBM Cognos Analytics.

Apéndice C. Permisos de acceso iniciales

En IBM Cognos Analytics, cuando Content Manager inicializa un almacén de contenido, crea estructuras básicas e información sobre seguridad. Estas estructuras incluyen una jerarquía de carpetas.

Content Manager incluye las carpetas y el contenido de las carpetas siguiente:

/Root Todas las carpetas que se encuentran bajo /Root en la jerarquía.

/Root/Directory

Información sobre los proveedores de autenticación y otro tipo de información que se suele encontrar en un servicio de directorio.

/Root/Directory/Cognos

Espacio de nombres del directorio Cognos que contiene los grupos, los orígenes de datos, las listas de distribución y los contactos de Cognos.

/Root/Directory/otros_proveedores

Otros espacios de nombres de seguridad, como LDAP y Active Directory.

/Root/Public Folders

Todos los datos de aplicación de Content Manager.

/Root/Directory/paquetes_aplicaciones

Una carpeta independiente para cada aplicación, que contiene información sobre la aplicación.

/Root/Configuration

Datos de configuración de todos los componentes y las plantillas de Cognos.

/Root/Capabilities

Objetos que se pueden proteger mediante políticas que restringen el acceso a funcionalidad, como Administración, Creación de informes y Query Studio; así como a características, como SQL definido por el usuario y separación.

/Root/Import

Información sobre el despliegue de cada archivo importado a Content Manager.

/Root/Export

Información sobre despliegue de cada archivo exportado desde Content Manager.

Se recomienda modificar los valores iniciales para proteger el software de IBM Cognos. Para obtener más información, consulte: Capítulo 15, "Seguridad inicial", en la página 243 y Capítulo 12, "Permisos de acceso y credenciales", en la página 213.

Permisos de acceso iniciales a los objetos raíz y de nivel superior de Content Manager

En IBM Cognos Analytics, cuando Content Manager inicializa un almacén de contenido, crea estructuras básicas e información sobre seguridad. Estas estructuras incluyen permisos de acceso iniciales para los objetos raíz y de nivel superior de Content Manager.

El objeto raíz

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 91. Objeto raíz y permisos para grupos y roles relacionados

		Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Objeto	Grupo o rol					
Raíz	Todos	X		X		X

Objetos de nivel superior de Content Manager

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 92. Objetos de nivel superior de Content Manager y permisos para grupos y roles relacionados

		Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Objeto	Grupo o rol					
Funciones	Admin. del directorio				X	X
	Todos					X
Configuración	Administradores del servidor	X	X	X	X	X
	Todos			X		X
Carpetas públicas	Admin. de informes	X	X	X	X	X
	Autores	X	X	X		X
	Usuarios de consultas	X		X		X
	Consumidores	X		X		X
	Autores de Express	X	X	X		X
	Lectores	X				X

Tabla 92. Objetos de nivel superior de Content Manager y permisos para grupos y roles relacionados (continuación)

		Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Objeto	Grupo o rol					
Exportar	Admin. de informes	X	X	X	X	X
Importar	Admin. de informes	X	X	X	X	X
Directorio	Todos					X

Permisos de acceso iniciales a las prestaciones

En IBM Cognos Analytics, cuando Content Manager inicializa un almacén de contenido, crea estructuras básicas e información sobre seguridad. Estas estructuras incluyen permisos de acceso iniciales para las prestaciones.

A las prestaciones también se las llama funciones protegidas y características protegidas.

Prestación Adaptive Analytics

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 93. Prestación Adaptive Analytics y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio				X	X

Prestación de administración

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 94. Prestación de administración y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio			X	X	X
Administradores de biblioteca			X		X

Tabla 94. Prestación de administración y permisos para grupos y roles relacionados (continuación)

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Administradores de Mobile			X		X
Modeladores			X		X
Administradores de portales			X		X
Admin. de PowerPlay			X		X
Admin. de informes			X		X
Administradores del servidor			X		X

Las características protegidas de la tabla siguiente son hijos de la prestación de administración.

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 95. Características protegidas de la prestación de administración y permisos para grupos y roles relacionados

		Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Característica protegida	Grupo o rol					
Administración de Adaptive Analytics	Administradores de Adaptive Analytics			X		X
	Admin. del directorio				X	X
Tareas de administración	Administradores del servidor			X		X
	Admin. de informes			X		X
	Administradores de métrica			X		X
	Administradores de Controller			X		X
	Admin. del directorio				X	X
	Admin. de PowerPlay			X		X
Configurar y gestionar el sistema	Administradores del servidor			X		X
	Admin. del directorio				X	X
Administración de Controller	Administradores de Controller			X		X
	Admin. del directorio				X	X

Tabla 95. Características protegidas de la prestación de administración y permisos para grupos y roles relacionados (continuación)

Característica protegida	Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Conexiones de orígenes de datos	Admin. del directorio			X	X	
	Modeladores			X		X
Listas de distribución y contactos	Admin. del directorio			X	X	X
Administración de Mobile	Admin. del directorio				X	X
	Administradores de Mobile			X		X
Administración de Mis conjuntos de datos	Administradores del directorio				X	X
	Administradores del servidor			X		X
Administración de Planning	Administradores de permisos de Planning			X		X
	Admin. del directorio				X	X
Servidores de PowerPlay	Admin. del directorio				X	X
	Admin. de PowerPlay			X		X
Impresoras	Admin. del directorio			X	X	X
Administración de Query Service	Admin. del directorio				X	X
	Administradores del servidor			X		X
Ejecutar actividades y planificaciones	Admin. de informes			X		X
	Administradores de métrica			X		X
	Administradores de Controller			X		X
	Admin. del directorio				X	X
	Admin. de PowerPlay			X		X
Establecer prestaciones y gestionar perfiles de IU	Admin. del directorio			X	X	X
Estilos y portlets	Administradores de portales			X		X
	Admin. del directorio				X	X
	Administradores de biblioteca			X		X

Tabla 95. Características protegidas de la prestación de administración y permisos para grupos y roles relacionados (continuación)

Característica protegida	Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Usuarios, grupos y roles	Admin. del directorio			X	X	X

Prestación Analysis Studio

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 96. Prestación Analysis Studio y permisos para grupos y roles relacionados

Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Usuarios del análisis			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X
Modeladores			X		X
Admin. de informes			X		X

Prestación Cognos Insight

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 97. Prestación Cognos Insight y permisos para grupos y roles relacionados

Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Admin. del directorio				X	X

Prestación Cognos Viewer

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 98. Prestación Cognos Viewer y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Usuarios del análisis			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Consumidores			X		X
Admin. del directorio				X	X
Distribución de información			X		X
Modeladores			X		X
Administradores de PowerPlay			X		X
Usuarios de PowerPlay			X		X
Usuarios de consultas			X		X
Lectores			X		X
Admin. de informes			X		X

Las características protegidas de la tabla siguiente son hijos de la prestación Cognos Viewer.

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 99. Características protegidas de la prestación Cognos Viewer y permisos para grupos y roles relacionados

Característica protegida	Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Menú contextual Selección Barra de herramientas	Admin. de informes			X		X
	Autores			X		X
	Consumidores			X		X
	Usuarios de consultas			X		X
	Usuarios del análisis			X		X
	Lectores			X		X
	Autores de Express			X		X
	Admin. del directorio				X	X
	Admin. de PowerPlay			X		X
	Usuarios de PowerPlay			X		X
	Admin. de informes			X		X
	Autores			X		X
Ejecutar con opciones	Consumidores			X		X
	Usuarios de consultas			X		X
	Usuarios del análisis			X		X
	Autores de Express			X		X
	Admin. del directorio				X	X
	Admin. de PowerPlay			X		X
	Usuarios de PowerPlay			X		X

Prestación de colaboración

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 100. Prestación de colaboración y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Usuarios del análisis			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Consumidores			X		X
Admin. del directorio				X	X
Modeladores			X		X
Administradores de PowerPlay			X		X
Usuarios de PowerPlay			X		X
Usuarios de consultas			X		X
Admin. de informes			X		X

Las características protegidas de la tabla siguiente son hijos de la prestación de colaboración.

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 101. Características protegidas de la prestación de colaboración y permisos para grupos y roles relacionados

		Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Característica protegida	Grupo o rol					
Permitir características de colaboración	Usuarios del análisis			X		X
	Autores			X		X
	Consumidores			X		X
Lanzar herramientas de colaboración	Admin. del directorio				X	X
	Autores de Express			X		X
	Admin. de PowerPlay			X		X
	Usuarios de PowerPlay			X		X
	Usuarios de consultas			X		X
	Admin. de informes			X		X

Prestación Controller Studio

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 102. Prestación Controller Studio y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio				X	X

Prestación Panel de control

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 103. Prestación Panel de control y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Usuarios del análisis			X		X
Administradores de Analytics			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X
Distribución de información			Permiso denegado		Permiso denegado
Administradores de biblioteca			X		X
Administradores de Mobile			X		X
Modeladores			X		X
Administradores de portales			X		X
Administradores de PowerPlay			X		X
Usuarios de PowerPlay			X		X
Usuarios de consultas			X		X
Admin. de informes			X		X
Administradores del servidor			X		X
Administradores de arrendatarios			X		X

Prestación Data Manager

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 104. Prestación Data Manager y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio				X	X

Prestación Conjuntos de datos

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 105. Prestación Conjuntos de datos y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Admin. del directorio				X	X
Todos			X		X

Función Desktop Tools

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 106. Función de Desktop Tools y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Exploradores de Analytics			X		X
Admin. del directorio				X	X

Prestación Errores detallados

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 107. Prestación Errores detallados y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Admin. del directorio				X	X

Prestación Ayudante para acceso a detalles

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 108. Prestación Ayudante para acceso a detalles y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Admin. del directorio				X	X

Prestación Event Studio

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 109. Prestación Event Studio y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X
Modeladores			X		X
Admin. de informes			X		X

Prestación Ejecutar búsqueda con índice

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 110. Prestación Ejecutar búsqueda con índice y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Usuarios del análisis			X		X
Exploradores de Analytics					
Usuarios de Analytics					
Autores					
Consumidores					
Distribución de información					
Modeladores					
Administradores de PowerPlay					
Usuarios de PowerPlay					
Usuarios de consultas					
Lectores					
Admin. de informes					
Admin. del directorio				X	X

Prestación Panel de control ejecutivo

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 111. Prestación Panel de control ejecutivo y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Usuarios del análisis			X		X
Administradores de Analytics			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X

Tabla 111. Prestación Panel de control ejecutivo y permisos para grupos y roles relacionados (continuación)

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Distribución de información			Permiso denegado		Permiso denegado
Administradores de biblioteca			X		X
Administradores de Mobile			X		X
Modeladores			X		X
Administradores de portales			X		X
Admin. de PowerPlay			X		X
Usuarios de PowerPlay			X		X
Usuarios de consultas			X		X
Admin. de informes			X		X
Administradores del servidor			X		X
Administradores de arrendatarios			X		X

Las características protegidas de la tabla siguiente son hijos de la prestación Panel de control ejecutivo.

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 112. Características protegidas de la prestación Panel de control ejecutivo y permisos para grupos y roles relacionados

Característica protegida	Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Utilizar características avanzadas de panel de control	Autores			X		X
	Admin. del directorio				X	X
Utilizar características interactivas de panel de control	Usuarios de consultas			X		X
	Admin. de informes			X		X

Prestación Repositorios externos

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 113. Prestación Repositorios externos y permisos para grupos y roles relacionados

Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Admin. del directorio				X	X
Todos			X		X

Las características protegidas de la tabla siguiente son hijos de la prestación Repositorios externos.

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 114. Características protegidas de la prestación Repositorios externos y permisos para grupos y roles relacionados

Característica protegida	Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Administrar conexiones de repositorios	Admin. del directorio				X	X
Ver documentos externos	Admin. del directorio				X	X
	Todos			X		X

Generar salida CSV

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 115. Prestación Generar salida CSV y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio				X	X
Todos			X		X

Generar salida PDF

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 116. Prestación Generar salida PDF y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio				X	X
Todos			X		X

Generar salida XLS

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 117. Prestación Generar salida XLS y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio				X	X
Todos			X		X

Generar salida XML

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 118. Prestación Generar salida XML y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Admin. del directorio				X	X
Todos			X		X

Prestación Glosario

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 119. Prestación Glosario y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Todos			X		X
Admin. del directorio				X	X

Prestación Ocultar entradas

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 120. Prestación Ocultar entradas y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Todos			X		X
Admin. del directorio				X	X

Prestación Importar metadatos relacionales

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 121. Prestación Importar metadatos relacionales y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Admin. del directorio				X	X
Admin. de informes			X		X

Prestación Linaje

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 122. Prestación Linaje y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Todos			X		X
Admin. del directorio				X	X

Prestación Gestionar contenido

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 123. Prestación Gestionar contenido y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Administradores de biblioteca			X		X
Administradores de Mobile					
Administradores de portales					
Administradores de PowerPlay					
Admin. de informes					
Administradores del servidor					
Admin. del directorio			X	X	X

Prestación Administrar inicios de sesión de origen de datos propios

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 124. Prestación Administrar inicios de sesión de origen de datos propios y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio				X	X

Prestación Metric Studio

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 125. Prestación Metric Studio y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Grupo o rol					
Exploradores de Analytics			X		X
Admin. del directorio				X	X

Prestación Mobile

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 126. Prestación Mobile y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Grupo o rol					
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Admin. del directorio				X	X
Distribución de información			X		X
Administradores de Mobile			X		X
Usuarios de Mobile			X		X

Prestación Planning Contributor

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 127. Prestación Planning Contributor y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Admin. del directorio				X	X

Prestación PowerPlay Studio

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 128. Prestación PowerPlay Studio y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X
Modeladores			X		X
Admin. de PowerPlay			X		X
Usuarios de PowerPlay			X		X

Prestación Query Studio

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 129. Prestación Query Studio y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X

Tabla 129. Prestación Query Studio y permisos para grupos y roles relacionados (continuación)

	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Grupo o rol					
Modeladores			X		X
Usuarios de consultas			X		X
Admin. de informes			X		X

Las características protegidas de la tabla siguiente son hijos de la prestación Query Studio.

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 130. Características protegidas de la prestación Query Studio y permisos para grupos y roles relacionados

		Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Característica protegida	Grupo o rol					
Crear Advanced	Autores			X		X
	Usuarios de consultas			X		X
	Admin. de informes			X		X
	Admin. del directorio				X	X

Prestación Report Studio

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 131. Prestación Creación de informes y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Grupo o rol					
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X
Administradores de biblioteca			X		X

Tabla 131. Prestación Creación de informes y permisos para grupos y roles relacionados (continuación)

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Modeladores			X		X
Admin. de informes			X		X

Las características protegidas de la tabla siguiente son hijos de la prestación Creación de informes.

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 132. Características protegidas de la prestación de Creación de informes y permisos para grupos y roles relacionados

		Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Característica protegida	Grupo o rol					
Separación	Autores			X		X
Elementos HTML en informe	Admin. de informes			X		X
	Admin. del directorio				X	X
SQL definido por el usuario						
Crear/Suprimir	Autores			X		X
	Admin. de informes			X		X
	Admin. del directorio				X	X
	Autores de Express			X		X
Permitir datos externos	Admin. del directorio				X	X

Prestación de planificación

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 133. Prestación de planificación y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Usuarios del análisis			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Consumidores					X
Admin. del directorio				X	X
Modeladores			X		X
Admin. de PowerPlay			X		X
Usuarios de PowerPlay			X		X
Usuarios de consultas			X		X
Admin. de informes			X		X

Las características protegidas de la tabla siguiente son hijos de la prestación de planificación.

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 134. Características protegidas de la prestación de planificación y permisos para grupos y roles relacionados

Característica protegida	Grupo o rol	Lectura 	Escritura 	Ejecución 	Establecimiento de políticas 	Visita 
Planificación por día	Usuarios del análisis			X		X
	Autores			X		X
Planificación por hora	Consumidores			X		X
	Administradores de Controller			X		X
Planificación por minuto	Usuarios de Controller			X		X
Planificación por mes	Admin. del directorio				X	X
Planificación por activador	Autores de Express			X		X
	Administradores de métrica			X		X
Planificación por semana	Autores de métrica			X		X
	Usuarios de consultas			X		X
Planificación por año	Admin. de informes			X		X
	Admin. de PowerPlay			X		X
	Usuarios de PowerPlay			X		X
	Admin. de informes			X		X
Prioridad de planificación	Administradores de métrica			X		X
	Administradores de Controller			X		X
	Admin. del directorio				X	X
	Admin. de PowerPlay			X		X
	Admin. de informes			X		X

Prestación Asistente para paquetes de autoservicio

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 135. Prestación Asistente para paquetes de autoservicio y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Admin. del directorio			X	X	X

Prestación Establecer funciones específicas de entradas

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 136. Prestación Establecer funciones específicas de entradas y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Admin. del directorio				X	X

Prestación de instantáneas

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 137. Prestación Instantáneas y permisos iniciales para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Estable- cimiento de políticas	Visita
Grupo o rol					
Admin. del directorio				X	X
Todos			X		X
Modeladores			X		X

Prestación de Ejecución de especificaciones

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 138. Prestación Ejecución de especificaciones y permisos iniciales para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Establecimiento de políticas	Visita
Grupo o rol					
Admin. del directorio				X	X

Cargar archivos

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 139. Prestación Cargar archivos y permisos para grupos y roles relacionados

	Lectura	Escritura	Ejecución	Establecimiento de políticas	Visita
Grupo o rol					
Usuarios del análisis			X		X
Administradores de Analytics			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X
Distribución de información			Permiso denegado		Permiso denegado
Administradores de biblioteca			X		X
Administradores de Mobile			X		X
Modeladores			X		X
Administradores de portales			X		X
Administradores de PowerPlay			X		X
Usuarios de PowerPlay			X		X
Usuarios de consultas			X		X
Admin. de informes			X		X
Administradores del servidor			X		X

Prestación Reglas de observación

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 140. Prestación Reglas de observación y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Usuarios del análisis			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Consumidores			X		X
Admin. del directorio				X	X
Modeladores			X		X
Administradores de PowerPlay			X		X
Usuarios de PowerPlay			X		X
Usuarios de consultas			X		X
Admin. de informes			X		X

Prestación Modelado basado en web

En la tabla siguiente, la letra X indica que se otorga un permiso a un grupo o a un rol sobre un objeto.

Tabla 141. Prestación Modelado basado en web y permisos para grupos y roles relacionados

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Administradores de Analytics			X		X
Exploradores de Analytics			X		X
Usuarios de Analytics			X		X
Autores			X		X
Admin. del directorio				X	X
Distribución de información			Permiso denegado		Permiso denegado
Administradores de biblioteca			X		X
Administradores de Mobile			X		X
Modeladores			X		X
Administradores de portales			X		X
Administradores de PowerPlay			X		X
Usuarios de PowerPlay			X		X
Usuarios de consultas			X		X

Tabla 141. Prestación Modelado basado en web y permisos para grupos y roles relacionados (continuación)

	Lectura 	Escritura 	Ejecución 	Estable- cimiento de políticas 	Visita 
Grupo o rol					
Admin. de informes			X		X
Administradores del servidor			X		X
Administradores de arrendatarios			X		X

Apéndice D. Localización de bases de datos de ejemplos

Las bases de datos de ejemplo que se proporcionan con el software de IBM Cognos ofrecen una demostración de un entorno de creación de informes multilingüe.

Los ejemplos almacenan una selección de campos de texto, como nombres y descripciones, en 23 idiomas.

Este apéndice describe cómo se almacenan los datos en las bases de datos de ejemplos y cómo se configuran estas bases de datos para utilizar los datos multilingües.

Para obtener más información sobre los ejemplos, consulte *IBM Cognos Analytics Guía de ejemplos*.

Una columna por idioma

En esta estructura, las tablas contienen conjuntos de 23 columnas, una por cada idioma.

Se utiliza una convención de nomenclatura lógica para indicar el idioma que contiene una columna. El nombre de cada columna termina con un código de idioma, como `_EN` para inglés y `_FR` para francés. Por ejemplo, la columna que contiene información sobre los países y regiones será `COUNTR_FR` para los datos en francés y `COUNTRY_DE` para los datos en alemán. Todas las tablas usan esta estructura salvo `PRODUCT_LOOKUP`.

Determinación del idioma (columnas) en el modelo

En Framework Manager, puede insertar una macro en la SQL del asunto de consulta de orígenes de datos para devolver una columna específica de datos. El asunto de consulta usará la macro para aplicar el valor de entorno local y devolver un código de idioma. Un entorno local especifica la información lingüística y las convenciones culturales para tipo de carácter, ordenación, formato de fecha y hora, unidad de moneda y mensajes.

La macro, `runLocale`, usa un mapa de parámetros para convertir el idioma del contenido del usuario en un nombre de columna completo o parcial. A continuación, este nombre de columna se sustituye en la SQL antes de que se ejecute la consulta.

Las bases de datos de ejemplos usan un código de idioma como sufijo para el nombre de la columna, por lo que la macro correlaciona un mapa de parámetros con los que convertir entornos locales de ejecución válidos en un código de idioma para, a continuación, concatenar el código de idioma al nombre de columna base.

Consulta de ejemplo

La macro de esta consulta de ejemplo usa la variable de la sesión `runLocale` como clave de mapa de parámetros de `Language_lookup`.

Devuelve el código de idioma que se usará como sufijo del nombre de la columna. En la siguiente sentencia de selección, en la que francés es el idioma, la macro genera el nombre de columna `COUNTRY_FR`.

```

Select
COUNTRY.COUNTRY_CODE,
#'COUNTRY.COUNTRY_' + $Language_lookup{$runLocale}# as
Product_Line
from
[great_outdoors].COUNTRY

```

Gracias a la flexibilidad de Framework Manager, las columnas multilingües no tienen que usar el sistema de nombres usados en los ejemplos. De hecho, puede nombrar a las columnas multilingües usando cualquier sistema. Puede codificar su esquema de definición de nombres en el de mapa de parámetros, según sea necesario. Puede usar cualquier variable de la sesión como clave de mapa de parámetros y devolver cualquier sintaxis SQL que necesite sustituir en tiempo de ejecución. Para obtener más información, consulte el documento Framework Manager *User Guide*.

Una fila por idioma

En esta estructura, cada valor de la cadena tiene una fila con una columna de código que identifica el idioma.

Los datos se filtran para devolver sólo la fila que contenga los datos de idioma solicitados. Por lo general, los datos multilingües se almacenan en una tabla independiente para evitar la duplicación no descriptiva o los datos monolingües.

En las bases de datos de ejemplos, la tabla de datos contiene la clave principal y los datos monolingües, como la información de fecha. La tabla multilingüe contiene datos y una clave compuesta del código de idioma y la clave foránea. Por ejemplo, la tabla PRODUCT_NAME_LOOKUP contiene las columnas PRODUCT_NUMBER, PRODUCT_LANGUAGE y PRODUCT_NAME, donde PRODUCT_NUMBER y PRODUCT LANGUAGE forman la clave principal. Cada elemento localizado se expresa en 23 filas, una por cada idioma.

La siguiente tabla de clave foránea contiene uno o varios elementos localizados.

Tabla 142. Ejemplo de tabla de claves foráneas que contiene elementos localizados

Tabla de clave principal	Tabla de clave foránea	Base de datos
PRODUCTO	PRODUCT_NAME_LOOKUP	VENTASVA
DIM PRODUCTO SLS	SLS_PRODUCT_LOOKUP	VENTASGADW

Las bases de datos de ejemplos usan los códigos de idioma ISO para identificar cada fila de datos.

Determinación del idioma (filas) en el modelo

En Framework Manager, puede insertar una macro en la SQL del asunto de consulta de orígenes de datos para devolver una fila específica de datos.

El asunto de consulta usará la macro para aplicar el valor de entorno local y devolver un código de idioma.

Consulta de ejemplo

La macro de la siguiente consulta de ejemplo usa la variable de sesión `runLocale` como la clave de mapa del parámetro `Language_lookup` y devuelve el código de idioma correspondiente. La función `sq()` especifica que el valor devuelto de la macro se debe incluir entre comillas simples para producir un predicado válido del filtro SQL. En el siguiente enunciado de selección, donde Alemán es el idioma, el macro identifica el idioma como DE (Alemán), y produce el filtro `(PRODUCT_MULTILINGUAL."LANGUAGE" = 'DE')`.

```
Select
P.INTRODUCTION_DATE,
P.PRODUCT_TYPE_CODE,
P.PRODUCTION_COST,
P.MARGIN,
PRODUCT_LOOKUP.PRODUCT_NUMBER as PRODUCT_NUMBER1,
PRODUCT_LOOKUP."PRODUCT_LANGUAGE",
PRODUCT_LOOKUP.PRODUCT_NAME,
PRODUCT_LOOKUP.PRODUCT_DESCRIPTION
From
gosales].PRODUCT as P,
[gosales].PRODUCT_LOOKUP
Where
P.PRODUCT_NUMBER = PRODUCT_LOOKUP.PRODUCT_NUMBER
and
(PRODUCT_LOOKUP."PRODUCT_LANGUAGE" = #sq($Language_lookup{$runLocale})#)
```

Transcripciones y extensiones multialfabeto

Para la transcripción de los idiomas asiáticos, una tabla contiene dos columnas con información equivalente.

Una columna muestra los valores de la cadena sólo con caracteres latinos. La otra columna muestra los valores de la cadena con caracteres latinos y asiáticos. La convención de nomenclatura consiste en añadir el sufijo `_MB`.

En la columna de sólo caracteres latinos, la transcripción define el equivalente fonético del valor definido en la columna `_MB`.

Las siguientes tablas incluyen columnas con valores transcritos.

Tabla 143. Columnas con valores convertidos equivalentes, ejemplo

Tabla	Base de datos
CABECERA_PEDIDO	VENTASVA
MINORISTA	VENTASVA
SEDE_MINORISTA_MB	VENTASVA
SUCURSAL	VENTASVA
EMPLEADO	VENTASVA

Trascripciones en el modelo

El siguiente ejemplo crea un origen de datos simple, basado en un asunto de consulta de dos tablas. Las tablas son idénticas salvo por el uso de caracteres asiáticos en una de ellas.

La columna con nombres que terminan con el sufijo _MB almacena datos asiáticos con caracteres de esta región, como los ideogramas del chino. Así se elimina parte de la duplicación y se facilita la definición de relaciones para otros asuntos de consulta en el modelo.

```
Select
RS.RTL_RETAILER_SITE_CODE,
RS.RTL_RETAILER_CODE,
RS.RTL_ADDRESS1,
RS.RTL_ADDRESS2,
RS.RTL_CITY,
RS.RTL_REGION,
RS.RTL_POSTAL_ZONE,
RS.RTL_COUNTRY_CODE,
RS.RTL_ACTIVITY_STATUS_CODE,
RS_MB.RTL_ADDRESS1 as Address1_MB,
RS_MB.RTL_ADDRESS2 as Address2_MB,
RS_MB.RTL_CITY as City_MB,
RS_MB.RTL_REGION as Region_MB
from
[goretailers].RETAILER_SITE as RS,
[goretailers].RETAILER_SITE_MB
as RS_MB
where
RETAILER_SITE.RETAILER_SITE_CODE = RETAILER_SITE_MB.RETAILER_SITE_CODE
```

Extensiones multialfabeto

Tras definir los asuntos de consulta en el modelo, se cambia el nombre a los elementos con la extensión _MB por una extensión multialfabeto, como Dirección 1 (multialfabeto) para facilitar el uso y la lectura.

Uso de extensiones multialfabeto para el formateo condicional

Un ejemplo de uso del multialfabeto se da en una dirección postal en la que los valores multialfabeto garantizan que el formato de las etiquetas sea el adecuado para la entrega y gestión local.

Para añadir más valores a las etiquetas postales, el modelo Ventas de VA y Minoristas aplica el formateo condicional para generar formatos de direcciones internacionales.

En el siguiente ejemplo, Línea de dirección 3 es el nombre de un cálculo definido por el usuario que se utiliza para generar la tercera línea de una etiqueta postal. La expresión usa un valor de código de país o región para especificar cómo aplicar formato a la línea.

```
if ([Retailers].[Retailer
site].[Country or region code] = 6) then
(' ' + [Retailers].[Retailer
site].[Address 1 (multiscript)])
else
if ([Retailers].[Retailer site].[Country or region
code] = 8) then
([Retailers].[Retailer site].[Address
2 (multiscript)])
else
if ([Retailers].[Retailer site].[Country or region
```

```

code] = 13) then
([Retailers].[Retailer site].[Region
(multiscript)] + ' ' + [Retailers].[Retailer
site].[City (multiscript)]
+ ' ' + [Retailers].[Retailer
site].[Address 1 (multiscript)] + '
' + [Retailers].[Retailer site].[Address
2 (multiscript)])
else
if ([Retailers].[Retailer site].[Country or region
code] = 14) then
([Retailers].[Retailer site].[Address
2 (multiscript)])
else
([Retailers].[Retailer site].[Address
1 (multiscript)])

```

Las extensiones multialfabeto permiten a un usuario de cualquier idioma usar las mismas columnas del modelo para crear un bloque de direcciones y comprobar la dirección con el formato correcto para cada destino de entrega. Para obtener más información, consulte los asuntos de consulta de orígenes de datos Dirección postal del modelo de ejemplo ventasva_minoristasva.

Apéndice E. Esquema para los comandos de orígenes de datos

Cuando trabaja con conexiones con orígenes de datos, también puede añadir o editar comandos de orígenes de datos.

Los comandos de orígenes de datos se ejecutan cuando el motor de consulta realiza acciones específicas en una base de datos, como abrir una conexión o cerrar una sesión de usuario. Por ejemplo, puede utilizar los comandos de orígenes de datos para configurar una conexión proxy de Oracle o una base de datos privada virtual. Para obtener más información, consulte “Transferencia de contexto de IBM Cognos a una base de datos” en la página 160.

Un bloque de comandos de orígenes de datos es un documento XML que se utiliza para especificar los comandos que debe ejecutar la base de datos.

Este documento contiene material de referencia sobre cada elemento del esquema XML que define los bloques de comandos.

Después de la descripción de cada elemento, en secciones separadas se describen:

- Los elementos hijo que puede o debe tener el elemento.
- Los elementos padre que puede contener el elemento.

También figuran ejemplos de código que muestran cómo puede utilizar los elementos en un bloque de comandos.

La lista de hijos de cada elemento se presenta como un grupo de modelo DTD y los elementos se enumeran en el orden en el que deben aparecer. Se utiliza la siguiente notación estándar.

Tabla 144. Notación estándar para editar comandos de orígenes de datos

Símbolo	Significado
Signo más (+)	El elemento precedente se puede repetir varias veces, pero debe aparecer una vez como mínimo.
Signo de interrogación (?)	El elemento precedente es opcional. Puede estar ausente o puede aparecer exactamente una vez.
Asterisco (*)	Un asterisco (*) después de un elemento especifica que el elemento es opcional. Puede aparecer varias veces o ninguna.
Ninguno	Si un elemento no tiene ningún signo más (+), signo de interrogación (?) ni asterisco (*) después de él, el elemento deberá aparecer sólo una vez.

Tabla 144. Notación estándar para editar comandos de orígenes de datos (continuación)

Símbolo	Significado
Paréntesis	Elementos de grupo de paréntesis. Los grupos de elementos se controlan utilizando los mismos símbolos que los elementos.
Barra ()	Una barra () entre elementos especifica que uno de los elementos enumerados puede estar presente.
Coma (,)	Los elementos que separa deben estar presentes en el orden especificado.

commandBlock

Define un grupo de comandos que ejecuta la base de datos cuando se produce un evento concreto. Éste es el elemento raíz del esquema.

Elementos hijo del elemento commandBlock

(commands) +

Elementos padre del elemento commandBlock

El elemento commandBlock no tiene elementos padre.

comandos

Especifica el conjunto de comandos que ejecuta la base de datos. Los comandos se ejecutan en el orden en que aparecen dentro de commandBlock.

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Elementos hijo del elemento commands

(sessionStartCommand | sessionEndCommand | setCommand | sqlCommand) *

Elementos padre del elemento commands

commandBlock

sessionStartCommand

Define un comando que se utiliza para iniciar una sesión proxy en la base de datos.

Sólo debe haber un sessionStartCommand por commandBlock. Si el commandBlock contiene más de un sessionStartCommand, sólo el último se utilizará para crear una sesión proxy.

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
        <argument>
          <name>OCI_ATTR_PASSWORD</name>
          <value>password1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
```

Elementos hijo del elemento sessionStartCommand

(arguments) ?

Elementos padre del elemento sessionStartCommand

commands

sessionEndCommand

Define un comando que se utiliza para finalizar una sesión proxy en la base de datos.

Si no se suministra ningún sessionEndCommand, la sesión proxy finalizará tras la desconexión de la base de datos.

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```
<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>
```

Elementos hijo del elemento sessionEndCommand

(arguments) ?

Elementos padre del elemento sessionEndCommand

commands

arguments

Especifica los valores de argumento que se utilizarán con el comando.

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```
<commandBlock>
  <commands>
    <sessionEndCommand>
      <arguments/>
    </sessionEndCommand>
  </commands>
</commandBlock>
```

Elementos hijo del elemento arguments

(argument) *

Elementos padre del elemento arguments

- sessionStart
- sessionEnd

argument

Define un valor de argumento para una llamada a una base de datos API.

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
        <argument>
          <name>OCI_ATTR_PASSWORD</name>
          <value>password1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>
```

Elementos hijo del elemento argument

(name y value)

Elementos padre del elemento argument

arguments

setCommand

Este elemento se reserva para utilizarlo en el futuro.

sqlCommand

Define un comando que representa una sentencia SQL nativo para que la ejecute la base de datos.

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> BEGIN PKG1.STORED_PROC1; END; </sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Elementos hijo del elemento sqlCommand

(sql)

Elementos padre del elemento sqlCommand

commands

sql

Especifica la sentencia SQL para que la ejecute la base de datos. La sentencia SQL debe estar en SQL nativo.

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```
<commandBlock>
  <commands>
    <sqlCommand>
      <sql> BEGIN PKG1.STORED_PROC1; END; </sql>
    </sqlCommand>
  </commands>
</commandBlock>
```

Elementos hijo del elemento sql

El elemento sql no tiene elementos hijo.

Elementos padre del elemento sql

sqlCommand

name

Identifica el argumento que se va a configurar.

El valor del elemento name debe ser uno de los siguientes:

- OCI_ATTR_USERNAME
- OCI_ATTR_PASSWORD

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```
<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
```

```

        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>

```

Elementos hijo del elemento name

El elemento name no tiene elementos hijo.

Elementos padre del elemento name

- argument
- setCommand

value

Especifica el valor que se va a utilizar para el argumento.

Este es un ejemplo de cómo se puede utilizar este elemento en un commandBlock.

```

<commandBlock>
  <commands>
    <sessionStartCommand>
      <arguments>
        <argument>
          <name>OCI_ATTR_USERNAME</name>
          <value>PROXY_USER1</value>
        </argument>
      </arguments>
    </sessionStartCommand>
  </commands>
</commandBlock>

```

Elementos hijo del elemento value

El elemento value no tiene elementos hijo.

Elementos padre del elemento value

- argument
- setCommand

Apéndice F. Esquema de datos para mensajes de registro

Si configura el software de IBM Cognos para que envíe mensajes de registro a una base de datos, las tablas y las columnas de cada tabla se crearán automáticamente al iniciar los servicios de IBM Cognos.

Para evitar conflictos de nombres con palabras clave de la base de datos, todos los nombres de las columnas de la base de datos de registro llevan el prefijo "COGIPF". Si ha creado su propio modelo de base de datos de registro, deberá añadir el prefijo "COGIPF" a los nombres de columna de las tablas de base de datos de registro del modelo.

Definiciones de tablas

Los mensajes de registro se registran en una tabla de la base de datos de registro bajo determinadas condiciones. Dichas condiciones dependen en el nivel de registro configurado en el portal web.

Para obtener información sobre los niveles de registro, consulte "Mensajes de registro" en la página 18.

Cuando un usuario inicia sesión en el software de IBM Cognos, se asigna un identificador de sesión y se registra en todos los mensajes de registro. Puede utilizar el identificador de sesión para identificar todas las acciones realizadas por un usuario.

Tabla COGIPF_ACTION

Almacena información sobre operaciones realizadas en objetos.

Tabla 145. Columnas de tabla, descripciones y tipos de datos de COGIPF_ACTION

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCAL_TIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)

Tabla 145. Columnas de tabla, descripciones y tipos de datos de COGIPF_ACTION (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_OPERATION	La acción realizada en el objeto	VARCHAR (255)
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación	VARCHAR (255)
COGIPF_TARGET_PATH	La ruta de acceso del objeto de destino	VARCHAR (1024)
COGIPF_STATUS	El estado de la operación: en blanco (si la ejecución no ha finalizado), correcto, aviso o error	VARCHAR (255)
COGIPF_ERRORDETAILS	Detalles del error	VARCHAR (2000)

Tabla COGIPF_AGENTBUILD

Almacena información sobre la entrega de correo electrónico del agente.

Tabla 146. Columnas de tabla, descripciones y tipos de datos de COGIPF_AGENTBUILD

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILD_NUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_OPERATION	Operación	VARCHAR (128)
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación	VARCHAR (255)

Tabla 146. Columnas de tabla, descripciones y tipos de datos de COGIPF_AGENTBUILD (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_TARGET_NAME	El nombre de destino	VARCHAR (512)
COGIPF_TARGET_PATH	La ruta de acceso de destino	VARCHAR (1024)
COGIPF_STATUS	El estado de la operación: en blanco, correcto, aviso o error	VARCHAR (255)
COGIPF_ERRORDETAILS	Detalles del error	VARCHAR (2000)
COGIPF_AGENT_PATH	El nombre del agente	VARCHAR (1024)
COGIPF_SCHEDULETIME	El tiempo de planificación de destino	INTEGER
COGIPF_USER	El usuario que ha creado el agente	VARCHAR (512)
COGIPF_EMAIL	La dirección de correo electrónico	VARCHAR (512)

Tabla COGIPF_AGENTRUN

Almacena información sobre la actividad del agente, incluidas las tareas y la entrega.

Tabla 147. Columnas de tabla, descripciones y tipos de datos de COGIPF_AGENTRUN

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER

Tabla 147. Columnas de tabla, descripciones y tipos de datos de COGIPF_AGENTRUN (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILD_NUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_OPERATION	Operación	VARCHAR (128)
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación	VARCHAR (255)
COGIPF_TARGET_PATH	La ruta de acceso de destino	VARCHAR (1024)
COGIPF_STATUS	El estado de la operación: en blanco, correcto, aviso o error	VARCHAR (255)
COGIPF_ERROR_DETAILS	Detalles del error	VARCHAR (2000)
COGIPF_AGENTPATH	El nombre del agente	VARCHAR (1024)
COGIPF_SCHEDULETIME	El tiempo de planificación de destino	INTEGER
COGIPF_TARGET_NAME	El nombre de destino	VARCHAR (512)

Tabla 147. Columnas de tabla, descripciones y tipos de datos de COGIPF_AGENTRUN (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_USER	El usuario que ha creado el agente	VARCHAR (512)
COGIPF_EMAIL	La dirección de correo electrónico	VARCHAR (512)
COGIPF_MESSAGEID	Identificación del mensaje	VARCHAR (255)

Tabla COGIPF_ANNOTATIONSERVICE

Almacena información de auditoría sobre las operaciones del servicio de anotaciones.

Para obtener más información, consulte Capítulo 4, “Métricas de rendimiento del sistema”, en la página 29.

Tabla 148. Columnas de tabla, descripciones y tipos de datos de COGIPF_ANNOTATIONSERVICE

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso; vacío si no hay ninguno	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria	VARCHAR (255)

Tabla 148. Columnas de tabla, descripciones y tipos de datos de COGIPF_ANNOTATIONSERVICE (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_OPERATION	La acción realizada en el objeto	VARCHAR (255)
COGIPF_TARGET_TYPE	El tipo de destino	VARCHAR (255)
COGIPF_TARGET_PATH	Ruta de acceso de objeto	VARCHAR (1024)
COGIPF_ANNOTATION	Identificación alfanumérica de la anotación	BIGINT
COGIPF_USER	Identificador del usuario que ha realizado la operación en la anotación; por ejemplo, crear, actualizar o suprimir	VARCHAR (1024)
COGIPF_PARENT_ID	Identificación del objeto padre	VARCHAR (1024)
COGIPF_CREATION_TIME	Hora y fecha en la que se creó la anotación	TIMESTAMP
COGIPF_UPDATE_TIME	Hora y fecha en la que se actualizó la anotación	TIMESTAMP

Tabla COGIPF_EDITQUERY

Almacena información sobre ejecuciones de consultas.

Tabla 149. Columnas de tabla, descripciones y tipos de datos de COGIPF_EDITQUERY

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)

Tabla 149. Columnas de tabla, descripciones y tipos de datos de COGIPF_EDITQUERY (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro Mientras se ejecuta el informe, ésta es la hora a la que comenzó la ejecución. Tras la conclusión de la ejecución del informe, ésta es la hora final de su ejecución. Para comprobar si la ejecución ha finalizado, consulte COGIPF_STATUS. Una entrada en blanco significa que la ejecución no se ha completado. Una entrada rellena significa que la ejecución se ha completado. Para calcular la hora de inicio de la ejecución de un informe que ya se ha ejecutado, reste COGIPF_RUNTIME de COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)

Tabla 149. Columnas de tabla, descripciones y tipos de datos de COGIPF_EDITQUERY (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación	VARCHAR (255)
COGIPF_QUERYPATH	La ruta del informe	VARCHAR (1024)
COGIPF_STATUS	El estado de la operación: en blanco, correcto, aviso o error	VARCHAR (255)
COGIPF_ERRORDETAILS	Detalles del error	VARCHAR (2000)
COGIPF_RUNTIME	El número de milisegundos que ha tardado en ejecutarse la consulta	INTEGER
COGIPF_QUERYNAME	El nombre del informe que se ha consultado	VARCHAR (512)
COGIPF_PACKAGE	El paquete con el que se asocia el informe	VARCHAR (1024)
COGIPF_MODEL	El modelo con el que se asocia el informe	VARCHAR (512)

Tabla COGIPF_HUMANTASKSERVICE

Almacena información de auditoría sobre las operaciones del servicio de tareas humanas Human Task Service (las tareas y los estados de las tareas correspondientes).

Para obtener más información, consulte Capítulo 4, “Métricas de rendimiento del sistema”, en la página 29.

Tabla 150. Columnas de tabla, descripciones y tipos de datos de COGIPF_HUMANTASKSERVICE

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER

Tabla 150. Columnas de tabla, descripciones y tipos de datos de COGIPF_HUMANTASKSERVICE (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255)
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_OPERATION	Acción realizada sobre el objeto; por ejemplo, ADD, UPDATE	VARCHAR (128)
COGIPF_TARGET_TYPE	El tipo de destino	VARCHAR (255)
COGIPF_TARGET_PATH	Ruta de acceso de objeto	VARCHAR (1024)
COGIPF_STATUS	El estado de la operación: en blanco (si la ejecución no ha finalizado), correcto, aviso o error	VARCHAR (50)
COGIPF_LOGENTRYID	Clave principal utilizada para enlazar las tablas COGIPF_HUMANTASKSERVICE y COGIPF_HUMANTASKSERVICE_DETAIL	VARCHAR (50) NOT NULL
COGIPF_TASKID	Identificación de la tarea	VARCHAR (50)

Tabla 150. Columnas de tabla, descripciones y tipos de datos de COGIPF_HUMANTASKSERVICE (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_TRANSACTION_TYPE	Operación que se realiza, propia del servicio de tareas humanas; por ejemplo, claim, setPriority, getTaskInfo, changeSubscription	VARCHAR (255)
COGIPF_USER	Usuario que ha realizado la transacción en COGIPF_TRANSACTION_TYPE	VARCHAR (255)
COGIPF_TASK_PRIORITY	Prioridad de la tarea: • 1 = alta • 3 = media • 5 = baja	INTEGER
COGIPF_TASK_STATUS	Estado de la tarea: en blanco (si la ejecución no ha finalizado), correcto, aviso o error	VARCHAR (255)
COGIPF_TASK_ACTIVATION_TIME	Hora a la que se activó la tarea Valor de fecha/hora que se almacena en la base de datos en formato numérico largo	BIGINT
COGIPF_TASK_EXPIRATION_TIME	Fecha y hora en la que caducó la tarea	BIGINT
COGIPF_TASK_NAME	El nombre de la tarea.	NTEXT
COGIPF_TASK_SUBJECT	El asunto de la tarea.	NTEXT
COGIPF_TASK_DESCRIPTION	La descripción de la tarea.	NTEXT
COGIPF_TASK_TIMEZONEID	El identificador del huso horario de la tarea.	VARCHAR (50)
COGIPF_TASK_ACTUAL_OWNER	Propietario de la tarea	VARCHAR (255)
COGIPF_TASK_INITIATOR	Iniciador (creador) de la tarea	VARCHAR (255)
COGIPF_TASK_CLASS_NAME	Nombre de la clase de tarea de la que la tarea es una instancia	VARCHAR (255)
COGIPF_TASK_CLASS_OPERATION	La acción realizada en el objeto	VARCHAR (255)

Tabla 150. Columnas de tabla, descripciones y tipos de datos de COGIPF_HUMANTASKSERVICE (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_TASK_COMMENT	Comentarios que están relacionados con la tarea	VARCHAR (2048)

Tabla COGIPF_HUMANTASKSERVICE_DETAIL

Almacena detalles adicionales sobre las operaciones del servicio de tareas humanas Human Task Service (que no se requieren necesariamente para cada entrada de auditoría; por ejemplo, los detalles de notificaciones y los detalles de los roles humanos).

Para obtener más información, consulte Capítulo 4, “Métricas de rendimiento del sistema”, en la página 29.

Tabla 151. Columnas de tabla, descripciones y tipos de datos de COGIPF_HUMANTASKSERVICE

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255)
COGIPF_STEPID	Identificación alfanumérica del paso; vacío si no hay ninguno	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria	VARCHAR (255)
COGIPF_TASKID	Identificación alfanumérica de la tarea	VARCHAR (50)
COGIPF_LOGENTRYID	Clave principal utilizada para enlazar las tablas COGIPF_HUMANTASKSERVICE y COGIPF_HUMANTASKSERVICE_DETAIL	VARCHAR (50) NOT NULL
COGIPF_NOTIFICATION_DETAILS	Detalles sobre los correos electrónicos de notificación enviados sobre la tarea	NTEXT

Tabla 151. Columnas de tabla, descripciones y tipos de datos de COGIPF_HUMANTASKSERVICE (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_HUMANROLE_USER	Identificador del usuario que desempeña un rol para una tarea Se combina con COGIPF_HUMANROLE para definir el rol del usuario para la tarea.	VARCHAR (255)
COGIPF_HUMANROLE_ROLE	Rol del usuario Se combina con COGIPF_HUMAN_USER para definir el rol del usuario para la tarea.	VARCHAR (50)
COGIPF_SUBSCRIPTION_OPERATION	Operación de suscripción; por ejemplo, SUBSCRIBE o UNSUBSCRIBE	VARCHAR (50)
COGIPF_SUBSCRIPTION_EVENT	Evento de tarea al que el usuario se suscribe o cuya suscripción anula	SMALLINT
COGIPF_SUBSCRIPTION_USER	Usuario que se suscribe o que anula su suscripción a un evento de tarea	VARCHAR (255)
COGIPF_TASK_MESSAGE	Mensaje de la tarea	NTEXT
COGIPF_TASK_MESSAGE_TYPE	Tipo de mensaje almacenado en COGIPF_TASK_MESSAGE Los valores pueden ser INPUT, OUTPUT o FAULT	VARCHAR (20)
COGIPF_DETAIL_ID	Número de secuencia del registro de detalle	VARCHAR (50) NOT NULL

Tabla COGIPF_NATIVEQUERY

Almacena información sobre consultas realizadas por el software de IBM Cognos en otros componentes.

Tabla 152. Columnas de tabla, descripciones y tipos de datos de COGIPF_NATIVEQUERY

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)

Tabla 152. Columnas de tabla, descripciones y tipos de datos de COGIPF_NATIVEQUERY (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR2 (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_REQUESTSTRING	La cadena de solicitud de consulta realizada a otros componentes	NTEXT (1G)

Tabla COGIPF_PARAMETER

Almacena información de parámetros registrada por un componente.

Tabla 153. Columnas de tabla, descripciones y tipos de datos de COGIPF_PARAMETER

Nombre de columna	Descripción	Tipo de datos
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_OPERATION	La acción realizada en el objeto	VARCHAR (255)
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación	VARCHAR (255)
COGIPF_PARAMETER_NAME	El nombre del parámetro registrado por un componente	VARCHAR (255)
COGIPF_PARAMETER_VALUE	El valor del parámetro registrado por un componente	VARCHAR (512)
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_PARAMETER_VALUE_BLOB	Parámetros de solicitud de informes y opciones de ejecución de informes	NTEXT

Tabla COGIPF_RUNJOB

Almacena información sobre ejecuciones de trabajos.

Tabla 154. Columnas de tabla, descripciones y tipos de datos de COGIPF_RUNJOB

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER

Tabla 154. Columnas de tabla, descripciones y tipos de datos de COGIPF_RUNJOB (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro Mientras se ejecuta el informe, ésta es la hora a la que comenzó la ejecución. Tras la conclusión de la ejecución del informe, ésta es la hora final de su ejecución. Para comprobar si la ejecución ha finalizado, consulte COGIPF_STATUS. Una entrada en blanco significa que la ejecución no se ha completado. Una entrada rellena significa que la ejecución se ha completado. Para calcular la hora de inicio de la ejecución de un informe que ya se ha ejecutado, reste COGIPF_RUNTIME de COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación	VARCHAR (255)

Tabla 154. Columnas de tabla, descripciones y tipos de datos de COGIPF_RUNJOB (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_JOBPATH	La ruta de acceso del trabajo	VARCHAR (512)
COGIPF_STATUS	El estado de la operación: en blanco, correcto, aviso o error	VARCHAR (255)
COGIPF_ERRORDETAILS	Detalles del error	VARCHAR (2000)
COGIPF_RUNTIME	El número de milisegundos que ha tardado en ejecutarse el trabajo	INTEGER

Tabla COGIPF_RUNJOBSTEP

Almacena información sobre ejecuciones de pasos de trabajos.

Tabla 155. Columnas de tabla, descripciones y tipos de datos de COGIPF_RUNJOBSTEP

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro Mientras se ejecuta el informe, ésta es la hora a la que comenzó la ejecución. Tras la conclusión de la ejecución del informe, ésta es la hora final de su ejecución. Para comprobar si la ejecución ha finalizado, consulte COGIPF_STATUS. Una entrada en blanco significa que la ejecución no se ha completado. Una entrada rellena significa que la ejecución se ha completado. Para calcular la hora de inicio de la ejecución de un informe que ya se ha ejecutado, reste COGIPF_RUNTIME de COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER

Tabla 155. Columnas de tabla, descripciones y tipos de datos de COGIPF_RUNJOBSTEP (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación	VARCHAR (255)
COGIPF_JOBSTEPPATH	La ruta de acceso del paso del trabajo	VARCHAR (512)
COGIPF_STATUS	El estado de la operación: en blanco, correcto, aviso o error	VARCHAR (255)
COGIPF_ERRORDETAILS	Detalles del error	VARCHAR (2000)
COGIPF_RUNTIME	El número de milisegundos que ha tardado en ejecutarse el paso del trabajo	INTEGER

Tabla COGIPF_RUNREPORT

Almacena información sobre ejecuciones de informes.

Tabla 156. Columnas de tabla, descripciones y tipos de datos de COGIPF_RUNREPORT

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)

Tabla 156. Columnas de tabla, descripciones y tipos de datos de COGIPF_RUNREPORT (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro Mientras se ejecuta el informe, ésta es la hora a la que comenzó la ejecución. Tras la conclusión de la ejecución del informe, ésta es la hora final de su ejecución. Para comprobar si la ejecución ha finalizado, consulte COGIPF_STATUS. Una entrada en blanco significa que la ejecución no se ha completado. Una entrada rellena significa que la ejecución se ha completado. Para calcular la hora de inicio de la ejecución de un informe que ya se ha ejecutado, reste COGIPF_RUNTIME de COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER

Tabla 156. Columnas de tabla, descripciones y tipos de datos de COGIPF_RUNREPORT (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación Los valores incluyen: • Report ReportService es un informe interactivo • PromptForward ReportService es un informe generado tras una solicitud • PromptBackward ReportService es un informe generado después de que el usuario se haya desplazado a la página de solicitud anterior • Report BatchReportService es un informe de ejecución planificado o un informe por lotes Nota: El valor de esta columna es expresa en dos partes: el tipo de objeto de ejecución y desde qué servicio se ejecuta el informe; por ejemplo, "Report ReportService" y "Query BatchReportService".	VARCHAR (255)
COGIPF_REPORTPATH	La ruta del informe	VARCHAR (1024)
COGIPF_STATUS	El estado de la operación: en blanco, correcto, aviso o error	VARCHAR (255)
COGIPF_ERRORDETAILS	Detalles del error	VARCHAR (2000)
COGIPF_RUNTIME	El número de milisegundos que ha tardado en ejecutarse el informe	INTEGER
COGIPF_REPORTNAME	El nombre del informe que se ha ejecutado	VARCHAR (512)
COGIPF_PACKAGE	El paquete con el que se asocia el informe	VARCHAR (1024)
COGIPF_MODEL	El modelo con el que se asocia el informe	VARCHAR (512)

Tabla COGIPF_THRESHOLD_VIOLATIONS

Almacena información sobre infracciones de los umbrales de las métricas del sistema.

Para obtener más información, consulte: Capítulo 4, “Métricas de rendimiento del sistema”, en la página 29.

Tabla 157. Columnas de tabla, descripciones y tipos de datos de COGIPF_THRESHOLD_VIOLATIONS

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_COMPONENTID	Identificación alfanumérica del componente	VARCHAR (64)
COGIPF_BUILDNUMBER	Identificación alfanumérica de la compilación	INTEGER
COGIPF_LOG_LEVEL	El nivel de registro. Siempre debe ser 1 para garantizar que la información sobre infracción de umbrales esté disponible.	INTEGER
COGIPF_OPERATION	Se ha traspasado un umbral de la métrica.	VARCHAR (128)
COGIPF_TARGET_TYPE	El tipo de destino	VARCHAR (255)
COGIPF_TARGETNAME	El nombre de destino	VARCHAR (512)
COGIPF_TARGET_PATH	La ruta de destino del asignador que contiene el administrador de umbrales	VARCHAR (1024)
COGIPF_RESOURCE_TYPE	El tipo de recurso que sobrepasa el umbral	VARCHAR (128)
COGIPF_RESOURCE_PATH	La ruta del recurso que ha sobrepasado el valor de umbral	VARCHAR (512)
COGIPF_METRIC_NAME	El nombre de la métrica	VARCHAR (255)
COGIPF_METRIC_VALUE	El valor de la métrica	VARCHAR (128)
COGIPF_METRIC_HEALTH	El estado de la métrica: bueno, promedio o malo	VARCHAR (128)

Tabla 157. Columnas de tabla, descripciones y tipos de datos de COGIPF_THRESHOLD_VIOLATIONS (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_LOWER_AVG_THRSHLD	El valor del umbral promedio inferior Si COGIPF_LOWER_AVG_THRSHLD_XCL es 1, la puntuación de métrica será promedio cuando sea inferior a este valor de umbral. La puntuación de métrica es buena si es mayor o igual que este valor. Si COGIPF_LOWER_AVG_THRSHLD_XCL es 0 (cero), la puntuación de métrica será promedio si es inferior o igual a este valor. La puntuación de métrica es buena si es mayor que este valor.	VARCHAR (128)
COGIPF_LOWER_AVG_THRSHLD_EXCL	Distintivo que señala si el valor de umbral de COGIPF_LOWER_AVG_THRSHLD se incluye al determinar la puntuación de métrica Si es 0, el valor del umbral se incluirá cuando se haya determinado la puntuación de métrica. Si es 1, el valor del umbral no se incluirá cuando se haya determinado la puntuación de métrica.	DECIMAL (1,0)
COGIPF_LOWER_POOR_THRSHLD	El valor del umbral malo inferior Si COGIPF_LOWER_POOR_THRSHLD_XCL es 1, la puntuación de métrica será mala cuando sea inferior a este valor de umbral. Si COGIPF_LOWER_POOR_THRSHLD_XCL es 0 (cero), la puntuación de métrica será mala si es inferior o igual a este valor.	VARCHAR (128)
COGIPF_LOWER_POOR_THRSHLD_EXCL	Distintivo que señala si el valor de umbral de COGIPF_LOWER_POOR_THRSHLD se incluye al determinar la puntuación de métrica. Si es 0, el valor del umbral se incluirá cuando se haya determinado la puntuación de métrica. Si es 1, el valor del umbral no se incluirá cuando se haya determinado la puntuación de métrica.	DECIMAL (1,0)

Tabla 157. Columnas de tabla, descripciones y tipos de datos de COGIPF_THRESHOLD_VIOLATIONS (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_UPPER_AVG_THRSHLD	El valor de umbral promedio superior Si COGIPF_UPPER_AVG_THRSHLD_XC es 1, la puntuación de métrica será mala cuando sea inferior a este valor de umbral. Si COGIPF_UPPER_AVG_THRSHLD_XCL es 0 (cero), la puntuación de métrica será promedio si es mayor o igual a este valor. La puntuación de métrica es bueno si es inferior o igual que este valor.	VARCHAR (128)
COGIPF_UPPER_AVG_THRSHLD_EXCL	Distintivo que señala si el valor de umbral de COGIPF_UPPER_AVG_THRSHLD se incluye al determinar la puntuación de métrica. Si es 0, el valor del umbral se incluirá cuando se haya determinado la puntuación de métrica. Si es 1, el valor del umbral no se incluirá cuando se haya determinado la puntuación de métrica.	DECIMAL (1,0)
COGIPF_UPPER_POOR_THRSHLD	El valor de umbral malo superior Si COGIPF_UPPER_POOR_THRSHLD_XCL es 1, la puntuación de métrica será mala cuando sea inferior a este valor de umbral. Si COGIPF_UPPER_POOR_THRSHLD_XCL es 0 (cero), la puntuación de métrica será mala si es mayor o igual a este valor.	VARCHAR (128)
COGIPF_UPPER_POOR_THRSHLD_EXCL	Distintivo que señala si el valor de umbral de COGIPF_UPPER_POOR_THRSHLD se incluye al determinar la puntuación de métrica. Si es 0, el valor del umbral se incluirá cuando se haya determinado la puntuación de métrica. Si es 1, el valor del umbral no se incluirá cuando se haya determinado la puntuación de métrica.	DECIMAL (1,0)

Tabla COGIPF_USERLOGON

Almacena información de inicio y cierre de sesión del usuario.

Tabla 158. Columnas de tabla, descripciones y tipos de datos de COGIPF_USERLOGON

Nombre de columna	Descripción	Tipo de datos
COGIPF_CAMID	El CAMID del usuario	VARCHAR (512)

Tabla 158. Columnas de tabla, descripciones y tipos de datos de COGIPF_USERLOGON (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_STATUS	El estado de la operación: en blanco, correcto, aviso o error	VARCHAR (255)
COGIPF_ERRORDETAILS	Detalles del error	VARCHAR (2000)

Tabla 158. Columnas de tabla, descripciones y tipos de datos de COGIPF_USERLOGON (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_LOGON_OPERATION	Inicio de sesión, cierre de sesión o inicio de sesión caducado	VARCHAR (255)
COGIPF_USERNAME	El nombre de visualización del usuario	VARCHAR2 (255)
COGIPF_USERID	El nombre de usuario del usuario	VARCHAR (255)
COGIPF_NAMESPACE	El ID de espacio de nombre	VARCHAR (255)
COGIPF_REMOTE_IPADDR	Dirección IP del usuario	VARCHAR (128)
COGIPF_TENANTID	El ID de arrendatario	VARCHAR(255)

Tabla COGIPF_VIEWREPORT

Almacena información sobre solicitudes de vista de informes.

Tabla 159. Columnas de tabla, descripciones y tipos de datos de COGIPF_VIEWREPORT

Nombre de columna	Descripción	Tipo de datos
COGIPF_HOST_IPADDR	La dirección IP de host en la que se ha generado el mensaje de registro	VARCHAR (128)
COGIPF_HOST_PORT	El número de puerto de host	INTEGER
COGIPF_PROC_ID	El ID de proceso asignado por el sistema operativo	INTEGER

Tabla 159. Columnas de tabla, descripciones y tipos de datos de COGIPF_VIEWREPORT (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_LOCALTIMESTAMP	La fecha y la hora locales del momento en el que se generó el mensaje de registro Mientras se ejecuta el informe, ésta es la hora a la que comenzó la ejecución. Tras la conclusión de la ejecución del informe, ésta es la hora final de su ejecución. Para comprobar si la ejecución ha finalizado, consulte COGIPF_STATUS. Una entrada en blanco significa que la ejecución no se ha completado. Una entrada rellena significa que la ejecución se ha completado. Para calcular la hora de inicio de la ejecución de un informe que ya se ha ejecutado, reste COGIPF_RUNTIME de COGIPF_LOCALTIMESTAMP.	TIMESTAMP
COGIPF_TIMEZONE_OFFSET	El huso horario, respecto a GMT	INTEGER
COGIPF_SESSIONID	Identificación alfanumérica de la sesión del usuario	VARCHAR (255)
COGIPF_REQUESTID	Identificación alfanumérica de la solicitud	VARCHAR2 (255) NOT NULL
COGIPF_STEPID	Identificación alfanumérica del paso de la ejecución de un trabajo (vacío si no hay ninguno)	VARCHAR (255)
COGIPF_SUBREQUESTID	Identificación alfanumérica de la solicitud secundaria del componente	VARCHAR (255)
COGIPF_THREADID	Identificación alfanumérica del subproceso en el que se ejecuta la solicitud	VARCHAR (255)
COGIPF_COMPONENTID	El nombre del componente que genera la indicación	VARCHAR (64)
COGIPF_BUILDNUMBER	El número de compilación principal del componente que genera la indicación	INTEGER
COGIPF_LOG_LEVEL	El nivel de la indicación	INTEGER
COGIPF_TARGET_TYPE	El objeto en el que se ejecuta la operación	VARCHAR (255)

Tabla 159. Columnas de tabla, descripciones y tipos de datos de COGIPF_VIEWREPORT (continuación)

Nombre de columna	Descripción	Tipo de datos
COGIPF_REPORTPATH	La ruta del informe	VARCHAR (1024)
COGIPF_STATUS	El estado de la operación: en blanco, correcto, aviso o error	VARCHAR (255)
COGIPF_ERRORDETAILS	Detalles del error	VARCHAR (2000)
COGIPF_REPORTNAME	El nombre del informe que se ha visualizado	VARCHAR (512)
COGIPF_PACKAGE	El paquete con el que se asocia el informe	VARCHAR (1024)
COGIPF_REPORTFORMAT	El formato del informe. Para obtener más información, consulte: "Formatos de informe" en la página 363.	VARCHAR (255)
COGIPF_MODEL	El modelo con el que se asocia el informe	VARCHAR (512)

Apéndice G. Configuración de valores avanzados

Puede configurar valores avanzados globalmente, para la totalidad del entorno de IBM Cognos, o de forma individual para un asignador o servicio de asignador. La práctica recomendada consiste en especificar los valores de forma global y después, en caso necesario, personalizarlos para asignadores o servicios de asignador específicos.

Los valores avanzados están asociados con la entrada de configuración de IBM Cognos Administration. Los valores se agrupan en las categorías de reemplazo de registro, ajuste, entorno y administrador.

Si se especifican los valores avanzados globalmente para la entrada de configuración, todas las entradas contenidas adquieren los valores que se especifiquen, a menos que la propiedad de la entrada contenida esté definida para que se reemplacen los valores globales. Puede reemplazar los valores globales y, en su lugar, indicar valores personalizados para entradas específicas; no obstante, esto podría crear una sobrecarga en la administración.

Para poder cambiar los valores avanzados, debe disponer de los permisos de acceso siguientes para la entrada de configuración y las entradas hijo afectadas:

- Permisos de lectura y escritura para la entrada que quiere actualizar
- Permisos de visita para el padre de la entrada que quiere actualizar

Configuración de valores avanzados globalmente

Puede configurar valores avanzados globalmente para la totalidad del entorno de IBM Cognos.

Acerca de esta tarea

Todas las entradas contenidas adquieren los valores que se especifican. Puede reemplazar los valores globales especificando valores personalizados en el nivel del asignador o del servicio de asignador.

Si la entrada de configuración contiene entradas hijo con valores que reemplazan a los valores globales, se pueden restablecer los valores personalizados de las entradas hijo para que utilicen los valores predeterminados.

Puede configurar valores avanzados globalmente para las categorías de reemplazo de registro, ajuste, entorno y administrador.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios**.
2. En la barra de herramientas de la página **Configuración**, pulse **Establecer propiedades – Configuración** .
3. Pulse la pestaña **Valores**.
4. Para filtrar la lista de valores, seleccione una categoría de la lista **Categoría**.

5. Seleccione el parámetro necesario en la lista y especifique un valor de una de las formas siguientes.
 - Especifique un valor
 - Seleccione un valor en una lista
 - Pulse **Editar** y añada un nombre de parámetro y valor
6. Opcional: Para restablecer las entradas hijo para utilizar los valores predeterminados, seleccione la casilla de verificación **Suprimir los valores de configuración de todas las entradas hijo**.
7. Pulse **Aceptar**.
8. Para aplicar los valores, detenga y reinicie los servicios de IBM Cognos. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Configuración de valores avanzados para asignadores específicos

Puede configurar valores avanzados para un asignador específico. De esta forma podrá especificar valores de configuración personalizados para el asignador que reemplazarán a los valores de configuración globales en el entorno de IBM Cognos.

Acerca de esta tarea

Si el asignador contiene entradas hijo con valores que reemplazan los valores globales, puede restablecer los valores personalizados en las entradas hijo para utilizar los valores predeterminados

Puede especificar valores avanzados en el nivel de asignador para las categorías siguientes: registro, ajuste y entorno.

Importante: Algunos valores avanzados asociados con la categoría de entorno no se pueden especificar en el nivel del asignador. Deben especificarse globalmente, o para un servicio de asignador.

Para obtener más información, consulte: “Configuración de valores avanzados globalmente” en la página 513 y “Configuración de valores avanzados para servicios específicos” en la página 515

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios**.
2. Busque el asignador y, en la columna **Acciones**, pulse el icono **Establecer propiedades** .
3. Pulse la pestaña **Valores**.
4. Para filtrar la lista de valores, seleccione una categoría de la lista **Categoría**.
5. Seleccione un parámetro de configuración en la lista y especifique un valor de una de las formas siguientes:
 - Especifique un valor
 - Seleccione un valor en una lista
 - Pulsando **Editar**, seleccione la casilla de verificación **Reemplazar los valores adquiridos de la entrada padre** y añada el nombre y valor de parámetro
6. Opcional: Para restablecer los valores personalizados en las entradas hijo para utilizar los valores predeterminados, seleccione la casilla de verificación **Suprimir los valores de configuración de todas las entradas hijo**.

7. Pulse **Aceptar**.
8. Para aplicar los valores, detenga y reinicie los servicios de IBM Cognos. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Configuración de valores avanzados para servicios específicos

Puede configurar valores avanzados para servicios de asignador específicos, como AgentService. De esta forma podrá especificar valores de configuración personalizados para el servicio que reemplazarán a los valores de configuración globales en el entorno de IBM Cognos.

Acerca de esta tarea

Puede establecer valores avanzados para un servicio de asignador en las categorías siguientes: registro, ajuste y entorno.

Para obtener más información, consulte: “Configuración de valores avanzados globalmente” en la página 513 y “Configuración de valores avanzados para asignadores específicos” en la página 514.

Procedimiento

1. En **IBM Cognos Administration**, en la pestaña **Configuración**, pulse **Asignadores y servicios**.
2. Pulse el nombre del asignador.
3. En la lista de servicios de asignador, busque el servicio requerido y, en la columna **Acciones**, pulse el icono **Establecer propiedades** .
4. Pulse la pestaña **Valores**. Puede filtrar la lista de valores por **Categoría**. Las opciones de categoría son: **Todos**, **Entorno**, **Registro** y **Ajuste**.
5. Defina el valor en una de las siguientes maneras:
 - Busque el valor que desea personalizar y escriba o seleccione un valor para configurar en el espacio que se proporciona.
 - Si el valor no aparece para **Valores avanzados**, haga clic en el enlace asociado **Editar**. En la página que se muestra, seleccione **Anular los valores adquiridos de la casilla de verificación de entrada principal** y añada el nombre y valor del valor.
6. Pulse **Aceptar**.
7. Para aplicar los valores, detenga y reinicie los servicios de IBM Cognos. Para obtener más información, consulte *IBM Cognos Analytics Guía de instalación y configuración*.

Referencia de valores avanzados

En esta sección se describen los valores avanzados para el servicio de IBM Cognos.

Valores avanzados del servicio de agente

En esta sección se describen los valores avanzados para el servicio de agente.

asv.preview.maxRows

Especifica el número máximo de filas para visualizar en una solicitud **Vista previa de todo** de IBM Cognos Event Studio.

Tipo de datos:

Entero

Valor predeterminado:

500

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

housekeeping.run.startup

Especifica si los objetos de estado de tareas ejecutadas previamente se eliminan del almacén de contenido durante el inicio. Si el valor es false, la limpieza sólo se realiza en el intervalo especificado por housekeeping.run.interval.

Tipo de datos:

Booleano

Valor predeterminado:

false

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

housekeeping.run.interval

Especifica el intervalo, en horas, cuando tendrán lugar las operaciones de mantenimiento para agentes ejecutados anteriormente. Este valor sólo se utiliza si housekeeping.run.startup está establecido en false.

Tipo de datos:

Entero

Valor predeterminado:

12

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

primary.wait.asv

Especifica el tiempo, en segundos, para el umbral de espera principal para el servicio de agente. Este valor se utiliza si no se establece un valor en la solicitud.

Tipo de datos:

Entero

Valor predeterminado:

120

secondary.threshold

Especifica el tiempo, en segundos, para el umbral de espera secundario para solicitudes asíncronas. El servicio de agente sólo utiliza este servicio al ejecutar sus tareas (rss, report, sql y webservice).

Tipo de datos:

Entero

Valor predeterminado:

30

Valores avanzados del servicio de Content Manager

En esta sección se describen los valores avanzados para el servicio de Content Manager.

CM.CMSync_CheckActiveTime

Especifica el periodo en el que un Content Manager activo entra en modo en espera si otro Content Manager pasa a estar activo.

Tipo de datos:

Entero

Valor predeterminado:

10000

CM.CMSync_NegotiationTime

Especifica el tiempo de elección de migración tras error en milisegundos.

El tiempo de elección es el período de espera después del error de una instancia de Content Manager, antes de que otras instancias de Content Manager intenten convertirse en el servicio activo. Este período garantiza que otra instancia de servicio de Content Manager no se active a menos que el Content Manager original esté realmente fallando.

Tipo de datos:

Entero

Valor predeterminado:

2000

CM.CMSync_NegotiationTimeForStartUp

Especifica el tiempo de elección de inicio en milisegundos, tras un cierre del sistema.

Este tiempo de elección es el periodo de espera durante el cual está previsto que el Content Manager predeterminado se inicie antes de que otras instancias de Content Manager en espera intenten iniciarse. Esto garantiza que el Content Manager preferido se inicie después de un cierre del sistema.

Tipo de datos:

Entero

Valor predeterminado:

60000

CM.CMSync_PingTimeout

Especifica el tiempo máximo en milisegundos dentro del cual un Content Manager ocupado debería enviar una respuesta.

Tras el período de tiempo de espera, comienza el proceso de elección para seleccionar un nuevo Content Manager de las instancias de Content Manager en espera, si existen.

Tipo de datos:

Entero

Valor predeterminado:

120000

CM.CMSync_ShortNetworkInterruptionTime

Especifica una breve interrupción de red, en milisegundos, dentro de la cual no se produce la migración tras error.

Tipo de datos:

Entero

Valor predeterminado:

3000

CM.DbConnectPoolMax

Especifica el número máximo de conexiones de base de datos simultáneas permitido para el almacén de contenido.

Los valores válidos son -1, o de 5 a 2147483647, o el valor de base de datos (el valor que sea inferior).

Un valor de -1 significa que las conexiones son ilimitadas.

Este valor se aplica únicamente a los valores de agrupación de conexiones de Content Manager. Si hay otros servicios que accedan al mismo almacén de contenido, es posible que haya más conexiones de base de datos simultáneas que las especificadas en este parámetro.

Tipo de datos:

Entero

Valor predeterminado:

-1

CM.DbConnectPoolTimeout

Especifica el tiempo máximo, en milisegundos, que espera un subproceso a que esté disponible una conexión de la agrupación.

Un valor de 0 especifica que los subprocesos nunca esperan una conexión si no hay una disponible inmediatamente. Un valor de -1 significa que el tiempo de espera es ilimitado.

Tipo de datos:

Entero

Valor predeterminado:

-1

CM.DbConnectPoolIdleTime

Especifica el tiempo mínimo en milisegundos que una conexión permanece inactiva en la agrupación.

Este valor solo es válido si el valor de DbConnectPoolCleanupPeriod es positivo.

Un valor de 0 o -1 especifica que las conexiones inactivas se cierran cuando Content Manager se reinicia.

Tipo de datos:

Entero

Valor predeterminado:

300000

CM.DbConnectPoolCleanUpPeriod

Especifica el tiempo, en milisegundos, entre llamadas de un subproceso de limpieza que cierra las conexiones inactivas de la agrupación que superan el valor de DbConnectPoolIdleTime.

Un valor de 0 o -1 especifica ningún subproceso de limpieza.

Tipo de datos:

Entero

Valor predeterminado:

300000

CM.DeploymentIncludeConfiguration

Especifica si los objetos de configuración deben importarse desde el archivo de almacén de contenido completo durante el despliegue.

Estos objetos incluyen asignadores y las carpetas de configuración que se utilizan para agrupar los asignadores. Por ejemplo, puede que desee importar la configuración porque tiene una serie de valores avanzados para sus servicios que desea llevar a partir del entorno de origen.

Para obtener los mejores resultados, no es recomendable importar los objetos de configuración. Configure los asignadores en el entorno de destino antes de importar los datos de un entorno de origen.

Tipo de datos:

Booleano

Valor predeterminado:

false

CM.DeploymentSkipUserReportOutput

Si este valor se establece en true, las salidas de informe y sus objetos hijo (gráfico y página) de las cuentas de usuario no se exportan ni importan. Utilice este valor para reducir el tamaño de los archivos del almacén de contenido y mejorar el rendimiento de despliegue.

Tipo de datos:

Booleano

Valor predeterminado:

false

CM.DeploymentDetailErrorsOnly

Si se establece en true, este valor genera sólo información de resumen y errores para despliegues de paquete y carpeta. De forma predeterminada, Content Manager genera detalles completos para historiales de despliegue de paquete y carpeta. Utilice este valor para reducir el tamaño de los archivos del almacén de contenido y mejorar el rendimiento de despliegue.

Tipo de datos:

Booleano

Valor predeterminado:

false

CM.DeploymentDetailEntireContent

Si se establece en true, genera detalles completos para un historial de despliegue de almacén de contenido completo. De forma predeterminada, Content Manager genera sólo información de resumen y errores para un despliegue de almacén de contenido completo.

Tipo de datos:

Booleano

Valor predeterminado:

false

CM.DeploymentUpdateScheduleCredential

Si se establece en true y se utiliza la opción **takeOwnership** durante la importación de un archivo de despliegue, la propiedad de credencial de todos los objetos de planificación importados se cambia para hacer referencia a la credencial contenida en la cuenta que se utiliza para importar el despliegue.

Tipo de datos:

Booleano

Valor predeterminado:

false

CM.OutPutLocation

Especifica la ubicación del sistema de archivos donde se guardarán las salidas de informe generadas.

Cada archivo de salida también tiene un descriptor de salida del mismo nombre, con extensión XML.

Las versiones antiguas del informe no se suprimen cuando se guarda una nueva. Se debe gestionar el contenido del directorio de salida para guardar sólo las versiones que se deseen.

Las salidas de informe siempre se escriben en el directorio configurado para cada instancia del servicio de entrega. Para evitar que se escriban salidas de informes en varias ubicaciones, asegúrese de que se está ejecutando solamente una instancia del servicio de entrega o bien configure todas las instancias de servicio para que utilicen una ubicación de archivo de red compartida. Todos los asignadores que ejecuten el servicio de entrega deben tener acceso al sistema de archivos o estar inhabilitados en todos los sistemas en los que no está previsto que se guarde la salida de informe.

Tipo de datos:

Cadena

Valor predeterminado:

ninguno

CM.OutputScript

Especifica la ubicación y el nombre de un script externo que se ejecutará cada vez que se guarde una salida de informe.

Los parámetros de script son la salida de informe y los nombres de archivo de descriptor de salida.

Tipo de datos:

Cadena

Valor predeterminado:
ninguno

CM.OutputByBurstKey

Especifica si las salidas deben organizarse en el sistema de archivos según la clave de separación.

Si se establece en true, la salida se coloca en un subdirectorio del mismo nombre que la clave de separación.

Tipo de datos:
Booleano

Valor predeterminado:
false

CM.SecurityQueryRequiresRead

Controla si Content Manager fuerza un filtro de permiso de lectura para resultados de consultas de espacios de nombres externos.

Cuando esta opción está habilitada, Content Manager puede evitar el examen de espacios de nombres externos, si la política de espacios de nombres externos también se ha actualizado para negar el permiso de lectura a usuarios o grupos.

Tipo de datos:
Booleano

Valor predeterminado:
false

CM.SortCollation

El nombre de la ordenación específica de base de datos utilizada para la ordenación en algunas bases de datos, como Oracle y SQL Server.

Si se deja en blanco, la base de datos utiliza su ordenación predeterminada.

Por ejemplo, en Oracle, si especifica la secuencia de ordenación como binario en el nivel de base de datos, debe proporcionar el mismo valor de secuencia de ordenación en la cadena de conexión.

A continuación se muestra una cadena de conexión de ejemplo para una base de datos Oracle que utiliza la base de datos de ejemplo gosl: ORACLE@GOSL0703@GOSL/GOSL0703@COLSEQ=Binary

Para obtener más información sobre las ordenaciones soportadas, consulte la documentación de Oracle y de SQL Server.

El valor CM.SortCollation no tiene ningún efecto en los administradores de contenido que se ejecutan en las bases de datos Sybase o IBM Db2.

Tipo de datos:
Cadena

Valor predeterminado:
ninguno

CM.UpdateInitialContentNamesAfterImport

Añade nombres de objetos localizados para los idiomas no compatibles previamente.

En algunos entornos locales, si desea actualizar a IBM Cognos Analytics desde IBM Cognos Business Intelligence versión 10.1.1 o anterior y planea importar un almacén de contenidos que se creó con una versión anterior de Cognos BI, utilice este valor avanzado para asegurarse que todos los nombres de objetos se han localizado correctamente.

Los siguientes idiomas se ven afectados: catalán, danés, griego, kazajo, noruego, eslovaco, esloveno y tailandés. El soporte para estos idiomas se ha añadido en las versiones 10.1.1 y 10.2 de IBM Cognos Business Intelligence. Si su almacén de contenidos se creó con una versión anterior, y el valor `CM.UpdateInitialContentNamesAfterImport` no se especificó antes de importar el almacén de contenidos, algunos nombres de objetos pueden aparecer en inglés y no en el idioma especificado.

Especifique los idiomas afectados, separando cada uno con una coma. Por ejemplo, para los idiomas de contenido esloveno y croata, escriba: `sl,hr`

Nota: Elimine este valor avanzado cuando ya no se necesita el soporte para el almacén de contenido anterior debido a que hay un impacto de rendimiento asociado con este valor.

Tipo de datos:

Cadena

Valor predeterminado:

ninguno

Valores comunes de configuración

En esta sección se describen los valores avanzados comunes a todos los servicios.

trustedSession.pool.max

Especifica el número máximo de sesiones de confianza que se pueden utilizar simultáneamente. Las sesiones de confianza utilizan un mecanismo de seguridad interno para cifrar las comunicaciones de los componentes internos.

Las sesiones se implementan como agrupación de recursos.

Tipo de datos:

Entero

Valor predeterminado:

100

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

axis.timeout

Especifica el umbral de espera principal, en segundos, para el servidor de eje interno. Es el tiempo que esperará el eje una respuesta a llamadas de servicio antes de exceder el tiempo de espera.

El eje es una herramienta de código abierto para convertir los objetos XML en objetos Java.

Tipo de datos:

Entero

Valor predeterminado:

0

COGADMIN.filterInteractiveActivitiesOfUnknownUsers

Especifica si las actividades en IBM Cognos Administration están ocultas cuando el usuario no tiene permiso para ver el usuario que realiza la actividad.

Tipo de datos:

Booleano

Valor predeterminado:

false

COGADMIN.restrictInteractiveActivitiesToSystemAdministrators

Especifica si las actividades interactivas de IBM Cognos Administration están restringidas a los administradores del sistema.

Si este valor se establece en true, la herramienta Actividades actuales proporcionará acceso de administrador que no es del sistema solamente a las actividades en segundo plano.

Tipo de datos:

Booleano

Valor predeterminado:

false

DISP.InteractiveProcessUseLimit

Fuerza al asignador para que deje de enviar solicitudes a un proceso de servidor de informes después del límite prescrito.

Por ejemplo, si se establece el límite en 500, fuerza que el asignador deje de enviar solicitudes a un proceso tras 500 solicitudes.

Tipo de datos:

Entero

Valor predeterminado:

0

DISP.BatchProcessUseLimit

Fuerza que el asignador deje de enviar solicitudes a un proceso de servidor de informes por lotes después del límite prescrito.

Tipo de datos:

Entero

Valor predeterminado:

0

VIEWER_CW_BACKWARDS_COMPATIBLE_DRILL

Especifica si la funcionalidad para ver los detalles heredada se utiliza en IBM Cognos Workspace.

De manera predeterminada, este valor no se especifica y se utiliza la funcionalidad actual para detallar más y detallar menos en Cognos Workspace.

Cuando este valor se establece en true, la funcionalidad para ver los detalles en Cognos Workspace presenta el comportamiento de la versión 10.2.0 y versiones anteriores.

Cuando este valor se establece en false, se utiliza la funcionalidad para ver los detalles actual de Cognos Workspace.

Especifique este valor en el nivel de configuración en su sistema. No lo establezca para servicios individuales.

Tipo de datos:

Booleano

Valor predeterminado:

false

Valores avanzados de Portal Services (servicio de presentación)

En esta sección se describen los valores avanzados para el servicio de presentación.

CPSMaxCacheSizePerPortlet

Especifica el número de fragmentos de marcación almacenados en la memoria caché de cada portlet, por página y usuario.

Por ejemplo, un valor de 5 con 1.000 usuarios, 10 páginas y 4 portlets por página puede generar un máximo de 200.000 entradas en la memoria caché (1000 x 10 x 4 x 5).

Los siguientes valores son válidos:

- -1 guarda un número ilimitado de marcaciones.
- 0 inhabilita la caché de marcación.
- 1 o un entero mayor que 1 limita el número de marcaciones al número especificado.

Tipo de datos:

Entero

Valor predeterminado:

-1

properties.config.cps.cache.timeToldleSeconds

Especifica el periodo de tiempo, en segundos, durante el cual se conservan los fragmentos de marcación de página en la memoria caché en un periodo de inactividad.

Si no se accede a la página durante ese tiempo, se suprime el contenido de la memoria caché.

Los datos en memoria caché guardados en disco se pueden cifrar si el valor de **¿Cifrar archivos temporales?** se ha establecido en **True** en la carpeta **Entorno** en IBM Cognos Configuration.

Tipo de datos:

Entero

Valor predeterminado:

1800 (30 minutos)

properties.config.cps.cache.timeToLiveSeconds

Especifica el periodo de tiempo, en segundos, durante el cual se conservan los fragmentos de marcación de página en la memoria caché.

Después del tiempo especificado, se suprime la marcación aunque la memoria caché todavía esté activa.

Los datos en memoria caché guardados en disco se pueden cifrar si el valor de **¿Cifrar archivos temporales?** se ha establecido en **True** en la carpeta **Entorno** en IBM Cognos Configuration.

Tipo de datos:

Entero

Valor predeterminado:

86400 (24 horas)

properties.config.cps.cache.checkExpiryIntervalSeconds

Especifica la frecuencia, en segundos, con la que el sistema busca fragmentos de marcación caducados en la memoria caché.

Los datos en memoria caché guardados en disco se pueden cifrar si el valor de **¿Cifrar archivos temporales?** se ha establecido en **True** en la carpeta **Entorno** en IBM Cognos Configuration.

Tipo de datos:

Entero

Valor predeterminado:

300 (5 minutos)

xts.tempdir

Especifica la ubicación de la carpeta en la unidad local donde se almacenan los fragmentos de marcación.

El valor puede ser cualquier ruta de la unidad local. Si no se especifica ningún valor, se utiliza el área de trabajo del servidor de aplicaciones predeterminado.

Tipo de datos:

Cadena

Valor predeterminado:

en blanco

CPSPropagatePassport

Especifica si el ID de pasaporte de IBM Cognos se transfiere como un parámetro de URL.

Cuando se establece en 0, este distintivo impide la transferencia del ID de pasaporte de IBM Cognos como parámetro de URL.

Cualquier valor distinto de cero permite la transferencia del ID de pasaporte.

Tipo de datos:

Valor predeterminado:

Ninguno

CPSPropagateTicket

Especifica si el ID de tiquet de IBM Cognos Configuration se transfiere como un parámetro de URL.

Cuando se establece en 0, este distintivo impide la transferencia del ID de tiquet de IBM Cognos Configuration como parámetro de URL.

Cualquier valor distinto de cero permite la transferencia del ID de tíquet.

Tipo de datos:

Valor predeterminado:

Ninguno.

CPSProtocolScheme

Reemplaza el esquema de protocolo utilizado al generar el punto final de Web Service Definition Language (WSDL) para Portal Services para Web Services Remote Portlets (WSRP) Producers.

Para generar WSDL para WSRP, Portal Services utiliza el esquema de protocolo especificado en el parámetro de pasarela de IBM Cognos Configuration. Cuando hay varias pasarelas y no todas se puedan configurar utilizando el mismo esquema de protocolo, como http o https, este parámetro reemplaza a todos los demás valores.

Los valores válidos son http y https

Tipo de datos:

Cadena

Valor predeterminado:

Ninguno

portal.showTenantInfoForAllUsers

Si tiene el valor True, los usuarios que no tienen permisos de administrador pueden ver la información de arrendatario.

Por ejemplo, en la página Establecer propiedades, se muestra el arrendatario de un objeto. En las listas de objetos, los usuarios pueden ver el campo de arrendatario.

Los usuarios no pueden cambiar el arrendamiento ni suplantar a arrendatarios.

Tipo de datos:

Booleano

Valor predeterminado:

Falso

Valores avanzados del servicio de entrega

En esta sección se describen los valores avanzados para el servicio de entrega.

emf.archive.filetimestamp.enabled

Fuerza la marca de hora en archivos archivados.

Tipo de datos:

Booleano

Valor predeterminado:

true

max.smtp.connections

Especifica el número máximo de conexiones SMTP.

Este valor limita el número de subprocesos que el servicio de entrega puede generar para enviar mensajes.

Los valores válidos son enteros que sean mayor o igual que 1.

Tipo de datos:

Entero

Valor predeterminado:

10

Consejo: Debe reiniciar el servicio para que este valor surta efecto.

primary.wait.dls

Especifica el umbral de espera principal, en segundos, para el servicio de entrega.

Este valor se utiliza si no se establece un valor en una solicitud.

Si el valor es menor que 0, se ignora. Si el valor es 0, el cliente esperará indefinidamente.

Tipo de datos:

Entero

Valor predeterminado:

120

smtp.reconnection.delay

Especifica el intervalo de tiempo, en segundos, antes de que se realice un intento de volver a conectar con un servidor SMTP.

Tipo de datos:**Valor predeterminado:**

10

Consejo: Debe reiniciar el servicio para que este valor surta efecto.

enable.tide.metrics.smtpqueue

Habilita la recopilación y visualización de las métricas para el servicio de entrega de IBM Cognos Administration.

Se realiza un seguimiento de las métricas siguientes:

- Marca de agua máxima de tiempo en cola
- Marca de agua mínima de tiempo en cola
- Tiempo en cola
- Número de solicitudes de cola
- Marca de agua máxima de longitud de la cola
- Marca de agua mínima de longitud de la cola

Tipo de datos:

Booleano

Valor predeterminado:

false

dls.connection.pool.force.clean

Fuerza la limpieza de las conexiones de transporte SMTP. Esto evita tener que llamar al método close(), lo que hace que tengan que esperar los sockets. En su lugar, las variables simplemente se establecen en un valor nulo.

Tipo de datos:

Booleano

Valor predeterminado:

false

Establézcalo en true para forzar una limpieza.

Consejo: Después de aplicar los cambios, establézcalo en true para probar el valor.

dls.connection.pool.used

Especifica si se utiliza la agrupación de conexiones del transporte DLS.

Tipo de datos:

Booleano

Valor predeterminado:

true

Establézcalo en true para utilizar la agrupación de conexiones.

Consejo: Establézcalo en false para que no se utilice la agrupación de conexiones. El resultado es cada correo electrónico hace que DLS abra una conexión de transporte SMTP nueva con el servidor de correo electrónico. Esto puede resultar útil si se descartan los sockets del servidor de correo electrónico después de cada uso.

Valores avanzados del servicio de asignador

En esta sección se describen los valores avanzados para el asignador.

DISP.InteractiveProcessUseLimit

Fuerza al asignador para que deje de enviar solicitudes a un proceso de servidor de informes después del límite prescrito.

Por ejemplo, si se establece el límite en 500, fuerza que el asignador deje de enviar solicitudes a un proceso tras 500 solicitudes.

Tipo de datos:

Entero

Valor predeterminado:

0

DISP.BatchProcessUseLimit

Fuerza que el asignador deje de enviar solicitudes a un proceso de servidor de informes por lotes después del límite prescrito.

Tipo de datos:**Valor predeterminado:**

0

Valores avanzados del servicio de gestión de eventos

En esta sección se describen los valores avanzados para el servicio de gestión de eventos.

run.task.max.thread

Especifica el número máximo de subprocesos que están asignados para transferir solicitudes planificadas a una cola de retención.

Cuando el servicio de gestión de eventos ejecuta una tarea, la tarea se coloca en una cola, esperando los recursos para ejecutarla. Se crea un subproceso para gestionar la solicitud para el subproceso de planificador del servicio de gestión de eventos.

Valor predeterminado: 20

Tipo de datos:

Entero

Valor predeterminado:

20

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

authenticate_when_scheduled

Determina si se comprueban los permisos de una cabecera de solicitud runAt para execute para el objeto que se ejecutará.

Si una comprobación es necesaria y falla, se envía una excepción.

Si se establece, esta comprobación también falla si el usuario tiene los permisos, pero las credenciales necesarias para ejecutar la tarea a la hora planificada no se pueden recuperar.

Tipo de datos:

Booleano

Valor predeterminado:

false

enable.tide.metrics.jobqueue

Habilita la recopilación y visualización de métricas específicas para el servicio de gestión de eventos en IBM Cognos Administration.

Se incluyen las métricas siguientes:

- Marca de agua máxima de tiempo en cola
- Marca de agua mínima de tiempo en cola
- Tiempo en cola
- Número de solicitudes de cola
- Marca de agua máxima de longitud de la cola
- Marca de agua mínima de longitud de la cola

Tipo de datos:

Booleano

Valor predeterminado:

false

ems.action.requires.permissions.check

Fuerza la comprobación de permisos de objeto.

Si esta opción está habilitada, un llamador con la función de usuario canUseMonitorActivityTool también debe cumplir una de las condiciones siguientes antes de llamar al método runSpecification() con respecto al servicio de gestión de eventos:

- La cuenta del llamador debe coincidir con la credencial de cuenta que se utiliza para planificar el evento.
- El llamador debe tener permisos de visita y ejecución en el objeto de destino.

Tipo de datos:

Booleano

Valor predeterminado:

false

emf.schedule.validation.enabled

Valida las propiedades de planificación tales como la fecha de inicio, la fecha de finalización, los tipos de datos y las credenciales de cuenta de usuario cuando Content Manager procesa las solicitudes para añadir o actualizar planificaciones. Inhabilita las planificaciones no válidas.

Los detalles de las planificaciones inhabilitadas se registran en los archivos de registro.

Tipo de datos:

Booleano

Valor predeterminado:

false

emf.dls.attachment.timestamp.enabled

Si se establece en true, los archivos adjuntos de correo electrónico tienen nombres de informes con una indicación de fecha y hora. El formato predeterminado para la indicación de fecha y hora es yyyy.MM.dd, siendo yyyy el año expresado con cuatro dígitos, MM el mes expresado con dos dígitos y dd el día expresado con dos dígitos.

Por ejemplo, si adjunta el informe Resultado anual en un mensaje, el mensaje de correo electrónico que se envía tiene un archivo adjunto que se llama Resultado anual - 2014.07.15.pdf.

Establezca esta propiedad avanzada si necesita añadir una indicación de fecha y hora a los archivos adjuntos de informe en los mensajes de correo electrónico. También puede optar por cambiar el formato de fecha y hora predeterminado; para ello, establezca la propiedad avanzada emf.dls.attachment.timestamp.format.

Tipo de datos:

Booleano

Valor predeterminado:

false

emf.dls.attachment.timestamp.format

Especifica el formato de fecha y hora que se añade a los nombres de los informes en los archivos adjuntos de correo electrónico cuando la propiedad avanzada emf.dls.attachment.timestamp.enabled se ha establecido en true.

Los valores posibles son diversos formatos de fecha. Por ejemplo, 15.07.2014 tiene el formato dd.MM.yyyy y 140704120856-0700 tiene el formato yyMMddHHmmssZ. Para obtener más información sobre SimpleDateFormat, consulte el sitio web de Oracle. No use una barra inclinada ni caracteres especiales en el formato.

Tipo de datos:

Cadena

Valor predeterminado:

aaaa-MM-dd

emf.preview.max.items

Utilice este valor para aumentar el número máximo de eventos que se pueden mostrar en la lista de eventos.

El aumento de este valor puede afectar al rendimiento del sistema que necesitará leer más datos y representar los datos en la interfaz de usuario.

Tipo de datos:

Entero

Valor predeterminado:

50

Valores avanzados del servicio de trabajos

En esta sección se describen los valores avanzados para el servicio de trabajos.

primary.wait.js

Especifica el tiempo, en segundos, para el umbral de espera principal para el servicio de trabajos.

Este valor se utiliza si no se establece un valor en la solicitud.

Tipo de datos:

Entero

Valor predeterminado:

120

Valores avanzados del Metrics Manager Service

En esta sección se describen los valores avanzados para el Metrics Manager Service.

initialConnections

Especifica el número de conexiones para crear cuando la agrupación de conexiones está inicializada.

Tipo de datos:

Entero

Valor predeterminado:

5

Consejo: Debe reiniciar el servicio para que estos valores surtan efecto.

incrementConnections

Especifica el número de conexiones para aumentar cuando la agrupación de conexiones debe ser mayor.

Tipo de datos:

Entero

Valor predeterminado:

5

Consejo: Debe reiniciar el servicio para que estos valores surtan efecto.

maximumConnections

Especifica el número máximo de conexiones que esta agrupación puede utilizar.

Tipo de datos:

Entero

Valor predeterminado:

200

Consejo: Debe reiniciar el servicio para que estos valores surtan efecto.

Valores avanzados del servicio de control

En esta sección se describen los valores avanzados para el servicio de control.

enable.session.affinity

Indica si la afinidad de sesiones está habilitada.

Este valor se utiliza junto con el valor avanzado `session.affinity.services`.

Tipo de datos:

Booleano

Valor predeterminado:

false

event.check.active

Especifica si la comprobación de consistencia está activa.

Los valores posibles: 1 para true, 0 (o cualquier otro) para false

Tipo de datos:

Entero

Valor predeterminado:

0

event.check.interval

Especifica el intervalo, en minutos, cuando se efectúa una comprobación de consistencia para asegurarse de que el registro de servicio de control de eventos coincida con el de Content Store.

Un subproceso de comprobador de consistencia de eventos borra todas las discrepancias.

Tipo de datos:

Entero

Valor predeterminado:

10

event.finished.check.active

Habilita o inhabilita el proceso de limpieza masivo de tareas finalizadas en tablas NC. El proceso utiliza el script `BulkFinishedTaskCleanerThread`. El script lo inicia el servicio de supervisión cuando el servicio se inicia como parte del inicio de servicio de Cognos.

Cuando el sistema detecta que esta propiedad está habilitada, el script de limpieza se carga desde BulkCleanStmtsObjectFactory. El script depende de la base de datos y se ejecuta en una única transacción para suprimir los registros finalizados que cumplen los criterios de eliminación.

Tipo de datos:

Booleano

Valor predeterminado:

true

event.finished.check.interval

Especifica el intervalo, en segundos, en que el proceso de limpieza masivo busca tareas finalizadas en las tablas NC. Las tareas finalizadas más de 24 horas atrás son candidatas para esa limpieza masiva.

El valor predeterminado es 3600 segundos (1 hora), pero lo ideal son 86400 segundos (24 horas).

Tipo de datos:

Entero

Valor predeterminado:

3600

event.finished.check.threshold

Define el número máximo de tareas finalizadas en las tablas NC que se han seleccionado para su eliminación.

Tipo de datos:

Entero

Valor predeterminado:

10

primary.wait.ms

Especifica el umbral de espera principal, en segundos, para el servicio de control.

Este valor se utiliza si no se establece un valor en la solicitud.

Tipo de datos:

Entero

Valor predeterminado:

120

session.affinity.services

Si enable.session.affinity se ha establecido en true, este valor especifica los servicios para configurar para afinidad de sesiones.

En un escenario N/N-1, este valor está soportado sólo por los siguientes servicios de IBM Cognos Planning: planningAdministrationConsoleService, planningDataService, planningRuntimeService y planningTaskService. De lo contrario, en un entorno homogéneo distribuido, este valor está soportado por todos los servicios.

Para especificar el/los servicio(s), utilice el parámetro serviceName obligatorio. Para configurar varios servicios, separe cada uno de ellos mediante un punto y coma (;). A continuación se muestran dos ejemplos:

- serviceName=planningTaskService

- `serviceName=planningTaskService;serviceName=planningDataService`

Dos parámetros opcionales proporcionan opciones de configuración más específicas:

- `serverGroup`: Especifica el nombre del grupo de servidores.
- `numThreads`: Especifica el número máximo de tareas simultáneas permitidas. El valor predeterminado es 2.

Los parámetros deben estar separados por una coma (.). Por ejemplo:

`serviceName=planningTaskService,serverGroup=mygroup,numThreads=4`

Tipo de datos:

Cadena

Valor predeterminado:

Ninguno

sds.instance.interval

Especifica el intervalo de actualización, en segundos, para que las instancias de servicio registren que están en ejecución.

El servicio de control utiliza este mecanismo para determinar que otros servicios de control estén activos. Si un servicio de control falla, otro servicio de control puede optar por la limpieza en nombre del servicio que ha fallado, incluida la actualización del historial de tareas que han fallado.

Los servicios pueden optar por limpieza en nombre de otro servicio, si el servicio no ha actualizado su registro dentro de un límite de tiempo razonable. Actualmente dicho límite es dos veces el valor de `sds.instance.interval`.

Tipo de datos:

Entero

Valor predeterminado:

30

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

enable.tide.metrics.taskqueue

Habilita la recopilación y visualización de métricas específicas para el servicio de supervisión de IBM Cognos Administration.

Se incluyen las métricas siguientes:

- Marca de agua máxima de tiempo en cola
- Marca de agua mínima de tiempo en cola
- Tiempo en cola
- Número de solicitudes de cola
- Marca de agua máxima de longitud de la cola
- Marca de agua mínima de longitud de la cola

Tipo de datos:

Booleano

Valor predeterminado:

false

sdk.service.poll.interval

El intervalo de tiempo, en segundos, que espera el servicio de supervisor antes de volver a intentar una solicitud de aplicación cliente para un servicio de reconexión.

Tipo de datos:

Entero

Valor predeterminado:

30

advanced.history.write

Indica si se escriben historiales de final utilizando la agrupación de subprocesos avanzada (mejorada).

Si true, los historiales finales se escriben utilizando varios subprocesos. Si false, los historiales finales se escriben en un único subproceso.

Tipo de datos:

Booleano

Valor predeterminado:

true

advanced.parent.history.threads

El número de subprocesos de trabajo utilizados para crear objetos de historial raíz en el almacén de contenido.

Establezca advanced.history.write en true para habilitar este valor.

Tipo de datos:

Entero

Valor predeterminado:

2

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

advanced.child.history.threads

El número de subprocesos utilizados para crear objetos de historial hijo para los pasos en el almacén de contenido.

Establezca advanced.history.write en true para habilitar este valor.

Tipo de datos:

Entero

Valor predeterminado:

5

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

write.child.histories

Controla la escritura de objetos de historial hijo para el almacén de contenido.

Si true, se escriben los objetos de historial final para todas las tareas hijas. Si false, sólo se escribe el objeto de historial final para la tarea raíz y se descartan los

objetos de historial para las tareas hijas. Puede utilizar este valor para mejorar el rendimiento de tareas donde el tiempo de escritura del objeto de historial hijo es muy largo.

Tipo de datos:

Booleano

Valor predeterminado:

true

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

write.child.histories.during.failover

Especifica si los objetos de historial final de una tarea se escriben en el almacén de contenido durante una migración tras error.

Si el valor de `write.child.histories` se ha establecido en `true`, se escriben los objetos de historial hijo y los objetos de historial para tareas raíz.

Tipo de datos:

Booleano

Valor predeterminado:

true

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

connection.tracker.use

Realiza un seguimiento del uso de las conexiones.

Cuando `true`, los objetos proxy java se utilizan para realizar un seguimiento de las actividades de los objetos JDBC.

Tipo de datos:

Booleano

Valor predeterminado:

false

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

connection.write.maxwaittime

El periodo de tiempo máximo, en segundos, que un objeto espera para obtener una conexión de lectura-escritura de la agrupación de conexiones JDBC.

Tipo de datos:

Entero

Valor predeterminado:

10

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

connection.write.maxConnections

El número máximo de conexiones JDBC de lectura-escritura utilizadas en la agrupación de conexiones.

Todos los valores establecidos por debajo del mínimo no tienen ningún efecto y se aplica el valor mínimo especificado.

Valor mínimo: 5

Tipo de datos:

Entero

Valor predeterminado:

10

connection.read.maxwaittime

El periodo de tiempo máximo, en segundos, que un objeto espera para obtener una conexión de sólo lectura de la agrupación de conexiones JDBC.

Tipo de datos:

Entero

Valor predeterminado:

10

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

connection.read.maxConnections

El número máximo de conexiones JDBC de sólo lectura utilizadas en la agrupación de conexiones.

Todos los valores establecidos por debajo del mínimo no tienen ningún efecto y se aplica el valor mínimo especificado.

Tipo de datos:

Entero

Valor predeterminado:

8

Nota:

Debe reiniciar el servicio para que este valor surta efecto.

Valores avanzados de servicio de informes y servicio de informes por lotes

En esta sección se describen valores avanzados para el servicio de informes y servicio de informes por lotes.

BDS.split.maxKeysPerChunk

Especifica el límite de clave máximo para el procesamiento de informes de separación. Establecer el límite clave le permite evitar cláusulas SQL complejas cuando se establece el valor RSVP.BURST_DISTRIBUTION en true. El valor de 0 no establece ningún límite en este parámetro.

Tipo de datos:

Entero positivo

Valor predeterminado:

1000

EnableChartTransparencyle

Especifica si los gráficos utilizan Internet Explorer para mostrar filtros para habilitar la transparencia.

Tipo de datos:

Booleano

Valor predeterminado:

true

HyperlinkButtonNewWindow

Especifica que cuando se pulse un botón de hiperenlace, se cree una nueva ventana.

Tipo de datos:

Booleano

Valor predeterminado:

false

HyperlinkMultipleToolbars

Especifica que las barras de herramientas duplicadas en los informes HTML están permitidas. Establezca como false para eliminar la aparición de barras duplicadas.

Tipo de datos:

Booleano

Valor predeterminado:

true

RSVP.ATTACHMENTENCODING.BASE64EXTENDED

Especifica si se utiliza la codificación base64 al generar un resultado de un informe en formato MHT o XWLA.

En algunos casos, si las aplicaciones personalizadas especifican el formato de salida MHT o XLWA para informes, problemas con caracteres al final de la línea utilizados en el resultado XML pueden evitar que las aplicaciones abran el informe.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.BURST_DISTRIBUTION

Especifica si los informes de separación se ejecutan en paralelo o de forma secuencial. Si utiliza el valor predeterminado de false, los trabajos se ejecutan de forma secuencia, lo que tardará más tiempo.

Este valor corresponde a la opción de separación **Ejecutar en paralelo** en la interfaz de usuario. Este valor solo es válido cuando **Ejecutar en paralelo** se ha establecido en **Predeterminado**. Cuando se establece la opción **Ejecutar en paralelo** en **Inhabilitado** o **Habilitado**, se reemplaza este valor.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.BURST_QUERY_PREFETCH

Si establece esta opción en true, se habilita la captura previa de consultas. Como resultado, las salidas del informe de separación se producen mucho más rápido porque las consultas se ejecutan en paralelo con la presentación de informes. Este valor se aplica solo a los modelos relacionales del modo de consulta dinámica.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.CHARTS.ALTERNATECOLOURS

Especifica que cada una de las instancias del gráfico asigna colores en el orden de la paleta y que no intenta conservar el color de los elementos de una instancia del gráfico en otra.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.CONCURRENTQUERY.ENABLEDFORINTERACTIVEOUTPUT

Habilita la ejecución simultánea de consultas cuando el servicio de informes genera salidas interactivas.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.CONCURRENTQUERY.MAXNUMHELPERSPERREPORT

Especifica el número máximo de ayudantes de ejecución de consultas para cada informe. Este parámetro se utiliza para impedir que un único informe consuma todos los ayudantes de ejecución de consultas disponibles.

Tipo de datos:

Entero

Valor predeterminado:

1

RSVP.CONCURRENTQUERY.NUMHELPERSPERPROCESS

Habilita la ejecución simultánea de consultas y establece el número máximo de ayudantes de ejecución de consultas para cada proceso del servicio de informes o del servicio de informes por lotes. El valor predeterminado es 0, que indica que la ejecución simultánea de consultas está inhabilitada.

Tipo de datos:

Entero

Valor predeterminado:

0

RSVP.CSV.DELIMITER

Especifica el carácter delimitador de campo utilizado para la salida CSV.

Tipo de datos:

Cadena

Valor predeterminado:

TAB

RSVP.CSV.ENCODING

Especifica la codificación utilizada al generar la salida CSV.

Tipo de datos:

Cadena

Valor predeterminado:

utf-16le

RSVP.GROUP_METADATA_REQUESTS

Especifica si las solicitudes de metadatos se agrupan, cuando sea posible, para mejorar el rendimiento. Los usuarios pueden inhabilitar la agrupación de solicitudes de metadatos estableciendo este parámetro en false.

Tipo de datos:

Booleano

Valor predeterminado:

true

RSVP.CSV.MIMETYPE

Especifica el tipo MIME atribuido a la salida CSV.

Tipo de datos:

Cadena

Valor predeterminado:

application/vnd.ms-excel/

RSVP.CSV.QUALIFIER

Especifica el calificador de cadena utilizado para la salida CSV.

Tipo de datos:

Cadena

Valor predeterminado:

"

RSVP.CSV.REPEAT_XTAB_LABELS

Especifica si se deben repetir las etiquetas del borde en un informe de tabla de referencias cruzadas anidada.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.CSV.TERMINATOR

Especifica el terminador de línea utilizado para la salida CSV.

Tipo de datos:

Cadena

Valor predeterminado:

LF

RSVP.DRILL.clearAllMappedParamsOnMismatch

Especifica cómo se procesará la correlación de valores de parámetro aprobados durante una operación de acceso a detalles cuando no se pueden correlacionar algunos parámetros. La correlación de parámetros continúa (valor predeterminado) o se descarta la totalidad de la correlación y se solicitan valores al usuario.

Si establece esta propiedad en 1, si falla la correlación de cualquier parámetro, los demás parámetros correlacionados se eliminan de la tabla de correlaciones. Esto podría originar que se solicitaran otra vez todos los parámetros que faltan. Si establece esta propiedad en 0, si no se puede correlacionar algún parámetro mientras el componente de acceso a los detalles intenta correlacionar los parámetros, la correlación de los parámetros restantes no se verá afectada.

Tipo de datos:

Entero

Valor predeterminado:

0

RSVP.CSV.TRIMSPACES

Especifica que los espacios finales se eliminan de la salida CSV.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.DRILL.DynamicFilterUsesBusinessKey

Especifica el comportamiento del filtro de acceso a detalles dinámico. Establezca esta opción en 1 si desea obtener detalles para generar un filtro mediante la utilización de la clave de empresa de miembro en lugar del título de miembro predeterminado.

Tipo de datos:

Entero positivo

Valor predeterminado:

0

RSVP.DRILL.ExtractSourceContextFromRequest

Especifica si el servidor de informes intenta extraer los metadatos de los parámetros de la solicitud de acceso a los detalles desde el contexto de origen de la solicitud en lugar de emitir una nueva solicitud de metadatos. Este tipo de procesamiento mejora el rendimiento de una operación de acceso a los detalles. Está activado de forma predeterminada.

Si establece esta propiedad en 0, siempre se emiten solicitudes de metadatos.

Tipo de datos:

Entero

Valor predeterminado:

1

RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET

Habilita el soporte para hojas de trabajo de Microsoft Excel 2007 de gran tamaño. Si esta opción está establecida en true, se admiten las hojas de trabajo con un máximo de 1.048.576 filas.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE

Ajusta el tamaño de fragmentos de la memoria interna, en filas, que el servidor IBM Cognos Analytics genera antes de vaciarlo a un disco. Esta propiedad puede ser útil cuando hay problemas, como agotar la memoria al generar informes con el valor predeterminado. Es posible que sea necesario disminuir los valores para permitir que el informe se ejecute correctamente.

Tipo de datos:

Entero

Valor predeterminado:

45000 (aprox.)

RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS

Especifica el número de filas para el resultado antes de moverlo a una nueva hoja de trabajo.

Tipo de datos:

Entero

RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE

Especifica que, cuando se genera salida en formato Microsoft Excel 2007 y se han especificado saltos de página, las pestañas de la hoja de trabajo toman el nombre de los elementos de datos utilizados para el salto de página.

Nota: Esta propiedad no se aplica a Analysis Studio.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.EXCEL.XLS2007_PRINT_MEDIA

Especifica si el estilo No imprimir se aplica los resultados de informes en Excel 2007.

Tipo de datos:

Booleano

Valor predeterminado:

true

RSVP.FILE.EXTENSION.XLS

Especifica que se utilice XLS, en lugar de HTML, como extensión de archivo en los archivos adjuntos de correo electrónico con formato de salida XLS.

Tipo de datos:

Cadena

Valor predeterminado:

false

RSVP.PARAMETER_CACHE

Especifica si el almacenamiento de los parámetros en la memoria caché está inhabilitado o habilitado en el nivel de servidor. De forma predeterminada, el almacenamiento de los parámetros en la memoria caché está habilitado.

Cuando RSVP emite una solicitud `getParameters`, almacena los resultados en un objeto hijo bajo el objeto de informe en IBM Cognos Content Manager. Esto permite crear la memoria caché o actualizarla sin modificar la especificación de informe. Cuando RSVP necesita información de parámetros, utiliza la información guardada en la memoria caché de Content Manager. Si la memoria caché no contiene la información que necesita RSVP, RSVP invoca el motor de consultas directamente para obtener la información.

La caché se rellena realizan una solicitud SOAP `ReportService getParameters` SOAP al servicio de informes por lotes con la opción de ejecución `http://developer.cognos.com/ceba/constants/runOptionEnum#createParameterCache`. De este modo, si RSVP determina que falta la memoria caché o que está obsoleta, crear la memoria caché no afecta a la ejecución del informe, ya que la memoria caché se crea mediante una solicitud independiente. No obstante, dado que la solicitud la maneja el servicio de informes por lotes, se crea una entrada de historial que se puede ver en el historial de ejecuciones de un informe.

La creación de la memoria caché se activa cuando se crea o actualiza un informe desde Cognos Analytics Reporting, así como cuando se ejecuta un informe y RSVP determina que la memoria caché existente está obsoleta. RSVP utiliza la versión del módulo o el modelo raíz del informe para determinar si la memoria caché está obsoleta.

Tipo de datos:

Booleano

Valor predeterminado:

true

RSVP.PARAMETERS.LOG

Especifica si las opciones de ejecución de informes y los parámetros de solicitud deben registrarse en el sistema de registro.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.PARAMETERS.SAVE

Especifica que los valores de la solicitud de informe que haya especificado el usuario se guardan automáticamente.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.PRINT.POSTSCRIPT

Especifica qué interfaz utilizar para imprimir documentos en PDF desde un sistema operativo UNIX. Si esta opción está establecida en false, se utiliza la interfaz Adobe Acrobat PDF. En caso contrario, se utiliza la interfaz de postscript interna.

Tipo de datos:

Booleano

Valor predeterminado:

true

RSVP.PROMPT.CASTNUMERICSEARCHKEYTOSTRING

Especifica que los elementos de datos numéricos se convierten a un formato de cadena (varchar). Esto puede ser necesario si el origen de datos no convierte los elementos de datos numéricos en cadenas.

Tipo de datos:

Booleano

Valor predeterminado:

true

RSVP.PROMPT.EFFECTIVEPROMPTINFO.IGNORE

Inhabilita el envío del atributo effectivePromptInfo en las solicitudes de metadatos e inhabilita el movimiento de la información de solicitud desde el nivel inferior del atributo de título de un nivel hasta el propio nivel. Este es el comportamiento predeterminado.

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.PROMPT.RECONCILIATION

Especifica una configuración de todo el sistema que define la manera en que se procesan las consultas y los grupos de consultas.

Consulte el tema sobre el establecimiento de la prioridad de las consultas en la publicación *IBM Cognos Analytics Guía de administración y seguridad* para obtener una descripción de los valores posibles de este parámetro.

Tipo de datos:

Entero positivo o cadena

Valor predeterminado:

0 o COMPLETE

RSVP.PROMPT.RECONCILIATION.CHUNKSIZE

Especifica el tamaño del trozo cuando el valor de RSVP.PROMPT.RECONCILIATION es CHUNKED GROUPED o CHUNKED.

Tipo de datos:

Entero positivo

Valor predeterminado:

5

RSVP.PROMPTCACHE.LOCALE

Especifica el entorno local que se utilizará en lugar del entorno local especificado en el informe cada vez que se crean, actualizan o utilizan datos de la memoria caché de solicitud. Esto significa que se utiliza una única memoria caché de solicitud para cada informe independientemente del entorno local del usuario del informe.

Tipo de datos:

Cadena

RSVP.RENDER.PDF_FONT_SWITCHING

Especifica que cada carácter en una cadena se muestra en la fuente preferida. La fuente preferida es cualquier fuente que se enumera en una especificación de informe, seguida por las fuentes que se enumeran en el archivo (css) de la hoja de estilos en cascada de estilos globales. Cuando un carácter no está disponible en la fuente preferida, se muestra utilizando la siguiente fuente de la lista.

En las versiones anteriores, se utilizó una fuente solo si todos los caracteres en una cadena se pueden mostrar con esa fuente. A partir de IBM Cognos Business Intelligence 10.1, la fuente preferida se aplica en el nivel de caracteres. Como resultado, una palabra se puede mostrar con diferentes fuentes o algunas fuentes pueden ser más grandes, lo cual puede ocasionar ajuste de palabras.

Establezca el valor del parámetro en false para restaurar el comportamiento de selección de fuentes de las versiones anteriores.

Tipo de datos:

Booleano

Valor predeterminado:

true

RSVP.RENDER.ROUNDING

Especifica la regla de redondeo para el formato de los datos.

En las versiones anteriores, se utilizaba la regla `halfEven` al redondear los números. Esta regla suele utilizarse en contabilidad. Sin embargo, las normativas de precisión de algunas regiones requieren el uso de reglas de redondeo distintas; por ejemplo, la regla `halfUp`. A partir de la versión 10.2.0 de IBM Cognos Business Intelligence 10.2.0, puede elegir una regla de redondeo que se ajuste a las normativas de precisión de su organización.

Están disponibles las reglas de redondeo siguientes:

halfEven

Redondea al número más próximo, donde un valor equidistante se redondea al número par más cercano.

halfDown

Redondea al número más próximo, donde un valor equidistante se redondea al número inferior.

halfUp

Redondea al número más próximo, donde un valor equidistante se redondea al número superior.

ceiling

Redondea a un número más positivo.

floor Redondea a un número más negativo.

down Redondea hacia cero.

up Redondea alejándose de cero.

Tipo de datos:

Cadena

Valor predeterminado:

halfEven

RSVP.RENDER.VALIDATEURL

Especifica si la validación de IBM Cognos Application Firewall se impone en los URL que contiene una especificación de informe (incluidos URL en etiquetas de imagen, botones, hiperenlaces e imágenes de fondo en reglas CSS), o los especifica la opción de ejecución de cssURL del informe.

Cuando esta opción está establecida en true y se ha habilitado CAF, la validación se produce utilizando las siguientes reglas:

- Direcciones URL de nombre completo o absolutas:
protocol://host[:port]/path[?query]
Donde protocol es 'http' o 'https' y el host se valida con la lista de dominios válidos
- URL relativos a la raíz web de instalación de servidor:
/<install root>/.*
Donde <install root> es la ruta de archivo de pasarela, que se toma del URI de pasarela de IBM Cognos Configuration. Por ejemplo, /ibmcognos/ps/portal/images/action_delete.gif
- Alguno de los siguientes URL permitidos específicamente:
 - about:blank (no distingue mayúsculas y minúsculas)
 - JavaScript>window.close() (no distingue mayúsculas y minúsculas, con o sin punto y coma final)
 - JavaScript:parent.close() (no distingue mayúsculas y minúsculas, con o sin punto y coma final)
 - JavaScript:history.back() (no distingue mayúsculas y minúsculas, con o sin punto y coma final)
 - parent.cancelErrorPage() (no distingue mayúsculas y minúsculas, con o sin punto y coma final)
 - doCancel() (no distingue mayúsculas y minúsculas, con o sin punto y coma final)

Tipo de datos:

Booleano

Valor predeterminado:

false

RSVP.REPORTSPEC.LOG

Especifica si las especificaciones de informes deben registrarse en el sistema de registro.

Tipo de datos:

Booleano

Valor predeterminado:

false

Valores avanzados del servicio de repositorio

En esta sección se describen los valores avanzados para el servicio de repositorio.

repository.maxCacheDocSize

Tamaño máximo, en MB, de un informe individual que se puede almacenar en la memoria caché.

El valor debe ser un entero positivo (mayor que 0). Los informes con un tamaño mayor que el especificado no se almacenarán en la memoria caché y se recuperarán del repositorio.

Tipo de datos:

Entero

Valor predeterminado:

10

Valores avanzados de UDA

En esta sección se describen los valores avanzados para UDA (Universal Data Access).

Se reconocen los nombres de base de datos siguientes en los valores avanzados de UDA:

- SYBASE ASE
- IBM Db2
- INFORMIX
- MICROSOFT SQL SERVER
- NETEZZASQL
- NCLUSTER
- WEBSPHERE CLASSIC FEDERATION
- GREENPLUM
- INTERBASE
- INGRES
- SYBASE IQ
- INGRES_VECTORWISE
- PARACCEL
- POSTGRESQL
- TERADATA
- VERTICA DATABASE
- ORACLE
- SAP R3
- XML

Si el nombre de la base de datos no se reconoce, el valor no se lee. Si tiene otras bases de datos que no figuran en la lista o si los controladores ODBC devuelven un nombre de base de datos distinto, utilice el nombre de base de datos que se ha obtenido con el atributo SQL_DBMS_NAME de ODBC SQLGetInfo().

UDA.CALL_ODBC_SQLNUMRESULTCOLS

Recupera el número de columnas que está definido para una consulta.

Sintaxis:

UDA.CALL_ODBC_SQLNUMRESULTCOLS= "nombre de base de datos:valor booleano"

Tipo de datos:

Booleano

Valor predeterminado:

Verdadero

UDA.CONVERT_TIMESTAMP_LITERAL_TO_DATE_LITERAL

Puesto que la columna DATE de Oracle contiene las partes de fecha y hora, UDA informa del tipo de datos DATE de Oracle como TIMESTAMP.

El producto de IBM Cognos trata la columna DATE de Oracle como TIMESTAMP y genera un literal TIMESTAMP en el filtro.

Al comparar la columna DATE y el literal TIMESTAMP, la optimización de Oracle añade una función interna en la columna DATE para que la comparación sea compatible. Esto afecta al rendimiento de Oracle.

Esta entrada es específica de Oracle solamente. Cuando el valor booleano está establecido en TRUE, UDA convierte el literal TIMESTAMP con valor de hora 0 en un literal DATE. Oracle utiliza la exploración del índice en una columna DATE.

Sintaxis:

UDA.CONVERT_TIMESTAMP_LITERAL_TO_DATE_LITERAL= "nombre de base de datos:valor booleano"

Tipo de datos:

Booleano

Valor predeterminado:

Falso

UDA.INCLUDE_DST_TIMEZONE

Utilice este valor para incluir el horario de verano en la indicación de fecha y hora con el tipo de datos de huso horario.

Si este valor se establece en TRUE, el horario de verano se incluye en todas las operaciones que utilizan la indicación de fecha y hora de tipo de datos con el huso horario, como current_timestamp. Cuando este valor es FALSE, el horario de verano se excluye de estas operaciones.

Sintaxis:

UDA.INCLUDE_DST_TIMEZONE= valor booleano

Tipo de datos:

Booleano

Valor predeterminado:

Verdadero

UDA.NATIVE_SQL_IN_CTE

Controla cómo se procesa el SQL nativo en la expresión de tabla de comando de una cláusula WITH.

Cuando el valor booleano es KEEP, se envía a la base de datos subyacente el SQL nativo como parte de una cláusula WITH.

Cuando el valor booleano es PT, el SQL nativo se considera SQL nativo pass-through. El propio SQL se envía a la base de datos.

Cuando el valor booleano es DT, la cláusula WITH se elimina y todas las expresiones de tabla de comando se convierten en tablas derivadas.

Sintaxis:

UDA.NATIVE_SQL_IN_CTE= "nombre de base de datos:valor de cadena"

Tipo de datos:

Booleano

Valor predeterminado:

KEEP

UDA.PARSE_ANSI_NUMERIC_LITERAL

Especifica si el analizador de SQL de UDA lee el literal numérico con comas decimales (por ejemplo, 1,23), como un valor numérico exacto (por ejemplo, decimal) o como un valor aproximado (por ejemplo, doble).

Si este valor es TRUE, el analizador de SQL de UDA lee el literal numérico con comas decimales como un valor numérico exacto. Los valores con un número de dígitos inferior a 9 se leen como un entero con escala. Los valores con un número de dígitos comprendido entre 10 y 18 se leen como cuádruple con escala. Los valores con un número de dígitos comprendido entre 19 y 77 se leen como decimal (precisión, escala). Un valor con un número de dígitos superior a 77 se leen como doble. Si este valor es FALSE, el analizador de SQL de UDA lee el literal numérico con comas decimales como doble.

Sintaxis:

UDA.PARSE_ANSI_NUMERIC_LITERAL= valor booleano

Tipo de datos:

Booleano

Valor predeterminado:

Verdadero

UDA.PARSE_STRING_LITERAL_AS_VARCHAR

Este valor indica si una cadena literal se analiza como tipo de datos char o como tipo de datos varchar.

Si este valor es FALSE, el analizador de SQL de UDA lee el literal de cadena como char y el literal de cadena con el prefijo N como nchar. Si este valor es TRUE, el analizador de SQL de UDA lee el literal de cadena como varchar y el literal de cadena con el prefijo N como nvarchar.

Sintaxis:

UDA.PARSE_STRING_LITERAL_AS_VARCHAR= valor booleano

Tipo de datos:

Booleano

Valor predeterminado:

Falso

UDA.REPREPARE_QUERY_FOR_PARAMETER_VALUE

Especifica si las pasarelas ODBC de UDA vuelven a preparar la consulta para cada valor de parámetro.

Sintaxis:

UDA.REPREPARE_QUERY_FOR_PARAMETER_VALUE= "nombre de base de datos:valor booleano"

Tipo de datos:

Booleano

Valor predeterminado:

Falso

UDA.SET_READONLY_TRANSACTION_AUTOCOMMIT

Al conectar varias bases de datos, establezca esta propiedad en TRUE para habilitar el modo de confirmación automática para una sola base de datos si la base de datos da soporte a las transacciones con confirmación automática.

De forma predeterminada, si una de las bases de datos de la operación de conexión no da soporte a la confirmación automática, la operación de conexión no da soporte a estas transacciones para todas las bases de datos. Si se establece esta propiedad en TRUE, se habilita la confirmación automática para las transacciones de solo lectura. El valor FALSE inhabilita esta funcionalidad.

Si una base de datos no da soporte a las transacciones con confirmación automática, al habilitar esta funcionalidad podría aparecer la siguiente excepción: UDA-SQL-0178 No se soporta la opción de bloque de parámetros "start ".

Sintaxis:

UDA.SET_READONLY_TRANSACTION_AUTOCOMMIT= "nombre de base de datos:valor booleano"

Tipo de datos:

Booleano

Valor predeterminado:

Falso

UDA.THREADSTART_TIMEOUT

Especifica el tiempo, en segundos, que se espera a que se inicie un subproceso en la API sqlAOpen de UDA. En la API sqlAOpen, UDA utiliza un subproceso por separado para crear un conjunto de resultados, de modo que el conjunto de resultados podría cancelarse con la API sqlCancelOpen.

Para las prestaciones de versiones anteriores, se sigue dando soporte a la propiedad avanzada UDA_THREADSTART_TIMEOUT, que se establece en Cognos Configuration. Sin embargo, si la propiedad avanzada UDA.THREADSTART_TIMEOUT figura en Valores avanzados, se pasa por alto la propiedad avanzada UDA_THREADSTART_TIMEOUT de Cognos Configuration.

Sintaxis:

UDA.THREADSTART_TIMEOUT= valor numérico

Tipo de datos:

Entero positivo (1 - 600)

Valor predeterminado:

20

Índice

Caracteres Especiales

.cnv

aplicar sustituciones 443

.xml

aplicar conversiones 443

especificar conversiones 441

A

acceder a detalles 383

acceso basado en informe 384

acceso basado en modelo 384

cambiar el comportamiento del filtro 109

claves de empresa 389

con dimensiones compatibles 388

conceptos 384

configurar destinos en Analysis Studio 396

configurar en paquetes 392, 394

configurar parámetros de destino 394

contextos de selección 385

crear informes 399

definir el acceso en paquetes 392, 394

especificar texto de acceso a detalles 400

formatos de informe 385

miembros y valores 387

múltiples valores 400

Paquetes 386

PowerCubes y paquetes 391

rutas 384

utilizar ámbito en creación de informes basados en modelos 389

utilizar fechas 391

utilizar marcadores 386

utilizar URL 386

acceso a detalles

Ayudante para acceso a detalles 396

depurar 396

acceso a detalles,

Véase acceder a detalles

acciones

credenciales 222

permisos 215

acciones de detallar más

linaje 363

activar

servicios 54

Active Directory

listas de distribución como miembros de grupos y roles 210

actividades

administrar 263

actividades en segundo plano

Content Manager 74

iniciar o detener 74

actividades interactivas

arrendamiento múltiple 355

actuales

actividades 264

entradas 264

actualización de regla de conservación 194

actualizar

especificaciones de informe 312

grupos y roles 212

administración

IBM Cognos Analytics 1

Administración

funciones y características protegidas 227

administración del almacenamiento en memoria caché

Query Service 178

Administradores de biblioteca

Biblioteca de recursos 357

Administradores del sistema

desplegar 295

agente, servicio 49

exclusión del ID de contexto para un agente de las tareas de servicio web de WebSphere 90

agentes

propiedades 261

repetición fallida 274

servicios 49

agrupar

asignadores 57

ajustar

rendimiento de servidor 74

almacén de contenido

proteger 256

realizar copia de seguridad 183

almacén objeto externo. 100

almacenamiento de la sesión en la memoria caché

inhabilitar 98

almacenar en la caché

inhabilitar para una sesión 98

almacenes de contenido

desplegar 291

mantener 71

almacenes de datos

dimensiones compatibles 388

ámbito

utilizar en acceso a detalles 389

Analysis Studio

configurar destinos de acceso a detalles 396

funciones y características protegidas 227

limitar zonas interactivas 89

propiedades de informe 259

anotaciones

duración de las terminadas 109

anular el registro

asignadores 56

espacios de nombres 201

API 3

API de línea de comandos

Query Service 181

aprobar

solicitud de aprobación 378

archivado de contenido 194

archivar

Contenido de IBM Cognos 185

solicitudes de aprobación 382

solicitudes de notificación 382

tareas 382

tareas ad-hoc 382

- archivo de despliegue de exportación
 - ejecutar 307
- archivo descriptor
 - los archivos de resultado de informe en el software IBM Cognos 102
- archivo mob.log 419
 - añadir nivel de depuración 420
- archivos
 - despliegue 288
- archivos cargados
 - establecer etiquetas de direccionamiento 59
- archivos de salida de informe
 - guardar 100
 - guardar en software IBM Cognos 102
 - guardar fuera del software IBM Cognos 101
- archivos ipf
 - registro 25
- archivos principales de volcado 24
- arrendamiento múltiple
 - actividades interactivas 355
 - administración de arrendatarios 339
 - arrendatarios 327, 339
 - arrendatarios virtuales 333
 - asignar contenido a los arrendatarios 340
 - configuración que se basa en un atributo de cuenta de usuario 331
 - configuración que se basa en un nodo de jerarquía 329
 - configuración que se basa en un proveedor de arrendatarios personalizado 332
 - configurar 329
 - conjunto delimitador de arrendatario 335, 336
 - desplegar contenido de arrendatario 346
 - ID de arrendatario 341
 - inhabilitar valores de arrendamiento múltiple 338
 - propiedad conjunto delimitador de arrendatario 333
 - reglas de contención 339
 - tareas de utilización de almacén de contenido 352
 - verificación de consistencia del almacén de contenidos 353
- arrendatarios
 - crear 340
 - entornos de varios arrendatarios 327
 - habilitar 351
 - inhabilitar 351
 - perfiles de usuario 345
 - suprimir 351
 - terminar sesiones de usuarios activos 350
- arrendatarios virtuales
 - arrendamiento múltiple 333
- asignador 65
- asignadores 49, 65
 - agrupar 57
 - detener e iniciar 53, 54
 - equilibrar carga utilizando factor de solicitudes en curso 76
 - equilibrio de carga 78
 - equilibrio de carga utilizando capacidad de procesamiento 76
 - establecer búsquedas de estado 64
 - establecer reglas de direccionamiento 58
 - importar 311
 - migración tras error para varios 63
 - modo compatible con clúster 78
 - mover 57
 - probar 62
 - proteger 64
 - renombrar 62

- asignadores (*continuación*)
 - suprimir 56
- asignar ID de contenido 313
- Atajos 418
- atajos del teclado 435
 - espacios Mis informes, Contenido importado y Ejemplos 435
 - pantalla de inicio de IBM Cognos Mobile 435
 - Report Viewer 436
 - ventana Escribir código de seguridad 437
 - vistas Examinar y Búsqueda 436
- atributos
 - puntuación de métrica 45
- autenticación 199
 - pass-through de usuario, Microsoft Analysis Services 125
 - solicitudes 220
- autenticación de certificado
 - PKCS12 428
- autenticación pass-through del usuario, Microsoft Analysis Services 125
- autenticación SSL bidireccional 428
- autorización 202

B

- base de datos del almacén de contenido 111
- bases de datos
 - bloques de comandos 166
 - comandos 160, 480
 - comandos SQL nativo 483
 - configuración para multilingües 6
 - detener sesiones proxy 481
 - ejemplos de bloques de comandos 163
 - iniciar sesiones proxy 481
 - ordenación de entradas para entornos locales no ingleses 68
 - tablas para mensajes de registro 485
- bases de datos de Oracle
 - bases de datos privadas virtuales 160, 165
 - conexiones de proxy 160, 164
- bases de datos privadas virtuales
 - bases de datos de Oracle 160, 165
- biblioteca
 - visualizaciones 359
- Biblioteca
 - visualizaciones 357
- bloques de comandos
 - conexiones de base de datos 161
- borrado
 - datos de dispositivo 430
- buscar, contenido archivado 197

C

- cadenas de formato 124
- cadenas en las consultas
 - conversión de claves de búsqueda numéricas 96
- CAM, cookie de pasaporte 99
- cancelar
 - solicitud de aprobación 379
 - tarea ad-hoc 379
- cancelar ejecución de entrada 264
- capacidad
 - asignadores 76
- capacidad de procesamiento 76
- capacidades de objeto 239

- capacidades de objeto (*continuación*)
 - Véase también* funciones protegidas
 - configurar 241
 - Glosario 239
 - Linaje 239
- caracteres japoneses
 - seguridad de recorrido de ida y vuelta 440
- características,
 - Véase* características protegidas
- características de accesibilidad 433, 434
- características de Microsoft Office
 - instalar para consultas de MDX 131
- características nuevas del Fixpack 2
 - atributos de conexión de Db2 CLI 168
- características protegidas
 - Véase también* funciones protegidas
 - permisos de acceso 235
- cargar
 - reducir carga de Content Manager, archivos de sesión de usuario 70
- carpetas
 - archivar en repositorio externo 193
 - configuración 57
 - desplegar públicas 293
 - especificar repositorio externo 193
 - informes 193
 - inhabilitar al desplegar 294
- Carpetas públicas
 - desplegar 293
- certificados de cliente 428
- clave de contrato 430
- claves de búsqueda
 - conversión en cadenas en las consultas 96
- claves de búsqueda numéricas
 - conversión en cadenas en las consultas 96
- claves de empresa
 - utilizar para el acceso a detalles 389
- codificación Shift-JIS
 - ejemplo 440
- codificar caracteres en archivos PDF 83
- cogmob.log 422
- Cognos Analytics en dispositivos móviles 405
- Cognos SQL
 - añadir comentarios a sentencias SQL 169, 171
- Cognos Viewer
 - inhabilitar el almacenamiento de la sesión en la memoria caché 98
- Cognos Workspace, crear informes sobre comentarios 317
- comandos
 - base de datos 480
 - detener sesiones proxy 481
 - iniciar sesiones proxy 481
 - SQL nativo 483
- comentarios
 - Cognos SQL 169, 171
 - solicitud de aprobación 372, 377
 - SQL nativo 169, 171
 - tarea ad-hoc 372, 377
- comentarios, almacenar Cognos Workspace 317
- comentarios, crear informes de Cognos Workspace 317
- comentarios, desplegar IBM Cognos Workspace 316
- componentes de nivel de aplicación
 - servidor de registro 17
- conexiones
 - administrar 67
 - asignadores 80
 - establecer número 80
 - conexiones a orígenes de datos 113
 - conexiones con orígenes de datos JDBC 146, 155
 - conexiones de base de datos
 - bloques de comandos 161
 - conexiones de origen de datos 136, 155
 - añadir conexiones nuevas 153
 - cambiar valores 155
 - crear 146, 147
 - inicios de sesión 156
 - conexiones de proxy
 - bases de datos de Oracle 160, 164
 - configuración
 - asignadores y servicios 74
 - caracteres Shift-JIS 439
 - carpetas 57
 - codificación de caracteres japoneses 439
 - configurar
 - aplicaciones nativas de Cognos Mobile 406
 - arrendamiento múltiple 329
 - Impresoras 8
 - navegadores web 9
 - confirmar
 - solicitudes de notificación 381
 - conjunto delimitador de arrendatario
 - configuración que se basa en un atributo de cuenta de usuario 335
 - configuración que se basa en un proveedor personalizado 336
 - conjuntos con nombre
 - limitaciones 367
 - consola de administración de Planning, servicio 51
 - consultas
 - priorizar 96
 - consultas de MDX 131
 - contenido archivado, buscar 197
 - contenido de informe, buscar archivado 197
 - Content Manager
 - control de examen de espacios de nombres externos 69
 - jerarquía de objetos 445
 - límite de tamaño de la memoria caché 69
 - número máximo de conexiones 67
 - objetos 446
 - permisos de acceso iniciales 445, 446, 447
 - reducir carga, archivos de sesión de usuario 70
 - servicio 49
 - sincronizar en espera 68
 - valores avanzados 66
 - Valores de agrupación de conexiones de base de datos 67
 - Content Manager 8
 - desactivar archivado de especificación de informe 192
 - control, servicio 51
 - conversión de cadenas de búsqueda numéricas en cadenas en las consultas 96
 - cookies
 - habilitar en navegadores web 9
 - cortafuegos
 - IBM Cognos Application Firewall 203
 - Creación de informes
 - crear informes de acceso a detalles 399
 - funciones y características protegidas 227
 - inhabilitar el almacenamiento de la sesión en la memoria caché 98
 - Map Manager 4
 - propiedades de informe 259
 - crear
 - carpetas de configuración 57

- crear paquetes
 - para PowerCubes 319
 - para SAP BW 319
- crear tarea de mantenimiento de archivado de contenido 194
- credenciales
 - cambiar planificación 281
 - de confianza 222
 - origen de datos 156, 224
- credenciales de confianza 222
 - crear 222
 - planificar 222
 - renovación 222, 223
- cubo
 - renovar las conexiones de servicio de informes para PowerCubes reconstruidos 47
- cubos 361
 - IBM Cognos Series 7 368
 - propiedades multilingües de IBM Cognos Series 7 369
- cubos de Cognos 116
- cuentas de usuario
 - exportar 305
 - importar 309

D

- datos
 - borrado desde dispositivos 430
 - desplegar 303
 - ejemplos multilingües 473
 - exportar 305
 - importar 308
 - realizar copia de seguridad 183
 - visualizar linaje 363
- datos de informes, servicio 49, 52
 - especificar correlaciones de pasarelas 61
- datos Planning, servicio 51
- Db2
 - soporte para atributos de conexión de Db2 CLI 168
- Db2, origen de datos 114
- Db2 OLAP
 - orígenes de datos 120, 121
- definición para acceso a detalles
 - Ayudante para acceso a detalles 396
 - depurar 396
- Delivery Service 50
- denegar acceso 219
- desplegar
 - Administradores del sistema 295
 - almacén de contenido entero 291
 - archivos 288
 - Carpetas públicas 293
 - contenido de directorio 293
 - datos 303
 - despliegue parcial 293
 - especificaciones 288
 - exportar 305
 - grupos 295
 - importar 308
 - informes 287
 - líneas de comandos 287
 - mover archivos 308
 - objetos de configuración 311
 - Orígenes de datos 296
 - Paquetes 293
 - permisos 303
 - planificador 288
 - PowerCubes actualizados 171

- desplegar (*continuación*)
 - probar 312
 - referencias externas de espacio de nombres 288
 - requisitos previos 303
 - roles 295
 - seguridad 220, 288
- despliegue 287
 - Véase también* desplegar
 - crear una especificación de exportación 305
 - documento de prácticas recomendables 287
 - entornos de varios arrendatarios 346
 - Human Task and Annotation Services 314
 - reglas 298
- destinos de registro
 - tipos 17
- detener
 - servicios 53
 - solicitud de aprobación 378
 - tarea ad-hoc 378
- diagnóstico de Android
 - cogmob.log 422
- diagnóstico de iOS
 - mobile_ios.log 422
- diagnósticos
 - Véase* solucionar problemas
- dimensiones
 - compatibles para acceso a detalles 388
- directorios
 - desplegar contenido 293
- dispositivos Android
 - configurar para usuarios 406
- dispositivos iOS
 - configurar para usuarios 406
- documentación de seguridad
 - prácticas recomendables de Cognos 199
- documentos de prácticas recomendables
 - despliegue 287
- dominio de workspace 111

E

- ejecución de consultas
 - simultánea 92
- ejecución simultánea de consultas 92
- ejecutar
 - historial de entrada 272
- ejecutar informes
 - roles 209
- ejecutar rastreo de árbol
 - Query Service 175
- ejemplos
 - codificación Shift-JIS 440
 - Mobile 423
 - utilizar datos multilingües 473
- ejemplos de Mobile 423
- elementos de observación
 - propiedades de regla 262
- entornos
 - configuración de multilingües 4
- entornos de destino
 - despliegue 287
- entornos locales 290
 - Microsoft Analysis Services 125
 - ordenación de entradas 68
 - reemplazar en la memoria caché de solicitud 71
 - usuarios 208

- entradas
 - actuales 264
 - cancelar ejecución 264
 - habilitar 257
 - historial de ejecución 272
 - pasadas 265
 - planificadas 270
 - planificar 279
 - planificar basándose en apariciones 286
 - prioridad de ejecución 271
 - propiedades 257
 - próximas 266
 - repetición fallida 274
 - suspender ejecución 264
 - suspendidas 267
- entradas fallidas
 - repetir ejecución 274
- entradas predefinidas 244, 254
- entrega
 - servicio 49
- equilibrar carga de asignadores
 - capacidad de procesamiento 76
 - factor de solicitudes en curso 76
- equilibrio de carga 76
 - asignadores 78
 - capacidad de procesamiento 76
 - factor de solicitudes en curso 76
- Errores detallados
 - funciones y características protegidas 227
- escribir estado de la memoria caché 179
- escribir modelo en archivo
 - Query Service 175
- espacio de nombres eTrust SiteMinder 199
- espacio de nombres LDAP 199
- espacio de nombres SAP 199
- espacios de nombres 199
 - Véase también* espacios de nombres externos
 - Véase también* proveedores de autenticación
- desplegar referencias externas 288
- examinar externos 69
- IBM Cognos 202
- múltiples 199, 220
- restaurar 201
- suprimir 201
- utilizar desde IBM Cognos Series 7 12
- espacios de nombres externos 199
 - control de examen 69
 - desplegar referencias 288
 - eTrust SiteMinder 199
 - IBM Cognos Series 7 199
 - LDAP 199
 - Microsoft Active Directory 199
 - SAP 199
- espacios de nombres IBM Cognos Series 7 199
 - inicio de sesión único 368
- espacios de trabajo
 - IBM Cognos Workspace 403
- especificaciones
 - despliegue 288
- Especificaciones de despliegue
 - modificar existentes 307
- especificaciones de informe
 - actualizar 312
 - desactivar archivado 192
 - registro 20
- esquema de datos para mensajes de registro 485

- Essbase
 - Véase* Oracle Essbase
- establecer
 - acceso a funciones y características protegidas 235
 - frecuencia de las búsquedas de estado del asignador 64
 - permisos de acceso 221
 - retención de documentos periódicos 88
 - retención de salida de la lista de observación 88
 - tiempo máximo de ejecución 87
- estado del panel Tabla de puntuación 42
- etiquetas de direccionamiento 58
 - establecer grupos de servidores 75
 - establecer para objetos de datos 59
- evaluación del rendimiento del sistema 44
- Event Studio
 - funciones y características protegidas 227
- eventos
 - registro 18
 - registros 18
- evitar bloque al añadir o actualizar planificaciones 111
- examinar
 - controlar espacios de nombres externos 69
- Excel 2007
 - hojas de trabajo grandes 103
- exportar 305
 - Carpetas públicas 305
 - crear una especificación 305
 - cuentas de usuario individuales 305
 - datos 305
 - mis carpetas 305
 - visualizaciones 305
- extensiones multialfabeto 473

F

- factor de solicitudes en curso 76
- fechas
 - utilizar para acceso a detalles 391
- fechas límite
 - solicitudes de aprobación 377
- FileNet
 - desactivar archivado de especificación de informe 192
 - importar clases personalizadas 188
- filtrado
 - acceder a detalles, dimensiones descriptivas 399
 - acceder a detalles, medidas 399
 - cambiar el comportamiento del filtro de acceso a detalles 109
- finalizar
 - solicitud de aprobación 378
 - tarea ad-hoc 378
- Firefox
 - valores 9
- formatear
 - informes 364
 - informes en formato CSV 366
 - informes en formato Excel 365
 - informes en HTML 364
- formateo CSV
 - informes 366
- formato PDF
 - informes 364
 - valores de archivos 83
 - valores de codificación de caracteres 83
 - valores de inclusión de fuentes 83
 - valores de nivel del algoritmo de compresión 83
 - valores de tipo de compresión de contenido 83

- formatos de salida
 - restringir 191
- formatos numéricos 124
- forwardURLParamsToCM, parámetro 110
- Framework Manager
 - realizar copia de seguridad 183
- fuentes
 - archivos PDF 83
 - instalar 6
- funciones
 - Administración de Mobile 426
 - funciones protegidas 227
 - Mobile 426
- funciones,
 - Véase* funciones protegidas
- funciones protegidas
 - Administración 227
 - Analysis Studio 227
 - Creación de informes 227
 - Errores detallados 227
 - Event Studio 227
 - Generar salida CSV 227
 - Generar salida PDF 227
 - Generar salida XLS 227
 - Generar salida XML 227
 - Glosario 227
 - IBM Cognos Viewer 227
 - Linaje 227
 - Mis datos 227
 - Mobile 227
 - permisos de acceso 235
 - Planificación 227
 - Query Studio 227
- funciones y características protegidas
 - Cognos Mobile 426
 - permisos de acceso iniciales 447

G

- GDPR, cumplimiento
 - informes de auditoría 22
- gestión de eventos, servicio 50
- gestor de contenidos
 - actividades en segundo plano 74
- Glosario
 - Véase también* InfoSphere Business Glossary
 - capacidades de objeto 239
 - funciones y características protegidas 227
- Google Chrome
 - valores 9
- gráficos, servicio 50
- grupo Todos 243
- grupos 208
 - añadir listas de distribución 210
 - añadir y eliminar miembros 212
 - asignar tema de Mobile 409
 - crear 211
 - desplegar 295
 - establecer palabras clave de direccionamiento 59
 - IBM Cognos Controller 210
 - incorporados 243
 - modificar los valores después de la instalación 254
 - seguridad 207
- grupos de IBM Cognos
 - actualizar 212
 - crear 211

- grupos de servidores
 - establecer 75
 - establecer reglas de direccionamiento 60, 75
- guardar
 - archivos de salida de informe 100
 - los archivos de resultado de informe en el software IBM Cognos 102
 - resultados del informe fuera del software IBM Cognos 101
- guardar resultados de informe 102

H

- habilitar
 - conversión de claves de búsqueda numéricas en cadenas de las consultas 96
 - entradas 257
 - métricas de cola 108
- historial de ejecución
 - cuánto tiempo guardarlas 273
 - entradas planificadas 279
 - visualizar 272
- historiales
 - despliegue 312
- historiales de salida de informe
 - cuánto tiempo guardarlas 367
- hojas de trabajo
 - Excel 2007 103
- horas
 - punta, establecer 79
- horas de archivado
 - especificar 190
- HTML
 - formatear informes 364
- HTTPOnly 99

I

- IBM Cognos
 - espacio de nombres 202
- IBM Cognos Administration
 - página de estado 42
 - valores avanzados 513
- IBM Cognos Analytics
 - administración 1
 - asignadores 52
 - servicios 52
- IBM Cognos Analytics Community
 - visualizaciones 357
- IBM Cognos Analytics y PowerPlay
 - inicio de sesión único 368
- IBM Cognos Application Firewall 203
- IBM Cognos content archival
 - repositorio externo 185
- IBM Cognos Controller
 - seguridad 210
- IBM Cognos Series 7
 - añadir contenido al portal 12
 - informes y cubos PowerPlay 368
 - usuarios 207
 - utilizar espacios de nombres 12
- IBM Cognos Viewer
 - funciones y características protegidas 227
- IBM Cognos Workspace
 - espacios de trabajo 403
- IBM Cognos Workspace, almacenar comentarios 317

- IBM Cognos Workspace, desplegar comentarios 316
- IBM Connections
 - configurar colaboración 107
- IBM Content Manager 8
 - importar
 - clases personalizadas para IBM Content Manager 8 188
 - importar clases personalizadas 188
- IBM Db2
 - Véase Db2
- IBM FileNet Content Manager 136, 185
- IBM InfoSphere Information Governance Catalog
 - solución de linaje 105
- IBM Infosphere Warehouse Cubing Services 124
- IBM Metadata Workbench
 - solución de linaje 363
- ID de arrendatario
 - objeto público 341
- ID de contenido, asignar 313
- idiomas
 - elegir para informes 366
 - orígenes de datos SAP BW 366
 - valores predeterminados para informes 366
- importar
 - Carpetas públicas 309
 - clases personalizadas en FileNet 188
 - configuraciones 311
 - cuentas de usuario individuales 309
 - mis carpetas 309
 - visualizaciones 309
- importar archivos 290
- importar datos
 - IBM Cognos Analytics 308
 - reglas 298
- Impresoras
 - configurar 8
- imprimir
 - Configuración de impresoras 8
 - UNIX, sistema operativo 111
- información de conexión
 - renovar 47
- información de conexión, renovar 47
- informes 361
 - accesibilidad para los discapacitados 361
 - accesibles, crear 2, 433
 - activos 362
 - cambiar opciones predeterminadas de PowerPlay 369
 - capacidades de generar salidas 364
 - configuración para multilingües 6
 - crear vistas 362
 - desplegar 287
 - ejecución desde un dispositivo 418
 - ejecución desde un sistema de sobremesa 418
 - elegir idiomas 366
 - especificar los valores de solicitud predeterminados 367
 - establecer límites en cola 82
 - formato PDF 364
 - formatos 364
 - formatos CSV 366
 - formatos de Excel 365
 - formatos HTML 364
 - Generar salida CSV 364
 - Generar salida PDF 364
 - Generar salida XLS 364
 - Generar salida XML 364
 - IBM Cognos Series 7 368
 - idiomas predeterminados 366

- informes (*continuación*)
 - planificar 277
 - propiedades multilingües de IBM Cognos Series 7 369
 - repetición fallida 274
 - restricción del acceso a los formatos de salida 364
 - vistas de planificación 277
- informes accesibles
 - habilitar 2, 433
- informes activos 362
- informes de auditoría 22
 - configurar 22
- informes de Excel
 - formatear 365
- informes en Excel 2007
 - nombre de pestañas de hoja de trabajo 104
- informes web de Series 7 PowerPlay
 - seguridad de recorrido de ida y vuelta 444
- InfoSphere Business Glossary
 - Cognos Viewer 363
 - configurar URI 106
- inhabilitar
 - acceso a informes 361
 - almacenamiento de la sesión en la memoria caché 98
 - archivos principales de volcado 24
 - carpetas al desplegar 294
 - mensajes de error de protección 23
 - paquetes al desplegar 294
 - trabajo de mantenimiento de contenido 73, 180
- iniciar
 - servicios 53, 54
 - solicitud de aprobación 378
 - tarea ad-hoc 378
- iniciar la sesión
 - múltiples espacios de nombres 220
- inicio de sesión
 - modificar 157
- inicio de sesión único
 - IBM Cognos Analytics y PowerPlay 368
 - Microsoft Analysis Services 125
 - Microsoft SQL Server 130
- inicios de sesión
 - orígenes de datos 156, 224
- inicios de sesión de origen de datos
 - cambiar 156
 - crear 156
- instalar
 - fuentes 6
- Internet Explorer
 - valores 9

J

- Java Management Extensions 65
- jerarquías
 - Essbase 122
- jerarquías desequilibradas
 - Essbase 122
- jerarquías equilibradas
 - Essbase 122
- JMX 65
- JMX, servidor proxy 65
- jmxProxyHostDispatchers 65

L

- leer
 - solicitudes de notificación 381
- límites en cola
 - establecer 82
- linaje
 - acciones de detallar más 363
 - configurar 105
 - IBM InfoSphere Information Governance Catalog 105
 - IBM Metadata Workbench 363
 - visualizar 363
- Linaje
 - capacidades de objeto 239
 - funciones y características protegidas 227
- lista de dominios de confianza 111
- lista de dominios válidos 111
- listas de distribución
 - pertenencia a grupos y roles 210
- los archivos de resultado de informe en el software IBM Cognos
 - archivo descriptor 102
- lote
 - informes 49
 - servicios de informes 49

M

- Map Manager
 - configuración para multilingües 4
- marcadores
 - crear para acceso a detalles 386
- mecanismos de seguridad 425
- medidas
 - cadenas de formato 124
 - no filtradas en acceso a detalles 399
- mejorar
 - rendimiento 74
- memoria caché
 - borrar, Query Service 178
- memoria caché de Query Service
 - analizar uso 179
- memoria caché de solicitud
 - reemplazar entornos locales 71
- memorias caché
 - límite de memoria caché de Content Manager 69
 - sesión 70
- mensajes
 - registro 18
- mensajes de error
 - protección 23
- mensajes de error de protección, ver detalles 23
- mensajes de registro
 - Véase también* solucionar problemas
 - servidor de registro remoto 17
- metadatos 319
- métricas
 - restablecer 47
 - restablecer del sistema 47
- métricas de cola
 - habilitar 108
- métricas de cola de tareas
 - habilitar 108
- métricas de cola de trabajo
 - habilitar 108
- métricas de cola SMTP
 - habilitar 108

- métricas de rendimiento del sistema 29
 - cola 32
 - jvm 34
 - lista de métricas 31
 - proceso 40
 - recopilación de datos 29
 - renovar conexiones de servicio de informes 47
 - sesión 31
 - solicitud 36
- métricas del sistema
 - restablecer 47
- Microsoft Active Directory 199
- Microsoft Analysis Services
 - inicio de sesión único 125
 - Microsoft SQL Server Analysis Services 2005 (SSAS 2005) 125
 - orígenes de datos 125
- Microsoft Office
 - datos de informes, servicio 52
- Microsoft SQL Server 130
 - inicio de sesión único 130
 - instalar características de Microsoft Office para aplicaciones VBA 131
 - orígenes de datos 130
- miembros
 - acceso a detalles 387
 - grupos y roles de IBM Cognos 212
- migraciones tras error
 - varios asignadores 63
- Mis páginas
 - añadir contenido de IBM Cognos Series 7 12
- Mobile
 - funciones y características protegidas 227
- mobile_ios.log 422
- modelado de datos 319
- modelos 319
 - optimizar 75
 - realizar copia de seguridad 183
- modificar un inicio de sesión 157
- modo compatible con clúster 78
- módulos de datos
 - establecer etiquetas de direccionamiento 59
- monedas
 - visualizar mixtas 361
- mover
 - archivos de despliegue 308
 - asignadores 57

N

- navegadores web
 - configurar 9
- NewsBoxes de Upfront
 - añadir a portales 12
- nivel del algoritmo de compresión en archivos PDF 83
- niveles de aislamiento
 - orígenes de datos 158
- niveles de validación del informe 19
- notificaciones por correo electrónico
 - solicitud de aprobación 372
 - tarea ad-hoc 372
- notificaciones push 415
 - Apple 415
- notificaciones push de Apple
 - certificado SSL 416
- número máximo de objetos en paquete de SAP BW 321

O

- ODBC
 - Orígenes de datos 133
- opciones de despliegue
 - parcial 294
- optimizar
 - modelos 75
 - rendimiento 74
- Oracle Essbase
 - orígenes de datos 120
- Ordenación
 - entornos locales no ingleses 68
- orígenes
 - entornos de despliegue 287
- orígenes de datos 113, 125
 - archivos XML 144
 - bloques de comandos 166, 167
 - comandos 479
 - comandos de conexión 480
 - conexiones 147
 - crear inicios de sesión 156
 - credenciales 156, 224
 - cubos de Cognos 116
 - Db2 OLAP 120, 121
 - IBM Infosphere Warehouse Cubing Services 124
 - Informix 124
 - inicio de sesión 156, 224
 - Microsoft SQL Server 130
 - Microsoft SQL Server Analysis Services 2005 (SSAS 2005) 125
 - Microsoft SQL Server Analysis Services 2008 (SSAS 2008) 125
 - modificar conexiones existentes 154
 - modificar orígenes 156
- ODBC 133
- Oracle 135
- Oracle Essbase 120
- proteger frente a múltiples espacios de nombres 220
- rutas a conexiones de orígenes de datos basados en archivos 147
- SAP Business Information Warehouse (SAP BW) 138
- seguridad 172
- Sybase Adaptive Server Enterprise 141
- tiempos de espera de la conexión 155
- TM1 143

Orígenes de datos

- comandos de base de datos 160
- Db2 114
- desplegar 296
- ejemplos de bloques de comandos 163
- niveles de aislamiento 158
- utilizar conexiones JDBC 146

orígenes de datos basados en archivos

- rutas 147

orígenes de datos de Sybase Adaptive Server Enterprise 141

orígenes de datos Informix 124

orígenes de datos Oracle 135

orígenes de datos SAP Business Information Warehouse (SAP BW) 138

orígenes de datos SAP BW

- idiomas 366

orígenes de datos TM1 143

otorgar acceso 219

P

Página de estado de IBM Cognos Administration 42

palabras clave de direccionamiento

- establecer para grupos y roles 59

panel Métricas de IBM Cognos Administration 42

panel Tabla de puntuación de IBM Cognos Administration 42

panel Valores de IBM Cognos Administration 44

Paquetes 319

- acceder a detalles 386
- administrar 319
- configurar el acceso a detalles 392, 394
- crear para PowerCubes 319
- crear para SAP BW 319
- desplegar 293
- editar SAP BW 319
- especificar repositorio externo 193
- establecer etiquetas de direccionamiento 59
- inhabilitar al desplegar 294

parámetros de conexión 136, 149, 155

partes interesadas

- solicitudes de aprobación 375
- tareas ad-hoc 375

pasadas

- actividades 265
- entradas 265

pasarelas

- especificar correlaciones del servicio de datos de informes 61

pcactivate

- desplegar PowerCubes actualizados 171

perfiles

- usuario 323

perfiles de usuario

- arrendamiento múltiple 345
- copiar 326
- default 323

periodos de inactividad

- especificar 190

permisos

- Véase también* permisos de acceso
- acciones 215
- desplegar 303
- despliegue 220
- ejecución 213
- escritura 213
- establecer política 213
- funciones y características protegidas 227, 235
- lectura 213
- otorgar o denegar 219
- padre/hijo 219
- suprimir grupos y roles 220
- visita 213

permisos de acceso 235

- Véase también* permisos
- anónimos 243
- credenciales 222
- establecer 221
- funciones 447
- funciones y características protegidas 235, 447
- iniciales 445, 446
- otorgar o denegar 219
- propiedad de entradas 219
- usuarios 214

permisos de ejecución 213

- funciones y características protegidas 235

permisos de escritura 213

permisos de lectura 213

- permisos para establecer política 213
- permisos y acciones permitidas
 - Cognos Workspace
 - informes, partes de informes, carpetas, espacios de trabajo 215
- PKCS12 428
- planificación
 - tareas de almacenamiento en memoria caché de Query Service 178
- Planificación
 - funciones y características protegidas 227
- planificación basada en activadores 284
- planificaciones
 - administrar 270, 272, 277
 - administrar entradas suspendidas 267
 - administrar próximas actividades 266
 - basadas en activadores 284
 - cambiar credenciales 281
 - credenciales 222
 - entradas 279
 - entradas basadas en apariciones 286
 - historial de ejecución 279
 - informes y vistas de informe 277
 - solicitudes 278
 - tareas de administración de Query Service 180
 - trabajos 282
 - validar propiedades al añadir o actualizar 111
 - varias entradas 282
- planificador
 - despliegue 288
- planificar 418
- políticas de autenticación 431
- posibles propietarios
 - solicitudes de aprobación 375
 - tareas ad-hoc 375
- PowerCubes
 - actualizar 171
 - crear paquetes 319
 - pactivate 171
 - renovar conexiones de servicio de informes 47
 - rutas a archivos de cubo 147
- PowerPlay
 - cambiar valores predeterminados del informe 369
 - conversiones de fuentes en informes web de Series 7 444
 - informes 368
 - propiedades de informe 259
 - utilizar las herramientas de creación de informes de PowerPlay 368
- prácticas recomendables de Cognos
 - documentación de seguridad 199
- precisión decimal
 - reducir 100
- presentación, servicio 52
- prestación Administración de Mobile 426
- Prestación Mobile 426
- prioridad
 - solicitudes de aprobación 377
 - tareas ad-hoc 377
- prioridad de ejecución 271
- priorizar consultas 96
- probar
 - asignadores 62
 - despliegue 312
- problemas conocidos de accesibilidad
 - suprimir en campos de entrada de texto 439
 - tocar en modo VoiceOver 438
 - ver contenido de informe 438

- procesos
 - capacidad de asignadores 76
 - establecer número 80
- procesos y conexiones
 - establecer número máximo 81
- programas de utilidad
 - configuración de seguridad de recorrido de ida y vuelta 440
- propiedad conjunto delimitador de arrendatario
 - arrendamiento múltiple 333
- propiedades
 - agentes 261
 - Atajos 257
 - contactos 257
 - ejecutar como propietario 259
 - entradas 257
 - formatos 259
 - historiales de ejecución 257
 - idiomas 257, 259
 - informes de origen 257
 - informes y cubos multilingües de IBM Cognos Series 7 369
 - propietarios 257
 - Query Service 175
 - reglas 262
 - sugerencias 257
 - trabajos 261
 - valores de solicitud 259
 - versiones de salida de informe 257
- propietario
 - solicitudes de aprobación 375
 - tareas ad-hoc 375
- protección de contraseña 427
- proteger
 - almacén de contenido 256
 - asignadores 64
- proveedores
 - seguridad 199
- proveedores de autenticación 199
- próximas actividades 266
- Proyectos
 - realizar copia de seguridad 183
- puntuaciones de métrica
 - atributos, visualización 45
- puntuaciones de métrica del panel Tabla de puntuación 42

Q

- Query Service 52
 - administración 175
 - administración del almacenamiento en memoria caché 178
 - analizar uso de memoria caché 178
 - API de línea de comandos 181
 - borrar memoria caché 178
 - creación y planificación de tareas de administración 180
 - ejecutar rastreo de árbol 175
 - escribir modelo en archivo 175
 - propiedades 175
 - rastreo de ejecución 175
 - rastreo de planificación de consultas 175
 - tiempo de espera de conexión inactiva 175
 - uso de memoria caché 178
- Query Studio
 - funciones y características protegidas 227
 - inhabilitar el almacenamiento de la sesión en la memoria caché 98
 - propiedades de informe 259

R

- rastreo de ejecución
 - Query Service 175
- rastreo de planificación de consultas
 - Query Service 175
- realizar copia de seguridad
 - datos 183
 - restaurar archivos 183
- rechazar
 - solicitud de aprobación 378
- reclamar
 - solicitudes de aprobación 375
 - tareas ad-hoc 375
- registrar
 - usuarios específicos 26
- registrar consultas nativas 20
- registrar mediante archivos ipf 25
- registrar para un usuario específico 25
- registro
 - archivo mob.log 419
 - configurar 18
 - consultas nativas 20
 - definición de nivel 21
 - diagnóstico de un problema para un usuario específico 25
 - esquema de datos para mensajes 485
 - informes de auditoría 22
 - inhabilitar registro para usuarios específicos 27
 - mensajes 18
 - métodos 419
 - niveles 18
 - niveles de validación del informe 19
 - opciones de ejecución de informes 20
 - registro de Cognos Analytics para Cognos Mobile 421
- registros
 - procesamiento de mensajes 17
 - servicio 50
 - servicios 49
 - tablas de base de datos para mensajes 485
- registros de auditoría
 - Véase también* mensajes de registro
 - Véase también* solucionar problemas
 - destinos de registro 17
- reglas
 - despliegue 298
 - propiedades 262
- reglas de direccionamiento 58
 - establecer 60
- rendimiento
 - ajustar 74
 - horas punta 79
 - sistema 29
 - sistema, evaluación 44
- renombrar
 - asignadores 62
- renovación
 - credenciales de confianza 222, 223
- renovar
 - conexiones de servicio de informes 47
 - datos en memoria caché 282
- repositorio
 - especificar externo 193
- repositorio de informes 136
- repositorio externo
 - archivar contenido 185
- requisitos previos
 - desplegar 303
- restablecer
 - métricas 47
 - métricas del sistema 47
- restaurar
 - datos 183
 - espacios de nombres 201
- restricción del acceso a IBM Cognos Analytics 13
- retención 194
- revocar
 - solicitudes de aprobación 376
 - tareas ad-hoc 376, 377
- rol Administradores de arrendatarios 244
- rol Administradores del sistema 244, 426
- rol Usuarios de Mobile 426
- roles 208
 - Administradores de Mobile 426
 - añadir listas de distribución 210
 - añadir y eliminar miembros 212
 - asignar tema de Mobile 409
 - crear 211
 - desplegar 295
 - ejecutar informes 209
 - establecer palabras clave de direccionamiento 59
 - IBM Cognos Controller 210
 - IBM Cognos Series 7 209
 - incorporados 243
 - modificar los valores después de la instalación 254
 - predefinidos 244, 254
 - seguridad 207
 - Usuarios de Mobile 426
- roles de IBM Cognos
 - actualizar 212
 - crear 211
- RSVP.EXCEL.EXCEL_2007_LARGE_WORKSHEET 103
- RSVP.EXCEL.EXCEL_2007_OUTPUT_FRAGMENT_SIZE 103
- RSVP.EXCEL.EXCEL_2007_WORKSHEET_MAXIMUM_ROWS 103
- RSVP.EXCEL.PAGEGROUP_WSNAME_ITEMVALUE 104
- RSVP.PRINT.POSTSCRIPT 111

S

- Safari 5
 - valores 9
- salida de informe accesible
 - establecer para todo el sistema 3, 434
- salida de informe accesible en todo el sistema 3, 434
- salida de la lista de observación
 - retención 88
- SAP BW
 - crear paquetes 319
 - paquetes, editar 319
 - paquetes, número máximo de objetos 321
- schema
 - comandos de orígenes de datos 479
- scripts Java
 - habilitar en navegadores web 9
- secuencias de comandos ActiveX
 - habilitar en navegadores web 9
- seguridad
 - aplicaciones nativas 429
 - autenticación 199
 - clave de contrato 430
 - configurar 243, 254
 - datos de informe 430
 - despliegue 220, 288
 - entradas incorporadas 243
 - entradas predefinidas 244, 254

- seguridad (*continuación*)
 - establecer para salida en PDF 364
 - funciones y características 227
 - grupo Todos 13, 243
 - IBM Cognos Application Firewall 203
 - modelos 199
 - modificar los valores después de la instalación 254
 - niveles de aplicación 203
 - orígenes de datos 172
 - permisos de acceso 213
 - políticas de autenticación 431
 - políticas iniciales 243
 - protección de contraseña 427
 - proveedores 199
 - restricción del acceso a IBM Cognos Analytics 13
 - rol Administradores del sistema 244
 - tecnología de clave de contrato 430
 - usuarios, grupos y roles 207
 - valores de pasaporte CAM 431
 - valores iniciales 243
- seguridad de datos de informe 430
- seguridad de PDF
 - establecer en informes 364
- seguridad de recorrido de ida y vuelta
 - aplicar conversiones y sustituciones 443
 - caracteres japoneses 440
 - especificar conversiones 441
 - informes web de Series 7 PowerPlay 444
 - programa de utilidad de configuración 440
 - restaurar valores predeterminados de conversión 443
- separación
 - desplegar resultados 288
- servicio
 - gráficos 50
 - tarea humana 50
- servicio de anotaciones 49
 - despliegue 314
- servicio de Cognos Mobile
 - configuración global 411
- Servicio de Content Manager 50
 - especificar un valor predeterminado 55
- servicio de datos de informes (RDS)
 - límite de tamaño del informe 90
- servicio de informes por lotes 49
- servicio de la galería de visualización 52
- Servicio de metadatos 51
- servicio de metadatos relacionales 52
- Servicio de migración 51
- servicio de Mobile
 - valores avanzados 408
- Servicio de visualización de descubrimiento interactivo 50
- servicio móvil 51
- servicios 49
 - activar 54
 - administración de eventos 50
 - agente 49
 - anotación 49
 - consulta 52
 - Content Manager 50, 66
 - control 51
 - datos de informe 52
 - datos Planning 51
 - detener e iniciar 53
 - entrega 50
 - IBM Cognos Analytics 52
 - informe 52
 - informe por lotes 49
- servicios (*continuación*)
 - informes 49
 - log 50
 - Metadatos 51
 - metadatos relacionales 52
 - Migración 51
 - móvil 51
 - Presentación 49, 52
 - registros 49
 - repositorio 52
 - servicio de la galería de visualización 52
 - servicios de agente 49
 - servicios de control 49
 - servicios de entrega 49
 - servicios de gestión de eventos 49
 - servicios de trabajo 49
 - sistema 52
 - trabajo 50
 - Visualización de descubrimiento interactivo 50
- servicios de gestión de eventos 49
- servicios de informes 49, 52
 - conexiones 47
- servicios de presentación 49
- servicios de repositorio 52
- servidor de informes
 - administrar tiempos de espera de conexión 155
 - valores 96
- servidor proxy 65
- servidores
 - administración 49
 - ejecución simultánea de consultas 92
- servidores de datos
 - parámetros de conexión 149
- sesión del navegador web 99
- sesiones
 - detener proxy 481
 - iniciar proxy 481
- sesiones proxy
 - detener en bases de datos 481
 - iniciar en bases de datos 481
- sincronizar
 - Content Manager en espera 68
- sistema
 - rendimiento 29
- sistema, servicio 52
- solicitudes 418
 - datos en memoria caché 282
 - entradas planificadas 278
 - equilibrio de carga 76
 - especificar los valores de informe predeterminados 367
 - procesar 80
 - registro 20
- solicitudes de aprobación
 - aprobar 378
 - archivar 382
 - cambiar destinatarios para 375
 - cancelar 379
 - comentarios 372, 377
 - detener 378
 - fechas límite 377
 - finalizar 378
 - iniciar 378
 - prioridad 377
 - realizar acciones 371, 374
 - rechazar 378
 - reclamar 375
 - revocar participación de 376

- solicitudes de aprobación (*continuación*)
 - suscribirse a notificaciones de correo electrónico para 372
- solicitudes de notificación 379
 - archivar 382
 - confirmar 381
 - crear 380
 - leer 381
- solucionar problemas
 - diagnóstico de un problema para un usuario específico 25
 - mensajes de registro 18
 - registro 17
- soporte de accesibilidad
 - habilitar salida de informe 2, 433
- soporte HTML y HTTP 427
- SQL,
 - Véase Cognos SQL
 - Véase SQL nativo
- SQL nativo
 - añadir comentarios a sentencias SQL 169, 171
 - comandos 483
- supervisar
 - eventos 18
 - servicios 49
- supresión de valores nulos 319
- suprimir
 - asignadores 56
 - espacios de nombres 201
 - perfiles de usuario 325
 - valores nulos 319
- suspender
 - entradas 264

T

- Tablas
 - base de datos de mensajes de registro 485
- tamaños de papel
 - definir 259
- tarea de mantenimiento de contenidos 194
- tareas
 - archivar 382
 - automatizar 3
 - cancelar 379
 - comentarios 372, 377
 - confirmar 381
 - detener 378
 - fechas límite 377
 - finalizar 378
 - iniciar 378
 - notificaciones por correo electrónico 372
 - partes interesadas 375
 - posible propietario 375
 - prioridad 377
 - propietario 375
 - realizar acciones 371, 374
 - reclamar 375
 - revocar participación de 376
 - solicitudes de notificación 379
 - visualizar archivo 382
- tareas ad-hoc
 - archivar 382
 - cambiar destinatarios para 375
 - cancelar 379
 - comentarios 372, 377
 - crear 373
 - detener 378
 - fechas límite 377

- tareas ad-hoc (*continuación*)
 - finalizar 378
 - iniciar 378
 - prioridad 377
 - realizar acciones 371, 374
 - reclamar 375
 - revocar participación de 376
 - suscribirse a notificaciones de correo electrónico para 372
- tareas automatizadas 3
- tareas de almacenamiento en memoria caché de Query Service
 - planificación 178
- tareas de servicio web
 - exclusión del ID de contexto de un agente de WebSphere 90
- tareas de utilización de almacén de contenido
 - arrendamiento múltiple 352
- tareas humanas 371
 - duración de las terminadas 109
- tareas humanas, servicio 50
 - despliegue 314
- tecnología de clave de contrato 430
- tema de Mobile
 - configurar 409
 - editar 409
 - habilitar 409
 - suprimir 409
- temas
 - crear 410
- tiempo de ejecución
 - máximo 87
- tiempo de espera
 - conexiones de origen de datos 155
- tiempo de espera de conexión inactiva
 - Query Service 175
- tiempos de ejecución de subprocesos
 - especificar 190
- tiempos de espera 82
 - especificar para conexiones de base de datos de Content Manager 67
- tipo de compresión de contenido en archivos PDF 83
- trabajos
 - envío de pasos 261
 - opciones de entrega 261
 - pasos 282
 - planificar 282
 - propiedades 261
 - repetición fallida 274
 - servicios 49
- trabajos, servicio 50
- trabajos Planning, servicio 52
- transcripciones de datos multilingües 473

U

- ubicación de objetos temporales 70
- ubicación de resultado de informes 102
- umbral
 - establecer métrica 46
- umbral de la métrica
 - establecer 46
- UNIX, sistema operativo
 - imprimir 111
- URI de descubrimiento de colaboración
 - configurar 107
- uso de memoria caché
 - Query Service 178
- usuarios 207

- usuarios (*continuación*)
 - anónimos 243
 - autenticados 243
 - cambiar perfiles 324
 - clases y permisos 214
 - diagnóstico de un problema para usuarios específicos 25
 - entornos locales 208
 - IBM Cognos Series 7 207
 - perfiles 323
 - seguridad 207
 - suprimir perfiles 325
 - suprimir y volver a crear 207

V

- valor de límite de regulador
 - tamaños de informe para el servicio de datos de informes 90
- valores avanzados
 - configuración 513
 - establecer globalmente 513
 - establecer para asignadores 514
 - establecer para servicios 515
 - servicio de Mobile 408
- valores de afinidad 80
- valores de agrupación de conexiones
 - base de datos de Content Manager 67
- valores de configuración del servidor 411
- valores de documentos periódicos 88
- valores de pasaporte CAM
 - tiempo de espera 431
- valores de RSVP.PROMPT.RECONCILIATION 96
- valores de seguridad iniciales 243
- valores predeterminados
 - idiomas de informes 366
 - Informes de PowerPlay 369
 - perfiles de usuario 323
 - servicio 54
 - valores de solicitud de informe 367

- variable de sesión 155
- verificación de consistencia del almacén de contenidos
 - arrendamiento múltiple 353
- versiones
 - desplegar salida de informe 294
- versiones de salida de informe
 - conservar 367
- vida útil
 - archivos de sesión de usuario 70
 - tareas humanas y anotaciones terminadas 109
- visita
 - permisos 213
- vistas
 - informe 362
- visualizaciones
 - despliegue 305
 - establecer propiedades y acceder a los permisos 359
 - IBM Cognos Analytics Community 357
 - importar 358
 - suprimir 359
 - ver permisos 359
- visualizar
 - monedas mixtas 361

W

- web de Planning, servicio 52

X

- XML
 - Orígenes de datos 144

Z

- zonas activas, limitar 89