PUBLIC (PÚBLICO)

Plataforma SAP BusinessObjects Business Intelligence

Versión del documento: 4.3 Support Package 4 – 2023-12-07

# Manual del administrador de la plataforma Business Intelligence

© 2024 SAP SE o una empresa filial de SAP. Reservados todos los derechos.

THE BEST RUN SAP

# Contenido


**1 Historial de documentos. . . . . 21**

**2 Primeros pasos. . . . . 23**

2.1 Acerca de este manual. . . . . 23

Usuarios de este manual. . . . . 23

Acerca de la plataforma de Business Intelligence. . . . . 23

Variables. . . . . 24

Terminología. . . . . 24

2.2 Antes de comenzar. . . . . 26

Conceptos clave. . . . . 26

Herramientas administrativas clave. . . . . 29

Tareas clave. . . . . 32

**3 Arquitectura. . . . . 35**

3.1 Información general de la arquitectura. . . . . 35

Diagrama de componentes. . . . . 36

Niveles de arquitectura. . . . . 37

Bases de datos. . . . . 38

Servidores, hosts, y clústeres. . . . . 39

Servidores de aplicaciones Web. . . . . 40

Kits de desarrollo de software. . . . . 45

Fuentes de datos. . . . . 47

Autenticación e inicio de sesión único. . . . . 47

Integración de SAP. . . . . 49

Control de versiones integrado. . . . . 50

3.2 Servidores, servicios, nodos y hosts. . . . . 50

Cambios del servidor desde XI 3.1. . . . . 52

Servicios. . . . . 55

Categorías de servicio. . . . . 61

Tipos de servidor. . . . . 64

Servidores. . . . . 69

3.3 Aplicaciones cliente. . . . . 70

Instalado con las herramientas de cliente de la plataforma SAP BusinessObjects Business Intelligence. . . . . 71

Instalado con la plataforma SAP BusinessObjects Business Intelligence. . . . . 74

Disponible por separado. . . . . 75

Clientes de las aplicaciones Web. . . . . 76

3.4 Flujos de trabajo de procesos. . . . . 78
Inicio y autenticación. . . . . 79
Objetos de programa. . . . . 80
Crystal Reports. . . . . 82
Web Intelligence. . . . . 86
Análisis. . . . . 88
3.5 Integración con la plataforma de lanzamiento de SAP Fiori en SAP Enterprise Portal. . . . . 89

**4 Asistente de configuración del sistema. . . . . 91**
4.1 Introducción al Asistente de configuración del sistema. . . . . 91
4.2 Especificar los productos que utiliza. . . . . 91
4.3 Elección de una plantilla de despliegue. . . . . 93
4.4 Especificar ubicaciones de carpetas de datos. . . . . 95
4.5 Revisar los cambios. . . . . 96
4.6 Archivos de registro y archivos de respuesta. . . . . 97
Uso de un archivo de respuesta. . . . . 97

**5 Administración de licencias. . . . . 101**
5.1 Administrar claves de licencia. . . . . 101
Para ver la información de licencia. . . . . 101
Para agregar una clave de licencia. . . . . 101
Para ver la actividad actual de las cuentas:. . . . . 102

**6 Administrar usuarios y grupos. . . . . 103**
6.1 Información general de administración de cuentas. . . . . 103
Administración de usuarios. . . . . 103
Administración de grupos. . . . . 104
Tipos de autenticación disponibles. . . . . 105
6.2 Administración de cuentas Enterprise y generales. . . . . 106
Para crear una cuenta de usuario. . . . . 106
Para modificar una cuenta de usuario. . . . . 107
Para eliminar una cuenta de usuario. . . . . 108
Para crear un nuevo grupo. . . . . 109
Para modificar las propiedades de un grupo. . . . . 109
Para ver miembros de grupo. . . . . 109
Para agregar subgrupos. . . . . 110
Para especificar la pertenencia al grupo. . . . . 110
Para eliminar un grupo. . . . . 111
Agregar usuarios o grupos de usuarios en masa. . . . . 111
Para habilitar la cuenta de invitado. . . . . 112
Adición de usuarios a grupos. . . . . 112
Cambio de la configuración de la contraseña. . . . . 114

Concesión de acceso a usuarios y grupos. . . . 116
Control del acceso a las bandejas de entrada de usuario. . . . 116
Configurar las opciones de la plataforma de lanzamiento de BI de Fiori. . . . 116
Administrar atributos para usuarios del sistema . . . . 120
Priorización de atributos de usuario en varias opciones de autenticación. . . . 121
Agregar un nuevo atributo de usuario. . . . 121
Editar los atributos de usuario personalizados. . . . 123
6.3 Administración de alias. . . . 123
Para crear un usuario y agregar un alias de terceros. . . . 123
Para crear un nuevo alias para un usuario existente. . . . 124
Para asignar un alias desde otro usuario. . . . 125
Para eliminar un alias. . . . 125
Para desactivar un alias. . . . 126

**7 Establecimiento de derechos. . . . 127**
7.1 Cómo funcionan los derechos en la Plataforma de BI. . . . 127
Niveles de acceso. . . . 127
Configuración de derechos avanzados. . . . 128
Herencia. . . . 129
Derechos específicos del tipo. . . . 134
Determinación de los derechos efectivos. . . . 135
7.2 Administración de la configuración de seguridad para los objetos en la CMC. . . . 136
Para ver los derechos de un principal en un objeto. . . . 136
Para asignar principales a una lista de control de acceso para un objeto. . . . 137
Para modificar la seguridad de un principal en un objeto. . . . 137
Establecer derechos en una carpeta de nivel superior en la plataforma de BI. . . . 138
Comprobación de la configuración de seguridad de un principal. . . . 139
7.3 Uso de niveles de acceso. . . . 141
Elección entre los niveles de acceso *Ver* y *Ver a petición*. . . . 143
Para copiar un nivel de acceso existente. . . . 144
Para crear un nivel de acceso. . . . 144
Para cambiar el nombre de un nivel de acceso. . . . 145
Para eliminar un nivel de acceso. . . . 145
Para modificar los derechos en un nivel de acceso. . . . 145
Seguimiento de la relación entre los niveles de acceso y los objetos. . . . 146
Administración de los niveles de acceso entre sitios. . . . 147
7.4 Interrupción de la herencia. . . . 148
Para desactivar la herencia. . . . 149
7.5 Uso de derechos para la administración delegada. . . . 150
Elegir entre las opciones «*Modificar los derechos de los usuarios para los objetos*» . . . . 151
Derechos de propietario. . . . 153
7.6 Resumen de recomendaciones para la administración de derechos. . . . 153

**8 Protección de la plataforma de BI. . . . . 154**
8.1 Información general de seguridad . . . . . 154
8.2 Uso seguro de objetos de programa. . . . . 154
8.3 Planificación de recuperación tras desastres. . . . . 155
8.4 Recomendaciones generales para proteger el despliegue. . . . . 156
8.5 Configuración de la seguridad para servidores de terceros en paquetes. . . . . 157
8.6 Relación de confianza activa. . . . . 157
Tokens de inicio de sesión. . . . . 157
Mecanismo de vales para seguridad distribuida. . . . . 158
8.7 Sesiones y seguimiento de sesiones. . . . . 159
Seguimiento de sesiones CMS. . . . . 159
Administración de sesiones. . . . . 160
Script para borrar sesiones obsoletas. . . . . 161
8.8 Protección de entornos. . . . . 161
De explorador Web a servidor Web. . . . . 162
Servidor Web en la Plataforma de BI. . . . . 162
Protección frente a intentos de conexión malintencionados. . . . . 162
Restricciones para las contraseñas. . . . . 163
Restricciones de conexión. . . . . 163
Restricciones para los usuarios. . . . . 163
Restricciones de la cuenta Invitado. . . . . 164
8.9 Auditoría de modificaciones de configuración de seguridad . . . . . 164
8.10 Procesamiento de extensiones. . . . . 164
8.11 Interfase de búsqueda de virus. . . . . 165
Habilitar la búsqueda de virus. . . . . 165
8.12 Seguridad de datos de la plataforma de BI. . . . . 166
Modos de seguridad de procesamiento de datos. . . . . 166
Cuentas de administrador. . . . . 168
Derechos de conexión. . . . . 169
8.13 Criptografía en la plataforma de BI. . . . . 170
Trabajar con claves de clúster. . . . . 170
Oficiales criptográficos. . . . . 172
Administrar claves criptográficas en la CMC. . . . . 174
8.14 Protección de datos y privacidad. . . . . 178
Glosario. . . . . 178
Consentimiento del usuario. . . . . 180
Informe de información. . . . . 181
Registro de acceso de lectura. . . . . 181
Supresión de datos personales. . . . . 181
Log de modificaciones. . . . . 183
8.15 Configuración de servidores backend para SSL. . . . . 183

Para crear el archivo de configuración predeterminada. . . . . 184
Crear archivos de clave y de certificado. . . . . 185
Configurar SSL cuando el certificado lo administra una autoridad de certificados. . . . . .187
Configurar el protocolo SSL. . . . . 189
8.16 Comprender la comunicación entre los componentes de la Plataforma de BI. . . . . 193
Introducción a los servidores y los puertos de comunicación de la Plataforma de BI. . . . . 194
Comunicación entre los componentes de la Plataforma de BI . . . . . 196
8.17 Configuración de la plataforma de BI para los servidores de seguridad. . . . . .208
Para configurar el sistema para servidores de seguridad. . . . . 208
Depurar un despliegue con cortafuegos. . . . . 211
8.18 Ejemplos de escenarios normales de servidores de seguridad. . . . . 213
Ejemplo: Nivel de aplicación implementado en una red aparte. . . . . 213
Ejemplo: cliente grueso y nivel de base de datos separados de los servidores de la Plataforma de BI por un servidor de seguridad. . . . . .216
8.19 Configuración del servidor de seguridad para entornos integrados. . . . . .218
Información general específica del servidor de seguridad para la integración de SAP. . . . . 219
Configuración del servidor de seguridad para la integración de JD Edwards EnterpriseOne . . . . . 220
Directrices específicas del servidor de seguridad para Oracle EBS. . . . . 222
Configuración del servidor de seguridad para la integración de PeopleSoft Enterprise. . . . . 223
Configuración del servidor de seguridad para la integración de Siebel. . . . . .224
8.20 Plataforma de BI y servidores proxy inversos . . . . . 226
Comprender el modo en que se despliegan las aplicaciones Web. . . . . 226
8.21 Configuración de servidores proxy inversos para las aplicaciones Web de la Plataforma de BI. . . . . .226
Instrucciones detalladas para configurar servidores proxy inversos. . . . . .227
Para configurar el servidor proxy inverso. . . . . 228
Configurar el servidor proxy inverso de Apache 2.2 para la plataforma de BI . . . . . 228
Para configurar el servidor proxy inverso de WebSEAL 6.0 para la plataforma de BI . . . . . 228
Configurar Microsoft ISA 2006 para la plataforma de BI . . . . . 229
8.22 Configuración especial para la plataforma de BI en despliegues de proxy inverso. . . . . .231
Habilitar el proxy inverso para los servicios Web. . . . . 231
Activar la ruta raíz para las cookies de sesión para ISA 2006. . . . . 234
Habilitar proxy inverso para SAP BusinessObjects Live Office. . . . . .236

**9 Autenticación. . . . . 237**
9.1 Opciones de autenticación en la plataforma de BI. . . . . .237
Autenticación principal. . . . . .237
Complementos de seguridad. . . . . 238
Inicio de sesión único en la plataforma de BI. . . . . .239
9.2 Autenticación Enterprise. . . . . 242
Información general de la autenticación Enterprise. . . . . 242
Configuración de la autenticación Enterprise. . . . . 242

Cambiar la configuración de Enterprise. . . . 244
Autenticación SAML 2.0. . . . 245
Establecer una autenticación de confianza entre el servidor de aplicaciones de SAP NetWeaver SAP NetWeaver Java y la plataforma de BI. . . . 258
Para utilizar la autenticación SAML 2.0 con el servidor de aplicaciones Java de SAP NetWeaver . . . 262
Habilitación de la autenticación de confianza. . . . 262
Configuración de la autenticación de confianza para la aplicación Web. . . . 265
9.3 Autenticación LDAP. . . . 274
Uso de la autenticación LDAP. . . . 274
Configuración de la autenticación LDAP. . . . 276
Asignar grupos LDAP. . . . 287
9.4 Autenticación de Windows AD. . . . 298
Uso de la autenticación de Windows AD. . . . 298
Preparación del Controlador de dominio. . . . 299
Configuración de la autenticación de AD en la Consola de administración central (CMC). . . . 300
Configuración del servicio de la plataforma de BI para ejecutar el SIA. . . . 308
Configuración del servidor de aplicaciones Web para la autenticación de AD. . . . 310
Configuración del inicio de sesión único. . . . 319
Resolución de problemas de la autenticación de Windows AD. . . . 336
9.5 Autenticación de SAP. . . . 338
Configurar la autenticación SAP . . . 338
Creación de una cuenta de usuario para la plataforma de BI. . . . 339
Conectar a sistemas de derechos de SAP. . . . 340
Establecer opciones de autenticación SAP. . . . 342
Importación de funciones de SAP. . . . 346
Configuración de la Comunicación de red segura (SNC). . . . 349
Configuración del inicio de sesión único en el sistema de SAP. . . . 363
Configurar el SSO para SAP Crystal Reports y SAP Netweaver. . . . 367
9.6 Autenticación de PeopleSoft. . . . 369
Información general. . . . 369
Habilitar la autenticación de PeopleSoft Enterprise. . . . 369
Asignar funciones de PeopleSoft a la plataforma de BI. . . . 370
Programación de actualizaciones de usuario. . . . 373
Uso del puente de seguridad de PeopleSoft. . . . 374
9.7 Autenticación de JD Edwards. . . . 384
Introducción. . . . 384
Habilitar la autenticación de JD Edwards EnterpriseOne. . . . 384
Asignar funciones de JD Edwards EnterpriseOne a la plataforma de BI. . . . 385
Programación de actualizaciones de usuario. . . . 387
9.8 Autenticación de Siebel. . . . 389

Habilitar la autenticación de Siebel. . . . 389
Asignar funciones a la plataforma de BI. . . . 389
Programación de actualizaciones de usuario. . . . 392
9.9 Autenticación de Oracle EBS. . . . 394
Habilitar la autenticación de Oracle EBS. . . . 394
Asignar funciones de Oracle E-Business Suite a la plataforma de BI. . . . 395
Desasignar funciones . . . 399
Personalizar derechos para los grupos y usuario de Oracle EBS asignados . . . 400
Configurar el inicio de sesión único (SSO) para SAP Crystal Reports y Oracle EBS. . . . 401
9.10 Autenticación X.509. . . . 402
Autenticación X.509 para plataforma de lanzamiento de BI. . . . 402
X.509 Autenticación para servicios Web. . . . 410
Autenticación X.509 para CMC. . . . 413
9.11 Autenticación de OpenID Connect. . . . 416
Habilitar autenticación OpenID Connect. . . . 416

**10 Referencia a origen de datos:. . . . 417**
10.1 Asignación de credenciales mejorada. . . . 417
Crear una referencia de fuente de datos. . . . 418
Definir las credenciales de la base de datos para una referencia de fuente de datos para un usuario en CMC. . . . 419
Definir las credenciales de la base de datos para una referencia de fuente de datos para un usuario en la rampa de lanzamiento BI. . . . 419
Definir las credenciales de la base de datos para una referencia de fuente de datos para un grupo. . . . 420
Asociar referencia de fuente de datos en conexión OLAP. . . . 420

**11 Administración del servidor. . . . 422**
11.1 Uso del área de administración Servidores de la CMC. . . . 422
11.2 Administrar servidores con el uso de secuencias de comandos en Windows . . . 425
11.3 Administración de servidores en Unix . . . 425
11.4 Visualizar y cambiar el estado del servidor. . . . 425
Visualizar el estado de servidores. . . . 425
Iniciar, detener y reiniciar servidores. . . . 427
Detener un Servidor de administración central (CMS). . . . 429
Habilitar y deshabilitar servidores. . . . 430
11.5 Agregar, clonar o eliminar servidores. . . . 431
Adición, clonación y eliminación de servidores. . . . 431
11.6 Agregar cabeceras de internet personalizadas. . . . 434
11.7 Agrupar Servidores de administración central. . . . 435
Agrupar Servidores de administración central. . . . 435
11.8 Administración de grupos de servidores. . . . 439
Creación de un grupo de servidores. . . . 440

Convertir un grupo de servidores exclusivo en grupo de servidores no exclusivo y a la inversa . . . 442
Trabajo con subgrupos de servidores. . . . 444
Modificación de la pertenencia a grupos de un servidor. . . . 445
Acceso administrativo a servidores y grupos de servidores para usuarios. . . . 446
Asignación de un grupo de usuarios a un grupo de servidores. . . . 448
Asignación de una carpeta a un grupo de servidores. . . . 451
Comprender la gestión de los derechos del grupo de servidores. . . . 453
11.9 Configurar servidores de procesamiento de Adaptive para sistemas de producción. . . . 458
11.10 Evaluación del rendimiento del sistema. . . . 459
Supervisar servidores de la plataforma de BI. . . . 459
Análisis de las medidas del servidor. . . . 459
Ver las medidas del sistema. . . . 460
Registrar la actividad de los servidores. . . . 460
11.11 Configuración de las opciones de servidor. . . . 461
Para cambiar las propiedades de un servidor. . . . 462
Aplicar configuraciones de servicios a varios servidores. . . . 462
Trabajo con plantillas de configuración. . . . 463
11.12 Configuración de las opciones de red. . . . 465
Opciones de entorno de red. . . . 465
Opciones de identificación de host de servidor. . . . 466
Configurar un equipo multibase. . . . 468
Configurar los números de puerto. . . . 471
11.13 Administración de nodos. . . . 474
Uso de nodos. . . . 474
Adición de un nuevo nodo. . . . 476
Creación de nuevo de un nodo. . . . 481
Eliminación de un nodo. . . . 485
Cambiar el nombre de un nodo. . . . 487
Mover un nodo. . . . 489
Parámetros de la secuencia de comandos. . . . 493
Agregar dependencias del servidor de Windows. . . . 498
Cambiar la credenciales de usuario para un nodo. . . . 499
11.14 Cambio del nombre de un equipo en un despliegue de la plataforma de BI. . . . 499
Cambio de los nombres de clúster. . . . 499
Cambio de direcciones IP. . . . 500
Cambio del nombre de los equipos. . . . 501
11.15 Uso de bibliotecas de 32 bits y 64 bits de terceros con la plataforma de BI. . . . 505
11.16 Administrar marcadores de posición del servidor y del nodo. . . . 505
Ver los marcadores de posición de un servidor. . . . 505
Ver y editar los marcadores de posición de un nodo. . . . 506

**12 Administración de bases de datos del Servidor de administración central (CMS). . . . . 507**
12.1 Administrar las conexiones de la base de datos de sistema del CMS. . . . . 507
Para seleccionar SQL Anywhere como base de datos CMS. . . . . 507
Para seleccionar SAP HANA como base de datos de CMS. . . . . 508
12.2 Selección de una base de datos del CMS nueva o existente. . . . . 509
Para seleccionar una base de datos de CMS nueva o existente en Windows. . . . . 511
Para seleccionar una base de datos de CMS nueva o existente en UNIX. . . . . 511
12.3 Creación de nuevo de la base de datos del sistema de CMS. . . . . 512
Para volver a crear la base de datos de sistema de CMS en Windows. . . . . 512
Para volver a crear la base de datos de sistema de CMS en UNIX. . . . . 513
12.4 Copia de datos de una base de datos de sistema de CMS a otra. . . . . 514
Preparar la copia de una base de datos de sistema de CMS. . . . . 515
Para copiar una base de datos de sistema del CMS en Windows. . . . . 515
Para copiar datos de una base de datos del sistema del CMS en Unix. . . . . 516
12.5 Controlador de base de datos de servidor de administración central. . . . . 516

**13 Administración de servidores del contenedor de aplicaciones Web (WACS). . . . . 518**
13.1 WACS. . . . . 518
Servidor de contenedor de aplicación Web (WACS). . . . . 518
Agregar o eliminar WACS adicionales al despliegue. . . . . 520
Agregar o eliminar servicios de WACS. . . . . 524
Configurar HTTPS/SSL. . . . . 525
Métodos de autenticación admitidos. . . . . 529
Configurar AD Kerberos para WACS . . . . . 529
Configuración del inicio de sesión único de AD Kerberos . . . . . 537
Configurar servicios Web RESTful. . . . . 539
WACS y el entorno de TI. . . . . 549
Configurar propiedades de aplicaciones Web. . . . . 552
Solución de problemas. . . . . 553
Propiedades de WACS. . . . . 556

**14 Copia de seguridad y restauración del sistema. . . . . 558**
14.1 Presentación general de la copia de seguridad y de la restauración. . . . . 558
14.2 Terminología. . . . . 558
14.3 Usa mayúsculas o minúsculas para realizar copias de seguridad y restauraciones. . . . . 560
14.4 Copias de seguridad. . . . . 561
Copia de seguridad de todo el sistema. . . . . 562
Copia de seguridad de la configuración del servidor. . . . . 565
Copia de seguridad de contenido de BI. . . . . 568
14.5 Restaurar el sistema. . . . . 569
Restauración de todo el sistema. . . . . 569
Restauración de la configuración del servidor. . . . . 576

Restauración del contenido de BI. . . . . 579
14.6 Secuencias de comandos BackupCluster y RestoreCluster. . . . . 579

**15 Copia de su despliegue de la plataforma de BI. . . . . 583**
15.1 Información general de la copia del sistema. . . . . 583
15.2 Terminología. . . . . 583
15.3 Usa casos para la copia de sistemas. . . . . 584
15.4 Planificación de la copia del sistema. . . . . 584
15.5 Consideraciones y limitaciones. . . . . 586
15.6 Procedimiento de copia del sistema. . . . . 587
Exportar de un sistema de origen. . . . . 588
Importar a un sistema de destino. . . . . 592

**16 Administración de promociones. . . . . 595**
16.1 Bienvenido a la administración de promociones. . . . . 595
Resumen. . . . . 595
Características. . . . . 595
Derechos de acceso a la aplicación. . . . . 596
Soporte para WinAD en Administración de promociones. . . . . 597
16.2 Introducción a la herramienta de administración de promociones. . . . . 598
Acceder a la herramienta de administración de promociones. . . . . 598
Componentes de la interfaz de usuario. . . . . 598
Uso de la opción de configuración. . . . . 600
16.3 Usar la herramienta de administración de promociones. . . . . 608
Creación y eliminación de carpetas. . . . . 609
Crear una tarea. . . . . 610
Para crear una nueva tarea copiando una tarea existente. . . . . 612
Para buscar una tarea. . . . . 613
Para editar una tarea. . . . . 614
Para añadir un InfoObjeto a una tarea. . . . . 614
Para gestionar las dependencias de una tarea. . . . . 616
Para buscar dependientes. . . . . 617
Para promover una tarea cuando los repositorios están conectados. . . . . 617
Promover una tarea con un archivo LCMBIAR. . . . . 620
Para programar una promoción de tarea. . . . . 624
Para ver el historial de una tarea. . . . . 625
Para restaurar una tarea. . . . . 626
16.4 Promover contenido de repositorio completo con la herramienta de administración de promociones. . . . . 628
Preparar los sistemas de origen y destino. . . . . 629
Estrategias de migración. . . . . 630
16.5 Pasos de la promoción del sistema completo. . . . . 631

Promover usuarios y grupos de usuarios (tarea 1). . . . 632
Promover objetos dependientes (tarea 2). . . . 632
Promover objetos principales (tarea 3). . . . 634
Después de promoción. . . . 635
16.6 Usar la opción Línea de comandos. . . . 635
Para ejecutar la línea de comandos en Windows. . . . 635
Ejecutar la línea de comandos en Unix. . . . 636
Parámetros de la herramienta de línea de comandos . . . 637
Ejemplo de archivo de propiedades. . . . 660
16.7 Usar el Sistema de transporte y cambio mejorado. . . . 661
Requisitos previos. . . . 662
Para configurar la plataforma de BI y de la integración CTS+. . . . 662
Para promover una tarea usando CTS. . . . 669
16.8 Utilizar el asistente de gestión de promociones . . . 672
Para excluir objetos de la promoción. . . . 673
Cuándo utilizar el asistente de gestión de promociones. . . . 674
Escenario. . . . 675
Objetos. . . . 677
Dependencias. . . . 681
Resumen. . . . 681
(Opcional) Fichero de propiedades. . . . 682
Asistente de gestión de promociones en Linux. . . . 685

**17 Administración de versión. . . . 686**
17.1 Para administrar versiones distintas de un InfoObjeto. . . . 686
derechos de acceso a la aplicación de administración de versión. . . . 686
Realización de una copia de seguridad y restauración de archivos de subversión. . . . 687
17.2 Para administrar versiones distintas de recursos de BI. . . . 688
17.3 Iniciar y detener la subversión manualmente en Unix. . . . 690
17.4 Archivos requeridos para subversión en Solaris 10 y RedHat Linux 5. . . . 690
17.5 Para utilizar la subversión Apache como el sistema de administración de versión. . . . 691
17.6 Para utilizar Git como el sistema de administración de versión. . . . 691
17.7 Configuración del sistema de administración de versiones predeterminada. . . . 692
17.8 Comparar versiones distintas del mismo trabajo. . . . 693
17.9 Actualizar el contenido de subversión. . . . 694
17.10 Configurar subversión para servidores de tareas de procesamiento agrupadas. . . . 694
Opción A: Configurar el equipo de subversión antes de cualquier operación del sistema de administración de versiones. . . . 694
Opción B: Configurar la subversión después de que el sistema de administración de versiones cree un directorio de copia de trabajo. . . . 695
Configurar otros equipos de subversión. . . . 696

**18 Administración de aplicaciones. . . . 697**

18.1 Desactivar el mensaje emergente GDPR. . . . 697
18.2 Administrar aplicaciones mediante la CMC. . . . 699
Información general. . . . 699
Configuración común para aplicaciones. . . . 700
Configuración específica de la aplicación. . . . 701
18.3 Administración de aplicaciones mediante propiedades de la capa semántica. . . . 760
18.4 Administración de aplicaciones mediante las propiedades de BOE.war. . . . 761
El archivo BOE WAR. . . . 761
18.5 Personalizar los puntos de acceso de inicio de sesión de la plataforma de lanzamiento de BI y OpenDocument. . . . 779
Ubicaciones de la plataforma de lanzamiento de BI y OpenDocument. . . . 780
Definir una página de inicio de sesión personalizada. . . . 781
Agregar una autenticación de confianza al inicio de sesión. . . . 781
18.6 Personalización de interfaces de usuario de aplicación. . . . 782
Web Intelligence. . . . 783
Plataforma de lanzamiento de BI. . . . 789
18.7 Configurar los servicios Web RESTful de la plataforma de BI en el servidor Web.. . . . 790
18.8 Gestión híbrida de usuarios. . . . 793
18.9 Proporcionar SAP Analytics Cloud a los usuarios locales. . . . 794
Establecer conexión entre el sistema local y la nube. . . . 794
18.10 Crear credenciales de cliente OAuth en SAP Analytics Cloud. . . . 795
18.11 Configurar el sistema fuente. . . . 796
18.12 Configurar el sistema destino. . . . 797
18.13 Proporcionar SAP Analytics Cloud a sus usuarios y grupos de usuarios. . . . 798
18.14 Visualizar usuarios aprovisionados en SAP Analytics Cloud. . . . 798
18.15 Plantillas de muestra. . . . 799

**19 Administrar conexiones y universos. . . . 803**
19.1 Administrar conexiones. . . . 803
Para eliminar una conexión de universo. . . . 803
19.2 Administrar universos. . . . 804
Para eliminar universos. . . . 805

**20 BI Admin Studio. . . . 806**
20.1 Cockpit de administración. . . . 807
Cockpit de administración. . . . 807
BI en servidores. . . . 808
BI en instancias de documento. . . . 809
BI en usuarios y sesiones. . . . 810
BI en Utilización del contenido. . . . 810
BI en aplicaciones. . . . 811
20.2 Supervisión. . . . 811

Términos de supervisión. . . . . 812
Configurar la compatibilidad de la base de datos para la supervisión. . . . . 816
Propiedades de configuración. . . . . 824
Integración con otras aplicaciones. . . . . 831
Soporte de clúster para el servidor de supervisión. . . . . 831
Solución de problemas. . . . . 832
20.3 Diferencia visual. . . . . 835
Comparar objetos o archivos con diferencia visual. . . . . 836
Comparar objetos o archivos con el sistema de administración de versiones. . . . . 837
20.4 Autorización de elementos HTML. . . . . 838
Modificar la lista de elementos HTML autorizados. . . . . 840

**21 Reporting CMS. . . . . 841**
21.1 Reporting CMS. . . . . 841
La arquitectura de la plataforma SAP BusinessObjects. . . . . 841
La estructura de la base de datos del sistema CMS. . . . . 842
Acerca de InfoObjects. . . . . 844
21.2 Resumen de gestión de informes de CMS. . . . . 846
21.3 Conexión de la base de datos CMS. . . . . 847
21.4 Kit de ejemplo de la gestión de informes de CMS. . . . . 848
Importación del kit de ejemplo de gestión de informes de CMS con Gestión de promociones . . . . . 849
El universo de ejemplo de CMS . . . . . 850
Ampliación del universo de ejemplo de CMS. . . . . 850
21.5 Creación de un informe en el CMS. . . . . 850

**22 Asistente de workflow. . . . . 852**
22.1 Audiencia de destino. . . . . 853
22.2 Comprender la arquitectura. . . . . 853
22.3 Glosario. . . . . 854
22.4 Acerca de la instalación y la actualización. . . . . 857
22.5 Configurar el asistente de workflow. . . . . 858
Configuración básica. . . . . 858
22.6 Gestión de derechos del asistente de workflow mediante la Consola de administración central . . . . . 860
22.7 Trabajar con el asistente de workflow. . . . . 865
Acerca de las plantillas para tareas estándar. . . . . 865
Acerca de las plantillas de workflow estándar. . . . . 874
Acerca de las plantillas para tareas personalizadas. . . . . 875
Gestión de plantillas de workflow. . . . . 875
Gestión de escenarios y visualización de resultados. . . . . 877
Comprensión de los estados de las plantillas de tarea, plantillas de workflow y escenarios. . . . . 882

Trabajar con sistemas. . . . . 884
Flujo de proceso integral del asistente de workflow. . . . . 887
22.8 Verificación de archivos de log. . . . . 887

**23 Papelera de reciclaje. . . . . 889**
23.1 Papelera de reciclaje. . . . . 889
Restaurar un elemento de la Papelera de reciclaje. . . . . 889
Borrar permanentemente un elemento de la Papelera de reciclaje. . . . . 890
Habilitar limpieza automática de la Papelera de reciclaje. . . . . 890

**24 Auditoría. . . . . 892**
24.1 Introducción. . . . . 892
24.2 Página de auditoría de la CMC. . . . . 898
Estado de auditoría. . . . . 899
Configurar eventos de Auditoría. . . . . 900
Opciones de configuración de memoria de datos de auditoría. . . . . 904
24.3 Eventos de auditoría. . . . . 906
Audit events and details. . . . . 915

**25 Eventos. . . . . 937**
25.1 Acerca de Eventos. . . . . 937
Notificaciones de usuario. . . . . 938

**26 Búsqueda de plataforma. . . . . 942**
26.1 Información de Búsqueda de plataforma. . . . . 942
SDK de la Búsqueda de plataforma. . . . . 942
Entorno agrupado. . . . . 942
26.2 Configuración de la búsqueda de plataforma. . . . . 943
Desplegar OpenSearch. . . . . 943
Configuración del proxy inverso. . . . . 945
Configurar las propiedades de aplicaciones en la CMC. . . . . 945
26.3 Uso de la búsqueda de plataforma. . . . . 953
Indexación de contenido en el repositorio CMS. . . . . 953
Lista de errores de indexación. . . . . 954
Búsqueda de resultados. . . . . 955
26.4 Integración de Búsqueda de plataforma con la búsqueda de SAP NetWeaver Enterprise. . . . . 961
Creación de un conector en SAP NetWeaver Enterprise Search . . . . . 962
Importar una función de usuario en la plataforma de BI.. . . . . 962
26.5 Buscar desde SAP NetWeaver Enterprise Search. . . . . 963
26.6 Auditoría. . . . . 963
26.7 Solución de problemas. . . . . 965
Corrección automática. . . . . 965
Escenarios de problemas. . . . . 965

**27 Federación. . . . . 968**
27.1 Federación. . . . . 968
27.2 Términos de Federación. . . . . 969
27.3 Administrar derechos de seguridad. . . . . 971
Derechos necesarios en el sitio de origen. . . . . 971
Derechos necesarios en el sitio de destino. . . . . 972
Derechos específicos de Federación. . . . . 973
Réplica de la seguridad en un objeto. . . . . 974
Réplica de la seguridad mediante niveles de acceso. . . . . 974
27.4 Opciones de tipos y modos de réplica. . . . . 975
Réplica unidireccional . . . . . 975
Réplica bidireccional . . . . . 975
Actualizar a partir de origen o Actualizar a partir de destino. . . . . 976
27.5 Replicar usuarios y grupos de terceros. . . . . 977
27.6 Replicar universos y conexiones de universos. . . . . 979
27.7 Administración de listas de réplicas. . . . . 980
Creación de listas de réplicas. . . . . 981
Modificar listas de réplicas. . . . . 982
27.8 Administrar conexiones remotas. . . . . 983
Crear conexiones remotas. . . . . 984
Modificar conexiones remotas. . . . . 985
27.9 Administración de tareas de réplica. . . . . 986
Creación de tareas de réplica. . . . . 986
Programación de tareas de réplica. . . . . 988
Modificar las tareas de réplica. . . . . 989
Visualización de un registro después de una tarea de réplica. . . . . 989
27.10 Administración de la limpieza de objeto. . . . . 990
Cómo usar la limpieza de objetos. . . . . 990
Límites de la limpieza de objetos. . . . . 991
Frecuencia de la limpieza de objetos. . . . . 991
27.11 Administrar la detección y resolución de conflictos. . . . . 992
Resolución de conflictos de réplica unidireccional. . . . . 992
Resolución de conflictos de réplica bidireccional. . . . . 994
27.12 Uso de servicios Web en Federación. . . . . 997
Variables de sesión . . . . . 998
Memoria caché de archivos . . . . . 998
Despliegue personalizado . . . . . 999
27.13 Programación remota e instancias ejecutadas localmente. . . . . 1000
Programación remota. . . . . 1000
Instancias ejecutadas localmente. . . . . 1001
Uso compartido de instancias. . . . . 1002

27.14 Importar y promover contenido replicado. . . . . 1003
Importar contenido replicado. . . . . 1003
Importar contenido replicado y continuar la réplica . . . . . .1004
Promover contenido desde un entorno de prueba. . . . . 1004
Volver a dirigir un sitio de destino. . . . . .1005
27.15 Procedimientos recomendados. . . . . 1005
Limitaciones de la versión actual. . . . . .1009
Solución de problemas de mensajes de error. . . . . 1010

**28 Configuración suplementaria para entornos ERP. . . . . .1015**
28.1 Configuración para la integración de SAP NetWeaver. . . . . 1015
Integración con SAP Business Warehouse (BW). . . . . .1015
28.2 Configurar para la integración de JD Edwards. . . . . .1061
Configurar el inicio de sesión único (SSO) para SAP Crystal Reports. . . . . 1061
Configuración del Nivel de socket seguro para integraciones de JD Edwards. . . . . 1062
28.3 Configurar para la integración de PeopleSoft Enterprise. . . . . 1063
Configurar el inicio de sesión único (SSO) para SAP Crystal Reports y PeopleSoft Enterprise . . . . . 1063
Configuración de la comunicación de Capa de sockets seguros (SSL). . . . . .1064
Sintonización del rendimiento para sistemas de PeopleSoft. . . . . .1066
28.4 Configurar para la integración de Siebel. . . . . .1067
Configurar Siebel para la integración con la plataforma SAP BI. . . . . .1067
Crear el elemento de menú Crystal Reports. . . . . 1068
Conocimiento contextual. . . . . 1070
Configurar el inicio de sesión único (SSO) para SAP Crystal Reports y Siebel. . . . . 1072
Configuración de la comunicación de Capa de sockets seguros (SSL). . . . . 1072

**29 Administrar y configurar registros. . . . . .1075**
29.1 Registro de seguimientos para componentes. . . . . .1075
29.2 Niveles de registro de seguimiento. . . . . 1075
29.3 Configurar el seguimiento para los servidores. . . . . 1076
Configurar un nivel de registro en la CMC. . . . . 1077
Configurar el nivel de registro para varios servidores en la CMC. . . . . .1077
Para configurar el seguimiento del servidor mediante el archivo BO_trace.ini. . . . . 1078
29.4 Configurar el seguimiento para las aplicaciones Web. . . . . 1080
Para definir el nivel de registro de seguimiento de la aplicación Web en la CMC. . . . . .1081
Para configurar el seguimiento del servidor mediante el archivo `BO_trace.ini`. . . . . 1082
29.5 Configurar el seguimiento para las aplicaciones de cliente de la plataforma de BI. . . . . 1086
29.6 Configuración del seguimiento de mensajes de error ampliado. . . . . 1087
29.7 Para habilitar los archivos de registro de información de ampliación de mensajes de error. . . . . 1087

**30 Integración en SAP Solution Manager. . . . . .1089**
30.1 Información general de la integración. . . . . 1089

30.2 Lista de comprobación de la integración de SAP Solution Manager. . . . . 1089
30.3 Administrar el registro del directorio horizontal del sistema. . . . . .1090
Registro de la plataforma de BI en la infraestructura horizontal del sistema. . . . . 1090
¿Cuándo se desencadena el registro de SLD?. . . . . 1092
Limpieza SLD antes de instalaciones de patch. . . . . 1092
Iniciar sesión en la conectividad SLD . . . . . .1093
Nombre de host virtual. . . . . 1093
30.4 Administrar agentes de Solution Management Diagnostics. . . . . 1094
Información general de Solution Manager Diagnostics (SMD). . . . . .1094
Trabajar con agentes SMD. . . . . .1094
Cuenta de usuario SMAdmin. . . . . .1095
30.5 Administrar la instrumentación del rendimiento. . . . . .1096
Instrumentación del rendimiento para la plataforma de BI. . . . . 1096
Configurar la instrumentación del rendimiento para la plataforma de BI. . . . . 1096
Instrumentación del rendimientos para el nivel Web. . . . . .1097
Archivos de registro de instrumentación . . . . . 1098
30.6 Seguimiento con SAP Passport. . . . . 1098

**31 Administración de líneas de comandos. . . . . .1100**
31.1 Scripts de Unix. . . . . 1100
Utilidades de secuencia de comandos. . . . . 1100
Plantillas de secuencia de comandos. . . . . 1106
Secuencias de comandos usadas por la plataforma de BI. . . . . .1106
31.2 Secuencias de comandos de Windows. . . . . .1108
ccm.exe. . . . . .1108
31.3 Líneas de comandos de los servidores. . . . . 1111
Información general de las líneas de comandos. . . . . .1111
Opciones estándar para todos los servidores. . . . . 1112
Servidor de administración central. . . . . 1112
Servidor de procesamiento de Crystal Reports y servidor de caché de Crystal Reports. . . . . .1114
Servidores de tareas. . . . . 1115
Servidor de procesamiento de Adaptive. . . . . .1116
Servidor de aplicaciones de informes. . . . . 1116
Servidor de procesamiento de Web Intelligence. . . . . 1118
Servidores del repositorio de archivos de entrada y de salida. . . . . .1119
Servidor de eventos. . . . . .1121

**32 Herramienta de diagnóstico del repositorio. . . . . .1122**
32.1 Resumen de la herramienta de diagnóstico del repositorio. . . . . .1122
32.2 Uso de la herramienta de diagnóstico del repositorio. . . . . .1123
Para usar la herramienta de diagnóstico del repositorio. . . . . 1123
Parámetros de la Herramienta de diagnóstico del repositorio. . . . . 1124

32.3 Incoherencias entre el CMS y el FRS. . . . . 1133
32.4 Incoherencias en los metadatos de CMS. . . . . 1133
32.5 Gestionar SDK restaurado dentro de BOE WebApp. . . . . 1136

**33 Seguridad estricta de transporte HTTP (HSTS). . . . . 1138**
33.1 Configuración de HTTP Strict Transport Security (HSTS). . . . . 1138

**34 Apéndice de derechos. . . . . 1140**
34.1 Acerca del apéndice de derechos. . . . . 1140
34.2 Derechos generales. . . . . 1140
Derechos de destino. . . . . 1144
34.3 Derechos para tipos de objeto específicos. . . . . 1145
Derechos de carpeta. . . . . 1145
Categorías. . . . . 1145
Informes de Crystal. . . . . 1145
Documentos de Web Intelligence. . . . . 1146
Usuarios y grupos. . . . . 1147
Niveles de acceso. . . . . 1149
Derechos de universo (.unv). . . . . 1149
Derechos de universos (.unx). . . . . 1150
Niveles de acceso a objeto de universo. . . . . 1152
Derechos de conexión. . . . . 1153
Aplicaciones. . . . . 1154

**35 Apéndice de propiedades de servidor. . . . . 1163**
35.1 Acerca del apéndice de propiedades de servidor. . . . . 1163
Propiedades comunes de los servidores. . . . . 1163
Propiedades de servicios principales. . . . . 1165
Propiedades de los servicios de conectividad. . . . . 1176
Propiedades de los servicios de Crystal Reports. . . . . 1180
Propiedades de los servicios de análisis. . . . . 1189
Propiedades de los servicios de federación de datos. . . . . 1190
Propiedades de los servicios de Web Intelligence. . . . . 1190

**36 Apéndice de métricas de servidor. . . . . 1199**
36.1 Acerca del apéndice de métrica de servidor. . . . . 1199
Métricas de servidor común. . . . . 1199
Métricas del servidor de administración central. . . . . 1201
Métrica del servidor de conexión. . . . . 1204
Métricas del servidor de eventos. . . . . 1205
Métricas del servidor del repositorio de archivos. . . . . 1205
Métricas del servidor de procesamiento de Adaptive. . . . . 1206
Métricas del Servidor de contenedor de aplicación Web. . . . . 1211

Métricas del servidor de tareas de Adaptive. . . . . 1211
Métricas de Crystal Reports Server. . . . . .1213
Métricas del servidor de Web Intelligence. . . . . 1216

**37 Apéndice del marcador de posición del servidor y del nodo. . . . . .1218**
37.1 Marcadores de posición de servidor y nodo. . . . . 1218

**38 Apéndice del esquema del almacén de datos de auditoría. . . . . .1227**
38.1 Información general. . . . . .1227
38.2 Diagrama del esquema. . . . . .1227
38.3 Auditing Data Store Tables. . . . . 1227

**39 Apéndice del esquema de base de datos de supervisión. . . . . 1235**
39.1 Esquema de base de datos de tendencias. . . . . 1235

**40 Apéndice de la hoja de cálculo de copia del sistema. . . . . 1238**
40.1 Hoja de cálculo de copia del sistema. . . . . 1238

# 1 Historial de documentos

En la siguiente tabla se ofrece información general sobre los cambios más importantes del documento.

| Versión | Fecha | Descripción |
|---|---|---|
| Plataforma SAP BusinessObjects Business Intelligence 4.3 SP3 | Diciembre de 2022 | Se han actualizado los siguientes temas con el nuevo campo de longitud máxima de contraseña para la autenticación empresarial:<br>• Configuración de la autenticación Enterprise [página 242]<br>• Para crear una cuenta de usuario [página 106]<br>• Cambiar la configuración de contraseña general [página 115]<br>• Cambiar la configuración de contraseña general [página 244]<br>• Se ha introducido la opción activar Utilizar vía de acceso de URL relativa para utilizar la URL relativa del navegador. |
| Plataforma de SAP BusinessObjects Business Intelligence 4.3 SP2 | Diciembre de 2021 | Agregado Configuración del servidor de autorizaciones [página 755].<br>Actualizado Personalizar los elementos de interfaz de Web Intelligence por grupos de usuario y carpetas [página 783]. |
| Plataforma de SAP BusinessObjects Business Intelligence 4.3 SP1 | Diciembre de 2020 | • Se han agregado los siguientes temas nuevos:<br>  • un tema sobre la personalización de la IU de Web Intelligence. Consulte Personalizar los elementos de interfaz de Web Intelligence por grupos de usuario y carpetas [página 783].<br>  • Script para borrar sesiones obsoletas [página 161].<br>  • Definir las credenciales de la base de datos para una referencia de fuente de datos para un usuario en la rampa de lanzamiento BI [página 419]<br>  • Configuración SSL JMX [página 828]<br>• Se han actualizado dos temas:<br>  • Actualizar rutas [página 30].<br>  • Derechos de destino [página 1144] para *Opciones de destino* y *Propiedades de destino de correo electrónico* con el campo recién introducido *Responder a* para todos los escenarios de publicación. |

| Versión | Fecha | Descripción |
| --- | --- | --- |
| Plataforma de SAP BusinessObjects Business Intelligence 4.3 | Junio de 2020 | • SAP BusinessObjects Explorer, SAP BusinessObjects Dashboards, Herramienta de conversión de informes, Herramienta de administración de actualizaciones y Widgets de BI se han quedado obsoletos en la versión 4.3.<br>• Se ha añadido un tema nuevo Asistente de workflow [página 852]. |

# 2 Primeros pasos

## 2.1 Acerca de este manual

Este manual le proporciona información y procedimientos para desplegar y configurar la plataforma SAP BusinessObjects Business Intelligence (la «plataforma de BI»). Se proporcionan procedimientos para las tareas habituales. Para todos los temas avanzados se proporciona información conceptual y detalles técnicos.

Para obtener información sobre la instalación de este producto, consulte el *Manual de instalación de la plataforma SAP BusinessObjects Business Intelligence*.

### 2.1.1 Usuarios de este manual

Este manual trata el despliegue y la configuración de la plataforma de BI. Recomendamos que consulte este manual si realiza cualquiera de las siguientes tareas:

- Planificar el primer despliegue
- Configurar el primer despliegue
- Hacer cambios significativos en la arquitectura de un despliegue existente
- Mejorar el rendimiento del sistema

Este manual está dirigido a los administradores del sistema encargados de la configuración, administración y mantenimiento de una instalación de la plataforma de BI. El conocimiento del sistema operativo y del entorno de red resulta muy útil, ya que significa una comprensión general de la administración de servidores de aplicaciones Web y de las tecnologías de secuencias de comandos. Sin embargo, para abarcar todos los niveles de experiencia administrativa, en este manual se pretende ofrecer suficiente información básica y conceptual para clarificar todas las tareas y funciones administrativas.

### 2.1.2 Acerca de la plataforma de Business Intelligence

La plataforma de Business Intelligence (BI) es una solución flexible y escalable para enviar información a usuarios finales, de múltiples formas, incluidos los cuadros de mandos y los informes interactivos, a través de cualquier aplicación Web: Intranet, extranet, Internet o portal corporativo.

La plataforma ofrece ventajas tangibles que se extienden por toda la organización, en forma de suite integrada para la generación de informes, el análisis y la entrega de información.

También ofrece una solución para aumentar la productividad de los usuarios finales y reducir los esfuerzos administrativos.

Por ejemplo, se utiliza para distribuir informes de ventas semanales, para proporcionar a los clientes ofertas de servicios personalizadas o para integrar información crítica en portales corporativos.

## 2.1.3 Variables

En este manual se usan las siguientes variables.

| Variable | Descripción |
| --- | --- |
| `<INSTALLDIR >` | El directorio en el que está instalada la Plataforma de BI.<br>En Windows, el directorio predeterminado es `C:\Archivos de programa (x86)\SAP BusinessObjects\`. |
| `<PLATFORM64DIR>` | El nombre del sistema operativo de Unix. Los valores aceptables son:<br>• aix_rs6000_64<br>• linux_x64<br>• solaris_sparcv9<br>• hpux_ia64 |
| `<SCRIPTDIR>` | El directorio en el que se encuentran las secuencias de comandos para la administración de la plataforma de BI.<br>En un equipo Windows, el directorio es `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.<br>En Unix, el directorio es `<DIRINSTAL>/sap_bobj/enterprise_xi40/<PLATFORM64DIR>/scripts`. |

## 2.1.4 Terminología

Los siguientes términos se utilizan en la documentación de la plataforma de BI:

| Término | Definición |
| --- | --- |
| productos de add-on | Productos que funcionan con la plataforma de BI pero que tienen su propio programa de instalación. |
| Almacén de datos de auditoría (ADS) | La base de datos utilizada para almacenar los datos de auditoría |
| Plataforma de BI | Abreviatura de la plataforma SAP BusinessObjects Business Intelligence |
| Base de datos empaquetada; servidor de aplicaciones Web empaquetado | La base de datos o servidor de aplicación Web enviada con la plataforma de BI. |

| Término | Definición |
| --- | --- |
| Clúster (nombre) | Dos o más Servidores de administración central (CMS) que trabajan conjuntamente y usan una única base de datos de CMS. |
| Clusterizar (verbo) | Crear un clúster:<br>1. Instale un CMS y una base de datos del CMS en el equipo A.<br>2. Instale un CMS en el equipo B.<br>3. Apunte el CMS del equipo B a la base de datos del CMS del equipo A. |
| Clave de clúster | Usado para descifrar las claves en la base de datos del CMS.<br>Puede modificar la clave de clúster mediante el CCM, pero no puede reinicializarla como una contraseña. Contiene contenido cifrado y es muy importante no perderla. |
| CMS | Abreviatura del Servidor de administración central |
| Base de datos del CMS | La base de datos usada por el CMS para almacenar información acerca de la plataforma de BI. |
| Despliegue | El software de la plataforma de BI instalado, configurado y que se ejecuta en uno o más equipos. |
| Instalación | Una instancia de los archivos la plataforma de BI creada por el programa de instalación en un equipo. |
| Equipo | Ordenador en el que está instalada la plataforma de BI |
| Versión principal | Una versión completa del software |
| Versión menor | Una versión de varios componentes del software |
| Nodo | Un grupo de servidores de la plataforma de BI que se ejecuta en el mismo equipo y que el mismo Agente de inteligencia de servidor (SIA) se encarga de gestionar |
| Revisión | Una pequeña actualización para una versión específica de un Support Package |
| Promoción | El proceso de transferir contenido de BI entre despliegues con la misma versión principal (p. ej. de 4.3 a 4.3) mediante la aplicación de administración de promociones |
| Servidor | Un proceso de plataforma de BI. Un servidor aloja uno o más servicios. |

| Término | Definición |
| --- | --- |
| Server Intelligence Agent (SIA) | Un proceso que gestiona un grupo de servidores, incluidos los servidores de parada, inicio y reinicio |
| Paquete de soporte técnico | Una actualización de software para un release principal o menor |
| Servidor de aplicaciones Web | Un servidor que procesa contenido dinámico |
| Actualización | Los procesos de planificación, preparación, migración y procesos posteriores que se requieren para completar un proceso de migración |
| Instalador ONE | El instalador ONE es un único paquete de instalación que admite varios escenarios de instalación de BI, como instalación nueva o revisión de un paquete de servicios, cualquier revisión o actualización de la revisión, o cualquier paquete de servicios para la actualización de revisión. |

## 2.2 Antes de comenzar

### 2.2.1 Conceptos clave

#### 2.2.1.1 Server Intelligence

Inteligencia de servidor es un componente central de la plataforma de BI. Los cambios que se realizan en los procesos de servidor y que se aplican en la Consola de administración central (CMC) el Servidor de administración central (CMS) los propaga a los objetos de servidor correspondientes. El Agente de inteligencia de servidor (SIA) se usa para reiniciar o apagar automáticamente un servidor cuando se encuentre una condición inesperada y el administrador accede a él al gestionar nodos.

El CMS almacena información sobre servidores en la base de datos del sistema CMS para poder restablecer fácilmente los parámetros predeterminados de servidor. Puesto que el SIA realiza consultas periódicas al CMS para obtener información sobre los servidores que gestiona, el SIA sabe en qué estado deberían estar los servidores y cuándo tomar medidas.

> **Nota**
>
> Una instalación de la plataforma de BI es una instancia única de archivos de la plataforma de BI creada por el instalador en un equipo. Una instancia de la instalación de la plataforma de BI se puede usar solo en un clúster individual. Los nodos que pertenecen a distintos clústeres que comparten la misma instalación de la plataforma de BI no se soportan porque este tipo de despliegue no se puede revisar o actualizar. Solo las plataformas Unix admiten varias instalaciones del software en el mismo equipo. Si cada instalación se

> lleva a cabo en una cuenta de usuario única y se instala en una carpeta independiente, las instalaciones no compartirán ningún archivo. Recuerde que todos los equipos del clúster deben tener la misma versión y el mismo nivel de revisión.

### Información relacionada

Servidores, hosts, y clústeres [página 39]

## 2.2.1.2 Servidores, servicios, nodos y hosts

La plataforma de BI usa los términos servidor y servicio para hacer referencia a los dos tipos de software que se ejecutan en un equipo de la plataforma de BI.

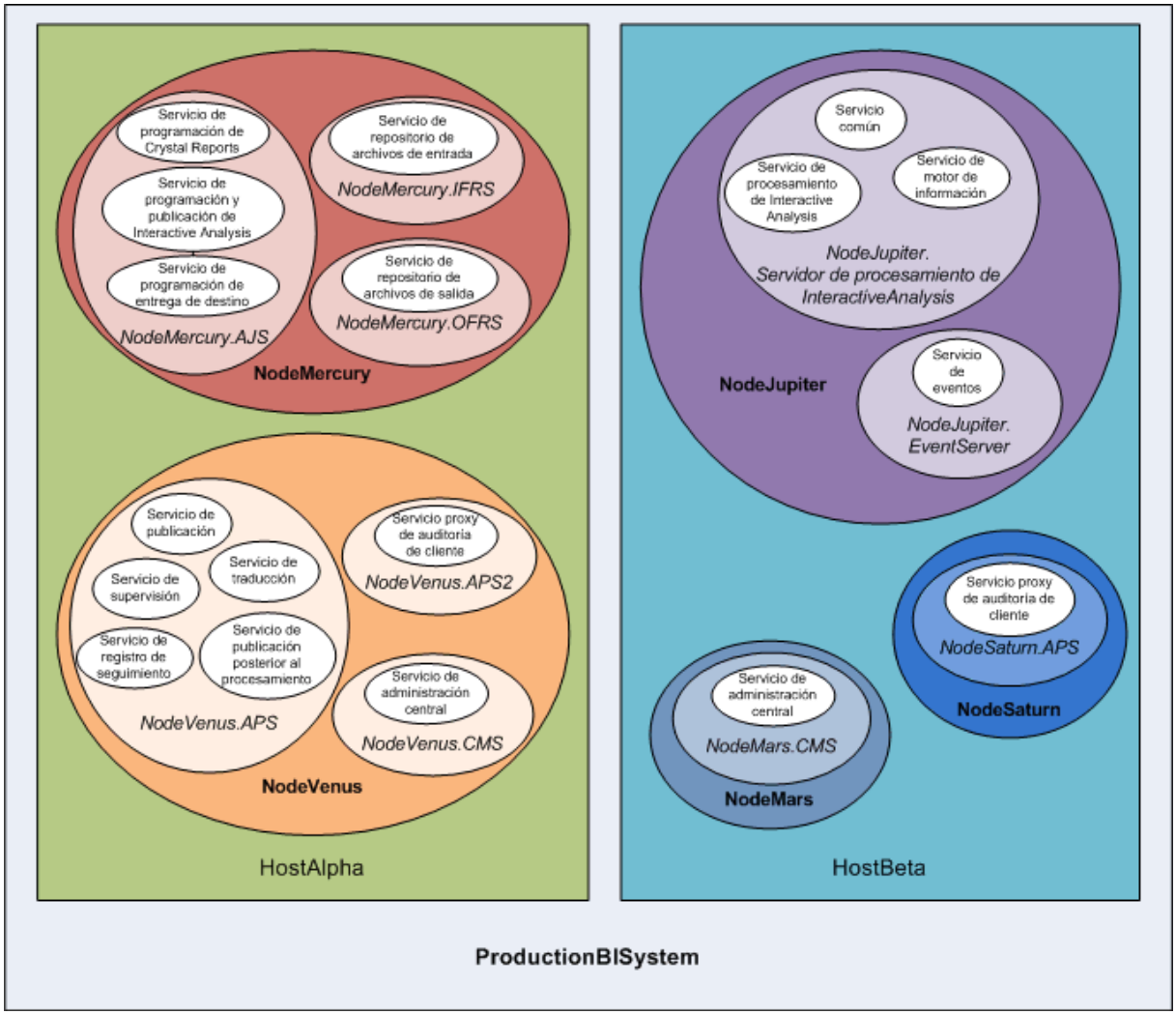
El término «servidor» se usa para describir un proceso de nivel del sistema operativo (en algunos sistemas se conoce como demonio) que aloja uno o varios servicios. Por ejemplo, el Servidor de administración central (CMS) y el Servidor de procesamiento de Adaptive son servidores. Un servidor se ejecuta en una cuenta específica del sistema operativo y tiene su propio ID de proceso (PID).

Un servicio es un subsistema de servidor que realiza una función específica. El servicio se ejecuta en el espacio de memoria de su servidor con el ID de proceso del contenedor principal (servidor). Por ejemplo, el servicio de programación de Web Intelligence es un subsistema que se ejecuta dentro del servidor de tareas de Adaptive.

Un nodo es una colección de servidores de la plataforma de BI que se ejecutan en el mismo host y los gestiona un solo Agente de inteligencia de servidor (SIA). Uno o varios nodos pueden estar en un solo host.

La plataforma de BI se puede instalar en un equipo, se puede distribuir en varios equipos de una intranet o se puede separar en una red de área extensa (WAN).

El siguiente diagrama muestra una instalación hipotética de la plataforma de BI. El número de hosts, nodos, servidores y servicios, así como el tipo de servidores y servicios, variará en instalaciones reales.




Dos hosts del clúster llamado ProductionBISystem:

- El host denominado HostAlpha tiene instalada la plataforma de BI y está configurado para disponer de dos nodos:
  - NodeMercury contiene un servidor de tareas de Adaptive (`NodeMercury.AJS`) con servicios para programar y publicar informes, un Servidor del repositorio de archivos de entrada (`NodeMercury.IFRS`) con un servicio para almacenar informes de entrada y un Servicio del repositorio de archivos de salida (`NodeMercury.OFRS`) con un servicio para almacenar la salida de informes.
  - NodeVenus contiene un servidor de procesamiento de Adaptive (`NodeVenus.APS`) con servicios para proporcionar funciones de publicación, supervisión y traducción, un servidor de procesamiento de Adaptive (`NodeVenus.APS2`) con un servicio para proporcionar auditoría de cliente, y un Servidor de administración central (`NodeVenus.CMS`) con un servicio para proporcionar los servicios del CMS.
- El host denominado HostBeta tiene instalada la plataforma de BI y está configurado para disponer de tres nodos:
  - NodeMars contiene un Servidor de administración central (`NodeMars.CMS`) con un servicio para proporcionar los servicios del CMS. Tener el CMS en dos equipos permite tener capacidades de equilibrio de carga, migración y conmutación por error.

- NodeJupiter contiene un servidor de procesamiento de Web Intelligence (`NodeJupiter.Web Intelligence`) con un servicio para proporcionar informes de Web Intelligence, y un servidor de eventos (`NodeJupiter.EventServer`) para proporcionar la supervisión de archivos.
- NodeSaturn contiene un servidor de procesamiento de Adaptive (`NodeSaturn.APS`) con un servicio para proporcionar la auditoría de clientes.

## 2.2.2 Herramientas administrativas clave

### 2.2.2.1 Asistente de configuración del sistema

El asistente de configuración del sistema es una herramienta que puede usar para configurar el despliegue de la plataforma de BI de forma rápida y fácil. El asistente le guía a través de las opciones de configuración básicas, le que resulta en un despliegue de trabajo usando configuraciones comunes, como por ejemplo:

- Los servidores de productos que desea iniciar automáticamente con la plataforma de BI
- Si desea optimizar el despliegue para un rendimiento máximo, o para recursos de hardware limitados
- Las ubicaciones de las carpetas de sistema

De forma predeterminada, el asistente está configurado para ejecutarse automáticamente cuando inicia sesión en la Consola de administración central (CMC), pero puede modificarlo en el asistente. También puede iniciar el asistente en cualquier momento desde el área *Administrar* en la CMC.

> ⓘ Nota
>
> En los sistemas de producción, resulta oportuno establecer que el asistente no se ejecute automáticamente para impedir una reconfiguración accidental.

> ⓘ Nota
>
> Se recomienda ejecutar una copia de seguridad completa antes de utilizar el asistente para realizar cambios en un sistema existente.

### 2.2.2.2 Consola de administración central (CMC)

La Consola de administración central (CMC) es una herramienta basada en Web que puede usar para realizar tareas administrativas (incluida la administración de usuarios, contenidos y servidores) y para configurar los parámetros de seguridad. Como la CMC es una aplicación basada en Web, podrá realizar todas las tareas administrativas mediante un explorador Web en cualquier equipo que se pueda conectar al servidor de aplicaciones Web.

Los únicos que pueden cambiar la configuración de administración son los miembros del grupo Administradores, a menos que a un usuario se le concedan los derechos para hacerlo. Se pueden asignar funciones en la CMC para conceder privilegios de usuario para realizar tareas administrativas de menor importancia, como la gestión de usuarios del grupo y la gestión de informes en carpetas que le pertenezcan al equipo.

### 2.2.2.3 Administrador de configuración central (CCM)

El Administrador de configuración central (CCM) es una herramienta de resolución de problemas y de gestión de nodos que se proporciona de dos formas. En un entorno de Microsoft Windows, el CCM permite administrar servidores locales y remotos a través de la interfaz gráfica de usuario (GUI) o desde una línea de comandos. En un entorno UNIX, la secuencia de comandos del shell del CCM (`ccm.sh`) le permite administrar servidores desde una línea de comandos.

El CCM se usa para crear y configurar nodos y para iniciar o detener el servidor de aplicaciones Web, si es el servidor de aplicaciones Web de Tomcat agrupado predeterminado. En Windows, también permite configurar parámetros de red, como el cifrado SSL (Nivel de socket seguro). Estos parámetros se aplican a todos los servidores de un nodo.

> **Nota**
>
> La mayoría de las tareas de administración ahora se llevan a cabo mediante la CMC y no el CCM. El CCM se usa para solucionar problemas y configurar nodos.

### 2.2.2.4 Herramienta de diagnóstico del repositorio

La Herramienta de diagnóstico del repositorio (RDT) puede analizar, diagnosticar y reparar incoherencias que se puedan producir entre la base de datos de sistema del Servidor de administración central (CMS) y el almacén de archivos de los Servidores del repositorio de archivos (FRS). Puede configurar un límite para el número de errores que RDT encontrará y reparará antes de detenerse.

La RDT se debe usar después de restaurar el sistema de la plataforma de BI.

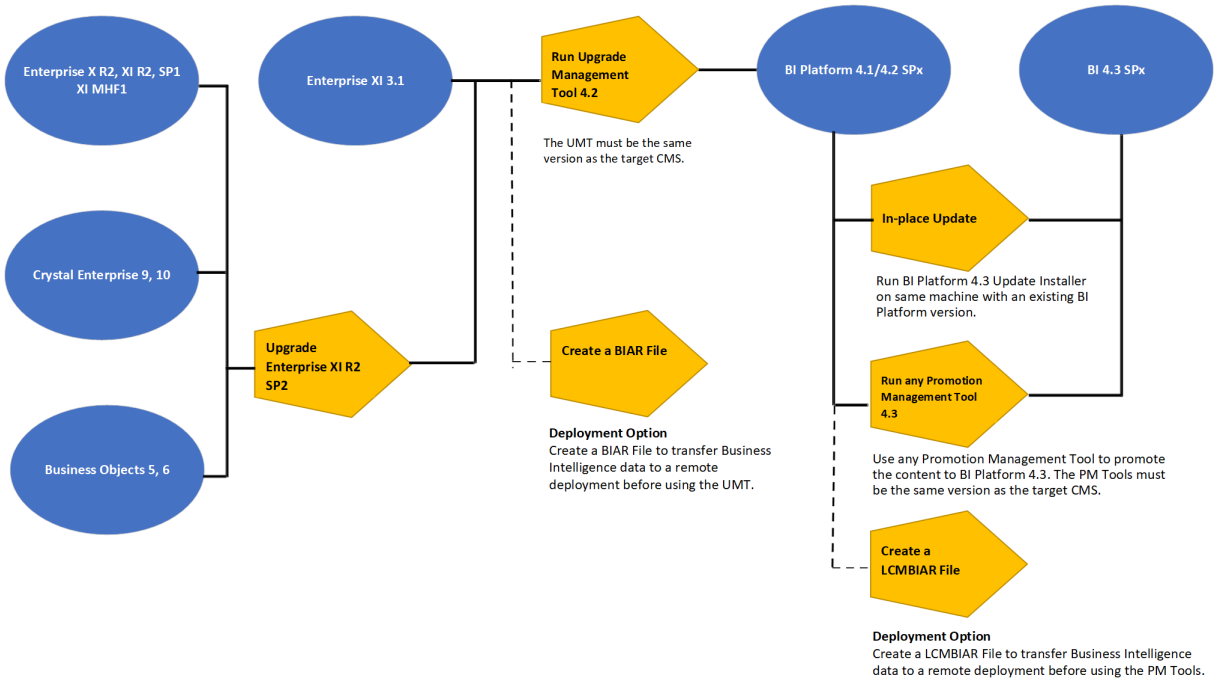
> **Nota**
>
> En los sistemas de producción resulta oportuno ejecutar regularmente la RDT, pero con la opción «Reparar» deshabilitada, para vigilar si existen temas de estado del sistema subyacente. Ejecute solo la RDT con la opción Reparar habilitada si está seguro de que desea que la RDT ejecute reparaciones en su sistema.

### 2.2.2.5 Herramienta de administración de actualizaciones

UMT quedará obsoleto en la versión 4.3 de BI. Para obtener más información, consulte 2801797

### 2.2.2.6 Actualizar rutas

Puede migrar los datos del sistema y el contenido de Business Intelligence desde las versiones anteriores de BI 4.x a la plataforma SAP BusinessObjects Business Intelligence 4.3.




La herramienta de administración de actualizaciones ha quedado obsoleta en la plataforma SAP BusinessObjects Business Intelligence 4.3, aunque puede seguir las rutas de actualización que se mencionan a continuación para cambiar a la versión 4.3.

Si tiene un despliegue más antiguo, utilice las siguientes directrices para actualizar el despliegue existente a la plataforma BI 4.3:

1. Si su despliegue existente es de XI R2, XI MHF1, XI R2 SP1, BusinessObjects 5/6 o Crystal Enterprise 9/10, primero debe actualizar a XI R2 SP2 (o superior) y continuar desde el paso 3.
2. Si su despliegue existente es de XI 3.x, puede continuar directamente con la actualización desde el paso 3.
3. Instale BI 4.1/4.2 SPx en un equipo independiente y ejecute la herramienta de administración de actualizaciones de la versión 4.1/4.2 SPx para migrar el contenido de las versiones mencionadas al nivel de BI 4.1/4.2 SPx.
4. Una vez que disponga de su contenido en el nivel de BI 4.1/4.2 SPx, puede seleccionar cualquiera de los siguientes métodos para cambiar a la versión 4.3.
   1. Ejecute el software de instalación de actualización de BI 4.3.x en el equipo a nivel de 4.1/4.2 SPx; o
   2. instale BI 4.3 en un equipo independiente y utilice la herramienta de administración de promociones de BI 4.3.x para promocionar el contenido del nivel de BI 4.1/4.2 SPx al nivel de BI 4.3.x.

### ⓘ Nota

1. Para promover el contenido del nivel de BI 4.1/4.2 SPx al nivel de BI 4.3.x, la herramienta de administración de promociones debe tener la misma versión que el CMS de destino.
2. Para obtener más información sobre BusinessObjects 5/6 a XI 3.1, consulte el manual de migración y el manual de instalación de la plataforma BI para su versión, disponible en https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_ENTERPRISE_BUSINESS_INTELLIGENCE_PLATFORM/XI.3.1/en-US.
3. La herramienta de administración de actualizaciones (UMT) solo actualiza las funciones Servidor y Nivel web del despliegue. Para obtener más información sobre UMT, consulte el manual de

actualización de la plataforma Business Intelligence de su versión, disponible en https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_BUSINESS_INTELLIGENCE_PLATFORM/4.2/en-US.

## 2.2.3 Tareas clave

Dependiendo de su situación, puede que le interesen secciones específicas de este manual y es posible que haya otros recursos disponibles. Para cada una de las siguientes situaciones, se sugiere una lista de tareas que puede realizar y temas que puede leer.

### Información relacionada

Planificación o realización del primer despliegue [página 32]
Configuración del despliegue [página 33]
Mejora del rendimiento del sistema [página 33]
Consola de administración central (CMC) [página 29]

## 2.2.3.1 Planificación o realización del primer despliegue

Si está planificando o realizando su primer despliegue de la plataforma de BI, le recomendamos que lea estas secciones del manual:

- Para conocer los componentes de la plataforma de BI, lea la «Visión general de la arquitectura».
- «Comprender la comunicación entre los componentes de la plataforma de BI»
- «Información general sobre seguridad»
- Si tiene pensado usar autenticación de terceros, lea las «Opciones de autenticación de la plataforma de BI»
- Después de la instalación, lea «Trabajar con el área de administración de servidores en la CMC»

Para obtener más información acerca de la instalación de la plataforma de BI, consulte el *Manual de instalación de la plataforma de SAP BusinessObjects Business Intelligence*. Para evaluar las necesidades y diseñar una arquitectura de despliegue que funcione de la mejor manera, lea el *Manual de planificación de la plataforma SAP BusinessObjects Business Intelligence*.

### Información relacionada

Información general de la arquitectura [página 35]
Comunicación entre los componentes de la Plataforma de BI [página 196]
Información general de seguridad [página 154]
Opciones de autenticación en la plataforma de BI [página 237]
Uso del área de administración Servidores de la CMC [página 422]

## 2.2.3.2 Configuración del despliegue

Si acaba de finalizar la instalación de la Plataforma de BI y debe realizar tareas de configuración iniciales, como la configuración del servidor de seguridad y la administración de usuarios, se recomienda leer las siguientes secciones.

### Información relacionada

Introducción al Asistente de configuración del sistema [página 91]
Comunicación entre los componentes de la Plataforma de BI [página 196]
Información general de seguridad [página 154]
Supervisión [página 811]

## 2.2.3.3 Mejora del rendimiento del sistema

Si desea asesorar la eficiencia del despliegue y ajustarla para maximizar los recursos, lea las secciones siguientes:

- Si desea usar un plantilla de despliegue para configurar el sistema, lea «Introducción al asistente de configuración del sistema».
- Si desea supervisar el sistema existente, consulte «Acerca de la supervisión».
- Para procedimientos y tareas de mantenimiento diario para trabajar con servidores en la CMC, lea «Trabajar con el área de administración de servidores en la CMC».

### Información relacionada

Introducción al Asistente de configuración del sistema [página 91]
Supervisión [página 811]
Uso del área de administración Servidores de la CMC [página 422]

## 2.2.3.4 Trabajo con objetos en la CMC

Un objeto es un documento o archivo creado en la plataforma de BI u otro software que se almacena y administra en el repositorio de la plataforma de BI. Si trabaja con objetos en la CMC, consulte las secciones siguientes:

- Para obtener información acerca de la configuración de usuarios y grupos en la CMC, consulte «Información general de la administración de cuentas».
- Para configurar la seguridad de los objetos, consulte «Funcionamiento de los derechos en la plataforma de BI».

- Para obtener información general acerca del trabajo con objetos, consulte el *Manual del usuario de la plataforma de SAP BusinessObjects Business Intelligence*.

## Información relacionada

Información general de administración de cuentas [página 103]
Cómo funcionan los derechos en la Plataforma de BI [página 127]

# 3 Arquitectura

## 3.1 Información general de la arquitectura

En esta sección se describe la arquitectura general de la plataforma, el sistema y los componentes de servicio que componen la plataforma SAP BusinessObjects Business Intelligence. Esta información ayuda a los administradores a comprender los aspectos fundamentales del sistema, y les ayudará a crear un plan para el despliegue, la administración y el mantenimiento de éste.

> **Nota**
>
> Para obtener una lista de las plataformas, idiomas, bases de datos, servidores de aplicaciones Web, servidores Web y otros sistemas admitidos en esta versión, consulte la *Matriz de disponibilidad de productos* (PAM), disponible en http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540.

> **Nota**
>
> Debido a que PAM se actualiza continuamente, consulte siempre la versión en línea y no una cópia descargada.

La plataforma de Business Intelligence (BI) está diseñada para ofrecer un elevado rendimiento en una amplia gama de escenarios de usuarios y despliegues. Puede cargar la programación y el procesamiento intensivo del procesador mediante la creación de servidores dedicados para que alojen servicios específicos. La arquitectura se ha diseñado para satisfacer las necesidades de prácticamente cualquier despliegue de BI y es suficientemente flexible para crecer desde varios usuarios con una sola herramienta hasta decenas de miles de usuarios con varias herramientas e interfaces.

Los desarrolladores pueden integrar la plataforma de BI en otros sistemas de tecnología de la organización mediante el uso de interfaces de programación de aplicaciones (API) de servicios Web, Java o .NET.

Los usuarios finales pueden tener acceso a los informes, crearlos, editarlos e interactuar con ellos mediante herramientas y aplicaciones especializadas, entre otras:

- Clientes que se instalan mediante el programa de instalación de las herramientas de cliente de la plataforma de BI:
  - Cliente enriquecido de Web Intelligence
  - Administrador de vistas empresariales
  - Herramienta de diseño de universos
  - Query as a Web Service
  - Herramienta de diseño de información (antes Information Designer)
  - Herramienta de administración de traducciones (antes Administrador de traducciones)
- Clientes disponibles de forma independiente:
  - SAP Crystal Reports
  - SAP BusinessObjects Analysis (antes Voyager)

- Áreas de trabajo de BI (antes Dashboard Builder)

Los departamentos de TI pueden usar herramientas de administración de datos y sistemas, entre las que se incluye:

- Visores de informes
- Consola de administración central (CMC)
- Administrador de configuración central (CCM)
- Herramienta de diagnóstico del repositorio (RDT)
- Herramienta de administración de Data Federation
- Herramienta de diseño de universos (antes Diseñador de universos)
- SAP BusinessObjects Mobile

Para proporcionar flexibilidad, fiabilidad y escalabilidad, los componentes de la plataforma de BI se pueden instalar en uno o varios equipos. Puede instalar simultáneamente dos versiones distintas de la plataforma de BI en el mismo equipo, aunque esta configuración solo se recomienda como parte del proceso de actualización o para su prueba.

Los procesos de servidor se pueden ampliar verticalmente (donde un equipo ejecuta varios o todos los procesos del lado del servidor) para reducir costos o bien ampliar horizontalmente (donde los procesos de servidor se distribuyen entre dos o más máquinas en red) para mejorar el rendimiento. También es posible ejecutar varias versiones redundantes del mismo proceso del servidor en varios equipos, de modo que el procesamiento puede continuar si se produce un problema en el proceso principal.

> **Nota**
>
> Es posible usar una mezcla de plataformas Unix o Linux y Windows, se recomienda no mezclar sistemas operativos para los procesos del Servidor de administración central (CMS).

## 3.1.1 Diagrama de componentes

La plataforma de SAP BusinessObjects Business Intelligence es una plataforma de Business Intelligence (BI) que proporciona herramientas de análisis y de creación de informes de nivel empresarial para facilitar la entrega de información. Los datos se pueden analizar desde cualquier sistema de bases de datos admitidas (incluyendo sistemas OLAP multidimensionales o de texto) y los informes de BI se pueden publicar en diferentes formatos a varios sistemas de publicación distintos.

Este diagrama de arquitectura ilustra los componentes de la plataforma de BI, como los servidores y herramientas de cliente y otros productos de análisis, componentes de aplicaciones web y bases de datos que pueden formar parte de la infraestructura de la plataforma de BI. Diagrama de arquitectura de BI 4.3.

La plataforma de BI informa desde una conexión de solo lectura a las bases de datos de la organización y usa sus propias bases de datos para almacenar su configuración, auditoría y otra información operativa. Los informes de BI creados por el sistema se pueden enviar a distintos destinos, incluidos sistemas de archivos y correo electrónico, o se puede acceder a ellos a través de sitios Web o portales.

La plataforma de BI es un sistema autónomo que puede existir en un único equipo (por ejemplo, como una pequeña implementación o un entorno de prueba de preproducción) o se puede ampliar a un clúster de varios equipos que ejecutan componentes distintos (por ejemplo, como un entorno de producción a gran escala).

## 3.1.2 Niveles de arquitectura

La plataforma SAP BusinessObjects Business Intelligence se puede entender como una serie de niveles conceptuales:

### Nivel de cliente

El nivel de cliente contiene todas las aplicaciones cliente de escritorio que interactúan con la plataforma de BI para proporcionar varias capacidades administrativas, de generación de informes y analíticas. Los ejemplos incluyen el Administrador de configuración central (programa de instalación de la plataforma de BI), la herramienta de diseño de información (programa de instalación de las herramientas de cliente de la plataforma de BI) y SAP Crystal Reports (está disponible y se instala independientemente).

A partir de SAP BI 4.3, las aplicaciones de cliente de escritorio (Cliente enriquecido de Web Intelligence, Herramienta de diseño de información, Herramienta de diseño de universos...) son aplicaciones de 64 bits. Ya no son de 32 bits.

### Nivel Web

El nivel Web contiene las aplicaciones Web desplegadas en un servidor de aplicaciones Web Java. Las aplicaciones Web proporcionan la funcionalidad de la plataforma de BI a los usuarios finales a través de un explorador Web. Ejemplos de aplicaciones Web incluyen la interfaz Web administrativa de la Consola de administración central (CMC) y la plataforma de lanzamiento de BI.

El nivel Web también contiene los servicios Web. Los servicios Web proporcionan la funcionalidad de la plataforma de BI para herramientas de software mediante el servidor de aplicaciones Web, como la autenticación de sesión, administración de privilegios de usuario, programación, búsqueda, administración, generación de informes y administración de consultas. Por ejemplo, Live Office es un producto que usa los servicios Web para integrar la creación de informes de la plataforma de BI en los productos de Microsoft Office.

### Nivel de gestión

El nivel de administración (también conocido como el nivel de inteligencia) coordina y controla todos los componentes que crean la plataforma de BI. Está compuesto por el Servidor de administración central (CMS), el servidor de eventos y los servicios asociados. El CMS mantiene información de seguridad y configuración, dirige solicitudes de servicios a los servidores, administra la auditoría y mantiene la base de datos del sistema CMS. El servidor de eventos administra los eventos basados en archivos que ocurren en un nivel de almacenamiento definido.

### Nivel de almacenamiento

El nivel de almacenamiento es el responsable de gestionar archivos, como documentos e informes.

El servidor del repositorio de archivos de entrada administra archivos que contienen información que se usará en los informes, como los siguientes tipos de archivos: `.rpt`, `.car`, `.exe`, `.bat`, `.js`, `.xls`, `.doc`, `.ppt`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`, `.unv`, `.unx`.

> **Nota**
>
> El tamaño del almacén de archivos del servidor del repositorio de archivos no viene administrado por el sistema; por ello, un administrador debería gestionar un plan de supervisión y mantenimiento.

El servidor del repositorio de archivos de salida administra los informes creados por el sistema, como los siguientes tipos de archivos: `.rpt`, `.csv`, `.xls`, `.doc`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`.

El nivel de almacenamiento también maneja el almacenamiento en caché para guardar los recursos del sistema cuando los usuarios acceden a los informes.

### Nivel de procesamiento

El nivel de procesamiento analiza los datos y produce informes y otros tipos de salidas. Éste es el único nivel que accede a las bases de datos que contienen los datos de los informes. Este nivel está compuesto por el servidor de tareas de Adaptive, el servidor de conexión (de 64 bits) y los servidores de procesamiento, como el servidor de procesamiento de Adaptive o el servidor de procesamiento de Crystal Reports.

### Nivel de datos

El nivel de datos consiste en los servidores de base de datos que alojan la base de datos del sistema del CMS y el almacén de datos de auditoría. También consiste en servidores de base de datos que contienen tipos de datos relacionales, OLAP, u otros tipos de datos para aplicaciones de generación de informes y analíticas.

## 3.1.3 Bases de datos

La plataforma de BI utiliza varias bases de datos distintas.

- Base de datos de generación de informes
  Esto hace referencia a los datos de su organización. Se trata de los datos de origen que analiza y notifica SAP BusinessObjects Business Intelligence Suite. En general, los datos se almacenan dentro de la base de datos relacional pero también pueden estar contenidos en archivos de texto, documentos de Microsoft Office o sistemas OLAP.
- Base de datos del sistema CMS

La base de datos del sistema del CMS se usa para almacenar información de la plataforma de BI, como detalles de usuario, servidor, carpeta, documento, configuración y autenticación. Se conserva en el Servidor de administración central (CMS) y se conoce como el *repositorio del sistema*.

- Almacén de datos de auditoría
  El almacén de datos de auditoría (ADS) se usa para almacenar información sobre eventos que se pueden seguir que ocurren en la plataforma de BI. Esta información se puede usar para supervisar el uso de los componentes de sistema, la actividad del usuario u otros aspectos del funcionamiento diario.
- Supervisión de base de datos
  La supervisión utiliza la base de datos de Almacén de datos de auditoría (ADS) para almacenar la información de la configuración y los componentes del sistema para la compatibilidad de SAP.
- Base de datos de comentarios
  Comentario de BI es una aplicación que se ha introducido en CMC. Permite a los usuarios colaborar comentando cualquiera de los datos o estadísticas disponibles en un documento determinado.
  La base de datos de comentarios está configurada en la misma base de datos que la base de datos de auditoría. Se crea de forma predeterminada en la base de datos de auditoría.

Si no dispone de un servidor de base de datos para usar con el sistema del CMS y bases de datos del almacén de datos de auditoría, el programa de instalación de la plataforma de BI puede instalar y configurar uno por usted. Se recomienda evaluar los requisitos en la información del proveedor del servidor de la base de datos para determinar qué base de datos admitida se adecua más a los requisitos de la organización.

> **Nota**
>
> No se recomienda la base de datos predeterminada SQL Anywhere para sistemas de producción. Está agrupada con los paquetes de servidor de plataforma de BI, que le permite desplegar y probar la plataforma de BI inmediatamente, pero tiene capacidades limitadas necesarias para gestionar una base de datos. Se recomienda utilizar SQL Anywhere en su forma completa, o bien una instancia de base de datos compatible existente para el sistema de producción, ya que es esencial para que la base de datos de CMS resida en el centro de datos. Lo gestionan los administradores de bases de datos con procesos adecuados que se han establecido para la seguridad de los datos y la disponibilidad de los servidores.

## 3.1.4 Servidores, hosts, y clústeres

La plataforma de BI consta de colecciones de servidores que se ejecutan en uno o varios hosts. Las instalaciones pequeñas (como sistemas de prueba o de desarrollo) pueden usar un único host para un servidor de aplicaciones Web, un servidor de base de datos, y todos los servidores de la plataforma de BI.

Las instalaciones pequeñas y grandes pueden tener varios servidores en ejecución en varios hosts. Por ejemplo, un host de servidor de aplicaciones Web se puede usar en combinación con un host de servidor de la plataforma de BI. Esto libera recursos en el host de servidor de la plataforma de BI, lo que permite procesar más información que si también alojara el servidor de aplicaciones Web.

Las grandes instalaciones pueden disponer de varios hosts de servidores de la plataforma de BI trabajando juntos en un clúster. Por ejemplo, si una organización dispone de un gran número de usuarios de SAP Crystal Reports, los servidores de procesamiento de Crystal Reports se pueden crear en varios hosts de servidores de la plataforma de BI para asegurar que existen muchos recursos disponibles para procesar las solicitudes de los clientes.

Las ventajas de disponer de varios servidores incluyen:

- Rendimiento mejorado
  Varios hosts de servidor de la plataforma de BI pueden procesar una cola de información de generación de informes más rápidamente que un único host de servidor de la plataforma de BI.
- Equilibrio de carga
  Si un servidor experimenta un exceso de carga, el CMS envía automáticamente trabajo nuevo a otros servidores del clúster.
- Disponibilidad mejorada
  Si un servidor se encuentra con una condición inesperada, el CMS vuelve a dirigir automáticamente el trabajo a diferentes servidores hasta que se corrija la condición.

## 3.1.5 Servidores de aplicaciones Web

Un servidor de aplicaciones Web actúa como la capa de traducción entre un explorador Web o una aplicación enriquecida y la plataforma de BI. Se admiten servidores de aplicaciones Web que se ejecutan en Windows, Unix y Linux.

Para obtener una lista detallada de los servidores de aplicaciones Web admitidos, consulte las *plataformas admitidas/PAR*, disponibles en: https://support.sap.com/home.html.

Si no dispone de un servidor de aplicaciones Web para su uso con la plataforma de BI, el programa de instalación puede instalar y configurar un servidor de aplicaciones Web de Tomcat. Se recomienda que evalúe los requisitos en la información del vendedor del servidor de aplicaciones Web para determinar qué servidor de aplicaciones Web se adecua más a los requisitos de su organización.

> **Nota**
>
> Al configurar un entorno de producción, se recomienda que el servidor de aplicaciones Web se aloje en un sistema independiente. La ejecución de la plataforma de BI y un servidor de aplicaciones Web en el mismo host en un entorno de producción puede reducir el rendimiento.

### 3.1.5.1 Habilitación de la agrupación en clústeres en la aplicación web de la plataforma de lanzamiento de BI como soporte para escalabilidad y fallo de modo

En esta sección se describe cómo habilitar la agrupación en clústeres en la aplicación web de la plataforma de lanzamiento de BI para ofrecer soporte a la escalabilidad y al fallo de modo. En esta sección se explican también los pasos para configurar los servidores de aplicación Apache Tomcat y WebSphere para este mismo fin.

Para habilitar la agrupación en clústeres de cualquier servidor de aplicaciones (por ejemplo, Tomcat o WebSphere), necesita los siguientes componentes:

- Un servidor HTTP
- Un equilibrador de carga compatible
- Dos o más instancias del servidor de aplicaciones con la aplicación web necesaria ya instalada

- Una instalación completa de BOE (repositorio)

> **Nota**
>
> Los pasos que se describen en esta sección son genéricos y se pueden utilizar para habilitar la agrupación en clústeres para cualquier otra aplicación. Las únicas diferencias son los cambios efectuados en el descriptor de deployment de la aplicación web (web.xml). Le recomendamos que consulte a su proveedor del servidor de aplicaciones web para saber cómo configurar el equilibrio de carga de nivel web.

#### 3.1.5.1.1 Instalación de Apache Tomcat

Para instalar el servidor Apache Tomcat, siga estos pasos:

1. Instale el servidor Apache HTTP.
2. Instale el servidor Apache Tomcat en los equipos de instancia.
3. Descargue mod_jk (equilibrador de carga) y grábelo en el directorio "modules" del servidor Apache HTTPD desde http://tomcat.apache.org/download-connectors.cgi .
4. Ejecute el agente SI en un equipo con toda la instalación de BOE ya realizada.

   > **Nota**
   >
   > Para verificar la compatibilidad para mod_jk, inicie su servidor HTTP. En la consola se muestra un mensaje si la versión descargada de mod_jk no es compatible con su versión del servidor HTTP.

## Configuración de Apache Tomcat

Para configurar Apache Tomcat, siga estos pasos:

1. Configure el servidor Apache HTTP.
   a. Configure httpd.conf (equilibrador de carga, aplicación web de carga, monitorización, vía de acceso al fichero worker.properties).
   b. Configure el fichero workers.properties y grábelo en la biblioteca Apache\Conf.

C:\Server\Apache2\Apache2\conf\httpd.conf - Notepad++

File Edit Search View Format Language Settings Macro Run TextFX Plugins Window ?

httpd.conf | httpd.default.conf

```
64  # If specified, ensure that no two invocations of Apache share the same
65  # scoreboard file. The scoreboard file MUST BE STORED ON A LOCAL DISK.
66  #
67  #ScoreBoardFile logs/apache_runtime_status
68
69  # Used for clustering
70
71  # Specify path to worker configuration file
72  #
73  JkWorkersFile C:\Server\Apache2\Apache2\conf\workers.properties
74  # Configure logging and memory
75  JkShmFile logs/mod_jk.shm
76  JkLogFile logs/mod_jk.log
77  JkLogLevel info
78
79  # Configure monitoring
80  JKMount /jkmanager jkstatus
81  JkMount /jkmanager/* jkstatus
82  <Location /jkmanager>
83  Order deny,allow
84  Deny from all
85  Allow from localhost
86  </Location>
87
88  # Configure applications
89  # JkMount /webapp-directory/* loadBalancer
90  JKMount /clusterjsp loadBalancer
91  JKMount /clusterjsp/* loadBalancer
92  JKMount /login loadBalancer
93  JKMount /login/* loadBalancer
94  JKMount /boe loadBalancer
95  JKMount /boe/* loadBalancer
96  #JKMount /BOE loadBalancer
97  #JKMount /BOE/* loadBalancer
98  JKMount /docs loadBalancer
99  JKMount /docs/* loadBalancer
100
```

```
182 LoadModule env_module modules/mod_env.so
183 #LoadModule expires_module modules/mod_expires.so
184 #LoadModule file_cache_module modules/mod_file_cache.so
185 #LoadModule headers_module modules/mod_headers.so
186 LoadModule imap_module modules/mod_imap.so
187 LoadModule include_module modules/mod_include.so
188 #LoadModule info_module modules/mod_info.so
189 LoadModule isapi_module modules/mod_isapi.so
190
191 # Used for clustering
192 #LoadModule for clustering
193
194 LoadModule jk_module modules/mod_jk.so
195
196 LoadModule log_config_module modules/mod_log_config.so
197 LoadModule mime_module modules/mod_mime.so
```

Load Tomcat Connector (mod_jk)

2. Configure server.xml en Tomcat (añada etiquetas de agrupación en clústeres).
   a. En server.xml, el atributo jvmRoute debería corresponder al nombre utilizado en el fichero workers.properties.
   b. Si trabaja con Tomcat 8 u otra versión superior, elimine JvmRouteSessionIDBinderListener (obsoleto).
3. Añada una etiqueta distribuible al fichero web.xml (descriptor de deployment) de la aplicación web que quiere que ofrezca soporte a la agrupación en clústeres.

El valor personalizado que llama la válvula predeterminada para cada solicitud se especifica a continuación. Si utiliza Tomcat 8, en todos los archivos server.xml de Tomcat, reemplace:

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Inte
rceptor"/>
```

por

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatchInterc
eptor"/>
```

```
    <Sender className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
      <Transport className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>
    </Sender>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interceptor"/>
  </Channel>

  <Valve className="com.sap.customvalve.ForceReplicationValve"/>
   <Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=".*\.gif;.*\.jpg;.*\.png;.*\.js;.*\.htm
  <Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>

  <Deployer className="org.apache.catalina.ha.deploy.FarmWarDeployer" deployDir="/tmp/war-deploy/" tempDir="/tmp
```

4. Exporte JAR para la válvula personalizada (si se necesitan modificaciones) desde el código. Copie el archivo `forcereplicationvalve.jar` de `<BOEInstallDir>/SAP BusinessObjects XI 4.0/java/lib` y péguelo en `<TomcatInstallDir>/tomcat/lib` (en todos los nodos Tomcat).
5. Almacene este JAR en la carpeta `tomcat/lib` de cada instancia.
6. Reinicie todos los servidores.

> **Nota**
>
> - Como mejor práctica, se recomienda iniciar los servidores de uno en uno; espere a que se haya iniciado totalmente un servidor antes de iniciar el siguiente.
> - No utilice localhost:6400 como nombre del sistema en la pantalla de inicio de sesión para la plataforma de lanzamiento. Proporcione el nombre (o IP) del equipo de instalación BOE en cuestión. Asegúrese de que el agente SI se esté ejecutando en esta instalación.
> - Explore el atributo channelSendOptions para la opción más adecuada. Se utiliza para establecer opciones para la respuesta sincronizada, la asincrónica, etc.
> - Cuando exporte JAR para la válvula personalizada desde el código, recuerde crear una jerarquía de paquetes adecuada para JAR e incluirla en server.xml.

## 3.1.5.1.2 Instalación de WebSphere

## Configuración de WebSphere

Para configurar WebSphere, siga estos pasos:

1. Añada la etiqueta distribuible en web.xml de la aplicación web BOE para las dos instancias de servidor de aplicaciones WebSphere.
2. En la consola IBM, vaya a *Todos los servidores* > *member1* > *Gestión de sesiones*.
   a. Verifique y habilite las cookies.
   b. Habilite *Permitir acceso en serie* y modifique el tiempo de espera a 10 segundos.
3. Vaya a *Configuración de entorno de distribución* > *Replicación memoria a memoria*.
   a. Cree un dominio de replicación y selecciónelo.
   b. Seleccione el modo de replicación, tanto cliente como servidor.
4. En cada instancia de *Todos los servidores*, seleccione el mismo dominio de replicación del paso anterior.
5. Vaya a *Configuración de entorno de distribución* > *Personalizar parámetros de optimización*.
   a. En caso de failover, marque el nivel de optimización *Bajo*.
6. Reinicie todos los servidores.

## 3.1.5.2 Servidor de contenedor de aplicación Web (WACS)

Para albergar aplicaciones Web de la plataforma de BI se requiere un servidor de aplicaciones Web.

Si usted es un administrador de servidores de aplicaciones Web Java avanzado con necesidades de administración avanzadas, use un servidor de aplicaciones Web Java admitido para alojar aplicaciones Web de la plataforma de BI. Si usa un sistema operativo Windows admitido para alojar la plataforma de BI y prefiere un proceso de instalación del servidor de aplicaciones Web sencillo, o no dispone de los recursos para administrar un servidor de aplicaciones Web Java, puede instalar el Servidor de contenedor de aplicación Web (WACS) al instalar la plataforma de BI.

WACS es un servidor de plataforma de BI que permite que las aplicaciones Web de plataforma de BI, como la consola de administración central (CMC), la plataforma de lanzamiento de BI y servicios Web, se ejecuten sin la necesidad de un servidor de aplicaciones Web Java instalado anteriormente.

El uso de WACS proporciona ciertas ventajas:

- WACS requiere un mínimo esfuerzo de instalación, mantenimiento y configuración. El programa de instalación de la plataforma de BI lo instala y configura, y no son necesarios pasos adicionales para empezar a usarlo.
- WACS elimina la necesidad de conocimientos de administración y mantenimiento del servidor de aplicaciones Java.
- WACS proporciona una interfaz administrativa que es coherente con otros servidores de la plataforma de BI.
- Igual que otros servidores de la plataforma de BI, WACS se puede instalar en un host dedicado.

> **Nota**
>
> Existen algunos límites en el uso de WACS en lugar de un servidor de aplicaciones web Java dedicado:

- WACS solo está disponible en sistemas operativos Windows admitidos.
- Las aplicaciones Web personalizadas no se pueden desplegar en WACS ya que solo admite las aplicaciones Web instaladas con la plataforma de BI.
- WACS no se puede usar con un equilibrador de carga Apache.

Es posible usar un servidor de aplicaciones Web dedicado además de WACS. Esto permite que el servidor de aplicaciones Web dedicado aloje aplicaciones Web personalizadas, mientras que WACS aloja la CMC y otras aplicaciones Web de la plataforma de BI.

## 3.1.6 Kits de desarrollo de software

Un Kit de desarrollo de software (SDK) permite que un desarrollador incorpore aspectos de la plataforma SAP BusinessObjects Business Intelligence en las aplicaciones y sistemas propios de la organización.

La plataforma de BI tiene SDK para el desarrollo de software en plataformas Java y .NET.

> **Nota**
>
> Los SDK .NET de la plataforma de BI no están instalados de forma predeterminada y se deben descargar de SAP Service Marketplace.

La plataforma de BI admite los siguientes SDK:

- SDK Java y SDK .NET de la plataforma de Business Intelligence
  Los SDK de la plataforma de BI permiten que las aplicaciones realicen tareas como la autenticación, la administración de sesiones, el trabajo con objetos del repositorio, la programación y publicación de informes y la administración de servidores.

  > **Nota**
  >
  > Para obtener acceso completo a la seguridad, administración de servidores y funciones de auditoría, use el SDK de Java.

- SDK de servicios Web RESTful de la plataforma de Business Intelligence
  El SDK de servicios Web RESTful de la plataforma de BI permite acceder a la plataforma de BI con el protocolo HTTP. Puede usar este SDK para iniciar sesión en la plataforma de BI, desplazarse al repositorio de la plataforma de BI, acceder a los recursos y realizar la programación básica de los recursos. Puede acceder a este SDK al escribir aplicaciones que usen cualquier idioma de programación que admita el protocolo HTTP o mediante el uso de cualquier herramienta que admita realizar solicitudes HTTP.
- SDK de consumidor Java y SDK de consumidor .NET de la plataforma de Business Intelligence
  Una implementación de servicios Web basados en SOAP que permite manejar la autenticación y seguridad del usuario, el acceso a documentos e informes, la programación, las publicaciones y la administración de servidores.
  Los servicios Web de la plataforma de BI usan estándares, como XML, SOAP, AXIS 2.0 y WSDL. La plataforma sigue la especificación de servicios Web Perfil básico de interoperabilidad WS 1.0.

  > **Nota**
  >
  > Las aplicaciones de servicios Web solo son compatibles actualmente con las siguientes configuraciones del equilibrador de carga:

1. Persistencia de dirección IP de origen.
2. Persistencia de puerto de destino y dirección IP de origen (solo disponible en un conmutador de servicios de contenido de Cisco).
3. Persistencia de SSL.
4. Persistencia de sesión basada en cookies.

> **Nota**
>
> La persistencia de SSL puede causar problemas de seguridad y fiabilidad en algunos exploradores Web. Consulte al administrador de la red para determinar si la persistencia de SSL resulta adecuada para su organización.

- Controlador de acceso a datos y SDK Java de conexión
  Estos SDK permiten crear controladores de base de datos para el servidor de conexión y administrar las conexiones a la base de datos.
- SDK Java de la capa semántica
  El SDK Java de la capa semántica permite desarrollar una aplicación Java que realiza tareas de administración y seguridad en universos y conexiones. Por ejemplo, puede implementar servicios para publicar un universo en un repositorio o recuperar una conexión segura desde el repositorio en el área de trabajo. Esta aplicación se puede incorporar en soluciones de la plataforma de BI que integran la plataforma de BI como OEM.
- SDK de Java y SDK de .NET del Servidor de aplicaciones de informes
  Los SDK del Servidor de aplicaciones informes permiten que las aplicaciones abran, creen y modifiquen informes de Crystal existentes, incluida la configuración de valores de parámetros, el cambio de orígenes de datos y la exportación a otros formatos como XML, PDF, Microsoft Word y Microsoft Excel.
- Visores de informes de Crystal Java y .NET
  Los visores permiten que las aplicaciones muestren y exporten informes de Crystal. Están disponibles los siguientes visores:
  - Visor de páginas de informe DHTML: presenta datos y permite profundizar, navegar por páginas, hacer zoom, solicitar, buscar, resaltar, exportar e imprimir.
  - Visor de partes del informe: proporciona la habilidad de ver partes individuales de un informe, incluyendo gráficos, texto y campos.
- SDK de Java y SDK de .NET del motor de informes
  Los SDK del motor de informes permiten que las aplicaciones interactúen con los informes creados con SAP BusinessObjects Web Intelligence.
  Los SDK del motor de informes contienen bibliotecas que se pueden usar para crear una herramienta de diseño de informes Web. Las aplicaciones creadas con estos SDK pueden ver, crear o modificar varios documentos distintos de Web Intelligence. Los usuarios pueden modificar documentos existentes agregando, eliminando y modificando objetos, como tablas, gráficos, condiciones y filtros.
- SDK de búsqueda de plataforma: el SDK de búsqueda de plataforma es la interfaz entre la aplicación cliente y el servicio de búsqueda de plataforma. La búsqueda de plataforma admite el SDK público que forma parte del SDK de búsqueda de plataforma.
  Cuando se envía un parámetro de solicitud de búsqueda mediante la aplicación cliente a la capa SDK, este convierte el parámetro de solicitud al formato codificado XML y lo pasa al servicio de búsqueda de plataforma.

Los SDK se pueden combinar para proporcionar una amplia gama de funcionalidades de BI a las aplicaciones. Para obtener más información acerca de estos SDK, incluidos los manuales del desarrollador y las referencias de API, consulte la página del producto SAP BusinessObjects Business Intelligence Platform.

## 3.1.7 Fuentes de datos

### 3.1.7.1 Universos

El universo es una capa semántica que abstrae la complejidad de los datos usando un lenguaje empresarial en lugar del lenguaje de datos para acceder, manipular y organizar los datos. Este lenguaje empresarial se almacena como objetos en un archivo de universo. Web Intelligence, Crystal Reports y otras aplicaciones usan universos para simplificar el proceso de creación de usuarios necesario para las consultas y análisis del usuario final de simples a complejos.

Los universos son un componente principal de la plataforma de BI. El servidor de conexión almacena y protege todos los objetos y conexiones del universo en el repositorio central. Las herramientas de cliente para diseñar universos deben iniciar sesión en la plataforma de BI para acceder al sistema y crear universos. El acceso a los universos y la seguridad del nivel de fila/columna también se pueden administrar en el nivel de grupo o de usuario individual desde dentro del entorno de diseño.

La capa semántica permite que Web Intelligence ofrezca documentos mediante el uso de varios proveedores de datos sincronizados, incluidos los orígenes de datos de procesamiento analítico en línea (OLAP) y metamodelo de almacenamiento común (CWM).

### 3.1.7.2 Vistas empresariales

Las vistas empresariales simplifican la creación de informes y la interacción con la abstracción de la complejidad de los datos para los desarrolladores de informes. Las vistas empresariales ayudan a separar las conexiones de datos, el acceso a datos, los elementos empresariales y el control de acceso.

Las vistas empresariales solo las puede usar Crystal Reports y están diseñadas para simplificar el acceso de datos y la seguridad en tiempo de visualización requerida para la creación de informes de Crystal. Las vistas empresariales admiten la combinación de varios orígenes de datos en una misma vista. Las vistas empresariales son totalmente admitidas en la plataforma de BI.

## 3.1.8 Autenticación e inicio de sesión único

El Servidor de administración central (CMS) administra la seguridad del sistema, los complementos de seguridad y las herramientas de autenticación de terceros, como SiteMinder o Kerberos. Estos componentes autentican a los usuarios y autorizan el acceso de los usuarios a la plataforma de BI, sus carpetas y otros objetos.

Están disponibles los siguientes complementos de seguridad de inicio de sesión único de autenticación de usuarios:

- Enterprise (predeterminado), incluyendo soporte de autenticación de confianza para usar con métodos de autenticación como SAML, X.509, SAP NW SSO, y otros métodos admitidos por su servidor de aplicaciones.
- LDAP

- Windows Active Directory (AD)

Al usar un sistema de Planificación de recursos de Enterprise (ERP), se usa el inicio de sesión único para autenticar el acceso de los usuarios al sistema de ERP de modo que los informes puedan originar datos de ERP. Se admite el siguiente inicio de sesión único de autenticación de usuarios para sistemas de ERP:

- SAP ERP y Business Warehouse (BW)
- Oracle E-Business Suite (EBS)
- Siebel Enterprise
- JD Edwards Enterprise One
- PeopleSoft Enterprise

### 3.1.8.1 Complementos de seguridad

Los complementos de seguridad automatizan la creación y administración de cuentas, ya que permiten asignar cuentas de usuario y grupos desde sistemas de terceros a la plataforma de BI. Puede asignar cuentas de usuario de terceros a cuentas de usuario de Enterprise existentes, o puede crear nuevas cuentas de usuario de Enterprise que se correspondan a cada entrada asignada en el sistema externo.

Los componentes de seguridad mantienen dinámicamente listas de usuarios y grupos de terceros. Por lo tanto, una vez asignado un Protocolo ligero de acceso a directorios (LDAP) o un grupo de Windows Active Directory (AD) a la plataforma de BI, todos los usuarios que pertenecen a ese grupo pueden iniciar sesión en la plataforma de BI. Los cambios siguientes de los miembros del grupo de terceros se propagan automáticamente.

La plataforma de BI es compatible con los siguientes complementos de seguridad:

- Complemento de seguridad de Enterprise
  El Servidor de administración central (CMS) administra la información de seguridad, como las cuentas de usuario, los miembros de grupos y los derechos de los objetos que definen los privilegios de usuario y grupo. Esto se conoce como la autenticación de Enterprise.
  La autenticación de Enterprise siempre está habilitada y no se puede deshabilitar. Use la autenticación Enterprise predeterminada del sistema si prefiere crear cuentas y grupos diferentes para su uso con la plataforma de BI, o si todavía no ha configurado una jerarquía de usuarios y grupos en un servidor LDAP o Windows AD.
  La autenticación de confianza es un componente de la autenticación de Enterprise que se integra con soluciones de inicio de sesión único de terceros, incluyendo la autenticación Java y el servicio de autorización (JAAS). Las aplicaciones que han establecido confianza con el Servidor de administración central pueden usar la autenticación de confianza para permitirles a los usuarios iniciar sesión sin proporcionar sus contraseñas.
- Complemento de seguridad de LDAP
- Windows AD

> **Nota**
>
> Aunque un usuario puede configurar la autenticación de Windows AD para la plataforma de BI y aplicaciones personalizadas a través de la CMC, la CMC y la plataforma de lanzamiento de BI no admiten la autenticación de Windows AD con NTLM. Los únicos métodos de autenticación que la CMC y la plataforma de lanzamiento de BI admiten son Windows AD con Kerberos, LDAP, Enterprise y Autenticación de confianza.

### 3.1.8.2 Integración de Planificación de recursos comerciales (ERP)

Una aplicación Planificación de recursos empresariales (ERP) admite las funciones esenciales de los procesos de una organización mediante la recopilación de información en tiempo real relacionada con las operaciones diarias. La plataforma de BI admite el inicio de sesión único y la creación de informes a partir de los sistemas ERP siguientes:

- SAP ERP y Business Warehouse (BW)
- Siebel Enterprise
- Oracle E-Business Suite
- JD Edwards EnterpriseOne
- PeopleSoft Enterprise

> **Nota**
>
> - La compatibilidad con SAP ERP y BW se instala de forma predeterminada. Si no desea tener compatibilidad con SAP ERP o BW, utilice la opción de instalación *Personalizar/Expandir* para anular la selección de la compatibilidad de integración de SAP.
> - La compatibilidad con Siebel Enterprise, Oracle E-Business Suite, JD Edwards EnterpriseOne o PeopleSoft no se instala de forma predeterminada. Utilice la opción de instalación *Personalizar/Expandir* para seleccionar e instalar la integración para sistemas que no sean SAP ERP.

Para obtener información detallada sobre versiones específicas que admiten la plataforma de BI, *Plataformas admitidas/PARs*, disponible enhttps://support.sap.com/home.html.

Para configurar la integración ERP, consulte el capítulo *Configuraciones suplementarias para entornos ERP* en este manual.

## 3.1.9 Integración de SAP

La plataforma de BI se integra con la estructura SAP existente con las siguientes herramientas SAP:

- Directorio horizontal del sistema (SLD) de SAP
  El directorio horizontal del sistema de SAP NetWeaver es el origen central de información horizontal del sistema y es importante para administrar el ciclo de vida del software. Ya que proporciona un directorio que contiene información sobre el software instalable disponible desde SAP y acerca de los datos actualizados automáticamente sobre los sistemas ya instalados en un entorno, obtendrá la infraestructura para la compatibilidad de la herramienta para planificar las tareas de ciclo de vida del software en el entorno del sistema.
  El programa de instalación de la plataforma de BI registra los nombres del producto y del distribuidor con el SLD, así como los nombres, versiones y ubicación del servidor y del componente front-end.
- SAP Solution Manager
  SAP Solution Manager es una plataforma que proporciona el contenido integrado, herramientas y metodologías para implementas, admitir, operar y supervisar las soluciones SAP y que no sean de SAP de la organización.
  El software que no sea SAP con una integración certificada por SAP se introduce en el repositorio central y se transfiere automáticamente en los Directorios horizontales del sistema de SAP (SLD). Los clientes de

SAP pueden identificar fácilmente la versión de la integración del producto de terceros que ha certificado SAP dentro de su entorno del sistema de SAP. Este servicio proporciona una conciencia adicional para productos de terceros además de los catálogos para productos de terceros.
SAP Solution Manager está disponible para los clientes de SAP sin cargo adicional, e incluye acceso directo al soporte técnico de SAP y a la información de ruta de actualización del producto de SAP. Para obtener más información sobre SLD, consulte «Registro de la plataforma de BI en la infraestructura horizontal del sistema».

- Sistema de modificación y transporte (CTS+)
  El CTS ayuda a organizar los proyectos de desarrollo en ABAP Workbench y en Personalización y, a continuación, transporta los cambios entre los sistemas SAP a su entorno de sistemas. Así como los proyectos ABAP, también se pueden transportar objetos Java (J2EE, JEE) y tecnologías que no son ABAP específicas de SAP (como Web Dynpro Java o SAP NetWeaver Portal) en el entorno.
- Supervisión con CA Wily Introscope
  CA Wily Introscope es un producto de administración de aplicaciones Web que ofrece la posibilidad de supervisar y diagnosticar los problemas de rendimiento que pueden producirse dentro de los módulos SAP basados en Java que están en producción, incluida la visibilidad en aplicaciones y las conexiones Java personalizadas en sistemas back-end. Permite aislar cuellos de botella del rendimiento en módulos de NetWeaver, incluidos Servlets individuales, JSP, EJB, JCO, Clases, Métodos y mucho más. Ofrece una supervisión a tiempo real y de baja transparencia, visibilidad de transacción de un extremo a otro, datos históricos para planificar el análisis o la capacidad, cuadros de mandos personalizados, alarmas de umbrales automáticas y una arquitectura abierta para desplegarse más allá de lo entornos de NetWeaver.

### 3.1.10 Control de versiones integrado

Los archivos que conforman la plataforma de BI en un sistema de servidor se mantienen en el control de versiones. El programa de instalación instalará y configurará el sistema de control de versiones Subversión, o puede introducir detalles para usar un sistema de control de versiones Subversión o Clearcase.

Un sistema de control de versiones hace posible mantener y restaurar diferentes revisiones de la configuración y otros archivos, lo que significa que siempre es posible revertir el sistema a un estado conocido de cualquier momento del pasado.

## 3.2 Servidores, servicios, nodos y hosts

La plataforma de BI usa los términos servidor y servicio para hacer referencia a los dos tipos de software que se ejecutan en un equipo de la plataforma de BI.

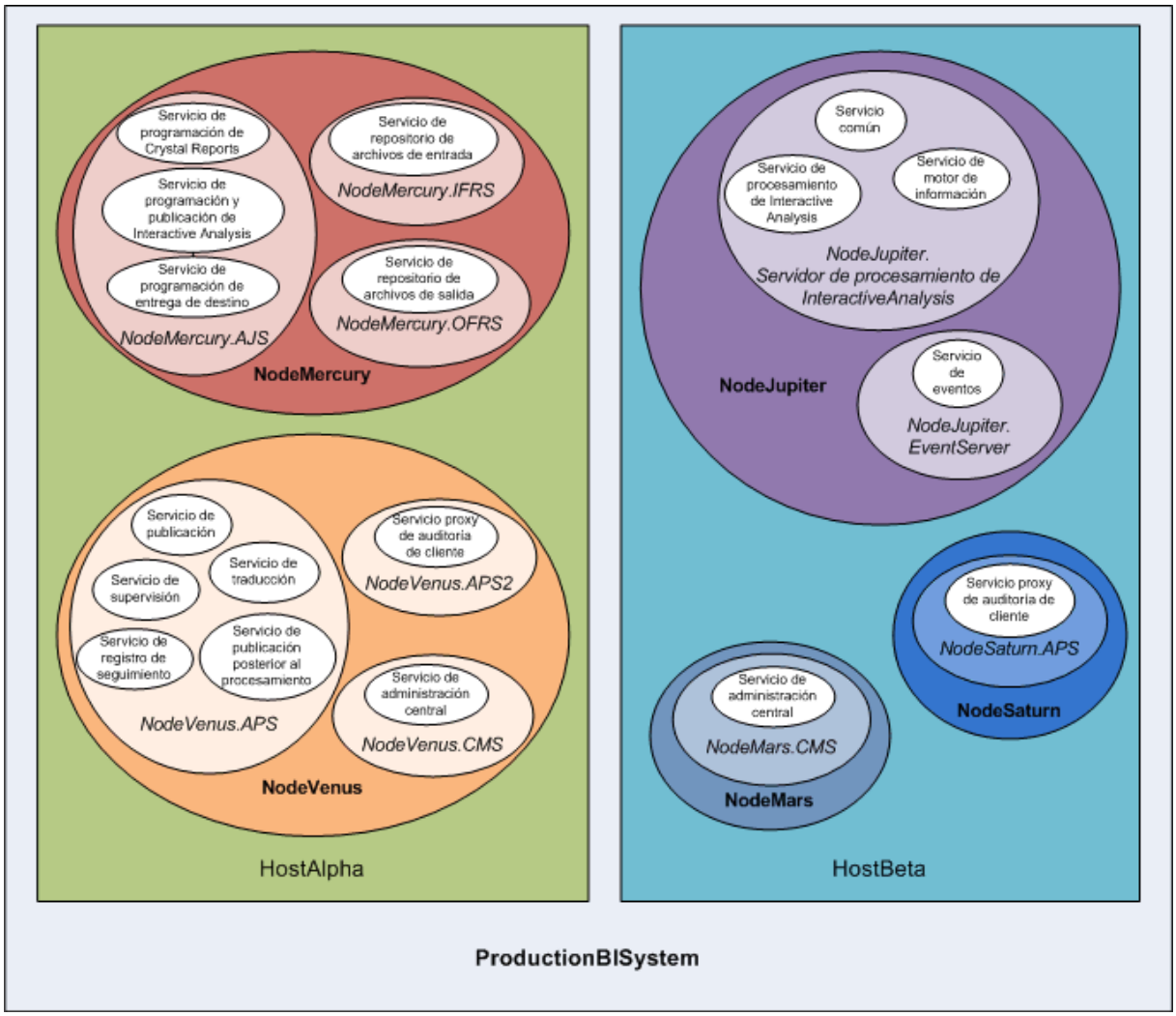
El término «servidor» se usa para describir un proceso de nivel del sistema operativo (en algunos sistemas se conoce como demonio) que aloja uno o varios servicios. Por ejemplo, el Servidor de administración central (CMS) y el Servidor de procesamiento de Adaptive son servidores. Un servidor se ejecuta en una cuenta específica del sistema operativo y tiene su propio ID de proceso (PID).

Un servicio es un subsistema de servidor que realiza una función específica. El servicio se ejecuta en el espacio de memoria de su servidor con el ID de proceso del contenedor principal (servidor). Por ejemplo, el servicio de programación de Web Intelligence es un subsistema que se ejecuta dentro del servidor de tareas de Adaptive.

Un nodo es una colección de servidores de la plataforma de BI que se ejecutan en el mismo host y los gestiona un solo Agente de inteligencia de servidor (SIA). Uno o varios nodos pueden estar en un solo host.

La plataforma de BI se puede instalar en un equipo, se puede distribuir en varios equipos de una intranet o se puede separar en una red de área extensa (WAN).

El siguiente diagrama muestra una instalación hipotética de la plataforma de BI. El número de hosts, nodos, servidores y servicios, así como el tipo de servidores y servicios, variará en instalaciones reales.




Dos hosts del clúster llamado ProductionBISystem:

- El host denominado HostAlpha tiene instalada la plataforma de BI y está configurado para disponer de dos nodos:
  - NodeMercury contiene un servidor de tareas de Adaptive (`NodeMercury.AJS`) con servicios para programar y publicar informes, un Servidor del repositorio de archivos de entrada (`NodeMercury.IFRS`) con un servicio para almacenar informes de entrada y un Servicio del repositorio de archivos de salida (`NodeMercury.OFRS`) con un servicio para almacenar la salida de informes.
  - NodeVenus contiene un servidor de procesamiento de Adaptive (`NodeVenus.APS`) con servicios para proporcionar funciones de publicación, supervisión y traducción, un servidor de procesamiento de

Adaptive (`NodeVenus.APS2`) con un servicio para proporcionar auditoría de cliente, y un Servidor de administración central (`NodeVenus.CMS`) con un servicio para proporcionar los servicios del CMS.

- El host denominado HostBeta tiene instalada la plataforma de BI y está configurado para disponer de tres nodos:
  - NodeMars contiene un Servidor de administración central (`NodeMars.CMS`) con un servicio para proporcionar los servicios del CMS. Tener el CMS en dos equipos permite tener capacidades de equilibrio de carga, migración y conmutación por error.
  - NodeJupiter contiene un servidor de procesamiento de Web Intelligence (`NodeJupiter.Web Intelligence`) con un servicio para proporcionar informes de Web Intelligence, y un servidor de eventos (`NodeJupiter.EventServer`) para proporcionar la supervisión de archivos.
  - NodeSaturn contiene un servidor de procesamiento de Adaptive (`NodeSaturn.APS`) con un servicio para proporcionar la auditoría de clientes.

## 3.2.1 Cambios del servidor desde XI 3.1

En la siguiente tabla se describen los principales cambios de los servidores de la plataforma de BI desde XI 3.1. Entre los tipos de cambios hay:

- Servidores cuyos nombres han cambiado entre versiones pero que siguen proporcionando las mismas funcionalidades o similares.
- Servidores que la nueva versión ya no ofrece.
- Servicios comunes o relacionados que se han consolidado en los servidores de Adaptive.
  Por ejemplo, los servicios de programación que proporcionan los servidores de tareas individuales de XI 3.1 se han movido al servidor de tareas de Adaptive desde 4.0.
- Nuevos servidores que se han introducido.

Cambios del servidor

| XI 3.1 | 4,0 | Feature Pack 3 para 4.0 | 4,1 | 4,2 | 4,3 |
|---|---|---|---|---|---|
| Servidor de conexión [1] | Servidor de conexión<br>Servidor de conexión 32 | Servidor de conexión<br>Servidor de conexión 32 | Servidor de conexión<br>Servidor de conexión 32 | Servidor de conexión<br>Servidor de conexión 32 | Servidor de conexión<br>Servidor de conexión 32 |
| Servidor de tareas de Crystal Reports | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive |

| XI 3.1 | 4,0 | Feature Pack 3 para 4.0 | 4,1 | 4,2 | 4,3 |
|---|---|---|---|---|---|
| Servidor de procesamiento de Crystal Reports | Servidor de procesamiento de Crystal Reports 2011<br>Servidor de procesamiento de Crystal Reports (para SAP Crystal Reports para informes de Enterprise) | Servidor de procesamiento de Crystal Reports 2011<br>Servidor de procesamiento de Crystal Reports (para SAP Crystal Reports para informes de Enterprise) | Servidor de procesamiento de Crystal Reports 2013<br>Servidor de procesamiento de Crystal Reports (para SAP Crystal Reports para informes de Enterprise) | Servidor de procesamiento de Crystal Reports 2016<br>Servidor de procesamiento de Crystal Reports (para SAP Crystal Reports para informes de Enterprise) | Servidor de procesamiento de Crystal Reports 2020<br>Servidor de procesamiento de Crystal Reports (para SAP Crystal Reports para informes de Enterprise) |
| Servidor de cuadros de mandos (Generador de cuadros de mandos) [2] | Servidor de Dashboard (Áreas de trabajo de BI) | No disponible como Feature Pack 3 de 4.0 | No disponible en 4.1 | No disponible en 4.2 | No disponible en 4.3 |
| Servidor de analíticas de cuadros de mandos (Generador de cuadros de mandos) [2] | Servidor de analíticas de cuadros de mandos (Áreas de trabajo de BI) | No disponible como Feature Pack 3 de 4.0 | No disponible en 4.1 | No disponible en 4.2 | No disponible en 4.3 |
| Servidor de caché de Desktop Intelligence [3] | No disponible para 4.0 | No disponible para 4.0 | No disponible en 4.1 [3] | No disponible en 4.2 [3] | No disponible en 4.3 [3] |
| Servidor de tareas de Desktop Intelligence [3] | No disponible para 4.0 | No disponible para 4.0 | No disponible en 4.1 [3] | No disponible en 4.2 [3] | No disponible en 4.3 [3] |
| Servidor de procesamiento de Desktop Intelligence [3] | No disponible para 4.0 | No disponible para 4.0 | No disponible en 4.1 [3] | No disponible en 4.2 [3] | No disponible en 4.3 [3] |
| Servidor de tareas de destino | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive |
| Servidor de análisis multidimensional | Servidor de procesamiento de Adaptive | Servidor de procesamiento de Adaptive | Servidor de procesamiento de Adaptive | Servidor de procesamiento de Adaptive | Servidor de procesamiento de Adaptive |
| Servidor de tareas de programa | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive |
| Servidor de aplicaciones de informes (RAS) | Servidor de aplicaciones de informes (RAS) de Crystal Reports 2011 | Servidor de aplicaciones de informes (RAS) de Crystal Reports 2011 | Servidor de aplicaciones de informes (RAS) de Crystal Reports 2013 | Servidor de aplicaciones de informes (RAS) de Crystal Reports 2016 | Servidor de aplicaciones de informes (RAS) de Crystal Reports 2020 |

| XI 3.1 | 4,0 | Feature Pack 3 para 4.0 | 4,1 | 4,2 | 4,3 |
|---|---|---|---|---|---|
| Servidor de tareas de Web Intelligence | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive | Servidor de tareas de Adaptive |
| Servidor de caché de Xcelsius [4] | Servidor de caché de Dashboard Design (Xcelsius) [5] | Servidor de caché de Dashboards (Xcelsius) | Servidor de caché de Dashboards (Xcelsius) | Servidor de caché de Dashboards (Xcelsius) | No disponible en 4.3 [7] |
| Servidor de procesamiento de Xcelsius [4] | Servidor de procesamiento de Dashboard Design (Xcelsius) [5] | Servidor de procesamiento de Dashboards (Xcelsius) | Servidor de procesamiento de Dashboards (Xcelsius) | Servidor de procesamiento de Dashboards (Xcelsius) | No disponible en 4.3 [7] |
| Partes web específicas de contenido [6] | Visor de informes de Crystal, Visor Xcelsius y Visor de informes analíticos | Visor de informes de Crystal, Visor Xcelsius y Visor de informes analíticos | Visor de informes de Crystal, Visor Xcelsius y Visor de informes analíticos | Visor de informes de Crystal, Visor Xcelsius y Visor de informes analíticos | Las partes web específicas de contenido quedarán obsoletas en 4.3 |

- [1] En 4.0, el servidor de conexión 32 es de 32 bits y ejecuta conexiones específicamente para orígenes de datos que no soportan el middleware de 64 bits. El servidor de conexión es de 64 bits y ejecuta conexiones para el resto de orígenes de datos. Para obtener más información, consulte el *Manual de acceso a los datos*.
- [2] El servidor de cuadros de mandos y el servidor de analíticas de cuadros de mandos se han eliminado del Feature Pack 3 de 4.0. Ya no se requiere configurar el servidor para la funcionalidad de área de trabajo de BI (antes generador de cuadros de mandos en XI 3.1).
- [3] Desktop Intelligence no estaba disponible en la versión 4.0 ni en los paquetes de mantenimiento 4.0. La aplicación de cliente de Desktop Intelligence está disponible en la versión 4.1, pero no los servidores de Desktop Intelligence. Los informes de Desktop Intelligence se pueden convertir en documentos de Web Intelligence mediante la herramienta de conversión de informes.
- [4] Los servicios de caché y de procesamiento de Xcelsius se presentaron en el Feature Pack 3 de XI 3.1 para optimizar las solicitudes Consulta como servicio Web en orígenes de datos relacionales de Xcelsius. Los servicios de caché y de procesamiento equivalentes están disponibles en el servidor de caché de cuadros de mandos y en el servicio de procesamiento de cuadros de mandos del Feature Pack 3 de 4.0.
- [5] Se ha cambiado el nombre de los servidores de Dashboard Design en 4.0 a «Dashboards» en el Feature Pack 3 de 4.0 para alinearlo con el cambio de nombre de producto a SAP BusinessObjects Dashboards.
- [6] Las siguientes partes web específicas de contenido quedarán obsoletas en 4.3:
  - Visor de informes de Crystal
  - Visor Xcelsius
  - Visor de informes analíticos
- [7] Tanto el servidor de procesamiento de dashboards (Xcelsius) como el servidor de caché de dashboards (Xcelsius) han quedado obsoletos.

## 3.2.2 Servicios

Al agregar servidores, debe incluir algunos servicios en el servidor de tareas de Adaptive. Por ejemplo, el servicio de programación de entrega en destino.

> **Nota**
>
> - Es posible que se añadan nuevos servicios o tipos de servidores en futuras versiones de mantenimiento.
> - El servicio de programación Java de modelo se consume sólo para el desarrollo interno y no está disponible para el consumo por partes implicadas externas.

| Servicio | Categoría de servicio | Tipo de servidor | Descripción del servicio |
|---|---|---|---|
| Servicio de conectividad de Adaptive | Servicios de conectividad | Servidor de procesamiento de Adaptive | Proporciona servicios de conectividad para controladores basados en Java |
| Servicio de Analytics Hub | Servicios principales | Servidor de procesamiento de Adaptive | Este servicio se ejecuta en el servidor de procesamiento de Adaptive y se comunica con el sistema SAP Analytics Cloud y SAP Analytics Hub. |
| Servicio de programación de actualización de autenticaciones | Servicios principales | Servidor de tareas de Adaptive | Proporciona la sincronización de actualizaciones para complementos de seguridad de terceros |
| Servicio de aplicación Web BEx | Servicios de análisis | Servidor de procesamiento de Adaptive | Proporciona la integración de aplicaciones Web SAP Business Warehouse (BW) Business Explorer (BEx) con la plataforma de lanzamiento de BI. |
| BIMobileService(OCA) | Servicios principales | Servidor de procesamiento de Adaptive | Activa notificaciones push en dispositivos móviles. |
| Servicio de contenedor de aplicaciones Web | Servicios principales | Servidor de contenedor de aplicación Web | Proporciona aplicaciones Web para WACS: incluye la Consola de administración central (CMC), la plataforma de lanzamiento de BI y OpenDocument. |

| Servicio | Categoría de servicio | Tipo de servidor | Descripción del servicio |
|---|---|---|---|
| Servicio de administración central | Servicios principales | Servidor de administración central | Proporciona servidor, usuario, administración de sesión y administración de seguridad (derechos de acceso y autenticación). Debe estar disponible al menos un Servicio de administración central en un clúster para que el clúster funcione. |
| Servicio proxy de auditoría de cliente | Servicios principales | Servidor de procesamiento de Adaptive | Recopila eventos de auditoría enviados desde clientes y los reenvía al servidor del CMS. |
| Servicio de comentarios | Servicios principales | Servidor de procesamiento de Adaptive | Permite operaciones de comentario en documentos. |
| Servicio de procesamiento de Crystal Reports 2020 | Servicios de Crystal Reports | Servidor de procesamiento de Crystal Reports | Acepta y procesa informes de Crystal Reports 2020; puede compartir datos entre informes para reducir el número de accesos a la base de datos. |
| Servicio de programación de Crystal Reports 2020 | Servicios de Crystal Reports | Servidor de tareas de Adaptive | Ejecuta tareas de Crystal Reports existentes y publica los resultados en una ubicación de salida. |
| Servicio de visualización y modificación de Crystal Reports 2020 | Servicios de Crystal Reports | Servidor de aplicaciones de informes (RAS) | Vistas de procesos y solicitudes de modificación para informes de Crystal Reports 2020. |
| Servicio de caché de Crystal Reports | Servicios de Crystal Reports | Servidor de caché de Crystal Reports | Limita el número de accesos a la base de datos generados desde informes de Crystal y acelera la generación de informes al administrar una caché de informes. |
| Servicio de procesamiento de Crystal Reports | Servicios de Crystal Reports | Servidor de procesamiento de Crystal Reports | Acepta y procesa informes de Crystal; puede compartir datos entre informes para reducir el número de accesos a la base de datos. |
| Servicio de programación de Crystal Reports | Servicios de Crystal Reports | Servidor de tareas de Adaptive | Ejecuta nuevas tareas de Crystal Reports programadas y publica los resultados en una ubicación de salida. |

| Servicio | Categoría de servicio | Tipo de servidor | Descripción del servicio |
|---|---|---|---|
| Servicio de acceso a datos personalizado | Servicios de Web Intelligence | Servidor de procesamiento de Adaptive | Proporciona conexiones dinámicas a orígenes de datos que no necesitan un servidor de conexión. Este servicio permite acceder y actualizar informes creados con algunos proveedores de datos personales como archivos CSV files. Consulte el *Manual de usuario de cliente enriquecido de SAP BusinessObjects Web Intelligence* para obtener más información sobre la creación de una consulta o la actualización de un documento basado en un archivo de texto. |
| Servicio de federación de datos | Servicios de federación de datos | Servidor de procesamiento de Adaptive | Consulta y procesa los orígenes de datos subyacentes para un universo de varios orígenes |
| Servicio de programación de entrega de destino | Servicios principales | Servidor de tareas de Adaptive | Ejecuta tareas programadas y publica los resultados en una ubicación de salida, como un sistema de archivos, un servidor FTP, un servidor SFTP, un correo electrónico o la bandeja de entrada de un usuario.<br>**Nota**<br>Cuando se añaden servidores, debe incluir algunos servicios del servidor de tareas Adaptive, incluido este servicio. |
| Servicio de recuperación de documentos | Servicios de Web Intelligence | Servidor de procesamiento de Adaptive | Guardado automático y recuperación de documentos de Web Intelligence |
| Servicio de DSL Bridge | Servicios de Web Intelligence | Servidor de procesamiento de Adaptive | Compatibilidad de la sesión de la capa semántica de dimensión (DSL) |

| Servicio | Categoría de servicio | Tipo de servidor | Descripción del servicio |
|---|---|---|---|
| Servicio de eventos | Servicios principales | Servidor de eventos | Supervisa los eventos de archivos en un servidor de repositorio de archivos (FRS) y desencadena los informes para que se ejecuten cuando sea necesario |
| Servicio de acceso a datos de Excel | Servicios de Web Intelligence | Servidor de procesamiento de Adaptive | Admite archivos Excel cargados en la plataforma de BI como orígenes de datos. Consulte *Manual de usuario de cliente enriquecido de SAP BusinessObjects Web Intelligence* para obtener más información sobre la creación de una consulta o la actualización de un documento basado en un archivo de Excel. |
| Servicio del motor de información | Servicios de Web Intelligence | Servidor de procesamiento de Web Intelligence | Servicio necesario para procesar documentos de Web Intelligence |
| Servicio de almacenamiento de archivos de entrada | Servicios principales | Servidor del repositorio de archivos de entrada | Conserva informes publicados y objetos de programa que se pueden usar en la generación de nuevos informes al recibir un archivo de entrada |
| Servicio Insight to Action | Servicios principales | Servidor de procesamiento de Adaptive | Permite que se invoquen acciones y proporciona compatibilidad para RRI |
| Servicio ClearCase de administración de promociones | Servicios de administración de promociones | Servidor de procesamiento de Adaptive | Proporciona compatibilidad ClearCase para LCM |
| Servicio programación de administración de promociones | Servicios de administración de promociones | Servidor de tareas de Adaptive | Ejecuta tareas de administración de promoción programadas |
| Servicio de administración de promociones | Servicios de administración de promociones | Servidor de procesamiento de Adaptive | Servicio principal de la administración de promociones |
| Servicio de supervisión | Servicios principales | Servidor de procesamiento de Adaptive | Proporciona funciones de supervisión |

| Servicio | Categoría de servicio | Tipo de servidor | Descripción del servicio |
|---|---|---|---|
| Servicio de análisis multidimensional | Servicios de análisis | Servidor de procesamiento de Adaptive | Proporciona acceso a datos de procesamiento analítico en línea (OLAP) multidimensionales; convierte los datos sin procesar en XML, que se pueden procesar en tablas de referencias cruzadas y gráficos de Excel, PDF o Analysis (antes Voyager) |
| Servicio de conectividad nativa | Servicios de conectividad | Servidor de conexión | Proporciona servicios de conectividad nativa para arquitecturas de 64 bits |
| Servicio de conectividad nativa (32 bits) | Servicios de conectividad | Servidor de conexión | Proporciona servicios de conectividad nativa para arquitecturas de 32 bits |
| Servicio de almacenamiento de archivos de salida | Servicios principales | Servidor del repositorio de archivos de salida | Conserva una colección de documentos finalizados |
| Servicio de programación de búsqueda en plataforma | Servicios principales | Servidor de tareas de Adaptive | Ejecuta búsquedas programadas para indexar todo el contenido en el repositorio del Servidor de administración central (CMS) |
| Servicio de búsqueda de plataforma | Servicios principales | Servidor de procesamiento de Adaptive | Proporciona la funcionalidad de búsqueda para la plataforma de BI |
| Servicio de programación de métrica | Servicios principales | Servidor de tareas de Adaptive | Proporciona tareas de métricas programadas y publica los resultados en una ubicación de salida |
| Servicio de programación de programa | Servicios principales | Servidor de tareas de Adaptive | Ejecuta programas que se han programado para ejecutarse en un momento determinado |
| Servicio de programación de publicación | Servicios principales | Servidor de tareas de Adaptive | Ejecuta tareas de publicación programadas y publica los resultados en una ubicación de salida |
| Servicio de publicación posterior al procesamiento | Servicios principales | Servidor de procesamiento de Adaptive | Efectúa acciones en informes después de que hayan finalizado, como enviar un informe a una ubicación de salida |

| Servicio | Categoría de servicio | Tipo de servidor | Descripción del servicio |
|---|---|---|---|
| Servicio de publicación | Servicios principales | Servidor de procesamiento de Adaptive | Se coordina con el servicio de publicación posterior al procesamiento y el servicio de tareas de destino para publicar informes en una ubicación de salida, como un sistema de archivos, un servidor FTP, un servidor SFTP, un correo electrónico o la bandeja de entrada de un usuario. |
| Servicio Rebean | Servicios de Web Intelligence | Servidor de procesamiento de Adaptive | SDK que utilizan Web Intelligence y Explorer |
| Servicio de réplica | Servicios principales | Servidor de tareas de Adaptive | Ejecuta tareas de federación programadas para replicar el contenido entre sitios federados |
| Servicio Web RESTful | Servicios principales | Servidor de contenedor de aplicación Web (WACS) | Proporciona la administración de sesiones para solicitudes de servicio Web RESTful. |
| Servicio de programación de consulta de seguridad | Servicios principales | Servidor de tareas de Adaptive | Ejecuta tareas de consulta de seguridad programadas |
| Servicio de token de seguridad | Servicios principales | Servidor de procesamiento de Adaptive | Soporte de inicio de sesión único de SAP |
| Servicio de materialización de conjuntos. | Servicios principales | Servidor de procesamiento de Adaptive | Opera la materialización de conjuntos y grupos de conjuntos. |
| Servicio de programación de materialización de conjuntos | Servicios principales | Servidor de tareas de Adaptive | Permite programar conjuntos y grupos de conjuntos para su materialización. |
| Servicio de traducción | Servicios principales | Servidor de procesamiento de Adaptive | Traduce InfoObjects con entradas del cliente del administrador de traducciones |
| Servicio de programación para importar usuarios y grupos | Servicios principales | Servidor de tareas de Adaptive | Permite programar importaciones de archivos principales |
| Servicio de programación de diferencia visual | Servicios de administración de promociones | Servidor de tareas de Adaptive | Ejecuta tareas de diferencia visual (administración de promociones) programadas y publica los resultados en una ubicación de salida |

| Servicio | Categoría de servicio | Tipo de servidor | Descripción del servicio |
|---|---|---|---|
| Servicio de diferencia visual | Servicios de administración de promociones | Servidor de procesamiento de Adaptive | Determina si los documentos son visualmente idénticos para la promoción de documentos y la administración de promociones |
| Servicio de visualización | Servicios de Web Intelligence | Servidor de procesamiento de Adaptive | Servicio de modelo de objeto de visualización común, usado por Web Intelligence |
| Servicio común de Web Intelligence | Servicios de Web Intelligence | Servidor de procesamiento de Web Intelligence | Admite el procesamiento de documentos de Web Intelligence |
| Servicio central de Web Intelligence | Servicios de Web Intelligence | Servidor de procesamiento de Web Intelligence | Admite el procesamiento de documentos de Web Intelligence |
| Servicio de procesamiento de Web Intelligence | Servicios de Web Intelligence | Servidor de procesamiento de Web Intelligence | Acepta y procesa los documentos de Web Intelligence |
| Servicio de programación de Web Intelligence | Servicios de Web Intelligence | Servidor de tareas de Adaptive | Habilita la admisión de tareas programadas para Web Intelligence |
| Servicio de administración de versiones | Servicios de administración de promociones | Servidor de procesamiento de Adaptive | Gestionar múltiples versiones de recursos BI utilizando IBM Rational ClearCase o Apache Subversion. |

## 3.2.3 Categorías de servicio

> **Nota**
>
> Es posible que se añadan nuevos servicios o tipos de servidores en futuras versiones de mantenimiento.

| Categoría de servicio | Servicio | Tipo de servidor |
|---|---|---|
| Servicios de análisis | Servicio de aplicación Web BEx | Servidor de procesamiento de Adaptive |
| Servicios de análisis | Servicio de análisis multidimensional | Servidor de procesamiento de Adaptive |
| Servicios de conectividad | Servicio de conectividad de Adaptive | Servidor de procesamiento de Adaptive |
| Servicios de conectividad | Servicio de conectividad nativa | Servidor de conexión |
| Servicios de conectividad | Servicio de conectividad nativa (32 bits) | Servidor de conexión |
| Servicios principales | Servicio de Analytics Hub | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de programación de actualización de autenticaciones | Servidor de tareas de Adaptive |

| Categoría de servicio | Servicio | Tipo de servidor |
|---|---|---|
| Servicios principales | BIMobileService(OCA) | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de administración central | Servidor de administración central |
| Servicios principales | Servicio proxy de auditoría de cliente | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de comentarios | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de configuración de destino | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de programación de entrega de destino | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de eventos | Servidor de eventos |
| Servicios principales | Servicio Insight to Action | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de almacenamiento de archivos de entrada | Servidor del repositorio de archivos de entrada |
| Servicios principales | Servicio de supervisión | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de almacenamiento de archivos de salida | Servidor del repositorio de archivos de salida |
| Servicios principales | Servicio de programación de búsqueda en plataforma | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de búsqueda de plataforma | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de programación de análisis | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de programación de programa | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de programación de publicación | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de publicación posterior al procesamiento | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de publicación | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio Web RESTful | Servidor de contenedor de aplicación Web |
| Servicios principales | Servicio de réplica | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de programación de consulta de seguridad | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de token de seguridad | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de materialización de conjuntos. | Servidor de procesamiento de Adaptive |
| Servicios principales | Definición del servicio de programación de materialización | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de inicio de sesión único | Servidor de administración central, servidor de conexión, servidor de procesamiento de Crystal Reports, RAS y servidor de procesamiento de Web Intelligence |
| Servicios principales | Servicio de registro de seguimiento | Cualquier servidor |

| Categoría de servicio | Servicio | Tipo de servidor |
|---|---|---|
| Servicios principales | Servicio de traducción | Servidor de procesamiento de Adaptive |
| Servicios principales | Servicio de programación para importar grupos y usuarios | Servidor de tareas de Adaptive |
| Servicios principales | Servicio de contenedor de aplicaciones Web | Servidor de contenedor de aplicación Web |
| Servicios de Crystal Reports | Servicio de procesamiento de Crystal Reports 2020 | Servidor de procesamiento de Crystal Reports |
| Servicios de Crystal Reports | Servicio de programación de Crystal Reports 2020 | Servidor de tareas de Adaptive |
| Servicios de Crystal Reports | Servicio de visualización y modificación de Crystal Reports 2020 | Servidor de aplicaciones de informes (RAS) |
| Servicios de Crystal Reports | Servicio de caché de Crystal Reports | Servidor de caché de Crystal Reports |
| Servicios de Crystal Reports | Servicio de procesamiento de Crystal Reports | Servidor de procesamiento de Crystal Reports |
| Servicios de Crystal Reports | Servicio de programación de Crystal Reports | Servidor de tareas de Adaptive |
| Servicios de federación de datos | Servicio de federación de datos | Servidor de procesamiento de Adaptive |
| Servicios de administración de ciclo de vida | Servicio ClearCase de administración de promociones | Servidor de procesamiento de Adaptive |
| Servicios de administración de ciclo de vida | Servicio programación de administración de promociones | Servidor de tareas de Adaptive |
| Servicios de administración de ciclo de vida | Servicio de administración de promociones | Servidor de procesamiento de Adaptive |
| Servicios de administración de ciclo de vida | Servicio de programación de diferencia visual | Servidor de tareas de Adaptive |
| Servicios de administración de ciclo de vida | Servicio de diferencia visual | Servidor de procesamiento de Adaptive |
| Servicios de Web Intelligence | Servicio de acceso a datos personalizado | Servidor de procesamiento de Adaptive |
| Servicios de Web Intelligence | Servicio de recuperación de documentos | Servidor de procesamiento de Adaptive |
| Servicios de Web Intelligence | Servicio de DSL Bridge | Servidor de procesamiento de Adaptive |
| Servicios de Web Intelligence | Servicio de acceso a datos de Excel | Servidor de procesamiento de Adaptive |
| Servicios de Web Intelligence | Servicio del motor de información | Servidor de procesamiento de Web Intelligence |
| Servicios de Web Intelligence | Servicio Rebean | Servidor de procesamiento de Adaptive |
| Servicios de Web Intelligence | Servicio de visualización | Servidor de procesamiento de Adaptive |
| Servicios de Web Intelligence | Servicio común de Web Intelligence | Servidor de procesamiento de Web Intelligence |
| Servicios de Web Intelligence | Servicio central de Web Intelligence | Servidor de procesamiento de Web Intelligence |

| Categoría de servicio | Servicio | Tipo de servidor |
|---|---|---|
| Servicios de Web Intelligence | Servicio de supervisión de Web Intelligence | Servidor de procesamiento de Adaptive |
| Servicios de Web Intelligence | Servicio de procesamiento de Web Intelligence | Servidor de procesamiento de Web Intelligence |
| Servicios de Web Intelligence | Servicio de programación de Web Intelligence | Servidor de tareas de Adaptive |
| Servicios de administración de promociones | Servicio de administración de versiones | Servidor de procesamiento de Adaptive |

## 3.2.4 Tipos de servidor

Un asterisco junto a un nombre de servicio indica que es un servicio secundario. Algunos servicios secundarios se crean automáticamente, pero debe seleccionar incluir otros servicios secundarios después de seleccionar el servicio principal del que depende un servicio secundario.

> **Nota**
>
> Es posible que se añadan nuevos servicios o tipos de servidores en futuras versiones de mantenimiento.

| Tipo de servidor | Servicio | Categoría de servicio |
|---|---|---|
| Cualquier servidor | Servicio de registro de seguimiento | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de actualización de autenticaciones | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de Crystal Reports 2020 | Servicios de Crystal Reports |
| Servidor de tareas de Adaptive | Servicio de programación de Crystal Reports | Servicios de Crystal Reports |
| Servidor de tareas de Adaptive | Servicio de configuración de destino | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de entrega de destino | Servicios principales |
| Servidor de tareas de Adaptive | Servicio programación de administración de promociones | Servicios de administración de promociones |
| Servidor de tareas de Adaptive | Servicio de programación de búsqueda en plataforma | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de métrica | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de programa | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de publicación | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de réplica | Servicios principales |

| Tipo de servidor | Servicio | Categoría de servicio |
|---|---|---|
| Servidor de tareas de Adaptive | Servicio de programación de consulta de seguridad | Servicios principales |
| Servidor de tareas de Adaptive | Fijar servicios de programación de materialización | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación para importar grupos y usuarios | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de diferencia visual | Servicios de administración de promociones |
| Servidor de tareas de Adaptive | Servicio de programación de Web Intelligence | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de conectividad de Adaptive | Servicios de conectividad |
| Servidor de procesamiento de Adaptive | Servicios de Analytical Hub | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de aplicación Web BEx | Servicios de análisis |
| Servidor de procesamiento de Adaptive | Servicio proxy de auditoría de cliente | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de acceso a datos personalizado | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de federación de datos | Servicios de federación de datos |
| Servidor de procesamiento de Adaptive | Servicio de recuperación de documentos | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de DSL Bridge | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de acceso a datos de Excel | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio Insight to Action | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio ClearCase de administración de promociones | Servicios de administración de promociones |
| Servidor de procesamiento de Adaptive | Servicio de administración de promociones | Servicios de administración de promociones |
| Servidor de procesamiento de Adaptive | Servicio de supervisión | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de análisis multidimensional | Servicios de análisis |
| Servidor de procesamiento de Adaptive | Servicio de búsqueda de plataforma | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de publicación posterior al procesamiento | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de publicación | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio Rebean | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de token de seguridad | Servicios principales |
| Servidor de procesamiento de Adaptive | Fijar servicio de materialización | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de traducción | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de diferencia visual | Servicios de administración de promociones |

| Tipo de servidor | Servicio | Categoría de servicio |
|---|---|---|
| Servidor de procesamiento de Adaptive | Servicio de visualización | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de supervisión de Web Intelligence | Servicios de Web Intelligence |
| Servidor de administración central | Servicio de administración central | Servicios principales |
| Servidor de administración central | Servicio de inicio de sesión único | Servicios principales |
| Servidor de conexión | Servicio de conectividad nativa | Servicios de conectividad |
| Servidor de conexión | Servicio de conectividad nativa (32 bits) | Servicios de conectividad |
| Servidor de conexión | Servicio de inicio de sesión único | Servicios principales |
| Servidor de caché de Crystal Reports | Servicio de caché de Crystal Reports | Servicios de Crystal Reports |
| Servidor de procesamiento de Crystal Reports | Servicio de procesamiento de Crystal Reports 2020 | Servicios de Crystal Reports |
| Servidor de procesamiento de Crystal Reports | Servicio de procesamiento de Crystal Reports | Servicios de Crystal Reports |
| Servidor de procesamiento de Crystal Reports | Servicio de inicio de sesión único | Servicios principales |
| Servidor de eventos | Servicio de eventos | Servicios principales |
| Servidor del repositorio de archivos de entrada | Servicio de almacenamiento de archivos de entrada | Servicios principales |
| Servidor del repositorio de archivos de salida | Servicio de almacenamiento de archivos de salida | Servicios principales |
| Servidor de aplicaciones de informes (RAS) | Servicio de visualización y modificación de Crystal Reports 2020 | Servicios de Crystal Reports |
| RAS | Servicio de inicio de sesión único | Servicios principales |
| Servidor de contenedor de aplicación Web | Servicio Web RESTful | Servicios principales |
| Servidor de contenedor de aplicación Web | Servicio de contenedor de aplicaciones Web | Servicios principales |
| Servidor de procesamiento de Web Intelligence | Servicio del motor de información | Servicios de Web Intelligence |
| Servidor de procesamiento de Web Intelligence | Servicio de inicio de sesión único | Servicios principales |
| Servidor de procesamiento de Web Intelligence | Servicio común de Web Intelligence | Servicios de Web Intelligence |
| Servidor de procesamiento de Web Intelligence | Servicio central de Web Intelligence | Servicios de Web Intelligence |
| Servidor de procesamiento de Web Intelligence | Servicio de procesamiento de Web Intelligence | Servicios de Web Intelligence |

| Tipo de servidor | Servicio | Categoría de servicio |
|---|---|---|
| Servidor de tareas de Adaptive | Servicio de programación de actualización de autenticaciones | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de Crystal Reports 2020 | Servicios de Crystal Reports |
| Servidor de tareas de Adaptive | Servicio de programación de Crystal Reports | Servicios de Crystal Reports |
| Servidor de tareas de Adaptive | Servicio de programación de entrega de destino | Servicios principales |
| Servidor de tareas de Adaptive | Servicio programación de administración de promociones | Servicios de administración de promociones |
| Servidor de tareas de Adaptive | Servicio de programación de búsqueda en plataforma | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de métrica | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de programa | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de publicación | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de réplica | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de consulta de seguridad | Servicios principales |
| Servidor de tareas de Adaptive | Servicio de programación de diferencia visual | Servicios de administración de promociones |
| Servidor de tareas de Adaptive | Servicio de programación de Web Intelligence | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de conectividad de Adaptive | Servicios de conectividad |
| Servidor de procesamiento de Adaptive | Servicio de aplicación Web BEx | Servicios de análisis |
| Servidor de procesamiento de Adaptive | Servicio proxy de auditoría de cliente | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de acceso a datos personalizado | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de federación de datos | Servicios de federación de datos |
| Servidor de procesamiento de Adaptive | Servicio de recuperación de documentos | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de DSL Bridge | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de acceso a datos de Excel | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio Insight to Action | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio ClearCase de administración de promociones | Servicios de administración de promociones |
| Servidor de procesamiento de Adaptive | Servicio de administración de promociones | Servicios de administración de promociones |
| Servidor de procesamiento de Adaptive | Servicio de supervisión | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de análisis multidimensional | Servicios de análisis |

| Tipo de servidor | Servicio | Categoría de servicio |
|---|---|---|
| Servidor de procesamiento de Adaptive | Servicio de búsqueda de plataforma | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de publicación posterior al procesamiento | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de publicación | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio Rebean | Servicios de Web Intelligence |
| Servidor de procesamiento de Adaptive | Servicio de token de seguridad | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de traducción | Servicios principales |
| Servidor de procesamiento de Adaptive | Servicio de diferencia visual | Servicios de administración de promociones |
| Servidor de procesamiento de Adaptive | Servicio de visualización | Servicios de Web Intelligence |
| Servidor de administración central | Servicio de administración central | Servicios principales |
| Servidor de conexión | Servicio de conectividad nativa | Servicios de conectividad |
| Servidor de conexión | Servicio de conectividad nativa (32 bits) | Servicios de conectividad |
| Servidor de caché de Crystal Reports | Servicio de caché de Crystal Reports | Servicios de Crystal Reports |
| Servidor de procesamiento de Crystal Reports | Servicio de procesamiento de Crystal Reports 2020 | Servicios de Crystal Reports |
| Servidor de procesamiento de Crystal Reports | Servicio de procesamiento de Crystal Reports | Servicios de Crystal Reports |
| Servidor de eventos | Servicio de eventos | Servicios principales |
| Servidor del repositorio de archivos de entrada | Servicio de almacenamiento de archivos de entrada | Servicios principales |
| Servidor del repositorio de archivos de salida | Servicio de almacenamiento de archivos de salida | Servicios principales |
| Servidor de aplicaciones de informes (RAS) | Servicio de visualización y modificación de Crystal Reports 2020 | Servicios de Crystal Reports |
| Servidor de contenedor de aplicación Web | Servicio Web RESTful | Servicios principales |
| Servidor de procesamiento de Web Intelligence | Servicio del motor de información | Servicios de Web Intelligence |
| Servidor de procesamiento de Web Intelligence | Servicio común de Web Intelligence | Servicios de Web Intelligence |
| Servidor de procesamiento de Web Intelligence | Servicio central de Web Intelligence | Servicios de Web Intelligence |
| Servidor de procesamiento de Web Intelligence | Servicio de procesamiento de Web Intelligence | Servicios de Web Intelligence |

## 3.2.5 Servidores

Los servidores son colecciones de servicios que se ejecutan en un Server Intelligence Agent (SIA) en un host. El tipo de servidor se determina por los servicios que se ejecutan en él. Los servidores se pueden crear en la Consola de administración central (CMC). En la siguiente tabla se enumeran los diferentes tipos de servidores que se pueden crear en la CMC.

| Servidor | Descripción |
|---|---|
| Servidor de tareas de Adaptive | Un servidor genérico que procesa tareas programadas. Al agregar un servidor de tareas al sistema de la plataforma de BI, puede configurar el servidor de tareas para procesar informes, documentos, programas o publicaciones, y para enviar los resultados a diferentes destinos. |
| Servidor de procesamiento de Adaptive | Un servidor genérico que aloja los servicios responsables del procesamiento de las solicitudes desde varios orígenes.<br><br>El programa de instalación instala un servidor de procesamiento de Adaptive (APS) por sistema de host. Dependiendo de las funciones que tenga instaladas, este APS puede alojar un gran número de servicios, como el servicio de supervisión, el servicio de administración de ciclo de vida, el servicio de análisis multidimensional (MDAS), el servicio de publicación, entre otros.<br><br>Para los sistemas de producción o de prueba, la mejor práctica es crear APS adicionales y configurar los APS para que cumplan con los requisitos empresariales. Para más información, consulte Introducción al Asistente de configuración del sistema [página 91] y Configurar servidores de procesamiento de Adaptive para sistemas de producción [página 458]. |
| Servidor de administración central (CMS) | Conserva una base de datos de información acerca del sistema de la plataforma de BI (en la base de datos del sistema del CMS) y acciones de usuarios auditados (en el almacén de datos de auditoría). El CMS administra todos los servicios de la plataforma. El CMS también controla el acceso a los archivos del sistema en el que se almacenan los documentos y la información de los usuarios, grupos de usuarios, niveles de seguridad (incluyendo la autenticación y la autorización) y el contenido. |
| Servidor de conexión | Proporciona acceso a la base de datos para los datos de origen. Admite bases de datos relacionales, así como OLAP y otros formatos. El Servidor de conexión es el responsable de gestionar la conexión y la interacción con los diferentes orígenes de datos y proporcionar un conjunto de funciones comunes a los clientes. |
| Servidor de caché de Crystal Reports | Intercepta las solicitudes de informe enviadas desde clientes al servidor de páginas. Si el servidor de caché no puede cumplir la solicitud con una página de informe almacenada en caché, para la solicitud al servidor de procesamiento de Crystal Reports,, que ejecuta el informe |

| Servidor | Descripción |
| --- | --- |
| | y devuelve los resultados. A continuación, el servidor de caché almacena en caché la página del informe para un uso futuro. |
| Servidor de procesamiento de Crystal Reports | Responde a solicitudes de página mediante el procesamiento de informes y la generación de páginas en formato encapsulado (EPF). La ventaja clave del EPF es que admite el acceso de páginas a petición, de modo que sólo de devuelve la página solicitada, no todo el informe. Esto mejora el rendimiento del sistema y reduce el tráfico de red innecesario en los informes grandes. |
| Servidor de eventos | Supervisa el sistema en busca de eventos , que pueden actuar como desencadenadores para ejecutar un informe. Al configurar un desencadenador de eventos, el servidor de eventos supervisa la condición y notifica al CMS que se ha producido el evento. A continuación, el CMS puede iniciar las tareas que se configuren para que inicien en el evento. El servidor de eventos administra los eventos basados en archivos que ocurren en el nivel de almacenamiento. |
| Servidor del repositorio de archivos | Responsable de la creación de objetos del sistema, como informes exportados y archivos importados en formatos no nativos. Un FRS de entrada almacena objetos de informes y programas que los administradores o usuarios finales han publicado en el sistema. Un FRS de salida almacena todas las instancias de informes generadas por el servidor de tareas. |
| Servidor de procesamiento de Web Intelligence | Procesa documentos de SAP BusinessObjects Web Intelligence. |
| Servidor de aplicaciones de informes | Proporciona funcionalidad de generación de informes ad hoc que permite a los usuarios crear y modificar informes de Crystal mediante el kit de desarrollo de software (SDK) de SAP Crystal Reports Server Embedded. |

## 3.3 Aplicaciones cliente

Puede interactuar con la plataforma de BI mediante dos tipos principales de aplicaciones de cliente:

- Aplicaciones de escritorio
  Estas aplicaciones se deben instalar en un sistema operativo de Microsoft Windows admitido, y pueden procesar datos y crear informes de forma local.

  > **Nota**
  >
  > El programa de instalación de la plataforma de BI ya no instala las aplicaciones de escritorio. Para instalar aplicaciones de escritorio en un servidor, use el programa de instalación independiente de las herramientas cliente de la plataforma de SAP BusinessObjects Business Intelligence.

  Los clientes de escritorio permiten descargar algunos procesamientos de informes de BI en equipos cliente concretos. La mayoría de las aplicaciones de escritorio tienen directamente acceso a los datos de

su organización a través de controladores instalados en el escritorio, y se comunican con el despliegue de la plataforma de BI a través de CORBA o de CORBA SSL cifrado.
Entre los ejemplos de este tipo de aplicación se encuentran Crystal Reports y Live Office.

> **Nota**
>
> A pesar de que Live Office es una aplicación de funcionalidad enriquecida, interactúa con los servicios Web de la plataforma de BI a través de HTTP.

- Aplicaciones Web
  Un servidor de aplicaciones Web aloja estas aplicaciones, y se puede acceder a ellas con un explorador Web admitido en los sistemas operativos de Windows, Macintosh, Unix y Linux.
  Esto permite proporcionar acceso a Business Intelligence (BI) a grandes grupos de usuarios sin tener que afrontar los retos de implementar productos de software de escritorio. La comunicación se lleva a cabo a través de HTTP, con o sin cifrado SSL (HTTPS).
  Ejemplos de este tipo de aplicación son la plataforma de lanzamiento de BI, SAP BusinessObjects Web Intelligence, la consola de administración central (CMC) y los visores de informes.

## 3.3.1 Instalado con las herramientas de cliente de la plataforma SAP BusinessObjects Business Intelligence

### 3.3.1.1 Cliente enriquecido de Web Intelligence

El Cliente enriquecido de Web Intelligence es una herramienta de análisis y creación de informes especial para los usuarios empresariales con o sin acceso a la plataforma de BI.

Permite a los usuarios empresariales acceder a los datos mediante universos (.unv and .unx), consultas BEx, u otros orígenes, usando términos empresariales familiares en una interfaz de arrastrar y soltar. Los flujos de trabajo permiten analizar preguntas muy amplias o muy concretas, y que se realicen preguntas posteriores en un punto del flujo de trabajo del análisis.

Los usuarios del Cliente enriquecido de Web Intelligence pueden continuar funcionando con los archivos de documentos de Web Intelligence (.wid) incluso cuando no puedan conectarse a un Servidor de administración central (CMS).

> **Nota**
>
> - No se recomienda instalar el cliente enriquecido de Web Intelligence en el mismo equipo que los servidores de la plataforma de BI. El cliente enriquecido de Web Intelligence y los servidores de la plataforma de BI tienen binarios en común, lo que podría causar problemas al despliegue si actualiza la instalación (cliente o servidor). Si va a instalar el cliente enriquecido de Web Intelligence, instálelo en un equipo independiente.
> - Si va a efectuar la actualización desde la versión 4.2, asegúrese de detener y cerrar la versión anterior antes de instalar la versión 4.3. Compruebe la bandeja del sistema de Windows, ya que el cliente enriquecido podría estar minimizado y seguir en ejecución.

### 3.3.1.2 Administrador de vistas empresariales

El Administrador de vistas empresariales permite a los usuarios crear objetos de capa semántica que simplifican la complejidad de la base de datos subyacente.

El administrador de vistas empresariales puede crear conexiones de datos, conexiones de datos dinámicos, infraestructuras de datos, elementos empresariales, vistas empresariales y vistas relacionales. También permite establecer la seguridad detallada de nivel de columna y fila para los objetos de un informe.

Los diseñadores pueden crear conexiones a varios orígenes de datos, unir tablas, crear alias de nombres de campo, crear campos calculados y, a continuación, usar la estructura simplificada como una vista empresarial. Los diseñadores de informes y los usuarios pueden usar la vista empresarial como base para sus informes, en lugar de crear sus propias consultas directamente desde los datos.

### 3.3.1.3 Herramienta de conversión de informes

La RCT queda obsoleta en la versión 4.3 de BI. Para obtener más información, consulte 2801797

### 3.3.1.4 Herramienta de diseño de universos

La herramienta de diseño de universos (antes llamada "Diseñador de universos") permite que los diseñadores de datos combinen datos de varios orígenes en una capa semántica que oculta la complejidad de la base de datos a los usuarios finales. Abstrae la complejidad de los datos mediante el uso de un lenguaje técnico para acceder, manipular y organizar los datos.

La herramienta de diseño de universos ofrece una interfaz gráfica para seleccionar y ver las tablas de una base de datos. En un diagrama de esquema, las tablas de la base de datos están representadas por símbolos de tabla. Los diseñadores pueden usar esta interfaz para manipular tablas, crear combinaciones entre tablas, crear tablas con alias, crear contextos y resolver bucles del esquema.

También se pueden crear universos desde los orígenes de metadatos. La herramienta de diseño de universos se usa para generar universos al final del proceso de creación.

### 3.3.1.5 Herramienta de diseño de información

La herramienta de diseño de información (antes llamada "Diseñador de información") es un entorno de diseño de metadatos con el que un diseñador puede extraer, definir y manipular metadatos de orígenes relacionales y orígenes OLAP para crear y desplegar universos de SAP BusinessObjects.

### 3.3.1.6 Herramienta de administración de traducciones

La plataforma de BI proporciona soporte para documentos y universos multilingües. Un documento multilingüe contiene versiones localizadas de metadatos de universos y peticiones de documentos. Un usuario puede crear informes, por ejemplo, desde el mismo universo en los idiomas seleccionados.

La herramienta de administración de traducciones (antes, administrador de traducciones) define los universos multilingües y administra la traducción de los universos y otros recursos analíticos y de informes del repositorio CMS.

Herramienta de administración de traducciones:

- Traduce universos o documentos para un público multilingüe.
- Define las partes del documento del idioma de metadatos y la traducción adecuada. Genera el formato de XLIFF externo e importa archivos XLIFF para obtener información traducida.
- Enumera la estructura del documento o universo que se va a traducir.
- Permite traducir los metadatos a través de la interfaz de usuario o a través de una herramienta de traducción externa mediante la importación de archivos XLIFF.
- Crea documentos multilingües.

### 3.3.1.7 Herramienta de administración de Data Federation

La herramienta de administración de la federación de datos (antes Data Federator) es una aplicación de cliente enriquecido que ofrece funciones fáciles de usar para administrar el servicio de federación de datos.

Perfectamente integrado en la plataforma de BI, el servicio de federación de datos habilita universos de varios orígenes mediante la distribución de consultas en diferentes orígenes de datos y permite federar datos a través de una única infraestructura de datos.

La herramienta de administración de la federación de datos permite optimizar las consultas de la federación de datos y ajustar el motor de consultas de la federación de datos para obtener el mejor rendimiento posible.

Use la herramienta de administración de la federación de datos para realizar las siguientes tareas:

- Probar las consultas SQL.
- Visualizar planes de optimización que detallan cómo se distribuyen las consultas federadas en cada origen.
- Calcular estadísticas y establecer los parámetros del sistema para ajustar los servicios de federación de datos y obtener el mejor rendimiento posible.
- Administrar propiedades para controlar cómo se ejecutan las consultas en cada origen de datos en el nivel de conector.
- Supervisar las consultas SQL en ejecución.
- Buscar en el historial de consultas ejecutadas.

## 3.3.2 Instalado con la plataforma SAP BusinessObjects Business Intelligence

### 3.3.2.1 Administrador de configuración central (CCM)

El Administrador de configuración central (CCM) es una herramienta de resolución de problemas y de gestión de nodos que se proporciona de dos formas. En un entorno de Microsoft Windows, el CCM permite administrar servidores locales y remotos a través de la interfaz gráfica de usuario (GUI) o desde una línea de comandos. En un entorno UNIX, la secuencia de comandos del shell del CCM (`ccm.sh`) le permite administrar servidores desde una línea de comandos.

El CCM se usa para crear y configurar nodos y para iniciar o detener el servidor de aplicaciones Web, si es el servidor de aplicaciones Web de Tomcat agrupado predeterminado. En Windows, también permite configurar parámetros de red, como el cifrado SSL (Nivel de socket seguro). Estos parámetros se aplican a todos los servidores de un nodo.

> **Nota**
>
> La mayoría de las tareas de administración ahora se llevan a cabo mediante la CMC y no el CCM. El CCM se usa para solucionar problemas y configurar nodos.

### 3.3.2.2 Herramienta de administración de actualizaciones

UMT quedará obsoleto en la versión 4.3 de BI. Para obtener más información, consulte 2801797

### 3.3.2.3 Herramienta de diagnóstico del repositorio

La Herramienta de diagnóstico del repositorio (RDT) puede analizar, diagnosticar y reparar incoherencias que se puedan producir entre la base de datos de sistema del Servidor de administración central (CMS) y el almacén de archivos de los Servidores del repositorio de archivos (FRS).

También puede informar del estado de reparación y las acciones finalizadas. Para determinar la sincronización entre el sistema de archivos y la base de datos, se debe usar RDT después de que el usuario haya realizado una copia de seguridad en caliente por primera vez. También se puede utilizar después de una restauración antes de iniciar los servicios de la plataforma de BI. El usuario puede definir un límite del número de errores que RDT encontrará y reparará antes de detenerse.

## 3.3.3 Disponible por separado

### 3.3.3.1 SAP BusinessObjects Analysis, edición para Microsoft Office

SAP BusinessObjects Analysis, edición para Microsoft Office es una alternativa de primera categoría a Business Explorer (BEx) y permite que los analistas empresariales exploren los datos de procesamiento analítico en línea (OLAP) multidimensional.

Estos analistas pueden dar respuesta rápidamente a las cuestiones empresariales i, a continuación, compartir sus análisis y su área de trabajo con otros como *análisis*.

SAP BusinessObjects Analysis, edición para Microsoft Office permite que los analistas realicen las siguientes acciones:

- Descubrir tendencias, valores atípicos y detalles, almacenados en los sistemas financieros y sin necesidad de recurrir a un administrador de bases de datos.
- Obtener respuestas a cuestiones empresariales a la vez que visualizan conjuntos de datos multidimensionales, ya sean grandes o pequeños, de forma eficiente.
- Acceder a toda la gama de orígenes de datos disponibles en la organización y compartir los resultados mediante una interfaz sencilla e intuitiva.
- Acceder a distintos orígenes de datos OLAP en los mismos análisis para obtener una visión completa de los negocios y del impacto en todos los ámbitos que puede tener una tendencia u otra.
- Interrogar, analizar, comparar y predecir factores clave de impulso empresarial.
- Usar una completa gama de cálculos de tiempo y negocios.

### 3.3.3.2 SAP Crystal Reports

El software de SAP Crystal Reports permite a los usuarios diseñar informes interactivos desde un origen de datos.

### 3.3.3.3 SAP Lumira

La aplicación SAP Lumira ayuda a visualizar datos y crear guiones de los datos. Con SAP Lumira, puede manipular, tratar, formatear y definar sus datos, crear visualizaciones para representar los datos gráficamente y compartir sus visualizaciones utilizando guiones.

SAP Lumira ahora está listado como una aplicación en CMC, lo que le permite gestionar derechos relacionados con la adquisición de datos y la función de compartimiento de datos de SAP Lumira para cada usuario o grupo de usuarios.

> **Nota**
>
> Todos los eventos relacionados con la aplicación SAP Lumira se registran sin un ID de cliente en la base de datos de la auditoría.

## 3.3.4 Clientes de las aplicaciones Web

Los clientes de aplicaciones web residen en un servidor de aplicaciones web y se accede a ellos en un explorador web cliente. Las aplicaciones Web se despliegan automáticamente cuando se instala la plataforma de BI.

Es fácil para los usuarios acceder a las aplicaciones Web desde un explorador Web, y la comunicación se puede asegurar con el cifrado SSL si tiene intención de permitir que los usuarios accedan desde una red externa a la organización.

Las aplicaciones Web Java también se pueden configurar o implementar después de la instalación inicial mediante el uso de la herramienta de línea de comandos WDeploy en paquete, que permite implementar las aplicaciones Web en un servidor de aplicaciones Web de dos modos:

1. Modo independiente
   Todos los recursos de las aplicaciones Web se implementan en un servidor de aplicaciones Web que proporciona contenido dinámico y estático. Esta organización es adecuada para las pequeñas instalaciones.
2. Modo de división
   El contenido estático de las aplicaciones Web (HTML, imágenes, CSS) se implementa en un servidor Web dedicado, mientras que el contenido dinámico (JSP) se implementa en un servidor de aplicaciones Web. Esta organización es adecuada para las grandes instalaciones que se beneficiarán de que el servidor de aplicaciones Web se libere de servir contenido Web estático.

Para obtener más información acerca de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

### 3.3.4.1 Consola de administración central (CMC)

La Consola de administración central (CMC) es una herramienta basada en Web que puede usar para realizar tareas administrativas (incluida la administración de usuarios, contenidos y servidores) y para configurar los parámetros de seguridad. Como la CMC es una aplicación basada en Web, podrá realizar todas las tareas administrativas mediante un explorador Web en cualquier equipo que se pueda conectar al servidor de aplicaciones Web.

Los únicos que pueden cambiar la configuración de administración son los miembros del grupo Administradores, a menos que a un usuario se le concedan los derechos para hacerlo. Se pueden asignar funciones en la CMC para conceder privilegios de usuario para realizar tareas administrativas de menor importancia, como la gestión de usuarios del grupo y la gestión de informes en carpetas que le pertenezcan al equipo.

### 3.3.4.2 Rampa de lanzamiento BI de Fiori

La rampa de lanzamiento BI de Fiori (antes InfoView) es una interfaz basada en Web a la que pueden acceder los usuarios para ver, programar y realizar el seguimiento de los informes publicados de Business Intelligence (BI). La rampa de lanzamiento BI de Fiori puede acceder, interactuar con y exportar cualquier tipo de Business Intelligence, incluidos informes, análisis y cuadros de mandos.

La rampa de lanzamiento BI de Fiori permite a los usuarios administrar:

- La exploración y la búsqueda de contenido de BI.
- Acceso a contenidos de BI (creación, edición y visualización).
- Programación y publicación de contenidos de BI.

### 3.3.4.3 Áreas de trabajo de BI

Las áreas de trabajo de BI ayudan a realizar el seguimiento de las actividades empresariales y del rendimiento mediante módulos (plantillas de datos) y áreas de trabajo de Business Intelligence (BI) (los datos se ven en uno o varios módulos). Los módulos y las áreas de trabajo de BI proporcionan la información necesaria para ajustar las reglas empresariales a medida que las condiciones cambian. Ayudan a realizar el seguimiento y analizar datos empresariales clave mediante la administración de módulos y áreas de trabajo de BI. También admite la toma de decisiones de grupos y el análisis a través de la colaboración integrada y las capacidades del flujo de trabajo. Las áreas de trabajo de BI proporcionan las siguientes funciones:

- Exploración basada en fichas
- Creación de páginas: administrar módulos y áreas de trabajo de BI
- Creador de aplicaciones de señalar y hacer clic
- Vinculación de contenido entre módulos para un análisis de datos exhaustivo

> ⓘ Nota
>
> No se soporta el vinculación de contenido para documentos de Design Studio.

### 3.3.4.4 SAP BusinessObjects Web Intelligence

La solución de SAP BusinessObjects Web Intelligence es una herramienta basada en Web que proporciona funciones de consulta, informes y análisis para orígenes de datos relacionados en un único producto basado en Web.

Permite a los usuarios crear informes, realizar consultas especiales, analizar datos y dar formato a informes en una interfaz arrastrar y colocar. Web Intelligence oculta la complejidad de los orígenes de datos subyacentes.

Los informes se pueden publicar en un portal web admitido o en aplicaciones de Microsoft Office mediante SAP BusinessObjects Live Office.

### 3.3.4.5 SAP BusinessObjects Analysis, edición para OLAP

SAP BusinessObjects Analysis, edición para OLAP (anteriormente Voyager) es una herramienta de procesamiento analítico en línea (OLAP) del portal de la plataforma de lanzamiento de BI para trabajar con datos multidimensionales. También puede combinar información de diferentes orígenes de datos OLAP dentro de una única área de trabajo. Entre los proveedores de OLAP admitidos se encuentra SAP BW y Microsoft Analysis Services.

El conjunto de funciones OLAP de Analysis combina elementos de SAP Crystal Reports (acceso directo a datos de cubos OLAP para la producción de informes) y SAP BusinessObjects Web Intelligence (informes analíticos especiales con universos desde orígenes de datos OLAP). Ofrece una amplia gama de cálculos comerciales y de tiempo, e incluye características como controles deslizantes de tiempo para lograr que el análisis se datos OLAP sea lo más sencillo posible.

> **Nota**
>
> La aplicación Web de Analysis, edición para OLAP está disponible solo como una aplicación Web Java. No existe una aplicación correspondiente para .NET.

### 3.3.4.6 SAP BusinessObjects Mobile

SAP BusinessObjects Mobile permite a los usuarios acceder de forma remota a los mismos informes, métricas y datos en tiempo real de Business Intelligence (BI) disponibles en los clientes de escritorio desde un dispositivo inalámbrico. El contenido está optimizado para dispositivos móviles, de modo que los usuarios podrán acceder, navegar y analizar fácilmente los informes sin necesidad de formación adicional.

Con SAP BusinessObjects Mobile, el personal encargado de la administración y la información puede mantenerse al día y tomar decisiones con los datos más actualizados. El personal de ventas y de servicio de campo puede proporcionar la información correcta de clientes, productos y peticiones de trabajo cuando y donde sea necesario.

SAP BusinessObjects Mobile admite un amplio conjunto de dispositivos móviles incluyendo BlackBerry, Windows Mobile y Symbian.

Para obtener más información sobre la instalación, configuración y despliegue en dispositivos móviles, consulte el *Manual de despliegue e instalación de SAP BusinessObjects Mobile*. Para obtener más información sobre el uso de SAP BusinessObjects Mobile, consulte el *Manual de uso de SAP BusinessObjects Mobile*.

## 3.4 Flujos de trabajo de procesos

Cuando se llevan a cabo tareas como iniciar la sesión, programar un informe o ver un informe, la información fluye por el sistema y los servidores se comunican entre sí. En la siguiente sección se describen algunos de los flujos de proceso tal y como suceden en la plataforma de BI.

Para ver flujos de proceso adicionales con recursos visuales, consulte los programas de aprendizaje del producto oficiales de la plataforma SAP BusinessObjects Business Intelligence que hay en: http://scn.sap.com/docs/DOC-8292

## 3.4.1 Inicio y autenticación

### 3.4.1.1 Inicio de sesión en la plataforma de BI

Este flujo de trabajo describe el inicio de sesión de un usuario en una aplicación Web de la plataforma de BI desde un explorador Web. Este flujo de trabajo se aplica a aplicaciones Web, como la plataforma de lanzamiento de BI y la Consola de administración central (CMC).

1. El explorador (cliente Web) envía la solicitud de inicio de sesión al servidor de aplicaciones Web, en el que se está ejecutando la aplicación Web.
2. El servidor de aplicaciones Web determina que la solicitud es una solicitud de inicio de sesión. El servidor de aplicaciones web envía el nombre de usuario, la contraseña y el tipo de autenticación al CMS para su autenticación.
3. El CMS valida el nombre de usuario y la contraseña en la base de datos adecuada. En este caso, se usa la autenticación Enterprise y las credenciales del usuario se autentican en la base de datos del sistema del CMS.
4. Tras la validación correcta, el CMS crea una sesión para el usuario en su memoria.
5. El CMS envía una respuesta al servidor de aplicaciones Web para hacerle saber que la validación se ha realizado correctamente.
6. El servidor de aplicaciones Web genera un identificador de inicio de sesión para la sesión de usuario en la memoria. Para el resto de esta sesión, el servidor de aplicaciones Web usa el identificador de inicio de sesión para validar el usuario con el CMS. El servidor de aplicaciones Web genera la siguiente página Web para enviar al cliente Web.
7. El servidor de aplicaciones Web envía la siguiente página Web al servidor Web.
8. El servidor Web envía la página Web al cliente Web donde se representa en el explorador del usuario.

### 3.4.1.2 Inicio de SIA

Se puede configurar un Agente de inteligencia de servidor (SIA) para que se inicie automáticamente con el sistema operativo del host, o se puede iniciar manualmente con el Administrador de configuración central (CCM).

Un SIA recupera la información acerca de los servidores que administra desde un Servidor de administración central (CMS). Si el SIA usa un CMS local y ese CMS no se está ejecutando, el SIA inicia el CMS. Si un SIA usa un CMS remoto, intenta conectarse con el CMS.

Una vez iniciado el SIA, se llevará a cabo la siguiente secuencia de eventos.

1. El SIA busca en su caché para localizar un CMS.
   a. Si el SIA está configurado para iniciar un CMS local, y el CMS no se está ejecutando, el SIA iniciará el CMS y se conectará.
   b. Si el SIA está configurado para usar un CMS (local o remoto) que se está ejecutando, intentará conectarse al primer CMS de su caché. SI el CMS no está disponible, intentará conectarse al siguiente CMS de la caché. Si no están disponible ninguno de los CMS de la caché, el SIA espera a que uno esté disponible.
2. El CMS confirma la identidad del SIA para asegurar que es válida.

3. Una vez conectado correctamente el SIA a un CMS, solicita una lista de servidores para administrar.

> **Nota**
>
> Un SIA no almacena información acerca de los servidores que administra. La información de configuración que dicta qué servidor administra el SIA se almacena en la base de datos del sistema del CMS y el SIA lo recupera desde el CMS cuando se inicia.

4. El CMS consulta a la base de datos del sistema del CMS para obtener una lista de servidores administrados por el SIA. También se recupera la configuración para cada servidor.
5. El CMS devuelve la lista de servidores y su configuración al SIA.
6. Para cada servidor que está configurado para que se inicie automáticamente, el SIA lo inicia con la configuración adecuada y supervisa su estado. Cada servidor que ha iniciado el SIA está configurado para usar el mismo CMS que usa el SIA.

   Los servidores que no estén configurados para que se inicien automáticamente con el SIA no se iniciarán.

#### 3.4.1.3 Cierre de sesión de SIA

El agente de Server Intelligence (SIA) se detiene automáticamente cuando apaga el sistema operativo del host, o puede detener el SIA manualmente en el administrador de configuración central (CCM).

Al cerrar la sesión del SIA, se llevan a cabo los siguientes pasos:

El SIA indica al CMS que está cerrando la sesión.

a. Si el SIA se detiene porque el sistema operativo del host está cerrando sesión, el SIA solicita a sus servidores que se detengan. Los servidores que no se detienen durante esos 25 segundos, finalizarán de manera forzosa.
b. Si el SIA se detiene manualmente, esperará a que el servidor administrado termine de procesar los trabajos existentes. Los servidores administrados no aceptarán nuevos trabajos. Una vez finalizados todos los trabajos, los servidores se detendrán. Una vez detenidos todos los servidores, también se detendrá el SIA.

Durante un cierre de sesión forzado, el SIA indicará a todos los servidores gestionados que se detengan inmediatamente.

### 3.4.2 Objetos de programa

#### 3.4.2.1 Establecimiento de una planificación para un objeto de programa

Este flujo de trabajo describe cómo un usuario programa un objeto de programa que se ejecutará en el futuro desde una aplicación Web, como la Consola de administración central (CMC) o la plataforma de lanzamiento de BI.

1. El usuario envía la solicitud de planificación desde el cliente web a través del servidor web al servidor de aplicaciones web.

2. El servidor de aplicaciones Web interpreta la solicitud de y determina que se trata de una solicitud de planificación. El servidor de aplicaciones Web envía la hora de planificación, los valores de inicio de sesión de base de datos, los valores de parámetro, el destino y el formato al Servidor de administración central (CMS) especificado.
3. El CMS se asegura de que el usuario tenga los derechos adecuados para planificar el objeto. Si el usuario tiene derechos suficientes, el CMS agrega un informe nuevo a la base de datos del sistema del CMS y agrega la instancia a la lista de programaciones pendientes.
4. El CMS envía una respuesta satisfactoria por parte de la operación de programación al servidor de aplicaciones Web.
5. El servidor de aplicaciones Web genera la siguiente página HTML y la envía a través del servidor Web al cliente Web.

### 3.4.2.2 Se ejecuta un objeto de programa planificado

Este flujo de trabajo describe el proceso de un objeto de programa programado ejecutándose a una hora programada. El servidor de tareas de Adaptive y el servidor del repositorio de archivos de entrada también deben ejecutarse.

> **Nota**
>
> Este flujo de trabajo requiere que se ejecuten el CMS, el servidor de tarea de Adaptive, y el servidor del repositorio de archivos de entrada.

1. El Servidor de administración central (CMS) comprueba la base de datos del sistema del CMS para determinar si existe algún informe de SAP Crystal programado para que se ejecute a dicha hora.
2. Cuando llega la hora de la tarea programada, el CMS localiza un Servicio de programación de programa disponible que se ejecute en el Servidor de tareas de Adaptive. El CMS envía la información de tarea al Servicio de programación de programa.
3. El Servicio de programación de programa se comunica con el Servidor del repositorio de archivos de entrada (FRS) para obtener el objeto de programa.

   > **Nota**
   >
   > Este paso requiere también la comunicación con el CMS para localizar el servidor y los objetos necesarios.

4. El Servicio de programación de programa inicia el programa.
5. El Servicio de programación de programa actualiza el CMS periódicamente con el estado de la tarea. El estado actual es En procesamiento.
6. El Servicio de programación de programa envía un archivo de registro al FRS de salida. El FRS de salida notifica al Servicio de programación de programa que el objeto se ha programado correctamente mediante el envío de un archivo de registro de objeto.

   > **Nota**
   >
   > Este paso requiere también la comunicación con el CMS para localizar el servidor y los objetos necesarios.

7. El Servicio de programación de programa actualiza el CMS con el estado de la tarea. El estado actual es Correcto.
8. El CMS actualiza el estado de la tarea en la memoria y, a continuación, escribe la información de la instancia en la base de datos del sistema del CMS.

## 3.4.3 Crystal Reports

### 3.4.3.1 Visualización de una página de informe de SAP Crystal en caché

Este flujo de trabajo describe el proceso de un usuario que solicita una página en un informe de SAP Crystal (por ejemplo desde el visor de informes en la plataforma de lanzamiento de BI), cuando la página de informe existe en un servidor de caché. Este flujo de trabajo se aplica a SAP Crystal Reports 2020 y a SAP Crystal Reports para Enterprise.

> **Nota**
>
> Este flujo de trabajo requiere que se ejecuten el CMS y el servidor de caché de Crystal Reports.

1. El cliente Web envía una solicitud de visualización en una dirección URL a través del servidor Web al servidor de aplicaciones Web.
2. El servidor de aplicaciones Web interpreta la solicitud y determina que se trata de una solicitud para visualizar una página de informe seleccionada. El servidor de aplicaciones Web envía una solicitud al Servidor de administración central (CMS) para asegurarse de que el usuario dispone de los derechos suficientes para ver el informe.
3. El Servidor de administración central (CMS) comprueba la base de datos del sistema CMS para asegurarse de que el usuario tiene suficientes derechos para ver el informe.
4. El CMS envía una respuesta al servidor de aplicaciones Web para confirmar que el usuario tiene suficientes derechos para ver el informe.
5. El servidor de aplicaciones Web envía una solicitud al servidor de caché de Crystal Reports en la que se pide la página del informe (archivo `.epf`).
6. El Servidor de caché de Crystal Reports comprueba si el archivo `.epf` solicitado existe en el directorio de caché. En este ejemplo, el archivo `.epf` no se encuentra.
7. El Servidor de caché de Crystal Reports devuelve la página solicitada al servidor de aplicaciones Web.
8. El servidor de aplicaciones Web envía la página al cliente Web mediante el servidor Web, donde la página se presenta y se muestra.

### 3.4.3.2 Visualizar una página de SAP Crystal Reports 2020 que no está en caché

Este flujo de trabajo describe el proceso que sigue un usuario para solicitar una página en un informe de SAP Crystal Reports 2020 (por ejemplo, desde el visor de informes de la plataforma de lanzamiento de BI), cuando la página ya no existe en un servidor de caché.

> **Nota**
>
> Este flujo de trabajo requiere que se ejecuten el CMS, el servidor de caché de Crystal Reports, el servidor de procesamiento de Crystal Reports 2020, y el servidor del repositorio de archivos de salida.

1. El usuario envía la solicitud de visualización mediante el servidor Web al servidor de aplicaciones Web.
2. El servidor de aplicaciones Web interpreta la solicitud, determina que se trata de una solicitud para ver una página de informe seleccionada, y envía una solicitud al servidor de administración central (CMS) para asegurar que el usuario tiene derechos suficientes para ver el informe.
3. El Servidor de administración central (CMS) comprueba la base de datos del sistema CMS para asegurarse de que el usuario tiene suficientes derechos para ver el informe.
4. El CMS envía una respuesta al servidor de aplicaciones Web para confirmar que el usuario tiene suficientes derechos para ver el informe.
5. El servidor de aplicaciones Web envía una solicitud al servidor de caché de Crystal Reports en la que se pide la página del informe (archivo `.epf`).
6. El servidor de caché de Crystal Reports determina si el archivo solicitado existe en el directorio de caché. En este ejemplo, el archivo `.epf` solicitado no se encuentra en el directorio de caché.
7. El servidor de caché de Crystal Reports envía la solicitud al servidor de procesamiento de Crystal Reports 2020.
8. El servidor de procesamiento de Crystal Reports 2020 consulta el servidor del repositorio de archivos de salida (FRS) para la instancia del informe solicitado, y el FRS de salida envía la instancia de informe solicitada al servidor de procesamiento de Crystal Reports 2020.

   > **Nota**
   >
   > Este paso también necesita la comunicación con el CMS para localizar el servidor y los objetos necesarios.

9. El servidor de procesamiento de Crystal Reports 2020 abre la instancia de informe y comprueba el informe para determinar si tiene datos.

   El servidor de procesamiento de Crystal Reports 2020 determina que el informe contiene datos y crea el archivo `.epf` para la página de informe solicitada sin tener que conectarse a la base de datos de producción.
10. El servidor de procesamiento de Crystal Reports 2020 envía el archivo `.epf` al servidor de caché de Crystal Reports.
11. El servidor de caché de Crystal Reports escribe el archivo `.epf` en el directorio de caché.
12. El servidor de caché de Crystal Reports envía la página solicitada al servidor de aplicaciones Web.
13. El servidor de aplicaciones Web envía la página al cliente Web mediante el servidor Web, donde la página se presenta y se muestra.

### 3.4.3.3 Visualizar un informe de SAP Crystal Reports 2020 a petición

Este flujo de trabajo describe el proceso de un usuario que solicita una página de informe de SAP Crystal Reports 2020 a petición para ver los datos más recientes; por ejemplo, desde un visor de informes en la plataforma de lanzamiento de BI.

> **Nota**
>
> Este flujo de trabajo requiere que se ejecuten el CMS, el servidor de caché de Crystal Reports, el servidor de procesamiento de Crystal Reports 2020, y el servidor del repositorio de archivos de entrada.

1. El usuario envía la solicitud de visualización mediante el servidor Web al servidor de aplicaciones Web.
2. El servidor de aplicaciones Web interpreta la solicitud y determina que se trata de una solicitud para visualizar una página de informe seleccionada. El servidor de aplicaciones Web envía una solicitud al Servidor de administración central (CMS) para asegurarse de que el usuario dispone de los derechos suficientes para ver el informe.
3. El Servidor de administración central (CMS) comprueba la base de datos del sistema CMS para asegurarse de que el usuario tiene suficientes derechos para ver el informe.
4. El CMS envía una respuesta al servidor de aplicaciones Web para confirmar que el usuario tiene suficientes derechos para ver el informe.
5. El servidor de aplicaciones Web envía una solicitud al servidor de caché de Crystal Reports en la que se pide la página del informe (archivo `.epf`).
6. El servidor de caché de Crystal Reports comprueba si todavía existe la página. A menos que el informe cumpla los requisitos de uso compartido de informes a petición (que se encuentre en el tiempo establecido de otra solicitud a petición, conexión de base de datos, parámetros), el servidor de caché de Crystal Reports envía una solicitud para que el servidor de procesamiento de Crystal Reports 2020 genere la página.
7. El servidor de procesamiento de Crystal Reports 2020 solicita el objeto de informe al servidor del repositorio de archivos (FRS) de entrada. El FRS de entrada transmite una copia del objeto al servidor de procesamiento de Crystal Reports 2020.

   > **Nota**
   >
   > Este paso también necesita la comunicación con el CMS para localizar el servidor y los objetos necesarios.

8. El servidor de procesamiento de Crystal Reports 2020 abre el informe en su memoria y comprueba si el informe contiene datos. En este ejemplo, el objeto de informe no contiene datos, por lo que el servidor de procesamiento de Crystal Reports 2020 se conecta al origen de datos para recuperar datos y generar el informe.
9. El servidor de procesamiento de Crystal Reports 2020 envía la página (archivo `.epf`) al servidor de caché de Crystal Reports. El servidor de caché de Crystal Reports almacena una copia del archivo `.epf` en su directorio de caché para anticiparse a las nuevas solicitudes de visualización.
10. El servidor de caché de Crystal Reports envía la página al servidor de aplicaciones Web.
11. El servidor de aplicaciones Web envía la página al cliente Web mediante el servidor Web, donde la página se presenta y se muestra.

### 3.4.3.4 Establecimiento de una planificación para un informe de SAP Crystal

Este flujo de trabajo describe el proceso de un usuario que planifica un informe de SAP Crystal que se ejecutará en el futuro desde una aplicación Web como la Consola de administración central (CMC) o la

plataforma de lanzamiento de BI. Este flujo de trabajo se aplica a SAP Crystal Reports 2020 y a SAP Crystal Reports para Enterprise.

1. El cliente Web envía una solicitud de programación en una URL a través del servidor Web al servidor de aplicaciones Web.
2. El servidor de aplicaciones Web interpreta la solicitud de URL y determina que se trata de una solicitud de planificación. El servidor de aplicaciones Web envía la hora de planificación, los valores de inicio de sesión de base de datos, los valores de parámetro, el destino y el formato al Servidor de administración central (CMS) especificado.
3. El CMS se asegura de que el usuario tenga los derechos adecuados para planificar el objeto. Si el usuario dispone de los derechos suficientes, el CMS agrega un nuevo registro en la base de datos del sistema del CMS. El CMS también agrega la instancia a su lista de programaciones pendientes.
4. El CMS envía una respuesta al servidor de aplicaciones Web para hacerle saber que la operación de planificación se ha realizado correctamente.
5. El servidor de aplicaciones Web genera la siguiente página HTML y la envía a través del servidor Web al cliente Web.

### 3.4.3.5 Se ejecuta un informe de SAP Crystal Reports 2020 programado

Este flujo de trabajo describe el proceso de un informe de SAP Crystal Reports 2020 programado que se ejecuta a una hora programada.

1. El Servidor de administración central (CMS) comprueba la base de datos del sistema del CMS para determinar si existe algún informe de SAP Crystal programado para que se ejecute a dicha hora.
2. Cuando llega la hora de la tarea programada, el CMS busca un servicio de programación de Crystal Reports 2020 que se esté ejecutando en un servidor de tareas de Adaptive (basado en el valor *Número máximo de tareas permitidas* configurado en cada servidor de tareas de Adaptive). El CMS envía la información de la tarea (ID del informe, formato, destino, información de conexión, parámetros y fórmulas de selección) al Servicio de programación de Crystal Reports 2020.
3. El Servicio de programación de Crystal Reports 2020 se comunica con el servidor del repositorio de archivos de entrada (FRS) para obtener una plantilla de informe según el ID de informe solicitado.

   > **Nota**
   >
   > Este paso requiere también comunicarse con el CMS para localizar el servidor y los objetos necesarios.

4. El Servicio de programación de Crystal Reports 2020 inicia el proceso del servidor de elementos secundarios de tarea.
5. El proceso secundario (servidor de elementos secundarios de tarea) inicia el (`ProcReport.dll` cuando recibe la plantilla del Servidor del repositorio de archivos. `ProcReport.dll` contiene todos los parámetros que se han pasado del CMS al Servicio de programación de Crystal Reports 2020.
6. `ProcReport.dll` inicia `crpe32.dll`, que procesa el informe según los parámetros aprobados.
7. Mientras `crpe32.dll` continúa procesando el informe, se recuperan los registros del origen de datos tal y como se define en el informe.
8. El Servicio de programación de Crystal Reports 2020 actualiza el CMS periódicamente con el estado de la tarea. El estado actual es Procesando.

9. Una vez compilado el informe en la memoria del Servicio de programación de Crystal Reports 2020, se tiene que exportar a un formato distinto, como el formato de documento portable (PDF). Al exportar un PDF se utiliza un `crxfpdf.dll`.
10. El informe con los datos almacenados se envía a la ubicación programada (como el correo electrónico) y después al FRS de salida.

    > **Nota**
    >
    > Este paso también necesita la comunicación con el CMS para localizar el servidor y los objetos necesarios.

11. El Servicio de programación de Crystal Reports 2020 actualiza el CMS con el estado de la tarea. El estado actual es Correcto.
12. El CMS actualiza el estado de la tarea en la memoria y, a continuación, escribe la información de la instancia en la base de datos del sistema del CMS.

## 3.4.4 Web Intelligence

### 3.4.4.1 Visualización de un documento a petición de SAP BusinessObjects Web Intelligence

Este flujo de trabajo describe el proceso de un usuario visualizando un documento de SAP BusinessObjects Web Intelligence a demanda para ver los datos más actuales; por ejemplo, desde el visor de Web Intelligence en la plataforma de lanzamiento de BI.

1. Un explorador Web envía la solicitud de visualización al servidor de aplicaciones Web mediante el servidor Web.
2. El servidor de aplicaciones Web interpreta la solicitud y determina que es una solicitud para visualizar un documento de Web Intelligence. El servidor de aplicaciones Web envía una solicitud al Servidor de administración central (CMS) para asegurarse de que el usuario dispone de los derechos para ver el documento.
3. La CMS comprueba la Base de datos del sistema de CMS para verificar que el usuario dispone de los derechos para ver el documento
4. El CMS envía una respuesta al servidor de aplicaciones Web para confirmar que el usuario tiene suficientes derechos para ver el documento.
5. El servidor de aplicaciones Web envía una solicitud al servidor de procesamiento de Web Intelligence en la que se pide el documento.
6. El servidor de procesamiento de Web Intelligence solicita el documento al servidor del repositorio de archivos de entrada (FRS) así como el archivo de universo en el que se basa el documento solicitado. El archivo de universo contiene información de metanivel, incluida la seguridad de nivel de fila y de columna.
7. El FRS de entrada transmite una copia del documento al servidor de procesamiento de Web Intelligence, así como el archivo de universo en el que se basa el documento solicitado.

    > **Nota**
    >
    > Este paso requiere también la comunicación con el CMS para localizar el servidor y los objetos necesarios.

8. El motor de informes de Web Intelligence (en el Servidor de procesamiento de Web Intelligence) abre el documento en la memoria y lanza `QT.dll` y un Servidor de conexión en proceso.
9. `QT.dll` genera, valida y regenera el SQL y se conecta a la base de datos para ejecutar una consulta. El servidor de conexión usa el SQL para obtener los datos desde la base de datos hasta el motor de informes en el que se procesa el documento.
10. El servidor de procesamiento de Web Intelligence envía la página de documento visualizable que se ha solicitado al servidor de aplicaciones Web.
11. El servidor de aplicaciones Web envía la página al cliente Web a través del servidor Web, en el que la página se procesa y se muestra.

### 3.4.4.2 Establecimiento de una planificación para un documento de SAP BusinessObjects Web Intelligence

Este flujo de trabajo describe el proceso de un usuario que planifica un documento de SAP BusinessObjects Web Intelligence que se ejecutará en el futuro desde una aplicación Web como la Consola de administración central (CMC) o la plataforma de lanzamiento de BI.

1. El cliente Web envía una solicitud de programación en una URL a través del servidor Web al servidor de aplicaciones Web.
2. El servidor de aplicaciones Web interpreta la solicitud de URL y determina que se trata de una solicitud de planificación. El servidor de aplicaciones Web envía la hora de planificación, los valores de inicio de sesión de base de datos, los valores de parámetro, el destino y el formato al Servidor de administración central (CMS) especificado.
3. El CMS se asegura de que el usuario tenga los derechos adecuados para planificar el objeto. Si el usuario dispone de los derechos suficientes, el CMS agrega un nuevo registro en la base de datos del sistema del CMS. El CMS también agrega la instancia a su lista de programaciones pendientes.
4. El CMS envía una respuesta al servidor de aplicaciones Web para hacerle saber que la operación de planificación se ha realizado correctamente.
5. El servidor de aplicaciones Web genera la siguiente página HTML y la envía a través del servidor Web al cliente Web.

### 3.4.4.3 Se ejecuta un documento de SAP BusinessObjects Web Intelligence programado

Este flujo de trabajo describe el proceso de un documento de SAP BusinessObjects Web Intelligence programado que se ejecuta en un momento programado.

1. El Servidor de administración central (CMS) comprueba la base de datos del sistema del CMS para determinar si se ha programado un documento de Web Intelligence para su ejecución.
2. Cuando llega el momento programado, el CMS localiza un servicio de programación de Web Intelligence disponible que se ejecute en un servidor de tareas de Adaptive. El CMS envía la solicitud de programación y toda la información acerca de la solicitud al servicio de programación de Web Intelligence.

3. El servicio de programación de Web Intelligence localiza un servidor de procesamiento de Web Intelligence disponible según el valor *Conexiones máximas* que está configurado en cada servidor de procesamiento de Web Intelligence.
4. El servidor de procesamiento de Web Intelligence determina la ubicación del servidor del repositorio de archivos (FRS) de entrada que aloja el documento y el archivo de multinivel de universo en el que se basa el documento. A continuación, el servidor de procesamiento de Web Intelligence solicita el documento del FRS de entrada. El FRS de entrada busca el documento de Web Intelligence, así como el archivo de universo en el que se basa el documento y, a continuación, lo transmite al servidor de procesamiento de Web Intelligence.

   > **Nota**
   >
   > Este paso también necesita comunicación con el CMS para localizar el servidor y los objetos necesarios.

5. El documento de Web Intelligence se coloca en un directorio temporal en el servidor de procesamiento de Web Intelligence. El servidor de procesamiento de Web Intelligence abre el documento en la memoria, y `QT.dll` genera el SQL desde el universo en el que se basa el documento. Las bibliotecas del servidor de conexión se incluyen en el servidor de procesamiento de Web Intelligence se conectas al origen de datos. Los datos de consulta pasan a través de `QT.dll` hacia el motor de informes del servidor de procesamiento de Web Intelligence, donde se procesa el documento. Se crea una nueva instancia correcta.
6. El servidor de procesamiento de Web Intelligence carga la instancia de documento en el FRS de salida.

   > **Nota**
   >
   > Este paso también necesita comunicación con el CMS para localizar el servidor y los objetos necesarios.

7. El servidor de procesamiento de Web Intelligence notifica al servicio de programación de Web Intelligence (del servidor de tareas de Adaptive) que ha finalizado la creación del documento. Si el documento está programado para ir a un destino (sistema de archivos, FTP, SFTP, SMTP o bandeja de entrada), el servidor de tareas de Adaptive recupera el documento procesado del FRS de salida y lo entrega en los destinos especificados. Supongamos que no es así en este ejemplo.
8. El servicio de programación de Web Intelligence actualiza el CMS con el estado de tarea.
9. El CMS actualiza el estado de la tarea en la memoria y, a continuación, escribe la información de la instancia en la base de datos del sistema del CMS.

## 3.4.5 Análisis

### 3.4.5.1 Visualización de SAP BusinessObjects Analysis, edición para el área de trabajo OLAP

Este flujo de trabajo describe el proceso de un usuario que solicita ver SAP BusinessObjects Analysis, edición para el área de trabajo OLAP desde la plataforma de lanzamiento de BI.

> **Nota**
>
> Este flujo de trabajo requiere que se ejecuten el CMS, el servidor de procesamiento de Adaptive (que contiene el servicio de análisis multidimensional (MDAS)), y el servidor del repositorio de archivos de entrada.

1. El cliente Web envía una solicitud mediante el servidor Web al servidor de aplicaciones Web para ver una nueva área de trabajo. El cliente Web se comunica con el servidor de aplicaciones Web mediante tecnología DHTML AJAX (JavaScript asincrónico y XML). La tecnología AJAX permite actualizaciones de página parciales, por lo que no se tiene que representar una nueva página por cada nueva solicitud.
2. El servidor de aplicaciones Web traduce la solicitud y la envía al Servidor de administración central (CMS) para determinar si el usuario tiene derecho a ver o crear una nueva área de trabajo.
3. El CMS recupera las credenciales de usuario de la base de datos del sistema del CMS.
4. Si el usuario tiene permiso para ver o crear un área de trabajo, el CMS se lo confirma al servidor de aplicaciones Web. Al mismo tiempo, también envía uno o varios servidores de Servicios de análisis multidimensional (MDAS) disponibles.
5. El servidor de aplicaciones web elige un MDAS de la lista de elecciones disponibles y envía una solicitud CORBA al servicio para buscar los servidores OLAP adecuados para crear una nueva área de trabajo o para actualizar una existente.
6. El MDAS debe comunicarse con el servidor del repositorio de archivos de entrada (FRS) para recuperar el documento de área de trabajo adecuado que contiene la información acerca de la base de datos subyacente y una consulta OLAP inicial guardada en ella. El FRS de entrada recupera el área de trabajo de Analysis del directorio subyacente y transmite dicha área de trabajo al MDAS.
7. El MDAS abre el área de trabajo, formula una consulta y la envía al servidor de base de datos OLAP. El MDAS debe tener un cliente de base de datos de OLAP adecuado configurado para el origen de datos OLAP. Se debe producir la traducción de la consulta del cliente Web en la consulta OLAP adecuada. El servidor de base de datos OLAP envía el resultado de la consulta de nuevo al MDAS.
8. El MDAS, según la solicitud para crear, visualizar, imprimir o exportar, representa previamente el resultado para que WAS Java pueda finalizar la representación más rápidamente. El MDAS envía paquetes XML del resultado representado al servidor de aplicaciones web.
9. El servidor de aplicaciones Web representa el área de trabajo y envía la página formateada o parte de la página al cliente Web mediante el servidor Web. El cliente Web muestra la página actualizada o solicitada recientemente. Es una solución sin cliente que no necesita que se descargue ningún componente Java o ActiveX.

## 3.5 Integración con la plataforma de lanzamiento de SAP Fiori en SAP Enterprise Portal

### Resumen

La integración BI de SAP BusinessObjects con plataformas de lanzamiento de SAP Fiori permite a los usuarios finales del SAP Enterprise Portal visualizar los informes BI reports en el CMS SAP BusinessObjects. En la pestaña Menú de usuario, los usuarios finales tienen acceso a informes BI, cuya jerarquía de carpetas se corresponde con la del CMS SAP BusinessObjects.

## Requisitos previos

- Business Intelligence 4.2 SP4
- SAP Web Dispatcher 7.49 para la conectividad
- NetWeaver 7.5 SP7
- Autenticación de directorio activa y Kerberos-basado en configuración SSO como se describe en la nota SAP 1631734

## Procedimiento

El administrador de contenido de la plataforma de lanzamiento de SAP Fiori y el administrador del Enterprise Portal pueden integrar SAP BusinessObjects Enterprise con la plataforma de lanzamiento de SAP Fiori.

Encontrará completa información sobre la configuración en la Integración SAP BusinessObjects Enterprise, en la documentación de portal SAP NetWeaver 7.5.

> **Nota**
>
> - La plataforma de BI admite servicios OData para la integración entre la rampa de lanzamiento Fiori y SAP Enterprise Portal.
> - La Plataforma de BI admite servicios OData en el servidor de aplicación de SAP NetWeaver.
> - Puede acceder a las carpetas públicas, carpetas personales y la bandeja de entrada de BI desde SAP Enterprise Portal después de efectuar la integración.

# 4 Asistente de configuración del sistema

## 4.1 Introducción al Asistente de configuración del sistema

Después de instalar la plataforma SAP BusinessObjects Business Intelligence, es posible que desee realizar una configuración posterior a la instalación esencial, como por ejemplo seleccionar una plantilla de despliegue, y seleccionar los productos de SAP BusinessObjects que va a utilizar su organización. Para llevar a cabo esta configuración, y para que la plataforma de BI se ejecute en el menor tiempo posible, ejecute el *Asistente de configuración del sistema*.

Beneficios importantes de la utilización del asistente:

- El asistente le explica y guía a través de los pasos de configuración que tendrá que seguir.
- Si se utiliza el asistente es más probable que disminuyan los errores de configuración del sistema.
- El asistente configura los ajustes, lo que acelera enormemente la configuración del sistema.

De forma predeterminada, el asistente está fijado para que se ejecute automáticamente cuando inicia sesión en la Consola de administración central (CMC), pero también puede iniciarlo desde el área *Administrar* en la CMC. Puede volver a ejecutar el asistente en cualquier momento para ajustar la configuración, y siempre puede utilizar la página de administración *Servidores* en la CMC para ajustar la configuración, incluida la configuración que realizó con el asistente.

> ⓘ Nota
>
> Para mejorar la seguridad, solo los miembros del grupo de administradores pueden acceder al asistente.

> ⓘ Nota
>
> Para evitar que el asistente se ejecute automáticamente, el usuario «Administrador» puede seleccionar la casilla de verificación *No mostrar este asistente cuando se haya iniciado CMC* en la primera página del asistente.

> ⓘ Nota
>
> Si planea instalar cualquier complemento, o agregar nodos al despliegue de la plataforma de BI, le recomendamos que lleve a cabo estos pasos antes de ejecutar el asistente de configuración del sistema.

## 4.2 Especificar los productos que utiliza

Puede simplificar la configuración de los servidores de la plataforma de BI especificando los productos que utiliza su organización, y puede optimizar la asignación de recursos deteniendo los servidores de los productos que su organización no utiliza. Para hacerlo, seleccione los productos en la página *Productos*. Al especificar los productos que utiliza su organización, el asistente inicia todos los servidores y dependencias necesarios para

ejecutar los productos, y configura los servidores y las dependencias para iniciarse automáticamente cuando se inicia la plataforma de BI. También, anulando la selección de los productos no utilizados, puede mejorar el tiempo de inicio y el uso de recursos de la plataforma de BI.

Por ejemplo, si selecciona el producto Crystal Reports, la plataforma de BI iniciará automáticamente todos los servidores de Crystal Reports y las dependencias adecuadas.

Para ver una lista de los servidores que se iniciarán automáticamente para un producto, haga clic en el icono *?* junto al nombre del producto.

El asistente configura servidores de producto de la forma siguiente:

- La selección de un producto resulta en iniciar todos los servidores que pertenecen a dicho producto, así como otros servidores necesarios para que el producto funciones (dependencias), cuando finalice el asistente. La selección de un producto también fija que los servidores del producto se inicien automáticamente con la plataforma de BI. Si un servidor almacena servicios para varios productos, y si alguno de estos productos está seleccionado, se iniciará el servidor. Tenga en cuenta que algunos servicios de productos que no están seleccionados pueden estar ejecutándose si están almacenados por un servidor que también almacena servicios de productos seleccionados.
- La anulación de un producto provoca que se detengan los servidores utilizados por ese producto, siempre y cuando esos servidores no almacenen también servicios de un producto que aún está seleccionado o servicios pertenecientes a la categoría Servicios principales. Los servidores detenidos del producto están fijados en inicio no automático con la plataforma de BI. Si un servidor almacena servicios de productos seleccionados y no seleccionados, el servidor permanece ejecutándose.
- La anulación de un producto también puede provocar que se detengan los servidores que no pertenecen al producto anulado, en caso de que haya servicios dependientes utilizados solo pro el producto anulado. Esto liberará recursos, ya que estos servidores dependientes ya no serán necesarios.
- Cada vez que se selecciona o anula un producto, todos los servicios host que pertenecen a la categoría de servicios principales en la plataforma de BI (excepto servicios almacenados por WACS) se iniciarán automáticamente. WACS permanecerá en el estado actual.
- Si se deseleccionan productos, esto no desinstala o elimina archivos de estos productos.

Cada vez que abra la página *Productos*, los estados del producto en dicha página representan el estado del sistema actual.

Si todos los servidores de un producto se están ejecutando, la casilla de verificación de dicho producto está seleccionada. Si todos los servidores de un producto están detenidos, se borra la casilla de verificación. Si solo se ejecutan algunos servidores de un producto, mientras que otros servidores tienen otros estados, por ejemplo detenido, la página *Productos* muestra la casilla de verificación *Conservar la configuración existente*, para indicar que el sistema se ha configurado fuera del asistente. Puede borrar la casilla de verificación si desea utilizar el asistente para modificar la configuración.

> **Nota**
>
> La página *Productos* muestra todos los productos instalados en el clúster. Por ejemplo, si el equipo A tiene instalados los productos P1 y P2, y el equipo B tiene instalados los productos P2 y P3, la página *Productos* muestra los productos P1, P2, y P3. Los productos que no están instalados no aparecen en la página *Productos*.

> **Nota**
>
> Para simplificar el despliegue, la configuración de esta página no necesita que se repita para cada nodo; en su lugar, se aplica a todo el clúster.

> **Nota**
>
> Si se ha modificado previamente algún ajuste en la CMC, el asistente muestra un mensaje informándole que la configuración ha sido modificada fuera del asistente. Puede escoger entre conservar la configuración existente o sobrescribir la configuración actual.

> **Nota**
>
> Los cambios realizados en el asistente no se aplican hasta que hace clic en *Aplicar* en la página *Revisar*.

Cuando termine de realizar los cambios, haga clic en *Siguiente* para ir a la siguiente página del asistente. También puede utilizar el panel de navegación de la izquierda para saltar directamente a cualquier página que ya haya visitado.

## 4.3 Elección de una plantilla de despliegue

La instalación predeterminada de la plataforma de BI configura un despliegue pequeño que es adecuado para un entorno de demostración en el hardware limitado del sistema. Para adaptarse mejor al hardware y al caso de uso previsto (por ejemplo, preparar un sistema de prueba o un sistema de producción), seleccione una de las plantillas de despliegue predefinidas en la página *Capacidad*. Estas plantillas le serán de ayuda para iniciar rápidamente el sistema de la plataforma de BI y ejecutarla, y para reducir el tiempo de despliegue inicial.

Aunque la elección de una plantilla de despliegue adecuada le ayuda con la configuración inicial y proporciona un buen punto de inicio, no es un sustituto del tamaño y la optimización del sistema, que hay que llevar a cabo. Para obtener un mejor rendimiento, debe cambiar el tamaño del sistema, para ello consulte el manual de cambio de tamaño: http://www.sap.com/bisizing

La elección de una plantilla de despliegue adecuada es importante para varias razones:

- El tamaño de implementación que seleccione afecta a la capacidad de tratamiento de solicitudes de su sistema. Una implementación mayor proporciona más capacidad para tratar más solicitudes o solicitudes más complejas. Sin embargo, un despliegue más amplio requiere más recursos del sistema.
- La elección de un despliegue mayor no garantiza un rendimiento mejor, particularmente si no tiene suficientes recursos de hardware disponibles.
- La plantilla de despliegue que seleccione debe coincidir con sus necesidades empresariales y con los recursos de hardware disponibles. El sistema puede tener capacidad y rendimiento reducidos si selecciona una plantilla de despliegue demasiado pequeña para sus necesidades empresariales o demasiado grande para los recursos de hardware disponibles.
- Las plantillas de despliegue más amplias proporcionan una mejor compartimentación: es menos probable que lo fallos de un producto afecten otros productos. Seleccione una plantilla que equilibre la utilización y el rendimiento de recursos (RAM). Por ejemplo, si está disponible una cantidad más amplia de RAM, es probable que desee coger la plantilla de despliegue más grande que le permita su RAM; esto dará como resultado una mejor compartimentación del sistema.

Puede utilizar el control deslizante para seleccionar una plantilla de despliegue, o puede seleccionar una cantidad RAM de la lista desplegable. A medida que modifique la configuración, tenga en cuenta que el indicador *Número de servidores de procesamiento de Adaptive* cambia para mostrar cómo quedará configurado el sistema si selecciona esta configuración.

> **Nota**
>
> La plantilla de despliegue que seleccione solo afecta los servidores de procesamiento de Adaptive (APS). Otros servidores, por ejemplo CMS, o los servidores de tareas de Adaptive, no quedan afectados.

> **Nota**
>
> La RAM necesaria es la cantidad mínima de RAM necesaria para los servidores de la plataforma de BI. Por ejemplo, en un equipo con 16 GB de RAM, en el que el sistema operativo utiliza 1 GB de RAM, el servidor de la base de datos utiliza otro 1 GB, y el servidor de la plataforma de BI utiliza 10 GB, RAM obligatoria es de 10 GB, no 12 GB ni 16 GB. El número de RAM obligatoria solo representa el valor típico; puede que su sistema necesite más RAM en exceso de carga. Para un rendimiento del sistema óptimo, debe llevar a cabo el tamaño del sistema siempre.

> **Nota**
>
> Cada vez que abre la página *Capacidad*, la plantilla de despliegue que se muestra en la página representa el estado del sistema actual, en caso de que coincida con una de las plantillas de despliegue predefinidas. Por ejemplo, si ha creado manualmente un servidor de procesamiento de Adaptive extra mediante la CMC, el estado actual del sistema no coincide con ninguna de las plantillas de despliegue y, por lo tanto, la página *Capacidad* muestra la casilla de verificación *Conservar la configuración existente* para indicar que el sistema no se configuró en el asistente. En un despliegue de varios nodos, la casilla de verificación *Conservar la configuración existente* también se muestra en caso de que algún nodo tenga un número de APS que no coincida con la plantilla de despliegue, o si el número de APS en distintos nodos es diferente. Puede borrar la casilla de verificación si desea utilizar el asistente para modificar la configuración.

> **Nota**
>
> Para simplificar el despliegue, la configuración APS que selecciona se aplica en cada nodo (siempre que estos nodos tengan un APS instalado); por lo tanto, cuantos más nodos tenga, más capacidad tendrá el clúster.

> **Nota**
>
> El administrador no administra los complementos, por ejemplo, Servicios de datos o Servicio de diseño de aplicación de análisis (AADS). El asistente no moverá los servicios creados por los complementos a APS distintos.
>
> Ejemplos:
>
> - Si un APS que aloja otros servicios desde la instalación principal de la plataforma de BI aloja AADS, al ejecutar el asistente y cambiar el tamaño de la plantilla del despliegue de XS a M, el asistente creará siete APS nuevos y moverá todos los servicios a los siete APS, excepto el servicio AADS, que permanecerá en el APS inicial.
> - El complemento de Servicios de datos crea un APS dedicado. El asistente no altera este APS dedicado y no cuanta el APS cuando informa del número de APS del sistema.

### El archivo DeploymentTemplates.pdf

Para obtener una descripción detallada de la configuración que realizará el asistente para cada plantilla de despliegue disponible, haga clic en el vínculo *plantilla de despliegue* en la página *Capacidad* para abrir el archivo `DeploymentTemplates.pdf`.

El archivo `DeploymentTemplates.pdf` describe detalladamente las plantillas de despliegue. Tenga en cuenta que las plantillas no especifican el número de usuarios admitidos, ya que el número de usuarios admitidos dependen de la carga. Debe realizar el tamaño del sistema para determinar el número de usuarios que tendrá que admitir y, por tanto, la cantidad de RAM que necesitará, los requisitos de la CPU, etc.

## 4.4 Especificar ubicaciones de carpetas de datos

Utilice la página *Carpetas* para especificar dónde desea guardar la plataforma de BI para guardar sus archivos de datos y de registro. Puede especificar ubicaciones de carpetas, o aceptar las ubicaciones actuales.

Si el despliegue de la plataforma de BI tiene varios nodos, tiene dos opciones para definir las ubicaciones de carpetas:

- Si desea configurar las mismas ubicaciones de carpetas para todos los nodos, seleccione la opción *Todos los nodos tienen las mismas ubicaciones de carpetas*.
- Si los servidores del clúster no están configurados de la misma forma, las rutas de instalación o las estructuras del directorio de archivos pueden ser diferentes. Puede seleccionar la opción *Los nodos tienen distintas ubicaciones de carpetas* para configurar ubicaciones de carpetas específicas para cada nodo.

Cada vez que se abre el asistente en la página *Carpetas*, visualiza los nombres de carpetas de la forma siguiente:

- Si todos los nodos tienen carpetas con los mismos valores (es decir, las carpetas de registro en todos los servidores en el clúster son idénticas, y las carpetas de datos en todos los servidores en el clúster son idénticas, etc.), la opción *Todos los nodos tienen las mismas ubicaciones de carpetas* está seleccionada y los nombres de las carpetas actuales se muestran.
- Si todas las carpetas de un tipo en concreto (registro, datos, auditoría, almacén de archivos de entrada, o almacén de archivos de salida) son idénticas en cada nodo, pero distintas entre los nodos, la opción *Los nodos tienen distintas ubicaciones de carpetas* está seleccionada y los nombres de las carpetas actuales se muestran.
- Si todas las carpetas de un tipo en particular no son idénticas en cada nodo, y distintas entre nodos, la opción *Los nodos tienen distintas ubicaciones de carpetas* está seleccionada pero los nombres de las carpetas se dejan en blanco.

Si modifica las ubicaciones de las carpetas, el asistente configura el sistema para utilizar las nuevas carpetas. Con la excepción de auditar carpetas de datos, el asistente no copia ni mueve los contenidos de las carpetas originales a las carpetas nuevas. Si las carpetas nuevas no contienen el contenido correcto, o si tiene datos en las carpetas originales y desea migrarlos, puede ser que desee copiar o mover los datos a carpetas nuevas.

Para el almacén de archivos de entrada, almacén de archivos de salida, y las carpetas de datos, si la nueva ubicación de carpetas está vacía, debe copiar de forma manual los archivos desde la ubicación de carpetas antigua, restáurelos a partir de la copia de seguridad. Para la carpeta de registro, copie los archivos desde la carpeta antigua solo si desea que la carpeta nueva contenga los archivos de registro que existen en la ubicación de carpetas.

> → Sugerencias
>
> Si planea copiar o restaurar archivos a carpetas nuevas, llévelo a cabo antes de reinicializar los nodos.

Escenarios de ejemplo:

- Si modifica la ubicación de carpetas, y la carpeta original contiene informes, estos informes no estarán disponibles en la plataforma de BI hasta que los copie a la carpeta nueva y reinicialice los nodos.
- Si la carpeta original contiene informes dañados o modificados, y desea revertirlos a una copia de seguridad bien conocida, debe recuperar los informes de la copia de seguridad y colocarlos en la carpeta nueva, no copiar los contenidos de la carpeta original.
- Si los archivos de datos estaban originalmente ubicados en un disco en la unidad X, y modifica esta unidad a Y en el sistema operativo, no es necesario que mueva los archivos de datos; solo tiene que modificar la ubicación de carpetas en la plataforma de BI.

Si ha modificado manualmente algunas ubicaciones de carpetas, para que algunos servidores en un nodo utilicen un conjunto de carpetas, mientras otros servidores en el mismo nodo utilizan distintas carpetas, la página *Carpetas* muestran la casilla de verificación *Conservar la configuración existente* para indicar que el sistema se ha configurado fuera del asistente. Por ejemplo, puede que tenga dos servidores del repositorio de archivos del mismo nodo configurados para utilizar distintas rutas del archivo de registro. Puede borrar la casilla de verificación si desea utilizar el asistente para modificar la configuración actual.

Para obtener más información sobre los tipos de archivos almacenados en cada carpeta, haga clic en los iconos *?*.

> ⓘ Nota
>
> Si modifica cualquiera de las siguientes ubicaciones de carpetas, tendrá que reiniciar manualmente todos los nodos cuando el asistente se haya completado para que los cambios tengan efecto:
>
> - Almacén de archivos de entrada
> - Almacén de archivos de salida
> - Carpeta de registro
> - Carpeta de datos

## 4.5 Revisar los cambios

Cuando haya terminado de seleccionar los ajustes de configuración, se visualizan en la página *Revisar* para que los revise, antes de que se apliquen en el sistema de la plataforma de BI. Para cada categoría de ajustes, puede hacer clic en *Detalles* para ver una lista o descripción detallada de los ajustes y los cambios que se aplicarán.

Si desea cambiar algún ajuste, puede acceder a las páginas individuales directamente desde el menú de navegación a la izquierda del asistente.

Las selecciones se guardan en un archivo de registro, que puede descargar desde la página Finalizado.

También se genera y guarda un archivo de respuesta. El archivo de respuesta le ayuda a automatizar la configuración del sistema. Puede hacer clic en el botón *Descargar* para ver el archivo de respuesta o descargarlo en el disco local.

Cuando hace clic en *Aplicar*, los ajustes de configuración se aplican al despliegue de la plataforma de BI. Cuando el asistente finaliza, se muestra la página *Finalizado*, que muestra los siguientes pasos que debe llevar a cabo manualmente.

### Información relacionada

Archivos de registro y archivos de respuesta [página 97]

## 4.6 Archivos de registro y archivos de respuesta

La página *Completado* muestra el estado de sus modificaciones, y le permite descargar y ver los archivos de registro y de respuesta para su sesión.

Los archivos de registro y de respuesta se guardan automáticamente en la carpeta Asistente de configuración del sistema, a la que puede acceder desde la CMC. Los nombres de los archivos están fechados en el formato `año_mes_día_hora_minuto_segundo`. Los archivos de registro utilizan una extensión `.log`, y los archivos de respuesta utilizan una extensión `.ini`.

También puede hacer clic en los botones *Descargar* para ver los archivos de registro y de respuesta, o descargarlos en el disco local.

El archivo de registro contiene lo siguiente:

- Un registro de todas las modificaciones realizadas en esta sesión de configuración.
- La ubicación en la que se ha guardado el archivo de respuesta.
- Una lista con la descripción de los siguientes pasos que debe llevar a cabo.

### Información relacionada

Uso de un archivo de respuesta [página 97]

### 4.6.1 Uso de un archivo de respuesta

Cada vez que se completa el asistente, guarda el archivo de respuesta, que contiene sus selecciones o respuestas (respuestas) a todas las preguntas de las páginas del asistente. El archivo de respuesta se puede utilizar para configurar otros clústeres en el despliegue de la plataforma de BI sin tener que pasar por el asistente de cada uno, o se puede utilizar en una fecha tardía si desea establecer el sistema en el mismo estado de configuración. El uso de un archivo de respuesta le permite automatizar el despliegue y evitar errores del operario.

Para usar un archivo de respuesta, ejecute una secuencia de comandos que tome un archivo de respuesta como un parámetro. Primero, localice el archivo de respuesta que desee utilizar, y guárdelo en un disco. Los

archivos de respuesta se guardan automáticamente en la carpeta Asistente de configuración del sistema, a la que los administradores pueden acceder desde la CMC. El horario y la fecha de los nombres de los archivos están fijados en el formato `año_mes_día_hora_minuto_segundo` y tienen una extensión `.ini`. Desde la CMC, puede ver el archivo de respuesta y guardarlo en el disco, o utilizar los comandos de menú *Organizar* > *Enviar* > *Ubicación de archivo*.

También puede descargar el archivo de respuesta para la sesión del asistente actual desde la página *Revisar* o *Completado*, y guardarlo en el disco.

Si desea modificar la configuración en el archivo de respuesta antes de utilizarlo, puede editar el archivo de respuesta en un editor de texto. Consulte el archivo de respuesta de ejemplo siguiente para obtener más detalles.

## Ejecución de la secuencia de comandos

Cuando tenga el archivo de respuesta adecuado, utilice el archivo como un parámetro de línea de comando para la secuencia de comandos que ejecutan el asistente:

- En Windows, ejecute el archivo del lote `SCW.bat`.
- En Unix, ejecute el archivo de secuencia de comandos `scw.sh`.

Los archivos de lote y de secuencia de comandos se ubican en la misma carpeta en la que se ubican otras secuencias de comandos de administración del servidor:

- En Windows: `<installdir>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.
- En Unix: `<installdir>/sap_bobj/enterprise_xi40/linux_x64/scripts`.

Los archivos de lote y de secuencia de comandos toman estos parámetros de línea de comandos:

- `-ayuda`: Visualiza la ayuda de línea de comandos.
- `-r`: Especifica la ruta y el nombre del archivo de respuesta.
- `-cms`: Especifica el Servidor de administración central (CMS) al que desea iniciar sesión. Si se omite este parámetro, el CMS se predetermina en el equipo local y el puerto predeterminado (6400). Ejemplo: `nombre_equipo: 6500`
- `-username`: especifica la cuenta que proporciona derechos administrativos a la plataforma de BI. Si se omite este parámetro, se utiliza la cuenta de administrador predeterminada.
- `-contraseña`: Especifica la contraseña de la cuenta. Si no se especifica, se intenta con una contraseña en blanco. Para utilizar el parámetro `-contraseña`, también debe utilizar el parámetro `-nombredeusuario`.

## Ejemplos

En Windows: `SCW.bat –r c:\carpeta\nombrearchivo.ini –cms nombrecms:6400 –nombreusuario "administrador" –contraseña contraseñaejemplo`

En Unix: `./scw.sh –r /inicio/carpeta/nombrearchivo.ini –cms nombrecms:6400 –nombreusuario "administrador" –contraseña contraseñaejemplo`

## Archivo de respuesta de ejemplo

```
# ********************************************
# ****************** Products ******************
# ********************************************
# Keep the existing configuration for products.
# Valid values = true or false.
# "true": the existing product configuration will be preserved.
# "false": the product configuration will be modified according to the
“Products.” settings below.
Products.KeepExistingConfiguration = true
# The “Products.” settings below will be ignored if
Products.KeepExistingConfiguration = true.
# Auto-start the servers for these products.
# Valid values = true or false.
# "true": the product's servers and their dependencies are auto-started with BI
platform.
# "false": the product's servers are not auto-started with BI platform.
# Crystal Reports
Products.crystalreports = true
# Analysis edition for OLAP
Products.olap = true
# Web Intelligence
Products.webintelligence = false
# Dashboards (Xcelsius)
Products.dashboards = false
# Data Federator
Products.datafederator = true
# Lifecycle Manager
Products.LCM = true
# ********************************************************
# ****************** Deployment Template ******************
# ********************************************************
# Keep the existing configuration for the deployment template.
# Valid values = true or false.
# "true": the existing deployment template configuration will be preserved and
the Capacity.DeploymentTemplate setting below will be ignored.
# "false": the deployment template configuration will be modified according to
the Capacity.DeploymentTemplate setting below.
Capacity.KeepExistingConfiguration = true
# Specify the deployment template for all nodes.
# Valid values = xs, s, m, l, xl.
Capacity.DeploymentTemplate = xs
# ********************************************
# ****************** Folders ******************
# ********************************************
# Keep the existing configuration for folder locations.
# Valid values = true or false.
# "true": the existing folder configuration will be preserved.
# "false": the folder configuration will be modified according to the "Folders."
settings below.
Folders.KeepExistingConfiguration = true
# The “Folders.” settings below will be ignored if
Folders.KeepExistingConfiguration = true.
# ------ All nodes use the same folders ------
# Use this section when you have one node, or when all nodes have the same
folder locations. Otherwise, comment it out.
Folders.InputFileStore = <Path>
Folders.OutputFileStore = <Path>
Folders.Log = <Path>
Folders.Data = <Path>
Folders.Auditing = <Path>
# ------ Nodes use different folders ------
# Use this section when nodes have different folder locations. Otherwise,
comment it out.
# ------ NodeOne ------
```

```
# Folders.NodeOne.InputFileStore = <Path>
# Folders.NodeOne.OutputFileStore = <Path>
# Folders.NodeOne.Log = <Path>
# Folders.NodeOne.Data = <Path>
# Folders.NodeOne.Auditing = <Path>
# ------ NodeTwo ------
# Folders.NodeTwo.InputFileStore = <Path>
# Folders.NodeTwo.OutputFileStore = <Path>
# Folders.NodeTwo.Log = <Path>
# Folders.NodeTwo.Data = <Path>
# Folders.NodeTwo.Auditing = <Path>
```

Hay que especificar todas las configuraciones en el archivo de respuesta, y ninguna puede estar vacía, excepto en los casos siguientes:

- Si tiene un despliegue con varios nodos, puede seleccionar omitir la configuración de la carpeta para uno o más nodos, que dejarán las carpetas en los nodos no modificados. Sin embargo, para los nodos que especifica en el archivo de respuesta, hay que especificar las ubicaciones de carpetas.
- Si el parámetro `ConservarConfiguraciónExistente` está fijando en `verdadero`, puede omitir la configuración restante de la página. Por ejemplo, si `Productos.ConservarConfiguraciónExistente = verdadero`, puede omitir la configuración restante de los *Productos* del archivo de respuesta.

En algunos casos, el archivo de respuesta incluirá distintos productos que están instalados en el clúster de destino. En estos casos, los comportamientos se aplican a:

- Si el archivo de respuesta no contiene definiciones para los productos instalados en el clúster de destino, la operación fallará.
- Si el archivo de respuesta contiene definiciones de productos que no están presentes en el clúster de destino, se agrega un mensaje de advertencia al archivo de respuesta, y los productos restantes se configurarán adecuadamente.

> **ⓘ Nota**
>
> Cuando haya utilizado un archivo de respuesta para configurar un clúster, tendrá que realizar manualmente los pasos adicionales descritos en la sección «Siguientes pasos» del archivo de registro.

> **ⓘ Nota**
>
> Para una mayor seguridad, solo es necesario el soporte de autenticación de Enterprise (no Windows AD, LDAP, o SAP).

> **ⓘ Nota**
>
> Si prefiere posponer el reinicio del cualquier nodo a la siguiente reinicialización planificada, ejecute la secuencia de comandos justo antes del descanso planificado del sistema.

# 5 Administración de licencias

## 5.1 Administrar claves de licencia

En esta sección se describe cómo administrar claves de licencia para el despliegue de la plataforma de BI.

### Información relacionada

Para ver la información de licencia [página 101]
Para agregar una clave de licencia [página 101]
Para ver la actividad actual de las cuentas: [página 102]

## 5.1.1 Para ver la información de licencia

El área de administración *Claves de licencia* de la CMC identifica el número de licencias simultáneas, con nombre y de procesador asociadas con cada clave.

1. Vaya al área de administración *Claves de licencia* de la CMC.
2. Seleccione una clave de licencia.

   Los detalles asociados a la clave aparecen en el área *Información de clave de licencia*. Para adquirir claves de licencia adicionales, póngase en contacto con su representante de ventas de SAP.

### Información relacionada

Para agregar una clave de licencia [página 101]
Para ver la actividad actual de las cuentas: [página 102]

## 5.1.2 Para agregar una clave de licencia

Si se actualiza a partir de una versión de prueba del producto, asegúrese de eliminar la clave de evaluación antes de agregar licencias o códigos de clave de activación del producto nuevos. Después de agregar las nuevas claves de la licencia, tendrá que volver a activar todos los servidores.

> **Nota**
>
> Si ha recibido unas claves de licencia nuevas después de un cambio en la forma en que la organización implementa las licencias de la plataforma de Business Intelligence, tiene que eliminar todas las claves de licencia anteriores del sistema para conservar la compatibilidad.

> **Nota**
>
> Al actualizar a la plataforma SAP BusinessObjects Business Intelligence 4.2 Support Package 2 o a una versión posterior desde cualquier de las versiones anteriores, las licencias existentes se comportan como licencias caducadas. Debe generar una nueva clave de licencia paral a plataforma SAP BusinessObjects Business Intelligence 4.2 y usarla.

1. Vaya al área de administración *Claves de licencia* de la CMC.
2. Escriba la clave en el campo *Agregar clave*.
3. Haga clic en *Agregar*.

Se agrega la clave a la lista.

### Información relacionada

Para ver la información de licencia [página 101]
Para ver la actividad actual de las cuentas: [página 102]

## 5.1.3 Para ver la actividad actual de las cuentas:

1. Diríjase al área de administración *Configuración* de la CMC.
2. Haga clic en *Ver métricas globales del sistema*.

   Esta sección muestra el uso actual de las licencias junto con las medidas de trabajos adicionales.

### Información relacionada

Para agregar una clave de licencia [página 101]
Para ver la información de licencia [página 101]

# 6 Administrar usuarios y grupos

## 6.1 Información general de administración de cuentas

La administración de cuentas implica todas las tareas relativas a la creación, asignación, cambio y organización de la información de usuario y grupo. El área de administración *Usuarios y grupos* de la Consola de administración central (CMC) proporciona un punto central para realizar estas tareas.

Después de haber creado las cuentas y grupos de usuarios, puede agregar objetos y especificar sus derechos. Cuando un usuario inicia sesión, puede ver los objetos mediante la plataforma de lanzamiento de BI o su aplicación Web personalizada.

### 6.1.1 Administración de usuarios

En el área de administración *Usuarios y grupos*, puede especificar todo lo que un usuario necesita para acceder a la plataforma de BI. También puede ver las dos cuentas de usuario predeterminadas resumidas en la tabla «Cuentas de usuario predeterminadas».

Cuentas de usuario predeterminadas

| Nombre de cuenta | Descripción |
|---|---|
| *Administrador* | Este usuario pertenece a los grupos *Administradores* y *Todos*. Un administrador puede realizar todas las tareas de todas las aplicaciones de la Plataforma de BI (por ejemplo, la CMC, el CCM, el Asistente de publicación y la Plataforma de lanzamiento de BI). |
| *Invitado* | Este usuario pertenece al grupo *Todos*. Esta cuenta está activada de forma predeterminada, y el sistema no le asigna ninguna contraseña. Si le asigna una contraseña, se interrumpirá el inicio de sesión único en la plataforma de lanzamiento de BI. |
| *SMAdmin* | Se trata de una cuenta de solo lectura que SAP Solution Manager usa para acceder a los componentes de la Plataforma de BI. |

> **Nota**
>
> Las migraciones de objetos las realizan mejor los miembros del grupo Administradores; concretamente, la cuenta de usuario Administrador. Para migrar un objeto, es posible que también deban migrarse muchos objetos relacionados. Es posible que no pueda obtener para una cuenta de administrador delegado los derechos de seguridad necesarios para todos los objetos.

## 6.1.2 Administración de grupos

Los grupos son colecciones de usuarios que comparten los mismos privilegios de cuenta; por lo tanto, puede crear grupos basados en departamento, función o ubicación. Los grupos permiten cambiar los derechos de los usuarios en un lugar (o grupo) en vez de modificar los derechos de cada cuenta de usuario individualmente. Además, puede asignar derechos de objeto a un grupo o grupos.

En el área *Usuarios y grupos*, puede crear grupos que faciliten acceso al informe o carpeta a varias personas. De esta manera, podrá realizar cambios en un sitio en lugar de tener que modificar cada cuenta de usuario de manera individual. También puede ver las distintas cuentas de grupo predeterminadas resumidas en la tabla «Cuentas de grupo predeterminadas».

Para ver los grupos disponibles en la CMC, haga clic en *Listas de grupos* en el panel *Árbol*. También puede hacer clic en *Jerarquía de grupos* para mostrar una lista jerárquica de todos los grupos disponibles.

Cuentas de grupo predeterminadas

| Nombre de cuenta | Descripción |
|---|---|
| *Administradores* | Los miembros de este grupo pueden realizar todas las tareas en todas las aplicaciones de Plataforma de BI (CMC, CCM, Asistente de publicación y Plataforma de lanzamiento de BI). De forma predeterminada, el grupo *Administrador* sólo contiene el usuario Administrador. |
| *Todos* | Cada usuario pertenece al grupo *Todos*. |
| *Diseñador de grupos QaaWS* | Los miembros de este grupo tienen acceso a Query as a Web Service. |
| *Usuarios de la Herramienta de conversión de informes* | Los miembros de este grupo tienen acceso a la aplicación Herramienta de conversión de informes. |
| *Traductores* | Los miembros de este grupo tienen acceso a la aplicación Administrador de traducciones. |
| *Usuarios de Universe Designer* | Los usuarios que pertenecen a este grupo tienen acceso a las carpetas *Universe Designer* y *Conexiones*. Pueden controlar quién tiene derechos de acceso a la aplicación Designer. Deberá agregar usuarios a este grupo según lo necesite. De forma predeterminada ningún usuario pertenece a este grupo. |

### Información relacionada

Cómo funcionan los derechos en la Plataforma de BI [página 127]
Concesión de acceso a usuarios y grupos [página 116]

## 6.1.3 Tipos de autenticación disponibles

Antes de configurar los grupos y las cuentas de usuario dentro de la plataforma de BI, decida qué tipo de autenticación desea usar: En la tabla «Tipos de autenticación» se resumen las opciones de autenticación que puede tener disponibles, según las herramientas de seguridad que utilice su organización.

Tipos de autenticación

| Tipo de autenticación | Descripción |
|---|---|
| Enterprise | Use la autenticación de Enterprise predeterminada del sistema si prefiere crear cuentas y grupos distintos para su uso con la Plataforma de BI, o si aún no ha configurado una jerarquía de usuarios y grupos en un servidor de directorios LDAP o un servidor de Windows AD. |
| LDAP | Si configura un servidor de directorio LDAP, puede usar las cuentas de usuario y grupos LDAP existentes en la plataforma de BI. Al asignar cuentas LDAP a la plataforma de BI, los usuarios pueden acceder a las aplicaciones de la plataforma de BI con su nombre de usuario y contraseña LDAP. De esta manera se elimina la necesidad de volver a crear cuentas de usuario y grupos individuales dentro de la plataforma de BI. |
| Windows AD | Se pueden usar cuentas de usuarios y grupos de Windows AD existentes en la plataforma de BI. Al asignar cuentas AD a la plataforma de BI, los usuarios pueden iniciar sesión en las aplicaciones de la plataforma de BI con su nombre de usuario y contraseña AD. De esta manera se elimina la necesidad de volver a crear cuentas de usuario y grupos individuales dentro de la plataforma de BI. |
| SAP | Puede asignar funciones de SAP existentes en las cuentas de la Plataforma de BI. Después de asignar funciones de SAP, los usuarios pueden iniciar sesión en las aplicaciones de la Plataforma de BI con las credenciales de SAP. De esta manera se elimina la necesidad de volver a crear cuentas de usuario y grupos individuales dentro de la plataforma de BI. |
| Oracle EBS | Puede asignar funciones de Oracle EBS existentes en las cuentas de la Plataforma de BI. Después de asignar las funciones de Oracle EBS, los usuarios pueden iniciar sesión en las aplicaciones de la Plataforma de BI con las credenciales de Oracle EBS. De esta manera se elimina la necesidad de volver a crear cuentas de usuario y grupos individuales dentro de la plataforma de BI. |
| Siebel | Puede asignar funciones de Siebel existentes en las cuentas de la Plataforma de BI. Después de asignar funciones de Siebel, los usuarios pueden iniciar sesión en las aplicaciones de la Plataforma de BI con las credenciales de Siebel. De esta manera se elimina la necesidad de volver a crear cuentas de usuario y grupos individuales dentro de la plataforma de BI. |

| Tipo de autenticación | Descripción |
| --- | --- |
| PeopleSoft Enterprise | Puede asignar funciones de PeopleSoft existentes en las cuentas de la Plataforma de BI. Después de asignar funciones de PeopleSoft, los usuarios pueden iniciar sesión en las aplicaciones de la Plataforma de BI con las credenciales de PeopleSoft. De esta manera se elimina la necesidad de volver a crear cuentas de usuario y grupos individuales dentro de la plataforma de BI. |
| JD Edwards EnterpriseOne | Puede asignar funciones de JD Edwards existentes en las cuentas de la Plataforma de BI. Después de asignar las funciones de JD Edwards, lo usuarios pueden iniciar sesión en las aplicaciones de la Plataforma de BI con las credenciales de JD Edwards. De esta manera se elimina la necesidad de volver a crear cuentas de usuario y grupos individuales dentro de la plataforma de BI. |

## 6.2 Administración de cuentas Enterprise y generales

Puesto que la autenticación de Enterprise es el método de autenticación predeterminado de la plataforma de BI, se habilita automáticamente al instalar por primera vez el sistema. Al agregar y administrar usuarios y grupos, la plataforma mantiene la información de usuario y grupo dentro de su base de datos.

> **Nota**
>
> Cuando un usuario cierra la sesión Web en la plataforma de BI desplazándose a una página que no es de la plataforma o cerrando el explorador Web, no se cierra la sesión de Enterprise y sigue teniendo la licencia. El tiempo de la sesión de Enterprise se agotará en 24 horas aproximadamente. Para finalizar la sesión de Enterprise del usuario y liberar la licencia para que la usen otros usuarios, el usuario debe cerrar la sesión de la plataforma de BI.

### 6.2.1 Para crear una cuenta de usuario

Al crear un nuevo usuario, se especifican las propiedades del usuario y se selecciona el grupo o grupos para el usuario.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Haga clic en *Administrar* > *Nuevo* > *Nuevo usuario*.
   Aparece el cuadro de diálogo *Nuevo usuario*.
3. Para crear un usuario de Enterprise:
   a. En la lista *Tipo de autenticación*, seleccione *Enterprise*.
   b. Escriba el nombre de cuenta, el nombre completo, la dirección de correo electrónico y la información de descripción.

> → Sugerencias
>
> Utilice el área de descripción para incluir información adicional acerca del usuario o cuenta.

c. Especifique la información de la clave de acceso y las opciones que cumplen los criterios de clave de acceso definidos para la autenticación empresarial.

4. Para crear un usuario que iniciará la sesión con un tipo de autenticación diferente, seleccione la opción adecuada en la lista *Tipo de autenticación* y escriba un nombre de cuenta.
5. Realice una de las siguientes acciones para designar la cuenta de usuario (según el contrato de licencia de la plataforma de BI):
   - Seleccione *Usuario simultáneo* si este usuario pertenece a un contrato de licencia en el que se estipula el número de usuarios que se pueden conectar al mismo tiempo.
   - Seleccione *Usuario con nombre* si este usuario pertenece a un contrato de licencia que asocia un usuario específico con una licencia. Las licencias de los usuarios con nombre resultan útiles para aquellos que necesitan acceso a la plataforma de BI, independientemente del número de usuarios conectados.

   > ⓘ Nota
   >
   > El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.
   >
   > Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

6. Haga clic en *Crear y cerrar*.

   El usuario se añade al sistema y también se añade automáticamente al grupo Todos. Se crea automáticamente una bandeja de entrada para el usuario, con un alias de Enterprise.

Ahora puede agregar el usuario a un grupo o especificar derechos para el usuario.

## 6.2.2 Para modificar una cuenta de usuario

Utilice este procedimiento para modificar las propiedades o pertenencia al grupo de un usuario.

> ⓘ Nota
>
> El usuario se verá afectado si se conecta al efectuar el cambio.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Seleccione el usuario cuyas propiedades desee cambiar.
3. Haga clic en *Administrar* > *Propiedades*.
   Aparecerá el cuadro de diálogo *Propiedades* del usuario.
4. Modifique las propiedades del usuario.

   Además de todas las opciones que estaban disponibles cuando se creó inicialmente la cuenta, ahora puede deshabilitar la cuenta mediante la activación de la casilla de verificación *La cuenta está desactivada*.

> **Nota**
>
> Los cambios que realice en la cuenta de usuario no aparecerán hasta la próxima vez que el usuario inicie sesión.

5. Haga clic en *Guardar y cerrar*.

### Información relacionada

Para crear un nuevo alias para un usuario existente [página 124]

## 6.2.3 Para eliminar una cuenta de usuario

Utilice este procedimiento para eliminar una cuenta de usuario. El usuario podría recibir un error si se conectan cuando se elimina la cuenta. Al eliminar una cuenta de usuario, también se borrarán la carpeta Favoritos, las categorías personales y la bandeja de entrada de dicho usuario.

Si piensa que el usuario necesitará tener acceso a la cuenta en el futuro, active la casilla de verificación *La cuenta está deshabilitada* de la página *Propiedades* del usuario seleccionado en vez de eliminar la cuenta.

> **Nota**
>
> La eliminación de una cuenta de usuario no evita necesariamente que el usuario pueda iniciar sesión de nuevo en la plataforma de BI. Si la cuenta de usuario también existe en el sistema de terceros, y si la cuenta pertenece al grupo de terceros asignado a la plataforma de BI, el usuario aún podrá iniciar sesión.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Seleccione el usuario que desee eliminar.
3. Haga clic en *Administrar* > *Eliminar*.

   Aparecerá el cuadro de diálogo de confirmación de la eliminación, notificándole si el usuario seleccionado es el propietario de uno o más objetos.
4. Seleccione *OK*.
   La cuenta de usuario queda eliminada.

### Información relacionada

Para modificar una cuenta de usuario [página 107]
Para desactivar un alias [página 126]

## 6.2.4 Para crear un nuevo grupo

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Haga clic en *Administrar* > *Nuevo* > *Nuevo grupo*.
   Aparece el cuadro de diálogo *Crear nuevo grupo de usuarios*.
3. Introduzca el nombre y la descripción del grupo.
4. Haga clic en *Aceptar*.

Después de crear un grupo nuevo, puede agregar usuarios, agregar subgrupos o especificar la pertenencia de grupo para que el grupo nuevo sea realmente un subgrupo. Puesto que los subgrupos le proporcionan niveles de organización adicionales, resultan útiles al configurar derechos de objeto para controlar el acceso de usuarios al contenido de la plataforma de BI.

## 6.2.5 Para modificar las propiedades de un grupo

Puede modificar las propiedades de un grupo si cambia cualquiera de las opciones.

> **Nota**
>
> Los usuarios que pertenecen al grupo se verán afectados por la modificación la próxima vez que se conecten.

1. En el área de administración *Usuarios y grupos* de la CMC, seleccione el grupo.
2. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
3. Modifique las propiedades del grupo.

   Haga clic en los vínculos de la lista de navegación para acceder a otros cuadros de diálogo y modificar otras propiedades.

   - Si desea cambiar el título o la descripción del grupo, haga clic en *Propiedades*.
   - Si desea modificar los derechos que las entidades de seguridad tienen en el grupo, haga clic en *Seguridad de usuario*.
   - Si desea modificar los valores de perfil de los miembros de grupo, haga clic en *Valores del perfil*.
   - Si desea agregar el grupo como un subgrupo a otro grupo, haga clic en *Miembro de*.
4. Haga clic en *Guardar*.

## 6.2.6 Para ver miembros de grupo

Puede utilizar este procedimiento para ver los usuarios que pertenecen a un grupo específico.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Expanda *Jerarquía de grupos* en el panel *Árbol*.
3. Seleccione el grupo en el panel *Árbol*.

> **Nota**
>
> Puede que la lista tarde unos minutos en aparecer si tiene un gran número de usuarios en el grupo o si el grupo está asignado a un directorio de terceros.

Se muestra la lista de los usuarios que pertenecen al grupo.

## 6.2.7 Para agregar subgrupos

Puede agregar un grupo a otro. Al hacerlo, el grupo que ha agregado se convierte en un subgrupo.

> **Nota**
>
> Agregar un subgrupo es similar a especificar la pertenencia al grupo.

1. En el área de administración *Usuarios y grupos* de la CMC, seleccione el grupo que desea agregar como subgrupo a otro grupo.
2. Haga clic en *Acciones* > *Unirse al grupo*.
   Aparecerá el cuadro de diálogo *Unirse al grupo*.
3. Mueva el grupo al que desee agregar el primer grupo de la lista *Grupos disponibles* a la lista *Grupo(s) de destino*.
4. Haga clic en *Aceptar*.

### Información relacionada

Para especificar la pertenencia al grupo [página 110]

## 6.2.8 Para especificar la pertenencia al grupo

Puede hacer que un grupo sea miembro de otro grupo. El grupo que se convierte en miembro de otro se denomina subgrupo. El grupo al que se le añade el subgrupo es el grupo principal. Un subgrupo hereda los derechos del grupo principal.

1. En el área de administración *Usuarios y grupos* de la CMC, haga clic en el grupo que desea agregar a otro grupo.
2. Haga clic en *Acciones* > *Miembro*.
   Aparece el cuadro de diálogo *Miembro de*.
3. Haga clic en *Unirse al grupo*.
   Aparecerá el cuadro de diálogo *Unirse al grupo*.
4. Mueva el grupo al que desee agregar el primer grupo de *Grupos disponibles* a la lista *Grupo(s) de destino*.

   El grupo nuevo que haya creado heredará cualquier derecho asociado al grupo principal.

5. Haga clic en *Aceptar*.
   Volverá al cuadro de diálogo *Miembro de* y el grupo principal aparecerá en la lista de grupos.

## 6.2.9 Para eliminar un grupo

Puede eliminar un grupo cuando dicho grupo ya no sea necesario. No puede eliminar los grupos predeterminados Administrador y Todos.

> **Nota**
>
> Los usuarios que pertenecen al grupo eliminado se verán afectados por el cambio la próxima vez que se conecten.

> **Nota**
>
> Los usuarios que pertenecen al grupo eliminado perderán los derechos que hereden del grupo.

Para eliminar un grupo de autenticación de terceros, como el grupo de usuarios de Windows AD, use el área de administración *Autenticación* de la CMC.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Seleccione el grupo que desee eliminar.
3. Haga clic en *Administrar* > *Eliminar*.
   Aparece el cuadro de diálogo confirmación de eliminación.
4. Haga clic en *Aceptar*.
   Se elimina el grupo.

## 6.2.10 Agregar usuarios o grupos de usuarios en masa

Puede utilizar un archivo CSV (Valores separados por coma) para agregar usuarios o grupos de usuarios a grandes cantidades a la CMC. En un archivo CSV con el formato correcto, las comas separan datos en una línea, tal y como se muestra en el siguiente ejemplo:

```
Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue
```

Las siguientes condiciones se aplican al proceso de adición masiva:

- Cualquier línea del archivo CSV que contenga un error se omitirá del proceso de importación.
- Las cuentas de usuario se deshabilitan inicialmente después de la importación.
- Puede usar contraseñas en blanco al crear nuevos usuarios. Sin embargo, debe usar una contraseña de autenticación de Enterprise válida para cualquier actualización posterior de los usuarios existentes.
- Cuando se agrega una credencial de BD a una cuenta, las credenciales de bases de datos se activarán en el perfil del usuario.

> **Nota**
>
> Solo los usuarios que forman parte del grupo de administradores predeterminado pueden añadir usuarios en grandes cantidades. Esta función no está disponible para administradores delegados.

1. En el área de administración de la CMC *Usuarios y grupos*, seleccione *Administrar* > *Importar* > *Usuario/Grupo/Credencial de BD*
   Aparece el cuadro de diálogo *Importar usuario/grupo/credencialBD*.
2. Haga clic en *Examinar*, seleccione un archivo CSV y haga clic en *Verificar*.

   El archivo se procesa. Si los datos tienen el formato correcto en el archivo, se activa el botón *Importar*. Si los datos no tienen el formato correcto , aparece información sobre el error, y debe corregir el error antes de que la CMC pueda verificar el archivo a importar.
3. Haga clic en *Importar*.

Los usuarios o grupos de usuarios se importan a la CMC.

Para revisar los usuarios o los grupos de usuarios que ha agregado, seleccione *Administrar* > *Importar* > *Historial* en el área de administración *Usuarios y grupos*.

## 6.2.11 Para habilitar la cuenta de invitado

La cuenta de invitado está desactivada de forma predeterminada para garantizar que nadie pueda iniciar sesión en la plataforma de BI con esta cuenta. Esta configuración predeterminada también deshabilita la funcionalidad de inicio de sesión único anónimo de la plataforma de BI, de modo que los usuarios no pueden acceder a la plataforma de lanzamiento de BI sin tener que proporcionar un nombre de usuario y una contraseña válidos.

Realice esta tarea si desea activar la cuenta de invitado de modo que los usuarios no requieran sus propias cuentas para acceder a la plataforma de lanzamiento de BI.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Haga clic en *Lista de usuarios* en el panel de navegación.
3. Seleccione *Invitado*.
4. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
5. Desactive la casilla de verificación *La cuenta está desactivada*.
6. Haga clic en *Guardar y cerrar*.

## 6.2.12 Adición de usuarios a grupos

Los grupos de usuarios permiten a los administradores realizar tareas de la plataforma de lanzamiento de BI para lotes de usuarios (por ejemplo, puede personalizar las preferencias o planificar publicaciones para grupos de usuarios en particular).

Puede agregar usuarios a los grupos de las siguientes formas:

- Seleccione el grupo y haga clic en *Acciones* > *Agregar miembros al grupo*.
- Seleccione el usuario y haga clic en *Acciones* > *Miembro de*.
- Seleccione el usuario y haga clic en *Acciones* > *Unirse al grupo*.

Puede agregar un usuario a más de un grupo de usuarios. No obstante, si un usuario pertenece a dos o más grupos de usuarios, la plataforma de lanzamiento de BI mostrará las preferencias para un solo grupo.

### Información relacionada

Para especificar la pertenencia al grupo [página 110]

## 6.2.12.1 Agregar un usuario a uno o más grupos de usuarios

Puede agregar un usuario a más de un grupo de usuarios. Sin embargo, la plataforma de lanzamiento de BI visualiza las preferencias solo para un grupo de usuarios.

1. En el área de administración *Usuarios y grupos* de la CMC, seleccione el usuario a agregar.
2. Seleccione *Acciones* > *Unirse al grupo*.

   > **Nota**
   >
   > Todos los usuarios de la plataforma de BI del sistema pertenecen al grupo Todos.

3. En el cuadro de diálogo *Unirse al grupo*, mueva el grupo para agregar el usuario desde la lista *Grupos disponibles* en la lista *Grupos de destino*.

   > **→ Sugerencias**
   >
   > Use `SHIFT`+`clic` o `CTRL`+`clic` para seleccionar varios grupos.

4. Haga clic en *Aceptar*.

## 6.2.12.2 Agregar uno o varios usuarios a un grupo de usuarios

Puede agregar múltiples usuarios a un grupo de usuarios.

Las preferencias configuradas para un grupo de usuarios se aplican a todos los usuarios en el grupo. La plataforma de lanzamiento de BI muestra las preferencias para un grupo de usuarios cada vez.

1. En el área de administración *Usuarios y grupos* de la CMC, seleccione el grupo de usuarios.
2. Seleccione *Acciones* > *Agregar miembros al grupo*.
3. En el cuadro de diálogo *Agregar*, haga clic en *Lista de usuarios*.

La lista *Usuarios/grupos disponibles* se actualiza y muestra todas las cuentas de usuario del sistema.

4. Mueva uno o más usuarios al grupo desde la lista *Usuarios/grupos disponibles* a la lista *Usuarios/grupos seleccionados*.

> → Sugerencias
>
> Use `SHIFT`+`clic` o `CTRL`+`clic` para seleccionar varios usuarios. Para buscar un usuario específico, introduzca el nombre de usuario en el cuadro *buscar*.

> → Sugerencias
>
> Si su sistema tiene gran número de usuarios, haga clic en los botones *Anterior* y *Siguiente* para navegar por la lista de usuarios.

5. Haga clic en *Aceptar*.

## 6.2.13 Cambio de la configuración de la contraseña

Dentro de la CMC, puede modificar la configuración de contraseña para un usuario específico o para todos los usuarios del sistema. Las distintas restricciones enumeradas a continuación solo se aplican a las cuentas Enterprise; es decir, las restricciones no se aplican a cuentas asignadas a una base de datos de usuarios externa (LDAP o Windows AD). No obstante, en general, el sistema externo le permitirá asignar restricciones similares a las cuentas externas.

### 6.2.13.1 Para cambiar la configuración de la contraseña de usuario

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Seleccione el usuario cuya configuración de contraseña quiera cambiar.
3. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
4. Seleccione o cancele la selección de la casilla de verificación asociada a la configuración de contraseña que desea cambiar.

   Las opciones disponibles son:

   - *La contraseña nunca caduca*
   - *El usuario debe cambiar la contraseña la próxima vez que se conecte*
   - *El usuario no puede cambiar la contraseña*
5. Haga clic en *Guardar y cerrar*.

> ⓘ Nota
>
> Cuando modifica la contraseña de un usuario, se cerrarán las sesiones existentes y se le redirigirá a la página de inicio para que vuelva a iniciar sesión.

## 6.2.13.2 Cambiar la configuración de contraseña general

> **Nota**
>
> Las cuentas de usuario inactivas no se desactivarán automáticamente.

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *Enterprise*.
   Aparecerá el cuadro de diálogo *Enterprise*.
3. Seleccione la casilla de verificación asociada a cada configuración de contraseña que desee utilizar y, en caso necesario, proporcione un valor.

   En la siguiente tabla se identifican los valores mínimo y máximo para cada una de las configuraciones que se pueden efectuar.

   Opciones de contraseña

| Opción de la contraseña | Por defecto | Mínimo | Máximo recomendado |
|---|---|---|---|
| *Debe contener al menos N caracteres* | 8 caracteres | 6 caracteres | 255 caracteres |
| *No debe superar los N caracteres* | 255 caracteres | 13 caracteres | 255 caracteres |
| *Debe cambiar la contraseña cada N días* | 30 días | 2 días | 100 días |
| *No puede volver a usar las últimas N contraseñas* | 3 contraseñas | 1 contraseña | 100 contraseñas |
| *Debe esperar N minutos para cambiar la contraseña* | 0 minutos | 0 minutos | 100 minutos |
| *Deshabilitar la cuenta tras N intentos fallidos de conexión* | 10 fallido | 1 fallidos | 100 fallidos |
| *Restablecer conexión fallida después de N minutos* | 5 minutos | 1 minuto | 100 minutos |
| *Reactivar la cuenta después de N minutos* | 5 minutos | 0 minutos | 100 minutos |

> **Nota**
>
> Si realiza la actualización desde una versión inferior de Plataforma de SAP BusinessObjects Business Intelligence a cualquier versión superior, o intenta realizar cualquier tipo de instalación ampliada, deberá fijar *Deshabilitar cuenta después de N intentos fallidos de conexión* al valor predeterminado establecido.

> **Nota**
>
> Las reglas mencionadas anteriormente solo se aplican a los usuarios empresariales y no para otros tipos de autenticación de terceros.

4. Haga clic en *Actualizar*.

## 6.2.14 Concesión de acceso a usuarios y grupos

Puede otorgar acceso administrativo de usuarios y grupos a otros usuarios y grupos. Los derechos administrativos incluyen: consultar, editar y eliminar objetos; consultar y eliminar instancias de objeto; y hacer una pausa en las instancias de objeto. Por ejemplo, si se trata de la solución de problemas y el mantenimiento del sistema, quizá desee otorgar acceso al personal informático para que pueda editar y eliminar objetos.

### Información relacionada

Para asignar principales a una lista de control de acceso para un objeto [página 137]

## 6.2.15 Control del acceso a las bandejas de entrada de usuario

Al agregar un usuario, el sistema crea automáticamente una bandeja de entrada para dicho usuario. La bandeja de entrada tiene el mismo nombre que el usuario. De forma predeterminada, solo el usuario y el administrador tienen derecho a acceder a la bandeja de entrada de un usuario.

### Información relacionada

Administración de la configuración de seguridad para los objetos en la CMC [página 136]

## 6.2.16 Configurar las opciones de la plataforma de lanzamiento de BI de Fiori

En la CMC, los administradores pueden configurar las preferencias de la plataforma de lanzamiento de BI de Fiori para grupos de usuarios.

> **Nota**
>
> Si un usuario pertenece a dos o más grupos de usuarios, la plataforma de lanzamiento de BI de Fiori mostrará las preferencias configuradas para un solo grupo.

## 6.2.16.1 Configurar la pantalla de inicio de sesión de la rampa de lanzamiento BI

De forma predeterminada, la pantalla de inicio de sesión de la rampa de lanzamiento BI solicita a los usuarios el nombre de usuario y la contraseña. También puede solicitar a los usuarios el nombre del CMS y el tipo de autenticación. Para cambiar esta configuración, debe editar las propiedades de la rampa de lanzamiento BI de Fiori para el archivo BOE.war.

### 6.2.16.1.1 Configurar la pantalla de inicio de sesión de la rampa de lanzamiento BI

Para modificar la configuración predeterminada de la rampa de lanzamiento BI de Fiori, debe configurar las propiedades personalizadas del archivo BOE.war. Este archivo se despliega en el equipo que aloja el servidor de aplicaciones web.

1. Vaya al siguiente directorio de la instalación de la Plataforma de BI:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Cree un archivo nuevo con un editor de texto.
3. Guarde el archivo con el siguiente nombre:

   **`FioriBI.properties`**
4. Para incluir las opciones de autenticación en la pantalla de inicio de sesión de la rampa de lanzamiento BI de Fiori, añada la línea siguiente:

   ```
   authentication.visible=true
   ```
5. Para cambiar el tipo de autenticación predeterminado, agregue la línea siguiente:

   ```
   authentication.default=<authentication>
   ```

   Sustituya `<autenticación>` con alguna de las siguientes opciones:

| Tipo de autenticación | Valor de <autenticación> |
|---|---|
| Enterprise | `secEnterprise` |
| LDAP | `secLDAP` |
| Windows AD | `secWinAD` |
| SAP | `secSAPR3` |

6. Para solicitar a los usuarios el nombre de CMS que aparece en la pantalla de inicio de sesión de la rampa de lanzamiento BI, añada la línea siguiente:

```
cms.visible=true
```

7. Guarde y cierre el archivo.
8. Reinicie el servidor de aplicaciones Web.

Use WDeploy para volver a desplegar el archivo `BOE.war` en el servidor de aplicaciones Web. Para obtener más información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 6.2.16.2 Configuración de las preferencias de la plataforma de lanzamiento de BI de Fiori para grupos de usuarios en la CMC

Los administradores configuran las preferencias predeterminadas de la plataforma de lanzamiento de BI de Fiori para grupos de usuarios en la CMC.

Las preferencias configuradas por administrador para un grupo de usuarios se aplican a todos los usuarios en el grupo. Si un usuario pertenece a dos o más grupos de usuarios, la plataforma de lanzamiento de BI de Fiori mostrará las preferencias configuradas para un solo grupo.

Los usuarios pueden configurar sus propias preferencias en la plataforma de lanzamiento de BI de Fiori, y sus preferencias tienen prioridad sobre los valores predeterminados. Podrán volver a las preferencias predeterminadas en todo momento. Consulte la sección *Preferencias para la página de Ajustes* para el *Manual de usuario de plataforma de lanzamiento de BI de Fiori*.

No obstante, si un administrador modifica las preferencias predeterminadas de la plataforma de lanzamiento de BI de Fiori en la CMC, los valores predeterminados tendrán prioridad sobre los valores definidos por el usuario.

### 6.2.16.2.1 Configuración de las preferencias de la rampa de lanzamiento BI de Fiori para un grupo de usuarios

1. Vaya al área *Administración de usuarios y grupos* de la CMC.
2. En *Lista de grupos*, seleccione el grupo de usuarios para el que definir las preferencias de plataforma de lanzamiento de BI de Fiori.
3. Haga clic con el botón derecho y elija *Preferencias de la plataforma de lanzamiento de BI de Fiori*.
4. Borre la casilla de verificación *No se han definido preferencias*.
5. Si ha seleccionado la ficha *Inicio*, realice una de las acciones siguientes para elegir la página de inicio de la ficha:

| Opción de ficha de página de inicio | Acción |
| --- | --- |
| **Visualizar la ficha de inicio de la plataforma de lanzamiento de BI de Fiori por defecto** | Seleccione *Ficha de inicio predeterminada* |
| **Visualizar una ficha de inicio específica** | Elija *Seleccionar ficha Inicio*, luego:<br>1. En el campo *Página de aterrizaje*, seleccione la página de aterrizaje deseada.<br>• *Mi inicio*<br>• *Programar*<br>• *Bandeja de entrada*<br>• *Carpetas*<br>• *Papelera de reciclaje*<br>2. En el campo *Enumerar documentos como*, seleccione *Vista de mosaico (predeterminada)* o *Vista de lista*.<br>3. En el campo *Filtro de aterrizaje*, seleccione el filtro de aterrizaje deseado.<br>• *Mostrar todo*<br>• *Mis documentos*<br>• *Todas las categorías*<br>• *Mis favoritos*<br>• *Mis documentos vistos recientemente*<br>• *Mi ejecución reciente*<br>Puede seleccionar un objeto de *Mis carpetas*, *Carpetas públicas*, *Categorías personales* y *Categorías de la empresa* para visualizarlo como la página de inicio predeterminada. |
| **Visualizar un informe específico como página de inicio** | Elija *Seleccionar informe* y, a continuación, haga clic en *Explorar documentos* para seleccionar un documento de *Mis carpetas* o *Carpetas públicas*. |
| **Visualizar una categoría como página de inicio** | Elija *Seleccionar categoría*, luego haga clic en *Explorar categorías* para seleccionar una categoría de *Categorías personales* o *Categorías corporativas*. |

6. En el campo *Seleccionar columna para visualizar en la ficha Documentos*, seleccione las preferencias de la columna:
   - *Tipo*
   - *Última ejecución*
   - *Instancias*
   - *Descripción*
   - *Creado por*
   - *Última actualización*
   - *Creado el*
   - *Ubicación (categorías)*

- *Mis favoritos (página de inicio)*
- *Estado (programación)*
- *Hora de la instancia (programación)*
- *Ruta de acceso de carpeta*

> **Nota**
>
> De forma predeterminada, *Tipo*, *Descripción*, *Última actualización*, *Mis favoritos (página de inicio)*, *Estado (programación)* y *Hora de instancia (programación)* están seleccionados. Puede modificar la selección de columnas que desea mostrar.

7. Seleccione *Grabar y cerrar*.

Para que las preferencias definidas por un administrador se reflejen en la interfaz, los usuarios deben iniciar sesión en la plataforma de lanzamiento de BI de Fiori, seleccione *Configuración* > *Preferencias de cuenta* > *Preferencias de página*, y active *Utilizar configuración proporcionada por el administrador*.

## 6.2.17 Administrar atributos para usuarios del sistema

Los administradores de la plataforma de BI definen y agregan atributos de usuarios para usuarios del sistema a través del área *Administración de atributos de usuario* en la Consola de administración central (CMC). Puede administrar ampliar los atributos para los siguientes directorios de usuario:

- Enterprise
- SAP
- LDAP
- Windows AD

Cuando se importan usuarios desde directorios externos, como SAP, LDAP y Windows AD, normalmente estarán disponibles los siguientes atributos para las cuentas de usuario:

- Nombre completo
- Dirección de correo electrónico

### Nombres de atributo

Todos los atributos de usuario añadidos al sistema deben tener las siguientes propiedades:

- *Nombre*
- *Nombre interno*

La propiedad del «Nombre» es el identificador descriptivo del atributo y se usa para a consultar filtros al trabajar con la capa semántica universo. Para obtener más información, consulte la documentación de la herramienta de diseño de universos. Los desarrolladores usan el «Nombre interno» al trabajar con el SDK de la plataforma de BI. Esta propiedad es un nombre que se genera automáticamente.

Los nombres de atributo no deben superar los 256 caracteres y solo deben contener caracteres alfanuméricos y guiones bajos.

→ Sugerencias

Si se especifican caracteres no válidos para el atributo del nombre, la plataforma de BI no generará un nombre interno. Los nombres internos no pueden modificarse una vez añadidos al sistema. Se recomienda que seleccione con cuidado los nombres de atributos adecuados que contengan caracteres alfanuméricos y guiones bajos.

### Requisitos previos para expandir atributos de usuario asignados

Antes de añadir atributos de usuario al sistema, todos los complementos de autenticación relevantes para usuarios externos deben ser configurados para asignar e importar usuarios. Además, deberá familiarizarse con el esquema de los directorios externos, en particular con los nombres utilizados para los atributos objetivo.

ⓘ Nota

Para el complemento de autenticación de SAP, solo se pueden especificar los atributos de la estructura BAPIADDR3.

Una vez configurada la plataforma de BI para asignar los nuevos atributos de usuario, los valores se rellenarán en la siguiente actualización programada. Todos los atributos de usuarios se muestran en el área de administración *Usuarios y grupos* de la CMC.

## 6.2.18 Priorización de atributos de usuario en varias opciones de autenticación

Al configurar los complementos de autenticación de SAP, LDAP y AD, puede especificar los niveles de prioridad para cada complemento en relación con los otros dos. Por ejemplo, en el área de autenticación LDAP, use la opción *Establecer la prioridad del enlace de atributos de LDAP respecto a otros enlaces de atributos* para especificar la prioridad de LDAP en relación con SAP y AD. De forma predeterminada, el valor de atributo de Enterprise tiene prioridad por delante de cualquier valor de un directorio externo. Las prioridades de enlace de atributos se configuran en el nivel de complemento de autenticación y no para cualquier atributo específico.

### Información relacionada

Configurar el host LDAP [página 276]
Importar funciones de SAP [página 347]

## 6.2.19 Agregar un nuevo atributo de usuario

Antes de agregar un nuevo atributo de usuario a la plataforma de BI, debe configurar el complemento de autenticación para el directorio externo desde el que se asignan cuentas de usuario. Esto se aplica a SAP, LDAP

y Windows AD. Específicamente, debe seleccionar la opción *Importar nombre completo, dirección de correo electrónico y otros atributos* para todos los complementos necesarios.

> **ⓘ Nota**
>
> No debe realizar ninguna tarea preliminar antes de dedicar atributos para las cuentas de usuario de Enterprise.

> **→ Sugerencias**
>
> Si planea extender el mismo atributo en varios complementos, se recomienda configurar el nivel de prioridad de enlace de atributos según los requisitos de la organización.

1. Vaya al área de administración *Administración de atributos de usuario* de la CMC.
2. Haga clic en el icono *Agregar un nuevo atributo asignado personalizado*.
   Aparece el cuadro de diálogo *Agregar atributo*.
3. Especifique un nombre para el nuevo atributo en el campo *Nombre*.

   La plataforma de BI usará el nombre proporcionado como un nombre descriptivo para el nuevo atributo.

   Al introducir el nombre descriptivo, el campo *Nombre interno* se rellena automáticamente según el siguiente formato: `SI_[Friendlyname]`. A medida que el administrador del sistema especifica un nombre de atributo "descriptivo", la plataforma de BI genera automáticamente el nombre "interno".
4. En caso necesario, modifique el campo *Nombre interno* mediante letras, números o guiones bajos.

   > **→ Sugerencias**
   >
   > El valor del campo *Nombre interno* solo se puede modificar en este paso. No puede editar este valor una vez que se guarde el nuevo atributo.

   Si el nuevo atributo es para cuentas de Enterprise, vaya al paso 8.
5. Seleccione la opción adecuada para *Agregar un nuevo origen para* de la lista y haga clic en el icono *Agregar*.
   Están disponibles las siguientes opciones:

   - *SAP*
   - *LDAP*
   - *AD*

   La fila de la tabla se crea para el origen del atributo especificado del atributo.
6. En la columna *Nombre del origen del atributo*, especifique el nombre del atributo del directorio de origen.

   La plataforma de BI no proporciona un mecanismo para verificar automáticamente que el nombre del atributo proporcionado existe en el directorio externo. Asegúrese de que el nombre proporcionado es correcto y válido.
7. Repita los pasos 5 y 6 si se necesitan orígenes adicionales para el nuevo atributo.
8. Haga clic en *Aceptar* para guardar y enviar el nuevo atributo a la plataforma de BI.
   El nuevo Nombre de atributo, Nombre interno, Origen y Nombre de origen de atributo aparece en el área de administración *Administración de atributos de usuario* de la CMC.

El nuevo atributo y su valor correspondiente para cada cuenta de usuario afectada. se mostrará en la siguiente actualización programada en el área de administración *Usuarios y grupos*.

Si se usan varios orígenes para el nuevo atributo, asegúrese de que se especifican las prioridades de enlace de atributos correctos para cada complemento de autenticación.

### 6.2.20 Editar los atributos de usuario personalizados

Para editar los atributos de usuario que se hayan creado en la plataforma de BI, use el procedimiento siguiente. Puede editar lo siguiente:

- El nombre del atributo en la plataforma de BI

  > **Nota**
  >
  > No se trata del nombre interno que se usa para el atributo. Una vez se haya creado y agregado un atributo a la plataforma de BI, el nombre interno no se puede modificar. Para eliminar un nombre interno, los administradores tienen que suprimir el atributo asociado.

- El nombre de origen del atributo
- Los orígenes adicionales para el atributo

1. Vaya al área de administración *Administración de atributos de usuario* de la CMC.
2. Seleccione el atributo que desea editar.
3. Haga clic en el icono *Editar atributo seleccionado*.
   Aparecerá el cuadro de diálogo *Editar*.
4. Modifique el nombre o la información de origen del atributo.
5. Haga clic en *Aceptar* para guardar y enviar las modificaciones a la plataforma de BI.
   Los valores modificados aparecen en el área de administración *Gestión de atributos de usuario* de la CMC.

El nombre de atributo y los valores modificados aparecerán después de la siguiente actualización programada en el área de administración de *Usuarios y grupos*.

## 6.3 Administración de alias

Si un usuario tiene varias cuentas en la plataforma de BI, éstas se pueden vincular con la función de asignación de alias. Esto resulta útil cuando un usuario tiene una cuenta de terceros que está asignada a Enterprise y una cuenta de Enterprise.

Si se asigna un alias al usuario, éste puede iniciar una sesión mediante un nombre de usuario y una contraseña de terceros o un nombre de usuario y una contraseña de Enterprise. Por tanto, un alias permite al usuario conectarse a través de más de un tipo de autenticación.

En la CMC, la información de alias se muestra en la parte inferior del cuadro de diálogo *Propiedades* de un usuario. Un usuario puede tener cualquier combinación de alias de Enterprise, LDAP o Windows AD.

### 6.3.1 Para crear un usuario y agregar un alias de terceros

Al crear un usuario y seleccionar un tipo de autenticación diferente al de Enterprise, el sistema crea el nuevo usuario en la plataforma de BI y crea un alias de terceros para el usuario.

> **Nota**
>
> Para que el sistema cree el alias de terceros, se deben cumplir los siguientes criterios:
>
> - La herramienta de autenticación tiene que haberse activado en la CMC.
> - El formato del nombre de cuenta debe concordar con el formato requerido para el tipo de autenticación.
> - La cuenta de usuario debe existir en la herramienta de autenticación de terceros y debe pertenecer a un grupo que ya esté asignado a la plataforma de BI.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Haga clic en *Administrar* > *Nuevo* > *Nuevo usuario*.
   Aparece el cuadro de diálogo *Nuevo usuario*.
3. Seleccione el tipo de autenticación del usuario, por ejemplo, Windows AD.
4. Escriba el nombre de cuenta de terceros del usuario, por ejemplo, **`bsmith`**.
5. Seleccione el tipo de conexión del usuario.
6. Haga clic en *Crear y cerrar*.

   El usuario se agrega a la plataforma de BI y se le asigna un alias para el tipo de autenticación seleccionado, por ejemplo, secWindowsAD:ENTERPRISE:bsmith. Si es necesario, puede agregar, asignar y reasignar alias a los usuarios.

## 6.3.2 Para crear un nuevo alias para un usuario existente

Puede crear alias para usuarios de la plataforma de BI existentes. El alias puede ser un alias de Enterprise, o un alias de una herramienta de autenticación de terceros.

> **Nota**
>
> Para que el sistema cree el alias de terceros, se deben cumplir los siguientes criterios:
>
> - La herramienta de autenticación tiene que haberse activado en la CMC.
> - El formato del nombre de cuenta debe concordar con el formato requerido para el tipo de autenticación.
> - La cuenta de usuario debe existir en la herramienta de autenticación de terceros y debe pertenecer a un grupo asignado a la plataforma.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Seleccione el usuario al que desee agregar un alias.
3. Haga clic en *Administrar* > *Propiedades*.
   Aparecerá el cuadro de diálogo *Propiedades*.
4. Haga clic en *Nuevo alias*.
5. Seleccione el tipo de autenticación.
6. Escriba el nombre de cuenta del usuario.
7. Haga clic en *Actualizar*.

Se creará un alias para el usuario. Al ver el usuario en la CMC, aparecerán al menos dos alias, el que ya se asignó al usuario y el que se acaba de crear.

8. Haga clic en *Guardar y cerrar* para salir del cuadro de diálogo *Propiedades*.

## 6.3.3 Para asignar un alias desde otro usuario

Al asignar un alias a un usuario, se traslada un alias de terceros de otro usuario al usuario que se está viendo actualmente. No se pueden asignar o reasignar alias de Enterprise.

> **Nota**
>
> Si un usuario solo tiene un alias y se asigna ese último alias a otro usuario, el sistema eliminará la cuenta de usuario, la carpeta Favoritos, las categorías personales y la bandeja de entrada de dicha cuenta.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Seleccione al usuario que desee asignar un alias.
3. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
4. Haga clic en *Asignar alias*.
5. Escriba la cuenta de usuario que tiene el alias que desea asignar y haga clic en *Buscar ahora*.
6. Mueva el alias que desee asignar de la lista *Alias disponibles* a la lista *Alias que se agregarán a* `<nombre de usuario>`.

   Aquí `<nombre de usuario>` representa el nombre de usuario al que va a asignar un alias.

   > **→ Sugerencias**
   >
   > Para seleccionar varios alias, utilice la combinación `MAYÚS` + `clic` o `CTRL` + `clic`.

7. Haga clic en *Aceptar*.

## 6.3.4 Para eliminar un alias

Al eliminar un alias, esté se borrará del sistema. Si un usuario solo tiene un alias y éste se elimina, el sistema borrará automáticamente la cuenta de usuario, la carpeta Favoritos, las categorías personales y la bandeja de entrada de dicha cuenta.

> **Nota**
>
> La eliminación del alias de un usuario no impide necesariamente que el usuario pueda iniciar sesión de nuevo en la plataforma de BI. Si la cuenta de usuario aún existe en el sistema de terceros, y si la cuenta pertenece a un grupo asignado a la plataforma de BI, la plataforma de BI aún permitirá que el usuario inicie sesión. Que el sistema cree un nuevo usuario o que asigne el alias a un usuario existente, dependerá de qué opciones de actualización se hayan seleccionado para la herramienta de autenticación en el área de administración *Autenticación* de la CMC.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Seleccione el usuario cuyo alias desee eliminar.
3. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
4. Haga clic en el botón *Eliminar alias* situado junto al alias que desee eliminar.
5. Si se le pide confirmación, haga clic en *Aceptar*.
   El alias se elimina.
6. Haga clic en *Guardar y cerrar* para salir del cuadro de diálogo *Propiedades*.

## 6.3.5 Para desactivar un alias

Puede evitar que un usuario inicie sesión en la plataforma de BI mediante un método de autenticación concreto si deshabilita el alias del usuario asociado a dicho método. Para evitar que un usuario acceda a la plataforma por completo, deshabilite todos los alias de dicho usuario.

> **Nota**
>
> La eliminación de un usuario del sistema no impide necesariamente que el usuario pueda iniciar sesión de nuevo en la plataforma de BI. Si la cuenta de usuario aún existe en el sistema de terceros, y si la cuenta pertenece a un grupo asignado a la plataforma, el sistema aún permitirá al usuario iniciar sesión. Para asegurarse de que un usuario ya no pueda usar uno de sus alias para iniciar sesión en la plataforma, es mejor deshabilitar el alias.

1. Vaya al área de administración *Usuarios y grupos* de la CMC.
2. Seleccione el usuario cuyo alias desee desactivar.
3. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
4. Desactive la casilla de verificación *Habilitado* del alias que desee desactivar.

   Repita este paso para cada alias que desee desactivar.
5. Haga clic en *Guardar y cerrar*.
   El usuario ya no podrá iniciar una sesión mediante el tipo de autenticación que acaba de desactivar.

### Información relacionada

Para eliminar un alias [página 125]

# 7 Establecimiento de derechos

## 7.1 Cómo funcionan los derechos en la Plataforma de BI

Los derechos son unidades básicas para controlar el acceso de los usuarios a los objetos, usuarios, aplicaciones, servidores y otras funciones de la plataforma de BI. Desempeñan un papel importante en la protección del sistema especificando las acciones individuales que pueden realizar los usuarios con los objetos. Además de permitir controlar el acceso al contenido de la Plataforma de BI, los derechos permiten delegar la administración de usuarios y grupos en departamentos distintos, y proporcionar al personal informático acceso administrativo a los servidores y grupos de servidores.

Es importante tener en cuenta que los derechos se establecen en objetos como informes y carpetas en lugar de hacerlo en los principales (los usuarios y grupos) que acceden a ellos. Por ejemplo, para conceder acceso a un administrador a una determinada carpeta del área *Carpetas* se agrega el administrador a la lista de control de acceso (la lista de los principales que tienen acceso a un objeto) para la carpeta. No puede conceder acceso al administrador mediante la configuración de los derechos del administrador en el área *Usuarios y grupos*. La configuración de derechos del administrador en el área *Usuarios y grupos* se utiliza para conceder a otros principales (como los administradores delegados) acceso al administrador como un objeto del sistema. De este modo, los propios principales son como objetos para otros con mayores derechos de administración.

Cada derecho de un objeto se puede conceder, denegar o dejar sin especificar. El modelo de seguridad de la Plataforma de BI está diseñado de manera que si se deja sin especificar un derecho, éste se deniega. Asimismo, si se establecen ajustes en un derecho, de manera que un usuario o grupo lo tiene concedido y denegado al mismo tiempo, el derecho queda denegado. Este diseño «basado en la denegación» sirve para garantizar que ningún usuario o grupo adquiera automáticamente derechos que no se les haya concedido explícitamente.

Esta regla tiene una excepción importante. Si un derecho está establecido específicamente en un objeto secundario que contradice los derechos heredados del objeto principal, el derecho establecido en el objeto secundario reemplaza los derechos heredados. Esta excepción se aplica a los usuarios que también son miembros de los grupos. Si a un usuario se le concede explícitamente un derecho que se deniega al grupo del usuario, el derecho establecido en el usuario reemplaza los derechos heredados.

### Información relacionada

Reemplazo de derechos [página 131]

### 7.1.1 Niveles de acceso

Los niveles de acceso son grupos de derechos que los usuarios necesitan frecuentemente. Permiten a los administradores establecer niveles de seguridad comunes rápida y uniformemente en lugar de tener que establecer los derechos individuales uno a uno.

La plataforma de BI dispone de varios niveles de acceso predefinidos. Estos niveles de acceso predefinidos se basan en un modelo de derechos incrementales: empezando por *Ver* y terminando por *Control total*, cada nivel de acceso agrega nuevos derechos a los otorgados por el nivel precedente.

No obstante, también puede crear y personalizar sus propios niveles de acceso; esto puede reducir considerablemente los costes administrativos y de mantenimiento asociados a la seguridad. Considere una situación en la que un administrador debe administrar dos grupos: jefes de ventas y empleados de ventas. Ambos grupos necesitan acceder a cinco informes del sistema de la Plataforma de BI, pero los jefes de ventas necesitan más derechos que los empleados de ventas. Los niveles de acceso predefinidos no satisfacen las necesidades de ningún grupo. En vez de agregar grupos a cada informe como principales y modificar sus derechos en cinco lugares distintos, el administrador puede crear dos nuevos niveles de acceso, Jefes de ventas y Empleados de ventas. A continuación, el administrador agrega ambos grupos como principales a los informes y asigna a los grupos sus correspondientes niveles de acceso. Cuando se deban modificar los derechos, el administrador puede modificar los niveles de acceso. Como los niveles de acceso se aplican a ambos grupos en los cinco informes, los derechos de dichos grupos tienen que actualizarse rápidamente.

### Información relacionada

Uso de niveles de acceso [página 141]

## 7.1.2 Configuración de derechos avanzados

Para proporcionarle un control total sobre la seguridad de los objetos, la CMC le permite establecer derechos avanzados. Estos derechos avanzados proporcionan mayor flexibilidad ya que la seguridad de los objetos se define a un nivel granular.

Use la configuración de derechos avanzados, por ejemplo, si debe personalizar los derechos de una entidad de seguridad sobre un determinado objeto o conjunto de objetos. Sobre todo, utilice los derechos avanzados para denegar explícitamente a un usuario o a un grupo cualquier derecho que no debería cambiar cuando, en el futuro, haga cambios en las pertenencias a grupos o en los niveles de seguridad de las carpetas.

En la tabla siguiente se resumen las opciones de las que se dispone al establecer los derechos avanzados.

Opciones de derechos

| Icono | Opción de derechos | Descripción |
|---|---|---|
| | *Concedido* | El derecho se ha concedido a una entidad de seguridad. |
| | *Denegado* | El derecho se ha denegado a una entidad de seguridad. |
| | *No especificado* | El derecho no se ha especificado para una entidad de seguridad. De forma predeterminada, los derechos establecidos en *No especificado* se deniegan. |
| | *Aplicar a objeto* | El derecho se aplica al objeto. Esta opción está disponible al hacer clic en *Concedido* o en *Denegado*. |

| Icono | Opción de derechos | Descripción |
|---|---|---|
| | *Aplicar a objeto secundario* | El derecho se aplica a objetos secundarios. Esta opción está disponible al hacer clic en *Concedido* o en *Denegado*. |

## Información relacionada

Derechos específicos del tipo [página 134]

## 7.1.3 Herencia

Los derechos se establecen en un objeto de un principal para controlar el acceso al objeto; sin embargo, no resulta práctico establecer el valor explícito de cada posible derecho de cada principal en cada objeto. Considere un sistema con 100 derechos, 1.000 usuarios y 10.000 objetos: para establecer derechos explícitamente en cada objeto requeriría que el CMS almacenara miles de millones de derechos en su memoria, y, lo más importante, haría falta que un administrador estableciera manualmente cada uno.

Los patrones de herencia solucionan este problema. Con la herencia, los derechos que tienen los usuarios sobre los objetos del sistema proceden de una combinación de la pertenencia a diferentes grupos y subgrupos y de objetos que han heredado derechos de las carpetas y subcarpetas principales. Estos usuarios pueden heredar derechos como resultado de su pertenencia a un grupo; los subgrupos pueden heredar derechos de sus grupos principales, y tanto usuarios como grupos pueden heredar derechos de sus carpetas principales.

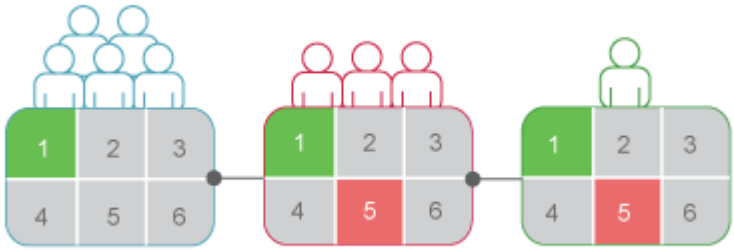
De manera predeterminada, los usuarios o grupos que tienen derechos sobre una carpeta heredan los mismos derechos para cualquier objeto que se publique posteriormente en esa carpeta. Por lo tanto, lo mejor es establecer primero derechos adecuados para usuarios y grupos en el nivel de carpeta y, después, publicar los objetos en dicha carpeta.

La plataforma de BI reconoce dos tipos de herencia: grupo y carpeta.

### 7.1.3.1 Herencia de grupo

La herencia de grupo permite que los principales hereden derechos como resultado de su pertenencia a un grupo. La herencia de grupo resulta especialmente eficaz a la hora de organizar todos los usuarios en grupos según las convenciones de seguridad actuales de una organización.

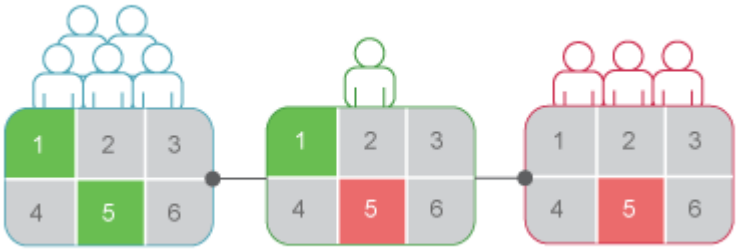
En el «ejemplo 1 de herencia de grupo» se puede ver el funcionamiento de la herencia de grupo. El Grupo rojo es un subgrupo del Grupo azul, por lo que hereda los derechos del Grupo azul. En este caso, hereda el derecho 1 como concedido y el resto de los derechos como no especificados. Cada miembro del Grupo rojo hereda estos derechos. Además, cualquier otro derecho establecido en el subgrupo lo heredan sus miembros. En este ejemplo, el usuario verde es miembro del grupo rojo y por ello hereda el derecho 1 como concedido, los derechos 2, 3, 4 y 6 como no especificados y el derecho 5 como denegado.




Ejemplo 1 de la herencia de grupo

Cuando se habilita la herencia de grupo para un usuario que pertenece a más de un grupo, el sistema tiene en cuenta los derechos de todos los grupos principales cuando comprueba las credenciales. El usuario tiene denegado todo derecho que tenga denegado explícitamente en cualquiera de los grupos principales, y el usuario tiene denegado todo derecho que esté no especificado; por lo tanto, el usuario sólo tiene otorgados los derechos que tenga otorgados en uno o más grupos (explícitamente o a través de niveles de acceso) y nunca los que tenga explícitamente denegados.

En el «ejemplo 2 de herencia de grupo», el usuario verde es miembro de dos grupos no relacionados. Del grupo azul, hereda los derechos 1 y 5 como concedidos y el resto como no especificados; sin embargo, como el usuario verde también pertenece al grupo rojo, y al grupo rojo se le ha denegado explícitamente el derecho 5, se anulará la herencia por parte del usuario verde del derecho 5 del grupo azul.




Ejemplo 2 de la herencia de grupo

## Información relacionada

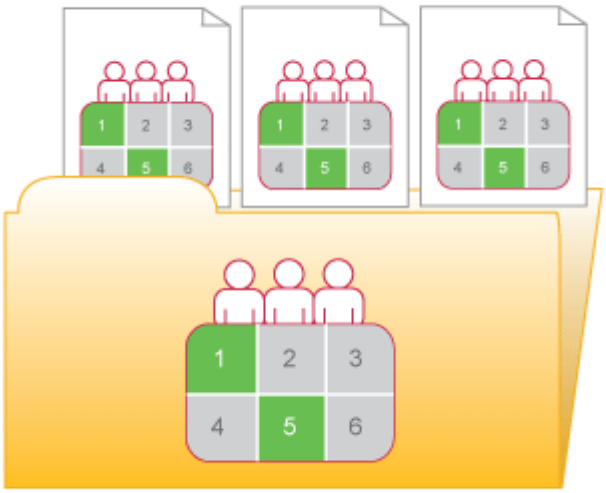
Reemplazo de derechos [página 131]

## 7.1.3.2 Herencia de carpeta

La herencia de carpeta permite que los principales hereden los derechos que tienen otorgados en la carpeta principal de un objeto. La herencia de carpeta resulta especialmente útil al organizar el contenido de la Plataforma de BI en una jerarquía de carpetas que refleje las convenciones de seguridad actuales de la organización. Por ejemplo, imagine que crea una carpeta denominada Informes de ventas y que otorga a su

grupo Ventas acceso a esta carpeta de tipo *Ver a petición*. De manera predeterminada, todos los usuarios que tengan derechos sobre la carpeta Informes de ventas heredarán los mismos derechos sobre los informes que se publiquen en esa carpeta posteriormente. Por lo tanto, el grupo Ventas tendrá acceso de tipo *Ver a petición* a todos los informes, y tendrá que establecer los derechos sobre objetos sólo una vez, en el nivel de carpeta.

En la «Ejemplo de herencia de carpeta», se han establecido los derechos del grupo rojo en una carpeta. Los derechos 1 y 5 se han concedido, mientras que el resto se ha dejado sin especificar. Con la herencia de carpeta activada, los miembros del Grupo rojo tienen los mismos derechos en el nivel de objeto que los derechos del grupo en el nivel de carpeta. Los derechos 1 y 5 se heredan como concedidos, mientras que el resto se ha dejado sin especificar.




Ejemplo de herencia de carpeta

## Información relacionada

Reemplazo de derechos [página 131]

## 7.1.3.3 Reemplazo de derechos

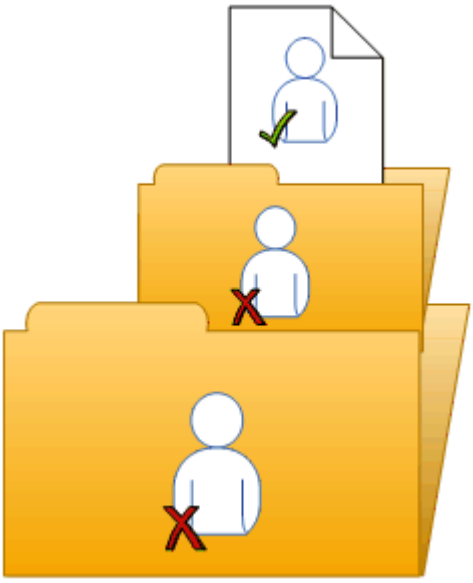
El reemplazo de derechos es un comportamiento de los derechos en el que los derechos que se han establecido en los objetos secundarios reemplazan los derechos establecidos en los objetos principales. El reemplazo de derechos se produce en las siguientes circunstancias:

- En general, los derechos que están establecidos en los objetos secundarios reemplazan los derechos correspondientes que están establecidos en los objetos principales.
- En general, los derechos que están establecidos en subgrupos o miembros de grupos reemplazan los derechos correspondientes que están establecidos en grupos.

No necesita deshabilitar la herencia para configurar los derechos personalizados en un objeto. El objeto secundario hereda la configuración de derechos del objeto principal excepto en lo que respecta a los derechos

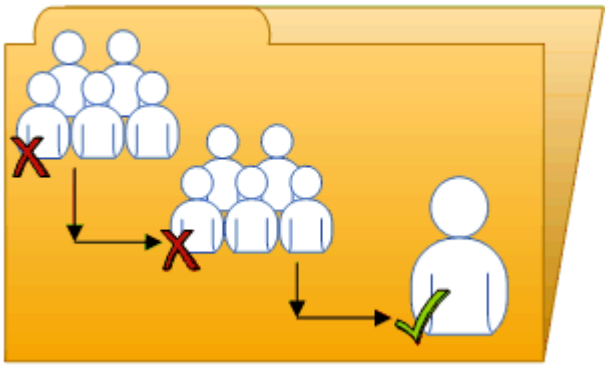
que se establecen explícitamente en el objeto secundario. Además, los cambios en la configuración de derechos en el objeto principal se aplican al objeto secundario.

«Ejemplo 1 de reemplazo de derechos» ilustra el modo en que funciona el reemplazo de derechos en los objetos principales y secundarios. Al usuario azul se le deniega el derecho a editar el contenido de una carpeta; la subcarpeta hereda la configuración de derechos. No obstante, un administrador concede al usuario azul derechos de *edición* en un documento de la subcarpeta. El derecho de *edición* que recibe el usuario azul en el documento reemplaza los derechos heredados que proceden de la carpeta y subcarpeta.



Ejemplo 1 de reemplazo de derechos

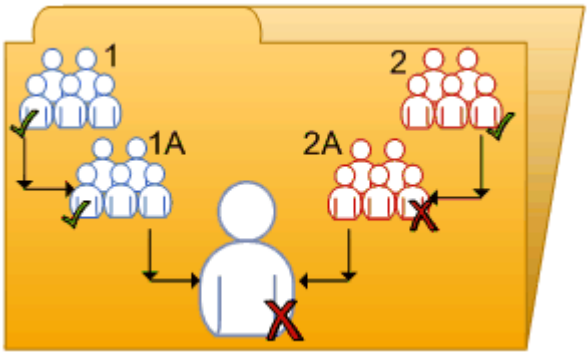
«Ejemplo 2 de reemplazo de derechos» ilustra el modo en que funciona el reemplazo de derechos en miembros y grupos. Al grupo azul se le deniega el derecho para editar una carpeta; el subgrupo azul hereda esta configuración de derechos. No obstante, un administrador concede al usuario azul, que es miembro del grupo azul y del subgrupo azul, derechos de *edición* en la carpeta. Los derechos de *edición* que recibe el usuario azul en la carpeta azul reemplazan los derechos heredados que proceden del grupo azul y del subgrupo azul.



Ejemplo 2 de reemplazo de derechos

«Reemplazo de derechos complejo» ilustra una situación en la que los efectos del reemplazo de derechos son menos evidentes. El usuario morado es miembro de los subgrupos 1A y 2A, que son los grupos 1 y 2, respectivamente. Los grupos 1 y 2 tienen derechos de *edición* en la carpeta. El subgrupo 1A hereda los

derechos de *edición* que tiene el grupo 1, pero un administrador deniega los derechos de *edición* al subgrupo 2A. La configuración de derechos del subgrupo 2A reemplaza la configuración de derechos en el grupo 2 debido al reemplazo de derechos. Por lo tanto, el usuario morado hereda una configuración de derechos contradictoria de 1A y 2A. Los subgrupos 1A y 2A no tienen relación de principal-secundario, por lo que no se produce el reemplazo de derechos, es decir, la configuración de derechos de un subgrupo no reemplaza la del otro porque tienen el mismo estado. Finalmente, al usuario morado se le deniegan los derechos *Editar* debido al modelo de derechos «basado en denegación» de la plataforma de BI.




Reemplazo de derechos complejo

El reemplazo de derechos permite realizar ajustes menores en la configuración de derechos en un objeto secundario sin descartar toda la configuración de derechos heredada. Considere una situación en la que un responsable de ventas tiene que ver los informes confidenciales de la carpeta Confidencial. El responsable de ventas forma parte del grupo Ventas, al que se le ha denegado el acceso a la carpeta y su contenido. El administrador del sistema concede al responsable los derechos de *visualización* en la carpeta Confidencial y sigue denegando el acceso al grupo Ventas. En este caso, los derechos de *visualización* concedidos al responsable de ventas reemplazan el acceso denegado que el responsable hereda de su pertenencia al grupo Ventas.

## 7.1.3.4 Alcance de los derechos

El ámbito de los derechos hace referencia a la capacidad para controlar la extensión de la herencia de derechos. Para definir el alcance de un derecho, se decide si el derecho se aplica al objeto, a sus objetos secundarios o a ambos. De forma predeterminada, el alcance de un derecho se extiende tanto a objetos como a subobjetos.

El alcance de los derechos se puede utilizar para proteger contenido personal en ubicaciones compartidas. Considere una situación en la que el departamento financiero tiene una carpeta Justificaciones de gastos compartida que contiene una subcarpeta Justificaciones de gastos personales por empleado. Los empleados desean poder ver la carpeta Justificaciones de gastos y agregar objetos en ella, pero también proteger sus subcarpetas Justificaciones de gastos personales. El administrador concede a todos los empleados los derechos de *visualización* y *adición* en la carpeta Justificaciones de gastos y limita el alcance de estos derechos sólo a la carpeta Justificaciones de gastos. Esto significa que los derechos de *visualización* y *adición* no se aplican a los objetos secundarios de la carpeta Justificaciones de gastos. Después, el administrador concede a los empleados los derechos de *visualización* y *adición* en sus propias subcarpetas Justificaciones de gastos personales.

El alcance de los derechos también puede limitar los derechos efectivos que tiene un administrador delegado. Por ejemplo, un administrador delegado puede tener los derechos *Modificar de forma segura los derechos* y

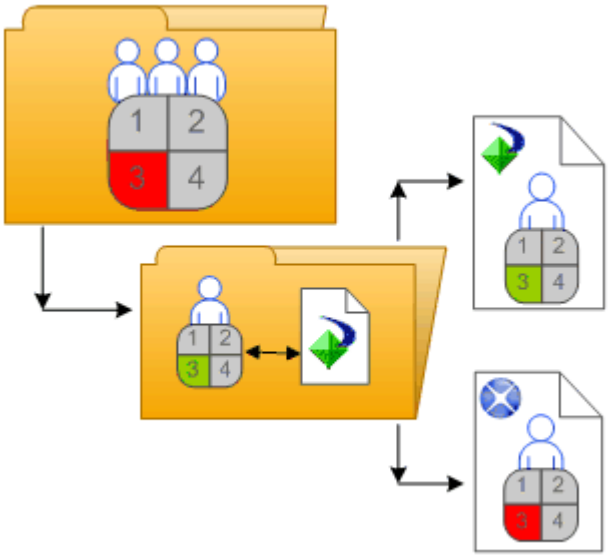
*Editar* en una carpeta, pero el alcance de estos derechos está limitado a la carpeta únicamente y no se aplica a sus objetos secundarios. El administrador delegado no puede conceder estos derechos a otro usuario en uno de los objetos secundarios de la carpeta.

## 7.1.4 Derechos específicos del tipo

Los derechos específicos del tipo son los que afectan únicamente a determinados tipos de objeto, como Crystal Reports, carpetas o niveles de acceso. Los derechos específicos del tipo constan de lo siguiente:

- Derechos generales para el tipo de objeto
  Estos derechos son idénticos a los derechos globales generales (por ejemplo, el derecho de adición, eliminación o edición de un objeto), pero se establecen en tipos de objeto específicos para reemplazar la configuración de derechos global general.
- Derechos específicos para el tipo de objeto
  Estos derechos están disponibles solo para determinados tipos de objeto. Por ejemplo, el derecho de exportación de datos de un informe aparece para Crystal Reports pero no para documentos de Word.

En el diagrama «Ejemplos de derechos específicos del tipo» se ilustra el funcionamiento de los derechos específicos del tipo. Aquí el derecho 3 representa el derecho para editar un objeto. Al grupo azul se le deniegan los derechos de *edición* en la carpeta de nivel superior y se le conceden derechos de *edición* para los Crystal Reports en la carpeta y la subcarpeta. Estos derechos de *edición* son específicos de los Crystal Reports y reemplazan la configuración de derechos en un nivel global general. Como resultado, los miembros del grupo azul tienen derechos *Editar* para los Crystal Reports, pero no para el archivo XLF de a subcarpeta.




Ejemplo de derechos específicos del tipo

Los derechos específicos del tipo son útiles porque permiten limitar los derechos de los principales según el tipo de objeto. Considere una situación en la que un administrador desee que los empleados puedan agregar objetos a una carpeta pero no puedan crear subcarpetas. El administrador concede los derechos de *adición* en el nivel global general para la carpeta y, a continuación, deniega los derechos de *adición* para el tipo de objeto carpeta.

Los derechos se dividen en las siguientes colecciones según los tipos de objetos a los que se apliquen:

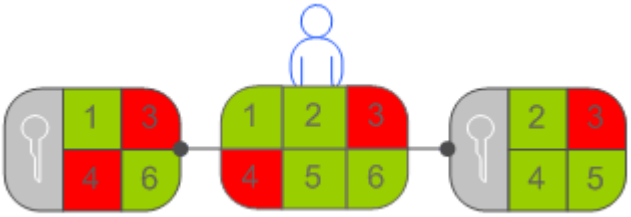
- *General*
  Estos derechos afectan a todos los objetos.
- *Contenido*
  Estos derechos están divididos según los tipos de objetos de contenido concretos. Ejemplos de tipos de objeto de contenido incluyen Crystal Reports y PDF de Adobe Acrobat.
- *Aplicación*
  Estos derechos se dividen según la aplicación de la Plataforma de BI a la que afectan. Ejemplos de aplicaciones incluyen la CMC y la plataforma de lanzamiento de BI.
- *Sistema*
  Estos derechos están divididos según el componente principal del sistema al que afectan. Algunos ejemplos de componentes principales del sistema son: calendarios, eventos, usuarios y grupos.

Los derechos específicos del tipo están en las colecciones *Contenido*, *Aplicación* y *Sistema*. En cada colección, se dividen en categorías según el tipo de objeto.

## 7.1.5 Determinación de los derechos efectivos

Tenga en cuenta estas consideraciones al establecer los derechos en un objeto:

- Cada nivel de acceso concede algunos derechos, deniega otros y deja los demás sin especificar. Cuando a un usuario se le conceden varios niveles de acceso, el sistema agrega los derechos efectivos y deniega los derechos no especificados de forma predeterminada.
- Cuando se asignan varios niveles de acceso a una entidad de seguridad en un objeto, la entidad de seguridad tiene la combinación de los derechos de cada nivel de acceso. Al usuario en «varios niveles de acceso» se le asignan dos niveles de acceso. Un nivel de acceso concede al usuario los derechos 3 y 4, mientras que el otro nivel de acceso concede solo el derecho 3. Los derechos efectivos para el usuario son 3 y 4.




Varios niveles de acceso

- Los derechos avanzados se pueden combinar con niveles de acceso para personalizar la configuración de derechos para una entidad de seguridad de un objeto. Por ejemplo, si un derecho avanzado y un nivel de acceso se asignan explícitamente a una entidad de seguridad de un objeto y el derecho avanzado contradice un derecho del nivel de acceso, el derecho avanzado reemplazará el derecho en el nivel de acceso.
  Los derechos avanzados pueden anular sus equivalentes en los niveles de acceso solo cuando se definen en el mismo objeto para el mismo principal. Por ejemplo, un derecho avanzado Agregar establecido en el nivel global general puede reemplazar la configuración de derecho general Agregar en un nivel de acceso; no puede reemplazar una configuración de derecho Agregar específico en un nivel de acceso.
  No obstante, los derechos avanzados no siempre reemplazan los niveles de acceso. Por ejemplo, a una entidad de seguridad se le deniega un derecho de *edición* en un objeto principal. En el objeto secundario,

a la entidad de seguridad se le asigna un nivel de acceso que le concede el derecho de *edición*. Al final, la entidad de seguridad tiene derechos de *edición* en el objeto secundario porque los derechos establecidos en el objeto secundario reemplazan los derechos que están establecidos en el objeto principal.

- El reemplazo de derechos permite que los derechos establecidos en un objeto secundario reemplacen los derechos que se heredan del objeto principal.

## 7.2 Administración de la configuración de seguridad para los objetos en la CMC

Puede administrar la configuración de seguridad de la mayoría de los objetos en la CMC con las opciones de seguridad del menú *Administrar*. Estas opciones permiten asignar entidades de seguridad a la lista de control de acceso de un objeto, ver los derechos que tiene una entidad de seguridad y modificar los derechos que tiene la entidad de seguridad en un objeto.

Los detalles específicos de la administración de seguridad varían según las necesidades de seguridad y el tipo de objeto para el que se configuren los derechos. No obstante, en general los flujos de trabajo de las tareas siguientes son muy similares:

- Visualización de los derechos de una entidad de seguridad en un objeto.
- Asignación de las entidades de seguridad a una lista de control de acceso para un objeto y especificar los derechos y niveles de acceso que tendrán las entidades de seguridad.
- Configuración de derechos en una carpeta de nivel superior en la plataforma de BI.

### 7.2.1 Para ver los derechos de un principal en un objeto

En general, debe seguir este flujo de trabajo para ver los derechos de una entidad de seguridad en un objeto.

1. Seleccione el objeto cuya configuración de seguridad desea visualizar.
2. Haga clic en *Administrar* > *Seguridad de usuario*.
   Aparecerá el cuadro de diálogo *Seguridad de usuario* y se mostrará la lista de control de acceso del objeto.
3. Seleccione una entidad de seguridad en la lista de control de acceso y haga clic en *Ver seguridad*.

   Se inicia el *Explorador de permisos* y muestra una lista de los derechos efectivo de la entidad de seguridad en el objeto. Además, el *Explorador de permisos* permite realizar las siguientes acciones:

   - Buscar otra entidad de seguridad cuyos derechos desee ver.
   - Filtrar los derechos mostrados según estos criterios:

     Derechos asignados
     Derechos otorgados
     Derechos no asignados
     Desde nivel de acceso
     Tipo de objeto
     El nombre del derecho

- Ordene la lista de derechos mostrada en orden ascendente o descendente según estos criterios:

  Colección
  Tipo
  Nombre del derecho
  Estado del derecho (concedido, denegado o sin especificar)

Además, puede hacer clic en uno de los vínculos de la columna *Origen* para mostrar el origen de los derechos heredados.

## 7.2.2 Para asignar principales a una lista de control de acceso para un objeto

Una lista de control de acceso especifica los usuarios a los que se les conceden o deniegan derechos en un objeto. En general, siga este flujo de trabajo para asignar una entidad de seguridad a una lista de control de acceso y especificar los derechos que tendrá la entidad de seguridad en el objeto.

1. Seleccione el objeto al que desea agregar una entidad de seguridad.
2. Haga clic en *Administrar* > *Seguridad de usuario*.
   Aparecerá el cuadro de diálogo *Seguridad de usuario* y se mostrará la lista de control de acceso.
3. Haga clic en *Agregar principales*.
   Aparecerá el cuadro de diálogo *Agregar principales*.
4. Mueva los usuarios y grupos que desee agregar como entidades de seguridad en la lista *Usuarios/grupos disponibles* a la lista *Usuarios/grupos seleccionados*.
5. Haga clic en *Agregar y asignar seguridad*.
6. Seleccione los niveles de acceso que desee conceder a la entidad de seguridad.
7. Elija si se habilitará o deshabilitará la herencia de carpetas o grupos.

Si es necesario, también puede modificar los derechos en un nivel granular para reemplazar determinados derechos en un nivel de acceso.

### Información relacionada

Para modificar la seguridad de un principal en un objeto [página 137]

## 7.2.3 Para modificar la seguridad de un principal en un objeto

En general ser recomienda utilizar niveles de acceso para asignar derechos a una entidad de seguridad. No obstante, en ocasiones es posible que deba reemplazar determinados derechos granulares en un nivel de acceso. Los derechos avanzados permiten personalizar los derechos de una entidad de seguridad encima de los niveles de acceso que ya tiene la entidad de seguridad. En general, debe seguir este flujo de trabajo para asignar derechos avanzados a una entidad de seguridad en un objeto.

1. Asigne la entidad de seguridad a la lista de control de acceso para el objeto.
2. Cuando la entidad de seguridad se haya agregado, vaya a *Administrar* > *Seguridad de usuario* para administrar la lista de control de acceso del objeto.
3. Seleccione la entidad de seguridad en la lista de control de acceso y haga clic en *Asignar seguridad*. Aparecerá el cuadro de diálogo *Asignar seguridad*.
4. Haga clic en la ficha *Opciones avanzadas*.
5. Haga clic en *Agregar o eliminar derechos*.
6. Modifique los derechos de la entidad de seguridad.

   Todos los derechos disponibles se resumen en el *apéndice Derechos*.

### Información relacionada

Para asignar principales a una lista de control de acceso para un objeto [página 137]

## 7.2.4 Establecer derechos en una carpeta de nivel superior en la plataforma de BI

En general, este flujo de trabajo se sigue para configurar los derechos en una carpeta de nivel superior en la plataforma de BI.

> **Nota**
>
> Para esta versión, las entidades de seguridad requieren derechos de *visualización* en una carpeta contenedora para poder navegar por dicha carpeta y ver sus subobjetos. Esto significa que las entidades de seguridad requieren derechos de *visualización* en la carpeta de nivel superior para ver los objetos que hay en las carpetas. Si desea limitar los derechos de *visualización* de una entidad de seguridad, puede conceder los derechos de *visualización* a una entidad de seguridad en una carpeta específica y establecer el alcance de los derechos únicamente a esa carpeta.

1. Vaya al área de CMC que tenga la carpeta de nivel superior para la que desee establecer los derechos.
2. Haga clic en *Administrar* > *Seguridad de nivel superior* > *Todo*`<Objetos>`.

   Aquí `<Objetos>` representa el contenido de la carpeta de nivel superior. Si se le pide confirmación, haga clic en *Aceptar*.

   Aparecerá el cuadro de diálogo *Seguridad de usuario* y se mostrará la lista de control de acceso de la carpeta de nivel superior.
3. Asigne la entidad de seguridad a la lista de control de acceso para la carpeta de nivel superior.
4. Si es necesario, asigne derechos avanzadas a la entidad de seguridad.

### Información relacionada

Para asignar principales a una lista de control de acceso para un objeto [página 137]

Para modificar la seguridad de un principal en un objeto [página 137]

## 7.2.5 Comprobación de la configuración de seguridad de un principal

En algunos casos puede desear saber los objetos a los que se le ha concedido o denegado el acceso a una entidad de seguridad. Puede utilizar una consulta de seguridad para ello. Las consultas de seguridad permiten determinar los objetos en los que una entidad de seguridad tiene determinados derechos y administrar los derechos de usuario. Por cada consulta de seguridad, se proporciona la siguiente información:

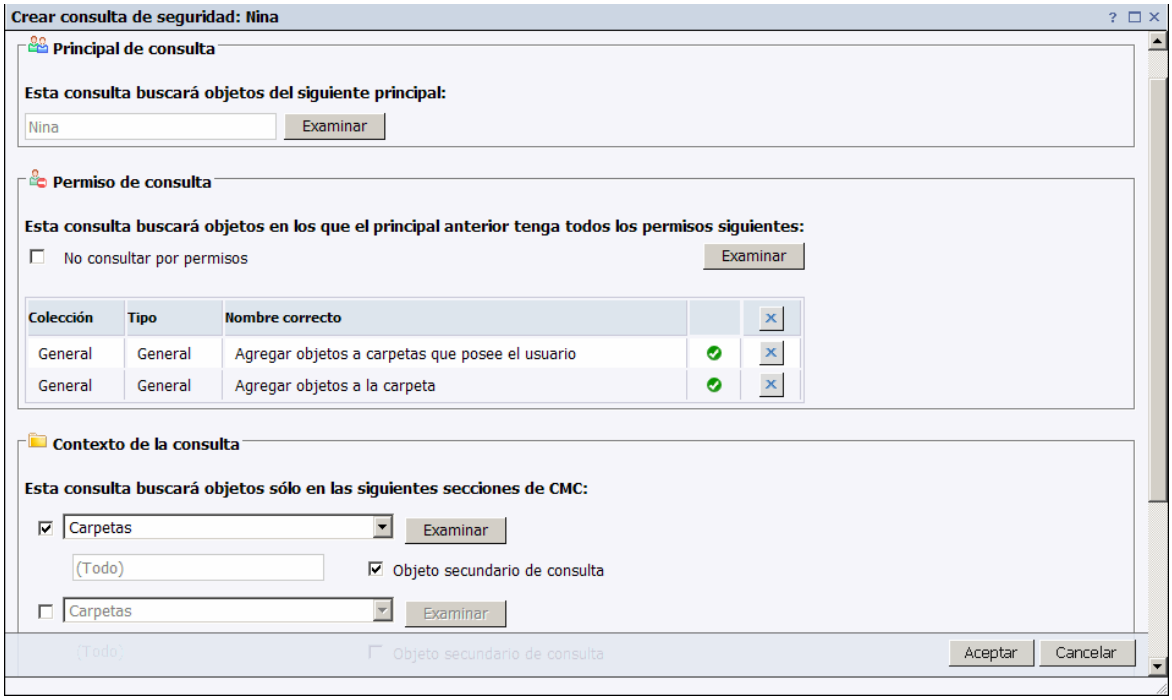
- Principal de la consulta
  Especifique el usuario o grupo para el que desee ejecutar la consulta de seguridad. Puede especificar un principal para cada consulta de seguridad.
- Permiso de la consulta
  Puede especificar el derecho o los derechos para los que desee ejecutar la consulta, el estado de estos derechos y el tipo de objeto en que están establecidos estos derechos. Por ejemplo, puede ejecutar una consulta de seguridad para todos los informes que puede actualizar un usuario o para todos los informes que no puede exportar un usuario.
- Contexto de la consulta
  Puede especificar las áreas de CMC que desee que busque la consulta de seguridad. Por cada área puede elegir si se incluirán los objetos secundarios en la consulta de seguridad. Una consulta de seguridad puede tener un máximo de cuatro áreas.

Cuando se ejecuta una consulta de seguridad, los resultados aparecen en el área *Resultados de la consulta* en el panel *Árbol* en *Consultas de seguridad*. Si desea refinar una consulta de seguridad, puede ejecutar una segunda consulta en los resultados de la primera consulta.

Las consultas de seguridad son útiles porque permiten ver los objetos en los que un principal tiene determinados derechos y proporcionan las ubicaciones de estos objetos si desea dichos derechos. Considere una situación en la que un empleado de ventas se promociona a jefe de ventas. El jefe de ventas necesita derechos de *programación* para los informes de Crystal en los que anteriormente sólo tenía derechos de *visualización* y estos informes se encuentran en diferentes carpetas. En este caso, el administrador ejecuta una consulta de seguridad para el derecho que tiene el jefe de ventas para ver informes de Crystal en todas las carpetas e incluye objetos secundarios en la consulta. Después de que se ejecute la consulta de seguridad, el administrador puede ver todos los informes de Crystal en el que el jefe de ventas tiene derechos de *visualización* en el área *Resultados de la consulta*. Como el panel *Detalles* muestra la ubicación de cada informe de Crystal, el administrador puede examinar cada informe y modificar los derechos del jefe de ventas en él.

### 7.2.5.1 Para ejecutar una consulta de seguridad

1. En el área *Usuarios y grupos*, en el panel *Detalles*, seleccione el usuario o grupo para el que desee ejecutar una consulta de seguridad.
2. Haga clic en *Administrar* > *Herramientas* > *Crear consulta de seguridad*.




Aparecerá el cuadro de diálogo *Crear consulta de seguridad*.

3. Asegúrese de que la entidad de seguridad en el área *Entidad de seguridad de consulta* es correcta.

   Si decide ejecutar una consulta de seguridad para otra entidad de seguridad, puede hacer clic en *Examinar* para seleccionar otra entidad de seguridad. En el cuadro de diálogo *Buscar principal de consulta*, expanda *Lista de usuarios* o *Lista de grupos* para buscar la entidad de seguridad o buscarla por nombre. Cuando haya finalizado, haga clic en *Aceptar* para volver al cuadro de diálogo *Crear consulta de seguridad*.

4. En el área *Permiso de consulta*, especifique los derechos y el estado de cada derecho para el que desee ejecutar la consulta.

   - Si desea ejecutar una consulta para derechos específicos que el principal tiene en los objetos, haga clic en *Examinar*, establezca el estado de cada derecho para el que desee ejecutar la consulta y haga clic en *Aceptar*.

     > → Sugerencias
     >
     > Puede eliminar derechos específicos de la consulta si hace clic en el botón Eliminar situado a la derecha o eliminar todos los derechos de la consulta si hace clic en el botón Eliminar en la fila de encabezado.

   - Si desea ejecutar una consulta de seguridad general, seleccione la casilla de verificación *No consultar por permisos*.
     Al hacerlo, la plataforma de BI ejecuta una consulta de seguridad general para todos los objetos que tienen el principal en sus listas de control de acceso independientemente de los permisos que el principal tenga en los objetos.

5. En el área *Contexto de la consulta*, especifique las áreas de la CMC que desea consultar.

   a. Seleccione una casilla de verificación situada junto a una lista.
   b. En la lista, seleccione un área de la CMC que desee consultar.

      Si desea consultar una ubicación más específica dentro de un área (por ejemplo, una determinada carpeta en Carpetas), haga clic en *Examinar* para abrir el cuadro de diálogo *Buscar contexto de la*

*consulta*. En el panel de *detalles*, seleccione la carpeta que desee consultar y haga clic en *Aceptar*. Al volver al cuadro de diálogo *Consulta de seguridad*, la carpeta que ha especificado aparece en el cuadro situado debajo de la lista.

c. Seleccione *Objeto secundario de consulta*.

d. Repita los pasos anteriores por cada área de la CMC que desee consultar.

> **Nota**
>
> Puede consultar un máximo de cuatro áreas.

6. Haga clic en *Aceptar*.
   La consulta de seguridad se ejecuta y accede al área *Resultados de la consulta*.
7. Para ver los resultados de la consulta, en el panel *Árbol*, expanda *Consultas de seguridad* y haga clic en un resultado de la consulta.

> **→ Sugerencias**
>
> Los resultados de la consulta se enumeran según los nombres de las entidades de seguridad.

   Los resultados de la consulta se muestran en el panel *Detalles*.

El área *Resultados de la consulta* conserva todos los resultados de la consulta de seguridad desde una sola sesión de usuario hasta que el usuario cierra la sesión. Si desea ejecutar la consulta otra vez pero con especificaciones nuevas, haga clic en *Acciones* > *Editar consulta*. También puede volver a ejecutar la misma consulta exacta si selecciona la consulta y hace clic en *Acciones* > *Volver a ejecutar la consulta*. Si desea conservar los resultados de la consulta de seguridad, haga clic en *Acciones* > *Exportar* para exportar los resultados de consulta como un archivo CSV.

## 7.3 Uso de niveles de acceso

Puede realizar las siguientes operaciones con los niveles de acceso:

- Copie un nivel de acceso existente, realice cambios en la copia, cámbiele el nombre y guárdela como un nuevo nivel de acceso.
- Crear, eliminar y cambiar el nombre de niveles de acceso.
- Modificar los derechos en un nivel de acceso.
- Realizar el seguimiento de la relación entre los niveles de acceso y otros objetos del sistema.
- Repetir y administrar niveles de acceso entre los sitios.
- Use uno de los niveles de acceso predefinidos en la plataforma de BI para configurar los derechos rápida y uniformemente para varios elementos principales.

En la siguiente tabla se resumen los derechos que contiene cada nivel de acceso predefinido.

Niveles de acceso predefinidos

| Nivel de acceso | Descripción | Derechos implicados |
|---|---|---|
| *Vista* | Si se establece en el nivel de carpeta, un principal puede ver la carpeta, los objetos incluidos en la carpeta y las instancias generadas por cada objeto. Si se establece en el nivel de objeto, un principal puede ver el objeto, su historial y sus instancias generadas. | • Ver objetos<br>• Ver instancias de documento |
| *Programar* | Un principal puede generar instancias programando un objeto para que se ejecute respecto a un origen de datos especificado una vez o de forma periódica. El principal puede ver, eliminar y detener la programación de instancias que posea. También puede programar usando distintos formatos y destinos, establecer parámetros e información de conexión a la base de datos, elegir servidores para procesar tareas, agregar contenido a la carpeta y copiar el objeto o carpeta. | *Derechos de nivel de acceso de visualización*, más:<br>• Programar el documento que debe ejecutarse<br>• Definir grupos de servidor para procesar tareas<br>• Copiar objetos en otra carpeta<br>• Programar para destinos<br>• Imprimir datos del informe<br>• Exportar datos del informe<br>• Editar objetos que son propiedad del usuario<br>• Eliminar instancias que son propiedad del usuario<br>• Poner en pausa y reanudar instancias de documento que son propiedad del usuario |
| *Ver a petición* | Un principal puede actualizar los datos a petición respecto a un origen de datos. | *Derechos de nivel de acceso de programación*, más:<br>• Actualizar datos del informe |
| *Control total* | Un principal tiene el control administrativo total del objeto. | Todos los derechos disponibles, incluidos:<br>• Agregar objetos a la carpeta<br>• Editar objetos<br>• Modificar los derechos que los usuarios tienen sobre los objetos<br>• Eliminar objetos<br>• Eliminar instancias |

En la tabla siguiente se resumen los derechos necesarios para realizar determinadas tareas en los niveles de acceso.

| Tarea de nivel de acceso | Derechos necesarios |
|---|---|
| Crear un nivel de acceso | *Derecho de adición* en la carpeta de nivel superior de *niveles de acceso* |
| Ver derechos granulares en un nivel de acceso | *Derecho de visualización* sobre el nivel de acceso |
| Asignar un nivel de acceso a un principal en un objeto | *Derecho de visualización* sobre el nivel de acceso |

| Tarea de nivel de acceso | Derechos necesarios |
|---|---|
| | *Derecho de uso del nivel de acceso para asignación de seguridad* en el nivel de acceso<br>*Derecho de modificación de derechos* en el objeto o derecho de *modificación segura de derechos* en el objeto y en la entidad de seguridad<br>**Nota**<br>Los usuarios que tienen el derecho de *modificación segura de los derechos* y deseen asignar un nivel de acceso a una entidad de seguridad, deben tener asignado el mismo nivel de acceso. |
| Modificar un nivel de acceso | *Derechos de visualización* y *edición* en el nivel de acceso |
| Eliminar un nivel de acceso | *Derechos de visualización* y *eliminación* en el nivel de acceso |
| Clonar un nivel de acceso | *Derecho de visualización* sobre el nivel de acceso<br>*Derecho* de copia en el nivel de acceso<br>*Derecho de adición* en la carpeta de nivel superior de *niveles de acceso* |

## 7.3.1 Elección entre los niveles de acceso *Ver* y *Ver a petición*

Al generar informes en Internet, la elección respecto al uso de datos dinámicos o guardados es una de las decisiones más importantes que tomará. Decida lo que decida, no obstante, la plataforma de BI muestra la primera página lo antes posible, por lo que puede ver el informe mientras se procesan el resto de los datos. En esta sección se explica la diferencia entre los dos niveles de acceso predefinidos que se pueden utilizar para realizar esta elección.

### *Nivel de acceso Ver a petición*

Los informes a petición proporcionan a los usuarios acceso en tiempo real a los datos dinámicos directamente desde el servidor de base de datos. Utilice datos dinámicos para que los usuarios estén actualizados con datos que cambian constantemente, por lo que pueden tener acceso a una información actualizada al segundo. Por ejemplo, si los directores de un centro de distribución grande deben realizar el seguimiento continuo del inventario enviado, los informes dinámicos son la forma de facilitarles la información que necesitan.

Antes de proporcionar datos dinámicos a todos los informes, sin embargo, piense si desea que todos los usuarios envíen solicitudes al servidor de base de datos continuamente. Si los datos no cambian rápida y continuamente, todas estas solicitudes a la base de datos lo único que hacen es incrementar el tráfico de la red y consumir recursos del servidor. En estos casos, quizá prefiera programar informes periódicamente para que los usuarios puedan ver los datos recientes, las copias de los informes, sin recurrir al servidor de base de datos.

Los usuarios requieren acceso de *Ver a petición* para poder actualizar los informes con la base de datos.

### *Nivel de acceso Ver*

Para reducir el tráfico de red y el número de accesos a los servidores de base de datos, puede programar los informes para que se ejecuten a una hora especificada. Cuando se ha ejecutado el informe, los usuarios pueden ver la instancia del informe siempre que lo necesiten, sin tener que realizar más accesos a la base de datos.

Las copias de los informes son útiles para trabajar con datos que no se actualizan constantemente. Cuando los usuarios se desplazan por las copias de los informes y profundizan buscando detalles en columnas o gráficos, no tienen acceso al servidor de base de datos directamente, sino a los datos guardados. En consecuencia, los informes con datos guardados no sólo minimizan la transferencia de datos por la red sino que también aligeran la carga de trabajo del servidor de base de datos.

Por ejemplo, si su base de datos de ventas se actualiza una vez al día, puede ejecutar el informe con una periodicidad similar. Los representantes de ventas siempre tienen acceso a los datos de ventas reales, pero no recurren a la base de datos cada vez que abren un informe.

Los usuarios sólo requieren acceso *Ver* para visualizar las copias de los informes.

## 7.3.2 Para copiar un nivel de acceso existente

Ésta es la mejor forma de crear un nivel de acceso si se desea un nivel de acceso que sea ligeramente distinto de uno de los niveles de acceso existentes.

1. Vaya al área *Niveles de acceso*.
2. En el panel *Detalles* seleccione un nivel de acceso.

   > → Sugerencias
   >
   > Seleccione un nivel de acceso que contenga derechos que sean similares a los que desea para el nivel de acceso.

3. Haga clic en *Organizar* > *Copiar*.
   Una copia del nivel de acceso que ha seleccionado aparece en el panel *Detalles*.

## 7.3.3 Para crear un nivel de acceso

Ésta es la mejor forma de crear un nivel de acceso si se desea un nivel de acceso que sea muy distinto de uno de los niveles de acceso existentes.

1. Vaya al área *Niveles de acceso*.
2. Haga clic en *Administrar* > *Nuevo* > *Crear nivel de acceso*.
   Aparecerá el cuadro de diálogo *Crear nuevo nivel de acceso*.
3. Introduzca un título y una descripción para el nuevo nivel de acceso y, a continuación, haga clic en *Aceptar*.
   Volverá al área *Niveles de acceso* y el nuevo nivel de acceso aparecerá en el panel *Detalles*.

## 7.3.4 Para cambiar el nombre de un nivel de acceso

1. En el área *Niveles de acceso*, en el panel *Detalles*, seleccione el nivel de acceso cuyo nombre desee cambiar.
2. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
3. En el campo *Título*, introduzca un nombre nuevo para el nivel de acceso y, a continuación, haga clic en *Guardar y cerrar*.
   Volverá al área *Niveles de acceso*.

## 7.3.5 Para eliminar un nivel de acceso

1. En el área *Niveles de acceso*, en el panel *Detalles*, seleccione el nivel de acceso que desee eliminar.
2. Haga clic en *Administrar* > *Eliminar nivel de acceso*.

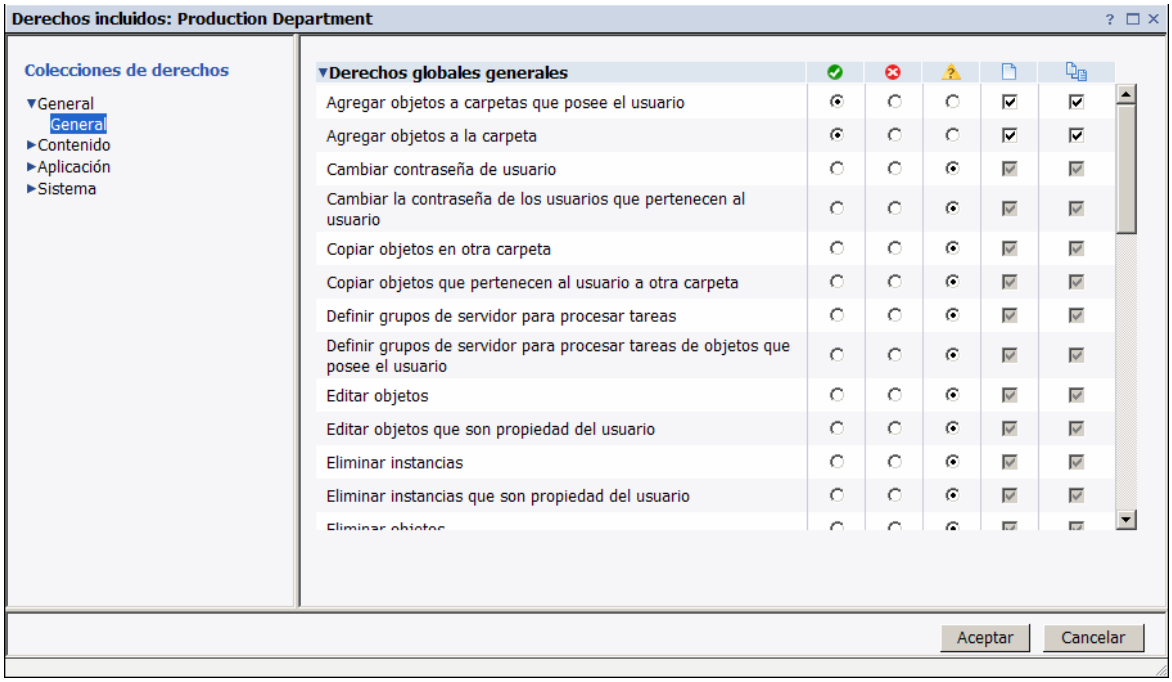
   > **Nota**
   >
   > No puede eliminar los niveles de acceso predefinidos.

   Aparece un cuadro de diálogo con la información acerca de los objetos a los que afecta este nivel de acceso. Si no desea eliminar este nivel de acceso, haga clic en *Cancelar* para salir del cuadro de diálogo.
3. Haga clic en *Eliminar*.
   Se elimina el nivel de acceso y vuelve al área *Niveles de acceso*.

## 7.3.6 Para modificar los derechos en un nivel de acceso

Para establecer los derechos de un nivel de acceso, primero se establecen los derechos globales generales que se aplican a todos los objetos independientemente del tipo y, a continuación, se especifica cuándo se desea reemplazar la configuración general según el tipo de objeto específico.

1. En el área *Niveles de acceso*, en el panel *Detalles*, seleccione el nivel de acceso del que desee modificar los derechos.
2. Haga clic en *Acciones* > *Derechos incluidos*.
   Aparece el cuadro de diálogo *Derechos incluidos* y muestra una lista de derechos efectivos.
3. Haga clic en *Agregar o eliminar derechos*.




El cuadro de diálogo *Derechos incluidos* muestra las colecciones adecuadas al nivel de acceso en la lista de navegación. La sección *Derechos globales generales* está expandida de forma predeterminada.

4. Establezca los derechos globales generales.

   Cada derecho puede tener un estado de *Concedido*, *Denegado* o *No especificado*. También puede elegir si desea aplicar dicho derecho solo al objeto, aplicarlo a los objetos secundarios o a ambos.

5. Para establecer los derechos específicos de tipo para el nivel de acceso, en la lista de navegación, haga clic en la colección de derechos y, a continuación, en la subcolección que se aplica al tipo de objeto para el que desea establecer los derechos.

6. Cuando haya terminado, haga clic en *Aceptar*.
   Volverá a la lista de derechos efectivos.

## 7.3.7 Seguimiento de la relación entre los niveles de acceso y los objetos

Antes de modificar o eliminar un nivel de acceso, es importante confirmar que los cambios que realice en el nivel de acceso no afectarán negativamente a los objetos de la CMC. Puede realizar esta operación ejecutando una consulta de relación en el nivel de acceso.

Las consultas de relación son útiles para la administración de derechos porque permiten ver los objetos afectados por un nivel de acceso en una ubicación cómoda. Considere una situación en la que una compañía reestructura su organización y fusiona dos departamentos, A y B, en el departamento C. El administrador decide eliminar los niveles de acceso de los departamentos A y B porque ya no existen. El administrador ejecuta consultas de relación para ambos niveles de acceso antes de eliminarlos. En el área *Resultados de la consulta*, el administrador puede ver los objetos que se verán afectados si el administrador elimina los niveles de acceso. El panel *Detalles* también muestra al administrador la ubicación de los objetos en la CMC si los derechos en los objetos se deben modificar antes de que se eliminen los niveles de acceso.

> **Nota**
>
> Para ver la lista de los objetos afectados, debe tener derechos de *visualización* en ellos.

> **Nota**
>
> Los resultados de la consulta de relación para un nivel de acceso solo devuelven los objetos en los que el nivel de acceso está asignado explícitamente. Si un objeto usa un nivel de acceso debido a la configuración de herencia, dicho objeto no aparece en los resultados de la consulta.

## 7.3.8 Administración de los niveles de acceso entre sitios

Los niveles de acceso son uno de los objetos que se pueden replicar desde un sitio de origen en los sitios de destino. Puede optar por replicar los niveles de acceso si aparecen en la lista de control de acceso de un objeto de réplica. Por ejemplo, si a una entidad de seguridad se le concede el nivel de acceso A en el informe de Crystal y dicho informe se replica entre sitios, el nivel de acceso A también se replica.

> **Nota**
>
> Si un nivel de acceso con el mismo nombre existe en el sitio de destino, no se realizará la réplica del nivel de acceso. El usuario o el administrador del sitio de destino deben cambiar el nombre de uno de los niveles de acceso antes de la réplica.

Después de replicar un nivel de acceso entre sitios, tenga presentes las consideraciones de administración de esta sección.

### Modificación de niveles de acceso replicados en el sitio de origen

Si un nivel de acceso se modifica en el sitio de origen, el nivel de acceso del sitio de destino se actualizará la próxima vez que la réplica esté programada para ejecutarse. En los escenarios de réplica bidireccional, si modifica un nivel de acceso replicado en el sitio de destino, se cambia el nivel de acceso en el sitio de origen.

> **Nota**
>
> Asegúrese de que los cambios en un nivel de acceso de un sitio no afecten negativamente a los objetos de otros sitios. Consulte a los administradores del sitio y aconséjeles que ejecuten consultas de relaciones del nivel de acceso replicado antes de realizar cambios.

### Modificación de niveles de acceso replicados en el sitio de destino

> **Nota**
>
> Esto sólo se aplica a la réplica unidireccional.

Los cambios en los niveles de acceso replicados que se han efectuado en un sitio de destino no se reflejan en el sitio de origen. Por ejemplo, un administrador del sitio de destino puede conceder el derecho para programar informes de Crystal en el nivel de acceso replicado aunque este derecho se haya denegado en el sitio de origen. Como resultado, aunque los nombres de nivel de acceso y los nombres de objeto replicado permanecen iguales, los derechos efectivos que las entidades de seguridad tienen en los objetos pueden ser distintos en el sitio de destino y en el sitio de origen.

Si el nivel de acceso replicado es distinto entre los sitios de origen y de destino, la diferencia en los derechos efectivos se detectará la próxima vez que esté programada la ejecución de una tarea de réplica. Puede forzar que el nivel de acceso del sitio de origen omita el del sitio de destino o permitir que el nivel de acceso del sitio de destino permanezca intacto. No obstante, si no fuerza que el nivel de acceso del sitio de origen omita el del sitio de destino, los objetos pendientes de réplica que utilicen dicho nivel de acceso no se replicarán.

Para restringir la modificación de los niveles de acceso replicados en el sitio de destino por parte de los usuarios, puede agregar los usuarios del sitio de destino al nivel de acceso como entidades de seguridad y concederles sólo derechos de *visualización*. Esto significa que los usuarios del sitio de destino pueden ver el nivel de acceso pero no pueden modificar su configuración de derechos ni asignarlo a otros usuarios.

### Información relacionada

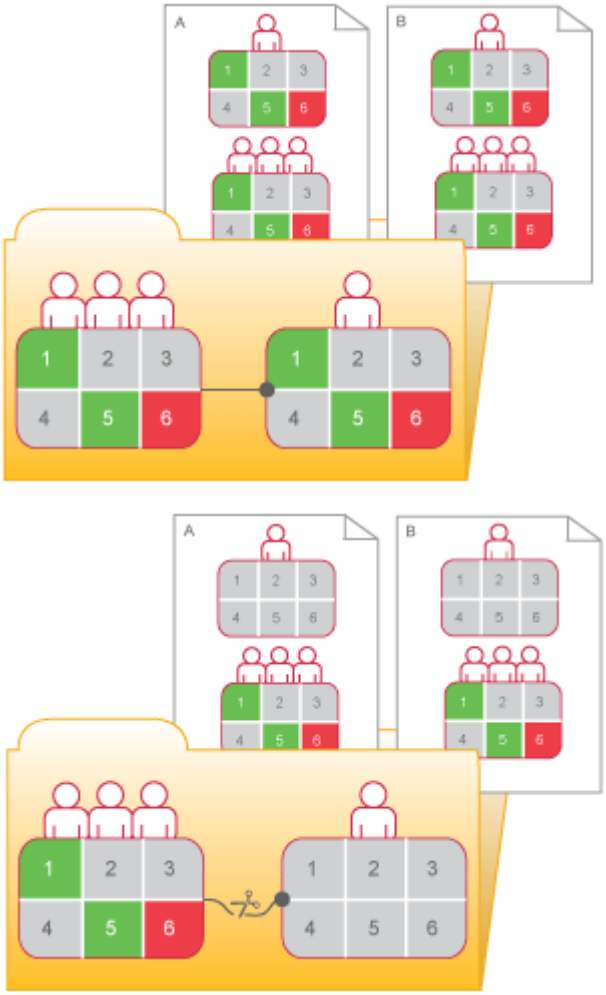
Federación [página 968]
Seguimiento de la relación entre los niveles de acceso y los objetos [página 146]

## 7.4 Interrupción de la herencia

La herencia permite administrar la configuración de seguridad sin establecer derechos para cada objeto individual. No obstante, en algunos casos, puede que no desee que se hereden los derechos. Por ejemplo, puede personalizar los derechos para cada objeto. Puede deshabilitar la herencia para un principal en una lista de control de acceso de un objeto. Al hacerlo, puede optar por deshabilitar la herencia de grupo, la herencia de carpeta o ambas.

> **Nota**
>
> Si se interrumpe la herencia, ocurre para todos los derechos; no es posible desactivar la herencia para unos derechos sí y para otros no.

En el diagrama «Interrupción de la herencia», la herencia de grupo y carpeta está efectiva inicialmente. El Usuario rojo hereda los derechos 1 y 5 como concedidos, los derechos 2, 3 y 4 como sin especificar, y el derecho 6 como denegado explícitamente. Estos derechos, establecidos en el nivel de carpeta para el grupo, significan que el usuario rojo, y todos los miembros del grupo, tienen estos derechos de los objetos de la carpeta, A y B. Si se interrumpe la herencia en el nivel de carpeta, el conjunto de derechos del usuario rojo respecto a los objetos de dicha carpeta se anulan hasta que un administrador le asigne nuevos derechos.




Interrupción de la herencia

## 7.4.1 Para desactivar la herencia

Este procedimiento permite desactivar la herencia de grupo o carpeta, o ambas, para una entidad de seguridad en una lista de control de acceso.

1. Seleccione el objeto para el que desee desactivar la seguridad.
2. Haga clic en *Administrar* > *Seguridad de usuario*.
   Aparecerá el cuadro de diálogo *Seguridad de usuario*.
3. Seleccione la entidad de seguridad para la que desee desactivar la herencia y haga clic en *Asignar seguridad*.
   Aparecerá el cuadro de diálogo *Asignar seguridad*.
4. Configure las opciones de herencia.
   - Si desea desactivar la herencia de grupo (los derechos que la entidad de seguridad hereda de la pertenencia al grupo), desactive la casilla de verificación *Heredar de grupo principal*.
   - Si desea desactivar la herencia de carpeta (los derechos que el objeto hereda de la carpeta), desactive la casilla de verificación *Heredar de carpeta principal*.

5. Haga clic en *Aceptar*.

## 7.5 Uso de derechos para la administración delegada

Además de permitir el control de los accesos a objetos y parámetros, puede utilizar los derechos para dividir tareas administrativas entre grupos funcionales de la organización. Por ejemplo, puede que desee que las personas de los distintos departamentos administren sus propios usuarios y grupos. O puede que tenga un administrador que gestione la administración de alto nivel de la plataforma de BI, pero desea que la administración de todos los servidores la lleven a cabo personas del departamento de TI.

Suponiendo que la estructura de grupos y de carpetas se alinea con la estructura de seguridad de la administración delegada, deberá conceder al administrador delegado derechos sobre todos los grupos de usuarios, pero deberá concederle derechos inferiores a los derechos completos sobre los usuarios que va a controlar. Por ejemplo, puede que no desee que el administrador delegado edite atributos de usuario o los reasigne a grupos diferentes.

> **Nota**
>
> Las migraciones de objetos las realizan mejor los miembros del grupo Administradores; concretamente, la cuenta de usuario Administrador. Para migrar un objeto, es posible que también deban migrarse muchos objetos relacionados. Es posible que no pueda obtener para una cuenta de administrador delegado los derechos de seguridad necesarios para todos los objetos.

La tabla «Derechos de administradores delegados» resume los derechos necesarios para que los administradores delegados realicen acciones comunes.

Derechos de administradores delegados

| Acción del administrador delegado | Derechos que necesita el administrador delegado |
|---|---|
| Crear nuevos usuarios | *Derecho Agregar* en la carpeta *Usuarios* de nivel superior |
| Crear nuevos grupos | *Derecho Agregar* en la carpeta *Grupos de usuarios* de nivel superior |
| Eliminar cualquier grupo controlado, así como usuarios individuales de dichos grupos | *Derecho Eliminar* en los grupos relevantes |
| Eliminar sólo los usuarios que crea el administrador delegado | *Derecho Eliminar propietario* en la carpeta *Usuarios* de nivel superior |
| Eliminar sólo los usuarios y grupos que crea el administrador delegado | *Derecho Eliminar propietario* en la carpeta *Grupos de usuarios* de nivel superior |
| Manipular sólo los usuarios que crea el administrador delegado (incluido agregar dichos usuarios a dichos grupos) | *Derecho Editar propietario* y *Modificar derechos de usuario de forma segura* en la carpeta *Usuarios* de nivel superior |
| Manipular sólo los grupos que crea el administrador delegado (incluido agregar usuarios a dichos grupos) | *Editar propietario* y *Modificar derechos de usuario de forma segura* en la carpeta *Grupos de usuarios* de nivel superior |

| Acción del administrador delegado | Derechos que necesita el administrador delegado |
|---|---|
| Modificar contraseñas de usuarios en sus grupos controlados | *Derecho Editar contraseña* en los grupos relevantes |
| Modificar contraseñas sólo de los principales que crea el administrador delegado | *Derecho Editar contraseña de propietario* en la carpeta *Usuarios* de nivel superior o en los grupos relevantes<br>**Nota**<br>Establecer el derecho *Editar contraseña de propietario* en un grupo sólo tiene efecto en un usuario cuando se agrega el usuario al grupo relevante. |
| Modificar nombres de usuario, descripción, otros atributos y reasignar usuarios a grupos diferentes | *Derecho Editar* en los grupos relevantes |
| Modificar nombres de usuario, descripción, otros atributos y reasignar usuarios a grupos diferentes, pero sólo para los usuarios que crea el administrador | *Derecho Editar propietario* en la carpeta *Usuarios* de nivel superior o en los grupos relevantes<br>**Nota**<br>Establecer el derecho *Editar propietario* en los grupos relevantes sólo tiene efecto en un usuario cuando se agrega el usuario al grupo relevante. |

## 7.5.1 Elegir entre las opciones «*Modificar los derechos de los usuarios para los objetos*»

Al configurar la administración delegada, conceda al administrador delegado los derechos sobre los principales que va a controlar. Puede concederle todos los derechos (*Control total*); no obstante, resulta adecuado usar la configuración de derechos avanzados para denegar el derecho *Modificar derechos* y otorgar al administrador delegado el derecho *Modificar derechos de forma segura* en su lugar. También puede conceder a su administrador el derecho *Modificar de forma segura la configuración de la herencia de derechos* en vez del derecho *Modificar la configuración de la herencia de derechos*. Las diferencias entre estos derechos se resumen a continuación.

### *Modificar los derechos de los usuarios para los objetos*

Este derecho permite que un usuario modifique cualquier derecho de cualquier usuario en dicho objeto. Por ejemplo, si el usuario A tiene los derechos *Ver objetos* y *Modificar los derechos de los usuarios para los objetos* en un objeto, el usuario A puede cambiar los derechos de dicho objeto para que éste o cualquier otro usuario tenga el control total de este objeto.

## *Modificar de forma segura los derechos que tienen los usuarios sobre los objetos que son propiedad del usuario*

Este derecho permite a un usuario conceder, denegar o revertir a no especificado solo los derechos que ya tiene concedidos. Por ejemplo, si el usuario A tiene los derechos *Ver* y *Modificar de forma segura los derechos que tienen los usuarios sobre los objetos*, el usuario A no se puede conceder más derechos y puede conceder o denegar a los demás usuarios solo estos dos derechos (*Ver* y *Modificar de forma segura los derechos*). Además, el usuario A solo puede cambiar los derechos de los usuarios sobre objetos para los que tenga el derecho *Modificar de forma segura los derechos*.

Éstas son todas las condiciones que deben existir bajo las cuales el usuario A puede modificar los derechos del usuario B sobre el objeto O:

- El usuario A tiene el derecho *Modificar de forma segura los derechos* sobre el objeto O.
- Cada derecho o nivel de acceso que el usuario A cambia para el usuario B, se concede a A.
- El usuario A tiene el derecho *Modificar de forma segura los derechos* sobre el usuario B.
- Si se está asignado un nivel de acceso, el usuario A tiene el derecho *Asignar nivel de acceso* sobre el nivel de acceso que está cambiando para el usuario B.

El alcance de los derechos puede limitar más los derechos efectivos que puede asignar un administrador delegado. Por ejemplo, un administrador delegado puede tener los derechos *Modificar de forma segura los derechos* y *Editar* en una carpeta, pero el alcance de estos derechos está limitado a la carpeta únicamente y no se aplica a sus objetos secundarios. De forma efectiva, el administrador delegado puede conceder el derecho *Editar* en la carpeta (pero no en sus objetos secundarios) únicamente y solo con un ámbito «Aplicar a objetos». Por otro lado, si al administrador delegado se le concede el derecho *Editar* en una carpeta con un ámbito «Aplicar a objetos secundarios» únicamente, puede conceder a otros principales el derecho *Editar* con ambos ámbitos sobre los objetos secundarios de la carpeta, pero en la propia carpeta solo puede conceder el derecho *Editar* con un ámbito «Aplicar a objetos secundarios».

Además, el administrador delegado tendrá restricciones para modificar derechos en los grupos de otros principales para los que no tiene el derecho *Modificar de forma segura los derechos*. Esto resulta útil, por ejemplo, si tiene dos administradores delegados responsables de conceder derechos a diferentes grupos de usuarios para la misma carpeta, pero no desea que un administrador delegado puede denegar el acceso a los grupos controlados por el otro administrador delegado. El derecho *Modificar de forma segura los derechos* garantiza esto, ya que los administradores delegados generalmente no tienen el derecho *Modificar de forma segura los derechos* recíprocamente.

## *Modificar de forma segura la configuración de la herencia de derechos*

Este derecho permite a un administrador delegado modificar la configuración de herencia para otras entidades de seguridad sobre los objetos a los que el administrador delegado tiene acceso. Para modificar correctamente la configuración de herencia de otras entidades de seguridad, un administrador delegado debe tener este derecho sobre el objeto y sobre las cuentas de usuario para las entidades de seguridad.

### 7.5.2 Derechos de propietario

Los derechos de propietario se aplican sólo al propietario del objeto en el que se comprueban los derechos. En la plataforma de BI, el propietario de un objeto es el principal que lo ha creado; si dicho principal se elimina del sistema, la propiedad revierte al administrador.

Los derechos de propietario resultan útiles en la administración de la seguridad basada en propietario. Por ejemplo, podría crear una carpeta o jerarquía de carpetas en la que varios usuarios puedan crear y ver documentos, pero sólo puedan modificar o eliminar sus propios documentos. Además, los derechos de propietario son adecuados para permitir a los usuarios manipular las instancias de los informes que crean, pero no las instancias de otros. En el caso del nivel de acceso de programación, esto permite a los usuarios editar, eliminar, detener y reprogramar sólo sus propias instancias.

Los derechos de propietario funcionan de forma similar a sus derechos normales correspondientes. No obstante, los derechos de propietario sólo son efectivos cuando a la entidad de seguridad se le han concedido derechos de propietario pero los derechos normales se le han denegado o no se han especificado.

## 7.6 Resumen de recomendaciones para la administración de derechos

Tenga en cuenta estas consideraciones para la administración de derechos:

- Siempre que sea posible utilice niveles de acceso. Estos conjuntos de derechos predefinidos simplifican la administración agrupando los derechos asociados con las necesidades comunes del usuario.
- Establezca los derechos y los niveles de acceso en las carpetas de nivel superior. Activar la herencia permitirá que estos derechos se transmitan por el sistema con una intervención administrativa mínima.
- Evite la interrupción de herencia siempre que sea posible. De esta forma, puede reducir el tiempo que tarda en proteger el contenido que ha agregado a la plataforma de BI.
- Establezca los derechos adecuados para usuarios y grupos en el nivel de carpeta y, a continuación, publique los objetos en dicha carpeta. De manera predeterminada, los usuarios o grupos que tienen derechos sobre una carpeta heredan los mismos derechos para cualquier objeto que se publique posteriormente en esa carpeta.
- Organice los usuarios en grupos de usuarios, asigne niveles y derechos de acceso a todo el grupo, y asigne niveles y derechos de acceso a miembros específicos cuando sea necesario.
- Cree cuentas de administrador individuales para cada administrador del sistema y agréguelas al grupo Administradores para mejorar la capacidad de administración de los cambios del sistema.
- De forma predeterminada, al grupo Todos se le conceden derechos muy limitados a las carpetas de nivel superior en la plataforma de BI. Tras la instalación se recomienda revisar los derechos de los miembros del grupo Todos y asignar la seguridad en consecuencia.

# 8 Protección de la plataforma de BI

## 8.1 Información general de seguridad

En esta sección se explican detalladamente las formas en que la plataforma de BI satisface los requisitos de seguridad de las empresas, con lo que proporciona a los administradores y arquitectos del sistema soluciones a los problemas cotidianos de seguridad.

La arquitectura de la Plataforma de BI satisface los muchos requisitos de seguridad de las empresas y organizaciones de hoy en día. La última versión es compatible con funciones como la seguridad distribuida, el inicio de sesión único, la seguridad de acceso a los recursos, los derechos granulares sobre objetos y la autenticación de terceros con el fin de proteger de accesos no autorizados.

Ya que la plataforma de BI proporciona el marco para un número cada vez mayor de componentes de la familia Enterprise de los productos SAP BusinessObjects , en esta sección se describen con detalle las funciones de seguridad y la funcionalidad adicional relacionada que muestran cómo el propio marco impone y mantiene la seguridad. No obstante, en esta sección no se incluyen todos los detalles de los procesos, sólo conceptos y vínculos a los procedimientos más importantes.

Después de una breve introducción a los conceptos de seguridad para el sistema, los detalles se muestran en los siguientes temas:

- Cómo usar los modos de seguridad de cifrado y procesamiento de datos para proteger los datos.
- Cómo configurar el Nivel se sockets seguros para los despliegues de la Plataforma de BI.
- Directrices para configurar y actualizar los servidores de seguridad para la plataforma de BI.
- Configurar servidores proxy inversos

## 8.2 Uso seguro de objetos de programa

Si un usuario tiene derechos de programación para objetos de programa, tiene derecho a ejecutarlo.

En el caso de los programas Java, los usuarios pueden:

- Especificar la clase principal. El autor del programa debe asegurarse de que no quede ninguna clase principal secundaria/de test en el programa involuntariamente.
- Especificar la ruta de clase. No deberían tener derecho a cargar `jar` en el sistema. Podría utilizarse para ejecutar código de diseño especial.

### Recomendaciones generales para proteger objetos de programa

- No proporcione al usuario información de credenciales de inicio de sesión en el servidor.

- Otorgue derechos mínimos a la cuenta de usuario que ejecuta el programa en el servidor. Prohíba expresamente el acceso a la ruta de instalación de la plataforma SAP BusinessObjects Business Intelligence.
- Se recomienda seleccionar la opción *Fallar tarea* en *Aplicaciones* > *Consola de administración central* > *Derechos de objetos de programa*.
- Se recomienda utilizar carpetas para el control de acceso. Los objetos de programa con diferentes niveles de seguridad deben colocarse en carpetas distintas.

## 8.3 Planificación de recuperación tras desastres

Se deben realizar determinados pasos para proteger la inversión de la organización en la plataforma de BI para garantizar la continuidad máxima de las líneas de funciones de empresas en el caso de un desastre. En esta sección se proporcionan las directrices para diseñar un plan de recuperación tras desastres para la organización. También puede verificar esta nota SAP para obtener más información.

### Instrucciones generales

- Realice con regularidad copias de seguridad del sistema y envíe fuera copias de algunos de los medios de copia de seguridad, en caso necesario.
- Almacene de forma segura todos los medios del software.
- Almacene de forma segura toda la documentación de las licencias.

### Instrucciones específicas

Estos son tres recursos del sistema que requieren atención especial en términos de planificación de recuperación tras desastres:

- Contenido en los servidores del repositorio de archivos: Incluye contenido de propietario como los informes. Debe realizar la copia de seguridad regular de este contenido: en el caso de desastre no existe ningún modo de regenerar este contenido sin un proceso de copia de seguridad regular.
- La base de datos del sistema utilizada por CMS: Este recurso contiene todos los metadatos importantes para el despliegue, como la información de usuario, informes y otra información importante concreta de la organización.
- Archivo de clave de información de base de datos (.dbinfo de archivo): Este recurso contiene la clave maestra de la base de datos del sistema. Si por algún motivo esta clave no está disponible, no podrá acceder a la base de datos del sistema. Después de desplegar la plataforma de BI, se recomienda encarecidamente almacenar la contraseña para este recurso en una ubicación segura y conocida. Sin la contraseña no podrá regenerar el archivo y, por lo tanto, perderá el acceso a la base de datos del sistema.

## 8.4 Recomendaciones generales para proteger el despliegue

A continuación, se presentan las directrices recomendadas para proteger los despliegues de la Plataforma de BI.

- Use servidores de seguridad para proteger la comunicación entre el CMS y otros componentes del sistema. Si es posible, oculte siempre el CMS detrás de un servidor de seguridad. Para finalizar, asegúrese que la base de datos del sistema está protegida detrás de un servidor de seguridad.
- Agregue un cifrado adicional a los servidores del repositorio de archivos. Cuando el sistema esté configurado y en ejecución, el contenido registrado se almacenara en estos servidores. Agregue un cifrado adicional a través del SO o use una herramienta de terceros.
- Despliegue un servidor proxy inverso delante de los servidores de aplicaciones Web para poder ocultarlos detrás de una única dirección IP. Esta configuración enruta todo el tráfico de Internet dirigido a servidores de aplicaciones Web privados a través del servidor proxy inverso, por lo tanto se ocultan las direcciones IP privadas.
- Refuerce severamente las políticas de contraseñas corporativas. Asegúrese de que las contraseñas de usuario se cambian de forma rutinaria.
- Si ha optado por instalar la base de datos del sistema y el servidor de aplicaciones Web que se incluyen con la plataforma de BI, deberá acceder a la documentación importante para garantizar que los componentes se despliegan con la configuración de seguridad adecuada.
- Use el protocolo Nivel de socket seguro (SSL) para todas las comunicaciones de red entre los clientes y los servidores del despliegue.
- Asegúrese de que el directorio de instalación de la plataforma y los subdirectorios son seguros. Los datos temporales sensibles se almacenarán en estos directorios durante la operación del sistema.
- El acceso a la Consola de administración central (CMC) debería estar restringido a solo acceso local. Para obtener información sobre las opciones del despliegue de la CMC, consulte el *Manual del despliegue de aplicaciones web de la plataforma SAP BusinessObjects Business Intelligence*.
- Por defecto, los mensajes de error Web Intelligence incluyen información del esquema de la base de datos. Para mostrar mensajes de error sin información de esquema de base de datos ejcecute lo pasos siguientes:
  1. Abra el archivo de configuración `WebIContainer_ServerDescriptor.xml` para editar. De manera predeterminada se encuentra en `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64config`.
  2. Modifique el valor de este parámero a False: `WebiParamDetailedDbErrorsEnabled = False`.

> ⚠ Precaución
>
> Los marcadores de posición que no sean los previstos para la edición no deben cambiarse de ninguna manera. El administrador del sistema debe asegurarse de que solo la persona adecuada del grupo de administradores (que está prevista para la gestión de nodos) tenga los derechos de edición en el nodo. Todos los demás usuarios, incluidos los demás miembros del grupo de administradores, deben estar restringidos para ver/administrar los objetos Nodo aplicando los derechos de seguridad adecuados. En caso de que alguno de los valores de marcador de posición esté dañado accidentalmente y no aparezca CMS, consulte la siguiente nota SAP.

> **Nota**
>
> Consulte el siguiente artículo de la base de conocimientos de SAP 3278916 para saber cómo restringir los marcadores de posición que se modifican para evitar posibles interferencias con fines maliciosos con la infraestructura de BI.

### Información relacionada

Configurar el protocolo SSL [página 189]
Restricciones para las contraseñas [página 163]
Configuración de la seguridad para servidores de terceros en paquetes [página 157]

## 8.5 Configuración de la seguridad para servidores de terceros en paquetes

Si ha optado por instalar componentes externos en paquete con la plataforma de BI, se recomienda verificar las secciones de seguridad de la documentación oficial de SAP SQL Anywhere y Apache Tomcat .

## 8.6 Relación de confianza activa

En un entorno de red, una relación de confianza entre dos dominios suele ser una conexión que permite que un domino reconozca con precisión a los usuarios que han sido autenticados por el otro dominio. Además de mantener la seguridad, la relación de confianza permite que los usuarios obtengan acceso a recursos en varios dominios sin necesidad de proporcionar repetidamente sus credenciales.

En el entorno de la Plataforma de BI, la relación de confianza activa funciona de forma parecida para proporcionar a cada usuario un acceso uniforme a los recursos de todo el sistema. Una vez que el usuario se ha autenticado y se le ha otorgado una sesión activa, el resto de los componentes de la Plataforma de BI pueden procesar las solicitudes y acciones del usuario sin pedirle sus credenciales. Como tal, la relación de confianza activa proporciona una base para la seguridad distribuida de la plataforma de BI.

### 8.6.1 Tokens de inicio de sesión

Un token de inicio de sesión es una cadena codificada que define sus propios atributos de uso y contiene la información de la sesión de un usuario. Los atributos de uso del token de inicio de sesión se especifican cuando se genera este símbolo. Estos atributos permiten establecer restricciones en el token de inicio de sesión para reducir la posibilidad de que usuarios malintencionados lo usen. Los atributos de uso actuales del token de inicio de sesión son:

- *Número de minutos*
  Este atributo reduce la vida útil del token de inicio de sesión.
- *Número de inicios de sesión*
  Este atributo restringe el número de veces que se puede usar el token de inicio de sesión en la plataforma de BI.

Ambos atributos dificultan a los usuarios malintencionados el acceso no autorizado a la plataforma de BI con tokens de inicio de sesión que se obtienen de usuarios legítimos.

> **Nota**
>
> Almacenar el token de inicio de sesión en una cookie es un riesgo de seguridad potencial si la red que se encuentra entre el explorador y el servidor de aplicaciones Web no es segura; por ejemplo si el inicio de sesión se realiza en una red pública y no usa SSL ni Autenticación de confianza. Es una buena idea usar Secure Sockets Layer (SSL) para reducir los riesgos de seguridad entre el explorador y el servidor de aplicaciones Web o servidor Web.

Cuando se ha desactivado la cookie de inicio de sesión y se agota el tiempo de espera del servidor Web o del explorador Web, al usuario se le presenta la pantalla de inicio de sesión. Cuando la cookie está activada y se agota el tiempo de espera del servidor o del explorador, el usuario se vuelve a iniciar sesión en el sistema de forma transparente. Sin embargo, puesto que la información de estado está vinculada a la sesión Web, se pierde el estado del usuario. Por ejemplo, si el usuario tenía un árbol de navegación expandido y había seleccionado un elemento en particular, el árbol se restablece.

Para la plataforma de BI, la opción predeterminada es activar los tokens de inicio de sesión en el cliente Web; no obstante, puede desactivar los tokens de inicio de sesión para la plataforma de lanzamiento de BI. Si deshabilita los tokens de inicio de sesión en el cliente, la sesión de usuario estará limitada por el tiempo de espera del explorador Web o del servidor Web. Cuando caduque dicha sesión, se solicitará al usuario que inicie sesión de nuevo en la plataforma de BI.

## 8.6.2 Mecanismo de vales para seguridad distribuida

Los sistemas Enterprise dedicados a servir a un gran número de usuarios suelen requerir alguna forma de seguridad distribuida. Un sistema Enterprise puede requerir seguridad distribuida para admitir funciones como la transferencia de confianza (la capacidad de permitir que otro componente actúe en nombre del usuario).

La plataforma de BI lleva a cabo la seguridad distribuida mediante la implementación de un mecanismo de vales (parecido al mecanismo de vales Kerberos). El CMS otorga vales que autorizan a los componentes a realizar acciones en nombre de un determinado usuario. En la plataforma de BI, el vale se denomina token de inicio de sesión.

Este token de inicio de sesión se usa normalmente en la Web. Cuando la plataforma de BI autentica a los usuarios por primera vez, reciben tokens de inicio de sesión del CMS. El explorador Web del usuario almacena en caché este token de inicio de sesión. Cuando el usuario realiza una solicitud nueva, otros componentes de la Plataforma de BI pueden leer el token de inicio de sesión en el explorador Web del usuario.

## 8.7 Sesiones y seguimiento de sesiones

En general, una sesión es una conexión de un cliente y un servidor que permite el intercambio de información entre dos equipos. El estado de una sesión es un conjunto de datos que describe los atributos de la sesión, su configuración o su contenido. Cuando establece una conexión cliente-servidor a través de Internet, la naturaleza de HTTP limita la duración de cada sesión a una sola página de información; por lo tanto, el explorador Web sólo mantiene el estado de cada sesión en memoria mientras se muestra una página Web. En cuanto pasa de una página Web a otra, el estado de la primera sesión se desecha y se sustituye por el estado de la siguiente sesión. Como consecuencia, los sitios Web y las aplicaciones Web tienen que almacenar de alguna forma el estado de una sesión si necesitan volver a utilizar su información en otra.

La plataforma de BI usa dos métodos comunes para almacenar el estado de las sesiones:

- Cookies: una cookie es un pequeño archivo de texto que almacena el estado de las sesiones en el cliente: el explorador Web del usuario almacena en caché la cookie para su uso posterior. El token de inicio de sesión de la Plataforma de BI es un ejemplo de este método.
- Variables de sesión: una variable de sesión es una porción de memoria que almacena el estado de las sesiones en el servidor. Cuando la plataforma de BI otorga a un usuario una identidad activa en el sistema, la información, como el tipo de autenticación del usuario, se almacena en una variable de sesión. Mientras se mantenga la sesión, el sistema no necesita pedir al usuario la información una segunda vez, ni tiene que repetir ninguna tarea necesaria para llevar a cabo la solicitud siguiente.
  Para los despliegues Java, la sesión se usa para gestionar solicitudes .jsp; para los despliegues .NET, la sesión se usa para gestionar solicitudes .aspx.

> ⓘ Nota
>
> Lo ideal sería que el sistema conservase la variable de sesión mientras el usuario trabaja en el sistema. Y, para garantizar la seguridad y reducir el uso de recursos, el sistema debería destruir la variable de sesión en cuanto el usuario termina de trabajar en el sistema. Sin embargo, debido a que la interacción entre un explorador Web y un servidor Web puede ser independiente, puede resultar difícil saber cuándo los usuarios han dejado el sistema, si no se desconectan explícitamente. Para solucionar este problema, la plataforma de BI realiza un seguimiento de las sesiones.

### 8.7.1 Seguimiento de sesiones CMS

El CMS implementa un sencillo algoritmo de seguimiento. Cuando un usuario inicia una sesión, se le concede una sesión del CMS, que el CMS conserva hasta que el usuario cierra la sesión, o hasta que se libera la variable de sesión del servidor de aplicaciones Web.

La sesión del servidor de aplicaciones Web está diseñada para notificar al CMS periódicamente que todavía está activa, de manera que se retenga la sesión del CMS mientras exista la sesión del servidor de aplicaciones Web. Si la sesión del servidor de aplicaciones Web no puede comunicarse con el CMS durante un periodo de diez minutos, el CMS destruye la sesión del CMS. Esto controla situaciones en las que los componentes del cliente se cierran de forma irregular.

## 8.7.2 Administración de sesiones

Puede ver y finalizar sesiones en la CMC.

Puede visualizar y finalizar sesiones de usuario en la Consola de administración central (CMC). Por ejemplo, puede querer ver qué usuarios están utilizando sesiones múltiples. O puede querer finalizar sesiones que utilicen demasiado recursos de sistema o que sean muy antiguas. También puede que tenga que finalizar sesiones al preparar para una parada del sistema o actualizaciones.

### 8.7.2.1 Para ver la lista de sesiones

Visualizar sesiones en la CMC.

Puede visualizar una lista de sesiones en la Consola de administración central.

1. Inicie sesión en la CMC como administrador.
2. Desde el área *Administrar*, haga clic en *Sesiones*.

Se visualiza la lista de sesiones de usuario para el clúster. Puede hacer clic sobre los encabezados de columna para clasificar la lista por nombre de usuario, por el número de sesiones abiertas o por las horas de inicio de sesión. También puede hacer clic sobre el nombre de usuario o recuento de sesión o la hora de inicio de sesión para visualizar los detalles de las sesiones de ese usuario en el panel inferior.

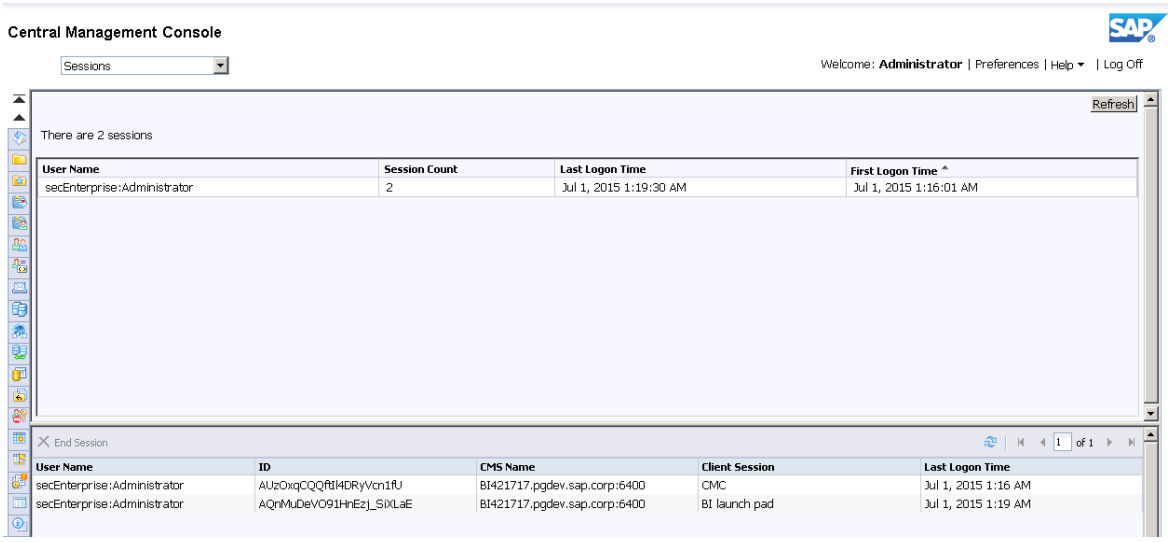
### 8.7.2.2 Para cerrar sesiones

Cerrar sesiones en la CMC.

Puede cerrar sesiones individuales o múltiples.

1. Inicie sesión en la CMC como administrador.
2. Desde el área *Administrar*, haga clic en *Sesiones*.

   Se visualiza la lista de sesiones de usuario para el clúster.



3. Haga clic sobre un nombre de usuario, recuento de sesión u hora de inicio de sesión, para visualizar las sesiones de un usuario en el panel inferior.
4. Haga clic para seleccionar una sola sesión o `CTRL` + `clic` para seleccionar varias sesiones.
5. Haga clic en *Finalizar sesión*.

> **Nota**
>
> La sesión de usuario se libera cuando el usuario cierra el navegador.

> **Nota**
>
> Para cerrar sesiones, debe tener el derecho «Editar objetos» sobre el objeto CMS.

> **Nota**
>
> No puede cerrar la sesión de administrador actual.

## 8.7.3 Script para borrar sesiones obsoletas

### Script

Se introduce un script para borrar las sesiones obsoletas y liberar las licencias no utilizadas para que estén disponibles para los usuarios que esperan iniciar sesión. Este script continúa ejecutándose hasta que se cierra manualmente y comprueba si hay sesiones obsoletas y las finaliza en cada intervalo de 10 minutos.

- Para Windows, puede encontrar un script aquí: `<BI_Install_Dir>\SAP BusinessObjects Enterprise XI 4.0\java\lib\StaleSessionCleaner.jar`
- Para Unix, puede encontrar un script aquí: `<BI_Install_Dir>/sap_bobj/enterprise_xi40/java/lib/StaleSessionCleaner.jar`

La sintaxis utilizada para el script es

> **Sintaxis de código**
>
> ```
> java -jar StaleSessionCleaner.jar <username> <password>
> <machine:port><authentication> <logdir>
> ```

## 8.8 Protección de entornos

La protección de entornos se refiere a la seguridad de todo el entorno en el que el cliente y el servidor se comunican. Aunque Internet y los sistemas Web son cada vez más populares debido a su flexibilidad y a su amplia funcionalidad, funcionan en un entorno que es muy difícil de proteger. Al implementar la plataforma de BI, la protección del entorno se divide en dos áreas de comunicación: explorador Web a servidor Web y servidor Web a plataforma de BI.

## 8.8.1 De explorador Web a servidor Web

Cuando se transmiten datos de un explorador Web a un servidor Web, suele ser necesario cierto grado de protección. Las medidas de seguridad apropiadas suelen implicar dos tareas:

- Asegurar que la comunicación de los datos es segura.
- Asegurar que sólo los usuarios válidos obtienen la información del servidor Web.

> ⓘ Nota
>
> Estas tareas suelen realizarlas los servidores Web mediante una serie de mecanismos de seguridad, entre los que se incluye el protocolo Nivel de socket seguro (SSL) y otros mecanismos del mismo tipo. Es una buena idea usar SSL para reducir los riesgos de seguridad entre el explorador y el servidor de aplicaciones Web o servidor Web.

Debe proteger la comunicación entre el explorador Web y el servidor Web independientemente de la plataforma de BI. Para obtener información detallada acerca de la protección de conexiones a clientes, consulte la documentación de su servidor Web.

## 8.8.2 Servidor Web en la Plataforma de BI

Los servidores de seguridad se usan con frecuencia para proteger el área de comunicación entre el servidor Web y el resto de la Intranet corporativa (incluida la plataforma de BI). La plataforma admite servidores de seguridad que usan el filtrado de IP o la traducción de dirección de red estática (NAT). Los entornos compatibles pueden tener varios servidores de seguridad, servidores Web y servidores de aplicaciones.

## 8.8.3 Protección frente a intentos de conexión malintencionados

No importa lo seguro que sea un sistema, suele haber al menos un punto en el que es vulnerable: la ubicación donde los usuarios se conectan al sistema. Es prácticamente imposible proteger este punto completamente, debido a que el proceso de adivinar simplemente un nombre de usuario y una contraseña válidos sigue siendo una forma factible de intentar entrar sin permiso en el sistema.

La plataforma de BI implementa varias técnicas para reducir la probabilidad de que un usuario malintencionado acceda al sistema. Las distintas restricciones enumeradas a continuación solo se aplican a las cuentas Enterprise; es decir, las restricciones no se aplican a cuentas asignadas a una base de datos de usuarios externa (LDAP o Windows AD). No obstante, en general, el sistema externo le permitirá asignar restricciones similares a las cuentas externas.

## 8.8.4 Restricciones para las contraseñas

Las restricciones de contraseña garantizan que los usuarios que se autentican en la autenticación de Enterprise predeterminada crean contraseñas que son relativamente complejas. Puede habilitar las siguientes opciones:

1. Exigir contraseñas con minúsculas y mayúsculas
   Esta opción garantiza que las contraseñas contienen como mínimo una mayúscula y una minúscula. Esta opción se verifica de forma predeterminada, a no ser que haya sido modificada por el administrador.
2. Exigir numeral(es) en contraseñas
   Esta opción asegura que las contraseñas contienen como mínimo un carácter numérico.
3. Incluir contraseñas con caracteres especiales
   Esta opción asegura que las contraseñas contienen como mínimo un carácter especial.

Al imponer una complejidad mínima para las contraseñas, reduce las probabilidades de que un usuario malintencionado pueda simplemente adivinar una contraseña válida de usuario.

## 8.8.5 Restricciones de conexión

Las restricciones de conexión sirven principalmente para impedir ataques de diccionarios (un método por el que un usuario malintencionado obtiene un nombre válido de usuario e intenta averiguar la correspondiente contraseña probando todas las palabras de un diccionario). Con la velocidad del hardware moderno, los programas malintencionados pueden adivinar millones de palabras por minuto. Para impedir ataques de diccionarios, la plataforma de BI tiene un mecanismo interno que fuerza un retraso (entre 0,5 y 1 segundo) entre intentos de inicio de sesión. Además, la plataforma proporciona varias opciones personalizables que puede usar para reducir el riesgo de un ataque de diccionario:

- Deshabilitar la cuenta tras N intentos de conexión
- Restablecer el recuento de conexiones con errores cada N minutos
- Rehabilitar la cuenta después de un determinado número de minutos.

## 8.8.6 Restricciones para los usuarios

Las restricciones de usuario garantizan que los usuarios que se autentican en la autenticación de Enterprise predeterminada crean nuevas contraseñas de forma regular. Puede habilitar las siguientes opciones:

- Debe cambiar la contraseña cada N días.
- No puede volver a usar las últimas N contraseñas
- Debe esperar N minutos para cambiar la contraseña

Estas opciones son útiles para varias cosas. En primer lugar, cualquier usuario malintencionado que intente un ataque de diccionario tendrá que volver a empezar cada vez que cambien las contraseñas. Y, puesto que los cambios de la contraseña están basados en la primera vez que inicia sesión cada usuario, el usuario malintencionado no puede determinar con facilidad cuándo una determinada contraseña va a cambiar. Asimismo, incluso si un usuario malicioso consigue adivinar las credenciales de otro usuario, o las obtiene por cualquier otro medio, sólo son válidas durante un tiempo limitado.

### 8.8.7 Restricciones de la cuenta Invitado

La Plataforma de BI admite el inicio de sesión único anónimo para la cuenta de invitado. Por lo tanto, cuando los usuarios se conectan a la plataforma de BI sin especificar un nombre de usuario ni una contraseña, el sistema los registra automáticamente en la cuenta de invitados. Si asigna una contraseña segura a la cuenta Invitado, o si deshabilita la cuenta Invitado, deshabilita este comportamiento predeterminado.

## 8.9 Auditoría de modificaciones de configuración de seguridad

La plataforma de BI no auditará los cambios realizados en la configuración de seguridad predeterminada para:

- Archivos de propiedades para las aplicaciones Web (BOE, servicios Web)
- TrustedPrincipal.conf
- Personalización realizada en la plataforma de lanzamiento de BI y en Open Document

En general, no se auditará ninguna modificación de la configuración de seguridad realizada fuera de la CMC. Esto también se aplica a modificaciones realizadas a través de la Consola de administración central (CCM). Los cambios realizados a través de la CMC se pueden auditar.

## 8.10 Procesamiento de extensiones

La plataforma de BI permite proteger más el entorno de informes mediante el uso de extensiones de procesamiento personalizadas. Una extensión de procesamiento es una biblioteca de códigos cargada de forma dinámica que aplica la lógica empresarial a peticiones de vista o de programación concretas de la Plataforma de BI antes de que el sistema las procese.

Mediante su compatibilidad para las extensiones de procesamiento, el SDK de administración de la Plataforma de BI básicamente expone un "identificador" que permite a los desarrolladores interceptar la solicitud. Los programadores pueden así adjuntar fórmulas de selección a la solicitud antes de procesar el informe.

Un ejemplo típico es una extensión de procesamiento para informe que impone la seguridad de nivel de filas. Este tipo de seguridad limita el acceso a los datos por filas en una o más tablas de bases de datos. El programador escribe una biblioteca cargada dinámicamente que intercepta las solicitudes de vista o de programación correspondiente al informe (antes de que un servidor de páginas, servidor de procesamiento o servidor de aplicaciones de informes (RAS) procesen las solicitudes). El código del programador determina primero el usuario que posee el trabajo de procesamiento, después busca los privilegios de acceso a los datos correspondientes al usuario en un sistema de terceros. Después, el código genera y adjunta una fórmula de selección de registro al informe, con el fin de limitar los datos que se reciben desde la base de datos. En este caso, la extensión de procesamiento sirve para incorporar la seguridad personalizada de nivel de fila en el entorno de la Plataforma de BI.

Al habilitar las extensiones de procesamiento, se configuran los componentes de servidor de la Plataforma de BI apropiados para cargar de forma dinámica las extensiones de procesamiento en tiempo de

ejecución. En el SDK se incluye una API totalmente documentada que los programadores pueden usar para escribir extensiones de procesamiento. Para obtener más información, consulte la documentación para programadores disponible en la distribución del producto.

## 8.11 Interfase de búsqueda de virus

Puede confirmar distintas clases de ficheros (Adobe Acrobat, Microsoft Excel, Microsoft Word, Microsoft Powerpoint, Lumira, Crystal Reports, Web Intelligence, etc.) en la plataforma de BI mediante la CMC, la rampa de lanzamiento BI, los servicios Web REST y aplicaciones SDK personalizadas. Estos ficheros están sujetos a verificación del tamaño (para garantizar que el tamaño del fichero no sea cero) y a verificación de autorización en el directorio de destino. Con la introducción de la interfase de búsqueda de virus en BI 4.2 SP4, los ficheros que se confirman en la plataforma de BI también se confirman para la búsqueda de virus para garantizar que el contenido de dichos ficheros no esté infectado y no tenga virus.

Los ficheros se someten a una búsqueda de virus cuando el usuario

- añade un nuevo fichero
- guarda un documento
- copia un documento
- "envía un documento a la carpeta de entrada BI"
- crea una instancia de un documento
- o lleva a cabo cualquier otra operación que confirma un nuevo fichero en los servidores de repositorio de archivos.

> **Nota**
>
> Solo los ficheros recién confirmados en la plataforma de BI en BI 4.2 SP4 (tras habilitar la búsqueda de virus) son sometidos a una búsqueda de virus.

### 8.11.1 Habilitar la búsqueda de virus

Puede habilitar la búsqueda de virus para los archivos comprometidos con la plataforma de BI para los servidores de repositorio de archivos de entrada y salida.

Ha descargado la biblioteca Adaptador de la búsqueda de virus (VSA) desde un proveedor de certificados SAP. Para obtener una lista de los proveedores certificados por SAP, consulte http://global.sap.com/community/ebook/2013_09_adpd/enEN/search.html#search=NW-VSI.

> **Nota**
>
> Si necesita ayuda para cualquier proveedor o plataforma nuevos, póngase en contacto con los proveedores correspondientes.

Para habilitar la búsqueda de virus en el servidor de respositorios de archivos de entrada, realice lo siguiente:

1. Inicie sesión en la CMC.
2. Navegue hasta *Servidores* > *Lista de servidores*.
3. Haga clic con el botón derecho del ratón en el servidor de repositorios de archivos de entrada y seleccione *Propiedades* en el menú desplegable.

   Aparece la ventana *Propiedades*.
4. En la sección *Servicio Filestore de entrada*, seleccione la casilla de verificación *Habilitar búsqueda de virus*.
5. En el campo *Ubicación de archivos del adaptador de la búsqueda de virus*, introduzca la ruta absoluta al archivo de biblioteca del adaptador de la búsqueda de virus.
6. Seleccione *Grabar y cerrar*

> **Nota**
>
> - De forma predeterminada, la búsqueda de virus está deshabilitada para todos los archivos comprometidos con la plataforma de BI en BI 4.2 SP4.
> - Puede habilitar la búsqueda de virus utilizando GUI o CLI. El argumento de la línea de comandos que debe proporcionar en los servidores de repositorio de archivos para habilitar la búsqueda de virus es `vsaFileLoc`.
> - Puede seguir pasos similares para habilitar la búsqueda de virus en el servidor de repositorios de archivos de salida. Si tiene varios servidores de repositorios de archivos de entrada y de salida, compruebe que habilita la búsqueda de virus en cada uno de los servidores.
> - Debe reiniciar los servidores de repositorios de archivos después de habilitar la búsqueda de virus para que los cambios surtan efecto.

## 8.12 Seguridad de datos de la plataforma de BI

Los administradores de sistemas de la plataforma de BI administran el modo en el que la información confidencial se protege mediante:

- Un ajuste de seguridad en el nivel de clúster que determina las aplicaciones y clientes que pueden acceder al CMS. Esta configuración se administra a través del Administrador de configuración central.
- Un sistema de criptografía de dos claves que controla el acceso al repositorio del CMS y las claves que se usan para cifrar o descifrar los objetos del repositorio. El acceso al repositorio del CMS se establece a través del Administrador de configuración central, mientras que la Consola de administración central tiene un área de administración dedicada para las claves criptográficas.

Estas funciones permiten a los administradores configurar los despliegues de la plataforma de BI en niveles de cumplimento de seguridad de datos concretos, así como administrar las claves de cifrado que se usan para cifrar y descifrar los datos del repositorio del CMS.

### 8.12.1 Modos de seguridad de procesamiento de datos

La plataforma de BI puede funcionar en dos posibles modos de seguridad de procesamiento de datos:

- El modo de seguridad de procesamiento de datos predeterminado. En determinadas instancias, los sistemas que se ejecutan en este modo usarán claves de cifrado codificadas de forma rígida y no seguirán un estándar específico. El nodo predeterminado habilita la compatibilidad con versiones anteriores de las herramientas y aplicaciones cliente de la plataforma de BI.
- Un modo de seguridad de datos diseñado para cumplir con las directrices estipuladas en el Estándar federal de procesamiento de información (FIPS), concretamente FIPS 140-2. En este modo los algoritmos y módulos criptográficos compatibles con FIPS se usan para proteger los datos sensibles. Cuando se ejecuta la plataforma en modo compatible con FIPS, todas las herramientas y aplicaciones cliente que no cumplan con las directrices FIPS se deshabilitan automáticamente. Las herramientas y aplicaciones cliente de la plataforma están diseñadas para cumplir con el estándar FIPS 140-2. Los clientes y aplicaciones más antiguos no funcionarán cuando la plataforma de BI se ejecute en modo compatible con FIPS.

El modo de procesamiento de datos es transparente para los usuarios del sistema. En ambos modos de seguridad de procesamiento de datos, un motor de cifrado interno cifra y descifra los datos sensibles.

Se recomienda el uso del modo compatible con FIPS en las siguientes circunstancias:

- El despliegue de la plataforma de BI no necesita usar o interactuar con ninguna herramienta o aplicación cliente de la plataforma de BI heredada.
- Los estándares y directrices de procesamiento de datos de la organización prohíben el uso de claves de cifrado codificadas de forma rígida.
- La organización debe asegurar los datos según las regulaciones FIPS 140-2.

El modo de seguridad de procesamiento de datos se establece a través del Administrador de configuración central en las plataformas Windows y UNIX. Todos los nodos de un entorno en clúster se deben establecer en el mismo modo.

### 8.12.1.1 Para activar el modo compatible con FIPS en Windows

De forma predeterminada, el modo compatible con FIPS se desactiva cuando se instala la plataforma de BI.

1. Para iniciar el CCM, haga clic en *Programas* > *SAP Business Intelligence* > *Plataforma de SAP BusinessObjects BI* > *Administrador de configuración central*.
2. En el CCM, haga clic con el botón derecho en Server Intelligence Agent (SIA) y seleccione *Detener*.

   > ⚠ Precaución
   >
   > No vaya al paso 3 hasta que el estado del SIA sea Detenido.

3. Haga clic con el botón derecho en el SIA y seleccione *Propiedades*.
   Aparecerá el cuadro de diálogo *Propiedades* y mostrará la ficha *Propiedades*.
4. Agregue `-fips` al campo *Comando* y haga clic en *Aplicar*.
5. Haga clic en *Aceptar* para cerrar el cuadro de diálogo *Propiedades*.
6. Reinicie el SIA.

El SIA está funcionando en modo compatible con FIPS.

Debe activar la configuración compatible con FIPS en todos los SIA del despliegue de la plataforma de BI.

### 8.12.1.2 Para activar el modo compatible con FIPS en UNIX

Se deben detener todos los nodos del despliegue de la plataforma de BI antes de intentar el siguiente procedimiento.

De forma predeterminada, el modo compatible con FIPS se desactiva después de instalar la plataforma de BI. Use las siguientes instrucciones para activar la configuración compatible con FIPS para todos los nodos del despliegue.

1. Desde el directorio `<DIRINSTAL>/sap_bobj`, abra el archivo `ccm.config` para editarlo.
2. Agregue `-fips` al parámetro del comando de inicio del nodo.

   El parámetro de comandos de inicio de nodos se muestra en el formato siguiente: `<NOMBRENODO>INICIAR`. Por ejemplo, para un nodo denominado «SAP», el parámetro de comandos de inicio de nodos es `INICIARSAP`.
3. Guarde los cambios y seleccione *Salir*.
4. Reinicie el nodo.

El nodo está funcionando en modo compatible con FIPS.

Debe activar la configuración compatible con FIPS en todos los nodos del despliegue de la Plataforma de BI.

### 8.12.1.3 Para desactivar el modo compatible con FIPS en Windows

Se deben detener todos los servidores del despliegue de la plataforma de BI antes de intentar el siguiente procedimiento.

Si el despliegue se ejecuta en modo compatible con FIPS, use las siguientes instrucciones para desactivar la configuración.

1. En el CCM, haga clic con el botón derecho en Server Intelligence Agent (SIA) y haga clic en *Detener*.

   > ⚠ Precaución
   >
   > No vaya al paso 2 hasta que el estado del nodo aparezca marcado como *Detenido*.
2. Haga clic con el botón derecho del ratón en el SIA y elija *Propiedades*.
   Aparecerá el cuadro de diálogo *Propiedades* con la ficha *Propiedades* a la vista.
3. Elimine `-FIPS` del campo *Comando* y haga clic en *Aplicar*.
4. Haga clic en *Aceptar* para cerrar el cuadro de diálogo *Propiedades*.
5. Reinicie el SIA.

## 8.12.2 Cuentas de administrador

La plataforma de BI crea automáticamente una cuenta de administrador inicial. Recomendamos crear una cuenta en el grupo Administradores para cada persona.

El usuario administrador recibe automáticamente el derecho *Modificar los derechos que los usuarios tienen para los objetos*. Una vez que haya creado la cuenta de administrador, recuerde desactivar la cuenta de administrador inicial.

## 8.12.3 Derechos de conexión

De forma predeterminada, los administradores tienen acceso a los detalles de las conexiones, incluidas las contraseñas, si las conexiones se definen con credenciales.

En esta sección se explica cómo aplicar el principio de privilegios mínimos en las conexiones si no se supone que los administradores deben acceder a las fuentes de datos.

### Restringir el derecho "Descargar conexión localmente"

El derecho *Descargar conexión localmente* solo es estrictamente necesario para los usuarios que gestionan las conexiones (consulte Derechos de conexión [página 1153]). Debería concederse solo a usuarios individuales, no a grupos. Si un grupo tiene el derecho, cualquier usuario que agregue el grupo puede tener acceso a los detalles de las conexiones.

Para proteger completamente las conexiones:

1. Conceda el derecho *Descargar conexión localmente* a los usuarios que gestionen las conexiones.
2. Deniegue *Descargar conexión localmente* en la carpeta superior de Conexiones para los grupos Administradores y usuarios de diseñadores de universos.

Para evitar que los usuarios se concedan el derecho, consulte la sección siguiente.

### Asegurar el derecho "Modificar los derechos de los usuarios sobre los objetos"

El derecho predeterminado *Modificar derechos de los usuarios para los objetos* permite a los usuarios conceder un derecho incluso si no lo tienen ellos mismos. Para las conexiones, se debe sustituir por el derecho *Modificar de forma segura los derechos de los usuarios sobre los objetos*. Si los administradores no tienen el derecho *Descargar conexión localmente*, no deben tener derecho a concederlo a otros usuarios.

En la carpeta Conexiones de nivel superior:

1. Conceda a los grupos Administradores y Diseñador de universos el derecho *Modificar de forma segura los derechos de los usuarios sobre los objetos*.
2. Otorgue el derecho *Modificar de forma segura los derechos de los usuarios a los objetos* a los usuarios que gestionen las conexiones tal como se define en la sección anterior. Tendrán derecho a conceder el derecho *Descargar conexión localmente*.
3. Deniegue a los grupos Administradores y Diseñador de universos el derecho *Modificar los derechos de los usuarios sobre los objetos*.

# 8.13 Criptografía en la plataforma de BI

## Datos sensibles

La criptografía de la plataforma de BI está diseñada para proteger la información confidencial almacenada en el repositorio del CMS. Los datos sensibles incluyen credenciales de usuario, datos de conectividad a origen de datos y cualquier otro objeto de información que almacene contraseñas. Los datos se cifran para asegurar la privacidad, mantenerlos a salvo de daños y mantener el control de acceso. Todos los recursos de cifrado necesarios (incluido el motor de cifrado y las bibliotecas RSA) se instalan de forma predeterminada en cada despliegue de la plataforma de BI.

El sistema de la plataforma de BI usa un sistema de cifrado de dos claves.

## Claves criptográficas

El cifrado y descifrado de la información confidencial se realiza en segundo plano mediante el SDK que interactúa con el motor de cifrado interno. Los administradores del sistema administran la seguridad de los datos a través de claves de cifrado simétricas sin que cifren o descifren directamente bloques de datos específicos.

En la plataforma de BI, las claves de cifrado simétricas, conocidas como Claves criptográficas, se usan para cifrar/descifrar la información confidencial. La Consola de administración central tiene un área de administración dedicada para las claves criptográficas. Use las *claves criptográficas* para ver, generar, desactivar, revocar y eliminar claves. El sistema asegura que las claves necesarias para descifrar datos sensibles no se puedan eliminar.

## Claves de clúster

Las claves de clúster son claves de encapsulación de claves simétricas que protegen las claves criptográficas almacenadas en el repositorio del CMS. Al usar algoritmos de claves simétricas, las claves de clúster mantienen un nivel de control de acceso al repositorio del CMS. A cada nodo de la plataforma de BI se le asigna una clave de clúster durante la instalación. Los administradores del sistema pueden usar el CCM para restablecer la clave de clúster.

# 8.13.1 Trabajar con claves de clúster

Durante la configuración de la instalación de la plataforma de BI se crea una clave de clúster de ocho caracteres para Server Intelligence Agent. La clave se usa para cifrar todas las claves criptográficas del repositorio del CMS. Sin la clave correcta de clúster, no se puede acceder el CMS.

La clave de clúster se almacena con formato cifrado en el archivo `dbinfo`. El nombre del archivo `dbinfo` sigue esta convención: `_boe_<sia_name>.dbinfo`, en que `<sia_name>` es el nombre del Server Intelligence Agent para el clúster.

En Windows, el archivo se almacena en el directorio siguiente: `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

En los sistemas Unix, el archivo se almacena en el directorio de la plataforma en `<DIRINSTAL>/sap_bobj/enterprise_xi40/`:

| Plataforma Unix | Directorio de la plataforma |
|---|---|
| AIX | `<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/` |
| Solaris | `<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/` |
| Linux | `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/` |

> **Nota**
>
> La clave de clúster para los nodos dados no se puede recuperar desde el archivo `dbinfo`. Se recomienda que los administradores del sistema tomen medidas para proteger las claves de clúster.

Sólo los usuarios con derechos administrativos pueden restablecer las claves de clúster. Cuando sea necesario, use el CCM para restablecer la clave de clúster para todos los nodos del despliegue. Se usan nuevas claves de clúster automáticamente para ajustar las claves criptográficas dentro del repositorio del CMS.

### 8.13.1.1 Para restablecer la clave de clúster en Windows

Antes de restablecer la clave de clúster para el nodo, asegúrese de que se han detenido todos los servidores administrados por Server Intelligence Agent.

1. Para iniciar el CCM, desplácese a *Programas* > *SAP Business Intelligence* > *Plataforma de SAP BusinessObjects BI 4* > *Administrador de configuración central*.
2. En el CCM, haga clic con el botón derecho en Server Intelligence Agent (SIA) y seleccione *Detener*.

   > **Precaución**
   >
   > No vaya al paso 3 hasta que el estado del SIA sea Detenido.

3. Haga clic con el botón derecho en Server Intelligence Agent (SIA) y seleccione *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
4. Haga clic en la ficha *Configuración*.
5. Haga clic en *Cambiar* en *Configuración de la clave de clúster del CMS*.
   Aparecerá un mensaje de advertencia.
6. Haga clic en *Sí* para continuar.
   Se abre el cuadro de diálogo *Cambiar clave de clúster*.
7. Introduzca la misma clave de ocho caracteres en los campos *Nueva clave de clúster* y *Confirmar nueva clave de clúster*.

> **Nota**
>
> En Windows, las claves de clúster deben contener una combinación de caracteres en mayúsculas y minúsculas. O los usuarios pueden también generar una clave aleatoria. Se necesita una clave aleatoria para cumplir con FIPS.

8. Haga clic en *Aceptar* para enviar la nueva clave de clúster al sistema.
   Se mostrará un mensaje que confirma que la clave de clúster se ha restablecido correctamente.
9. Reinicie el SIA.

En un clúster de varios nodos, debe restablecer las claves de clúster para todos los SIA del despliegue de la plataforma de BI a la nueva clave.

### 8.13.1.2 Restablecer la clave de clúster en UNIX

Antes de restablecer la clave de clúster para un nodo, asegúrese de que se han detenido todos los servidores administrados por el nodo.

1. Navegue hasta el directorio `<DIRINSTAL>/sap_bobj`.
2. Escriba **`./cmsdbsetup.sh`** y pulse *Intro*.
   Aparece la pantalla *Configuración de base de datos de CMS*.
3. Escriba el nombre del nodo y pulse *Intro*.
4. Escriba **2** para cambiar la clave de clúster.
   Aparecerá un mensaje de advertencia.
5. Seleccione *Sí* para continuar.
6. En el campo proporcionado, escriba una nueva clave de clúster de ocho caracteres y pulse *Intro*.

   > **Nota**
   >
   > Asegúrese de que la clave tenga al menos seis caracteres y combine dos de los siguientes tipos de caracteres: mayúsculas, minúsculas, números o signos de puntuación. Por ejemplo, puede tener un carácter en minúscula con un número, un carácter en mayúscula con un carácter de puntuación, etc.

7. Vuelva a introducir la nueva clave de clúster en el campo proporcionado y pulse *Intro*.
   Aparecerá un mensaje que informa de que la clave de clúster se ha reinicializado correctamente.
8. Reinicie el nodo.

Debe restablecer todos los nodos del despliegue de la Plataforma de BI para usar la misma clave de clúster.

## 8.13.2 Oficiales criptográficos

Para administrar las claves criptográficas en la CMC, debe ser miembro del grupo Oficiales criptográficos. La cuenta de administrador predeterminada creada para la plataforma de BI también es miembro del grupo Agentes de criptografía. Use esta cuenta para agregar usuarios al grupo Oficiales criptográficos, según sea necesario. Se recomienda que la pertenencia al grupo se restrinja a un número limitado de usuarios.

> **Nota**
>
> Al agregar usuarios al grupo Administradores, éstos no heredan los derechos necesarios para llevar a cabo tareas de administración sobre las claves criptográficas.

### 8.13.2.1 Para agregar un usuario al grupo Oficiales criptográficos

Debe existir una cuenta de usuario en la plataforma de BI antes de que se pueda agregar al grupo Agentes de criptografía.

> **Nota**
>
> Debe ser miembro de los grupos *Administradores* y *Oficiales criptográficos* para agregar un usuario al grupo Oficiales criptográficos.

1. En el área de administración *Usuarios y grupos* de la CMC, seleccione el grupo *Oficiales criptográficos*.
2. Haga clic en *Acciones* > *Agregar miembros al grupo*.
   Aparecerá el cuadro de diálogo *Agregar*.
3. Haga clic en *Lista de usuarios*.
   La lista *Usuarios/grupos disponibles* se actualiza y muestra todas las cuentas de usuario del sistema.
4. Mueva la cuenta de usuario que desea agregar al grupo Oficiales de cifrado desde la lista *Usuarios/grupos disponibles* a la lista *Usuarios/grupos seleccionados*.

   > **→ Sugerencias**
   >
   > Para buscar un usuario específico, utilice el campo de búsqueda.

5. Haga clic en *Aceptar*.

Como miembro del grupo Oficiales criptográficos, la cuenta agregada recientemente tendrá acceso al área de administración *Claves criptográficas* de la CMC.

### 8.13.2.2 Para ver claves criptográficas en la CMC

La aplicación de la CMC contiene un área de administración dedicada para claves criptográficas que usa el sistema de la Plataforma de BI. El acceso a esta área está restringido a los miembros del grupo Agentes de criptografía.

1. Para iniciar la CMC, desplácese a *Programas* > *SAP Business Intelligence* > *Plataforma de SAP BusinessObjects BI 4* > *Consola de administración central de la plataforma de SAP BusinessObjects BI*.
   Aparecerá la página principal de la CMC.
2. Haga clic en la ficha *Claves criptográficas*.
   Aparece el área de administración de las *Claves criptográficas*.
3. Haga doble clic en la clave criptográfica para la que desea ver más detalles.

## Información relacionada

Para ver objetos asociados con una clave criptográfica [página 175]

# 8.13.3 Administrar claves criptográficas en la CMC

Los agentes de criptografía utilizan el área de administración *Claves criptográficas* para revisar, generar, desactivar, revocar y eliminar claves utilizadas para proteger datos confidenciales almacenados en el repositorio del CMS.

Todas las claves criptográficas actualmente definidas se enumeran en el área de administración de *Claves criptográficas*. En los encabezado descritos en la siguiente tabla se proporciona información básica de cada clave:

| Encabezado | Descripción |
|---|---|
| Título | Identificador de nombre de la clave criptográfica |
| Estado | Estado actual de la clave |
| Última modificación de estado | Fecha y fechador del último cambio asociado a la clave criptográfica |
| Objetos | Número de objetos asociados a la clave |

## Información relacionada

Estado de las claves criptográficas [página 174]
Para crear una nueva clave criptográfica [página 176]
Para eliminar una clave criptográfica del sistema [página 177]
Para revocar una clave criptográfica [página 177]
Para ver objetos asociados con una clave criptográfica [página 175]
Para marcar claves criptográficas como comprometidas [página 176]

# 8.13.3.1 Estado de las claves criptográficas

La siguiente tabla muestra todos las opciones de estado posibles para las claves criptográficas de la plataforma de BI:

| Estado | Descripción |
|---|---|
| Active | Sólo se puede designar *Activa* una única clave criptográfica en el sistema. Esta clave se usa para cifrar los datos sensibles actuales que se almacenarán en la base de datos |

| Estado | Descripción |
| --- | --- |
| | de la CMC. La clave también se usa para descifrar todos los objetos que aparecen el la lista Objetos. Una vez creada una nueva clave criptográfica, el estado actual *Activa* cambia a *Desactivada*. Una clave activa no se puede eliminar del sistema. |
| Desactivado | Una clave *Desactivada* no se puede usar para cifrar datos. Sin embargo, se puede usar para descifrar todos los objetos que aparecen en su lista Objetos. No se puede volver a activar una clave una vez que se ha desactivado. Una clave marcada como *Desactivada* no se puede borrar del sistema. Debe cambiar el estado de una clave a *Revocada* para que se pueda eliminar. |
| Comprometida | Una clave criptográfica que se considera que no es segura se puede marcar como comprometida. Al etiquetar estas calves, más tarde podrá volver a cifrar los objetos de datos que todavía se asocien a la clave. Una vez que la clave se ha marcado como comprometida, se debe revocar antes de que se pueda eliminar del sistema. |
| Revocada | Cuando se revoca una clave criptográfica, se inicia un proceso en el que todos los objetos que están asociados actualmente con la calve se vuelven a cifrar con la clave criptográfica actual "Activa". Cuando se revoca una clave, se puede eliminar con seguridad del sistema. El mecanismo de revocación asegura que los datos de la base de datos del CMS siempre se pueden descifrar. No hay modo alguno de volver a activar una clave una vez revocada. |
| Desactivada: regeneración de clave en proceso | Indica que la clave criptográfica está en proceso de ser revocada. Una vez finalizado el proceso, la clave se marcará como *Revocada*. |
| Desactivada: regeneración de clave suspendida | Indica que el proceso para revocar una clave criptográfica se ha suspendido. Normalmente, esto ocurre si se ha suspendido el proceso voluntariamente o si no está disponible un objeto de datos asociado con la clave. |
| Revocada-comprometida | Una clave se marca como Revocada-comprometida si se ha marcado como comprometida y todos los datos asociados anteriormente con ella se han cifrado con otra clave. Cuando una clave *Desactivada* se marca como comprometida, tendrá la opción de no llevar a cabo ninguna acción o de revocar la clave. Una vez revocada la clave comprometida, se podrá eliminar. |

## 8.13.3.2 Para ver objetos asociados con una clave criptográfica

1. Seleccione la clave en el área de administración *Claves criptográficas* de la CMC.
2. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades* de la clave criptográfica.

3. Haga clic en *Lista de objetos* del panel de navegación situado a la izquierda del cuadro de diálogo *Propiedades*.
   Todos los objetos asociados con la clave criptográfica se muestran a la derecha del panel de navegación.

   > → Sugerencias
   >
   > Use las funciones de búsqueda para encontrar un objeto concreto.

### 8.13.3.3 Para crear una nueva clave criptográfica

> ⚠ Precaución
>
> Al crear una nueva clave criptográfica, el sistema desactiva automáticamente la clave *activa* actual. Una vez desactivada una clave, no se puede restaurar como la clave *activa*.

1. En el área de administración de *Claves criptográficas* de la CMC, haga clic en *Administrar* > *Nueva* > *Clave criptográfica*.
   Aparece el cuadro de diálogo *Crear nueva clave criptográfica*.
2. Haga clic en *Continuar* para crear la nueva clave criptográfica.
3. Escriba el nombre y una descripción de la nueva clave criptográfica. Haga clic en *Aceptar* para guardar la información.
   La nueva clave se enumera como la única clave activa en el área de administración *Clave criptográficas*. La clave anteriormente *activa* se marca ahora como *Desactivada*.

Todos los nuevos datos confidenciales generados y almacenados en la base de datos de CMS se cifrarán ahora con la nueva clave criptográfica. Puede revocar la clave anterior y volver a cifrar todos sus objetos de datos con la nueva clave activa.

### 8.13.3.4 Para marcar claves criptográficas como comprometidas

Si por algún motivo una clave criptográfica ya no se considera como segura, puede marcarla como comprometida. Esto resulta útil para realizar un seguimiento, y puede proceder a identificar qué objetos de datos están asociados a la clave. Para poder marcar una clave criptográfica como comprometida, ésta debe desactivarse antes.

> ⓘ Nota
>
> También puede marcar una clave como comprometida una vez se haya revocado.

1. Vaya al área de administración *Claves criptográficas* de la CMC.
2. Seleccione la clave criptográfica que desee marcar como comprometida.
3. Haga clic en *Acciones* > *Marcar como comprometida*.
   Aparecerá en cuadro de diálogo *Marcar como comprometida*.

4. Haga clic en *Continuar*.
5. Seleccione una de las siguientes opciones del cuadro de diálogo *Marcar como comprometida*:
   - *Sí*: Inicia el proceso de volver a cifrar todos los objetos de datos asociados a la clave comprometida.
   - *No*: El cuadro de diálogo *Marcar como comprometida* está cerrado y la clave criptográfica se marca como *Comprometida* en el área de administración de *Claves criptográficas*.

   > **Nota**
   >
   > Si selecciona *No*, los datos confidenciales continuarán estando asociados a la clave comprometida. El sistema utilizará la clave comprometida para descifrar los objetos asociados.

### Información relacionada

Para revocar una clave criptográfica [página 177]
Estado de las claves criptográficas [página 174]
Para ver objetos asociados con una clave criptográfica [página 175]

## 8.13.3.5 Para revocar una clave criptográfica

Los objetos de datos asociados a una clave criptográfica desactivada pueden seguir usándola. Para anular la asociación entre los objetos cifrados y la clave desactivada, deberá revocar la clave.

1. Seleccione la clave que desea revocar de las claves enumeradas en el área de administración de *Claves criptográficas*.
2. Haga clic en *Acciones* > *Revocar*.
   Aparecerá el cuadro de diálogo *Revocar*.
3. Haga clic en *Aceptar*.
   Se inicia un proceso para cifrar todos los objetos de la clave con la clave activa actual. Si la clave está asociada a muchos objetos de datos, se marcará como *Desactivada: recifrado en curso* hasta que finalice el proceso de recifrado.

Una vez revocada una clave criptográfica, puede eliminarse con seguridad del sistema ya que ningún objeto de datos confidenciales requiere la clave para su descifrado.

## 8.13.3.6 Para eliminar una clave criptográfica del sistema

Antes de poder eliminar una clave criptográfica de la plataforma de BI, deberá asegurarse de que ningún objeto de datos del sistema necesita dicha clave. Esta restricción garantiza que todos los datos confidenciales almacenados en el repositorio del CMS se puedan descifrar siempre.

Una vez revocada correctamente una clave criptográfica, utilice las siguientes instrucciones para eliminar la clave del sistema.

1. Vaya al área de administración *Claves criptográficas* de la CMC.
2. Seleccione la clave criptográfica que desee eliminar.
3. Haga clic en *Administrar* > *Eliminar*.
   Aparece el cuadro de diálogo *Eliminar*.
4. Haga clic en *Eliminar* para eliminar la clave criptográfica del sistema.
   La clave eliminada deja de aparecer en el área de administración de *Claves criptográficas* de la CMC.

> **Nota**
>
> Una vez eliminada una clave criptográfica del sistema, no se puede restaurar.

### Información relacionada

Para revocar una clave criptográfica [página 177]
Estado de las claves criptográficas [página 174]

## 8.14 Protección de datos y privacidad

La protección de datos está asociada con muchos requisitos legales y de privacidad. Además del cumplimiento de las normativas de protección de datos, también debe tenerse en cuenta el cumplimiento de la legislación específica del sector en diferentes países. SAP ofrece funciones específicas para ayudar al cumplimiento respecto a requisitos legales relevantes, incluida la protección de datos. SAP no da ningún consejo sobre su estas funciones son el método para admitir requisitos específicos de empresa, sector, región o país. Además, esta información no da ningún consejo ni recomendación en lo que respecta a las características adicionales que serían necesarias en determinados entornos de TI. Las decisiones relacionadas con la protección de datos deben hacerse caso por caso, teniendo en cuenta la infraestructura del sistema y los requisitos legales aplicables.

> **Nota**
>
> En la mayoría de casos, el cumplimiento de leyes de protección de datos no queda cubierto con una función de producto. El software de SAP admite el cumplimento de protección de datos ofreciendo características de seguridad y funciones relevante spara la protección de datos específicas, como bloqueo simplificado y borrado de datos personales. SAP no ofrece asesoramiento legal de ninguna forma. Las definiciones y otras condiciones utilizadas en este documento no se obtienen de ninguna fuente legal.

### 8.14.1 Glosario

| Término | Definición |
| --- | --- |
| **Datos personales** | Cualquier información relacionada con una persona física identificada o identificable («sujeto de datos»). Una persona física identificable es una que se puede identificar, directa o indirectamente, de forma particular con referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o por uno o más factores específicos de la identidad física, psicológica, genética, mental, económica, cultural o social de esa persona física. |
| **Objetivo** | Un motivo justificado de forma legal, contractual o en otra forma para el procesamiento de **datos personales**. La suposición es que cualquier objetivo tiene un fin que normalmente ya está definido cuando se inicia el objetivo. |
| **Bloqueo** | Un método de restricción del acceso a datos para los cuales ha finalizado el **objetivo empresarial**. |
| **Supresión** | La destrucción irreversible de **datos personales**. |
| **Período de retención** | El período de tiempo entre el fin del objetivo para un conjunto de datos y el momento en el que este conjunto de datos se elimina según la legislación aplicable. Es una combinación del período de residencia y el período de bloqueo. |
| **Fin del objetivo** | Un método para identificar el punto en el tiempo para un conjunto de datos cuando el procesamiento de **datos personales** ya no se requiere para el principal **objetivo empresarial**. Después de haber alcanzado el **fin del objetivo**, los datos se **bloquean** y solamente los usuarios con una autorización especial pueden acceder a ellos (por ejemplo, auditores fiscales). |
| **Datos personales confidenciales** | Una categoría de datos personales que normalmente incluye el siguiente tipo de información:<br>• Categorías especiales de datos personales como los datos que revelan el origen étnico o racial, las opiniones políticas, las creencias religiosas o filosóficas, o la membresía a un sindicato y el procesamiento de datos genéticos, biométricos, o que hacen referencia a la vida sexual, la orientación sexual o la salud<br>• Datos personales sujetos al secreto profesional<br>• Datos personales relacionados con delitos criminales o administrativos<br>• Datos personales referentes a seguros y cuentas bancarias o de tarjetas de crédito |

| Término | Definición |
| --- | --- |
| **Período de residencia** | El período de tiempo después del fin del objetivo para un conjunto de datos durante el cual los datos permanecen en la base de datos y se pueden utilizar en el caso de procesos siguientes relacionados con el objetivo original. Al final del período de residencia más largo, se bloquean o se eliminan los datos. El período de residencia forma parte del período de retención global. |
| **Verificación de utilización** | Un proceso designado para garantizar la integridad de los datos en el caso de un potencial bloqueo de los datos del interlocutor comercial. Una verificación de utilización de una aplicación determina si hay datos dependientes para un interlocutor comercial determinado en la base de datos. Si existen datos dependientes, esto significa que los datos aún se requieren para las actividades empresariales. Por lo tanto, se evita el bloqueo de los interlocutores comerciales en los datos. |
| **Consentimiento** | La acción del sujeto de datos que confirma que el uso de sus datos personales se otorga para un objetivo determinado. Una funcionalidad de consentimiento permite el almacenamiento de un registro de consentimiento en relación con un objetivo específico y muestra si un sujeto de datos ha otorgado, retirado o denegado el consentimiento. |

## 8.14.2 Consentimiento del usuario

Las aplicaciones de SAP piden el consentimiento del usuario antes de recopilar datos personales. La Plataforma de SAP BusinessObjects Business Intelligence proporciona una funcionalidad que permite a los sujetos de datos dar el consentimiento para recopilar y procesar sus datos personales. SAP asume que el usuario, por ejemplo un cliente de SAP que recopila datos, tiene el consentimiento del sujeto de datos (una persona física como un cliente, un contacto o una cuenta) para recopilar o transferir datos a la solución.

> **Nota**
>
> *Mensaje de consentimiento de usuario*
>
> Este producto contiene campos de entrada abierta o libremente configurables, que no están previstos para el almacenamiento de datos personales sin la adopción de medidas técnicas y organizativas adicionales para garantizar la protección y la privacidad de los datos.

## 8.14.3 Informe de información

Cada persona tiene el derecho a obtener una confirmación respecto a si se están procesando los datos personales que le hacen referencia o no. En la Plataforma de SAP BusinessObjects Business Intelligence, es posible visualizar toda la información almacenada sobre un sujeto de datos en particular.

Para más detalles sobre cómo un usuario puede acceder a la información almacenada sobre el tema de los datos, consulte la sección "Acceder a su info", en el *Manual de usuario de la plataforma de lanzamiento de Business Intelligence de Fiori* , en el SAP Help Portal.

> **Nota**
>
> Los documentos almacenados de forma local no están protegidos por la Plataforma de SAP BusinessObjects Business Intelligence. La protección debe proporcionarla la gestión de dispositivos (por ejemplo, control de acceso, encriptación, etc.).

## 8.14.4 Registro de acceso de lectura

Se utiliza el registro de acceso de lectura para supervisar y registrar en un log el acceso de lectura a datos confidenciales. Estos datos se pueden categorizar como confidenciales según la legislación, según las políticas externas de la empresa o según las políticas internas de la empresa. Estas cuestiones comunes pueden ser de interés para una aplicación que utilice el registro de acceso de lectura:

- ¿Quién ha accedido a los datos de una entidad empresarial determinada, por ejemplo, una cuenta bancaria?
- ¿Quién ha accedido a datos personales, por ejemplo, un interlocutor comercial?
- ¿Qué empleado ha accedido a información personal, por ejemplo, la religión?
- ¿Qué usuarios han accedido a qué cuentas o interlocutores comerciales?

Estas cuestiones se pueden responder utilizando información sobre quién ha accedido a datos en particular dentro de un período de tiempo especificado. Técnicamente, esto significa que todas las infoestructuras de IU y API remoto (que acceden a los datos) se tienen que activar para el registro en el log.

La plataforma de BI de SAP BusinessObjects no identifica, procesa ni guarda datos personales sensibles. Por tanto, la plataforma de BI no guarda en log los accesos de lectura.

## 8.14.5 Supresión de datos personales

- Bloqueo y supresión simplificados: Además del cumplimiento de las normativas de protección de datos, también debe tenerse en cuenta el cumplimiento de la legislación específica del sector en diferentes países. Un escenario potencial normal en algunos países es que se tengan que eliminar los datos personales después de que haya finalizado el objetivo especificado, explícito y legítimo para el procesamiento de datos personales, pero siempre que no haya otros períodos de retención definidos en la legislación, por ejemplo, períodos de retención para los documentos financieros. Los requisitos legales en

algunos escenarios o países a menudo también requieren el bloqueo de datos en los casos en los que haya finalizado el objetivo especificado, explícito y legítimo para el procesamiento de estos datos, pero los datos se tienen que retener en la base de datos debido a otros períodos de retención definidos legalmente. En algunos escenarios, los datos personales también incluyen datos referenciados. Por lo tanto, el reto para la supresión y el bloqueo es primero gestionar los datos referenciados y finalmente los demás datos, como los datos del interlocutor comercial.

- Supresión de datos personales: El tratamiento de los datos personales está sujeto a la legislación aplicable relacionada con la supresión de tales datos al final del objetivo. Si ya no hay un objetivo legítimo que requiere el uso de datos personales, se tienen que eliminar. Cuando se eliminan datos en un conjunto de datos, también se tienen que eliminar todos los objetos referenciados relacionados con el conjunto de datos. También es necesario tener en cuenta la legislación específica del sector en diferentes países además de las leyes de protección de datos generales. Después del vencimiento del período de retención más largo, se tienen que eliminar los datos.

## Supresión de datos personales en la plataforma de BI de SAP BusinessObjects

La plataforma de BI de SAP BusinessObjects y sus mandantes no marcan ni categorizan datos (adquiridos de fuentes de datos para análisis y reporting) en los datos personales. El sistema que tiene los datos tiene que gestionar el requisito de transparencia y la recuperación de información. La supresión de datos es una funcionalidad estándar del sistema que tiene los datos. Adicionalmente, la plataforma de SAP BusinessObjects BI y sus mandantes proporcionan funcionalidades (conectividad en vivo a fuentes de datos) para mantener los datos en sincronización con el sistema que tiene los datos.

Sin embargo, los propios usuarios o los usuarios con autorización para gestionar los datos por ellos pueden acceder a los datos del usuario actualizados en el sistema. Los usuarios importados desde proveedores de identidades (como Windows AD, LDAP, etc.) se mantienen sincronizados con ellos y tienen que actualizarse en el propio proveedor de identidades.

Los usuarios creados en la plataforma de BI pueden eliminarse o desactivarse por usuarios autorizados para gestionar los datos por ellos. En este caso, la retención sólo puede gestionarse desactivando los usuarios en el sistema y, después del período de retención, estos usuarios se pueden borrar del sistema de forma manual mediante los usuarios autorizados para gestionar estos datos para ellos.

Al eliminar una cuenta de usuario, también se borrarán la carpeta Favoritos, las categorías personales y la bandeja de entrada de dicho usuario. La propiedad de los artefactos en la carpeta pública se transferirá del usuario borrado al administrador. Tenga en cuenta que para el usuario deshabilitado, los usuarios autorizados para gestionar estos datos para ellos deben realizar esto manualmente.

El identificador de objeto de usuario se almacena en una base de datos de auditoría y también en una base de datos de comentarios. Sin embargo, no se elimina al borrar usuarios, puesto que el ID de usuario en los logs de auditoría es necesario para los requisitos legales y de seguridad. De manera similar, los comentarios realizados por el usuario son para objetivos empresariales y, por lo tanto, deben conservarse para el historial de conversación. No se prevé que los comentarios contengan datos personales, ya que se informa con antelación al usuario de que no actualice datos personales en campos abiertos.

Además, los usuarios autorizados pueden borrar manualmente tanto las entradas de base de datos de auditoría como de comentarios.

Para más información acerca de cómo desactivar un usuario, consulte Para modificar una cuenta de usuario [página 107].

Para obtener más detalles sobre cómo borrar entradas de comentarios realizadas por un usuario, consulte Administrar la configuración de la aplicación Comentario BI [página 728]

### 8.14.6 Log de modificaciones

El Log de modificaciones en la plataforma de SAP BusinessObjects Business Intelligence procesa los datos personales de los interlocutores comerciales que estén implicados en las solicitudes de modificación y las actividades. Si se realiza alguna modificación respecto al interlocutor comercial, el sistema graba en un log la siguiente información sobre los datos personales por cada solicitud de modificación y actividad:

- El usuario que ha modificado los datos
- La fecha y la hora de la modificación
- El tipo de modificación (actualización, inserción, supresión, documentación de campo individual)
- Las claves de identificación y sus valores de los registros de datos
- Los valores antiguo y nuevo del atributo que se han modificado
- El nombre de la cabecera del atributo que se haya modificado

Puede definir los campos a grabar en el log.

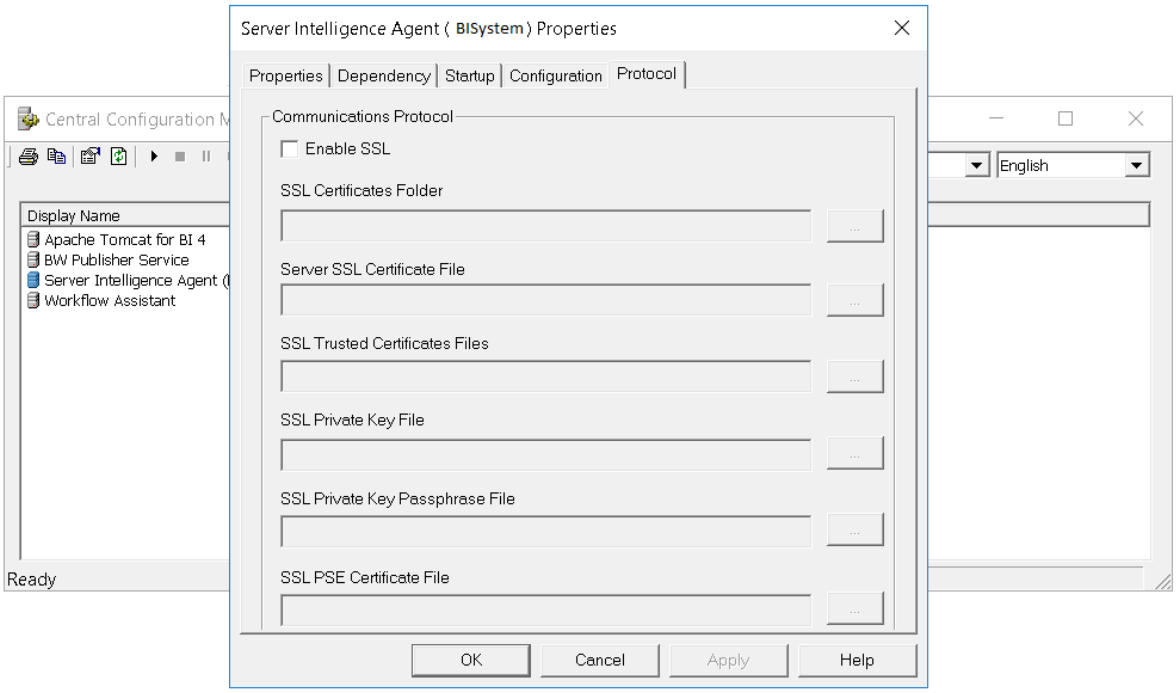
Para más detalles acerca de los logs de actualización de la cuenta de usuario, consulte ID de tipo de evento: 1007 en Audit events and details [página 915].

## 8.15 Configuración de servidores backend para SSL

Puede usar el protocolo Nivel de socket seguro (SSL) para todas las comunicaciones de red entre clientes y servidores BI del despliegue de la Plataforma de BI.

Para configurar SSL para toda la comunicación entre los servidores, debe realizar los pasos siguientes:

- El despliegue de la plataforma de BI con SSL está habilitado.
- Cree archivos de clave y de certificado para cada equipo del despliegue.
- Configure la ubicación de estos archivos en el Administrador de configuración central (CCM) y en el servidor de aplicaciones Web.
- También puede configurar SSL para certificados autofirmados o gestionados por una autoridad de certificados.




> **Nota**
>
> Si utiliza clientes gruesos como Crystal Reports, también deberá configurarlos para SSL si se va a conectar al CMS. En caso contrario, recibirá errores al intentar conectar al CMS que se ha configurado para SSL desde un cliente pesado (thick client) que no se ha configurado de este modo.

## 8.15.1 Para crear el archivo de configuración predeterminada

Puede crear un archivo de configuración predeterminada para evitar tener que añadir constantemente los valores durante la generación del certificado o de la solicitud de firma de certificado.

> **Nota**
>
> Debe seguir las siguientes reglas al crear el archivo de configuración predeterminada.
>
> - Debería añadir los valores en la parte izquierda exactamente como se menciona más abajo.
> - Los valores de la parte izquierda dependen de mayúsculas y minúsculas.
> - Sólo debería haber un espacio entre un valor y el signo «igual» (=). Por ejemplo, sólo hay un espacio entre *CA_Common_Name* y el signo «igual».
> - Debe asegurarse de que no haya espacios después de los valores en la parte derecha.

Siga los pasos a continuación para crear un archivo de configuración predeterminada con el nombre **Name.cnf**:

1. Abra un documento nuevo en un editor de texto.
2. Añada los valores indicados a continuación:

```
CA_Common_Name = rootnm
```

```
CA_Country = DE
CA_State = BW
CA_Locality = RRR
CA_Email = example@example.com
CA_Unit = root_u
CA_Expiration[YYMMDD] = yymmdd
User_Expiration[YYMMDD] = yymmdd
User_Country = IN
User_State = KA
User_Locality = BLR
User_Organization = SSS
User_Unit = Unit
User_Common_Name = UserName
```

3. Guarde al archivo con el nombre **Name.cnf** en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` en Windows y `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` en un entorno Unix.

## 8.15.2 Crear archivos de clave y de certificado

Para configurar el protocolo SSL para la comunicación de su servidor, utilice la herramienta GENPSE de la línea de comandos con el fin de crear un archivo de claves y un archivo de certificado para cada equipo del despliegue.

> **Nota**
>
> Necesita volver a crear los certificados para todos los equipos del despliegue, incluidos los equipos que ejecutan componentes de cliente grueso como Crystal Reports. Para estos equipos de mandante, utilice la herramienta de la línea de comandos `sslconfig` para realizar la configuración.

> **Nota**
>
> Para máxima seguridad, se deberían proteger todas las claves privadas y no se deberían transferir a través de canales de comunicación no seguros.

### 8.15.2.1 Para crear archivos de claves y certificados para un equipo

Esta sección trata la generación de clave autofirmada y certificados que son necesarios para comunicaciones seguras entre servidores o entre el servidor y el cliente. Puede generar los certificados utilizando la herramienta GENPSE, una herramienta de línea de comandos para ejecutar numerosas tareas relacionadas con la infraestructura de clave pública. La herramienta GENPSE se utiliza para generar los certificados X.509, solicitudes de firma de certificados, así como archivos PSE que se utilizan en el workflow del SSL CORBA. Se basa en la biblioteca de cifrado de SAP y admite el mecanismo **CommonCryptoLib** SHA-2 hasing.

Ejecute los siguientes pasos para crear los certificados necesarios para la comunicación segura:

> **Nota**
>
> Puede crear un archivo de configuración predeterminada **Name.cnf** con los valores estándar de la información solicitada al generar certificados. El archivo de configuración predeterminada le ahorra añadir

constantemente la información de cada certificado. Consulte Para crear el archivo de configuración predeterminada [página 184] para obtener más información.

1. Vaya a `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` en Windows y a `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` en Unix.
2. Ejecute el comando:
   - En Windows: `GenPSE.exe selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`
   - En Unix: `GenPSE.sh selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`

   Consulte la tabla a continuación para entender el comando:

| Comando | Función |
|---|---|
| GenPSE.exe o GenPSE.sh | Inicie la herramienta de criptografía |
| selfsigned | Para generar certificados autofirmados |
| <Name.pse> | Nombre de archivo PSE de servidor |
| <Name.der> | Nombre de archivo de certificado de servidor |
| <root Cert.der> | Nombre de certificado de autoridad de certificado |
| <Name.key> | Nombre de archivo de clave privada de servidor |
| <private key password.txt> | Frase de contraseña para archivo de clave privada de servidor |
| < path to Name.cnf > | Ruta del archivo de configuración predeterminada |

3. Introduzca la siguiente información para generar autoridad de certificado raíz, servidor y certificado de cliente.
   - *Nombre del país*
   - *Estado o nombre de provincia*
   - *Nombre de localidad*
   - *Nombre de organización*
   - *Nombre de unidad organizativa*
   - *Introduzca su nombre*
   - *Nombre común*
   - *Dirección de correo electrónico*
   - *Introduzca la fecha de vencimiento en formato AAMMDD*
4. Su archivo PSE y los certificados se generan y almacenan en`<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` en Windows y en `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` en Unix.

→ Sugerencias

Al generar el certificado de usuario, hay un parámetro adicional , *Tipo de certificado de usuario* , que permite que la herramienta cree el certificado para la autenticación del servidor o del cliente. Actualmente, cualquier decisión tomada bajo este parámetro no afecta a la configuración CORBA SSL.

ⓘ Nota

- El archivo PSE de servidor y el de autoridad de certificado deberían tener nombres diferentes.
- La fecha de vencimiento se admite hasta el 2049.

## 8.15.3 Configurar SSL cuando el certificado lo administra una autoridad de certificados

Debería generar una solicitud de firma de certificado para que una autoridad de certificación de terceros firme los certificados. La herramienta GenPSE genera una solicitud de firma de certificado ejecutando comandos simples y ofreciendo la información necesaria cuando se le pide.

Ejecute los siguientes pasos para generar una solicitud de firma de certificado:

ⓘ Nota

Puede crear un archivo de configuración predeterminada `Name.cnf` con los valores estándar de la información solicitada al generar certificados. El archivo de configuración predeterminada le ahorra añadir constantemente la información de cada certificado. Consulte Para crear el archivo de configuración predeterminada [página 184] para obtener más información.

1. Vaya a `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\win64_x64` en Windows y`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` en Unix.
2. Ejecute el comando:
   - En Windows: `GenPSE.exe gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`
   - En Unix: `GenPSE.sh gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`

| Comando | Función |
|---|---|
| GenPSE.exe o GenPSE.sh | Inicie la herramienta de criptografía |
| gencsr | Para generar la solicitud de firma de certificado |
| <csrname.p10> | Nombre de archivo de solicitud de firma de certificado |
| <Name.key> | Nombre de archivo de clave privada de servidor |
| <private key password.txt> | Frase de contraseña para archivo de clave privada de servidor |

| Comando | Función |
| --- | --- |
| <path to Name.cnf> | Ruta del archivo de configuración predeterminada |

3. Introduzca la siguiente información:
   - *Introducir frase de contraseña de clave privada en conjunto*
   - *Volver a introducir frase de contraseña de clave privada para confirmar*
   - *Nombre del país*
   - *Estado o nombre de provincia*
   - *Nombre de localidad*
   - *Nombre de unidad organizativa*
   - *Nombre común*
   - *Dirección de correo electrónico*
4. El archivo CSR en formato p10, clave privada del servidor y el archivo de frase de contraseña se generan y almacenan en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64` (Windows) y en `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` (Unix). El archivo CSR generado se envía a la autoridad de certificación para generar un certificado firmado.

## 8.15.3.1 Generar un archivo pse

Cuando sus certificados son administrados por una autoridad certificadora externa, debe generar un archivo PSE. Siga los pasos a continuación para generar un archivo PSE:

1. Abra `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Lance la consola de línea de comandos y ejecute `set SECUDIR=.` para Windows y `export SECUDIR=.` para Linux.
3. Ejecute `sapgenpse import_p8 -p <file_path_PSE> -c <file_path_server_certificate> -r <file_path_CA_certificate> -z <file_path_passphrase_text_file> <file_path_server_key>`.

   Consulte la tabla a continuación para entender mejor el comando:

| Comando | Descripción |
| --- | --- |
| sapgenpse | Inicie la herramienta de criptografía |
| import_p8 | Cree un nuevo archivo PSE a partir de una clave privada de formato PKCS N.° 8 (protegida de forma opcional por el cifrado basado en contraseña PKCS N.° 5) junto con todos los certificados X.509 necesarios. |
| -p <file_path_PSE> | Ruta del archivo al nuevo archivo PSE que se crea |
| -c <file_path_server_certificate> | Ruta del archivo al certificado del servidor |

| Comando | Descripción |
| --- | --- |
| -r <file_path_CA_certificate> | Ruta del archivo al certificado CA |
| -z <file_path_passphrase_text_file> | Ruta del archivo de texto de frase de contraseña |
| <file_path_server_key> | Ruta del archivo de clave privada del servidor |

> **Ejemplo**
>
> sapgenpse import_p8 -p C:\SSL\cert.pse -c C:\SSL\servercert.der -r C:\SSL\cacert.der -z C:\SSL\passphrase.txt C:\SSL\server.key

4. Indique una contraseña vacía pulsando Intro cuando se le solicite la contraseña.
5. Añada las credenciales de usuario al archivo pse creado.

> **→ Sugerencias**
>
> Si SIA se está ejecutando con una cuenta LocalSystem, deberá ejecutar el comando siguiente: `sapgenpse seclogin -p C:\SSL\cert.pse -O SYSTEM` para añadir las credenciales de usuario en el archivo pse.

> **Nota**
>
> Puede usar el nombre que desee para el archivo pse.

## 8.15.4 Configurar el protocolo SSL

Después de crear claves y certificados para cada equipo del despliegue, y de almacenarlos en una ubicación segura, debe proporcionar la ubicación segura al Administrador de configuración central (CCM) y al servidor de aplicaciones Web.

También debe desplegar pasos específicos para configurar el protocolo SSL para el servidor de aplicaciones Web y para cualquier equipo que ejecute una aplicación de cliente grueso.

### Activar FIPS en la plataforma basada en Unix para configuración de SSL

Se activa FIPS de forma estándar para una instalación completa de 4.2 SP04 o superior pero debería activarlo manualmente para los escenarios mencionados a continuación:

- Actualización de patch de 4.1 SPXX a 4.2 SP04
- Actualización de patch de 4.1 SPXX a 4.2 SP02 o SP03 y actualización posterior a 4.2 SP04

> **Nota**
>
> En Windows, CORBA SSL funciona incluso cuando FIPS no está habilitado, mientras que en plataformas basadas en Unix, es necesario comprobar que FIPS esté habilitado para servidores antes de configurar CORBA SSL.

Pasos para habilitar FIPS:

- Vaya a `<INSTALLDIR>/sap_bobj.`
- Ejecute `./stopservers`
- Abra el fichero ccm.config.
- Añada el texto "-FIPS" desde la lista de propiedades del nodo SIA.
- Ejecute `./startservers`

## 8.15.4.1 Para configurar el protocolo SSL en el CCM

1. En el CCM, haga clic con el botón derecho en Server Intelligence Agent y elija *Propiedades*.
2. En el cuadro de diálogo Propiedades, haga clic en la ficha *Protocolo*.
3. Asegúrese de que *Habilitar SSL* está seleccionado.
4. Especifique la ruta de acceso del archivo al directorio donde almacenó los archivos de clave y de certificado.

| Campo | Descripción |
|---|---|
| Carpeta de certificados de SSL | Carpeta donde se almacenan todos los archivos y certificados de SSL necesarios. Por ejemplo: `d:\ssl` |
| Archivo del certificado SSL del servidor | Nombre del archivo usado para almacenar el certificado SSL del servidor. De forma predeterminada, `servercert.der` |
| Archivo de certificados de confianza SSL | Nombre del archivo con el certificado de confianza SSL. De forma predeterminada, `cacert.der` |
| Archivo de clave privada SSL | Nombre del archivo de clave privada SSL usado para acceder al certificado. De forma predeterminada, `server.key` |
| Archivo de contraseña clave privada SSL | Nombre del archivo de texto que contiene la contraseña usada para acceder a la clave privada. De forma predeterminada, `passphrase.txt` |
| Archivo de certificado Pse SSL | Nombre del archivo pse que contiene información acerca de los certificados de servidor y de confianza. |

> **Nota**
>
> Asegúrese de indicar el directorio para el equipo donde se está ejecutando el servidor.

## 8.15.4.2 Para configurar el protocolo SSL en Unix

Debe usar la secuencia de comandos `serverconfig.sh` para configurar el protocolo SSL para un SIA. Esta secuencia de comandos proporciona un programa basado en texto que permite ver información de servidor así como agregar y eliminar servidores de la instalación. La secuencia de comandos `serverconfig.sh` se instala en el directorio `sap_bobj` de la instalación.

1. Use la secuencia de comandos `ccm.sh` para detener el SIA y todos los servidores de SAP BusinessObjects.
2. Ejecute la secuencia de comandos `serverconfig.sh`.
3. Seleccione *3 - Modificar nodo* y pulse `Intro`.
4. Especifique el SIA de destino y pulse `Intro`.
5. Seleccione la opción *1 - Modificar configuración SSL de Agente de inteligencia de servidor*.
6. Seleccione *ssl*.
   Cuando se le solicite, especifique las ubicaciones del certificado SSL.
7. Repita los pasos 1 a 6 para todos los SIA si el despliegue de la plataforma de BI es un clúster de SIA.
8. Inicie el SIA con la secuencia de comandos `ccm.sh` y espere a que se inicien los servidores.

## 8.15.4.3 Para configurar el protocolo SSL para el servidor de aplicaciones Web

1. Si tiene un servidor de aplicaciones Web J2EE, ejecute el SDK de Java con el siguiente conjunto de propiedades del sistema. Por ejemplo:

   ```
   -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:\ssl
   -DtrustedCert=cacert.der -DsslCert=clientcert.der -DsslKey=client.key
   -Dpassphrase=passphrase.txt
   ```

   En la tabla siguiente se muestran las descripciones que corresponden a estos ejemplos:

| Ejemplo | Descripción |
|---|---|
| `<DcertDir>=d:\ssl` | Directorio en el que se almacenan todos los certificados y claves. |
| `<DtrustedCert>=cacert.der` | Archivo de certificado de confianza. Si se especifica más de uno, sepárense con puntos y coma. |
| `<DsslCert>=clientcert.der` | Certificado utilizado por el SDK. |
| `<DsslKey>=client.key` | Clave privada del certificado del SDK. |
| `<Dpassphrase>=passphrase.txt` | Archivo que almacena la frase de acceso para la clave privada. |

| Ejemplo | Descripción |
| --- | --- |
| `<Dpsecert>=cert.pse` | Un PSE es un repositorio que contiene claves y certificados utilizados para proteger la comunicación.<br>Para obtener más información, consulte 3026364 |

2. Si tiene un servidor de aplicaciones Web IIS, ejecute la herramienta `sslconfig` desde la línea de comandos y siga los pasos de configuración.

## 8.15.4.4 Para configurar clientes complejos

Antes de realizar el procedimiento que se indica a continuación, tiene que crear y guardar todos los recursos SSL necesarios (por ejemplo, certificados y claves privadas) en un directorio conocido.

En el siguiente procedimiento se da por sentado que ha seguido las instrucciones para crear los siguientes recursos SSL:

| Recurso SSL | |
| --- | --- |
| Carpeta de certificados SSL | `d:\ssl` |
| Nombre del archivo de certificados SSL del servidor | `servercert.der` |
| Certificado de confianza SSL o nombre del archivo de certificados raíz | `cacert.der` |
| Nombre del archivo de clave privada SSL | `server.key` |
| El archivo que contiene la contraseña para acceder al archivo de clave privada SSL | `passphrase.txt` |
| Nombre de archivo de certificado Pse SSL | cert.pse |

Una vez creados los recursos anteriores, use las instrucciones que se indican a continuación para configurar aplicaciones de clientes complejos como, por ejemplo, el Administrador de configuración central (CCM).

1. Asegúrese de que no está funcionando la aplicación de cliente grueso.

   > **Nota**
   >
   > Asegúrese de indicar el directorio para el equipo donde se está ejecutando el servidor.

2. Ejecute la herramienta de línea de comandos `sslconfig.exe`. En función de su configuración, asegúrese de ejecutar la herramienta de win32_x86 para clientes de 32 bits o win64_x64 para clientes de 64 bits.

   La herramienta SSLC se instala junto con el software de la Plataforma de BI. (En Windows, por ejemplo, está instalado de forma predeterminada en `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.)

3. Escriba el siguiente comando:

```
sslconfig.exe -dir d:\SSL -mycert servercert.der -rootcert cacert.der -mykey
server.key
-passphrase     passphrase.txt -psecert cert.pse -protocol ssl
```

4. Reinicie la aplicación de cliente grueso.

### Información relacionada

Para crear archivos de claves y certificados para un equipo [página 185]

## 8.15.4.4.1 Para configurar el inicio de sesión en SSL para la herramienta de administración de traducciones

Para permitir que los usuarios utilicen el inicio de sesión de SSL con la herramienta de administración de traducciones, deberá agregar al archivo de configuración de la herramienta (`.ini`) información sobre los recursos de SSL.

1. Localice el archivo `TransMgr.ini` en el directorio: `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.
2. Con un editor de texto, abra el archivo `TransMgr.ini`.
3. Agregue los parámetros siguientes:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=<D:\SSLCert>
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. Guarde el archivo y cierre el editor de texto.

Ahora los usuarios podrán usar SSL para iniciar la sesión en la herramienta de administración de traducciones.

## 8.15.4.4.2 Para configurar SSL para la herramienta de conversión de informes

RCT quedará obsoleto en la versión 4.3 de BI. Para obtener más información, consulte **2801797**

# 8.16 Comprender la comunicación entre los componentes de la Plataforma de BI

Si el sistema de la Plataforma de BI se despliega completamente en la misma subred de seguridad, no hay que realizar ninguna configuración especial de los servidores de seguridad. Sin embargo, puede optar por desplegar algunos componentes en diferentes subredes separadas por uno o varios cortafuegos.

Es importante entender la comunicación entres los servidores de la Plataforma de BI, los clientes enriquecidos y el servidor de aplicaciones Web que aloja el SDK de SAP BusinessObjects, antes de configurar el sistema para que funcione con servidores de seguridad.

## Información relacionada

Configuración de la plataforma de BI para los servidores de seguridad [página 208]
Ejemplos de escenarios normales de servidores de seguridad [página 213]

## 8.16.1 Introducción a los servidores y los puertos de comunicación de la Plataforma de BI

Es importante entender los servidores de la Plataforma de BI y sus puertos de comunicación si el sistema se despliega con servidores de seguridad.

### 8.16.1.1 Cada servidor de la Plataforma de BI se enlaza con un puerto de solicitud.

Un servidor de la Plataforma de BI, por ejemplo, el servidor del repositorio de archivos de entrada, se enlaza con un puerto de solicitud cuando se inicia. Otros componentes de la Plataforma de BI, incluyendo servidores, clientes enriquecidos y el SDK alojado en el servidor de aplicaciones Web, pueden usar este puerto de solicitud para comunicarse con el servidor.

Un servidor seleccionará el número de puerto de solicitud dinámicamente cuando el servidor se inicie o reinicie, a menos que se configure para usar un número de puerto específico. Se debe configurar manualmente un número de puerto de solicitud específico para los servidores que se comunican con otros componentes de la Plataforma de BI a través de un servidor de seguridad.

### 8.16.1.2 Cada servidor de la Plataforma de BI se registra con el CMS

Los servidores de la Plataforma de BI se registran con el CMS al iniciarse. Cuando un servidor se registra, el CMS registra:

- El nombre de host (o dirección IP) del equipo host del servidor.
- El número de puerto de solicitud del servidor.

### 8.16.1.3 El CMS usa dos puertos

El CMS usa dos puertos: el puerto de solicitud y el puerto del servidor de nombres. El puerto de solicitud se selecciona dinámicamente de forma predeterminada. El puerto del servidor de nombres es el 6400 de forma predeterminada.

Todos los servidores de la Plataforma de BI y las aplicaciones cliente se pondrán en contacto inicialmente con el CMS™ en su puerto de servidor de nombres. El CMS™ responderá a este contacto inicial devolviendo el valor de su puerto de solicitud. Los servidores usarán este puerto de solicitud para la comunicación posterior con el CMS™.

### 8.16.1.4 Directorio del Servidor de administración central (CMS) de servicios registrados

El CMS proporciona un directorio de los servicios que se han registrado en él. Otros componentes de la Plataforma de BI, como los servicios, los clientes enriquecidos y el SDK alojado en el servidor de aplicaciones Web, pueden ponerse en contacto con el CMS y solicitar una referencia a un servicio concreto. La referencia de un servicio contiene el número de puerto de solicitud del servicio y el nombre de host (o dirección IP) del equipo host del servidor e ID del servicio.

Los componentes de la Plataforma de BI pueden residir en una subred diferente de la del servidor que usan. El nombre de host (o la dirección IP) contenido en la referencia del servicio se debe poder dirigir desde el equipo del componente.

> ⓘ Nota
>
> La referencia a un servidor de la plataforma de BI incluirá el nombre de host del equipo del servidor de forma predeterminada. (Si un equipo tiene más de un nombre de host, se selecciona el nombre de host principal). Puede configurar un servidor de modo que su referencia contenga en su lugar la dirección IP.

#### Información relacionada

Comunicación entre los componentes de la Plataforma de BI [página 196]

### 8.16.1.5 Comunicar Server Intelligence Agents (SIA) con el Servidor de administración central (CMS)

El despliegue no funcionará si el Server Intelligence Agent (SIA) y el Servidor de administración central (CMS) no se pueden comunicar entre sí. Asegúrese de que los puertos del servidor de seguridad están configurados para permitir la comunicación entre todos los SIA y todos los CMS del clúster.

### 8.16.1.6 Los procesos secundarios del servidor de tareas se comunican con su nivel de datos en el CMS

La mayoría de los servidores crean un proceso secundario para controlar una tarea, como la generación de un informe. El servidor de tareas crea uno o varios procesos secundarios. Cada proceso secundario tiene su propio puerto de solicitud.

De forma predeterminada, un servidor de tareas seleccionará dinámicamente un puerto de solicitud para cada proceso secundario. Puede especificar un rango de números de puerto entre los que el servidor de tareas podrá seleccionar.

Todos los procesos secundarios se comunican con el CMS. Si esta comunicación atraviesa un servidor de seguridad, debe:

- Especifique el rango de los números del puerto desde los que el servidor de tareas puede seleccionar agregando los parámetros `-requestJSChildPorts <puertoinferior>-<puertosuperior>` y `-requestPort <puerto>` a la línea de comandos del servidor. Tenga en cuenta que el rango de puertos debe ser lo suficientemente amplio para permitir el número máximo de procesos secundarios especificado por `-maxJobs`.
- Abra el rango de puertos especificado en el servidor de seguridad.

Muchos procesos secundarios se comunican con el nivel de datos. Por ejemplo, un proceso secundario puede conectarse a una base de datos de generación de informes, extraer datos y calcular valores para un informe. Si el proceso secundario del servidor de tareas se comunica con el nivel de datos a través de un servidor de seguridad, debe:

- Abrir una ruta de comunicación en el servidor de seguridad desde cualquier puerto del equipo servidor de tareas al puerto de escucha de la base de datos en el equipo servidor de base de datos.

#### Información relacionada

Información general de las líneas de comandos [página 1111]

## 8.16.2 Comunicación entre los componentes de la Plataforma de BI

Los componentes de la Plataforma de BI, como los clientes de explorador, los clientes enriquecidos, los servidores y el SDK alojado en el servidor de aplicaciones Web, se comunican entre sí a través de la red durante los flujos de trabajo normales. Es necesario entender estos flujos de trabajo para desplegar los productos de SAP BusinessObjects en diferentes subredes separadas por un servidor de seguridad.

## 8.16.2.1 Requisitos para la comunicación entre los componentes de la Plataforma de BI

Los despliegues de la plataforma de BI deben cumplir estos requisitos generales.

1. Todos los servidores deben poder inicializar la comunicación con el resto de servidores de la Plataforma de BI en el puerto de solicitud de dicho servidor.
2. El servidor de administración central usa dos puertos Todos los servidores de la plataforma de BI, los clientes enriquecidos y el servidor de aplicaciones Web que aloja el SDK, deben poder inicializar la comunicación con el CMS en sus dos puertos.
3. Cada proceso secundarios del servidor de tareas debe poder comunicarse con el CMS.
4. Los clientes gruesos deben poder iniciar la comunicación con el puerto de solicitud de los servidores del repositorio de archivos de entrada y salida.
5. Si está habilitada la auditoría para los clientes gruesos y las aplicaciones Web, deben poder iniciar la comunicación con el puerto de solicitud de los servidores de procesamiento de Adaptive que aloja el servicio proxy de auditoría del cliente.
6. En general, el servidor de aplicaciones Web que aloja el SDK debe poder comunicarse con el puerto de solicitud de todos los servidores de la Plataforma de BI.

   > **Nota**
   >
   > El servidor de aplicaciones Web solo necesita comunicarse con los servidores de la Plataforma de BI que se usan en el despliegue. Por ejemplo, si Crystal Reports no se usa, el servidor de aplicaciones Web no necesita comunicarse con los servidores de caché de Crystal Reports.

7. Los servidores de tareas usan los números de puerto que están especificados con el comando `-requestJSChildPorts <puertoinferior>-<puertosuperior>`. Si no se ha especificado un rango en la línea de comandos, los servidores usan números de puertos aleatorios. Para permitir que un servidor de tareas se comunique con un CMS, FTP, SFTP o servidor de correo en otro equipo, abra todos los puertos del rango especificado mediante `-requestJSChildPorts` en el servidor de seguridad.
8. El CMS debe poder comunicarse con el CMS del puerto de escucha.
9. El servidor de conexión, la mayoría de los procesos secundarios del servidor de tareas y todas las bases de datos del sistema y servidor de procesamiento de auditoría deben poder iniciar la comunicación con el puerto de escucha de la base de datos de informes.

### Información relacionada

Requisitos de puerto de la Plataforma de BI [página 197]

## 8.16.2.2 Requisitos de puerto de la Plataforma de BI

En esta sección se enumeran los puertos de comunicación que usan los servidores de la Plataforma de BI, los clientes gruesos, el servidor de aplicaciones Web que aloja el SDK y las aplicaciones de software de terceros. Si despliega la plataforma de BI con servidores de seguridad, puede usar esta información para abrir el mínimo número de puertos en dichos servidores de seguridad.

## 8.16.2.2.1 Requisitos de puerto para aplicaciones de la Plataforma de BI

En esta tabla se enumeran los servidores y números de puerto que usan las aplicaciones de la plataforma de BI.

| Producto | Aplicación cliente | Servidores asociados | Requisitos de puertos de servidor |
|---|---|---|---|
| Crystal Reports | Diseñador de SAP Crystal Reports 2020 | CMS<br>FRS de entrada<br>Servidor FRS de salida<br>Servidor de aplicaciones de informes (RAS) de Crystal Reports 2020<br>Servidor de procesamiento de Crystal Reports 2020<br>Servidor de caché de Crystal Reports | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS<br>Puerto de solicitud del FRS de entrada<br>Puerto de solicitud del FRS de salida<br>Puerto de solicitud del servidor de aplicaciones de informes de Crystal Reports 2020<br>Puerto de solicitud del servidor de procesamiento de Crystal Reports 2020<br>Puerto de solicitud del servidor de caché de Crystal Reports |
| Crystal Reports | SAP Crystal Reports para el diseñador de Enterprise | CMS<br>FRS de entrada<br>Servidor FRS de salida<br>Servidor de procesamiento de Crystal Reports<br>Servidor de caché de Crystal Reports | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS<br>Puerto de solicitud del FRS de entrada<br>Puerto de solicitud del FRS de salida<br>Puerto de solicitud del servidor de procesamiento de Crystal Reports<br>Puerto de solicitud del servidor de caché de Crystal Reports |
| Live Office | Cliente Live Office | Aplicación del proveedor de servicios Web (`dswsbobje.war`) que aloja el servicio Web de Live Office | Puerto HTTP (80 de forma predeterminada) |

| Producto | Aplicación cliente | Servidores asociados | Requisitos de puertos de servidor |
|---|---|---|---|
| SAP Analysis para Microsoft Office | SAP Analysis para Microsoft Office | CMS<br>Servidor de procesamiento de Adaptive que aloja el servicio de análisis multidimensional<br>FRS de entrada<br>Servidor FRS de salida | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS<br>Puerto de solicitud del servidor de procesamiento de Adaptive<br>Puerto de solicitud del FRS de entrada<br>Puerto de solicitud del FRS de salida |
| Plataforma de BI | Cliente enriquecido de SAP BusinessObjects Web Intelligence | CMS<br>FRS de entrada | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS<br>Puerto de solicitud del FRS de entrada |
| Plataforma de BI | Herramienta de diseño de universos | CMS<br>FRS de entrada<br>Servidor de conexión | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS<br>Puerto de solicitud del FRS de entrada<br>Puerto del servidor de conexión |
| Plataforma de BI | Administrador de vistas empresariales | CMS<br>FRS de entrada | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS<br>Puerto de solicitud del FRS de entrada |

| Producto | Aplicación cliente | Servidores asociados | Requisitos de puertos de servidor |
|---|---|---|---|
| Plataforma de BI | Administrador de configuración central (CCM) | CMS<br>Server Intelligence Agent (SIA) | Los siguientes puertos deben estar abiertos para que el CCM administre los servidores remotos de la Plataforma de BI:<br>Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS<br>Los siguientes puertos deben estar abiertos para que CCM administre los procesos SIA remotos:<br>Microsoft Directory Services (puerto TCP 445)<br>Servicio de sesión NetBIOS (puerto TCP 139)<br>Servicio de datagramas NetBIOS (puerto UDP 138)<br>Servicio de nombres NetBIOS (puerto UDP 137)<br>DNS (puerto TCP/UDP 53)<br>(Tenga en cuenta que algunos de los puertos indicados anteriormente pueden no ser necesarios. Consulte al administrador de Windows.) |
| Plataforma de BI | Server Intelligence Agent (SIA) | Todos los servidores de la Plataforma de BI, incluido el CMS | Puerto de solicitud del SIA (6410 de forma predeterminada)<br>Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS |
| Plataforma de BI | Herramienta de diagnóstico del repositorio | CMS<br>FRS de entrada<br>Servidor FRS de salida | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br>Puerto de solicitud del CMS<br>Puerto de solicitud del FRS de entrada<br>Puerto de solicitud del FRS de salida |

| Producto | Aplicación cliente | Servidores asociados | Requisitos de puertos de servidor |
|---|---|---|---|
| Plataforma de BI | SDK de la Plataforma de BI alojado en el servidor de aplicaciones Web | Todos los servidores de la Plataforma de BI que los productos desplegados necesitan<br><br>Por ejemplo, la comunicación con el puerto de solicitud del servidor de procesamiento de Crystal Reports 2020 es necesario si el SDK se recupera e interactúa con informes de Crystal desde el CMS. | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br><br>Puerto de solicitud del CMS<br><br>Puerto de solicitud para cada servidor que se requiera. Por ejemplo, el puerto de solicitud del servidor de procesamiento de Crystal Reports 2020. |
| Plataforma de BI | Proveedor de servicios Web (`dswsbobje.war`) | Todos los servidores de la Plataforma de BI que los productos que acceden a los servicios Web necesitan.<br><br>Por ejemplo, la comunicación con la caché de Dashboards y los puertos de solicitud del servidor de procesamiento son necesarios si SAP BusinessObjects Dashboards accede a las conexiones de origen de datos de Enterprise a través del proveedor de servicios Web. | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br><br>Puerto de solicitud del CMS<br><br>Puerto de solicitud para cada servidor que se requiera. Por ejemplo, el servidor de caché de Dashboards Cache Server y los puertos de solicitud del servidor de procesamiento de Dashboards. |
| Plataforma de BI | SAP BusinessObjects Analysis, edición para OLAP | CMS<br><br>Servidor de procesamiento de Adaptive que aloja el servicio de análisis multidimensional<br><br>FRS de entrada<br><br>Servidor FRS de salida | Puerto del servidor de nombres del CMS (6400 de forma predeterminada)<br><br>Puerto de solicitud del CMS<br><br>Puerto de solicitud del servidor de procesamiento de Adaptive<br><br>Puerto de solicitud del FRS de entrada<br><br>Puerto de solicitud del FRS de salida |

## 8.16.2.2.2 Requisitos de puertos para aplicaciones de terceros

Esta tabla muestra en una lista el software de terceros que usan los productos de SAP BusinessObjects. Incluye ejemplos específicos de algunos proveedores de software, pero los distintos proveedores tendrán requisitos de puertos diferentes.

| Aplicación de terceros | Componente de SAP BusinessObjects que usa el producto de terceros | Requisito de puertos de la aplicación de terceros | Descripción |
|---|---|---|---|
| Base de datos del sistema de CMS | Servidor de administración central (CMS) | Puerto de escucha del servidor de base de datos | El CMS es el único servidor que se comunica con la base de datos del sistema de CMS. |
| Base de datos de auditoría del CMS | Servidor de administración central (CMS) | Puerto de escucha del servidor de base de datos | El CMS es el único servidor que se comunica con la base de datos de auditoría del CMS. |
| Base de datos de generación de informes | Servidor de conexión<br>Cada proceso secundario del servidor de tareas<br>Cada servidor de procesamiento | Puerto de escucha del servidor de base de datos | Estos servidores recuperan información de la base de datos de generación de informes. |
| Servidor de aplicaciones Web | Todos los servicios Web de SAP BusinessObjects y aplicaciones Web, incluyendo la plataforma de lanzamiento de BI y la CMC | Puerto HTTP y puerto HTTPS.<br>Por ejemplo, en Tomcat el puerto HTTP predeterminado es el 8080 y el puerto HTTPS predeterminado es el 443. | El puerto HTTPS solo es necesario si se usa la comunicación HTTP segura. |
| Servidor FTP | Cada servidor de tareas | Entrada de FTP (puerto 21)<br>Salida de FTP (puerto 22) | Los servidores de tareas usan los puertos FTP para permitir el *envío a FTP*. |

| Aplicación de terceros | Componente de SAP BusinessObjects que usa el producto de terceros | Requisito de puertos de la aplicación de terceros | Descripción |
|---|---|---|---|
| Servidor SFTP | Cada servidor de tareas | SFTP (puerto 22) | Los servidores de tareas usan los puertos SFTP para permitir el *envío a SFTP*.<br><br>**Nota**<br><br>Se utiliza un fingerprint clave de host para asegurar una conexión SSH y evita ataques de intermediarios (man-in-the-middle). Se trata de un parámetro no nulo obligatorio necesario para configurar SFTP. El proceso para generar el fingerprint clave de host varía en función del servidor SFTP utilizado.<br><br>El administrador/usuario debe configurar una huella digital SHA-2 para habilitar SFTP. El administrador/usuario puede consultar la documentación del producto de sus implementaciones del servidor SSH/SFTP para generar una huella digital SHA-2.<br><br>**Ejemplo**<br><br>Los clientes SFTP comunes, como PuTTY y WinSCP, utilizan huellas digitales MD5 para identificar de forma exclusiva servidores SFTP. Las huellas digitales MD5 no funcionan. Consulte la documentación de las instrucciones del servidor SFTP para saber cómo se recuperan huellas digitales SHA-2. A continuación se describe un método de prueba, dado un archivo de claves públicas y herramientas de Unix OpenSSH. Dado un archivo de claves públicas denominado RSAKey.pub que contiene: `ssh-rsa <base64 encoded key>`, ejecute la siguiente secuencia de comandos: `cut -d ' ' -f 2 < RSAKey.pub` |

| Aplicación de terceros | Componente de SAP BusinessObjects que usa el producto de terceros | Requisito de puertos de la aplicación de terceros | Descripción |
|---|---|---|---|
| | | | `\| base64 -d \| openssl dgst -c -sha256`.<br>que da como resultado, por ejemplo: `(stdin)= 00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8`, donde la encriptación de 20 dígitos depende del valor de la clave pública codificada base64. Use el valor de 20 dígitos `00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8` para la huella digital de clave de host.<br>→ Recomendación<br>La recomendación es habilitar la configuración de SFTP en la página de los servidores de la CMC y BOE y utilizar las opciones de configuración predeterminadas cuando se realice el envío por los servidores SFTP. |

| Aplicación de terceros | Componente de SAP BusinessObjects que usa el producto de terceros | Requisito de puertos de la aplicación de terceros | Descripción |
|---|---|---|---|
| Servidor de correo electrónico | Cada servidor de tareas | SMTP (puerto como servidor SMTP) | Puede utilizar el mismo puerto para SMTPS y SMTP. De todos modos, para SMTPs, asegúrese de que el servidor tiene SSL/TLS habilitado utilizando el comando STARTTLS smtp.<br><br>Los servidores de tareas usan el puerto SMTP para permitir el *envío al correo electrónico*.<br><br>**Configurar servidor de tareas de Adaptive:**<br><br>Para configurar el servidor de tareas de Adaptive, siga los pasos descritos:<br><br>1. Lance la Consola de administración central (CMC)<br>2. Seleccione *Servidores* del desplegable.<br>3. Haga clic con el botón derecho del ratón en **AdaptiveJobServer** y seleccione *Destino*<br>4. Seleccione *Correo electrónico* del desplegable.<br>Si aún no ha añadido un servidor de correo electrónico como destino, primero añada un servidor de correo electrónico electrónico como destino antes de continuar.<br>5. Introduzca los detalles necesarios.<br>6. Compruebe la opción *Habilitar SSL* en caso necesario.<br>7. Seleccione *Guardar y cerrar*.<br><br>**Configurar SMTP sobre SSL:**<br><br>Para configurar SMTP sobre SSL, es necesario que el certificado de servidor esté presente en el servidor y en los sistemasBOE.<br><br>Para configurar SMTP sobre SSL, siga los siguientes pasos: |

| Aplicación de terceros | Componente de SAP BusinessObjects que usa el producto de terceros | Requisito de puertos de la aplicación de terceros | Descripción |
|---|---|---|---|
| | | | 1. Genere el certificado desde el servidor SMTP.<br>2. En la ventana *Destino*, marque la casilla *Habilitar SSL*.<br>3. Introduzca la ruta absoluta al certificado SMTP.<br>**Nota**<br>Introduzca una ruta absoluta al certificado SMTP. Si no introduce una ruta absoluta al certificado SMTP, puede introducir a reserva-espacio. (%SI_DEFAULT_CERT_LOC%) y el sistema lo lee como la ubicación predeterminada, por ejemplo, `\SAP BusinessObjects Enterprise XI 4.0\win64_x64\` or `\SAP BusinessObjects Enterprise XI 4.0\win32_x86\` y busca el certificado (nombre por defecto del certificado es certificate.crt).<br>4. Seleccione la *seguridad de conexión* deseada.<br>**Nota**<br>De forma predeterminada, la opción *StartTLS* está seleccionada. Puede seleccionar *SSL/TLS*.<br>5. Seleccione la versión TLS deseada. |

| Aplicación de terceros | Componente de SAP BusinessObjects que usa el producto de terceros | Requisito de puertos de la aplicación de terceros | Descripción |
|---|---|---|---|
| | | | **Nota**<br>De forma predeterminada, TLS v1.0 está seleccionada. Puede seleccionar TLS v1.1 o TLS v1.2.<br>6. Seleccione *Guardar y cerrar*<br>SMTP sobre SSL ahora está configurado.<br>**Nota**<br>Cuando ejecute una actualización de la revisión de BI 4.1 SP6 a cualquier versión superior, por defecto está seleccionada la opción StartTLS y TLS v1.0.<br>**Nota**<br>• Si el usuario marca la casilla de selección *Habilitar SSL* , se habilitará un canal seguro. Esto permite una transmisión SMTP segura vía SSL.<br>• Solo puede configurar un certificado SMTP por servidor de tareas de Adaptive. No puede tener varios certificados configurados para un servidor de tareas.<br>• La opción*Habilitar SSL* solo está disponible en el servidor de tareas de Adaptive y no en el nivel del documento. |
| Servidores Unix a los que los servidores de tareas pueden enviar contenido | Cada servidor de tareas | rexec out (puerto 512)<br>(solo Unix) rsh out (puerto 514) | (Solo Unix) Los servidores de tareas utilizan estos puertos para permitir el envío al disco. |

| Aplicación de terceros | Componente de SAP BusinessObjects que usa el producto de terceros | Requisito de puertos de la aplicación de terceros | Descripción |
|---|---|---|---|
| Servidor de autenticación | CMS™<br>Servidor de aplicaciones Web que aloja el SDK<br>cada cliente grueso, por ejemplo Live Office. | Puerto de conexión para autenticación de terceros.<br>Por ejemplo, el usuario define el servidor de conexión para el servidor LDAP de Oracle en el archivo ldap.ora. | Las credenciales de usuario se almacenan en el servidor de autenticación de terceros. El CMS™, el SDK y los clientes gruesos que se enumeran aquí necesitan comunicarse con el servidor de autenticación de terceros cuando un usuario inicia sesión. |

## 8.17 Configuración de la plataforma de BI para los servidores de seguridad

En esta sección se proporcionan instrucciones paso a paso para configurar el sistema de la Plataforma de BI para trabajar en un entorno con servidores de seguridad.

### 8.17.1 Para configurar el sistema para servidores de seguridad

1. Determine qué componentes de la Plataforma de BI se deben comunicar a través del servidor de seguridad.
2. Configurar manualmente el puerto de solicitud para cada servidor de la Plataforma de BI que se deba comunicar a través de un servidor de seguridad.
3. Configure el rango de puerto para cualquier elemento secundario del servidor de tareas que se deba comunicar a través de un cortafuegos agregando los parámetros `-requestJSChildPorts<>puertoinferior<->puertosuperior< y >-requestPort` puerto a la línea de comandos del servidor.
4. Configure el servidor de seguridad para permitir la comunicación con los puertos de solicitud y el rango de puerto de servidor de tareas en los servidores de la Plataforma de BI que se configuraron en el paso anterior.
5. (Opcional) Configure el archivo hosts en cada equipo que aloje un servidor de la plataforma de BI que se deba comunicar a través de un servidor de seguridad.

#### Información relacionada

Comunicación entre los componentes de la Plataforma de BI [página 196]
Configurar los números de puerto [página 471]

Información general de las líneas de comandos [página 1111]
Especificar las reglas del servidor de seguridad [página 209]
Configurar el archivo de hosts para servidores de seguridad que usan NAT [página 210]

## 8.17.1.1 Especificar las reglas del servidor de seguridad

Debe configurar el servidor de seguridad para permitir el tráfico necesario entre los componentes de la Plataforma de BI. Consulte la documentación del servidor de seguridad para obtener información acerca de cómo especificar estas reglas.

Especifique una regla de acceso de entrada para cada ruta de comunicación que cruce el servidor de seguridad. Es posible que no sea necesario especificar una regla de acceso para cada servidor de la plataforma de BI detrás del servidor de seguridad.

Utilice el número de puerto especificado en el cuadro del servidor *Puerto de solicitud* en la página de propiedades del servidor en la CMC. Recuerde que cada servidor de un equipo debe usar un número de puerto único. Algunos servidores de SAP BusinessObjects usan más de un puerto.

> **Nota**
>
> Si se despliega la plataforma de BI a través de servidores de seguridad que usan NAT, cada servidor de todos los equipos necesitará un número de puerto de solicitud único. Es decir, no puede haber dos servidores en todo el despliegue que compartan el mismo puerto de solicitud.

> **Nota**
>
> No es necesario que especifique ninguna regla de acceso de salida. Los servidores de la Plataforma de BI no inicializan la comunicación con el servidor de aplicaciones Web ni con ninguna aplicación cliente. Los servidores de la Plataforma de BI pueden inicializar la comunicación con otros servidores de la plataforma del mismo clúster. No se admiten los despliegues con servidores con clústeres en un entorno con servidor de seguridad de salida.

### Ejemplo

En este ejemplo se muestran las reglas de acceso de entrada para un servidor de seguridad entre el servidor de aplicaciones Web y los servidores de la Plataforma de BI. En este caso, se abrirían dos puertos para el CMS, un puerto para el Servidor del repositorio de archivos (FRS) de entrada y un puerto para el FRS de salida. Los números de puerto de solicitud son los números de puerto que se especifican en el cuadro *Puerto de solicitud* en la página de configuración de la CMC para un servidor.

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| Servidor de aplicaciones Web | Cualquiera | CMS | 6400 | Permitir |

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| Servidor de aplicaciones Web | Cualquiera | CMS | <Número de puerto de solicitud> | Permitir |
| Servidor de aplicaciones Web | Cualquiera | FRS de entrada | <Número de puerto de solicitud> | Permitir |
| Servidor de aplicaciones Web | Cualquiera | Servidor FRS de salida | <Número de puerto de solicitud> | Permitir |
| Cualquiera | Cualquiera | CMS | Cualquiera | Rechazar |
| Cualquiera | Cualquiera | Otros servidores de la plataforma | Cualquiera | Rechazar |

## Información relacionada

Comunicación entre los componentes de la Plataforma de BI [página 196]

# 8.17.1.2 Configurar el archivo de hosts para servidores de seguridad que usan NAT

Este paso es necesario solo si los servidores de la Plataforma de BI se deben comunicar a través de un servidor de seguridad en el que está habilitada la Traducción de direcciones de red (NAT). Este paso permite a los equipos cliente asignar un nombre de host de servidor a una dirección IP enrutable.

> **Nota**
>
> La plataforma de BI se puede desplegar en equipos que usen el sistema de nombres de dominio (DNS). En este caso, los nombres de host de equipo servidor se pueden asignar a una dirección IP enrutable externamente en el servidor DNS, en vez de hacerlo en el archivo `hosts` de cada equipo.

## Descripción de la traducción de direcciones de red

Se despliega un servidor de seguridad para proteger una red interna frente al acceso no autorizado. Los servidores de seguridad que utilizan NAT asignarán las direcciones IP de la red interna a otra dirección que utiliza la red externa. Esta traducción de direcciones mejora la seguridad al ocultar las direcciones IP internas a la red externa.

Los componentes de la Plataforma de BI, como los servidores, los clientes gruesos y el servidor de aplicaciones Web que aloja el SDK, usarán una referencia se servicio para ponerse en contacto con un servidor. La referencia de servicio contiene el nombre de host del equipo del servidor. Este nombre de host se debe

poder enrutar desde el equipo del componente de la Plataforma de BI. Esto significa que el archivo `hosts` del equipo del componente debe asignar el nombre de host del equipo del servidor a la dirección IP externa del equipo del servidor. La dirección IP externa del equipo servidor se puede enrutar desde el lado externo del servidor de seguridad, mientras que la dirección IP interna no se puede.

El procedimiento para configurar el archivo `hosts` es diferente en Windows y Unix.

### 8.17.1.2.1 Para configurar el archivo hosts en Windows

1. Busque todos los equipos que ejecuten un componente de la Plataforma de BI que se deba comunicar a través del servidor de seguridad en el que está habilitada la traducción de direcciones de red (NAT).
2. En cada equipo encontrado en el paso anterior, abra el archivo `hosts` con un editor de textos como el Bloc de notas. El archivo `hosts` se encuentra en `\Windows\System32\drivers\etc\hosts`.
3. Siga las instrucciones del archivo `hosts` para agregar una entrada para cada equipo situado detrás del servidor de seguridad que ejecute los servidores de la Plataforma de BI. Asigne el nombre de host del equipo servidor o el nombre de dominio completo a su dirección IP externa.
4. Guarde el archivo `hosts`.

### 8.17.1.2.2 Para configurar el archivo hosts en Unix

> **Nota**
>
> El sistema operativo UNIX se debe configurar para que primero consulte el archivo hosts con el fin de resolver los nombres de dominio antes de consultar el DNS. Consulte la documentación de los sistemas UNIX para obtener más detalles al respecto.

1. Busque todos los equipos que ejecuten un componente de la Plataforma de BI que se deba comunicar a través del servidor de seguridad en el que está habilitada la traducción de direcciones de red (NAT).
2. Abra el archivo hosts mediante un editor como `vi`. El archivo `hosts` se encuentra en el siguiente directorio `\etc`
3. Siga las instrucciones del archivo `hosts` para agregar una entrada para cada equipo situado detrás del servidor de seguridad que ejecute los servidores de la Plataforma de BI. Asigne el nombre de host del equipo servidor o el nombre de dominio completo a su dirección IP externa.
4. Guarde el archivo `hosts`.

## 8.17.2 Depurar un despliegue con cortafuegos

Si uno o varios servidores de la Plataforma de BI no funcionan cuando está habilitado el servidor de seguridad, aunque los puertos esperados estén abiertos en éste, puede usar los registros de eventos para determinar qué servidor está intentando escuchar en qué puertos o direcciones IP. Puede abrir estos puertos en el cortafuegos o usar la Consola de administración central (CMC) para cambiar los números de puerto o direcciones IP a los que estos servidores están intentando escuchar.

Cada vez que se inicia un servidor de la Plataforma de BI, el servidor escribe la siguiente información en el registro de eventos para cada puerto de solicitud al que intenta enlazarse.

- *Servidor*: el nombre del servidor y si se ha iniciado correctamente.
- *Direcciones publicadas*: una lista de direcciones IP y combinaciones de puertos que se publican en el servicio de nombres y que otros servidores usarán para comunicarse con este servidor.

Si el servidor se enlaza correctamente a un puerto, el archivo de registro muestra *Escuchando en los puertos*, la dirección IP y el puerto a los que está escuchando el servidor. Si el servidor no se enlaza correctamente al puerto, el archivo de registro muestra *Error al escuchar los puertos*, la dirección IP y el puerto a los que el servidor intenta escuchar y falla.

Cuando se inicia un Servidor de administración central, también escribe la información Direcciones publicadas, Escuchando en los puertos y Error al escuchar para el puerto del servicio de nombres del servidor.

> **Nota**
>
> Si el servidor está configurado para usar un puerto que se asigna automáticamente y para usar un nombre de host o una dirección IP que no sean válidos, el registro de eventos indica que el servidor no ha podido escuchar el nombre de host o la dirección IP y el puerto «0». Si un nombre de host o una dirección IP especificados no son válidos, el servidor generará un error antes de que el sistema operativo del host pueda asignar un puerto.

### Ejemplo

El siguiente ejemplo muestra una entrada para un Servidor de administración central que se ha escuchado correctamente en dos puertos de solicitud y en un puerto de servicio de nombres.

```
Server mynode.cms1 successfully started.
Request Port :
     Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
     Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032,
10.90.172.216:8765
Name Service Port :
     Published Address(es): mymachine.corp.com:6400
     Listening on port(s):  [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400,
10.90.172.216:6400
```

## 8.17.2.1 Para depurar un despliegue con cortafuegos

1. Lea el registro de eventos para determinar si el servidor se ha enlazado correctamente con el puerto que se ha especificado.

   Si el servidor no se ha podido enlazar correctamente a un puerto, probablemente exista un conflicto de puertos entre el servidor y otros procesos que se ejecuten en el mismo equipo. La entrada *Error al escuchar* indica al puerto que el servidor está intentando escuchar. Ejecute una utilidad, como netstat, para determinar el proceso que ha cogido el puerto y, a continuación, configure el otro proceso o el servidor para que escuche a otro puerto.
2. So el servidor se puede enlazar correctamente a un puerto, *Escuchando a* indica a qué puerto está escuchando el servidor. Si un servidor está escuchando un puerto y sigue sin funcionar correctamente,

asegúrese de que el puerto está abierto en el cortafuegos o configure el servidor de modo que escuche a un puerto que esté abierto.

Si todos los Servidores de administración central del despliegue intentan escuchar a los puertos o las direcciones IP no están disponibles, los CMS no se iniciarán y no podrá iniciar sesión en la CMC. Si desea cambiar el número de puerto o la dirección IP a los que el CMS intenta escuchar, debe usar el Administración de configuración central (CCM) para especificar un número de puerto o una dirección IP.

### Información relacionada

Configurar los números de puerto [página 471]

## 8.18 Ejemplos de escenarios normales de servidores de seguridad

Esta sección contiene ejemplos de escenarios normales de servidores de seguridad.

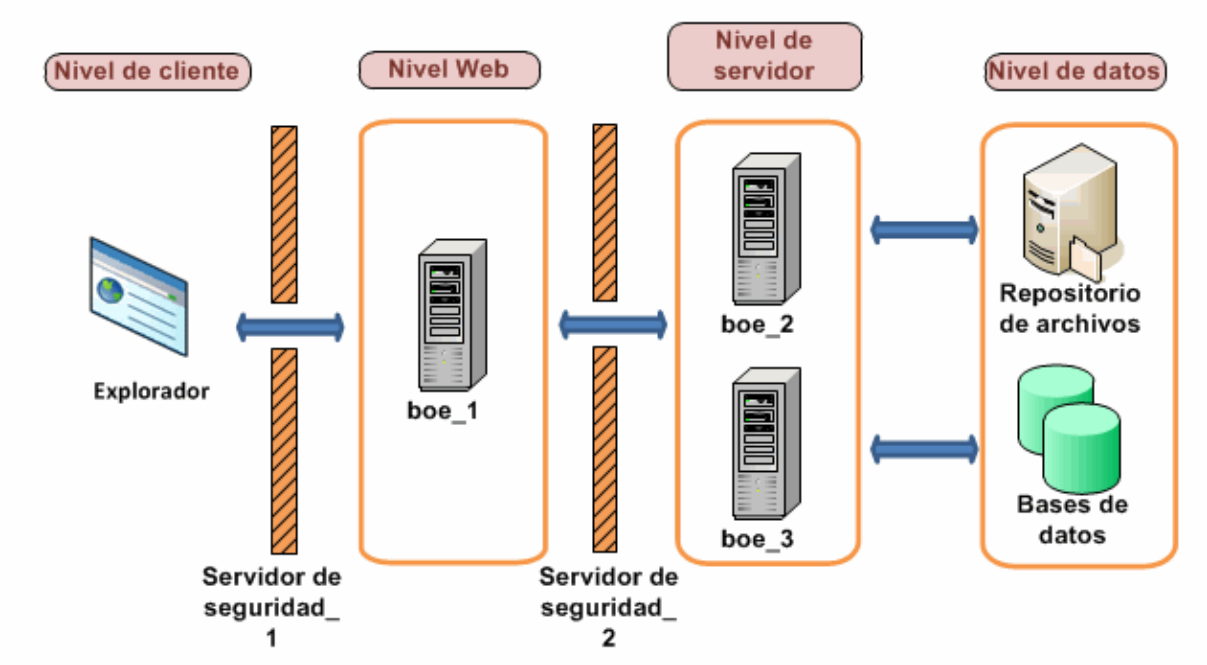
### 8.18.1 Ejemplo: Nivel de aplicación implementado en una red aparte

En este ejemplo se muestra cómo configurar un servidor de seguridad y la plataforma de BI para que trabajen conjuntamente en un despliegue en el que el servidor de seguridad separa el servidor de aplicaciones Web de los otros servidores de la plataforma de BI.

En este ejemplo, los componentes de la Plataforma de BI están desplegados en estos equipos:

- El equipo `boe_1` aloja el servidor de aplicaciones Web y el SDK.
- El equipo `boe_2` aloja los servidores del nivel de Intelligence, incluidos el Servidor de administración central, el servidor del repositorio de archivos de entrada, el servidor del repositorio de archivos de salida y el servidor de eventos.
- El equipo `boe_3` aloja los servidores de nivel de procesamiento, incluyendo el Servidor de tareas de Adaptive, el servidor de procesamiento de Web Intelligence, el Servidor de aplicaciones de informes, el servidor de caché de informes de Crystal Reports y el servidor de procesamiento de Crystal Reports.

Nivel de aplicación desplegado en una red aparte




## 8.18.1.1 Para configurar un nivel de aplicación desplegado en una red aparte

En los siguientes pasos se explica cómo configurar este ejemplo.

1. Se aplican los siguientes requisitos de comunicación a este ejemplo:
   - El servidor de aplicaciones Web que aloja el SDK debe poder comunicarse con el CMS en sus dos puertos.
   - El servidor de aplicaciones Web que aloja el SDK debe poder comunicarse con todos los servidores de la Plataforma de BI.
   - El explorador debe tener acceso al puerto de solicitud http o https en el servidor de aplicaciones Web.
2. El servidor de aplicaciones Web debe comunicarse con todos los servidores de la Plataforma de BI en los equipos boe_2 y boe_3. Configure los números de puerto para cada servidor en estos equipos. Tenga en cuenta que puede usar cualquier puerto libre entre 1.025 y 65.535.
   Los números de puerto elegidos para este ejemplo se enumeran en la tabla:

| Servidor | Número de puerto |
|---|---|
| Servidor de administración central | 6400 |
| Servidor de administración central | 6411 |
| Servidor del repositorio de archivos de entrada | 6415 |
| Servidor del repositorio de archivos de salida | 6420 |
| Servidor de eventos | 6425 |
| Servidor de tareas de Adaptive | 6435 |

| Servidor | Número de puerto |
|---|---|
| Servidor de caché de Crystal Reports | 6440 |
| Servidor de procesamiento de Web Intelligence | 6460 |
| Servidor de aplicaciones de informes | 6465 |
| Servidor de procesamiento de Crystal Reports | 6470 |

3. Configure los servidores de seguridad `Firewall_1` y `Firewall_2` para permitir la comunicación con los puertos fijos en los servidores y el servidor de aplicaciones Web que configuró en el paso anterior.

   En este ejemplo, abrimos el puerto HTTP para el servidor de aplicaciones Tomcat.

   Configuración de Firewall_1

| Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|
| Cualquiera | boe_1 | 8080 | Permitir |

   Configuración de Firewall_2

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| boe_1 | Cualquiera | boe_2 | 6400 | Permitir |
| boe_1 | Cualquiera | boe_2 | 6411 | Permitir |
| boe_1 | Cualquiera | boe_2 | 6415 | Permitir |
| boe_1 | Cualquiera | boe_2 | 6420 | Permitir |
| boe_1 | Cualquiera | boe_2 | 6425 | Permitir |
| boe_1 | Cualquiera | boe_3 | 6435 | Permitir |
| boe_1 | Cualquiera | boe_3 | 6440 | Permitir |
| boe_1 | Cualquiera | boe_3 | 6460 | Permitir |
| boe_1 | Cualquiera | boe_3 | 6465 | Permitir |
| boe_1 | Cualquiera | boe_3 | 6470 | Permitir |

4. Este servidor de seguridad no está habilitado para NAT, por lo que no es necesario configurar el archivo `hosts`.

## Información relacionada

Configurar los números de puerto [página 471]
Comprender la comunicación entre los componentes de la Plataforma de BI [página 193]

## 8.18.2 Ejemplo: cliente grueso y nivel de base de datos separados de los servidores de la Plataforma de BI por un servidor de seguridad

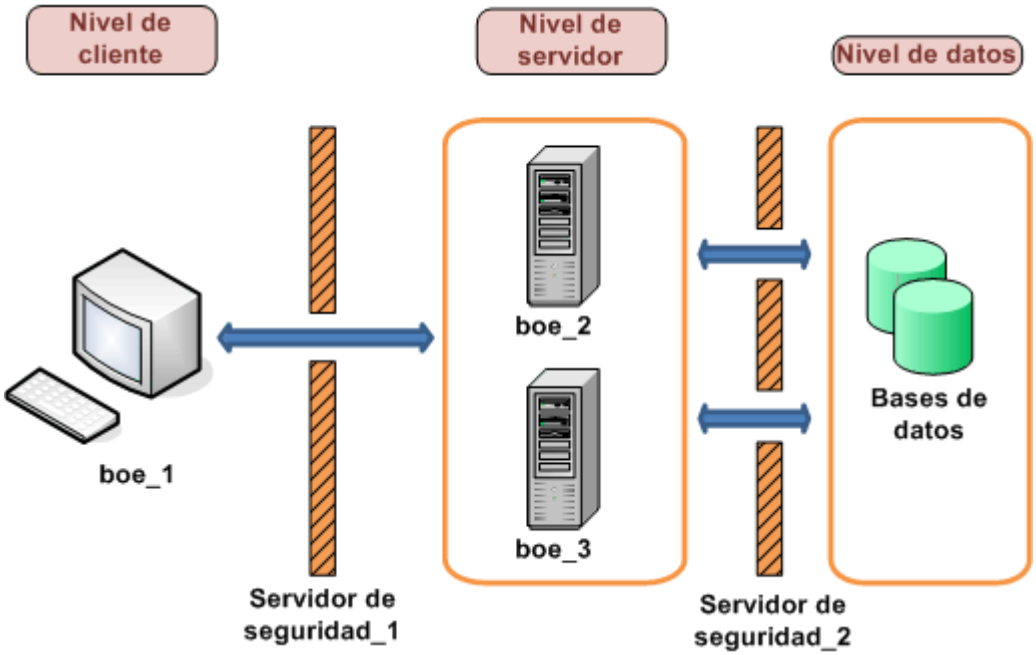
En este ejemplo se muestra cómo configurar un servidor de seguridad y la plataforma de BI para que funcionen conjuntamente en un escenario de despliegue en el que:

- Un servidor de seguridad separa el cliente grueso de los servidores de la Plataforma de BI.
- Un servidor de seguridad separa los servidores de la Plataforma de BI del nivel de base de datos.

En este ejemplo, los componentes de la Plataforma de BI están desplegados en estos equipos:

- El equipo `boe_1` aloja el Asistente de publicación. El Asistente de publicación es un cliente grueso de la Plataforma de BI.
- El equipo `boe_2` aloja los servidores del nivel de Intelligence, incluidos el servidor de administración central (CMS), el servidor del repositorio de archivos de entrada, el servidor del repositorio de archivos de salida y el servidor de eventos.
- El equipo `boe_3` aloja los servidores de nivel de procesamiento, que incluyen: el Servidor de tareas de Adaptive, el Servidor de procesamiento de Web Intelligence, el Servidor de aplicaciones de informes, el Servidor de procesamiento de Crystal Reports y el Servidor de almacenamiento en caché de Crystal Reports.
- El equipo `Databases` aloja el sistema del CMS y las bases de datos de auditoría, y la base de datos de generación de informes. Tenga en cuenta que puede desplegar ambas bases de datos en el mismo servidor de base de datos o bien puede desplegar cada una en su propio servidor de base de datos. En este ejemplo, todas las bases de datos del CMS y la base de datos de generación de informes se despliegan en el mismo servidor de base de datos.

Cliente enriquecido y nivel de base de datos desplegados en redes separadas



### 8.18.2.1 Configurar los niveles independientes de los servidores de la Plataforma de BI mediante un servidor de seguridad

En los siguientes pasos se explica cómo configurar este ejemplo.

1. Aplique los siguientes requisitos de comunicación a este ejemplo:
   - El Asistente de publicación debe poder iniciar la comunicación con el CMS™ en sus dos puertos.
   - El Asistente de publicación debe poder iniciar la comunicación con el servidor del repositorio de archivos de entrada y con el servidor del repositorio de archivos de salida.
   - El servidor de conexión, cada proceso secundario del servidor de tareas y cada servidor de procesamiento deben tener acceso al puerto de escucha en el servidor de base de datos de generación de informes.
   - El CMS™ debe tener acceso al puerto de escucha de base de datos en el servidor de base de datos del CMS™.
2. Configure un puerto específico para el CMS™, el FRS de entrada y el FRS de salida. Tenga en cuenta que puede usar cualquier puerto libre entre 1.025 y 65.535.
   Los números de puerto elegidos para este ejemplo se enumeran en la tabla:

| Servidor | Número de puerto |
|---|---|
| Servidor de administración central™ | 6411 |
| Servidor del repositorio de archivos de entrada | 6415 |
| Servidor del repositorio de archivos de salida | 6416 |

3. No es necesario configurar un rango de puertos para los secundarios del servidor de tareas, porque el servidor de seguridad situado entre los servidores de tareas y los servidores de base de datos se configurará para permitir que cualquier puerto pueda iniciar la comunicación.
4. Configure `<Firewall_1>` para permitir la comunicación con los puertos fijos en los servidores de la plataforma que configuró en el paso anterior. Tenga en cuenta que el puerto 6400 es el número de puerto predeterminado para el puerto del servidor de nombres del CMS™ y no debía configurarse explícitamente en el paso anterior.

| Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|
| Cualquiera | boe_2 | 6400 | Permitir |
| Cualquiera | boe_2 | 6411 | Permitir |
| Cualquiera | boe_2 | 6415 | Permitir |
| Cualquiera | boe_2 | 6416 | Permitir |

   Configure `<Firewall_2 >`para permitir la comunicación con el puerto de escucha del servidor de base de datos. El CMS™ (en *boe_2*) debe tener acceso al sistema del CMS™ y a la base de datos de auditoría, y los servidores de tareas (en *boe_3*) deben tener acceso a las bases de datos del sistema y de auditoría. Tenga en cuenta que no es necesario configurar un rango de puertos para los procesos secundarios del servidor de tareas, porque su comunicación con el CMS no cruzaba ningún servidor de seguridad.

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| boe_2 | Cualquiera | Bases de datos | 3306 | Permitir |
| boe_3 | Cualquiera | Bases de datos | 3306 | Permitir |

5. Este servidor de seguridad no está habilitado para NAT, por lo que no es necesario configurar el archivo `hosts`.

### Información relacionada

Comprender la comunicación entre los componentes de la Plataforma de BI [página 193]
Configuración de la plataforma de BI para los servidores de seguridad [página 208]

## 8.19 Configuración del servidor de seguridad para entornos integrados

En esta sección se detallan las consideraciones específicas y la configuración del puerto para los despliegues de la Plataforma de BI que se integran con los siguientes entornos ERP.

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Los componentes de la Plataforma de BI incluyen clientes de explorador, clientes enriquecidos, servidores y el SDK alojado en el servidor de aplicaciones Web. Los componentes del sistema se pueden instalar en varios equipos. Es útil comprender los conceptos básicos de la comunicación entre los componentes de la plataforma de BI y ERP antes de configurar el sistema para que trabaje con servidores de seguridad.

### Requisitos de puerto para servidores de la Plataforma de BI

Los siguientes puertos son necesarios para los servidores correspondientes en la plataforma de BI:

| Requisitos de puertos de servidor |
| --- |
| • Puerto Servidor de nombres del Servidor de administración central<br>• Puerto de solicitud del Servidor de administración central<br>• Puerto de solicitud del FRS de entrada<br>• Puerto de solicitud del FRS de salida<br>• Puerto de solicitud del Servidor de aplicaciones de informes<br>• Puerto de solicitud del servidor de caché de Crystal Reports<br>• Puerto de solicitud frl servidor de páginas de Crystal Reports<br>• Puerto de solicitud del servidor de procesamiento de Crystal Reports |

## 8.19.1 Información general específica del servidor de seguridad para la integración de SAP

El despliegue de la Plataforma de BI debe cumplir con las siguientes reglas de comunicación:

- El CMS debe poder iniciar la comunicación con el sistema de SAP en el puerto de puerta de enlace del sistema de SAP.
- El Servidor de tareas de Adaptive y el Servidor de procesamiento de Crystal Reports (junto con los componentes de acceso a datos) deben poder iniciar la comunicación con el sistema SAP en el puerto del Gateway del sistema SAP.
- El componente Publicador de BW debe poder iniciar la comunicación con el sistema SAP en el puerto Gateway del sistema SAP.
- Los componentes de la Plataforma de BI desplegados en el lado de SAP Enterprise Portal (por ejemplo, iViews y KMC) deben poder inicializar la comunicación con las aplicaciones Web de la Plataforma de BI en puertos HTTP/HTTPS.
- El servidor de aplicaciones Web deben poder iniciar la comunicación en el servicio Gateway del sistema SAP.
- Crystal Reports debe poder iniciar la comunicación con el host SAP en el puerto Gateway del sistema SAP y en el puerto Dispatcher del sistema SAP.

El puerto en el que recibe el servicio Gateway de SAP es el mismo que el especificado en la instalación.

> **Nota**
>
> Si un componente necesita un enrutador de SAP para conectarse a un sistema de SAP, puede configurar el componente mediante la cadena del enrutador de SAP. Por ejemplo, al configurar un sistema de derechos de SAP para importar funciones y usuarios, la cadena del enrutador de SAP se puede sustituir por el nombre del servidor de aplicaciones. De este modo se garantiza que el sistema CMS se comunicará con el sistema SAP a través del enrutador SAP.

### Información relacionada

Instalación de un gateway de SAP local [página 1023]

### 8.19.1.1 Requisitos detallados del puerto

#### Requisitos de puertos de SAP

La plataforma de BI usa el Conector Java de SAP (SAP JCO) para comunicarse con SAP NetWeaver. Debe configurar y asegurar la disponibilidad de los siguientes puertos:

- Puerto de recepción del servicio Gateway de SAP (por ejemplo, 3300).
- Puerto de recepción del servicio Dispatcher de SAP (por ejemplo, 3200).

En la siguiente tabla se resumen las configuraciones específicas de puertos que se necesitan.

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| SAP | Cualquiera | Servidor de aplicaciones Web de la Plataforma de BI | Puerto HTTP/HTTPS del servicio Web | Permitir |
| SAP | Cualquiera | CMS | Puerto del servidor de nombres del CMS | Permitir |
| SAP | Cualquiera | CMS | Puerto de solicitud del CMS | Permitir |
| Servidor de aplicaciones Web | Cualquiera | SAP | Puerto Servicio Gateway del Sistema SAP | Permitir |
| Servidor de administración central (CMS) | Cualquiera | SAP | Puerto Servicio Gateway del Sistema SAP | Permitir |
| Crystal Reports™ | Cualquiera | SAP | Puerto Servicio Gateway del sistema SAP y puerto Dispatcher del sistema SAP | Permitir |

## 8.19.2 Configuración del servidor de seguridad para la integración de JD Edwards EnterpriseOne

Los despliegues de la plataforma de BI que se comunicarán con el software de JD Edwards deben cumplir con estas reglas de comunicación generales:

- Las aplicaciones Web de la Consola de administración central deben poder iniciar la comunicación con JD Edwards EnterpriseOne a través del puerto JDENET y un puerto seleccionado aleatoriamente.
- Crystal Reports con el componente de cliente Conectividad de datos debe poder iniciar la comunicación con JD Edwards EnterpriseOne a través del puerto JDNET. Para recuperar datos, JD Edwards EnterpriseOne debe ser capaz de comunicarse con el controlador a través de un puerto aleatorio que no puede ser controlado.
- El Servidor de administración central debe poder iniciar la comunicación con JD Edwards EnterpriseOne a través del puerto JDENET y un puerto seleccionado aleatoriamente.

- El número del puerto JDENET se encuentra en el archivo de configuración del servidor de aplicaciones de JD Edwards EnterpriseOne, `JDE.INI`, en la sección JDENET.

## Requisitos de puerto para servidores de la Plataforma de BI

| Producto | Requisitos de puertos de servidor |
|---|---|
| Plataforma de SAP BusinessObjects Business Intelligence | Puerto del servidor de inicio de sesión de la Plataforma de BI |

## Requisitos de puerto para JD Edwards EnterpriseOne

| Producto | Requisito de puerto | Descripción |
|---|---|---|
| JD Edwards EnterpriseOne | Puerto JDENET y un puerto seleccionado aleatoriamente | Se usa para la comunicación entre la plataforma de BI y el servidor de aplicaciones de JD Edwards EnterpriseOne. |

## Configurar el servidor de aplicaciones Web para la comunicación con JD Edwards

En esta sección se muestra cómo configurar un servidor de seguridad y la plataforma de BI para que trabajen conjuntamente en un escenario de despliegue en el que el servidor de seguridad separa el servidor de aplicaciones Web de los otros servidores de la plataforma.

Para obtener la configuración del servidor de seguridad con los servidores y clientes de la Plataforma de BI, consulte la sección *Requisitos de puerto de la Plataforma de BI* de este manual. Además de la configuración del servidor de seguridad estándar, la comunicación con los servidores de JD Edwards necesita la apertura de algunos puertos adicionales.

Para JD Edwards EnterpriseOne Enterprise

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| CMS con la función Conectividad de seguridad para JD Edwards EnterpriseOne | Cualquiera | JD Edwards EnterpriseOne | Cualquiera | Permitir |
| Servidores de la Plataforma de BI con conectividad de datos para JD Edwards EnterpriseOne | Cualquiera | JD Edwards EnterpriseOne | Cualquiera | Permitir |
| Crystal Reports con la función Conectividad de datos desde el lado cliente para JD Edwards EnterpriseOne | Cualquiera | JD Edwards EnterpriseOne | Cualquiera | Permitir |

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| Servidor de aplicaciones Web | Cual-quiera | JD Edwards EnterpriseOne | Cualquiera | Permitir |

## 8.19.3 Directrices específicas del servidor de seguridad para Oracle EBS

El despliegue de la plataforma de BI debe permitir que los siguientes componentes inicien la comunicación con el puerto de escucha de la base de datos de Oracle.

- Componentes Web de la Plataforma BI
- CMS (específicamente el complemento de seguridad de Oracle EBS)
- Servidores backend de la Plataforma de BI (específicamente, el componente Acceso a datos EBS)
- Crystal Reports (específicamente el componente de acceso a datos EBS)

> **Nota**
>
> El valor predeterminado del puerto de escucha de la base de datos de Oracle en todos los casos anteriores es el 1521.

### 8.19.3.1 Requisitos detallados del puerto

Además de la configuración estándar del servidor de seguridad para la plataforma de BI, se deben abrir algunos puertos adicionales para que funcione en un entorno de Oracle EBS integrado:

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| Servidor de aplicaciones Web | Cual-quiera | Oracle EBS | Puerto de la base de datos de Oracle | Permitir |
| CMS con conectividad de seguridad para Oracle EBS | Cual-quiera | Oracle EBS | Puerto de la base de datos de Oracle | Permitir |
| Servidores de la Plataforma de BI con conectividad de datos en el servidor para Oracle EBS | Cual-quiera | Oracle EBS | Puerto de la base de datos de Oracle | Permitir |
| Crystal Reports con conectividad de datos en el cliente para Oracle EBS | Cual-quiera | Oracle EBS | Puerto de la base de datos de Oracle | Permitir |

## 8.19.4 Configuración del servidor de seguridad para la integración de PeopleSoft Enterprise

Los despliegues de la plataforma de BI que se comunicarán con PeopleSoft Enterprise deben cumplir las siguientes reglas de comunicación generales:

- El Servidor de administración central (CMS) con el componente Conectividad de seguridad debe ser capaz de iniciar una comunicación con el servicio Web de PeopleSoft Query Access (QAS).
- Los servidores de la Plataforma de BI con un componente Conectividad de datos deben ser capaces de inicializar la comunicación con el servicio Web de PeopleSoft QAS.
- Crystal Reports con componentes cliente de Conectividad de datos debe ser capaz de iniciar una comunicación con el servicio Web de PeopleSoft QAS.
- El puente de Enterprise Management (EPM) debe ser capaz de comunicarse con el Servidor de administración central y el Servidor del repositorio de archivos de entrada.
- El puente de EPM debe ser capaz de comunicarse con la base de datos de PeopleSoft a través de una conexión ODBC.

El número de puerto del servicio Web es el mismo que el especificado en el nombre de dominio de PeopleSoft Enterprise.

### Requisitos de puerto para servidores de la Plataforma de BI

| Producto | Requisitos de puertos de servidor |
|---|---|
| Plataforma de BI de SAP | Puerto del servidor de inicio de sesión de la Plataforma de BI |

### Requisitos de puertos de PeopleSoft

| Producto | Requisito de puerto | Descripción |
|---|---|---|
| PeopleSoft Enterprise: People Tools 8.46 o posterior | Puerto HTTP/HTTPS del servicio Web | Este puerto es necesario al usar la conexión SOAP con PeopleSoft Enterprise para People Tools 8.46 y soluciones posteriores |

### Configurar la Plataforma de BI y PeopleSoft para los servidores de seguridad

En esta sección se muestra cómo configurar la plataforma de BI y PeopleSoft Enterprise para que trabajen conjuntamente en un escenario de despliegue en el que el servidor de seguridad separa el servidor de aplicaciones Web de los otros servidores de la plataforma de BI.

Para obtener la configuración del servidor de seguridad con los servidores y clientes de la plataforma de BI, consulte el *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*.

Además de configurar el servidor de seguridad con la plataforma de BI, deberá realizar una configuración adicional.

Para PeopleSoft Enterprise: PeopleTools 8.46 o posterior

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| CMS con la función Conectividad de seguridad para PeopleSoft | Cualquiera | PeopleSoft | Puerto HTTP /HTTPS del servicio Web de PeopleSoft | Permitir |
| Servidores de la Plataforma de BI con conectividad de datos para PeopleSoft | Cualquiera | PeopleSoft | Puerto HTTP /HTTPS del servicio Web de PeopleSoft | Permitir |
| Crystal Reports con Conectividad de datos en el cliente para PeopleSoft | Cualquiera | PeopleSoft | Puerto HTTP /HTTPS del servicio Web de PeopleSoft | Permitir |
| Puente de EPM | Cualquiera | CMS | Puerto del servidor de nombres del CMS | Permitir |
| Puente de EPM | Cualquiera | CMS | Puerto de solicitud del CMS | Permitir |
| Puente de EPM | Cualquiera | Servidor del repositorio de archivos de entrada | Puerto del FRS de entrada | Permitir |
| Puente de EPM | Cualquiera | PeopleSoft | Puerto de base de datos de PeopleSoft | Permitir |

## 8.19.5 Configuración del servidor de seguridad para la integración de Siebel

En esta sección se muestran los puertos específicos que se usan para la comunicación entre los sistemas de aplicaciones de la plataforma de BI y Siebel eBusiness cuando están separados por servidores de seguridad.

- La aplicación Web debe ser capaz de iniciar la comunicación con el servidor de inicio de sesión único de la plataforma de BI para Siebel. Para el servidor de inicio de sesión empresarial para Siebel se necesitan tres puertos:
  1. El puerto Echo (TCP) 7 para comprobar el acceso al servidor de inicio de sesión.
  2. El servidor de inicio de sesión de la plataforma de BI para el puerto de Siebel (de forma predeterminada, 8448) para el puerto de escucha de CORBA IOR.
  3. Un puerto POA aleatorio para comunicaciones CORBA que no se pueda controlar y por lo tanto se deban abrir todos los puertos.
- El CMS debe poder inicializar la comunicación con el servidor de inicio de sesión de la Plataforma de BI para Siebel. Puerto de escucha IOR de CORBA configurado para cada servidor de inicio de sesión (por ejemplo, 8448). También tendrá que abrir un número de puerto POA aleatorio que no se conocerá hasta que se instale la plataforma de BI.
- El servidor de inicio de sesión de la Plataforma de BI para Siebel debe poder inicializar la comunicación con el puerto SCBroker (agente de conexión de Siebel) por ejemplo, 2321.
- Los servidores backend de la Plataforma de BI (componente de acceso a datos de Siebel) deben poder inicializar la comunicación con el puerto SCBroker (agente de conexión de Siebel) por ejemplo, 2321.

- Crystal Reports (componente de acceso a datos de Siebel) debe ser capaz de iniciar la comunicación con el puerto SCBroker (agente de conexión de Siebel) como, por ejemplo, 2321.

## Descripción detallada de los puertos

En esta sección se enumeran los puertos que la Plataforma de BI usa. Si despliega la plataforma de BI con servidores de seguridad, puede usar esta información para abrir el mínimo número de puertos en esos servidores de seguridad específicos para la integración con Siebel.

Requisitos de puerto para servidores de la Plataforma de BI

| Producto | Requisitos de puertos de servidor |
|---|---|
| Plataforma de BI de SAP | Puerto del servidor de inicio de sesión de la Plataforma de BI |

Requisito de puerto de Siebel

| Producto | Requisito de puerto | Descripción |
|---|---|---|
| Siebel eBusiness Application | 2321 | Puerto SCBroker predeterminado (agente de conexión de Siebel) |

## Configurar los servidores de seguridad de la Plataforma de BI para la integración con Siebel

En esta sección se muestra cómo configurar un servidor de seguridad para Siebel y la plataforma de BI para que trabajen conjuntamente en un escenario en el que el servidor de seguridad separa el servidor de aplicaciones web de los otros servidores de la plataforma.

| Equipo de origen | Puerto | Equipo de destino | Puerto | Acción |
|---|---|---|---|---|
| Servidor de aplicaciones Web | Cual-quiera | Servidor de inicio de sesión de la Plataforma de BI para Siebel | Cualquiera | Permitir |
| CMS | Cual-quiera | Servidor de inicio de sesión de la plataforma de BI para Siebel | Cualquiera | Permitir |
| Servidor de inicio de sesión de la plataforma de BI para Siebel | Cual-quiera | Siebel | Puerto SCBroker | Permitir |
| Servidores de la Plataforma de BI con conectividad de datos en el servidor para Siebel | Cual-quiera | Siebel | Puerto SCBroker | Permitir |
| Crystal Reports con Conectividad de datos en el cliente para Siebel | Cual-quiera | Siebel | Puerto SCBroker | Permitir |

## 8.20 Plataforma de BI y servidores proxy inversos

La plataforma de BI se puede desplegar en un entorno con uno o varios servidores proxy inversos. Los servidores proxy inversos suelen desplegarse delante del servidor de aplicaciones Web para ocultarlos detrás de una única dirección IP. Esta configuración enruta todo el tráfico de Internet dirigido a servidores de aplicaciones Web privados a través del servidor proxy inverso ocultando las direcciones IP privadas.

Debido a que el servidor proxy inverso traduce las direcciones URL públicas a direcciones URL internas, se debe configurar con las direcciones URL de las aplicaciones Web de la Plataforma de BI desplegadas en la red interna.

### 8.20.1 Comprender el modo en que se despliegan las aplicaciones Web

Las aplicaciones Web de la Plataforma de BI se despliegan en un servidor de aplicaciones Web. Las aplicaciones se implementan automáticamente durante la instalación a través de la herramienta WDeploy. La herramienta también se puede usar para desplegar las aplicaciones después de desplegar la plataforma de BI. Las aplicaciones Web se encuentran en el siguiente directorio en la instalación predeterminada de Windows:

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps
```

WDeploy se usa para desplegar archivos WAR como por ejemplo:

- `BOE`: incluye la Consola de administración central (CMC), la rampa de lanzamiento BI y Open Document
- `dswsbobje`: contiene la aplicación de servicios Web

Si el servidor de aplicaciones Web se encuentra detrás de un servidor proxy inverso, éste se debe configurar con las rutas de contexto correctas de los archivos WAR. Para exponer todas las funcionalidades de la Plataforma de BI, configure una ruta de contexto para cada archivo WAR de la Plataforma de BI que se despliega.

## 8.21 Configuración de servidores proxy inversos para las aplicaciones Web de la Plataforma de BI

El servidor proxy inverso se debe configurar para asignar las solicitudes de dirección URL entrantes a la aplicación Web correcta en aquellos despliegues en los que las aplicaciones Web de la Plataforma de BI se despliegan detrás de un servidor proxy inverso.

Esta sección contiene ejemplos de configuración específicos para algunos de los servidores proxy inversos compatibles. Consulte la documentación del proveedor de su servidor proxy inverso para obtener más información.

## 8.21.1 Instrucciones detalladas para configurar servidores proxy inversos

### Configurar los archivos WAR

Las aplicaciones Web de la Plataforma de BI se despliegan como archivos WAR en un servidor de aplicaciones Web. Asegúrese de que configura una directiva en el servidor proxy inverso para el archivo WAR necesario para el despliegue. Puede usar WDeploy para desplegar ya sea los archivos WAR `BOE` o `dswsbobje`. Para obtener más información acerca de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la Plataforma de BI*.

### Especifique las propiedades BOE en el directorio de configuración personalizado.

El archivo `BOE.war` incluye propiedades específicas globales y de aplicaciones. Si necesita modificar alguna de las propiedades use el directorio de configuración personalizada. De forma predeterminada, el directorio se encuentra en `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> ⚠ Precaución
>
> Para evitar que se sobrescriban archivos en el directorio predeterminado, no modifique las propiedades del directorio `config\default`. Los usuarios deberían usar el directorio `personalizado`.

> ⓘ Nota
>
> En algunos servidores de aplicaciones Web, como la versión de Tomcat en paquete con la plataforma de BI, puede acceder al archivo `BOE.war` directamente. En este escenario, puede configurar los ajustes personalizados directamente sin tener que anular el despliegue del archivo WAR. Cuando no se puede acceder al archivo `BOE.war`, debe anular el despliegue, personalizar y, a continuación, volver a desplegar el archivo.

### Uso consistente de barras (/)

Defina las rutas de contexto en el servidor proxy inverso de la misma manera que se escriben en una dirección URL del explorador. Por ejemplo, si la directiva contiene una barra diagonal (/) al final de la ruta reflejada en el servidor proxy inverso, introduzca una barra diagonal al final de la dirección URL del explorador.

Asegúrese de usar el carácter '/' de forma coherente en la dirección URL de origen y de destino en la directiva del servidor proxy inverso. Si el carácter '/' se agrega al final de la dirección URL de origen, también debe agregarse al final de la dirección URL de destino.

## 8.21.2 Para configurar el servidor proxy inverso

Los siguientes pasos son necesarios para que las aplicaciones Web de la Plataforma de BI funcionen en un servidor proxy inverso admitido.

1. Asegúrese de que el servidor proxy inverso se configure correctamente según las instrucciones del proveedor y la topología de red del despliegue.
2. Determine qué archivo WAR de la Plataforma de BI es necesario.
3. Configure el servidor proxy inverso para cada archivo WAR de la Plataforma de BI. Tenga en cuenta que las reglas se especifican de maneras distintas en cada tipo de servidor proxy inverso.
4. Lleve a cabo cualquier configuración especial que sea necesaria. Algunas aplicaciones Web requieren una configuración especial cuando se despliegan en determinados servidores de aplicaciones Web.

## 8.21.3 Configurar el servidor proxy inverso de Apache 2.2 para la plataforma de BI

En esta sección se proporciona un flujo de trabajo para configurar la plataforma de BI y Apache 2.2 para que funcionen conjuntamente.

1. Asegúrese de que la plataforma de BI y Apache 2.2 se instalan en equipos independientes.
2. Asegúrese de que Apache 2.2 se ha instalado y configurado como servidor proxy inverso, como se describe en la documentación del proveedor.
3. Configure el `ProxyPass` para cada archivo WAR que se despliegue detrás del servidor proxy inverso.
4. Abra el archivo *httpd.conf* que está ubicado en la carpeta de instalación proxy inverso de Apache.
5. Configure `ProxyPassReverseCookiePath` para cada aplicación Web implementada detrás del servidor proxy inverso. Por ejemplo:

```
ProxyPass /C1/BOE/ http://<appservername>:80/BOE/
ProxyPassReverseCookiePath /BOE/C1/BOE/
ProxyPassReverse /C1/BOE/ http://<appservername>:80/BOE/
ProxyPass /C1/explorer/ http://<appservername>:80/explorer/
ProxyPassReverseCookiePath /BOE/C1/explorer/
ProxyPassReverse /C1/explorer/ http://<appservername>:80/explorer/
```

## 8.21.4 Para configurar el servidor proxy inverso de WebSEAL 6.0 para la plataforma de BI

En esta sección se explica cómo configurar la plataforma de BI y WebSEAL 6.0 para que funcionen conjuntamente.

El método de configuración recomendado es crear una única unión estándar que asigne todas las aplicaciones Web de la Plataforma de BI alojadas en un servidor de aplicaciones Web o un servidor Web interno a un mismo punto de montaje.

1. Asegúrese de que la plataforma de BI y WebSEAL 6.0 se instalan en equipos independientes.

   Es posible, pero no se recomienda, desplegar la plataforma de BI y WebSEAL 6.0 en el mismo equipo. Consulte la documentación del proveedor de WebSEAL 6.0 para obtener las instrucciones acerca de la configuración de este escenario de despliegue.
2. Asegúrese de que WebSEAL 6.0 se ha instalado y configurado como se describe en la documentación del proveedor.
3. Inicie la utilidad de línea de comandos *pdadmin* de WebSEAL. Inicie sesión en un dominio seguro, por ejemplo, *sec_master*, como usuario con privilegios de administración.
4. Introduzca el siguiente comando en la secuencia de comandos *pdadmin sec_master*:

   ```
   server task <instance_name-webseald-host_name> create -t
   <type> -h <host_name> -p <port> <junction_point>
   ```

   Ubicación:

   - `<instance_name-webseald-host_name>` especifica el nombre de servidor completo de la instancia de WebSEAL instalada. Use este nombre de servidor completo con el mismo formato que se muestra en la salida del comando `server list`.
   - `<type>` especifica el tipo de unión. Use `tcp` si la unión se asigna a un puerto HTTP interno. Use `ssl` si la unión se asigna a un puerto HTTPS interno.
   - `<host_name>` especifica el nombre DNS del host o la dirección IP del servidor interno que recibirá las solicitudes.
   - `<port>` especifica el puerto TCP del servidor interno que recibirá las solicitudes.
   - `<junction_point>` especifica el directorio en el espacio protegido de WebSEAL donde se ha montado el espacio de documentos del servidor interno.

### Ejemplo

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

## 8.21.5 Configurar Microsoft ISA 2006 para la plataforma de BI

En esta sección se explica cómo configurar la plataforma de BI e ISA 2006 para que funcionen conjuntamente.

El método de configuración recomendado es crear una única unión estándar que asigne todos los archivos WAR de la Plataforma de BI alojados en un servidor de aplicaciones Web o un servidor Web interno a un mismo punto de montaje. Según su servidor de aplicaciones Web, se requiere configuración adicional en el servidor de aplicaciones para que funcione con ISA 2006.

1. Asegúrese de que la plataforma de BI e ISA 2006 se instalan en equipos independientes.

   Es posible, pero no se recomienda, desplegar la plataforma de BI e ISA 2006 en el mismo equipo. Consulte la documentación de ISA 2006 para obtener las instrucciones acerca de la configuración de este escenario de despliegue.

2. Asegúrese de que ISA 2006 se ha instalado y configurado, como se describe en la documentación del proveedor.
3. Inicie la utilidad de administración de ISA Server.
4. Utilice el panel de navegación para iniciar una nueva regla de publicación
   a. Vaya a

      *Matrices* > *NombreEquipo* > *Directiva de firewall* > *Nuevo* > *Regla de publicación de sitio web*

      > **→ Recuerde**
      >
      > Reemplace `NombreEquipo` por el nombre del equipo en el que está instalado ISA 2006.

   b. Escriba un nombre de regla en *Nombre de regla de publicación web* y haga clic en *Siguiente*
   c. Seleccione *Permitir* como la acción de red y haga clic en *Siguiente*.
   d. Seleccione *Publicar un solo sitio web o equilibrador de carga* como el tipo de publicación y haga clic en *Siguiente*.
   e. Seleccione un tipo de conexión entre ISA Server y el sitio Web publicado y haga clic en *Siguiente*.

      Por ejemplo, seleccione *Usar conexiones no seguras para conectar el servidor web publicado o granja de servidores*.
   f. Escriba el nombre interno del sitio Web que va a publicar (por ejemplo, el nombre del equipo que aloja la Plataforma de BI) en *Nombre de sitio interno* y haga clic en *Siguiente*.

      > **ⓘ Nota**
      >
      > Si el equipo que aloja ISA 2006 no se puede conectar al servidor de destino, seleccione *Usar un nombre de equipo o dirección IP para conectar con el servidor publicado* y escriba el nombre o la dirección IP en el campo proporcionado.

   g. En *Detalles de nombre público* seleccione el nombre de dominio (por ejemplo, *Cualquier nombre de dominio*) y especifique los detalles de publicación internos (por ejemplo, `/*`). Haga clic en *Siguiente*.
      Ahora debe crear un proceso de escucha para supervisar las solicitudes Web entrantes.
5. Haga clic en *Nuevo* para iniciar el asistente de definición de nueva escucha Web.
   a. Escriba un nombre en *Nombre de escucha web* y haga clic en *Siguiente*.
   b. Seleccione un tipo de conexión entre ISA Server y el sitio Web publicado y haga clic en *Siguiente*.

      Por ejemplo, seleccione *No requerir conexiones protegidas con SSL con clientes*.
   c. En la sección *Direcciones IP de escucha Web*, seleccione lo siguiente y haga clic en *Siguiente*.
      - Interfaz
      - Usuarios
      - Host local
      - Todas las redes

      ISA Server está configurado para publicar solo en HTTP.
   d. Seleccione una opción de *Configuración de autenticación*, haga clic en *Siguiente* y, a continuación, haga clic en *Finalizar*.
      El nuevo proceso de escucha ya está configurado para la regla de publicación de Web.
6. Haga clic en *Siguiente* en *Conjuntos de usuarios* y haga clic en *Finalizar*.
7. Haga clic en *Aplicar* para guardar toda la configuración de la regla de publicación Web y actualizar la configuración de ISA 2006.
   Ahora tiene que actualizar las propiedades de la regla de publicación Web para asignar rutas a las aplicaciones Web.

8. En el panel de navegación, haga clic con el botón derecho en la directiva de servidor de seguridad que ha configurado y seleccione *Propiedades*.
9. Seleccione la ficha *Rutas*, haga clic en *Agregar* para asignar rutas a las aplicaciones Web de SAP BusinessObjects.
10. En la ficha *Nombre público*, seleccione *Solicitar los siguientes sitios web* y haga clic en *Agregar*.
11. En el cuadro de diálogo *Nombre público*, escriba el nombre de usuario de servidor ISA 2006 y haga clic en *Aceptar*.
12. Haga clic en *Aplicar* para guardar toda la configuración de la regla de publicación Web y actualizar la configuración de ISA 2006.
13. Compruebe las conexiones accediendo a la siguiente dirección URL:

    **`http://<nombre de host de ISA Server>:<número de puerto de escucha Web>/<Ruta externa de la aplicación>`**

    Por ejemplo: **`http://myISAserver:80/Product/BOE/CMC`**

    > **Nota**
    >
    > Es posible que tenga que actualizar el explorador varias veces.

Debe modificar la directiva HTTP para la regla que acaba de configurar para asegurarse de que podrá iniciar sesión en la CMC. Haga clic con el botón derecho en la regla que ha creado en la utilidad de administración de ISA Server y seleccione *Configurar HTTP*. Ahora debe anular la selección de *Comprobar normalización* en el área *Protección de URL*.

Para acceder de forma remota a la plataforma de BI debe crear una regla de acceso.

## 8.22 Configuración especial para la plataforma de BI en despliegues de proxy inverso

Algunos productos de la Plataforma de BI necesitan configuraciones adicionales para funcionar correctamente en despliegues de proxy inverso. En esta sección se explica cómo realizar las configuraciones adicionales.

### 8.22.1 Habilitar el proxy inverso para los servicios Web

En esta sección se describen los procedimientos necesarios para habilitar los proxies inversos para los Servicios Web.

#### 8.22.1.1 Para habilitar el proxy inverso en Tomcat

Para habilitar el proxy inverso en el servidor de aplicaciones Web Tomcat, debe modificar el archivo `server.xml`. Las modificaciones necesarias incluyen configurar un.`proxyPort` como puerto de escucha del servidor proxy inverso y agregar un`proxyName` nuevo. En esta sección se explica el procedimiento.

1. Detenga Tomcat.
2. Abra el archivo `server.xml` para Tomcat.

   En Windows, `server.xml` se encuentra en: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf`

   En Unix `server.xml` se encuentra en `<CATALINA_HOME>/conf`. El valor predeterminado de `<INICIO_CATALINA>` es `<DIRINSTALACIÓN>/sap_bobj/tomcat`.
3. Localice esta sección en el archivo server.xml:

```
<!-- A "Connector" represents an endpoint by which requests are received
         and responses are returned. Documentation at :
         Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
         Java AJP  Connector: /docs/config/ajp.html
         APR (HTTP/AJP) Connector: /docs/apr.html
         Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" compression="on" URIEncoding="UTF-8"
compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata" compressableMimeType="text/html,text/xml,text/plain,text/css,text/
javascript,text/json,application/javascript,application/json"/>
```

4. Quite los comentarios del elemento Conector eliminando `<!--` y `-->`.
5. Modifique el valor de `proxyPort` para que sea el puerto de escucha del servidor proxy inverso.
6. Agregue un nuevo atributo `proxyName` a la lista de atributos del conector. El valor de `proxyName` debe ser el nombre del servidor proxy que Tomcat debería resolver a la dirección IP correcta.

   Ejemplo:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082 -->
                <!--See proxy documentation for more information about using
                  this.-->
                <Connector port="8082"
                maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
                enableLookups="false"
                acceptCount="100" debug="0"
connectionTimeout="20000"

proxyName="my_reverse_proxy_server.domain.com"
                proxyPort="ReverseProxyServerPort"
                disableUploadTimeout="true" />
```

   Donde `my_reverse_proxy_server.domain.com` y `ReverseProxyServerPort` se deben sustituir por el nombre de servidor proxy inverso correcto y su puerto de escucha.
7. Guarde y cierre el archivo `server.xml`.
8. Reinicie Tomcat.
9. Compruebe que el servidor proxy inverso asigna su ruta de acceso virtual al puerto de conector de Tomcat correcto. En el ejemplo anterior, el puerto es 8082.

   En el siguiente ejemplo se muestra una configuración de ejemplo de Apache HTTP Server 2.2 para el proxy inverso de los servicios Web de SAP Business Objects™ desplegados en Tomcat:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/
dswsbobje
                ProxyPassReverseCookiePath /dswsbobje /XI3.0/
dswsbobje
```

Para habilitar los servicios Web, se tienen que identificar el nombre de proxy y el número de puerto para el conector.

### 8.22.1.2 Habilitar el proxy inverso para los servicios Web en servidores de aplicaciones Web distintos de Tomcat

El siguiente procedimiento requiere que las aplicaciones Web de la Plataforma de BI se configuren correctamente respecto al servidor de aplicaciones Web escogido. Tenga en cuenta que `wsresources` distinguen entre mayúsculas y minúsculas.

1. Detenga el servidor de aplicaciones Web.
2. Especifique la dirección URL externa de los servicios Web en el archivo `dsws.properties`.

   Este archivo se encuentra en la aplicación Web `dswsbobje`. Por ejemplo, si la dirección URL externa es `http://my_reverse_proxy_server.domain.com/dswsbobje/`, actualice las propiedades en el archivo dsws.properties:

   - `wsresource1=ReportEngine|reportengine web service alone|http://mi_servidor_proxy_inverso.domain.com/SAP/dswsbobje/services/ReportEngine`
   - `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatalog`
   - `wsresource3=Publish|publish web service alone|http://mi_servidor_proxy_inverso.domain.com/SAP/dswsbobje/services/Publish`
   - `wsresource4=QueryService|query web service alone|http://mi_servidor_proxy_inverso.domain.com/SAP/dswsbobje/services/QueryService`
   - `wsresource5=BIPlatform|BIPlatform web service|http://mi_servidor_proxy_inverso.domain.com/SAP/dswsbobje/services/BIPlatform`
   - `wsresource6=LiveOffice|Live Office web service|http://mi_servidor_proxy_inverso.domain.com/SAP/dswsbobje/services/LiveOffice`
3. Guarde y cierre el archivo `dsws.properties`.
4. Reinicie el servidor de aplicaciones y Web.
5. Compruebe que el servidor proxy inverso asigna su ruta de acceso virtual al puerto de conector del servidor de aplicaciones Web correcto. En el siguiente ejemplo se muestra una configuración de ejemplo de Apache HTTP Server 2.2 para el proxy inverso de los servicios Web de la Plataforma de BI desplegados en el servidor de aplicaciones Web de su elección:

   ```
   ProxyPass /SAP/dswsbobje http://internalServer:<puerto de escucha> /dswsbobje
   ```

   ```
   ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
   ```

   Donde `<puerto de escucha>` es el puerto de escucha de su servidor de aplicaciones Web.

## 8.22.2 Activar la ruta raíz para las cookies de sesión para ISA 2006

En esta sección se describe cómo configurar servidores Web específicos para habilitar la ruta de raíz para que las cookies de sesión funcionen con ISA 2006 como el servidor proxy inverso.

### 8.22.2.1 Configurar Apache Tomcat

Para configurar la ruta raíz para que las cookies de sesión funcionen con ISA 2006 como el servidor proxy inverso, agregue lo siguiente al elemento `<Connector>` en `server.xml`:

```
emptySessionPath="true"
```

1. Detenga Tomcat.
2. Abra server.xml, que se encuentra en:

   `<CATALINA_HOME>\conf`
3. Identifique la sección siguiente en el archivo server.xml:

   ```
   <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
   <!-- See proxy documentation for more information about using this -->
   <!--
   <Connector port="8082"
   maxThreads="150" minSpareThreads="25" maxS
   pareThreads="75" enableLookups="false"
   acceptCount="100" debug="0" connectionTimeout="20000"
   proxyPort="80" disableUploadTimeout="true" />
   -->
   ```
4. Quite los comentarios del elemento Conector eliminando `<!--` y `-->`.
5. Para configurar la ruta raíz para que las cookies de sesión funcionen con ISA 2006 como el servidor proxy inverso, agregue lo siguiente al elemento `<Connector>` en `server.xml`:

   ```
   emptySessionPath="true"
   ```
6. Modifique el valor de `proxyPort` para que sea el puerto de escucha del servidor proxy inverso.
7. Agregue un nuevo atributo `proxyName` a la lista de atributos del conector. El valor debe ser el nombre del servidor proxy que Tomcat debe resolver en la dirección IP correcta.

   Por ejemplo:

   ```
   <!--Define a Proxied HTTP/1.1 Connector on port 8082
   -->
   <!-- See proxy documentation for more information about using
   this -->
   <Connector port="8082"
   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
   enableLookups="false" emptySessionPath="true"
   acceptCount="100" debug="0" connectionTimeout="20000"
   proxyName="my_reverse_proxy_server.domain.com"
   proxyPort="ReverseProxyServerPort"
   disableUploadTimeout="true" />
   ```
8. Guarde y cierre el archivo `server.xml`.

9. Reinicie Tomcat.

Compruebe que el servidor proxy inverso asigna su ruta de acceso virtual al puerto de conector de Tomcat correcto. En el ejemplo anterior, el puerto es 8082.

### 8.22.2.2 Para configurar Sun Java 8.2

Debe modificar `sun-web.xml` para cada aplicación Web de la Plataforma de BI.

1. Vaya a `<SUN_WEBAPP_DOMAIN>`\generated\xml\j2ee-modules\webapps\BOE\WEB-INF
2. Abra `sun-web.xml`
3. Después del contenedor `<context-root>` agregue lo siguiente:

```
        <session-config>
                <cookie-properties>
                        <property name="cookiePath" value="/" />
                </cookie-properties>
        </session-config>
   <property name="reuseSessionID" value="true"/>
```

4. Guarde y cierre `sun-web.xml`.
5. Repita los pasos 1-4 por cada aplicación Web.

### 8.22.2.3 Para configurar Oracle Application Server 10gR3

Debe modificar `global-web-application.xml` u `orion-web.xml` para cada directorio de despliegue de aplicación Web de la Plataforma de BI.

1. Vaya a `<ORACLE_HOME>\j2ee\home\config\`
2. Abra `global-web-application.xml` u `orion-web.xml`.
3. Agregue la siguiente línea al contenedor `<orion-web-app>`:

```
<session-tracking cookie-path="/" />
```

4. Guarde y cierre el archivo de configuración.
5. Inicie sesión en Oracle Admin Console:
   a. Vaya a *OC4J:home* > *Administración* > *Propiedades de servidor*.
   b. Seleccione *Options* (Opciones) en *Command Line Options* (Opciones de la línea de comandos).
   c. Haga clic en *Add another Row* (Agregar otra fila) y escriba lo siguiente:

```
Doracle.useSessionIDFromCookie=true
```

6. Reinicie el servidor Oracle.

### 8.22.2.4 Para configurar WebSphere Community Edition 2.0

1. Abra WebSphere Community Edition 2.0 Admin Console.
2. En el panel de navegación izquierdo, busque *Servidor* y seleccione *Servidor Web*.
3. Seleccione los conectores y haga clic en *Editar*.
4. Seleccione el cuadro de diálogo *emptySessionPath* y haga clic en *Guardar*.
5. Escriba el nombre del servidor ISA en*ProxyName*.
6. Escriba el número de puerto de escucha ISA en *ProxyPort*.
7. Detenga y, a continuación, reinicie el conecto.

## 8.22.3 Habilitar proxy inverso para SAP BusinessObjects Live Office

Para habilitar la función Ver objeto en el explorador Web de SAP BusinessObjects Live Office para los proxies inversos, ajuste la dirección URL del visor predeterminado. Esto se puede hacer en la Consola de administración central (CMC) o a través de las opciones de Live Office.

> **Nota**
>
> En esta sección se asume que los proxies inversos para la Plataforma de lanzamiento de BI y para los servicios Web de la Plataforma de BI se han habilitado correctamente.

### 8.22.3.1 Para ajustar la dirección URL del visor predeterminado en la CMC

1. Inicie una sesión en la CMC.
2. En la página *Aplicaciones*, haga clic en la *Consola de administración central*.
3. Seleccione *Acciones* > *Configuración de procesamiento*.
4. En el campo *URL*, seleccione la URL del visor predeterminado, y haga clic en *Guardar y cerrar*.
   Por ejemplo:

   ```
   http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?
   sIDType=CUID&iDocID=%SI_CUID%
   ```

   `ServidorProxyInverso` y `PuertoServidorProxyInverso` son el nombre del servidor proxy inverso correcto y su puerto de escucha.

# 9 Autenticación

## 9.1 Opciones de autenticación en la plataforma de BI

La autenticación es el proceso de verificación de la identidad de un usuario que intenta acceder al sistema, y la administración de derechos es el proceso de verificación de que se han concedido al usuario los derechos suficientes para realizar la acción solicitada en el objeto en cuestión.

Los complementos de seguridad expanden y personalizan los métodos de autenticación de usuarios de la plataforma de BI. Los complementos de seguridad facilitan la creación y administración de cuentas, ya que permiten asignar cuentas de usuario y grupos desde sistemas de terceros a la plataforma. Puede asignar cuentas de usuario de terceros o grupos en cuentas de usuario de la plataforma de BI o grupos existentes, o puede crear nuevas cuentas de usuario de Enterprise o grupos que se correspondan a cada entrada asignada en el sistema externo.

La versión actual admite los siguientes métodos de autenticación:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Debido a que la plataforma de BI se puede personalizar completamente, los procesos y la autenticación pueden variar de un sistema a otro.

### 9.1.1 Autenticación principal

La autenticación principal se lleva a cabo la primera vez que un usuario intenta obtener acceso al sistema. Una de las dos cosas que puede ocurrir durante la autenticación principal:

- Si no está configurado el inicio de sesión único, el usuario proporciona sus credenciales, como su nombre de usuario, contraseña y tipo de autenticación.
  Estos datos los especifican los usuarios en la pantalla de inicio de sesión.

  > **Nota**
  >
  > De forma predeterminada, solo se verifica la configuración de contraseña para incluir caracteres que combinan mayúsculas y minúsculas en las contraseñas, a menos que lo modifique el administrador. Esto requiere que la contraseña contenga como mínimo una mayúscula y una minúscula. En caso necesario, el administrador puede imponer ajustes adicionales para la contraseña.

- Si está configurado un método de inicio de sesión único, las credenciales de los usuarios se propagan en silencio.
  Estos detalles se extraen mediante otros métodos como Kerberos y SiteMinder.

El tipo de autenticación puede ser Enterprise, LDAP, Windows AD, SAP, Oracle EBS, Siebel, JD Edwards EnterpriseOne, PeopleSoft Enterprise dependiendo de los tipos que se hayan habilitado y configurado en el área de administración Autenticación de la Consola de administración central (CMC). El explorador Web del usuario envía la información por HTTP a su servidor Web, que dirige la información al CMS o al servidor de la plataforma apropiado.

El servidor de aplicaciones Web pasa la información del usuario mediante una secuencia de comandos en el servidor. Internamente, esta secuencia de comandos se comunica con el SDK y, al final, el complemento de seguridad apropiado para autenticar al usuario comparando sus datos con los de la base de datos de usuarios.

Por ejemplo, si el usuario inicia sesión en la Plataforma de lanzamiento de BI y especifica la autenticación de Enterprise, el SDK garantiza que el complemento de seguridad de la Plataforma de BI lleva a cabo la autenticación. El Servidor de administración central (CMS) usa el complemento de seguridad para verificar el nombre de usuario y la contraseña en la base de datos del sistema. Además, si el usuario especifica un método de autenticación diferente, el SDK usa el complemento de seguridad correspondiente para autenticar el usuario.

Si el complemento de seguridad informa de que los datos de las credenciales coinciden, el CMS concederá al usuario una identidad de sistema activa y se realizan las siguientes acciones:

- El CMS crea una sesión de Enterprise para el usuario. Mientras la sesión esté activa, utilizará una licencia de usuario en el sistema.
- El CMS genera y codifica un token de inicio de sesión y lo envía al servidor de aplicaciones Web.
- El servidor de aplicaciones Web almacena la información del usuario en memoria en una variable de sesión. Mientras está activa, esta sesión almacena información que permite a la Plataforma de BI responder a las solicitudes del usuario.

  > **Nota**
  >
  > La variable de sesión no contiene la contraseña del usuario.

- El servidor de aplicaciones Web mantiene el token de inicio de sesión en una cookie en el explorador del cliente. Sólo se usa con fines de conmutación por error, como cuando tiene un CMS en clúster en un clúster o cuando la plataforma de lanzamiento de BI se agrupa en un clúster para la afinidad de sesión.

  > **Nota**
  >
  > Es posible deshabilitar el token de inicio de sesión. De todos modos, si deshabilita el token de inicio de sesión, deshabilitará la conmutación por error.

## 9.1.2 Complementos de seguridad

Los complementos de seguridad expanden y personalizan los métodos de autenticación de usuarios de la plataforma de BI. La plataforma de BI se entrega con los siguientes complementos:

- Enterprise
- LDAP

- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Los complementos de seguridad facilitan la creación y administración de cuentas, ya que permiten asignar cuentas de usuario y grupos desde sistemas de terceros a la plataforma de BI. Puede asignar cuentas de usuario de terceros o grupos en cuentas de usuario de la plataforma de BI o grupos existentes, o puede crear nuevas cuentas de usuario de Enterprise o grupos que se correspondan a cada entrada asignada en el sistema externo.

Los componentes de seguridad mantienen dinámicamente listas de usuarios y grupos de terceros. Al asignar un grupo externo a la plataforma de BI, todos los usuarios que pertenecen a dicho grupo pueden iniciar sesión correctamente en la plataforma de BI. Cuando posteriormente realice cambios en la pertenencia al grupo de terceros, no tendrá que actualizar la lista de la plataforma de BI. Por ejemplo, si asigna un grupo de LDAP a la plataforma de BI y, a continuación, agrega un nuevo usuario al grupo, el complemento de seguridad crea dinámicamente un alias para el nuevo usuario cuando inicie sesión por primera vez en la plataforma de BI con credenciales LDAP válidas.

Además, los complementos de seguridad le permiten asignar derechos a usuarios y grupos de manera coherente, ya que los usuarios y grupos asignados son tratados como si fueran cuentas de Enterprise. Por ejemplo, puede asignar algunas cuentas de usuario o grupos desde Windows AD, y varias desde un servidor de directorios LDAP. A continuación, cuando tenga que asignar derechos o crear nuevos grupos personalizados en la plataforma de BI, realizará toda la configuración en la CMC.

Cada complemento de seguridad actúa como proveedor de autenticación que verifica las credenciales de los usuarios comparándolas con las de la base de datos de usuarios apropiada. Cuando los usuarios inicien sesión en la plataforma de BI, eligen entre los tipos disponibles de autenticación que se habilitaron y configuraron en el área de administración Autorización de la CMC.

> **Nota**
>
> El complemento de seguridad de Windows AD no puede autenticar usuarios si los componentes del servidor de la Plataforma de BI se están ejecutando en UNIX.

## 9.1.3 Inicio de sesión único en la plataforma de BI

El inicio de sesión único en la plataforma de BI significa que una vez que los usuarios han iniciado sesión en el sistema operativo, pueden acceder a las aplicaciones que admiten el SSO sin tener que proporcionar las credenciales de nuevo. Cuando un usuario inicia una sesión, se crea un contexto de seguridad para dicho usuario. Este contexto puede propagarse a la plataforma de BI para realizar el SSO.

El término «inicio de sesión único anónimo» también hace referencia al inicio de sesión único a la plataforma de BI, pero se refiere específicamente a la funcionalidad de inicio de sesión único para la cuenta de usuario Invitado. Cuando está habilitada la cuenta de usuario Invitado de forma predeterminada, cualquier persona puede iniciar sesión en la plataforma de BI como Invitado y tener acceso al sistema.

### 9.1.3.1 Compatibilidad con el inicio de sesión único

El término inicio de sesión único se utiliza para describir diferentes situaciones. En su nivel más básico, hace referencia a una situación en la que el usuario puede acceder a dos o más aplicaciones o sistemas proporcionando solo una vez sus credenciales de inicio de sesión, lo que facilita la interacción de los usuarios con el sistema.

La plataforma de BI u otras herramientas de autenticación distintas pueden proporcionar el inicio de sesión único en la plataforma de lanzamiento de BI dependiendo del tipo de servidor de aplicaciones y del sistema operativo.

Estos métodos de inicio de sesión único están disponibles si usa un servidor de aplicaciones Java en Windows:

- Windows AD con Kerberos
- Windows AD con SiteMinder

Estos métodos de inicio de sesión único están disponibles si usa IIS en Windows:

- Windows AD con Kerberos
- Windows AD con NTLM
- Windows AD con SiteMinder

Estos métodos de compatibilidad con el inicio de sesión único están disponibles en Windows o Unix, con cualquier servidor de aplicaciones Web admitido para la plataforma.

- LDAP con SiteMinder
- Autenticación con confianza
- Windows AD con Kerberos
- LDAP a través de Kerberos en SUSE 11
- SSO SAP NetWeaver a través de la autenticación de confianza

> **Nota**
>
> Windows AD con Kerberos se admite si la aplicación Java está en UNIX. Sin embargo, los servicios de la plataforma de BI se deben ejecutar en un servidor de Windows.

La siguiente tabla describe los métodos de la compatibilidad del inicio de sesión único para la plataforma de lanzamiento de BI.

| Modo de autenticación | Servidor CMS | Opciones | Notas |
|---|---|---|---|
| Windows AD | solo Windows | Sólo Windows AD con Kerberos | La autenticación de Windows AD para la plataforma de lanzamiento de BI y la CMC está disponible de serie. |
| LDAP | Cualquier plataforma compatible. | Se admiten los servidores de directorio LDAP, solo con SiteMinder | La autenticación de LDAP para la plataforma de lanzamiento de BI y la CMC está disponible de serie. El SSO en la plataforma de lanzamiento de NI y la CMC necesita SiteMinder. |

| Modo de autenticación | Servidor CMS | Opciones | Notas |
|---|---|---|---|
| Enterprise | Cualquier plataforma compatible. | Autenticación con confianza | La autenticación de Enterprise para la plataforma de lanzamiento de BI y la CMC está disponible de serie. El SSO con la autenticación de Enterprise en la plataforma de lanzamiento de BI y la CMC requiere la autenticación de confianza. |

#### 9.1.3.1.1 Habilitar el inicio de sesión único para CMC

Para habilitar SSO para CMC, siga los siguiente pasos:

En el lado del cliente, la caché debe borrarse antes de la configuración de CMC inicial. Además, la autenticación de Enterprise se grabará en caché.

En el servidor Tomcat, realice los pasos siguientes:

1. En un sistema ya configurado para SSO para ILP, vaya a `C:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\custom`.
2. Cree un archivo CmcApp.properties y la mención
   - sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter, trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela, trustedX509, sapSSO, siteminder
   - authentication.default=secWinAD

   en este archivo.
3. Reinicie tomcat.

   Se habilita SSO para CMC.

> **Nota**
>
> Después del límite de espera de la sesión de la plataforma de lanzamiento o CMC, cuando está habilitado SSO en ambos casos, se pedirá al usuario que se conecte. Al actualizar la página, el usuario vuelve a conectarse sin tener que proporcionar ninguna contraseña. No deberían deshabilitarse los registros de ping durante el proceso.

### 9.1.3.2 Inicio de sesión único en la base de datos

Después de que los usuarios hayan iniciado sesión en la plataforma de BI, el inicio de sesión único en base de datos les permite realizar acciones que precisan acceso a la base de datos, en particular, ver y actualizar informes, sin necesidad de volver a proporcionar sus credenciales de conexión. El inicio de sesión único en base de datos se puede combinar con el inicio de sesión único en la plataforma de BI para facilitar todavía más a los usuarios el acceso a los recursos que necesitan.

#### 9.1.3.3 Inicio de sesión único integral

El inicio de sesión único integral hace referencia a una configuración en la que los usuarios disponen de acceso de inicio de sesión único a la plataforma de BI en el primer plano y de acceso de inicio de sesión único a las bases de datos en el fondo. Así, los usuarios solo deben proporcionar sus credenciales de inicio de sesión una vez, cuando inician sesión en el sistema operativo, para acceder a la plataforma de BI y para poder realizar acciones que precisan el acceso a la base de datos, como la visualización de informes

En la plataforma de BI, el inicio de sesión único integral se admite a través de Windows AD y Kerberos.

## 9.2 Autenticación Enterprise

### 9.2.1 Información general de la autenticación Enterprise

La autenticación de Enterprise es el método de autenticación predeterminado para la plataforma de BI. Se activa automáticamente al instalar el sistema por primera vez (no se puede deshabilitar). Al agregar y administrar usuarios y grupos, la plataforma mantiene la información de usuario y grupo dentro de su base de datos.

> → Sugerencias
>
> Use la autenticación Enterprise predeterminada del sistema si prefiere crear cuentas y grupos distintivos para usarlos con la plataforma de BI, o si aún no ha configurado una jerarquía de usuarios y grupos en un servidor de directorio de terceros.
>
> No tiene que configurar o habilitar la autenticación Enterprise. Sin embargo, puede modificar la configuración de autenticación Enterprise para cumplir con los requisitos de seguridad concretos de la organización. Solo se puede modificar la configuración de autenticación de Enterprise a través de la Consola de administración central (CMC).

### 9.2.2 Configuración de la autenticación Enterprise

| Parámetros | Opciones | Descripción |
|---|---|---|
| *Restricciones de contraseña* | *Exigir contraseñas con minúsculas y mayúsculas* | Esta opción garantiza que las contraseñas contienen como mínimo una mayúscula y una minúscula.<br>**ⓘ Nota**<br>De forma predeterminada se selecciona esta opción. Si es necesario, el administrador puede desmarcarla. |

| Parámetros | Opciones | Descripción |
|---|---|---|
| | *Exigir numeral(es) en la contraseña* | Esta opción asegura que las contraseñas contienen como mínimo un carácter numérico. |
| | *Exigir carácter(es) especial(es) en la contraseña* | Esta opción asegura que las contraseñas contienen como mínimo un carácter especial. |
| | *Debe contener como mínimo N caracteres, donde N es* | Esta opción garantiza que las contraseñas tengan al menos N caracteres de largo. |
| | *No puede superar los N caracteres, donde N es* | Esta opción garantiza que las contraseñas no deben superar los N caracteres. |
| | *No debe contener las siguientes secuencias de caracteres* | Esta opción garantiza que la contraseña no deba contener secuencias de caracteres restringidas. El valor predeterminado para este fin es el siguiente: Contraseña 12345678 administrador. |
| *Restricciones de usuario* | *Debe cambiar la contraseña cada N días* | Esta opción asegura que las contraseñas no son una responsabilidad y se actualizan regularmente. |
| | *No puede volver a usar las últimas N contraseñas* | Esta opción asegura que las contraseñas no se repetirán de forma rutinaria. |
| | *Debe esperar N minutos para cambiar la contraseña* | Esta opción asegura que las nuevas contraseñas no se pueden cambiar inmediatamente cuando se introducen en el sistema. |
| | *Debe cambiar la contraseña después de N día(s) de inactividad* | Esta opción garantiza que la contraseña deba cambiar después de N días de inactividad. |
| | *Debe cambiar la contraseña inicial después de N día(s)* | Esta opción garantiza que la contraseña inicial cambie después de N días |
| *Restricciones de conexión* | *Deshabilitar la cuenta tras N intentos de conexión* | Esta opción de seguridad especifica la cantidad de intentos que se permiten a un usuario para iniciar sesión en el sistema antes de que se deshabilite la cuenta. |
| | *Restablecer conexión fallida después de N minutos* | Esta opción especifica el intervalo de tiempo para restablecer el contador de intentos de inicio de sesión. |
| | *Restablecer conexión fallida después de N minutos* | Esta opción determina cuánto tiempo se suspende una cuenta después de N intentos de inicio de sesión fallidos. |

| Parámetros | Opciones | Descripción |
|---|---|---|
| *Sincronizar credenciales de origen de datos con inicio de sesión* | *Habilitar y actualizar las credenciales de origen de datos del usuario en el tiempo de inicio de sesión* | Esta opción habilita las credenciales de origen de datos después de que el usuario haya iniciado sesión. |
| *Autenticación con confianza* | *Autenticación con confianza activada* | Proporciona los ajustes para configurar la Autenticación con confianza. |
| *Autenticación de OpenID Connect* | *La autenticación de OpenID Connect está activada* | Para activar la *autenticación de OpenID Connect*, marque la casilla de selección *La autenticación de OpenID Connect está activada*. Al autenticar mediante OpenID Connect, se crea una sesión interna de Enterprise en la plataforma de BI. |

## 9.2.3 Cambiar la configuración de Enterprise

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *Enterprise*.
   Aparecerá el cuadro de diálogo *Enterprise*.
3. Cambie la configuración.

   > → Sugerencias
   >
   > Para revertir toda la configuración al valor predeterminado, haga clic en *Restablecer*.

4. Haga clic en *Actualizar* para guardar las modificaciones.

### 9.2.3.1 Cambiar la configuración de contraseña general

> ⓘ Nota
>
> Las cuentas que no se usan durante un período prolongado no se desactivan automáticamente. Los administradores tienen que suprimir las cuentas inactivas manualmente.

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *Enterprise*.
   Aparecerá el cuadro de diálogo *Enterprise*.
3. Seleccione la casilla de verificación asociada a cada configuración de contraseña que desee utilizar y, en caso necesario, proporcione un valor.

   En la siguiente tabla se identifican los valores mínimo y máximo para cada una de las configuraciones relacionadas con contraseñas que se pueden efectuar.

| Opción de la contraseña | Predeterminado | Mínimo | Máximo recomendado |
|---|---|---|---|
| *No debe contener las siguientes secuencias de caracteres* | contraseña 12345678 administrador | 1 carácter | 25550 caracteres |
| *Debe contener al menos N caracteres* | 8 caracteres | 6 caracteres | 255 caracteres |
| *No debe superar los N caracteres* | 255 caracteres | 13 caracteres | 255 caracteres |
| *Debe cambiar la contraseña cada N días* | 30 días | 2 días | 100 días |
| *No puede volver a usar las últimas N contraseñas* | 3 contraseñas | 1 contraseña | 100 contraseñas |
| *Debe esperar N minutos para cambiar la contraseña* | 0 minutos | 0 minutos | 100 minutos |
| *Debe cambiar la contraseña después de N día(s) de inactividad* | 20 días | 2 días | 365 días |
| *Debe cambiar la contraseña inicial después de N día(s)* | 7 días | 2 días | 15 días |
| *Deshabilitar la cuenta tras N intentos fallidos de conexión* | 10 fallido | 1 fallido | 100 fallidos |
| *Restablecer conexión fallida después de N minutos* | 5 minutos | 1 minuto | 100 minutos |
| *Reactivar la cuenta después de N minutos* | 5 minutos | 0 minutos | 100 minutos |

4. Haga clic en *Actualizar*.

## 9.2.4 Autenticación SAML 2.0

### 9.2.4.1 Para conseguir Single Sign-On mediante SAML 2.0

La Plataforma de Business Intelligence puede integrarse a cualquier portal o aplicación habilitada con SAML, como un mecanismo de autentificación para la experiencia de Single Sign-On. Esto significa que ahora puede iniciar sesión en una aplicación en la nube como Analytics Hub o SAP Analytics Cloud y acceder a los recursos de aplicaciones de BI como la rampa de lanzamiento BI de Fiori u Open Document durante la misma sesión de trabajo.

Tiene que configurar el servidor de aplicación para conseguir Single Sign-On mediante SAML 2.0.

> **Nota**
>
> Configure los siguientes requisitos previos para utilizar la función de autenticación SAML al iniciar sesión mediante la dirección de correo electrónico de:
>
> - usuarios externos.
>  Utilice el parámetro de línea de comandos `"-importtpemailduringsync"` para activar la importación de direcciones de correo electrónico a partir de un sistema externo:
>  1. Añada el parámetro `"-importtpemailduringsync"` a *CMS* > *propiedades* > *Parámetros de línea de comandos*.
>  2. Reinicie el CMS.
>  3. Actualice la autentificación de terceros cuyo correo electrónico del usuario desee utilizar para iniciar sesión.
>
>  Los tipos de autenticación de terceros compatibles con esta característica son SAP, LDAP y WinAD.
> - Usuarios empresariales.
>  Consulte la nota SAP 2642247.

### 9.2.4.2 Configuración de la plataforma de BI como proveedor de servicios SAML

Para usar la plataforma de BI como proveedor de servicios de SAML, debe configurarla para la autenticación de SAML 2.0.

En esta versión se han simplificado los pasos para configurar un servidor de aplicaciones como proveedor de servicios SAML. Se han eliminado los siguientes pasos como parte de esta simplificación:

- Copiar archivos JAR SAML en el directorio de instalación de la plataforma de BI
- Editar el archivo securitycontext.xml
- Editar el archivo web.xml

Esto significa que los archivos JAR SAML, las etiquetas XML de cada aplicación web en el archivo securitycontext.xml y filtros en el archivo web.xml están disponibles por defecto. Por este motivo, después de seguir los pasos siguientes, puede habilitar o deshabilitar la autenticación SAML 2.0 para cada aplicación Web a través del fichero de propiedades de cada aplicación Web.

> **Nota**
>
> Utilice el proveedor SAP Cloud Identity como proveedor de identidades por defecto.

> **Nota**
>
> Puede utilizar los servidores de aplicaciones Tomcat, WebSphere y Jboss como proveedor de servicios SAML.

1. Siga el procedimiento de Configuración de la autenticación de confianza con sesiones Web [página 249].
2. Si está utilizando el proveedor SAP Cloud Platform Identity, exporte todos los usuarios y luego impórtelos a la plataforma BI. Consulte Cómo importar usuarios en masa desde la consola de administración central.

Para exportar usuarios de SAP Cloud Platform a CSV, consulte Exportar usuarios existentes de un arrendatario del servicio de autentificación de SAP Cloud Platform Identity

3. Edite el archivo de propiedades modificando `logon.webssoauthnetication.framework=None` por `logon.webssoauthnetication.framework=SAML`.
   - Para la plataforma de lanzamiento BI de Fiori, vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` y edite el archivo `fioriBI.properties`.
   - Para Open Document, vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` y edite el archivo `OpenDocument.properties`.
   - Para CMC, vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` y edite el archivo `CMCApp.properties`.

   > **Nota**
   >
   > Además de añadir `saml.enabled=true`, fije la propiedad `sso.supported.types = trustedSession` en los archivos de propiedad `CMC\FioriBI\OpenDocument`.

4. Para actualizar los metadatos IDP en SP, primero descargue los metadatos de los proveedores de servicio respectivos, copie el archivo de metadatos en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF` y modifique el nombre a `idp-meta-downloaded.xml`.

   Para más detalles sobre la descarga de los metadatos IDP, consulte Configuración de arrendatario SAML 2.0.

   > **Nota**
   >
   > Si la plataforma de BI está desplegada en una máquina no Windows, debe modificar los separadores de la vía de acceso a los metadatos IDP bajo el bean **FilesystemMetadataProvider** en el archivo `securityContext.xml` bajo `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
   >
   > Por ejemplo, cambie `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` a `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

   Si desea generar un almacén de claves para la activación de SAML 2.0, consulte Generar un keystore para SAML 2.0 [página 249].

5. (Opcional) Puede utilizar la dirección de correo electrónico como un atributo de aserción SAML. Consulte el tema Para utilizar la dirección de correo electrónico como atributo de aserción SAML [página 251] para obtener más información.
6. (Opcional) Si utiliza un equilibrador de carga o un servidor proxy inverso, consulte 2621904 para obtener más información.
7. Cree el archivo WAR con la herramienta wdeploy.
   a. Navegue hasta el directorio `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Utilice el comando de despliegue apropiado para crear el fichero war para versiones específicas de la aplicación.

   - Para Windows: `wdeploy.bat <App_Server_Name><Version_Name> -DAPP=BOE predeploy`
   - Para UNIX: `wdeploy.sh <App_Server_Name><Version_Name> -DAPP=BOE predeploy`

> **Nota**
>
> Debería sustituir <App_Server><Version_Name> con el tipo de servidor de aplicación y su versión. Por ejemplo, puede utilizar tomcat8 para el servidor de aplicaciones Tomcat v8.0. Del mismo modo, puede utilizar jboss7 para el servidor de aplicaciones JBoss v7.0 y websphere9 para el servidor de aplicaciones WebSphere v9.0.

8. Una vez que el archivo WAR se haya creado, copie el archivo WAR e impleméntelo en su servidor de aplicaciones.
9. Genere y cargue los metadatos de proveedor de servicios.

> **Nota**
>
> Puede definir la URL base de la entidad de propiedades en el archivo securitycontext.xml para generar los metadatos del proveedor de servicios con su URL de punto final. Por defecto, se tienen en cuenta el nombre de host y el número de puerto que se proporcionan en la URL para descargar los metadatos del proveedor de servicios.

   a. Vaya a `http(s)://host:port/BOE/saml/metadata`.

      El fichero XML se descarga automáticamente.
   b. Cargue el archivo XML en el proveedor de identidades. Si usa Microsoft Active Directory Federation Services como el proveedor de identidad, entonces consulte Crear emisor de confianza [página 252] para obtener más información.

> **Nota**
>
> Puede utilizar el archivo de metadatos de proveedor de servicios estándar `spring_saml_metadata.xml` ubicado en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`, en vez de generarlo manualmente. Debe sustituir la etiqueta XML`<replace_withip>` con la dirección IP o el nombre de host del equipo basado en su red y `<replace_withport>` , con el número de puerto del servidor de un servidor de aplicación. Sustituya HTTP con HTTPS si ha activado HTTPS en el servidor de aplicación.

10. Si está utilizando SAP Cloud Identity, para crear una aplicación SAML en IDP y cargue el SP `metadata.xml` en el IDP para configurar SAML SSO para la plataforma de BI, consulte Configurar un proveedor de servicios de confianza.

> **Nota**
>
> Deberá generar los metadatos del proveedor de servicios más recientes después de modificar el archivo de almacén de claves.

> **→ Sugerencias**
>
> Para permitirle verificar si la integración SAML es correcta, una vez que inicie la aplicación SAML configurada (plataforma de lanzamiento de BI, plataforma de lanzamiento de BI de Fiori u OpenDocument), se le redirigirá al IDP.

### 9.2.4.2.1 Configuración de la autenticación de confianza con sesiones Web

Debe configurar la autenticación de confianza con sesiones Web como parte de la configuración de un servidor de aplicación como un proveedor de servicios SAML.

> **Nota**
>
> No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

1. Cree el archivo `global.properties` bajo la carpeta personalizada `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.
2. Introduzca como contenido del archivo `global.properties` :

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=MyUser
   trusted.auth.shared.secret=MySecret
   ```

   > **Nota**
   >
   > Debe asegurarse de actualizar los mismos valores para `trusted.auth.user.param` y parámetros `trusted.auth.shared.secret` en el archivo *custom.jsp*.

3. Vaya a *CMC* > *Autentificación* > *Empresa* .
4. Definir un valor de 0 a 365 (en términos de *días*) como la *validez*.
5. Seleccione *Nuevo secreto compartido*.
6. Para descargar el secreto compartido generado, seleccione *Descargar secreto compartido*.

   El archivo `TrustedPrincipal.conf` se descarga.
7. Copie y pegue el archivo `TrustedPrincipal.conf` en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` y `\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
8. Vaya a *CMC* > *Autentificación* > *Empresa* y seleccione *Actualizar*.
9. Actualice el archivo custom.jsp con el valor clave de secreto compartido para la plataforma de lanzamiento de BI y de Fiori clásica y la plataforma de lanzamiento de BI de Fiori. Para obtener más información, vea Edición del archivo custom.jsp [página 407] .

   > **Nota**
   >
   > Debe actualizar el archivo .jsp personalizado si está usando Micrsoft ADFS y Microsoft Azure como proveedor de identidad.

### 9.2.4.2.2 Generar un keystore para SAML 2.0

Para usar su propio archivo keystore para SAML 2.0 se necesita una generación.

El intercambio SAML utiliza la criptografía para firmar y cifrar datos. Un archivo keystore autofirmado modelo, `sampletestKeystore.jks`,está empaquetado con el producto y es válido hasta el 18 de octubre de 2019. `sampletestKeystore.jks` tiene un nombre de alias **Testkey**y contraseña **Password1**.

Ahora puede generar un archivo keystore autofirmado utilizando la herramienta clave de utilidad JAVA.

1. Navegue a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`.
2. Ejecute el comando:`keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

| Comando | Descripción |
|---|---|
| -alias | Introduzca el alias del certificado |
| -keypass | Introduzca la contraseña del certificado |
| -keystore | Nombre del archivo keystore |
| -validity | Validez del certificado |
| numberofdays | Cantidad de días en los que es válido el certificado autofirmado. |

Responda a las siguientes preguntas después de ejecutar el comando:

- Introduzca la contraseña del keystore: *****
- Vuelva a introducir la contraseña: *****
- ¿Cuáles son su nombre y apellidos? : **`MY_FIRST_AND_LAST_NAME`**
- ¿Cuál es el nombre de su unidad organizativa? : **`MY_ORGANIZATIONAL_UNIT`**
- ¿Cuál es el nombre de su organización? : **`MY_ORGANIZATION`**
- ¿Cuál es el nombre de su población o localidad? : **`MY_CITY`**
- ¿Cuál es el nombre de su comunidad autónoma o provincia? : **`MY_STATE`**
- ¿Cuál es el código del país de dos letras para esta unidad? : **`COUNTRY_CODE`**

Se ha generado el archivo keystore en `INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin.`

3. Desplace el archivo keystore a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
4. Edite el archivo `securityContext.xml` ubicado en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\` con alias, contraseña y nombre de archivo keystore nuevos.

   Consulte el código XML a continuación:

   **Código de ejemplo**

```
<bean id="keyManager"
class="org.springframework.security.saml.key.JKSKeyManager">
<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
```

```
<constructor-arg type="java.lang.String" value="Password1"/>
<constructor-arg>
<map>
<entry key="aliasname" value="password"/>
</map>
</constructor-arg>
<constructor-arg type="java.lang.String" value="Testkey"/>
</bean>
```

Consulte la tabla siguiente para comprender los argumentos:

| Etiqueta XML | Descripción |
|---|---|
| `<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>` | Localiza el archivo keystore. |
| `<constructor-arg type="java.lang.String" value="Password1"/>` | Contraseña del archivo keystore. |
| `<entry key="aliasname" value="password"/>` | Alias y contraseña |
| `<constructor-arg type="java.lang.String" value="Testkey"/>` | Alias del certificado por defecto |

### 9.2.4.2.3 Para utilizar la dirección de correo electrónico como atributo de aserción SAML

Puede habilitar la autenticación de correo electrónico en SAML para la plataforma de lanzamiento de BI de Fiori, OpenDocument y la Consola de administración central (CMC).

1. En función de la aplicación en la que trabaja, edite el archivo de propiedades correspondiente sumando estas dos líneas:

```
saml.enabled=true
saml.isUseEmailAddress=true
saml.authType=secEnterprise
```

> **Nota**
>
> `saml.isUseEmailAddress` toma valores booleanos y `saml.authType` corresponde al tipo de autenticación de los detalles de usuario/alias con los que se espera que se realice el inicio de sesión. La función de correo electrónico se puede tratar individualmente para cada una de las aplicaciones enumeradas anteriormente. Si `saml.isUseEmailAddress` está definido como `false`, el inicio de sesión se realiza según el parámetro del nombre. Si se define como `true`, el inicio de sesión se realiza según el parámetro de correo electrónico. `saml.authType` comprueba si hay posibles duplicados y garantiza que dos alias con el mismo tipo de autenticación no tengan la misma dirección de correo electrónico.

- Para la plataforma de lanzamiento de BI de tipo Fiori, `fioriBI.properties` en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`
- Para Opendocument, `OpenDocument.properties` en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`
- Para la CMC, `CMCApp.properties` en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`

> **Nota**
>
> Para la CMC, asegúrese de establecer la propiedad `sso.supported.types = trustedSession` en el archivo `CMCApp.properties`.

2. Configure IDP para obtener compatibilidad para correo electrónico. También puede consultar la Guía del servicio SAP Cloud Platform Identity Authentication para obtener más información si usa SAP Cloud Identity Provider.
   a. Acceda a la URL de consola de administración del arrendatario del servicio SAP Cloud Platform Identity Authentication.

   > **Nota**
   >
   > La URL tiene el formulario `https://<tenant ID>.accounts.ondemand.com/admin`. El sistema genera automáticamente el ID de arrendatario. El primer administrador creado para el arrendatario recibe un correo electrónico de activación con una URL que contiene el ID de arrendatario.

   b. Seleccione *Aplicaciones*.
   c. Seleccione una aplicación.
   d. En la pestaña *De confianza*, en la sección *SAML 2.0*, haga clic en *Atributo de ID de nombre*.
   e. Seleccione *Correo electrónico*.
   f. Haga clic en *Guardar*.

## 9.2.4.2.4 Crear emisor de confianza

Debe crear un emisor de confirmar y una regla de reclamación en la herramienta de gestión Michrosoft ADFS para actualizar los metadatos del proveedor de servicios.

1. Inicie el *administrador de servidores*.
2. Vaya a *Herramientas* > *AD FS Management*.
3. Expanda las *relaciones de confianza*.
4. Haga clic con el botón derecho *Crear emisor de confianza* y seleccione *Añadir emisor de confianza*.
5. En el asistente *Añadir emisor de confianza* , seleccione *Iniciar*.
6. Seleccione *Importar datos sobre el emisor de confianza desde el archivo* y seleccione *Explorar*.
7. Navegue hasta el archivo de metadatos del proveedor de servicios descargado y selecciónelo.
8. Seleccione *Siguiente*.
9. Introduzca el *Nombre de visualización* y seleccione *Siguiente*.
10. En el paso *¿Configurar autenticación de multifactor ahora?*, seleccione *Siguiente*.

11. Seleccione *Permitir a todos los usuarios acceder a este usuario autenticado* y seleccione *Siguiente*.
12. Revise la información en la pantalla *Listo para añadir confianza* y seleccione *Siguiente*.
13. Seleccione *Finalizar*.
    Aparece el cuadro de diálogo *Editar reglas de reclamación* . Puede crear reglas de reclamación con el nombre de usuario o dirección de correo electrónico como un atributo.

Ha creado un emisor de confianza con éxito.

## 9.2.4.2.4.1 Creación de una regla de reclamación con nombre de usuario como atributo

Puede crear una regla de reclamación con nombre de usuario como un atributo de una aserción SAML

Una relación de confianza para usuarios autenticados debería estar disponible.

1. En el cuadro de diálogo *Editar reglas de reclamación*, seleccione *Añadir regla*.
2. En *Añadir asistente de regla reclamación de transformación* seleccione *Enviar los atributos LDAP como créditos* y seleccione *Siguiente*.
3. Introduzca el *nombre de la regla de reclamación* y seleccione *Directorio activo* como *Tienda de atributo*.
4. Bajo *Atributo LDAP*, seleccione *Nombre de cuenta SAM*.
5. Bajo *Tipo de reclamación saliente* seleccione *ID de nombre*.
6. Seleccione *Finalizar*.

La regla de reclamación se crear para el nombre de usuario como un atributo.

## 9.2.4.2.4.2 Creación de una regla de reclamación con dirección de correo electrónico como atributo

Debe crear dos reglas de reclamación para utilizar una dirección de correo electrónico como una aserción de atributo SAML.

1. En el cuadro de diálogo *Editar reglas de reclamación*, seleccione *Añadir regla*.
2. En *Añadir asistente de regla reclamación de transformación*, seleccione *Enviar atributos LDAP como reclamaciones* y seleccione *Siguiente*.
3. Introduzca el *Nombre de la regla de reclamación* y seleccione *Directorio activo* como *Tienda de atributo*.
4. Bajo *Atributo LDAP*, seleccione *Direcciones de correo electrónico* y a continuación, en *Tipo de reclamación saliente*, seleccione *Dirección de correo electrónico*.
5. En la segunda entrada, bajo *Atributo LDAP*, seleccione *Nombre asignado* y, a continuación, en *Tipo de reclamación saliente*, escriba el *Nombre*.
6. Seleccione *Finalizar*.

   Ha creado la primera regla. Siga los pasos a continuación para crear una segunda regla de reclamación.
7. En el cuadro de diálogo*Editar reglas de reclamación* , seleccione *Añadir regla*.
8. En el *Añadir asistente de regla reclamación de reclamación* , seleccione *Transferir una reclamación entrante* y seleccione *Siguiente*.

9. Introduzca el *Nombre de regla de reclamación*, seleccione *Dirección de correo electrónico* como *Tipo de reclamación entrante*, *ID de nombre* como *Tipo de reclamación de salida* y *Correo electrónico* como *Formato de nombre de salida*.
10. Seleccione *Finalizar*.

### 9.2.4.3 Utilizar servidor de aplicación WebSphere como proveedor de servicios SAML

El tema contiene instrucciones para configurar el servidor de aplicación WebSphere para la autentificación SAML 2.0.

> **Nota**
>
> Los pasos mencionados a continuación utilizan el proveedor SAP Cloud Identity como proveedor de identidades por defecto.

Siga los siguientes pasos:

1. Copie los archivos JAR SAML presentes en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\SAMLJARS` en `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF\lib`.
2. Para configurar la autenticación de confianza con la sesión web, siga estos pasos:
   1. Añada el archivo global.properties a la carpeta custom `<WebSphere_InstallDir>\WebSphere\\AppServer\profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF\config\custom`. A continuación encontrará el contenido de las propiedades globales:
      ```
      sso.enabled=true
      trusted.auth.user.retrieval=WEB_SESSION
      trusted.auth.user.param=UserName
      ```
   2. Vaya a *CMC* > *Autentificación* > *Empresa*.
   3. Habilite la *autenticación de confianza*.
   4. Establezca la *validez*.
   5. Seleccione *Nuevo secreto compartido*.
   6. Para descargar el secreto compartido generado, seleccione *Descargar secreto compartido*.
      <El archivo `TrustedPrincipal.conf` se descarga.
   7. Pegue el archivo TrustedPrincipal.conf en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` y en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
   8. Vaya a *CMC* > *Autenticación* > *Empresa* y seleccione *Actualizar*.
   9. Reinicie el servidor de aplicaciones WebSphere.
3. Si está utilizando el proveedor SAP Cloud Platform Identity, exporte todos los usuarios y luego impórtelos a la plataforma BI. Consulte Cómo importar usuarios en masa desde la consola de administración central

   Para exportar usuarios de SAP Cloud Platform a CSV, consulte Exportar usuarios existentes de un arrendatario del servicio de autentificación de SAP Cloud Platform Identity
4. Edite el archivo de propiedades añadiendo `saml.enabled=true`. Consulte los nombres de archivo y su ubicación a continuación:

1. Para la plataforma de lanzamiento BI de Fiori, vaya a `<WebSphere_InstallDir>\WebSphere\AppServer\Profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF\config\custom` y edite el archivo *fioriBI.properties*.
2. Para Open Document, vaya a `<WebSphere_InstallDir>\WebSphere\AppServer\Profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF\config\custom` y edite el archivo *OpenDocument.properties*.
3. Para CMC, vaya a `<WebSphere_InstallDir>\WebSphere\AppServer\Profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF\config\custom` y edite el archivo *CMCApp.properties*.

> **Nota**
>
> Para CMC, debería configurar otra propiedad `sso.supported.types = trustedSession` en el archivo *CMCApp.properties*.

> **Nota**
>
> Si la aplicación no contiene las propiedades personalizadas, cree uno nuevo.

5. Para actualizar los metadatos IDP en SP, descargue los metadatos IDP de los proveedores de servicios IDP correspondientes. Copie el archivo de metadatos en `<WebSphere_InstallDir>\WebSphere\AppServer\profile\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF` y cámbiele el nombre por **idp-meta-downloaded.xml**. Para obtener más información sobre cómo descargar los metadatos IDP, consulte Configuración de arrendatario SAML 2.0.

> **Nota**
>
> Ahora es compatible un nuevo algoritmo SHA-256 con la integración de SAML.

6. Reinicie el servidor de aplicaciones WebSphere.

> **Nota**
>
> Si se despliega BOE en cualquier equipo que no sea de Windows, los separadores de ruta de archivo a los metadatos IDP que están en el bean **FilesystemMetadataProvider** deberían modificarse en `securityContext.xml` en `<WebSphere_InstallDir>\WebSphere\AppServer\profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF`.
>
> Por ejemplo, `<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` se debe cambiar a `<value type="java.io.File">\WEB-INF\idp-meta-downloaded.xml</value>`.

**Generar keystore para activar SAML 2.0 (opcional)**

Este paso sólo es aplicable si desea utilizar su propio archivo keystore.

Los intercambios SAML implican utilizar criptografía para la firma y el cifrado de datos. Un keystore autofirmado de modelo `sampletestKeystore.jks` está empaquetado con el producto y es válido hasta

el 18 de octubre de 2019. `sampletestKeystore.jks` tiene el alias `Testkey` y la contraseña `Password1`. Ahora puede generar un archivo keystore autofirmado utilizando la herramienta clave de utilidad JAVA. Siga los pasos a continuación para generar un archivo keystore:

1. Navegue a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`.
2. Ejecute el comando `keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

| Comando | Descripción |
|---|---|
| -alias | Introduzca el alias del certificado |
| -keypass | Introduzca la contraseña del certificado |
| -keystore | Nombre del archivo keystore |
| -validity | Validez del certificado |
| numberofdays | Cantidad de días en los que es válido el certificado autofirmado. |

Los siguientes preguntas se realizan después de ejecutar el comando:

- Introduzca la contraseña del keystore: *****
- Vuelva a introducir la contraseña: *****
- ¿Cuáles son su nombre y apellidos? : <Nombre y apellidos>
- ¿Cuál es el nombre de su unidad organizativa? : <Nombre del departamento>
- ¿Cuál es el nombre de su organización? : <Nombre de la empresa>
- ¿Cuál es el nombre de su población y localidad? : <Nombre de la población>
- ¿Cuál es el nombre de su estado y provincia? : <Nombre de estado o provincia>
- ¿Cuál es el código del país de dos letras para esta unidad? : <Nombre de país o código ISO>

3. Detenga el servidor de aplicaciones WebSphere.
   Se ha generado el archivo keystore en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`.
4. Mueva el archivo de almacén de claves a `<WebSphere_InstallDir>\WebSphere\AppServer\Profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF`.
5. Edite el archivo `securityContext.xml` ubicado en `<WebSphere_InstallDir>\WebSphere\AppServer\Profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\WEB-INF` con el nombre de alias, la contraseña y el nombre de archivo de almacén de claves nuevos. Consulte el siguiente código XML:

Código de ejemplo

```
<bean id="keyManager"
class="org.springframework.security.saml.key.JKSKeyManager">
<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
```

```
<constructor-arg type="java.lang.String" value="Password1"/>
<constructor-arg>
<map>
<entry key="aliasname" value="password"/>
</map>
</constructor-arg>
<constructor-arg type="java.lang.String" value="Testkey"/>
</bean>
```

Consulte la tabla a continuacón para entender los argumentos:

| Etiqueta XML | Descripción |
|---|---|
| `<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>` | Localiza el archivo keystore. |
| `<constructor-arg type="java.lang.String" value="Password1"/>` | Contraseña del archivo keystore. |
| `<entry key="aliasname" value="password"/>` | Alias y contraseña |
| `<constructor-arg type="java.lang.String" value="Testkey"/>` | Alias del certificado por defecto |

7. Generar y cargar los metadatos de proveedor de servicios.
   1. Vaya a http(s)://host:port/BOE/saml/metadata. El archivo XML se descarga automáticamente después de navegar a la URL anterior.
   2. Cargue el archivo XML en el proveedor de identidades.

> **Nota**
>
> Puede utilizar el archivo de metadatos del proveedor de servicios estándar `spring_saml_metadata.xml`, ubicado en `<WebSphere_InstallDir>\WebSphere\AppServer\Profiles\<Nombre_Perfil>\installedApps\<Nombre_Nodo>\BOE.ear\BOE.war\biprws\WEB-INF`, en vez de generarlo manualmente. Debe sustituir la etiqueta XML `<replace_withip>` por la dirección IP o el nombre de host del equipo basado en su red, y `<replace_withport>` por el número de puerto del servidor de aplicaciones WebSphere. Sustituya HTTP por HTTPS si ha activado HTTPS en WebSphere.

8. Si está utilizando SAP Cloud Identity, para crear una aplicación SAML en IDP y cargar el SP `metadata.xml` en el IDP para configurar el SAML SSO para la plataforma BI, consulte Configurar un proveedor de servicios de confianza.
9. Reinicie el servidor de aplicaciones WebSphere.

> **Nota**
>
> Los últimos metadatos de productor de servicios deben generarse después de modificar el archivo keystore.

→ Sugerencias

Para comprobar su la integración SAML es correcta, una vez que inicie la aplicación SAML configurada (plataforma de lanzamiento de BI, plataforma de lanzamiento de BI de Fiori u OpenDocument), se le redirigirá al IDP.

### 9.2.5 Establecer una autenticación de confianza entre el servidor de aplicaciones de SAP NetWeaver SAP NetWeaver Java y la plataforma de BI

- El servidor de aplicaciones SAP NetWeaver Java está configurado para la autenticación SAML 2.0 como un proveedor de servicios.
- Debe existir un usuario en el servidor de aplicaciones SAP NetWeaver Java.
- Los certificados SAML 2.0 del proveedor de servicios y del proveedor de identidades se intercambian para configurar la confianza entre ellos.
  El mismo usuario debe importarse como usuario empresarial a la plataforma de BI.

Para establecer una autentificación de confianza entre el servidor de aplicación SAP NetWeaver Java y la plataforma de BI, ejecute los siguientes pasos:

ⓘ Nota

- Debería utilizar el método `USER_PRINCIPAL` para recuperar el usuario al activar la autentificación de confianza para aplicaciones web.
- No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

1. Genere una aplicación web BI utilizando Wdeploy.
   a. Vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   b. Ejecute el comando para generar el archivo `BOE.sca`: `wdeploy.bat sapappsvr73 -DAPP=BOE predeploy`

      `BOE.sca` se genera en `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application`.
2. Active la autentificación de confianza editando el archivo `web.xml` .
   a. Extraiga el archivo `BOE.sca` en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application` utilizando herramientas como winrar o winzip.
   b. Haga una copia del archivo `BOE.sca` antes de realizar ninguna modificación. En `BOE.sca`, navegue a *DEPLOYARCHIVES* > *BOE.ear* > *BOE.war* > *WEB-INF* .
   c. Edite el archivo `web.xml` añadiendo las etiquetas XML siguientes antes de `</web-app>`.

> **Nota**
>
> Asegúrese de que añade los roles (mencionados en el código XML de abajo) al servidor de aplicación SAP NetWeaver Java y asígnelos a un grupos de usuarios o usuario.
>
> - j2ee-admin
> - j2ee-guest
> - j2ee-special

> **Código de ejemplo**

```
<security-constraint>
<web-resource-collection>
 <web-resource-name>InfoView</web-resource-name>
<url-pattern>*</url-pattern>
<http-method>DELETE</http-method>
<http-method>GET</http-method>
<http-method>POST</http-method>
<http-method>PUT</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>j2ee-admin</role-name>
<role-name>j2ee-guest</role-name>
<role-name>j2ee-special</role-name>
</auth-constraint>
<user-data-constraint>
<transport-guarantee>NONE</transport-guarantee>
</user-data-constraint>
</security-constraint>
<login-config>
<auth-method>BASIC</auth-method>
<realm-name>InfoView</realm-name>
</login-config>
<security-role>
<description>Assigned to the SAP J2EE Engine System Administrators</
description>
<role-name>j2ee-admin</role-name>
</security-role>
<security-role>
<description>Assigned to all users</description>
<role-name>j2ee-guest</role-name>
</security-role>
<security-role>
<description>Assigned to a special group of users</description>
<role-name>j2ee-special</role-name>
</security-role>
```

d. Cree un nuevo archivo XML `web-j2ee-engine.xml` con las etiquetas XML indicadas abajo y guárdelo en `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application\BOE.sca\DEPLOYARCHIVES\BOE.ear\BOE.war\WEB-INF`.

> **Código de ejemplo**

```
<?xml version="1.0" encoding="UTF-8"?>
<web-j2ee-engine xsi:noNamespaceSchemaLocation="web-j2ee-engine.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<security-role-map>
    <role-name>j2ee-admin</role-name>
    <server-role-name>administrators</server-role-name>
</security-role-map>
<security-role-map>
```

```
        <role-name>j2ee-guest</role-name>
        <server-role-name>guests</server-role-name>
</security-role-map>
<security-role-map>
        <role-name>j2ee-special</role-name>
        <server-role-name>all</server-role-name>
</security-role-map>
 <login-module-configuration>
        <security-policy-domain>/irj</security-policy-domain>
 </login-module-configuration>
</web-j2ee-engine>
```

e. Guarde el archivo `web-j2ee-engine.xml` .

f. Arrastre el archivo a la carpeta `WEB-INF` del archivo `BOE.war` .

**Activar SSO en BIP - USER PRINCIPAL, secreto compartido –** `Trustedprincipal.conf`

Activamos SSO utilizando el método USER PRINCIPAL para autorizar el nombre de usuario NW y el archivo `Trustedprincipal.conf` para autorizar el secreto compartido.

Para activar la autentificación de confianza y generar un secreto compartido, ejecute los siguientes pasos:

1. Vaya a *CMC* > *Autentificación* > *Empresa* .
2. Habilite la *autenticación de confianza*.
3. Seleccione *Crear nuevo secreto compartido*.
4. Seleccione *Descargar secreto compartido* y guárdelo en su equipo BOE.
5. Seleccione *Actualizar*.
6. En `BOE.war/web-inf/config/default/folder`, extraiga el siguiente archivo a `BOE.war/web-inf/config/custom/folder`:
   - `global.properties`
7. Añada lo siguiente en `global.properties`:
   - `sso.enabled=true`
   - `trusted.auth.user.retrieval=USER_PRINCIPAL`
   - `trusted.auth.user.namespace.enabled=true`
   - `trusted.auth.shared.secret=MySecret`

     > **Nota**
     >
     > We enabled trusted.auth.user.namespace.enabled=true

     La primera vez, deberá recibir el mensaje de error: Logon denied: User "secExternal:samltest" not found (FWB 00007). Hay una funcionalidad de vinculación automática que asigna `secExternal: samltest` como alias al usuario BOE. Inicie sesión normalmente mediante el formulario de inicio de sesión de InfoView. La credencial BOE que utilice tiene un alias `secExternal: samltest` creado. Por ejemplo, si utiliza la cuenta de usuario samltest, en sus propiedades de usuario podrá ver que `secExternal: samltest` tiene un alias asignado.
8. Vaya a `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\wdeploy\workdir\sapappsvr73\application\ BOE.sca\DEPLOYARCHIVES\BOE.ear\BOE.war\ WEB-INF\ Eclipse\plugins\webpath.InfoView\web\custom.jsp`
9. Añada las etiquetas XML de abajo al archivo `custom.jsp` .

Bloqueo de código:

Código de ejemplo

```
<%@ page language="java" contentType="text/html;charset=utf-8"%>
<%@ page
import="com.businessobjects.bip.core.web.appcontext.RequestInfo"%>
<%
 request.getSession().setAttribute("MySecret","Your generated shared
secret content");
%>
 <html>
<head>
    <title></title>
 </head>
    <body>
   <script     type="text/javascript"     src="noCacheCustomResources/
custom.js"></script>
   <script     type="text/javascript">
   window.location = "logon.faces";
   </script>
   </body>
</html>
```

10. Guarde el archivo.

3. Actualice y cierre el fichero de archivo.
4. Después de ejecutar los pasos anteriores en el archivo `BOE.sca` , despliéguelo en NetWeaver.
5. Una vez que haya desplegado BOE.sca correctamente, inícielo para verificar (http://<hostname>:<port_number>/nwa).
6. Cuando se desclare la autentificación BASIC en `web.xml` verá una ventana emergente de navegador para la autentificación.

Acaba de establecer la autentificación de confianza entre el servidor de aplicación SAP NetWeaver Java y la plataforma de BI.

Nota

Si aparece una ventana emergente de navegador para la autentificación, siga ejecute los siguientes pasos:

1. Inicie sesión Log en el servidor de aplicación SAP NetWeaver Java, en http://<hostname>:<port_number>/nwa.
2. Navegue a *Configuración* > *Seguridad* > *Autentificación* > *Single Sign-On*
3. Localice la configuración de política de la aplicación BI.
4. Cambie al modo *Editar* .
5. En la etiqueta *Pila de autentificación* , deje el campo *Modelo utilizando* en blanco y añada *SAML2LoginModule* a la pila en la parte superior con el indicador *SUFFICIENT*.
6. Guarde los cambios y cierre.

## 9.2.6 Para utilizar la autenticación SAML 2.0 con el servidor de aplicaciones Java de SAP NetWeaver

Para permitir que los usuarios del servidor de aplicaciones Java de SAP NetWeaver accedan al contenido de la plataforma de SAP Business Intelligence mediante Single Sign-On (SSO), se tiene que establecer un mecanismo para autorizar el acceso a esas aplicaciones. Los pasos siguientes describen cómo puede establecer la autenticación de confianza entre el servidor de aplicaciones Java de SAP NetWeaver y SAP Business Intelligence.

Alcance: El alcance de estos pasos no es para configurar la autenticación SAML, ya que IDP puede variar de un suministrador a otro. Consulte los documentos específicos del suministrador para configurar la autenticación SAML.

La configuración se divide en los siguientes pasos:

1. Configure la autenticación SAML en el servidor de aplicaciones Java de SAP NetWeaver.
2. Configurar la autenticación de confianza para la plataforma de BI.

Para obtener más información sobre la activación de la autenticación SAML en el servidor de aplicaciones Java de SAP NetWeaver, consulte Utilización de SAML 2.0.

## 9.2.7 Habilitación de la autenticación de confianza

La autenticación de confianza de Enterprise se usa para llevar a cabo el inicio de sesión único mediante la confianza del servidor de aplicaciones Web para verificar la identidad de un usuario. Este método de autenticación implica el establecimiento de confianza entre el Servidor de administración central (CMS) y el servidor de aplicaciones Web que aloja la aplicación Web de la plataforma de BI. Cuando se establece la confianza, el sistema aplaza la verificación de la identidad de un usuario en el servidor de aplicaciones Web. La autenticación de confianza se puede usar para admitir métodos de autenticación como SAML, x.509 y otros métodos que no dispongan de complementos de autenticación dedicados.

Los usuarios prefieren conectarse al sistema una sola vez, sin tener que proporcionar su contraseña varias veces durante una sesión. La autenticación con confianza proporciona una solución de inicio de sesión único Java para integrar la solución de autenticación de la Plataforma de BI con soluciones de autenticación de terceros. Las aplicaciones que han establecido confianza con el Servidor de administración central (CMC) pueden usar la autenticación con confianza para permitir que los usuarios inicien sesión sin proporcionar sus contraseñas.

Para habilitar la autenticación de confianza, debe configurar un secreto compartido en el servidor a través de la configuración de autenticación de Enterprise, mientras que el cliente se configura a través de las propiedades especificadas por el archivo war de `BOE`.

> **Nota**
>
> - Para poder usar la autenticación con confianza, debe haber creado usuarios de Enterprise o haber asignado los usuarios de terceros que necesita para iniciar sesión en la plataforma de BI.
> - No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

## Información relacionada

Para configurar el servidor para utilizar la autenticación de confianza [página 264]
Configurar la autenticación de confianza para la aplicación Web [página 269]

## 9.2.7.1 Autenticación de confianza para los servicios Web RESTful en el servidor Web

El tema proporciona instrucciones para activar la autenticación de confianza para los servicios Web RESTful en el servidor Web.

> **Nota**
>
> No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

Siga los pasos siguientes para activar la autenticación de confianza:

1. Genere una clave de secreto compartido. Consulte Generación de un valor de secreto compartido [página 411] para obtener más información.
2. Guarde la clave de secreto compartido en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin` en Windows.
3. Abra la clave de secreto compartido en un editor de texto.
4. Copie la clave de secreto compartido.
5. 5. Copie el archivo biprws.properties de `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps` y péguelo en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom`.
6. Abra el archivo *biprws.properties* en un editor de texto.
7. Pegue la clave de secreto compartido frente al valor *Trusted_Auth_Shared_Secret=*.
8. Añada el *Método de recuperación* y el *Parámetro de nombre de usuario*. Consulte la tabla siguiente para añadir el Método de recuperación y el Parámetro de nombre de usuario.

Servicio Web RESTful: propiedades de la configuración de autenticación de confianza

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Recuperando método* | Esta configuración es un menú que establece qué método de consulta se utilizará para recuperar tokens de inicio de sesión con autenticación con confianza al utilizar el servicio Web RESTful de API `/logon/trusted`.<br>• *HTTP_HEADER* se utiliza para consultas GET con el encabezado de solicitud aceptar=aplicación/xml (o aplicación/json).<br>• *QUERY_STRING* se utiliza para agregar un nombre de inicio de sesión al final de la consulta de la dirección URL mediante el servicio web RESTful de API, por ejemplo /iniciosesión/confianza/?usuario=johndoe.<br>• *COOKIE* se utiliza cuando el nombre de inicio de sesión se recupera desde una cookie del explorador web. El dominio, el nombre, el valor y la ruta se deben almacenar en la cookie. | **HTTP_HEADER** |
| *Parámetro de nombre de usuario* | Esta es la etiqueta que se utiliza para identificar el usuario de confianza para recuperar el token de inicio de sesión. | **X-SAP-TRUSTED-USER** |

9. Guarde el archivo *biprws.properties*.
10. Reinicie el servidor Web.

## 9.2.7.2 Para configurar el servidor para utilizar la autenticación de confianza

Antes de que pueda configurar la autenticación de confianza, debe haber creado usuarios de Enterprise o debe haber asignado usuarios de terceros que deben iniciar sesión en la plataforma de BI.

> **Nota**
>
> No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

1. Inicie una sesión en la CMC.
2. Vaya al área de administración *Autenticación*.
3. Haga clic en la opción *Enterprise*.
   Aparecerá el cuadro de diálogo *Enterprise*.
4. En *Autenticación de confianza*:
   a. Haga clic en *Autenticación con confianza activada*.
   b. Haga clic en *Nuevo secreto compartido*.
      Aparece el mensaje `Se ha generado la clave del secreto compartido y está lista para la descarga`.
   c. Haga clic en *Descargar secreto compartido*.

      El secreto compartido lo utilizan el cliente y el CMS para establecer la confianza. Primero configure el servidor y, a continuación, el cliente para la autenticación de confianza.

Aparecerá el cuadro de diálogo *Descarga de archivos*.

d. Haga clic en *Guardar* y guarde el archivo `TrustedPrincipal.conf` en uno de los directorios siguientes:

> ⚠ Precaución
>
> No establezca el tiempo de espera en **0** (cero). Un valor **0** significa que la duración que puede diferir no es limitada, lo que puede aumentar la vulnerabilidad para responder a los ataques.

e. En el campo *Período de validez del secreto compartido*, introduzca el número de días que faltan para que el secreto compartido sea válido.

f. Especifique el tiempo máximo, en milisegundos, que pueden diferir las horas del cliente y en los del CMS para solicitudes de autenticación de confianza.

g. Si planifica compartir el secreto mediante el archivo TrustedPrincipal.conf en lugar de la sesión web, cópielo en uno de los siguientes directorios:

   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

5. Haga clic en *Actualizar* para confirmar el secreto compartido.

La plataforma de BI no audita todas las modificaciones de los parámetros de la autenticación de confianza. Debe realizar una copia de seguridad manual de la información de la autenticación de confianza.

El secreto compartido lo utilizan el cliente y el CMS para establecer la confianza. El siguiente paso es configurar el cliente para Autenticación de confianza.

## 9.2.8 Configuración de la autenticación de confianza para la aplicación Web

Para configurar la Autenticación de confianza para el cliente, debe modificar las propiedades globales para el archivo `BOE.war` y las propiedades específicas de las aplicaciones plataforma de lanzamiento de BI y OpenDocument.

Use uno de los métodos siguientes para pasarle el secreto compartido al cliente:

- Opción `WEB_SESSION`
- Archivo `TrustedPrincipal.conf`

Use uno de los métodos siguientes para pasarle el nombre de usuario al cliente:

- `REMOTE_USER`
- `HTTP_HEADER`
- `COOKIE`
- `QUERY_STRING`
- `WEB_SESSION`
- `USER_PRINCIPAL`

Sea cual sea el método usado para pasar el secreto compartido, debe personalizarlo en las propiedades globales `Trusted.auth.user.retrieval` del archivo `BOE.war`.

> **Nota**
>
> No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

## 9.2.8.1 Uso de la autenticación de confianza para el inicio de sesión único de SAML

El lenguaje de marcado de aserción de seguridad (SAML) es un estándar basado en XML para comunicar información de identidad. SAML proporciona una conexión segura en la que la identidad y la confianza se comunican, por lo que se habilita un mecanismo de inicio de sesión único que elimina los inicios de sesión adicionales para los usuarios con confianza que desean acceder a la plataforma de BI.

### Habilitar la autenticación SAML

Si el servidor de aplicaciones puede trabajar como un proveedor de datos SAML, puede usar la autenticación con confianza para proporcionar el SSO SAML a la plataforma de BI.

Para ello, primero debe configurar el servidor de aplicaciones Web para la autenticación SAML.

Asimismo, debe usar uno de estos métodos para pasar el nombre de usuario al cliente:

- `REMOTE_USER`
- `USER_PRINCIPAL`

El siguiente ejemplo contiene un archivo web.xml de ejemplo configurado para la autenticación SAML:

```
<security-constraint>
      <web-resource-collection>
        <web-resource-name>InfoView</web-resource-name>
        <url-pattern>*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
        <role-name>j2ee-admin</role-name>
        <role-name>j2ee-guest</role-name>
        <role-name>j2ee-special</role-name>
      </auth-constraint>
      <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
      </user-data-constraint>
    </security-constraint>
    <login-config>
      <auth-method>FORM</auth-method>
      <realm-name>InfoView</realm-name>
      <form-login-config>
        <form-login-page>/logon.jsp</form-login-page>
        <form-error-page>/logon.jsp</form-error-page>
      </form-login-config>
    </login-config>
    <security-role>
```

```
      <description>Assigned to the SAP J2EE Engine System Administrators</
description>
      <role-name>j2ee-admin</role-name>
    </security-role>
    <security-role>
      <description>Assigned to all users</description>
      <role-name>j2ee-guest</role-name>
    </security-role>
    <security-role>
      <description>Assigned to a special group of users</description>
      <role-name>j2ee-special</role-name>
    </security-role>
```

Consulte la documentación del servidor de aplicaciones para obtener más instrucciones sobre cómo conseguirlo, ya que pueden variar según el servidor de aplicaciones.

### Uso de la autenticación de confianza

Una vez configurado el servidor de aplicaciones Web para que funcione como un proveedor de servicios de SAML, debe usar la autenticación de confianza para proporcionar el SSO de SAML.

Para habilitar el SSO se usan alias dinámicos. La primera vez que un usuario accede a la página de inicio de sesión a través de SAML, se les solicitará que inicien sesión manualmente con las credenciales de la cuenta de la Plataforma de BI existentes. Una vez que se verifican las credenciales del usuario, el sistema dará un alias a la identidad de SAML del usuario para la cuenta de la Plataforma de BI. Los siguientes intentos de acceso del usuario se realizarán mediante el SSO, ya que el sistema dispondrá del alias del usuario que coincide de forma dinámica con una cuenta existente.

> **Nota**
>
> Los usuarios se deben importar a la plataforma de BI o deben disponer de cuentas de Enterprise.

> **Nota**
>
> Debe habilitarse una propiedad específica para el archivo BOE war, `trusted.auth.user.namespace.enabled` , para que este mecanismo funcione.

## 9.2.8.2 Propiedades de la autenticación de confianza para las aplicaciones Web

La tabla siguiente lista la configuración de autenticación de confianza en `global.properties` predeterminado para el archivo `BOE.war`. Para sobrescribir la configuración, cree un archivo en `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> **Nota**
>
> No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda

expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

| Propiedad | Valor predeterminado | Descripción |
| --- | --- | --- |
| `sso.enabled=true` | `sso.enabled=false` | Habilita y deshabilita el inicio de sesión único (SSO) en la plataforma de BI. Establézcalo como `true` para habilitar la autenticación de confianza. |
| `trusted.auth.shared.secret` | Ninguno | Nombre de la variable de sesión que se usa para recuperar el secreto para la autenticación de confianza. Sólo se aplica si se usa la sesión Web para pasar el secreto compartido. |
| `trusted.auth.user.param` | Ninguno | Especifica la variable que se usa para recuperar el nombre de usuario para la autenticación de confianza. |
| `trusted.auth.user.retrieval` | Ninguno | Especifica el método que se usa para recuperar el nombre de usuario para la autenticación de confianza.<br>• `REMOTE_USER`<br>• `HTTP_HEADER`<br>• `COOKIE`<br>• `QUERY_STRING`<br>• `WEB_SESSION`<br>• `USER_PRINCIPAL`<br>Establecer en vacío para deshabilitar la autenticación de confianza. |
| `trusted.auth.user.namespace.enabled` | Ninguno | Habilita y deshabilita el enlazado dinámico de alias a cuentas de usuario existentes. Si se configura con el valor `true`, la autenticación de confianza usa el enlace de alias para autenticar usuarios en la plataforma de BI. Con el enlace de alias, el servidor de aplicaciones puede trabajar como un proveedor de servicios SAML por lo que se habilita la autenticación de confianza para proporcionar el inicio de sesión único de SAML en el sistema.<br>Si esta propiedad está en blanco, la autenticación de confianza usará la coincidencia de nombres cuando se autentiquen los usuarios. |

## 9.2.8.3 Configurar la autenticación de confianza para la aplicación Web

Si planea almacenar el secreto compartido en el archivo `TrustedPrincipal.conf`, asegúrese de que el archivo está almacenado en el directorio de la plataforma adecuado:

| Plataforma | Ubicación de TrustedPrincipal.conf |
|---|---|
| Windows, instalación predeterminada | • `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`<br>• `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\` |
| AIX | `<INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/` |
| Solaris | `<INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/` |
| Linux | `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86` |

La variable de nombre de usuario utilizada para configurar la Autenticación con confianza para las aplicaciones Web se obtiene por diversos mecanismos. Configure o defina el servidor de aplicaciones Web para que sus nombres de usuario se muestren antes de usar los métodos de recuperación del nombre de usuario. Consulte http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html para más información.

Para configurar la Autenticación con confianza para el cliente, debe acceder y modificar las propiedades globales para el archivo `BOE.war`, y las propiedades específicas de la plataforma de lanzamiento de BI y las aplicaciones de OpenDocument.

> **Nota**
>
> Puede que se requieran pasos adicionales dependiendo de cómo planee recuperar el nombre de usuario o el secreto compartido.

1. Acceda a la carpeta personalizada para el archivo `BOE.war` en el equipo que aloja las aplicaciones Web: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Más adelante, debe volver a desplegar el archivo `BOE.war` modificado.
2. Cree un nuevo archivo, utilizando el Bloc de notas u otro programa de edición de textos.
3. Introduzca las siguientes propiedades de Autenticación con confianza:

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=<Method for user ID retrieval>
   trusted.auth.user.param=<User Variable>
   trusted.auth.shared.secret=<Secret Variable>
   ```

   Para la propiedad `trusted.auth.user.retrieval`, seleccione una de las siguientes opciones de recuperación del nombre de usuario:

| Opción | Cómo se recuperará el nombre de usuario |
| --- | --- |
| `HTTP_HEADER` | El nombre de usuario se recupera del contenido de un encabezado HTTP. Debe especificar qué encabezado HTTP desea usar en la propiedad `trusted.auth.user.param`. |
| `QUERY_STRING` | El nombre de usuario se recupera desde un parámetro de la dirección URL de la solicitud. Debe especificar qué cadena de consulta usar en la propiedad `trusted.auth.user.param`. |
| `COOKIE` | El nombre de usuario se recupera desde una cookie especificada. Debe especificar qué cookie de consulta usar en la propiedad `trusted.auth.user.param`. |
| `WEB_SESSION` | El nombre de usuario se obtiene del contenido de una variable de sesión especificada. Debe especificar la variable de la sesión Web para usar en `trusted.auth.user.param` en `global.properties`. |
| `REMOTE_USER` | El nombre de usuario se recupera mediante una llamada a `HttpServletRequest.getRemoteUser()`. |
| `USER_PRINCIPAL` | El nombre de usuario se recupera mediante una llamada a `getUserPrincipal().getName()` en el objeto `HttpServletRequest` de la solicitud actual en un servlet o JSP. |

→ Recomendación

Cuando utiliza SSO basado en HTTP_HEADER o SSO basado en QUERY_STRING, debe asegurarse de que los usuarios finales (navegadores) no acceden directamente a BOE para autentificarse. En su lugar, SAP recomienda que los usuarios finales (navegadores) accedan a BOE solo a través del portal o la aplicación personalizada.

ⓘ Nota

Algunos servidores de aplicaciones Web requieren que la variable de entorno `USUARIO_REMOTO` esté configurada como `true` en el servidor. Para saber si se requiere o no en cada caso, consulte la documentación de su servidor de aplicaciones Web. Si se requiere, confirme que la variable de entorno esté configurada como `true`.

ⓘ Nota

Si está utilizando `USUARIO_PRINCIPAL` o `USUARIO_REMOTO` para obtener el nombre de usuario, deje `trusted.auth.user.param` en blanco.

4. Guarde el archivo con el nombre `global.properties`.

5. Reinicie el servidor de aplicaciones Web.

Las nuevas propiedades surten efecto solo después de que la aplicación Web BOE modificada se vuelva a desplegar en el equipo que ejecuta el servidor de aplicaciones Web. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web. Para obtener más información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 9.2.8.3.1 Configuraciones de ejemplo

### 9.2.8.3.1.1 Pasar el secreto compartido a través del archivo TrustedPrincipal.conf

La información de usuario se almacena y se pasa a través de la sesión Web y el secreto compartido se pasa por medio del archivo `TrustedPrincipal.conf`, ubicado de forma predeterminada en el directorio `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. La versión en paquete de Tomcat es el servidor de aplicaciones Web.

1. En el directorio `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`, cree un archivo nuevo con el bloc de notas u otra utilidad de edición de texto.
2. Para especificar las propiedades de Autenticación de confianza, introduzca los valores siguientes:

```
sso.enabled=true
trusted.auth.user.retrieval=<Method for user ID retrieval>
trusted.auth.user.param=<User Variable>
```

3. Guarde el archivo con el nombre **`global.properties`**.
4. Ubique el archivo `custom.jsp` dentro de la carpeta `web` del archivo `com.businessobjects.webpath.InfoView.jar` en `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins`.
5. Inserte el código java personalizado siguiente en el archivo `custom.jsp` en el archivo `com.businessobjects.webpath.InfoView.jar`:

```
<%
//custom Java code
request.getSession().setAttribute("MyUser","<Username>");
%>
```

> **Nota**
>
> En el fragmento de código anterior, la variable <Nombre de usuario> debe ser un usuario de Enterprise válido en la plataforma de BI.

6. Reinicie el servidor de aplicaciones Web.
7. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web.

   Para obtener información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma de SAP BusinessObjects Business Intelligence*.

Para verificar que ha configurado correctamente la autenticación de confianza, use la siguiente dirección URL para acceder a la plataforma de lanzamiento de BI: `http://<[cmsname]>:8080/BOE/BI/custom.jsp` donde `<[cmsname]>` es el nombre del equipo que aloja el CMS. Se le ha solicitado introducir su nombre de usuario y contraseña solo la primera vez. Si la autenticación fue correcta, se le redirigirá automáticamente a la plataforma de lanzamiento de BI.

### 9.2.8.3.1.2 Pasar el secreto compartido a través de la variable de la sesión Web

Tanto la información del usuario como el secreto compartido se almacenarán y pasarán a través de la variable de sesión web. Abra el archivo TrustedPrincipal.conf que se ha guardado anteriormente y anote el contenido del archivo. En esta configuración de ejemplo se supone que el secreto compartido es el siguiente:

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc6577
3841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

La versión en paquete de Tomcat es el servidor de aplicaciones Web.

1. Acceda al siguiente directorio:

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`

2. Cree un archivo nuevo con un editor de texto.
3. Especifique las propiedades de autenticación de confianza introduciendo lo siguiente:

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=MyUser
   trusted.auth.shared.secret=MySecret
   ```

4. Guarde el archivo con el siguiente nombre:

   **`global.properties`**

5. Acceda al siguiente archivo:

   Plataforma de lanzamiento de BI clásica: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`

   Plataforma de lanzamiento de BI de Fiori: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.FioriBI\web\custom.jsp`

6. Modifique el contenido del archivo para que incluya lo siguiente:

   ```
   <%
   //custom Java code
   request.getSession().setAttribute("MySecret","9ecb0778edcff048edae0fcdde1a5db8
   211293486774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b
   6a3f1345285b55a0a7");
   request.getSession().setAttribute("MyUser","<Username>");
   %>
   ```

   > **Nota**
   >
   > En el fragmento de código anterior, la variable <Nombre de usuario> debe ser un usuario de Enterprise válido en la plataforma de BI.

7. Reinicie el servidor de aplicaciones Web.
8. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones web.

   Para obtener más información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

Para verificar que ha configurado correctamente la autenticación de confianza, use la siguiente dirección URL para acceder a la aplicación de la plataforma de lanzamiento: `http://[cmsname]:8080/BOE/BI/custom.jsp` en que [cmsname] es el nombre del sistema host de CMS. Se le ha solicitado introducir su nombre de usuario y contraseña solo la primera vez. Si la autenticación fue correcta, se le redirigirá automáticamente a la plataforma de lanzamiento de BI.

### 9.2.8.3.1.3 Pasar el nombre de usuario a través del principal de usuario

El siguiente ejemplo de configuración asume que se ha creado un usuario llamado «JohnDoe» en la plataforma de BI.

La información sobre el usuario se almacena y se pasa a través de la opción Principal de usuario, y el secreto compartido se pasa a través del archivo `TrustedPrincipal.conf`, que se encuentra situado de forma predeterminada en el directorio `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. La versión en paquete de Tomcat es el servidor de aplicaciones Web.

1. Detenga el servidor Tomcat.
2. Abra el archivo `server.xml` para Tomcat en el directorio predeterminado `C:\Archivos de programa (x86)\SAP BusinessObjects\Tomcat\conf\`.
3. Localice `<Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>` y cámbielo al siguiente valor:

   ```
   Realm className=" org.apache.catalina.realm.UserDatabaseRealm".../
   ```

4. Abra el archivo `tomcat-users.xml` ubicado en el directorio predeterminado `C:\Archivos de programa (x86)\SAP BusinessObjects\Tomcat\conf\`.
5. Localice la etiqueta `<tomcat-users>` y modifique el valor siguiente:

   ```
   <user name=«JohnDoe» password=«password»
   roles=«onjavauser»/>
   ```

6. Abra el archivo `web.xml` del directorio `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.
7. Antes de la etiqueta `</web-app>`, inserte los valores siguientes:

   ```
   <security-constraint>
       <web-resource-collection>
            <web-resource-name>OnJavaApplication</web-resource-name>
            <url-pattern>/*</url-pattern>
       </web-resource-collection>
       <auth-constraint>
            <role-name>onjavauser</role-name>
       </auth-constraint>
   </security-constraint>
   ```

```
<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>OnJava Application</realm-name>
</login-config>
```

Introduzca una página específica para el parámetro `<url-pattern></url-pattern>`. Normalmente esta página no es la dirección URL predeterminada para la plataforma de lanzamiento de BI o cualquier otra aplicación Web.

8. En el archivo personalizado `global.properties` introduzca los valores siguientes:

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

> **Nota**
>
> Es opcional configurar `trusted.auth.user.namespace.enabled=true`. Agregue el parámetro si desea asignar un nombre de usuario externo a un nombre de usuario de plataforma de BI distinto.

9. Reinicie el servidor de aplicaciones Web.
10. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web.

    Para obtener información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma de SAP BusinessObjects Business Intelligence*.

Las configuraciones del servidor de aplicaciones Web son las mismas que si se usara el método Usuario remoto.

Para verificar que ha configurado correctamente la autenticación de confianza, use la siguiente dirección URL para acceder a la plataforma de lanzamiento de BI: `http://<[cmsname]>:8080/BOE/BI`, donde `<[cmsname]>` es el nombre del equipo que aloja el CMS. Al cabo de un momento aparece un cuadro de diálogo de inicio de sesión.

## 9.3 Autenticación LDAP

### 9.3.1 Uso de la autenticación LDAP

En esta sección se proporciona una descripción general del funcionamiento de la autenticación LDAP con la plataforma de BI. A continuación, se presentan las herramientas de administración que permiten administrar y configurar cuentas de LDAP para la plataforma.

Al instalar la plataforma de BI, se instala automáticamente el complemento de autenticación LDAP pero no se activa de forma predeterminada. Para utilizar autenticación LDAP, tendrá que asegurarse primero de que ha instalado el directorio LDAP correspondiente. Para obtener más información acerca de LDAP, consulte su documentación de LDAP.

El Protocolo ligero de acceso a directorios (LDAP), un directorio común e independiente de la aplicación, permite a los usuarios compartir información entre varias aplicaciones. LDAP, basado en un estándar abierto, proporciona una forma de obtener acceso a la información de un directorio y actualizarla.

LDAP está basado en el estándar X.500, que usa un protocolo de acceso a directorios (directory access protocol, DAP) para comunicar un cliente de directorios con un servidor de directorios. LDAP es una alternativa a DAP, ya que usa menos recursos y simplifica y hace caso omiso de algunas operaciones y funciones X.500.

La estructura de los directorios en LDAP tiene entradas dispuestas en un esquema determinado. Cada entrada se identifica por medio de su nombre completo (distinguished name, DN) o su nombre común (common name, CN). Otros atributos comunes son el nombre de unidad organizativa (organizational unit, OU) y el nombre de organización (organization name, O). Por ejemplo, un grupo de miembros puede estar ubicado en un árbol de directorio de la siguiente manera: cn=Plataforma de BI, ou=Usuarios empresariales A, o=Investigación. Consulte la documentación de LDAP para obtener más información.

Debido a que LDAP no depende de ninguna aplicación, cualquier cliente con los privilegios adecuados puede acceder a sus directorios. LDAP ofrece la capacidad de configurar a los usuarios para que inicien sesión en la plataforma de BI mediante la autenticación LDAP. Proporciona a los usuarios derechos de acceso para los objetos del sistema. Siempre y cuando ejecute un servidor o servidores LDAP y use LDAP en los sistemas de equipos de la red existentes, podrá usar la autenticación LDAP (junto con las autenticaciones Enterprise y Windows AD).

Si lo desea, el complemento de seguridad de LDAP incluido en la plataforma de BI se puede comunicar con el servidor LDAP a través de una conexión SSL establecida mediante la autenticación de servidor o la autenticación mutua. Con la autenticación de servidor, el servidor LDAP dispone de un certificado de seguridad que la plataforma de BI usa para verificar que confía en el servidor mientras el servidor LDAP permite conexiones de clientes anónimos. Con la autenticación mutua, el servidor LDAP y la plataforma de BI disponen de certificados de seguridad y el servidor LDAP también debe verificar el certificado cliente antes de establecer una conexión.

El complemento de seguridad de LDAP incluido en la plataforma de BI se puede configurar para que se comunique con el servidor LDAP mediante SSL pero siempre realiza una autenticación básica al verificar las credenciales de los usuarios. Antes de desplegar la autenticación LDAP junto con la plataforma de BI, asegúrese de que conoce las diferencias entre estos tipos de LDAP. Para obtener información más detallada, consulte RFC2251, que está disponible en http://www.faqs.org/rfcs/rfc2251.html .

### Información relacionada

Configuración de la autenticación LDAP [página 276]
Asignar grupos LDAP [página 287]

## 9.3.1.1 Complemento de seguridad de LDAP

El complemento de seguridad de LDAP permite asignar cuentas de usuario y grupos desde el servidor de directorio LDAP a la plataforma de BI; también permite que el sistema compruebe todas las solicitudes de inicio de sesión que especifique la autenticación LDAP. Los usuarios se autentican al comparar sus datos con los del servidor de directorios de LDAP y al comprobar que sean miembros de un grupo LDAP asignado antes de que el CMS les conceda una sesión activa de la Plataforma de BI. El sistema mantiene de forma dinámica las listas de usuarios y las pertenencias a grupos. Puede especificar que la plataforma use una conexión de Nivel de socket seguro (SSL) para comunicarse con el servidor de directorios LDAP para obtener seguridad adicional.

La autenticación LDAP para la plataforma de BI se parece a la autenticación de Windows AD en que se pueden asignar grupos y configurar la autenticación, los derechos de acceso y la creación de alias. Del mismo modo que en la autenticación NT o AD, puede crear nuevas cuentas Enterprise para los usuarios LDAP existentes y

puede asignar alias LDAP a los usuarios existentes si los nombres de usuario coinciden con los de Enterprise. También puede hacer lo siguiente:

- Asignar usuarios y grupos del servicio de directorios LDAP.
- Asignar LDAP respecto a AD. Hay una serie de restricciones si configura LDAP respecto a AD.
- Especificar varios nombres de host y sus puertos.
- Configurar LDAP con SiteMinder.

Una vez que asignados los usuarios y grupos de LDAP, todas las herramientas cliente de la Plataforma de BI admitirán la autenticación LDAP. También puede crear sus propias aplicaciones compatibles con la autenticación LDAP.

### Información relacionada

Configurar los ajustes SSL para el servidor de LDAP o la autenticación mutua [página 280]
Asignar LDAP en Windows AD [página 290]
Configurar el complemento LDAP para SiteMinder [página 285]

## 9.3.2 Configuración de la autenticación LDAP

Para simplificar la administración, la plataforma de BI admite autenticación LDAP para cuentas de usuario y grupos. Antes de que los usuarios puedan usar su nombre de usuario y contraseña LDAP para iniciar sesión en el sistema, tendrá que asignar sus cuentas LDAP a la plataforma de BI. Al asignar una cuenta LDAP, puede elegir crear una nueva cuenta o vincularse a una cuenta existente de la Plataforma de BI.

Antes de configurar y habilitar la autenticación LDAP, asegúrese de haber configurado su directorio LDAP. Para obtener más información, consulte su documentación de LDAP.

La configuración de la autenticación LDAP incluye las siguientes tareas:

- Configuración del host LDAP
- Preparar el servidor de LDAP para SSL (en caso necesario)
- Configurar el complemento de LDAP para SiteMinder (en caso necesario)

> **Nota**
>
> Si configura LDAP respecto a AD, podrá asignar sus usuarios, pero no podrá configurar el inicio de sesión único de AD o el inicio de sesión único en la base de datos. No obstante, los métodos de inicio de sesión único LDAP, como SiteMinder y la autenticación de confianza, seguirán estando disponibles.

### 9.3.2.1 Configurar el host LDAP

Se recomienda que el servidor LDAP esté instalado y en ejecución antes de configurar el host LDAP.

1. Seleccione *Autenticación* de la lista de navegación para ir al área de administración de la CMC *Autenticación*.
2. Haga doble clic en *LDAP*.
3. Si está estableciendo la autenticación LDAP por primera vez, haga clic en *Iniciar asistente para configuración de LDAP*.
4. Escriba el nombre y el número de puerto de los hosts LDAP en el campo *Agregar host LDAP (nombre de host:puerto)* (por ejemplo, "miservidor:123"), haga clic en *Agregar* y, a continuación, haga clic en *Siguiente*.

   > → Sugerencias
   >
   > Repita este paso para agregar varios hosts LDAP del mismo tipo de servidor si desea agregar hosts que puedan actuar como servidores de conmutación por error. Si desea eliminar un host, seleccione el nombre del host y haga clic en *Eliminar*.

5. Seleccione el tipo de servidor de la lista *Tipo de servidor de LDAP*.

   > ⓘ Nota
   >
   > Si asigna LDAP a AD, seleccione *Servidor de aplicaciones de Microsoft Active Directory* para el tipo de servidor.

6. Si desea ver o cambiar alguna de las asignaciones de atributo de servidor LDAP o los atributos de búsqueda predeterminados de LDAP, haga clic en *Mostrar asignaciones de atributos*.

   Cada asignación de atributo de servidor y atributo de búsqueda del tipo de servidor compatible está establecida de manera predeterminada.
7. Haga clic en *Siguiente*.
8. En el campo *Nombre completo de LDAP base*, escriba el nombre completo (por ejemplo, o=AlgunaBase) del servidor LDAP, y haga clic en *Siguiente*.
9. En el área *Credenciales de administración de servidor LDAP*, especifique el nombre completo y la contraseña de una cuenta de usuario que disponga de acceso de lectura al directorio.

   No se requieren las credenciales de administrador.

   Si el servidor LDAP permite una vinculación anónima, deje esta área en blanco. Los servidores y los mandantes de la plataforma BI establecerán el vínculo con el host primario mediante un inicio de sesión anónimo.
10. Si ha configurado referencias en el host LDAP, especifique la información de autenticación en el área *Credenciales de referencia de LDAP* y el número de saltos de referencia en el campo *Máximo de saltos de referencia*.

    Debe configurar el área *Credenciales de referencia de LDAP* si se aplican todos los criterios siguientes:
    - El host principal se ha configurado para hacer referencia a otro servidor de directorios que administra consultas para entradas de una base especificada.
    - El host al que se hace referencia se ha configurado para no permitir enlaces anónimos.
    - Se asignará a la plataforma de BI un grupo del host al que se hace referencia.

    > ⓘ Nota
    >
    > Aunque los grupos pueden asignarse desde varios hosts, sólo puede establecerse un conjunto de credenciales de referencia. Por lo tanto, si dispone de varios hosts de referencia, debe crear una cuenta de usuario en cada host que use el mismo nombre completo y la misma contraseña.

> **Nota**
>
> Si *Máximo de saltos de referencia* se configura en cero, no se seguirá ninguna referencia.

11. Haga clic en *Siguiente*.
12. Seleccione el tipo de autenticación Secure Sockets Layer (SSL) utilizado:
    - *Básico (no SSL)*
    - *Autenticación de servidor*
    - *Autenticación mutua*

    Los detalles y requisitos previos de la autenticación del servidor y de la autenticación mutua se exponen en una sección posterior. Para configurar correctamente la autenticación LDAP mediante cualquier tipo de SSL, consulte *Configuración de ajustes de SSL para la autenticación de servidor LDAP o la autenticación mutua* en este documento antes de proseguir con este procedimiento.
13. Haga clic en *Siguiente*, y seleccione un método de autenticación de inicio de sesión único LDAP:
    - *Básico (no SSO)*
    - *SiteMinder*
14. Haga clic en *Siguiente* y seleccione el modo en que se asignarán los alias y usuarios a las cuentas la plataforma de BI.
    a. En el área *Opciones de alias nuevos*, seleccione el modo en que los nuevos alias se asignan a cuentas de Enterprise:
       - *Asignar cada alias de LDAP agregado a una cuenta con el mismo nombre*
         Utilice esta opción cuando sepa que algunos usuarios tienen una cuenta de Enterprise con el mismo nombre; es decir, los alias LDAP se asignarán a usuarios existentes (la creación automática de alias está activada). Los usuarios que no tengan cuentas Enterprise existentes o que no tengan el mismo nombre en las cuentas Enterprise y LDAP, se agregan como usuarios nuevos.
       - *Crear una cuenta nueva para cada alias de LDAP agregado*
         Utilice esta opción cuando desee crear una cuenta nueva para cada usuario.

    b. En el área *Opciones de actualización del alias*, seleccione el modo de administrar las actualizaciones de alias para las cuentas de Enterprise:
       - *Crear nuevos alias cuando se actualice el alias*
         Use esta opción para crear automáticamente nuevos alias para todos los usuarios LDAP asignados a la plataforma de BI. Se agregan nuevas cuentas LDAP para los usuarios sin cuentas de la plataforma de BI o para todos los usuarios si se selecciona *Crear una cuenta nueva para cada alias de LDAP agregado*.
       - *Crear nuevos alias solo cuando el usuario inicie sesión*
         Use esta opción cuando el directorio LDAP que está asignando contiene varios usuarios, pero solo unos pocos de ellos usarán la plataforma de BI. El sistema no crea automáticamente alias ni cuentas de Enterprise para todos los usuarios. En su lugar, crea alias (y cuentas, en caso necesario) solo para los usuarios que inician sesión en la plataforma de BI.

    c. En el área *Opciones de usuarios nuevos*, especifique el modo en que se crean los usuarios:
       - *Los usuarios nuevos se crean como usuarios con nombre*
         Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios con nombre. Las licencias de usuario con nombre se asocian con usuarios específicos y permiten que tengan acceso al sistema basándose en sus nombres de usuario y en sus contraseñas. De esta forma, los usuarios con nombre pueden tener acceso al sistema independientemente del número de

personas conectadas. Debe tener una licencia de usuario con nombre disponible por cada cuenta de usuario creada mediante esta opción.

> **Nota**
>
> El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.
>
> Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

- *Los usuarios nuevos se crean como usuarios simultáneos*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios simultáneos. Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque una licencia simultánea pequeña puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios a la plataforma, una licencia simultánea de 100 usuarios puede admitir 250, 500 o 700 usuarios.

15. Lleve a cabo este paso si está configurando asignaciones de atributo de usuario o si planea importar direcciones de correo electrónico desde el servidor LDAP. En el área *Opciones de enlace de atributos*, especifique la prioridad de enlace de atributos para el complemento de AD:
    a. Haga clic en el cuadro *Importar nombre completo, dirección de correo electrónico y otros atributos*. Los nombres completos y descripciones que se usan en las cuentas LDAP se importan y almacenan con los objetos de usuario en el sistema.
    b. Especifique una opción para *Configurar prioridad del enlace del atributo LDAP en relación a otros enlaces de atributos*.

    > **Nota**
    >
    > Si la opción está configurada en 1, los atributos LDAP tendrán prioridad en escenarios en los que estén habilitados LDAP y otros complementos (Windows AD y SAP). Si la opción está configurada en 3, tendrán prioridad los atributos de otros complementos habilitados.

16. Haga clic en *Finalizar*..

## Información relacionada

Configurar los ajustes SSL para el servidor de LDAP o la autenticación mutua [página 280]
Configurar el complemento LDAP para SiteMinder [página 285]

## 9.3.2.2 Administración de varios hosts LDAP

Al usar LDAP y la plataforma de BI, se puede agregar tolerancia a fallos en el sistema mediante la adición de varios hosts de LDAP. El sistema usa el primer host que se agrega como el host de LDAP principal. Los hosts subsiguientes se tratan como hosts de conmutación por error.

Se deben configurar el host LDAP principal y todos los hosts de conmutación por error exactamente de la misma forma y cada uno de ellos debe hacer referencia a todos los hosts adicionales desde los que desee asignar grupos. Para obtener más información acerca de hosts y referencias LDAP, consulte su documentación de LDAP.

Para agregar varios hosts de LDAP, introduzca todos los hosts al configurar LDAP con el Asistente de configuración de LDAP (consulte para obtener más detalles.) O bien, si ya ha configurado LDAP, vaya al área Autenticación de la Consola de administración central (CMC) y haga clic en la ficha LDAP. En el área Resumen de configuración del servidor de LDAP, haga clic en el nombre del host LDAP para abrir la página que le permite agregar o eliminar hosts.

> **Nota**
>
> Procure añadir el host principal primero, seguido de los demás hosts de conmutación por error.

> **Nota**
>
> Si utiliza hosts LDAP de conmutación por error, no puede usar el nivel más alto de seguridad SSL; es decir, no puede seleccionar "Aceptar el certificado del servidor si proviene de una entidad emisora de certificados de confianza y si el atributo CN del certificado coincide con el nombre del host del DNS del servidor".

### Información relacionada

Configuración de la autenticación LDAP [página 276]

## 9.3.2.3 Configurar los ajustes SSL para el servidor de LDAP o la autenticación mutua

Esta sección contiene información detallada acerca de la autenticación de servidor o la autenticación mutua basada en SSL para LDAP. Los pasos previos son necesarios para configurar la autenticación basada en SSL. Esta sección también proporciona información específica para configurar la autenticación SSL con servidor LDAP y la autenticación mutua en la CMC. Supone que ha configurado el host de LDAP y que ha seleccionado una de estas opciones para la autenticación SSL.

Para obtener información adicional o información sobre la configuración del servidor host de LDAP, consulte la documentación del proveedor de LDAP.

Para los sistemas Windows, la comunicación SSL predeterminada se realiza mediante TLS 1.2. Para los sistemas Linux, consulte la nota SAP. 2623529.

## Información relacionada

Configurar el host LDAP [página 276]

# 9.3.2.3.1 Para configurar el servidor LDAP o la autenticación mutua

| Recurso | Efectúe esta acción antes de iniciar la tarea |
|---|---|
| Certificado CA | Esta acción es necesaria para la autenticación de servidor y la autenticación mutua con SSL.<br>1. Obtenga un entidad emisora de certificados (CA) para generar un certificado CA.<br>2. Agregue el certificado en su servidor LDAP.<br>Para obtener información, consulte la documentación de su proveedor de LDAP. |
| Certificado del servidor | Esta acción es necesaria para la autenticación de servidor y la autenticación mutua con SSL.<br>1. Solicite y luego genere un certificado del servidor.<br>2. Autorice el certificado y, a continuación, agréguelo al servidor LDAP. |
| cert7.db o cert8.db, key3.db | Estos archivos son necesarios para la autenticación de servidor y la autenticación mutua con SSL.<br>1. Descargue la aplicación certutil que genera un archivo `cert7.db` o `cert8.db` (según sus requisitos) desde https://developer.mozilla.org/en-US/docs/NSS/tools .<br>2. Copie el certificado CA en el mismo directorio que la aplicación certutil.<br>3. Use el comando siguiente para generar los archivos `cert7.db` o `cert8.db`, `key3.db` y `secmod.db`:<br>`certutil -N -d .`<br>4. Use el comando siguiente para agregar el certificado CA al archivo `cert7.db` o `cert8.db`:<br>`certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer`<br>5. Almacene los tres archivos en un directorio del equipo que aloja la plataforma de BI. |
| cacerts | Este archivo es necesario para la autenticación mutua con SSL para las aplicaciones Java, como la rampa de lanzamiento BI. |

| Recurso | Efectúe esta acción antes de iniciar la tarea |
| --- | --- |
| | 1. Coloque el archivo `keytool` en su directorio `bin` de Java.<br>2. Use el siguiente comando para crear el archivo `cacerts`:<br>`keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore`<br>3. Almacene el archivo `cacerts` en el mismo directorio que los archivos `cert7.db` o `cert8.db` y `key3.db`. |
| Certificado de cliente | 1. Cree solicitudes de cliente individuales para los archivos `cert7.db` o `cert8.db` y `.keystore`:<br>• Para configurar el complemento LDAP, use la aplicación certutil para generar una solicitud de certificado de cliente.<br>• Use el comando siguiente para generar la solicitud de certificado de cliente:<br>`certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .`<br>`<client_dn>` incluye información como "CN=`<nombre_cliente>`, Ou=unidad`<unidad organizativa>`, O=`<nombreEmpresa>`, L=`<ciudad>`, ST=`<provincia>` y C=`<país>`.<br>2. Use la CA para autenticar la solicitud de certificado. Use el comando siguiente para recuperar el certificado e insertarlo en el archivo `cert7.db` o `cert8.db`:<br>`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`<br>3. Para facilitar la autenticación Java con SSL:<br>• Use la utilidad de herramientas clave del directorio `bin` de Java para generar una solicitud de certificado de cliente.<br>• Use el comando siguiente para generar un par clave:<br>`keytool -genkey -keystore .keystore`<br>4. Una vez especificada la información acerca del cliente, use el siguiente comando para generar una solicitud de certificado de cliente:<br>`keytool -certreq -file <certificate_request_name> -keystore .keystore` |

| Recurso | Efectúe esta acción antes de iniciar la tarea |
| --- | --- |
| | 5. Una vez la CA haya autenticado la solicitud de certificado de cliente, use el comando siguiente para agregar el certificado CA al archivo `.keystore`:<br>`keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore`<br>6. Recupere la solicitud de certificado del cliente desde la CA y use el comando siguiente para agregarlo al archivo `.keystore`:<br>`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`<br>7. Almacene el archivo `.keystore` en el mismo directorio que los archivos `cert7.db` o `cert8.db` y `cacerts` del equipo que aloja la plataforma de BI. |

1. Seleccione el nivel de seguridad SSL para usar.

   Si está usando el asistente de configuración de LDAP para configurar la autenticación LDAP por primera vez, seleccione *Autenticación mutua* desde la lista *Tipo de autenticación de SSL*, y haga clic en *Siguiente*. O, si está volviendo a configurar la configuración de autenticación LDAP, vaya al área *Autenticación* de la CMC, y haga doble clic en *LDAP*. Aparece la página *Resumen de configuración del servidor de LDAP*. Haga clic en el valor *Tipo de SSL*, y seleccione *Autenticación mutua* desde la lista *Tipo de autenticación de SSL*.

   - *Aceptar siempre el certificado del servidor*
     Es la opción de seguridad más baja. Antes de que la plataforma de BI pueda establecer una conexión SSL con el host LDAP (para autenticar usuarios y grupos de LDAP), debe recibir un certificado de seguridad del host LDAP. La plataforma de BI no comprueba el certificado que recibe.
   - *Aceptar el certificado del servidor si proviene de una entidad emisora de certificados de confianza*
     Es la opción de seguridad media. Antes de que la plataforma de BI pueda establecer una conexión SSL con el host LDAP (para autenticar usuarios y grupos LDAP), debe recibir y comprobar un certificado de seguridad enviado por el host LDAP. Para comprobar el certificado, el sistema debe buscar la CA que emitió el certificado en su base de datos de certificados.
   - *Aceptar el certificado del servidor si proviene de una entidad emisora de certificados de confianza, y si el atributo CN del certificado coincide con el nombre del host del DNS del servidor*
     Es la opción de seguridad más alta. Antes de que la plataforma de BI pueda establecer una conexión SSL con el host LDAP (para autenticar usuarios y grupos LDAP), debe recibir y comprobar un certificado de seguridad enviado por el host LDAP. Para comprobar el certificado, la plataforma de BI debe encontrar la CA que ha emitido el certificado en su base de datos de certificados y confirmar que el atributo CN del certificado del servidor coincide exactamente con el nombre de host LDAP que ha introducido en el cuadro *Agregar host LDAP* en el primer paso del asistente, si ha introducido el nombre de host LDAP como **`ABALONE.rd.crystald.net:389`**. (Utilizar **`CN =ABALONE:389`** en el certificado no funciona.) .
     El nombre del host del certificado de seguridad del servidor es el nombre del host LDAP principal. Si selecciona esta opción, no puede usar un host LDAP de conmutación por error.

> **Nota**
>
> Las aplicaciones Java ignorarán el primer y último valor y solo aceptarán el certificado de servidor si proviene de una CA de confianza.

2. En el cuadro *Host de SSL*, escriba el nombre de host de cada equipo y haga clic en *Agregar*.

   A continuación, debe agregar el nombre de host de cada equipo del despliegue de la plataforma de BI que use el SDK de la plataforma de BI. (Esto incluye el equipo que ejecuta el Servidor de administración central y el equipo que ejecuta el servidor de aplicaciones web).
3. Especifique la configuración de SSL para cada host de SSL que agregue a la lista:
   a. Seleccione *Predeterminado* en la lista de SSL.
   b. Desactive las casillas de verificación *Usar valor predeterminado*.
   c. Escriba un valor en los cuadros *Ruta del certificado y archivos de la base de datos de claves* y *Contraseña para la base de datos de claves*.
   d. Si especifica configuraciones para autenticación mutua, escriba un valor en el cuadro *Sobrenombre del certificado de cliente en la base de datos del certificado*.

> **Nota**
>
> Se usará la configuración predeterminada (para cualquier ajuste) para cualquier host con la casilla de verificación *Usar valor predeterminado* seleccionada o para cualquier nombre de equipo que no se agregue a la lista de hosts de SSL.

4. Especifique las configuraciones predeterminadas para cada host que no se encuentre en la lista y haga clic en *Siguiente*.

   Para especificar la configuración de otro host, seleccione su nombre de la lista de la izquierda y escriba los valores en los cuadros de la derecha.

> **Nota**
>
> Se usará la configuración predeterminada para cualquier ajuste (para cualquier host) con la casilla de verificación *Usar valor predeterminado* seleccionada o para cualquier nombre de equipo que no se agregue a la lista de hosts de SSL.

5. Seleccione *Básico (no SSO)* o *SiteMinder* como el método de autenticación de inicio de sesión único LDAP.
6. Seleccione cómo se crean nuevos usuarios y alias LDAP.
7. Haga clic en *Finalizar*.

## Información relacionada

Configurar el complemento LDAP para SiteMinder [página 285]

## 9.3.2.4 Modificar los ajustes de configuración de LDAP

Después de haber configurado la autenticación LDAP con el asistente de configuración de LDAP, puede modificar los parámetros de conexión y los grupos de miembros LDAP en la página *Resumen de configuración del servidor de LDAP*.

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *LDAP*.

   Si está configurada la autenticación LDAP, aparece la página *Resumen de configuración del servidor de LDAP*. En esta página, puede modificar cualquier área o campo de parámetro de conexión y modificar las opciones en el área *Grupos de miembros LDAP asignados*.
3. Elimine los grupos asignados actualmente a los que no se podrá acceder con la nueva configuración de conexión y haga clic en *Actualizar*.

   Puede eliminar grupos asignados seleccionando el grupo de usuarios y, a continuación, haciendo clic en el botón *Eliminar* en la sección *Grupos de miembros LDAP asignados*.
4. Cambie la configuración de conexión y, haga clic en *Actualizar*.
5. Modifique sus *Opciones de alias nuevos*, *Opciones de actualización del alias*, y *Opciones de usuarios nuevos* en caso necesario, y haga clic en *Actualizar*.
6. Asigne sus nuevos grupos de miembros LDAP y haga clic en *Actualizar*.

## 9.3.2.5 Configurar el complemento LDAP para SiteMinder

En esta sección se explica cómo configurar la CMC para utilizar LDAP con SiteMinder. SiteMinder es una herramienta de autenticación y acceso de usuarios de terceros que puede usar con el complemento de seguridad LDAP para crear un inicio de sesión único a la plataforma de BI.

Para usar SiteMinder y LDAP con la plataforma de BI deberá realizar cambios de configuración en dos lugares:

- Complemento de LDAP a través de la CMC
- Propiedades del archivo `BOE.war`

> **Nota**
>
> Compruebe que el administrador de SiteMinder ha activado la compatibilidad con agentes 4.x. Esto debe hacerse independientemente de la versión compatible de SiteMinder que se use. Para obtener más información sobre SiteMinder y cómo instalarlo, consulte la documentación de SiteMinder.

### Información relacionada

Configurar el host LDAP [página 276]

### 9.3.2.5.1 Para instalar las bibliotecas ETPKI

Debería instalar las bibliotecas ETPKI para asegurar el intercambio de información entre el servidor de directivas del inicio de sesión único CA y la plataforma de BI.

Antes de instalar las bibliotecas ETPKI, debe descargar e instalar el inicio de sesión único CA SDK.

La plataforma de BI admite solo el inicio de sesión único CA 12.x. Si tiene una versión anterior del inicio de sesión único CA, conocido anteriormente como CA Siteminder, debe realizar el upgrade a la versión 12.x.

1. Vaya a `<CA Single Sign-On_INSTALLDIR>\CA\sdk\etpki-install-64` para 64 bits `<CA Single Sign-On_INSTALLDIR>\CA\sdk\etpki-install` para sistemas operativos de 32 bits.

   > **Nota**
   >
   > Si el inicio de sesión único CA no está instalado en el equipo en el que está instalada la plataforma de BI, a continuación, copie las bibliotecas ETPKI en el mismo equipo.

2. Instale las bibliotecas ETPKI en un entorno de Linux:
   a. Inicie sesión con acceso root y ejecute el comando `./setup install caller=sdk veryverbose`. Aparece el mensaje de instalación correcta al final de la consola o instalación.
   b. Ejecute los comandos `export CAPKIHOME=/opt/CA/SharedComponents/CAPKI` and `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<BOE_INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/` para fijar la vía de acceso como el directorio de instalación con el usuario de la plataforma de BI.
   c. Reinicie *Server Intelligence Agent*.
3. Instale las bibliotecas ETPKI en un entorno de Windows:
   a. Inicie el símbolo del sistema con privilegios administrativos desde la ubicación de la biblioteca ETPKI.
   b. Ejecute el comando `setup.exe install caller=sdk veryverbose`.
   c. Verifique el *capki_install.log* en *%temp%* para el mensaje de conclusión exitosa de la instalación.
   d. Reinicie *Server Intelligence Agent*.

Ha instalado las bibliotecas ETPKI con éxito.

### 9.3.2.5.2 Para configurar el inicio de sesión único de LDAP con SiteMinder

1. Abra la pantalla *Configure los valores de SiteMinder* mediante uno de los siguientes métodos:
   - Seleccione SiteMinder en la pantalla *Elija un método de autenticación de inicio de sesión único LDAP* en el asistente de configuración de LDAP.
   - Seleccione *Tipo de inicio de sesión único* en la pantalla de autenticación LDAP, que está disponible si ya ha configurado LDAP y ahora está agregando SSO.
2. En el cuadro *Host de servidor de directivas*, escriba el nombre de cada servidor de directivas y, a continuación, haga clic en *Agregar*.
3. En cada host de servidor de directivas, especifique los números de puerto de *Contabilidad*, *Autenticación* y *Autorización*.
4. Introduzca el *Nombre del agente* y el *Secreto compartido*. Vuelva a introducir el secreto compartido en el cuadro *Confirmar secreto compartido*.

5. Haga clic en *Siguiente*.
6. Proceda a la configuración de las opciones LDAP.

### 9.3.2.5.3 Habilitar LDAP y SiteMinder en el archivo BOE.war

Además de especificar la configuración de SiteMinder para el complemento de seguridad de LDAP, se debe especificar la configuración de SiteMinder para las propiedades de BOE.war.

1. Vaya al directorio `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` en la instalación de la plataforma de BI.
2. Cree un nuevo archivo, utilizando el Bloc de notas u otro programa de edición de textos.
3. Especifique la siguiente declaración:

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

4. Cierre el archivo y guárdelo con el nombre **`global.properties`**, sin una extensión de archivo.
5. Cree otro archivo en el mismo directorio.
6. Especifique la siguiente declaración:

```
authentication.default=secLDAP
cms.default=[<your cms name>]:[<the CMS port number>]
```

   Por ejemplo:

```
authentication.default=secLDAP
cms.default=mycms:6400
```

7. Cierre el archivo y guárdelo con el nombre `bilaunchpad.properties`.

Las nuevas propiedades surten efecto solo después de que la aplicación Web BOE modificada se vuelva a desplegar en el equipo que ejecuta el servidor de aplicaciones Web. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web. Para obtener información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 9.3.3 Asignar grupos LDAP

Después de configurar el host de LDAP con el asistente de configuración de LDAP, se puede asignar grupos LDAP a los grupos Enterprise.

Una vez asignados los grupos LDAP, se pueden visualizar los grupos al hacer clic en la opción LDAP del área de administración *Autenticación*. Si está configurada la autenticación LDAP, el área Grupos de miembros LDAP asignados muestra los grupos LDAP asignados a la plataforma de BI.

> **Nota**
>
> También se pueden asignar grupos de Windows AD para que se autentiquen en la plataforma de BI a través del complemento de seguridad LDAP.

> **Nota**
>
> Si ha configurado LDAP respecto a AD, este procedimiento asignará sus grupos AD.

### 9.3.3.1 Asignar grupos LDAP mediante la plataforma de BI

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *LDAP*.

   Si está configurada la autenticación LDAP, aparece la página de resumen de LDAP.
3. En el área *Grupos de miembros LDAP asignados*, especifique el grupo LDAP (por nombre común o nombre completo) en el campo *Agregar grupo LDAP (por cn o dn)*, y haga clic en *Agregar*.

   Para agregar varios grupos LDAP, repita este paso. Para eliminar un grupo, resalte el grupo LDAP y haga clic en *Eliminar*.
4. En el área *Opciones de alias nuevos*, seleccione una opción para asignar alias LDAP a las cuentas de Enterprise:
   - *Asignar cada alias de LDAP agregado a una cuenta con el mismo nombre*
     Utilice esta opción cuando sepa que algunos usuarios tienen una cuenta de Enterprise existente con el mismo nombre (es decir, los alias LDAP se asignarán a usuarios existentes: la creación automática de alias está activada). Los usuarios que no tengan cuentas Enterprise existentes o que no tengan el mismo nombre en las cuentas Enterprise y LDAP, se agregan como usuarios nuevos LDAP.
   - *Crear una cuenta nueva para cada alias de LDAP agregado*
     Utilice esta opción cuando desee crear una cuenta nueva para cada usuario.
5. En el área *Opciones de actualización de alias*, seleccione una opción para especificar si los alias LDAP se crean automáticamente para todos los nuevos usuarios:
   - *Crear nuevos alias cuando se actualice el alias*
     Use esta opción para crear automáticamente nuevos alias para todos los usuarios LDAP asignados a la plataforma de BI. Se agregan nuevas cuentas LDAP para los usuarios sin cuentas de la plataforma de BI o para todos los usuarios, si se selecciona *Crear una cuenta para cada alias de LDAP agregado* y se hace clic en *Actualizar*.
   - *Crear nuevos alias solo cuando el usuario inicie una sesión*
     Use esta opción cuando el directorio LDAP que está asignando contiene varios usuarios, pero solo unos pocos de ellos usarán la plataforma de BI. El sistema no crea automáticamente alias ni cuentas de Enterprise para todos los usuarios. En su lugar, crea alias (y cuentas, en caso necesario) solo para los usuarios que inician sesión en la plataforma de BI.
6. En el área *Opciones de usuarios nuevos*, si la licencia de la plataforma de BI se basa en las funciones de usuarios, seleccione una opción para especificar las propiedades de las nuevas cuentas de Enterprise que se crean para asignar cuentas LDAP:
   - *Los usuarios nuevos se crean como usuarios con nombre*
     Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios con nombre. Las licencias de usuario con nombre se asocian con usuarios específicos y permiten que tengan

acceso al sistema basándose en sus nombres de usuario y en sus contraseñas. De esta forma, los usuarios con nombre pueden tener acceso al sistema independientemente del número de personas conectadas. Debe tener una licencia de usuario con nombre disponible por cada cuenta de usuario creada mediante esta opción.

> **Nota**
>
> El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.
>
> Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

- *Los usuarios nuevos se crean como usuarios simultáneos*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios simultáneos. Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque una licencia simultánea pequeña puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios al sistema, una licencia simultánea de 100 usuarios puede admitir 250, 500 o 700 usuarios.

7. Haga clic en *Actualizar*.

### 9.3.3.2 Desasignar grupos LDAP mediante la plataforma de BI

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *LDAP*.

   Si está configurada la autenticación LDAP, aparece la página de resumen de LDAP.
3. En el área "Grupos de miembros LDAP asignados", seleccione el grupo LDAP que desee eliminar.
4. Haga clic en *Eliminar* y en *Actualizar*.

   Los usuarios de este grupo no podrán tener acceso a la plataforma de BI.

   > **Nota**
   >
   > Las únicas excepciones ocurren cuando un usuario tiene un alias en una cuenta Enterprise. Para restringir el acceso, desactive o elimine la cuenta Enterprise del usuario.

Para denegar la autenticación LDAP para todos los grupos, desactive la casilla de verificación "Autenticación LDAP habilitada" y haga clic en *Actualizar*.

### 9.3.3.3 Asignar LDAP en Windows AD

Si se configura LDAP en Windows AD (AD), tenga en cuenta las siguientes restricciones:

- Si configura LDAP respecto a AD, podrá asignar sus usuarios, pero no podrá configurar el inicio de sesión único de AD o el inicio de sesión único en la base de datos. No obstante, los métodos de inicio de sesión único LDAP, como SiteMinder y la autenticación de confianza, seguirán estando disponibles.
- Los usuarios que sólo son miembros de grupos predeterminados de AD no podrán conectarse correctamente. Los usuarios también deben ser miembros de otro grupo creado explícitamente en AD y, además, este grupo debe asignarse. Un ejemplo de dicho grupo es el grupo "usuarios de dominio".
- Si un grupo local de dominio asignado contiene un usuario de un dominio diferente del bosque, dicho usuario no podrá conectarse con éxito.
- Los usuarios de un grupo universal perteneciente a un dominio diferente al DC especificado como host LDAP no podrán conectarse correctamente.
- No puede usar el complemento de LDAP para asignar usuarios y grupos de bosques de AD externos al bosque en el que está instalada la plataforma de BI.
- No puede asignar el grupo Usuario de dominio en AD.
- No puede asignar un grupo local de equipos.
- Si utiliza el controlador de dominio de catálogo global, existen consideraciones adicionales al asignar LDAP con respecto a AD:

| Situación | Consideraciones |
|---|---|
| Varios dominios al dirigirse al controlador de dominio de catálogo global | Puede asignar en:<br>• Grupos universales en un dominio secundario,<br>• Grupos en el mismo dominio que contiene grupos universales de un dominio secundario y<br>• Grupos universales en un dominio cruzado.<br>No puede asignar en:<br>• Grupos globales en un dominio secundario,<br>• Grupos locales en un dominio secundario,<br>• Grupos en el mismo dominio que contiene un grupo global del dominio secundario y<br>• Grupos globales de dominio cruzado.<br>Por lo general, si el grupo es universal, admitirá usuarios de dominios cruzados o secundarios. Otros usuarios no se asignarán si contienen usuarios de dominios cruzados o secundarios. Dentro del dominio al que se dirige, puede asignar grupos de dominio locales, globales y universales. |
| Asignar en grupos universales | Para asignar en grupos universales, debe dirigirse al controlador de dominio de catálogo global. También debe utilizar el número de puerto 3268 en vez del predeterminado 389. |

- Si usa varios dominios pero no se dirige al controlador de dominio de catálogo global, no se puede asignar ningún tipo de grupo desde los dominios cruzados o secundarios. Puede asignar en todos los tipos de grupos sólo desde el dominio específico al que se dirige.

## 9.3.3.4 Uso del complemento LDAP para configurar el SSO para la base de datos de SAP HANA

En esta sección se proporciona a los administradores los pasos necesarios para configurar el inicio de sesión único (SSO) entre la plataforma BI que se ejecuta en SUSE Linux 11 y la base de datos SAP HANA. La autenticación LDAP mediante Kerberos permite a los usuarios de AD autenticarse en una plataforma BI que se ejecuta en Linux, concretamente SUSE. Este escenario también admite el inicio de sesión único a SAP HANA como base de datos de generación de informes.

> **Nota**
>
> Para obtener información sobre cómo configurar la base de datos SAP HANA, consulte el *Manual de instalación del servidor y actualización de la base de datos SAP HANA*. Para obtener información sobre cómo configurar el componente de acceso a datos para SAP HANA, consulte el *Manual de acceso a datos*.

### Información general de la implementación

Para que el SSO de Kerberos funcione, los siguientes componentes deben estar en su sitio.

| Componente | Requisito |
|---|---|
| Controlador de dominio | Se debe alojar en un equipo que ejecute Active Directory configurado para usar la autenticación Kerberos. |
| Servidor de administración central | Se debe instalar y ejecutar en un equipo que ejecute SUSE Linux Enterprise 11 (SUSE). |
| Cliente Kerberos V5 | Se debe instalar junto con las utilidades y las bibliotecas requeridas en el host SUSE.<br>**Nota**<br>Use la última versión del cliente Kerberos V5. Agregue las carpetas `bin` y `lib` a las variables de entorno `PATH` y `LD_LIBRARY_PATH`. |
| complemento de autenticación de LDAP | Debe estar habilitado en el host SUSE. |
| Archivo de configuración de inicio de sesión Kerberos | Debe estar creado en el equipo que aloja el servidor de aplicaciones Web. |

### Flujo de trabajo de implementación

Deben realizarse las tareas siguientes para permitir a los usuarios de la plataforma de BI el acceso a SSO y SAP HANA mediante la autenticación Kerberos por JDBC.

1. Configuración del host AD.
2. Creación de cuentas y archivos keytab para el host SUSE y la plataforma de BI en el host AD.
3. Instalación de recursos Kerberos en el host SUSE.

4. Configuración del host SUSE para autenticación Kerberos.
5. Configuración de las opciones de autenticación Kerberos en el complemento de autenticación de LDAP.
6. Creación de un archivo de configuración de inicio de sesión Kerberos para el host de aplicación Web.

### 9.3.3.4.1 Para configurar el controlador de dominio

Es posible que tenga que establecer una relación de confianza entre el host SUSE y el controlador de dominio. Si el host SUSE se encuentra en el controlador de dominio de Windows, no tendrá que establecer la relación de confianza. Sin embargo, si el despliegue de la plataforma de lanzamiento BI y el controlador de dominio se encuentra en dominios diferentes, es posible que necesite establecer una relación de confianza entre el equipo de SUSE Linux y el controlador de dominio. Sería necesario lo siguiente:

1. Cree una cuenta de usuario para el equipo SUSE que ejecute la plataforma de BI.
2. Crear un Nombre de principal de servicios (SPN) de host.

> **Nota**
>
> El SPN debería tener un formato adecuado a las convenciones de Windows AD: host/`<nombre de host>`@`<DNS_REALM_NAME>`. Use, en minúsculas, un nombre completo de dominio para /`<nombre de host>`. El `<DNS_REALM_NAME>` se debería especificar en mayúsculas.

3. Ejecute el comando de configuración de keytab de Kerberos, `ktpass` para asociar el SPN con la cuenta de usuario:

```
c:\> ktpass -princ host/<hostname>@<DNS_REALM_NAME>-mapuser <username> -pass
Password1 -crypto RC4-HMAC-NT -out <username>base.keytab
```

Los pasos que se indican a continuación se deben realizar en el equipo que aloja el controlador de dominio.

1. Cree una cuenta de usuario para el servicio que ejecute la plataforma de BI.
2. En la página *Cuentas de usuario*, haga clic con el botón derecho en la nueva cuenta de servicio y seleccione *Propiedades* > *Delegación*.
3. Seleccione *Trust this user for delegation to any service (Kerberos only) (Confiar en este usuario para la delegación a cualquier servicio [solo Kerberos])*
4. Ejecute el comando de configuración de keytab de Kerberos, `ktpass` para crear una cuenta SPN para la nueva cuenta de servicio:

```
c:\>ktpass -princ <sianame>/<service_name>@<DNS_REALM_NAME> -mapuser
<service_name> -pass <password> -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
-out <sianame>.keytab
```

> **Nota**
>
> El SPN deberá tener un formato adecuado a las convenciones de Windows AD: sianame/`<nombre_servicio>`@`<DNS_REALM_NAME>`. Especifique el `<nombre de servicio>` en minúsculas, ya que, de lo contrario, la plataforma de SUSE no podrá resolverla. El `<DNS_REALM_NAME>` se debería especificar en mayúsculas.

| Parámetro | Descripción |
| --- | --- |
| `-princ` | Especifica el nombre de principal para la autenticación de Kerberos. |
| `-out` | Especifica el nombre del archivo `keytab` de Kerberos que se debe generar. Debería coincidir con el `<sianame>` utilizado en `-princ`. |
| `-mapuser` | Especifica el nombre de la cuenta de usuario a la que se ha asignado el SPN. El Agente de inteligencia de servidor se ejecuta en esta cuenta. |
| `-pass` | Especifica la contraseña que usa la cuenta de servicio. |
| `-ptype` | Especifica el tipo de principal:<br>`-ptype KRB5_NT_PRINCIPAL` |
| `-crypto` | Especifica el tipo de cifrado que se debe usar con la cuenta de servicio:<br>`-crypto RC4-HMAC-NT` |

Ha generado los archivos keytab necesarios para la relación de confianza entre el equipo SUSE y el controlador de dominio.

Debe transferir el archivo o archivos keytab al equipo SUSE y guardarlos en el directorio `/etc`.

## 9.3.3.4.2 Para configurar el equipo SUSE Linux Enterprise 11

Se requieren los siguientes recursos para configurar Kerberos en el equipo SUSE Linux que ejecuta la plataforma de BI:

- Archivos keytab creados en el controlador de dominio. El archivo keytab creado por el servicio de la plataforma de BI es obligatorio. El keytab para el host del SUSE se recomienda específicamente para los casos en los que el host de la plataforma de BI y el controlador del dominio estén en dominios distintos.
- La última biblioteca Kerberos V5 (incluido el cliente Kerberos) debe instalarse en el host del SUSE. Debe añadir la ubicación para los binarios a la `RUTA` y a las variables de entorno de `LD_LIBRARY_PATH`. Para verificar que el cliente Kerberos está instalado y configurado correctamente, asegúrese de que en el host del SUSE existen las siguientes utilidades y bibliotecas:
  - `kinit`
  - `ktutil`
  - `kdestroy`
  - `klist`
  - `/lib64/libgssapi_krb5.so.2.2`
  - `/lib64/libkrb5.so.3.3`
  - `/lib/libkrb5support.so.0.1`
  - `/lib64/libk5crypto.so.3`
  - `/lib64/libcom_err.so.2`

> → Sugerencias
>
> Ejecutar `rpm -qa | grep krb` para comprobar la versión de estas bibliotecas.
> Para obtener información sobre el último cliente Kerberos, bibliotecas Kerberos y configuración del host de UNIX, consulte http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5 .

Después de que todos los recursos necesarios estén disponibles en el host de SUSE, siga las instrucciones que figuran más abajo para configurar la autenticación Kerberos.

> ⓘ Nota
>
> Para llevar a cabo estos pasos debe tener privilegios de raíz.

1. Para fusionar los archivos keytab, ejecute el comando siguiente:

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. Edite el archivo `/etc/kerb5.conf` para hacer referencia al controlador de dominio (en la plataforma de Windows) como el controlador de dominio Kerberos (KDC).

   Use el ejemplo siguiente:

```
[domain_realm]
 .name.mycompany.corp = DOMAINNAME.COM
  name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
        forwardable = true
           default_realm = DOMAINNAME.COM
           default_tkt_enctypes = rc4-hmac
           default_tgs_enctypes = rc4-hmac

[realms]
        DOMAINNAME.COM = {
             kdc = machinename.domainname.com
            }
```

> ⓘ Nota
>
> El archivo `krb5.conf` contiene información sobre la configuración de Kerberos, incluidas las ubicaciones de KDC y los servidores para las zonas de interés de Kerberos, las aplicaciones Kerberos y las asignaciones de nombres de host para las zonas Kerberos. Normalmente, el archivo `krb5.conf` se instala en el directorio `/etc`.

3. Añada el controlador de dominio a `/etc/hosts` para que el host SUSE pueda ubicar el KDC.
4. Ejecute el programa `kinit` del directorio `/usr/local/bin` para verificar que Kerberos se ha configurado correctamente. Verifique que una cuente de usuario de cuenta AD puede iniciar sesión en el equipo SUSE.

> → Sugerencias
>
> El KDC debería emitir un vale de concesión de vales (TGT) que puede visualizarse en la caché. Use el programa `klist` para visualizar el TGT.

## Ejemplo

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>
> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal08/10/11 17:33:43 08/11/11 03:33:46
krbtgt/<domain>@<domain>renew until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached
>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

Use también el `kinit` para probar los SPN.

## 9.3.3.4.3 Para configurar las opciones de autenticación de Kerberos para LDAP

Antes de configurar la autenticación de Kerberos para LDAP, primero tiene que habilitar y configurar el complemento de autenticación LDAP de la plataforma de BI para conectarse al directorio AD. Para utilizar la autenticación LDAP, tendrá que asegurarse primero de que ha configurado el directorio LDAP correspondiente.

> **Nota**
>
> Al ejecutar el *Asistente de configuración LDAP* tiene que especificar el *Servidor de aplicaciones de Microsoft Active Directory* y proporcionar la información detallada de configuración solicitada.

Después de haber habilitado y conectado la autenticación de LDAP al Servidor de aplicaciones de Microsoft Active Directory, aparece el área *Habilitar autenticación de Kerberos* en la página de Resumen de la configuración del servidor LDAP. Use esta área para configurar la autenticación de Kerberos, que se requiere para el inicio de sesión único en la base de datos SAP HANA desde un despliegue de plataforma de BI en SUSE.

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *LDAP*.

   La página de *Resumen de la configuración del servidor LDAP* aparece en los casos en que pueda modificar cualquiera de los parámetros o campos de conexión.
3. Para configurar la autenticación de Kerberos, lleve a cabo los siguientes pasos en el área *Habilitar autenticación de Kerberos*:
   a. Haga clic en *Habilitar autenticación de Kerberos*.
   b. Haga clic en *Contexto de seguridad de caché (requerido para SSO en base de datos)*.

      > **Nota**
      >
      > Se requiere específicamente la habilitación del contexto de seguridad de caché para un inicio de sesión único en SAP HANA.

   c. Especifique el Nombre de principal de servicios (SPN) para la cuenta de la plataforma de BI en el *Nombre de principal de servicios*.

      El formato para especificar el SPN es `<sianame/service>@<DNS_REALM_NAME>`, donde

| | |
|---|---|
| `<sianame>` | Nombre del Agente de inteligencia de servidor |
| `<service >` | Nombre de la cuenta de servicio utilizada para ejecutar la plataforma de BI |
| DNS_REALM_NAME | El nombre del dominio del controlador de dominio en mayúsculas |

> → Sugerencias
>
> Al especificar el SPN, recuerde que `<sianame/service>` es sensible a mayúsculas y minúsculas.

d. Especifique el dominio para el controlador de dominio en*Área Kerberos predeterminada*.

e. Especifique `userPrincipalName` en *Nombre principal de usuario*.

   La aplicación autenticación LDAP usa este valor para proporcionar valores de usuario ID requeridos por Kerberos. El valor especificado debería coincidir con el nombre proporcionado al crear los archivos keytab.

4. Haga clic en *Actualizar* para guardar y enviar los cambios.

Ha configurado las opciones de autenticación de Kerberos para hacer referencia a cuentas de usuario en el directorio AD.

Tiene que crear un archivo de configuración de inicio de sesión Kerberos - `bscLogin.conf` - para habilitar el inicio de sesión Kerberos y el inicio de sesión único.

### Información relacionada

Configuración de la autenticación LDAP [página 276]

## 9.3.3.4.4 Para crear un archivo de configuración de inicio de sesión de Kerberos

Para habilitar el de inicio de sesión y el inicio de sesión único de Kerberos, tiene que agregar un archivo de configuración de inicio de sesión en el equipo que tenga alojado el servidor de aplicaciones Web de la plataforma de Business Intelligence.

1. Cree un archivo llamado `bscLogin.conf` y almacénelo en el directorio `/etc`.

> ⓘ Nota
>
> Puede almacenar este archivo en una ubicación diferente. Sin embargo, si lo hace, deberá especificar su ubicación en las opciones de Java. Recomendamos que el archivo `bscLogin.conf` y los archivos keytab de Kerberos se coloquen en el mismo directorio. En un despliegue distribuido, tiene que agregar un archivo `bscLogin.conf` para cada equipo que aloje un servidor de aplicaciones Web.

2. Agregue el código siguiente al archivo de configuración `bscLogin.conf` de inicio de sesión:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

```
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="<nombre principal>";
};
```

> **Nota**
>
> La sección siguiente es necesaria para el inicio de sesión único:
>
> ```
> com.businessobjects.security.jgss.accept {
> com.sun.security.auth.module.Krb5LoginModule required
> storeKey=true
> useKeyTab=true
> keyTab="/etc/krb5.keytab"
> principal="<nombre principal>";
> };
> ```

3. Guarde y cierre el archivo.

## 9.3.3.5 Solución de problemas de cuentas LDAP nuevas

- Si crea una nueva cuenta de usuario LDAP y no pertenece a una cuenta de grupo asignada a la plataforma de BI, asigne el grupo o agregue la nueva cuenta de usuario LDAP a un grupo que ya esté asignado al sistema.
- Si crea una nueva cuenta de usuario LDAP y la cuenta pertenece a una cuenta de grupo asignada a la plataforma de BI, actualice la lista de usuarios.

### Información relacionada

Configuración de la autenticación LDAP [página 276]
Asignar grupos LDAP [página 287]

# 9.4 Autenticación de Windows AD

## 9.4.1 Uso de la autenticación de Windows AD

### 9.4.1.1 Configuración inicial y requisitos de compatibilidad de Windows AD

En esta sección, se indica el proceso de configuración de la autenticación de Windows Active Directory (AD) para trabajar con la plataforma de BI. Todos los flujos de trabajo punto a punto necesarios para funcionar se presentan junto con las pruebas de validación y las comprobaciones de los requisitos previos.

> **Nota**
>
> Para obtener información adicional sobre cómo se configura la autentificación de Windows AD, consulte la base de conocimientos de SAP 1631734, disponible enhttps://service.sap.com/sap/support/notes/1631734.

#### Requisitos de compatibilidad

Para facilitar la autenticación de AD en la plataforma de BI, debe recordar los siguientes requisitos de compatibilidad.

- El CMS siempre se debe instalar en una plataforma Windows compatible.
- Determinadas aplicaciones de la plataforma de BI solo pueden utilizar métodos de autenticación concretos. Por ejemplo, las aplicaciones como la Plataforma de lanzamiento de BI y La Consola de administración central solo admiten Kerberos.

#### Flujo de trabajo recomendado de configuración de AD

Para configurar por primera vez la autenticación de AD con la plataforma de BI, use el siguiente flujo de trabajo:

1. Configure el controlador de dominio.
2. Configure la autenticación de AD en la CMC.
3. Configure la cuenta de usuario de AD en el Agente de inteligencia de servidor (SIA).
4. Configure el servidor de aplicaciones web para la autenticación de AD con Kerberos.

> **Nota**
>
> Use este flujo de trabajo tanto si necesita inicio de sesión único (SSO) como si no. El flujo de trabajo descrito en las secciones siguientes le permitirá conectarse manualmente (usando un nombre de usuario y contraseña de AD) a la plataforma de BI. Una vez que haya configurado correctamente la autenticación de AD manual, tendrá acceso a una sección detallada para guiarle a lo largo del proceso de configuración del SSO para la autenticación de AD.

## 9.4.2 Preparación del Controlador de dominio

### 9.4.2.1 Configuración de una cuenta de servicio para la autenticación de AD con Kerberos

Para configurar la plataforma de BI para que funcione con la autenticación de Windows AD (Kerberos) es necesaria una cuenta de servicio. Puede crear una nueva cuenta de dominio o utilizar una existente. La cuenta de servicio se usará para ejecutar los servidores de la plataforma de BI. Después de configurar la cuenta, deberá configurar un SPN para la cuenta. Este SPN se usa para importar grupos de usuarios de AD a la plataforma de BI.

> **Nota**
>
> Para usar AD con el SSO, deberá repetir más adelante la configuración de la cuenta de servicio para otorgar a la cuenta los derechos apropiados y configurarla para la delegación limitada.

#### 9.4.2.1.1 Para configurar la cuenta de servicio en un dominio de Windows 2008

Deberá configurar una nueva cuenta de servicio para habilitar correctamente la autenticación de Windows AD usando el protocolo de Kerberos. Dicha cuenta de servicio se usará primordialmente para permitir que los usuarios de un grupo de Windows AD determinado inicien sesión en la plataforma de lanzamiento de BI. Esta tarea se realiza en el equipo del controlador del dominio de AD.

1. Cree una cuenta de servicio nueva con una contraseña en el controlador de dominio principal.
2. Use el comando `setspn -s` para añadir los nombres principales del servicio (SPN) en la cuenta de servicio que ha creado en el paso 1. Especifique los nombres principales de servicio (SPN) para la cuenta de servicio, así como el servidor, el dominio completo del servidor (Fully Qualified Domain Server) y la dirección IP del equipo en el que se despliega la plataforma de lanzamiento de BI.
   Por ejemplo:

   ```
   setspn –s BICMS/service_account_name.domain.com serviceaccountname
   setspn -s HTTP/<servername> <servicename>
   setspn -s HTTP/<servername.domain.com> <servicename>
   setspn -s HTTP/<ip address of server> <servicename>
   ```

   `BICMS` es el nombre del equipo sobre el cual se ejecuta el SIA, `<servername>` es el nombre del servidor sobre el que se despliega la plataforma de lanzamiento de BI y `< servernamedomain>` es el nombre completo del dominio (Fully Qualified Domain Name).
3. Ejecute `setspn -l <servicename>`para verificar que los nombres de representantes de servicio se han agregado a la cuenta de servicio.
   El resultado del comando debería contener todos los nombres SPN registrados, como se muestra a continuación:

   ```
   Registered ServicePrincipalNames for
   CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
   HTTP/<ip address of server>
   HTTP/<servername>.@example.com
   ```

```
HTTP/<servername>
<servername>/<servicename>@example.com
```

A continuación aparece un ejemplo de resultado:

```
C:\Users\Admin>setspn -L bossosvcacct
Registered ServicePrincipalNames for
CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
        BICMS/bossosvcacct@example.com
        HTTP/Tomcat HTTP/Tomcat@example.com
        HTTP/Load_Balancer.@example.com
```

Una vez creada, debe otorgarse derechos a la cuenta de servicio y agregarla al grupo de administradores locales del servidor. El SPN se usará para importar grupos de AD en la próxima sección.

## 9.4.3 Configuración de la autenticación de AD en la Consola de administración central (CMC)

### 9.4.3.1 Complemento de seguridad de Windows AD

El complemento de seguridad de Windows AD le permite asignar cuentas de usuario y grupos desde la base de datos de usuario de AD 2008 a la plataforma de BI. También permite que el sistema verifique todas las solicitudes de inicio de sesión que especifican la autenticación de AD. Los usuarios se autentican en la base de datos de usuarios de AD y se comprueba que sean miembros de un grupo de AD asignado antes de que el Servidor de administración central (CMS) les conceda una sesión activa. Puede usar el complemento para configurar actualizaciones para los grupos de AD importados.

El complemento de seguridad de Windows AD le permite configurar lo siguiente:

- La autenticación de Windows AD con Kerberos
- La autenticación de Windows AD con NTLM

- La autenticación de Windows AD con SiteMinder para el inicio de sesión único

El complemento de seguridad de AD es compatible con dominios de AD 2008 que se ejecuten en modo nativo o en modo mixto.

Una vez asignados, los usuarios y grupos de AD podrán acceder a las herramientas cliente de la plataforma de BI mediante la opción de autenticación de *Windows AD*.

- La autenticación de Windows AD funciona si el CMS se ejecuta en Windows. Para que funcione el inicio de sesión único en la base de datos, los servidores de informes también se deben ejecutar en Windows. Si no, el resto de servidores y servicios pueden ejecutarse en cualquier plataforma compatible con la plataforma de BI.

  > **Nota**
  >
  > La configuración se ha realizado y probado solo con SUSE linux Enterprise 11.

- El complemento de Windows AD para la plataforma de BI admite dominios dentro de varios bosques.

## 9.4.3.2 Asignar grupos y usuarios de Windows AD

Para poder importar los grupos de usuarios de AD en la plataforma de BI, debe haber completado las siguientes acciones previas:

- Haber creado una cuenta de servicio en el controlador de dominio para la plataforma de BI. La cuenta se usará para ejecutar los servidores de la plataforma de BI.

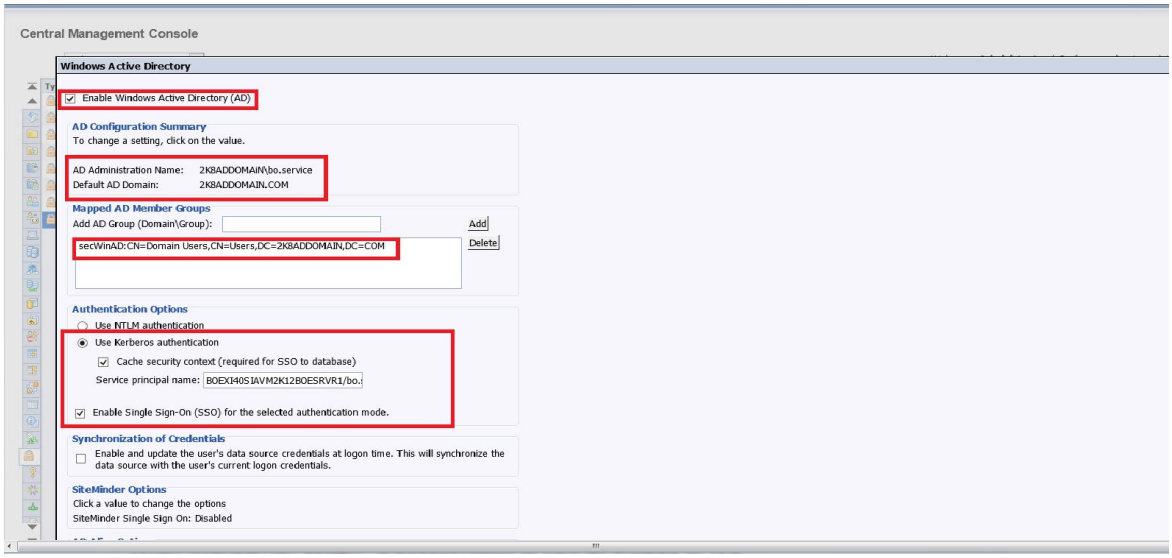
  > **Nota**
  >
  > Para habilitar la autenticación de AD con inicio de sesión único (SSO) de Vintela, debe proporcionar un SPN que esté configurado para este fin. Los pasos siguientes son para configurar la autenticación manual de AD en la plataforma de BI. Una vez que haya configurado la autenticación manual de AD, consulte la sección *Configuración de inicio de sesión único* en este capítulo para obtener detalles sobre cómo agregar el SSO a la configuración de autenticación de AD.

- Verificado que el SPN que contiene el nombre del equipo en el cual se ejecuta el SIA se haya agregado a la cuenta de servicio.

Los pasos 1 a 11 siguientes son obligatorios para importar los grupos de AD en la plataforma de BI.

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *Windows AD*.
3. Seleccione la casilla de verificación *Habilitar Windows Active Directory (AD)*.
4. En el área *Resumen de configuración de AD*, haga clic en el vínculo situado junto a *Nombre de administración de AD*.

   > **Nota**
   >
   > Antes de configurar los complementos de Windows AD, aparecerá este vínculo como comillas. Una vez que se haya guardado la configuración, el enlace se rellenará con nombres de administración de AD.




5. Introduzca el nombre y la contraseña de una cuenta de usuario de dominio habilitada.

   Las credenciales de administración pueden tener cualquiera de los siguientes formatos:

   - Nombre NT (`NombreDominio\NombreUsuario`)
   - UPN (`usuario@nombre_dominio_DNS`)

   La plataforma de BI usará esta cuenta para consultar la información desde AD. La plataforma no modifica, agrega ni elimina contenidos de AD. Dado que solo lee la información, solo se necesitan los derechos adecuados.

   > **Nota**
   >
   > La autenticación de AD no continuará si la cuenta usada para leer el directorio AD pasa a ser no válida (por ejemplo, si la contraseña de la cuenta se cambia o caduca o bien si la cuenta se desactiva).

6. Escriba el dominio de AD en el cuadro *Dominio predeterminado de AD*.

   El dominio debe especificarse como el NOMBRE COMPLETO DE DOMINIO en MAYÚSCULAS o un nombre de dominio secundario desde el que la mayor parte de los usuarios iniciarán la sesión en la plataforma de BI. Esto debe coincidir con el dominio predeterminado especificado en los archivos de configuración Kerberos que se utilizan para configurar el servidor de aplicaciones. Puede asignar grupos desde el dominio predeterminado sin especificar el prefijo del nombre del dominio. Si se introduce un nombre de dominio de AD predeterminado, los usuarios de dicho dominio no tendrán que especificar el nombre de dominio de AD al iniciar sesión en la plataforma de BI mediante la autenticación de AD.

7. En el área *Grupos de miembros de AD asignados*, introduzca el dominio/grupo de AD en el cuadro *Agregar grupo de AD (dominio\grupo)* y use uno de estos formatos para asignar los grupos:

   - El nombre de cuenta de Security Account Manager (SAM), también denominado nombre NT (`NombreDominio\NombreGrupo`)
   - DN (`cn=GroupName, ....., dc=DomainName, dc=com`)

   > **Nota**
   >
   > Si desea asignar un grupo local, puede usar solo el formato de nombre NT: `\\<ServerName>\<GroupName>`. AD no admite usuarios locales. Los usuarios locales pertenecientes a un grupo local asignado no se asignarán a la plataforma de BI. Por este motivo, no pueden acceder al sistema.

> → Sugerencias
>
> Al iniciar una sesión manualmente en la plataforma de lanzamiento de BI, los usuarios de otros dominios deben añadir en mayúsculas el nombre de dominio después de su nombre de usuario. Por ejemplo `CHILD.PARENTDOMAIN.COM` es el dominio en
>
> ```
> user@CHILD.PARENTDOMAIN.COM
> ```

8. Haga clic en *Agregar*.

   El grupo se agrega a la lista situada debajo de *Grupos de miembros de AD asignados* .

9. En el área *Grupos de miembros AD asignados*, especifique el dominio\grupo deseado en el campo *Buscar grupo AD (Dominio\Grupo)*.

   Buscará el grupo deseado de la lista. Puede elegir también *Mostrar* para ver la lista completa de grupos AD en un cuadro de diálogo separado.

10. En *Opciones de autenticación*, seleccione *Utilizar autenticación Kerberos*.
11. En el cuadro *Nombre principal del servicio*, introduzca el SPN asignado a la cuenta de servicio que creó para ejecutar los servidores de la plataforma de BI.

    > ⓘ Nota
    >
    > Es necesario especificar el SPN para la cuenta de servicio de ejecuta el SIA. Por ejemplo: `BICMS/bossosvcacct.domain.com`.

12. Haga clic en *Actualizar*.

    > ⚠ Precaución
    >
    > No siga adelante si las asignaciones de los grupos o usuarios no son correctas. Para solucionar cuestiones de asignación específicas de grupos de AD consulte la nota 1631734 de SAP.

    > ⓘ Nota
    >
    > Si ha asignado correctamente las cuentas de grupo de AD y no quiere configurar las opciones de autenticación de AD o las actualizaciones de grupos de AD, omita los pasos 12 a 19. Puede configurar esta configuración opcional después de que haya instalado satisfactoriamente la autentificación manual AD Kerberos.

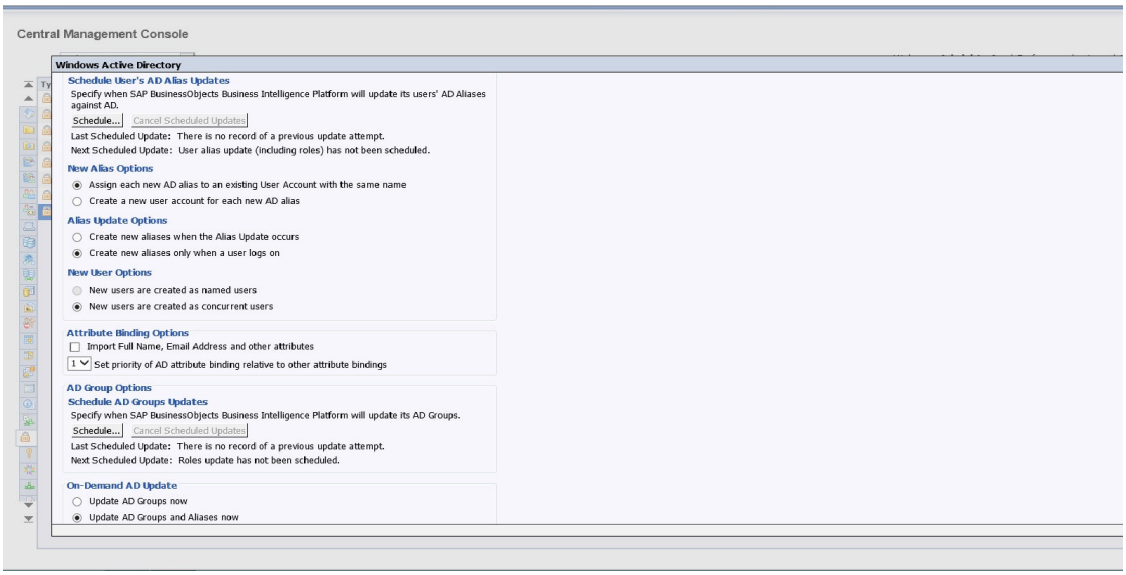
13. Si su configuración requiere el SSO en una base de datos, seleccione *Contexto de seguridad de caché*.

    > ⓘ Nota
    >
    > Si esta es su configuración inicial de la autenticación de AD, se recomienda que primero configure correctamente la autenticación manual de AD antes de considerar la configuración adicional que se necesita para el SSO.

14. Seleccione *Habilitar el inicio de sesión único para el modo de autenticación seleccionado* si necesita SSO para la configuración de la autenticación de AD.
15. En el área *Sincronización de credenciales*, seleccione una opción para habilitar y actualizar las credenciales de inicio de sesión de origen de datos del usuario de AD.

    Esta opción sincroniza el origen de datos con las credenciales actuales de inicio de sesión del usuario, lo que permite que se ejecuten informes programados cuando el usuario no haya iniciado la sesión en la plataforma de BI y el SSO de Kerberos no esté disponible.

16. En el área *Opciones de alias de AD*, especifique el modo en que los nuevos alias se agregan y se actualizan en la plataforma de BI.
    a. En el área *Opciones de alias nuevos*, seleccione una opción para asignar nuevos alias a las cuentas de Enterprise:
        - *Asignar cada nuevo alias de AD a una cuenta de usuario existente con el mismo nombre*
          Seleccione esta opción cuando sepa que algunos usuarios disponen de una cuenta de Enterprise existente con el mismo nombre; es decir, los alias de AD se asignarán a usuarios existentes (la creación automática de alias está activada). Los usuarios que no tengan cuentas de Enterprise existentes o que no tengan el mismo nombre en las cuentas de Enterprise y AD, se agregan como usuarios nuevos.
        - *Crear una nueva cuenta de usuario para cada nuevo alias de AD*
          Seleccione esta opción cuando desee crear una cuenta nueva para cada usuario.
    b. En el área *Opciones de actualización de alias*, seleccione una opción para administrar las actualizaciones de alias de las cuentas de Enterprise:
        - *Crear nuevos alias cuando se actualice el alias*
          Use esta opción para crear automáticamente nuevos alias para todos los usuarios de AD asignados en la plataforma de BI. Se agregan nuevas cuentas de AD para los usuarios sin cuentas de la *plataforma de BI* o para todos los usuarios si ha seleccionado la opción *Crear una nueva cuenta de usuario para cada nuevo alias de AD* y ha hecho clic en Actualizar.
        - *Crear nuevos alias solo cuando el usuario inicie sesión*
          Use esta opción cuando el directorio de AD que está asignando contiene varios usuarios, pero solo unos pocos de ellos usarán la plataforma de BI. La plataforma no crea automáticamente alias ni cuentas de Enterprise para todos los usuarios. En su lugar, crea alias (y cuentas, en caso necesario) solo para los usuarios que inician sesión en la plataforma de BI.




    c. En el área *Opciones de usuarios nuevos*, seleccione una opción para crear nuevos usuarios:
        - *Los usuarios nuevos se crean como usuarios con nombre*
          Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios con nombre. Las licencias de usuario con nombre están asociadas a usuarios específicos y permiten el acceso a la plataforma de BI en función de sus nombres de usuario y sus contraseñas. Esto da acceso al sistema a los usuarios con nombre, independientemente del número de personas conectadas.

Debe tener una licencia de usuario con nombre disponible por cada cuenta de usuario creada mediante esta opción.

> **Nota**
>
> El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.
>
> Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

- *Los usuarios nuevos se crean como usuarios simultáneos*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios simultáneos. Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque una licencia simultánea pequeña puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios al sistema, una licencia simultánea de 100 usuarios puede admitir 250, 500 o 700 usuarios.

17. Para configurar cómo se programan actualizaciones de alias de AD, haga clic en *Programar*.
    a. En el cuadro de diálogo *Programar*, seleccione una periodicidad de la lista *Ejecutar objeto*.
    b. Configure otras opciones y parámetros de programación según sea necesario.
    c. Haga clic en *Programar*.
    Cuando se produce una actualización de alias, la información de grupo también se actualiza.
18. En el área *Opciones de enlace de atributos*, especifique la prioridad de enlace de atributos para el complemento de AD:
    a. Seleccione la casilla de verificación *Importar nombre completo, dirección de correo electrónico y otros atributos*.
    Los nombres completos y descripciones que se usan en las cuentas de AD se importan y almacenan con los objetos de usuario en la plataforma de BI.
    b. Especifique una opción para *Establecer prioridad del enlace de atributos de AD en relación con otros enlaces de atributos*.

    Si la opción está configurada en 1, los atributos de AD tendrán prioridad cuando estén habilitados AD y otros complementos (LDAP y SAP). Si la opción está configurada en 3, tendrán prioridad los atributos de otros complementos habilitados. Las vinculaciones deben estar fijadas en diferentes valores. Si fija varios complementos de autenticación al mismo valor de vinculación, es posible que se produzcan resultados no esperados.
19. En el área *Opciones de grupo de AD*, configure las actualizaciones del grupo de AD:
    a. Haga clic en *Programar*.
    Aparecerá el cuadro de diálogo *Programar*.
    b. Seleccione una periodicidad de la lista *Ejecutar objeto*.
    c. Configure otras opciones y parámetros de programación según sea necesario.
    d. Haga clic en *Programar*.

    El sistema programará la actualización y la ejecutará según la programación que haya especificado. La siguiente actualización programada para las cuentas de grupo de AD se muestra bajo las *Opciones de grupo de AD*.

20. En el área *Actualización de AD a petición*, seleccione una de las siguientes opciones:
    - *Actualizar grupos AD ahora*
      Seleccione esta opción si quiere que se inicie la actualización de todos los grupos programados de AD al hacer clic en *Actualizar*. La siguiente actualización de grupo de AD programa se enumera en *Opciones del grupo AD*.
    - *Actualizar grupos AD y alias ahora*
      Seleccione esta opción si quiere que se inicie la actualización de todos los grupos de AD y los alias de usuario programados al hacer clic en *Actualizar*. Las siguientes actualizaciones programadas se enumeran en *Opciones de grupo de AD* y *Opciones de alias de AD*.
    - *No actualizar ahora grupos y alias de AD*
      No se actualizará ningún grupo de AD ni alias de usuario al hacer clic en *Actualizar*.
21. Haga clic en *Actualizar* y en *Aceptar*.

Para verificar que realmente haya importado las cuentas de usuario de AD, vaya a *CMC* > *Usuarios y grupos* > *Jerarquía de grupos* y seleccione el grupo de AD que ha asignado para ver los usuarios de ese grupo. Se mostrarán los usuarios actuales y anidados del grupo de AD.

## Información relacionada

Para crear un archivo de configuración de Kerberos [página 311]

## 9.4.3.3 Programar actualizaciones para grupos de Windows AD

La plataforma de BI permite a los administradores programar actualizaciones para los grupos y alias de usuario de AD. Esta función está disponible para la autenticación AD con Kerberos o NTLM. La CMC también permite ver la hora y la fecha de cuando se realizó la última actualización.

> **Nota**
>
> Para que la autenticación AD funcione en la plataforma de BI, debe configurar el modo en que se programan las actualizaciones para los grupos y alias de AD.

Cuando programa una actualización, puede elegir entre los patrones de repetición que se resumen en la siguiente tabla:

| Patrón de periodicidad | Descripción |
|---|---|
| Cada hora | La actualización se ejecutará cada hora. Se debe especificar a qué hora comenzará así como las fechas de inicio y fin. |
| Diario | La actualización se ejecutará cada día o se ejecutará el número de días especificado. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |

| Patrón de periodicidad | Descripción |
|---|---|
| Semanal | La actualización se ejecutará cada semana. Se puede ejecutar una o varias veces a la semana. Puede especificar en qué días y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Mensual | La actualización se ejecutará cada mes o cada varios meses. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día N de cada mes | La actualización se ejecutará un día específico del mes. Puede especificar en qué día del mes y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Primer lunes de cada mes | La actualización se ejecutará el primer lunes de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Último día del mes | La actualización se ejecutará el último día de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día X de la semana N de cada mes | La actualización se ejecutará un día especificado de una semana especificada del mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Calendario | La actualización se ejecutará en las fechas indicadas en un calendario que se haya creado previamente. |

## Programación de actualizaciones de grupos AD

La plataforma de BI se basa en AD para la información de usuario y grupo. Para minimizar el volumen de consultas enviadas a AD, el complemento de AD almacena en caché la información sobre los grupos y cómo se relacionan entre sí y su pertenencia de usuario. La actualización no se ejecuta cuando no se ha definido una programación específica.

Debe usar la CMC para configurar la periodicidad de la actualización del grupo. Esto se debe programar para que refleje la frecuencia con la que se modifica la información de los miembros del grupo.

## Programar actualizaciones de alias de usuario de AD

Se puede crear un alias para los objetos de usuario en una cuenta de AD, lo que permite que los usuarios usen sus credenciales de AD para iniciar sesión en la plataforma de BI. Las actualizaciones de cuentas AD se propagan a la plataforma de BI con el complemento de AD. Las cuentas que se crean, eliminan o deshabilitan en AD se crearán, eliminarán o deshabilitarán de igual modo en la plataforma de BI.

Si no programa actualizaciones de alias de AD, las actualizaciones solo se producirán cuando:

- Un usuario inicia sesión.
- Un administrador selecciona la opción *Actualizar ahora grupo y alias de AD* en el área *Actualización de AD a petición* de la CMC.

> **Nota**
>
> No se almacena ninguna contraseña de AD en el alias de usuario.

## 9.4.4 Configuración del servicio de la plataforma de BI para ejecutar el SIA

### 9.4.4.1 Ejecución de SIA bajo la cuenta de servicio de la plataforma de BI

Para admitir la autenticación de AD Kerberos en la plataforma de BI, deberá conceder a la cuenta de servicio el derecho para actuar como parte del sistema operativo. Esto debe llevarse a cabo en cada equipo que ejecute un Agente de inteligencia de servidor (SIA) con el Servidor de administración central (CMS).

Para permitir que la cuenta de servicio ejecute/inicie el SIA, debe configurar ajustes específicos del sistema operativo que se describen en esta sección.

> **Nota**
>
> Si va a necesitar inicio de sesión único en la base de datos, el SIA debe incluir los servidores siguientes:
>
> - Servidor de procesamiento de Crystal Reports
> - Servidor de aplicaciones de informes
> - Servidor de procesamiento de Web Intelligence

### 9.4.4.2 Para configurar el SIA para ejecutarse bajo la cuenta de servicio

Antes de configurar la cuenta de SIA para que se ejecute bajo la cuenta de servicio de la plataforma de BI, es necesario completar las siguientes acciones previas:

- Ha creado una cuenta de servicio en el controlador de dominio de la plataforma de BI.
- Ha verificado que los nombres principales del servicio (SPN) necesarios se hayan agregado a la cuenta de servicio.
- Ha asignado correctamente los grupos de usuarios de AD a la plataforma de BI.

Si desea conceder derechos específicos a un usuario:

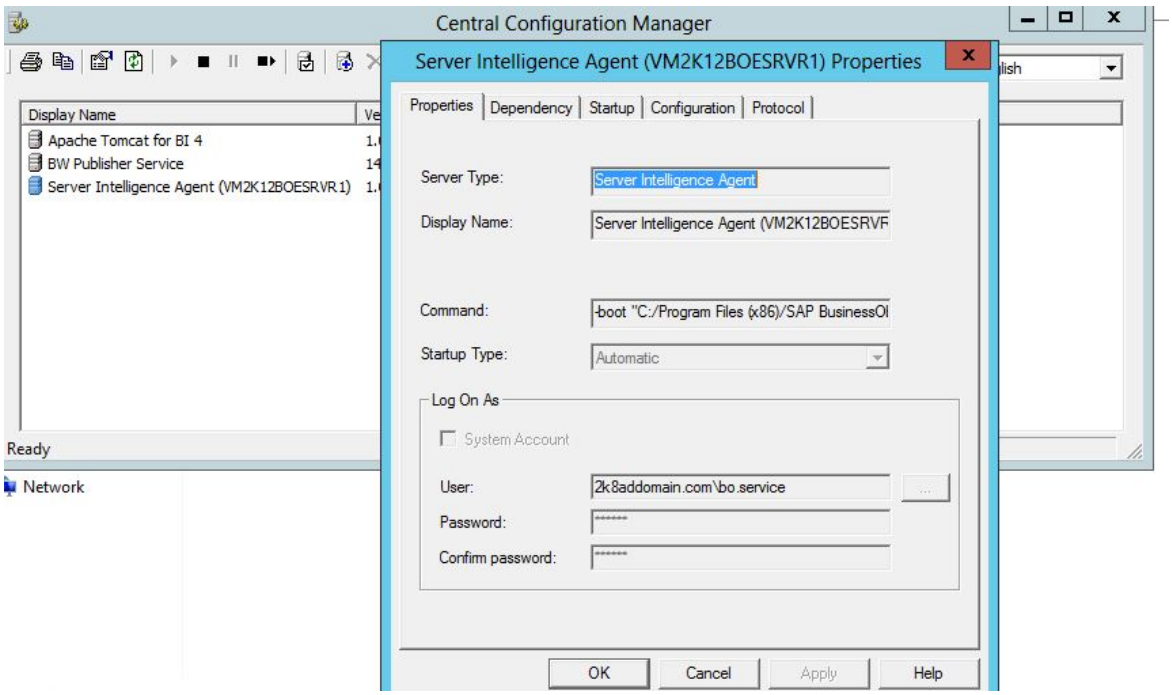
1. Haga clic en *Inicio > Panel de control > Herramientas administrativas > Directiva de seguridad local*.
2. Expanda *Directivas locales* y, a continuación, haga clic en *Asignación de derechos de usuario*.
3. Haga doble clic en *Actuar como parte del sistema operativo*.
4. Haga clic en *Agregar* , escriba el nombre de la cuenta de servicio creada y haga clic en *Aceptar*.

Realice esta tarea para cualquier Server Intelligence Agent (SIA) que ejecute servicios usados por la cuenta de servicio.

1. Para iniciar el CCM, seleccione *Programas* > *SAP Business Intelligence* > *Plataforma de SAP BusinessObjects BI 4* > *Administrador de configuración central* .
   Se abrirá la página de inicio del CCM.
2. En el CCM, haga clic con el botón derecho en Server Intelligence Agent (SIA) y seleccione *Detener*.

> **Nota**
>
> Cuando detenga el SIA, todos los servicios que administra el SIA se detendrán.

3. Haga clic con el botón derecho en el SIA y seleccione *Propiedades*.




4. Desactive la casilla de verificación *Cuenta del sistema*.
5. Escriba las credenciales de la cuenta de servicio (`<NOMBREDOMINIO>\<nombre de servicio>`) y haga clic en *Aceptar*.

   La cuenta de servicio debe tener concedidos los siguientes derechos en el equipo que ejecute el SIA:

   - La cuenta debe disponer específicamente del derecho de «actuar como parte del sistema operativo».
   - La cuenta debe disponer específicamente del derecho de «inicio de sesión como servicio».
   - Derechos de control completos para la carpeta en la que está instalada la plataforma de BI.
   - Derechos de control completo para « HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects» del registro del sistema.
6. Repita los pasos anteriores en todos los equipos que ejecuten un servidor de la plataforma de BI.

> **Nota**
>
> Es importante que el derecho efectivo termine activándose después de seleccionar *Actuar como parte del sistema operativo*. Normalmente, deberá reiniciar el servidor para que esto se produzca. Si, después de reiniciar el servidor, esta opción sigue sin estar activada, la configuración de la Directiva de dominio reemplazará a la configuración de la Directiva local.

7. Reinicie el SIA.
8. Si es necesario, repita los pasos del 1 al 5 para cada SIA que tenga en funcionamiento un servicio que se tenga que configurar.

Ahora debe poder iniciar la sesión en el CCM con las credenciales de AD.

### 9.4.4.3 Para probar las credenciales de AD en el CCM

Para realizar esta tarea, deberá haber asignado correctamente un grupo de usuarios de AD a la plataforma de BI.

1. Inicie el CCM y haga clic en el icono *Administrar servidores*.
2. Asegúrese de que se muestra la información correcta en el campo *Sistema*.
3. Seleccione *Windows AD* de la lista de opciones de autenticación.
   Aparecerá un cuadro de diálogo de identificación.
4. Inicie sesión usando una cuenta de AD existente del grupo de AD que asignó a la plataforma de BI.

> **Nota**
>
> Si usa una cuenta de AD que no reside en el dominio predeterminado, conéctese como `domain\username`.

No debería recibir ningún mensaje de error. Debe poder conectarse a través del CCM usando una cuenta de AD asignada antes de pasar a la siguiente sección.

> **→ Sugerencias**
>
> Si recibe un mensaje de error, vaya a *CMC* > *Autenticación* > *Windows AD*. En *Opciones de autenticación*, cambie *Usar autenticación de Kerberos* por *Usar autenticación de NTLM* y haga clic en *Actualizar*. Repita los pasos del 1 al 4 anteriores. Si esto funciona, hay un problema con la configuración de Kerberos.

## 9.4.5 Configuración del servidor de aplicaciones Web para la autenticación de AD

### 9.4.5.1 Preparación del servidor de aplicaciones para la autenticación de Windows AD (Kerberos)

El proceso de configuración de Kerberos para un servidor de aplicaciones Web tiene algunas pequeñas variaciones que dependen del servidor de aplicaciones específico. Sin embargo, el proceso general de configuración de Kerberos supone estos pasos:

- Creación del archivo de configuración Kerberos `(krb5.ini)`
- Creación del archivo de configuración de inicio de sesión JAAS `bscLogin.conf`.

  > **Nota**
  >
  > Este paso no es necesario para el servidor de aplicaciones Java de SAP NetWeaver 7.3. Sin embargo, tendrá que agregar el módulo de inicio de sesión al servidor de SAP NetWeaver.

- Modificación de las opciones de Java para su servidor de aplicaciones.
- Sobrescritura de las propiedades del archivo `BOE.war` para la autenticación de Windows AD.

- Reinicio del servidor de aplicaciones Java.

Esta sección contiene los detalles sobre la configuración de Kerberos para su uso con los siguientes servidores de aplicaciones:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

## 9.4.5.1.1 Creación de los archivos de configuración de Kerberos

### 9.4.5.1.1.1 Para crear un archivo de configuración de Kerberos

Antes de continuar, asegúrese de que ha realizado las siguientes tareas previas:

- Ha creado una cuenta de servicio en el controlador de dominio de la plataforma de BI.
- Ha verificado que los nombres de representante de servicio (SPN) se hayan agregado a la cuenta de servicio.
- Ha asignado correctamente los grupos de usuarios de AD a la plataforma de BI.
- Ha probado las credenciales de AD en el CCM.

Siga estos pasos para crear el archivo de configuración de Kerberos si usa SAP NetWeaver 7.3, Tomcat, el servidor de aplicaciones de Oracle, WebSphere o WebLogic como servidor de aplicaciones Web de su despliegue de la plataforma de BI.

1. Cree el archivo `krb5.ini`, si no existe, y almacénelo en `C:\Windows`.

   > **Nota**
   >
   > Si el servidor de aplicaciones está instalado en Unix, debe usar los siguientes directorios:
   >
   > Solaris: `/etc/krb5/krb5.conf`
   >
   > Linux: `/etc/krb5.conf`

   > **Nota**
   >
   > Puede almacenar este archivo en una ubicación diferente. Sin embargo, deberá especificar su ubicación en las opciones de Java. Para obtener más información sobre `krb5.ini` vaya a http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view .

2. Agregue la siguiente información necesaria en el archivo de configuración de Kerberos:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
```

```
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

**Nota**

En la tabla siguiente, se explican los parámetros clave.

| | |
|---|---|
| `DOMAIN.COM` | El nombre DNS del dominio que se debe introducir en formato FQDN en mayúsculas. |
| `kdc` | El nombre de host del controlador de dominio. |
| `[capath]` | Define la confianza entre dominios que están en otro bosque de AD. En el ejemplo anterior `DOMAIN2.COM` es un dominio en un bosque externo y tiene confianza transitiva, bidireccional y directa con `DOMAIN.COM`. |
| `default_realm` | En una configuración de varios dominios, en `[libdefaults]` el valor `default_realm` puede ser cualquiera de los dominios de origen. El procedimiento recomendado es utilizar el dominio con el número máximo de usuarios que se autenticarán con sus cuentas de AD. Si no se proporciona ningún sufijo UPN en el inicio de sesión, el valor predeterminado es `default_realm`. Este valor debe ser coherente con la configuración de *dominio predeterminado* en la CMC. Todos los dominios deben especificarse en mayúsculas, como se muestra en el ejemplo anterior. |

## 9.4.5.1.2 Creación de un archivo de configuración de inicio de sesión de JAAS

### 9.4.5.1.2.1 Crear un archivo de configuración de inicio de sesión de Tomcat o WebLogic JAAS

El archivo `bscLogin.conf` se usa para cargar el módulo de conexión de java y se necesita para la autenticación de AD Kerberos en los servidores de aplicaciones web de Java.

La ubicación predeterminada de los archivos es: `C:\Windows`.

1. Cree un archivo denominado `bscLogin.conf` si no existe y almacénelo en `C:\Windows`.

   > **Nota**
   >
   > Puede almacenar este archivo en una ubicación diferente. Sin embargo, si lo hace, deberá especificar su ubicación en las opciones de Java.

2. Agregue el código siguiente al archivo de configuración `bscLogin.conf` de JAAS:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Guarde y cierre el archivo.

### 9.4.5.1.2.2 Crear un archivo de configuración de inicio de sesión de JAAS de Oracle

1. Busque el archivo `jazn-data.xml`.

   > **Nota**
   >
   > La ubicación predeterminada de este archivo es `C:\OraHome_1\j2ee\home\config`. Si ha instalado el servidor de aplicaciones de Oracle en una ubicación distinta, busque el archivo específico correspondiente a su instalación.

2. Agregue el siguiente contenido al archivo entre las etiquetas `<jazn-loginconfig>`:

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. Guarde y cierre el archivo `jazn-data.xml`.

### 9.4.5.1.2.3 Crear un archivo de configuración de inicio de sesión de WebSphere JAAS

1. Cree un archivo denominado `bscLogin.conf` si no existe y almacénelo en la ubicación predeterminada: `C:\Windows`
2. Agregue el código siguiente al archivo de configuración `bscLogin.conf`:

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. Guarde y cierre el archivo.

### 9.4.5.1.2.4 Para agregar un LoginModule a SAP NetWeaver AS

Para usar Kerberos y SAP NetWeaver AS 7.3, configure el sistema como si usara el servidor de aplicaciones web de Tomcat. No tendrá que crear ningún archivo `bscLogin.conf`.

Cuando haya realizado esta tarea, debe agregar un módulo de inicio de sesión y actualizar algunos ajustes Java en SAP NetWeaver AS 7.3.

Para asignar `com.sun.security.auth.module.Krb5LoginModule` a `com.businessobjects.security.jgss.initiate`, debe agregar manualmente un módulo de inicio de sesión a SAP NetWeaver AS 7.3.

1. Abra el administrador de SAP NetWeaver escribiendo la siguiente dirección en un explorador Web: `http://<machine name>:<port>/nwa`.
2. Haga clic en *Administración de configuración* > *Seguridad* > *Autenticación* > *Módulos de inicio de sesión* > *Editar*.
3. Agregue un nuevo módulo de inicio de sesión con la siguiente información:

| | |
|---|---|
| Nombre visualizado | **`Krb5LoginModule`** |
| Nombre de la clase | **`com.sun.security.auth.module.Krb5LoginModule`** |

4. Haga clic en *Guardar*.
   SAP NetWeaver crea el nuevo módulo.
5. Haga clic en *Componentes* > *Editar*.
6. Agregue una nueva política denominada **`com.businessobjects.security.jgss.initiate`**.
7. En *Pila de autenticación*, agregue el módulo de inicio de sesión que se creó en el paso 3 y configúrelo como *Obligatorio*.
8. Confirme que no hay más entradas en las *Opciones para el módulo de inicio de sesión seleccionado*. Si las hay, quítelas.
9. Haga clic en *Guardar*.
10. Desconectarse del administrador SAP NetWeaver.

### 9.4.5.1.3 Modificación de los ajustes de Java del servidor de aplicaciones para cargar los archivos de configuración

#### 9.4.5.1.3.1 Para modificar las opciones de Java para Kerberos en Tomcat

1. En el menú *Inicio*, seleccione *Programas > Tomcat > Configuración de Tomcat*.
2. Haga clic en la ficha *Java*.
3. Agregue las opciones siguientes:

   ```
   -Djava.security.auth.login.config=C:\XXXX\bscLogin.conf
   -Djava.security.krb5.conf=C:\XXXX\krb5.ini
   ```

   Sustituya XXXX por la ubicación donde ha almacenado el archivo `bscLogin.conf`.
4. Cierre el archivo de configuración de Tomcat.
5. Reinicie Tomcat.

#### 9.4.5.1.3.2 Para modificar las opciones de Java para SAP NetWeaver AS 7.3

1. Vaya a la herramienta de configuración Java (ubicada en `C:\usr\sap\<ID de NetWeaver>\<instancia>\j2ee\configtool\` de forma predeterminada) y haga doble clic en `configtool.bat`.
   Se abre la herramienta de configuración.
2. Haga clic en *Ver* > *Modo experto*.
3. Expanda *Datos de clúster* > *Plantilla*.
4. Seleccione la instancia que se corresponda con el servidor de SAP NetWeaver AS (por ejemplo, *Instancia - `<ID de sistema><nombre del equipo>`*).
5. Haga clic en *Parámetros VM*.
6. Seleccione *SAP* de la lista *Proveedor* y *GLOBAL* de la lista *Plataforma*.
7. Haga clic en *Sistema* y agregue la información de parámetro personalizada siguiente:

| | |
|---|---|
| java.security.krb5.conf | `<ruta al archivo krb5.ini incluyendo el nombre del archivo>` |
| javax.security.auth.useSubjectCredsOnly | false |

8. Haga clic en *Guardar* y en *Editor de configuración*.
9. Haga clic en *Configuraciones* > *Seguridad* > *Configuraciones* > *com.businessobjects.security.jgss.initiate* > *Seguridad* > *Autenticación*.
10. Haga clic en *Modo de edición*.

11. Haga clic con el botón derecho en el nodo *Autenticación* y seleccione *Crear subnodo*.
12. Seleccione *Entrada del valor* de la lista superior.
13. Especifique los siguientes datos:

| | |
|---|---|
| Nombre | create_security_session |
| Valor | false |

14. Haga clic en *Crear* y cierre la ventana.
15. Haga clic en *Herramienta de configuración* y en *Guardar*.

Una vez actualizada la configuración, debe reiniciar el servidor de SAP NetWeaver AS.

## 9.4.5.1.3.3 Para modificar las opciones de Java para Kerberos en WebLogic

Si utiliza Kerberos con WebLogic, debe modificar las opciones de Java para especificar la ubicación del archivo de configuración de Kerberos y el módulo de inicio de sesión Kerberos.

1. Detenga el dominio WebLogic que ejecuta las aplicaciones de la plataforma de BI.
2. Abra la secuencia de comandos que inicia el dominio de WebLogic que ejecuta las aplicaciones de la plataforma de BI (`startWeblogic.cmd` para Windows, `startWebLogic.sh` para Unix).
3. Agregue la información siguiente en la sección Java_Options del archivo:

   ```
   set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf
   -Djava.security.krb5.conf=C:/XXX/krb5.ini
   ```

   Reemplace XXXX por la ubicación donde ha almacenado el archivo.
4. Reinicie el dominio de WebLogic que ejecuta las aplicaciones de la Plataforma de BI.

## 9.4.5.1.3.4 Para modificar las opciones de Java para Kerberos en WebSphere

1. Inicie sesión en la consola administrativa de WebSphere.

   Para IBM WebSphere 5.1, escriba `http://nombreservidor:9090/admin`. Para IBM WebSphere 6.0, escriba `http://nombreservidor:9060/ibm/console`
2. Expanda Servidor, haga clic en *Servidores de aplicaciones* y, a continuación, haga clic en el nombre del servidor de aplicaciones que creó para usar con la plataforma de BI.
3. Vaya a la página de la *JVM*.

   Si usa WebSphere 5.1, siga estos pasos para acceder a la página de la *JVM*.
   1. En la página del servidor, desplácese hacia abajo hasta que vea *Process Definition* (Definición del proceso) en la columna *Additional Properties* (Propiedades adicionales).
   2. Haga clic en *Process Definition* (Definición del proceso).
   3. Desplácese hacia abajo y haga clic en *Java Virtual Machine* (Máquina virtual Java).

Si usa WebSphere 6.0, siga estos pasos para acceder a la página de la *JVM*.

1. En la página del servidor, seleccione *Java and Process Management*.
2. Seleccione *Definición del proceso*.
3. Seleccione *Java Virtual Machine*.

4. Haga clic en *Argumentos de JVM genéricos* y, a continuación, escriba la ubicación de los archivos `Krb5.ini` y `bscLogin.conf` como se indica a continuación.

   -Djava.security.auth.login.config=C:\XXXX\bscLogin.conf

   -Djava.security.krb5.conf=C:\XXXX\krb5.ini

   Reemplace XXXX por la ubicación donde ha almacenado el archivo.
5. Haga clic en *Apply* (Aplicar) y, a continuación, haga clic en *Save* (Guardar).
6. Detenga y reinicie el servidor.

## 9.4.5.1.4 Para verificar que Java puede recibir un vale Kerberos

Antes de comprobar si Java ha recibido el vale Kerberos, debe completar las siguientes acciones previas:

- Cree el archivo `bscLogin.conf` para su servidor de aplicaciones.
- Cree el archivo `krb5.ini`.

1. Vaya a la línea de comandos y navegue hasta el directorio `jk\bin` en su instalación de la plataforma de BI.

   De manera predeterminada se encuentra en:`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin`.
2. Ejecute `kinit <username>`.
3. Pulse `Intro`.
4. Introduzca la contraseña.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\win64_x64\jdk\bin>kinit sfredell
Password for sfredell@VTIAUTH08.COM: password
New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator
```

   Si el archivo `krb5.ini` se configuró correctamente y el módulo de inicio de sesión de Java se ha cargado, debería ver el mensaje siguiente:

```
Nuevo vale guardado en el archivo de caché
C:\Users\Administrator\krb5cc_Administrator
```

No prosiga con la configuración de AD hasta que haya recibido correctamente un vale Kerberos.

Si no puede recibir el vale, considere las opciones siguientes:

- Consulte la sección de resolución de problemas al final de este apartado.
- Para cuestiones relacionadas con KDC, los archivos de configuración de Kerberos y las credenciales de usuario no disponibles en la base de datos de Kerberos, consulte los artículos KBA 1476374 y KBA 1245178 de la base de conocimientos de SAP.

### 9.4.5.1.5 Para configurar la plataforma de lanzamiento de BI para el inicio de sesión manual de AD

Antes de configurar las aplicaciones de la plataforma de BI para el inicio de sesión manual de AD, debe haber completado las siguientes acciones previas:

- Ha creado una cuenta de servicio en el controlador de dominio para la plataforma de BI.
- Ha verificado que los nombres de representantes del servicio (SPN) HTTP se hayan agregado a la cuenta de servicio.
- Ha asignado correctamente los grupos de usuarios de AD a la plataforma de BI.
- Ha probado las credenciales de AD en el CCM.
- Ha creado, configurado y probado los archivos de configuración necesarios de su servidor de aplicaciones Web.
- La configuración de Java del servidor de aplicaciones se ha modificado para cargar los archivos de configuración.

Para habilitar la opción de autenticación de Windows AD para la plataforma de lanzamiento de BI, realice estos pasos:

1. Acceda a la carpeta personalizada de la aplicación Web BOE en el equipo que contiene el servidor de aplicaciones Web:

   `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Realice las modificaciones en el directorio `config\custom` y no en `config\default`. De otro modo, los cambios se sobrescribirán al aplicar revisiones futuras al despliegue.

   Tendrá que volver a desplegar más tarde la aplicación web de BOE que se ha modificado.
2. Cree un nuevo archivo.

   > **Nota**
   >
   > Use el Bloc de notas o cualquier otra utilidad de edición de texto.
3. Guardar el archivo como `BIlaunchpad.properties`.
4. Escriba lo siguiente:

   ```
   authentication.visible=true
   authentication.default=secWinAD
   ```
5. Guarde y cierre el archivo.
6. Reinicie el servidor de aplicaciones Web.

Ahora debería poder iniciar la sesión manualmente en la rampa de lanzamiento BI, acceder a una de las aplicaciones y seleccionar Windows AD de la lista de opciones de autenticación.

> **Nota**
>
> No prosiga con la configuración de Windows AD hasta que pueda iniciar sesión manualmente en la plataforma de lanzamiento de BI mediante una cuenta de AD existente.

Las nuevas propiedades surtirán efecto sólo después de que la aplicación web de BOE se vuelva a desplegar en el equipo que ejecuta el servidor de aplicaciones web. Use WDeploy para volver a desplegar BOE en

el servidor de aplicaciones web. Para obtener más información sobre el uso de WDeploy para deshacer el despliegue de las aplicaciones Web, consulte el *Manual de despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

> **Nota**
>
> Si la implementación usa un servidor de seguridad, recuerde abrir todos los puertos necesarios; de lo contrario, las aplicaciones Web no podrán conectarse a los servidores de la plataforma de BI.

## 9.4.6 Configuración del inicio de sesión único

### 9.4.6.1 SSO a la plataforma de BI con autenticación de AD

#### Opciones de SSO con Windows AD

Existen tres métodos admitidos para configurar el inicio de sesión único (SSO) para la autenticación de Windows AD con la plataforma de BI:

- Vintela: Esta opción solo puede usarse con Kerberos.
- SiteMinder: Esta opción solo puede usarse con Kerberos.

#### SSO en la base de datos

El SSO a la base de datos permite que los usuarios que hayan iniciado la sesión realicen acciones que requieren acceso a la base de datos, concretamente, visualizar y actualizar informes sin tener que proporcionar sus credenciales de inicio de sesión de nuevo. Mientras que la delegación limitada es opcional para la autenticación de AD y el SSO de Vintela, es obligatoria para escenarios de despliegue que impliquen inicio de sesión único en la base de datos del sistema.

#### SSO integral

En la plataforma de BI, el inicio de sesión único integral se admite a través de Windows AD y Kerberos. En este escenario, los usuarios tienen disponible tanto el acceso de inicio de sesión único a la plataforma de BI en el front-end, como el acceso SSO en las bases de datos en el backend. Así, los usuarios solo deben proporcionar sus credenciales de inicio de sesión una vez, cuando inician sesión en el sistema operativo, para acceder a la plataforma de BI y para poder realizar acciones que precisan el acceso a la base de datos, como la visualización de informes

### Manual de configuración de autenticación de AD versus SSO

Una vez que haya configurado correctamente el despliegue para permitir que las cuentas de AD se conecten manualmente a la plataforma de lanzamiento de BI, deberá repetir la configuración de AD para habilitar los requisitos específicos del SSO. Los requisitos varían dependiendo del método de SSO que escoja.

## 9.4.6.2 Uso del SSO de Vintela

### 9.4.6.2.1 Lista de operaciones para la configuración del SSO de Vintela

Para configurar la plataforma de BI para que funcione con el SSO de Vintela, debe completar las siguientes tareas:

1. Configure su cuenta de servicio específicamente para el SSO de Vintela.
2. Configure la delegación limitada (opcional).
3. Configure las opciones de autenticación del SSO de Windows AD en la CMC.
4. Configure las propiedades generales de BOE y las específicas de la plataforma de lanzamiento de BI para el SSO de Vintela.
5. Si usa Tomcat como servidor de aplicaciones de su despliegue, deberá aumentar el límite de tamaño del encabezado.
6. Configure los exploradores de Internet para Vintela.

### 9.4.6.2.2 Para configurar la cuenta de servicio para el SSO de Vintela

La herramienta de línea de comandos `Ktpass` configura el nombre principal del servicio del host o servicio en Active Directory y genera un archivo "keytab" de Kerberos que contiene la clave del secreto compartido de la cuenta de servicio. Esta herramienta se encuentra normalmente en controladores de dominio, o puede descargarse de la página de ayuda de Microsoft: http://support.microsoft.com/kb/892777 .

Es necesaria una cuenta de servicio configurada específicamente para permitir que los usuarios de un grupo de Windows AD se autentiquen automáticamente en la plataforma de lanzamiento de BI con sus credenciales de AD. Puede cambiar la configuración de la cuenta de servicio creada para la autenticación de AD Kerberos en el Controlador de dominio.

Si un cliente intenta iniciar la sesión en la plataforma de lanzamiento de BI, se inicia una solicitud al servidor que genera el vale Kerberos. Para facilitar esta petición, la cuenta de servicio creada para la plataforma de BI debe tener un SPN que se coincida con la URL del servidor de aplicaciones. Realice los siguientes pasos en el equipo que aloja el Controlador de dominio.

1. Ejecute el comando de configuración de keytab de Kerberos, `ktpass`, para crear y ubicar un fichero `keytab`.

   Especifique los parámetros de `ktpass` que se enumeran en la tabla siguiente:

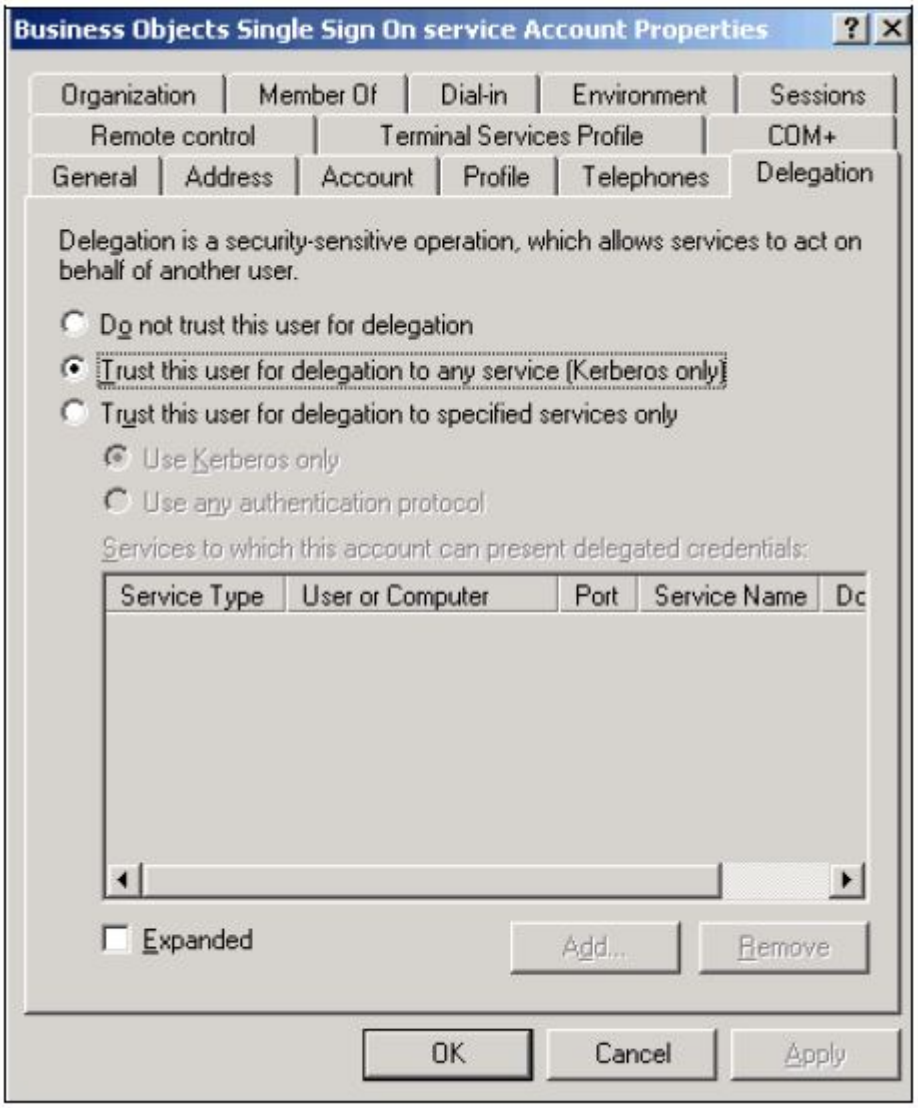
| Parámetro | Descripción |
|---|---|
| `-out` | Especifica el nombre del archivo `keytab` de Kerberos que se debe generar. |
| `-princ` | Especifica el nombre principal utilizado para la cuenta de servicio, en formato SPN:`< MYSIAMYSERVER>/<sbo.service.domain.com>@<DOMAIN>.COM`, donde `<MYSIAMYSERVER>` es el nombre del Service Intelligence Agent especificado en el Administrador de configuración central (CCM).<br><br>**Nota**<br>El nombre de la cuenta de servicio distingue entre mayúsculas y minúsculas. El SPN incluye el nombre del equipo host en el que la instancia de servicio está en ejecución.<br><br>**→ Sugerencias**<br>El SPN debe ser único en el bosque en que está registrado. Para realizar una comprobación, use la herramienta de ayuda de Windows `Ldp.exe` para buscar el SPN. |
| `-pass` | Especifica la contraseña que usa la cuenta de servicio. |
| `-ptype` | Especifica el tipo de principal:<br><br>`-ptype KRB5_NT_PRINCIPAL` |
| `-crypto` | Especifica el tipo de cifrado que se debe usar con la cuenta de servicio:<br><br>`-crypto RC4-HMAC-NT` |

Por ejemplo:

```
ktpass -out <keytab_filename>.keytab -princ <MYSIAMYSERVER>/
sbo.service.domain.com@DOMAIN.COM
-pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

La salida del comando `ktpass` debería confirmar el controlador de dominio de destino, y que se ha creado un archivo `keytab` de Kerberos que contiene el secreto compartido. El comando también asigna el nombre de principal a la cuenta de servicio (local).

2. Haga clic con el botón derecho sobre la cuenta de servicio, seleccione *Propiedades* > *Delegación*.
3. Haga clic en *Trust this user for delegation to any service (Kerberos only)* (Confiar en este usuario para la delegación a cualquier servicio [sólo Kerberos]).




4. Haga clic en *Aceptar* para guardar los cambios.

Ahora la cuenta de servicio tiene todos los nombres principales del servicio necesarios para el SSO de Vintela, y se ha generado un archivo keytab con la contraseña encriptada para la cuenta de servicio.

> **Nota**
>
> La plataforma de BI debe estar configurada para el inicio de sesión único final o para el inicio de sesión único en la base de datos.
>
> Si se han solucionado fallos mediante la modificación de KVNO en la keytab, es probable que el atributo KVNO en la cuenta de servicio sea más alto que el KVNO utilizado en la creación del keytab (durante ktpass). Para obtener información sobre cómo obtener el atributo KVNO correcto, véase http://service.sap.com/sap/support/notes/1853668.

### 9.4.6.2.2.1 Para configurar la delegación limitada para el SSO de Vintela

La delegación limitada es opcional para configurar el SSO de Vintela. En cambio, es obligatoria para las implementaciones que necesiten el SSO a la base de datos del sistema.

1. En el equipo del Controlador de dominio de AD, abra el complemento de Active Directory *Usuarios y equipos*.
2. Haga clic con el botón derecho sobre la cuenta de servicio que creó en la sección anterior, y haga clic en *Propiedades* > *Delegación*.
3. Seleccione *Confiar en este usuario para la delegación sólo a los servicios especificados*.
4. Seleccione *Usar solamente Kerberos*.
5. Haga clic en *Agregar* > *Usuarios o equipos*.
6. Escriba el nombre de la cuenta de servicio y haga clic en *Aceptar*.
   Aparecerá una lista de servicios.
7. Seleccione los servicios siguientes y haga clic en *Aceptar*.
   - El servicio HTTP
   - El servicio que se usa para ejecutar el Server Intelligence Agent (SIA) en el equipo que aloja la plataforma de BI.

   Los servicios se agregan a la lista de servicios que se pueden delegar para la cuenta de servicio.

Deberá modificar las propiedades de aplicaciones web para dar cuenta de esta modificación.

### 9.4.6.2.3 Para configurar los ajustes del SSO en la CMC

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *Windows AD*.
3. Asegúrese de que está activada la casilla de verificación *Habilitar Windows Active Directory (AD)*.
4. Bajo *Opciones de autenticación*, asegúrese de que está seleccionada la opción *Usar autenticación Kerberos*.
5. Si su configuración necesita SSO en la base de datos, seleccione *Contexto de seguridad de caché*.
6. Seleccione *Habilitar el inicio de sesión único para el modo de autenticación seleccionado*.
7. Haga clic en *Actualizar*.

### 9.4.6.2.4 Para activar el inicio de sesión único de Vintela para la plataforma de lanzamiento de BI y OpenDocument

Este procedimiento se usa para la plataforma de lanzamiento de BI y para OpenDocument. Para habilitar el SSO a las aplicaciones web de la plataforma de BI, deberá especificar las propiedades específicas de Vintela y

de SSO en el archivo `BOE.war`. Con el fin de configurar el SSO se recomienda que se concentre en habilitar el SSO en la plataforma de lanzamiento de BI para cuentas de AD antes de manejar otras aplicaciones.

1. Acceda a la carpeta personalizada de la aplicación Web BOE en el equipo que contiene el servidor de aplicaciones Web:

   `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Realice sus cambios en el directorio `config\custom` y no en el directorio `config\default`. De otro modo, los cambios se sobrescribirán al aplicar revisiones futuras al despliegue.

   Tendrá que volver a desplegar más tarde la aplicación web de BOE que se ha modificado.
2. Cree un archivo nuevo con un editor de texto.
3. Especifique los siguientes datos:

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=DOMAIN.COM
idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.keytab=C:/WIN/filename.keytab
idm.logger.props=error-log.properties
```

> **Nota**
>
> Los parámetros `idm.realm` y `idm.princ` requieren valores válidos. `idm.realm` debería ser el mismo valor que se estableció al configurar `default_realm` en el archivo `krb5.ini`. El valor debe estar en mayúsculas. El parámetro `idm.princ` es el SPN que se usa para la cuenta de servicio creada para el SSO de Vintela.

> **Nota**
>
> Es necesario usar barras diagonales al especificar la ubicación del archivo keytab.

   Omita el siguiente paso si no desea usar la delegación limitada para la autenticación de Windows AD y el SSO de Vintela.
4. Para usar la delegación limitada agregue:

```
idm.allowS4U=true
```

5. Cierre el archivo y guárdelo con el nombre `global.properties`:

> **Nota**
>
> Asegúrese de que el nombre del archivo no se guarda con extensiones como `.txt`.

6. Cree otro archivo en el mismo directorio. Guarde el archivo como `OpenDocument.properties` o `BIlaunchpad.properties` , en función de sus requisitos.
7. Escriba lo siguiente:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

Por ejemplo:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

8. Guarde y cierre el archivo.
9. Reinicie el servidor de aplicaciones Web.

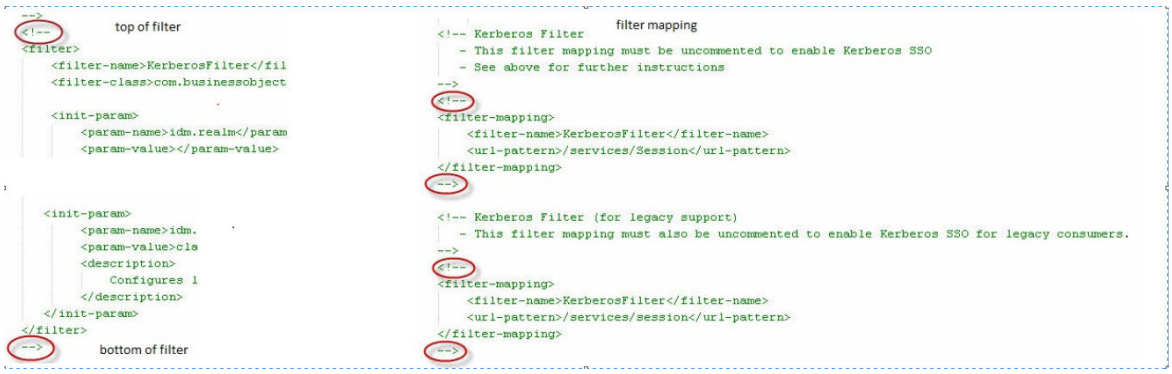
Las nuevas propiedades surtirán efecto sólo después de que la aplicación web de BOE se vuelva a desplegar en el equipo que ejecuta el servidor de aplicaciones web. Use WDeploy para volver a desplegar BOE en el servidor de aplicaciones web. Para obtener más información sobre el uso de WDeploy para deshacer el despliegue de las aplicaciones Web, consulte el *Manual de despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

> **Nota**
>
> Si el despliegue usa un servidor de seguridad, no olvide abrir todos los puertos necesarios o, de lo contrario, las aplicaciones web no se podrán conectar a los servidores de la Plataforma de BI.

## 9.4.6.2.5 Para habilitar el inicio de sesión único Vintela para servicios Web

Algunas herramientas de cliente requerirán autenticación a través de servicios Web. Siga estos pasos para habilitar inicio de sesión único (SSO) para servicios Web. Para obtener más información, consulte la nota SAP relacionada en: http://service.sap.com/sap/support/notes/1646920

1. Realice una copia de seguridad de este archivo: `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml` y, a continuación, ábralo para editarlo.
2. Elimine el comentario de las secciones Filtro de proxy Kerberos y Filtro Kerberos para habilitar el SSO Kerberos para la autenticación de Windows Active Directory (secWinAD).




Las siguientes opciones se deben especificar (el resto es opcional):

- `idm.realm` (el mismo que el default_realm especificado en el archivo Krb5.ini).
- `idm.princ` (el mismo que el especificado para idm.princ en el archivo global.properties ubicado en `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

- `idm.keytab` (el mismo que el especificado para idm.keytab en el archivo global.properties ubicado en `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

> **Nota**
>
> Si está utilizando la contraseña altamente codificada establecida en las opciones Java de Tomcat, no lleve a cabo ninguna modificación en las líneas keytab en el archivo `web.xml`.

3. Si SSL no se usa en el servidor de aplicaciones Java, establezca el parámetro idm.allowUnsecured en **`true`**.

   Para obtener más información sobre Tomcat SSL, consulte el ID de artículo base de conocimiento:1484802.

4. Realice una copia de seguridad de este archivo: `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\dsws.properties` y ábralo para editarlo.
5. Establecer kerberos.sso en **`true`** y guarde el archivo.

```
68  allowedOrderBy = SI_CREATION_TIME,SI_KIND,SI_LAST_RUN_TIME,SI_SCHEDULEINFO.SI_SUBMITTER,SI_OWNER
69
70  ##############################
71  # Kerberos SSO Properties #
72  ##############################
73  #Set this value to true and activate the Vintela Authentication Filter (in web.xml) to enable SSO via Kerberos
74  kerberos.sso=true
75
76  #Setting this value to true if user wants trusted authentication
77  trustedAuthentication.enabled = false
```

kerberos SSO setting

6. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones web.

   Para obtener más información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

7. Reinicie Tomcat.
8. Para probar la configuración, en el equipo del cliente con las herramientas de cliente instaladas, inicie el Diseñador de Query as a Web Service.
9. Agregar un nuevo host administrado.
10. Introduzca el nombre del servidor de aplicaciones.
11. Introduzca la URL de los servicios Web en este formato: `http://<WebAppServer>:<portNumber>/dswsbobje/services/Session`.

    Ejemplo: `http://BI4:8080/dswsbobje/services/Session`.

12. Introduzca el nombre de host del CMS.
13. Modifique el tipo de autenticación a *Windows AD*.
14. Seleccione *Habilitar Inicio de sesión único del Directorio de Windows Active*.
15. En la petición de inicio de sesión, deje los campos *Usuario* y *Contraseña* vacíos y haga clic en *Aceptar*.

## 9.4.6.2.6 Para habilitar el inicio de sesión único Vintela para servicios Web RESTful

Algunas herramientas del cliente requieren autenticación mediante los servicios Web RESTful Siga estos pasos para habilitar inicio de sesión único (SSO) para servicios Web.

1. Copie el archivo `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\biprws.properties` to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties`, y a continuación ábralo para editarlo.
2. Para habilitar Kerberos SSO para la autenticación de Windows Active Directory (secWinAD), fije `sso.enabled` to `true`. Véase la captura de pantalla a continuación:

```
# ---------------------------------------------------------- SSO Related Default Global Core Web Properties ----------------------------------------------------------
# Vintela single sign on properties
sso.enabled=
idm.realm=
idm.princ=
idm.keytab=
idm.allowUnsecured=
idm.allowNTLM=
idm.logger.name=
idm.logger.props=
```

   Especifique las siguientes opciones obligatorias:
   - `idm.realm` (el mismo que el default_realm especificado en el archivo Krb5.ini).
   - `idm.princ` (el mismo que el especificado para idm.princ en el archivo global.properties ubicado en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - `idm.keytab` (el mismo que el especificado para idm.keytab en el archivo global.properties ubicado en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
   - El parámetro `idm.allowUnsecured` debe fijarse en `true` si no se está utilizando SSL con el servidor de aplicaciones Java. Para obtener más información sobre Tomcat SSL, consulte el *ID de artículo base de conocimiento:1484802*.
3. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web. Para obtener información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma de SAP BusinessObjects Business Intelligence*.
4. Reinicie Tomcat.
5. Para realizar un test de las opciones en el equipo del cliente, abra cualquier navegador e inicie la URL: http://<WebAppServer>:<portnumber>/biprws/v1/logon/adsso.
   El token REST debe aparecer como respuesta a la API.

## 9.4.6.2.7 Para aumentar el límite de tamaño del encabezado para Tomcat

Active Directory crea un token de Kerberos que se utiliza en el proceso de autenticación. Este token se almacena en el encabezado HTTP. Su servidor de aplicaciones Java tendrá un tamaño de encabezado HTTP predeterminado. Para evitar errores, asegúrese de que tenga el tamaño mínimo predeterminado de 16384 bytes. (Algunos despliegues requerirán un tamaño mayor. Para obtener más información, consulte las instrucciones para tamaños de Microsoft en su sitio de soporte (http://support.microsoft.com/kb/327825).)

1. En el servidor que tiene Tomcat instalado, abra el archivo `server.xml`.

En Windows, este archivo se encuentra en `<DIRINSTALACIÓNTomcat>/conf`

- Si usa la versión de Tomcat instalada con la plataforma de BI en Windows y no ha modificado la ubicación predeterminada de la
  ubicación de instalación, sustituir `<DIRINSTALACIÓNTomcat>` con `C:\Archivos de programa (x86)\SAP BusinessObjects\Tomcat\`
- Si usa cualquier otro servidor de aplicaciones Web admitido, consulte la documentación de su servidor de aplicaciones Web para determinar la ruta apropiada.

2. Busque la etiqueta `<Connector …>` correspondiente del número de puerto que ha configurado.

   Si utiliza el puerto predeterminado 8080, busque la etiqueta `<Connector …>` que contiene port=«8080».

   Por ejemplo:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="8080" redirectPort="8443"
/>
```

3. Agregue el siguiente valor dentro de la etiqueta `<Connector …>`:

   `maxHttpHeaderSize="16384"`

   Por ejemplo:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" port="8080"
redirectPort="8443" />
```

4. Guarde y cierre el archivo `server.xml`.
5. Reinicie Tomcat.

> **Nota**
>
> Para otros servidores de aplicaciones Java, consulte la documentación del servidor de aplicaciones Java.

## 9.4.6.2.8 Configuración de los exploradores de Internet

Para admitir SSO de Vintela para la autenticación de AD Kerberos, debe configurar los clientes de la plataforma de BI. Esto involucra la configuración del explorador Web en los equipos de cliente.

### 9.4.6.2.8.1 Para configurar Internet Explorer en los equipos cliente

1. En el equipo cliente, abra un explorador IE.

2. Habilite la autenticación de Windows integrada.
   a. En el menú *Herramientas*, haga clic en *Opciones de Internet*.
   b. Haga clic en la ficha *Opciones avanzadas*.
   c. Desplácese a *Seguridad*, seleccione *Habilitar autenticación integrada de Windows* y, a continuación, haga clic en *Aplicar*.
3. Agregue el equipo de aplicaciones Java o la dirección URL a los sitios de confianza. Puede escribir el nombre de dominio completo del sitio.
   a. En el menú *Herramientas*, haga clic en *Opciones de Internet*.
   b. Haga clic en la ficha *Seguridad*.
   c. Haga clic en *Sitios* y, a continuación, haga clic en *Avanzadas.*
   d. Seleccione o introduzca el sitio y haga clic en *Agregar*.
   e. Haga clic en *Aceptar* hasta que se cierre el cuadro de diálogo Opciones de Internet.
4. Cierre y vuelva a abrir la ventana de Internet Explorer para que estos cambios surtan efecto.
5. Repita todos estos pasos en cada equipo cliente de la Plataforma de BI.

## 9.4.6.2.8.2 Para configurar Firefox en los equipos cliente

1. *Modifique network.negotiate-auth.delegation-uris*
   a. En el equipo cliente, abra una ventana del explorador Firefox.
   b. Escriba **`about:config`** en el campo de dirección URL.
      Aparece una lista de propiedades configurables.
   c. Haga doble clic en *network.negotiate-auth.delegation-uris* para editar la propiedad.
   d. Introduzca la dirección URL que usará para acceder a la plataforma de lanzamiento de BI.

      Por ejemplo, si la dirección URL de la plataforma de lanzamiento de BI es **`http://<equipo.dominio.com>:8080/BOE/BI`**, deberá introducir **`http://<equipo.dominio.com>`**.

      > ⓘ Nota
      >
      > Para agregar varias direcciones URL, sepárelas con una coma. Por ejemplo: **`http://<equipo.dominio.com>,<equipo2.dominio.com>`** .

   e. Haga clic en *Aceptar*.
2. *Modifique network.negotiate-auth.trusted-uris*
   a. En el equipo cliente, abra una ventana del explorador Firefox.
   b. Escriba **`about:config`** en el campo de dirección URL.
      Aparece una lista de propiedades configurables.
   c. Haga doble clic en *network.negotiate-auth.trusted-uris* para editar la propiedad.
   d. Introduzca la dirección URL que usará para acceder a la plataforma de lanzamiento de BI.
      Por ejemplo, si la dirección URL de la plataforma de lanzamiento de BI es **`http://<equipo.dominio.com>:8080/BOE/BI`**, deberá introducir **`http://<equipo.dominio.com>`**.

      > ⓘ Nota
      >
      > Para agregar varias direcciones URL, sepárelas con una coma. Por ejemplo: **`http://<equipo.dominio.com>,<equipo2.dominio.com>`** .

e. Haga clic en *Aceptar*.

3. Cierre y vuelva a abrir la ventana del explorador Firefox para que estos cambios surtan efecto.
4. Repita todos estos pasos en cada equipo cliente de la Plataforma de BI.

### 9.4.6.2.9 Probar el SSO de Vintela para la autenticación de AD Kerberos

Debería probar su configuración de SSO desde un equipo de trabajo cliente. Asegúrese de que el cliente esté en el mismo dominio que su despliegue de la plataforma de BI, y de que ha iniciado la sesión en el equipo de trabajo como un usuario asignado de AD. Esta cuenta de usuario debe poder iniciar la sesión manualmente en la plataforma de lanzamiento de BI.

Para probar el SSO, abra un explorador e introduzca la dirección URL de la plataforma de lanzamiento de BI. Si el SSO está configurado correctamente, no debería aparecer ninguna petición para solicitarle sus credenciales de inicio de sesión.

> → Sugerencias
>
> Se recomienda que pruebe varios escenarios de usuario de AD en su despliegue. Por ejemplo, si en el entorno habrá usuarios desde diferentes sistemas operativos, debería probar el SSO con usuarios de todos los sistemas operativos. También debería probar el SSO con todos los exploradores posibles admitidos en su organización. Si en el entorno habrá usuarios desde varios bosques o dominios, debería probar el SSO con una cuenta de usuario de cada dominio o bosque diferente.

### 9.4.6.2.10 Configuración de Kerberos y del inicio de sesión único en la base de datos para servidores de aplicaciones

Se admite el inicio de sesión único en la base de datos para los despliegues que cumplan estos requisitos:

- El despliegue de la plataforma de BI se encuentra en un servidor de aplicaciones Web.
- El servidor de aplicaciones web se ha configurado para el SSO de Vintela para la autenticación de AD.
- La base de datos en la que se requiere el inicio de sesión único es una versión compatible de SQL Server u Oracle.
- A los grupos o usuarios que necesitan acceso a la base de datos se les debe haber concedido permisos en SQL Server u Oracle.

El paso final consiste en modificar el archivo `krb5.ini` para admitir el SSO en la base de datos para aplicaciones web.

### 9.4.6.2.10.1 Para activar el inicio de sesión único para servidores de aplicaciones Java

1. Abra el archivo `krb5.ini` que se usa para el despliegue de la plataforma de BI.

   La ubicación predeterminada de este archivo es el directorio WIN en el servidor de aplicaciones web.

   > **Nota**
   >
   > Si no encuentra el archivo en el directorio WIN, compruebe este argumento Java para la ubicación del archivo:
   >
   > ```
   > -Djava.security.auth.login.config
   > ```
   >
   > Esta variable se especifica cuando está configurado AD con Kerberos en el servidor de aplicaciones web.

2. Vaya a la sección `[libdefaults]` del archivo.
3. Introduzca esta cadena antes del inicio de la sección `[realms]` del archivo:

   ```
   forwardable=true
   ```

4. Guarde y cierre el archivo.
5. Reinicie el servidor de aplicaciones Web.

El inicio de sesión único de la base de datos no estará activado hasta que marque la casilla *Contexto de seguridad de caché (requerido para SSO en base de datos)* que hay en la página de autenticación de Windows AD de la CMC.

## 9.4.6.3 Uso de SiteMinder

### 9.4.6.3.1 Uso de Windows AD con SiteMinder

En esta sección se explica cómo usar AD y SiteMinder. SiteMinder es una herramienta de autenticación y de acceso de usuarios de terceros que puede usar con el complemento de seguridad de AD para crear un inicio de sesión único en la plataforma de BI. Puede usar SiteMinder con Kerberos.

Asegúrese de que los recursos de administración de identidades de SiteMinder estén instalados y configurados antes de configurar la autenticación de Windows AD para que funciones con SiteMinder. Para obtener más información acerca de SiteMinder y su instalación, consulte la documentación de SiteMinder.

Existen dos tareas que debe completar para activar el inicio de sesión único de AD con SiteMinder:

- Configurar el complemento AD para el inicio de sesión único con SiteMinder
- Configurar las propiedades de SiteMinder para la aplicación web de BOE

> **Nota**
>
> Compruebe que el administrador de SiteMinder ha activado la compatibilidad con agentes 4.x. Esto debe hacerse independientemente de la versión compatible de SiteMinder que se utilice. Para obtener más información sobre la configuración de SiteMinder, consulte la documentación específica.

### 9.4.6.3.1.1 Para habilitar las propiedades de SiteMinder para la plataforma de lanzamiento de BI

Además de especificar la configuración de SiteMinder para el complemento de seguridad de Windows AD, se debe especificar la configuración de SiteMinder para las propiedades de WAR BOE.

1. Busque el directorio `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` en la instalación de la plataforma de BI.
2. Cree un archivo en el directorio con el Bloc de notas o con otra utilidad de edición de texto.
3. En el archivo nuevo, introduzca los valores siguiente:

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

4. Guarde el archivo con el nombre `global.properties`.

> **Nota**
>
> Asegúrese de que el nombre del archivo no se guarde con una extensión; por ejemplo, `.txt`.

5. Cree otro archivo en el mismo directorio.
6. En el archivo nuevo, introduzca los valores siguiente:

```
authentication.default=secWinAD
cms.default=[cms name]:[CMS port number]
```

Por ejemplo:

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. Guarde el archivo con el nombre `BIlaunchpad.properties` y ciérrelo.

Las nuevas propiedades surten efecto después de volver a implementar BOE.war en el equipo que ejecuta el servidor de aplicaciones Web. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web. Para obtener más información sobre el uso de WDeploy para deshacer el despliegue de las aplicaciones Web, consulte el *Manual de despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

### 9.4.6.3.1.2 Para configurar los ajustes de SiteMinder en la CMC

Antes de configurar la CMC para SiteMinder, debe completar las siguientes acciones previas:

- Ha asignado correctamente los grupos de usuarios de AD a la plataforma de BI.
- Ha probado las credenciales de AD en el CCM.

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *Windows AD*.

3. Seleccione la casilla de verificación *Habilitar Windows Active Directory (AD)*.
4. En Opciones de autenticación, seleccione *Utilizar autenticación NTLM* o *Utilizar autenticación Kerberos*.

   Para configurar la plataforma de BI para la autenticación Kerberos y AD mediante Kerberos, necesita una cuenta de servicio. Puede crear una nueva cuenta de dominio o usar una cuenta de dominio existente. La cuenta de servicio se usará para ejecutar los servidores de la plataforma de BI.

   > → Sugerencias
   >
   > Al iniciar una sesión manualmente en la plataforma de lanzamiento de BI, los usuarios de otros dominios deben añadir en mayúsculas el nombre de dominio después de su nombre de usuario. Por ejemplo, en `user@CHILD.PARENTDOMAIN.COM`, «CHILD.PARENTDOMAIN.COM» es el dominio.

5. Si ha seleccionado *Utilizar autenticación Kerberos*:
   a. Si quiere configurar el inicio de sesión único en una base de datos, seleccione *Contexto de seguridad de caché*.
   b. Elimine cualquier información del cuadro *Nombre principal del servicio*.
6. Si desea configurar el inicio de sesión único, active *Habilitar inicio de sesión único para el modo de autenticación seleccionado*.

   También debe configurar las propiedades generales de aplicaciones web BOE y las propiedades de la plataforma de lanzamiento de BI para habilitar el inicio de sesión único.
7. En el área *Sincronización de credenciales*, seleccione una opción para habilitar y actualizar las credenciales de origen de datos del usuario de AD al iniciar la sesión.

   Esto sincronizará el origen de datos con las credenciales de inicio de sesión actuales del usuario.
8. En el área *Opciones de SiteMinder*, configure SiteMinder como su opción de inicio de sesión único para la autenticación de AD con Kerberos:
   a. Haga clic en *Deshabilitado.*

      Aparecerá la página de *Windows Active Directory*.

      Si no ha configurado el complemento de Windows AD, aparece un aviso que le pregunta si desea continuar. Haga clic en *Aceptar*.
   b. Haga clic en *Utilice el inicio de sesión único de SiteMinder*.
   c. En el cuadro *Host de servidor de directivas*, escriba el nombre de cada servidor de directivas y haga clic en *Agregar*.
   d. Para cada host de servidor de directivas, introduzca un número de puerto en los cuadros *Contabilidad*, *Autenticación* y *Autorización*.
   e. En el cuadro *Nombre del agente*, introduzca el nombre del agente.
   f. En los cuadros *Secreto compartido*, introduzca el secreto compartido.

      Asegúrese de que el Administrador de SiteMinder ha habilitado la compatibilidad con Agentes 4.x, independientemente de qué versión admitida de SiteMinder esté usando. Para obtener más información sobre SiteMinder y cómo instalarlo, consulte la documentación de SiteMinder.
   g. Haga clic en *Actualizar* para guardar la información y volver a la página principal de autenticación de AD.
9. En el área *Opciones de alias de AD*, especifique el modo en que los nuevos alias se agregan y se actualizan en la plataforma de BI.
   a. En el área *Opciones de alias nuevos*, seleccione una opción para asignar nuevos alias a las cuentas de Enterprise:
      - *Asignar cada nuevo alias de AD a una cuenta de usuario existente con el mismo nombre*

Seleccione esta opción cuando sepa que algunos usuarios disponen de una cuenta de Enterprise existente con el mismo nombre; es decir, los alias de AD se asignarán a usuarios existentes (la creación automática de alias está activada). Los usuarios que no tengan cuentas de Enterprise existentes o que no tengan el mismo nombre en las cuentas de Enterprise y AD, se agregan como usuarios nuevos.

- *Crear una nueva cuenta de usuario para cada nuevo alias de AD*
  Seleccione esta opción cuando desee crear una cuenta nueva para cada usuario.

b. En el área *Opciones de actualización de alias*, seleccione una opción para administrar las actualizaciones de alias de las cuentas de Enterprise:

- *Crear nuevos alias cuando se actualice el alias*
  Use esta opción para crear automáticamente nuevos alias para todos los usuarios de AD asignados en la plataforma de BI. Se agregan nuevas cuentas de AD para los usuarios sin cuentas de la *plataforma de BI* o para todos los usuarios si ha seleccionado la opción *Crear una nueva cuenta de usuario para cada nuevo alias de AD* y ha hecho clic en Actualizar.
- *Crear nuevos alias solo cuando el usuario inicie sesión*
  Use esta opción cuando el directorio de AD que está asignando contiene varios usuarios, pero solo unos pocos de ellos usarán la plataforma de BI. La plataforma no crea automáticamente alias ni cuentas de Enterprise para todos los usuarios. En su lugar, crea alias (y cuentas, en caso necesario) solo para los usuarios que inician sesión en la plataforma de BI.

c. En el área *Opciones de usuarios nuevos*, seleccione una opción para crear nuevos usuarios:

- *Los usuarios nuevos se crean como usuarios con nombre*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios con nombre. Las licencias de usuario con nombre están asociadas a usuarios específicos y les permiten el acceso al sistema en base a sus nombres de usuario y sus contraseñas. Esto da acceso al sistema a los usuarios con nombre, independientemente del número de personas conectadas. Debe tener una licencia de usuario con nombre disponible por cada cuenta de usuario creada mediante esta opción.

  > **Nota**
  >
  > El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.
  >
  > Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

- *Los usuarios nuevos se crean como usuarios simultáneos*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios simultáneos. Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque una licencia simultánea pequeña puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios al sistema, una licencia simultánea de 100 usuarios puede admitir 250, 500 o 700 usuarios.

10. Para configurar cómo se programan actualizaciones de alias de AD, haga clic en *Programar*.

a. En el cuadro de diálogo *Programar*, seleccione una periodicidad de la lista *Ejecutar objeto*.

b. Configure otras opciones y parámetros de programación según sea necesario.
c. Haga clic en *Programar*.
Cuando se produce una actualización de alias, la información de grupo también se actualiza.

11. En el área *Opciones de enlace de atributos*, especifique la prioridad de enlace de atributos para el complemento de AD:
    a. Seleccione la casilla de verificación *Importar nombre completo, dirección de correo electrónico y otros atributos*.
    Los nombres completos y descripciones que se usan en las cuentas de AD se importan y se almacenan con los objetos de usuario en la plataforma de BI.
    b. Especifique una opción para *Establecer prioridad del enlace de atributos de AD en relación con otros enlaces de atributos*.
    Si la opción está configurada en 1, los atributos de AD tendrán prioridad cuando estén habilitados AD y otros complementos (LDAP y SAP). Si la opción está configurada en 3, tendrán prioridad los atributos de otros complementos habilitados. Las vinculaciones deben estar fijadas en diferentes valores. Si fija varios complementos de autenticación al mismo valor de vinculación, es posible que se produzcan resultados no esperados.
12. En el área *Opciones de grupo de AD*, configure las actualizaciones del grupo de AD:
    a. Haga clic en *Programar*.
    Aparecerá el cuadro de diálogo *Programar*.
    b. Seleccione una periodicidad de la lista *Ejecutar objeto*.
    c. Configure otras opciones y parámetros de programación según sea necesario.
    d. Haga clic en *Programar*.

    El sistema programará la actualización y la ejecutará según la programación que haya especificado. La siguiente actualización programada para las cuentas de grupo de AD se muestra bajo las *Opciones de grupo de AD*.
13. En el área *Actualización de AD a petición*, seleccione una opción para indicar si quiere que se actualicen los grupos de AD o bien los usuarios de AD (o ninguno de ellos) al hacer clic en *Actualizar*:
    - *Actualizar grupos AD ahora*
    Seleccione esta opción si quiere que se inicie la actualización de todos los grupos programados de AD al hacer clic en *Actualizar*. La siguiente actualización de grupo de AD programa se enumera en *Opciones del grupo AD*.
    - *Actualizar grupos AD y alias ahora*
    Seleccione esta opción si quiere que se inicie la actualización de todos los grupos de AD y los alias de usuario programados al hacer clic en *Actualizar*. Las siguientes actualizaciones programadas se enumeran en *Opciones de grupo de AD* y *Opciones de alias de AD*.
    - *No actualizar ahora grupos y alias de AD*
    No se actualizará ningún grupo de AD ni alias de usuario al hacer clic en *Actualizar*.
14. Haga clic en *Actualizar* y en *Aceptar*.

## 9.4.6.3.1.3 Deshabilitar SiteMinder

Si desea evitar que se configure SiteMinder, o para deshabilitarlo una vez configurado en la CMC, modifique el archivo de configuración Web para la plataforma de lanzamiento de BI.

#### 9.4.6.3.1.3.1 Para deshabilitar SiteMinder para clientes Java

Además de deshabilitar la configuración de SiteMinder para el complemento de seguridad de Windows AD, la configuración de SiteMinder debe estar deshabilitada para el archivo BOE WAR en el servidor de aplicaciones Web.

1. Vaya al siguiente directorio de la instalación de la Plataforma de BI:

   `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`
2. Abra el archivo `global.properties`.
3. Cambie `siteminder.enabled` a false

   ```
   siteminder.enabled=false
   ```
4. Guarde los cambios y cierre el archivo.

El cambio sólo surtirá efecto después de volver a desplegar `BOE.war` en el equipo que ejecuta el servidor de aplicaciones Web. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web. Para obtener más información sobre el uso de WDeploy para deshacer el despliegue de las aplicaciones Web, consulte el *Manual de despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 9.4.7 Resolución de problemas de la autenticación de Windows AD

### 9.4.7.1 Resolución de problemas de la configuración

Estos pasos pueden ser útiles si surgen problemas al configurar Kerberos:

- Habilitar el inicio de sesión
- Probar la configuración de Kerberos para SDK Java

#### 9.4.7.1.1 Para habilitar el inicio de sesión

1. En el menú *Inicio*, seleccione *Programas > Tomcat > Configuración de Tomcat*
2. Haga clic en la ficha *Java*.
3. Agregue las opciones siguientes:

   ```
   -Dcrystal.enterprise.trace.configuration=verbose
   -sun.security.krb5.debug=true
   ```

   Se creará un archivo de registro en la ubicación siguiente:

   ```
   C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
   ```

### 9.4.7.1.2 Para probar la configuración de Kerberos

Ejecute el comando siguiente para probar la configuración de Kerberos, donde `servant` es la cuenta de servicio y el dominio en el que se ejecuta el CMS, y `password` es la contraseña asociada a la cuenta de servicio.

```
<InstallDirectory>\SAP BusinessObjects Enterprise XI
4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

Por ejemplo:

```
C:\Program Files\SAP BusinessObjects\
 SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\
 servact@TESTM03.COM Password
```

Los nombres del dominio y del elemento principal del servicio tienen que coincidir exactamente con los nombres del dominio y del elemento principal del servicio de Active Directory. Si el problema continúa, compruebe si ha introducido el mismo nombre; tenga en cuenta que se distinguen las mayúsculas y minúsculas.

### 9.4.7.1.3 Error de inicio de sesión debido a nombres UPN y SAM de AD distintos

El ID de Active Directory de un usuario se ha asignado correctamente a la plataforma de BI. A pesar de esto, no pueden iniciar sesión correctamente en la CMC o la plataforma de lanzamiento de BI con la autenticación de Windows AD y Kerberos con el siguiente formato: `DOMAIN\ABC123`

Este problema puede aparecer cuando el usuario se configura en Active Directory con un UPN y un nombre SAM que no sean exactamente iguales. Los siguientes ejemplos pueden provocar un problema:

- El UPN es abc123@company.com pero el nombre SAM es DOMAIN\ABC123.
- El UPN es jsmith@company pero el nombre SAM es DOMAIN\johnsmith.

Hay dos formas de solucionar este problema:

- Pida a los usuarios que inicien la sesión mediante el UPN en lugar del nombre SAM.
- Compruebe que el nombre de cuenta SAM y el nombre UPN son los mismos.

### 9.4.7.1.4 Error de autenticación previa

Un usuario que anteriormente había podido iniciar sesión, ya no puede hacerlo correctamente. El usuario recibe este error: No se reconoció la información de la cuenta. El registro de errores de Tomcat muestra el siguiente error: `"Pre-authentication information was invalid (24)"`

Esto puede suceder porque la base de datos de usuarios de Kerberos no ha obtenido un cambio efectuado en UPN en AD. Puede significar que la base de datos de usuarios de Kerberos y la información de AD no están sincronizadas.

Para resolver este problema, restablezca la contraseña del usuario en AD. De este modo se garantiza que los cambios se propagan correctamente.

> **Nota**
>
> Esto no constituye un problema con J2SE 5.0.

## 9.5 Autenticación de SAP

### 9.5.1 Configurar la autenticación SAP

En esta sección se explica cómo configurar la autenticación de la Plataforma de BI para el entorno de SAP.

La autenticación SAP permite a los usuarios de SAP iniciar sesión en la plataforma de BI usando los nombres de usuario y las contraseñas de SAP, sin almacenar dichas contraseñas en la plataforma de BI. La autenticación SAP también permite conservar la información sobre las funciones de usuarios en SAP y usar esta información de funciones en la plataforma para asignar derechos para realizar tareas administrativas o acceder al contenido.

#### Acceder a la aplicación de autenticación SAP

Debe proporcionar información sobre su sistema SAP a la plataforma de BI. Puede acceder a una aplicación Web dedicada mediante la herramienta de administración principal de la plataforma de BI, la Consola de administración central (CMC). Para acceder a ella desde la página de inicio de CMC, haga clic en *Autenticación*.

#### Autenticar usuarios SAP

Los complementos de seguridad expanden y personalizan los métodos de autenticación de usuarios de la plataforma de BI. La función de autenticación SAP incluye un complemento de seguridad de SAP (`secSAPR3.dll`) para el componente Servidor de administración central (CMS) de la plataforma de BI. Este complemento de seguridad de SAP ofrece varias ventajas importantes:

- Actúa como un proveedor de autenticación que verifica las credenciales de usuario en el sistema SAP en nombre del CMS. Cuando los usuarios inician sesión directamente en la plataforma de BI, pueden elegir la autenticación SAP y proporcionar el nombre de usuario y la contraseña que normalmente usan para SAP. La plataforma de BI también puede validar vales de inicio de sesión de Enterprise Portal con sistemas SAP.
- Facilita la creación de cuentas ya que permite asignar funciones de SAP a grupos de usuarios de la plataforma de BI y facilita la administración de cuentas al permitir asignar derechos a usuarios y grupos de forma coherente en la plataforma de BI.
- Administra de forma dinámica las listas de funciones de SAP. Al asignar una función de SAP a la plataforma, todos los usuarios que pertenecen a dicha función pueden iniciar la sesión en el sistema. Al realizar cambios posteriores en los miembros de la función SAP, no necesitará actualizar la lista de la plataforma de BI.
- El componente Autenticación SAP incluye una aplicación Web para configurar el complemento. Puede acceder a esta aplicación en el área *Autenticación* de la Consola de administración central (CMC).

## 9.5.2 Creación de una cuenta de usuario para la plataforma de BI

El sistema de la Plataforma de BI necesita una cuenta de usuario con autorización para acceder a las listas de miembros de las funciones de SAP y para autenticar SAP. Necesita las credenciales de la cuenta para conectar la Plataforma de BI al sistema SAP. Para obtener instrucciones generales sobre la creación de cuentas de usuario SAP y la asignación de autorizaciones mediante funciones, consulte la documentación de SAP BW.

Utilice la transacción `SU01` para crear una nueva cuenta de usuario SAP con el nombre `CRYSTAL`. Utilice la transacción `PFCG` para crear una nueva función con el nombre `CRYSTAL_ENTITLEMENT`. (Se recomienda utilizar estos nombres, pero no es necesario hacerlo.) Cambie la autorización de la nueva función mediante la configuración de valores en los siguientes objetos de autorización:

| Objeto de autorización | Campo | Valor |
|---|---|---|
| Autorización de acceso a archivos (S_DATASET) | Actividad (ACTVT) | Lectura, escritura (33, 34) |
| | Nombre físico del archivo (FILENAME) | * (indica Todos) |
| | Nombre del programa ABAP (PROGRAM) | * |
| Comprobación de autorización para acceso RFC (S_RFC) | Actividad (ACTVT) | 16 |
| | Nombre del RFC que debe protegerse (RFC_NAME) | BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY |
| | Tipo del objeto RFC que debe protegerse (RFC_TYPE) | Grupo de funciones (FUGR) |
| Mantenimiento principal de usuarios: grupos de usuarios (S_USER_GRP) | Actividad (ACTVT) | Creación o generación, y visualización (03) |
| | Grupo de usuarios en mantenimiento principal de usuarios (CLASS) | * <br> **Nota** <br> Para obtener una mayor seguridad, es posible que prefiera indicar de forma explícita los grupos de usuarios cuyos miembros necesiten acceso a la plataforma de BI. |

Por último, agregue el usuario `CRYSTAL` a la función `CRYSTAL_ENTITLEMENT`.

> **→ Sugerencias**
>
> Si las directivas de su sistema requieren que los usuarios cambien su contraseña cuando inicien por primera vez la sesión en el sistema, inicie la sesión ahora con la cuenta de usuario `CRYSTAL` y vuelva a configurar su contraseña.

> **Nota**
>
> Es posible que se necesiten autorizaciones adicionales para el objeto S_RFC cuando se hayan habilitado determinadas ampliaciones de rendimiento en el entorno ABAP. Estos errores se informarán en la página Importación de rol y se anotará la función para la que ha fallado la autorización:
>
> **Ejemplo:** Sin autorización RFC para el módulo de funciones RFC_METADATA_GET.

| Objeto de autorización | Campo | Valor |
|---|---|---|
| Comprobación de autorización para acceso RFC (S_RFC) | Actividad (ACTVT) | 16 |
| | Nombre del RFC que debe protegerse (RFC_NAME) | BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY y RFC_METADATA |
| | Tipo del objeto RFC que debe protegerse (RFC_TYPE) | Grupo de funciones (FUGR) |

## 9.5.3 Conectar a sistemas de derechos de SAP

Antes de poder importar o publicar contenido de BW en la plataforma de BI, deberá proporcionar información acerca de los sistemas de derechos de SAP en los que desea integrarse. La plataforma de BI usa esta información para conectarse al sistema SAP de destino al determinar los miembros de la función y autenticar los usuarios de SAP.

### 9.5.3.1 Agregar un sistema de derechos de SAP

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en el vínculo *SAP*.

   Aparece la configuración de los sistemas de derechos.

   > **→ Sugerencias**
   >
   > Si la lista *Nombre del sistema lógico* ya muestra un sistema de derechos, haga clic en *Nuevo*.

3. En el campo *Sistema*, escriba el ID del sistema (SID) de tres caracteres del sistema SAP.
4. En el campo *Cliente*, escriba el número de cliente que debe usar la plataforma de BI al iniciar sesión en el sistema SAP.
   La plataforma de BI combina la información de sistema y cliente, y agrega una entrada a la lista *Nombre del sistema lógico*.
5. Compruebe que la casilla de verificación *Deshabilitado* está desactivada.

> **Nota**
>
> Use la casilla de verificación *Deshabilitado* para indicar a la plataforma de BI que un sistema SAP determinado se encuentra temporalmente deshabilitado.

6. Complete los campos *Servidor de mensajes* y *Grupo de inicio de sesión* según sea preciso, si ha configurado un equilibrio de carga de modo que la plataforma de BI deba iniciar sesión mediante un servidor de mensajes.

> **Nota**
>
> Debe efectuar las entradas adecuadas en el archivo `Servicios` del equipo de la plataforma de BI para habilitar el equilibrio de carga, sobre todo si el despliegue no se encuentra en un único equipo. Concretamente debe tener en cuenta todos los equipos que alberguen el CMS, el servidor de aplicaciones Web y todos los equipos que administren sus cuentas de autenticación y su configuración.

7. Si no ha configurado el equilibrio de carga (o si prefiere que la plataforma de BI inicie sesión directamente en el sistema SAP), complete los campos *Servidor de aplicaciones* y *Número del sistema* con los valores adecuados.
8. En los campos *Nombre de usuario*, *Contraseña* e *Idioma*, escriba el nombre de usuario, la contraseña y el código de idioma de la cuenta SAP que desea que use la plataforma de BI al iniciar sesión en SAP.

> **Nota**
>
> Estas credenciales se deben corresponder con las de la cuenta de usuario que se creó para la plataforma de BI.

9. Haga clic en *Actualizar*.

Si agrega varios sistemas de derecho, haga clic en la ficha *Opciones* para especificar el sistema que usa la plataforma de BI como valor predeterminado (es decir, el sistema con el que se pone en contacto para autenticar a los usuarios que intentan iniciar sesión con las credenciales de SAP sin especificar un sistema SAP determinado).

### 9.5.3.2 Para comprobar si el sistema de derechos se ha añadido correctamente

1. Haga clic en la ficha *Importación de función*.
2. Seleccione el nombre del sistema de derechos de la lista *Nombre del sistema lógico*.

   Si el sistema se ha agregado correctamente, la lista *Funciones disponibles* contendrá una lista de funciones que puede seleccionar para importar.

> **→ Sugerencias**
>
> Si no hay ninguna función visible en la lista *Nombre del sistema lógico*, busque mensajes de error en la página. Éstos pueden darle la información necesaria para corregir el problema.

### 9.5.3.3 Para deshabilitar temporalmente una conexión con un sistema de acceso condicionado SAP

En la CMC, puede deshabilitar temporalmente una conexión entre la plataforma de BI y un sistema de derechos de SAP. Puede ser útil mantener la receptividad de la Plataforma de BI en casos como el tiempo de inactividad programado de un sistema de derechos de SAP.

1. En la CMC, vaya al área de administración *Autenticación*.
2. Haga doble clic en el vínculo *SAP*.
3. En la lista *Nombre del sistema lógico*, seleccione el sistema que desee deshabilitar.
4. Active la casilla de verificación *Deshabilitado*.
5. Haga clic en *Actualizar*.

## 9.5.4 Establecer opciones de autenticación SAP

La autenticación SAP incluye varias opciones que se pueden especificar al integrar la plataforma de BI con el sistema SAP. Las opciones incluyen:

- Habilitar o deshabilitar la autenticación SAP
- Especificar la configuración de la conexión
- Vincular usuarios importados a los modelos de licencia de la plataforma de BI
- Configurar el inicio de sesión único en el sistema SAP

### 9.5.4.1 Para establecer las opciones de Autenticación SAP

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en el vínculo *SAP* y haga clic en la ficha *Opciones*.
3. Revise y modifique la siguiente configuración según sea necesario:

| Parámetro | Descripción |
|---|---|
| *Habilitar autenticación SAP* | Desactive esta casilla de verificación para deshabilitar la autenticación SAP.<br>**Nota**<br>Para deshabilitar la autenticación SAP en un sistema SAP específico, active la casilla de verificación *Deshabilitado* de la ficha *Sistemas de derechos*. |
| *Raíz de carpeta Contenido* | Especifique el lugar en el que desea que la plataforma de BI empiece a replicar la estructura de la carpeta de BW en la CMC y en la plataforma de lanzamiento de BI. |

| Parámetro | Descripción |
| --- | --- |
| | El valor predeterminado es `/SAP/2.0`, pero puede cambiarlo a una carpeta diferente. Si desea cambiar el valor, debe modificarlo en la CMC y el Trabajo de administración de contenidos. |
| *Sistema predeterminado* | Seleccione un sistema de derechos de SAP para la plataforma de BI para contactar con usuarios autenticados que intentan iniciar sesión con las credenciales de SAP pero sin especificar un sistema particular de SAP.<br><br>**Nota**<br>Si selecciona un sistema predeterminado, los usuarios de dicho sistema no tendrán que introducir su ID del sistema o cliente cuando se conecten desde herramientas cliente, como Live Office o Universe Designer, que utilizan la autenticación SAP. Por ejemplo, si SYS~100 está establecido como el sistema predeterminado, SYS~100/user1 podrá conectarse como user1 cuando se elija la autenticación SAP. |
| *Número máximo de intentos fallidos para acceder al sistema de derechos* | Escriba el número de veces que la plataforma de BI debe volver a intentar ponerse en contacto con un sistema SAP para realizar peticiones de autenticación.<br><br>Si configura el valor en -1, permite que la plataforma intente ponerse en contacto con el sistema de derechos un número ilimitado de veces. Si configura el valor en 0 limita a la plataforma de BI a un solo intento de ponerse en contacto con el sistema de derechos.<br><br>**Nota**<br>Use esta configuración junto con la opción *Mantener deshabilitado el sistema de derechos [segundos]* para configurar el modo en que la plataforma de BI administra los sistemas de derechos de SAP que no están disponibles temporalmente. El sistema usa las dos opciones para determinar cuándo debe detener la comunicación con un sistema SAP que no está disponible y cuándo debe reanudarla. |
| *Mantener deshabilitado el sistema de derechos [segundos]* | Escriba el número de segundos que la plataforma de BI debe esperar antes de volver a intentar autenticar a los usuarios con el sistema SAP.<br><br>Por ejemplo, si *Accesos fallidos máx. al sistema de derechos* está fijado en 3, la plataforma de BI permite un máximo de tres intentos fallidos de autenticar usuarios en un sistema SAP. Un cuarto intento fallido detiene |

| Parámetro | Descripción |
| --- | --- |
| | el sistema de intentar autenticar los usuarios contra el sistema durante el tiempo especificado. |
| *Número máximo de conexiones simultáneas por sistema* | Especifique el número de conexiones que desea mantener abiertas a la vez en el sistema SAP.<br><br>Por ejemplo, si escribe 2, la plataforma de BI mantiene dos conexiones abiertas en SAP. |
| *Número de usos por conexión* | Especifique el número de operaciones que desea permitir en el sistema SAP por conexión.<br><br>Por ejemplo, si *Conexiones simultáneas máx. por sistema* está fijado en 2 y *Número de usos por conexión* está fijado en 3, cuando haya tres inicios de sesión en una conexión, se cierra la plataforma de BI y reinicia la conexión. |
| *Usuarios simultáneos* y *Usuarios con nombre* | Especifique si las nuevas cuentas de usuario utilizarán licencias de usuario simultáneas o licencias de usuario con nombre.<br><br>Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque un pequeño número de licencias simultáneas puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios al sistema, una licencia simultánea de 100 usuarios puede admitir 250, 500 o 700 usuarios.<br><br>Las licencias de usuario con nombre se asocian con usuarios y permiten que tengan acceso al sistema basándose en sus nombres de usuario y en sus contraseñas. De esta forma, los usuarios con nombre pueden tener acceso al sistema independientemente del número de personas conectadas.<br><br>**Nota**<br><br>El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.<br><br>Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos. |

| Parámetro | Descripción |
| --- | --- |
| | **Nota**<br>La opción que seleccione no cambia el número o el tipo de licencias de usuario que ha instalado en la plataforma de BI. Debe disponer de las licencias apropiadas disponibles en el sistema. |
| *Importar nombre completo, dirección de correo electrónico y otros atributos* | Especifique un nivel de prioridad para el complemento de autenticación SAP.<br>Los nombres completos y las descripciones que se usan en las cuentas SAP se importan y almacenan con los objetos de usuario en la plataforma de BI. |
| *Configurar la prioridad del enlace del atributo de SAP en relación a otros enlaces de atributos* | Especifica una prioridad para enlazar atributos de usuario de SAP (nombre completo y dirección de correo electrónico).<br>Si la opción está configurada en 1, los atributos SAP tendrán prioridad en escenarios en los que estén habilitados SAP y otros complementos (Windows AD y LDAP). Si la opción está configurada en 3, tendrán prioridad los atributos de otros complementos habilitados. Las vinculaciones deben estar fijadas en diferentes valores. Si fija varios complementos de autenticación al mismo valor de vinculación, es posible que se produzcan resultados no esperados. |

Establezca las siguientes opciones para configurar el servicio de inicio de sesión único de SAP:

| Parámetro | Descripción |
| --- | --- |
| *ID del sistema* | El identificador de sistema que proporciona la plataforma de BI al sistema SAP al realizar un servicio de inicio de sesión único de SAP. |
| *Examinar* | Haga clic para cargar el archivo de `almacén de claves` generado para activar el inicio de sesión único SAP. También puede introducir manualmente la ruta completa al archivo. |
| *Contraseña del almacén de claves* | Proporciona la contraseña necesaria para acceder al archivo de `almacén de claves`. |
| *Contraseña de clave privada* | Proporciona la contraseña necesaria para acceder al certificado correspondiente al archivo de `almacén de claves`. El certificado se almacena en el sistema SAP. |
| *Alias de clave privada* | Proporciona el alias necesario para acceder al archivo de `almacén de claves`. |

4. Haga clic en *Actualizar*.

### 9.5.4.2 Para cambiar Raíz de carpeta Contenido

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en el vínculo *SAP*.
3. Haga clic *Opciones* y escriba el nombre de la carpeta en el campo *Raíz de carpeta de contenido*.

   El nombre de carpeta que escriba aquí será la carpeta a partir de la cual desea que la plataforma de BI comience a replicar la estructura de carpetas de BW.
4. Haga clic en *Actualizar*.
5. En el Puesto de trabajo de administración de contenido de BW, expanda *Sistema Enterprise*.
6. Expanda *Sistemas disponibles* y haga doble clic en el sistema al que se esté conectando la plataforma de BI.
7. Haga clic en la ficha *Diseño* y en *Carpeta de base de contenido*, escriba la carpeta que desee usar como la carpeta SAP raíz en la plataforma de BI (por ejemplo, `/SAP/2.0/`).

## 9.5.5 Importación de funciones de SAP

Al importar funciones de SAP en la plataforma de BI, permite que los miembros de funciones inicien sesión en el sistema con las credenciales de SAP normales. Además, el inicio de sesión único está habilitado de modo que los usuarios de SAP inician sesión automáticamente en la plataforma de BI al acceder a los informes desde la GUI de SAP o un SAP Enterprise Portal.

> **Nota**
>
> A menudo existen muchos requisitos para habilitar el inicio de sesión único. Algunos pueden incluir utilizar un controlador y una aplicación que admitan el inicio de sesión único o garantizar que el servidor y el servidor Web se encuentran en el mismo dominio.

Para cada función que importa, la plataforma de BI genera un grupo. Cada grupo recibe un nombre según la siguiente convención: **`<SystemID~ClientNumber@NameOfRole>`**. Puede ver los nuevos grupos en el área de administración *Usuarios y grupos* de la CMC. También puede usar estos grupos para definir la seguridad de objetos en la plataforma de BI.

Tenga en cuenta tres categorías principales de usuarios al configurar la plataforma de BI para la publicación y al importar funciones en el sistema:

- Administradores de la plataforma de BI
  Los administradores de Enterprise configuran el sistema para publicar contenido desde SAP. Importan las funciones adecuadas, crean las carpetas necesarias y asignan derechos a estas funciones y carpetas en la plataforma de BI.
- Editores de contenido
  Los editores de contenido son los usuarios que tienen derechos para publicar contenido en las funciones. Esta categoría de usuario tiene como finalidad separar los miembros de función normales de aquellos usuarios con derechos para publicar informes.
- Miembros de funciones
  Los miembros de funciones son usuarios que pertenecen a funciones «con contenido». Es decir, estos usuarios pertenecen a funciones donde se publican informes. Cuentan con derechos de *visualización*, *visualización a petición* y *programación* en cualquier informe publicado en las funciones a las que

pertenecen. Sin embargo, los miembros de función normales no pueden publicar nuevo contenido ni versiones actualizadas del contenido.

Debe importar todas las funciones de publicación de contenido y con contenido en la plataforma de BI antes de publicar por primera vez.

> **Nota**
>
> Se recomienda que mantenga independientes las actividades de las funciones. Por ejemplo, mientras que la función de administrador puede publicar, es mejor que sólo las funciones de los editores de contenido sean las que publiquen. Además, el cometido de las funciones de publicación de contenido es tan sólo definir los usuarios que pueden publicar contenido. De esta forma, las funciones de publicación de contenido no deben incluir contenido alguno; los editores de contenido deben publicar en funciones relacionadas con contenido a las que puedan acceder los miembros de funciones normales.

### 9.5.5.1 Importar funciones de SAP

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en el vínculo *SAP*.
3. En la ficha *Opciones*, seleccione *Usuarios simultáneos* o *Usuarios con nombre*, según su contrato de licencia.

   Esta opción no cambia el número o el tipo de licencias de usuario que ha instalado en la plataforma de BI. Debe disponer de las licencias apropiadas disponibles en el sistema.
4. Haga clic en *Actualizar*.
5. En la ficha *Importación de función*, seleccione el sistema de derechos adecuado de la lista *Nombre del sistema lógico*.
6. En el área *Funciones disponibles*, seleccione las funciones que desea importar, y haga clic en *Agregar*.
7. Haga clic en *Actualizar*.

### 9.5.5.2 Comprobar que las funciones y los usuarios se han importado correctamente

Antes de iniciar esta tarea, tome nota del nombre de usuario y la contraseña de un usuario SAP que pertenezca a una de las funciones que asignó a la plataforma de BI.

1. Para la plataforma de lanzamiento de BI Java , vaya a **`http://<servidorweb>:<númerodepuerto>/BOE/BI`**.

   Reemplace `<servidorWeb>` por el nombre del servidor Web y `<númeroPuerto>` por el número de puerto de la plataforma de BI. Es posible que tenga que solicitar al administrador el nombre del servidor Web, el número de puerto o la dirección URL para introducir.
2. En la lista *Tipo de autenticación*, seleccione *SAP*.

> **Nota**
>
> De forma predeterminada, la lista *Tipo de autenticación* está oculta en la plataforma de lanzamiento de BI. Si la lista no es visible, pida al administrador del sistema que active la lista *Tipo de autenticación* en el archivo `BIlaunchpad.properties` y, a continuación, reinicie el servidor de aplicaciones.

3. Introduzca el sistema SAP y el cliente del sistema con el que desea iniciar sesión.
4. Introduzca el nombre de usuario y la contraseña de un usuario asignado.
5. Haga clic en *Iniciar sesión*.

   Iniciará sesión en la plataforma de lanzamiento de BI como el usuario seleccionado.

## 9.5.5.3 Actualización de funciones y usuarios de SAP

Después de habilitar la autenticación SAP, es necesario programar y ejecutar regularmente actualizaciones en las funciones asignadas que se han importado en la plataforma de BI. Esto garantizará que la información de las funciones de SAP se refleja con exactitud en la plataforma.

Existen dos opciones para ejecutar y programar actualizaciones para las funciones de SAP:

- Solo actualizar funciones: Con esta opción solo se actualizarán los vínculos entre las funciones actualmente asignadas que se han importado en la plataforma de BI. Es aconsejable usar esta opción si tiene la intención de ejecutar actualizaciones con frecuencia y le preocupa el uso de los recursos del sistema. No se crearán cuentas de usuario si solo actualiza las funciones de SAP.
- Actualizar funciones y alias: Esta opción además de actualizar los vínculos entre las funciones, crea nuevas cuentas de usuario en la plataforma de BI para los alias de usuario agregados a las funciones en el sistema SAP.

> **Nota**
>
> Si, cuando ha activado la autenticación de SAP, no ha especificado crear automáticamente alias para las actualizaciones, no se crearán cuentas para los nuevos alias.

### 9.5.5.3.1 Programar actualizaciones para funciones de SAP

Después de asignar funciones en la plataforma de BI, debe especificar el modo en que el sistema actualiza las funciones.

1. Haga clic en la ficha *Actualización de usuario*.
2. Haga clic en *Programar* en la sección *Solo actualizar funciones* o el área *Actualizar funciones y alias*.

   > **→ Sugerencias**
   >
   > Para ejecutar inmediatamente una actualización, haga clic en *Actualizar ahora*.

> → Sugerencias
>
> Use la opción *Sólo actualizar funciones* si desea realizar actualizaciones con frecuencia y le preocupa el uso de los recursos del sistema. La actualización de funciones y alias tarda más en realizarse.

Aparece el cuadro de diálogo *Periodicidad*.

3. Seleccione una opción de la lista *Ejecutar objeto* y proporcione la información de programación que se le solicite en los campos provistos.

   Cuando programa una actualización, puede elegir entre los patrones de repetición que se resumen en la siguiente tabla:

| Patrón de periodicidad | Descripción |
|---|---|
| *Cada hora* | La actualización se ejecutará cada hora. Especifique la hora en que se iniciará y las fechas de inicio y de finalización. |
| *Diario* | La actualización se ejecutará cada día o cada <n> días (dónde <n> es el número de días que especifica). Puede especificar la hora en que se iniciará y las fechas de inicio y de finalización. |
| *Semanal* | La actualización se ejecutará una vez a la semana o varias veces a la semana. Puede especificar los días en que se ejecutará, la hora en que se iniciará, y las fechas de inicio y de finalización. |
| *Mensual* | La actualización se ejecutará cada mes o cada varios meses. Puede especificar la hora en que se iniciará y las fechas de inicio y de finalización. |
| *Día N de cada mes* | La actualización se ejecutará un día específico del mes. Puede especificar en qué día del mes y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| *Primer lunes de cada mes* | La actualización se ejecutará el primer lunes de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| *Último día del mes* | La actualización se ejecutará el último día de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| *Día X de la semana N de cada mes* | La actualización se ejecutará un día especificado de una semana especificada del mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| *Calendario* | La actualización se ejecutará en las fechas especificadas en un calendario que se haya creado previamente. |

4. Haga clic en *Programar*.
   La fecha de la siguiente actualización de función programada aparece en la ficha *Actualización de usuario*.

> → Sugerencias
>
> Para cancelar la siguiente actualización programada, haga clic en *Cancelar actualizaciones programadas* en el área *Solo actualizar funciones* o *Actualizar funciones y alias*.

## 9.5.6 Configuración de la Comunicación de red segura (SNC)

En esta sección se describe cómo configurar la SNC como parte del proceso de configuración de la autenticación SAP en la plataforma de BI.

Para obtener más información, consulte la Nota SAP 1396213.

Antes de configurar la confianza entre los sistemas de SAP y de la Plataforma de BI, debe asegurarse de que el SIA está configurado para iniciarse y ejecutarse en una cuenta que se ha configurado para SNC. También debe configurar el sistema SAP para que confíe en la plataforma de BI.

### Información relacionada

Introducción a la confianza en el lado del servidor de SAP [página 350]

## 9.5.6.1 Introducción a la confianza en el lado del servidor de SAP

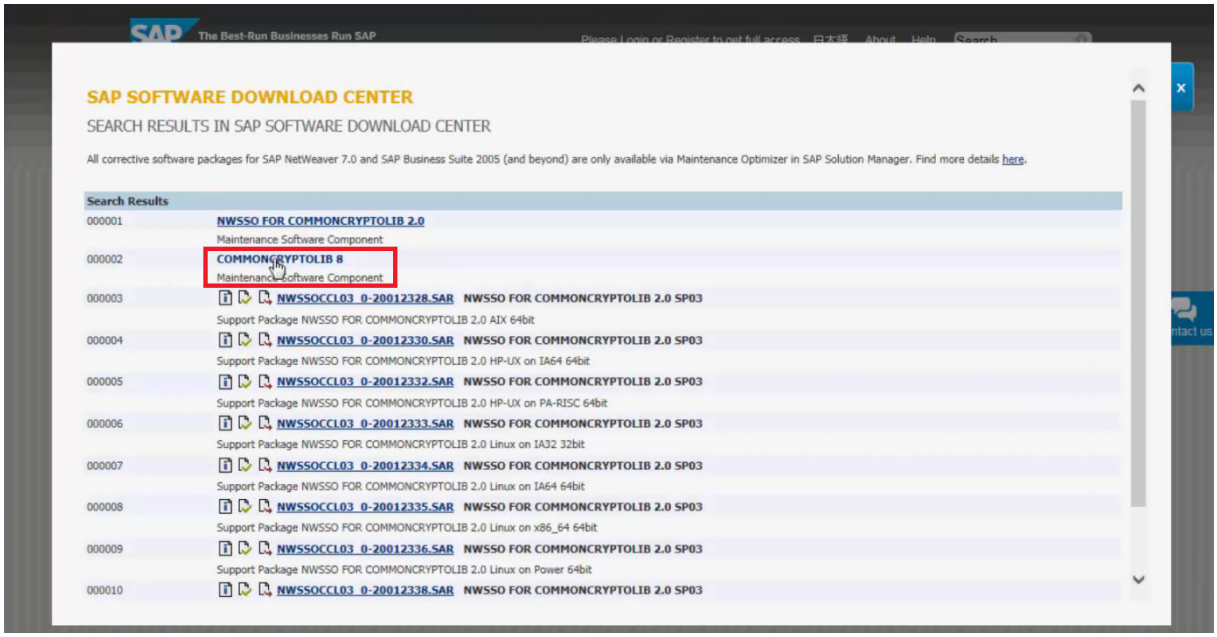
En esta sección se ofrecen procedimientos para configurar la confianza entre los servidores de aplicaciones Web de SAP (versión 6.20 y posteriores) y la plataforma SAP BusinessObjects Business Intelligence. Debe configurar la confianza en el lado del servidor si va a utilizar el envío masivo de informes en múltiples procesos (para las publicaciones donde la consulta del informe depende del contexto del usuario).

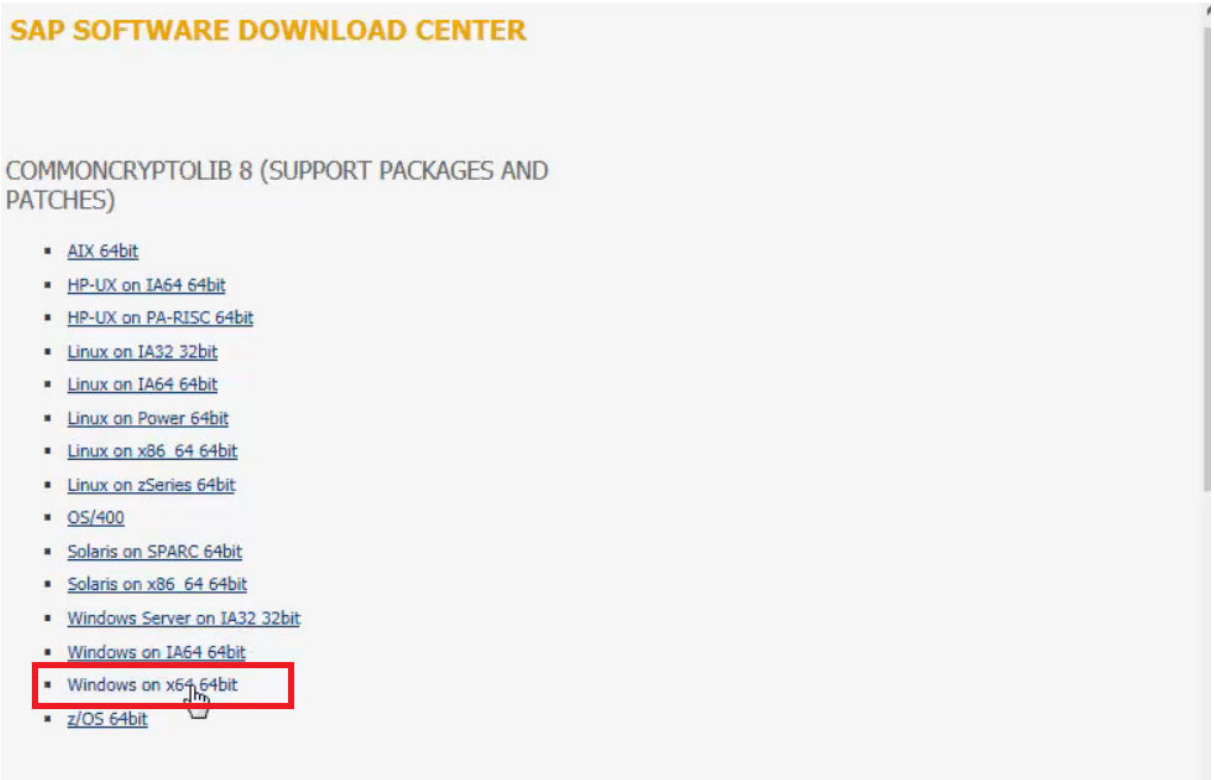
La confianza en el lado del servidor implica una suplantación sin contraseña. Para suplantar un usuario de SAP sin proporcionar una contraseña, el usuario debe identificarse con SAP por medio de un método más seguro que el de un nombre de usuario y una contraseña estándar. (Un usuario de SAP con el perfil de autorización SAP_ALL no puede suplantar a otro usuario de SAP sin conocer la contraseña de dicho usuario.)

### Activar la confianza en el lado del servidor por medio de la biblioteca de cifrado de SAP

Para habilitar la confianza del servidor para la plataforma de BI con la biblioteca de cifrado de SAP, debe ejecutar los servidores relevantes con credenciales que estén autenticadas con un proveedor de comunicación de red segura (SNC) registrado. Estas credenciales se configuran dentro de SAP para permitir la suplantación sin necesidad de contraseña. Para la plataforma de BI, debe ejecutar los servidores implicados en el envío masivo de informes con estas credenciales SNC, como el servidor de tareas de Adaptive.

Necesita binarios SNC de 32 bits para procesos de 32 bits; binarios SNC de 64 bits para procesos de 64 bits. Se ha instalado una biblioteca de cifrado de SAP junto con la plataforma de BI. Recuerde que la biblioteca de cifrado de SAP sólo se puede usar para configurar la confianza en el lado del servidor. La biblioteca de cifrado está disponible para Windows y Unix.


SAP
The Best-Run Businesses Run SAP
SAP SOFTWARE DOWNLOAD CENTER
SEARCH RESULTS IN SAP SOFTWARE DOWNLOAD CENTER
All corrective software packages for SAP NetWeaver 7.0 and SAP Business Suite 2005 (and beyond) are only available via Maintenance Optimizer in SAP Solution Manager. Find more details here.
Search Results
000001 NWSSO FOR COMMONCRYPTOLIB 2.0
Maintenance Software Component
000002 COMMONCRYPTOLIB 8
Maintenance Software Component
000003 NWSSOCCL03_0-20012328.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 AIX 64bit
000004 NWSSOCCL03_0-20012330.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 HP-UX on IA64 64bit
000005 NWSSOCCL03_0-20012332.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 HP-UX on PA-RISC 64bit
000006 NWSSOCCL03_0-20012333.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on IA32 32bit
000007 NWSSOCCL03_0-20012334.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on IA64 64bit
000008 NWSSOCCL03_0-20012335.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on x86_64 64bit
000009 NWSSOCCL03_0-20012336.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03
Support Package NWSSO FOR COMMONCRYPTOLIB 2.0 Linux on Power 64bit
000010 NWSSOCCL03_0-20012338.SAR NWSSO FOR COMMONCRYPTOLIB 2.0 SP03


SAP SOFTWARE DOWNLOAD CENTER
COMMONCRYPTOLIB 8 (SUPPORT PACKAGES AND PATCHES)
AIX 64bit
HP-UX on IA64 64bit
HP-UX on PA-RISC 64bit
Linux on IA32 32bit
Linux on IA64 64bit
Linux on Power 64bit
Linux on x86_64 64bit
Linux on zSeries 64bit
OS/400
Solaris on SPARC 64bit
Solaris on x86_64 64bit
Windows Server on IA32 32bit
Windows on IA64 64bit
Windows on x64 64bit
z/OS 64bit

Para obtener más información sobre la biblioteca de cifrado, consulte las notas de SAP 711093, 597059 y 397175 en el sitio Web de SAP.

En necesario asignar certificados al servidor SAP y a la plataforma de BI que demuestren la identidad de uno con otro. Cada servidor tendrá su propio certificado y una lista de certificados de las partes en las que se confía. Para configurar la confianza del servidor entre SAP y la plataforma de BI se debe crear un conjunto de certificados protegidos por contraseña denominado Entorno de seguridad personal (PSE). En esta sección se describe cómo configurar y mantener los PSE y cómo asociarlos de forma segura con servidores de procesamiento de la plataforma de BI.

## Responsabilidades del servidor de la plataforma de BI de SAP BusinessObjects

Algunos servidores específicos de la Plataforma de BI son importantes para la integración de SAP en cuanto al inicio de sesión único (SSO). La siguiente tabla enumera estos servidores y sus áreas de responsabilidad.

| Servidor | Áreas de responsabilidad |
|---|---|
| Servidor de aplicaciones Web | Lista de funciones de Autenticación SAP |
| Servicio del publicador de BW | Listas de selección y personalización de parámetros dinámicos de Crystal Reports |
| CMS | Contraseña, vale, comprobación de pertenencia de función y listas de usuarios |
| Servidor de páginas | Ver a petición de Crystal Reports |
| Servidor de tareas | Programación de Crystal Reports |
| Servidor de procesamiento de Web Intelligence | Visualización y programación de informes de Web Intelligence y peticiones de listas de valores (LOV) |
| Servicio de análisis multidimensional | Análisis |

## 9.5.6.2 Configurar SAP para la confianza en el lado del servidor

La confianza del lado servidor se aplica únicamente a los informes de Crystal y de Web Intelligence que están basados en Universos (`.unv`). Tiene que configurar SNC para su uso con la plataforma de BI. Para obtener información o para obtener asistencia de resolución de problemas, consulte la documentación de SAP proporcionada con el servidor de SAP.

### 9.5.6.2.1 Para configurar SAP para la confianza en el lado del servidor

1. Asegúrese de que dispone de las credenciales de administrador de SAP para SAP y para el equipo que ejecuta SAP, y las credenciales del administrador para la plataforma de BI y del equipo (o equipos) en el que se ejecuta.
2. En el equipo SAP, asegúrese de que la biblioteca de cifrado de SAP y la herramienta SAPGENPSE están ubicados en el directorio `<UNIDAD>:\usr\sap\<SID>\SYS\exe\run\` (en Windows).
3. Cree una variable de entorno llamada **`<SECUDIR>`** que apunte al directorio donde reside el ticket.

   > **Nota**
   >
   > Esta variable debe estar accesible para el usuario con el que se ejecuta el proceso *disp+work* de SAP.

4. En la interfaz de usuario de SAP, vaya a la transacción RZ10 y cambie el perfil de instancia en modo *Extended maintenance*.
5. En el modo de edición de perfiles, apunte las variables de perfil de SAP hacia la biblioteca de cifrado y proporcione un nombre completo (DN) al sistema SAP. Estas variables deberán seguir la convención de nomenclatura de LDAP:

| Etiqueta | Significado | Descripción |
|---|---|---|
| **`CN`** | Nombre común | Nombre común del propietario del certificado. |
| **`OU`** | Unidad organizacional | Por ejemplo, PG para Grupo de productos. |
| **`O`** | Organización | Nombre de la organización para la que se emitió el certificado. |
| **`C`** | País | País en el que se encuentra la organización. |

Por ejemplo, para R21: **`p:CN=R21, OU=PG, O=BOBJ, C=CA`**

> **Nota**
>
> El prefijo **`p:`** es para la biblioteca de cifrado de SAP. Es necesario a la hora de hacer referencia al DN desde SAP, aunque no estará visible cuando se examinen certificados en STRUST o con SAPGENPSE.

6. Introduzca los siguientes valores de perfil, reemplazando su sistema SAP donde sea necesario:

| Variable de perfil | Valor |
|---|---|
| `ssf/name` | `SAPSECULIB` |
| `ssf/ssfapi_lib` | Ruta completa a la biblioteca sapcrypto |
| `sec/libsapsecu` | Ruta completa a la biblioteca sapcrypto |
| `snc/gssapi_lib` | Ruta completa a la biblioteca sapcrypto |
| `snc/identity/as` | DN del sistema SAP |

7. Reinicie la instancia de SAP.
8. Cuando se vuelva a ejecutar el sistema, inicie sesión y vaya a la transacción STRUST, que ahora debe tener entradas adicionales para SNC y SSL.
9. Haga clic con el botón derecho del ratón en el nodo SNC y haga clic en *Crear*.
   Ahora debería aparecer la identidad que especificó en RZ10.
10. Haga clic en *Aceptar*.
11. Para asignar una contraseña al PSE de SNC, haga clic en el icono de candado.

> **Nota**
>
> No pierda esta contraseña. STRUST se la pedirá cada vez que consulte o edite el PSE de SNC.

12. Guarde los cambios.

> **Nota**
>
> Si no guarda los cambios, el servidor de aplicaciones no volverá a ejecutarse cuando active SNC.

13. Vuelva a la transacción RZ10 y agregue el recordatorio de los parámetros del perfil SNC:

| Variable de perfil | Parámetro |
|---|---|
| `snc/accept_insecure_rfc` | `1` |
| `snc/accept_insecure_r3int_rfc` | `1` |
| `snc/accept_insecure_gui` | `1` |
| `snc/accept_insecure_cpic` | `1` |
| `snc/permit_insecure_start` | `1` |
| `snc/data_protection/min` | `1` |
| `snc/data_protection/max` | `3` |
| `snc/enable` | `1` |

El nivel de protección mínimo está definido en solo autenticación (1) y el máximo es privacidad (3). El valor `snc/data_protection/use` define que en este caso se use solo autenticación, aunque también podría ser (2) para integridad, (3) para privacidad y (9) para el máximo disponible. Los valores de `snc/accept_insecure_rfc`, `snc/accept_insecure_r3int_rfc`, `snc/accept_insecure_gui` y `snc/accept_insecure_cpic` establecidos en (1) garantizan que se sigan permitiendo los métodos de comunicación anteriores (y potencialmente inseguros).

14. Reinicie el sistema SAP.

Ahora debe configurar la plataforma de BI para la confianza del servidor.

## 9.5.6.3 Configuración de la plataforma de BI para la confianza del servidor

Se deben llevar a cabo los siguientes procedimientos para poder configurar la confianza del servidor en la plataforma de BI. Tenga en cuenta que estos pasos están basados en Windows, pero ya que la herramienta de SAP es de línea de comandos, estos pasos son muy similares en Unix.

1. Configurar el entorno
2. Generar un entorno de seguridad personal (PSE)
3. Configuración de los servidores de la plataforma de BI
4. Configurar el acceso del PSE
5. Configurar los ajustes del SNC de la autenticación SAP
6. Configurar los servidores dedicados de SAP

### Información relacionada

Para configurar el entorno [página 355]
Para generar un PSE [página 356]
Configurar servidores de la Plataforma de BI [página 357]
Para configurar el acceso PSE [página 358]
Para realizar la configuración de SNC de la autenticación SAP [página 358]
Usar grupos de servidores [página 360]

## 9.5.6.3.1 Para configurar el entorno

La plataforma de BI incluye una biblioteca de cifrado de SAP. Si utiliza la biblioteca estándar, solo necesita realizar los dos últimos pasos: crear una subcarpeta y agregar una variable de entorno. Sin embargo, para configurar una copia personalizada de la biblioteca de cifrado de SAP, lleve a cabo todos estos pasos.

La biblioteca de cifrado de SAP se puede encontrar en esta ubicación:

- Windows: `<INSTALLDIR>\sap\sapcrypto.dll`
- Unix: `<INSTALLDIR>/sap/libsapcrypto.so`

Antes de comenzar, compruebe lo siguiente:

- La biblioteca de cifrado de SAP se ha descargado y se ha expandido en el host en el que se ejecutan los servidores de procesamiento de la plataforma de BI.
- Los sistemas SAP apropiados se han configurado para usar la biblioteca de cifrado de SAP como proveedor de SNC.

Antes de poder iniciar el mantenimiento del PSE, debe configurar la biblioteca, la herramienta y el entorno donde están almacenados los PSE.

1. Copie la biblioteca de cifrado de SAP (incluida la herramienta de mantenimiento de PSE) en una carpeta del equipo que ejecuta la plataforma de BI.

   Por ejemplo: `C:\Archivos de programa\SAP\Crypto`.
2. Agregue la carpeta a la variable de entorno `<PATH>`.
3. Agregue una variable de entorno para todo el sistema `<SNC_LIB>` que señale a la biblioteca de cifrado.

   Por ejemplo: `C:\Archivos de programa\SAP\Crypto\sapcrypto.dll`

   > **Nota**
   >
   > La longitud máxima de la ruta es de 100 caracteres.
4. Cree una subcarpeta llamada **`sec`**.

   Por ejemplo: `C:\Archivos de programa\SAP\Crypto\sec`.
5. Agregue una variable de entorno para todo el sistema `<SECUDIR>` que señale a la carpeta **`sec`**.

### Información relacionada

Configurar SAP para la confianza en el lado del servidor [página 353]

## 9.5.6.3.2 Para generar un PSE

SAP acepta un servidor de la plataforma de BI como entidad de confianza cuando los servidores de la plataforma de BI relevantes tienen un PSE y dicho PSE está asociado con SAP. Esta «confianza» entre componentes de SAP y de la Plataforma de BI se establece mediante el uso compartido de la versión pública de los certificados de uno y otro. El primer paso consiste en generar un PSE para la plataforma de BI que genere automáticamente su propio certificado.

1. Abra una petición de comandos y ejecute **`sapgenpse.exe gen_pse -a sha256WithRsaEncryption -s 2048 -v -p BOE.pse`** desde la carpeta de la biblioteca de cifrado.
2. Seleccione un PIN y el DN que desea para el sistema de la Plataforma de BI.

   Por ejemplo, **`CN=MyBOE01, OU=PG, O=BOBJ, C=CA`**.

   Ahora ya tiene un PSE predeterminado, con su propio certificado.
3. Use el siguiente comando para exportar el certificado en el PSE:

   ```
   sapgenpse.exe export_own_cert -v -p BOE.pse -o <MyBOECert.crt>
   ```
4. En la interfaz de usuario de SAP, vaya a la transacción STRUST y abra el sistema PSE asociado con el sistema SAP.

   El sistema le pedirá la contraseña que ya tiene asignada a este sistema PSE.
5. Importe el archivo `<MyBOECert.crt>` creado anteriormente haciendo clic en el botón «Importar certificado» en la parte inferior izquierda de la pantalla de transacción STRUST.

   Los certificados de SAPGENPSE tienen la codificación Base64. Asegúrese de que selecciona Base64 en el momento de importarlos.

6. Para agregar el certificado de la Plataforma de BI a la lista de certificados PSE del servidor SAP, haga clic en el botón *Agregar*.
7. Guarde los cambios en STRUST.
8. Haga clic en el botón *Exportar* y proporcione un nombre de archivo para el certificado.

   Por ejemplo, **`MySAPCert.crt`**.

   > ⓘ Nota
   >
   > El formato debe seguir siendo Base64.

9. Diríjase a la transacción SNC0.
10. Agregue una nueva entrada donde:
    - El ID del sistema es arbitrario pero refleja el sistema de la Plataforma de BI.
    - El nombre SNC debe ser el DN (prefijado por **`p:`**) que proporcionó al crear su plataforma de BI PSE (en el paso 2).
    - Las casillas de verificación *Entrada para RFC activada* y *Entrada para ID ext.activada* están seleccionadas:
11. Para agregar el certificado exportado al PSE de la Plataforma de BI, ejecute el siguiente comando en el símbolo del sistema:

    ```
    sapgenpse.exe maintain_pk -v -a <MySAPCert.crt> -p BOE.pse
    ```

La biblioteca de cifrado de SAP está instalada en el equipo de la Plataforma SAP . Ha creado un PSE que usarán los servidores de la Plataforma de BI para identificarse con servidores SAP. SAP y el PSE de la Plataforma de BI han intercambiado certificados. SAP permite que las entidades con acceso al PSE de la Plataforma de BI realicen llamadas RFC y suplantación sin contraseña.

### Información relacionada

Configurar servidores de la Plataforma de BI [página 357]

## 9.5.6.3.3 Configurar servidores de la Plataforma de BI

Después de generar un PSE para la plataforma de BI, debe configurar una estructura de servidor apropiada para el procesamiento de SAP. El procedimiento siguiente crea un nodo para servidores de procesamiento de SAP de modo que pueda establecer credenciales de sistema operativo a nivel de nodo.

> ⓘ Nota
>
> En esta versión de la plataforma de BI, los servidores ya no se configuran en el Administrador de configuración central (CCM). En vez de eso, se deben crear un Server Intelligence Agent (SIA) nuevo.

1. En el CCM, cree un nodo nuevo para los servidores de procesamiento de SAP.

   Asigne un nombre apropiado al nodo, por ejemplo, **`SAPProcessor`**.
2. En la CMC, agregue los servidores de procesamiento que necesite al nuevo nodo y, luego, inicie los nuevos servidores.

## 9.5.6.3.4 Para configurar el acceso PSE

Después de configurar el nodo y los servidores de la Plataforma de BI, debe configurar el acceso PSE con la herramienta SAPGENPSE.

1. Ejecute el comando siguiente desde el símbolo del sistema:

   ```
   sapgenpse.exe seclogin -p SBOE.pse
   ```

   > **Nota**
   >
   > El sistema le pedirá el PIN de PSE. No es necesario que especifique un nombre de usuario si ejecuta la herramienta con las mismas credenciales que usan los servidores de procesamiento de SAP de la Plataforma de BI.

2. Para verificar que el enlace de inicio de sesión único (SSO) está establecido, enumere el contenido de PSE con el siguiente comando:

   ```
   sapgenpse.exe maintain_pk -l
   ```

   Los resultados deben tener un aspecto similar al siguiente:

   ```
   C:\Documents and
   Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
   maintain_pk -l
    maintain_pk for PSE "C:\Documents and Settings\username\My
   Documents\snc\sec\bobjsapproc.pse"
   *** Object <PKList> is of the type <PKList_OID> ***
   1. ------------------------------------------------------------
              Version:                  0 (X.509v1-1988)
              SubjectName:              CN=R21Again, OU=PG, O=BOBJ, C=CA
              IssuerName:               CN=R21Again, OU=PG, O=BOBJ, C=CA
              SerialNumber:             00
              Validity  -  NotBefore:   Wed Nov 28 16:23:53 2007 (071129002353Z)
                                                                  NotAfter:
   Thu Dec 31 16:00:01 2037 (380101000001Z)
              Public Key Fingerprint:   851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
              SubjectKey:               Algorithm RSA (OID
   1.2.840.113549.1.1.1), NULL
   C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>
   ```

   No recibirá más peticiones de PIN de PSE si el comando **seclogin** se ejecuta correctamente.

   > **Nota**
   >
   > Si tiene problemas de acceso con PSE, utilice el comando `-O` para especificar el acceso PSE. Por ejemplo, para permitir acceso PSE a un usuario específico en un dominio específico, en Windows, escriba este comando:
   >
   > ```
   > sapgenpse seclogin -p SBOE.pse -O SYSTEM
   > ```

## 9.5.6.3.5 Para realizar la configuración de SNC de la autenticación SAP

Después de configurar el acceso PSE, debe configurar la autenticación SAP en la CMC.

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en el vínculo *SAP*.

Aparece la configuración de los sistemas de derechos.

3. Haga clic en la ficha *Configuración de SNC* en la página *Autenticación SAP*.
4. Seleccione el sistema de derechos de la lista *Nombre del sistema lógico*.
5. Seleccione *Habilitar comunicación de red segura (SNC)* en *Configuración básica*.
6. Seleccione la opción *Usar predeterminado* para aceptar la ruta predeterminada para la biblioteca o seleccione la opción *Definir ruta personalizada* para seleccionar una ubicación distinta.
7. Seleccione un nivel de protección en *Calidad de protección*.

   Por ejemplo, seleccione *Autenticación*.

   > **Nota**
   >
   > No supere el nivel de protección configurado en el sistema SAP. El nivel de protección es personalizable y está determinado por las necesidades de la organización y las capacidades de su biblioteca SNC.
   >
   > *Calidad de protección* solo hace referencia al procesamiento del lado de la plataforma. Por ejemplo, el visor Web Intelligence dHTML cumple con el nivel especificado. Sin embargo, la comunicación del lado del cliente con SAP Business Warehouse (BW) se debe considerar desprotegida. Por ejemplo, la comunicación del cliente enriquecido de Web Intelligence o la herramienta de diseño de información nunca están cifradas.

8. Introduzca el nombre SNC del sistema SAP en *Configuración de autenticación mutua*.

El formato del nombre SNC depende de la biblioteca SNC. Mediante la utilización de la biblioteca de criptografía SAP, la recomendación para el nombre completo es que éste siga las convenciones de nombres LDAP y que tenga `p:` como prefijo.

9. Confirme que el nombre SNC de las credenciales con las que se ejecutan los servidores de la plataforma de BI aparezca en el cuadro *Nombre SNC del sistema Enterprise*.

   Cuando se configuran varios nombres SNC, este campo se debe dejar en blanco.

10. Proporcione el DNS del sistema SAP y del PSE de la plataforma de BI.

## 9.5.6.3.6 Usar grupos de servidores

A menos que los servidores de procesamiento (Crystal Reports o Web Intelligence) se estén ejecutando con credenciales que tengan acceso al entorno de servidores de procesamiento, debe crear un grupo de servidores específico que sólo contenga estos servidores junto con los servidores compatibles necesarios. Para obtener más información y descripciones de los diferentes servidores de la Plataforma de BI, consulte el capítulo «Arquitectura».

Se puede seleccionar tres opciones al configurar los servidores de procesamiento de contenido para el contenido de SAP:

1. Mantenga un único SIA, que incluya todos los servidores de la Plataforma de BI, que se ejecute con credenciales que tengan acceso al PSE. Esta es la opción más sencilla, ya que no deben crearse grupos de servidores. Se trata del método menos seguro, ya que un gran número de servidores que no son necesarios tienen acceso al entorno de servidores de procesamiento.
2. Cree otro SIA con acceso al entorno de servidores de procesamiento y agréguelo a los servidores de procesamiento de Crystal Reports o Web Intelligence. Elimine los servidores duplicados del SIA original. No es necesario crear grupos de servidores, pero tienen acceso al entorno de servidores de procesamiento menos servidores.
3. Cree un SIA exclusivamente para SAP, con acceso al entorno de servidores de procesamiento. Agréguele los servidores de procesamiento de Crystal Reports o de Web Intelligence. Con esta opción, en estos servidores solo debe ejecutarse contenido SAP, y lo que es más importante, el contenido SAP solo debe ejecutarse en estos servidores. Dado que en esta situación el contenido debe enviarse a determinados servidores, debe crear un grupo de servidores para SIA.

### Directrices para utilizar un grupo de servidores

El grupo de servidores debe hacer referencia al SIA que se utiliza exclusivamente para gestionar contenido SAP. Además, el grupo de servidores debe hacer referencia a los siguientes servidores:

- Servidores adaptables
- Servidores de tareas de Adaptive

Todo el contenido de SAP, documentos de Web Intelligence y Crystal Reports deben asociarse con el grupo de servidores usando la asociación más estricta posible, es decir, deben ejecutarse en servidores del grupo. Cuando dicha asociación se haya realizado en un nivel de objeto, la configuración del grupo de servidores debe propagarse en configuraciones para programaciones directas y publicaciones.

Para impedir que se procese otro tipo de contenido, que no sea contenido SAP, en los servidores de procesamiento específicos de SAP, debe crear otro grupo de servidores que incluya todos los servidores que

haya en el SIA original. Se recomienda que configure una asociación estricta entre este contenido y el grupo de servidores que no sea de SAP.

## 9.5.6.4 Configurar publicaciones de paso múltiple

### Publicaciones de varios pasos de resolución de problemas

Si experimenta problemas con las publicaciones de varios pasos, habilite el rastreo para los controladores de Crystal Reports o Acceso a datos multidimensionales (MDA) para SAP y busque en la cadena de inicio de sesión utilizada las tareas o los destinatarios. Estas cadenas de conexión deberían ser similares a esta:

```
 SAP: Successfully logged on to SAP server.
Logon handle: 1. Logon string: CLIENT=800 LANG=en
ASHOST="vanrdw2k107.sap.crystald.net" SYSNR=00 SNC_MODE=1 SNC_QOP=1
SNC_LIB="C:\WINDOWS\System32\sapcrypto.dll"
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3
EXTIDTYPE=UN
```

La cadena de conexión debe tener el **EXTIDTYPE=UN** (para nombre de usuario) apropiado y **EXTIDDATA** debería ser el nombre de usuario de SAP del destinatario. En este ejemplo, el intento de conexión se ha realizado correctamente.

## 9.5.6.5 Flujo de trabajo para integrar la comunicación de red segura

La plataforma de BI admite entornos que implementan la comunicación de red segura (SNC) para la autenticación y para el cifrado de datos entre componentes SAP. Si ha desplegado la biblioteca cifrada de SAP (u otro producto de seguridad externo que utilice la interfaz SNC) debe configurar algunos valores adicionales para integrar la plataforma de BI de forma eficaz en su entorno seguro.

Para configurar la plataforma de modo que use la comunicación de red segura, debe llevar a cabo las tareas siguientes:

1. Configure los servidores de la plataforma de BI para que se inicien y se ejecuten con una cuenta de usuario adecuada.
2. Configure el sistema SAP de modo que confíe en el sistema de la plataforma de BI.
3. Configure los ajustes SNC en el vínculo de SNC de la Consola de administración central.
4. Importe funciones y usuarios SAP en la plataforma de BI.

### Información relacionada

Importación de funciones de SAP [página 346]

## 9.5.6.6 Configurar los ajustes de SNC en la Consola de administración central

Antes de poder configurar los ajustes de SNC, debe agregar un nuevo sistema de derechos a la plataforma de BI, asegurarse de que el archivo de biblioteca SNC es un directorio conocido y crear una variable de entorno `<RFC_LIB>` que indique al archivo.

1. Haga clic en la ficha *Configuración de SNC* en la página *Autenticación SAP*.
2. Seleccione el sistema de derechos de la lista *Nombre del sistema lógico*.
3. Seleccione *Habilitar comunicación de red segura (SNC)* en *Configuración básica*.
4. Si está configurando la autenticación SAP para el consumo de configuraciones de universos u OLAP BICS `.unx` y tiene intención de usar STS, seleccione la casilla de verificación *Prevenir conexiones entrantes RFC no seguras*.
5. Seleccione la opción *Usar predeterminado* para aceptar la ruta predeterminada para la biblioteca o seleccione la opción *Definir ruta personalizada* para seleccionar una ubicación distinta.

   El servidor de aplicaciones web y el CMS deben estar en el mismo tipo de sistema operativo con la misma ruta a la biblioteca criptográfica.
6. Seleccione un nivel de protección en *Calidad de protección*.

   Por ejemplo, seleccione *Autenticación*.

   > **Nota**
   >
   > El nivel de protección es personalizable y está determinado por las necesidades de la organización y las capacidades de su biblioteca SNC.
7. Introduzca el nombre SNC del sistema SAP en *Configuración de autenticación mutua*.

   El formato del nombre SNC depende de la biblioteca SNC. Mediante la utilización de la biblioteca de criptografía SAP, la recomendación para el nombre completo es que éste siga las convenciones de nombres LDAP y que `p:` sea su prefijo.
8. Confirme que el nombre SNC de las credenciales con las que se ejecutan los servidores de la plataforma de BI aparezca en el cuadro *Nombre SNC del sistema Enterprise*.
9. Haga clic en *Actualizar.*

### Información relacionada

Conectar a sistemas de derechos de SAP [página 340]

## 9.5.6.7 Para asociar el usuario con derechos a un nombre SNC

1. Conéctese al sistema SAP BW y ejecute la transacción `SU01`.

   Se abre la pantalla inicial de mantenimiento de usuarios.

2. En el campo *Usuario*, escriba el nombre de la cuenta SAP designada como usuario con derechos y, a continuación, haga clic en *Cambiar* de la barra de herramientas.

   Se abre la pantalla Mantain User (Mantenimiento de usuario).
3. Haga clic en la ficha SNC.
4. En el campo *SNC Name* (Nombre SNC), escriba la `CUENTA DE USUARIO SNC` que introdujo en el paso 2.
5. Haga clic en *Guardar*.

### 9.5.6.8 Para agregar un id. de sistema a la lista de control de acceso de SNC

1. Conéctese al sistema SAP BW y ejecute la transacción `SNC0`.

   Aparece la pantalla de información general de cambio de vista de la lista de control de acceso para sistemas.
2. Haga clic en *Nuevas entradas* de la barra de herramientas.

   Se abre la pantalla de detalles de las entradas agregadas, en el apartado de nuevas entradas.
3. Escriba el nombre del equipo de la Plataforma de BI en el campo *ID del sistema*.
4. Escriba `p:<NOMBRE DE USUARIO SNC>` en el campo *Nombre de usuario SNC*, donde `NOMBRE DE USUARIO SNC` representa la cuenta que se usó al configurar los servidores de la plataforma de BI.

   > **Nota**
   >
   > Si su proveedor SNC es gssapi32.dll, utilice mayúsculas para indicar el NOMBRE DE USUARIO SNC. Debe incluir el nombre de dominio cuando especifique la cuenta de usuario. Por ejemplo: dominio\nombre_de_usuario.
5. Seleccione *Entry for RFC activated* (Entrada para RFC activada) y *Entry for ext. ID activated* (Entrada para id. ext. activada).
6. Desactive todas las demás opciones y haga clic en *Save* (Guardar).

## 9.5.7 Configuración del inicio de sesión único en el sistema de SAP

Varios servicios back end y de cliente de la plataforma de BI interactúan con los sistemas backend SAP NetWeaver ABAP en un entorno integrado. Resulta de utilidad configurar un inicio de sesión único desde la plataforma de BI a estos sistemas backend (a menudo de BW). Después de configurar un sistema ABAP como sistema de autenticación externo, los token SAP propios se usan para proporcionar un mecanismo que habilite el inicio de sesión único para todos los servicios y clientes de la plataforma de BI que se conectan a los sistemas SAP NetWeaver ABAP.

Para obtener más información, consulte nota de soporte 1670073.

Para habilitar el inicio de sesión único en el sistema de SAP, debe crear un archivo de `almacén de claves` y un certificado correspondiente. Use la línea de comandos de la `herramienta clave` para generar el archivo y

el certificado. De forma predeterminada, el programa de herramienta clave se instala en el directorio `sdk/bin` para cada plataforma.

Se debe agregar el certificado al sistema SAP ABAP BW y a la plataforma de BI mediante la CMC.

> **Nota**
>
> El complemento de autenticación SAP se debe configurar antes de establecer el inicio de sesión único en la base de datos que SAP BW usa.

### 9.5.7.1 Generar el archivo de almacén de claves

El tema contiene instrucciones para utilizar Keytool de Java para generar archivos keystore. La tabla a continuación enumera las ubicaciones por defecto del Keytool de Java:

| Plataforma | Ubicación predeterminada |
|---|---|
| Windows | `<DIRINSTALACIÓN>/SAP BusinessObjects Enterprise XI 4.0/win64_x64/sapjvm/bin` |
| Linux | `sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool` |

1. Navegue a la ubicación por defecto de Keytool de Java e inicie Petición de comandos.
2. Ejecute el Keytool de Java para generar keystore.
   a. Navegue a <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin.
   b. Ejecute el comando:
      - Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`
      - Linux: `*/sap_bobj/enterprise_xi40/java/lib>/sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`

> **→ Sugerencias**
>
> Para sobrescribir los valores predeterminados, ejecute la herramienta junto con el parámetro -?. Aparece el siguiente mensaje:

> **{·} Código de ejemplo**

```
Usage: keytool -genkey <options>
        -keystore <filename(keystore.p12)>
        -alias <key entry alias(mywin)>
        -storepass <keystore password (admin1)>
        -dname <certificate subject DN(CN=palmtree)>
        -validity <number of days (365)>
        -cert <filename (cert.der)>
         (No certificate is generated when importing a keystore)
        -importkeystore <filename>
```

Puede usar los parámetros para sobrescribir los valores predeterminados.

> **Nota**
>
> Debe utilizar Keytool de Java en sustitución de la herramienta PKCS12 para generar keystore. Consulte 2524775 para obtener más información.

### 9.5.7.2 Exportar el certificado de clave pública

Debe crear y exportar un certificado para el archivo de almacén de claves.

1. Desencadene un símbolo de sistema y desplácese al directorio en el que está ubicado el programa de la herramienta clave
2. Para exportar un certificado clave para el archivo de almacén de claves use el siguiente comando:

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
-alias <alias>
```

| |
|---|
| Sustituya <keystore> con el nombre del archivo de almacén de claves. |
| Sustituya <filename> con el nombre del certificado. |
| Sustituya <alias> con el alias usado para crear el archivo de almacén de claves. |

3. Cuando se lo solicite, introduzca la contraseña que proporcionó para el archivo de almacén de claves.

Ahora tiene un archivo de almacén de claves y un certificado en el directorio en el que está ubicado el programa de la herramienta clave.

### 9.5.7.3 Importar el archivo de certificados en el sistema ABAP SAP de destino

Necesita un archivo de almacén de claves y un certificado asociado para el despliegue de la Plataforma de BI para realizar la siguiente tarea.

> **Nota**
>
> Esta acción sólo se puede realizar en un sistema ABAP SAP.

1. Conéctese al sistema SAP ABAP BW con la GUI de SAP.

   > **Nota**
   >
   > Se debe conectar como usuario con privilegios administrativos.

2. Ejecute STRUSTSSO2 en la GUI de SAP.
   El sistema está preparado para importar el archivo de certificados.

3. Vaya a la ficha *Certificado*.
4. Asegúrese de que la casilla de verificación *Usar opción binaria* está seleccionada.
5. Haga clic en el botón de ruta del archivo para dirigirse a la ubicación en la que está ubicado en archivo de certificados.
6. Haga clic en la marca de verificación verde.
   El archivo de certificados está cargado.
7. Haga clic en *Agregar a la lista de certificados*.
   El certificado se muestra en la lista de certificados.
8. Haga clic en *Agregar a ACL* y especifique un ID de sistema y cliente.

   El ID del sistema debe ser el mismo que se usa para identificar el sistema de la Plataforma de BI en SAP BW.

   El certificado se agrega a la lista de control de acceso (ACL). El cliente se debe especificar como «000».
9. Guarde la configuración y salga.
   Los cambios se guardan en el sistema de SAP.

## 9.5.7.4 Configurar el inicio de sesión único en la base de datos de SAP en la CMC

Para realizar el siguiente procedimiento debe acceder al complemento de seguridad SAP con una cuenta de administrador.

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en el vínculo *SAP* y, a continuación, haga clic en la ficha *Opciones*.

   Si no se ha importado un certificado, se mostrará el siguiente mensaje en la sección *Servicio SSO de SAP*:

   `No se ha cargado ningún archivo de almacén de claves`
3. Especifique el ID del sistema para el sistema de la plataforma de BI en el campo proporcionado.

   Este debe ser idéntico al valor usado al importar el certificado en el sistema SAP ABAP de destino.
4. Haga clic en el botón *Examinar* para dirigirse al archivo de almacén de claves.

5. Proporcione los siguientes detalles necesarios:

| Campo | Información necesaria |
|---|---|
| *Contraseña del almacén de claves* | Proporcione la contraseña necesaria para acceder al archivo de almacén de claves. Esta contraseña se especificó al crear el archivo de almacén de claves. |
| *Contraseña de clave privada* | Proporciona la contraseña necesaria para acceder al certificado correspondiente al archivo de almacén de claves. Esta contraseña se especificó al crear el certificado para el archivo de almacén de claves. |
| *Alias de clave privada* | Proporciona el alias necesario para acceder al archivo de almacén de claves. Este alias se especificó al crear el archivo de almacén de claves. |

6. Haga clic en *Actualizar* para enviar la configuración.
   Una vez enviada la configuración correctamente, se mostrará el siguiente mensaje en el campo ID de sistema:

   ```
   Se ha cargado el archivo de almacén de claves
   ```

### 9.5.7.5 Agregar el Servicio de identificadores de seguridad al servidor de procesamiento de Adaptive

En un entorno en clúster, los servicios de token de seguridad se agregan independientemente de cada servidor de procesamiento de Adaptive.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en *Servicios principales*.
   Aparece una lista de servidores en *Servicios principales*.
3. Haga clic con el botón derecho en el servidor de procesamiento de Adaptive y seleccione *Detener el servidor*.

   No siga hasta que el estado del servidor sea Detenido.
4. Haga clic con el botón derecho en el servidor de procesamiento de Adaptive y seleccione *Seleccionar servicios*.
   Aparecerá el cuadro de diálogo *Seleccionar servicios*.
5. Utilice el botón *Agregar* para mover el servicio de token de seguridad desde la lista *Servicios disponibles* a la lista *Servicios*.
6. Haga clic en *Aceptar*.
7. Reinicie el Servidor de procesamiento de Adaptive.

## 9.5.8 Configurar el SSO para SAP Crystal Reports y SAP Netweaver

De forma predeterminada, la plataforma de BI se configurará para permitir que los usuarios de SAP Crystal Reports accedan a los datos de SAP mediante el inicio de sesión único (SSO).

### 9.5.8.1 Desactivar el SSO para SAP Netweaver y SAP Crystal Reports

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. Seleccione uno de los siguientes controladores:

| Controlador | Nombre visualizado |
|---|---|
| Controlador de Operational Data Store | *crdb_ods* |
| Controlador de Open SQL | *crdb_opensql* |
| Controlador de InfoSet | *crdb_infoset* |
| Controlador de BW MDX Query | *crdb_bwmdx* |

5. Haga clic en *Eliminar*.
6. Haga clic en *Guardar y cerrar*.
7. Reinicie SAP Crystal Reports.

### 9.5.8.2 Volver a activar el SSO para SAP Netweaver y SAP Crystal Reports

Siga los siguientes pasos para volver a activar el SSO para SAP Netweaver (ABAP) y SAP Crystal Reports.

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. En *Usar contexto de SSO para conexión de base de datos* escriba:

| | |
|---|---|
| `crdb_ods` | Activar el controlador ODS |
| `crdb_opensql` | Activar el controlador Open SQL |
| `crdb_bwmdx` | Activar el controlador SAP BW MDX Query |
| `crdb_infoset` | Activar el controlador InfoSet |

5. Haga clic en *Agregar*.
6. Haga clic en *Guardar y cerrar*.
7. Reinicie SAP Crystal Reports.

## 9.6 Autenticación de PeopleSoft

### 9.6.1 Información general

Para usar los datos de PeopleSoft Enterprise con la Plataforma de BI, debe proporcionar el programa con la información del despliegue. Esta información permite que la Plataforma de BI autentique usuarios para que puedan usar las credenciales de PeopleSoft para iniciar sesión en el programa.

### 9.6.2 Habilitar la autenticación de PeopleSoft Enterprise

Para permitir que la Plataforma de BI use la información de PeopleSoft Enterprise, la Plataforma de BI necesita la información sobre cómo autenticarse en el sistema de PeopleSoft Enterprise.

#### 9.6.2.1 Habilitar la autenticación de PeopleSoft Enterprise en la plataforma de BI

1. Inicie una sesión en la Consola de administración central como administrador.
2. En el área Administrar, haga clic en *Autenticación*.
3. Haga doble clic en *PeopleSoft Enterprise*.
   Aparece la página de *PeopleSoft Enterprise*. Contiene cuatro fichas: *Opciones*, *Dominios*, *Funciones* y *Actualización de usuario*.
4. En la ficha *Opciones*, seleccione la casilla de verificación *Habilitar autenticación de PeopleSoft Enterprise*.
5. Realice los cambios necesarios en *Nuevo alias*, *Opciones de actualización* y *Opciones de usuarios nuevos* según su despliegue de la plataforma de BI.

   Haga clic en *Actualizar* para guardar los cambios antes de pasar a la ficha *Dominios*.
6. Haga clic en la ficha *Dominios*.
7. En el área *Usuario del sistema de PeopleSoft Enterprise*, escriba un nombre de usuario y contraseña para la base de datos para que la Plataforma de BI inicie sesión en la base de datos de PeopleSoft Enterprise.
8. En el área *Dominios de PeopleSoft Enterprise*, introduzca el nombre del dominio y la dirección QAS que se usa para conectarse al entorno de PeopleSoft Enterprise, y haga clic en *Agregar*.

   > **Nota**
   >
   > Si tiene varios dominios de PeopleSoft, repita este paso para cualquier dominio adicional al que desee tener acceso. El primer dominio que introduzca será el dominio predeterminado.
9. Haga clic en *Actualizar* para guardar los cambios.

## 9.6.3 Asignar funciones de PeopleSoft a la plataforma de BI

La Plataforma de BI crea automáticamente un grupo para cada función de PeopleSoft que asigne. A su vez, el programa crea alias para representar a los miembros de las funciones de PeopleSoft asignadas.

Puede crear una cuenta de usuario para cada alias generado.

Sin embargo, si se ejecutan varios sistemas y los usuarios tienen cuentas en varios de ellos, se puede asignar a cada usuario un alias con el mismo nombre antes de crear las cuentas en la Plataforma de BI.

De este modo se reduce el número de cuentas que se crean para el mismo usuario en la Plataforma de BI.

Por ejemplo, si ejecuta PeopleSoft HR 8.3 y PeopleSoft Financials 8.4, y 30 de sus usuarios tienen acceso a ambos sistemas, sólo se crearán 30 cuentas para dichos usuarios. Si decide no asignar a cada usuario un alias con el mismo nombre, se crearán 60 cuentas para los 30 usuarios en la Plataforma de BI.

Sin embargo, si ejecuta varios sistemas, y se repiten los nombres de usuario, deberá crear una nueva cuenta de miembro para cada alias creado.

Por ejemplo, si ejecuta PeopleSoft HR 8.3 con una cuenta de usuario de Russell Aquino (nombre de usuario "raquino"), y ejecuta PeopleSoft Financials 8.4 con una cuenta de usuario de Raúl Aquino (nombre de usuario "raquino"), deberá crear una cuenta independiente para cada alias de usuario. En caso contrario, los dos usuarios se agregan a la misma cuenta de la plataforma de BI; podrán iniciar sesión en la plataforma de BI con sus propias credenciales de PeopleSoft y tendrán acceso a los datos de ambos sistemas de PeopleSoft.

### 9.6.3.1 Asignar una función de PeopleSoft a la plataforma de BI

Si la plataforma de BI JVM (máquina virtual Java) no tiene un certificado al servidor PeopleSoft, tendrá que llevar a cabo estos pasos adicionales antes de llevar a cabo los siguientes pasos principales:

1. Obtenga el archivo .cer del servidor PeopleSoft.
2. Copie el archivo .cer en `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
3. Ejecute el siguiente comando desde el directorio de seguridad: `"<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file <peoplesoftserver>.cer -keystore cacerts -alias <peoplesoftserver>`.
4. Reinicie el servidor de aplicaciones Web.

Pasos principales:

1. Inicie una sesión como administrador en la Consola de administración central.
2. Haga clic en *Autenticación*.
3. Haga doble clic en *PeopleSoft Enterprise*.
4. En la ficha *Funciones*, en el área Dominios de PeopleSoft Enterprise, seleccione el dominio asociado a la función que desea asignar a la Plataforma de BI.
5. Use una de las opciones siguientes para seleccionar las funciones que desea asignar:
   - En el área *Funciones de PeopleSoft Enterprise*, en el cuadro Buscar funciones, introduzca la función que desee buscar y asignar a la Plataforma de BI y haga clic en > >.

- En la lista *Funciones disponibles* seleccione la función que desee asignar a la plataforma de BI y haga clic en >.

> **Nota**
>
> Al buscar un determinado usuario o función, puede utilizar el comodín %. Por ejemplo, para buscar todas las funciones que comience por "A", escriba *A%*. La función de búsqueda también distingue entre mayúsculas y minúsculas.

> **Nota**
>
> Si desea asignar una función de otro dominio, debe seleccionar el nuevo dominio en la lista de dominios disponibles que coincida con una función de otro dominio.

6. Vaya a la ficha *Actualización de usuario* y haga clic en el botón *Actualizar*, o planifique las actualizaciones.
7. En la ficha *Opciones*, vaya al área *Opciones de usuarios nuevos* y seleccione una de las opciones siguientes:
   - *Asignar cada alias agregado a una cuenta con el mismo nombre*
     Seleccione esta opción si ejecuta varios sistemas PeopleSoft Enterprise con usuarios que tienen cuentas en más de un sistema (y dos usuarios no tienen el mismo nombre de usuario para sistemas diferentes).
   - *Crear una cuenta nueva para cada alias agregado*
     Seleccione esta opción si solo se ejecuta un sistema PeopleSoft Enterprise, si la mayoría de los usuarios tienen cuentas en un único sistema, o si los nombres de usuario se solapan en el caso de distintos usuarios en dos o más de sus sistemas.
8. En el área *Opciones de actualización del alias*, seleccione una de las siguientes opciones:
   - *Crear nuevos alias cuando se actualice el alias*
     Seleccione esta opción para crear un nuevo alias para cada usuario que se asigne a la Plataforma de BI. Se agregan nuevas cuentas para los usuarios sin cuentas de la Plataforma de BI o para todos los usuarios si selecciona la opción Crear una cuenta nueva para cada alias agregado.
   - *Crear nuevos alias solo cuando el usuario inicie sesión*
     Seleccione esta opción si la función que desea asignar contiene varios usuarios, pero solo unos cuantos de ellos usan la Plataforma de BI. La plataforma no crea automáticamente alias ni cuentas para los usuarios. En su lugar, crea alias (y cuentas, en caso necesario) solo para los usuarios al iniciar sesión en la Plataforma de BI por primera vez. Esta es la opción predeterminada.
9. En el área *Opciones de usuarios nuevos*, especifique el modo en que se crean los usuarios.

   Seleccione una de las siguientes opciones:

   - *Los usuarios nuevos se crean como usuarios con nombre*
     Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios con nombre. Las licencias de usuario con nombre se asocian con usuarios específicos y permiten que tengan acceso al sistema basándose en sus nombres de usuario y en sus contraseñas. De esta forma, los usuarios con nombre pueden tener acceso al sistema independientemente del número de personas conectadas. Debe tener una licencia de usuario con nombre disponible por cada cuenta de usuario creada mediante esta opción.

     > **Nota**
     >
     > El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.

> Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

- *Los usuarios nuevos se crean como usuarios simultáneos*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios simultáneos. Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque una licencia simultánea pequeña puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios a la Plataforma de BI, una licencia simultánea de 100 usuarios puede admitir 250, 500 ó 700 usuarios.

Las funciones que seleccione ahora aparecerán como grupos en la Plataforma de BI.

## 9.6.3.2 Aspectos a tener en cuenta en la reasignación

Si se agregan usuarios a una función que ya se ha asignado a la Plataforma de BI, tendrá que volver a asignar la función para agregar usuarios a la Plataforma de BI. Al reasignar la función, la posibilidad de asignar usuarios como usuarios con nombre o simultáneos solo afecta a los nuevos usuarios agregados a la función.

Por ejemplo, primero se asigna una función a la Plataforma de BI con la opción "Se crean nuevos usuarios como usuarios *con nombre*" seleccionada. A continuación, se agregan usuarios a la misma función y ésta se reasigna con la opción "Se crean nuevos usuarios como *simultáneos*" seleccionada.

En esta situación, solo los nuevos usuarios de la función se asignan a la Plataforma de BI como usuarios simultáneos; los usuarios que ya estaban asignados permanecen como usuarios con nombre. La misma condición se aplica si primero se asignan usuarios como usuarios simultáneos y, a continuación, se cambia la configuración para reasignar nuevos usuarios como usuarios con nombre.

## 9.6.3.3 Para desasignar una función

1. Inicie sesión como administrador a la Consola de administración central.
2. Haga clic en *Autenticación*.
3. Haga clic en *PeopleSoft Enterprise*.
4. Haga clic en *Funciones*.
5. Seleccione la función que desea eliminar y haga clic en <.
6. Haga clic en *Actualizar*.

   Los miembros de la función ya no podrán acceder a la Plataforma de BI, a menos que tengan otras cuentas o alias.

   > ⓘ Nota
   >
   > También puede eliminar cuentas individuales o eliminar usuarios de las funciones antes de asignarlas a la Plataforma de BI para evitar que usuarios específicos inicien sesión.

## 9.6.4 Programación de actualizaciones de usuario

Para garantizar que los cambios realizados en los datos del usuario para el sistema ERP se reflejan en los datos de usuario de la plataforma de BI, puede programar actualizaciones de usuario a intervalos regulares. Estas actualizaciones sincronizarán automáticamente los usuarios del sistema ERP con los de la plataforma de BI según la configuración de asignación que se haya configurado en la Consola de administración central (CMC).

Existen dos opciones para ejecutar y programar actualizaciones para las funciones importadas:

- Solo actualizar funciones: con esta opción solo se actualizarán los vínculos entre las funciones actualmente asignadas que se han importado en la plataforma de BI. Use esta opción si espera ejecutar actualizaciones frecuentes y le preocupa el uso de los recursos del sistema. No se crearán cuentas de usuario si solo actualiza las funciones.
- Actualizar funciones y alias: esta opción además de actualizar los vínculos entre las funciones, creará cuentas de usuario nuevas en la plataforma de BI para los nuevos alias de usuario agregados al sistema ERP.

> ⓘ Nota
>
> Si, cuando ha activado la autenticación, no ha especificado crear automáticamente alias para las actualizaciones, no se crearán cuentas para los nuevos alias.

### 9.6.4.1 Programar actualizaciones de usuario

Después de asignar las funciones a la plataforma de BI debe especificar el modo en que el sistema actualiza estas funciones.

1. Haga clic en la ficha *Actualización de usuario*.
2. Haga clic en *Programar* en las secciones *Sólo actualizar funciones* o *Actualizar funciones y alias*.

   > → Sugerencias
   >
   > Si desea ejecutar una actualización inmediatamente, haga clic en *Actualizar ahora*.

   > → Sugerencias
   >
   > Use la opción *Sólo actualizar funciones* si desea realizar actualizaciones frecuentes y le preocupa el uso de los recursos del sistema. La actualización de funciones y alias tarda más en realizarse.

   Aparece el cuadro de diálogo *Periodicidad*.
3. Seleccione una opción de la lista *Ejecutar objeto* y proporcione la información de programación que se le solicite.

   Cuando programa una actualización, puede elegir entre los patrones de repetición que se resumen en la siguiente tabla:

| Patrón de periodicidad | Descripción |
|---|---|
| Cada hora | La actualización se ejecutará cada hora. Se debe especificar a qué hora comenzará así como las fechas de inicio y fin. |
| Cada día | La actualización se ejecutará cada día o se ejecutará el número de días especificado. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Cada semana | La actualización se ejecutará cada semana. Se puede ejecutar una o varias veces a la semana. Puede especificar en qué días y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Mensual | La actualización se ejecutará cada mes o cada varios meses. Puede indicar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día N de cada mes | La actualización se ejecutará un día específico del mes. Puede especificar en qué día del mes y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Primer lunes del mes | La actualización se ejecutará el primer lunes de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Último día de cada mes | La actualización se ejecutará el último día de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día X de la semana N de cada mes | La actualización se ejecutará un día especificado de una semana especificada del mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Calendario | La actualización se ejecutará en las fechas especificadas en un calendario que se haya creado previamente. |

4. Haga clic en *Programar* una vez que haya proporcionado toda la información de planificación.
   La fecha de la siguiente actualización de función programada se muestra en la ficha *Actualización de usuario*.

   > **Nota**
   >
   > Si lo desea puede cancelar la siguiente actualización programada haciendo clic en *Cancelar actualizaciones programadas* en las secciones *Sólo actualizar funciones* o *Actualizar funciones y alias*.

## 9.6.5 Uso del puente de seguridad de PeopleSoft

La función del puente de seguridad de la plataforma de BI permite importar la configuración de seguridad de PeopleSoft EPM a la plataforma de BI.

El Puente de seguridad funciona en dos modos:

- **Modo de configuración**
  En el modo de configuración, el Puente de seguridad proporciona una interfaz que permite crea un archivo de respuesta. Este archivo controla el comportamiento del Puente de seguridad durante el modo de ejecución.
- **Modo de ejecución**
  Según los parámetros definidos en el archivo de respuesta, el puente de seguridad importa la configuración de seguridad de las tablas de dimensiones en PeopleSoft EPM a los universos de la plataforma de BI.

## 9.6.5.1 Importación de la configuración de seguridad

Para importar la configuración de seguridad, debe efectuar las siguientes tareas en este orden:

- Definir los objetos que administrará el Puente de seguridad.
- Crear un archivo de respuesta.
- Ejecutar la aplicación Puente de seguridad.

Para obtener información sobre la administración de la seguridad tras importar la configuración, consulte Administración de la configuración de seguridad [página 378].

### 9.6.5.1.1 Definición de objetos administrados

Antes de ejecutar el Puente de seguridad, es importante determinar los objetos que administrará la aplicación. El puente de seguridad administra una o varias funciones de PeopleSoft, un grupo de la plataforma de BI y uno o varios universos.

- Funciones de PeopleSoft administradas
  Se trata de funciones en el sistema PeopleSoft. Los miembros de estas funciones trabajan con datos de PeopleSoft a través de PeopleSoft EPM. Debe elegir las funciones que incluyen los miembros a los que desee conceder/actualizar privilegios de acceso a los universos administrados en la plataforma de BI.
  Los derechos de acceso definidos para los miembros de estas funciones se basan en sus derechos en PeopleSoft EPM; el puente de seguridad importa esta configuración de seguridad a la plataforma de BI.
- Grupo administrado de la plataforma de BI
  Al ejecutar el puente de seguridad, el programa crea un usuario en la plataforma de BI para cada miembro de una función administrada de PeopleSoft.
  El grupo en el que se crean los usuarios es el grupo administrado de la plataforma de BI. Los miembros de este grupo son los usuarios cuyos derechos de acceso a los universos administrados se mantienen a través del Puente de seguridad. Como los usuarios se crean en un grupo, se puede configurar el puente de seguridad para que no actualice la configuración de seguridad de ciertos usuarios; solo tiene que eliminar los usuarios del grupo administrado de la plataforma de BI.
  Antes de ejecutar el puente de seguridad, debe seleccionar un grupo en la plataforma de BI para que sea la ubicación en la que se crearán los usuarios. Si especifica un grupo que no existe, el puente de seguridad creará el grupo en la plataforma de BI.
- Universos administrados
  Los universos administrados son los universos en los que el Puente de seguridad importa la configuración de seguridad desde PeopleSoft EPM. Desde los universos almacenados en el sistema de la plataforma de BI, debe elegir cuáles se administrarán a través del puente de seguridad. Los miembros de las funciones administradas de PeopleSoft que también sean miembros del grupo administrado de la plataforma de BI no pueden acceder a ningún dato a través de aquellos universos a los que no puedan acceder desde PeopleSoft EPM.

### 9.6.5.1.2 Para crear un archivo de respuesta

1. Vaya a la carpeta especificada durante la instalación del Puente de seguridad y ejecute el archivo `crpsepmsecuritybridge.bat` (en Windows) y `crpsepmsecuritybridge.sh` (en Unix).

> **Nota**
>
> La ubicación predeterminada en Windows es `C:\Archivos de programa\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm`.

Aparecerá el cuadro de diálogo Puente de seguridad para PeopleSoft EPM.

2. Seleccione *Nuevo* para crear un archivo de respuesta o bien seleccione *Abrir* y haga clic en *Examinar* para especificar un archivo de respuesta que desee modificar. Seleccione el idioma que desea para el archivo.
3. Haga clic en *Siguiente*.
4. Introduzca las ubicaciones del *SDK de PeopleSoft EPM* y el *SDK de la Plataforma de BI*.

> **Nota**
>
> El SDK de PeopleSoft EPM suele estar situado en el servidor PeopleSoft, en `<PS_HOME>/class/com.peoplesoft.epm.pf.jar`.

> **Nota**
>
> Normalmente, el SDK de la plataforma de BI está ubicado en `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`.

5. Haga clic en *Siguiente*.

   El cuadro de diálogo le pedirá la información de conexión y controlador de la base de datos de PeopleSoft.
6. Desde la lista de bases de datos, seleccione el tipo de base de datos apropiado e introduzca la información correspondiente en los siguientes campos:

| Campo | Descripción |
|---|---|
| Base de datos | Nombre de la base de datos de PeopleSoft. |
| Host | Nombre del servidor que almacena la base de datos. |
| Número de puerto | Número de puerto de acceso al servidor. |
| Ubicación de la clase | Ubicación de los archivos de clases para el controlador de la base de datos. |
| Nombre del usuario | Su nombre de usuario. |
| Contraseña | Su contraseña. |

7. Haga clic en *Siguiente*.

   El cuadro de diálogo muestra una lista de todas las clases que el Puente de seguridad utilizará al ejecutarse. En caso necesario, puede agregar o eliminar clases de la lista.
8. Haga clic en *Siguiente*.

   El cuadro de diálogo le solicitará la información de conexión para la plataforma de BI.
9. Proporcione la información adecuada en los siguientes campos:

| Campo | Descripción |
| --- | --- |
| Servidor | El nombre del servidor donde se encuentra el Servidor de administración central (CMS). |
| Nombre del usuario | Su nombre de usuario. |
| Contraseña | Su contraseña. |
| Autenticación | Su tipo de autenticación. |

10. Haga clic en *Siguiente*.
11. Seleccione un grupo de la plataforma de BI y haga clic en *Siguiente*.

> **Nota**
>
> El grupo especificado en este campo es el lugar donde el Puente de seguridad creará los usuarios para los miembros de las funciones de PeopleSoft administradas.

> **Nota**
>
> Si especifica un grupo que aún no existe, el Puente de seguridad lo creará.

El cuadro de diálogo muestra una lista de funciones del sistema PeopleSoft.

12. Seleccione la opción *Importada* junto a las funciones que desee que el Puente de seguridad administre y haga clic en *Siguiente*.

> **Nota**
>
> El puente de seguridad crea un usuario en el grupo administrado de la plataforma de BI (que se especificó en el paso anterior) para cada miembro de las funciones que haya seleccionado.

El cuadro de diálogo muestra una lista de universos de la plataforma de BI.

13. Seleccione los universos cuya configuración de seguridad desee importar a través del Puente de seguridad y haga clic en *Siguiente*.
14. Especifique un nombre para el archivo de registro del Puente de seguridad y la ubicación donde se guardará. Puede utilizar el archivo de registro para determinar si el Puente de seguridad importa correctamente la configuración de seguridad desde PeopleSoft EPM.
15. Haga clic en *Siguiente*.

    El cuadro de diálogo muestra una vista previa del archivo de respuesta que el Puente de seguridad utilizará durante el modo de ejecución.
16. Haga clic en *Guardar* y elija la ubicación donde desee guardar el archivo de respuesta.
17. Haga clic en *Siguiente*.

    Ha creado correctamente el archivo de respuesta para el Puente de seguridad.
18. Haga clic en *Salir*.

> **Nota**
>
> El archivo de respuesta es un archivo de propiedades de Java que también se puede crear y modificar manualmente. Para obtener más detalles, consulte la sección «Archivo de respuesta de PeopleSoft».

## 9.6.5.2 Aplicación de la configuración de seguridad

Para aplicar la configuración de seguridad, ejecute el archivo `crpsepmsecuritybridge.bat` (en Windows) o el archivo `crpsempsecuritybridge.sh` (en Unix) y use el archivo de respuesta creado como argumento. Por ejemplo, introduzca **`crpsepmsecuritybridge.bat myresponsefile.properties`** en Windows, o **`crpsempsecuritybridge.sh myresponsefile.properties`** en Unix.

La aplicación Puente de seguridad se ejecuta. Crea usuarios en la plataforma de BI para los miembros de las funciones de PeopleSoft que se especificaron en el archivo de respuesta e importa la configuración de seguridad desde PeopleSoft EPM a los universos adecuados.

### 9.6.5.2.1 Consideraciones sobre asignaciones

Durante el modo de ejecución, el puente de seguridad crea un usuario en la plataforma de BI para cada miembro de una función administrada de PeopleSoft.

Los usuarios se crean para que solo dispongan de alias de autenticación de Enterprise y la plataforma de BI asigna contraseñas aleatorias a dichos usuarios. Como resultado, los usuarios no pueden iniciar sesión en la plataforma de BI hasta que el administrador vuelva a asignar manualmente nuevas contraseñas o asigne las funciones a la plataforma de BI a través del complemento de seguridad de PeopleSoft para permitir que los usuarios inicien sesión con sus credenciales de PeopleSoft.

## 9.6.5.3 Administración de la configuración de seguridad

Puede administrar la configuración de seguridad aplicada modificando los objetos administrados por el Puente de seguridad.

### 9.6.5.3.1 Usuarios administrados

El Puente de seguridad administra los usuarios de acuerdo con los siguientes criterios:

- Si el usuario es miembro o no de una función de PeopleSoft administrada.
- Si el usuario es miembro o no del grupo administrado de la plataforma de BI.

Si desea que un usuario tenga acceso a los datos de PeopleSoft a través de universos de la plataforma de BI, asegúrese de que el usuario sea miembro *tanto de* una función administrada de PeopleSoft como del grupo administrado de la plataforma de BI.

- Para los miembros de funciones administradas de PeopleSoft que no dispongan de cuentas en la plataforma de BI, el puente de seguridad creará cuentas y les asignará contraseñas aleatorias. El administrador debe decidir si desea volver a asignar manualmente nuevas contraseñas o asignar las funciones a la plataforma de BI través del complemento de seguridad de PeopleSoft para permitir a los usuarios iniciar la sesión en la plataforma de BI.

- Para los miembros de funciones administradas de PeopleSoft que también sean miembros del grupo administrado de la plataforma de BI, el puente de seguridad actualiza la configuración de seguridad que se aplica a los usuarios para que tengan acceso a los datos adecuados de los universos administrados.

Si un miembro de una función administrada de PeopleSoft dispone de una cuenta existente en la *plataforma de BI* pero *no* es miembro del grupo administrado de la plataforma de BI, el puente de seguridad no actualiza la configuración de seguridad que se aplica al usuario. Normalmente, esta situación solo ocurre cuando el administrador elimina manualmente cuentas de usuario que el puente de seguridad ha creado a partir del grupo administrado de la plataforma de BI.

> **ⓘ Nota**
>
> Este método resulta eficaz para administrar la seguridad: al eliminar usuarios del grupo administrado de la plataforma de BI, puede hacer que la configuración de seguridad sea distinta de la configuración de seguridad en PeopleSoft.

Asimismo, si un miembro del grupo administrado de la *plataforma de BI no* es miembro de una función administrada de PeopleSoft, el puente de seguridad no le dará acceso a los universos administrados. Normalmente, esta situación solo ocurre cuando los administradores de PeopleSoft eliminan usuarios que el puente se seguridad había asignado anteriormente a la plataforma de BI desde las funciones administradas de PeopleSoft.

> **ⓘ Nota**
>
> Existe otro método para administrar la seguridad: eliminando usuarios de las funciones de PeopleSoft administradas, puede garantizar que los usuarios no tengan acceso a ningún dato de PeopleSoft.

## 9.6.5.3.2 Universos administrados

El Puente de seguridad administra los universos a través de conjuntos de restricciones, que limitan los datos a los que los usuarios administrados pueden acceder desde los universos administrados.

Los conjuntos de restricciones son grupos de restricciones (por ejemplo, restricciones a los controles de consultas, generación de SQL, etc.). El Puente de seguridad aplica/actualiza las restricciones de acceso a filas y objetos para los universos administrados:

- Aplica restricciones de acceso a filas a las tablas de dimensión definidas en PeopleSoft EPM. Estas restricciones son específicas de usuario y se pueden configurar con uno de los siguientes parámetros:
  - El usuario tiene acceso a todos los datos.
  - El usuario no tiene acceso a ningún dato.
  - El usuario tiene acceso a los datos según sus permisos de fila en PeopleSoft, que se muestran a través de las tablas combinadas de seguridad (SJT) definidas en PeopleSoft EPM.
- Aplica restricciones de acceso a objetos para objetos de tipo indicador de acuerdo con los campos a los que tienen acceso dichos objetos.
  Si un objeto de tipo indicador tiene acceso a campos definidos como métricas en PeopleSoft, entonces el acceso al objeto de tipo indicador se permitirá o denegará dependiendo de si el usuario puede acceder a las métricas referenciadas en PeopleSoft. Si un usuario no puede acceder a ninguna de las métricas, el acceso al objeto indicador se denegará. Si el usuario puede acceder a todas las métricas, se le concederá el acceso al objeto indicador.

Como administrador, también puede limitar los datos a los que los usuarios pueden acceder desde su sistema PeopleSoft limitando el número de universos administrados por el Puente de seguridad.

## 9.6.5.4 Archivo de respuesta de PeopleSoft

La función del puente de seguridad de la plataforma de BI funciona según la configuración especificada en un archivo de respuesta.

Normalmente, genera el archivo de respuesta utilizando la interfaz proporcionada por el Puente de seguridad en modo de configuración. Sin embargo, como el archivo es un archivo de propiedades de Java, también puede crearlo o modificarlo manualmente.

Este apéndice proporciona información sobre los parámetros que necesita incluir en el archivo de respuesta si decide generarlo manualmente.

> **Nota**
>
> Al crear el archivo, debe respetar el requisito de escape para archivos de propiedades Java (por ejemplo, ':' se escapa como '\:').

### 9.6.5.4.1 Parámetros del archivo de respuesta

La tabla siguiente describe los parámetros incluidos en el archivo de respuesta:

| Parámetro | Descripción |
|---|---|
| classpath | Ruta de acceso de clase para cargar los archivos .jar necesarios. Si hay varias rutas de acceso de clase se deben separar con ';' tanto en Windows como en UNIX.<br>Las rutas de acceso de clase necesarias son para los archivos .jar del controlador JDBC y `com.peoplesoft.epm.pf.jar`. |
| db.driver.name | Nombre del controlador JDBC utilizado para conectarse a la base de datos PeopleSoft (por ejemplo, `com.microsoft.jdbc.sqlserver.SQLServerDriver`). |
| db.connect.str | Cadena de conexión de JDBC utilizada para conectarse a la base de datos de PeopleSoft (por ejemplo, `jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO`) |
| db.user.name | Nombre de usuario para iniciar una sesión en la base de datos de PeopleSoft. |

| Parámetro | Descripción |
| --- | --- |
| db.password | Contraseña para iniciar una sesión en la base de datos de PeopleSoft. |
| db.password.encrypted | El valor de este parámetro determina si el parámetro de contraseña en el archivo de respuesta se cifrará o no. El valor se puede establecer como True o False. (Si no se especifica ningún valor, el valor se establece como False de forma predeterminada). |
| enterprise.cms.name | CMS en el que se encuentran los universos. |
| enterprise.user.name | Nombre de usuario para iniciar una sesión en el CMS. |
| enterprise.password | Contraseña para iniciar una sesión en el CMS. |
| enterprise.password.encrypted | El valor de este parámetro determina si el parámetro de contraseña en el archivo de respuesta se cifrará o no. El valor se puede establecer como True o False. (Si no se especifica ningún valor, el valor se establece como False de forma predeterminada). |
| enterprise.authMethod | Método de autenticación para iniciar una sesión en el CMS. |
| enterprise.role | El grupo administrado de la plataforma de BI. Para obtener más información, consulte Definición de objetos administrados [página 375]. |
| enterprise.licencia | Controla el tipo de licencia a la hora de importar usuarios desde PeopleSoft. "0" define la licencia de usuario designado, "1" define la licencia de usuario simultáneo. |
| peoplesoft.rol.n | Lista de funciones de PeopleSoft administradas. Para obtener más información, consulte Definición de objetos administrados [página 375].<br><br>**<n>** es un entero; cada entrada ocupa una propiedad con el prefijo peoplesoft.role.<br><br>**Nota**<br>**<n>** tiene la base 1.<br><br>Puede utilizar '*' para indicar todas las funciones de PeopleSoft disponibles siempre que n sea 1 y sea la única propiedad con peoplesoft.role como prefijo en el archivo de respuesta. |

| Parámetro | Descripción |
| --- | --- |
| mapped.universe.n | Lista de universos que desea que el Puente de seguridad actualice. Para obtener más información, consulte Definición de objetos administrados [página 375].<br><br>**<n>** es un entero; cada entrada ocupa una propiedad con el prefijo mapped.universe.<br><br>**Nota**<br>**<n>** tiene la base 1.<br><br>Puede utilizar '*' para indicar todos los universos disponibles siempre que n sea 1 y sea la única propiedad con mapped.universe como prefijo en el archivo de respuesta. |
| log4j.appender.file.File | Archivo de registro escrito por el Puente de seguridad. |
| log4j.* | Propiedades predeterminadas de log4j necesarias para que log4j funcione correctamente:<br><br>log4j.rootLogger=INFO, file, stdout<br><br>log4j.appender.file=org.apache.log4j.RollingFile Appender<br><br>log4j.appender.file.layout=org.apache.log4j.PatternLayout<br><br>log4j.appender.file.MaxFileSize=5000KB<br><br>log4j.appender.file.MaxBackupIndex=100<br><br>log4j.appender.file.layout.ConversionPattern=%d [ %-5 ] %c{1} - %m%n<br><br>log4j.appender.stdout=org.apache.log4j.ConsoleAppender<br><br>log4j.appender.stdout.layout = org.apache.log4j.PatternLayout<br><br>log4j.appender.file.layout.ConversionPattern=%d [ %-5 ] %c{1} - %m%n |
| peoplesoft classpath | Ruta de acceso de clase a los archivos .jar de la API de PeopleSoft EPM.<br><br>Este parámetro es opcional. |
| enterprise.classpath | Ruta de clase a los archivos .jar del SDK de la plataforma de BI.<br><br>Este parámetro es opcional. |

| Parámetro | Descripción |
| --- | --- |
| db.driver.type | Tipo de base de datos de PeopleSoft. Este parámetro puede tener uno de los siguientes valores:<br>Microsoft SQL Server 2000<br>Oracle Database 10.1<br>DB2 UDB 8.2 Fixpack 7<br>Personalizado<br>Éste último se puede utilizar para especificar bases de datos distintas de las versiones o tipos reconocidos.<br>Este parámetro es opcional. |
| sql.db.class.location<br>sql.db.host<br>sql.db.port<br>sql.db.database | Ubicación de los archivos .jar del controlador JDB de SQL Server, el equipo host de SQL Server, el puerto de SQL Server y el nombre de la base de datos de SQL Server.<br>Estos parámetros solo se pueden utilizar si db.driver.type es Microsoft SQL Server 2000.<br>Estos parámetros son opcionales. |
| oracle.db.class.location<br>oracle.db.host<br>oracle.db.port<br>oracle.db.sid | Ubicación de los archivos .jar del controlador JDBC de Oracle, el equipo host de la base de datos de Oracle, el puerto de la base de datos de Oracle y el SID de la base de datos de Oracle.<br>Estos parámetros solo se pueden utilizar si db.driver.type es Oracle Database 10.1.<br>Estos parámetros son opcionales. |
| db2.db.class.location<br>db2.db.host<br>db2.db.port<br>db2.db.sid | Ubicación de los archivos .jar del controlador JDBC de DB2, el equipo host de la base de datos DB2, el puerto de la base de datos DB2 y el SID de la base de datos DB2.<br>Estos parámetros solo se pueden utilizar si db.driver.type es DB2 UDB 8.2 Fixpack 7.<br>Estos parámetros son opcionales. |
| custom.db.class.location<br>custom.db.drivername<br>custom.db.connectStr | Ubicación, nombre y cadena de conexión del controlador JDBC personalizado.<br>Estos parámetros solo se pueden utilizar si db.driver.type es Personalizado.<br>Estos parámetros son opcionales. |

## 9.7 Autenticación de JD Edwards

### 9.7.1 Introducción

Para usar los datos de JD Edwards con la Plataforma de BI, se debe proporcionar al sistema la información acerca del despliegue de JD Edwards. Esta información es la que permite a la Plataforma de BI autenticar usuarios para que puedan usar sus credenciales de JD Edwards EnterpriseOne para iniciar sesión en la Plataforma de BI.

### 9.7.2 Habilitar la autenticación de JD Edwards EnterpriseOne

Para permitir que la plataforma de BI use la información de JD Edwards EnterpriseOne, la plataforma necesita la información sobre cómo autenticarse en el sistema de JD Edwards EnterpriseOne.

#### 9.7.2.1 Habilitar la autenticación de JD Edwards en la plataforma de BI

1. Inicie una sesión como administrador en la Consola de administración central.
2. En el área Administrar, haga clic en *Autenticación*.
3. Haga doble clic en *JD Edwards EnterpriseOne*.
   Aparece la página de *JD Edwards EnterpriseOne*.
4. En la ficha *Opciones*, seleccione la casilla de verificación *Habilitar autenticación de JD Edwards EnterpriseOne*.
5. Realice los cambios necesarios en *Nuevo alias*, *Opciones de actualización* y *Opciones de usuarios nuevos* según su despliegue de la plataforma de BI. Haga clic en *Actualizar* para guardar los cambios antes de pasar a la ficha *Sistemas*.
6. Haga clic en la ficha *Servidores*.
7. Copie `jdeutil.jar`, `kernel.jar`, y `log4j.jar` desde la instalación JD Edwards a estas ubicaciones (en Windows): `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\` e `<INSTALLDIR>\Tomcat\lib\`.
8. Reinicie Tomcat y Server Intelligence Agent.
9. En el área *Usuario del sistema JD Edwards EnterpriseOne*, escriba un nombre de usuario de base de datos y una contraseña para que la Plataforma de BI inicie sesión en la base de datos de JD Edwards EnterpriseOne.
10. En el área *Dominio de JD Edwards EnterpriseOne*,introduzca el nombre, host y puerto que se usa para conectarse al entorno de JD Edwards EnterpriseOne.
11. Introduzca un nombre para el entorno y haga clic en *Agregar*.
12. Haga clic en *Actualizar* para guardar los cambios.

## 9.7.3 Asignar funciones de JD Edwards EnterpriseOne a la plataforma de BI

La Plataforma de BI crea automáticamente un grupo para cada función de JD Edwards EnterpriseOne que asigne. A su vez, el sistema crea alias para representar a los miembros de las funciones de JD Edwards EnterpriseOne asignadas.

Puede crear una cuenta de usuario para cada alias generado.

Sin embargo, si se ejecutan varios sistemas y los usuarios tienen cuentas en varios de ellos, se puede asignar a cada usuario un alias con el mismo nombre antes de crear las cuentas en la Plataforma de BI.

De este modo se reduce el número de cuentas que se crean para el mismo usuario en la Plataforma de BI.

Por ejemplo, si ejecuta un entorno de prueba y un entorno de producción de JD Edwards EnterpriseOne, y 30 usuarios tienen acceso a ambos sistemas, sólo se crearán 30 cuentas para dichos usuarios. Si decide no asignar a cada usuario un alias con el mismo nombre, se crearán 60 cuentas para los 30 usuarios en la Plataforma de BI.

Sin embargo, si ejecuta varios sistemas, y se repiten los nombres de usuario, deberá crear una nueva cuenta de miembro para cada alias creado.

Por ejemplo, si ejecuta el entorno de prueba con una cuenta de usuario de Russell Aquino (nombre de usuario "raquino"), y ejecuta el entorno de producción con una cuenta de usuario de Raúl Aquino (nombre de usuario "raquino"), deberá crear una cuenta independiente para cada alias de usuario. De lo contrario, los dos usuarios se agregarán a la misma cuenta de la Plataforma de BI y no podrán iniciar sesión en la Plataforma de BI con sus credenciales de JD Edwards EnterpriseOne.

### 9.7.3.1 Asignar una función de JD Edwards EnterpriseOne

1. Inicie una sesión como administrador en la Consola de administración central.
2. En el área *Administrar*, haga clic en *Autenticación*.
3. Haga doble clic en *JD Edwards EnterpriseOne*.
4. En el área *Opciones de alias nuevos*, seleccione una de las siguientes opciones:
   - *Asignar cada alias agregado a una cuenta con el mismo nombre*
     Seleccione esta opción si tiene varios sistemas JD Edwards EnterpriseOne con usuarios que tienen cuentas en más de un sistema (y no hay dos usuarios que tengan el mismo nombre de usuario en diferentes sistemas).
   - *Crear una cuenta nueva para cada alias agregado*
     Seleccione esta opción si solo tiene un sistema JD Edwards EnterpriseOne, si la mayoría de usuarios tienen cuentas en un único sistema, o si los nombres de usuario de diferentes usuarios en dos o más sistemas coinciden.
5. En el área *Opciones de actualización*, seleccione una de las siguientes opciones:
   - *Se agregarán alias nuevos y se crearán usuarios*
     Seleccione esta opción para crear un nuevo alias para cada usuario que se asigne a la Plataforma de BI. Se agregan nuevas cuentas para los usuarios sin cuentas de la plataforma de BI o para todos los usuarios si selecciona la opción Crear una cuenta nueva para cada opción de alias agregado.

- *No se agregarán alias nuevos ni se crearán usuarios nuevos*
  Seleccione esta opción si la función que desea asignar contiene varios usuarios, pero solo unos cuantos de ellos usan la Plataforma de BI. El sistema no crea automáticamente alias ni cuentas para los usuarios. En su lugar, crea alias (y cuentas, en caso necesario) solo para los usuarios al iniciar sesión en la Plataforma de BI por primera vez. Esta es la opción predeterminada.

6. En el área *Opciones de usuarios nuevos*, especifique el modo en que se crean los usuarios nuevos.

   Seleccione una de las siguientes opciones:

   - *Los usuarios nuevos se crean como usuarios con nombre*
     Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios con nombre. Las licencias de usuario con nombre se asocian con usuarios específicos y permiten que tengan acceso al sistema basándose en sus nombres de usuario y en sus contraseñas. De esta forma, los usuarios con nombre pueden tener acceso al sistema independientemente del número de personas conectadas. Debe tener una licencia de usuario con nombre disponible por cada cuenta de usuario creada mediante esta opción.

     > **Nota**
     >
     > El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.
     >
     > Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

   - *Los usuarios nuevos se crean como usuarios simultáneos*
     Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios simultáneos. Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque una licencia simultánea pequeña puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios a la Plataforma de BI, una licencia simultánea de 100 usuarios puede admitir 250, 500 ó 700 usuarios.

   Las funciones que seleccione ahora aparecerán como grupos en la Plataforma de BI.

7. Haga clic en la ficha *Funciones*.
8. En *Lista de dominios*, seleccione el servidor de JD Edwards que contiene las funciones que desee asignar.
9. En *Funciones disponibles*, seleccione las funciones que desea asignar a la plataforma de BI y haga clic en <.
10. Haga clic en *Actualizar*.
    Las funciones se asignarán a la Plataforma de BI.

## 9.7.3.2 Aspectos a tener en cuenta en la reasignación

Si se agregan usuarios a una función que ya se ha asignado a la Plataforma de BI, tendrá que volver a asignar la función para agregar usuarios a la Plataforma de BI. Al reasignar la función, la posibilidad de asignar usuarios como usuarios con nombre o simultáneos solo afecta a los nuevos usuarios agregados a la función.

Por ejemplo, primero se asigna una función a la Plataforma de BI con la opción "Se crean nuevos usuarios como usuarios *con nombre*" seleccionada. A continuación, se agregan usuarios a la misma función y ésta se reasigna con la opción "Se crean nuevos usuarios como *simultáneos*" seleccionada.

En esta situación, solo los nuevos usuarios de la función se asignan a la Plataforma de BI como usuarios simultáneos; los usuarios que ya estaban asignados permanecen como usuarios con nombre. La misma condición se aplica si primero se asignan usuarios como usuarios simultáneos y, a continuación, se cambia la configuración para reasignar nuevos usuarios como usuarios con nombre.

### 9.7.3.3 Desasignar una función

1. Inicie una sesión en la Consola de administración central como administrador.
2. En el área *Administrar*, haga clic en *Autenticación*.
3. Haga clic en la ficha para *JD Edwards EnterpriseOne*.
4. En el área *Funciones*, seleccione la función que desee eliminar y haga clic en <.
5. Haga clic en *Actualizar*.

   Los miembros de la función ya no podrán acceder a la Plataforma de BI, a menos que tengan otras cuentas o alias.

   > **Nota**
   >
   > También puede eliminar cuentas individuales o eliminar usuarios de las funciones antes de asignarlas a la Plataforma de BI para evitar que usuarios específicos inicien sesión.

## 9.7.4 Programación de actualizaciones de usuario

Para garantizar que los cambios realizados en los datos del usuario para el sistema ERP se reflejan en los datos de usuario de la plataforma de BI, puede programar actualizaciones de usuario a intervalos regulares. Estas actualizaciones sincronizarán automáticamente los usuarios del sistema ERP con los de la plataforma de BI según la configuración de asignación que se haya configurado en la Consola de administración central (CMC).

Existen dos opciones para ejecutar y programar actualizaciones para las funciones importadas:

- Solo actualizar funciones: con esta opción solo se actualizarán los vínculos entre las funciones actualmente asignadas que se han importado en la plataforma de BI. Use esta opción si espera ejecutar actualizaciones frecuentes y le preocupa el uso de los recursos del sistema. No se crearán cuentas de usuario si solo actualiza las funciones.
- Actualizar funciones y alias: esta opción además de actualizar los vínculos entre las funciones, creará cuentas de usuario nuevas en la plataforma de BI para los nuevos alias de usuario agregados al sistema ERP.

> **Nota**
>
> Si, cuando ha activado la autenticación, no ha especificado crear automáticamente alias para las actualizaciones, no se crearán cuentas para los nuevos alias.

### 9.7.4.1 Programar actualizaciones de usuario

Después de asignar las funciones a la plataforma de BI debe especificar el modo en que el sistema actualiza estas funciones.

1. Haga clic en la ficha *Actualización de usuario*.
2. Haga clic en *Programar* en las secciones *Sólo actualizar funciones* o *Actualizar funciones y alias*.

   > → Sugerencias
   >
   > Si desea ejecutar una actualización inmediatamente, haga clic en *Actualizar ahora*.

   > → Sugerencias
   >
   > Use la opción *Sólo actualizar funciones* si desea realizar actualizaciones frecuentes y le preocupa el uso de los recursos del sistema. La actualización de funciones y alias tarda más en realizarse.

   Aparece el cuadro de diálogo *Periodicidad*.
3. Seleccione una opción de la lista *Ejecutar objeto* y proporcione la información de programación que se le solicite.

   Cuando programa una actualización, puede elegir entre los patrones de repetición que se resumen en la siguiente tabla:

| Patrón de periodicidad | Descripción |
|---|---|
| Cada hora | La actualización se ejecutará cada hora. Se debe especificar a qué hora comenzará así como las fechas de inicio y fin. |
| Cada día | La actualización se ejecutará cada día o se ejecutará el número de días especificado. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Cada semana | La actualización se ejecutará cada semana. Se puede ejecutar una o varias veces a la semana. Puede especificar en qué días y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Mensual | La actualización se ejecutará cada mes o cada varios meses. Puede indicar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día N de cada mes | La actualización se ejecutará un día específico del mes. Puede especificar en qué día del mes y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Primer lunes del mes | La actualización se ejecutará el primer lunes de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Último día de cada mes | La actualización se ejecutará el último día de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día X de la semana N de cada mes | La actualización se ejecutará un día especificado de una semana especificada del mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Calendario | La actualización se ejecutará en las fechas especificadas en un calendario que se haya creado previamente. |

4. Haga clic en *Programar* una vez que haya proporcionado toda la información de planificación.
   La fecha de la siguiente actualización de función programada se muestra en la ficha *Actualización de usuario*.

> **Nota**
>
> Si lo desea puede cancelar la siguiente actualización programada haciendo clic en *Cancelar actualizaciones programadas* en las secciones *Sólo actualizar funciones* o *Actualizar funciones y alias*.

## 9.8 Autenticación de Siebel

### 9.8.1 Habilitar la autenticación de Siebel

Para permitir que la Plataforma de BI use la información de Siebel, necesita la información sobre cómo autenticarse en el sistema de Siebel.

#### 9.8.1.1 Habilitar la autenticación de Siebel en la plataforma de BI

1. Inicie una sesión en la Consola de administración central como administrador.
2. En el área Administrar, haga clic en *Autenticación*.
3. Haga doble clic en *Siebel*.
   Aparece la página *Siebel*. Contiene cuatro fichas: *Opciones*, *Sistemas*, *Responsabilidades* y *Actualización de usuario*.
4. En la ficha *Opciones*, seleccione la casilla de verificación *Activar autenticación de Siebel*.
5. Realice los cambios necesarios en *Nuevo alias*, *Opciones de actualización* y *Opciones de usuarios nuevos* según su despliegue de la plataforma de BI. Haga clic en *Actualizar* para guardar los cambios antes de pasar a la ficha *Sistemas*.
6. Haga clic en la ficha *Dominios*.
7. En el campo *Nombre del dominio*, introduzca el nombre de dominio del sistema Siebel al que desea conectarse.
8. En *Conexión*, introduzca la cadena de conexión de este dominio.
9. En el área *Nombre de usuario*, escriba un nombre de usuario de base de datos y una contraseña para que la Plataforma de BI inicie sesión en la base de datos de Siebel.
10. En el área *Contraseña*, introduzca la contraseña del usuario que ha seleccionado.
11. Haga clic en *Agregar* para agregar la información del sistema a la lista *Dominios actuales*.
12. Haga clic en *Actualizar* para guardar los cambios.

### 9.8.2 Asignar funciones a la plataforma de BI

La Plataforma de BI crea automáticamente un grupo para cada función de Siebel que asigne. A su vez, el programa crea alias para representar a los miembros de las funciones de Siebel asignadas.

Puede crear una cuenta de usuario para cada alias generado.

Sin embargo, si se ejecutan varios sistemas y los usuarios tienen cuentas en varios de ellos, se puede asignar a cada usuario un alias con el mismo nombre antes de crear las cuentas en la Plataforma de BI.

Así se reduce el número de cuentas que se crean para el mismo usuario en el programa.

Por ejemplo, si ejecuta un entorno de prueba y un entorno de producción de Siebel eBusiness y 30 usuarios tienen acceso a ambos sistemas, solo se crearán 30 cuentas para dichos usuarios. Si decide no asignar a cada usuario un alias con el mismo nombre, se crearán 60 cuentas para los 30 usuarios en la Plataforma de BI.

Sin embargo, si ejecuta varios sistemas, y se repiten los nombres de usuario, deberá crear una nueva cuenta de miembro para cada alias creado.

Por ejemplo, si ejecuta el entorno de prueba con una cuenta de usuario de Russell Aquino (nombre de usuario "raquino"), y ejecuta el entorno de producción con una cuenta de usuario de Raúl Aquino (nombre de usuario "raquino"), deberá crear una cuenta independiente para cada alias de usuario. De lo contrario, los dos usuarios se agregan a la misma cuenta y no podrán iniciar sesión en la Plataforma de BI con sus credenciales de Siebel eBusiness.

### 9.8.2.1 Asignar una función de Siebel eBusiness a la plataforma de BI

1. Inicie una sesión como administrador en la Consola de administración central.
2. Haga clic en *Autenticación*.
3. Haga doble clic en *Siebel*.
4. Seleccione la casilla de verificación *Habilitar autenticación de Siebel*.
5. En el área *Opciones de alias nuevos*, seleccione una de las siguientes opciones:
   - *Asignar cada alias agregado a una cuenta con el mismo nombre*
     Seleccione esta opción si ejecuta varios sistemas Siebel eBusiness con usuarios que tienen cuentas en más de un sistema (y dos usuarios no tienen el mismo nombre de usuario para sistemas diferentes).
   - *Crear una cuenta nueva para cada alias agregado*
     Seleccione esta opción si solo ejecuta un sistema Siebel eBusiness, si la mayoría de los usuarios tiene cuentas en un único sistema, o si se repiten los nombres de usuario para diferentes usuarios en dos o más de sus sistemas.
6. En el área *Opciones de actualización del alias*, seleccione una de las siguientes opciones:
   - *Crear nuevos alias cuando se actualice el alias*
     Seleccione esta opción para crear un nuevo alias para cada usuario que se asigne a la Plataforma de BI. Se agregan nuevas cuentas para los usuarios sin cuentas de la plataforma de BI o para todos los usuarios si selecciona la opción Crear una cuenta nueva para cada opción de alias agregado.
   - *Crear nuevos alias solo cuando el usuario inicie sesión*
     Seleccione esta opción si la función que desea asignar contiene varios usuarios, pero solo unos cuantos de ellos usan la Plataforma de BI. El programa no crea automáticamente alias ni cuentas para los usuarios. En su lugar, crea alias (y cuentas, en caso necesario) solo para los usuarios al iniciar sesión en la Plataforma de BI por primera vez. Esta es la opción predeterminada.
7. En el área *Opciones de usuarios nuevos*, especifique el modo en que se crean los usuarios.

   Si la licencia de la plataforma de BI se basa en funciones de usuario, seleccione una de las siguientes opciones:

Seleccione una de las siguientes opciones:

- *Se crean nuevos usuarios como usuarios con nombre*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios con nombre. Las licencias de usuario con nombre se asocian con usuarios específicos y permiten que tengan acceso al sistema basándose en sus nombres de usuario y en sus contraseñas. De esta forma, los usuarios con nombre pueden tener acceso al sistema independientemente del número de personas conectadas. Debe tener una licencia de usuario con nombre disponible por cada cuenta de usuario creada mediante esta opción.

  > **Nota**
  >
  > El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.
  >
  > Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

- *Se crean nuevos usuarios como usuarios simultáneos*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios simultáneos. Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque una licencia simultánea pequeña puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios a la Plataforma de BI, una licencia simultánea de 100 usuarios puede admitir 250, 500 ó 700 usuarios.

8. Haga clic en la ficha *Funciones*.
9. Seleccione el dominio que corresponda al servidor Siebel al que desea asignar funciones.
10. En *Funciones disponibles*, seleccione las funciones que desee asignar y haga clic en >.

    > **Nota**
    >
    > Puede utilizar el campo *Buscar funciones que comiencen por:* para delimitar la búsqueda si tiene muchos roles. Escriba los caracteres por los que empieza la función o funciones, seguidos del carácter comodín (%) y haga clic en *Buscar*.

    > **Nota**
    >
    > Para que la función de búsqueda funcione, un archivo jar de complemento Siebel se debe desplegar al directorio lib de Tomcat: `<DIRINSTAL>\tomcat\webapps\BOE\WEB-INF\lib` y a `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\java\lib\siebel\default\siebel`. A continuación, reinicie el servidor Tomcat y Server Intelligence Agent.

11. Haga clic en *Actualizar*.
    Las funciones se asignarán a la Plataforma de BI.

### 9.8.2.2 Aspectos a tener en cuenta en la reasignación

Para forzar la sincronización de grupos y usuarios entre la Plataforma de BI y Siebel, configure *Forzar sincronización de usuarios*.

> **Nota**
>
> Para seleccionar *Forzar sincronización de usuarios*, primero debe seleccionar *Se agregarán alias nuevos y se crearán usuarios*.

Al reasignar la función, la posibilidad de asignar usuarios como usuarios con nombre o simultáneos solo afecta a los nuevos usuarios agregados a la función.

Por ejemplo, primero se asigna una función a la Plataforma de BI con la opción "Se crean nuevos usuarios como usuarios *con nombre*" seleccionada. A continuación, se agregan usuarios a la misma función y ésta se reasigna con la opción "Se crean nuevos usuarios como *simultáneos*" seleccionada.

En esta situación, solo los nuevos usuarios de la función se asignan a la Plataforma de BI como usuarios simultáneos; los usuarios que ya estaban asignados permanecen como usuarios con nombre. La misma condición se aplica si primero se asignan usuarios como usuarios simultáneos y, a continuación, se cambia la configuración para reasignar nuevos usuarios como usuarios con nombre.

### 9.8.2.3 Desasignar una función

1. Inicie una sesión en la Consola de administración central como administrador.
2. En el área *Administrar*, haga clic en *Autenticación*.
3. Haga doble clic en *Siebel*.
4. En la ficha *Dominios* seleccione el dominio Siebel que se corresponde con la función (o funciones) que desea desasignar.
5. En la ficha *Funciones*, seleccione la función que desee eliminar y haga clic en <.
6. Haga clic en *Actualizar*.

   Los miembros de la responsabilidad ya no podrán acceder a la Plataforma de BI, a no ser que dispongan de otras cuentas o alias.

   > **Nota**
   >
   > También puede eliminar cuentas individuales o eliminar usuarios de las funciones antes de asignarlas a la Plataforma de BI para evitar que usuarios específicos inicien sesión.

## 9.8.3 Programación de actualizaciones de usuario

Para garantizar que los cambios realizados en los datos del usuario para el sistema ERP se reflejan en los datos de usuario de la plataforma de BI, puede programar actualizaciones de usuario a intervalos regulares. Estas actualizaciones sincronizarán automáticamente los usuarios del sistema ERP con los de la plataforma de BI según la configuración de asignación que se haya configurado en la Consola de administración central (CMC).

Existen dos opciones para ejecutar y programar actualizaciones para las funciones importadas:

- Solo actualizar funciones: con esta opción solo se actualizarán los vínculos entre las funciones actualmente asignadas que se han importado en la plataforma de BI. Use esta opción si espera ejecutar actualizaciones frecuentes y le preocupa el uso de los recursos del sistema. No se crearán cuentas de usuario si solo actualiza las funciones.
- Actualizar funciones y alias: esta opción además de actualizar los vínculos entre las funciones, creará cuentas de usuario nuevas en la plataforma de BI para los nuevos alias de usuario agregados al sistema ERP.

> ⓘ Nota
>
> Si, cuando ha activado la autenticación, no ha especificado crear automáticamente alias para las actualizaciones, no se crearán cuentas para los nuevos alias.

### 9.8.3.1 Programar actualizaciones de usuario

Después de asignar las funciones a la plataforma de BI debe especificar el modo en que el sistema actualiza estas funciones.

1. Haga clic en la ficha *Actualización de usuario*.
2. Haga clic en *Programar* en las secciones *Sólo actualizar funciones* o *Actualizar funciones y alias*.

   > → Sugerencias
   >
   > Si desea ejecutar una actualización inmediatamente, haga clic en *Actualizar ahora*.

   > → Sugerencias
   >
   > Use la opción *Sólo actualizar funciones* si desea realizar actualizaciones frecuentes y le preocupa el uso de los recursos del sistema. La actualización de funciones y alias tarda más en realizarse.

   Aparece el cuadro de diálogo *Periodicidad*.
3. Seleccione una opción de la lista *Ejecutar objeto* y proporcione la información de programación que se le solicite.

   Cuando programa una actualización, puede elegir entre los patrones de repetición que se resumen en la siguiente tabla:

| Patrón de periodicidad | Descripción |
|---|---|
| Cada hora | La actualización se ejecutará cada hora. Se debe especificar a qué hora comenzará así como las fechas de inicio y fin. |
| Cada día | La actualización se ejecutará cada día o se ejecutará el número de días especificado. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |

| Patrón de periodicidad | Descripción |
|---|---|
| Cada semana | La actualización se ejecutará cada semana. Se puede ejecutar una o varias veces a la semana. Puede especificar en qué días y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Mensual | La actualización se ejecutará cada mes o cada varios meses. Puede indicar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día N de cada mes | La actualización se ejecutará un día específico del mes. Puede especificar en qué día del mes y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Primer lunes del mes | La actualización se ejecutará el primer lunes de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Último día de cada mes | La actualización se ejecutará el último día de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día X de la semana N de cada mes | La actualización se ejecutará un día especificado de una semana especificada del mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Calendario | La actualización se ejecutará en las fechas especificadas en un calendario que se haya creado previamente. |

4. Haga clic en *Programar* una vez que haya proporcionado toda la información de planificación.
   La fecha de la siguiente actualización de función programada se muestra en la ficha *Actualización de usuario*.

> **Nota**
>
> Si lo desea puede cancelar la siguiente actualización programada haciendo clic en *Cancelar actualizaciones programadas* en las secciones *Sólo actualizar funciones* o *Actualizar funciones y alias*.

# 9.9 Autenticación de Oracle EBS

## 9.9.1 Habilitar la autenticación de Oracle EBS

Para que la plataforma de BI pueda usar la información de Oracle EBS, el sistema necesita información sobre cómo autenticarse en el sistema de Oracle EBS.

### 9.9.1.1 Activar la autenticación de Oracle E-Business Suite

Antes de llevar a cabo el procedimiento, los archivos de DLL y JAR de Oracle se deben desplegar en la plataforma de BI:

1. Descargue `ojdbc11.dll` desde la aplicación de cliente de la base de datos de Oracle.
2. Copie el archivo a esta ubicación:
   - Windows: `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`

- UNIX: `<DIRINSTAL>/sap_bobj/enterprise_xi40/platform`

3. Descargue `ojdbc5.jar` desde la aplicación de cliente de base de datos de Oracle.
4. Copie el archivo a esta ubicación:
   - Windows: `<DIRINSTAL>\Tomcat\lib`
   - UNIX: `<DIRINSTAL>/sap_bobj/tomcat/lib`

1. Inicie una sesión en la Consola de administración central como administrador.
2. En el área Administrar, haga clic en *Autenticación*.
3. Haga clic en *Oracle EBS*.
   Se abrirá la página *Oracle EBS*. Contiene cuatro fichas: *Opciones*, *Sistemas*, *Responsabilidades* y *Actualización de usuario*.
4. En la ficha *Opciones*, seleccione la casilla de verificación *La autenticación de Oracle EBS está habilitada*.
5. Realice los cambios necesarios en *Nuevo alias*, *Opciones de actualización* y *Opciones de usuarios nuevos* según su despliegue de la plataforma de BI. Haga clic en *Actualizar* para guardar los cambios antes de pasar a la ficha *Sistemas*.
6. Haga clic en la ficha *Sistemas*.
7. En el área *Usuario del sistema de Oracle EBS*, escriba el nombre de usuario y la contraseña de la plataforma de BI que desee usar para iniciar sesión en la base de datos de Oracle E-Business Suite.
8. En el área *Servicios de Oracle EBS*, escriba el nombre del servicio usado en su entorno de Oracle EBS y haga clic en *Agregar*.
9. Haga clic en *Actualizar* para guardar los cambios.

Debe asignar las funciones de Oracle EBS en el sistema.

### Información relacionada

Asignar funciones de Oracle E-Business Suite [página 396]

## 9.9.2 Asignar funciones de Oracle E-Business Suite a la plataforma de BI

La plataforma de BI crea automáticamente un grupo para cada función de Oracle E-Business Suite (EBS) que asigne. El sistema también crea alias para representar a los miembros de las funciones de Oracle E-Business Suite asignadas.

Puede crear una cuenta de usuario para cada alias generado. Sin embargo, si se ejecutan varios sistemas y los usuarios tienen cuentas en varios de ellos, se puede asignar a cada usuario un alias con el mismo nombre antes de crear las cuentas en la Plataforma de BI.

De este modo se reduce el número de cuentas que se crean para el mismo usuario en el sistema.

Por ejemplo, si ejecuta un entorno de prueba y un entorno de producción de EBS y 30 usuarios tienen acceso a ambos sistemas, sólo se crearán 30 cuentas para dichos usuarios. Si decide no asignar a cada usuario un alias con el mismo nombre, se crearán 60 cuentas para los 30 usuarios en la Plataforma de BI.

Sin embargo, si ejecuta varios sistemas, y se repiten los nombres de usuario, deberá crear una nueva cuenta de miembro para cada alias creado.

Por ejemplo, si ejecuta el entorno de prueba con una cuenta de usuario de Russell Aquino (nombre de usuario "raquino"), y ejecuta el entorno de producción con una cuenta de usuario de Raúl Aquino (nombre de usuario "raquino"), deberá crear una cuenta independiente para cada alias de usuario. De lo contrario, los dos usuarios se agregarán a la misma cuenta de la plataforma de BI; podrán iniciar una sesión en el sistema con sus propias credenciales de Oracle EBS y tendrán acceso a los datos de ambos entornos EBS.

### 9.9.2.1 Asignar funciones de Oracle E-Business Suite

1. Inicie una sesión como administrador en la Consola de administración central.
2. En el área Administrar, haga clic en *Autenticación*.
3. Haga clic en *Oracle EBS*.
   La página *Oracle EBS* muestra la ficha *Opciones*.
4. En el área *Opciones de alias nuevos*, seleccione una de las siguientes opciones:
   - *Asignar cada alias de Oracle EBS agregado a una cuenta con el mismo nombre*
     Seleccione esta opción si ejecuta varios sistemas Oracle E-Business Suite con usuarios que tienen cuentas en más de un sistema (y dos usuarios no tienen el mismo nombre de usuario para sistemas diferentes).
   - *Crear una cuenta nueva para cada alias de Oracle EBS agregado*
     Seleccione esta opción si solo ejecuta un sistema Oracle E-Business Suite, si la mayoría de usuarios tienen cuentas en un único sistema, o si se repiten los nombres de usuario para diferentes usuarios en dos o más de sus sistemas.
5. En el área *Opciones de actualización*, seleccione una de las siguientes opciones:
   - *Crear nuevos alias cuando se actualice el alias*
     Seleccione esta opción para crear un nuevo alias para cada usuario que se asigne a la Plataforma de BI. Se agregan nuevas cuentas para los usuarios sin cuentas de la plataforma de BI o para todos los usuarios si selecciona la opción *Crear una cuenta nueva para cada alias de Oracle EBS agregado*.
   - *Crear nuevos alias solo cuando el usuario inicie sesión*
     Seleccione esta opción si la función que desea asignar contiene varios usuarios, pero solo unos cuantos de ellos usan la Plataforma de BI. La plataforma no crea automáticamente alias ni cuentas para los usuarios. En su lugar, crea alias (y cuentas, en caso necesario) solo para los usuarios al iniciar sesión en la Plataforma de BI por primera vez. Esta es la opción predeterminada.
6. En *Opciones de usuarios nuevos* especifique cómo se crean los nuevos usuarios y, después, haga clic en *Actualizar*.

   Seleccione una de las siguientes opciones:

   - *Los usuarios nuevos se crean como usuarios con nombre*
     Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios con nombre. Las licencias de usuario con nombre se asocian con usuarios específicos y permiten que tengan acceso al sistema basándose en sus nombres de usuario y en sus contraseñas. De esta forma, los usuarios con nombre pueden tener acceso al sistema independientemente del número de personas conectadas. Debe tener una licencia de usuario con nombre disponible por cada cuenta de usuario creada mediante esta opción.

> **Nota**
>
> El número máximo de sesiones simultáneas de inicio de sesión de un usuario con nombre creado con la licencia de usuario nombrado está limitada a 10. Si el usuario con nombre intenta iniciar una undécima sesión simultánea de inicio de sesión, el sistema mostrará un mensaje de error al respecto. Deberá finalizar una de las sesiones existentes antes de poder iniciar otra sesión.
>
> Sin embargo, no hay restricciones en el número de sesiones simultáneas de inicio de sesión para usuarios con nombre creados con la licencia de procesador y la licencia de documentos públicos.

- *Los usuarios nuevos se crean como usuarios simultáneos*
  Las cuentas de los nuevos usuarios se configuran para utilizar licencias de usuarios simultáneos. Las licencias simultáneas especifican el número de personas que se pueden conectar a la Plataforma de BI a la vez. Este tipo de licencias es muy flexible porque una licencia simultánea pequeña puede admitir una base de usuarios grande. Por ejemplo, dependiendo de la frecuencia y del período de acceso de los usuarios a la plataforma, una licencia simultánea de 100 usuarios puede admitir 250, 500 ó 700 usuarios.

Las funciones que seleccione ahora aparecerán como grupos en la Plataforma de BI.

7. Haga clic en la ficha *Responsabilidades*.
8. En *Servicios de Oracle EBS actuales*, seleccione el servicio Oracle EBS que contenga las funciones que desea asignar.
9. Puede especificar filtros para usuarios de Oracle EBS en *Funciones de Oracle EBS asignadas*.
   a. Seleccione qué aplicaciones pueden utilizar los usuarios para la nueva función, entre las opciones de la lista *Aplicación*.
   b. En la lista *Responsabilidad*, seleccione las aplicaciones, funciones e informes de Oracle, así como los programas simultáneos que puede ejecutar un usuario.
   c. En *Grupo de seguridad*, seleccione el grupo de seguridad al que se ha asignado la nueva función en el grupo Seguridad.
   d. Use los botones *Agregar* y *Eliminar*, en *Función actual*, para modificar las asignaciones de grupo de seguridad existentes para la función.
10. Haga clic en *Actualizar*.
    Las funciones se asignarán a la Plataforma de BI.

Después de asignar las funciones a la plataforma de BI debe especificar el modo en que el sistema actualiza estas funciones.

### 9.9.2.1.1 Actualizar las funciones y los usuarios de Oracle EBS

Tras activar la autenticación de Oracle EBS, es necesario programar y ejecutar regularmente actualizaciones en funciones asignadas que se han importado en la plataforma de BI. Esto garantizará que la información actualizada de las funciones de Oracle EBS se refleja con exactitud en la plataforma de BI.

Existen dos opciones para ejecutar y programar actualizaciones para las funciones de Oracle EBS:

- Solo actualizar funciones: Con esta opción solo se actualizarán los vínculos entre las funciones actualmente asignadas que se han importado en la plataforma de BI. Es aconsejable usar esta opción

si tiene la intención de ejecutar actualizaciones con frecuencia y le preocupa el uso de los recursos del sistema. No se crearán cuentas de usuario si solo actualiza las funciones de Oracle EBS.

- Actualizar funciones y alias: Esta opción además de actualizar los vínculos entre las funciones, crea nuevas cuentas de usuarios en la plataforma de BI para los alias de usuario agregados a las funciones en el sistema Oracle EBS.

> **Nota**
>
> Si, cuando ha activado la autenticación de Oracle EBS, no ha especificado crear automáticamente alias para las actualizaciones, no se crearán cuentas para los nuevos alias.

### 9.9.2.1.2 Programar actualizaciones para las funciones de Oracle EBS

Después de asignar las funciones a la plataforma de BI debe especificar el modo en que el sistema actualiza estas funciones.

1. Haga clic en la ficha *Actualización de usuario*.
2. Haga clic en *Programar* en las secciones *Sólo actualizar funciones* o *Actualizar funciones y alias*.

   > **Sugerencias**
   >
   > Si desea ejecutar y actualizar inmediatamente, haga clic en *Actualizar ahora*.

   > **Sugerencias**
   >
   > Use la opción *Sólo actualizar funciones* si desea realizar actualizaciones con frecuencia y le preocupa el uso de los recursos del sistema. La actualización de funciones y alias tarda más en realizarse.

   Aparece el cuadro de diálogo *Periodicidad*.
3. Seleccione una opción de la lista desplegable *Ejecutar objeto* y proporcione la información de programación que se le solicite en los campos provistos.

   Cuando programa una actualización, puede elegir entre los patrones de repetición que se resumen en la siguiente tabla:

| Patrón de periodicidad | Descripción |
|---|---|
| Cada hora | La actualización se ejecutará cada hora. Se debe especificar a qué hora comenzará así como las fechas de inicio y fin. |
| Cada día | La actualización se ejecutará cada día o el número de días especificado. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Cada semana | La actualización se ejecutará cada semana. Se puede ejecutar una o varias veces a la semana. Puede especificar en qué días y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Mensual | La actualización se ejecutará cada mes o cada varios meses. Puede indicar a qué hora se ejecutará, así como la fecha de inicio y fin. |

| Patrón de periodicidad | Descripción |
|---|---|
| Día N de cada mes | La actualización se ejecutará un día específico del mes. Puede especificar en qué día del mes y a qué hora se ejecutará, así como las fechas de inicio y fin. |
| Primer lunes del mes | La actualización se ejecutará el primer lunes de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Último día de cada mes | La actualización se ejecutará el último día de cada mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Día X de la semana N de cada mes | La actualización se ejecutará un día especificado de una semana especificada del mes. Puede especificar a qué hora se ejecutará, así como la fecha de inicio y fin. |
| Calendario | La actualización se ejecutará en las fechas especificadas en un calendario que se haya creado previamente. |

4. Haga clic en *Programar* una vez que haya proporcionado toda la información de planificación.
   La fecha de la siguiente actualización de función programada se muestra en la ficha *Actualización de usuario*.

> ⓘ Nota
>
> Si lo desea puede cancelar la siguiente actualización programada haciendo clic en *Cancelar actualizaciones programadas* en las secciones *Sólo actualizar funciones* o *Actualizar funciones y alias*.

## 9.9.3 Desasignar funciones

Para evitar que grupos de usuarios concretos inicien sesión en la plataforma de BI, puede desasignar las funciones a las que pertenecen.

### 9.9.3.1 Desasignar una función

1. Inicie una sesión en la Consola de administración central como administrador.
2. En el área Administrar, haga clic en *Autenticación*.
3. Haga doble clic en el nombre del sistema ERP, para el que desea desasignar funciones.
   La página del sistema ERP muestra la ficha *Opciones*.
4. Haga clic en la ficha *Responsabilidades*.
5. Seleccione el *Servicio de Oracle EBS actual*.
6. En *Función actual*, seleccione una función y, a continuación, haga clic en el botón *Eliminar*.
7. Haga clic en *Actualizar*.

   Los miembros de la función ya no podrán acceder a la Plataforma de BI, a menos que tengan otras cuentas o alias.

> **Nota**
>
> También puede eliminar cuentas individuales o eliminar usuarios de las funciones antes de asignarlas a la Plataforma de BI para evitar que usuarios específicos inicien sesión.

## 9.9.4 Personalizar derechos para los grupos y usuario de Oracle EBS asignados

Al asignar funciones a la plataforma de BI, puede definir derechos o conceder permisos para los grupos y usuarios creados.

### 9.9.4.1 Asignar derechos de administración

Para permitir que los usuarios mantengan la plataforma de BI, deberá hacer que sean miembros del grupo predeterminado del Administrador. Los miembros de este grupo tendrán control total sobre todos los aspectos del sistema, lo que incluye cuentas, servidores, carpetas, objetos, configuraciones, etc.

1. Inicie sesión como administrador a la Consola de administración central.
2. Desde el área *Organizar*, haga clic en *Usuarios y grupos*.
3. En la columna *Nombre*, haga clic con el botón derecho en *Administradores* y haga clic en *Agregar miembros al grupo*.

   Aparece la página *Usuarios o grupos disponibles*.
4. En el área *Lista de usuarios* o *Lista de grupos*, seleccione la función asignada a la que desee asignar derechos administrativos.
5. Haga clic en > para convertir la función en un subgrupo del grupo Administradores y haga clic en *Aceptar*.

Los miembros de la función tendrán ahora derechos administrativos en la plataforma de BI.

> **Nota**
>
> También puede crear una función dentro de Oracle EBS, agregar los usuarios apropiados a la función, asignarla a la plataforma de BI y convertir la función asignada en un subgrupo del grupo predeterminado de administradores para conceder a los miembros de la función derechos administrativos.

### 9.9.4.2 Asignar derechos de publicación

Si el sistema tiene usuarios que están designados como creadores de contenido dentro de la organización, puede concederles permiso para publicar objetos en la plataforma de BI.

1. Inicie una sesión en la Consola de administración central como administrador.
2. En el área *Organizar*, haga clic en *Carpetas*.
3. Vaya a la carpeta en la que desee permitir a los usuarios agregar objetos.

4. Haga clic en *Administrar*, *Seguridad del nivel superior* y, finalmente, en *Todas las carpetas*.
5. Haga clic en *Agregar principales*.

   Aparece la página Agregar principales.
6. En la lista *Usuarios o grupos disponibles*, seleccione el grupo que incluye los miembros a los que desea proporcionar derechos de publicación.
7. Haga clic en > para habilitar que el grupo pueda acceder a la carpeta y, a continuación, haga clic en *Agregar y asignar seguridad*.

   Aparece la página Asignar seguridad.
8. En la lista *Niveles de acceso disponibles*, seleccione el nivel de acceso que desee y haga clic en > para asignar explícitamente el nivel de acceso.
9. Si las opciones *Heredar de carpeta principal* y *Heredar de grupo principal* están seleccionadas, anule su selección y haga clic en *Aplicar*.
10. Haga clic en *Aceptar*.

Ahora los miembros de la función tienen permisos para agregar objetos a la carpeta y en todas sus subcarpetas. Para eliminar permisos asignados, seleccione un grupo, y haga clic en *Eliminar*.

## 9.9.5 Configurar el inicio de sesión único (SSO) para SAP Crystal Reports y Oracle EBS

De forma predeterminada, la plataforma de BI se configurará para permitir que los usuarios de SAP Crystal Reports accedan a los datos de Oracle EBS mediante el inicio de sesión único (SSO).

### 9.9.5.1 Desactivar el SSO para Oracle EBS y SAP Crystal Reports

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. Seleccione *crdb_oraapps*.
5. Haga clic en *Eliminar*.
6. Haga clic en *Guardar y cerrar*.
7. Vaya a la página *Servidores* en la CMC, y seleccione *Servicios de Crystal Reports*.
8. Haga clic en el botón *Reiniciar servidor*.

### 9.9.5.2 Volver a activar el SSO para Oracle EBS y SAP Crystal Reports

Siga los siguientes pasos para volver a activar el SSO para Oracle EBS y SAP Crystal Reports.

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. En *Usar contexto de SSO para conexión de base de datos con los siguientes controladores*, escriba **`crdb_oraapps`**.
5. Haga clic en *Agregar*.
6. Haga clic en *Guardar y cerrar*.
7. Vaya a la página *Servidores* en la CMC, y seleccione *Servicios de Crystal Reports*.
8. Haga clic en el botón *Reiniciar servidor*.

## 9.10 Autenticación X.509

### 9.10.1 Autenticación X.509 para plataforma de lanzamiento de BI

#### 9.10.1.1 Creación y configuración de certificados y keystores

> **Nota**
>
> Debería existir un usuario en la plataforma BI para conseguir Single Sign-On mediante la autenticación X.509.

> **Nota**
>
> Descargue e instale el juego de herramientas OpenSSL para llevar a cabo los pasos indicados abajo.

> **Nota**
>
> Siga los pasos indicados si tiene que crear un certificado CA y fírmelo.

> **Nota**
>
> En el caso de que tenga una autoridad de certificación de confianza, consulte Con CA de confianza [página 404] para crear y configurar certificados y keystores.

1. Ejecute el comando para crear la autoridad de certificación (CA) clave (ca.key) y los ficheros de solicitud de certificado (ca.csr). `Openssl.exe req -newkey rsa:2048 -nodes -out c:\ssl\ca.csr -keyout c:\ssl\ca.key`
2. Ejecute el comando para crear un certificado firmado ca.perm. `Openssl.exe x509 -req -trustout -signkey c:\ssl\ca.key -days 365 -in c:\ssl\ca.csr -out c:\ssl\ca.pem`
3. Cree un par de claves de servidor, un certificado y un keystore.
   a. Cree un fichero para retener los números de serie ejecutando el código: `Echo 02 >c:\ssl\ca.srl`

b. Vaya a `C:\Program Files\Java\jre7\bin` y utilice java keytool.exe para crear un keystore de servidor, certificado y clave privada.

> **Nota**
>
> En la ubicación de Java keytool.exe, 'jre7' puede variar según la versión Java.

```
Keytool.exe -genkey -alias server -keyalg RSA -keysize 2048 -keystore
c:\ssl\serverkeystore.jks -storetype JKS
Keytool.exe -certreq -keyalg RSA -alias server -file c:\ssl\server.csr -
keystore c:\ssl\serverkeystore.jks
```

> **→ Recuerde**
>
> Al generar el certificado, introduzca el nombre de host del equipo del servidor cuando se le pida. De lo contrario, obntedrá un error de certificado en el mandante al conectarse.

c. Introduzca la contraseña del keystore.

> **→ Recuerde**
>
> Necesita editar el servidor de ficheros de solicitud .csr en un editor de texto y modificar «Nuevo inicio de solicitud de certificado» a "Iniciar solicitud de certificado» y «Nuevo fin de solicitud de cambio» a «Finalizar solicitud de certificado».

4. Ejecute el comando para crear un servidor de certificado firmado .crt. `Openssl.exe x509 -CA c:\ssl\ca.pem -cakey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\server.csr -out c:\ssl\server.crt -days 365`
5. Importe la autoridad de certificados y el certificado del servidor a un keystore de servidor.

```
Keytool.exe -import -alias ca -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\ca.pem
Keytool.exe -import -alias server -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\server.crt
```

6. Ejecute el comando para crear certificados de cliente, client.req y client.key. `Openssl.exe -newkey rsa:2048 -nodes -out c:\ssl\client.req -keyout c:\ssl\client.key -config c:\ssl\sslc.cnf`

> **Nota**
>
> Copie el archivo sslc.cnf de `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` en C:\SSL y modifique los parámetros:
>
> Dir=c:/ssl # location for everything
>
> Certificate= $dir/ca.pem # CA certificate
>
> Private_key= $dir/ca.key # private key
>
> RANDFILE= $dir/.rand # private random number file

7. Ejecute el comando para firmar el certificado del cliente. `Openssl.exe x509 -CA c:\ssl\ca.pem -CAkey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\client.req -out c:\ssl\client.pem -days 365`

8. Importe el CA y el certificado de cliente en la keystore de confianza con el comando dado abajo. El comando crea trustkeystore.jks.

```
Keytool.exe –import –alias ca –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\ca.pem
Keytool.exe –import –alias client –keystore c:\ssl\trustkeystore.jks –
trustcacerts –file c:\ssl\client.pem
```

9. Exporte el certificado de cliente con la clave privada de cliente de formato PKCS12 . `Openssl.exe pkcs12 –export –clcerts –in c:\ssl\client.pem –inkey c:\ssl\client.key –out c:\ssl\client.p12 –name “client certificate”`. El comando crea el archivo client.p12.
10. Ejecute el comando para exportar el certificado CA y cree ca.crt. `Openssl.exe x509 –in c:\ssl\ca.pem –inform PEM –out c:\ssl\ca.crt –outform DER`
11. Copie .p12 y ca.crt en el equipo del cliente para instalar el cliente y el certificado CA.

> **Nota**
>
> Para instalar certificados en Mozilla Firefox, vaya a *Herramientas* > *Opciones* > *Avanzadas* y seleccione Visualizar certificados en la etiqueta Encryption para importar el archivo client.p12 en la etiqueta Certificados y el archivo ca.crt en la etiqueta Autoridades.

## 9.10.1.1.1 Con CA de confianza

1. Cree un par de claves de servidor, un certificado y un keystore.
   a. Cree un fichero para retener los números de serie de CA ejecutando el código: `Echo 02 >c:\ssl\ca.srl`
   b. Vaya a `C:\Program Files\Java\jre7\bin` y utilice keytool.exe para crear un keystore de servidor, certificado y clave privada.

   > **Nota**
   >
   > En la ubicación de keytool.exe, 'jre7' puede variar según la versión de Java.

   ```
   Keytool.exe –genkey –alias server –keyalg RSA –keysize 2048 –keystore
   c:\ssl\serverkeystore.jks –storetype JKS
   Keytool.exe –certreq –keyalg RSA –alias server –file c:\ssl\server.csr –
   keystore c:\ssl\serverkeystore.jks
   ```

   > **→ Recuerde**
   >
   > Al generar el certificado, introduzca el nombre de host del equipo del servidor cuando se le pida. De lo contrario, obntedrá un error de certificado en el mandante al conectarse.

   c. Introduzca la contraseña del keystore.

   > **→ Recuerde**
   >
   > Necesita editar el servidor de ficheros de solicitud .csr en un editor de texto y modificar «Nuevo inicio de solicitud de certificado» a "Iniciar solicitud de certificado» y «Nuevo fin de solicitud de cambio» a «Finalizar solicitud de certificado».

2. Ejecute el comando para crear un servidor de certificado firmado .crt. `Openssl.exe x509 -CA c:\ssl\ca.pem -cakey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\server.csr -out c:\ssl\server.crt -days 365`
3. Importe el certificado del servidor a un keystore de servidor.

```
Keytool.exe -import -alias server -keystore c:\ssl\serverkeystore.jks -
trustcacerts -file c:\ssl\server.crt
```

4. Ejecute el comando para crear certificados de cliente, client.req y client.key. `Openssl.exe -newkey rsa:2048 -nodes -out c:\ssl\client.req -keyout c:\ssl\client.key -config c:\ssl\sslc.cnf`

> **Nota**
>
> Copie el archivo sslc.cnf de `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86` en C:\SSL y modifique los parámetros:
>
> Dir=c:/ssl # location for everything
>
> Certificate= $dir/ca.pem # CA certificate
>
> Private_key= $dir/ca.key # private key
>
> RANDFILE= $dir/.rand # private random number file

5. Ejecute el comando para firmar el certificado del cliente. `Openssl.exe x509 -CA c:\ssl\ca.pem -CAkey c:\ssl\ca.key -CAserial c:\ssl\ca.srl -req -in c:\ssl\client.req -out c:\ssl\client.pem -days 365`
6. Importe el certificado de cliente en la keystore de confianza con el comando dado abajo. El comando crea trustkeystore.jks.

```
Keytool.exe -import -alias client -keystore c:\ssl\trustkeystore.jks -
trustcacerts -file c:\ssl\client.pem
```

7. Exporte el certificado de cliente con la clave privada de cliente de formato PKCS12 . `Openssl.exe pkcs12 -export -clcerts -in c:\ssl\client.pem -inkey c:\ssl\client.key -out c:\ssl\client.p12 -name "client certificate"`. El comando crea el archivo client.p12.
8. Copie el archivo .p12 en el equipo del cliente para instalarlo.

> **Nota**
>
> Para instalar certificados en Mozilla Firefox, vaya a *Herramientas* > *Opciones* > *Avanzadas* y seleccione Visualizar certificados en la etiqueta Encryption para importar el archivo client.p12 en la etiqueta Certificados y el archivo ca.crt en la etiqueta Autoridades.

## 9.10.1.2 Configuración de servidor SSL Tomcat

### 9.10.1.2.1 Configuración SSL unidireccional

1. Vaya a `<INSTALLDIR>\tomcat\conf\server.xml`

2. Trate la etiqueta XML: `<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" SSLEnabled="true" scheme="https" secure="true">`
```
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></Connector>
```

> **Nota**
>
> La contraseña (contraseña 1) y la ubicación (C:\ssl\serverkeystore.jks) del archivo de keystore que se utilizan en la etiqueta XML de arriba como ejemplo. Puede añadir la contraseña y la ubicación que desee.

3. Grabe el archivo y reinicie el servidor Tomcat.

## 9.10.1.2.2 Configuración SSL bidireccional

Configure el servidor Tomcat para solicitar la autentificación del cliente siguiendo estos pasos:

1. Vaya a `<INSTALLDIR>\tomcat\conf\server.xml`
2. Edite el servidor.xml con el tag xml indicado abajo:
```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
<SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></Connector>
```

> **Nota**
>
> La contraseña (contraseña 1) y la ubicación (C:\ssl\serverkeystore.jks orC:\ssl\trustkeystore.jks) del keystore del servidor y el fichero keystore de confianza se utilizan en el tag xml de arriba como ejemplo. Puede añadir la contraseña y la ubicación que desee.

3. Grabe el archivo y reinicie el servidor Tomcat.

> **Nota**
>
> En Internet Explorer, desactive la opción «No solicitar selección de certificado de cliente si no existen certificados o solo un existe uno» navegando hasta *Opciones de Internet* > *Seguridad* > *Internet local* > *Nivel de certificado de cliente* > *Varios*.

### 9.10.1.3 Configuración de la plataforma de lanzamiento de BI

#### 9.10.1.3.1 Creación de clave de secreto compartido

La clave de secreto compartido se utiliza para definir la confianza entre el mandante y el CMS. Debe configurar el servidor antes que el mandante para Autenticación de confianza.

1. Inicie sesión en CMC.
2. Navegue a la Autentificación y seleccione Empresa.
3. Habilite la autenticación de confianza.
4. Seleccione Nuevo secreto compartido.

   > **Nota**
   >
   > Se genera la clave del secreto compartido y aparece el mensaje de descarga.

5. Seleccione Descargar secreto compartido.
6. Seleccione Grabar en el cuadro de diálogo de descarga y marque uno de los directorios siguientes:
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
   - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`

#### 9.10.1.3.2 Paso de la clave de secreto compartido por el archivo TrustedPrincipal.conf

1. Cree un nuevo archivo de texto en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEBINF\config\custom\directory`.
2. En el archivo nuevo, agregue el texto que se indica a continuación.

```
sso.enabled=true
        trusted.auth.user.retrieval=WEB_SESSION
        trusted.auth.user.param=MyUser
        trusted.auth.shared.secret=MySecret
```

3. Grabe el archivo con el nombre «global.properties».

#### 9.10.1.3.3 Edición del archivo custom.jsp

> **Nota**
>
> Cree un usuario con el nombre del equipo en CMC antes de editar el archivo custom.jsp.

1. Vaya a

a. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *custom.jsp* en *com.businessobjects.webpath.InfoView.jar* para la plataforma de lanzamiento de BI.

b. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.fioriBI* > *web* > *custom.jsp* wn *com.businessobjects.webpath.fioriBI.jar* para la plataforma de lanzamiento de BI.

2. Edite el archivo custom.jsp.

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code
request.getSession().setAttribute("MySecret","<Shared_Secret_Key>")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **Nota**
>
> Deberá sustituir la <Shared_Secret_Key> con la nueva clave disponible en el archivo *TrustedPrincipal.conf*. Consulte Creación de clave de secreto compartido [página 407] para obtener información sobre cómo crear una clave secreta compartida.

## 9.10.1.3.4 Crear el fichero myScript.js

1. Vaya a *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *noCacheCustomResources* y cree myScript.js.
2. Agregue lo siguiente a myScript.js:

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Reinicie el servidor Tomcat.

## 9.10.1.3.5 Configuración de los archivos de propiedades personalizados e internos de BOE

1. Navegue a *<INSTALLDIR>* > *Tomcat* > *webapps* > *BOE* > *WEB-INF* > *internal*
2. Abra el archivo bilaunchpad.properties y modifique las propiedades siguientes:

```
redirection.iframe.1.incoming.url=property.ref.app.url.name
redirection.iframe.1.application=InfoView
redirection.iframe.1.bundle.path=/InfoView
redirection.iframe.1.redirectto.url=/custom.jsp
redirection.iframe.2.incoming.url=property.ref.app.url.name
redirection.iframe.2.incoming.url.suffix=/index.html
redirection.iframe.2.application=InfoView
redirection.iframe.2.bundle.path=/InfoView
redirection.iframe.2.redirectto.url=/custom.jsp
redirection.iframe.9.incoming.url=/InfoView/index.html
redirection.iframe.9.application=InfoView
redirection.iframe.9.bundle.path=/InfoView
redirection.iframe.9.redirectto.url=/custom.jsp
```

3. Reinicie el servidor Tomcat.

## 9.10.1.3.6 Configuración de los archivos Web.xml BOE

1. Vaya a `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`.
2. Edite el archivo web.xml en esta ubicación con el código que se indica a continuación:

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. Añada los parámetros al archivo web.xml siguiendo los pasos que se indican a continuación:
   a. `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`
   b. Añada los parámetros siguientes:

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>New_Shared_Secret_Key</param-value>
</init-param>
```

   c. Repita los pasos navegando a `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.BIPCoreWeb\web\WEB-INF`

> → Sugerencias
>
> Para verificar que ha configurado correctamente la autenticación de confianza, use la siguiente dirección URL para acceder a la aplicación de la plataforma de lanzamiento: http://[cmsname]:8443/BOE/BI/logon.jsp, donde [cmsname] es el nombre del equipo que aloja el CMS.

## 9.10.2 X.509 Autenticación para servicios Web

### 9.10.2.1 Para servicios Web SOAP

#### 9.10.2.1.1 Configuración SSL en Tomcat

En el caso de los servicios Web, debe configurar SSL en Tomcat antes de configurar la plataforma de SAP Business Intelligence.

> ⓘ Nota
>
> Debería existir un usuario en la plataforma BI para conseguir Single Sign-On mediante la autenticación X.509.

1. Vaya a `<INSTALLDIR>\tomcat\conf`.
2. Abra el .xml de servidor en un editor XMLy edite la etiqueta xml:

   ```
   <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
   maxThreads="200" SSLEnabled="true" scheme="https" secure="true">
   <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
   myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
   Connector>
   ```
3. Guarde el archivo.

   > ⓘ Nota
   >
   > La contraseña y la ubicación de los archivos mencionados antes solamente son un ejemplo. Puede añadir la contraseña y la ubicación que desee.

   > ⓘ Nota
   >
   > Puede consultar Creación y configuración de certificados y keystores [página 402] para obtener más información sobre cómo crear y configurar archivos keystore.

#### 9.10.2.1.2 Configuración del archivo axis2.xml

> **Nota**
>
> En Linux o Unix, asegúrese de que el usuario de instalación de BI OS tenga 755 derechos recursivos en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje` antes de realizar los pasos siguientes. Los derechos se otorgan con el comando `chmod -R 755`

1. Vaya `<InstallDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
2. Abra axis2.xml file en cualquier editor XML.
3. Actualice la etiqueta XML con el número de report nuevo para permitir una conexión segura.

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8080</parameter>
</transportReceiver>
<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8443</parameter>
</transportReceiver>
```

> **Nota**
>
> La configuración predeterminada supone que AxisServlet solamente recibe solicitudes mediante http. Para permitir https, debe configurar AxisServletListener con el nombre = "https" y especifique el parámetro de puerta en ambos receptores. Además, puede agregar o eliminar varios números de puerta actualizando las etiquetas XML.

4. Grabe axis2.xml.
5. Reinicie el servidor Tomcat.
6. Inicie el navegador y vaya a https://<dirección IP>:<https puerta>/dswsbobje/services/listServices para validar la conexión segura. Tras navegar al enlace, en la etiqueta Sesión se visualiza trustedLoginWithX509.

## 9.10.2.1.3 Generación de un valor de secreto compartido

1. Lanzar consola de administración central.
2. Vaya a *Autentificación* > *Empresa.*
3. En *Autenticación de confianza*, marque la casilla contra *La autenticación de confianza está activada*.
4. Seleccione *Nuevo secreto compartido*. Se generará la clave de secreto compartido.
5. Seleccione *Descargar secreto compartido* y haga clic en *Actualizar*.
6. Copie el archivo descargado TrustedPrincipal.conf en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin` in Windows.

> **Nota**
>
> Podrá ver el valor de secreto compartido abriendo TrustedPrincipal.conf en cualquier editor de XML.

### 9.10.2.1.4 Configuración del archivo web.xml

1. Vaya a `<Install_DIR>\tomcat\webapps\dswsbobje\WEB-INF.`
2. Abra el .xml de Web en un editor XML y actualice la etiqueta xml con el nombre del equipo host CMS:

```
<context-param>
        <param-name>cms.default</param-name>
        <param-value>EnterHostMachineName</param-value>
    </context-param>
```

3. Agregue la etiqueta XML que se indica a continuación con el valor secreto compartido. Para obtener más información sobre cómo generar un valor de secreto compartido, consulte Generación de un valor de secreto compartido [página 411].

```
<context-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>shared secret value</param-value>
</context-param>
```

4. Grabe el archivo XML Web.

> **Nota**
>
> Las configuraciones definidas en el archivo axis2.xml se descartarán si se actualiza de una versión inferior a BI 4.2 SP04.

### 9.10.2.2 Para servicios Web RESTful

> **Nota**
>
> Debería existir un usuario en la plataforma BI para conseguir Single Sign-On mediante la autenticación X.509.

Verifique el tema Configurar HTTPS/SSL en *Manual de administrador para plataforma de Business Intelligence* para establecer una autenticación segura para servicios web RESTful.

Para establecer la autenticación de confianza utilizando los certificados X.509, tiene que generar una clave secreta compartida. Consulte Generación de un valor secreto compartido en el *Manual del administrador de la plataforma de Business Intelligence* para más información.

Además, para más información acerca del punto final REST SDK, consulte *Referencia API* > *Autenticación* > */v1//logon/trustedx509* en la *Guía del programador de servicios Web RESTfulde plataforma de business intelligence*.

#### 9.10.2.2.1 Autenticación X.509 para los servicios Web RESTful en Tomcat

En la criptografía de clave pública, X.509 es un valor estándar que define los requisitos para un certificado digital seguro. Un certificado X.509 verifica la posesión de la clave pública por un usuario o una identidad de servicios.

Puede activar la autenticación X.509 para los servicios Web RESTful en el servidor de aplicación Tomcat realizando los pasos siguientes:

1. Active SSL en Tomcat. Consulte Configuración SSL en Tomcat [página 410] para obtener más información.
2. Genere una clave de secreto compartido. Consulte Generación de un valor de secreto compartido [página 411] para obtener más información.
3. Abra el archivo de clave de secreto compartido en un editor de texto.
4. Copie la clave de secreto compartido.
5. Edite el archivo *biprws.properties*.
   a. Vaya a `<INSTALLDIR>/tomcat/webapps/biprws/WEB-INF/config/default`.
   b. Abra el archivo *biprws.properties* en un editor de texto.
   c. Busque *Trusted_Auth_Shared_Secret=*.
   d. Pegue la clave de secreto compartido frente al valor *Trusted_Auth_Shared_Secret=*.
   e. Guarde el archivo *biprws.properties*.

### 9.10.3 Autenticación X.509 para CMC

> **Nota**
>
> Debería existir un usuario en la plataforma BI para conseguir Single Sign-On mediante la autenticación X.509.

Puede conseguir un Single Sign-On mediante la autenticación X.509 siguiendo estos pasos:

1. Creación y configuración de certificados y keystores [página 402]
2. Configuración SSL unidireccional [página 405]
3. Configuración SSL bidireccional [página 406]
4. Creación de clave de secreto compartido [página 407]
5. Paso de la clave de secreto compartido por el archivo TrustedPrincipal.conf [página 407]
6. Editar el archivo Custom.jsp (para CMC) [página 414]
7. Crear el archivo myScript.js (para CMC) [página 414]
8. Configuración de los archivos de propiedades personalizados e internos de BOE (para CMC) [página 415]
9. Configuración de los archivos Web.xml BOE (para CMC) [página 415]

## 9.10.3.1 Editar el archivo Custom.jsp (para CMC)

> **Nota**
>
> Cree un usuario con el nombre del equipo en CMC antes de editar el archivo custom.jsp. En un equipo, si existe un usuario, podrá continuar con los siguientes pasos.

1. Vaya a `<INSTALLDIR>\tomcat\webapps\BOE\WEBINF\eclipse\plugins\webpath.CmcApp\web\cutom.jsp` en com.businessobjects.webpath.InfoView.jar.
2. Edite el archivo custom.jsp

```
<\!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code request.getSession().setAttribute("MySecret","Shared
Secret Key")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **Nota**
>
> Debería sustituir el valor secreto compartido en este código con el nuevo valor y el usuario con el nombre del equipo creado en CMC.

## 9.10.3.2 Crear el archivo myScript.js (para CMC)

1. Vaya a `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\noCacheCustomResources y cree myScript.js`.
2. Agregue lo siguiente a myScript.js:

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Reinicie el servidor Tomcat.

### 9.10.3.3 Configuración de los archivos de propiedades personalizados e internos de BOE (para CMC)

1. Navegue a `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\internal\CmcApp.properties`.
2. Abra el archivo CmcApp.properties y agregue los parámetros:

   ```
   sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter,
   trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela,
   trustedX509, sapSSO, sitemindera
   ```

3. Reinicie el servidor Tomcat.

### 9.10.3.4 Configuración de los archivos Web.xml BOE (para CMC)

1. Vaya a `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF`.
2. Edite el archivo web.xml en esta ubicación con el código que se indica a continuación:

   ```
   <init-param>
   <param-name>extendedFrameworkExports</param-name>
   <param-
   value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
   idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
   ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
   bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
   value>
   </init-param>
   ```

3. Añada los parámetros al archivo web.xml siguiendo los pasos que se indican a continuación:
   a. Vaya a `<INSTALLDIR>\tomcat\webapps\BOE\WEB-INF\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`
   b. Añada los parámetros siguientes:

      ```
      <init-param>
      <param-name>trusted.auth.shared.secret</param-name>
      <param-value>Shared_Secret_Key</param-value>
      </init-param>
      ```

   c. Repita los pasos navegando a `<INSTALLDIR>\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.CmcApp\web\WEB-INF\web.xml`

> **Nota**
>
> Para verificar que ha configurado correctamente la autenticación de confianza, use la siguiente dirección URL para acceder a la aplicación de la plataforma de lanzamiento: http://[cmsname]:8443/BOE/BI/logon.jsp, donde [cmsname] es el nombre del equipo que aloja el CMS.

## 9.11 Autenticación de OpenID Connect

Puede habilitar la autenticación de OpenID Connect.

La autenticación de OpenID Connect funciona según el servidor de autenticación (OAuth). Al igual que para el soporte de la unidad en la nube, la autenticación de OpenID Connect también se basa en la configuración del servidor de autenticación. Para obtener más información acerca de la configuración de servidor de autenticación, consulte Configuración del servidor de autorizaciones [página 755].

La autenticación de OpenID Connect se desarrolla sobre la autenticación de Enterprise.

Igual que en el caso de la autenticación SAML, los usuarios deben importarse a la plataforma de BI por adelantado como usuarios Enterprise (secEnterprise).

> **Nota**
>
> Al importar usuarios, debe asegurarse de que el ID de correo electrónico del usuario también esté incluido.

A diferencia de la autenticación SAML, se aplica lo siguiente para la autenticación de OpenID Connect:

- Todas las configuraciones deben realizarse en el back end de la plataforma de BI, no en la capa del servidor de aplicaciones.
- No depende de la autenticación segura.

La autenticación de OpenID Connect solo se admite para la rampa de lanzamiento BI y OpenDocument.

### 9.11.1 Habilitar autenticación OpenID Connect

La autenticación de OpenID Connect solo se admite para la rampa de lanzamiento BI y OpenDocument.

Para obtener información sobre cómo activar la autenticación OpenID Connect, consulte Configuración de la autenticación Enterprise [página 242]. Después de activar la autenticación OpenID Connection en el plug-in de autenticación Enterprise en el back end, tendrá que activar la misma capa de aplicación para las aplicaciones compatibles (por ejemplo, el archivo `FioriBI.properties` para la rampa de lanzamiento BI y el archivo `OpenDocument.properties` para las aplicaciones de OpenDocument en `WEB-INF/config/custom`.

Para activar el workflow de autenticación SSO web, fije `logon.webssoauthentication.framework` en `OpenId`.

Fije `openid.restful.url` en la URL de servicios web RESTful de la infraestructura (por ejemplo, `https://<server>:8443/biprws`).

Puede iniciar sesión en la rampa de lanzamiento BI mediante OpenID utilizando la URL `…/BO/BI`. Sin embargo, una vez que inicie sesión con la autenticación OpenID Connect en la rampa de lanzamiento BI, podrá ver que la ruta de contexto de reserva-espacio "WEBSSO" se añadirá a la URL. Se mantendrá en la ruta de URL incluso después de cerrar sesión. Si desea volver a iniciar sesión desde la misma ventana con la misma URL, tendrá que eliminar "WEBSSO" de la URL del navegador.

# 10 Referencia a origen de datos:

## 10.1 Asignación de credenciales mejorada

En BI 4.2.X y versiones anteriores, un administrador puede guardar solo un conjunto de credenciales de base de datos para cada usuario de CMC.

Esta funcionalidad requiere que el administrador actualice las mismas credenciales para todas las diferentes bases de datos. De BI 4.3 en adelante, puede guardar varios conjuntos de credenciales de base de datos para cada usuario mediante referencias de fuente de datos.

> ⓘ Nota
>
> La función de asignación de credenciales mejorada introducida en la plataforma SAP BusinessObjects Business Intelligence 4.3 solo es compatible con la herramienta de diseño de información. La herramienta de diseño de universos no admite la asignación de credenciales mejorada.

### Referencia de fuente de datos en CMC

Un administrador crea una referencia de fuente de datos en la plataforma de BI. Esta referencia de origen de datos se utiliza en las propiedades de usuario donde el administrador define un conjunto de credenciales de base de datos frente a él. Esta referencia de fuente de datos se utiliza como parte de la asignación de credenciales que es un modo de autenticación disponible en las conexiones.

El administrador obtiene una opción para seleccionar la referencia de fuente de datos que desee cuando se seleccione la Asignación de credenciales como modo de autenticación. De forma similar, un administrador puede crear varias referencias de origen de datos si tienen varias bases de datos que se conectan a la plataforma de BI y definir credenciales únicas para cada usuario.

> ⓘ Nota
>
> Cuando importa usuarios a través de un archivo CSV, anime a los usuarios a usar la herramienta de gestión de promociones o cuando selecciona sincronizar las credenciales del origen de datos durante el inicio de sesión para Enterprise, LDAP, Windows AD, los tipos de autenticación de Windows, la plataforma de BI asigna las credenciales de base de datos a la referencia de origen de datos predeterminada.

### Referencia de fuente de datos en la rampa de lanzamiento BI

Ahora también están disponibles las referencias a fuentes de datos en la rampa de lanzamiento BI, donde puede actualizar y asignar sus credenciales de usuario.

> **Nota**
>
> No puede editar los detalles de *Referencia a fuente de datos*, pero puede editar los campos *Nombre de cuenta*, *Contraseña* y *Confirmar contraseña*.

### Funcionamiento

Supongamos que:

- Estas dos referencias de origen de datos están disponibles en la plataforma de BI, por ejemplo, DSR1 para la base de datos de ventas y DSR2 para la base de datos financiera.
- Cada referencia de origen de datos tiene credenciales de base de datos definidas en las propiedades de usuario de Usuario A
- Hay dos conexiones CN1 y CN2 que están configuradas para utilizar la asignación de credenciales como el modo de autenticación.
- DSR1 está asociada a la conexión CN1 y también DSR2 está asociada a CN2.

Ahora, si un usuario A intenta actualizar un informe que requiere acceso a la base de datos de ventas, entonces la plataforma de BI busca la DSR1 en las propiedades de usuario y consume las credenciales de base de datos definidas contra DSR1 para establecer una conexión.

Para utilizar una referencia de fuente de datos, debe completar las tareas siguientes.

1. Crear una referencia de fuente de datos [página 418]
2. Definir las credenciales de la base de datos para una referencia de fuente de datos para un usuario en CMC [página 419]
3. Asociar referencia de fuente de datos en conexión OLAP [página 420]

> **Nota**
>
> También es posible configurar la Asignación de credenciales para conexiones relacionales y conexiones OLAP en la herramienta de diseño de información.

## 10.1.1 Crear una referencia de fuente de datos

Una referencia de fuente de datos actúa como una variable que un administrador crea en la plataforma de BI para guardar un conjunto único de credenciales de base de datos para cada usuario. Siga los pasos siguientes para crear una referencia de fuente de datos.

1. Inicie la sesión en la CMC.
2. En Definir, vaya a Referencias de fuente de datos.
3. Seleccione el icono (Crear referencia de fuente de datos nueva).
4. Añada el título de la referencia de fuente de datos y una descripción.
5. Seleccione OK.

Ha creado correctamente una referencia de fuente de datos.

## 10.1.2 Definir las credenciales de la base de datos para una referencia de fuente de datos para un usuario en CMC

Una referencia de fuente de datos debe tener una credencial de base de datos definida en las propiedades de usuario para permitir que este se conecte a una base de datos. Para definir las credenciales de base de la datos, siga estos pasos en CMC:

1. Inicie la sesión en la CMC.
2. Vaya a *Usuarios y grupos*.
3. Abra el menú contextual de un usuario desde la *Lista de usuarios*.
4. Vaya a *Propiedades* y seleccione *Añadir* en *Credenciales de fuente de datos*.
5. Seleccione la referencia de fuente de datos preferida.
6. Introduzca los valores para *Nombre de la cuenta*, *Contraseña* y *Confirmar contraseña*.
7. Repita el proceso del paso 4 para añadir otra referencia de fuente de datos.
8. Seleccione *Guardar y cerrar*.

   Ha definido correctamente las credenciales de la base de datos para una referencia de fuente de datos.

## 10.1.3 Definir las credenciales de la base de datos para una referencia de fuente de datos para un usuario en la rampa de lanzamiento BI

Una referencia de fuente de datos debe tener una credencial de base de datos definida en las propiedades de usuario para permitir que este se conecte a una base de datos.

Ahora también están disponibles las referencias a fuentes de datos en la rampa de lanzamiento BI, donde puede actualizar y asignar sus credenciales de usuario. Las credenciales de la base de datos se sincronizan entre CMC y la rampa de lanzamiento BI.

Para definir las credenciales de base de la datos, siga estos pasos en la rampa de lanzamiento BI:

1. Iniciar sesión en la rampa de lanzamiento BI
2. Vaya a (Opciones de usuario), haga clic en la opción (*Opciones*) desde el menú desplegable.

   Se visualiza la ventana *Opciones*.
3. Haga clic en *Cuenta de usuario (administrador)*.

   La página de Cuenta de usuario se abre con dos fichas: *Información de cuenta*, *Credenciales de base de datos* y *Tokens de autorización*.
4. Haga clic en *Credenciales de base de datos*.

   Puede ver los datos sincronizados del usuario desde la CMC que se muestra aquí.

   > **Nota**
   >
   > No puede editar los detalles de *Referencia de la fuente de datos*.
   >
   > Pero puede editar los campos *Nombre de cuenta*, *Contraseña* y *Confirmar contraseña*.

Al cambiar la contraseña, se mostrará un mensaje de aviso en la pantalla *Los cambios de algunas preferencias se aplicarán después de que se vuelva a cargar la página*.

5. Haga clic en *Guardar* y *Cerrar* para guardar las modificaciones de credenciales asignadas.

## 10.1.4 Definir las credenciales de la base de datos para una referencia de fuente de datos para un grupo

Una referencia de fuente de datos debe tener una credencial de base de datos definida en las propiedades de usuario para permitir que este se conecte a una base de datos.

> **Nota**
>
> Esta tarea no actualiza las referencias de fuente de datos para los miembros de los subgrupos. Puede seguir los mismos pasos para que el subgrupo actualice las referencias de fuente de datos para sus miembros.

Para definir las credenciales de base de la datos, siga estos pasos:

1. Inicie la sesión en la CMC.
2. Vaya a *Usuarios y grupos*.
3. Abra el menú contextual de un grupo de usuarios y seleccione *Gestor de cuentas*.
4. Marque la casilla de selección para *Credenciales de base de datos* y luego seleccione *Añadir*.
5. Introduzca los valores en los campos obligatorios.
6. Seleccione *Guardar y cerrar*.

Ha definido correctamente una referencia de fuente de datos nueva con las credenciales para la base de datos para los miembros del grupo de usuarios. Puede ir a las *Propiedades* de cualquier usuario de este grupo de usuarios para verificar la referencia de fuente de datos que acaba de actualizar.

## 10.1.5 Asociar referencia de fuente de datos en conexión OLAP

Un administrador obtiene una opción para seleccionar la referencia de fuente de datos que desee cuando se seleccione la Asignación de credenciales como modo de autenticación para una conexión.

Siga los pasos siguientes para asociar una referencia de fuente de datos a una conexión.

1. Inicie la sesión en la CMC.
2. Vaya a *Conexiones OLAP*.
3. Abra una conexión existente o cree una conexión nueva.
4. En el campo *Autenticación*, seleccione *Asignación de credenciales*.
   Aparece el campo *Referencia de fuente de datos*.
5. Elija una referencia de fuente de datos

6. Introduzca los demás detalles necesarios y seleccione *Guardar*.

Ha asociado correctamente una referencia de fuente de datos en una conexión OLAP.

# 11 Administración del servidor

## 11.1 Uso del área de administración Servidores de la CMC

El área de administración Servidores de la CMC es la herramienta principal para las tareas de administración de servidores. Proporciona una lista de todos los servidores del despliegue. Para la mayoría de las tareas de administración y configuración, debe seleccionar un servidor de la lista y elegir un comando del menú Administrar o Acción.

### Acerca del árbol de navegación

El árbol de navegación de la parte izquierda del área de administración Servidores proporciona una serie de formas de ver la lista Servidores. Seleccione elementos en el árbol de navegación para cambiar la información mostrada en el panel *Detalles*.

| Opción del árbol de navegación | Descripción |
|---|---|
| *Lista de servidores* | Muestra una lista completa de todos los servidores del despliegue. |
| *Lista de grupos de servidores* | Muestra una lista sin formato de todos los grupos de servidores disponibles en el panel Detalles. Seleccione esta opción si desea configurar las opciones o la seguridad de varios grupos de servidores. |
| *Grupos de servidores* | Enumera los grupos de servidores y los servidores de cada grupo de servidores. Al seleccionar un grupo de servidores, sus servidores y grupos de servidores se muestran en el panel Detalles en una vista jerárquica. |
| *Nodos* | Muestra una lista de los nodos del despliegue. Los nodos se configuran en el CCM. Puede seleccionar un nodo haciendo clic en él para ver o administrar los servidores del nodo. |

| Opción del árbol de navegación | Descripción |
| --- | --- |
| *Categorías de servicio* | Proporciona una lista de los tipos de servicios que puede haber en el despliegue. Las categorías de servicio están divididas en servicios de la plataforma de BI principales y servicios asociados con componentes específicos de SAP BusinessObjects. Las categorías de servicio incluyen:<br>• *Servicios de conectividad*<br>• *Servicios principales*<br>• *Servicios de Crystal Reports*<br>• *Servicios de federación de datos*<br>• *Servicios de administración de promociones*<br>• *Servicios de análisis*<br>• *Servicios de Web Intelligence*<br>Seleccione una categoría de servicio en la lista de navegación para ver o administrar los servidores de la categoría.<br>**Nota**<br>Un servidor puede alojar servicios que pertenezcan a varias categorías de servicio. Por consiguiente, un servidor puede aparecer en varias categorías de servicio. |
| *Estado del servidor* | Muestra los servidores según su estado actual. Es una herramienta valiosa para comprobar los servidores que están en ejecución o detenidos. Si el sistema tiene un rendimiento lento, por ejemplo, puede usar la lista *Estado del servidor* para determinar rápidamente si alguno de los servidores tiene un estado anómalo. Los posibles estados de servidor son los siguientes:<br>• *Detenido*<br>• *Iniciando*<br>• *Inicializando*<br>• *En ejecución*<br>• *Deteniendo*<br>• *En ejecución con errores*<br>• *Error*<br>• *Esperando recursos* |

## Acerca del árbol Detalles

Según las opciones que ha seleccionado en el árbol de navegación, el panel *Detalles* de la parte derecha del área de administración Servidores muestra una lista de servidores, grupos de servidores, estados, categorías o nodos. En la tabla siguiente se describe la información enumerada para servidores en el panel *Detalles*.

> **Nota**
>
> Para nodos, grupos de servidores, categorías y estados, el panel *Detalles* normalmente muestra los nombres y las descripciones.

| Columna de panel Detalles | Descripción |
|---|---|
| *Nombre de servidor* o *Nombre* | Muestra el nombre del servidor. |
| *Estado* | Muestra el estado actual del servidor. Puede ordenar por estado de servidor con la lista *Estado del servidor* en el árbol de navegación. Los posibles estados de servidor son los siguientes:<br>• *Detenido*<br>• *Iniciando*<br>• *Inicializando*<br>• *En ejecución*<br>• *Deteniendo*<br>• *En ejecución con errores*<br>• *Error*<br>• *Esperando recursos* |
| *Activado* | Muestra si el servidor está activado o desactivado. |
| *Bloqueado* | Si el servidor está marcado como *Bloqueado*, requiere un reinicio. Por ejemplo, si cambia determinados ajustes de servidor en la pantalla *Propiedades* del servidor, debe reiniciar el servidor para que los cambios surtan efecto. |
| *Clase* | Muestra el tipo de servidor. |
| *Nombre de host* | Muestra el nombre de host del servidor. |
| *Condición* | Indica el estado general del servidor.<br>Los posibles estados de servidor son los siguientes:<br>• *Verde* (positivo)<br>• *Ámbar* (precaución)<br>• *Rojo* (peligro)<br>El estado de un servidor depende directamente del estado de la vigilancia del servidor. Por ejemplo, el estado del servidor de administración central depende del estado de `<NODENAME>.CentralManagementServer Watch`.<br>Puede acceder a los detalles de las vigilancias en la página *Supervisión* de la CMC: en la pestaña *Lista de vigilancia*, seleccionar la vigilancia y hacer clic en *Editar*. Verá la *Regla de precaución* y la *Regla de peligro* de la vigilancia, que se asignan a los estados de alerta ámbar y roja, respectivamente. |
| *PID* | Muestra el número ID de proceso único del servidor. |

| Columna de panel Detalles | Descripción |
| --- | --- |
| *Descripción* | Muestra una descripción del servidor. Puede cambiar esta descripción en la página *Propiedades* del servidor. |
| *Fecha de modificación* | Muestra la fecha en la que se ha modificado por última vez el servidor o cuando se cambió el estado del servidor. Esta columna resulta muy útil si desea comprobar el estado de los servidores cambiados recientemente. |

## 11.2 Administrar servidores con el uso de secuencias de comandos en Windows

El ejecutable `ccm.exe` permite iniciar, detener, reiniciar, habilitar y deshabilitar los servidores en el despliegue de Windows a través de la línea de comandos.

### Información relacionada

ccm.exe [página 1108]

## 11.3 Administración de servidores en Unix

El ejecutable `ccm.sh` permite iniciar, detener, reiniciar, habilitar y deshabilitar los servidores en el despliegue de Unix a través de la línea de comandos.

### Información relacionada

ccm.sh [página 1100]

## 11.4 Visualizar y cambiar el estado del servidor

### 11.4.1 Visualizar el estado de servidores

El estado de un servidor es el que tiene en el momento en que se ejecuta: un servidor se puede ejecutar, iniciar, detener, detenido, con errores, o esperando recursos. Para que un servidor responda a las solicitudes de la

plataforma de BI, debe estar ejecutándose y habilitado. Un servidor que está deshabilitado sigue ejecutándose como un proceso; sin embargo, no acepta solicitudes del resto de la plataforma de BI. Un servidor que está detenido ya no se ejecuta como un proceso.

En esta sección se muestra cómo modificar el estado de los servidores mediante la CMC.

### Información relacionada

Para ver el estado de un servidor [página 426]
Ver el estado de los servicios [página 426]
Iniciar, detener y reiniciar servidores [página 427]
Habilitar y deshabilitar servidores [página 430]
Detener un Servidor de administración central (CMS) [página 429]
Iniciar automáticamente un servidor [página 429]

## 11.4.1.1 Para ver el estado de un servidor

1. Vaya al área de administración *Servidores* de CMC.

   El panel *Detalles* muestra las categorías del servicio del despliegue.
2. Para ver una lista de servidores en un Grupo de servidores, Nodo o Categoría de servicio determinado, haga clic en el grupo de servidor, el nodo o la categoría, en el árbol de navegación.
   El panel *Detalles* muestra la lista de servidores del despliegue. La columna *Estado* proporciona el estado de cada servidor de la lista.
3. Si desea ver una lista de todos los servidores que actualmente tienen un determinado estado, expanda la opción *Estado del servidor* en el árbol de navegación y seleccione el estado que desee.

   En el panel Detalles aparecerá una lista de los servidores con el estado seleccionado.

   > **Nota**
   >
   > Esto puede resultar muy útil si necesita ver rápidamente una lista de servidores que no se están iniciando correctamente o que se han detenido de un modo inesperado.

## 11.4.1.2 Ver el estado de los servicios

Si algún servicio falla, el estado del servidor host se establece en *En ejecución con errores* (lo que significa que como mínimo un servicio se ha iniciado correctamente) o *Erróneo* (lo que significa que ninguno de los servicios se ha iniciado correctamente). Puede ver los estados del servidor en la CMC y el CCM. Sin embargo, también puede ver el estado de servicios individuales, en la página del servidor *Propiedades* en la CMC.

1. Vaya al área de administración *Servidores* de la CMC.

   El panel *Detalles* muestra las categorías del servicio del despliegue.

2. Para ver una lista de servidores en un Grupo de servidores, Nodo o Categoría de servicio determinado, haga clic en el grupo de servidor, el nodo o la categoría, en el árbol de navegación.
   El panel *Detalles* muestra la lista de servidores del despliegue.
3. Haga doble clic en un servidor para abrir su página *Propiedades*.

   La página *Propiedades* muestra las propiedades del servidor y los servicios que aloja. Para servicios fallidos, también se muestran los mensajes de error.

### Información relacionada

Visualizar el estado de servidores [página 425]

## 11.4.2 Iniciar, detener y reiniciar servidores

Iniciar, detener y reiniciar servidores son acciones comunes que se realizan al configurar servidores o dejarlos sin conexión. Por ejemplo, si desea cambiar el nombre de un servidor, en primer lugar debe detener el servidor. Una vez realizados los cambios, debe iniciarlo de nuevo para que los cambios surtan efecto. Si realiza cambios en los valores de configuración de un servidor, la CMC le preguntará si necesita reiniciar el servidor.

En lo que queda de esta sección se indica cuándo un cambio de configuración determinado hace necesario que primero detenga o reinicie el servidor. Sin embargo, debido a que estas tareas se producen con frecuencia, se explican primero los conceptos y las diferencias, y los procedimientos generales se ofrecen como referencia.

| Acción | Descripción |
|---|---|
| Detener un servidor | Es posible que deba detener los servidores de la plataforma de BI antes de que pueda modificar ciertas propiedades y configuraciones. |
| Iniciar un servidor | Si detiene un servidor para configurarlo, será necesario reiniciarlo para que surtan efecto los cambios y para que el servidor retome las solicitudes de procesamiento. |
| Reiniciar un servidor | Reiniciar un servidor es un acceso directo que equivale a detenerlo por completo y, a continuación, iniciarlo de nuevo. Si necesita reiniciar un servidor después de cambiar una configuración, la CMC se lo solicitará. |
| Inicio de un servidor automáticamente | Puede configurar los servidores para que se inicien automáticamente cuando se inicie Server Intelligence Agent. |
| Forzar terminación | Detiene un servidor inmediatamente (mientras que al detener un servidor, lo hará cuando haya terminado las actividades de procesamiento actuales). Forzar a que un servidor finalice sólo cuando no se puede detener el servidor y debe detener el servidor inmediatamente. |

→ Sugerencias

Cuando se detiene (o reinicia) un servidor, se pone fin a su proceso, deteniendo de este modo el servidor por completo. Antes de detener un servidor, se recomienda que:

- Deshabilite el servidor, de modo que pueda finalizar el procesamiento de las tareas en curso, y
- Se asegure de que no existen eventos de auditoría en la cola. Para ver el número de eventos de auditoría restantes en la cola, desplácese hasta la pantalla *Métrica* del servidor y visualice la métrica *Número actual de eventos de auditoría en cola*.

### Información relacionada

Habilitar y deshabilitar servidores [página 430]

## 11.4.2.1 Iniciar, detener o reiniciar servidores con la CMC

1. Vaya al área de administración *Servidores* de CMC.

   El panel *Detalles* muestra las categorías del servicio del despliegue.
2. Para ver una lista de servidores en un grupo de servidores, nodo o categoría de servicios concreto, seleccione el grupo, nodo o categoría en el panel de navegación.
   El panel *Detalles* muestra una lista de servidores.
3. Si desea ver una lista de todos los servidores que actualmente tienen un determinado estado, expanda la opción *Estado del servidor* en el árbol de navegación y seleccione el estado que desee.

   Aparece una lista de servidores con el estado seleccionado en el panel *Detalles*.

   ⓘ Nota

   Esto puede resultar muy útil si necesita ver rápidamente una lista de servidores que no se están iniciando correctamente o que se han detenido de un modo inesperado.
4. Haga clic con el botón derecho en el servidor cuyo estado desea cambiar y, dependiendo de la acción que deba realizar, seleccione *Iniciar servidor*, *Reiniciar servidor*, *Detener servidor* o *Forzar el cierre*.

## 11.4.2.2 Para iniciar, detener o reiniciar un servidor de Windows con CCM

1. En el CCM, haga clic en el botón *Administrar servidores* en la barra de herramientas.
2. Cuando se le indique, conéctese con el CMS con la cuenta administrativa.
3. En el cuadro de diálogo *Administrar servidores*, seleccione el servidor que desea iniciar, detener o reiniciar.
4. Haga clic en *Inicio*, *Detener*, *Reiniciar* o *Forzar el cierre*.

5. Haga clic en *Cerrar* para volver al CCM.

### 11.4.2.3 Iniciar automáticamente un servidor

De forma predeterminada, los servidores del despliegue se inician automáticamente cuando se inicia Server Intelligence Agent. Esta tarea muestra dónde definir la opción de inicio automático.

1. Vaya al área de administración *Servidores* de la CMC.
2. Seleccione el servidor que desee iniciar automáticamente.
   Aparecerá la pantalla *Propiedades*.
3. En *Configuración común*, seleccione la casilla de verificación *Iniciar automáticamente este servidor cuando se inicie Agente de inteligencia de servidor* y haga clic en *Guardar* o *Guardar y cerrar*.

> **Nota**
>
> Si la casilla de selección *Iniciar automáticamente este servidor cuando se inicie Agente de inteligencia de servidor* está desmarcada para cada CMS del clúster, tiene que usar el CCM para reiniciar el sistema. Después de utilizar el CCM para detener el SIA, haga clic con el botón derecho en el SIA y seleccione *Propiedades*. En la ficha *Inicio*, haga clic en *Propiedades* para abrir la página Propiedades del servidor para el CMS. Seleccione *Inicio automático* y, a continuación, haga clic en *Aceptar* para cerrar la página Propiedades del servidor y, a continuación, vuelva a hacer clic en *Aceptar*. Reinicie el SIA. La opción de *inicio automático* solo está disponible cuando la casilla de selección *Iniciar automáticamente este servidor cuando se inicie Agente de inteligencia de servidor* está desmarcada para cada CMS del clúster.

## 11.4.3 Detener un Servidor de administración central (CMS)

Si la instalación de la plataforma de BI tiene varios servidores de administración central (CMS) activos, puede cerrar un solo CMS sin perder datos o sin que se vea afectada la funcionalidad del sistema. Otro CMS del nodo asumirá la carga de trabajo del servidor detenido. La agrupación en clúster de varios CMS permite realizar el mantenimiento de cada Servidor de administración central por turnos sin que deje de funcionar la plataforma de BI.

No obstante, si el despliegue de la plataforma de BI dispone de un solo CMS, al cerrarlo no estará disponible para los usuarios y se interrumpirá el procesamiento de informes y programas. Para evitar este problema, Agente de inteligencia de servidor por cada nodo garantiza que al menos un CMS se está ejecutando en todo momento. Puede detener un CMS si detiene su SIA, pero antes de detener el SIA, debe deshabilitar los servidores de procesamiento mediante la CMC, de modo que pueden finalizar cualquier tarea en curso antes de que se cierre la plataforma de BI porque el resto de servidores del nodo también se cerrarán.

> **Nota**
>
> Puede encontrarse en situaciones donde el CMS se ha detenido y necesita reiniciar el sistema desde el CCM. Por ejemplo, si cierra cada CMS de un nodo y la casilla *Iniciar automáticamente este servidor al iniciar el Agente de inteligencia de servidor* no está seleccionada para cada CMS del clúster al iniciar el SIA, debe usar el CCM para reiniciar el sistema. En el CCM, haga clic con el botón derecho en el SIA y elija *Propiedades*. En la ficha *Inicio*, haga clic en *Propiedades* para abrir la página Propiedades del servidor

para el CMS. Seleccione *Inicio automático* y, a continuación, haga clic en *Aceptar* para cerrar la página Propiedades del servidor y, a continuación, vuelva a hacer clic en *Aceptar*. Reinicie el SIA. La opción *Inicio automático* solo está disponible cuando la casilla *Iniciar automáticamente este servidor al iniciar el Agente de inteligencia de servidor* no está seleccionada para ningún CMS del clúster.

Si desea configurar el sistema de modo que pueda iniciar y detener el Servidor de administración central en el clúster sin tener que iniciar y detener otros servicios, coloque el CMS en un nodo independiente. Cree un nuevo nodo y clone el CMS en el nodo. Con el CMS en su propio nodo, puede cerrar fácilmente el nodo sin que se vean afectados los demás servidores.

### Información relacionada

Uso de nodos [página 474]
Clonación de servidores [página 432]
Agrupar Servidores de administración central [página 435]

## 11.4.4 Habilitar y deshabilitar servidores

Al deshabilitar un servidor de la plataforma de BI, se impide que reciba y responda a nuevas solicitudes de la plataforma de BI pero, en realidad, no detiene el funcionamiento del servidor. Esto resulta útil si desea permitir que un servidor finalice el procesamiento de todas las solicitudes en curso antes de detenerlo por completo.

Por ejemplo, desea detener un Servidor de tareas antes de reiniciar el equipo en el que se está ejecutando. Sin embargo, desea permitir que el servidor complete todas las solicitudes de informes pendientes que están en la cola. En primer lugar, deshabilite el Servidor de tareas para que no acepte más solicitudes. A continuación, vaya a la Consola de administración central (CMC) para supervisar cuándo termina el servidor las tareas que tiene en curso. (Desde el área de administración de *Servidores*, haga clic con el botón derecho en el servidor y seleccione *Métrica*.) A continuación, una vez finalizado el procesamiento de las solicitudes en curso, puede detener el servidor con tranquilidad.

> **Nota**
>
> CMS debe estar en funcionamiento para poder habilitar y/o deshabilitar otros servidores.

> **Nota**
>
> Un CMS no se puede activar o desactivar.

### 11.4.4.1 Habilitar y deshabilitar servidores con la CMC

1. Vaya al área de administración *Servidores* de CMC.
2. Haga clic con el botón derecho en el servidor cuyo estado desea cambiar y, dependiendo de la acción que desee realizar, haga clic en *Habilitar servidor* o *Deshabilitar servidor*.

### 11.4.4.2 Para habilitar o deshabilitar un servidor de Windows con CCM

1. En el CCM, haga clic en *Administrar servidores*.
2. Cuando se le indique, inicie sesión en el CMS con las credenciales que le proporcionan privilegios administrativos para la plataforma de BI.
3. En el cuadro de diálogo *Administrar servidores*, seleccione el servidor que desea habilitar o deshabilitar.
4. Haga clic en *Habilitar* o *Deshabilitar*.
5. Haga clic en *Cerrar* para volver al CCM.

## 11.5 Agregar, clonar o eliminar servidores

## 11.5.1 Adición, clonación y eliminación de servidores

Si desea agregar hardware nuevo a la plataforma de BI mediante la instalación de componentes de servidor en nuevos equipos adicionales, ejecute el programa de instalación de la plataforma de BI en dichos equipos.
El programa de instalación permite llevar a cabo una instalación personalizada. Durante la instalación personalizada, especifique el CMS del despliegue existente y seleccione los componentes que desee instalar en el equipo local. Para obtener información detallada de las opciones de instalación, consulte el *Manual de instalación de la plataforma SAP BI*.

### 11.5.1.1 Adición de un servidor

Puede ejecutar varias instancias del mismo servidor de la plataforma de BI en el mismo equipo. Para agregar un servidor:

1. Vaya al área de administración *Servidores* de CMC.
2. En el menú *Administrar*, haga clic en *Nuevo* > *Nuevo servidor*.
   Aparece el cuadro de diálogo *Crear nuevo servidor*.
3. Elija la *categoría de servicio*.
4. Seleccione el tipo de servicio que necesita de la lista *Seleccionar servicio* y, a continuación, haga clic en *Siguiente*.
5. Para agregar un servicio adicional al servidor, seleccione el servicio en la lista *Servicios adicionales disponibles* y haga clic en >.

   > **Nota**
   >
   > Los servicios adicionales no están disponibles para todos los tipos de servidor.

6. Después de agregar los servicios adicionales que desee, haga clic en *Siguiente*.
7. Si la arquitectura de la plataforma de BI se compone de varios nodos, seleccione el nodo en el que desea agregar el nuevo servidor en la lista *Nodo*.

8. Escriba un nombre para el servidor en el cuadro *Nombre de servidor*.

   Cada servidor del sistema debe tener un nombre único. La convención de nomenclatura predeterminada es `<NODENAME>.<servertype>`(se agrega un número si hay varios servidores del mismo tipo en el mismo equipo host).
9. Para incluir una descripción para el servidor, escríbala en el cuadro *Descripción*.
10. Si agrega un nuevo Servidor de administración central, especifique un número de puerto en el campo *Puerto del servidor de nombres*.
11. Haga clic en *Crear*.
    El nuevo servidor aparecerá en la lista de servidores del área *Servidores* de la CMC, pero no se inicia ni habilita.
12. Use la CMC para iniciar y habilitar el nuevo servidor cuando desee que empiece a responder a las solicitudes de la plataforma de BI.

## 11.5.1.2 Clonación de servidores

Si desea agregar una nueva instancia de servidor al despliegue, puede clonar un servidor existente. El servidor clonado conserva las opciones de configuración del servidor regional, excepto Configuración común y Parámetros de la línea de comandos. Esto puede resultar muy útil si se expande el despliegue y se desean crear nuevas instancias de servidor que utilicen prácticamente los mismos valores de configuración que un servidor existente.

La clonación también simplifica el proceso de trasladar servidores de un nodo a otro. Si desea mover un CMS existente a otro nodo, puede clonarlo en el nuevo nodo. El CMS clonado aparece en el nuevo nodo y conserva toda la configuración del CMS original, excepto Configuración común y Parámetros de la línea de comandos.

Hay varias consideraciones que se deben tener en cuenta al clonar servidores. Es posible que no desee que se clonen todos los valores, por lo que constituye una buena práctica comprobar el servidor clonado para asegurarse de que satisface sus necesidades.

> **Nota**
>
> Antes de clonar servidores, asegúrese de que todos los equipos del despliegue tienen la misma versión de la plataforma de BI (y cualquier actualización, si procede).

> **Nota**
>
> Puede clonar servidores desde cualquier equipo. No obstante, sólo puede clonar servidores en equipos donde están instalados los binarios necesarios para el servidor.

> **Nota**
>
> Cuando clona un servidor, no necesariamente significa que el nuevo servidor usará las mismas credenciales de sistema operativo. La cuenta de usuario se controla mediante el Agente de inteligencia de servidor en el que se ejecuta el servidor.

## 11.5.1.2.1 Utilizar marcadores de posición para la configuración de servidor

Los marcadores de posición son variables de nivel de nodo que usan los servidores que se ejecutan en el nodo. Los marcadores de posición se enumeran en una página dedicad de la Consola de administración central (CMC). Al hacer doble clic en cualquier servidor enumerado en *Servidores* en la CMC, se proporciona un vínculo en el panel de exploración izquierdo para «Marcadores de posición». La página *Marcadores de posición* enumera todos los nombres de marcadores de posición y sus valores asociados para el servidor seleccionado. Los marcadores de posición contienen valores de sólo lectura y sus nombres empiezan por un carácter de porcentaje %.

> **Nota**
>
> Siempre se puede sobrescribir una configuración de marcador de posición con una cadena específica en la página *Propiedades* del servidor de CMC.

### Ejemplo

Los marcadores de posición resultan útiles al clonar servidores. Por ejemplo, el equipo de varios controladores A dispone de la plataforma de BI instalada en`C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0` . De modo que el marcador de posición `%DefaultAuditingDir%` será `D:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

En otro equipo, el equipo B, solo existe un controlador de disco (sin controlador D) y la plataforma de BI está instalada en `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0.` En este caso, el marcador de posición `%DefaultAuditingDir%` será `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\`.

Para clonar el servidor de evento del equipo A al equipo B, si se utilizan marcadores de posición para el directorio temporal de auditoría, se resolverán los marcadores de posición y el servidor de eventos funcionará correctamente. Si no se utilizan marcadores de posición, se producirá un error en el servidor de eventos a menos que se sobrescriba manualmente la configuración Directorio temporal de auditoría.

## 11.5.1.2.2 Para clonar un servidor

1. En el equipo en el que desee agregar el servidor clonado, vaya al área de administración *Servidores* de la CMC.
2. Haga clic con el botón derecho en el servidor que desee clonar y seleccione *Clonar servidor*.
   Aparecerá el cuadro de diálogo *Clonar servidor*.
3. Escriba un nombre para el servidor (o use el nombre predeterminado) en el campo *Nombre del servidor*.
4. Si está clonando un Servidor de administración central, especifique un número de puerto en el campo *Puerto del servidor de nombres*.

5. En la lista *Clonar a nodo*, elija el nodo donde desee agregar el servidor clonado y, a continuación, haga clic en *Aceptar*.
   El nuevo servidor aparecerá en el área de administración *Servidores* de la CMC.

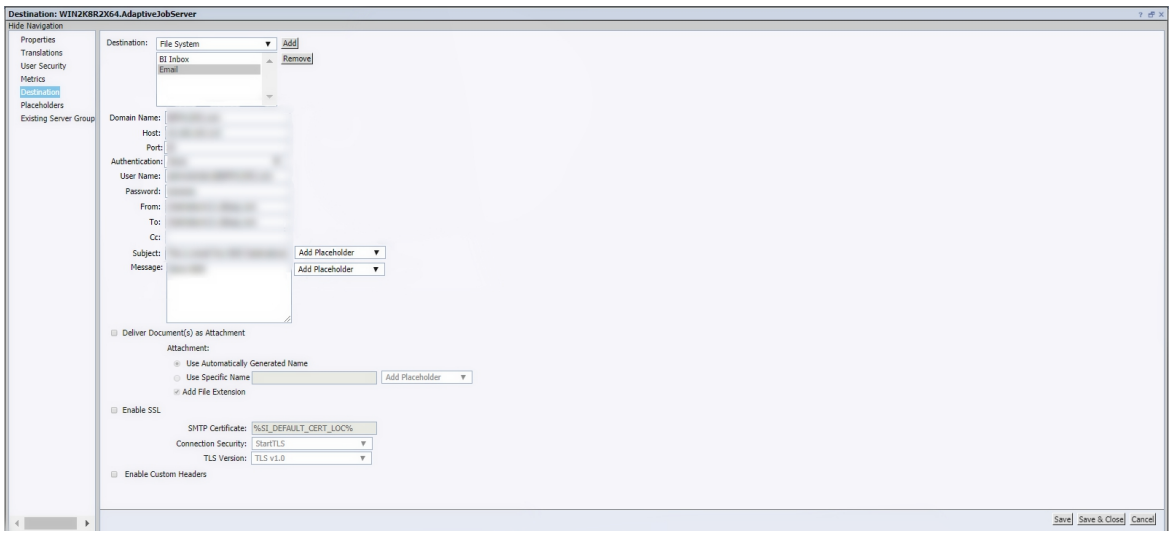
### 11.5.1.3 Eliminación de un servidor

1. Vaya al área de administración *Servidores* de CMC.
2. Detenga el servidor que desee eliminar.
3. Haga clic con el botón derecho en el servidor y seleccione *Eliminar*.
4. Cuando se le pida confirmación, haga clic en *Aceptar*.

## 11.6 Agregar cabeceras de internet personalizadas

La cabecera de internet de un mensaje de correo electrónico incluye información sobre el autor del mensaje, el servidor de correo electrónico por el que ha pasado el mensaje y la herramienta o software utilizado para componer el mensaje. Ahora puede agregar cabeceras de internet personalizadas a los correos electrónicos programados desde la SAP BusinessObjects BI platform. Siga los pasos siguientes para añadir cabeceras personalizadas:

1. Inicie la sesión en la *CMC*.
2. Vaya a *Servidores* y después a *Lista de servidores*.
3. Abra el menú contextual para *Servidor de tareas de Adaptive* y seleccione *Destinos*.
4. En el asistente *Destinos* seleccione *Correo electrónico* y añada los detalles necesarios para cada campo como se muestra a continuación:




5. Verifique *Habilitar cabeceras personalizadas* y añada las cabeceras de internet en el campo vacío como se muestra más abajo:

6. Seleccione *Guardar y cerrar*.

Los correos electrónicos con documentos programados ahora contienen las cabeceras de internet.

> **Nota**
>
> - Al programar, seleccione *Utilizar parametrizaciones predeterminadas* para añadir cabeceras de internet personalizadas en los correos electrónicos programados.
> - Cada *servidor de tareas de Adaptive* debería configurarse para garantizar que las cabeceras personalizadas se añaden a cada correo electrónico.

## 11.7 Agrupar Servidores de administración central

### 11.7.1 Agrupar Servidores de administración central

Si dispone de una implementación grande o decisiva de la plataforma SAP BusinessObjects Business Intelligence, probablemente deseará ejecutar varios equipos del CMS conjuntamente en un clúster. Un clúster consta de dos o más servidores CMS que trabajan juntos en una base de datos del sistema de CMS común. Si se produce un error en uno de los equipos que ejecuta el CMS, otro equipo con otro CMS continuará atendiendo las solicitudes de servicio de la plataforma de BI. Esta compatibilidad de "alta disponibilidad" ayuda a garantizar que los usuarios de la plataforma de BI puedan seguir accediendo a la información cuando se produce un error en el equipo.

En esta sección se muestra cómo agregar un nuevo miembro de clúster CMS a un sistema de producción ya configurado y en ejecución. Cuando se agrega un nuevo CMS a un clúster existente, se le indica al nuevo CMS que conecte con la base de datos de sistema de CMS existente y que comparta las tareas de procesamiento con los demás equipos CMS. Para obtener información acerca del CMS actual, diríjase al área de administración *Servidores* de la CMC.

Antes de agrupar en clúster equipos CMS, debe asegurarse de que cada CMS está instalado en un sistema que cumpla los requisitos detallados (incluidos los niveles de versión y revisión) para el sistema operativo, el servidor de base de datos, el método de acceso a la base de datos, el controlador de base de datos y el cliente de base de datos indicados en la matriz de disponibilidad del producto.

Además, se deben cumplir los siguientes requisitos de agrupamiento:

- Para obtener un rendimiento óptimo, el servidor de base de datos que elija para alojar la base de datos del sistema debe poder procesar consultas pequeñas muy rápidamente. El CMS establece comunicación con frecuencia con la base de datos del sistema y le envía muchas consultas pequeñas. Si el servidor de la base de datos no puede procesar estas solicitudes de modo puntual, el rendimiento de la plataforma de BI se verá afectado en gran medida.
- Para obtener un rendimiento óptimo, ejecute cada miembro del clúster CMS en un equipo que tenga la misma cantidad de memoria y el mismo tipo de CPU.
- Configure cada equipo de manera similar:
  - Instale el mismo sistema operativo, incluidos los mismos Service Pack de sistema operativo y las mismas revisiones.
  - Instale la misma versión de la plataforma de BI (incluidas revisiones, si se pueden aplicar).

    - Asegúrese de que todos los CMS se conectan con la base de datos de sistema de CMS de la misma forma: tanto si usa controladores nativos como ODBC. Compruebe que los controladores se encuentran en el mismo equipo y tienen una versión compatible.
    - Asegúrese de que todos los CMS utilizan el mismo cliente de base de datos para conectarse a su base de datos del sistema y de que tiene una versión compatible.
    - Compruebe que todos los CMS utilizan la misma cuenta de usuario y contraseña para conectarse a la base de datos de sistema de CMS. Esta cuenta debe tener los derechos de crear, eliminar y actualizar en la base de datos del sistema.
    - Asegúrese de que los nodos en los que se encuentra cada CMS se están ejecutando en la misma cuenta de sistema operativo. (En Windows, la cuenta predeterminada es "LocalSystem".)
    - Verifique que la fecha y hora actuales están configuradas correctamente en todos los equipos CMS (incluida la configuración del horario de verano).
    - Asegúrese de que todos los equipos del clúster (incluidos los equipos que alojan el CMS) están configurados en la misma hora del sistema. Para obtener mejores resultados, sincronice los equipos en un servidor horario (como, `yime.nist.gov`) o use una solución de supervisión central.
    - Asegúrese de que los mismos archivos WAR están instalados en todos los servidores de aplicaciones Web del clúster. Para obtener más información acerca del despliegue de archivos WAR, consulte el *Manual de instalación de la plataforma SAP BusinessObjects Business Intelligence*.
- Asegúrese de que todos los CMS de un clúster se encuentran en la misma red de área local.
- Los subprocesos fuera de banda (-oobthreads) los usan pings y notificaciones de agrupación en clúster. Dado que ambas operaciones son rápidas (las notificaciones son asincrónicas), la plataforma de BI ya no requiere subprocesos fuera de banda y solo se crea uno.
  Si el clúster incluye más de ocho miembros de clúster del CMS, asegúrese de que la línea de comandos para cada CMS incluye la opción `-oobthreads <numCMS>`, donde `<numCMS>` es el número de servidores CMS del clúster. Esta opción garantiza que el clúster puede admitir cargas elevadas. Para obtener información acerca de la configuración de las líneas de comandos de servidor, consulte el apéndice Líneas de comandos de servidor del *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*.
- La habilitación de la auditoría de un único CMS será como una configuración en un entorno agrupado. También puede modificar la base de datos de la auditoría en la página de configuración de la auditoría en CMC. Los requisitos para la base de datos de auditoría son los mismos que para la base de datos del sistema en lo que se refiere a servidores de base de datos, clientes, métodos de acceso, controladores e ID de usuario.

→ Sugerencias

De forma predeterminada, el nombre de un clúster refleja el nombre de host del equipo del primer CMS que desea instalar.

## Información relacionada

Cambio del nombre de un clúster CMS [página 438]

## 11.7.1.1 Adición de un CMS a un clúster

Hay varias formas de agregar un nuevo miembro del clúster de servidores CMS. Siga el procedimiento adecuado:

- Puede instalar un nodo nuevo con un CMS en un nuevo equipo
- Si ya tiene un nodo con archivos binarios de CMS, puede agregar un nuevo servidor CMS desde la CMC.
- Si ya tiene un nodo con archivos binarios de CMS, también puede agregar un nuevo servidor CMS si clona uno existente.

> **Nota**
>
> Realice la copia de seguridad de la base de datos del sistema del CMS actual, la de configuración del servidor y de los contenidos de los repositorios de archivos de entrada y salida antes de realizar los cambios. Si es necesario, póngase en contacto con el administrador de su base de datos.

### Información relacionada

Adición de un nuevo nodo a un clúster [página 437]
Adición de un servidor [página 431]
Clonación de servidores [página 432]
Presentación general de la copia de seguridad y de la restauración [página 558]

## 11.7.1.2 Adición de un nuevo nodo a un clúster

Cuando agregue un nodo (un nodo es un conjunto de servidores de la plataforma de BI administrados por un único Agente de inteligencia de servidor), se le solicitará crear un CMS nuevo o agrupar el nodo en un CMS actual.

Si desea agrupar un nodo con un CMS existente, también puede utilizar el programa de configuración de instalación. Ejecute el programa de instalación y configuración de la plataforma de BI en el equipo donde desea instalar el nuevo miembro de clúster del CMS. El programa de instalación permite llevar a cabo una instalación personalizada. Durante la instalación personalizada, se especifica el CMS existente cuyo sistema se desea expandir y se seleccionan los componentes que se desean instalar en el equipo local. En este caso, especifique el nombre del CMS que se ejecuta en el sistema actual, elija instalar un CMS nuevo en el equipo local y proporcione al programa de instalación la información que necesita para conectarse a la base de datos del sistema del CMS actual. Cuando el programa de instalación instala el nuevo CMS en el equipo local, agrega automáticamente el servidor al clúster existente.

> **Nota**
>
> Antes de agrupar un nodo nuevo en un CMS existente, si el nuevo nodo es un servidor completamente nuevo, compruebe que la instalación de la plataforma de BI en dicho servidor está en el mismo nivel de revisión que el entorno de la plataforma de BI actual.

> **Nota**
>
> Las licencias Edge BI y Crystal Server no permiten la agrupación en clústeres ni el despliegue de nodos múltiples. Sin embargo, a partir de Edge BI 4.3 SP2 y Crystal Server 2020 SP2, si Edge BI y Crystal Server se despliegan en Linux, se permite UN nodo Windows con los servicios de Crystal Reports 2020. Consulte Cómo distribuir los servicios de SAP Crystal Reports 2020 a un servidor de Windows para obtener más información.

### Información relacionada

Uso de nodos [página 474]

## 11.7.1.3 Agregar clústeres a los archivos de propiedades de aplicaciones web

Si ha agregado CMSs adicionales a su despliegue, esta información se captura en el fichero `clusterinfo.1400.properties` disponible en `C:/Users/<you_user>/.businessobjects`. Este fichero se genera o actualiza cuando reinicia el SIA.

> **Nota**
>
> En un despliegue Tomcat independiente, el fichero `clusterinfo.1400.properties` solo se obtiene cuando inicia sesión con un nombre del CMS. Cuando actualiza el cluster, el fichero en un Tomcat independiente no se actualiza. Debe copiar el fichero de su CMS en su equipo Tomcat.

## 11.7.1.4 Cambio del nombre de un clúster CMS

Este procedimiento le permite cambiar el nombre de un clúster que ya está instalado. Después de cambiar el nombre del clúster del CMS, el Server Intelligence Agent vuelve a configurar automáticamente cada servidor de SAP Business Objects, de modo que se registra con el clúster del CMS, en lugar de con un CMS individual.

> **Nota**
>
> Los administradores experimentados de la plataforma de BI deben tener en cuenta que ya no se puede utilizar la opción `-ns` en la línea de comandos del servidor para configurar el CMS con el que se debe registrar un servidor. Ahora, el SIA se encarga de esta tarea automáticamente.

### 11.7.1.4.1 Para cambiar el nombre del clúster en Windows

1. Utilice CCM para detener Server Intelligence Agent para el nodo que contiene un servidor de administración central que sea miembro del clúster cuyo nombre desea cambiar.
2. Haga clic con el botón derecho del ratón en Server Intelligence Agent y elija *Propiedades*.
3. En el cuadro de diálogo Propiedades, haga clic en la ficha *Configuración*.
4. Active la casilla de verificación *Cambiar nombre de clúster a*.
5. Escriba el nuevo nombre del clúster.
6. Haga clic en *Aceptar* y, a continuación, reinicie Server Intelligence Agent.

   Ya se ha cambiado el nombre del clúster CMS. Los demás miembros del clúster CMS reciben una notificación dinámica del nuevo nombre de clúster (aunque pueden pasar varios minutos hasta que los cambios se hayan propagado a los miembros del clúster).
7. Vaya al área de administración *Servidores* del CMC y compruebe que todos los servidores permanecen habilitados. Si es necesario, habilite los servidores que se hayan deshabilitado por los cambios.

### 11.7.1.4.2 Para cambiar el nombre del clúster en UNIX

Utilice la secuencia de comandos `cmsdbsetup.sh`. Como referencia, consulte el tema «Secuencias de comandos Unix» en el capítulo sobre la Gestión de líneas de comandos del *Manual del administrador de la plataforma BI*.

#### Información relacionada

Scripts de Unix [página 1100]

## 11.8 Administración de grupos de servidores

Los grupos de servidores pueden organizar y ayudar a administrar los servidores de la plataforma de BI en su sistema. Puede seleccionar un servidor o grupo de servidores en particular por publicación (no por usuario), y puede agrupar los servidores por región o tipo.

Agrupar servidores por región para configurar de forma sencilla la configuración de procesamiento predeterminada, programaciones periódicas y programar destinos para los usuarios que trabajen en una determinada oficina regional. Puede asociar un objeto de informe (como un Crystal Report o un documento de Web Intelligence) con un único grupo de servidores, de modo que el objeto siempre se procesará por parte de los mismos servidores. También puede asociar objetos de informe programados con un determinado grupo de servidores para asegurarse de que los objetos programados se enviarán a las impresoras, servidores de archivos, etc., correctos. Los grupos de servidores resultan especialmente útiles al hacer el mantenimiento de sistemas que abarcan varias ubicaciones y múltiples zonas horarias.

Los grupos de servidores resultan especialmente útiles al hacer el mantenimiento de sistemas que abarcan varias ubicaciones y múltiples zonas horarias. Por ejemplo, utilice grupos de servidores para personalizar su sistema de plataforma de BI para los informes visualizados en diferentes ubicaciones y para diferentes tipos de informe. Al organizar los servidores por región, puede realizar las siguientes acciones para los grupos de servidores:

- Configurar las opciones de procesamiento estándar
- Configurar programaciones periódicas
- Configurar la programación de destinos para usuarios que trabajen en una determinada oficina regional
- Asociar un objeto de informe (como un Crystal Report o un documento de Web Intelligence) con un único grupo de servidores, de modo que el objeto siempre se procese por los mismos servidores
- Asociar objetos de informe programados con un determinado grupo de servidores para garantizar que los objetos programados se envían a las impresoras, servidores de archivos, etc., correctos

Agrupar servidores por tipo cuando se configuran los objetos para que sean procesados por servidores optimizados para estos objetos.

Después de crear los grupos de servidores, configure los objetos para que utilicen grupos de servidores específicos para programar o visualizar y modificar los informes. Utilice el árbol de navegación del área de administración *Servidores* de la CMC para visualizar los grupos de servidores. La opción *Lista de grupos de servidores* muestra una lista de los grupos de servidores en el panel *Detalles*, y la opción *Grupos de servidores* le permite ver los servidores en el grupo.

### Ejemplo: Agrupar servidores de procesamiento por tipo

Por ejemplo, los servidores de procesamiento necesitan establecer comunicación frecuentemente con la base de datos que contiene los datos de los informes publicados. Si los servidores de procesamiento se colocan cerca del servidor de base de datos al que necesitan acceder, se mejora el rendimiento del sistema y se reduce el tráfico de red. Por lo tanto, para varios informes que se ejecutan en una base de datos DB2, puede crear un grupo de servidores de procesamiento que solo procesen informes en el servidor de la base de datos DB2. Para mejorar el rendimiento del sistema al visualizar los informes, puede configurar los informes para que siempre utilicen este servidor de procesamiento para la visualización.

## 11.8.1 Creación de un grupo de servidores

Para crear un grupo de servidores, tiene que especificar el nombre y la descripción del grupo y, a continuación, agregar servidores a dicho grupo.

### 11.8.1.1 Crear un grupo no exclusivo de servidores

Los grupos de servidores no exclusivos pueden contener servidores o grupos de servidores que forman parte de cualquier otro grupo de servidores no exclusivo o el pool de servidores común.

1. Vaya al área de administración *Servidores* de CMC.

2. Seleccione *Administrar* > *Nuevo* > *Crear grupo de servidores*.

   Aparece el cuadro de diálogo *Crear grupo de servidores*.
3. En el campo *Nombre*, escriba el nombre del nuevo grupo de servidores.
4. Si desea incluir información adicional sobre los grupos de servidores, escríbala en el campo *Descripción*.
5. Haga clic en *Aceptar*.
6. En el área de administración *Servidores*, haga clic en *Grupos de servidores* en el árbol de navegación y seleccione el nuevo grupo de servidores.
7. Elija *Agregar miembros* en el menú *Acciones*.
8. Seleccione los servidores que desea agregar a este grupo; a continuación, haga clic en >.

   > **→ Sugerencias**
   >
   > Use `CTRL` + `clic` para seleccionar varios servidores.

   > **ⓘ Nota**
   >
   > Los servidores listados solo incluyen servidores que no forman parte de cualquier otro grupo de servidores.
9. Haga clic en *Aceptar*.

   Volverá al área de administración *Servidores*, donde se enumeran todos los servidores que se han agregado al grupo. Ahora puede cambiar el estado, ver las medidas del servidor y cambiar las propiedades de los servidores del grupo.

## 11.8.1.2 Para crear un grupo exclusivo de servidores

Los grupos de servidores exclusivos contienen servidores o grupos de servidores que no forman parte de ningún otro grupo de servidores o pool de servidores común. Si se crea un grupo de servidores como grupo de servidores exclusivos, los servidores que forma parte de este grupo no se pueden asignar a otro grupo (exclusivo o no exclusivo) y los servidores añadidos al grupo exclusivo se excluyen del pool común. Esto le permite crear grupos de servidores aislados de la carga general del sistema BI.

1. Vaya al área de administración *Servidores* de CMC.
2. Seleccione *Administrar* > *Nuevo* > *Crear grupo de servidores*.

   Aparece el cuadro de diálogo *Crear grupo de servidores*.
3. En el campo *Nombre*, escriba el nombre del nuevo grupo de servidores.
4. Si desea incluir información adicional sobre los grupos de servidores, escríbala en el campo *Descripción*.
5. Seleccione la casilla de selección *Grupo de servidores exclusivo* .

   > **ⓘ Nota**
   >
   > Puede crear un grupo de servidores exclusivo solo a nivel de raíz. Para un nodo subordinado, puede crear un grupo de servidores solo si el grupo de servidores raíz o superior es exclusivo.
   >
   > > **✤ Ejemplo**
   > >
   > > Tome este escenario como ejemplo para entender los grupos de servidores exclusivos:

> Dos servidores de tareas: JS1 y JS2 forman parte del pool de servidores común.
>
> Cree un grupo de servidores exclusivo. SG1.
>
> Añada JS1 a SG1.
>
> Programe el documento (D) seleccionando la opción *Utilice solamente servidores del grupo seleccionado*.
>
> Supongamos que JS1 y JS2 ya tienen varias tareas en ejecución.
>
> **Resultado:** JS1 ya está cargado con varias tareas que necesitan procesarse. Sin embargo, ya que JS1 ya forma parte de SG1, JS1 solo recibe solicitudes de flujos de trabajo de proceso asignados a SG1, por lo que está libre de la carga del sistema general.

6. Haga clic en *Aceptar*.
7. En el área de administración *Servidores*, haga clic en *Grupos de servidores* en el árbol de navegación y seleccione el nuevo grupo de servidores.
8. Elija *Agregar miembros* en el menú *Acciones*.
9. Seleccione los servidores que desea agregar a este grupo; a continuación, haga clic en >.

> → Sugerencias
>
> Use `CTRL` + `clic` para seleccionar varios servidores.

> ⓘ Nota
>
> Los servidores enumerados solo incluyen servidores que aún no forman parte de otros grupos de servidores o del pool de servidores comunes.

10. Haga clic en *Aceptar*.

    Volverá al área de administración *Servidores*, donde se enumeran todos los servidores que se han agregado al grupo. Ahora puede cambiar el estado, ver las medidas del servidor y cambiar las propiedades de los servidores del grupo.

## 11.8.2 Convertir un grupo de servidores exclusivo en grupo de servidores no exclusivo y a la inversa

### 11.8.2.1 Convertir un grupo de servidores exclusivo en grupo de servidores no exclusivo

Ahora puede modificar un grupo de servidores existente exclusivo para convertirlo en no exclusivo.

Para convertir un grupo de servidores exclusivo a nivel de raí en no exclusivo haga lo siguiente:

1. Haga clic con el botón derecho del ratón en el grupo de servidores exclusivo que quiere convertir y seleccione *Propiedades* del desplegable.

   Se abre el cuadro de diálogo*Propiedades* . Verá que la casilla de selección *Grupo de servidores exclusivo* está seleccionada
2. Desmarque la casilla de selección *Grupo de servidores exclusivo* .

   Aparecerá un mensaje de advertencia.
3. Haga clic en *Aceptar* para confirmar la conversión.
4. Seleccione *Guardar y cerrar*

   Ahora ha convertido un grupo de servidores exclusivo en no exclusivo.

   > ⓘ Nota
   >
   > Ahora ha convertido un grupo de servidores exclusivo en no exclusivo.

### 11.8.2.2 Conversión de un grupo de servidores no exclusivo a grupo de servidores exclusivo

Ahora puede modificar un grupo de servidores existente no exclusivo para convertirlo en exclusivo.

Para convertir un grupo de servidores no exclusivo que contiene servidores **independientes** y grupos de servidores, realice lo siguiente:

1. Haga clic con el botón derecho del ratón en el grupo de servidores no exclusivo que quiere convertir y seleccione *Propiedades* del desplegable.

   Se abre el cuadro de diálogo*Propiedades* . Verá que la casilla de selección *Grupo de servidores exclusivo* no está seleccionada
2. Seleccione la casilla de selección *Grupo de servidores exclusivo* .

   Aparecerá un mensaje de éxito.
3. Seleccione *Aceptar*.
4. Seleccione *Guardar y cerrar*

   Ahora ha convertido un grupo de servidores no exclusivo en exclusivo.

   > ⓘ Nota
   >
   > Solo puede convertir un grupo de servidores no exclusivo que tiene servidores independientes y grupos de servidores en exclusivo. Servidores y grupos de servidores independientes son aquellos que no forman parte de ningún otro grupo de servidores.

## 11.8.3 Trabajo con subgrupos de servidores

Los subgrupos de servidores proporcionan una manera de organizar aún más los servidores. Un subgrupo es un grupo de servidores que es miembro de otro grupo de servidores.

Por ejemplo, si agrupa servidores por región y país, cada grupo regional se convierte en un subgrupo de un grupo de país. Para organizar los servidores de este modo, primero cree un grupo para cada región y agregue los servidores adecuados a cada grupo regional. A continuación, cree un grupo para cada país y agregue cada grupo regional al correspondiente grupo de país.

Existen dos formas para configurar los subgrupos: puede modificar los subgrupos de un grupo de servidores o puede crear un grupo de servidores en miembro de otro. Los resultados son los mismos, por lo tanto, utilice el método que resulte más adecuado.

### 11.8.3.1 Para agregar subgrupos a un grupo de servidores

1. Vaya al área de administración *Servidores* de CMC.
2. Haga clic en *Grupos de servidores* en el árbol de navegación y seleccione el grupo de servidores al que desee agregar subgrupos.

   Este grupo es el principal.
3. Elija *Agregar miembros* en el menú *Acciones*.
4. Haga clic en *Grupos de servidores* en el árbol de navegación, seleccione los grupos de servidores que desea agregar a este grupo y, a continuación, haga clic en >.

   → Sugerencias

   Use `CTRL` + `clic` para seleccionar varios grupos de servidores.
5. Haga clic en *Aceptar*.

   Volverá al área de administración *Servidores*, donde se enumeran todos los grupos de servidores que se han agregado al grupo principal.

### 11.8.3.2 Para convertir un grupo de servidores en miembro de otro

1. Vaya al área de administración *Servidores* de CMC.
2. Haga clic en el grupo que desea agregar a otro grupo.

   ⓘ Nota

   Para grupos de servidores exclusivos a nivel de pie, todos los grupos de servidores se listan bajo *Grupos de servidores disponibles*. Solo puede seleccionar un grupos de servidores exclusivo y moverlo a *Miembro del grupo de servidores*, ya que un grupo de servidores exclusivo solo puede tener un grupo de servidores superior.

> Los grupos de servidores exclusivos a nivel inferior no listan ninguno de los grupos de servidores en *Grupos de servidores disponibles*, ya que im grupo de servidores exclusivo solo puede tener un superior.

3. Elija *Agregar a grupo de servidores* en el menú *Acciones*.
4. En la lista *Grupos de servidores disponibles*, seleccione el resto de grupos a los que desea agregar el grupo y, a continuación, haga clic en >.

> → Sugerencias
>
> Use `CTRL` + `clic` para seleccionar varios grupos de servidores.

5. Haga clic en *Aceptar*.

## 11.8.4 Modificación de la pertenencia a grupos de un servidor

Puede modificar la pertenencia a grupos de un servidor para agregarlo rápidamente (o eliminarlo) a cualquier grupo o subgrupo que ya esté creado en el sistema.

Por ejemplo, suponga que ha creado grupos de servidores para varias regiones. Es posible que desee utilizar un solo Servidor de administración central (CMS) para varias regiones. En lugar de tener que agregar el CMS de forma individual a cada grupo de servidores regionales, puede hacer clic en el vínculo *Miembro de* del servidor para agregarlo en las tres regiones a la vez.

### 11.8.4.1 Para modificar la pertenencia a grupos de un servidor

1. Vaya al área de administración *Servidores* de CMC.
2. Haga clic con el botón derecho en el servidor cuya información de suscripción desea cambiar y seleccione *Grupos de servidores existentes*.
   En el panel de detalles, la lista *Grupos de servidores disponibles* muestra los grupos a los que puede agregar el servidor. La lista *Miembro de los grupos de servidores* enumera los grupos de servidores a los que pertenece actualmente el servidor.

> ⓘ Nota
>
> Para grupos de servidores exclusivos a nivel de pie, todos los grupos de servidores se listan bajo *Grupos de servidores disponibles*. Solo puede seleccionar un grupos de servidores exclusivo y moverlo a *Miembro del grupo de servidores*, ya que un grupo de servidores exclusivo solo puede tener un grupo de servidores superior. Cuando haya seleccionado un grupo de servidores desde *Grupos de servidores disponibles* y muévalo a *Miembro de grupos de servidores*, el grupo de servidores exclusivo se mueve a su grupo de servidores raíz y a un grupo de servidores nuevo en el que se asigna.
>
> Para grupo de servidores inferiores, se muestran grupos de servidores superiores bajo *Miembro de grupos de servidores* y otros grupos de servidores se listan bajo *Grupos de servidores disponibles*. Puede modificar la asignación de un grupo de servidores inferior de un superior exclusivo a otro.

3. Para cambiar los grupos de los que es miembro el servidor, utilice las flechas para mover los grupos de servidores entre las listas y, a continuación, haga clic en *Aceptar*.

> **Nota**
>
> La opción*Eliminar del grupo de servidores* solo se lista para grupos de servidores exclusivos a nivel inferior. Cuando se elimina un grupo de servidores exclusivo a nivel inferior del grupo de servidores superior, retendrá su exclusividad y se moverá al nivel de raíz.
>
> En la rampa de lanzamiento BI aparecen grupos de servidores si el administrador de CMC concede derechos de seguridad de usuario para grupos de servidores específicos.

## 11.8.5 Acceso administrativo a servidores y grupos de servidores para usuarios

El garantizarles derechos de administración a los usuarios les permite llevar a cabo tareas de servidor y grupos de servidores, tales como iniciar y detener los servidores.

En función de la configuración de su sistema y los requisitos de seguridad, puede que limite la administración del servidor al administrador de la plataforme de BI o puede que necesite proporcionarle acceso de administración a otras personas que estén utilizando estos servidores. Muchas organizaciones tiene un grupo de profesiones de la informática dedicado a la administración de servidores. Si el equipo dedicado a los servidores necesita realizar tareas de mantenimiento de servidores regularmente que impliquen apagar y encender los servidores, debe otorgarles derechos de administración sobre los servidores. También puede ser que desee delegar tareas de administración del servidor de la plataforma de BI en otras personas o desee que algunos grupos en su organización controlen su propia administración del servidor.

> **Nota**
>
> Puede seleccionar un servidor o grupo de servidores para una publicación (no para un usuario en particular). No obstante, puede asignar derechos de administración a usuarios o grupos de usuarios para un determinado servidor o grupo de servidores.

### 11.8.5.1 Concesión de derechos administrativos de acceso a un servidor o un grupo de servidores

Puede asignar derechos de administración a usuarios o grupos de usuarios para un determinado servidor o grupo de servidores.

> **Nota**
>
> Puede seleccionar un servidor o grupo de servidores para una publicación (no para un usuario).

1. Vaya al área de administración *Servidores* de CMC.
2. Haga clic con el botón derecho en el servidor o grupo de servidores a los que desea conceder derechos administrativos de acceso y seleccione *Seguridad de usuario*.

3. Haga clic en *Agregar principales* para agregar los usuarios o los grupos a los que desea conceder derechos administrativos al servidor o grupo de servidores seleccionados.
4. En el cuadro de diálogo *Añadir principales*, seleccione un usuario o grupo para el que desea conceder derechos administrativos al servidor o grupo de servidores y haga clic en >.
5. Haga clic en *Agregar y asignar seguridad*.
6. En la pantalla *Asignar seguridad*, seleccione los ajustes de seguridad que desea para el usuario o grupo y haga clic en *Aceptar*.

### Información relacionada

Cómo funcionan los derechos en la Plataforma de BI [página 127]

## 11.8.5.2 Derechos de objeto para el servidor de aplicaciones de informes (RAS)

Para permitir que los usuarios creen o modifiquen informes a través del Web mediante el Servidor de aplicaciones de informes (RAS), debe disponer de las licencias de modificación de informes de RAS en el sistema. También debe conceder a los usuarios un conjunto mínimo de derechos de objeto. Cuando se otorga a los usuarios derechos sobre un objeto de informe, pueden seleccionar el informe como origen de datos para un nuevo informe o modificarlo directamente:

- Ver objetos (o «Ver instancias de documento», según resulte adecuado)
- Editar objetos
- Actualizar datos del informe
- Exportar datos del informe

El usuario también debe disponer de permiso para agregar objetos al menos en una carpeta para poder guardar nuevos informes en la plataforma de BI.

Para garantizar que los usuarios conservan la capacidad de realizar tareas de informe adicionales (como copiar, programar, imprimir, etc.), se recomienda asignar primero el nivel de acceso adecuado y actualizar los cambios. A continuación, cambie el nivel de acceso a Avanzado y agregue cualquiera de los derechos necesarios que todavía no estén concedidos. Por ejemplo, si los usuarios ya disponen derechos Ver a petición sobre un objeto de informe, les puede permitir modificar el informe cambiando el nivel de acceso a Avanzando y concediendo explícitamente el derecho Editar objetos.

Cuando los usuarios ven los informes mediante el Visor DHTML avanzado y RAS, el nivel de acceso Ver es suficiente para mostrar el informe, pero el nivel Ver a petición es necesario para utilizar realmente las funciones de búsqueda avanzada. El derecho Editar objetos adicional no es necesario.

## 11.8.6 Asignación de un grupo de usuarios a un grupo de servidores

Ahora puede asignar un grupo de usuarios a un grupo de servidores en concreto con la nueva opción *Parametrizaciones predeterminadas*.

Para asignar un grupo de usuarios a un grupo de servidores, realice los pasos siguientes:

1. Inicie una sesión en CMC.
2. Seleccione *Usuarios y grupos*.
3. En la página *Usuarios y grupos* haga clic con el botón derecho en el grupo de usuarios deseado que quiere asignar al grupo de servidores.
4. Seleccione *Configuración predeterminada*.
5. En la página *Programar grupo de servidores* , fije los servidores predeterminados para usar en la programación del grupo de usuarios.

   Puede seleccionar una de las opciones siguientes:

   - (Valor predeterminado) Seleccione *Usar el primer servidor disponible* para ejecutar el objeto en el servidor con más recursos libres en el momento de la programación.
   - Seleccione *Dar preferencia a los servidores del grupo seleccionado* para ejecutar el objeto en servidores de un grupo de servidores concreto. Luego seleccione el grupo de servidores requerido en el cuadro desplegable para fijar una preferencia para un grupo de servidores concreto. Si no hay ningún servidor disponible en el grupo de servidores seleccionado, el objeto se ejecuta en el siguiente servidor disponible del pool de servidores comunes.
   - Seleccione *Usar solo servidores del grupo seleccionado* para ejecutar el objeto solamente en servidores de un grupo de servidores concreto y seleccione el grupo de servidores necesario del cuadro desplegable para utilizar exclusivamente un grupo de servidores. Si no hay servidores disponibles en el grupo, el objeto no se procesa. Además, si un servidor de tareas no está presente en el grupo de servidores asignado, la tarea permanece en el estado pendiente.

> **Nota**
>
> Puede elegir asignar un grupo de servidores exclusivo o no exclusivo a un grupo de usuarios pulsando uno de los dos botones de selección: *Dar preferencia a los servidores del grupo seleccionado* o *Usar solo servidores del grupo seleccionado*.
>
> De forma similar, puede asignar grupos de servidores para la visualización o el tratamiento de documentos de Crystal Reports y Web Intelligence navegando a *Parametrizaciones estándar*, y *Opciones de proceso de Crystal Reports* y *Opciones de proceso de Web Intelligence*, respectivamente.
>
> Si hay un grupo de servidores asociado tal como se requiere, significa que **solamente** se utilizan los servidores de ese grupo de servidores. No se utilizan los servidores del pool común. Si un grupo de servidores está asociado como preferido, cuando los servidores del grupo de servidores estén ocupados, se utilizarán los servidores del pool de servidores comunes. El pool de servidores comunes incluye todos los servidores que no forman parte de un grupo de servidores exclusivo. Para obtener más información sobre grupos de servidores exclusivos, consulte Para crear un grupo exclusivo de servidores [página 441].

La asignación de un grupo de servidores a un grupo de usuarios puede ser compleja porque un usuario puede formar parte de múltiples grupos de usuarios. Y cada grupo de usuarios puede asignarse a diferentes grupos. Cada grupo de servidores puede asignarse según sus necesidades o preferencias.

### Ejemplo

Considere este escenario:

Si un usuario (U) forma parte de dos grupos de usuarios - GU1 y GU2. Y si cada grupo se asigna a un grupo de servidores diferente - GU1 y GU2. Entonces, los resultados para varios escenarios sería:

| Escenario | Resultado |
|---|---|
| Planificar un documento (D).<br>El grupo de servidores 1 (GS1) se ha establecido en GS1 y el grupo de servidores 2 (GS2) se ha establecido en GS2.<br>GS1 está establecido como requerido (R). GS2 también está establecido como requerido (R).<br>No hay ningún grupo de servidores asignado en el nivel de documento (D). | La combinación de los dos grupos de servidores (GS1 y GS2) actúa como un grupo de servidores requerido (R).<br>Como ambos grupos de servidores (GS1 y GS2) se configuran como requerido, los servidores del conjunto común NO se utilizan. |
| Planificar un documento (D).<br>El grupo de servidores 1 (GS1) se ha establecido en GS1 y el grupo de servidores 2 (GS2) se ha establecido en GS2.<br>GS1 está establecido como preferido (P). GS2 también está establecido como preferido (P).<br>No hay ningún grupo de servidores asignado en el nivel de documento (D). | La combinación de los dos grupos de servidores (GS1 y GS2) actúa como un grupo de servidores preferido (P).<br>Dado que ambos grupos de servidores (GS1 y GS2) están establecidos como preferidos, si no hay servidores disponibles en los grupos seleccionados, se utilizan los servidores del grupo común. |
| Planificar un documento (D).<br>El grupo de servidores 1 (GS1) se ha establecido en GS1 y el grupo de servidores 2 (GS2) se ha establecido en GS2.<br>GS1 está establecido como requerido (R). GS2 está establecido como preferido (P).<br>No hay ningún grupo de servidores asignado en el nivel de documento (D). | La combinación de los dos grupos de servidores (GS1 y GS2) actúa como un grupo de servidores requerido (R).<br>Dado que la combinación (GS1 y GS2) actúa como un grupo de servidores requerido, los servidores del conjunto común NO se utilizan. |

6. Seleccione *Guardar y cerrar*

   Ahora ha asignado correctamente un grupo de usuarios a un grupo de servidores.

### Nota

- Un usuario puede pertenecer a uno o más grupos de usuarios y cada uno de estos grupos de usuarios puede pertenecer a otros grupos de usuarios. Si no hay ningún grupo de servidores asociado con el grupo de usuarios inmediato al que pertenece un usuario, el programa verifica si un grupo de servidores está asociado con el siguiente nivel de grupos de usuarios. Este proceso continúa hasta que el programa encuentra un grupo de usuarios superior al que hay asignado un grupo de servidores. Cuando el programa encuentra un grupo de servidores a nivel de grupo de usuarios, ya no sigue verificando. Si hay más de un grupo de servidores asociado en el nivel de grupo de usuarios, entonces se considera el comportamiento de la combinación de los dos grupos de servidores (como se explica en la tabla anterior). Tenga en cuenta el siguiente escenario para comprender la asignación de un grupo de servidores:

  #### Ejemplo

  **Escenario:** Planifica un documento (D).

  Un usuario (U) pertenece a dos grupos de usuarios (GU1 y GU2). Pero no hay un grupo de servidores asignado a GU1 y GU2.

  GU1 pertenece a grupo de usuarios 3 (GU3) y GU2 pertenece a grupo de usuarios 4 (GU4).

  El grupo de servidores 3 (GS3) está establecido en GU3.

  GS3 está establecido como requerido (R).

  **Resultado:** Puesto que no hay grupos de servidores configurados en el primer nivel (GU1 y GU2), el programa verifica si hay grupos de servidores configurados en el siguiente nivel (GU3 y GU4). Puesto que GS3 está fijado en GU3, y GS3 está establecido como requerido, solamente se utilizan los servidores de GS3 para procesar el objeto y no pueden utilizarse los servidores del pool común.

  Esto implica que si no hay grupos de servidores definidos a nivel de grupo de usuarios, el programa verifica el siguiente nivel inmediato para ver si hay definidos grupos de servidores. Si el programa identifica que un grupo de servidores está fijado en alguno de los niveles de grupo de usuarios, el programa deja de verificar grupos de servidores en el siguiente nivel.

- A nivel de documento, solamente puede haber un grupo de servidores que puede asignarse y puede ser tanto Requerido (R) como Preferido (P). Sin embargo, un usuario puede pertenecer a uno o más grupos de usuarios y esto puede dar como resultado la asignación de más de un grupo de servidores a un usuario. Si un grupo de servidores está configurado en el nivel de documento (D) y de grupo de usuarios (GU), la asociación de grupo de servidores a nivel de documento siempre se considera sobre la asociación de grupo de servidores a nivel de grupo de usuarios. Tenga en cuenta el siguiente escenario para comprender la asignación de un grupo de servidores:

  #### Ejemplo

  **Escenario:** Planifica un documento (D).

  El grupo de servidores 1 (GS1) está establecido en D, y GS1 está establecido como requerido.

  El grupo de servidores 2 (GS2) está establecido en GU y GS2 está establecido como preferido.

  **Resultado:** Se utiliza GS1. Dado que GS1 está establecido como requerido, los servidores del conjunto común no se pueden utilizar.

> Dado que un grupo de servidores (GS1) ya está establecido en el nivel de documento (D), el programa ignora la asignación del grupo de servidores en el nivel del grupo de usuarios. Implica que la asignación del grupo de servidores a nivel de documento se considera a nivel de grupo de usuarios.

- Necesita garantizar que todos los servidores necesarios son parte del grupo de servidores.
- Para tener un conocimiento más profundo de la asignación de grupos de servidores a carpetas y grupos de usuarios, lea https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/.

## 11.8.7 Asignación de una carpeta a un grupo de servidores

Ahora puede asignar una carpeta a un grupo de servidores en concreto con la nueva opción *Parametrizaciones predeterminadas*.

Para asignar una carpeta a un grupo de servidores, realice los pasos siguientes:

1. Inicie sesión en la CMC.
2. Navegue a *Carpetas* y haga clic con el botón derecho en la carpeta deseada (a la que quiera asignar el grupo de servidores).
3. Seleccione *Configuración predeterminada*.
4. En la página *Programar grupo de servidores* , fije los servidores predeterminados para usar en la programación a nivel de carpeta.

   Puede seleccionar una de las opciones siguientes:

   - (Valor predeterminado) Seleccione *Usar el primer servidor disponible* para ejecutar el objeto en el servidor con más recursos libres en el momento de la programación.
   - Seleccione *Dar preferencia a los servidores del grupo seleccionado* para ejecutar el objeto en servidores de un grupo de servidores concreto. Luego seleccione el grupo de servidores requerido en el cuadro desplegable para fijar una preferencia para un grupo de servidores concreto. Si no hay ningún servidor disponible en el grupo de servidores seleccionado, el objeto se ejecuta en el siguiente servidor disponible del pool de servidores comunes.
   - Seleccione *Usar solo servidores del grupo seleccionado* para ejecutar el objeto solamente en servidores de un grupo de servidores concreto y seleccione el grupo de servidores necesario del cuadro desplegable para utilizar exclusivamente un grupo de servidores. Si no hay servidores disponibles en el grupo, el objeto no se procesa.

> **Nota**
>
> Puede elegir asignar un grupo de servidores exclusivo o no exclusivo a una carpeta pulsando uno de los dos botones de selección: *Dar preferencia a los servidores del grupo seleccionado* o *Usar solo servidores del grupo seleccionado*.
>
> De forma similar, puede asignar grupos de servidores para la visualización o el tratamiento de documentos de Crystal Reports y Web Intelligence navegando a *Parametrizaciones estándar*, y *Opciones de proceso de Crystal Reports* y *Opciones de proceso de Web Intelligence*, respectivamente.
>
> Si hay un grupo de servidores asociado tal como se requiere, significa que **solamente** se utilizan los servidores de ese grupo de servidores. No se utilizan los servidores del pool común. Si un grupo

de servidores está asociado como preferido, cuando los servidores del grupo de servidores estén ocupados, se utilizarán los servidores del pool de servidores comunes. El pool de servidores comunes incluye todos los servidores que no forman parte de un grupo de servidores exclusivo. Para obtener más información sobre grupos de servidores exclusivos, consulte Para crear un grupo exclusivo de servidores [página 441].

5. Seleccione *Guardar y cerrar*

Ahora ha asignado correctamente una carpeta a un grupo de servidores.

### Nota

- A nivel de carpeta o de documento, solamente puede haber un grupo de servidores que puede asignarse y puede ser tanto Requerido (R) como Preferido (P). Si un grupo de servidores está definido a nivel de carpeta (F), documento (D) y grupo de usuarios (UG), la asociación del grupo de servidores a nivel de documento siempre se considerará por encima de la asociación del grupo de servidores a nivel de carpeta seguida de la asociación del grupo de servidores a nivel de grupo de usuarios. Por tanto, el orden de prioridad de la asignación del grupo de servidores es el siguiente: **Documento > Carpeta > Grupo de usuarios**
- Un documento puede pertenecer a una carpeta que, a su vez, puede pertenecer a otra carpeta superior. Teniendo en cuenta que no hay un grupo de servidores asignado a nivel de documento, si no hay un grupo de servidores asociado con la carpeta inmediata a la que pertenece un documento, el programa verifica para ver si un grupo de servidores está asociado con la siguiente carpeta superior inmediata. Este proceso continúa hasta que el programa encuentra una carpeta superior a la que hay asignado un grupo de servidores. Cuando el programa encuentra un grupo de servidores a nivel de carpeta, ya no sigue verificando. Tenga en cuenta el siguiente escenario para comprender la asignación de un grupo de servidores:

  #### Ejemplo

  **Escenario:** Planifica un documento (D).

  Pero no hay un grupo de servidores asignado a nivel de documento.

  El documento (D) pertenece a la carpeta (F). Pero no hay un grupo de servidores asignado a F.

  A su vez, la carpeta (F) es parte de otra carpeta: Carpeta superior (PF). El grupo de servidores (SG) está fijado en PF.

  SG está definido como requerido (R).

  **Resultado:** Puesto que no hay grupos de servidores definidos en el documento (D), el programa verifica si hay grupos de servidores definidos en el nivel de carpeta (F). Como que, nuevamente, no hay grupos de servidores definidos en F, el programa verifica si hay grupos de servidores definidos en el siguiente nivel - carpeta superior (PF). Como que SG está fijado en PF, y SG está definido como requerido, solamente se utilizan los servidores de SG para procesar el objeto y no pueden utilizarse los servidores del pool común.

  Esto implica que si no hay grupos de servidores definidos a nivel de documento, el programa verifica la carpeta inmediata para ver si hay definidos grupos de servidores. Si el programa identifica que un grupo de servidores está fijado en alguno de los niveles de carpeta, el programa deja de verificar grupos de servidores en el siguiente nivel.

> De forma similar, si no hay un grupo de servidores definido a nivel de documento y tampoco hay un grupo de servidores definido a nivel de carpeta, el programa considera la asignación de grupo de servidores a nivel de grupo de usuarios.

- Necesita garantizar que todos los servidores necesarios son parte del grupo de servidores.
- Para tener un conocimiento más profundo de la asignación de grupos de servidores a carpetas y grupos de usuarios, lea https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/.

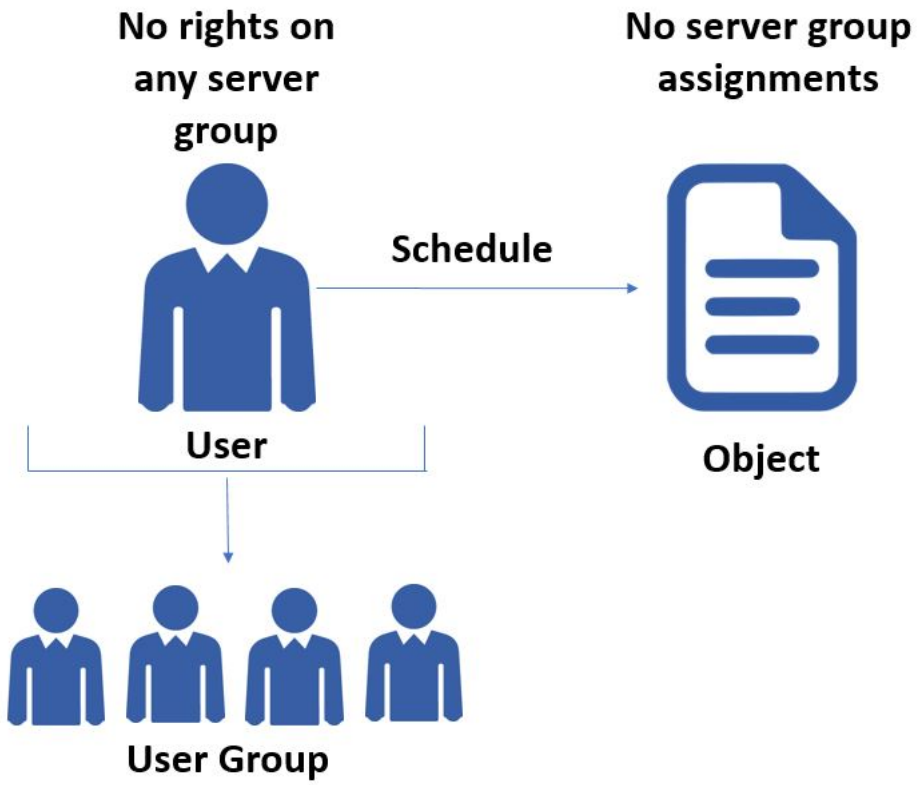
## 11.8.8 Comprender la gestión de los derechos del grupo de servidores

Puede activar derechos de acceso para grupos de servidores a nivel de usuario o de grupo de usuarios. Esto significa que puede controlar el acceso a los grupos de servidores para cada usuario o grupo de usuarios.

> **Nota**
>
> - Los escenarios mencionados más abajo han utilizado la programación como un proceso para explicar la gestión de derechos de grupo de servidores. De forma análoga, puede comprender la gestión de derechos de grupo para visualizar y almacenar en caché.
> - Puede programar un objeto correctamente si los servidores están disponibles en un grupo de servidores o en una combinación de grupos de servidores. La programación falla si no existen servidores disponibles.

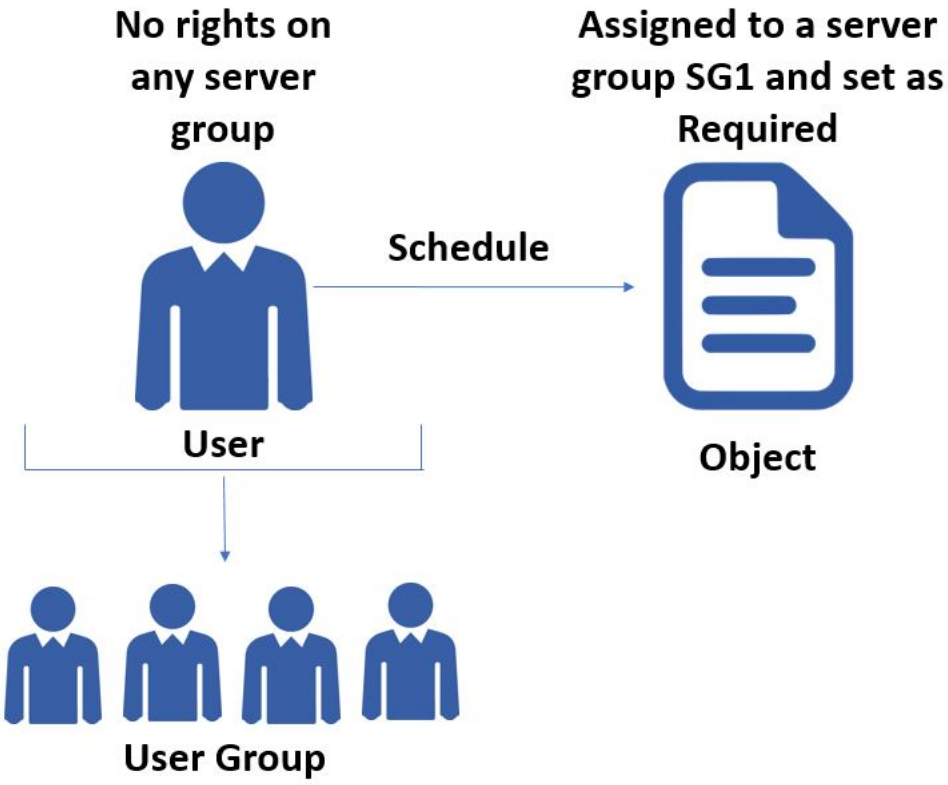
**Escenario 1:**

Considere un escenario ideal en el que un usuario es parte de un grupo de usuarios en la Business Intelligence platform. El usuario y su grupo de usuarios asociado no tienen derechos en ningún grupo de servidores. El usuario ahora desea programar un objeto que tampoco está asignado a ningún grupo de servidores.




**Escenario 2:**

Al modificar el escenario anterior asignando un grupo de servidores al objeto, la programación del objeto falla.



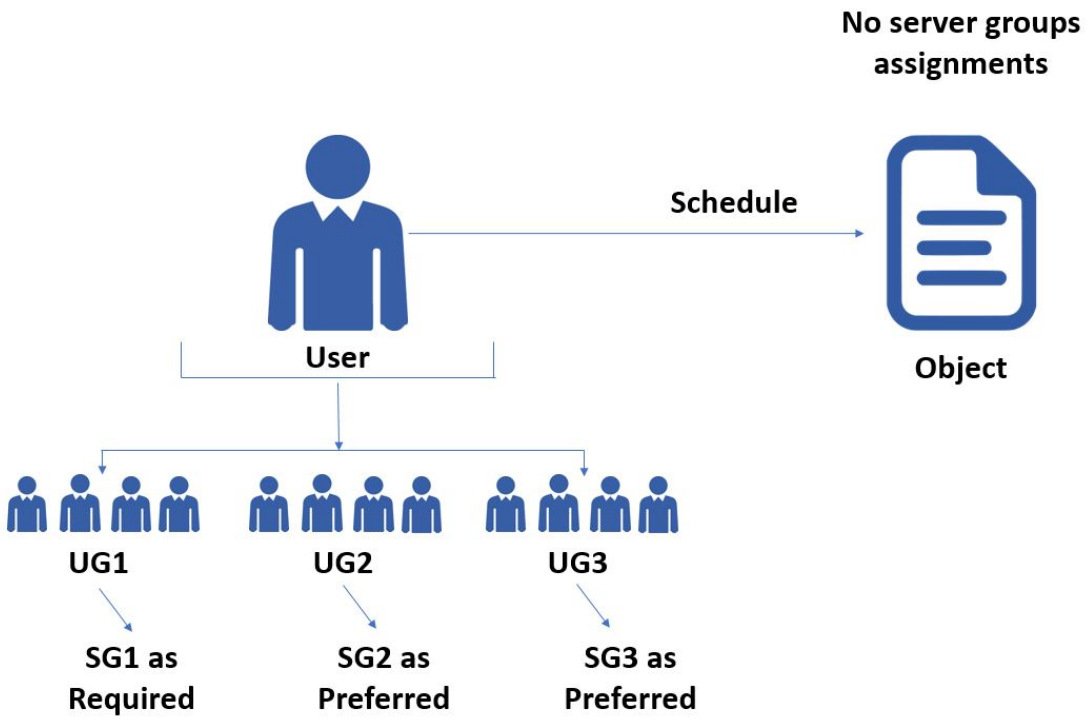

Si un usuario programa un objeto, la plataforma verifica las asignaciones de grupo de servidores al objeto. Si un grupo de servidores se asigna al objeto, la plataforma comprueba si el usuario tiene derechos de visualización en el grupo de servidores.

En el segundo escenario, ni el usuario ni su grupo de usuarios asociado tiene derecho a SG1. Esto provoca el fallo del job de programación. Si desea que un usuario programe un objeto correctamente en este escenario, asegúrese de que el usuario o cualquier grupo de usuarios asociado tiene derechos de visualización en SG1.

**Escenario 3:**

> ⓘ Nota
>
> Para los escenarios 3 y 4 se supone que el usuario hereda los derechos de sus grupos de usuarios asociados.

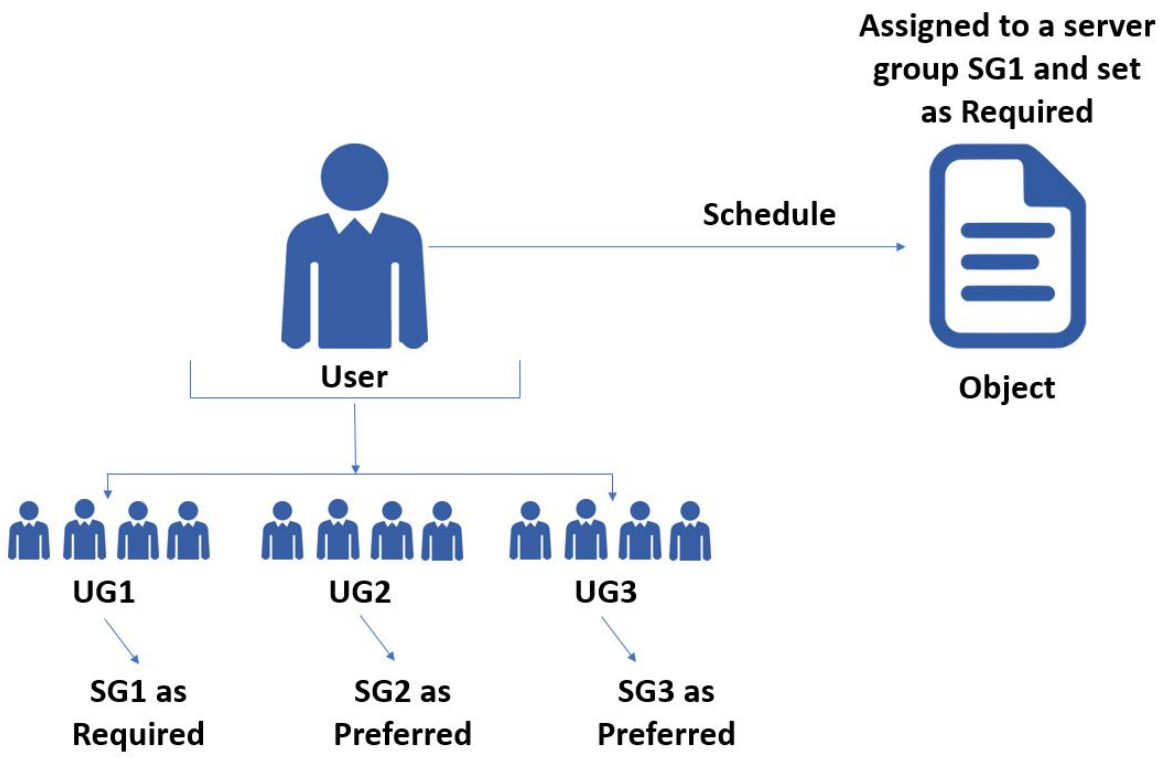
Un usuario forma parte de tres grupos de usuarios UG1, UG2 y UG3 y se ha asignado cada grupo de usuarios a grupos de servidores SG1, SG2 y SG3 respectivamente. Pero SG1 está establecido como grupo de servidores necesario y SG2 y SG3 están establecidos como grupos de servidores preferidos. Para obtener más información sobre cómo establecer un grupo de servidores como necesario o preferido, consulte *Asignación de un grupo de usuarios a grupo de servidores* en *Manual del administrador de la plataforma de Business Intelligence*.




Si un usuario está asociado con múltiples grupos de usuarios y cada grupo de usuarios está asignado a un grupo de servidores diferente, la plataforma calcula el grupo de servidores disponible. En el escenario antes mencionado, el job de programación se ejecuta con éxito porque el objeto no tiene asignaciones de grupo de usuarios y el grupo de servidores disponible para programar el objeto es la combinación de SG1, SG2 y SG3.

**Escenario 4:**

Además del escenario 3, ha asignado el objeto a SG1 y ha establecido SG1 como necesario. Para obtener más información sobre cómo establecer un grupo de servidores como necesario o preferido, consulte *Asignación de un grupo de usuarios a grupo de servidores* en *Manual del administrador de la plataforma de Business Intelligence*.




Si un grupo de servidores se asigna a un objeto, la plataforma comprueba si usted ha proporcionado el usuario con los derechos de visualización en el grupo de servidores. En este escenario, la plataforma no calcula el grupo de servidores disponible porque una asignación de grupo de servidores a nivel de objeto tiene la prioridad más alta. En el escenario 4, el objeto está programado correctamente porque UG1 tiene derechos de visualización en SG1 y el usuario hereda estos derechos de UG1.

→ Recuerde

- Antes de programar un objeto, verifique las asignaciones del grupo de servidores a todos los grupos de usuarios asociado con el usuario y calcule el grupo de servidores disponible.
- Un job de programación se ejecuta con éxito si el grupo de servidores disponible para un usuario incluye el grupo de servidores asignado al objeto.

Consulte la tabla siguiente:

ⓘ Nota

Considere que SG1 y SG2 están asignados a los grupos de usuarios UG1 y UG2, respectivamente.

| Nivel de acceso | Combinación de grupos de servidores (SG1 + SG2) | Buscar servidores en el pool común |
|---|---|---|
| El usuario tiene derechos en todos los grupos de servidores | Requerido + Requerido | False |

| Nivel de acceso | Combinación de grupos de servidores (SG1 + SG2) | Buscar servidores en el pool común |
|---|---|---|
| El usuario tiene derechos en todos los grupos de servidores | Requerido + Preferido | False |
| El usuario tiene derechos en todos los grupos de servidores | Preferido + Preferido | True |
| El usuario no tiene derechos en ningún grupo de servidores | Requerido + Requerido | False |
| El usuario no tiene derechos en ningún grupo de servidores | Requerido + Preferido | False |
| El usuario no tiene derechos en ningún grupo de servidores | Preferido + Preferido | True |
| El usuario tiene derechos en algunos grupos de servidores | Requerido (No) + Requerido (Sí) | False |
| El usuario tiene derechos en algunos grupos de servidores | Requerido (No) + Preferido (Sí) | False |
| El usuario tiene derechos en algunos grupos de servidores | Requerido (Sí) + Preferido (No) | False |
| El usuario tiene derechos en algunos grupos de servidores | Preferido (No) + Preferido (Sí) | True |

## 11.9 Configurar servidores de procesamiento de Adaptive para sistemas de producción

El programa de instalación instala un servidor de procesamiento de Adaptive (APS) por sistema de host. Dependiendo de las funciones que tenga instaladas, este APS puede alojar un gran número de servicios, como el servicio de supervisión, el servicio de administración de promociones, el servicio de análisis multidimensional (MDAS), el servicio de publicación, entre otros.

Para los sistemas de producción o de prueba, la mejor práctica es crear APS adicionales y configurar los APS para que cumplan con los requisitos empresariales.

Puede crear APS adiciones de dos modos:

- Ejecutar el Asistente de configuración del sistema.
  El asistente le ayuda con la configuración básica del sistema de la plataforma de BI, incluida la configuración de APS según plantillas de despliegue predefinidas. La configuración de APS que proporciona el asistente es un buen punto de inicio; sin embargo, se debe realizar el cambio de tamaño del sistema.

- Use la CMC para crear y configurar manualmente APS adicionales.

Para obtener información acerca de cómo configurar servidores de procesamiento Adaptive para sistemas de producción, consulte el siguiente artículo KBA en: 1694041.

> → Recuerde
>
> Seleccionar una plantilla del despliegue en el asistente o crear manualmente APS adicionales no reemplaza el cambio de tamaño del sistema. Asegúrese de que se lleva a cabo el cambio de tamaño: http://www.sap.com/bisizing.

## 11.10 Evaluación del rendimiento del sistema

### 11.10.1 Supervisar servidores de la plataforma de BI

La aplicación de supervisión proporciona la capacidad de capturar métricas históricas y de tiempo de ejecución de los servidores de la plataforma de BI para la generación de informes y notificaciones. La aplicación ayuda a los administradores del sistema a identificar si los servidores funcionan de forma normal y si los tiempos de respuesta son los esperados.

#### Información relacionada

Supervisión [página 811]

### 11.10.2 Análisis de las medidas del servidor

La consola de administración central (CMC) permite ver las medidas para los servidores del sistema. Estas medidas incluyen información general acerca de cada equipo, junto con detalles que son específicos del tipo de servidor. La CMC también permite ver las medidas del sistema, que incluyen información acerca de la versión del producto, el CMS y la actividad del sistema actual.

> ⓘ Nota
>
> Sólo se pueden ver las medidas para servidores que se ejecuten actualmente.

#### 11.10.2.1 Para ver las medidas de un servidor

1. Vaya al área de administración *Servidores* de CMC.

2. Haga clic con el botón derecho en el servidor cuyas métricas desea ver y seleccione *Métricas*.

La ficha *Métricas* muestra una lista de métricas para el servidor.

### Información relacionada

Para cambiar las propiedades de un servidor [página 462]
Acerca del apéndice de métrica de servidor [página 1199]

## 11.10.3 Ver las medidas del sistema

En el área de administración *Configuración* de la CMC se muestran las métricas del sistema que proporcionan información general acerca de la instalación de la plataforma de BI. La sección *Propiedades* incluye información acerca de la versión y la compilación del producto. También muestra el origen de datos, el nombre de base de datos y el nombre de usuario de la base de datos de CMS. La sección *Ver métricas globales del sistema* muestra la actividad de la cuenta actual, junto con las estadísticas acerca de las tareas actuales y procesadas. La sección *Clúster* muestra el nombre del CMS al que está conectado, el nombre del clúster del CMS y los nombres de los miembros de otros clústeres.

### 11.10.3.1 Para ver las medidas del sistema

1. Diríjase al área de administración *Configuración* de la CMC.
2. Haga clic en una flecha para expandir y ver la configuración en el área *Propiedades*, *Ver métricas globales del sistema*, *Clúster*, o *Copia de seguridad activa*.

## 11.10.4 Registrar la actividad de los servidores

La plataforma de BI le permite registrar información específica sobre la actividad Web de la plataforma de BI.

- Además, cada servidor de la plataforma de BI está diseñado para registrar mensajes en el registro del sistema estándar del sistema operativo.
  - En Windows, la plataforma de BI se registra en el servicio de Registro de eventos. Puede ver los resultados con Visor de sucesos (en Registro de aplicación).
  - En UNIX, la plataforma de BI registra la subrutina syslog como aplicación de usuario. Cada servidor antepone su nombre y PID a los mensajes que registra.

Cada servidor también registra mensajes de confirmación en el directorio de registro de la instalación del producto. La información programática registrada en estos archivos normalmente solo resulta útil para el personal de soporte de SAP BusinessObjects, con el fin de llevar a cabo una depuración avanzada. La ubicación de estos archivos de registro depende del sistema operativo:

- En Windows, el directorio de registro predeterminado es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\logging`.
- En UNIX, el directorio de registro predeterminado es `<DIRINSTALACIÓN>/sap_bobj/logging` de la instalación.

La cuestión importante que hay que tener en cuenta es que estos archivos de registro se limpian automáticamente, por lo que nunca habrá más de 1 MB (aproximadamente) de datos registrados por servidor.

> **Nota**
>
> Para que funcione el registro en equipos UNIX que alojan servidores de la plataforma de BI, debe instalar y configurar el registro del sistema de registro de modo que se guarden todos los mensajes registrados en la función «user» del nivel «info» o superior. Debe configurar `SYSLOGD` para aceptar el registro remoto.
>
> Los procedimientos de configuración varían de un sistema a otro. Consulte la documentación del sistema operativo para obtener instrucciones específicas.

## 11.11 Configuración de las opciones de servidor

En esta sección se incluye información técnica y procedimientos que muestran cómo modificar la configuración de los servidores de la plataforma de BI.

La mayoría de los parámetros que se tratan en esta sección le permiten integrar de forma más eficaz la plataforma de BI con sus configuraciones actuales de hardware, software y red. Por lo tanto, los valores que elija dependerán considerablemente de sus propios requisitos.

Puede cambiar la configuración del servidor a través de la Consola de administración central (CMC) de dos modos.

- En la pantalla *Propiedades* para el servidor.
- En la pantalla *Editar servicios comunes* del servidor.

Es importante tener en cuenta que no todos los cambios se producen inmediatamente. Si una configuración no se puede cambiar de inmediato, las pantallas *Propiedades* y *Editar servicios comunes* mostrarán la configuración actual (en texto rojo) y la configuración deseada. Al volver al área de administración Servidores, el servidor se marcará como Bloqueado. Al reiniciar el servidor, usará la configuración deseada y el marcador bloqueado se eliminará del servidor.

> **Nota**
>
> En esta sección no se muestra cómo configurar el servidor de aplicaciones Web para desplegar aplicaciones de la plataforma de BI. Esta tarea se suele llevar a cabo al instalar el producto. Para obtener más detalles, consulte el *Manual de instalación de la* plataforma SAP BusinessObjects Business Intelligence.

## Información relacionada

Configurar los números de puerto [página 471]
Para cambiar las propiedades de un servidor [página 462]
Creación de nuevo de la base de datos del sistema de CMS [página 512]
Selección de una base de datos del CMS nueva o existente [página 509]

## 11.11.1 Para cambiar las propiedades de un servidor

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el servidor cuya configuración desea cambiar.
   Aparecerá la pantalla *Propiedades*.
3. Realice los cambios que desee y, a continuación, haga clic en *Guardar* o *Guardar y cerrar*.

> ⓘ Nota
>
> No todos los cambios se producen inmediatamente. Si una configuración no cambia de inmediato, el cuadro de diálogo Propiedades muestra la configuración actual (en texto rojo) y la configuración deseada. Al volver al área de administración Servidores, el servidor se marcará como Bloqueado. Al reiniciar el servidor, utilizará la configuración deseada del cuadro de diálogo Propiedades y el marcador se eliminará del servidor.

## 11.11.2 Aplicar configuraciones de servicios a varios servidores

Puede aplicar la misma configuración a servicios que se alojan en varios servidores.

1. Vaya al área de administración *Servidores* de la CMC.
2. Mientras tiene `Ctrl` pulsado, haga clic en cada servidor que aloje servicios en los que quiera modificar la configuración y después haga clic con el botón derecho y seleccione *Editar servicios comunes*.
   Aparece el cuadro de diálogo *Editar servicios comunes*, en el que se muestra una lista de los servicios alojados en los servidores que ha seleccionado que tienen una configuración que puede cambiar.
3. Si en el cuadro de diálogo *Editar servicios comunes* se muestra más de un servicio, seleccione el servicio que desea editar y haga clic en *Continuar*.
4. Realice los cambios oportunos y haga clic en *Aceptar*.

> ⓘ Nota
>
> Se le redirigirá al área de administración *Servidores* de la CMC. Si un servidor necesita que se reinicie, se marca como Bloqueado. Al reiniciar el servidor, usa la configuración nueva y se elimina la etiqueta Bloqueado.

## 11.11.3 Trabajo con plantillas de configuración

Las plantillas de configuración permiten configurar fácilmente varias instancias de servidores. Las plantillas de configuración almacenan una lista de configuraciones para cada tipo de servicio, que se puede usar para configurar instancias de servidor adicionales. Por ejemplo, si tiene una docena de servidores de procesamiento de Web Intelligence que desea configurar idénticamente, solo necesita configurar las opciones de uno de ellas. A continuación, puede utilizar el servicio configurado para definir la plantilla de configuración para servidores de procesamiento de Web Intelligence y, a continuación, aplicar la plantilla a los demás 11 instancias de servicio.

Cada tipo de servicio de plataforma BI tiene su propia plantilla de configuración. Por ejemplo, si hay una plantilla de configuración para el tipo de servicio de procesamiento de Web Intelligence, uno para el tipo de servicio Publishing, etc. La plantilla de configuración está definida en las propiedades del servidor en la Consola de administración central (CMC).

Cuando se asigna una plantilla de configuración a un servidor, los valores existentes del servidor se sobrescriben con los valores de la plantilla. Si posteriormente decide dejar de usar la plantilla, no se restaurará la configuración original. Los cambios posteriores en la plantilla de configuración no afectarán al servidor.

Resulta conveniente utilizar las plantillas de configuración del siguiente modo:

1. Defina la plantilla de configuración en un servidor.
2. Suponiendo que desea la misma configuración en todos los servidores del mismo tipo, active *Usar plantilla de configuración* para todos los servidores del mismo tipo, también en el que se ha establecido la plantilla de configuración.
3. Más tarde, si desea cambiar la configuración de todos los servicios de este tipo, ver las propiedades de cualquiera de los servicios, anule la selección de la casilla de verificación *Usar plantilla de configuración*. Cambie la configuración que desee y, a continuación, seleccione *Establecer plantilla de configuración* para este servidor y haga clic en *Guardar*. Todos los servicios de este tipo se actualizan. Al no tener un servidor que siempre esté establecido como la plantilla de configuración, asegúrese de que no cambia accidentalmente las opciones de configuración para todos los servidores de este tipo.

### Información relacionada

Para establecer una plantilla de configuración [página 463]
Para aplicar una plantilla de configuración a un servidor [página 464]

## 11.11.3.1 Para establecer una plantilla de configuración

Puede establecer una plantilla de configuración para cada tipo de servicio. No puede configurar varias plantillas de configuración para un servicio. Puede utilizar la página *Propiedades* de cualquier servidor para configurar las opciones que utilizará la plantilla de configuración para un tipo de servicio que está alojado en el servidor.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el servidor que aloja los servicios cuya plantilla de configuración desea establecer.

Aparecerá la pantalla *Propiedades*.

3. Para configurar las opciones de servicio que desee utilizar en la plantilla, seleccione la casilla de verificación *Establecer plantilla de configuración* y haga clic en *Guardar* o *Guardar y cerrar*.

La plantilla de configuración para el tipo de servicio que ha seleccionado se define según la configuración del servidor actual. Otros servidores del mismo tipo que alojen los mismos servicios se volverán a configurar automática e inmediatamente para corresponderse con la plantilla de configuración si tienen activada la opción *Establecer plantilla de configuración* en sus propiedades.

> **Nota**
>
> Si no define explícitamente las opciones de la plantilla de configuración, se usará la configuración predeterminada del servicio.

### Información relacionada

Para aplicar una plantilla de configuración a un servidor [página 464]

## 11.11.3.2 Para aplicar una plantilla de configuración a un servidor

Antes de aplicar una plantilla de configuración, asegúrese de que ha definido las opciones de plantilla de configuración para el tipo del servidor al que desea aplicar la plantilla. Si no ha definido explícitamente los valores de la plantilla de configuración, se utilizará la configuración predeterminada del servicio.

> **Nota**
>
> Los servidores que no tienen la opción Usar plantilla de configuración no se actualizarán al modificar la configuración de la plantilla de configuración.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el servidor que aloja el servicio al que desea aplicar la plantilla de configuración. Aparecerá la pantalla *Propiedades*.
3. Seleccione la casilla de verificación *Usar plantilla de configuración* y haga clic en *Guardar* o *Guardar y cerrar*.

   > **Nota**
   >
   > Si el servidor requiere reiniciarlo para que surta efecto la nueva configuración, se mostrará como "bloqueado" en la lista de servidores.

Se aplica la plantilla de configuración adecuada al servidor actual. Los cambios posteriores en la plantilla de configuración cambiarán la configuración de todos los servidores que usan dicha plantilla.

La desactivación de *Usar plantilla de configuración* no restaura la configuración de servidor a los valores que había cuando se aplicó la plantilla de configuración. Los cambios posteriores en la plantilla de configuración no afectan a la configuración de los servidores que usan la plantilla de configuración.

### Información relacionada

Para establecer una plantilla de configuración [página 463]

## 11.11.3.3 Para restaurar los valores predeterminados del sistema

Puede restaurar la configuración de un servicio según los valores con los que se había instalado inicialmente (por ejemplo, si configura incorrectamente los servidores o se producen problemas de rendimiento).

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el servidor que aloja un servicio para el que desea restaurar los valores predeterminados del sistema.
   Aparecerá la pantalla *Propiedades*.
3. Seleccione la casilla de verificación *Restaurar valores predeterminados del sistema* y haga clic en *Guardar* o *Guardar y cerrar*.
   Se restauran los ajustes predeterminados para el tipo de servicio concreto.

# 11.12 Configuración de las opciones de red

La configuración de red de los servidores de la plataforma de BI se administra mediante la CMC. Esta configuración se divide en dos categorías: configuración de puerto e identificación de host.

### configuración predeterminada

Durante la instalación, los identificadores de host se configuran en *Asignar automáticamente*. No obstante, a cada servidor se le puede asignar una dirección IP específica o un nombre de host. El puerto predeterminado del CMS es el 6400. Los demás servidores de BusinessObjects Enterprise se enlazan dinámicamente a los puertos disponibles. Los números de puerto los administra automáticamente la plataforma de BI, pero puede utilizar la configuración de CMC para especificar números de puerto.

## 11.12.1 Opciones de entorno de red

La plataforma de BI es compatible con la versión 4 del protocolo de Internet (IPv4) y tráfico en la red mixta IPv4/IPv6. Puede usar los componentes de servidor y cliente en cualquiera de los siguientes entornos:

- Red IPv4: todos los componentes de servidor y cliente se ejecutan sólo con el protocolo IPv4.
- Red IPv6/IPv4 mixta: los componentes de servidor y cliente se pueden ejecutar con los protocolos IPv6 e IPv4.

por ejemplo

- solo IPv6-(con una pila IPv6 habilitada, una pila IPv4 instalada y una pila IPv4 deshabilitada)
- IPv6/IPv4 mixta (ambos con una pila IPv6 y IPv4 habilitada)
- solo hosts IPv4 (con una pila IPv4 habilitada, con una pila IPv6 deshabilitada o desinstalada).

> **Nota**
>
> - El administrador del sistema y de la red debe efectuar la configuración de la red. La plataforma de BI no proporciona ningún mecanismo para designar un entorno de red. Puede usar la CMC para enlazar a una dirección IPv6 o IPv4 específica para cualquiera de los servidores de la plataforma de BI.
> - No es compatible con pila IPv6 pura (IPV6 instalada y habilitada sola). De todos modos, la red IPv6 mixta es compatible.

### 11.12.1.1 Entorno IPv6/IPv4 mixto

El entorno de red IPv6/IPv4 mixto le permite lo siguiente:

- Los servidores de la plataforma de BI pueden proporcionar servicio a ambas solicitudes IPv6 y IPv4 al ejecutarlas en modo IPv6/IPv4.
- Los componentes de cliente pueden interoperar con servidores como nodos IPv4 solo o nodos IPv6/IPv4.

El modo mixto resulta muy útil en los siguientes escenarios:

- Está cambiando de un entorno de nodo solo IPv4 a un nodo IPv6 mixto. Todos los componentes de cliente y de servidor seguirán interoperando perfectamente hasta que se complete la transición. A continuación, puede desactivar la configuración de IPv4 para todos los servidores.
- El software de terceros que no es compatible con IPv6 seguirá funcionando en el entorno de nodos IPv6/IPv4.

## 11.12.2 Opciones de identificación de host de servidor

Las opciones de identificación de host se pueden especificar en la CMC para todos los servidores de la plataforma de BI. En la tabla siguiente se resumen las opciones disponibles en el área *Configuración común*:

| Opción | Descripción |
|---|---|
| *Asignar automáticamente* | Es el comportamiento predeterminado para todos los servidores. Cuando se activa Asignar automáticamente, el servidor enlaza automáticamente el puerto de solicitud del servidor en la primera interfaz de red del equipo.<br><br>**Nota**<br>Es una buena práctica seleccionar la casilla de verificación *Asignar automáticamente* para la |

| Opción | Descripción |
| --- | --- |
| | configuración del nombre de host. Sin embargo, en algunos casos, como, por ejemplo, cuando el servidor se está ejecutando en un equipo multibase, o cuando el servidor necesita interactuar con una determinada configuración, debe considerar la posibilidad de usar un nombre de host específico o una dirección IP.<br>Para obtener más información sobre cómo configurar un equipo multibase y trabajar con servidores de seguridad, consulte el*Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*. |
| *Nombre de host* | Especifica el nombre de host de la interfaz de red en la que el servidor escucha las solicitudes. Para el CMS, esta configuración especifica el nombre de host de la interfaz de red que el CMS enlaza al puerto del servidor de nombres y al puerto de solicitud. |
| *Dirección IP* | Especifica la dirección IP de la interfaz de red en la que el servidor escucha las solicitudes. Para el CMS, esta configuración especifica la dirección de la interfaz de red que el CMS enlaza al puerto del servidor de nombres y al puerto de solicitud. Para todos los servidores se proporcionan campos independientes para especificar las direcciones IP IPv4 y/o IPv6. |

⚠ Precaución

Si especifica *Asignar automáticamente* en equipos multibase, el CMS puede enlazar automáticamente con la interfaz de red errónea. Para impedir que esto ocurra, asegúrese de que las interfaces de red del equipo host estén enumeradas en el orden correcto (mediante las herramientas del SO del equipo). También debe especificar la configuración de nombre de host para el CMS en la CMC.

ⓘ Nota

Si trabaja con equipos multibase o en determinadas configuraciones de servidor de seguridad NAT, puede que necesite especificar el nombre de host mediante nombres de dominio completos en vez de nombres de host.

## Información relacionada

Para configurar el sistema para servidores de seguridad [página 208]
Configurar un equipo multibase [página 468]
Para solucionar problemas de varias interfaces de red [página 470]

### 11.12.2.1 Para modificar la identificación de host de un servidor

1. Vaya al área de administración *Servidores* de CMC.
2. Seleccione el servidor y, a continuación, elija *Detener servidor* en el menú *Acciones*.
3. Elija *Propiedades* en el menú *Administrar*.
4. En *Configuración común*, seleccione una de las siguientes opciones:

| Opción | Descripción |
|---|---|
| **Asignar automáticamente** | El servidor enlazará a una de las interfaces de red disponibles. |
| **Nombre de host** | Introduzca el nombre de host de la interfaz de red en la que el servidor escucha las solicitudes. |
| **Dirección IP** | Introduzca en los campos proporcionados una dirección IP IPv4 o IPv6 para la interfaz de red en la que el servidor escucha las solicitudes.<br>**Nota**<br>Para activar el servidor con el fin de que actúe como un nodo IPv4/IPv6 dual, introduzca una dirección IP válida en ambos campos. |

5. Haga clic en *Guardar* o en *Guardar y cerrar*.
   Los cambios se reflejan en la línea de comandos que se muestra en la ficha *Propiedades*.
6. Inicie y habilite el servidor.

## 11.12.3 Configurar un equipo multibase

Un equipo multibase es el que tiene varias direcciones de red. Se puede realizar con varias interfaces de red, cada una con una o varias direcciones IP, o con una sola interfaz de red a la que se hayan asignado varias direcciones IP.

Si tiene varias interfaces de red, cada una con una sola dirección IP, cambie el orden de enlace de modo que la interfaz de red del principio del orden de enlace sea a la que desea enlazar los servidores de los Servicios de la plataforma de BI. Si la interfaz dispone de varias direcciones IP, use la opción Nombre de host de la CMC para especificar una tarjeta de interfaz de red para el servidor de la plataforma de BI. Se puede especificar por nombre de host o por dirección IP. Para obtener información acerca de la configuración del ajuste de *Identificadores de host*, consulte «Para solucionar problemas en varias interfaces de red».

**→ Sugerencias**

En esta sección se muestra el modo de restringir todos los servidores a la misma dirección de red, pero es posible enlazar servidores individuales a direcciones distintas. Por ejemplo, puede que desee enlazar los servidores del repositorio de archivos a una dirección privada que no se pueda enrutar desde los equipos de los usuarios. Las configuraciones avanzadas como ésta requieren que la configuración de DNS direccione las comunicaciones de forma eficaz entre todos los componentes de servidor de la plataforma de BI. En este ejemplo, el DNS debe direccionar las comunicaciones desde los otros servidores de la plataforma de BI a la dirección privada de los Servidores del repositorio de archivos.

## Información relacionada

Para solucionar problemas de varias interfaces de red [página 470]

# 11.12.3.1 Para configurar el CMS para enlazar a una dirección de red

> **Nota**
>
> En un equipo multibase, el identificador de host se puede configurar en el nombre de dominio completamente cualificado o la dirección IP de la interfaz a la que desea enlazar el servidor.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el CMS.
3. En *Configuración común*, seleccione una de las siguientes opciones:
   - *Nombre de host*
   - Introduzca el nombre de host de la interfaz de red a la que se enlazará el servidor.
   - *Dirección IP*
   - Introduzca en los campos proporcionados una dirección IP IPv4 o IPv6 para la interfaz de red a la que se enlazará el servidor.

     > **Nota**
     >
     > Para activar el servidor con el fin de que actúe como un nodo IPv4/IPv6 dual, introduzca una dirección IP válida en ambos campos.

   > **Precaución**
   >
   > No seleccione Asignar automáticamente.

4. Para *Puerto de solicitud* puede realizar una de las acciones siguientes:
   - Seleccione la opción *Asignar automáticamente*.
   - Introduzca un número de puerto válido en el campo *Puerto de solicitud*.
5. Asegúrese de que se especifica un número de puerto en el cuadro de diálogo Puerto del servidor de nombres.

   > **Nota**
   >
   > El número de puerto predeterminado es el 6400.

## 11.12.3.2 Configuración de los demás servidores para enlazar a una dirección de red

Los servidores restantes de la plataforma de BI seleccionan sus puertos dinámicamente de forma predeterminada. Para obtener información sobre cómo desactivar el valor Asignar automáticamente que propaga dinámicamente esta información, consulte «Cambiar el puerto que utiliza un servidor para aceptar solicitudes».

### Información relacionada

Para cambiar el puerto que un servidor usa para aceptar solicitudes [página 474]

## 11.12.3.3 Para solucionar problemas de varias interfaces de red

En un equipo multibase, el CMS puede enlazar automáticamente con la interfaz de red errónea. Para impedir que esto ocurra, puede asegurarse de que las interfaces de red del equipo host estén enumeradas en el orden correcto (mediante las herramientas del sistema operativo del equipo), o asegúrese de especificar la configuración Nombre de host para el CMS en la CMC. Si la interfaz de red principal no se puede enrutar, puede usar el siguiente procedimiento para configurar la plataforma de BI para que se enlace a una interfaz de red no primaria que se pueda enrutar. Lleve a cabo estos pasos justo después de instalar la plataforma de BI en el equipo local, antes de instalar la plataforma de BI en otros equipos.

1. Abra el CCM y detenga el SIA correspondiente al nodo en el equipo que tiene varias interfaces de red.
2. Haga clic con el botón derecho del ratón en el SIA y elija *Propiedades*.
3. En el cuadro de diálogo *Propiedades*, haga clic en la ficha *Configuración*.
4. Para vincular SIA a una interfaz de red específica, escriba el número de puerto de la interfaz de red de destino en el campo *Puerto*.
5. Haga clic en *Aceptar* y seleccione la ficha *Inicio*.
6. En la lista *Servidores del CMS locales* seleccione el CMS y haga clic en *Propiedades*.
7. Para vincular el CMS a una interfaz de red específica, escriba el número de puerto de la interfaz de red de destino en el campo *Puerto*.
8. Haga clic en *Aceptar* para aplicar los nuevos ajustes.
9. Inicie el SIA y espere a que se inicien los servidores.
10. Inicie la Consola de administración central (CMC) y vaya al área de administración *Servidores*. Repita los pasos 11 a 14 por cada servidor.
11. Seleccione el servidor y, a continuación, elija *Detener servidor* en el menú *Acciones*.
12. Elija *Propiedades* en el menú *Administrar*.
13. En *Configuración común*, seleccione una de las siguientes opciones:
    - Nombre de host: introduzca el nombre de host de la interfaz de red a la que se enlazará el servidor.

- Dirección IP: introduzca en los campos proporcionados una dirección IP IPv4 o IPv6 para la interfaz de red a la que se enlazará el servidor.

  > **Nota**
  >
  > Para activar el servidor con el fin de que actúe como un nodo IPv4/IPv6 dual, introduzca una dirección IP válida en ambos campos.

> **Precaución**
>
> No seleccione Asignar automáticamente.

14. Haga clic en *Guardar* o en *Guardar y cerrar*.
15. Vuelva al CCM y reinicie el SIA.

    El SIA reinicia todos los servidores del nodo. Todos los servidores del equipo ahora se enlazan a la interfaz de red correcta.

## 11.12.4 Configurar los números de puerto

Durante la instalación, el CMS se configura para que use los números de puerto predeterminados. El puerto predeterminado del CMS es el 6400. Este puerto se encuentra dentro del intervalo de puertos reservados por SAP Business Objects (del 6400 al 6410). La comunicación en estos puertos no debería entrar en conflicto con aplicaciones de terceros.

Una vez iniciados y habilitados, cada uno de los otros servidores de la plataforma de BI se enlaza de manera dinámica con un puerto disponible (superior al 1024), se registra con este puerto en el CMS y, a continuación, atiende las solicitudes de la plataforma de BI. Si es necesario, puede ordenar a cada componente del servidor que escuche en un puerto específico (en lugar de seleccionar de manera dinámica cualquier puerto disponible). Por ejemplo, tendrá que configurar manualmente un puerto de solicitud para cada servidor de la plataforma de BI que debe comunicarse a través de un servidor de seguridad.

Los números de puerto se pueden especificar en la ficha Propiedades de cada servidor en la CMC. En esta tabla se resume cómo se relacionan las opciones en el área *Configuración común* con el uso de puertos para tipos de servidores específicos.

| Parámetro | CMS | Otros servidores |
|---|---|---|
| Puerto de solicitud | Especifica el puerto que el CMS utiliza para aceptar todas las solicitudes de otros servidores (excepto para las solicitudes del servidor de nombres). Utiliza la misma interfaz de red que el puerto del servidor de nombres. Cuando se activa *Asignar automáticamente*, el servidor utiliza automáticamente un número de puerto asignado por el sistema operativo. | Especifica el puerto en el que el servidor escucha todas las solicitudes. Cuando se activa *Asignar automáticamente*, el servidor utiliza automáticamente un número de puerto asignado por el sistema operativo. |

| Parámetro | CMS | Otros servidores |
|---|---|---|
| Puerto del servidor de nombres | Especifica el puerto de la plataforma de BI en el que el CMS atiende a solicitudes de servicio de nombres. El predeterminado es el 6400. | No aplicable. |

## 11.12.4.1 Para cambiar el puerto CMS predeterminado en la CMC

Si hay un CMS que ya se está ejecutando en el clúster, puede usar la CMC para cambiar el número de puerto de CMS predeterminado. Si no hay ningún CMS ejecutándose en el clúster, debe usar el CCM en Windows o la secuencia de comandos `serverconfig.sh` para cambiar el número de puerto.

> **Nota**
>
> El CMS utiliza la misma tarjeta de interfaz de red para el puerto de solicitud y para el puerto del servidor de nombres.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el CMS en la lista de servidores.
3. Reemplace el número del *Puerto del servidor de nombres* por el puerto en el que desea que CMS escuche. (El puerto predeterminado es el 6400.)
4. Haga clic en *Guardar y cerrar*.
5. Reinicie el CMS.

   El CMS comienza a escuchar en el número de puerto que especifique. El Agente de inteligencia de servidor propaga dinámicamente la nueva configuración a los demás servidores del nodo si tienen seleccionada la opción *Asignar automáticamente* para el puerto de solicitud. (Pueden pasar unos minutos antes de que los cambios aparezcan en la configuración de propiedades de todos los miembros del nodo.)

   La configuración que elija en la página *Propiedades* se reflejará en la línea de comandos del servidor, que también aparece en la página *Propiedades*.

## 11.12.4.2 Para cambiar el puerto CMS predeterminado en el CCM en Windows

Si no se puede acceder a ningún CMS en el clúster y desea modificar el puerto CMS predeterminado para uno o varios CMS del despliegue, deberá usar el CCM para cambiar el número de puerto del CMS.

1. Abra el CCM y detenga el SIA correspondiente al nodo.
2. Haga clic con el botón derecho del ratón en el SIA y elija *Propiedades*.
3. En el cuadro de diálogo *Propiedades*, haga clic en la ficha *Inicio*.
4. En la lista *Servidores del CMS locales*, seleccione el CMS para el que desea cambiar el número de puerto y haga clic en *Propiedades*.

5. Para vincular el CMS a un puerto específico, escriba el número de puerto en el campo *Puerto*.
6. Haga clic en *Aceptar* para aplicar los nuevos ajustes.
7. Inicie el SIA y espere a que se inicien los servidores.

### 11.12.4.3 Para cambiar el puerto CMS predeterminado en el CCM en Unix

Si no se puede acceder a ningún CMS en el clúster y desea modificar el puerto del CMS predeterminado para uno o varios CMS del despliegue, debe usar la secuencia de comandos `serverconfig.sh` para cambiar el número de puerto del CMS.

1. Use la secuencia de comandos `ccm.sh` para detener el Agente de inteligencia de servidor (SIA) que aloja el CMS cuyo número de puerto desea cambiar.
2. Ejecute la secuencia de comandos `serverconfig.sh`.

   De forma predeterminada, esta secuencia de comandos se encuentra en el directorio `<InstallDir>/sap_bobj`.
3. Seleccione *3: Modificar nodo* y pulse `Intro`.
4. Seleccione el nodo que aloja el CMS que desea modificar y pulse `Intro`.
5. Seleccione *3: Modificar un CMS local* y pulse `Intro`.
   Aparecerá una lista de los CMS alojados en el nodo.
6. Seleccione el CMS a modificar, y pulse `Intro`.
7. Escriba el nuevo número de puerto del CMS y pulse `Intro`.
8. Especifique si desea que el CMS se inicie automáticamente al iniciar el SIA y pulse `Intro`.
9. Escriba los argumentos de la línea de comandos del CMS o acepte los argumentos actuales y pulse `Intro`.
10. Escriba **`quit`** para salir de la secuencia de comandos.
11. Inicie el SIA con la secuencia de comandos `ccm.sh` y espere a que se inicien los servidores.

### 11.12.4.4 Cambiar el puerto que usa un CMS para aceptar solicitudes

1. Vaya al área de administración *Servidores* de CMC.
2. Seleccione el CMS y, a continuación, elija *Propiedades* en el menú *Gestionar*.
3. En *Configuración común*, desactive la casilla de verificación *Asignar automáticamente* para *Puerto de solicitud* y, a continuación, escriba el número de puerto en el que desee que escuche el servidor.
4. Haga clic en *Guardar* o en *Guardar y cerrar*.
5. Reinicie el CMS.

El CMS enlaza al puerto nuevo y empieza a escuchar las solicitudes de otros servidores.

### 11.12.4.5 Para cambiar el puerto que un servidor usa para aceptar solicitudes

> **Nota**
>
> Estos pasos no sirven para cambiar el puerto de peticiones del servidor de administración central (CMS). Consulte en su lugar «Para cambiar el puerto que usa un CMS para aceptar peticiones».

1. Vaya al área de administración *Servidores* de CMC.
2. Seleccione el servidor y, a continuación, elija *Detener servidor* en el menú *Acciones*.
3. Haga doble clic en el servidor.
   Aparecerá la pantalla *Propiedades*.
4. En *Configuración común*, desactive la casilla de verificación *Asignar automáticamente* para *Puerto de solicitud* y, a continuación, escriba el número de puerto en el que desee que escuche el servidor.
5. Haga clic en *Guardar* o en *Guardar y cerrar*.
6. Inicie y habilite el servidor.

El servidor se enlaza al nuevo puerto, se registra con el CMS y comienza a escuchar solicitudes de la plataforma de BI en el nuevo puerto.

## 11.13 Administración de nodos

### 11.13.1 Uso de nodos

Un nodo es un grupo de servidores de la plataforma de BI que se ejecuta en el mismo host y que el mismo Agente de inteligencia de servidor (SIA) se encarga de gestionar. Todos los servidores de un nodo se ejecutan en la misma cuenta de usuario. Un equipo puede contener varios nodos, de modo que puede ejecutar procesos bajo distintas cuentas de usuario. Un SIA gestiona y supervisa todos los servidores de un nodo, asegurándose de que funcionen correctamente.

> **Nota**
>
> Debe usar una cuenta de administración con autenticación de Enterprise para realizar todos los procedimientos de administración de nodos de forma segura. Sin embargo, si la comunicación SSL entre los servidores está habilitada, debe deshabilitar el SSL antes de realizar tareas de administración de nodos.

> **Nota**
>
> Asegúrese de que todos los controladores de base de datos para cualquier servidor de la plataforma de BI para conectarse a los orígenes de datos (por ejemplo, para que el CMS se conecte a la base de datos del CMS) estén presentes, y que el entorno correcto ya se ha establecido (por ejemplo, se han establecido las variables de entorno adecuadas).

### 11.13.1.1 Variables

| Variable | Descripción |
| --- | --- |
| `<INSTALLDIR>` | El directorio en el que la plataforma Business Intelligence de SAP BusinessObjects está instalada.<br>En Windows: `C:\Archivos de programa (x86)\SAP BusinessObjects` |
| `<SCRIPTDIR>` | El directorio en el que se ubican las secuencias de comandos de administración de nodos.<br>• En Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`<br>• En Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts` |
| `<PLATFORM32>` | El nombre del sistema operativo de Unix. Los valores aceptables son:<br>• `aix_rs6000`<br>• `linux_x86`<br>• `solaris_sparc`<br>• `win32_x86` |
| `<PLATFORM64>` | El nombre del sistema operativo de Unix. Los valores aceptables son:<br>• `aix_rs6000_64`<br>• `linux_x64`<br>• `solaris_sparcv9`<br>• `win64_x64` |

### 11.13.1.2 Preparar un equipo Unix para SQL Anywhere

Debe crear un archivo `odbc.ini` y hacer que sea el origen para poder usar SQL Anywhere como un origen de datos ODBC en un equipo Unix.

> **Nota**
>
> Este procedimiento no es necesario si usa el SQL Anywhere en paquete instalado con la plataforma de BI.

1. Cree `odbc.ini` en `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/<PLATAFORMA64>`
2. Introduzca el nombre de origen (DNS) de la base de datos, el nombre de la base de datos y el nombre del servidor de SQL Anywhere, y la dirección IP y el número de puerto del equipo que aloja el servidor de base de datos de SQL Anywhere.

3. Guarde `odbc.ini`.
4. Lleve el entorno SQL Anywhere en su entorno actual.

   Por ejemplo, si está usando Bash como shell de la línea de comandos, el origen es la versión de 64 bits de `sa_config.sh`.
5. Defina una variable de entorno denominada `ODBCINI` que indica la ubicación en el que se creó el archivo `odbc.ini`.

   Establezca la variable de entorno para que los procesos secundarios puedan ver la variable de entorno `ODBCINI`.

## Ejemplo

Un archivo `odbc.ini` de ejemplo:

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0
[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

Un comando `source` de ejemplo:

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

## Información relacionada

Variables [página 475]

# 11.13.2 Adición de un nuevo nodo

El programa de instalación crea un nodo único cuando se instala la plataforma de BI por primera vez.

Es probable que necesite nodos adicionales si desea ejecutar servidores en distintas cuentas de usuario.

Puede agregar un nuevo nodo con el Administrador de configuración central (CCM) o mediante una secuencia de comandos de administración de nodos. Si usa un servidor de seguridad, asegúrese de que los puertos del Server Intelligence Agent (SIA) y del Servidor de administración central (CMS) están abiertos.

> **Nota**
>
> Use el CCM o la secuencia de comandos de administración de nodos en el equipo en el que desea agregar un nodo. No es posible agregar un nodo en un equipo remoto.

Una instalación de la plataforma de BI es una instancia única de archivos de la plataforma de BI creada por el instalador en un equipo. Una instancia de la instalación de la plataforma de BI se puede usar solo en un clúster individual. Los nodos que pertenecen a distintos clústeres que comparten la misma instalación de la plataforma de BI no se soportan porque este tipo de despliegue no se puede revisar o actualizar. Solo la plataforma de Unix soporta varias instalaciones del software en el mismo equipo, y solo si cada instalación se lleva a cabo en una única cuenta de usuario y se instala en una carpeta separada para que las instalaciones no compartan ningún archivo.

Recuerde que todos los equipos del clúster deben tener la misma versión y el mismo nivel de revisión.

> → Recomendación
>
> Para añadir nodos a un despliegue de plataforma de BI en la que FIPS está activo y se ha configurado CORBA SSL, se recomienda utilizar la opción "Iniciar un nuevo CMS temporal".
>
> Para añadir nodos a un despliegue de plataforma de BI en la que FIPS no está activo y se ha configurado CORBA SSL, se recomienda utilizar la opción "Iniciar un nuevo CMS temporal".
>
> Para añadir nodos a un despliegue de plataforma de BI en la que FIPS está activo y no se ha configurado CORBA SSL, se recomienda utilizar el CMS existente.

## 11.13.2.1 Agregar un nodo a un nuevo equipo de un despliegue existente

Puede crear automáticamente el primer nodo en el equipo al usar el programa de instalación para agregar un nuevo equipo a un despliegue existente.

> → Sugerencias
>
> Durante la instalación, haga clic en *Expandir* y especifique el servidor de administración central existente.

Si desea crear nodos adicionales, use el Administrador de configuración central o la secuencia de comandos `serverconfig.sh`.

Para obtener más información acerca de la instalación, consulte el *Manual de instalación de la plataforma de SAP BI* .

## 11.13.2.2 Agregar un nodo en Windows

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del sistema de todo el clúster antes y después de agregar el nodo.

1. En el Administrador de configuración central (CCM), en la barra de herramientas, haga clic en *Agregar nodo*.
2. En el *Asistente para agregar nodo*, introduzca el nombre del nodo y el número de puerto del nuevo Server Intelligence Agent (SIA).

3. Seleccione si desea crear servidores en el nuevo nodo.
   - *Agregar nodo sin servidores*
   - *Agregar nodo con CMS*
   - *Agregar nodo con servidores predeterminados*
     Esta opción solo crea los servidores instalados en este equipo. No incluye todos los posibles servidores.
4. Seleccione un CMS.
   - Si el despliegue se está ejecutando, seleccione *Usar un CMS en funcionamiento* y haga clic en *Siguiente*.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS existente, las credenciales de administrador, el nombre del origen de datos, las credenciales de la base de datos del sistema y la clave de clúster.
   - Si se detiene el despliegue, seleccione *Iniciar un CMS temporal* y haga clic en *Siguiente*.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS temporal, las credenciales de administrador, el nombre del origen de datos, las credenciales de la base de datos para la base de datos del sistema y la clave de clúster. Se inicia un CMS temporal. (Se detendrá cuando el proceso finalice).

     > ⚠ Precaución
     >
     > Evite usar el despliegue mientras se ejecuta el CMS temporal. Asegúrese de que el CMS existente y el CMS nuevo usan puertos distintos.
5. Revise la página de confirmación y haga clic en *Finalizar*.
   El CCM creará un nodo. Si se producen errores, consulte el archivo de registro.

Ahora puede usar el nuevo CCM para iniciar el nuevo nodo.

## 11.13.2.2.1 Agregar un nodo en Windows con una secuencia de comandos

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del sistema de todo el clúster antes y después de agregar el nodo.

Puede usar `AddNode.bat` para agregar un nodo en un equipo Windows. Para obtener más información, consulte la sección «Parámetros de la secuencia de comandos para agregar, volver a crear y eliminar nodos».

## Ejemplo

Debido a las limitaciones de la petición de comando, debe usar una marca de inserción (^) para eludir espacios, el signo de igual (=) y el punto y coma (;) en estos parámetros, a menos que cerque el texto con comillas.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
  -siaport 6415
      -cms mycms:6400
      -username Administrator
      -password My^ Password
      -cmsport 7400
      -dbdriver mysqldatabasesubsystem
      -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
      -dbkey abc1234
      -noservers
      -createcms
```

> **Nota**
>
> Para evitar usar el acento circunflejo en las cadenas largas, puede escribir el nombre de la secuencia de comandos y todos sus parámetros en un archivo `response.bat` temporal y, a continuación, ejecutar `response.bat` sin parámetros.

## Información relacionada

Variables [página 475]
Parámetros de secuencia de comandos para agregar, volver a crear y eliminar nodos [página 493]

# 11.13.2.3 Agregar un nodo en Unix

> **Precaución**
>
> Realice la copia de seguridad de la configuración del sistema de todo el clúster antes y después de agregar el nodo.

1. Ejecute `<DIRINSTALACIÓN>/sap_bobj/serverconfig.sh`
2. Seleccione *1 - Add node* (Agregar nodo) y pulse `Intro`.
3. Escriba el nombre del nodo nuevo y pulse `Intro`.
4. Escriba el número de puerto del nuevo SIA y pulse `Intro`.
5. Seleccione si desea crear servidores en el nuevo nodo.
   - *no servers* (sin servidores)
     Crea un nodo que no contiene servidores.
   - *cms*
     Crea un CMS en el nodo pero no crea otros servidores.

- *default servers* (servidores predeterminados)
  Sólo crea los servidores instalados en este equipo. No incluye todos los posibles servidores.

6. Seleccione un CMS.
   - Si el despliegue se está ejecutando, seleccione *existing* (existente) y pulse `Intro`.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS existente, las credenciales de administrador, la información de conexión de la base de datos y las credenciales para la base de datos del sistema, y la clave de clúster.
   - Si el despliegue se detiene, seleccione *temporary* (temporal) y pulse `Intro`.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS temporal, las credenciales de administrador, la información de conexión de la base de datos y las credenciales para la base de datos del sistema, y la clave de clúster. Se inicia un CMS temporal. (Se detendrá cuando el proceso finalice).

     > ⚠ Precaución
     >
     > Evite usar el despliegue mientras se ejecuta el CMS temporal. Asegúrese de que el CMS existente y el CMS nuevo usan puertos distintos.

7. Revise la página de confirmación y pulse `Intro`.
   El CCM creará un nodo. Si se producen errores, consulte el archivo de registro.

Ahora puede ejecutar `<DIRINSTALACIÓN>/sap_bobj/ccm.sh -start <nodeName>` para iniciar el nuevo nodo.

## 11.13.2.3.1 Agregar un nodo en Unix con una secuencia de comandos

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del sistema de todo el clúster antes y después de agregar el nodo.

Puede usar `addnode.sh` para agregar un nodo en un equipo Unix. Para obtener más información, consulte la sección «Parámetros de la secuencia de comandos para agregar, volver a crear y eliminar nodos».

### Ejemplo

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
        -dbkey abc1234
  -noservers
```

```
-createcms
```

### Información relacionada

Variables [página 475]
Parámetros de secuencia de comandos para agregar, volver a crear y eliminar nodos [página 493]

## 11.13.3 Creación de nuevo de un nodo

Puede volver a crear un nodo con el Administrador de configuración central (CCM) o con una secuencia de comandos de administración de nodo, después de restaurar la configuración del servidor de todo el clúster, o si el equipo que aloja el despliegue falla, se daña o tiene un sistema de archivos dañado. Use las siguientes directrices:

- No es necesario volver a crear un nodo si vuelve a instalar el despliegue en un equipo de sustitución con las mismas opciones de instalación y el mismo nombre de nodo. El programa de instalación vuelve a crear automáticamente el nodo.
- Se debe volver a crear un nodo solo en un equipo con un despliegue existente con las mismas opciones de instalación y el mismo nivel de revisión.
- Solo debe volver a crear nodos que no existan en ningún equipo del despliegue. Asegúrese de que ningún otro equipo aloja el mismo nodo.
- A pesar de que el despliegue permite que los nodos se ejecuten en diferentes sistemas operativos, solo debe volver a crear los nodos que usen el mismo sistema operativo.
- Si usa un servidor de seguridad, asegúrese de que los puertos del Server Intelligence Agent (SIA) y del Servidor de administración central (CMS) están abiertos.

> ⓘ Nota
>
> Se deben parar todos los servidores, excepto CMS, antes de que pueda crear un nodo.

> → Recuerde
>
> Puede volver a crear un nodo solo en el equipo donde se encuentra el nodo.

### 11.13.3.1 Volver a crear un nodo en Windows

1. En el Administrador de configuración central (CCM), en la barra de herramientas, haga clic en *Agregar nodo*.
2. En el *Asistente para agregar un nodo*, introduzca el nombre del nodo y el número de puerto del Server Intelligence Agent (SIA) que se ha vuelto a crear.

> **Nota**
>
> Los nombres del nodo original y del nodo que se ha vuelto a crear deben ser idénticos.

3. Seleccione *Volver a crear nodo* y haga clic en *Siguiente*.
   - Si el nodo existe en la base de datos del sistema del Servidor de administración central (CMS), se vuelve a crear en el host local.

     > **Precaución**
     >
     > Use esta opción solo si el nodo no existe en ningún host del clúster.

   - Si el nodo no existe en la base de datos del sistema del CMS, se agregará un nuevo nodo con servidores predeterminados. Los servidores predeterminados incluyen todos los servidores instalados en el host.
4. Seleccione un CMS.
   - Si se está ejecutando el CMS, seleccione *Usar un CMS en funcionamiento* y haga clic en *Siguiente*.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS existente, las credenciales de administrador, el nombre del origen de datos, las credenciales de la base de datos del sistema y la clave de clúster.
   - Si se detiene el CMS, seleccione *Iniciar un CMS temporal* y haga clic en *Siguiente*.
     Cuando se le solicite, introduzca el nombre de host del CMS temporal, las credenciales de administrador, el nombre del origen de datos, las credenciales de la base de datos del sistema y la clave de clúster. Se inicia un CMS temporal. (Se detendrá cuando el proceso finalice).

     > **Precaución**
     >
     > Evite usar el despliegue mientras se ejecuta el CMS temporal.

5. Revise la página de confirmación y haga clic en *Finalizar*.
   El CCM vuelve a crear el nodo y agrega información acerca del nodo en el equipo local. Si se producen errores, consulte el archivo de registro.

Ahora puede usar el CCM para iniciar el nodo que se ha vuelto a crear.

### 11.13.3.1.1 Volver a crear un nodo en Windows con una secuencia de comandos

Puede usar `AddNode.bat` para volver a crear un nodo en un equipo Windows. Para obtener más información, consulte la sección «Parámetros de la secuencia de comandos para agregar, volver a crear y eliminar nodos».

## Ejemplo

Debido a las limitaciones de la petición de comando, debe usar una marca de inserción (^) para eludir espacios, el signo de igual (=) y el punto y coma (;) en estos parámetros, a menos que cerque el texto con comillas.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
  -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
  -adopt
```

> **Nota**
>
> Para evitar usar el acento circunflejo en las cadenas largas, puede escribir el nombre de la secuencia de comandos y todos sus parámetros en un archivo `response.bat` temporal y, a continuación, ejecutar `response.bat` sin parámetros.

## Información relacionada

Variables [página 475]
Parámetros de secuencia de comandos para agregar, volver a crear y eliminar nodos [página 493]

# 11.13.3.2 Volver a crear un nodo en Unix

1. Ejecute `<DIRINSTALACIÓN>/sap_bobj/serverconfig.sh`
2. Seleccione *1 - Add node* (Agregar nodo) y pulse `Intro`.
3. Escriba el nombre del nodo nuevo y pulse `Intro`.

   > **Nota**
   >
   > Los nombres del nodo original y del nodo que se ha vuelto a crear deben ser idénticos.

4. Escriba el número de puerto del nuevo SIA y pulse `Intro`.
5. Seleccione *volver a crear nodo* y pulse `Intro`.
   - Si el nodo existe en la base de datos del sistema del Servidor de administración central (CMS), se vuelve a crear en el host local.

     > **Precaución**
     >
     > Use esta opción solo si el nodo no existe en ningún host del clúster.

- Si el nodo no existe en la base de datos del sistema del CMS, se agregará un nuevo nodo con servidores predeterminados. Los servidores predeterminados incluyen todos los servidores instalados en el host.

6. Seleccione un CMS.
   - Si el despliegue se está ejecutando, seleccione *existing* (existente) y pulse `Intro`.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS existente, las credenciales de administrador, la información de conexión de la base de datos y las credenciales para la base de datos del sistema, y la clave de clúster.
   - Si el despliegue se detiene, seleccione *temporary* (temporal) y pulse `Intro`.
     Si se le solicita, introduzca el nombre de host del CMS temporal, las credenciales de administrador, la información de conexión de la base de datos y las credenciales de la base de datos del sistema, y la clave de clúster. Se inicia un CMS temporal. (Se detendrá cuando el proceso finalice).

   > ⚠ Precaución
   >
   > Evite usar el despliegue mientras se ejecuta el CMS temporal.

7. Revise la página de confirmación y pulse `Intro`.
   El CCM vuelve a crear el nodo y agrega información acerca del nodo en el equipo local. Si se producen errores, consulte el archivo de registro.

Ahora puede ejecutar `<DIRINSTALACIÓN>/sap_bobj/ccm.sh -start <nombreNodo>` para iniciar el nodo que se va vuelto a crear.

## 11.13.3.2.1 Volver a crear un nodo en Unix con una secuencia de comandos

Puede usar `addnode.sh` para volver a crear un nodo en un equipo Unix. Para obtener más información, consulte la sección «Parámetros de la secuencia de comandos para agregar, volver a crear y eliminar nodos».

### Ejemplo

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
        -adopt
```

### Información relacionada

Variables [página 475]
Parámetros de secuencia de comandos para agregar, volver a crear y eliminar nodos [página 493]

## 11.13.4 Eliminación de un nodo

Puede eliminar un nodo detenido con un Administrador de configuración central (CCM) en ejecución o con una secuencia de comandos de administración de nodo. Use las siguientes directrices:

- Eliminar un nodo también elimina permanentemente los servidores de un nodo.
- Si el clúster tiene varios equipos, elimine los nodos antes de eliminar un equipo del clúster y desinstale el software. Si elimina un equipo del clúster antes de eliminar el nodo, o si el sistema de archivos de un equipo no funciona correctamente, debe volver a crear el nodo en un equipo distinto con los mismos servidores, en el mismo clúster y, a continuación eliminar el nodo.

> → Recuerde
>
> Puede eliminar un nodo solo del equipo donde se encuentra el nodo.

### Información relacionada

Creación de nuevo de un nodo [página 481]

## 11.13.4.1 Eliminar un nodo en Windows

> ⚠ Precaución
>
> Realice la copia de seguridad de todo el clúster antes y después de eliminar un nodo.

1. Ejecute el Administrador de configuración central (CCM).
2. En el CCM, detenga el nodo que desea eliminar.
3. Seleccione el nodo y haga clic en *Eliminar nodo* en la barra de herramientas.
4. Si se le solicita, introduzca el nombre de host, el puerto y las credenciales de administrador del CMS.

El CCM elimina el nodo y todos los servidores del nodo.

> ⓘ Nota
>
> Puede borrar un nodo añadido recientemente después de configurar SSL utilizando los dos modos siguientes:
>
> - Elimine los parámetros SSL tanto del nodo creado recientemente como del nodo SIA cuyos CMSes intenta conectar.

- Añada los siguientes parámetros SSL a RemoveNode.bat antes de la declaración de clase principal y ejecútela: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Path to the SSL certificate directory" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt

### 11.13.4.1.1 Eliminar un nodo en Windows con una secuencia de comandos.

> ⚠ Precaución
>
> Realice la copia de seguridad de todo el clúster antes y después de eliminar un nodo.

Puede usar `RemoveNode.bat` para eliminar un nodo en un equipo Windows. Para obtener más información, consulte la sección «Parámetros de la secuencia de comandos para agregar, volver a crear y eliminar nodos».

#### Ejemplo

```
<SCRIPTDIR>\RemoveNode.bat -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

#### Información relacionada

Variables [página 475]
Parámetros de secuencia de comandos para agregar, volver a crear y eliminar nodos [página 493]

### 11.13.4.2 Eliminar un nodo en Unix

Antes y después de eliminar un nodo, realice una copia de seguridad de la configuración del servidor para todo el clúster.

1. Ejecute `<DIRINSTALACIÓN>/sap_bobj/ccm.sh -stop <NombreNodo>` para detener el nodo que desea eliminar.
2. Ejecute `<DIRINSTALACIÓN>/sap_bobj/serverconfig.sh`
3. Seleccione *2 - Delete node* (Eliminar nodo) y pulse `Intro`.
4. Seleccione el nodo que desee eliminar y pulse `Intro`.
5. Si se le solicita, introduzca el nombre de host, el número de puerto y las credenciales de administrador del CMS.

Se eliminan el nodo y todos los servidores del nodo.

> **Nota**
>
> Puede borrar un nodo añadido recientemente después de configurar SSL utilizando los dos modos siguientes:
>
> - Elimine los parámetros SSL tanto del nodo creado recientemente como del nodo SIA cuyos CMSes intenta conectar.
> - Añada los siguientes parámetros SSL a RemoveNode.bat antes de la declaración de clase principal y ejecútela: -Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Path to the SSL certificate directory" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt

### 11.13.4.2.1 Eliminar un nodo en Unix con una secuencia de comandos

> **Precaución**
>
> Realice la copia de seguridad de todo el clúster antes y después de eliminar un nodo.

Puede usar `removenode.sh` para eliminar un nodo de un equipo Unix. Para obtener más información, consulte la sección «Parámetros de la secuencia de comandos para agregar, volver a crear y eliminar nodos».

#### Ejemplo

```
<SCRIPTDIR>\removenode.sh -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

#### Información relacionada

Variables [página 475]
Parámetros de secuencia de comandos para agregar, volver a crear y eliminar nodos [página 493]

## 11.13.5 Cambiar el nombre de un nodo

Puede cambiar el nombre de un nodo con el Administrador de configuración central (CCM). Para poder cambiar el nombre de un nodo, debe crear un nuevo nodo con el nuevo nodo, clonar los servidores del nodo original en el nuevo nodo y eliminar el nodo original. Use las siguientes directrices:

- Si cambia el nombre del equipo en el que está ubicado el nodo, no necesita cambiar el nombre del nodo. Puede seguir usando el nombre del nodo existente.

- Si usa un servidor de seguridad, asegúrese de que los puertos del Server Intelligence Agent (SIA) y del Servidor de administración central (CMS) están abiertos.

> → Recuerde
>
> Puede cambiar el nombre de un nodo solo en el equipo donde se encuentra el nodo.

### Información relacionada

Adición de un nuevo nodo [página 476]
Eliminación de un nodo [página 485]

## 11.13.5.1 Cambiar el nombre de un nodo en Windows

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del servidor de todo el clúster antes y después de cambiar el nombre del nodo.

1. Inicie el Administrador de configuración central (CCM).
2. En el Administrador de configuración central (CCM), en la barra de herramientas, haga clic en *Agregar nodo*.
3. En el *Asistente para agregar un nodo*, introduzca el nombre del nodo y el número de puerto del nuevo Server Intelligence Agent (SIA), las credenciales de administrador, la información de conexión de la base de datos, las credenciales de la base de datos del sistema y la clave de clúster.
4. Seleccione *Agregar nodo sin servidores*.
5. Después de crear el nodo, use la página *Administración del servidor* de la Consola de administración central para clonar todos los servidores del nodo original en el nuevo nodo.

   > ⓘ Nota
   >
   > Asegúrese de que los servidores clonados no presentan conflictos en los puertos con servidores del nodo antiguo.

6. En el CCM, inicie el nuevo nodo.
7. Después de que el nuevo nodo se haya ejecutado durante cinco minutos, use el CCM para eliminar el nodo original.

### Información relacionada

Adición de un nuevo nodo [página 476]
Eliminación de un nodo [página 485]

## 11.13.5.2 Cambiar el nombre de un nodo en Unix

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del servidor de todo el clúster antes y después de cambiar el nombre del nodo.

1. Ejecute `<DIRINSTALACIÓN>/sap_bobj/serverconfig.sh`
2. Seleccione *1 - Add node* (Agregar nodo) y pulse `Intro`.
3. Escriba el nombre del nodo nuevo y pulse `Intro`.
4. Escriba el número de puerto del nuevo SIA y pulse `Intro`.
5. Si se solicita, introduzca las credenciales de administrador, la información de conexión de la base de datos, las credenciales para la base de datos del sistema y la clave de clúster.
6. Seleccione *sin servidores* y pulse `Intro`.
7. Después de crear el nodo, use la página *Administración del servidor* de la Consola de administración central para clonar todos los servidores del nodo original en el nuevo nodo.

   > ⓘ Nota
   >
   > Asegúrese de que los servidores clonados no presentan conflictos en los puertos con servidores del nodo antiguo.

8. Ejecute `<DIRINSTALACIÓN>/sap_bobj/ccm.sh -start <nombreNodo>` para iniciar el nuevo nodo.
9. Después de que el nuevo nodo se haya ejecutado durante cinco minutos, use `serverconfig.sh` para eliminar el nodo original.

### Información relacionada

Adición de un nuevo nodo [página 476]
Clonación de servidores [página 432]
Eliminación de un nodo [página 485]

## 11.13.6 Mover un nodo

Puede mover un nodo detenido desde un clúster a otro mediante el Administrador de configuración central (CCM) o mediante una secuencia de comandos de administración de nodo. Use las siguientes directrices:

- Asegúrese de que el clúster de destino no tiene un nodo con el mismo nombre.
- Asegúrese de que todos los tipos de servidor instalados en el equipo en el que se encuentra el nodo de origen también están instalados en el clúster de destino.
- Si desea agregar un nuevo equipo al clúster de producción, pero no desea que se pueda usar el equipo hasta que haya terminado de probarlo, instale la plataforma de BI en un equipo independiente, pruebe el equipo y mueva el nodo a un clúster de producción.

- La versión de la plataforma de BI y el nivel del paquete de servicios para este equipo debe ser consistente con el resto del clúster.

> → Recuerde
>
> Puede mover un nodo solo en el equipo donde se encuentra el nodo.

## 11.13.6.1 Mover un nodo existente en Windows

En este ejemplo, el nodo que desea mover está instalado en el sistema de origen. El equipo del sistema de origen era inicialmente independiente, pero ahora se agregará al clúster de destino.

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del servidor de todo el clúster antes y después de mover un nodo.

1. Detenga el nodo en el Administrador de configuración central (CCM).
2. Haga clic con el botón derecho en el nodo y seleccione *Mover*.
3. Cuando se le solicite, seleccione el nombre del origen de datos e introduzca el nombre de host, el puerto, la información de conexión de la base de datos, las credenciales de administrador del CMS de destino y la clave de clúster.
4. Seleccione un CMS.
   - Si se está ejecutando el despliegue de origen, seleccione *Usar un CMS en funcionamiento* y haga clic en *Siguiente*.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS existente en el sistema de origen y las credenciales de administrador.
   - Si se detiene el despliegue de origen, seleccione *Iniciar un CMS temporal* y haga clic en *Siguiente*.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS temporal del sistema de origen, las credenciales de administrador, el nombre del origen de datos, las credenciales de la base de datos para la base de datos del sistema de origen y la clave de clúster. Se inicia un CMS temporal. (Se detendrá cuando el proceso finalice).

     > ⚠ Precaución
     >
     > Evite usar el despliegue mientras se ejecuta el CMS temporal.
5. Revise la página de confirmación y haga clic en *Finalizar*.
   El CCM crea un nuevo nodo en el clúster de destino con el mismo nombre y los mismos servidores que el nodo del clúster de origen. En el clúster de origen permanece una copia del nodo. Las plantillas de configuración de los servidores del nodo no se mueven. Si se producen errores, consulte el archivo de registro.

   > ⚠ Precaución
   >
   > No use el clúster de origen después de mover el nodo.
6. En el CCM, inicie el nodo que se ha movido.

## 11.13.6.1.1 Mover un nodo en Windows con una secuencia de comandos

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del servidor de todo el clúster antes y después de mover un nodo.

Puede usar `MoveNode.bat` para mover un nodo en un equipo Windows. Para obtener más información, consulte la sección «Parámetros de la secuencia de comandos para mover nodos».

### Ejemplo

Debido a las limitaciones de la petición de comando, debe usar una marca de inserción (^) para eludir espacios, el signo de igual (=) y el punto y coma (;) en estos parámetros, a menos que cerque el texto con comillas.

```
<SCRIPTDIR>\MoveNode.bat -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

> ⓘ Nota
>
> Para evitar usar el acento circunflejo en las cadenas largas, puede escribir el nombre de la secuencia de comandos y todos sus parámetros en un archivo `response.bat` temporal y, a continuación, ejecutar `response.bat` sin parámetros.

### Información relacionada

Variables [página 475]
Parámetros de secuencia de comandos para mover nodos [página 496]

## 11.13.6.2 Mover un nodo existente en Unix

En este ejemplo, el nodo que desea mover está instalado en el sistema de origen. El equipo del sistema de origen era inicialmente independiente, pero ahora se agregará al clúster de destino.

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del servidor de todo el clúster antes y después de mover un nodo.

1. Ejecute `<DIRINSTALACIÓN>/sap_bobj/ccm.sh -stop <nombreNodo>` para detener el nodo.
2. Ejecute `<DIRINSTALACIÓN>/sap_bobj/serverconfig.sh`
3. Seleccione *4 - Mover nodo* y pulse `Intro`.
4. Seleccione el nodo que desea mover y pulse `Intro`.
5. Cuando se le solicite, seleccione la información de conexión de la base de datos del sistema e introduzca el nombre de host, el puerto, las credenciales de administrador del CMS de destino y la clave de clúster.
6. Seleccione un CMS.
   - Si se está ejecutando el despliegue de origen, seleccione *existente* y pulse `Intro`.
     Si se le solicita, introduzca el nombre de host y el número de puerto del CMS existente en el sistema de origen y las credenciales de administrador.
   - Si se detiene el despliegue de origen, seleccione *temporal* y pulse `Intro`.
     Si se le solicita, introduzca el nombre de host y el puerto del CMS temporal del sistema de origen, las credenciales de administrador, la información de conexión de la base de datos y las credenciales de la base de datos del sistema de origen, y la clave de clúster. Se inicia un CMS temporal. (Se detendrá cuando el proceso finalice).

     > ⚠ Precaución
     >
     > Evite usar el despliegue mientras se ejecuta el CMS temporal. Asegúrese de que los CMS existente y temporal usan puertos distintos.
7. Revise la página de confirmación y pulse `Intro`.
   El CCM crea un nuevo nodo en el clúster de destino con el mismo nombre y los mismos servidores que el nodo del clúster de origen. En el clúster de origen permanece una copia del nodo. Las plantillas de configuración de los servidores del nodo no se mueven. Si se producen errores, consulte el archivo de registro.

   > ⚠ Precaución
   >
   > No use el clúster de origen después de mover el nodo.
8. Ejecute `<DIRINSTALACIÓN>/sap_bobj/ccm.sh -start <nombreNodo>` para iniciar el nodo que se ha movido.

### 11.13.6.2.1 Mover un nodo en Unix con una secuencia de comandos

> ⚠ Precaución
>
> Realice la copia de seguridad de la configuración del servidor de todo el clúster antes y después de mover un nodo.

Puede usar `movenode.sh` para mover un nodo en un equipo Unix. Para obtener más información, consulte la sección «Parámetros de la secuencia de comandos para mover nodos».

#### Ejemplo

```
<SCRIPTDIR>/movenode.sh -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID^=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

#### Información relacionada

Variables [página 475]
Parámetros de secuencia de comandos para mover nodos [página 496]

## 11.13.7 Parámetros de la secuencia de comandos

### 11.13.7.1 Parámetros de secuencia de comandos para agregar, volver a crear y eliminar nodos

| Parámetro | Descripción | Ejemplo |
|---|---|---|
| `-adopt` | Vuelve a crear el nodo si ya existe en el CMS. | **`-adopt`** |

| Parámetro | Descripción | Ejemplo |
| --- | --- | --- |
| `-cms` | El nombre y número de puerto del Servidor de administración central (CMS).<br><br>**⚠ Precaución**<br>No use este parámetro si usa `-usetempcms`<br><br>**ⓘ Nota**<br>Debe especificar un número de puerto si el CMS no se ejecuta en el puerto 6400 predeterminado. | **`-cms mycms:6409`** |
| `-cmsport` | • El número de puerto del CMS al iniciar un CMS temporal.<br><br>**⚠ Restricción**<br>También debe usar los parámetros `-usetempcms`, `-dbdriver`, `-connect` y `-dbkey`.<br><br>• El número puerto del CMS al crear un nuevo CMS.<br><br>**⚠ Restricción**<br>También debe usar los parámetros `-dbdriver`, `-connect` y `-dbkey`. | **`-cmsport 6401`** |
| `-connect` | La cadena de conexión de la base de datos del sistema del CMS (o del CMS temporal).<br><br>**ⓘ Nota**<br>Omita los atributos `HOSTNAME` y `PORT` al conectarse a las bases de datos de DB2, Oracle, SQL Anywhere, SQL Server o Sybase. | **`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"`** |
| `-dbdriver` | El controlador de base de datos del CMS.<br><br>Valores aceptados:<br><br>• **`db2databasesubsystem`**<br>• **`mysqldatabasesubsystem`**<br>• **`oracledatabasesubsystem`**<br>• **`sqlanywheredatabasesubsystem`**<br>• **`sqlserverdatabasesubsystem`**<br>• **`sybasedatabasesubsystem`**<br>• **`newdbdatabasesubsystem`** | **`-dbdriver mysqldatabasesubsystem`** |

| Parámetro | Descripción | Ejemplo |
|---|---|---|
| `-dbkey` | La clave del clúster. | **`-dbkey abc1234`** |
| `-name` | El nombre del nodo. | **`-name mynode2`** |
| `-noservers` | Crea un nodo sin servidores.<br>**Nota**<br>El parámetro `-createcms` adicional crea un nodo con un CMS, pero ningún otro servidor. Omita estos parámetros para crear un nodo con todos los servidores predeterminados. | **`-noservers`** |
| `-password` | La contraseña de la cuenta de administrador. | **`-password Password1`** |
| `-siaport` | El número de puerto del Server Intelligence Agent para el nodo. | **`-siaport 6409`** |
| `-username` | El nombre de usuario de la cuenta de administrador. | **`-username Administrator`** |
| `-usetempcms` | **Precaución**<br>No use este parámetro si usa `-cms`<br>Inicia y usa el CMS temporal.<br>**Nota**<br>Use un CMS temporal cuando no se esté ejecutando el despliegue. | **`-usetempcms`** |

## Información relacionada


Agregar un nodo en Windows con una secuencia de comandos [página 478]
Agregar un nodo en Unix con una secuencia de comandos [página 480]
Volver a crear un nodo en Windows con una secuencia de comandos [página 482]
Volver a crear un nodo en Unix con una secuencia de comandos [página 484]
Eliminar un nodo en Windows con una secuencia de comandos. [página 486]
Eliminar un nodo en Unix con una secuencia de comandos [página 487]

## 11.13.7.2 Parámetros de secuencia de comandos para mover nodos

| Parámetro | Descripción | Ejemplo |
|---|---|---|
| `-cms` | El nombre del Servidor de administración central (CMS) de origen.<br>**⚠ Precaución**<br>No use este parámetro si usa `-usetempcms`<br>**ⓘ Nota**<br>Debe especificar un número de puerto si el CMS no se ejecuta en el puerto 6400 predeterminado. | `-cms sourceMachine:6409` |
| `-cmsport` | • El número de puerto del CMS al iniciar un CMS temporal.<br>**⚠ Restricción**<br>También debe usar los parámetros `-usetempcms`, `-dbdriver`, `-connect` y `-dbkey`.<br>• El número puerto del CMS al crear un nuevo CMS.<br>**⚠ Restricción**<br>También debe usar los parámetros `-dbdriver`, `-connect` y `-dbkey`. | `-cmsport 6401` |
| `-connect` | La cadena de conexión de la base de datos del sistema del CMS (o el CMS temporal).<br>**ⓘ Nota**<br>Omita los atributos `HOSTNAME` y `PORT` al conectarse a las bases de datos de DB2, Oracle, SQL Anywhere, SQL Server o Sybase. | `-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"` |

| Parámetro | Descripción | Ejemplo |
| --- | --- | --- |
| `-dbdriver` | El controlador de la base de datos del CMS de origen.<br>Valores aceptados:<br>• **`db2databasesubsystem`**<br>• **`mysqldatabasesubsystem`**<br>• **`oracledatabasesubsystem`**<br>• **`sqlanywheredatabasesubsystem`**<br>• **`sqlserverdatabasesubsystem`**<br>• **`sybasedatabasesubsystem`**<br>• **`newdbdatabasesubsystem`** | **`-dbdriver mysqldatabasesubsystem`** |
| `-dbkey` | La clave de clúster de origen. | **`-dbkey abc1234`** |
| `-destcms` | El nombre del CMS de destino.<br>**Nota**<br>Debe especificar un número de puerto si el CMS no se ejecuta en el puerto 6400 predeterminado. | **`-destcms destinationMachine:6401`** |
| `-destconnect` | La cadena de conexión del la base de datos del sistema del CMS de destino.<br>**Nota**<br>Omita los atributos `HOSTNAME` y `PORT` al conectarse a las bases de datos de DB2, Oracle, SQL Anywhere, SQL Server o Sybase. | **`-destconnect "DSN=Destin BOEXI40;UID=username;PWD=passwor d;HOSTNAME=database;PORT=3306"`** |
| `-destdbdriver` | El controlador de la base de datos del CMS de destino.<br>Valores aceptados:<br>• **`db2databasesubsystem`**<br>• **`mysqldatabasesubsystem`**<br>• **`oracledatabasesubsystem`**<br>• **`sqlanywheredatabasesubsystem`**<br>• **`sybasedatabasesubsystem`**<br>• **`newdbdatabasesubsystem`** | **`-destdbdriver sybasedatabasesubsystem`** |
| `-destdbkey` | La clave de clúster de destino. | **`-destdbkey def5678`** |
| `-destpassword` | La contraseña de la cuenta de administrador en el CMS de destino. | **`-destpassword Password2`** |
| `-destusername` | El nombre de usuario de la cuenta de administrador en el CMS de destino. | **`-destusername Administrator`** |

| Parámetro | Descripción | Ejemplo |
| --- | --- | --- |
| `-password` | La contraseña de la cuenta de administrador en el CMS de origen. | `-password Password1` |
| `-username` | El nombre de usuario de la cuenta de administrador en el CMS de origen. | `-username Administrator` |
| `-usetempcms` | **⚠ Precaución**<br>No use este parámetro si usa `-cms`<br>Inicia y usa el CMS temporal.<br>**ⓘ Nota**<br>Use un CMS temporal cuando no se esté ejecutando el despliegue. | `-usetempcms` |

### Información relacionada

Mover un nodo en Windows con una secuencia de comandos [página 491]
Mover un nodo en Unix con una secuencia de comandos [página 493]

## 11.13.8 Agregar dependencias del servidor de Windows

En un entorno de Windows, cada instancia del Server Intelligence Agent (SIA) depende de los servicios Registro de eventos y Llamada a procedimiento remoto (RPC).

Si un SIA no funciona correctamente, asegúrese de que los dos servicios aparecen en la ficha *Dependencia* del SIA.

### 11.13.8.1 Agregar dependencias del servidor de Windows

1. Use el administrador de configuración central (CCM) para detener el Server Intelligence Agent (SIA).
2. Haga clic con el botón derecho en el SIA y seleccione *Propiedades*.
3. Haga clic en la ficha *Dependencia*.
4. Haga clic en *Agregar*.
   Aparece el cuadro de diálogo *Agregar dependencia* que muestra una lista de todas las dependencias disponibles.
5. Seleccione una dependencia y haga clic en *Agregar*.
6. Haga clic en *Aceptar*.
7. Use el CCM para reiniciar el SIA.

## 11.13.9 Cambiar la credenciales de usuario para un nodo

Puede usar el Administrador de configuración central (CCM) para especificar o actualizar las credenciales de usuario para el Server Intelligence Agent (SIA) si cambia la contraseña del sistema operativo o si desea ejecutar todos los servidores en un nodo con una cuenta de usuario distinta.

Todos los servidores administrados por el SIA se ejecutan en la misma cuenta. Para ejecutar un servidor mediante una cuenta que no sea del sistema, asegúrese de que la cuenta es miembro del grupo de administradores locales en el equipo del servidor y que dispone del derecho «Reemplazar un símbolo (token) de nivel de proceso».

> ⚠ Restricción
>
> En un equipo Unix, debe ejecutar la plataforma de BI con la misma cuenta que usó para instalarla. Para usar otra cuenta, vuelva a instalar el despliegue con la otra cuenta.

### 11.13.9.1 Cambiar las credenciales de usuario para un nodo en Windows

1. Use el administrador de configuración central (CCM) para detener el Server Intelligence Agent (SIA).
2. Haga clic con el botón derecho en el SIA y seleccione *Propiedades*.
3. Desactive la casilla de verificación *Cuenta del sistema*.
4. Introduzca el nombre de usuario y la contraseña y haga clic en *Aceptar*.
5. Use el CCM para reiniciar el SIA.

El SIA y los procesos del servidor inician sesión en el equipo local con la nueva cuenta de usuario.

# 11.14 Cambio del nombre de un equipo en un despliegue de la plataforma de BI

## 11.14.1 Cambio de los nombres de clúster

A continuación le presentamos las prácticas recomendadas para cambiar el nombre del clúster:

> ⚠ Precaución
>
> No implemente nunca varios clústeres con el mismo nombre.

| Condición | Acción |
| --- | --- |
| El nombre del clúster cambia. | Informe a los usuarios del nuevo nombre del clúster y pídales que lo usen (después de la primera conexión al CMS mediante la sintaxis `<nombredehost>:<puerto>`). En el nivel Web, actualice el nombre del clúster en los archivos de propiedades de todos los servidores de aplicación Web. |
| Instala otra versión de la plataforma de BI en un equipo que anteriormente tenía un CMS en ejecución o agrega el equipo a otro clúster. | • Asegúrese de que el CMS se ejecuta en otro puerto.<br>• Use varias contraseñas para los diferentes clústeres para evitar que los usuarios inicien la sesión en un clúster incorrecto. |

## 11.14.2 Cambio de direcciones IP

Para evitar cambios en la configuración que den lugar a cambios en la dirección IP del equipo, seleccione *Propiedades del servidor* en la ficha *Servidores* de la CMC y, a continuación, asegúrese de que todos los servidores enlazan a nombres de host o utilice la opción *Asignar automáticamente*. Asimismo, siga estas prácticas recomendadas:

| Condición | Acción |
| --- | --- |
| Use ODBC con la base de datos CMS o la base de datos de auditoría. | Asegúrese de que el DSN usa el nombre de host del servidor de base de datos CMS. |
| Use otro tipo de conexión de base de datos con la base de datos CMS o la base de datos de auditoría. | Use el CCM para actualizar la base de datos para usar el nombre de host del servidor de base de datos. |
| La base de datos CMS o la base de datos de auditoría se encuentra en el mismo host que el CMS. | Use `localhost` para el nombre del equipo. |
| Use la URL para las aplicaciones Web de la plataforma de BI a las que acceden los usuarios mediante exploradores Web (por ejemplo, la CMC). | Use nombres de host en lugar de direcciones IP para la URL predeterminada. Para actualizar la URL del visor predeterminado, seleccione *Configuración de procesamiento* para la aplicación seleccionada.<br><br>Por ejemplo, para Open Document, haga clic en la ficha *Aplicaciones* de la CMC, haga clic con el botón derecho en *Open Document*, y seleccione *Configuración de procesamiento*. |
| Use la URL para clientes de la plataforma de BI basados en servicios Web (por ejemplo, Crystal Reports para Java o LiveOffice). | |
| Use OpenDocument. | |

### Instrucciones alternativas

> **Nota**
>
> Siga estas instrucciones únicamente si no puede seguir las prácticas recomendadas descritas anteriormente.

Para equipos que alojen servidores

| Condición | Acción |
| --- | --- |
| El host contiene servidores de la plataforma de BI y los servidores deben estar enlazados a direcciones IP específicas. | Cambie las direcciones IP en la ficha *Servidores* de la CMC, pero no reinicie los servidores hasta que se haya actualizado todo en el equipo. A continuación, reinicie el equipo; no los servidores individuales de la plataforma de BI. |
| Una conexión de base de datos debe usar una dirección IP. | Cambie la dirección IP. |
| Se necesita cambiar una dirección IP en una red IP estática. | Cambie la dirección IP del equipo de la plataforma de BI.<br>→ Sugerencias<br>Inicie la sesión en la CMC para asegurarse de que la plataforma de BI está operativa. |

→ Recuerde

Reinicie el equipo después de realizar una acción.

Para equipos que alojen el servidor de aplicaciones Web

| Condición | Acción |
| --- | --- |
| La URL del visor predeterminado de OpenDocument debe usar una dirección IP. | Actualice la dirección IP en el campo *Establecer la dirección URL del visor predeterminado* de la sección *Configuración de procesamiento* de la ficha *Aplicaciones* de la CMC. |
| Los usuarios acceden a las aplicaciones Web de la plataforma de BI (por ejemplo, la CMC), al proporcionar una URL con una dirección IP en sus exploradores. | Informe a los usuarios de la nueva dirección IP. |
| Los clientes de la plataforma de BI basados en servicios Web (por ejemplo, Crystal Reports para Java, o LiveOffice) deben usar direcciones IP. | Configure todos los clientes para que usen la nueva dirección IP. |

## Información relacionada

Selección de una base de datos del CMS nueva o existente [página 509]

# 11.14.3 Cambio del nombre de los equipos

Puede cambiar el nombre de los equipos de un despliegue de la plataforma de BI en cualquier momento; para ello, tiene que detener todos los servidores de la plataforma de BI del equipo y después cambiarle el nombre al equipo. A continuación se indican las prácticas recomendadas para cambiar el nombre de los equipos:

| Condición | Acción |
| --- | --- |
| Inicia la sesión por primera vez. | Use el nombre del equipo del CMS (en vez del nombre del clúster). |
| Tiene un despliegue en varios equipos. | Asegúrese de que todos los servidores del CMS que hay en el resto de equipos estén en funcionamiento durante el cambio de nombre. |

## 11.14.3.1 Nivel de servidor

> **Nota**
>
> Antes de cambiar el nombre del equipo del CMS, inspeccione la configuración de todos los servidores ubicados en el equipo al que desea cambiar el nombre en la ficha «Administración del servidor» de la CMC. Si la propiedad *Nombre de host* usa el nombre de host del CMS antiguo, actualícelo con el nuevo nombre del host del CMS.

> **→ Recuerde**
>
> No reinicie los servidores hasta que termine con todos los procedimientos de cambio de nombre del equipo.

Siga estas instrucciones para cambiar el nombre de todos los equipos de nivel de servidor:

| Condición | Acción |
| --- | --- |
| El equipo al que se ha cambiado el nombre aloja un CMS y los usuarios han iniciado sesión anteriormente al proporcionar el nombre antiguo del equipo. | Informe a los usuarios del nombre del equipo del CMS y solicíteles que lo usen. |
| El equipo al que se ha cambiado el nombre aloja un CMS y los archivos de propiedades predeterminadas de la aplicación Web de la plataforma de BI contienen el nombre de host antiguo del CMS en la propiedad `cms.default`. | Actualice el nombre del equipo del CMS en la propiedad `cms.default` de todos los archivos de propiedades personalizados de todos los equipos de nivel Web. En Tomcat, los archivos de propiedades que se han creado se encuentran en `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom` de forma predeterminada.<br>**Nota**<br>So no existe ningún archivo de propiedades personalizado, cree unos nuevos. Copie los archivos de propiedades predeterminados en una carpeta personalizada y elimine todo el contenido excepto la línea `cms.default` de los archivos de propiedades personalizados. |
| Use los kits de integración de portal o las aplicaciones personalizadas. | Configure los kits de integración de portal o las aplicaciones personalizadas para usar el nuevo nombre del host del CMS. |

| Condición | Acción |
| --- | --- |
| El despliegue cumple con todas las condiciones siguientes:<br>• Un clúster tiene varios nodos.<br>• Todos los servidores del CMS se ejecutan solo en el equipo al que se ha cambiado el nombre.<br>• Al menos un nodo no aloja el CMS.<br>• Ha cambiado el nombre de un equipo con un nodo como mínimo.<br>• La dirección IP cambia durante el proceso de cambio de nombre. | Use el CCM para realizar el flujo de trabajo «Recrear nodo» en todos los nodos, excepto el nodo que aloja el CMS y, a continuación, inicie todos los nodos de la plataforma de BI del despliegue. Para obtener más información, consulte el capítulo «Administrar nodos». |

→ Recuerde

Reinicie la aplicación Web o el servidor de aplicaciones después de realizar la acción.

## Información relacionada

Creación de nuevo de un nodo [página 481]

## 11.14.3.2 Nivel Web

Si cambia el nombre del equipo que aloja el servidor de aplicaciones Web de la plataforma de SAP BusinessObjects BI, siga estas instrucciones:

| Condición | Acción |
| --- | --- |
| Cambia el nombre del equipo que aloja el servidor de aplicaciones Web de la plataforma de BI, y la dirección URL del visor predeterminado de OpenDocument usa un nombre de host del servidor de aplicaciones Web. | Inicie la sesión en la CMC y actualice la dirección URL del visor predeterminado en *Aplicaciones* > *CMC* > *Configuración de procesamiento*. |
| Cambia el nombre del equipo que aloja el servidor de aplicaciones Web de la plataforma de BI y los usuarios acceden a las aplicaciones Web de la plataforma de BI mediante una dirección URL que incluye un nombre de host del servidor de aplicaciones Web. | Solicite a sus usuarios que accedan a las aplicaciones Web de la plataforma de BI mediante una URL que incluya el nuevo nombre de host del servidor de aplicaciones Web. |
| Cambia el nombre del equipo que aloja el servidor de aplicaciones Web de la plataforma de BI y los clientes de la plataforma de BI basada en servicio Web usan los nombres de host del servidor de aplicaciones Web que hay en la URL. | Vuelva a configurar todos los clientes de la plataforma de BI basada en servicio Web para que usen el nuevo nombre de host del servidor de aplicaciones Web. |

## 11.14.3.3 Bases de datos

Si cambia el nombre del equipo que aloja la base de datos del sistema de CMS o la base de datos de auditoría, siga estas prácticas recomendadas:

| Condición | Acción |
|---|---|
| Es recomendable evitar la actualización de la dirección IP. | Use el nombre del equipo de la base de datos CMS o de la base de datos de auditoría en el nombre de origen de datos (DSN). |
| La base de datos del CMS o la base de datos de auditoría se encuentra en el mismo anfitrión que el CMS. | Use `localhost` en el DSN para evitar actualizarlo si el nombre del anfitrión cambia. |

### Base de datos del sistema de CMS

| Condición | Acción |
|---|---|
| Se cambia el nombre de un equipo que aloja la base de datos del sistema de CMS y se usa ODBC. | Actualice el DSN de la base de datos CMS al nombre de anfitrión del nuevo servidor de base de datos. |
| Se cambia el nombre de un equipo que aloja la base de datos del sistema de CMS y se usa otro tipo de conexión que no es ODBC. | Use el CCM para actualizar la base de datos CMS al nombre de anfitrión del servidor de base de datos nuevo en cada nodo del clúster. |

### Base de datos de auditoría

| Condición | Acción |
|---|---|
| Se cambia el nombre de un equipo que aloja la base de datos de auditoría y se usa ODBC. | Actualice el DSN de la base de datos de auditoría para que use el nombre de anfitrión del nuevo servidor de base de datos. |
| Se cambia el nombre de un equipo que aloja la base de datos de auditoría y se usa otro tipo de conexión que no es ODBC. | Actualice el nombre del equipo del servidor de base de datos al nombre de anfitrión del servidor de base de datos nuevo en la ficha *Auditoría* de la CMC. |

## 11.14.3.4 Servidores de repositorios de archivos

Si cambia el nombre del equipo que aloja el almacén de archivos FRS, tiene que actualizar los servidores del *repositorio de archivos de entrada* y del *repositorio de archivos de salida* de la página «Administración del servidor» de la CMC; asegurarse de que las propiedades del *Directorio de almacenamiento de archivos* y del *Directorio temporal* usen la nueva ruta de almacén de archivos; y después reiniciar los servidores.

## 11.15 Uso de bibliotecas de 32 bits y 64 bits de terceros con la plataforma de BI

Los servidores de la plataforma de BI son una combinación de procesos de 32 bits y 64 bits. Adicionalmente, algunos servidores inician procesos de 32 y 64 bits. Para usar la versión correcta de las bibliotecas de terceros (32 bits o 64 bits) con los proceso de la plataforma de BI, debe definir variables de entorno independientes de 32 o 64 bits en el equipo que hospeda la plataforma de BI. A continuación, debe establecer una variable de entorno adicional que contenga una lista separada por comas de las variables de entorno que tengan versiones de 32 y 64 bits. Cuando la plataforma de BI inicia un proceso, seleccionará la variable adecuada en función de si se trata de un proceso de 32 bits o de 64 bits.

- `<FIRST_ENV_VAR>`=el valor que usarán los procesos de la plataforma de BI de 64 bits.
- `<FIRST_ENV_VAR32>`=el valor que se debe utilizar para procesos de 32 bits.
- `<FIRST_ENV_VAR 64>`= el valor que se debe utilizar para procesos de 64 bits.
- `<FIRST_ENV_VAR 32>`= el valor que se debe utilizar para procesos de 32 bits.
- BOE_USE_32BIT_ENV_FOR=`<FIRST_ENV_VAR>`,`<SECOND_ENV_VAR>`

Por ejemplo, si ha instalado la plataforma de BI en un equipo AIX y en clientes de Oracle de 32 bits y de 64 bits, y tiene que definir la variable LIBPATH, defina las variables siguientes:

- ORACLE_HOME=`<directorio de inicio de versión de 64 bits del cliente de Oracle>`
- ORACLE_HOME32=`<directorio de inicio de versión de 32 bits>`
- LIBPATH=`<vía de acceso de biblioteca de versión de 64 bits>`
- LIBPATH32=`<vía de acceso de biblioteca de versión de 32 bits>`
- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH

> **Nota**
>
> En Linux y Solaris, no use BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH para separar las rutas de 32 bits y 64 bits. En su lugar, agregue ambas rutas de 32 bits y 64 bits a LD_LIBRARY_PATH.

## 11.16 Administrar marcadores de posición del servidor y del nodo

### 11.16.1 Ver los marcadores de posición de un servidor

En el área de administración *Servidores* de la CMC, haga clic en un servidor y seleccione *Marcadores de posición*.
El diálogo *Marcadores de posición* muestra una lista de marcadores de posición para todos los servidores del mismo clúster que el servidor seleccionado. Si desea cambiar un valor de un marcador de posición, modifique el marcador de posición para el nodo.

## Información relacionada

Marcadores de posición de servidor y nodo [página 1218]

# 11.16.2 Ver y editar los marcadores de posición de un nodo

1. En el área de administración *Servidores* de la Consola de administración central, haga clic con el botón derecho en el nodo cuyos marcadores de posición desea cambiar y seleccione *Marcadores de posición*.
2. Si desea editar alguno de los valores de los marcadores de posición, realice los cambios adecuados y haga clic en *Guardar* para continuar.

> ⚠ Precaución
>
> Los marcadores de posición que no sean los previstos para la edición no deben cambiarse de ninguna manera. El administrador del sistema debe asegurarse de que solo la persona adecuada del grupo de administradores (que está prevista para la gestión de nodos) tenga los derechos de edición en el nodo. Todos los demás usuarios, incluidos los demás miembros del grupo de administradores, deben estar restringidos para ver/administrar los objetos Nodo aplicando los derechos de seguridad adecuados. En caso de que alguno de los valores de marcador de posición esté dañado accidentalmente y no aparezca CMS, consulte la siguiente nota SAP.

> ⓘ Nota
>
> Consulte el siguiente artículo de la base de conocimientos de SAP 3278916 para saber cómo restringir los marcadores de posición que se modifican para evitar posibles interferencias con fines maliciosos con la infraestructura de BI.

## Información relacionada

Marcadores de posición de servidor y nodo [página 1218]

# 12 Administración de bases de datos del Servidor de administración central (CMS)

## 12.1 Administrar las conexiones de la base de datos de sistema del CMS

Si la base de datos de sistema del CMS no está disponible, por ejemplo, debido a un error de hardware o software o bien a un problema de red, el CMS cambia al estado «Esperando recursos». Si el despliegue de la plataforma de BI dispone de varios CMS, las siguientes peticiones de otros servidores se enviarán a cualquier CMS del clúster que disponga de una conexión activa a la base de datos del sistema. Mientras un CMS se encuentra en el estado «Esperando recursos», las solicitudes actuales que no requieran acceso de base de datos se seguirán procesando, pero no se realizarán las solicitudes que requieran acceso a la base de datos de sistema del CMS.

De forma predeterminada, un CMS en estado «Esperando recursos» intenta periódicamente volver a establecer el número de conexiones que están especificadas en la propiedad «Conexiones a la base de datos del sistema solicitadas». En cuanto se establezca al menos una conexión de base de datos, el CMS sincroniza todos los datos necesarios, va al estado «En ejecución» y reanuda las operaciones normales.

En algunos casos, se puede desear evitar que el CMS vuelva a establecer automáticamente una conexión a la base de datos. Por ejemplo, puede verificar la integridad de la base de datos antes de que se vuelvan a establecer las conexiones a la base de datos. Para ello, en la página *Propiedades* del servidor del CMS, desmarque *Base del datos del sistema de reconexión automática*.

### Información relacionada

Para cambiar las propiedades de un servidor [página 462]

## 12.1.1 Para seleccionar SQL Anywhere como base de datos CMS

Para usar SQL Anywhere como base de datos del CMS, debe seguir estos pasos:

1. Detenga todos los nodos del sistema.
2. Ejecute la aplicación adecuada:
   - En Unix, ejecute `./cmsdbsetup.sh`.
   - En Windows, inicie el Administrador de configuración central (CCM).

3. Copie sus datos de la base de datos CMS predeterminada; para ello seleccione SQL Anywhere como base de datos de destino. Para obtener más información, consulte el vínculo relacionado «Copiar datos de una base de datos de sistema de CMS a otra».
4. En implementaciones de varios nodos, actualice con la nueva base de datos SQL Anywhere el origen de datos CMS en cada uno de los nodos (excepto el nodo en el que copia la base de datos). Para obtener más información, consulte el vínculo relacionado «Seleccionar una base de datos de CMS nueva o existente».
5. Asegúrese de que el despliegue es operacional (por ejemplo, inicie sesión en el CMC y visualice un informe).

### Información relacionada

Copia de datos de una base de datos de sistema de CMS a otra [página 514]
Selección de una base de datos del CMS nueva o existente [página 509]

## 12.1.2 Para seleccionar SAP HANA como base de datos de CMS

Para usar SAP HANA como base de datos de CMS, debe realizar los siguientes pasos.

1. Instale la plataforma de BI con la base de datos CMS predeterminada.
2. Instale el cliente SAP HANA.
3. Cree una conexión a SAP HANA.
   - En Unix, compruebe la variable de entorno `ODBCINI`. Si la variable existe y apunta a un archivo `odbc.ini` existente, agregue las líneas siguientes a ese archivo:

     ```
     [ODBC Data Sources]
     NewDB=<New_DB_version>
     [NewDB]
     DRIVER=<HANA CLIENT PATH>/libodbcHDB.so
     SERVERNODE=<HANA Server IP address>:<HANA server port #>
     DATABASENAME=<DBNAME>
     DESCRIPTION=<DESCRIPTION>
     ```

     `<New_DB_version>` es la versión SAP HANA; por ejemplo, «NewDB 1.0», `<HANA Server IP address>` es la dirección IP SAP HANA, y `<HANA server port #>` es el número de puerto de servidor SAP HANA.
     Si la variable de entorno `ODBCINI` no existe, cree un archivo `odbc.ini` en el directorio `<DIRINSTAL>/sap_bobj/enterprise_xi40/`, agregue las líneas anteriores al archivo y defina la variable de entorno `ODBCINI` de este modo:

     ```
     ODBCINI=<INSTALLDIR>/sap_bobj/enterprise_xi40/odbc.ini
     ```

     Asegúrese de que la variable de entorno ODBCINI está fijada en el perfil del usuario que inicia los servidores BI.
   - En Windows, cree una conexión ODBC a SAP HANA.

> **Nota**
>
> Para modificaciones de conexión ODBC, asegúrese de ejecutar la versión de 64 bits del administrador de origen de datos ODBC: *Inicio* > *Panel de control* > *Herramientas administrativas* > *Fuentes de datos (ODBC)*.

4. Asegúrese de que se puedan establecer conexiones al servidor SAP HANA.
   - En Unix, puede probar la conexión al servidor SAP HANA ejecutando el comando siguiente. Las variables del ejemplo siguiente hacen referencia a la instalación SAP HANA:

     ```
     <INSTALLDIR>/odbcreg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID>
     <NONADMINUSER> <NONADMINPASSWORD>
     ```

   - En Windows, puede usar el administrador de origen de datos ODBC para probar la conexión ODBC SAP HANA.
5. En Unix, asegúrese de que las variables de entorno `LD_LIBRARY_PATH` o `LIBPATH` contienen la ruta a `libodbcHDB.so`. Para obtener más información, consulte 2792543, 1886746 y 2721890.
6. Instale el producto siguiendo las indicaciones del asistente, y seleccione SAP HANA como la base de datos CMS /de Auditoría.
7. Asegúrese de que el despliegue es operacional (por ejemplo, inicie sesión en el CMC y visualice un informe).

> **Nota**
>
> Este procedimiento no se aplica si está moviendo una base de datos de una base de datos existente a una base de datos SAP HANA. Si ese es el caso, utilice el procedimiento de fuente de datos de copia. Para obtener más información, consulte Copia de datos de una base de datos de sistema de CMS a otra [página 514].

### Información relacionada

Copia de datos de una base de datos de sistema de CMS a otra [página 514]
Selección de una base de datos del CMS nueva o existente [página 509]

## 12.2 Selección de una base de datos del CMS nueva o existente

Puede utilizar el CCM o `cmsdbsetup.sh` para especificar una base de datos de sistema de CMS nueva o existente para un nodo. Por lo general, sólo tendrá que realizar estos pasos en los siguientes casos:

- Si ha cambiado la contraseña de la base de datos de sistema de CMS actual, estos pasos le permiten desconectarse de la base de datos actual y, a continuación, conectarse de nuevo a ella. Cuando se le pida, especifique la nueva contraseña para CMS.
- Si desea seleccionar e inicializar una base de datos vacía para la plataforma de BI, estos pasos le permiten seleccionar ese nuevo origen de datos.

- Si ha restaurado una base de datos de sistema de CMS a partir de una copia de seguridad (utilizando sus procedimientos y herramientas de administración de base de datos estándar) de forma que la conexión de base de datos original deja de ser válida, necesitará conectar de nuevo CMS a la base de datos restaurada. (Esto se produce, por ejemplo, si restaura la base de datos CMS original en un servidor de base de datos recién instalado.)

> **Nota**
>
> Si usa IBM DB2 como base de datos CMS y la actualiza de una versión anterior a 9.5 Fix Pack 5 a una versión 9.5 Fix Pack 5 o posterior (para la línea 9.5), o si actualiza desde una versión anterior a 9.7 Fix Pack 1 a una versión 9.7 Fix Pack 1 o posterior (para la línea 9.7), durante el siguiente reinicio del nodo de la plataforma de BI o CMS, el esquema de la base de datos CMS será actualizada automáticamente por el CMS para admitir el esquema compatible con HADR.
>
> Puede tratarse de un proceso largo, durante el que el sistema de la plataforma de BI no estará disponible. No interrumpa el proceso de actualización para no dañar la base de datos CMS. Es muy recomendable realizar una copia de seguridad de la base de datos CMS antes de realizar esta acción. Asimismo, no intente usar IBM HADR con una base de datos IBM DB2 CMS de una versión anterior a la 9.5 Fix Pack 5 (para la línea 9.5) o 9.7 Fix Pack 1 (para la línea 9.7).

> **Nota**
>
> No configure una instalación de la plataforma de BI para usar una base de datos de sistema del CMS que corresponda a un clúster distinto, a menos que esté llevando a cabo un flujo de trabajo de copia del sistema.
>
> Se pueden producir daños en el sistema si las versiones y los niveles de revisión de las instalaciones de la plataforma de BI y las bases de datos del CMS son distintas, o si las revisiones de la instalación difieren, o si los componentes instalados difieren, etc.
>
> Para evitar los daños, no intente migrar contenido de BI de un sistema a otro apuntando el despliegue de la plataforma de BI a la base de datos del CMS de otro sistema de la plataforma de BI, especialmente a un sistema con versión y nivel de revisión distintos.

> **Nota**
>
> La plataforma de Business Intelligence es compatible con la comunicación SSL entre CMS bases de datos como la base de datos del CMS y la base de datos de auditoría. Para la comunicación SSL,
>
> - Se deberían utilizar las bases de datos SQL Anywhere, Servidor SQL y SAP HANA como un base de datos del CMS o de auditoría para comunicarse con el CMS.
> - Debería habilitar SSL en los respectivos servidores de bases de datos. Consulte la documentación específica de su base de datos.
> - Debería crear una conexión ODBC y pasar el certificado de servidor DB a través de dicha conexión ODBC.
> - Debería utilizar la misma conexión ODBC para conectar a la base de datos CMS y la base de datos de auditoría.

## 12.2.1 Para seleccionar una base de datos de CMS nueva o existente en Windows

1. Use el CCM para iniciar y detener el Agente de inteligencia de servidor (SIA).
2. Seleccione el SIA y haga clic en el botón *Especificar origen de datos del CMS*.
3. Seleccione *Actualizar configuración de origen de datos* y haga clic en *Aceptar*.
4. Seleccione un controlador de base de datos y haga clic en *Aceptar*.
5. Estos pasos dependen del tipo de conexión que seleccione:
   - Si seleccionó ODBC, aparece el cuadro de diálogo «Seleccionar origen de datos» de Windows. Seleccione el origen de datos ODBC que desee utilizar como base de datos CMS; a continuación, haga clic en *Aceptar*. (Haga clic en *Nuevo* para configurar un DSN nuevo.) Cuando se le pida, indique sus credenciales de bases de datos y haga clic en *Aceptar*.
   - Si seleccionó un controlador original, se le pide el Nombre de servidor, ID de inicio de sesión y Contraseña de base de datos. Proporcione esta información y, a continuación, haga clic en *Aceptar*.
6. Especifique la clave de clúster.
7. Reinicie el Server Intelligence Agent.

## 12.2.2 Para seleccionar una base de datos de CMS nueva o existente en UNIX

Utilice la secuencia de comandos `cmsdbsetup.sh`. Como referencia, consulte el tema «Secuencias de comandos Unix» en el capítulo sobre la Gestión de líneas de comandos del *Manual del administrador de la plataforma BI*.

1. Ejecute la secuencia de comandos `cmsdbsetup.sh` (ubicada en `<DIRINSTAL>/sap_bobj/` de forma predeterminada).
2. Seleccione la acción de actualización (opción 6).
3. Cuando se le solicite, proporcione el tipo de la nueva base de datos de CMS.
4. Proporcione la información de base de datos (por ejemplo: nombre de host, nombre de usuario, contraseña, y clave de clúster).
   Aparecerá un mensaje de notificación cuando la base de datos del CMS señale a la nueva ubicación.
5. Si se le pide que vuelva a generar el Agente de inteligencia de servidor (SIA), proporcione la contraseña de administrador y el número de puerto en el que desea que se comunique el CMS.

   > **Nota**
   >
   > Sólo se le pedirá esta información si dirige a una base de datos CMS vacía.

### Información relacionada

Scripts de Unix [página 1100]

## 12.3 Creación de nuevo de la base de datos del sistema de CMS

Este procedimiento muestra cómo volver a crear (reinicializar) la base de datos de sistema de CMS actual. Al realizar esta tarea, se destruyen todos los datos existentes en la base de datos. Este procedimiento es útil, por ejemplo, si tiene instalada la plataforma de BI en un entorno de desarrollo para diseñar y evaluar sus propias aplicaciones Web personalizadas. Puede reinicializar la base de datos de sistema de CMS en su entorno de desarrollo cada vez que necesite eliminar todos los datos del sistema.

> ⚠ Precaución
>
> Al implementar los pasos descritos en este flujo de trabajo eliminará todos los datos de la base de datos del CMS así como objetos tales como informes y usuarios. No realice estos pasos en un despliegue de producción.

Es muy importante que se realice la copia de seguridad de todas las opciones de configuración del servidor antes de reinicializar la base de datos del sistema del CMS. Al volver a crear la base de datos, los ajustes de configuración del servidor se borrarán y debe disponer de una copia de seguridad para poder restaurar esta información.

Cuando se vuelve a crear la base de datos de sistema, las claves de licencia existentes se deben conservar en la base de datos. Sin embargo, si tiene que introducir claves de licencia de nuevo, inicie sesión en la CMC con la cuenta de administrador predeterminada. Vaya al área de administración Autorización y especifique la información en la ficha Claves de licencia.

> ⓘ Nota
>
> Si reinicializa la base de datos de sistema de CMS, todos los datos de la misma se destruirán. Considere la posibilidad de realizar una copia de seguridad de la base de datos actual antes de empezar. Si es necesario, póngase en contacto con el administrador de su base de datos.

### Información relacionada

Copia de seguridad de la configuración del servidor [página 565]

## 12.3.1 Para volver a crear la base de datos de sistema de CMS en Windows

1. Use CCM para iniciar y detener el Agente de inteligencia de servidor (SIA).

   > ⓘ Nota
   >
   > Para este procedimiento no puede ejecutar el CCM en un equipo remoto; se debe ejecutar en un equipo con al menos un nodo válido. Además, los binarios del CMS se deben instalar en este esquipo.

2. Haga clic con el botón derecho del ratón en el SIA y elija *Propiedades*.
3. En el cuadro de diálogo *Propiedades*, vaya a la ficha *Configuración* y haga clic en *Especificar*.
4. En el cuadro de diálogo *Configuración de base de datos de CMS*, haga clic en *Volver a crear el origen de datos actual*.

   > **Nota**
   >
   > Los servidores y objetos del equipo donde ha ejecutado el CCM en el paso 1 también se volverán a crear. Sin embargo, no se volverán a crear todos los objetos; solo los objetos predeterminados clave. Por ejemplo, no se vuelven a crear informes de muestra.

5. Haga clic en *Aceptar* y, cuando se le pida confirmación, haga clic en *Sí*.
6. Especifique la contraseña para la base de datos del sistema del CMS y haga clic en *Aceptar*.

   > **Nota**
   >
   > Asegúrese de que establece una nueva contraseña de administrador. De forma predeterminada, la cuenta de administrador no tendrá contraseña.

   El CCM le notifica cuando se ha completado la configuración de la base de datos de sistema de CMS.
7. Haga clic en *Aceptar*.

   Regresará a CCM.
8. Reinicie Server Intelligence Agent y active los servicios.

   Mientras se está iniciando, Server Intelligence Agent inicia el CMS. El CMS escribe los datos del sistema necesarios para los orígenes de datos que se acaban de vaciar.
9. Si su despliegue tiene varios equipos, debe volver a crear los nodos en los demás equipos.

## 12.3.2 Para volver a crear la base de datos de sistema de CMS en UNIX

Utilice la secuencia de comandos `cmsdbsetup.sh`. Como referencia, consulte el tema «Secuencias de comandos Unix» en el capítulo sobre la Gestión de líneas de comandos del *Manual del administrador de la plataforma BI*.

1. Ejecute `cmsdbsetup.sh` (ubicado en `<DIRINSTAL>/sap_bobj/` de forma predeterminada).
2. Elija la opción "reinitialize" (opción 5) y confirme la selección realizada.
   La secuencia de comandos `cmsdbsetup.sh` vuelve a crear la base de datos de sistema de CMS.
3. Proporcione la contraseña de la base de datos del sistema de CMS.
4. Cuando haya finalizado la creación de la base de datos, salga de la secuencia de comandos `cmsdbsetup.sh`.
5. Proporcione la información de base de datos (por ejemplo: nombre de host, nombre de usuario y contraseña).
   Aparecerá un mensaje de notificación cuando la base de datos del CMS señale a la nueva ubicación.
6. Si se le pide que vuelva a generar el Agente de inteligencia de servidor (SIA), proporcione la contraseña de administrador y el número de puerto en el que desea que se comunique el CMS.

> **Nota**
>
> Sólo se le pedirá esta información si dirige a una base de datos CMS vacía.

7. En el directorio `<INSTALLDIR>/sap_bobj/` use el siguiente comando para iniciar el nodo.

```
ccm.sh -start <nodename>
```

8. Para activar los servicios, utilice el siguiente comando:

```
ccm.sh -enable all -cms <CMSNAME:PORT> -username administrator -password
<password>
```

> **Nota**
>
> Como acaba de volver a crear la base de datos de CMS, la contraseña del servidor está en blanco.

### Información relacionada

Scripts de Unix [página 1100]

## 12.4 Copia de datos de una base de datos de sistema de CMS a otra

Puede usar el Administrador de configuración central (CCM) o `cmsdbsetup.sh` para copiar los datos del sistema desde el servidor de la base de datos a otro servidor de base de datos. Por ejemplo, si desea sustituir la base de datos por otra base de datos porque la está actualizando o la está moviendo de un tipo de base de datos o otro, puede copiar el contenido de la base de datos existente en una nueva antes de retira la base de datos existente.

La base de datos de destino se inicializa antes de que los nuevos datos se copien, de forma que todo el contenido existente de la base de datos de destino se elimina permanentemente (todas las tablas de la plataforma de BI se destruyen de manera permanente y, a continuación, se vuelven a crear). Una vez copiados los datos, la base de datos de destino se establece como base de datos actual para el CMS.

> **Precaución**
>
> No intente nunca utilizar una base de datos CMS desde otro cluster de plataforma BI. Antes de iniciar este workflow, asegúrese de que la base de datos CMS de origen se haya utilizada con este cluster de plataforma BI y no con otro cluster de plataforma BI.

> **Precaución**
>
> Nunca intente efectuar un upgrade mediante la utilización del workflow de copia de base de datos CMS. El workflow de copia de base de datos CMS se ha diseñado para mover una base de datos CMS desde un servidor de base de datos a otro servidor de base de datos. No se ha concebido para efectuar un upgrade de la base de datos CMS. Antes de iniciar este workflow, asegúrese de que la base de datos CMS de origen

se haya utilizado con este cluster de plataforma BI y de que tenga la misma versión y los mismos niveles de patch que la instalación de plataforma BI actual.

## 12.4.1 Preparar la copia de una base de datos de sistema de CMS

Antes de copiar una base de datos de sistema de CMS, deje los entornos de origen y de destino sin conexión; para ello, deshabilite y, posteriormente, detenga todos los servidores. Realice una copia de seguridad de ambas bases de datos CMS y de los directorios raíz que utilizan todos los servidores de repositorio de archivos de entrada y de salida. Si es necesario, póngase en contacto con el administrador de la base de datos o de la red.

Asegúrese de que dispone de una cuenta de usuario de base de datos que tenga permiso para leer todos los datos de la base de datos de origen y una cuenta de usuario de base de datos que tenga los derechos Crear, Eliminar y Actualizar en la base de datos de destino. También asegúrese también de que se conecta a ambas bases de datos (a través del software cliente de base de datos o a través de ODBC, según la configuración) desde el equipo CMS cuya base de datos va a reemplazar.

Si va a copiar una base de datos CMS desde su ubicación actual a otro servidor de base de datos, la base de CMS actual es el entorno de origen. Su contenido se copia en la base de datos de destino, que se establece a continuación como base de datos activa para el CMS actual. Realice este procedimiento si desea mover la base de datos del CMS predeterminada desde la base de datos predeterminada existente al servidor de base de datos dedicado, como Microsoft SQL Server, Informix, Oracle, DB2 o Sybase. Conecte con una cuenta administrativa en el equipo que ejecuta el CMS cuya base de datos desea mover.

> **Nota**
>
> Cuando copia datos desde una base de datos a otra, la base de datos de destino se inicializa antes de que los nuevos datos se copien en ella. Es decir, si la base de datos de destino no contiene las tablas del sistema de la plataforma de BI, estas se crean. Si la base de datos de destino contiene las tablas del sistema de la plataforma de BI, las tablas se eliminarán de forma permanente, se crearán nuevas tablas de sistema y se copiarán los datos de la base de datos de origen en las nuevas tablas. Esta acción no afecta al resto de tablas de la base de datos.

> **Nota**
>
> Si copia una base de datos del sistema de CMS a una base de datos de destino MaxDB en Windows, debe asegurarse de que la ruta al cliente MaxDB se ha agregado a la variable del entorno `<PATH>`. Por ejemplo, `;C:\Archivos de programa\sdb\MAXDB1\pgm`.

## 12.4.2 Para copiar una base de datos de sistema del CMS en Windows

Antes de copiar el contenido de la base de datos de datos del CMS, asegúrese de que puede iniciar sesión en la base de datos de destino con una cuenta que tenga permisos para agregar o eliminar tablas, así como para agregar, eliminar o modificar datos en dichas tablas.

1. Abra el Administrador de configuración central (CCM) y detenga el Server Intelligence Agent (SIA).
2. Haga clic con el botón derecho del ratón en el SIA y elija *Propiedades*.
3. Haga clic en la ficha *Configuración* y, a continuación, en *Especificar*.
4. Elija *Copiar* y haga clic en *Aceptar*.
5. Seleccione el tipo de base de datos del CMS de origen y, a continuación, especifique la información de dicha base de datos (como el nombre de host, el nombre de usuario y la contraseña).
6. Seleccione el tipo de base de datos del CMS de destino y, a continuación, especifique la información de dicha base de datos (como el nombre de host, el nombre de usuario y la contraseña).
7. Cuando la base de datos del CMS finalice el proceso de copia, haga clic en *Aceptar*.

### 12.4.3 Para copiar datos de una base de datos del sistema del CMS en Unix

Antes de copiar el contenido de la base de datos de datos del CMS, asegúrese de que puede iniciar sesión en la base de datos de destino con una cuenta que tenga permisos para agregar o quitar tablas, así como para agregar, quitar o modificar datos en dichas tablas.

> **Nota**
>
> En UNIX no puede migrar directamente desde un entorno de origen que utilice una conexión ODBC a la base de datos CMS. Si la base de datos del CMS de origen utiliza ODBC, primero debe actualizar dicho sistema a un controlador nativo compatible.

1. Detenga el CMS escribiendo el siguiente comando:

   ```
   ./ccm.sh -stop <nodename>
   ```

2. Ejecute `cmsdbsetup.sh` (ubicado en `<DIRINSTAL>/sap_bobj/` de forma predeterminada).
3. Elija la opción «copy» (opción 4) y confirme la selección realizada.
4. Seleccione el tipo de base de datos del CMS de origen y, a continuación, especifique la información de base de datos (como el nombre del host, el nombre de usuario y la contraseña).
5. Seleccione el tipo de la base de datos del CMS de destino y, a continuación, especifique la información de base de datos (como el nombre del host, el nombre de usuario y la contraseña).
   La base de datos del CMS se copia en la base de datos de destino. Cuando finaliza la copia se muestra un mensaje.

## 12.5 Controlador de base de datos de servidor de administración central

Ahora puede acceder a la base de datos del repositorio del CMS de la plataforma de BI para el análisis de la gestión de informes aprovechando las funciones de la plataforma existentes (servidor de conexión, capa semántica, clientes de la gestión de informes). El controlador de acceso a datos de SAP BusinessObjects

le permite usar un universo para consultar la base de datos CMS. Para obtener más información, consulte http://scn.sap.com/docs/DOC-74580.

# 13 Administración de servidores del contenedor de aplicaciones Web (WACS)

## 13.1 WACS

### 13.1.1 Servidor de contenedor de aplicación Web (WACS)

Los servidores de contenedor de aplicaciones Web (WACS) proporcionan una plataforma para alojar aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence. Por ejemplo, una Consola de administración central (CMC) se puede alojar en un WACS.

WACS simplifica la administración del sistema al eliminar varios flujos de trabajo que anteriormente eran necesarios para la configuración de servidores de aplicaciones e implementar aplicaciones Web y al proporcionar una interfaz administrativa que está simplificada y es coherente.

Las aplicaciones Web se despliegan automáticamente en WACS. WACS no admite el despliegue manual o de WDeploy de la plataforma de BI o aplicaciones Web externas.

#### 13.1.1.1 ¿Necesito WACS?

Si no desea usar un servidor de aplicaciones Java para alojar las aplicaciones Web de SAP BusinessObjects, puede alojarlas en WACS.

Si tiene pensado usar un servidor de aplicaciones Java admitido para desplegar aplicaciones Web de la plataforma de BI o si está instalando la plataforma de BI en un sistema Unix, no tiene que instalar ni usar WACS.

#### 13.1.1.2 ¿Cuáles son las ventajas del uso de WACS?

Al usar WACS para alojar la CMC se obtiene una serie de ventajas:

- WACS requiere un mínimo esfuerzo de instalación, mantenimiento y configuración.
- Todas las aplicaciones alojadas se despliegan previamente en WACS, de modo que no se requieren pasos manuales adicionales.
- SAP admite WACS.
- WACS elimina la necesidad de conocimientos de administración y mantenimiento del servidor de aplicaciones Java.
- WACS proporciona una interfaz administrativa que es coherente con otros servidores de Servicios de la plataforma de BI

## 13.1.1.3 Tareas comunes

| Tarea | Descripción | Tema |
|---|---|---|
| Cómo mejorar el rendimiento de las aplicaciones Web o de los servicios Web que se alojan en WACS. | Puede mejorar el rendimiento de las aplicaciones Web o de los servicios Web instalando WACS en varios equipos. | • Agregar o eliminar WACS adicionales al despliegue [página 520]<br>• Clonar un servidor de contenedor de aplicación Web [página 523] |
| ¿Cómo puedo mejorar la disponibilidad de mi nivel web? | Cree un WACS adicional en el despliegue de modo que, si se produce un error de hardware o de software en un servidor, otro servidor puede continuar atendiendo las solicitudes. | Agregar o eliminar WACS adicionales al despliegue [página 520] |
| ¿Cómo puedo crear un entorno donde pueda realizar la recuperación fácilmente de una CMC configurada incorrectamente? | Cree un segundo WACS detenido y utilícelo para definir una plantilla de configuración. En el caso de que el WACS se configure incorrectamente, utilice el segundo WACS hasta que configure el primer servidor o aplique la plantilla al primer servidor. | Agregar o eliminar WACS adicionales al despliegue [página 520] |
| ¿Cómo puedo mejorar la seguridad de las comunicaciones entre los clientes y WACS? | Configure HTTPS en el WACS. | • Configurar HTTPS/SSL [página 525]<br>• Uso de WACS con servidores de seguridad [página 551] |
| ¿Cómo puedo mejorar la seguridad de las comunicaciones entre el WACS y otros servidores de la plataforma de BI en mi despliegue? | Configure las comunicaciones SSL entre WACS y otros servidores de la plataforma de BI en el despliegue. | • Configuración de servidores backend para SSL [página 183]<br>• Uso de WACS con servidores de seguridad [página 551] |
| ¿Puedo usar WACS con HTTPS y un proxy inverso? | Puede usar WACS con HTTPS y un proxy inverso si crea dos WACS y configura ambos servidores con HTTPS. Utilice el primer WACS para las comunicaciones en la red interna y el otro WACS para las comunicaciones con una red externa a través de un proxy inverso. | Para configurar WACS para admitir HTTPS con un proxy inverso [página 551] |
| ¿Cómo encaja WACS en mi entorno de TI? | WACS se puede desplegar en un entorno de TI con servidores web existentes, equilibradores de carga de hardware, servidores proxy inversos y servidores de seguridad. | • Utilizar WACS con otros servidores web [página 549]<br>• Usar WACS con un equilibrador de carga [página 550]<br>• Usar WACS con un proxy inverso [página 550]<br>• Uso de WACS con servidores de seguridad [página 551] |

| Tarea | Descripción | Tema |
| --- | --- | --- |
| ¿Puedo uso WACS en un despliegue con un equilibrador de carga? | Puede usar WACS en un despliegue que utilice un equilibrador de carga de hardware. WACS no se puede usar como un equilibrador de carga. | Usar WACS con un equilibrador de carga [página 550] |
| ¿Puedo usar WACS en un despliegue con un proxy inverso? | Puede usar WACS en un despliegue que utilice un proxy inverso. WACS no se puede usar como un proxy inverso. | Usar WACS con un proxy inverso [página 550] |
| ¿Cómo puedo solucionar los problemas de mis servidores WACS? | Si necesita determinar los motivos y las causas del rendimiento deficiente de su WACS, puede consultar los archivos de registro y las métricas del sistema. | • Configurar el seguimiento en WACS [página 553]<br>• Para ver las medidas de un servidor [página 553] |
| No se sirven páginas en un determinado puerto. ¿Qué sucede? | Existen muchos motivos por los que no se pueda conectar al WACS. Compruebe si:<br>• Los puertos HTTP, HTTP mediante proxy y HTTPS que ha especificado para el WACS los han ocupado otras aplicaciones.<br>• El WACS tiene suficiente memoria asignada.<br>• El WACS permite suficientes solicitudes simultáneas.<br>• Si es necesario, restaure los valores predeterminados del sistema para el WACS. | • Para resolver conflictos de puerto HTTP [página 554]<br>• Para cambiar la configuración de memoria [página 555]<br>• Para cambiar el números de solicitudes simultáneas [página 555]<br>• Para restaurar los valores predeterminados del sistema [página 556] |
| ¿Cómo puedo configurar las propiedades de las aplicaciones Web que se alojan en WACS? | El procedimiento para configurar las propiedades de aplicaciones Web depende de la propiedad y aplicación Web específicas. Para obtener más información, consulte la sección «Configuración de propiedades de aplicaciones Web» de este capítulo. | Configurar propiedades de aplicaciones Web [página 552] |
| ¿Dónde puedo encontrar una lista de las propiedades de WACS? | El «Apéndice de propiedades de servidor» de este manual contiene una lista de las propiedades del WACS. | Propiedades de servicios principales [página 1165] |

## 13.1.2 Agregar o eliminar WACS adicionales al despliegue

Agregar WACS adicionales al despliegue puede ofrecer una serie de ventajas:

- Recuperación más rápida de un servidor configurado incorrectamente.
- Disponibilidad de servidor mejorada.
- Mejor equilibrio de carga.

- Mejor rendimiento global.

Hay tres formas para agregar WACS adicionales a su despliegue:

- Instalar WACS en un equipo.
- Crear un nuevo WACS.
- Clonar un WACS.

> **Nota**
>
> Se recomienda ejecutar un solo WACS en el mismo equipo al mismo tiempo debido a la elevada utilización de recursos. No obstante, puede desplegar varios WACS en el mismo equipo y ejecutar solo uno de ellos, como ayuda de recuperación en el caso de un WACS configurado incorrectamente.

## 13.1.2.1 Instalar WACS

La instalación de WACS en equipos independientes puede proporcionar al despliegue un mejor rendimiento, mejor equilibrio de carga y mayor disponibilidad de servidor. Si su despliegue contiene dos o más WACS en equipos independientes, la disponibilidad de las aplicaciones Web y los servicios Web no se verá afectada por errores de hardware o de software en un equipo específico, porque los otros WACS seguirán proporcionando los servicios.

Puede instalar un servidor de contenedor de aplicación Web si usa el programa de instalación de la plataforma de BI. Existen dos formas en que puede instalar WACS:

- En una instalación completa, en la pantalla *Seleccionar servidor de aplicaciones Web Java*, seleccione *Instalar el servidor de contenedor de aplicación Web y desplegar automáticamente aplicaciones Web*. Si selecciona un servidor de aplicaciones Java en una instalación nueva, WACS no se instala.
- En una instalación personalizada o expandida, puede optar por instalar WACS en la pantalla *Seleccionar funciones* si expande *Servidores* > *Servicios de plataforma* y selecciona *Servidor de contenedor de aplicación Web*.

Si instala WACS, el programa de instalación crea automáticamente un servidor denominado `<NODO>.WebApplicationContainerServer`, donde `<NODO>` es el nombre de su nodo. Las aplicaciones Web y los servicios Web de la plataforma de BI se despliegan en dicho servidor. No se requieren pasos manuales para desplegar o configurar la CMC. El sistema está preparado para usarse.

Cuando instala WACS, el programa de instalación le pide que proporcione un número de puerto HTTP para el WACS. Asegúrese de especificar un número de puerto que no se use. El número de puerto es 6405. Si planea permitir que los usuarios se conecten al WACS desde fuera de un servidor de seguridad, debe asegurarse de que el puerto HTTP de dicho servidor está abierto en el servidor de seguridad.

> **Nota**
>
> Las aplicaciones Web que WACS aloja se despliegan automáticamente cuando se instala WACS o cuando se aplican actualizaciones o revisiones a WACS o las aplicaciones Web alojadas por WACS. El despliegue de las aplicaciones Web puede tardar varios minutos. El WACS estará en el estado «Iniciando» hasta que termine el despliegue de aplicaciones Web. Los usuarios no podrán acceder a las aplicaciones Web alojadas en WACS hasta que estén totalmente desplegadas. No detenga el servidor hasta que se complete el despliegue inicial. Puede ver el estado de servidor del WACS mediante el Administrador de configuración central (CCM).

> Este retraso sólo se produce cuando se inicia el WACS por primera vez después de instalar el WACS o aplicarle actualizaciones. Este retraso no se produce para los reinicios de WACS posteriores.
>
> Las aplicaciones Web no se pueden desplegar manualmente en un servidor WACS. No puede usar WDeploy para desplegar aplicaciones Web en WACS.

### 13.1.2.2 Agregar un servidor de contenedor de aplicación Web

> **Nota**
>
> Se recomienda ejecutar un solo WACS en el mismo equipo al mismo tiempo debido a la elevada utilización de recursos. No obstante, puede desplegar varios WACS en el mismo equipo y ejecutar solo uno de ellos, como ayuda de recuperación en el caso de un WACS configurado incorrectamente.

1. Vaya al área de administración *Servidores* de CMC.
2. Seleccione *Administrar* > *Nuevo* > *Nuevo servidor*.
   Aparece la pantalla *Crear nuevo servidor*.
3. En la lista *Categoría de servicio*, seleccione *Servicios principales*.
4. En la lista *Seleccionar servicio*, seleccione los servicios que desea que aloje WACS y haga clic en *Siguiente*.
   - Si desea que WACS aloje aplicaciones Web como la CMC, la plataforma de lanzamiento de BI u OpenDocument, seleccione *Servicio de aplicación Web BOE*.
   - Si desea que WACS aloje servicios Web como Live Office o Consulta como servicio Web (QaaWS), seleccione *Servicios Web SDK y QaaWS*.
   - Si desea que WACS aloje servicios Web de Business Process BI, seleccione *Servicio Web de Business Process BI*.
5. En la siguiente pantalla *Crear nuevo servidor*, seleccione cualquier servicio adicional que desee que aloje WACS y haga clic en *Siguiente*.
6. En la siguiente pantalla *Crear servidor*, seleccione un nodo al que agregar al servidor, escriba un nombre de servidor y una descripción del servidor y haga clic en *Crear*.

   > **Nota**
   >
   > Sólo los nodos que tienen instalado WACS aparecerán en la lista *Nodo*.

7. En la pantalla *Servidores*, haga doble clic en el nuevo WACS.
   Aparecerá la pantalla *Propiedades*.
8. Si no desea que WACS se inicie automáticamente cuando el sistema se reinicia, en el panel *Configuración común*, compruebe que la casilla de verificación *Iniciar automáticamente este servidor cuando se inicie Server Intelligence Agent* no está seleccionada.
9. Haga clic en *Guardar y cerrar*.

Se crea un nuevo WACS. La configuración y las propiedades predeterminadas se aplican al servidor.

## 13.1.2.3 Clonar un servidor de contenedor de aplicación Web

Como alternativa a agregar un nuevo WACS al despliegue, también puede clonar un WACS, en el mismo equipo o en otro. Mientras que la adición de un nuevo WACS crea un servidor con la configuración predeterminada, la clonación aplica la configuración del WACS de origen al nuevo.

Los servidores solo se pueden clonar en equipos que ya tienen instalado WACS.

> **Nota**
>
> Se recomienda ejecutar un solo WACS en el mismo equipo al mismo tiempo debido a la elevada utilización de recursos. No obstante, puede desplegar varios WACS en el mismo equipo y ejecutar solo uno de ellos, como ayuda de recuperación en el caso de un WACS configurado incorrectamente.

1. Vaya al área de administración *Servidores* de CMC.
2. Seleccione el WACS que desee clonar, haga clic con el botón derecho y seleccione *Clonar servidor*.

   La pantalla *Clonar servidor* muestra una lista de nodos en el despliegue en los que puede clonar el WACS. Solo los nodos que tienen instalado WACS aparecen en la lista *Clonar a nodo*.
3. En la pantalla *Clonar servidor* escribe un nuevo nombre de servidor, seleccione el nodo al que desee clonar el servidor y haga clic en *Aceptar*.

Se crea un nuevo WACS. El nuevo servidor contiene los mismos servicios que el servidor del que se va a clonar. El nuevo servidor y servicios que aloja tienen la misma configuración que el servidor del que se han clonado, con la excepción del nombre de servidor.

> **Nota**
>
> Si ha clonado un WACS en el mismo equipo, puede tener conflictos de puerto con el WACS que se usó para la clonación. Si esto sucede, debe cambiar los números de puerto en la instalación de WACS recién clonada.

### Información relacionada

Para resolver conflictos de puerto HTTP [página 554]

## 13.1.2.4 Eliminar WACS del despliegue

Solo puede eliminar un WACS si el servidor no está sirviendo actualmente la CMC. Si desea eliminar un WACS del despliegue, debe iniciar sesión en una CMC desde otro WACS o un servidor de aplicaciones Java. No puede eliminar un WACS que actualmente está sirviendo la CMC.

1. Vaya al área de administración *Servidores* de CMC.
2. Detenga el servidor que desea eliminar haciendo clic con botón derecho en el servidor y haciendo clic en *Detener servidor*.
3. Haga clic con el botón derecho en el servidor y seleccione *Eliminar*.

4. Cuando se le pida confirmación, haga clic en *Aceptar*.

## 13.1.3 Agregar o eliminar servicios de WACS

### 13.1.3.1 Agregar una aplicación Web o un servicio Web a un WACS

Para agregar aplicaciones o servicios Web de la plataforma de BI adicionales a WACS, se debe detener WACS. Por lo tanto, debe tener al menos una CMC adicional alojada en un WACS del despliegue que proporcione un servicio de aplicaciones Web BOE mientras detiene y agrega un servicio al otro WACS.

Al agregar un servicio a un WACS, el servicio se despliega automáticamente en el WACS cuando se reinicia el servidor.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS al que desee agregar el servicio y consulte las propiedades del servidor para asegurarse de que todavía no está presente el servicio que desea agregar.
3. Haga clic en *Cancelar* para volver a la pantalla *Servidores*.
4. Detenga el servidor haciendo clic con el botón derecho en el servidor y haciendo clic en *Detener servidor*.

   Si está intentando detener el WACS que le está sirviendo actualmente la CMC, aparecerá un mensaje de advertencia. No continúe hasta que tenga al menos un servicio de aplicación Web BOE adicional en ejecución en otro WACS del despliegue. Si lo hace, haga clic en *Aceptar*, inicie sesión en otro WACS e inicie este procedimiento desde el principio.
5. Haga clic con el botón derecho en el servidor y seleccione *Seleccionar servicios*.
   Aparecerá la pantalla *Seleccionar servicios*.
6. Seleccione el servicio que desea agregar al servidor y agréguelo haciendo clic en > y en *Aceptar*.
7. Inicie el WACS haciendo clic con botón derecho en el servidor y haciendo clic en *Iniciar servidor*.

El servicio se agrega al WACS. Se aplican la configuración y las propiedades predeterminadas para el servicio.

### 13.1.3.2 Eliminar una aplicación Web o un servicio Web de un WACS

Para eliminar un servicio Web o una aplicación Web de un WACS, debe iniciar sesión en una CMC en otro WACS o en un servidor de aplicaciones Java. No puede detener el WACS que le esté sirviendo la CMC en ese momento.

No puede eliminar el último servicio de un WACS. Por lo tanto, si está eliminando un servicio Web de un WACS, debe asegurarse de que el servidor aloja al menos un servicio más.

Si desea eliminar el último servicio de un WACS, elimine el WACS.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS del que desee eliminar el servicio web y consulte las propiedades del servidor para asegurarse de que está presente el servicio web que desea eliminar.

3. Haga clic en *Cancelar* para volver a la pantalla *Servidores*.
4. Detenga el WACS haciendo clic con el botón derecho en el servidor y haciendo clic en *Detener servidor*.

   Si está intentando detener el WACS que le está sirviendo actualmente la CMC, aparecerá un mensaje de advertencia. No continúe hasta que tenga al menos un servicio de aplicación Web BOE adicional en ejecución en otro WACS del despliegue. Si lo hace, haga clic en *Aceptar*, inicie sesión en otro WACS e inicie este procedimiento desde el principio.
5. Haga clic con el botón derecho en el WACS y seleccione *Seleccionar servicios.*
   Aparecerá la pantalla *Seleccionar servicios*.
6. Seleccione el servicio que desea eliminar, haga clic en < y, a continuación, haga clic en *Aceptar*.
7. Inicie el WACS haciendo clic con botón derecho en el servidor y haciendo clic en *Iniciar servidor*.

El servicio se elimina del WACS.

## 13.1.4 Configurar HTTPS/SSL

Puede usar el protocolo SSL (nivel de socket seguro) y HTTP para la comunicación de red entre los clientes y el WACS en el despliegue de la plataforma de BI. SSL/HTTPS cifra el tráfico de red y proporciona seguridad mejorada.

Existen dos tipos de SSL:

- SSL se usa entre los servidores de la plataforma de BI, incluyendo WACS y otros servidores de la plataforma de BI del despliegue. Esto se conoce como CORBA SSL. Para obtener más información sobre la utilización de SSL entre los servidores de la plataforma de BI en su despliegue, consulte la sección «Comprender la comunicación entre los componentes de la plataforma SAP BusinessObjects Business Intelligence» del capítulo «Trabajar con servidores de seguridad» del *Manual del administrador de la plataforma de SAP BusinessObjects Business Intelligence*.
- HTTP sobre SSL, que se produce entre WACS y los clientes (por ejemplo, exploradores) que se comunican con WACS.

> **Nota**
>
> Si va a desplegar WACS en un despliegue con un proxy o proxy inverso y desea usar SSL para proteger las comunicaciones de la red en el despliegue, debe crear dos WACS. Para obtener más información, consulte *Usar WACS con un proxy inverso*.

Para configurar HTTPS/SSL en un WACS, debe realizar los siguientes pasos:

- Genere u obtenga un almacén de certificados PKCS12 o un almacén de claves JKS que contenga sus certificados y claves privadas. Puede utilizar Internet Information Service (IIS) de Microsoft y Microsoft Management Console (MMC) para generar un archivo PCKS12 o usar openssl o la herramienta de la línea de comandos keytool de Java para generar un archivo de almacén de claves.
- Si desea que sólo determinados clientes se conecten a un WACS, debe generar un archivo de lista de certificados de confianza.
- Cuando tenga un almacén de certificados y, si es necesario, un archivo de lista de certificados de confianza, copie los archivos al equipo WACS.
- Configure HTTPS en el WACS.

## Información relacionada

Comprender la comunicación entre los componentes de la Plataforma de BI [página 193]
Usar WACS con un proxy inverso [página 550]

## 13.1.4.1 Para generar un almacén de archivos de certificados PKCS12

Existen numerosas formas de generar almacenes de archivos de certificados PKCS12 o almacenes de claves Java y herramientas que puede usar. El método que use dependerá de las herramientas a las que tenga acceso y con las que esté familiarizado.

En este ejemplo se demuestra cómo generar un archivo PKCS12 con Microsoft Internet Information Services (IIS) y Microsoft Management Console (MMC), para Windows Server 2008.

1. Inicie sesión en el equipo que aloja WACS como administrador.
2. En IIS, solicite un certificado a la autoridad de certificación. Para obtener información sobre cómo hacerlo, consulte la documentación de la ayuda de IIS.
3. Inicie MMC haciendo clic en *Inicio* > *Ejecutar* >, escribiendo `mmc.exe` y haciendo clic en *Aceptar*.
4. Agregue el complemento Certificados a MMC:
   a. En el menú *Archivo* haga clic en *Agregar o quitar complemento*.
      Aparece la pantalla *Agregar o quitar complementos*.
   b. Desde la lista *Complementos disponibles*, seleccione *Certificados*, y haga clic en agregar *Add*.
   c. Seleccione *Cuenta de equipo* y haga clic en *Siguiente*.
   d. Seleccione *Equipo local* y haga clic en *Finalizar*.
   e. Haga clic en *Aceptar*.

   El complemento Certificados se agrega a MMC.
5. En MMC expanda *Certificados* y seleccione el certificado que desee utilizar.
6. En el menú *Acción*, seleccione *Todas las tareas* > *Exportar* >.
   Se inicia el *Asistente para exportación de certificados*.
7. Haga clic en *Siguiente*.
8. Seleccione *Exportar la clave privada* y haga clic en *Siguiente*.
9. Seleccione *Personal Information Exchange - PKCS #12 (.PFX)* y haga clic en *Siguiente*.
10. Introduzca la contraseña que usó al crear el certificado y haga clic en *Siguiente*. Debe especificar esta contraseña en el campo *Contraseña de acceso a clave privada* al configurar HTTPS para el WACS.

Se crea un almacén de archivos de certificados PKCS12.

## 13.1.4.2 Para generar una lista de certificados de confianza

1. Inicie sesión en el equipo que aloja WACS como administrador.

2. Inicie Microsoft Management Console (MMC).
3. Agregue el complemento Internet Information Services:
   a. En el menú *Archivo*, seleccione *Agregar o quitar complemento*.
   b. En la lista *Agregar complementos independientes*, seleccione *Administrador de Internet Information Services (IIS)* y haga clic en *Agregar*.
   c. Haga clic en *Aceptar*.
   El complemento IIS se agrega a MMC.
4. Siga los pasos aquí descritos para crear una lista de confianza de certificados: http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard .

## 13.1.4.3 Para configurar HTTPS/SSL

Antes de configurar HTTP/SSL en el WACS, asegúrese de que ya ha creado un archivo PCKS12 o un almacén de claves JKS y que ha copiado o movido el archivo al equipo que aloja el WACS.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS del servidor para el que desea activar HTTP.
   Aparecerá la pantalla *Propiedades*.
3. En la sección *Configuración de HTTPS* active la casilla de verificación *Habilitar HTTPS*.
4. En el campo *Enlazar a nombre de host o dirección IP* especifique la dirección IP para la que se han emitido los certificados y a la que se enlazará el WACS.
   Los servicios HTTPS se proporcionarán mediante la dirección IP que especifique.
5. En el campo *Puerto HTTPS* especifique un número de puerto para que WACS proporcione el servicio HTTPS. Debe asegurarse de que este puerto está libre. Si planea permitir que los usuarios se conecten al WACS desde fuera de un servidor de seguridad, también debe asegurarse de que este puerto está abierto en el servidor de seguridad.
6. Si está configurando SSL con un proxy inverso, especifique el nombre de host y el puerto del servidor proxy en los campos *Nombre de host proxy* y *Puerto de proxy*.
7. En la lista *Protocolo*, seleccione un protocolo. Las opciones disponibles son:
   - *SSL*
     SSL es el protocolo de capa de socket seguro, que es un protocolo para cifrar el tráfico de red.
   - *TLS*
     TLS es el protocolo de seguridad de capa de transporte y se trata de un protocolo más reciente y mejorado. Las diferencias entre SSL y TLS son menores, pero se incluyen algoritmos de cifrado más sólidos en TLS.
8. En el campo *Tipo de almacén de certificados*, especifique el tipo de archivo del certificado. Las opciones disponibles son:
   - *PKCS12*
     Seleccione PKCS12 si se siente más cómodo trabajando con las herramientas de Microsoft.
   - *JKS*
     Seleccione JKS si se siente más cómodo trabajando con las herramientas de Java.
9. En el campo *Ubicación del archivo de almacén de certificados*, especifique la ruta donde ha copiado o movido el almacén de archivos de certificados o el archivo de almacén de claves de Java.
10. En el campo *Contraseña de acceso a clave privada* especifique la contraseña.

Los almacenes de certificados PKCS12 y los almacenes de claves de Java tienen claves privadas que están protegidas con contraseña, para prevenir el acceso no autorizado. Debe especificar la contraseña para acceder a las claves privadas, de modo que WACS pueda acceder a las claves privadas.

11. Se recomienda utilizar un almacén de archivos de certificados o un almacén de claves que contenga un solo certificado o donde el certificado que desea utilizar se enumere en primer lugar. No obstante, si utiliza un almacén de archivos de certificados o un almacén de claves que contiene varios certificados y dicho certificado no es el primero del almacén de archivos, en el campo *Alias de certificado*, debe especificar el alias del certificado.
12. Si desea que el WACS solo acepte solicitudes HTTPS de determinados clientes, active la autenticación de cliente.

    La autenticación de cliente no autentica a los usuarios. Garantiza que el WACS solo sirve solicitudes HTTPS a determinados clientes.

    a. Active *Habilitar la autenticación de cliente*.
    b. En *Ubicación del archivo de lista de certificados de confianza*, especifique la ubicación del archivo PCKS12 o el almacén de claves JKS que contenga el archivo de lista de confianzas.

    > **Nota**
    >
    > El tipo de la lista de certificados de confianza debe ser el mismo que el tipo del almacén de certificados.

    > **Nota**
    >
    > Consulte Para servicios Web RESTful [página 412] para obtener más información sobre el establecimiento de autenticación de confianza utilizando certificados X.509.

    > **Nota**
    >
    > Puede importar un certificado del sistema ABAP en la plataforma de BI ejecutando el comando: `keytool -import -trustcacerts -alias <Alias_Name> -file <CA_certificate_path> -keystore <trust_keystore_path>` . Consulte la tabla siguiente para comprender el comando:
    >
    > | Comando | Descripción |
    > | --- | --- |
    > | -alias | Nombre de alias |
    > | -file | Vía de acceso del certificado del sistema ABAP |
    > | -keystore | Ruta del archivo del almacén de claves de confianza |

    c. En el campo *Contraseña de acceso a clave privada de la lista de certificados de confianza* escriba la contraseña que protege el acceso a las claves privadas en el archivo de lista de certificados de confianza.

    > **Nota**
    >
    > Si activa la autenticación de cliente y un explorador o consumidor de servicio web no está autenticado, se rechaza la conexión HTTPS.

13. Haga clic en *Guardar y cerrar*.
14. Vaya a la pantalla *Métricas* y asegúrese de que el conector HTTPS aparece en *Lista de conectores de WACS en ejecución*. Si no aparece HTTPS, asegúrese de que el conector HTTPS esté configurado correctamente.

## 13.1.5 Métodos de autenticación admitidos

WACS admite los siguientes métodos de autenticación:

- Enterprise
- LDAP
- AD Kerberos

WACS no admite los siguientes métodos de autenticación:

- NT
- AD NTLM
- LDAP con inicio de sesión único

## 13.1.6 Configurar AD Kerberos para WACS

Para configurar la autenticación AD Kerberos para WACS, primero debe configurar el equipo para que admita AD. Es preciso llevar a cabo los siguientes pasos:

- Habilitar el complemento de seguridad de Windows AD.
- Asignar usuarios y grupos.
- Configurar una cuenta de servicio.
- Configurar la delegación restringida.
- Habilitar la autenticación Kerberos en el complemento de Windows AD para WACS.
- Crear los archivos de configuración.

Después de haber configurado el equipo que alojará WACS para usar la autenticación de AD Kerberos, debe llevar a cabo pasos de configuración adicionales mediante la Consola de administración central (CMC).

Si va a configurar el inicio de sesión único mediante AD Kerberos para Servicios Web SDK y QaaWS, también debe configurar WACS y el equipo que aloja WACS.

### Información relacionada

Complemento de seguridad de Windows AD [página 300]
Asignar grupos y usuarios de Windows AD [página 301]
Configuración de una cuenta de servicio para la autenticación de AD con Kerberos [página 299]
Ejecución de SIA bajo la cuenta de servicio de la plataforma de BI [página 308]
Habilitar la autenticación Kerberos en el complemento de Windows AD para WACS [página 530]

Crear los archivos de configuración [página 531]
Configurar WACS para AD Kerberos [página 534]
Configuración del inicio de sesión único de AD Kerberos [página 537]

## 13.1.6.1 Habilitar la autenticación Kerberos en el complemento de Windows AD para WACS

Para admitir Kerberos, debe configurar el complemento de seguridad Windows AD en la CMC para utilizar la autenticación Kerberos. Esto incluye:

- Comprobar que está habilitada la autenticación Windows AD.
- Especificar la cuenta de Administrador AD.

> **Nota**
>
> Esta cuenta requiere acceso de lectura sólo para Active Directory; no precisa ningún otro derecho.

- Activación de autenticación de Kerberos e inicio de sesión único, si se desea el inicio de sesión único.
- Escribir el nombre principal de servicio (SPN) de la cuenta de servicio.

### 13.1.6.1.1 Requisitos previos

Antes de configurar el complemento de seguridad de Windows AD para Kerberos, deberá haber completado las siguientes tareas:

- Configuración de una cuenta de servicio para la autenticación de AD con Kerberos [página 299]
- Ejecución de SIA bajo la cuenta de servicio de la plataforma de BI [página 308]
- Asignar grupos y usuarios de Windows AD [página 301]

### 13.1.6.1.2 Para configurar el complemento de seguridad de Windows AD para Kerberos

1. Diríjase al área de administración *Autenticación* de la CMC.
2. Haga doble clic en *Windows AD*.
3. Asegúrese de que está activada la casilla de verificación *Habilitar Windows Active Directory (AD)*.
4. En *Opciones de autenticación*, seleccione *Utilizar autenticación Kerberos*.
5. Si desea configurar el inicio de sesión único en una base de datos, active la casilla de verificación *Contexto de seguridad de caché (requerido para SSO en base de datos)*.
6. En el campo *Nombre de principal de servicios*, escriba la cuenta y el dominio de la cuenta de servicio o la asignación SPN a la cuenta de servicio.

Utilice el formato siguiente, en el que `<svcacct>` es el nombre de la cuenta de servicio o SPN creado anteriormente, y `<DNS.COM>` es el dominio completo en mayúsculas. Por ejemplo, la cuenta de servicio sería svcacct@DNS.COM y el SPN sería BOBJCentralMS/un_nombre@DOMINIO.COM

> **Nota**
>
> - Si tiene previsto permitir que usuarios de otros dominios distintos al predeterminado inicien sesión, debe proporcionar el SPN que asignó anteriormente.
> - La cuenta de servicio distingue entre mayúsculas y minúsculas. Las mayúsculas y minúsculas de la cuenta que se introduzca aquí deben coincidir con la configuración del dominio de Active Directory.
> - Ésta debe ser la misma cuenta que se utiliza para ejecutar los servidores de la plataforma de BI o el SPN que se asigna a esta cuenta.

7. Si desea configurar el inicio de sesión único, active *Habilitar inicio de sesión único para el modo de autenticación seleccionado*.

> **Nota**
>
> Si decidió habilitar el inicio de sesión único, deberá configurar el WACS.

### Información relacionada

Configuración del inicio de sesión único de AD Kerberos [página 537]

## 13.1.6.2 Crear los archivos de configuración

El proceso general de configuración de Kerberos en el servidor de aplicaciones implica estos pasos:

- Creación del archivo de configuración de Kerberos.
- Creación del archivo de configuración de inicio de sesión de JAAS.

> **Nota**
>
> - El dominio predeterminado de Active Directory debe tener el formato DNS en mayúsculas.
> - No necesita descargar e instalar MIT Kerberos para Windows. Tampoco resulta necesario disponer de un archivo keytab para la cuenta de servicio.

### 13.1.6.2.1 Para crear el archivo de configuración de Kerberos

Siga estos pasos para crear el archivo de configuración de Kerberos.

1. Cree el archivo `krb5.ini`, si no existe, y almacénelo en `C:\Windows`.

> **Nota**
>
> Puede almacenar este archivo en una ubicación diferente. No obstante, si lo hace, deberá especificar su ubicación en el campo *Ubicación del archivo Krb5.ini* en la página *Propiedades* del servidor WACS, en la CMC.

2. Agregue la siguiente información necesaria en el archivo de configuración de Kerberos:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

> **Nota**
>
> `DNS.COM` es el nombre DNS del dominio que se debe introducir en formato FQDN en mayúsculas.

> **Nota**
>
> `kdc` es el nombre de host del controlador de dominio.

> **Nota**
>
> Se pueden agregar varias entradas de dominio en la sección [realms] si los usuarios inician sesión desde distintos dominios. Para ver un ejemplo de archivo con varias entradas de dominio, consulte Archivos Krb5.ini de ejemplo [página 533].

> **Nota**
>
> En una configuración de varios dominios, en `[libdefaults]` el valor `default_realm` puede ser cualquiera de los dominios deseados. El procedimiento recomendado es utilizar el dominio con el número máximo de usuarios que se autenticarán con sus cuentas de AD.

## 13.1.6.2.2 Para crear el archivo de configuración de inicio de sesión de JAAS

1. Cree un archivo denominado `bscLogin.conf` si no existe y almacénelo en la ubicación predeterminada: `C:\Windows`

   > **Nota**
   >
   > Puede almacenar este archivo en una ubicación diferente. No obstante, si lo hace, deberá especificar su ubicación en el campo *Ubicación del archivo bscLogin.conf* en la página *Propiedades* del servidor WACS, en la CMC.

2. Agregue el código siguiente al archivo de configuración `bscLogin.conf` de JAAS:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Guarde y cierre el archivo.

## 13.1.6.2.3 Archivos Krb5.ini de ejemplo

### Ejemplo de archivo Krb5.ini con varios dominios

A continuación se muestra un ejemplo de archivo con varios dominios:

```
[domain_realm]
        .domain03.com = DOMAIN03.COM
        domain03.com = DOMAIN03.com
        .child1.domain03.com = CHILD1.DOMAIN03.COM
        child1.domain03.com = CHILD1.DOMAIN03.com
        .child2.domain03.com = CHILD2.DOMAIN03.COM
        child2.domain03.com = CHILD2.DOMAIN03.com
        .domain04.com = DOMAIN04.COM
        domain04.com = DOMAIN04.com
[libdefaults]
        default_realm = DOMAIN03.COM
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        DOMAIN03.COM = {
         admin_server = testvmw2k07
         kdc = testvmw2k07
         default_domain = domain03.com
        }
     CHILD1.DOMAIN03.COM = {
            admin_server = testvmw2k08
            kdc = testvmw2k08
            default_domain = child1.domain03.com
        }
        CHILD2.DOMAIN03.COM = {
            admin_server = testvmw2k09
            kdc = testvmw2k09
            default_domain = child2.domain03.com
        }
        DOMAIN04.COM = {
```

```
            admin_server = testvmw2k011
            kdc = testvmw2k011
            default_domain = domain04.com
        }
```

### Ejemplo de archivo Krb5.ini con un único dominio

A continuación se muestra un ejemplo de archivo krb5.ini con un único dominio.

```
[libdefaults]
        default_realm = ABCD.MFROOT.ORG
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        ABCD.MFROOT.ORG = {
            kdc = ABCDIR20.ABCD.MFROOT.ORG
            kdc = ABCDIR21.ABCD.MFROOT.ORG
            kdc = ABCDIR22.ABCD.MFROOT.ORG
            kdc = ABCDIR23.ABCD.MFROOT.ORG
            default_domain = ABCD.MFROOT.ORG
        }
```

## 13.1.6.3 Configurar WACS para AD Kerberos

Después de haber configurado el equipo que alojará WACS para la autenticación de AD Kerberos, debe configurar el WACS mediante la consola de administración central (CMC).

## 13.1.6.3.1 Para configurar WACS para AD Kerberos

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS para el que desea configurar AD.
   Aparecerá la pantalla *Propiedades*.
3. En el campo *Ubicación del archivo Krb5.ini*, especifique la ruta de acceso al archivo de configuración `krb5.ini`.
4. En el campo *Ubicación del archivo bscLogin.conf*, especifique la ruta de acceso al archivo de configuración `bscLogin.conf`.
5. Haga clic en *Guardar y cerrar*.
6. Renicie el WACS.

## 13.1.6.4 Solución de problemas de Kerberos

Estos pasos pueden ser útiles si surgen problemas al configurar Kerberos:

- Habilitar el inicio de sesión
- Probar la configuración de Kerberos

## 13.1.6.4.1 Para habilitar el registro de Kerberos

1. Inicie el Administrador de configuración central (CCM) y haga clic en *Administrar servidores*.
2. Especifique las credenciales de inicio de sesión.
3. En la pantalla *Administrar servidores*, detenga el WACS.
4. Haga clic en *Configuración del nivel Web*.

   > **Nota**
   >
   > El icono *Configuración del nivel Web* solo está activado cuando se selecciona un WACS que está detenido.

   Aparece la pantalla *Configuración del nivel Web*.
5. En *Parámetros de línea de comandos*, copie el siguiente texto al final de los parámetros:

   ```
   «-Dcrystal.enterprise.trace.configuration=verbose
    -Djcsi.Kerberos.debug=true»
   ```
6. Haga clic en *Aceptar*.
7. En la pantalla *Administrar servidores*, inicie el WACS.

## 13.1.6.4.2 Para probar la configuración de Kerberos

Ejecute el comando siguiente para probar la configuración de Kerberos, donde `servact` es la cuenta de servicio y el dominio en el que se ejecuta el CMS, y `contraseña` es la contraseña asociada con la cuenta de servicio.

```
<INSTALLDIR>\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

Por ejemplo:

```
 C:\Program Files\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM
Password
```

Si no se soluciona el problema, compruebe que las mayúsculas y minúsculas del dominio y del nombre principal de servicio coincidan exactamente con la configuración de Active Directory.

### 13.1.6.4.3 El usuario de AD asignado no puede iniciar una sesión en los servicios de la plataforma de BI en WACS

Se pueden producir los dos errores siguientes, a pesar de que los usuarios se hayan asignado a la plataforma de BI.

#### 13.1.6.4.3.1 Error de inicio de sesión debido a nombres UPN y SAM de AD distintos

El ID de Active Directory de un usuario se ha asignado correctamente a la plataforma de BI. A pesar de esto, no se puede iniciar la sesión correctamente en la CMC con la autenticación de AD y Kerberos con el formato siguiente: `DOMAIN\ABC123`

Este problema puede aparecer cuando el usuario se configura en Active Directory con un UPN y un nombre SAM que no son iguales, por las mayúsculas y minúsculas o por otra razón. A continuación se muestran dos ejemplos que pueden causar problemas:

- El UPN es abc123@company.com pero el nombre SAM es DOMAIN\ABC123.
- El UPN es jsmith@company pero el nombre SAM es DOMAIN\johnsmith.

Hay dos formas de solucionar este problema:

- Pida a los usuarios que inicien la sesión mediante el UPN en lugar del nombre SAM.
- Compruebe que el nombre de cuenta SAM y el nombre UPN son los mismos.

#### 13.1.6.4.3.2 Error de autenticación previa

Un usuario que anteriormente había podido iniciar sesión, ya no puede hacerlo correctamente. El usuario recibe este error: No se reconoció la información de la cuenta. Los registros de WACS muestran el siguiente error: `"Pre-authentication information was invalid (24)"`

Esto puede suceder porque la base de datos de usuarios de Kerberos no ha obtenido un cambio efectuado en UPN en AD. Puede significar que la base de datos de usuarios de Kerberos y la información de AD no están sincronizadas.

Para resolver este problema, restablezca la contraseña del usuario en AD. De este modo se garantiza que los cambios se propagan correctamente.

## 13.1.7 Configuración del inicio de sesión único de AD Kerberos

Si está configurando el inicio de sesión único de AD Kerberos para la plataforma de lanzamiento de BI o los SDK de servicios Web y QaaWS, debe asegurarse de que ha configurado WACS y el equipo que aloja WACS para la autenticación de AD Kerberos.

Para configurar WACS para el inicio de sesión único de AD Kerberos, primero debe configurar el equipo que aloja el WACS y, a continuación, configurar el propio WACS.

> **Nota**
>
> Si tiene pensado usar el inicio de sesión único en un entorno de proxy inverso, lea la información sobre seguridad de este manual.

### Información relacionada

Información general de seguridad [página 154]
Configurar AD Kerberos para WACS [página 529]
Configurar el equipo para el inicio de sesión único de AD Kerberos [página 537]
Configurar WACS para el inicio de sesión único de AD Kerberos [página 538]

## 13.1.7.1 Configurar el equipo para el inicio de sesión único de AD Kerberos

Para configurar el inicio de sesión único de AD Kerberos para SDK de servicios Web y QaaWS, primero debe configurar el equipo que aloje el WACS :

- Para configurar la delegación limitada para el SSO de Vintela [página 323]
- Para configurar la cuenta de servicio para el SSO de Vintela [página 320]
- Configuración de varios SPN [página 537]
- Aumentar el límite de tamaño del encabezado de WACS [página 538]

En las secciones siguientes se describe cómo completar cada uno de estos pasos.

## 13.1.7.1.1 Configuración de varios SPN

No se admite el uso de varios SPN.

### 13.1.7.1.2 Aumentar el límite de tamaño del encabezado de WACS

Active Directory crea un token de Kerberos que se utiliza en el proceso de autenticación. Este token se almacena en el encabezado HTTP. WACS tendrá un tamaño de encabezado HTTP predeterminado que será suficiente para la mayoría de usuarios. Este tamaño de encabezado se puede configurar.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS del que desea cambiar el tamaño del encabezado HTTP.
   Aparecerá la pantalla *Propiedades*.
3. En las secciones *Configuración HTTP*, *Configuración de HTTP a través de proxy* o *Configuración HTTPS*, especifique un valor en el campo *Tamaño máximo del encabezado HTTP (en bytes)*.
4. Haga clic en *Guardar y cerrar*.
5. Reinicie el servidor.

### 13.1.7.2 Configurar WACS para el inicio de sesión único de AD Kerberos

Puede configurar el servidor de contenedor de aplicaciones Web para usar el inicio de sesión único de AD Kerberos. Se admite el inicio de sesión único de AD Kerberos. No se admite AD NTLM.

Antes de configurar WACS, debe configurar el inicio de sesión único de AD Kerberos para el equipo que aloja el WACS.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS que desea configurar.
   Aparecerá la pantalla *Propiedades*.
3. Seleccione *Habilitar inicio de sesión único Kerberos de Active Directory*.
4. Especifique los valores para Dominio de AD predeterminado, Nombre principal del servicio y propiedades del archivo Keytab, y haga clic en *Guardar y cerrar* .
5. Reinicie WACS.

El inicio de sesión único de Active Directory está listo para su uso.

### 13.1.7.3 Configurar Kerberos y el inicio de sesión único en la base de datos

Se admite el inicio de sesión único en la base de datos para los despliegues que cumplan estos requisitos:

- El despliegue de la plataforma de información se encuentra en WACS.
- WACS se ha configurado con AD con Kerberos.
- La base de datos en la que se requiere el inicio de sesión único es una versión compatible de SQL Server u Oracle.

- A los grupos o usuarios que necesitan acceso a la base de datos se les debe haber concedido permisos en SQL Server u Oracle.
- La casilla de verificación de contexto de seguridad de caché (que se requiere para el inicio de sesión único en la base de datos) de la página de autenticación de AD está activada.

El paso final consiste en modificar el archivo `krb5.ini` para admitir el inicio de sesión único en la base de datos.

> **Nota**
>
> En estas instrucciones se explica cómo configurar el inicio de sesión único en la base de datos. Si desea configurar un inicio de sesión único integral en la base de datos, también debe realizar los pasos de configuración necesarios para el inicio de sesión único de Vintela. Para obtener información más detallada, consulte Configuración del inicio de sesión único de AD Kerberos [página 537].

### 13.1.7.3.1 Activar el inicio de sesión único en la base datos

1. Abra el archivo `krb5.ini` que se usa para el despliegue de la plataforma de BI.

   La ubicación predeterminada de este archivo es el directorio C:\Windows en el servidor de aplicaciones Web.
2. Vaya a la sección `[libdefaults]` del archivo.
3. Introduzca esta cadena antes del inicio de la sección `[realms]` del archivo:

   ```
   forwardable = true
   ```
4. Guarde y cierre el archivo.
5. Reiniciar el WACS

## 13.1.8 Configurar servicios Web RESTful

El SDK de servicios Web RESTful de la plataforma de Business Intelligence permite acceder a la plataforma de BI con el protocolo HTTP. Permite a los usuarios explorar el repositorio de la plataforma de BI y los objetos programados con cualquier idioma de programación que admita solicitudes HTTP. Los servicios Web RESTful se instalan como parte del WACS.

En esta sección se describe cómo administrar los servicios Web RESTful. Para obtener más información sobre los servicios Web RESTful, consulte el *Manual del desarrollador de servicios Web RESTful de la plataforma de Business Intelligence*.

## 13.1.8.1 Aplicaciones

### 13.1.8.1.1 Configurar la URL básica para servicios Web RESTful

Si el despliegue de la plataforma de BI usa un servidor proxy o contiene más una instancia del servidor contenedor de aplicaciones Web (WACS), es posible que necesite configurar la URL para su uso con servicios Web RESTful. Antes de configurar la URL básica, debe saber el nombre del servidor y el número de puerto que atiende a solicitudes de servicios Web RESTful.

La URL se usa como parte de las solicitudes de servicios Web RESTful. Los desarrolladores descubren mediante programación la URL básica y la usan para dirigir las solicitudes de servicios Web RESTful al servidor y al puerto correctos. La URL básica se usa además en las respuestas de servicios Web RESTFUL para definir hipervínculos a otros recursos RESTful.

> **Nota**
>
> En las instalaciones predeterminadas de la plataforma de BI, la URL básica se define como `http://<servername>:6405/biprws`. Sustituya `<servername>` con el nombre del servidor que tiene en host los servicios Web RESTful.

1. Inicie sesión en la Consola de administración central (CMC) como administrador.
2. En la CMC, haga clic en *Aplicaciones*.
   Se mostrará una lista de aplicaciones.
3. Haga clic con el botón derecho en *Servicio Web RESTful* > *Propiedades*.
   Aparece la página *Propiedades: Servicio Web RESTful*. Ahora se ha introducido la casilla de selección *Utilizar vía de acceso de URL relativa* en la página para tener en cuenta la URL de su navegador para iniciar el servicio Web RESTful. Para obtener más información, consulte la nota SAP 3048101.
4. En el cuadro de diálogo *Acceder a la dirección URL*, escriba el nombre de la URL base para los servicios Web RESTful.
   Por ejemplo, escriba `http://<servername>:<portnumber>/biprws`. Sustituya `<servername>` y `<portnumber>` por el nombre del servidor y el puerto que atiende a las solicitudes de servicios Web RESTful.

   > **Precaución**
   >
   > - **Se admiten los servidores Tomcat, WACS, JBoss, SAP NetWeaver y WebSphere** para las API de servicios Web RESTful.
   > - La *URL de acceso* muestra la URL WACS de **forma predeterminada**. Si desea utilizar las API de servicio web RESTful en el servidor web Tomcat, asegúrese de modificar los valores requeridos de `<server>` y `<port>` en consecuencia.

5. Haga clic en *Guardar y cerrar*.

   > **Nota**
   >
   > Si habilitamos *Utilizar vía de acceso de URL relativa*, se utiliza la URL relativa del navegador.

## 13.1.8.2 Propiedades de WACS

### 13.1.8.2.1 Configurar los parámetros de la línea de comandos de métodos y encabezados

Como administrador, puede restringir los métodos y los encabezados que usen los servicios Web RESTful, agregando las opciones adecuadas a los *Parámetros de la línea de comandos* en las propiedades del servicio de contenedores de aplicaciones Web (WACS). Las modificaciones de los parámetros requieren el reinicio del servicio WACS.

1. Inicie sesión en la Consola de administración central como usuario administrador.
2. Haga clic en *Servidores* y, a continuación, haga clic en *Lista de servidores*.
3. Haga clic con el botón derecho en el servidor de contenedor de aplicaciones Web (WACS), por ejemplo, `MySIA.WebApplicationContainerServer` y haga clic en *Propiedades*.
   Aparecerá la ficha *Propiedades* para el servidor WACS.
4. En el área *Parámetros de línea de comandos*, introduzca los métodos y encabezados permitidos.

   Cada grupo de opciones se encuentra entre comillas dobles. Use métodos que no sean `GET`, `HEAD` y `POST`. Use comas para separar valores de opción como por ejemplo `PUT` y `DELETE` tal y como se muestra en el ejemplo siguiente.

   ```
   "-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"
   "-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-
   Authenticate"
   ```

   > **Nota**
   >
   > El valor predeterminado para permitir todos los métodos y encabezados es * (asterisco). Si se omiten todos los parámetros de la línea de comandos, se consigue el mismo efecto.

5. Haga clic en *Guardar y cerrar*.
6. Reinicie el servicio haciendo clic con el botón derecho en el nombre del servidor WACS, por ejemplo `MySIA.WebApplicationContainerServer` y haga clic en *Reiniciar servidor*.

### 13.1.8.2.2 Configuración de la propiedad del sistema

#### 13.1.8.2.2.1 Habilitar la pila de mensajes de error

Como administrador, puede configurar los mensajes de error que devuelven los servicios Web RESTful para incluir la pila de errores. La pila de errores proporciona información adicional de depuración que puede usarse para descubrir en dónde se han producido los errores.

> **Nota**
>
> Es posible que no desee habilitar la pila de errores en escenarios de producción porque puede ofrecer información sobre la plataforma de BI que no desea revelar a los usuarios finales. Se recomienda habilitar la pila de errores en escenarios de producción ya que es necesaria para la depuración y desactivarla cuando no sea necesario.

1. Inicie sesión en la Consola de administración central como usuario administrador.
2. Haga clic en *Servidores* y, a continuación, haga clic en *Lista de servidores*.
3. Haga clic con el botón derecho en el servidor de contenedor de aplicaciones Web (WACS), por ejemplo, `MySIA.WebApplicationContainerServer` y haga clic en *Propiedades*.
   Aparecerá la ficha *Propiedades* para el servidor WACS.
4. En el área *Servicio Web RESTful*, seleccione *Mostrar pila de errores*.
5. Haga clic en *Guardar y cerrar*.

La información de la pila de errores se incluirá en los mensajes de error de los servicios Web RESTful.

### 13.1.8.2.2.2 Fijar el número predeterminado de entradas mostradas en cada página

Si una respuesta del servicio Web RESTful contiene un canal con una gran cantidad de entradas, la respuesta se puede dividir en páginas. Puede configurar el número predeterminado de entradas que se muestran en cada página. Si los desarrolladores realizan solicitudes de servicios Web RESTful, pueden especificar el número de entradas para mostrar en cada página. Sin embargo, si no especifica este valor, se utilizará el tamaño predeterminado de página.

1. Inicie sesión en la Consola de administración central como administrador.
2. Haga clic en *Servidores* y, a continuación, haga clic en *Lista de servidores*.
3. Haga clic con el botón derecho en el servidor de contenedor de aplicaciones Web (WACS), por ejemplo, `MySIA.WebApplicationContainerServer` y haga clic en *Propiedades*.
   Aparecerá la ficha *Propiedades* para el servidor WACS.
4. En el área *servicio Web RESTful*, escriba el tamaño predeterminado de página en el área de texto *Número predeterminado de objetos en una página*.
5. Haga clic en *Guardar y cerrar*.

### 13.1.8.2.2.3 Establecer el valor de tiempo de espera de un token de inicio de sesión

Los tokens de inicio de sesión caducan si no se usan durante un período de tiempo. Se puede establecer el tiempo de validez de un token de inicio de sesión sin usar.

> **Nota**
>
> De forma predeterminada, el valor de tiempo de espera de un token de inicio de sesión es de una hora.

1. Inicie sesión a la Consola de administración central como administrador.
2. Haga clic en *Servidores* y, a continuación, haga clic en *Lista de servidores*.
3. Haga clic con el botón derecho en el servidor de contenedor de aplicaciones Web (WACS), por ejemplo, `MySIA.WebApplicationContainerServer` y haga clic en *Propiedades*.
   Aparecerá la ficha *Propiedades* para el servidor WACS.

4. En el área *Servicio Web RESTful*, escriba el número de minutos de validez de un token de inicio de sesión en el área de texto *Tiempo de espera del token de sesión Enterprise (minutos)*.
5. Haga clic en *Guardar y cerrar*.

## 13.1.8.2.2.4 Configurar el grupo de sesiones

Puede mejorar el rendimiento del servidor con el grupo de sesiones. El grupo de sesiones atrapa sesiones de servicios Web RESTful de manera que se puedan volver a usar cuando el usuario envíe otra solicitud que use el mismo token de inicio de sesión en la cabecera de solicitud HTTP. El tamaño de grupo de sesiones determina el número de sesiones almacenadas en caché que se almacenarán en conjunto, y el valor de tiempo de espera de la sesión controla el tiempo que una sesión se almacena en caché.

Puede establecer el tamaño de grupo de sesiones y el valor de tiempo de espera de la sesión:

1. Inicie sesión en la Consola de administración central (CMC) como administrador.
2. Haga clic en *Servidores* y, a continuación, haga clic en *Lista de servidores*.
3. Haga clic con el botón derecho en el servidor de contenedor de aplicaciones Web (WACS), por ejemplo, `MySIA.WebApplicationContainerServer` y haga clic en *Propiedades*.
   Aparecerá la ficha *Propiedades* para el servidor WACS.
4. Escriba el número máximo de sesiones para almacenar en caché en el cuadro de texto *Tamaño de grupo de sesiones* del área *Servicio Web RESTful*.
5. Escriba el valor de tiempo de espera del grupo de sesiones en el cuadro de texto *Tiempo de espera del grupo de sesiones (minutos)* del área *Servicio Web RESTful*.
6. Haga clic en *Guardar y cerrar*.
7. Haga clic con el botón derecho en el servidor WACS, por ejemplo, `MySIA.WebApplicationContainerServer` y haga clic en *Reiniciar servidor*.

## 13.1.8.2.2.5 Habilitar la autenticación HTTP básica

La autenticación HTTP básica permite a los usuarios realizar consultas de servicios Web RESTful sin necesidad de proporcionar un token de inicio de sesión. Si está habilitada la autenticación HTTP básica, se pedirá a los usuarios que introduzca su nombre de usuario y contraseña la primera vez que realicen una solicitud de servicios Web RESTful.

> **Nota**
>
> Los nombres de usuario y las contraseñas no se transmiten de manera segura con la autenticación HTTP básica, a menos que se use junto con HTTPS.

Cuando habilita la autenticación HTTP básica, establece el tipo predeterminado de autenticación HTTP básica para SAP, Enterprise, LDAP o WinAD. Los usuarios pueden sobrescribir el tipo de autenticación HTTP básica cuando inicien sesión.

Al iniciar sesión en la plataforma de BI con una autenticación HTTP básica se consume la licencia. Si se usa la memoria caché del grupo de sesiones, la solicitud hace uso de la licencia asociada a la sesión almacenada en

caché. Si no se usa la memoria caché del grupo de sesiones, se consumirá la licencia mientras que la solicitud esté en progreso y se liberará cuando esta finalice.

1. Inicie sesión en la Consola de administración central (CMC) como administrador.
2. Haga clic en *Servidor* > *Lista de servidores*.
3. Haga clic con el botón derecho en el servidor de contenedor de aplicaciones Web (WACS), por ejemplo, `MySIA.WebApplicationContainerServer` y haga clic en *Propiedades*.
   Aparecerá la ficha *Propiedades* para el servidor WACS.
4. En el área *Servicio Web RESTful*, seleccione *Habilitar autenticación HTTP básica*.
5. (Opcional) En la lista *Esquema de autenticación predeterminado para HTTP básica*, seleccione el tipo predeterminado de autenticación HTTP básica.
6. Haga clic en *Guardar y cerrar*.

Cuando un usuario final inicia sesión con la autenticación HTTP básica, puede especificar el tipo de autenticación que desea usar. En un explorador Web, el usuario escribe `<tipo de autenticación>\<nombre de usuario>` en la petición del nombre de usuario y `<contraseña>` en la petición de contraseña.

Para iniciar sesión con la autenticación HTTP básica programada, los usuarios agregan el atributo `Autorización` a la cabecera de solicitud HTTP y establecen el valor para que sea `<tipo de autenticación> básica\<nombre de usuario>: <contraseña>`.

Sustituya `<tipo de autenticación>` por el tipo de autenticación, `<nombre de usuario>` por el nombre de usuario y `<contraseña>` por la contraseña. El tipo de autenticación, el nombre de usuario y la contraseña deben estar codificados como base64 y definidos por la RFC 2617. Los nombres de usuario que contengan el carácter `:` no se pueden usar con la autenticación HTTP básica.

### Información relacionada

Configurar el grupo de sesiones [página 543]

## 13.1.8.2.3 Uso compartido de recursos de origen cruzado

### 13.1.8.2.3.1 Configurar uso compartido de recursos de origen cruzado (CORS)

El ajuste *Configuración de uso compartido de recursos de origen cruzado* (CORS) le permite agregar una lista de nombres de dominio para que los usuarios recuperen datos de orígenes múltiples en páginas Web basadas en JavaScript. Esto es necesario para evitar la política de seguridad que los idiomas de JavaScript y Ajax emplean para prevenir acceso de dominios cruzados. Para evitar el compromiso de la seguridad, solo los sitios Web a los que se puede acceder se agregan a las propiedades del servidor WACS *Permitir orígenes* en la CMC.

También hay disponible un ajuste *Antigüedad máxima (minutos)* para ajustar el tiempo de expiración de caché, lo que establece el número máximo de minutos que los exploradores pueden conservar solicitudes HTTP.

> **Nota**
>
> De forma predeterminada, el acceso a todos los dominios se permite con un * (asterisco).

1. Inicie sesión en la Consola de administración central como administrador.
2. Haga clic en *Servidor* > *Lista de servidores*.
3. Haga clic con el botón derecho en el servidor de contenedor de aplicaciones Web (WACS), por ejemplo, `MySIA.WebApplicationContainerServer` y haga clic en *Propiedades*.
   Aparecerá la ficha *Propiedades* para el servidor WACS.
4. En el área *Servicio Web RESTful*, vaya al cuadro de texto *Configuración de uso compartido de recursos de origen cruzado* junto a *Permitir orígenes:* y sustituya el * (asterisco) por la lista de nombres de dominio, separados por una coma. Por ejemplo: `http://origin1.server:8080, http://origin2.server:8080`
5. En el cuadro de texto *Antigüedad máxima (minutos):* , escriba el número máximo de minutos que desea que los exploradores agrupen en caché las solicitudes HTTP.
6. Haga clic en *Guardar y cerrar*.

## 13.1.8.2.4 Autenticación

### 13.1.8.2.4.1 Configurar web.xml para habilitar WinAD SSO

La configuración de servicios Web RESTful para reconocer el inicio de sesión único de Windows Active Directory (WinAD SSO) requiere editar el archivo de configuración `web.xml`, ubicado en el servidor de la plataforma de BI. Para obtener más información, consulte «Usar el SDK > Autenticación > Obtener un identificador de inicio de sesión mediante el uso de una cuenta de inicio de sesión único de Active Directory (AD SSO) » en el *Manual del desarrollador de servicio Web RESTful de la plataforma de Business Intelligence*.

Para que el servidor de la plataforma de BI reconozca las credenciales de inicio de sesión SSO WinAD de un equipo de cliente, debe eliminar los comentarios de la sección del `filtro proxy de Kerberos` de `web.xml` y actualizar los valores de `idm.realm`, `idm.princ` e `idm.keytab` que reflejan el entorno del directorio activo usado.

1. Localice la configuración `web.xml` en `<raíz boe>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\`. La siguiente ruta de archivos es un ejemplo.

   ```
   C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
   4.0\java\
   pjs\services\RestWebService\biprws\WEB-INF\web.xml
   ```

2. En el archivo `web.xml`, borre el comentario de la sección Filtro proxy de Kerberos agregando una etiqueta de comentario de cierre `-->` antes de la etiqueta `<filtro>`, y elimine la etiqueta de cierre de comentario `-->`

   ```
     <!-- Kerberos Proxy Filter
       - Uncomment this filter and the corresponding filter-mapping to enable
   Kerberos SSO
       - for Windows AD (secWinAD) authentication.
       - The following options must be specified (the rest are optional):
       -   idm.realm
   ```

```
    -   idm.princ
    -   idm.keytab (unless using password, see below)
  -->
  <filter>
    <filter-name>WrappedResponseAuthFilter</filter-name>
      .
      .
      .
  </filter>
  <filter-mapping>
    <filter-name>WrappedResponseAuthFilter</filter-name>
    <url-pattern>/logon/adsso</url-pattern>
  </filter-mapping>

</web-app>
```

3. Actualice el `<param-value>` para cada ajuste de `idm.realm`, `idm.princ` e `idm.keytab` con los usados en el entorno del directorio activo.

```
    <init-param>
      <param-name>idm.realm</param-name>
      <param-value>ADDOM.COM</param-value>
      <description>
          Required: Set this value to the Kerberos realm to use.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.princ</param-name>
      <param-value>BOE120SIAVMBOESRVR/bo.service.addom.com</param-value>
      <description>
          Set this value to the Kerberos service principal to use.
          This will be a name of the form HTTP/fully-qualified-host.
          For example, HTTP/example.vintela.com
          If not set, defaults to the server's hostname and the
          idm.realm  property above.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.kdc</param-name>
      <param-value></param-value>
      <description>
          The KDC against which secondary credentials must be validated
          This can be used for BASIC fallback or credential delegation.
          By default the KDC will be discovered automatically and this
          parameter must only be used if automatic discovery fails, or
          if a different KDC to the one discovered must automatically be used.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.keytab</param-name>
      <param-value>C:/winnt/BOE120SIAVMBOESRVR.keytab</param-value>
      <description>
          The file containing the keytab that Kerberos will use for
          user-to-service authentication. If unspecified, SSO will default
          to using an in-memory keytab with a password specified in the
          com.wedgetail.idm.sso.password environment variable.
      </description>
    </init-param>
```

> **Nota**
>
> El valor `idm.keytab` hace referencia a una ruta de archivos del servidor de la plataforma de BI. Los valores para `idm.realm` e `idm.prince` se pueden ver desde la consola de administración central. En la ficha *Autenticación* en la CMC, haga doble clic en *Windows AD*. El valor de `idm.realm` se establece con el parámetro *Dominio predeterminado de AD*, en *Resumen de configuración de AD*. El

valor de `idm.prince` se establece con el parámetro *Nombre de principal de servicios*, en *Opciones de autenticación*.

4. Reinicie el servicio WACS para que se reconozcan los cambios realizados en `web.xml`.
5. Use un equipo de cliente para verificar que el identificador de inicio de sesión SSO AD se recupera mediante el API de servicios Web RESTful, (por ejemplo, `http://<boe host>:6405/biprws/logon/adsso`).
6. Verifique el identificador usando una consulta `GET` que incluya `X-SAP-LogonToken` en el encabezado y con el API `/infostore`.

## 13.1.8.2.4.2 Habilitar y configurar la autenticación de confianza

La autenticación de confianza se activa y se configura con la Consola de administración central (CMC) en las áreas que incluyen *Autenticación > Enterprise*, donde está habilitada. Se genera un archivo de claves de secretos compartidos, *Usuarios y grupos > Lista de usuarios*, donde se crea una cuenta para un usuario de confianza en la ruta *Servidores > Lista de servidores > WACS > Propiedades*. Aquí se selecciona la opción *Método de recuperación* para las solicitudes de token de inicio de sesión de API `/logon/trusted`.

> **Nota**
>
> No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

1. Inicie sesión en la Consola de administración central como administrador.
2. Vaya a *Autenticación* > *Enterprise* y haga clic en *Autenticación con confianza activada*.
3. Haga clic en *Nuevo secreto compartido* y haga clic en *Descargar secreto compartido*.
4. Haga clic en *Guardar* y coloque el archivo `TrustedPrincipal.conf` en la ubicación predeterminada, que es `<EnterpriseDir>\<platform>`.
   Aparece un ejemplo de ubicación de la forma siguiente:

   ```
   "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI 4.0\win64_x64\"
   ```

   > **Nota**
   >
   > Puede modificar la ubicación predeterminada del archivo de secretos compartidos `TrustedPrincipal.conf`; para ello, añada una entrada de la línea de comandos en la CMC, en *Servidores > Lista de servidores > WACS > Propiedades > Parámetros de la línea de comandos*, y luego reinicie el servicio WACS. Por ejemplo, una entrada de la línea de comandos con `-Dbobj.trustedauth.home=` y la carpeta `SharedSecrets` ubicada en la raíz de la unidad `C:\` del servidor de la plataforma de BI aparecería del siguiente modo:
   >
   > ```
   > "-Dbobj.trustedauth.home=C:\SharedSecrets"
   > ```

> **Nota**
>
> Puede dejar la opción *Período de validez (días) del secreto compartido* en el valor predeterminado cero (0) para que no caduque. La opción *La solicitud de conexión con confianza expira tras N milisegundo(s) (0 indica sin límite)* se puede dejar con el valor predeterminado cero (0) para que no haya límite de tiempo para las solicitudes de inicio de sesión de confianza.

5. Haga clic en *Actualizar* para guardar el cambio.
6. Añada un usuario y una contraseña nuevos (por ejemplo, `bob` y `Passw0rd`) en *Usuarios y grupos* > *Lista de usuarios* siguiendo la ruta *Administrar > Nuevo > Usuario nuevo*. Desmarque *El usuario debe cambiar la contraseña en la última conexión* y, a continuación, haga clic en *Crear y cerrar*.

   > **Nota**
   >
   > También puede crear un usuario nuevo haciendo clic en el icono *Crear usuario nuevo*, o haciendo clic con el botón derecho en un área abierta de la ventana que enumera los nombres de usuario, y seleccione *Nuevo* > *Usuario nuevo*.

7. Vaya a *Servidores* > *Servicios centrales* > *WACS* > *Propiedades*, desplácese hasta la sección *Configuración de autenticación de confianza* y utilice el menú *Método de recuperación* para seleccionar *HTTP_HEADER*, *QUERY_STRING* o *COOKIE*.

   > **Nota**
   >
   > De forma opcional, puede modificar el *parámetro de nombre de usuario* de la etiqueta predeterminada de `X-SAP-TRUSTED-USER` a cualquier otra etiqueta adecuada (por ejemplo, `UserName`, `bankteller` o `nurse`) que deberán utilizar los desarrolladores de servicios web RESTful.

8. Reinicie el servicio haciendo clic con el botón derecho en el nombre del servidor WACS (por ejemplo, `MySIA.WebApplicationContainerServer`) y haga clic en *Reiniciar servidor*.

   > **Nota**
   >
   > Después, cambiar la opción en *Recuperar método* como se muestra en el paso 7 no requiere que se reinicie el WACS.

9. Compruebe que puede recuperar un token de inicio de sesión utilizando la API `.../biprsw/logon/trusted/` y enviando una solicitud `GET` con la etiqueta de cabecera predeterminada de `X-SAP-TRUSTED-USER` con el nombre de usuario que ha creado en el paso 6.

### 13.1.8.2.4.3 Configurar el parámetro de la línea de comandos para reubicar el archivo de configuración `TrustedPrincipal.conf` del secreto compartido

Los servicios Web RESTful incluyen un parámetro de la línea de comandos para seleccionar una ubicación distinta para el archivo de autenticación de confianza `TrustedPrincipal.conf`.

El archivo `TrustedPrincipal.conf` contiene una clave de secreto compartido que se genera a través de CMC: haga clic en *Autenticación* y después doble clic en *Enterprise*. Seleccione *Autenticación de confianza habilitada* y haga clic en el botón *Nuevo secreto compartido*. Guarde el archivo haciendo clic en *Descargar secreto compartido* y guardando el archivo en la ubicación predeterminada.

Actualice la línea de comandos del servidor de contenedores de la aplicación Web (WACS) con una ruta personalizada para el archivo `TrustedPrincipal.conf` de la manera siguiente:

1. Inicie sesión en la Consola de administración central como usuario administrador.
2. Haga clic en *Servidores* y, a continuación, haga clic en *Lista de servidores*.
3. Haga clic con el botón derecho en el servicio WACS, por ejemplo, `MySIA.WebApplicationContainerServer`, y haga clic en *Propiedades*.
   Aparecerá la ficha *Propiedades* para el servidor WACS.
4. En el área *Parámetros de línea de comandos* introduzca la ruta al directorio que contiene el archivo `TrustedPrincipal.conf`.

   La cadena se encuentra entre comillas dobles tal como se muestra en el ejemplo siguiente.

   ```
   "-Dbobj.trustedauth.home=C:\SharedSecrets"
   ```

   > **Nota**
   >
   > La ubicación predeterminada del archivo `TrustedPrincipal.conf` es `<EnterpriseDir>\<platform>`. Un ejemplo de ubicación es:
   >
   > ```
   > C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise
   > XI 4.0\win64_x64
   > "
   > ```

5. Haga clic en *Guardar y cerrar*.
6. Reinicie el servicio haciendo clic con el botón derecho en el nombre del servidor WACS, por ejemplo `MySIA.WebApplicationContainerServer` y haga clic en *Reiniciar servidor*.

## 13.1.9 WACS y el entorno de TI

En esta sección se describe cómo configurar un WACS en un entorno complejo.

### 13.1.9.1 Utilizar WACS con otros servidores web

Cuando está instalado un servidor de contenedor de aplicación Web (WACS), funciona como un servidor de aplicaciones y un servidor web sin que sea necesario efectuar configuración adicional. Puede configurar los servidores web compatibles, como Internet Information Services (IIS) y Apache, para llevar a cabo el reenvío de URL al servidor WACS.

> **Nota**
>
> No se admite el reenvío de solicitudes desde IIS mediante un filtro ISAPI a WACS.

WACS no admite un escenario de despliegue donde un servidor web aloja contenido estático y WACS aloja contenido dinámico. El contenido estático y dinámico siempre se debe encontrar en el WACS.

## 13.1.9.2 Usar WACS con un equilibrador de carga

Para usar WACS en un despliegue con un equilibrador de carga de hardware, debe configurar el equilibrador de carga de modo que utilice el enrutamiento IP o cookies activas. De esta forma, una vez que se establece la sesión de un usuario en un WACS, todas las solicitudes posteriores efectuadas por el mismo usuario se envían al mismo WACS.

WACS no admite con equilibradores de carga de hardware que usen cookies pasivas.

Si su equilibrador de carga de hardware reenvía las solicitudes de HTTPS cifradas con SSL al WACS, debe configurar HTTPS en el WACS e instalar certificados SSL en cada WACS.

Si su equilibrador de carga de hardware descifra el tráfico HTTPS y reenvía solicitudes HTTP descifradas al WACS, no se requiere configuración de WACS adicional.

### Información relacionada

Configurar HTTPS/SSL [página 525]

## 13.1.9.3 Usar WACS con un proxy inverso

Puede usar WACS en un despliegue con un servidor de reenvío o proxy inverso. No puede usar el WACS como un servidor proxy.

### 13.1.9.3.1 Para configurar WACS para que admita HTTP con un proxy inverso

Para usar WACS en un despliegue con un proxy inverso, configure el WACS de modo que se utilice el puerto HTTP para las comunicaciones en un servidor de seguridad (por ejemplo, en una red segura) y el puerto HTTP mediante proxy se utiliza para las comunicaciones desde fuera del servidor de seguridad (por ejemplo, Internet).

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS que desea configurar.
   Aparecerá la pantalla *Propiedades*.
3. En la sección *Configuración de HTTP mediante proxy*:
   a. Active *Habilitar HTTP mediante proxy*.
   b. Especifique el puerto HTTP del WACS que se utilizará para las comunicaciones a través del proxy.
   c. Especifique el nombre de host de proxy y el puerto de proxy en el servidor proxy.
4. Haga clic en *Guardar y cerrar*.

### 13.1.9.3.2 Para configurar WACS para admitir HTTPS con un proxy inverso

Algunos equilibradores de carga y los servidores proxy inversos se pueden configurar para descifrar el tráfico HTTPS y, a continuación, reenviar el tráfico descifrado a los servidores de aplicaciones. En este caso, puede configurar WACS para usar HTTP o HTTP mediante proxy.

Si su equilibrador de carga o proxy inverso reenvía el tráfico HTTPS y desea configurar HTTPS con un proxy inverso, cree dos WACS. Configure un WACS para HTTPS para el tráfico externo a través del proxy inversos y el otro WACS para que se comunique con los clientes de la red interna a través de HTTPS.

## 13.1.9.4 Uso de WACS con servidores de seguridad

Se admite el despliegue de WACS en un entorno de TI con servidores de seguridad.

De forma predeterminada, WACS se enlaza a todas las direcciones IP del equipo en el que está instalado. Si planea usar un servidor de seguridad entre los clientes y el WACS, debe forzar que WACS se enlace a una dirección IP específica para HTTP o HTTP mediante proxy. Para ello, desactive *Enlazar a todas las direcciones IP* y, a continuación, especifique un nombre de host o una dirección IP para enlazar.

Si planea usar un servidor de seguridad entre un servidor WACS y otros servidores del despliegue, consulte la sección «Comprender la comunicación entre los componentes de la plataforma SAP BusinessObjects Business Intelligence» del *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*.

### Información relacionada

Comprender la comunicación entre los componentes de la Plataforma de BI [página 193]

## 13.1.9.5 Configurar WACS en un equipo multibase

Un equipo multibase es el que tiene varias direcciones de red. De forma predeterminada, una instancia de servidor de contenedor de aplicación Web enlaza su puerto HTTP a todas las direcciones IP. Si desea enlazar WACS a una tarjeta de interfaz de red específica (NIC), por ejemplo, cuando desea enlazar el puerto HTTP del WACS a una NIC y enlazar el puerto de solicitud a otra NIC:

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS que desea configurar.
   Aparecerá la pantalla *Propiedades*.
3. En la sección *Configuración de HTTP mediante proxy* del panel *Servicio de contenedor de aplicaciones Web*, desactive *Enlazar a todas las direcciones IP* y escriba una dirección IP para que se enlace el WACS.
4. En la sección *Configuración de HTTP*, desactive *Enlazar a todas las direcciones IP* y escriba una dirección IP o nombre de host para que se enlace el WACS.

5. En *Configuración común*, anule la selección de *Asignar automáticamente* y, a continuación, especifique el nombre de host o la dirección IP de la NIC que se usa para las comunicaciones entre WACS y los demás servidores de la plataforma de BI del despliegue.
6. Haga clic en *Guardar y cerrar*.
7. Renicie el WACS.

## 13.1.10 Configurar propiedades de aplicaciones Web

Las propiedades de aplicaciones Web alojadas en WACS se pueden configurar de las maneras siguientes:

- Las propiedades que se modifican con frecuencia están expuestas como propiedades de servicio configurables para WACS. Para editar estas propiedades, abra la página *Propiedades* de WACS en la Consola de administración central (CMC), modifique el valor para la propiedad adecuada y haga clic en *Guardar*.
- Para modificar los tiempos de espera de aplicaciones Web alojadas en WACS, en primer lugar determine si la aplicación Web tiene alguna propiedad que se pueda configurar en la CMC.
  Si la aplicación Web tiene propiedades que se puedan modificar en la CMC, modifique el archivo `web_xml.ino` de la aplicación Web. El archivo es `<nombre de la aplicación Web>_web_xml.ino`, donde `<nombre de la aplicación Web>` es el nombre de la aplicación Web que se puede encontrar en el directorio `<directorio de Enterprise>/java/pjs/services/<nombre de la aplicación Web>`.
  Si la aplicación Web no tiene propiedades que se puedan modificar en la CMC, modifique el archivo `web.xml` de la aplicación Web. Puede encontrar este archivo en `<directorio de Enterprise>/warfile/webapps/<nombre de la aplicación Web>`, donde `<nombre de la aplicación Web>` es el nombre de la aplicación Web.
- Para modificar otras propiedades distintas del tiempo de espera de la sesión o las propiedades que aparecen en la pantalla *Propiedades* de WACS en la CMC, modifique el archivo `.properties` de la aplicación Web. Para obtener más información, consulte la sección «Administrar aplicaciones mediante las propiedades de BOE.war» del *Manual del administrador de la plataforma de SAP BI*.

> **Nota**
>
> No modifique los archivos `web.xml`, `web_xml.ino` o `.properties` del directorio `<directorio de Enterprise>/java/pjs/container/work/<Nombre descriptivo del servidor>`, ya que los cambios se sobrescribirán cada vez que se inicie o reinicie el WACS.

> **Nota**
>
> Siempre tiene que reiniciar el WACS después de modificar sus propiedades.

### Información relacionada

Para cambiar las propiedades de un servidor [página 462]
El archivo BOE WAR [página 761]

## 13.1.11 Solución de problemas

### 13.1.11.1 Configurar el seguimiento en WACS

Para configurar el seguimiento para WACS, consulte Registro de seguimientos para componentes [página 1075].

### 13.1.11.2 Para ver las medidas de un servidor

Puede ver las métricas de servidor de un WACS desde la Consola de administración central (CMC).

1. Vaya al área de administración *Servidores* de CMC.
2. Haga clic con el botón derecho en el WACS y haga clic en *Métricas*.

#### Información relacionada

Métricas del Servidor de contenedor de aplicación Web [página 1211]

### 13.1.11.3 Para ver el estado de un WACS

Para ver el estado de un WACS, vaya al área *Servidores* de CMC. La *lista de servidores* incluye una columna *Estado* que proporciona el estado de cada servidor de la lista.

WACS tiene un nuevo estado de servidor denominado «Se ejecutó con errores». Este estado significa que WACS se está ejecutando, pero que tiene una o más de estas condiciones de error:

- Un conector HTTP, HTTP mediante Proxy, o HTTPS está mal configurado.
- Un servicio que se está ejecutando en WACS, como el servicio de registro de seguimiento, no funciona correctamente.
- No se ha podido implementar una aplicación web en WACS.

Consulte la página *Propiedades* de WACS para ver qué servicios han fallado.

### 13.1.11.4 Resolver conflictos de puerto

Si no puede obtener ninguna página cuando intenta acceder a la CMC a través de un determinado puerto, asegúrese de que otra aplicación no ha ocupado los puertos HTTP, HTTP mediante proxy o HTTPS que ha especificado para WACS.

Existen dos formas de determinar si hay conflictos de puerto con el WACS. Si tiene varios WACS en el despliegue, inicie sesión en la CMC y compruebe la lista de métricas Conectores de WACS en ejecución y

Errores de inicio de WACS. Si los conectores HTTP, HTTP mediante proxy o HTTP no aparecen en la lista Conectores WACS en ejecución, estos conectores no podrán iniciarse debido a un conflicto de puertos.

Si el despliegue solo tiene un WACS o si no puede acceder a la CMC mediante ningún WACS, use una utilidad como netstat para determinar si otra aplicación ha ocupado un puerto de WACS.

### 13.1.11.4.1 Para resolver conflictos de puerto HTTP

1. Inicie el Administrador de configuración central (CCM) y haga clic en el icono *Administrar servidores* .
2. Especifique las credenciales de inicio de sesión.
3. En la pantalla *Administrar servidores*, detenga el WACS.
4. Haga clic en el icono *Configuración del nivel Web* .

   > **Nota**
   >
   > El icono *Configuración del nivel Web* solo está activado cuando se selecciona un WACS que está detenido.

   Aparece la pantalla *Configuración del nivel Web*.
5. En el campo *Puerto HTTP* especifique un puerto HTTP libre que utilizará el servidor de contenedor de aplicación Web y haga clic en *Aceptar*.
6. En la pantalla *Administrar servidores*, inicie el WACS.

### 13.1.11.4.2 Para resolver conflictos de puerto HTTP mediante proxy o HTTPS

Si no puede acceder a un WACS mediante los puertos HTTP a través de HTTP o HTTPS, pero se puede seguir conectando a la Consola de administración central (CMC) mediante el puerto HTTP, cambie los números de puerto a través de la CMC.

1. Vaya al área de administración *Servidores* de CMC.
2. Para detener el WACS que desea configurar, haga clic con el botón derecho y haga clic en *Detener servidor*.
3. Haga doble clic en el WACS que desea configurar.
   Aparecerá la pantalla *Propiedades*.
4. En la sección *Configuración de HTTP mediante proxy* especifique un nuevo puerto HTTP.
5. Para cambiar el puerto HTTPS, en la sección *Configuración de HTTPS*, escriba un nuevo valor en el campo *Puerto HTTPS*.
6. Haga clic en *Guardar y cerrar*.
7. Para iniciar el WACS, haga clic con el botón derecho en el servidor y haga clic en *Iniciar servidor*.

## 13.1.11.5 Para cambiar la configuración de memoria

Para mejorar el rendimiento de un WACS, puede cambiar la cantidad de memoria que se asigna al servidor mediante el Administrador de configuración central (CCM).

1. Inicie el CCM y haga clic en el icono *Administrar servidores*.
2. Especifique las credenciales de inicio de sesión para la CMC.
3. En la pantalla *Administrar servidores*, detenga el WACS.
4. Haga clic en el icono *Configuración del nivel Web* .

   > **Nota**
   >
   > El icono *Configuración del nivel Web* solo está activado cuando se selecciona un WACS que está detenido.

   Aparece la pantalla *Configuración del nivel Web*.
5. En *Parámetros de línea de comandos*, especifique un nuevo valor de memoria editando la línea de comandos:
   a. Busque la opción `-Xmx`. Esta opción normalmente tiene un valor especificado.

      Por ejemplo, «-Xmx1g». Esta configuración asigna un gigabyte de memoria al servidor.
   b. Especifique un nuevo valor para el parámetro.
      - Para especificar un valor en megabytes, use «m». Por ejemplo, «**`-Xmx640m`**» asigna 640 megabytes de memoria a WACS.
      - Para especificar un valor en gigabytes, use «g». Por ejemplo, «**`-Xmx2g`**» asigna dos gigabytes de memoria a WACS.
   c. Haga clic en *Aceptar*.
6. En la pantalla *Administrar servidores*, inicie el WACS.

## 13.1.11.6 Para cambiar el números de solicitudes simultáneas

El número predeterminado de solicitudes HTTP simultáneas para las que WACS está configurado para atender es 150. Debe resultar aceptable para la mayoría de los escenarios de despliegue. Para mejorar el rendimiento de WACS, puede aumentar el número máximo de solicitudes HTTP simultáneas. Aunque el aumento de las solicitudes simultáneas puede mejorar el rendimiento, si se configura este valor demasiado alto se puede perjudicar al rendimiento. La configuración ideal depende de los requisitos de hardware, software y TI.

1. Vaya al área de administración *Servidores* de CMC.
2. Para detener el WACS que desea configurar, haga clic con el botón derecho y haga clic en *Detener servidor*.
3. Haga doble clic en el WACS que desea configurar.
   Aparecerá la pantalla *Propiedades*.
4. En la opción *Configuración de simultaneidad (por conector)*, del campo *Cantidad máxima de solicitudes simultáneas*, escriba el número de solicitudes simultáneas que desee y haga clic en *Guardar y cerrar*.
5. Para iniciar el WACS, haga clic con el botón derecho en el servidor y haga clic en *Iniciar servidor*.

### 13.1.11.7 Para restaurar los valores predeterminados del sistema

Si ha configurado incorrectamente un WACS, puede restaurar los valores predeterminados del sistema mediante el Administrador de configuración central (CCM).

1. Inicie el CCM y haga clic en el icono *Administrar servidores* .
2. Especifique las credenciales de inicio de sesión.
3. En la pantalla *Administrar servidores*, detenga el WACS.
4. Haga clic en el icono *Configuración del nivel Web* .

   > **Nota**
   >
   > El icono *Configuración del nivel Web* solo está habilitado al seleccionar un WACS que está detenido.

   Aparece la pantalla *Configuración del nivel Web*.
5. Haga clic en *Restaurar valores predeterminados del sistema*.
6. Si es necesario, especifique un puerto HTTP libre y haga clic en *Aceptar*.
7. En la pantalla *Administrar servidores*, inicie el WACS.

### 13.1.11.8 Para evitar que los usuarios se conecten al WACS a través de HTTP

En determinados casos, puede desear permitir solo a determinados usuarios del equipo local que se conecten a WACS a través de HTTP o HTTPS. Por ejemplo, aunque no puede cerrar el puerto HTTP, puede desear configurar WACS de modo que solo acepte solicitudes HTTP de clientes que se encuentren en el mismo equipo que WACS. De esta forma, puede realizar tareas de mantenimiento o configuración en el WACS a través de un explorador desde el mismo equipo que el WACS, a la vez que impide que otros usuarios accedan al servidor.

1. Vaya al área de administración *Servidores* de CMC.
2. Haga doble clic en el WACS que desea modificar.
   Aparecerá la pantalla *Propiedades*.
3. En la sección *Servicio de contenedor de aplicaciones Web*, anule la selección de la casilla de verificación *Enlazar a todas las direcciones IP*.
4. En el campo *Enlazar a nombre de host o dirección IP*, escriba `127.0.0.1` y haga clic en *Guardar y cerrar*.
5. Para iniciar el WACS, haga clic con el botón derecho en el servidor y haga clic en *Iniciar servidor*.
   El WACS que se configura de esta forma solo acepta conexiones del equipo local.

## 13.1.12 Propiedades de WACS

Para obtener una lista completa de las propiedades de configuración generales, HTTP, HTTP mediante proxy y HTTPS que se pueden configurar para el WACS, consulte la sección «Configuración de servidor principal» del «Apéndice de propiedades de servidor» se puede encontrar una lista de las propiedades de CMS.

## Información relacionada

Propiedades de servicios principales [página 1165]

# 14 Copia de seguridad y restauración del sistema

## 14.1 Presentación general de la copia de seguridad y de la restauración

En este capítulo se explica cómo realizar la copia de seguridad de la plataforma de BI y cómo recuperar el sistema frente a un fallo de hardware, de software o a la pérdida de datos. La ejecución de un plan de copia de seguridad y restauración debe realizarla un administrador de SAP BusinessObjects Professional, un administrador del sistema y un administrador de base de datos con experiencia.

### Información relacionada

Copia de seguridad de todo el sistema [página 562]
Copia de seguridad de contenido de BI [página 568]
Realizar una copia de seguridad de la configuración del servidor con el CCM en Windows [página 566]
Realizar la copia de seguridad de la configuración del servidor en UNIX [página 567]
Información general de la copia del sistema [página 583]

## 14.2 Terminología

| Término | Definición |
|---|---|
| Réplica de datos | La réplica de datos es el proceso de crear una o más copias de los datos. Las copias se actualizan en tiempo real; por ejemplo, al usar unidades sincronizadas. Ofrece protección de datos a tiempo real contra los daños físicos de los datos pero debido a que los controladores se actualizan constantemente, no es posible invertir el sistema a un estado anterior si los datos se dañan o se eliminan accidentalmente. |
| Versiones | La creación de versiones proporciona varias versiones de un archivo o archivos concretos del sistema. En este caso, es posible devolver el sistema a un estado anterior.<br><br>Todas las versiones de los datos se suelen almacenar en el mismo sistema host. Si se pone en peligro o se daña este sistema, se corre el riesgo de perder la versión actual y las versiones antiguas. Asimismo, las funciones de recuperación conservan copias de los archivos "eliminados" para recuperarlos más adelante. Sin embargo, estas copias también se suelen almacenar en el mismo sistema host que los datos originales. No ofrece protección contra los daños físicos de los datos (por ejemplo, fallos del disco). |

| Término | Definición |
| --- | --- |
| copia de seguridad del sistema directamente sobre el hardware | Una copia de seguridad del sistema directamente sobre el hardware es una copia de seguridad de un sistema de archivos entero, incluyendo el sistema operativo. Una copia de seguridad del sistema directamente sobre el hardware se utiliza para restaurar un sistema del que se ha realizado una copia de seguridad del hardware que no contiene ni software ni sistema operativo.<br><br>Para copias de seguridad del sistema directamente sobre el hardware, en caso de error, el sistema entero del archivo (incluyendo OS) se restaura al hardware idéntico, o, si restaura herramientas de soporte de hardware independiente, restaure a cualquier hardware. |
| Copia de seguridad del sistema directamente sobre el hardware contra copia de seguridad de aplicación | Una copia de seguridad del sistema directamente sobre el hardware crea una copia de todo el sistema, incluyendo el sistema operativo. Una copia de seguridad directamente sobre el hardware permite volver a una versión anterior del sistema entero.<br><br>Una copia de seguridad de aplicación realiza copias de seguridad de archivos relacionados con aplicaciones individuales.<br><br>La plataforma de BI admite copias de seguridad del sistema directamente sobre el hardware, pero no copias de seguridad de aplicación.<br><br>Para copias de seguridad del sistema directamente sobre el hardware, en caso de error, el sistema entero del archivo (incluyendo OS) se restaura al hardware idéntico, o, si restaura herramientas de soporte de hardware independiente, restaure a cualquier hardware.<br><br>Una copia de seguridad completa del sistema de la plataforma de BI se llama conjunto de copia de seguridad. |
| Conjunto de copias de seguridad | Un conjunto de copias de seguridad comprende estas copias de seguridad individuales, creadas al mismo tiempo:<br>• Una copia de seguridad de la base de datos del sistema del CMS.<br>• Realizar una copia de seguridad directamente sobre el hardware de todo el sistema de archivos, incluyendo el sistema operativo, de todos los equipos en el despliegue de la plataforma de BI.<br>• Una copia de seguridad de los almacenes de archivos de los FRS de entrada y los FRS de salida (si no se incluye en el sistema de archivos de la plataforma de BI)<br>• Una copia de seguridad de los componentes de nivel Web (si no se incluyen como parte del sistema de archivos de la plataforma de BI).<br>• Una copia de seguridad de la base de datos de auditoría. |
| Copia de seguridad activa contra copia de seguridad inactiva | Una copia de seguridad en frío se realiza mientras el sistema está detenido o no está disponible para los usuarios. Las copias de seguridad activas se realizan mientras el sistema se ejecuta y está disponible para los usuarios, y los datos se pueden modificar durante el proceso de copia de seguridad. Además, al llevar a cabo una copia de seguridad activa, debe realizar los pasos de la copia de seguridad en orden; este no es el caso de la copia de seguridad inactiva.<br><br>La plataforma de BI admite copias de seguridad activas e inactivas.<br><br>A menudo, la copia de seguridad activa se denomina «copia de seguridad en línea». |

## 14.3 Usa mayúsculas o minúsculas para realizar copias de seguridad y restauraciones

La tabla siguiente describe los objetivos que pueda que desee conseguir según los recursos que tenga, y le dirige la solución de copia de seguridad más apropiada.

| Objetivo | Recursos necesarios | Solución |
|---|---|---|
| Objetivo: restaurar un sistema<br>1. Mi sistema de la plataforma de BI está dañado. Por lo tanto, necesito restaurarlo al estado de funcionamiento en que estaba la última vez que se realizó la copia de seguridad.<br>2. Un equipo que almacena la plataforma de BI está dañado. Debo sustituirlo por un equipo nuevo. | • Sistema de destino con el mismo hardware que el sistema de origen<br>Y<br>• Copias de seguridad del sistema de origen | Use la copia de seguridad del sistema y restaure el flujo de trabajo descrito en este manual. Consulte el Copia de seguridad de todo el sistema [página 562] procedimiento. Vuelva a crear el sistema de destino a partir de las copias de seguridad del sistema de origen. |
| Objetivo: restaurar objetos<br>Deseo recuperar un documento u otro objeto que ha sido eliminado accidentalmente. | • Copias de seguridad de los archivos y bases de datos del sistema de origen<br>Y<br>• Información de sistema detallada descrita en Exportar de un sistema de origen [página 588] | Mediante la utilización de copias de seguridad, cree una copia del sistema en otro equipo, y mediante la utilización del flujo de trabajo de copia de sistema en el capítulo «Copiar el despliegue de la plataforma de BI». A continuación, utilice las herramientas de administración de promoción para promover los objetos eliminados accidentalmente desde el sistema nuevo. Consulte el flujo de trabajo de Copia del sistema, comenzando por Planificación de la copia del sistema [página 584], y siga las instrucciones para el resto del capítulo.<br>**Nota**<br>Puede crear el sistema de destino en un equipo con un despliegue existente de la plataforma de BI de la misma versión, paquete de soporte técnico y nivel de revisión, o en un equipo "limpio" que no tenga instalada ninguna plataforma de BI. |
| Objetivo: restaurar objetos 2<br>Deseo recuperar un documento u otro objeto que ha sido eliminado accidentalmente. | Sistema en el que se usa la versión de administración de promociones | Utilice la aplicación Administración de promociones para recuperar una versión anterior del documento. Para obtener más detalles, consulte el |

| Objetivo | Recursos necesarios | Solución |
| --- | --- | --- |
| | | tema relacionado en administración de promociones. |

> ⓘ Nota
>
> **Realizar una copia de seguridad del sistema antes y después de un upgrade de software:**
>
> CMS se asocia con la "versión" de un producto. No puede utilizar el sistema de la plataforma de SAP BusinessObjectsBusiness Intelligence con CMS y FRS de versiones diferentes. Siempre tiene que realizar una copia de seguridad del almacenamiento de archivos CMS y FRS antes y después de cualquier upgrade de software. Si "restaura" a rollback un upgrade de software, tiene que asegurarse de que CMS, FRS y el software pertenezcan todos a la misma versión.

## Información relacionada

Copias de seguridad [página 561]
Planificación de la copia del sistema [página 584]
Resumen [página 595]

# 14.4 Copias de seguridad

Un plan de copia de seguridad y recuperación consiste en los pasos que se deben tomar en previsión de un fallo del sistema debido a un desastre natural o un fallo inesperado. El plan pretende minimizar los efectos del desastre en las operaciones diarias, de modo que pueda conservar o resumir rápidamente funciones importantes.

Al realizar la copia de seguridad del despliegue de la plataforma de BI, dispone de tres opciones:

- Realizar la copia de seguridad de todo el sistema, lo que permite restaurar el sistema completo. En este caso, restaurar solo una parte del sistema no es posible. Si desea volver a construir la plataforma de BI en lugar de restaurarla desde una copia de seguridad, consulte el tema relacionado que describe la copia de sistemas.
- Realizar la copia de seguridad de la configuración del servidor, lo que permite restaurar solo la configuración del servidor sin tener que restaurar otros objetos y conservar el estado actual del contenido de BI del sistema.
- Realizar la copia de seguridad del contenido de BI (por ejemplo, documentos), lo que permite restaurar de forma selectiva partes del contenido de BI sin necesidad de restaurar todos los objetos.

Consulte los temas relacionados para obtener más información sobre los tres tipos de copias de seguridad.

> → Sugerencias
>
> Para evitar la pérdida de datos, realice copias de seguridad de forma regular.

→ Sugerencias

Puede realizar una copia de seguridad de un sistema de la plataforma de BI y, a continuación, restaurarlo en un equipo host igual o distinto para crear una copia del sistema.

### Información relacionada

Copia de seguridad de todo el sistema [página 562]
Copia de seguridad de la configuración del servidor [página 565]
Copia de seguridad de contenido de BI [página 568]
Información general de la copia del sistema [página 583]

## 14.4.1 Copia de seguridad de todo el sistema

Realice una copia de seguridad de todo el sistema de la plataforma de BI llevando a cabo una copia de seguridad activa o inactiva, lo que crea un conjunto de copias de seguridad. Conservar varios conjuntos de copia de seguridad de distintas horas ofrece más opciones al restaurar el sistema. Realice una copia de seguridad de su sistema con la frecuencia que requieren las necesidades empresariales de su organización.

Puede seleccionar detener el sistema de la plataforma de BI y realizar una copia de seguridad fría, o puede seleccionar realizar una copia de seguridad reciente. Con una copia de seguridad reciente, el sistema continúa funcionando y disponible durante el proceso de copia de seguridad. Esto tiene la ventaja de no tener tiempo de inactividad en el sistema.

ⓘ Nota

Se recomienda escribir el registro de transacciones en un sistema de archivos distinto al sistema del servidor de base de datos principal, realizar la copia de seguridad regularmente de este registro de transacciones y guardarla con el resto de archivos en el conjunto de copia de seguridad.

ⓘ Nota

Si realiza la copia de seguridad de los datos de auditoría, asegúrese de incluir el registro de transacciones de la base de datos para la base de datos de auditoría con el conjunto de archivos de copia de seguridad. No tiene que incluir los archivos temporales de auditoría con la copia de seguridad.

### 14.4.1.1 Copias de seguridad activa

La función de copia de seguridad activa permite realizar la copia de seguridad del sistema de la plataforma de BI mientras se permite a los usuarios usar el sistema de forma normal. Si su negocio debe continuar en funcionamiento mientras su sistema está realizando la copia de seguridad, active y configure copias de seguridad activas en la consola de administración central.

La configuración de la *Duración máxima de la copia de seguridad activa* especifica el número máximo de horas que tardará la copia de seguridad: desde el momento en que se inicia la copia de seguridad de CMS hasta que finaliza la copia de seguridad de FRS. Si la duración que especifica es demasiado corta, es posible que los archivos se eliminen antes de que la copia de seguridad haya tenido tiempo de copiarlos. Para evitarlo, es más seguro estimar al alza el tiempo necesario. Valore este aspecto en relación con los recursos del sistema porque un valor elevado puede aumentar ligeramente el tamaño de almacenamiento del archivo del FRS.

> **Nota**
>
> - La copia de seguridad activa no realiza realmente una copia de seguridad, solo retrasa el borrado de archivos. Cuando se tratan o actualizan los archivos, se mantienen varias copias. Esto significa que CMS y FRS siempre guardan la relación correcta, permitiendo que la copia de seguridad de cada uno se realice en momentos diferentes. Sin embargo, esto sucede en la ventana de copia de seguridad activa.
> - Cuando restaura el sistema, termina con muchos archivos extra en el FRS, que la Herramienta de diagnóstico del repository debe borrar.
> - Inicie siempre la copia de seguridad de CMS antes de hacer la copia de seguridad del repositorio de archivos FSR.
>
> La copia de seguridad activa está activada mientras la casilla de verificación *Activar copia de seguridad activa* está seleccionada en la CMC; la configuración *Duración máxima de la copia de seguridad activa* no afecta si está o no activada la copia de seguridad.

Es más sencillo restaurar el sistema a una hora de copia de seguridad específica. Por ejemplo, si las copias de seguridad del sistema se realizan a diario a las 3:00, puede restaurar el sistema fácilmente al estado en que estaba cuando se inició la copia de seguridad del sistema del CMS (a las 3:00 de la fecha de su elección). Después de un error de la base de datos CMS o de la base de datos de auditoría, si ha habilitado el registro de transacciones en la base de datos CMS o en la base de datos de auditoría, puede restaurar el sistema al estado en que se encontraba justo antes del error.

Para maximizar la seguridad, guarde los registros de transacción en una ubicación que no sea la misma que la de los registros de copia de seguridad de las bases de datos principal. Esto asegura que, en este caso de error en la base de datos, pueda restablecer la base de datos en el estado en que estaba antes del error.

> **Nota**
>
> Debido a una limitación del tamaño del archivo de transacciones en versiones anteriores de IBM DB2, las tareas relacionadas con el registro de transacciones y las copias de seguridad activas solo se admiten si la base de datos del sistema CMS está alojada en el servidor de bases de datos DB2 versión 9.5 Fix Pack 5 o posterior (para la línea 9.5) y 9.7 Fix Pack 1 o posterior (para la línea 9.7).

> **Nota**
>
> Se recomienda escribir el registro de transacciones en un sistema de archivos distinto al sistema del servidor de base de datos principal, realizar la copia de seguridad de este registro de transacciones regularmente y guardarla con otros archivos en el conjunto de copia de seguridad.

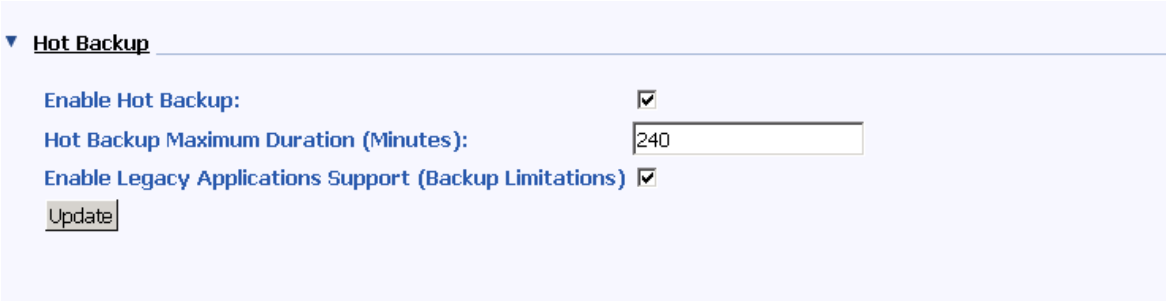
### 14.4.1.1.1 Para habilitar las copias de seguridad activas

1. Abra la Consola de administración central (CMC).
2. Desde el área *Gestión* abra la página *Opciones*.
3. En la sección *Copia de seguridad activa*, seleccione *Activar copia de seguridad activa*.
4. En el apartado *Duración máxima de la copia de seguridad activa (minutos)*, introduzca el número máximo de minutos que espera que suponga la copia de seguridad.

   Asegúrese de incluir la hora necesaria para realizar la copia de seguridad de la base de datos del CMS y del sistema de archivos del equipo anfitrión de la plataforma de BI.

   > **Nota**
   >
   > Si la duración real de la copia de seguridad es superior al límite indicado aquí, podrían producirse incoherencias en los datos copiados. Para evitarlo, es más seguro estimar al alza el tiempo necesario.

5. Haga clic en *Actualizar*.
   La copia de seguridad activa está habilitada.




Cuando esté habilitada la compatibilidad con la copia de seguridad activa, se pueden realizar copias de seguridad con las herramientas de copia de seguridad del proveedor de bases de datos y sistema de archivos.

### 14.4.1.2 Para realizar la copia de seguridad activa o inactiva de un sistema

Si desea llevar a cabo una copia de seguridad activa, consulte primero el tema relacionado sobre copias de seguridad activas para obtener más información sobre ello y los requisitos previos. Si realiza una copia de seguridad fría, detenga todos los nodos del despliegue de la plataforma de BI.

> **Precaución**
>
> Si realiza una copia de seguridad sin habilitar la copia de seguridad activa y sin detener todos los nodos, puede que resulten inconsistencias de datos entre la base de datos del CMS y el almacenamiento de archivos FRS.

> **Nota**
>
> Para copias de seguridad activas, es importante que los procedimientos se inicien en la secuencia descrita. Para copias de seguridad inactivas, los procedimientos se pueden llevar a cabo en cualquier orden. En

cualquier caso, no es necesario esperar que cada paso de la copia de seguridad haya terminado antes de iniciar el siguiente paso.

1. Use las herramientas del proveedor de base de datos para realizar la copia de seguridad de la base de datos del sistema del Servidor de administración central (CMS).

   > **Nota**
   >
   > Para realizar copias de seguridad activas, use las herramientas de copia de seguridad del proveedor de la base de datos en el modo atómico en línea.

2. Use las herramientas del proveedor de base de datos en el modo atómico en línea para realizar la copia de seguridad de la base de datos de auditoría de la plataforma de BI.
3. Realizar una copia de seguridad de todo el sistema de archivos, incluyendo el sistema operativo, de todos los equipos en el despliegue de la plataforma de BI. Para los equipos Unix, haga una copia de seguridad del directorio de instalación y del de inicio de la cuenta de instalación.
   a. Si los almacenes de archivos FRS de entrada y salida no se incluyen en la copia de seguridad de la plataforma de BI (equipos host independientes), cree una copia de seguridad de ambos mediante sus propias herramientas de copia de seguridad de archivos.
   b. Si los componentes de nivel Web no se incluyen en la copia de seguridad de la plataforma de BI (equipos host independientes), cree una copia de seguridad mediante sus propias herramientas de copia de seguridad de archivos.

   Para las copias de seguridad activas, use las herramientas de copia se seguridad de archivos atómicos, si es posible.

Si realiza una copia de seguridad en frío, espere a que finalicen todas las copias de seguridad y a continuación inicie los nodos de la plataforma de BI.

### Información relacionada

Copias de seguridad activa [página 562]

## 14.4.2 Copia de seguridad de la configuración del servidor

A fin de proteger el sistema de los valores del servidor mal configurados, realice regularmente copias de seguridad de la configuración del servidor en un archivo BIAR. Si dispone de copias de seguridad de los servidores podrá restaurar la configuración sin tener que restaurar el contenido de la base de datos del sistema del Servidor de administración central (CMS), de los repositorios de archivos o de Business Intelligence.

Es vital realizar copias de seguridad de la configuración del servidor siempre que realice cambios en el despliegue del sistema. Esto incluye crear, renombrar, mover y eliminar nodos, y crear o eliminar servidores. Es aconsejable realizar copias de seguridad de la configuración del servidor antes de cambiar los valores y, después, de nuevo, una vez que esté seguro de los cambios realizados.

> **Nota**
>
> Hacer una copia de seguridad de la configuración del servidor no es una tarea adicional a la copia de seguridad de CMS y del repositorio de archivos FRS, por ejemplo una restauración de CMS/FSR, si no que

también restaura la configuración del servidor. La configuración del servidor es un subconjunto pequeño de una copia de seguridad completa de la base de datos CMS. No necesita restaurar la configuración del servidor si ya ha restaurado el CMS.

Use el Administrador de configuración central (CCM) o una secuencia de comandos para realizar la copia de seguridad de la configuración del servidor de la plataforma de BI en un archivo BIAR y, a continuación, almacene el archivo en un equipo independiente o un medio de almacenamiento.

> **Nota**
>
> Si está realizando la copia de seguridad o restaurando la configuración del servidor en un despliegue en el que está habilitado SSL, primero debe deshabilitar SSL a través del CCM y, a continuación, volver a habilitarlo al finalizar la copia de seguridad o la restauración.

En Windows, la secuencia de comandos `BackupCluster.bat` se encuentra en el directorio `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

En Unix, la secuencia de comandos `backupcluster.sh` se encuentra en el directorio `/<DIRINSTAL>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

## 14.4.2.1 Realizar una copia de seguridad de la configuración del servidor con el CCM en Windows

Este procedimiento realiza una copia de seguridad de la configuración del servidor para todo un clúster. No es posible realizar copias de seguridad de la configuración de servidores individuales.

> **Nota**
>
> Si usa un CMS temporal, debe usar el CCM en un equipo que tenga instalados binarios del CMS local.

1. Inicie el CCM y en la barra de herramientas, haga clic en *Copia de seguridad de configuración del servidor*. Aparece el *Asistente para copia de seguridad de la configuración del servidor*.
2. Haga clic en el botón *Siguiente* para iniciar el asistente.
3. Especifique si usar un CMS existente para realizar la copia de seguridad de la configuración de servidor o para crear un CMS temporal.
   - Para realizar la copia de seguridad de la configuración del servidor, seleccione *Usar un CMS en funcionamiento* y haga clic en *Siguiente*.
   - Para realizar la copia de seguridad de la configuración del servidor desde un sistema que no funciona, seleccione *Iniciar un nuevo CMS temporal* y haga clic en *Siguiente*.
4. Si va a usar un CMS temporal, seleccione un número de puerto para el CMS y especifique la información de conexión de la base de datos.

   Para minimizar el riesgo de usuarios que acceden al sistema mientras está realizando la restauración del sistema, especifique un número de puerto distinto de los números de puerto que usan los CMS existentes.
5. Introduzca la clave de clúster y haga clic en *Siguiente* para continuar.
6. Cuando se le solicite, inicie la sesión en el CMS especificando el nombre de sistema y usuario y la contraseña de una cuenta con privilegios administrativos y haga clic en *Siguiente* para continuar.

7. Especifique la ubicación y el nombre de un archivo BIAR en el que desee realizar la copia de seguridad de la configuración del servidor y haga clic en *Siguiente* para continuar.
   En la pantalla de *confirmación* se muestra la información que ha proporcionado.
8. Compruebe que la información que se muestra en la pantalla de *confirmación* sea correcta y haga clic en *Finalizar* para continuar.
   El CCM realiza una copia de seguridad de la configuración del servidor para todo el clúster en el archivo BIAR que especifique. En un archivo de registro, se graban los detalles del procedimiento de copia de seguridad. El nombre y la ruta del archivo del registro se muestran en un cuadro de diálogo.
9. Si la operación de copia de seguridad falla, compruebe el archivo de registro para determinar el motivo.
10. Haga clic en *Aceptar* para cerrar el asistente.

### 14.4.2.2 Realizar la copia de seguridad de la configuración del servidor en UNIX

En equipos de UNIX, use la secuencia de comandos `serverconfig.sh` para realizar la copia de seguridad de la configuración de servidor del despliegue a un archivo BIAR.

1. Seleccione *5 - Copia de seguridad de la configuración de servidor* y pulse `Intro`

```
-----------------------------------------------------------

           SAP BusinessObjects

What do you want to do?

1 - Add node
2 - Delete node
3 - Modify node
4 - Move node
5 - Back up server configuration
6 - Restore server configuration
7 - Modify web tier configuration
8 - List all nodes


[quit(0)]
-----------------------------------------------------------

[8]5
```

2. Especifique si usar un CMS existente para realizar la copia de seguridad de la configuración de servidor o para crear un CMS temporal.
   - Para realizar la copia de seguridad de la configuración de servidor desde un sistema que se está ejecutando, seleccione *existente* y pulse `Intro`
   - Para realizar la copia de seguridad de la configuración de servidor desde un sistema que no se está ejecutando, o para restaurar la configuración de servidor, seleccione *temporal* y pulse `Intro`.
3. Si está usando un CMS temporal para realizar la copia de seguridad de la configuración de servidor, en las siguientes pantallas seleccione un número de puerto para que se ejecute el CMS temporal y la información de conexión de la base de datos del sistema del CMS.

Para minimizar el riesgo de usuarios que acceden al sistema mientras está realizando la restauración del sistema, especifique un número de puerto distinto de los números de puerto que usan los CMS existentes.

4. Cuando se solicite, inicie la sesión en el CMS especificando el nombre del sistema y de usuario y la contraseña de una cuenta con privilegios administrativos, y pulse `Intro`.
5. Cuando se solicite, especifique la ubicación y el nombre del archivo BIAR en el que desea realizar la copia de seguridad de la configuración de sistema y pulse `Intro`.
   Una pantalla de resumen muestra la información que ha proporcionado.
6. Verifique que la información que se muestra en la pantalla es correcta y pulse `Intro` para continuar.
   La secuencia de comandos `serverconfig.sh` realiza la copia de seguridad de los ajustes de configuración de servidor de todo el clúster al archivo BIAR que especifique. En un archivo de registro, se graban los detalles del procedimiento de copia de seguridad. El nombre y la ruta del archivo del registro se muestran en un diálogo.
7. Si la operación de copia de seguridad falla, compruebe el archivo de registro para determinar el motivo.

### 14.4.2.3 Realización de la copia de seguridad de la configuración de servidores con una secuencia de comandos

Puede realizar la copia de seguridad de la configuración de servidor del despliegue ejecutando la secuencia de comandos `BackupCluster.bat` en Windows o la secuencia de comandos `backupcluster.sh` en Unix.

En Windows, el archivo `BackupCluster.bat` se encuentra en el directorio `<DIRINSTAL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

En Unix, `backupcluster.sh` se encuentra en el directorio `/<DIRINSTAL>/sap_bobj/enterprise_xi40/<plataforma64>/scripts`.

#### Información relacionada

Secuencias de comandos BackupCluster y RestoreCluster [página 579]

## 14.4.3 Copia de seguridad de contenido de BI

Se recomienda que utilice las herramientas y los procedimientos de copia de seguridad estándar de la base de datos y archivos para hacer una copia de seguridad regularmente:

- La base de datos del CMS.
- Los almacenes de archivos FRS de entrada y FRS de salida.

Tener copias de seguridad actuales del contenido hace posible la restauración de Business Intelligence sin tener que restaurar todo el sistema o la configuración del servidor.

Para obtener más información sobre la copia de seguridad de su sistema, consulte Para realizar la copia de seguridad activa o inactiva de un sistema [página 564].

## 14.5 Restaurar el sistema

Si el sistema se ha visto dañado, puede restaurarlo todo, de forma que se restaura la plataforma de BI. Dependiendo de la condición del sistema, se posible que no sea necesaria una restauración completa. Si el sistema funciona de forma normal pero ha perdido contenido o está dañado, puede seleccionar restaurar solo el contenido de Business Intelligence (BI). Si el contenido de BI es válido pero los servidores de la plataforma se han desconfigurado, puede restaurar solo la configuración del servidor.

El procedimiento es el mismo para restaurar desde una copia de seguridad fría o caliente.

### Información relacionada

Restauración de todo el sistema [página 569]
Restauración de la configuración del servidor [página 576]
Restauración del contenido de BI [página 579]

## 14.5.1 Restauración de todo el sistema

Al restaurar todo el sistema, también se restaura el clúster de la plataforma de Business Intelligence. Dependiendo de lo que haya fallado en el sistema, todavía podría tener la opción de realizar una restauración parcial.

Si falla o se pierde uno de los componentes siguientes, debe restaurar todo el sistema:

- Base de datos del CMS

  > **Nota**
  >
  > Si se bloquea el servicio de base de datos, simplemente puede reiniciar el servicio sin restaurar todo el sistema.

- El almacén de archivos FRS
- Sistema de archivos del equipo

> **Nota**
>
> Para una restauración completa del sistema, el sistema de destino no requiere que la plataforma de BI esté instalada.

Si solo se ha dañado o perdido la base de datos de auditoría, puede restaurar la base de datos de auditoría, sin restaurar todo el sistema.

Si se daña o se pierde el contenido de nivel Web, puede restaurar el contenido de nivel Web, sin restaurar todo el sistema.

## Información relacionada

Restaurar todo el sistema [página 570]
Para restaurar solo la base de datos de auditoría [página 572]
Restaurar el contenido de nivel Web [página 572]
Restaurar solo la base de datos del CMS [página 573]

# 14.5.1.1 Restaurar todo el sistema

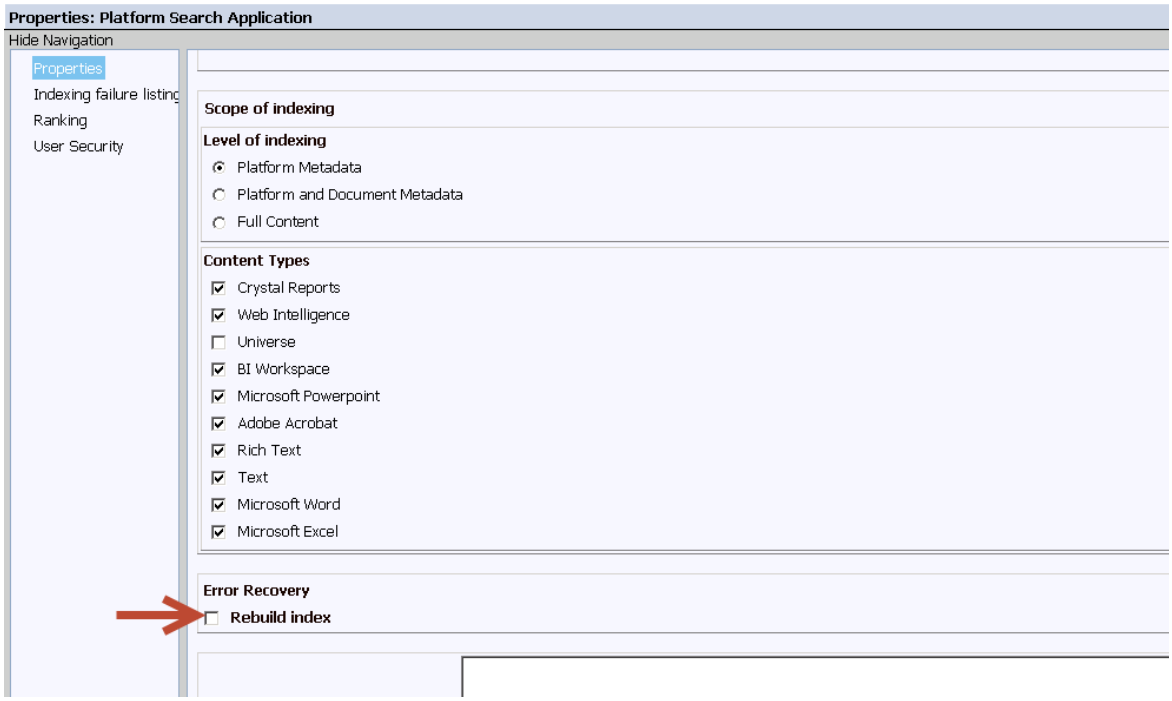
Antes de restaurar el sistema, debe usar el Administrador de configuración central (CCM) para detener todos los nodos del despliegue de la plataforma de BI y debe seleccionar el momento al que desea restaurar el sistema.

> **Nota**
>
> Si desea restaurar el sistema a su estado actual, haga la copia de seguridad del sistema antes de restaurarlo.

1. Localice los siguientes archivos de copia de seguridad:
   - Copia de seguridad de la base de datos del CMS
   - Copias de seguridad del almacén de archivos FRS de entrada y de salida
   - Copias de seguridad de los sistemas de archivos de cada equipo del host del clúster de la plataforma de BI

   > **Nota**
   >
   > - Asegúrese de validar las copias de seguridad y asegúrese de que todos los archivos enumerados anteriormente son del mismo conjunto de copia de seguridad.
   > - Cuando realice la copia de seguridad y la restauración, CMS y FRS se tratan como una sola unidad. Si restaura uno de ellos, tiene que restaurar el otro al mismo tiempo.
   > - Si la copia de seguridad establecida se obtuvo como una copia de seguridad activa, asegúrese de que la fecha y la hora de inicio de la copia de seguridad de la base de datos del CMS es anterior a la fecha y hora del almacenamiento de archivos FRS coincidentes, nivel Web, y sistema de archivos en el equipo host. Se necesitarán todos estos archivos, incluso si solo un componente falla.
2. Use las herramientas de restauración de archivos para restaurar el sistema de archivos de todos los equipos host del clúster de la plataforma de BI.
3. Use las herramientas de restauración de archivos para restaurar los almacenes de archivos FRS de entrada y de salida.
4. Use las herramientas de base de datos para restaurar la base de datos del CMS.
5. Si ha cambiado la contraseña de la base de datos del CMS desde que se creó la copia de seguridad, use el CCM para actualizar la contraseña de la base de datos del CMS en todos los nodos y equipos host de la plataforma de BI.
6. Si utiliza la propiedad Auditoría, utilice las herramientas de base de datos para restaurar la base de datos Auditoría.

7. Seleccione una de las siguientes opciones para restaurar los índices de búsqueda:
   - Si desea ejecutar la secuencia de comandos de recuperación de índices de búsqueda, consulte Ejecutar la secuencia de comandos de recuperación de índices de búsqueda [página 575] y siga las instrucciones. Esto le proporcionará un índice completo de forma más rápida.
   - Si desea volver a elaborar el índice de búsqueda en lugar de usar la secuencia de comandos de recuperación, use el CCM para reiniciar los nodos de la plataforma de BI. Se trata de un procedimiento más sencillo pero, mientras se vuelve a elaborar el índice, tendrá acceso de búsqueda parcial a los datos de la plataforma.




8. Inicie el sistema, y anote el tiempo que tarda al llevar a cabo los pasos de los requisitos posteriores.
9. Verifique que el sistema funciona tal y como se espera, y realice una prueba de integridad.

Una vez verificado el sistema, lleva a cabo las siguientes acciones:

- Ejecute la Herramienta de diagnóstico del repositorio para eliminar los archivos temporales que no se usan y compruebe la coherencia del repositorio. Consulte la sección Herramienta de diagnóstico de repositorio de este manual.
- Si no usó la secuencia de comandos de recuperación de índices, vuelva a elaborar el índice de búsqueda de la plataforma.
- Las tareas de publicación que estén en curso en el momento de realizar la copia de seguridad del sistema se mostrarán como con errores. No vuelva a ejecutar estas instancias; inicie nuevas tareas de publicación.
- Si la base de datos de auditoría está comprometida, debe ejecutar una consulta SQL para eliminar los eventos que pasen entre el error de base de datos y la hora del reinicio (la hora que anotó en el paso 8). Por ejemplo: `delete from [DB_NAME].ADS_EVENT where Start_Time > '<[time of DB failure]>' and Start_Time < '<[time of DB restoration]>'`

### Información relacionada

Indexación de contenido en el repositorio CMS [página 953]

## 14.5.1.2 Para restaurar solo la base de datos de auditoría

Antes de restaurar la base de datos de auditoría, use el Administrador de configuración central (CCM) para detener todos los nodos del despliegue de la plataforma de BI. También deberá decidir en qué punto desea restaurar la base de datos.

> **Nota**
>
> Realice esta tarea únicamente si está seguro de que la base de datos de auditoría es el único componente afectado de la plataforma de BI. Si hay otros componentes afectados, debe realizar una restauración del sistema completa.

Use las herramientas de base de datos para restaurar la base de datos Auditoría.

### Información relacionada

Restaurar todo el sistema [página 570]

## 14.5.1.3 Restaurar el contenido de nivel Web

Antes de restaurar el contenido de nivel Web, debe detener todos los nodos del despliegue de la plataforma de BI mediante el Administrador de configuración central (CCM). También deberá decidir a qué momento desea restaurar el contenido de nivel Web.

Si desea tener la opción de volver al estado actual del sistema, debe realizar una copia de seguridad del sistema antes de la restauración.

Si el nivel Web está dañado, se puede restaurar de forma individual.

1. Use las herramientas de restauración de archivos para restaurar las carpetas de nivel Web en el equipo host de nivel Web.
2. Use el CCM para reiniciar todos los nodos del despliegue de la plataforma de BI.

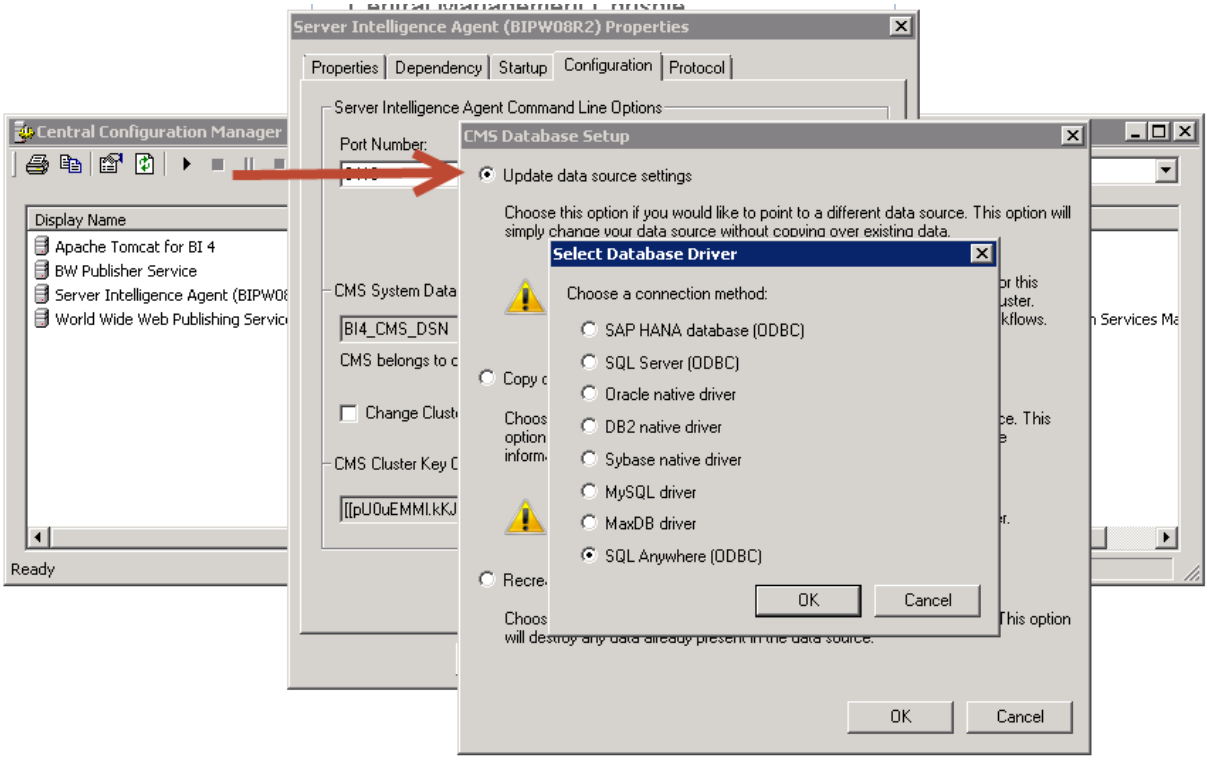
## 14.5.1.4 Restaurar solo la base de datos del CMS

> **Nota**
>
> Si se bloquea el servicio de base de datos, simplemente puede reiniciar el servicio sin restaurar todo el sistema. Si la base de datos está dañada o existen otros componentes comprometidos, debe realizar una restauración completa del sistema.

Repare o sustituya el equipo host de la base de datos del CMS. Si se sustituye, asegúrese de que tiene el mismo nombre del sistema que el equipo host anterior, así como la misma configuración de puerto y credenciales de base de datos.

> **Nota**
>
> Si no es posible restaurar el equipo con el mismo nombre y credenciales, deberá usar el CCM para actualizar esta información de conexión a base de datos para cada nodo del clúster y reiniciar dichos nodos.

Para Windows:




Para UNIX: Ejecute cmsdbsetup.sh, introduzca el nombre del nodo cuando se le pida y luego seleccione la opción 6 `update`.

```
-----------------------------------------------------------

           SAP BusinessObjects


Current CMS Data Source: BI4_CMS_DSN_1381344842

Current cluster name: LRHEL57x64:6400

Current cluster key: [[pU0uEMM1.kKJPezTK002bw]]


update (Update Data Source Settings)
reinitialize (Recreate the current data surce)
copy (Copy data from another Data Source)
change cluster (Change current cluster name)
change cluster key (Change current cluster key)


[update(6)/reinitialize(5)/copy(4)/change cluster(3)/change cluster key(2)/back(1)/quit(0)]
-----------------------------------------------------------

[update]6
```

1. Detenga todos los nodos de la plataforma de BI mediante el CCM.
2. Use las herramientas de base de datos para restaurar la base de datos Auditoría.
3. Use el CCM para iniciar los nodos de la plataforma de BI.

Una vez que se ha comprobado que el sistema funciona correctamente, lleve a cabo las siguientes acciones:

- Ejecute la Herramienta de diagnóstico del repositorio para eliminar los archivos temporales que no se usan y compruebe la coherencia del repositorio. Consulte la sección Herramienta de diagnóstico de repositorio de este manual.
- Las tareas de publicación que estén en curso en el momento de realizar la copia de seguridad del sistema se mostrarán como con errores. No vuelva a ejecutar estas instancias; inicie nuevas tareas de publicación.

### Información relacionada

Indexación de contenido en el repositorio CMS [página 953]

## 14.5.1.5 La recuperación del índice de búsqueda

La función de búsqueda de plataforma conserva una serie de índices y archivos de información en el sistema para que pueda buscar de forma más eficaz. Si es necesario restaurar el sistema, estos archivos de información pueden desarrollar incoherencias. Puede reparar estas incoherencias mediante la secuencia de comandos de recuperación de índice o al volver a elaborar el índice.

Volver a crear el índice es un procedimiento sencillo pero el proceso consumirá bastantes recursos y tardará algún tiempo en finalizar, las búsquedas que se lleven a cabo durante la creación solo devolverán resultados para las porciones indexadas de la base de datos. La recuperación del archivo de comandos implica un procedimiento más complicado pero proporcionará un índice de trabajo completo de forma más rápida.

Si restaura un despliegue con varios equipos, ejecute el archivo de comandos en los equipos que alojen el servicio de búsqueda. Para el primer equipo de un clúster, use la opción `-Both` y, a continuación, en todos los equipos posteriores de dicho clúster que usen la opción `-ContentStore`.

### Información relacionada

Indexación de contenido en el repositorio CMS [página 953]

## 14.5.1.5.1 Ejecutar la secuencia de comandos de recuperación de índices de búsqueda

- Confirme que el CMS se está ejecutando y detenga todos los servidores de procesamiento de Adaptive (APS) que tengan instalado el servicio de búsqueda.

  > **Nota**
  >
  > Debe detener estos APS lo antes posible después de que el nodo se inicie.

- Configure `JAVA_HOME` en la ubicación `sapjvm/bin` del directorio de instalación de la Plataforma de BI.
- Se puede acceder al directorio de datos Búsqueda de plataformas desde el equipo en el que se ejecuta el archivo de comandos.

1. En el equipo host del CMS o del APS, abra una ventana de línea de comandos (si se usa el sistema operativo Windows).
2. Cambie al siguiente directorio `<DIRINSTAL>\SAP BuinsessObjects Enterprise XI 4.0\java\lib\`.

   En los equipos Unix, use la ruta de archivos Unix equivalente.
3. Escriba `java -jar platformSearchOnlineHotbackupRestore.jar` y pulse *Intro*.
4. Cuando se le solicite, introduzca la siguiente información y pulse *Intro*:
   - Su ubicación de instalación de la Plataforma de BI (por ejemplo, `<INSTALLDIR>/SAP businessObjects Enterprise XI 4.0`)
   - Las credenciales de inicio de sesión del CMS, incluidos el nombre, el ID de usuario y la contraseña, y el tipo de autenticación. El tipo de autenticación dispone de las siguientes opciones:
     - `secEnterprise`
     - `secLDAP`
     - `secWinAD`
     - `secSAPR3`
5. Cuando se le solicite el tipo de restauración de índices, escriba una de las siguientes opciones y pulse *Intro*.

| Valor | Descripción |
| --- | --- |
| `-Both` | Se debe usar para los despliegues de servidores únicos o, en despliegues en varios equipos, para el primer equipo host del APS con el servicio de búsqueda:<br><br>En un sistema con APS de búsqueda múltiples, la primera vez que se ejecuta la secuencia de comandos, use el valor `-Both` (actualiza la base de datos y el almacén de contenidos). Al ejecutar una secuencia de comandos para las demás APS de búsqueda, use el valor `-ContentStore` (solo actualiza el almacén de contenidos). |
| `-ContentStore` | Se debe usar al ejecutar el archivo de comandos en equipos host del APS con el servicio de búsqueda instalado, a menos que se trate del primer equipo del clúster en el que se ejecuta el archivo de comandos. |
| `-Exit` | Salir de la secuencia de comandos sin realizar una restauración del índice. |

6. Cuando la secuencia de comandos ha terminado de ejecutarse, cierre la ventana de línea de comandos (para los equipos Windows).

Iniciar todos los APS detenidos.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\java\lib>java  -jar platformsearchOnlineHotbackupRestore.jar
Enter the BOE install location :
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0

Enter the CMS Credentials:
CMS NAME: BIPW08R2
USER NAME: Administrator
PASSWORD:
AUTHENTICATION: secEnterprise
BOE Install Location = C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessOb
jects Enterprise XI 4.0 CMS = BIPW08R2  User = Administrator    Authentication =
 secEnterprise

Please verify if the details given above are correct(y/n)...Press 'e' if you wan
t to exit  :y
 What would you like to restore?
 1. Index ?
 2. Content Store ?
 3. Both Index and Content Store (Choose this option only when index and content
 store are present on one node) ?
 4. Exit ?
3
```

## 14.5.2 Restauración de la configuración del servidor

Si tiene que restaurar la configuración del servidor del sistema a partir del archivo BIAR, puede usar el Administrador de configuración central (CCM) o la secuencia de comandos RestoreCluster. Restaurar el contenido del servidor a partir de un archivo BIAR no afecta al contenido de Business Intelligence, como la configuración de informes, usuarios y grupos, o seguridad.

> **Nota**
>
> Al restaurar la configuración del servidor, solo se admite la restauración de la configuración para todo un clúster. No se puede restaurar la configuración de solo algunos de los servidores del clúster.

> **Nota**
>
> Si está realizando la copia de seguridad o restaurando la configuración del servidor en un despliegue en el que está habilitado SSL, primero debe deshabilitar SSL a través del CCM y, a continuación, volver a habilitarlo al finalizar la copia de seguridad o la restauración.

### 14.5.2.1 Para restaurar la configuración del servidor con el CCM en Windows:

Puede usar el Administrador de configuración central (CCM) para restaurar la configuración del servidor. Tras restaurar la configuración del servidor, debe recrear los nodos del sistema en cada equipo del clúster del sistema.

1. Detenga todos los nodos de todos los equipos del clúster para el que esté restaurando la configuración del servidor mediante la detención del Agente de inteligencia de servidor para cada nodo.
2. Inicie el administrador de configuración central (CCM) en un equipo que disponga de un CMS.
3. Desde la barra de herramientas, haga clic en *Restaurar configuración del servidor*.
   Aparece el *Asistente para restaurar la configuración del servidor*.
4. Haga clic en el botón *Siguiente* para iniciar el asistente.
5. Cuando se le solicite, proporcione el número de puerto del Servidor de administración central (CMS) temporal que se va a usar y la información para conectar la base de datos del sistema CMS, y haga clic en *Siguiente* para continuar.
6. Introduzca la clave de clúster y haga clic en *Siguiente* para continuar.
7. Cuando se le solicite, introduzca el nombre del CMS y el nombre de usuario, así como la contraseña de una cuenta con privilegios administrativos para iniciar la sesión en el CMS y haga clic en *Siguiente* para continuar.
8. Especifique la ubicación y el nombre del archivo BIAR que contiene la configuración del servidor que desea restaurar, y haga clic en *Siguiente* para continuar.
   Una página de resumen muestra el contenido del archivo BIAR.
9. Haga clic en *Siguiente* para continuar.
   Una página de resumen muestra la información que ha introducido.
10. Haga clic en *Finalizar* para continuar.
    Un mensaje de advertencia indica que la configuración del servidor existente se sobrescribirá con los valores del archivo BIAR y, si continúa, la configuración actual del servidor se perderá.
11. Haga clic en *Sí* para restaurar la configuración del servidor.

    El CCM restaura la configuración del servidor para todo el clúster a partir del archivo BIAR. En un archivo de registro, se graban los detalles de la restauración. El nombre y la ruta del archivo del registro aparecen en un cuadro de diálogo.
12. Si la operación de restauración falla, compruebe el archivo de registro para determinar el motivo.
13. Haga clic en *Aceptar* para cerrar el asistente.

La configuración del servidor a partir del archivo BIAR se restaura en el sistema. Se crean los nodos y servidores existentes en el archivo BIAR que no existían en el sistema antes de la restauración.

> **Nota**
>
> Los nodos y servidores que había en el sistema, pero que no estaban en el archivo BIAR, se eliminan del repositorio. Los nodos y servidores seguirán apareciendo en el CCM, pero puede eliminar manualmente los archivos `dbinfo` y `bootstrap` para un nodo.

Debe volver a crear los nodos en el sistema en cada equipo del clúster.

### Información relacionada

Uso de nodos [página 474]

## 14.5.2.2 Restaurar parametrizaciones del servidor en UNIX

En equipos Unix, use la secuencia de comandos `serverconfig.sh` para restaurar la configuración del servidor del despliegue desde un archivo BIAR.

1. Seleccione *6: Restaurar la configuración del servidor* y pulse `Intro`.

```
-----------------------------------------------------------

           SAP BusinessObjects

What do you want to do?

1 - Add node
2 - Delete node
3 - Modify node
4 - Move node
5 - Back up server configuration
6 - Restore server configuration
7 - Modify web tier configuration
8 - List all nodes


[quit(0)]
-----------------------------------------------------------

[8]6
```

2. Introduzca un número de puerto para que lo use el Servidor de administración central (CMS) temporal y pulse `Intro`.
3. En las siguientes pantallas, especifique la información de conexión a la base de datos del sistema del CMS.
4. Cuando se solicite, inicie la sesión en el CMS especificando el nombre del sistema y de usuario y la contraseña de una cuenta con privilegios administrativos, y pulse `Intro`.
5. Cuando se solicite, especifique la ubicación y el nombre del archivo BIAR desde el que desea restaurar los ajustes de configuración del servidor y pulse `Intro`.

Una pantalla de resumen muestra la información que ha proporcionado.

6. Verifique que la información que se muestra en la pantalla es correcta y pulse *Intro* para continuar.
   La secuencia de comandos `serverconfig.sh` restaura los ajustes de configuración del servidor de todo el clúster desde el archivo BIAR que se especificó. Los detalles del procedimiento de restauración se escriben en un archivo de registro. El nombre y la ruta del archivo de registro se muestran en la pantalla.
7. Si la operación de restauración falla, compruebe el archivo de registro para determinar el motivo.

### 14.5.2.3 Restaurar la configuración del servidor con una secuencia de comandos

Si lo prefiere, puede restaurar la configuración del servidor del despliegue ejecutando la secuencia de comandos `RestoreCluster.bat` en Windows, o la secuencia de comandos `restorecluster.sh` en Unix.

En Windows, `RestoreCluster.bat` se encuentran en el directorio `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

En Unix, `restorecluster.sh` se encuentra en el directorio `/<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts`.

#### Información relacionada

Secuencias de comandos BackupCluster y RestoreCluster [página 579]

### 14.5.3 Restauración del contenido de BI

Si ha realizado una copia de seguridad del contenido de Business Intelligence (BI) en archivos LCMBIAR, puede usar la Herramienta de administración de promociones para restaurar el contenido de BI, sin necesidad de restaurar el sistema completo. Para obtener más información, consulte el capítulo «Administración de promociones».

## 14.6 Secuencias de comandos BackupCluster y RestoreCluster

En la siguiente tabla se describen los parámetros de línea de comandos que se usan con la secuencia de comandos `BackupCluster`.

> **Nota**
>
> Esta secuencia de comandos solo realiza la copia de seguridad de la configuración de un clúster. La copia de seguridad del resto de los datos se debe realizar por separado.

Parámetros BackupCluster

| Nombre | Descripción | Ejemplo |
|---|---|---|
| `-backup` | El nombre y la ruta del archivo BIAR del que desea realizar la copia de seguridad de la configuración del servidor del sistema para la restauración. | `-backup "C:\Users\Administrator\Desktop\my.biar"` |
| `-cms` | El nombre de host del equipo en el que se ubica el Servidor de administración central del sistema. Si el CMS se ejecuta en cualquier otro puerto que no sea el puerto predeterminado, 6400, también debe especificar el número de puerto. | `-cms mycms:6400` |
| `-username` | El nombre de usuario de una cuenta de administrador. | `-username Administrador` |
| `-password` | La contraseña de una cuenta de administrador. | `-password Password1` |

En la siguiente tabla se describen los parámetros de línea de comandos que se usan con la secuencia de comandos `RestoreCluster`.

Parámetros RestoreCluster

| Nombre | Descripción | Ejemplo |
|---|---|---|
| `-restore` | El nombre y la ruta del archivo BIAR que contiene los ajustes de configuración del servidor que desea restaurar. | `-restore "C:\Users\Administrator\Desktop\my.biar"` |
| `-username` | El nombre de usuario de una cuenta de administrador. | `-username Administrador` |
| `-password` | La contraseña de una cuenta de administrador. | `-password Password1` |
| `-displaycontents` | Muestra una lista de nodos y servidores que contiene el archivo BIAR. | `-displaycontents "C:\Users\Administrator\Desktop\my.biar"` |

> **Nota**
>
> Ejecute la secuencia de comandos `RestoreCluster` con el parámetro `-displaycontents` para mostrar los contenidos del archivo BIAR antes de restaurar la configuración del servidor.

Los siguientes parámetros son necesarios si realiza la copia de seguridad de la configuración del servidor desde un sistema que no se está ejecutando o si está restaurando la configuración del servidor.

Parámetros que se usan al usar un CMS temporal

| Nombre | Descripción | Ejemplo |
|---|---|---|
| `-usetempcms` | Crea un CMS temporal para la operación especificada. Después de finalizar la operación, se detiene el CMS temporal. | `-usetempcms` |

| Nombre | Descripción | Ejemplo |
| --- | --- | --- |
| `-cmsport` | El número de puerto del CMS temporal. | **`-cmsport 6700`** |
| `-dbdriver` | El controlador de base de datos de la base de datos de sistema de CMS. Los valores aceptados son:<br>• **`db2databasesubsystem`**<br>• **`maxdbdatabasesubsystem`**<br>• **`mysqldatabasesubsystem`**<br>• **`oracledatabasesubsystem`**<br>• **`sqlserverdatabasesubsystem`**<br>• **`sybasedatabasesubsystem`**<br>• **`sqlanywheredatabasesubsystem`**<br>• **`newdbdatabasesubsystem`**<br>**Nota**<br>El parámetro **`newdbdatabasesubsystem`** se usa con las bases de datos de SAP HANA. | **`-dbdriver sqlserverdatabasesubsystem`** |
| `-connect` | La cadena de conexión de la base de datos del sistema de CMS. | **`-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"`** |
| `-dbkey` | La clave del clúster. | **`-dbkey abc1234`** |

## Ejemplo

En el siguiente ejemplo se muestra cómo realizar la copia de seguridad de la configuración del servidor a un archivo BIAR con un CMS existente.

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

## Ejemplo

En el siguiente ejemplo se muestra cómo mostrar los contenidos de un archivo BIAR.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

## Ejemplo

En el siguiente ejemplo se muestra cómo restaurar la configuración desde un archivo BIAR. Siempre debe usar un CMS temporal al restaurar la configuración del servidor.

```
-restore "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
-usetempcms
-cmsport 6400
-dbdriver sqlserverdatabasesubsystem
-connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
```

# 15 Copia de su despliegue de la plataforma de BI

## 15.1 Información general de la copia del sistema

En este capítulo se describe cómo crear un duplicado del despliegue de la plataforma de BI para finalidades de prueba, standby y otras.

Para obtener más información, consulte 1275068.

### Información relacionada

Presentación general de la copia de seguridad y de la restauración [página 558]

## 15.2 Terminología

| Término | Definición |
|---|---|
| Sistema de origen | Despliegue de la plataforma de BI original. |
| Sistema de destino | El nuevo despliegue que desea crear. |
| Copia de sistema | El acto de crear un duplicado de un despliegue de la plataforma de BI. |
| Copia de sistema heterogéneo | El acto de crear un sistema duplicado en el que los sistemas de origen y destino tienen el mismo tipo de sistema operativo y base de datos. La plataforma de BI admite solo copias de sistema homogéneas. |
| Copia de sistema heterogéneo | El acto de crear un sistema duplicado en el que los sistemas de origen y destino usan diferentes tipos de sistema operativo o base de datos pero están basados en los mismos datos. |
| Copia de base de datos | El acto de crear un duplicado del sistema de CMS o de la base de datos de auditoría con las herramientas de proveedor de base de datos. |

## 15.3 Usa casos para la copia de sistemas

La tabla siguiente describe los objetivos que pueda que desee conseguir según los recursos que tenga, y le dirige a la solución más apropiada.

| Objetivo | Recursos necesarios | Solución |
|---|---|---|
| Objetivo: copia idéntica<br><br>Deseo crear un sistema duplicado para espera o pruebas con una configuración de hardware y direcciones IP/nombres de equipo idénticos | • Un sistema de destino con el mismo hardware que el sistema de origen y<br>• Copias de seguridad del sistema de origen o acceso al sistema de origen desde el que realizar una copia de seguridad. | Use la copia de seguridad del sistema y restaure el flujo de trabajo descrito en este manual. Consulte el Copia de seguridad de todo el sistema [página 562] procedimiento. Vuelva a crear el sistema de destino a partir de las copias de seguridad del sistema de origen. |
| Objetivo: Copiar<br><br>Deseo crear un sistema duplicado para esperar, probar, o formar que tiene distinto hardware y direcciones IP/nombre de equipo del sistema de origen. | • Sistema de origen (en funcionamiento o detenido) O copias de seguridad de bases de datos y archivos de sistema de origen, e<br>• Información detallada del sistema descrita en Exportar de un sistema de origen [página 588] | Use el flujo de trabajo de Copia del sistema, comenzando por Planificación de la copia del sistema [página 584], y siga las instrucciones para el resto del capítulo.<br><br>**Nota**<br>Puede crear el sistema de destino en un equipo con un despliegue existente de la plataforma de BI de la misma versión, paquete de soporte técnico y nivel de revisión, o en un equipo limpio que no tenga instalada ninguna plataforma de BI. |

### Información relacionada

Copias de seguridad [página 561]
Planificación de la copia del sistema [página 584]

## 15.4 Planificación de la copia del sistema

Copia de sistema que no se refleja en el sistema actual. Puede crear una copia del sistema y esperar un poco antes de continuar con la recreación de la copia en el sistema de destino, o puede usar una copia de seguridad anterior del sistema de origen como base para el sistema de origen. Esto significará que la copia será del sistema tal como se encontraba en el momento en el que se creó la copia. Por ejemplo, si espera un mes, la copia recreará el sistema tal como era hace un mes.

Después de revisar los casos de uso de la sección anterior y de decidir cuál de ellos se adapta mejor a sus necesidades, debería desarrollar un plan de copia del sistema.

## Crear un plan de copia del sistema

Al programar la copia de un sistema, debe decidir por adelantado los siguientes detalles:

- ¿Se detendrá el sistema o permanecerá activo mientras se lleva a cabo la copia? (El procedimiento se puede llevar a cabo en ciertas circunstancias.)
  - Si el sistema de origen se detiene, ¿cuánto tiempo tendrá que estar inactivo?
  - Planifique el tiempo para la realización de pruebas para garantizar la integridad del sistema de destino
- Qué herramientas de base de datos desea usar para la copia de seguridad y la restauración de la base de datos.
- En qué equipos se implementará el sistema de destino y dónde se alojará cada nodo.
- Qué componentes opcionales desea copiar.
- Copiará el tipo de base de datos que vaya a utilizar para la base de datos CMS de destino y cualquier otra base de datos opcional.

También deberá prestar atención a los siguientes temas:

- Los componentes de la plataforma de BI que tiene instalado el sistema de origen. Puede utilizar la función *Agregar/Eliminar* > *Modificar* del programa de instalación para ver la lista de los componentes instalados en ese momento.
- Si el sistema de destino está instalado en una configuración de hardware distinta al sistema de origen, es probable que tenga que ajustar el sistema de destino para un mejor rendimiento. Consulte la información sobre cómo mejorar el rendimiento del sistema en el *SAP BusinessObjects Business Intelligence sizing companion guide* (Manual adicional sobre tamaños de SAP BusinessObjects Business Intelligence).
- Es probable que desee que el sistema de origen genere informes desde bases de datos de generación de informes y no desde las bases de datos del sistema de origen. En este caso tendrá que modificar la información de conexión de base de datos para las bases de datos de generación de informes. Puede hacer esto mientras conserva el mismo nombre de DSN pero señala a un DSN en el sistema de destino para otra base de datos.

## Componentes de sistema de origen necesarios

- Base de datos del sistema de CMS
- Almacén de archivos FRS
- Los archivos de configuración de la capa semántica.
- Base de datos de auditoría (opcional)
- Base de datos de supervisión (opcional)
- Base de datos de subversión de administración de promoción (opcional)

## 15.5 Consideraciones y limitaciones

Debería tener en cuenta las observaciones siguientes cuando haga una copia de su despliegue de la plataforma de BI.

| Área | Consideración |
|---|---|
| Integraciones de SAP Business Warehouse | Si usa una plataforma de BI y SAP ERP o BW en un entorno integrado, antes de copiar su sistema, lea la documentación de copia del sistema de SAP. Las guías de copia del sistema están disponibles en http://www.sdn.sap.com/irj/sdn/systemcopy (se requiere inicio de sesión de SMP). Elija su versión de SAP NetWeaver. Las guías correspondientes a su copia se encuentran en la carpeta de guías de instalación. |
| Versión del programa | Los sistemas de origen y de destino deben estar en el mismo nivel de versión, paquete de soporte y revisión. |
| Ajustes de contenido y configuración | Solo se puede copiar el sistema de origen completo. Usted no puede copiar el contenido o los valores de configuración del sistema de forma selectiva. |
| Ruta de instalación | Las rutas de instalación en las ubicaciones de origen y destino tienen que ser idénticas: por ejemplo, si usted ha instalado el sistema de origen en `C:\SAP BusinessObjects Enterprise XI 4.0`, tiene que instalar el destino en `C:\SAP BusinessObjects Enterprise XI 4.0`. |
| Sistema operativo host | Los sistemas operativos de origen y de destino deben ser iguales. |
| Tipo de software de base de datos CMS | Las bases de datos de origen y de destino del CMS deben ser del mismo tipo. Tendrá la opción de cambiar a otro tipo de base de datos admitido después de copiar el sistema. |
| Tipo de software de base de datos de auditoría | Si está copiando datos de auditoría, las bases de datos de origen y de destino de auditoría deben ser del mismo tipo. Después de crear la copia, puede establecer una base de datos nueva de otro tipo distinto.<br>**Nota**<br>Si establece una nueva base de datos, los eventos existentes no se copiarán a esa base de datos, solo los nuevos eventos se guardarán en la base de datos nueva. |
| Personalización de Nivel Web | El procedimiento de copia no copiará los componentes de Nivel Web del sistema de origen. Si ha personalizado el nivel Web (modificando archivos `.properties` en la carpeta `personalizar`, por ejemplo), debe aplicar manualmente las características personalizadas a la carpeta de destino. |

| Área | Consideración |
| --- | --- |
| Temas no incluidos en estas instrucciones | Este flujo de trabajo no describe cómo exportar o importar una base de datos. Use las herramientas de su proveedor de base de datos para copiar y recuperar bases de datos. |

Se copiarán los siguientes datos durante el procedimiento de copia del sistema:

- La base de datos del repositorio del CMS. (contiene informes, analíticas, carpetas, derechos, usuarios y grupos de usuarios, configuración de servidores, y otros contenidos de BI y contenidos del sistema)
- La base de datos de auditoría. (contiene eventos de auditoría desencadenados por servicios de plataforma de BI o aplicaciones cliente)
- La base de datos de supervisión. (contiene datos de tendencias de métricas, métricas, y vigilancias)
- La base de datos de administración de versiones. (contiene diferentes versiones de informes, analíticas, otros recursos de BI, e información de versión)

> **Nota**
>
> Para obtener una descripción de las bases de datos y sus contenidos, vea la sección Bases de datos [página 38] de esta guía.

- Los archivos de configuración de la capa semántica.

No se copian la configuración del nivel Web, del índice de búsqueda, y cualquiera de los datos no mencionados específicamente más arriba.

### Consideraciones sobre las copias de recuperación de archivos

Si está copiando un sistema con el propósito concreto de recuperar un archivo que se eliminó accidentalmente, debería tener en cuenta las siguientes observaciones:

Al usar la copia de seguridad, realice los pasos del procedimiento Importar a un sistema de destino [página 592] del sistema de producción.

- No instale todos los nodos, instale solo el primer nodo que contendrá los CMS y su base de datos.
- No instale auditoría, administración de promociones o supervisión de base de datos.
- No recree conexiones a las bases de datos de auditoría o de generación de informes.

Use el LCM para promover el objeto que quiere recuperar desde el sistema de destino para el sistema de origen.

## 15.6 Procedimiento de copia del sistema

Los procedimientos siguientes le guían por las dos fases de la copia del despliegue de la plataforma de BI.

## 15.6.1 Exportar de un sistema de origen

También necesitará anotar los siguientes detalles acerca del sistema de origen. Si quiere copiar esta información, encontrará una hoja de cálculo que puede utilizar en Hoja de cálculo de copia del sistema [página 1238].

| Propiedad | Ubicación |
|---|---|
| La clave de clúster CMS (asegúrese de guardar bien el registro). | Creados por el administrador del sistema al instalar la plataforma de BI. |
| El nombre de los nodos. | Vaya a la ficha *Servidores* de CMC, y en el árbol izquierdo expanda *Nodos*. |
| El nombre del equipo y la carpeta de instalación de la plataforma de BI para cada equipo en el despliegue. | Vaya a la ficha *Servidores* de la CMC, haga clic con el botón derecho en el CMS y seleccione *Marcadores de posición*. Busque el valor del marcador de posición `%INSTALLROOTDIR%`. |
| La contraseña del administrador de la plataforma de BI (asegúrese de guardar bien el registro). | Creados por el administrador del sistema al instalar la plataforma de BI. |
| Todas las conexiones de base de datos que pueden ser utilizadas por el CMS, y los nombres de usuario y contraseñas asociados a esas conexiones. Esto puede incluir la auditoría de base de datos si quiere copiar esta información. Asegúrese de obtener esta información de todos los equipos del clúster.<br><br>**Nota**<br>Si va a copiar la base de datos de auditoría, necesitará también los nombres de conexión de la base de datos de auditoría y los credenciales. | Vaya a la ficha *Servidores* de la CMC, haga clic con el botón derecho en el CMS y seleccione *Métricas*.<br><br>Busque las métricas siguientes:<br>• *Nombre de conexión de la base de datos del sistema*<br>• *Nombre de servidor de base de datos del sistema*<br>• *Nombre de usuario de base de datos del sistema*<br>• *Nombre de origen de datos*<br>• *Nombre de la conexión de la base de datos de auditoría* (opcional)<br>• *Nombre de usuario de la base de datos de auditoría* (opcional) |
| De todos los equipos del clúster, los detalles (tipos de cliente, versiones) de cualquier otra conexión de base de datos (utilizada por universos y registros, por ejemplo). Asegúrese de que incluye nombres de usuario y contraseñas. | Para informes Crystal Reports que informan directamente desde bases de datos, consulte la información de conexión utilizando SAP Crystal Reports 2020 o el diseñador SAP Crystal Reports Enterprise. Para información sobre el universo de conexión, utilice la herramienta de diseño de información (.unx) o la herramienta de diseño de universo (.unv). |
| La versión, el paquete de soporte y la revisión del sistema de origen. | Desde Windows esto se puede determinar consultando la herramienta de *Eliminar o cambiar* programas.<br><br>En UNIX, puede utilizar la funcionalidad `modifyOrRemoveProducts.sh` en el directorio de instalación de la plataforma de BI. |

| Propiedad | Ubicación |
| --- | --- |
| Las ubicaciones de almacén de archivos para cada FRS de entrada y FRS de salida del despliegue. | Vaya a la ficha *Servidores* de la CMC, haga clic con el botón derecho en Input u Output FRS y seleccione *Propiedades*. Busque la propiedad de *Directorio de almacenamiento de archivos*.<br><br>**Nota**<br>Si el valor empieza por %, se trata de un marcador de posición, y deberá hacer clic en *Marcadores de posición* y tomar nota del directorio que se muestra bajo ese marcador de posición. |
| Si piensa copiar Gestión de promociones, la ubicación de la carpeta de la base de datos de Gestión de promociones y las carpetas de subversión. | La carpeta por defecto para la base de datos de administración de promociones en instalaciones de Windows es `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride` y en UNIX es `<INSTALLDIR>/sap_bobj/data/LCM/LCMOverride`.<br><br>Las ubicaciones por defecto para los ficheros de subversión en instalaciones de Windows son:<br>• `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut`<br>• `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository`<br><br>y en Unix son:<br>• `<INSTALLDIR>/check_out`(Este directorio solo se crea después de haber utilizado Subversión para desproteger ficheros.)<br>• `$HOME/LCM_Repository` |
| Si tiene pensado copiar la base de datos de supervisión, la carpeta de la base de datos de supervisión. | Esta está establecida en la consola de administración central (CMC). Vaya al área de gestión de *Aplicaciones* de la CMC, seleccione *Aplicación de supervisión* > *Propiedades* y consulte el *directorio de seguridad de la base de datos de tendencias*.<br><br>La carpeta predeterminada en las instalaciones de Windows es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB` y en Unix es `<DIRINSTALACIÓN>/sap_bobj/Data/TrendingDB`. |
| La ruta de la carpeta de capa semántica. | La ruta de carpeta predeterminada para las instalaciones en Windows es `<DIRINSTALACIÓN>\SAP` |

| Propiedad | Ubicación |
| --- | --- |
| | `BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\` de forma predeterminada. |

Después de que haya recuperado la información anterior:

1. Utilice las herramientas de su proveedor de base de datos para crear una copia de seguridad de las siguientes bases de datos:
   - Base de datos del sistema de CMS
   - Base de datos de auditoría (opcional)
2. Con las herramientas de seguridad de archivo, haga copias de seguridad de los siguientes conjuntos de archivos:
   - El almacenamiento de archivos de entrada y salida FRS.
   - La base de datos de supervisión (opcional). Esto se puede conseguir realizando una copia de seguridad de los archivos desde la carpeta de supervisión tal y como están registrados en la hoja de cálculo. De forma predeterminada, en Windows es: `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB` En Unix: `<DIRINSTALACIÓN>/sap_bobj/Data/TrendingDB`.
   - Base de datos de subversión de administración de promociones (opcional). Esto se puede conseguir realizando una copia de seguridad de los archivos desde la carpeta de subversión tal y como están registrados en la hoja de cálculo. De forma predeterminada, en Windows son:
     - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut`
     - `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository`.

     Y en Unix son:
     - `<INSTALLDIR>/check_out`(Este directorio solo se crea después de haber utilizado Subversión para desproteger ficheros.)
     - `$HOME/LCM_Repository`
   - Archivos de configuración de la carpeta de capa semántica: el archivo `cs.cfg` en la carpeta `connectionServer`, y cualquiera de los archivos `.sbo` y `.prm` de las subcarpetas.

   > **Nota**
   >
   > Para limitaciones y una descripción detallada de este flujo de trabajo, consulte la sección de Copias de seguridad activa [página 562].

3. Los archivos siguientes son personalizables por el usuario. Si ha personalizado alguno de ellos, realice una copia de seguridad de los archivos desde el sistema de origen, y después restáurelos en la misma carpeta del sistema de destino:
   - `BO_trace.ini` instalado en:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/conf`
   - `clientSDKOptions.xml` instalado para:
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
   - `CRConfig.xml` instalado en:

    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java`
  - `mdas.properties` instalado en:
    - `[INSTALLDIR]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services`
  - Los archivos de configuración WDeploy están instalados en `[DIRINSTAL]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf`:
    - `config.apache`
    - `config.jboss7`
    - `config.sapappsvr75`
    - `config.tomcat6`
    - `config.tomcat7`
    - `config.weblogic11`
    - `config.websphere7`
    - `config.websphere8`
    - `wdeploy.conf`
4. Los siguientes archivos de nivel Web son personalizables por el usuario. Si ha realizado modificaciones en cualquier archivo, realice una copia de seguridad de los archivos desde el sistema de origen. Más adelante, tendrá que restaurar estos archivos o volver a aplicar las modificaciones en el sistema de destino.
  - `BO_trace.ini`instalado para:
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog`
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf`
  - `clientaccesspolicy.xml` instalado en:
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
  - `clientSDKOptions.xml` instalado para:
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib`
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib`
  - `crossdomain.xml` instalado en:
    - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT`
    - `[INSTALLDIR]tomcat/webapps/ROOT`
  - Cualquier archivo personalizado en la carpeta `config/custom` (en el nivel Web). Realizar una copia de seguridad de los archivos de los que transferir la personalización al sistema de destino.
5. Realizar una copia de seguridad de extensiones personalizadas que ha agregado manualmente al sistema de origen; por ejemplo, extensiones de publicación, bibliotecas personalizadas, etc.

Guarde la información registrada más arriba con la copia de las bases de datos y los archivos. Puede que quiera guardar una segunda copia que podrá actualizar como sea necesario en procedimientos futuros de copia de sistema.

## 15.6.2 Importar a un sistema de destino

En este procedimiento se presupone que ha creado copias de seguridad de las bases de datos de despliegue de origen y de los archivos de sistema que desea usar en el sistema de destino. Todos los archivos de copias de seguridad deben proceder del mismo conjunto de copias de seguridad. También necesitará los detalles (clave de clúster y credenciales de la base de datos, por ejemplo) anotados en «Para efectuar una exportación de copia de seguridad desde el sistema de origen».

Si el sistema de destino residirá en una ubicación en red con acceso a los recursos del sistema de origen, deberá garantizar que el sistema de destino no intenta acceder a dichos recursos hasta que se haya configurado de nuevo. Esto se puede conseguir colocando un cortafuegos entre el sistema de destino y los recursos del sistema de origen, o dejando detenido el sistema de origen mientras inicia el sistema de destino. Una vez ha iniciado el sistema de destino por primera vez, se puede eliminar el cortafuegos o puede iniciar el sistema de origen.

Si el sistema de destino ya dispone de una plataforma de BI instalada, asegúrese de que la versión, el paquete de compatibilidad y el nivel de revisión coinciden con los del sistema de origen en el momento en que se creó la copia. Además, cerciórese de que usa la misma ruta de instalación que el sistema origen.

1. En el sistema de destino, cree las conexiones a la o las bases de datos donde intenta colocar el repositorio de CMS, la base de datos de auditoría y la base de datos de informes.

   > **Nota**
   >
   > Si bien las conexiones pueden apuntar a una base de datos distinta, deben tener el mismo nombre de conexión o DSN y usar las mismas credenciales que el sistema origen.

2. Use sus herramientas de la base de datos para restablecer la base de datos del sistema de CMS y la base de datos de auditoría (si es necesario) desde la copia de seguridad del sistema origen a la base de datos de destino.

   Si los universos o informes del sistema de destino tienen que usar una base de datos de informes diferente, modifique la conexión de la base de datos para que apunte a esta base de datos.

   Si necesita más instrucciones sobre este paso, consulte el tema Restaurar el sistema [página 569].

3. Si la plataforma BI está instalada en el sistema host objetivo, vaya directamente al Paso 4. Si la plataforma BI no está instalada, instálela en el sistema host objetivo teniendo en cuenta los siguientes pasos:
   a. Instale la misma versión del programa, el mismo paquete de compatibilidad y el mismo nivel de revisión del sistema origen.
   b. Use la misma ruta de instalación que en el sistema de origen.
   c. Seleccione los mismos componentes que se instalaron en el sistema de origen.
   d. Cuando el programa de instalación solicite crear la base de datos del CMS (y la base de datos de auditoría, si corresponde), seleccione la opción *Usar un servidor de base de datos existente* e introduzca el nombre y las credenciales de la conexión que se configuraron en el paso 1.

      > **Nota**
      >
      > No seleccione reinicializar la base de datos del CMS.

   e. Cuando se solicite para el *nombre de nodo*, use los mismos nombres, números de puerto, contraseña de administrador de plataforma y clave de clúster del sistema origen.

Para obtener las instrucciones de instalación completas, consulte el *Manual de instalación de la plataforma SAP BusinessObjects Business Intelligence*. Cuando el sistema se haya instalado completamente, vaya al paso 6.

> **Nota**
>
> Si no copia los datos de auditoría del sistema de origen, puede crear una nueva base de datos de auditoría configurando la auditoría durante el proceso de instalación.

f. Detenga todos los nodos del CCM.

4. Si la plataforma de BI ya está instalada en el sistema de destino, detenga todos los nodos del CCM. En el equipo host del CMS del sistema de destino, inicie el CCM.
5. Si la plataforma de BI ya está instalada, agregue un nodo nuevo mediante la opción *Volver a crear nodo*.
   a. Use el *nombre de nodo* y el *número de puerto del SIA* del sistema de origen.
   b. Seleccione *Iniciar un nuevo CMS temporal*.
   c. Seleccione un nuevo *Número de puerto del CMS* (puede ser cualquier puerto libre) y *Tipo de base de datos del CMS* (que coincida con el tipo de la base de datos restaurada).
   d. Introduzca los detalles para la conexión con la que se restauró la base de datos del CMS en el paso 1.
   e. Introduzca la clave de clúster desde el sistema de origen.
   f. Introduzca la contraseña del administrador desde el sistema de origen.
6. Restaure los almacenes de archivos FRS de entrada y salida en los almacenes de archivos del sistema de destino. Use la misma carpeta que usó en el sistema de origen.
7. Restaure la carpeta de base de datos de supervisión (si desea copiar información de supervisión) a la misma carpeta que se usó en el sistema de origen.
8. Recuperar la carpeta de base de datos de administración de promociones (si desea copiar información de administración de promociones) en la misma carpeta utilizada en el sistema fuente.
9. Recuperar los archivos de subversión (si desea copiar información de administración de promociones) en la misma carpeta utilizada en el sistema fuente.
10. Restaure los archivos del servidor de la capa semántica / configuración de conexión en la misma carpeta que se usó en el sistema de origen.
11. Reinicie los equipos host del sistema de destino
12. Si en el paso 3 ha instalado la plataforma de BI en el sistema de destino, aplique las revisiones o paquetes de compatibilidad necesarios para coincidir con el sistema origen.
13. Si el sistema de destino se ejecutará en varios equipos host, repita los pasos 1-11 para cada equipo host.

    Use la opción Instalación expandida cuando instale nodos adicionales de la plataforma de BI y tenga en cuenta que deben usarse los mismos nombres de nodo del sistema origen para los nodos adicionales en el sistema de destino.
14. Si la base de datos del CMS del sistema de destino usará un tipo de base de datos diferente desde el sistema de origen, use el CCM para ejecutar Copia de datos de una base de datos de sistema de CMS a otra [página 514] y especifique la base de datos que desea usar como destino para la copia.
15. Restaure los archivos personalizables de usuario de los que realizó una copia de seguridad en el paso 3 del procedimiento «Exportar desde un sistema de origen».
16. Restaure los archivos personalizables de usuario de los que realizó una copia de seguridad en el paso 4 del procedimiento «Exportar desde un sistema de origen».

    «Nivel Web» hace referencia al área de estado WDeploy en la que llevar a cabo las personalizaciones, y al contenido de nivel Web que se despliega en el servidor de aplicaciones.

Al aplicar modificaciones en el sistema de destino, no aplique modificaciones en el directorio del servidor de aplicaciones; aplíquelas al área de escalado WDeploy y, a continuación, vuelva a desplegar el nivel Web al servidor de aplicaciones usando WDeploy.

El área de escalado de WDeploy es esta ubicación en Windows: `<DIRINSTALACIÓN>/SAP BusinessObjects Enterprise XI 4.0/warfiles`.

17. Restaure los archivos personalizables de usuario de los que realizó una copia de seguridad en el paso 5 del procedimiento «Exportar desde un sistema de origen».

Cuando se haya efectuado la copia del sistema de la plataforma de BI:

1. La instalación del primer nodo del destino crea un CMS temporal que se detendrá cuando termine la instalación. Cuando use el CMC, vaya a la página Servidores y elimine este CMS.

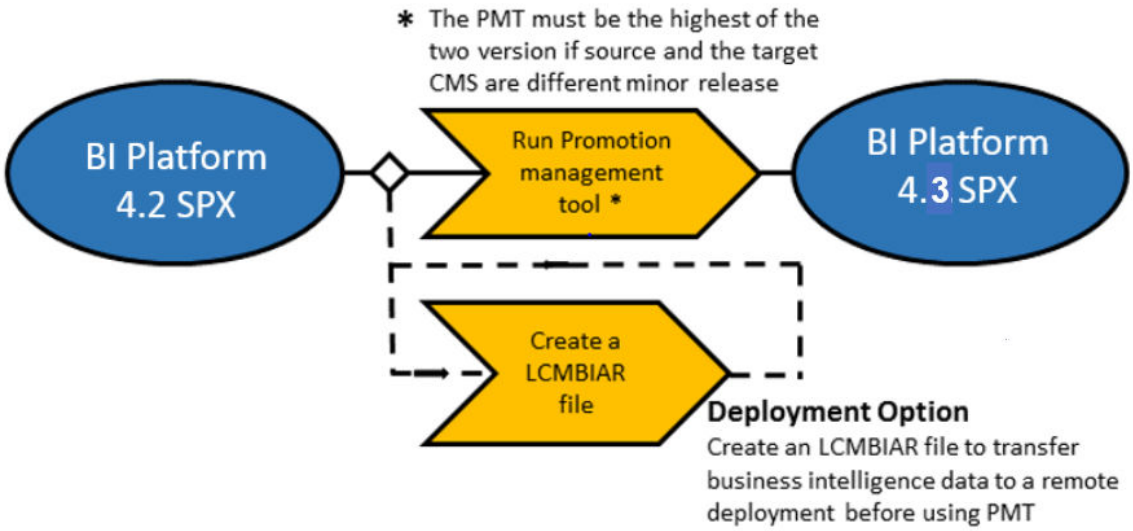
   > → Recuerde
   >
   > Si no elimina el sistema de origen (o si lo usa al mismo tiempo que el sistema de destino), es recomendable cambiar el nombre del clúster del sistema de destino.

2. Ejecute la herramienta de diagnóstico del repositorio en la base de datos del CMS de destino.
3. En caso necesario, configure el inicio de sesión único (SSO) de Windows AD en el sistema de destino. Consulte SSO a la plataforma de BI con autenticación de AD [página 319].
4. En caso necesario, configure SLD en el sistema de destino. Para obtener más detalles, consulte la nota SAP 1508421: «Proveedor de datos SAP SLD para Apache Tomcat».
5. Realice una comprobación de integridad en el sistema de destino para garantizar su integridad.
6. Efectúe una reindexación de la búsqueda completa.

# 16 Administración de promociones

## 16.1 Bienvenido a la administración de promociones

### 16.1.1 Resumen




La herramienta de administración de promociones le permite:

- Mover o transportar los recursos de Business Intelligence (BI) de un repositorio a otro.
- Gestionar dependencias de los recursos.
- Deshacer los recursos promocionados en el sistema de destino, si es necesario.

Además, la herramienta de administración de promociones permite la administración de versión del mismo recurso de BI.

La herramienta de administración de promociones se integra con la Consola de administración central. Puede promocionar un recurso de Business Intelligence desde un sistema a otro solo si está instalada la misma versión de la plataforma de BI en los sistemas de origen y destino.

### 16.1.2 Características

La herramienta de gestión de promociones le permite realizar las acciones siguientes en Infoobjetos en el despliegue de destino.

- Crear una tarea nueva
- Copiar una tarea existente
- Editar una tarea
- Programar una promoción de tarea
- Ver el historial de una tarea
- Exportar como LCMBIAR
- Importar BIAR y LCMBIAR

La promoción de flujo de trabajo también incluye las tareas siguientes:

- *Administrar dependencias* Esta función le permite seleccionar, filtrar y administrar los dependientes de los InfoObjects de la tarea que desea promover.
- *Programar* Esta función le permite especificar una hora para la promoción de la tarea, en lugar de promover una tarea en el momento en que se crea. Puede especificar la promoción de tarea para que se ejecute una vez o de forma periódica.
- *Seguridad* Esta función le permite promover InfoObjects junto con los derechos de seguridad asociados y, si es necesario, promover los InfoObjects asociados con los derechos de aplicación.
- *Promoción de pruebas* esta función le permite comprobar o realizar pruebas sobre la promoción para garantizar que todas las medidas preventivas se lleven a cabo antes de la promoción real de los InfoObjects.
- *Restauración* Esta función le permite restaurar el sistema de destino al estado anterior, después de promover una tarea. Puede restaurar toda una tarea o solo parte de esta.
- *Auditoría* los eventos generados por la herramienta de administración de promociones se almacenan en la base de datos de auditoría. Esta función le permite supervisar los eventos que se han registrado en la base de datos de auditoría.
- *Configuración de sobrescritura de administración de promociones* esta función permite explorar y promover las sustituciones mediante la promoción de una tarea.

## 16.1.3 Derechos de acceso a la aplicación

En esta sección se describen los derechos de acceso a la herramienta de administración de promociones.

- Puede configurar estos derechos de acceso a la herramienta de administración de promociones desde la CMC.
- Puede configurar los derechos granulares de la aplicación para varias funciones de la herramienta de administración de promociones.

Para configurar los derechos específicos en la herramienta de administración de promociones, lleve a cabo los siguientes pasos:

1. Inicie la sesión en la CMC y seleccione *Aplicaciones*.
2. Haga doble clic en *administración de promociones*.
3. Haga clic en *Seguridad de usuario* y seleccione un usuario. Puede ver o asignar derechos de seguridad para el usuario.
4. Están disponibles los siguientes derechos específicos de administración de promociones:
   - Permitir el acceso para editar modificaciones
   - Permitir el acceso para incluir seguridad

- Permitir el acceso a la administración
- Permitir el acceso para administrar dependencias
- Crear tarea
- Eliminar trabajos
- Editar trabajo
- Editar LCMBIAR
- Exportar como LCMBIAR
- Importar LCMBIAR
- Promover tarea
- Restaurar tarea
- Ver y seleccionar objetos BOMM (metadatos de BusinessObjects)
- Ver y seleccionar vistas empresariales
- Ver y seleccionar calendarios
- Ver y seleccionar conexiones
- Ver y seleccionar perfiles
- Ver y seleccionar QaaWS
- Ver y seleccionar objetos de informe
- Ver y seleccionar la configuración de seguridad
- Ver y seleccionar universos

5. Si desea asignar derechos a un usuario seleccionado, seleccione el derecho adecuado y haga clic en *Asignar seguridad*.

Los derechos de acceso a la herramienta de administración de promociones se configuran en la CMC.

## 16.1.4 Soporte para WinAD en Administración de promociones

Para que la herramienta de administración de promociones funcione correctamente, debe agregar lo siguiente a todos los argumentos `javaargs` para todos los servidores de tareas de Adaptive:

```
Djava.security.auth.login.config=<ruta de
acceso>\bsclogin.conf,Djava.security.krb5.conf=<ruta de acceso>\krb5.ini
```

> → Recuerde
>
> Especifique la ruta correcta a `bsclogin.conf` y `krb5.ini` en el despliegue.

## 16.2 Introducción a la herramienta de administración de promociones

### 16.2.1 Acceder a la herramienta de administración de promociones

Para acceder a la herramienta de administración de promociones, seleccione *Administración de promociones* desde la página de inicio de la CMC.

Cualquier usuario con permisos de visualización para la carpeta *Tareas de promoción* puede iniciar la herramienta de administración de promociones. Sin embargo, para crear, programar o promover una tarea, el administrador debe conceder otros derechos al usuario.

### 16.2.2 Componentes de la interfaz de usuario

En este capítulo se explican los componentes de la GUI de la herramienta de administración de promociones.

- Barra de herramientas del área de trabajo de la administración de promociones
- Panel de área de trabajo
- Panel de árbol
- Panel de detalles
- Página Carro de la compra y Visor de tareas

#### Barra de herramientas del área de trabajo de la administración de promociones

En la tabla siguiente se enumeran las opciones que se incluyen en la barra de herramientas del área de trabajo de la administración de promociones y se explican las tareas que se pueden realizar con estas opciones:

| Opción | Descripción |
|---|---|
| | Permite crear una carpeta nueva. La carpeta que se crea es una subcarpeta de la carpeta *Tareas de promoción*. |
| | Permite copiar y eliminar la tarea o carpeta seleccionada y eliminarla de su ubicación actual. |
| | Permite copiar la tarea o carpeta seleccionada de su ubicación actual. |
| | Permite pegar la tarea o carpeta copiada en una ubicación nueva. |
| | Permite eliminar una carpeta o tarea existente. |

| Opción | Descripción |
| --- | --- |
| | Permite actualizar la página de inicio para obtener la lista actualizada de tareas o carpetas. |
| Propiedades | Permite modificar las propiedades de la tarea seleccionada. Puede modificar el título, la descripción y las palabras clave de la tarea seleccionada. |
| Historial | Permite ver el historial de la tarea seleccionada. |
| Nuevo trabajo | Permite crear una tarea nueva. |
| Importar | Permite importar archivos BIAR, LCMBIAR o archivos de sustitución. |
| Editar | Permite editar la tarea seleccionada. |
| Promover | Permite promover la tarea seleccionada. |
| Restauración | Permite deshacer la tarea promovida del sistema de destino.<br>**Nota**<br>Si la tarea promueve objetos al destino, la restauración eliminará estos objetos. Si la tarea actualiza objetos en el destino, la restauración restaurará la versión anterior de los objetos. |
| 1 | Permite desplazarse entre páginas de una lista de tareas. Puede utilizar esta opción para desplazarse a una sola página o a una página específica introduciendo el número de página correspondiente. |
| Buscar | Permite buscar tareas específicas. Puede buscar una tarea por nombre, palabras clave, descripción o los tres parámetros a la vez. |
| Tareas de promoción | Permite visualizar las tareas y carpetas. |
| Estado de la promoción | Muestra las tareas promovidas según su estado, como Correcto, Error o Parcialmente correcto. |

## Panel de área de trabajo

El panel Área de trabajo de la página de inicio de la administración de promociones muestra la lista de tareas. Puede usar este panel para ver el nombre, estado, hora de creación y de última ejecución de la tarea, los sistemas de origen y de destino, y el creador de la tarea.

## Panel de árbol

El panel Árbol de la página de inicio de la administración de promociones muestra la estructura de árbol, que incluye la carpeta *Tarea de promoción* y la carpeta *Estado de promoción*. Las tareas se muestran en una estructura jerárquica en la carpeta *Tareas de promoción*. La carpeta *Estado de promoción* muestra las tareas promovidas según su estado.

### Página Visor de tareas

La página «Visor de tareas» se muestra cuando un usuario crea una tarea nueva o edita una tarea existente. Contiene una lista generada dinámicamente de infoobjetos a promover y un panel de detalles. La lista categoriza los infoobjetos en grupos de usuarios, universos y conexiones. El panel de detalles muestra los contenidos del nodo seleccionado de la lista.

## 16.2.3 Uso de la opción de configuración

La opción de configuración permite configurar los ajustes antes de promover InfoObjects de un despliegue de la plataforma de BI a otro despliegue de la plataforma de BI y SAP. En esta sección se describe cómo usar las opciones de configuración.

Haga clic en la lista desplegable *Configuración* de la pantalla *Tareas de promoción*. En esta lista desplegable se muestran las siguientes opciones:

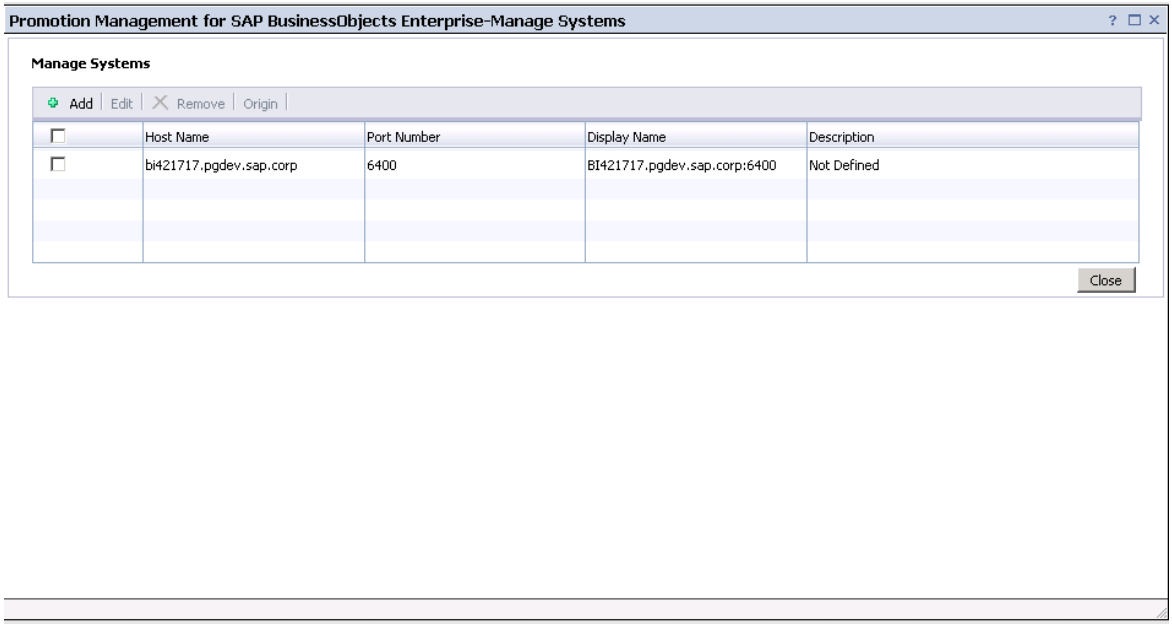
- *Administrar sistemas*: esta opción le permite agregar todos los sistemas necesarios para las actividades de la administración de promociones.
- *Configuración de restauración*: esta opción le permite seleccionar un sistema para el que se habilita la restauración.
- *Configuración de tarea* esta opción le permite ver instancias completas en la página Dependencias y permite gestionar actividades de limpieza de instancias de tarea. También permite filtrar por fecha de creación de tarea.
- *Configuración de CTS* Esta opción permite agregar el servicio Web y la información del sistema de SAP BW para la integración del Sistema de transporte de cambios mejorado.

### 16.2.3.1 Para usar la opción Administrar sistemas

En esta sección se describe cómo utilizar la opción Administrar sistemas. Esta opción le permite agregar o eliminar sistemas host.

Para agregar un sistema host, complete estos pasos:

1. En la barra de herramientas del área de trabajo de la administración de promociones, haga clic en *Configuración* y después haga clic en *Administrar sistemas*.
   Aparece la ventana *Administrar sistemas*. Esta ventana muestra una lista de nombres de host, números de puerto, nombres de presentación y descripciones.




2. Haga clic en *Agregar*.
   Aparece el cuadro de diálogo *Añadir sistema*.
3. Agregue el nombre de host, el número de puerto, el nombre de presentación y la descripción en los campos adecuados.

   > **Nota**
   >
   > Seleccione la opción *Marcar como 'Origen'* para identificar el sistema como sistema de origen (el sistema desde el que se origina la información de conexión) Esta opción resulta útil para trabajar con sustituciones.

4. Haga clic en *Aceptar* para agregar el sistema.
   El sistema host queda agregado a la lista.

> **Nota**
>
> Para eliminar o editar un sistema host, seleccione un sistema host y haga clic en *Eliminar* o *Editar*.

## Información relacionada

Para usar la opción Configuración de restauración [página 601]
Para usar la opción Configuración de tarea [página 602]

# 16.2.3.2 Para usar la opción Configuración de restauración

De forma predeterminada, el proceso de restauración está activado en el nivel del sistema. La opción *Configuración de restauración* permite deshabilitar el proceso de restauración en el nivel de sistema.

Para desactivar el proceso de restauración en el nivel de sistema, complete estos pasos:

1. En la ventana *Restaurar*, de la lista de sistemas host, seleccione el sistema host para deshabilitar el proceso de recuperación.
2. Haga clic en *Guardar y cerrar* para guardar las modificaciones.

## Información relacionada

Para usar la opción Configuración de tarea [página 602]

# 16.2.3.3 Para usar la opción Configuración de tarea

La opción Configuración de tarea le permite especifica si desea visualizar instancias completas en la página «Gestionar dependencias» y el número de instancias de tarea que pueden existir en el sistema. Puede especificar una de las opciones siguientes:

- *Visualizar instancias completas en la página Gestionar dependencias* Esta opción le permite visualizar instancias completas en la página «Gestionar dependencias» que puede añadirse a la tarea.
- *Borrar instancias si hay más de N instancias de una tarea* Esta opción le permite especificar la cantidad máxima de instancias de tarea por tarea en el sistema.
- *Borrar instancias después de N días para la tarea* Esta opción permite especificar las instancias de tarea creadas antes de un número específico de días que deben borrarse.
- En la lista desplegable *Mostrar tareas creadas*, se puede seleccionar el intervalo de tiempo para ver las tareas creadas durante el periodo especificado.

Para definir la opción *Configuración de tarea*, complete estos pasos:

1. Seleccione la opción y especifique el valor que prefiera.
2. Haga clic en *Guardar* para actualizar los cambios.

Para definir los valores predeterminados, haga clic en *Configuración predeterminada* y haga clic en *Cerrar* para cerrar la ventana.

> ⓘ Nota
>
> Las instancias de tarea antiguas se eliminan solo cuando la tarea se ejecuta la siguiente vez.

## Información relacionada

Para utilizar la subversión Apache como el sistema de administración de versión [página 691]

## 16.2.3.4 Usar la opción Reemplazar configuración

La opción Reemplazar configuración permite promover reemplazos con una promoción de tarea o un archivo LCMBIAR. Esta opción permite el escaneado, la promoción y edición de la información de conexión de base de datos para conexiones de universo y Crystal Reports. También puede usarla para editar las URLs QAAWS.

> **Nota**
>
> Para usar la opción Reemplazar configuración, debe instalar Adobe Flash Viewer.

El término *sistema* se usa en los procedimientos siguientes. Existen tres tipos de sistemas:

- *Origen*: El sistema que se origina para cualquier información de conexión.
- *Administración de promoción central*: El sistema que ejecuta la herramienta de administración de promociones.
- *Destino*: El sistema de destino en el que se promueven los recursos de BI.

### 16.2.3.4.1 Para promover modificaciones

Agregue un sistema host antes de promover las sustituciones. Para obtener información acerca de los sistemas de host, consulte Para usar la opción Administrar sistemas [página 600].

Para promover sustituciones, siga los siguientes pasos:

1. En la barra de herramientas de lugar de trabajo de gestión de promociones, haga clic en la opción *Sustituir configuración*.
   Aparece la ventana *Sustituir configuración*.
2. En el panel *Origen*, seleccione el sistema de origen deseado del menú desplegable.

   > **Nota**
   >
   > También puede seleccionar acceder a un *Nuevo sistema*. Para poder seleccionar un nuevo sistema como sistema de origen, haga lo siguiente:
   > 1. Seleccione *Nuevo sistema* en el menú desplegable.
   >  Aparece la ventana de diálogo Inicio de sesión al origen.
   > 2. Indicar las credenciales válidas en los campos *Sistema*, *Nombre de usuario*, *Contraseña*, y *Autenticación*.
   > 3. Seleccione *Iniciar sesión*.
3. Seleccione *Inicio de sesión*.
4. Marque *Examinar ahora*.

   El proceso de examen se inicia. Aparece la *lista de conexiones únicas*.

   > **Nota**
   >
   > Para programar un examen periódico, seleccione *Configuración periódica*.
5. En la lista de sobrescritos, seleccione los que quiere promover, clicando las casillas de selección correspondientes a cada sobrescrito.

> **Nota**
>
> Puede buscar sobrescritos de la lista, utilizando palabras clave como el nombre de sobrescrito, última fecha de actualización, etc.
>
> También puede Filtrar sobrescritos con los siguientes parámetros: Todos, Conexión, Qwaas, Crystal Report.
>
> Además, puede ordenar los sobrescritos en orden alfabético.

6. En el panel *Destino*, seleccione el sistema de destino deseado del menú desplegable. Puede especificar varios sistemas de destino.

   > **Nota**
   >
   > También puede seleccionar acceder a un *Nuevo sistema*. Para poder seleccionar un nuevo sistema como sistema de destino, haga lo siguiente:
   > 1. Seleccione *Nuevo sistema* en el menú desplegable.
   > Aparece la ventana de diálogo Inicio de sesión al origen.
   > 2. Indicar las credenciales válidas en los campos *Sistema*, *Nombre de usuario*, *Contraseña*, y *Autenticación*.
   > 3. Seleccione *Iniciar sesión*.

   Para exportar los sobrescritos como archivos LCMBIAR, haga lo siguiente:
   1. Seleccione Exportar a archivo LCMBIAR del menú desplegable.
   2. Seleccione *Exportar*.
   Aparece el cuadro de diálogo *Opciones de exportación*.
   3. Indicar las credenciales válidas en os campos respectivos.
   4. Seleccione *Fin*.
7. Seleccione*Promover*.

   Aparece la ventana de diálogo Sobrescritos de destino múltiple.

   > **Nota**
   >
   > Por defecto, están seleccionados todos los sistemas de destino en los que ha iniciado sesión. Puede seleccionar promover sobrescritos de manera selectiva a un destino particular verificando la casilla de selección que corresponde al sistema de destino deseado.

8. Seleccione *Fin*.

   Finaliza la promoción de sustituciones.
9. Inicie sesión en uno de los sistemas de destino con credenciales válidas.

   Aparecerá una lista de todos los objetos promovidos en una lista de conexión única. El estado de estos objetos es Inactivo.
10. Seleccione *Actualizar* para los objetos que queira tratar.

    Aparece el cuadro de diálogo *Propiedades de la conexión común*.
11. Actualice los valores necesarios y haga clic en *Listo*.

    El estado de los objetos editados se convierte en Activo.

> **Nota**
>
> También puede activar una conexión seleccionando *Inactiva*, sin la necesidad de editar la conexión en el sistema destino.

12. Seleccione *Guardar*.

### 16.2.3.4.2 Para promover modificaciones utilizando archivos BIAR

Agregue un sistema host antes de promover las sustituciones. Para obtener información acerca de los sistemas de host, consulte Para usar la opción Administrar sistemas [página 600].

Para promover sustituciones mediante archivos BIAR, realice los pasos siguientes:

1. En la barra de herramientas de lugar de trabajo de gestión de promociones, haga clic en la opción *Sustituir configuración*.
   Aparece la ventana *Sustituir configuración*.
2. Si ha iniciado sesión en el sistema de gestión de promociones central, cierre la sesión del sistema.
3. Haga clic en *Iniciar sesión* para conectarse al sistema de origen.
   Aparecerá la ventana *Iniciar sesión en sistema*.
4. En la pantalla *Reemplazar configuración*, seleccione el sistema de origen que está marcado como *Origen* para analizar los objetos e inicie la sesión en el sistema con unas credenciales válidas.
5. Desde la lista desplegable *Inicio* junto a *Examinar*, seleccione la opción *Inicio*.
   Se inicia el proceso de análisis. Aparece la Lista de sustituciones.

   > **Nota**
   >
   > Para programar un escaneo periódico, seleccione la opción *Configuración de periodicidad* de la lista desplegable.

6. En la lista de sustituciones, cambie el estado de los objetos que desee a Activo y haga clic en *Guardar*.
7. Haga clic en *Promover modificaciones*.
   Aparece la pantalla *Promover sustituciones* en la que se muestra la lista de sistemas de destino.
8. Para cifrar el archivo BIAR con una contraseña, marque la casilla de verificación *Cifrado de contraseña*.
   Se habilitan los campos *Contraseña* y *Confirmar contraseña*.
9. Introduzca una contraseña en el campo *Contraseña*. Vuelva a escribir la misma contraseña en el campo *Confirmar contraseña.*.
10. Haga clic en *Exportar* y guarde las sustituciones del archivo BIAR en un sistema de archivos.
11. Inicie sesión en el sistema de destino a través de la herramienta CCM y haga clic en *Importar* > *Sobrescribir archivo*.
    Aparece la ventana *Importar archivo LCMBIAR*.
12. Haga clic en *Examinar* para desplazarse hasta el archivo BIAR.
13. Introduzca la contraseña del archivo BIAR en el campo *Contraseña*.

> **Nota**
>
> El campo *Contraseña* sólo se muestra si el archivo BIAR que ha seleccionado está protegido con una contraseña

14. Haga clic en *Aceptar*. Finaliza la promoción de sustituciones.
15. Cierre sesión del sistema de origen.
16. En la pantalla *Reemplazar configuración*, haga clic en *Iniciar sesión*.
    Aparecerá la ventana *Iniciar sesión en sistema*.
17. Inicie la sesión en el sistema de destino con unas credenciales válidas.
    En la Lista de sustituciones aparece una lista de objetos importados. El estado de estos objetos es Inactivo.
18. Haga clic en la casilla de verificación *Seleccionar* de los objetos que desee editar y haga clic en *Editar*. Los objetos editados se indicarán con un icono.

    > **Nota**
    >
    > Puede eliminar los objetos de sustitución al hacer clic en el icono.

19. Actualice los valores necesarios y haga clic en *Listo*.
    El estado de los objetos editados se convierte en Activo.
20. Haga clic en *Guardar*.

## 16.2.3.4.3 Para promover modificaciones utilizando CTS+

Agregue un sistema host antes de promover las sustituciones. Para obtener información acerca de los sistemas de host, consulte Para usar la opción Administrar sistemas [página 600].

Para promover sustituciones a través del CTS+, realice los pasos siguientes:

> **Nota**
>
> Inicie la herramienta de administración de promociones con la autenticación de SAP para que esta opción esté disponible.

1. En la barra de herramientas de lugar de trabajo de gestión de promociones, haga clic en la opción *Sustituir configuración*.
   Aparece la ventana *Sustituir configuración*.
2. Si ha iniciado sesión en el sistema de gestión de promociones central, cierre la sesión del sistema.
3. Haga clic en *Iniciar sesión* para conectarse al sistema de origen.
   Aparecerá la ventana *Iniciar sesión en sistema*.
4. Seleccione el sistema de origen marcado como *Origen* para analizar los objetos e inicie la sesión en el sistema con unas credenciales válidas.
5. Desde la lista desplegable *Inicio* junto a *Examinar*, seleccione la opción *Inicio*.
   El proceso de examen se inicia. Aparece la *Lista de sustituciones*.

   > **Nota**
   >
   > Para programar un escaneo periódico, seleccione la opción *Configuración de periodicidad* de la lista desplegable.

6. En la lista de sustituciones, cambie el estado a Activo para los objetos que desea promover y haga clic en *Guardar*.
7. Haga clic en *Promover modificaciones*.
   Aparece la pantalla *Promover sustituciones* en la que se muestra la lista de sistemas de destino.
8. En la lista desplegable *Opciones de promoción*, seleccione la opción *Promover con CTS+*.
9. Haga clic en *Promover*.
10. Libere las sustituciones en el sistema de destino a través de los pasos siguientes:
    a. Inicie la sesión en el controlador de dominio del CTS+ y abra la IU Web del *Organizador de transporte*. Para obtener más información sobre cómo utilizar la IU de Web del Organizador de transporte, consulte IU de Web del Organizador de transporte.
    b. Si el estado de la solicitud es *Modificable*, haga clic en *Liberar* para liberar la solicitud de transporte de las sustituciones. Para obtener más información acerca de la liberación de solicitudes de transporte con objetos que no son ABAP, consulteLiberar solicitudes de transporte con objetos no ABAP.
    c. Cierre la IU Web del *Organizador de transporte*.
11. Importe las sustituciones en el sistema de destino a través de los pasos siguientes:
    a. Inicie la sesión en el Controlador de dominio de CTS+.
    b. Llame a la transacción de STMS para acceder al sistema de administración de transporte.
    c. Haga clic en el icono de *Información general de importación*.

       Se visualiza la pantalla *Información general de importación* y podrá ver los elementos de la cola de importaciones de todos los sistemas.
    d. Haga clic en el ID de sistema del sistema de administración de promociones.
       Puede ver la lista de solicitudes de transporte que se pueden importar en el sistema.
    e. Haga clic en *Actualizar*.
    f. Importe las solicitudes de transporte relevantes. Para obtener más información, consulte la documentación de Importar solicitudes.
12. Finaliza la promoción de sustituciones.
13. Inicie sesión en uno de los sistemas de destino con credenciales válidas.
    Se muestra una lista de todos los objetos promovidos en "lista de sustituciones". El estado de estos objetos es Inactivo.
14. Haga clic en la casilla de verificación *Seleccionar* de los objetos que desee editar y haga clic en *Editar*.
15. Actualice los valores necesarios y haga clic en *Listo*.
    El estado de los objetos editados se convierte en Activo.
16. Haga clic en *Guardar*.

## 16.2.3.5 Uso de la opción Configuración de CTS

Puede usar esta opción para agregar servicios Web y administrar sistemas BW en su entorno. Consulte la sección Para configurar la configuración CTS+ en la herramienta de administración de promoción [página 664] para obtener más información acerca del uso de la opción Configuración de CTS y la configuración de CTS para su uso con la herramienta de administración de promociones.

## 16.3 Usar la herramienta de administración de promociones

Al iniciar la herramienta de administración de promociones, de forma predeterminada, se le llevará a la página *Tareas de promoción*.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

La pantalla de la página de inicio *Tareas de promoción* incluye varias fichas que sirven para realizar las tareas siguientes:

- Haga clic en *Nueva tarea* para crear una tarea nueva. También puede hacer clic con el botón derecho en la pantalla de la página de inicio y seleccionar *Tarea nueva* de la lista.
- Haga clic en *Importar* > *Importar archivo* para importar un archivo BIAR o LCMBIAR directamente desde el sistema de archivos, en lugar de realizar todo el procedimiento de creación de una nueva tarea.
- Haga clic en *Importar* > *Reemplazar archivo* para importar sustituciones.
- Seleccione una tarea existente de la lista y haga clic en *Editar* para editar la tarea existente seleccionada.
- Seleccione una tarea existente de la lista y haga clic en *Promocionar* para promocionar la tarea del sistema de origen al sistema de destino, o exportar la tarea a un archivo LCMBIAR.
- Seleccione una tarea existente, ejecutada previamente de la lista y haga clic en *Restaurar* para anular los objetos promocionados del sistema de destino.
- Seleccione una tarea existente, ejecutada previamente de la lista y haga clic en *Historial* para ver las instancias de promoción anteriores de la tarea seleccionada.
- Seleccione una tarea existente de la lista y haga clic en *Propiedades* para ver las propiedades de la tarea seleccionada, como el título, ID, nombre de archivo y descripción.

El área de aplicación *Tareas de promoción* muestra la lista de tareas y carpetas que existen en el sistema junto con la información siguiente de cada tarea o carpeta:

- *Nombre:* Muestra el nombre de la tarea o carpeta que se creó.
- *Estado:* Muestra el estado de la tarea, como Creado, Correcto, Parcialmente correcto, En ejecución o Error.
- *Creado:* Muestra la fecha y la hora en que se creó la tarea o carpeta.
- *Última ejecución:* Muestra la fecha y la hora en que se promovió la tarea por última vez.
- *Sistema de origen:* Muestra el nombre del sistema desde el que se promueve la tarea.
- *Sistema de destino:* Muestra el nombre del sistema al que se promueve la tarea.
- *Creada por:* Muestra el nombre del usuario que creó la tarea o carpeta determinada.

> **Nota**
>
> La herramienta de administración de promociones usa el SDK de la plataforma de BI para todas sus actividades.

## 16.3.1 Creación y eliminación de carpetas

En esta sección se describe cómo crear y eliminar una carpeta en la página de inicio de tareas de promoción.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

### 16.3.1.1 Crear una carpeta

En esta sección, se describe cómo crear una carpeta.

Para crear una carpeta, complete estos pasos:

1. En la barra de herramientas de la administración de promociones, haga clic en .
2. En el cuadro de diálogo *Crear carpeta*, introduzca el nombre de la carpeta.
3. Haga clic en *Aceptar*.

Se crea una carpeta.

#### Información relacionada

Crear una tarea [página 610]
Para eliminar una carpeta [página 609]

### 16.3.1.2 Para eliminar una carpeta

En esta sección, se describe cómo eliminar una carpeta.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para eliminar una carpeta, complete estos pasos:

1. Seleccione una carpeta en la página de inicio *Tareas de promoción*.
2. Haga clic en .
   Aparece el cuadro de diálogo de confirmación.

3. Haga clic en *Aceptar*.

Se eliminará la carpeta seleccionada.

## Información relacionada

Crear una tarea [página 610]

# 16.3.2 Crear una tarea

En esta sección se describe cómo crear una tarea nueva con la herramienta de administración de promociones.

En la tabla siguiente, se indican los elementos de GUI y los campos que se pueden utilizar para crear una tarea

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

| Campo | Descripción |
|---|---|
| Nombre | Nombre de la tarea que desea crear. |
| Descripción | Descripción de la tarea que desea crear. |
| Palabras clave | Las palabras clave para el contenido de la tarea que desea crear. |
| Guardar tarea en | Se muestra la carpeta seleccionada predeterminada. |
| Sistema de origen | Nombre del sistema de la plataforma de BI desde el que desea promover una tarea. |
| Sistema de destino | Nombre del sistema de la plataforma de BI al que desea promover una tarea. |
| Nombre del usuario | ID de conexión que debe utilizar para conectarse al sistema de origen o de destino. |
| Contraseña | Contraseña que debe utilizar para conectarse al sistema de origen o de destino. |

| Campo | Descripción |
| --- | --- |
| Autenticación | Tipo de autenticación que se utiliza para conectarse al sistema de origen o de destino.<br>La herramienta de administración de promociones admite los siguientes tipos de autenticación:<br>• Enterprise<br>• Windows AD<br>• LDAP<br>• SAP |

> **Nota**
>
> Antes de crear una tarea, asegúrese de que las sustituciones, si las hubiera, se han editado y actualizado en el sistema de destino, de modo que el contenido de la Plataforma de BI se actualice automáticamente. Para obtener más información, consulte Usar la opción Sobrescribir configuración.

Para crear una nueva tarea con la herramienta de administración de promociones, siga los siguientes pasos:

1. Inicie la herramienta de administración de promociones.
2. En la página de inicio *Tareas de promoción*, haga clic en *Nueva tarea*.
3. Introduzca en los campos correspondientes el nombre, la descripción y las palabras clave para la tarea.

   > **Nota**
   >
   > No es obligatorio proporcionar la información de los campos Descripción, Palabras clave y Sistema de destino.

4. En el campo *Guardar tarea en*, localice y seleccione la carpeta en la que desea guardar la tarea.

   > **Nota**
   >
   > De forma predeterminada, el nombre de la carpeta resaltada en el panel de carpetas rellenará el campo *Guardar tarea en* antes de hacer clic en *Nueva tarea*.

5. Seleccione el sistema de origen y el sistema de destino en las respectivas listas desplegables.
   Si el nombre del sistema no aparece en la lista desplegable, haga clic en la opción *Conectar a nuevo CMS*. Se abre una nueva ventana. Introduzca el nombre del sistema junto con el nombre de usuario y la contraseña.
6. Haga clic en *Crear*.
   Aparece la ventana «Agregar objetos».
7. Seleccione los objetos del sistema de origen para agregarlos a la tarea y luego haga clic en *Agregar y cerrar*.
8. Haga clic en *Guardar*.

La tarea recién creada se almacena en el repositorio del CMS del sistema de origen.

> **Nota**
>
> Si crea una tarea con una carpeta como el objeto principal y la tarea es recurrente, la tarea incluirá el contenido agregado a la carpeta en el próximo tiempo de ejecución.

## Información relacionada

Usar la opción Reemplazar configuración [página 603]

### 16.3.2.1 Para iniciar sesión en un nuevo CMS

En esta sección se describe cómo conectarse a un nuevo CMS.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para conectarse a un nuevo CMS, complete estos pasos:

1. Inicie la aplicación de administración de promociones.
2. Crear una tarea nueva.
   Para obtener más información sobre la creación de una tarea, consulte Crear una tarea [página 610]
3. En la lista desplegable *Sistema de origen*, seleccione *Conectar a nuevo CMS*.
   Aparece el cuadro de diálogo *Iniciar sesión en sistema*.
4. Selecione el sistema de la lista desplegable o el tipo en un nuevo nombre de sistema.
5. Especifique las credenciales de usuario, seleccione el tipo de autenticación adecuado y haga clic en *Iniciar sesión*.
6. En la lista desplegable *Sistema de destino*, seleccione *Conectar a nuevo CMS*.
7. Selecione el sistema de la lista desplegable o el tipo en un nuevo nombre de sistema.
8. Especifique las credenciales de usuario, seleccione el tipo de autenticación adecuado y haga clic en *Iniciar sesión*.

## Información relacionada

Para editar una tarea [página 614]
Para añadir un InfoObjeto a una tarea [página 614]
Para promover una tarea cuando los repositorios están conectados [página 617]
Para programar una promoción de tarea [página 624]

### 16.3.3 Para crear una nueva tarea copiando una tarea existente

En esta sección se describe cómo crear una tarea copiando una tarea existente.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para crear una tarea copiando una tarea existente, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
2. En la página de inicio *Tareas de promoción*, haga clic en *Nueva tarea*.
3. Haga clic en la opción *Copiar una tarea existente*.
   Aparece la ventana *Copiar una tarea existente* en la que se muestra la lista de tareas de la carpeta *Tareas de promoción*.
4. Seleccione la tarea requerida de la lista y haga clic en *Crear*.
   Se visualizan el nombre, las palabras clave y la descripción de la tarea, así como los campos *Guardar tarea en* y *Destino*. Si es necesario, puede modificar estos campos.
5. En el campo *Guardar tarea en*, localice y seleccione la carpeta en la que desea guardar la tarea y haga clic en *Crear*.

Se crea una tarea y aparece la ventana *Agregar objetos*.

### Información relacionada

Para añadir un InfoObjeto a una tarea [página 614]
Para editar una tarea [página 614]
Para promover una tarea cuando los repositorios están conectados [página 617]

## 16.3.4 Para buscar una tarea

La función de búsqueda de la herramienta de administración de promociones permite localizar una tarea disponible en el repositorio.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para buscar una tarea, complete estos pasos:

1. En el campo *Buscar* de la página de inicio, introduzca el texto que desee buscar.
2. Haga clic en la lista que aparece junto al campo *Buscar* para especificar los parámetros de búsqueda.
   Puede especificar los parámetros de búsqueda siguientes:
   - *Buscar título* Esta opción permite buscar una tarea por su nombre.
   - *Buscar palabra clave* Esta opción permite buscar una tarea por sus palabras clave.

- *Buscar descripción* Esta opción permite buscar una tarea por su descripción.
- *Buscar en todos los campos* Esta opción permite buscar una tarea por su título, sus palabras clave y su descripción.

3. Haga clic en el icono de Buscar.

### Información relacionada

Para añadir un InfoObjeto a una tarea [página 614]
Para editar una tarea [página 614]

## 16.3.5 Para editar una tarea

En esta sección, se describe cómo editar una tarea.

> **Nota**
> - Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.
> - Editar una tarea no es lo mismo que crear una tarea.

Para editar una tarea, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
2. En la página de inicio *Tareas de promoción*, seleccione la tarea que desea editar.
3. Haga clic en *Editar*.
   Aparecen los detalles de la tarea seleccionada. Usted puede agregar o eliminar Infoobjetos, gestionar dependencias o promocionar la tarea, como sea necesario.

Al editar una tarea, no se puede cambiar el nombre de un sistema de origen.

### Información relacionada

Para añadir un InfoObjeto a una tarea [página 614]
Para promover una tarea cuando los repositorios están conectados [página 617]
Para programar una promoción de tarea [página 624]

## 16.3.6 Para añadir un InfoObjeto a una tarea

Cada tarea debe incluir un conjunto de infoobjetos. Por lo tanto, debe agregar InfoObjects a una tarea antes de promoverla al sistema de destino.

> **Nota**
>
> - Al promover un informe de Crystal basado en InfoObjects de vista empresarial (conexión de datos, infraestructura de datos, elementos empresariales, y vista empresarial) debe incluir la información de seguridad (derecho de DataAccess en conexión de datos y el derecho de ViewDataField en la infraestructura de datos y elementos empresariales) para ver datos en un informe del sistema de destino.
> - Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para agregar un InfoObject a una tarea, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
2. Crear una tarea nueva o edite una existente.
   Para obtener información sobre la creación de un tarea, consulte Crear una tarea [página 610] y Para editar una tarea [página 614].
3. Haga clic en *Agregar objetos* al editar una tarea.

   > **Nota**
   >
   > El cuadro de diálogo *Agregar objetos* se muestra al crear una tarea nueva.

4. Desplácese a la carpeta de la que desee seleccionar el InfoObject.
   Aparece la lista de InfoObjects de la carpeta seleccionada.
5. Seleccione el infoobjeto que desee agregar a la tarea y haga clic en *Agregar*

   Si desea agregar un infoobjeto y salir del cuadro de diálogo «Agregar objetos desde el sistema: `<NAME>`», haga clic en *Agregar y cerrar*. El infoobjeto se agrega a la tarea y el cuadro de diálogo se cierra.

Una vez agregado un InfoObject a una tarea, puede hacer clic con el botón derecho en la página *Visor de tareas* y seleccionar los procesos relacionados con la tarea para proseguir con la tarea de promoción. Puede administrar los dependientes del InfoObject que ha seleccionado utilizando la opción *Administrar dependencias* en la página *Visor de tareas*.

> **Nota**
>
> - En el carro de la compra, que aparece en el panel izquierdo de la página *Visor de tareas*, se muestra la tarea junto con sus dependientes, en una estructura de árbol plana.
> - Haga clic en la opción *Guardar*, después de agregar InfoObjects, para guardar los cambios. Si no lo hace, se solicitará al usuario que guarde la tarea cuando cierre la pestaña.

Práctica recomendada: SAP BusinessObjects recomienda seleccionar un número pequeño de InfoObjects (no más de 100 a la vez) para su promoción para obtener un rendimiento óptimo de la herramienta de administración de promociones.

## Información relacionada

Para gestionar las dependencias de una tarea [página 616]
Para promover una tarea cuando los repositorios están conectados [página 617]

Para programar una promoción de tarea [página 624]

## 16.3.7 Para gestionar las dependencias de una tarea

En esta sección se describe cómo administrar los dependientes de un InfoObject.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para administrar los dependientes de un InfoObject, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
2. Crear una tarea nueva o edite una existente.
   Para obtener información sobre la creación de un tarea, consulte Crear una tarea [página 610] y Para editar una tarea [página 614].
3. Añada los InfoObjetos necesaros a la tarea y cierre el diálogo *Añadir objetos* para volver a la ventana *Visor de tareas*.
4. Haga clic en *Administrar dependencias*.
   Aparece la ventana *Gestionar dependencias*. La ventana muestra la lista de InfoObjects y sus dependientes. Para ver solo los dependientes de los objetos que no se han seleccionado, haga clic en la casilla de verificación *Mostrar dependientes sin seleccionar*.
5. En la lista desplegable *Seleccionar dependientes*, seleccione las opciones para agregar los dependientes agrupados a la tarea. Los dependientes no están seleccionados de forma predeterminada; los dependientes que se deseen promover se deben seleccionar explícitamente.

   Por ejemplo, si selecciona *Todos los universos* en la lista desplegable *Seleccionar dependientes*, se seleccionan todos los universos incluidos en la lista de dependientes. También se pueden seleccionar los dependientes de forma individual.

   Puede hacer clic en el *Tipo* para ver las opciones de filtrado compatibles con los InfoObjetos. Se muestra una lista desplegable. En esta lista se muestran las opciones de filtrado compatibles. Seleccione la opción de filtrado y haga clic en *Aceptar*. Se muestran los InfoObjects filtrados.

   Cuando seleccione los dependientes en la columna *Dependientes* y haga clic en *Aplicar cambios*, los dependientes se mueven automáticamente a la columna *Objetos en tarea*.

   También, se puede escribir el nombre del dependiente en el campo *Buscar dependientes* para buscar un dependiente.

   Para obtener más información sobre cómo buscar dependientes, consulte Para buscar dependientes [página 617]
6. Haga clic en *Aplicar cambios* para actualizar la lista de dependientes y haga clic en *Aplicar cambios y cerrar* para guardar los cambios.

La herramienta contabiliza automáticamente los objetos dependientes. Estos dependientes se contabilizan sobre la base de las relaciones de los InfoObjects o las propiedades de los InfoObjects. Los dependientes que no cumplen los requisitos de los criterios anteriores no se contabilizan en esta versión de la herramienta.

> **Nota**
>
> Si selecciona una carpeta para promover, el contenido de la carpeta seleccionada se considera como recursos principales.

### Información relacionada

Para promover una tarea cuando los repositorios están conectados [página 617]

## 16.3.8 Para buscar dependientes

La función de búsqueda avanzada de la herramienta de administración de promociones permite buscar los dependientes de los infoobjetos disponibles en el repositorio.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para buscar los dependientes de un InfoObject, complete estos pasos:

1. Inicie la administración de promociones.
2. Crear una tarea nueva o edite una existente.
   Si ha creado una tarea, agregue InfoObjects a la tarea. Si edita una tarea existente, puede agregar infoobjetos, según sea necesario.
3. Haga clic en *Administración de dependencias*.
4. En el campo *>Buscar dependientes*, introduzca el nombre del dependiente que desea localizar.
5. Haga clic en el icono de Buscar.

### Información relacionada

Para gestionar las dependencias de una tarea [página 616]

## 16.3.9 Para promover una tarea cuando los repositorios están conectados

En esta sección se describe cómo promover una tarea del sistema de origen al sistema de destino cuando ambos sistemas están activos.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

En la siguiente tabla se enumeran los tipos de InfoObjects que se pueden promover con la herramienta de administración de promociones

| Categoría | Tipos de objeto que se pueden promover |
|---|---|
| Informes | Informes de Crystal, Web Intelligence, QaaWS, Lumira |
| Objetos de terceros | Texto enriquecido, documento de texto, Microsoft Excel, Microsoft Power Point, Microsoft Word, Flash, Adobe Acrobat |
| Usuarios | Usuarios y grupos de usuarios |
| Servidor | Grupos de servidores |
| Plataforma de Business Intelligence | Carpeta, programa, eventos, perfiles, paquetes de objetos, hipervínculo, categorías, documento de bandeja de entrada, carpetas Personal y Favoritos |
| Universo, espacio de trabajo, conjuntos | Universos UNV, conexiones, conjuntos |
| Cuadro de mandos EPM | Universos, conexiones, informes y analíticas |
| Vista empresarial | DataFoundation |
| Federación<br>• Lista de réplicas<br>• Tareas de réplica | La Lista de réplicas promueve los siguientes objetos: Flash, .txt, debates, .pdf, hipervínculo, .xls, paquete de objetos, informes de Crystal, documentos de Web Intelligence, universos, programa, conexiones, infraestructura de datos, vistas empresariales, .rtf, perfil, evento, usuarios y grupos de usuarios. Las Conexiones de réplica promueve tareas de réplica, conexión remota, publicaciones, debates, conexión a Pioneer |
| Servicios BI | Documentos de Web Intelligence, universos y conexiones |
| Nuevos InfoObjects | Crystal reports (rpt/rptr), Pioneer, DSL Universe (UNX), Business Layer (BLX), Connection (CNX), Data Fooundation (DFX), WebI, Data Federator, Data Steward, BI Workspace, etc. |
| Arrendatarios | La gestión de promociones admite la promoción de arrendatarios, junto con sus dependencias, del sistema fuente al de destino proporcionando opciones para seleccionar y agregar arrendatarios y los objetos de arrendatarios correspondientes para una tarea. También establece una relación entre arrendatarios y los objetos de arrendatarios correspondientes como dependencias. La función trabaja tanto en modo GUI como en modo CLI de la gestión de promociones. |

El comentario BI es compatible con la gestión de promociones. Cuando promueve un documento con comentarios, cualquier comentario sobre el documento también migrará del sistema fuente al sistema destino (Live to Live, Live to BIAR, BIAR to Live). Para promover un documento con comentarios, seleccione *Promover* > *Opciones de comentario* y seleccione la casilla de verificación *Incluir comentarios*.

> **Nota**
>
> Por defecto, la casilla de verificación *Incluir comentarios* no está seleccionada.

Al promocionar un objeto replicado, la información específica de la replicación asociada a los objetos también promocionados desde el origen al sistema de destino (Live a Live, Live a BIAR, BIAR a Live). Para promocionar un documento sin información específica de replicación, seleccione *Promocionar* > *Opciones de tareas de federación* y desmarque la casilla de selección *Incluir relación de tareas de federación*.

> **Nota**
>
> Por defecto, la casilla de verificación *Incluir relación de tareas de federación* está seleccionada.

Para promover una tarea, lleve a cabo estos pasos:

1. Inicie la administración de promociones.
2. En la página de inicio *Tareas de promoción*, seleccione la tarea que desea promover.
   También puede hacer clic con el botón derecho en la pantalla de la página de inicio y hacer clic en *Promover*.
3. De la lista de sistema de *Destino*, seleccione un sistema de destino diferente como sea necesario.

   > **Nota**
   >
   > Compruebe que se ha conectado tanto al sistema de origen como al de destino antes de continuar con el proceso de promoción.

4. En el campo *ID de administración de cambios externos*, introduzca el valor adecuado y haga clic en *Guardar*.

   > **Nota**
   >
   > El ID de administración de cambios externos se utiliza para obtener información relacionada con el registro, la auditoría, el historial de tareas. La herramienta gestión de promociones le permite asignar cada instancia de creación de tareas a un ID de gestión de modificaciones. Este ID es un atributo que establece el usuario en la definición de tarea al crear una tarea nueva. La herramienta genera automáticamente un ID para cada tarea.

5. Seleccione *Configuración de seguridad*, si es necesario. Aparecen las siguientes opciones:
   - *No promover seguridad* Ésta es la opción predeterminada.
   - *Promover seguridad* Utilice esta opción para promover tareas junto con los derechos de seguridad asociados.
   - *Promover seguridad del objeto* Utilice esta opción para promover la seguridad de objetos y carpetas
   - *Promover seguridad del usuario* permite promover los derechos de los usuarios que forman parte de la tarea
   - *Incluir derechos de aplicación* Puede seleccionar esta opción sólo si también selecciona *Promover seguridad del usuario*. Si los objetos de la tarea heredan derechos de aplicación, la tarea se promueve junto con estos derechos.
   - *Promocionar seguridad al nivel superior* Utilice esta opción para promocionar los derechos de seguridad del nivel superior.

     > **Precaución**
     >
     > La opción de seguridad *Promocionar nivel superior* sobrescribe los derechos de seguridad de nivel superior definidos en el sistema de destino.

   También puede hacer clic en *Ver derechos* para ver las dependencias de seguridad de los InfoObjects de la tarea.

> **Nota**
>
> El botón *Visualizar derechos* está desactivado hasta que grabe el nuevo trabajo.

6. Haga clic en *Grabar*.

   El botón *Visualizar derechos* está activado. Ahora puede visualizar las dependencias de seguridad.

7. Haga clic en *Probar promoción* para comprobar que no haya conflictos entre los CUID de los InfoObjects en los sistemas de origen y destino. Los detalles de promoción se muestran en las fichas *Correcto*, *Error* y *Advertencia*. La primera columna muestra los objetos que se van a promover y la segunda el estado de promoción de cada InfoObject. La herramienta de administración de promociones clasifica los objetos seleccionados en usuarios, grupos, universos.

   > **Nota**
   >
   > Esta opción no confirma la promoción de los InfoObjects.

   Los resultados de una prueba de promoción puede ser los siguientes:

   - `Sobreescrito` El InfoObjeto del sistema de destino se sobrescribe con el InfoObjeto del sistema de origen.
   - `Copiado` El InfoObjeto del sistema de origen se copia en el sistema de destino.
   - `Omitido` El InfoObjeto no se promueve del sistema de origen al sistema de destino.
   - `Advertencia` El InfoObjeto del sistema de destino es la versión más reciente y puede eliminar el InfoObjeto de la tarea. No obstante, si desea realizar la promoción, el InfoObject se promueve.
   - `Asignado` El Infoobjeto se asigna a un Infoobjeto del sistema destino.

8. Haga clic en *Programar* si desea que una promoción se ejecute en una hora específica o de forma recurrente.
9. Haga clic en *Promover*.
   La tarea seleccionada se promueve.

Si no desea promover la tarea, puede utilizar la opción *Guardar* para guardar las modificaciones como la seguridad, el ID de administración de cambios y la configuración de programación.

## 16.3.10 Promover una tarea con un archivo LCMBIAR

Promover significa transferir un recurso de BI de un repositorio a otro. Si los sistemas de origen y de destino están en la misma red, la herramienta de administración de promociones usa WAN o LAN para promover el infoobjeto. No obstante, la herramienta de administración de promociones también facilita la promoción de InfoObjects aunque los sistemas de origen y de destino no estén en la misma red.

En los casos en los que los sistemas de origen y de destino no están en la misma red, la herramienta de administración de promociones admite la promoción de tareas al sistema de destino al permitir la exportación de la tarea del sistema de origen a un archivo LCMBIAR y la importación de la tarea desde el archivo BIAR al sistema de destino.

En esta sección se describe cómo exportar una tarea a un archivo LCMBIAR y después importar la tarea del archivo BIAR en el sistema de destino.

> **Nota**
>
> - Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.
> - Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

## Información relacionada

Exportar una tarea a un archivo LCMBIAR [página 621]
Importar una tarea de un archivo LCMBIAR [página 622]

# 16.3.10.1 Exportar una tarea a un archivo LCMBIAR

En esta sección, se describe cómo exportar una tarea a un archivo LCMBIAR.

Para exportar una tarea a un archivo LCMBIAR, complete estos pasos:

1. Inicie la herramienta de administración de promociones y cree una nueva tarea.

   Para obtener más información sobre la creación de tareas, consulte Crear una tarea [página 610]
2. En la lista desplegable *Destino*, seleccione la opción *Resultados en archivo LCMBIAR* y haga clic en *Crear*.
3. Haga clic en *Agregar objetos* para agregar InfoObjects a la tarea.

   Puede utilizar la opción *Administrar dependencias* para administrar las dependencias de la tarea seleccionada.
4. Para cifrar el archivo LCMBIAR mediante una contraseña, marque la casilla de verificación *Cifrado de contraseña*.
5. Introduzca una contraseña en el campo *Contraseña*.
6. Vuelva a escribir la contraseña en el campo *Confirmar contraseña*.
7. Haga clic en *Promover*.
   Aparece la ventana *Promocionar*.
8. Modifique las opciones de seguridad según sea necesario y haga clic en *Exportar*.
   Se crea el archivo LCMBIAR. Puede guardar un archivo LCMBIAR en el sistema de archivos.
9. (Opcional) Haga clic en *Destino de archivo LCMBiar* y seleccione *FTP* para exportar el archivo LCMBIAR a un servidor FTP o SFTP respectivamente. Introduzca el nombre de host, puerto, nombre de usuario, contraseña, directorio y nombre de archivo y haga clic en *Exportar*.

   > **Nota**
   >
   > Si selecciona *SFTP* como *Destino de archivo LCMBiar*, debe indicar de forma adicional el fingerprint SFTP.

10. En la lista desplegable *Destino*, seleccione la opción *Resultados en archivo LCMBIAR* y haga clic en *Destino de archivo LCMBiar*.

Puede programar la exportación de una tarea a un archivo LCMBIAR. Para obtener más información, consulte la sección Para programar una promoción de tarea [página 624].

### Información relacionada

Para añadir un InfoObjeto a una tarea [página 614]
Para gestionar las dependencias de una tarea [página 616]

## 16.3.10.2 Importar una tarea de un archivo LCMBIAR

Puede importar una tarea de un archivo LCMBIAR. El archivo LCMBIAR se copia desde el dispositivo de almacenamiento al sistema de destino.

Para importar un archivo LCMBIAR, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
2. En la página de inicio *Tareas de promoción*, haga clic en *Importar* > *Importar archivo*.
   Aparece la ventana *Importar desde archivo*.
3. Puede importar un archivo BIAR desde el sistema de archivos o desde un servidor FTP o SFTP.
   - Para importar un archivo BIAR desde el sistema de archivos, lleve a cabo los siguientes pasos:
     1. Seleccione *Sistema de archivos*.
     2. Haga clic en *Examinar* y seleccione un archivo LCMBIAR del sistema de archivos.
     3. En el campo *Contraseña*, introduzca la contraseña del archivo LCMBIAR.

        > **Nota**
        > El campo Contraseña solo se muestra si el archivo LCMBIAR está protegido con una contraseña.

     4. Haga clic en *Crear*. La tarea se crea.

        > **Nota**
        > Si existe una tarea con el mismo nombre, aparece la ventana emergente Confirmar guardar. Haga clic en 'Sí' para sobrescribir la tarea existente; haga clic en 'No' para crear una tarea con un nuevo nombre `jobname_copy<CURRENT_DATE_AND_TIME>`
   - Para importar un archivo LCMBIAR desde un servidor FTP, complete estos pasos:
     1. Seleccione *FTP*.
     2. Introduzca los detalles adecuados en los campos de host, puerto, nombre de usuario, contraseña, directorio y nombre de archivo y haga clic en *Aceptar*.
   - Para importar un archivo LCMBIAR desde un servidor SFTP, complete estos pasos:
     1. Seleccione *SFTP*.

2. Introduzca los detalles adecuados en los campos host, puerta, nombre de usuario, contraseña, directorio, fingerprint y nombre de archivo y haga clic en *Aceptar*.

4. Haga clic en *Promover*.
   Aparece la ventana *Promover - Nombre de tarea*.
5. En la lista desplegable *Destino*, seleccione el sistema de destino. Si selecciona *Conectar a nuevo CMS*, se le solicitarán credenciales. Confirme las credenciales de conexión del sistema de destino.
6. Haga clic en *Promover* para promover el contenido al sistema de destino.

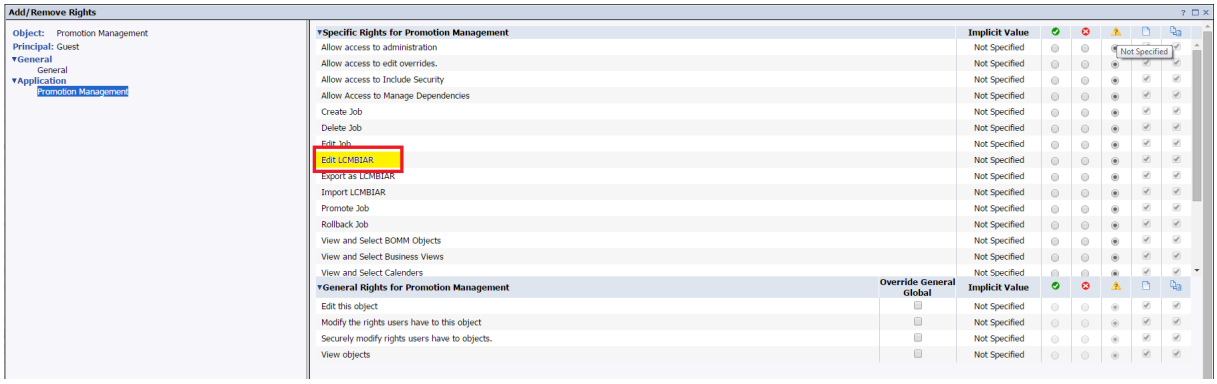
   Asimismo, puede hacer clic en la opción *Probar promoción* para ver los objetos que se van a promover y el estado de promoción.
7. **Opcional:** Si está importando un documento de Web Intelligence que usa personalización, en la ficha *Preferencias de BI de grupos de usuarios* asegúrese de marcar *Sobrescribir preferencias de BI de grupos de usuarios* para importar la personalización.

## Información relacionada

Para gestionar las dependencias de una tarea [página 616]

## 16.3.10.2.1 Recuperación selectiva de objetos de un archivo LCMBIAR

Para recuperar selectivamente objetos de un archivo LCMBIAR, se requiere que el usuario tenga derecho a *Editar LCMBIAR* right.




Para recuperar selectivamente objetos de un archivo LCMBIAR, haga lo siguiente:

1. Seleccione los objetos a promover.
2. Haga clic en *Promover*.

> ⓘ Nota
>
> - Se crea un nuevo job con los objetos seleccionados.
> - Se puede realizar la misma operación utilizando la herramienta Línea de comando. Para más información, vea Parámetros de la herramienta Línea de comando [página 637]

- Promoción selectiva no se soporta para el escenario live to live.

## 16.3.11 Para programar una promoción de tarea

En esta sección se describe cómo programar la promoción de una tarea. Además se describe cómo especificar las opciones de periodicidad y los parámetros

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para programar la promoción de una instancia de tarea, complete estos pasos:

1. En el cuadro de diálogo *Promover*, haga clic en la opción *Programar*.
2. Configure la opción de programación necesaria y haga clic en *Programar*.

Si agrega InfoObjetos a una carpeta existente después de que se haya programado la promoción de una tarea, también se promoverán en el destino a la hora programada. Sin embargo, esto no se mantiene en true cuando intenta programar una promoción de jobs con un archivo LCMBIAR, ya que LCMBIAR no se considera un destino 'real'.

> **→ Sugerencias**
>
> Después de completar la promoción de una tarea, podrá visualizar todas las instancias de la tarea seleccionando la tarea en la página *Tareas de promoción* y haciendo clic en *Historial* en la barra de herramientas.

La promoción de una tarea también se puede producir al desencadenar un evento.

Puede seleccionar notificaciones por correo electrónico según el estado de promoción de la tarea (como correcto/parcial, correcto/error). Para obtener información detallada acerca de las distintas opciones de programación y la configuración de las notificaciones, consulte la sección Programación.

### Información relacionada

Exportar una tarea a un archivo LCMBIAR [página 621]

## 16.3.11.1 Actualización de instancias de promoción de tareas pendientes y periódicas

La herramienta gestión de promociones le permite hacer el seguimiento del estado y volver a programar instancias de tareas de promoción mediante la opción *Instancias periódicas y pendientes*.

Para hacer un seguimiento del estado y volver a programar instancias de promociones de tareas, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
2. En la página de inicio *Tareas de promoción*, seleccione una tarea.
3. Haga clic en *Historial*.
   Aparece la ventana *Historial de tareas*.
4. Haga clic en *Instancias pendientes y periódicas*.
   Aparece la ventana *Historial de tareas para instancias periódicas y pendientes*. Esta ventana muestra la lista de instancias de promoción de tareas pendientes y pendientes.

   Puede utilizar las siguientes opciones, como sea necesario:
   - Haga clic en *Instancias promovidas* para ver la lista de instancias de tareas de promoción.
   - Haga clic en la opción *Pausar* para pausar la instancia pendiente o periódica seleccionada.
   - Haga clic en la opción *Reanudar* para reanudar la instancia de tarea de promoción programada pausada.
   - Haga clic en la opción *Reprogramar* para volver a programar la instancia de tarea de promoción seleccionada.
   - Haga clic en para borrar una instancia de tarea de promoción programada.
   - Haga clic en para actualizar el estado de una instancia de tarea de promoción programada.
   - Puede utilizar la opción para desplazarse por una sola página o desplazarse a una página específica introduciendo el número de página correspondiente.

   > **Nota**
   >
   > La columna de estado de la ventana *Historial de tareas para instancias peiódicas y pendientes* muestra el estado de la instancia de tarea de promoción, como por ejemplo, periódica, pendiente.

## Información relacionada

Para restaurar una tarea [página 626]

# 16.3.12 Para ver el historial de una tarea

En esta sección se describe cómo ver el historial de una tarea.

> **Nota**
>
> Para ver el historial de una tarea, debe comprobar que el estado de la tarea sea uno de los siguientes:
>
> - Correcto
> - Error
> - Parcialmente correcto

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para ver el historial de una tarea, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
   Aparece la página de inicio de *Tareas de promoción*.
2. Seleccione la tarea cuyo historial desea ver y haga clic en la ficha *Historial*.

   Se muestran el tiempo de instancia y el nombre de la tarea, los nombres de los sistemas de origen y destino, el ID del usuario que promovió la tarea y el estado (Correcto, Error o Parcialmente correcto) de la tarea.

   Puede ver el status detallado de la tarea haciendo clic en el vínculo que se muestra en la columna *Estado*.

## 16.3.13 Para restaurar una tarea

La opción Restauración permite restaurar el sistema de destino a su estado anterior, después de promover una tarea.

> **Nota**
>
> Las mejoras de seguridad se implementan en la herramienta de gestión de promociones, lo que provoca cambios en determinados comportamientos al ejecutar acciones. Para obtener más información, consulte 3350454.

Para restaurar una tarea, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
   Aparece la página de inicio de *Tareas de promoción*.
2. Realice cualquiera de las siguientes operaciones:
   - Haga clic con el botón derecho en la tarea que desea restaurar y seleccione *Restauración*.
   - Seleccione la tarea que desea restaurar y haga clic en la ficha *Restauración*.

   Aparece la ventana *Restauración*.
3. Seleccione la instancia que desea restaurar y haga clic en *Restauración completa*.
   La instancia se restaura.

Solo se puede restaurar la instancia más reciente de una tarea de promoción. Usted no puede restaurar al mismo tiempo múltiples instancias de tareas.

### 16.3.13.1 Para usar la opción Restauración parcial

La herramienta de administración de promociones permite restaurar InfoObjects en una tarea completa o parcialmente desde el sistema de destino.

Para restaurar los InfoObjects parcialmente, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
   Aparece la página de inicio de *Tareas de promoción*.
2. Realice cualquiera de las siguientes operaciones:
   - Haga clic con el botón derecho en la tarea que desea restaurar y seleccione *Restauración*.
   - Seleccione la tarea que desea restaurar y haga clic en la ficha *Restauración*.

   Aparece la ventana *Restauración*.
3. Seleccione la instancia de la lista y haga clic en *Restauración parcial*.

   La lista de los InfoObjects de la tarea seleccionada se muestra en la página *Visor de tareas*.
4. Seleccione los InfoObjects que desea restaurar y haga clic en *Restauración*.

> ⓘ Nota
>
> Debe comprobar que se han restaurado todos los InfoObjects de una instancia antes de restaurar los InfoObjects de la siguiente instancia.

> ⚠ Precaución
>
> Si una tarea se promueve con seguridad, es posible que durante la restauración parcial de los InfoObjects, la seguridad de los InfoObjects dependientes seleccionados no se restaure a su estado anterior.

### Información relacionada

Para administrar versiones distintas de recursos de BI [página 688]

## 16.3.13.2 Para restaurar una tarea después de caducar la contraseña

En esta sección, se describe cómo restaurar una tarea, después de que la contraseña que se utilizó para promoverla haya caducado.

Para restaurar una tarea después de que la contraseña haya caducado, complete estos pasos:

1. Seleccione la tarea que desea restaurar y haga clic en *Restauración*.
2. En la ventana *Restauración*, seleccione *Restauración completa*.
   Aparece un mensaje de error. En este mensaje, se indica que la tarea no puede restaurarse. Además, se le solicita que se conecte a los sistemas de origen y de destino.
3. Introduzca las nuevas credenciales de conexión y haga clic en *Iniciar sesión*.

Aparece un cuadro de diálogo donde se indica que el proceso de restauración se ha completado.

> ⓘ Nota
>
> Los recursos que se promovieron utilizando las credenciales de los sistemas de origen y destino se actualizan automáticamente.

## Información relacionada

Restaurar infoobjetos cuando haya caducado la contraseña [página 628]
Para usar la opción Restauración parcial [página 626]

### 16.3.13.2.1 Restaurar infoobjetos cuando haya caducado la contraseña

En esta sección se describe cómo restaurar infoobjetos parcialmente después de que la contraseña de los sistemas de origen y destino haya caducado.

Para restaurar infoobjetos parcialmente después de que la contraseña haya caducado, complete estos pasos:

1. Seleccione la tarea que desea restaurar y haga clic en *Restauración*.
   Aparece la ventana *Restauración*.
2. Seleccione la opción *Restauración parcial*.
   Aparece un mensaje de error. En este mensaje, se indica que los InfoObjects no pueden restaurarse. Además, se le solicita que se conecte a los sistemas de origen y de destino.
3. Introduzca las nuevas credenciales de conexión y haga clic en *Iniciar sesión*.
   Aparece la página *Visor de tareas*. En esta página se muestra la lista de InfoObjects.
4. Seleccione los InfoObjects que requiera y haga clic en *Restauración*.

> **Nota**
>
> Los recursos que se promovieron utilizando las credenciales de los sistemas de origen y destino se actualizan automáticamente.

## Información relacionada

Para restaurar una tarea [página 626]
Para usar la opción Restauración parcial [página 626]
Para restaurar una tarea después de caducar la contraseña [página 627]

## 16.4 Promover contenido de repositorio completo con la herramienta de administración de promociones

Promover los contenidos de un repositorio requiere planificación, preparación y tiempo suficiente. En esta sección se describen las acciones requeridas para una promoción correcta del contenido de un despliegue a otro.

## 16.4.1 Preparar los sistemas de origen y destino

Debe asegurarse de que los sistemas de origen y destino están configurados de forma óptima antes de promover el contenido.

1. En el sistema de origen:
   a. Use la herramienta de diagnóstico del repositorio (RDT) para escanear y corregir el sistema de origen y corregir cualquier inconsistencia del repositorio o FRS. Para obtener más información sobre la RDT, consulte el *Manual del usuario de la herramienta de diagnóstico del repositorio de la plataforma de SAP BusinessObjects Business Intelligence*.
   b. Minimice la utilización del sistema en el sistema de origen para garantizar cambios mínimos durante la promoción. Un sistema activo puede causar errores en el objeto.

      > **Nota**
      >
      > Si se producen errores, revise el estado de las tareas para resolver los problemas.

2. En el sistema de destino:
   a. Use el código clave de licencia para garantizar que se establezca una licencia correcta y suficiente en el sistema de destino.

      > **Nota**
      >
      > Para evitar errores en la promoción del contenido debido a una licencia insuficiente, use una licencia idéntica en ambos sistemas.

   b. Si usa una autentificación de terceros, deberá configurarla y habilitarla en el sistema de destino antes de promover el contenido.

      > **Nota**
      >
      > No asigne usuarios o grupos de usuarios. Conlleva la creación de usuarios o grupos de usuarios con CUIDs diferentes en el sistema de destino. El proceso de promoción usa CUIDs para identificar y asignar objetos entre el sistema de origen y destino. Los usuarios de asignación y grupos de usuarios provocarán inconsistencias de contenido y errores en la promoción.

   c. Asegúrese de que todos los complementos necesarios en el sistema de origen también estén instalados en el sistema de destino.

      > **Nota**
      >
      > Para garantizar el éxito de la migración, deberá instalar add-ons como Análisis o Design Studio en el sistema de origen.

   d. Si tiene un contenido que utiliza conexiones QaaWS, deberá habilitar sustituciones que garanticen que dichas conexiones señalen a los servicios Web correctos. Para más información sobre la configuración de sustituciones, consulte la sección «Sustituciones».
   e. Si debe migrar todas las instancias planificadas concluidas, haga clic en *Mostrar instancias concluidas en la página Administrar dependencias* en *Configuración de tarea* de la administración de promociones.
3. En el sistema central:
   a. Puede designar el sistema de origen, el sistema de destino o un sistema separado como el sistema central donde se ejecutan las tareas de administración de promociones. Si promueve un repositorio

completo, controlará un gran volumen de contenido que requerirá recursos de sistema adicionales en el sistema central. Use la referencia de tamaño siguiente para configurar el sistema central para 10.000 objetos:

| | Asignación de espacio temporal | Asignación de memoria | Configuración adicional |
|---|---|---|---|
| `LCM_CLI` | 2 GB | 2 GB | Actualizar `LCM_CLI.bat` y modificar el parámetro `-Xmx`. |
| Servidor de tareas de administración de promociones | 3 GB | 3 GB | En CMC, actualice la propiedad de inicio del servidor de tareas de administración de promociones agregando el parámetro `-javaargs Xmx3g`. Para obtener más información, consulte la Nota SAP 2286419. |

Por ejemplo, si estima que la tarea contiene 50.000 objetos:

- Asigne 10 GB de memoria a `LCM_CLI` (50.000 ÷ 10.000 × 2)
- Asigne 15 GB de memoria al servidor de tareas (50.000 ÷ 10.000 × 3)

> **Nota**
>
> Estas líneas guía de tamaño se aplican a la mayoría de entornos. Sin embargo, el tamaño de los documentos puede afectar a los requisitos de los recursos.

## 16.4.2 Estrategias de migración

- Utilice la interfase de línea de comando (ILC) en vez de la herramienta CMC de Web para todas las promociones de job.
  - La ILC ignora el límite de sesión Web de veinte minutos que se aplica durante un job de promoción que incluye más de 1000 objetos.

    > **Nota**
    >
    > El límite de objeto depende de suficientes recursos de sistema.

  - La ILC ofrece control granular sobre la promoción de contenidos utilizando el idioma de consulta para seleccionar el contenido que debe migrarse. Puede seleccionar contenido del mismo tipo o contenido ubicado en el mismo directorio.
  - LA ILC puede ejecutarse en lotes y los jobs de promoción pueden iniciarse mediante otras herramientas de scripts.
- Establezca seguridad promocionando primero los principales (usuarios y grupos de usuarios).
  - Al promocionar primero los usuarios y grupos de usuarios, se garantiza el modelo de seguridad en el sistema destino y también el éxito de la migración subsiguiente del contenido personal de los usuarios (como bandejas de entrada, vaforitos y categorías personales).

> **Nota**
>
> Es importante que realice primero esta tarea para que los CUID de los usuarios y grupos de usuarios del sistema destino sean idénticos a los del sistema fuente.

- Desactive el cálculo de dependencia.
  - El cálculo de dependencia es una de las tareas más intensivas en el proceso de creación de jobs. Durante la migración total del repository, todos los objetos se migran, de modo que el cálculo es innecesario.

    > **Nota**
    >
    > Esta función es útil sólo si no está seguro de qué objetos dependientes son necesarios.

- Evite incluir el cálculo de seguridad siempre que sea posible.
  - El cálculo de seguridad es la segunda tarea más intensiva en el proceso de creación de jobs. Divida la promoción en dos jobs si tiene demasiados documentos en diferentes directorios y la seguridad sólo está establecida en los directorios. El primer job debería contener sólo objetos con la seguridad activada y el segudo job debería contener sólo documentos con la seguridad desactivada. De esta manera, sólo puede realizar cálculos de seguridad en los directorios y se evita así el cálculo de seguridad de todos los documentos.

    > **Nota**
    >
    > La seguridad de objeto se mantiene porque se hereda de la seguridad de carpeta.

## 16.5 Pasos de la promoción del sistema completo

La promoción del sistema completo requiere la ejecución de tres tareas de promoción independientes por orden, cada una de ellas para promocionar tipos de contenido específicos. Para obtener más información sobre cómo promocionar varios objetos, consulte el artículo de la base de conocimientos 1969259.

La siguiente tabla resume los tipos de contenido y la configuración de los parámetros para cada tarea de promoción.

| Tarea de promoción | Tipo de contenido | `exportDependencies` | `includeSecurity` |
|---|---|---|---|
| 1 | Todos los usuarios y grupos de usuarios | falso | verdadero |
| 2 | Todos los objetos dependientes | falso | verdadero |
| 3 | Todos los objetos principales | falso | verdadero |

Utilice la interfaz de la línea de comandos (CLI) para crear y ejecutar cada tarea. Para obtener más información de CLI, consulte la sección Usar la opción Línea de comandos [página 635].

### Parámetros comunes

Utilice los siguientes parámetros para las tres tareas de promoción:

> → Recuerde
>
> Asegúrese de que cada parámetro esté en una nueva línea.

```
action=promote
Source_CMS=<SourceSystem>
Source_userName=Administrator
Source_password=<AdministratorPassword>
LCM_CMS=<NameOfCentralSystem>
LCM_userName=Administrator
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```

## 16.5.1 Promover usuarios y grupos de usuarios (tarea 1)

Para establecer modelos de seguridad idénticos entre el sistema de origen y de destino y para garantizar que los CUIDs de objeto de usuario y grupos de usuarios son idénticos, promueva primero los usuarios y los grupos de usuarios.

1. Cree un archivo `usersandgroups.properties` con los parámetros comunes y anexe los parámetros siguientes al archivo para seleccionar todos los usuarios y grupos de usuarios:

   ```
   exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
   SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
   (SI_KIND='User' OR SI_KIND='UserGroup') AND NOT (SI_ID in (11,12, 501, 1, 2,
   3))
   ```

2. Para ejecutar la tarea, navegue al directorio `<INSTALLDIR>\win64x64\scripts` y ejecute el comando siguiente:

   ```
   Lcm_cli.bat –lcmproperties=usersandgroups.properties
   ```

## 16.5.2 Promover objetos dependientes (tarea 2)

Los objetos dependientes dependen de los objetos principales en la carpeta Público y en la carpeta Favoritos de los usuarios. Para eliminar la necesidad de establecer `includeDependencies` a `true` para todas las demás tareas, promueva en segundo lugar los objetos dependientes. Los objetos siguientes son dependientes:

- Niveles de acceso
- Aplicaciones

- Vistas empresariales
- Calendarios
- Categorías
- Conexiones
- Eventos
- Conexiones OLAP
- Perfiles
- Proyectos
- QaaWS
- Conexiones remotas
- Listas de réplicas
- Grupos de servidores
- Universos

1. Cree el archivo dependencies.properties con los parámetros comunes y anexe los parámetros siguientes al archivo para seleccionar todos los objetos dependientes:

```
#total number of queries (if > 1)
exportQueriesTotal=12
#Projects, Universes, Connections, OLAP Connects: SI_ID=95
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (95)")
#QaaWS: SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'
#-need to ensure Overrides are scanned at the source, promoted to the target
and set to active
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'")
#Events: SI_ID=21
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (21)") and
si_specific_kind != 'MON.MonitoringEvent'
#Calendars: SI_ID=22
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (22)")
#Categories: SI_ID=45
exportQuery5=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID IN (45)")
#Access Levels: SI_ID=57
exportQuery6=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (57)")
#Server Groups: SI_ID=17
exportQuery7=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (17)")
#Profiles: SI_ID=50
exportQuery8=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (50)")
#Applications: SI_ID=99
exportQuery9=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (99)")
#Remote Connections:  SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'
```

```
exportQuery10=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS
WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID =
'AVwSekNrtFxGqJ6Jp2rLwrI'")
#Replication Lists:  SI_CUID = 'ASOr8wap3MJOgdWV5HLcZ1M'
exportQuery11=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='ASOr8wap3MJOgdWV5HLcZ1M'")
#BusinessViews: SI_ID=98
exportQuery12=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (98)")
```

2. Para ejecutar la tarea, navegue al directorio `<INSTALLDIR>\win64x64\scripts` y ejecute el comando siguiente:

```
Lcm_cli.bat –lcmproperties=dependencies.properties
```

## 16.5.3 Promover objetos principales (tarea 3)

Los objetos principales son documentos de BI principales que se encuentran el la carpeta Público y en la carpeta Favoritos de los usuarios. Si partimos de la base de que ya se ha ejecutado la segunda tarea de promoción, la migración de todos los objetos dependientes y por último la promoción de los objetos principales vuelve a establecer las relaciones con los objetos dependientes.

1. Cree un archivo `primaryobjects.properties` con los parámetros comunes y anexe los parámetros siguientes al archivo para seleccionar todos los usuarios y grupos de usuarios:

```
#total number of queries (if > 1)
exportQueriesTotal=4
#All Public Folders
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)")
#All user collaterals (Inbox, FavoriteFolder, PersonalCategory)
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='Inbox')")
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='FavoritesFolder')")
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```

   Si vuelve a ejecutar el mismo job, excluya el job LCM mediante la siguiente consulta:

```
SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") and SI_KIND not in
('LCMJob')
```

2. Para ejecutar la tarea, navegue al directorio `<INSTALLDIR>\win64x64\scripts` y ejecute el comando siguiente:

```
Lcm_cli.bat –lcmproperties=primaryobjects.properties
```

> **Nota**
>
> Si hay más de 50.000 objetos en la carpeta Público o en la carpeta Favoritos de los usuarios, quizá sea necesario dividir esta última tarea en tareas más pequeñas.

> **Nota**
>
> Asegúrese de que los equipos que ejecuten el comando de la interfaz de la línea de comandos y el servidor de tareas de gestión de promociones cumplan los requisitos de tamaño. Para obtener más información, consulte la sección «Tamaño».

### 16.5.4 Después de promoción

La gestión de promociones sólo promociona los grupos de servidores, no sus servidores. Para garantizar que los informes con servidores asignados siguen funcionando, deberá volver a crear y asignar los servidores a los grupos de servidores correctos.

## 16.6 Usar la opción Línea de comandos

La opción Línea de comandos de la herramienta de administración de promociones permite promover objetos de un despliegue de la plataforma de BI a otro. Puede crear una secuencia de comandos de lote para varias tareas.

> **→ Sugerencias**
>
> Use la opción de Línea de comandos para tareas que contienen un gran número de objetos.

La herramienta de administración de promociones admite los siguientes tipos de promoción de tareas a través de la línea de comandos:

- Exportar una plantilla de tarea de promoción existente a LCMBIAR con cifrado de contraseña.
- Exportar una plantilla de tarea de promoción existente a LCMBIAR sin cifrado de contraseña.
- Exportar una o varias consultas de plataforma
- Promocionar varias consultas de plataforma
- Promover con una plantilla de trabajo existente
- Importar y promover un archivo LCMBIAR existente
- Llevar a cabo una promoción Live a Live

### 16.6.1 Para ejecutar la línea de comandos en Windows

Para ejecutar la herramienta de línea de comandos, siga los siguientes pasos:

1. Inicie la ventana o el shell de línea de comandos.
2. Desplácese al directorio adecuado.

   Por ejemplo, la ruta de directorio para Windows es: `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`
3. Realice una de las siguientes acciones:
   - Ejecute LCMCLI, asegúrese de que la ruta java está establecida antes de ejecutar el programa. Comando: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <archivo de propiedades>`
   - Ejecute el archivo BAT desde `C:\Archivos de programa (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat` Comando: `lcm_cli.bat -lcmproperty <archivo de propiedades>`

     > **Nota**
     >
     > Introduzca las contraseñas válidas cuando se le solicite.

La herramienta de línea de comandos de administración de promociones toma un archivo de `<propiedades>` como parámetro. El archivo de `<propiedades>` contiene los parámetros necesarios para comunicar la herramienta de gestión de promociones acerca de las acciones para realizar, la conexión a qué despliegue de la plataforma SAP BusinessObjects Business Intelligence, los métodos de conexión, los objetos para promover.

El archivo debe tener la forma de `<NOMBRE DE ARCHIVO>.properties`

Por ejemplo: `<Myproperties.properties>`

## 16.6.2 Ejecutar la línea de comandos en Unix

Para ejecutar la herramienta de línea de comandos, siga los siguientes pasos:

1. Ejecute el shell.
2. Desplácese al directorio adecuado.

   Por ejemplo, `/usr/u/qaunix/Aurora604/sap_bobj/enterprise_xi40/java/lib`
3. Realice una de las siguientes acciones:
   - Ejecute LCMCLI, asegúrese de que la ruta java está establecida antes de ejecutar el programa. Comando: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <archivo de propiedades>`
   - Ejecute el archivo BAT desde `<ruta_directorio_instalación>\sap_bobj\lcm_cli.sh` Comando: `lcm_cli.sh -lcmproperty <archivo de propiedades>`

> **Nota**
>
> Introduzca las contraseñas válidas cuando se le solicite.

## 16.6.3 Parámetros de la herramienta de línea de comandos

Los parámetros de la opción de línea de comandos de la herramienta de gestión de promociones se organizan según los tres tipos de promoción principales:

- Promover objetos desde un fichero LCMBIAR a un CMS live
- Promover objetos dede un CMS live de origen a un CMS live de destino
- Exportar objetos desde un CMS live a un fichero LCMBIAR.

Además de los parámetros afectados por estos tres tipos de promoción, también hay parámetros para los comandos generales que pueden utilizarse en todos los escenarios de promoción.

> → Recuerde
>
> No coloque parámetros de la línea de comandos entre comillas.

> ⓘ Nota
>
> - Parecida a la creación de una tarea antes de la exportación, la opción Línea de comandos crea una tarea temporal rápidamente. Este nombre de trabajo puede ser una combinación de `Query_<USUARIO>_<fecha y hora>`. Este es específico sólo para `<exportQuery>`.
> - Solo puede restaurar la tarea a través de la herramienta de administración de promociones. No existe soporte de la línea de comandos para restaurar los trabajos.
> - Al trabajar con un garn número de objetos, se recomienda aumentar el tamaño heap Java máximo estableciendo el parámetro `-Xmx=8g` en la secuencia de comandos `LCMCLI`.

### Información relacionada

Fichero LCMBIAR para un CMS live [página 641]
CMS live de origen a CMS live de destino [página 647]
CMS live a fichero LCMBIAR [página 644]
Lista de todos los parámetros de líneas de comando [página 651]

## 16.6.3.1 Parámetros de línea de comandos por escenario de promoción

Los parámetros de línea de comandos se presentan en el orden recomendado para cada escenario de promoción. La tabla indica todos los parámetros disponibles y su status como obligatorios u opcionales para cada escenario de promoción. Cada parámetro obligatorio se describe para cada escenario de promoción correspondiente. Los parámetros opcionales se describen en la sección Lista de parámetros de línea de comandos. Consulte los Enlaces relacionados para obtener infromación de parámetros por escenario y los parámetros adicionales disponibles.

| Grupo de parámetros | Parámetro | LCMBIAR a Live | Live a LCMBIAR | Live a Live | Rollback |
|---|---|---|---|---|---|
| *Archivo de propiedades* | `lcmproperty` | Opcional | Recomendado | Recomendado | Recomendado |
| *Tipo de acción* | `action` | Obligatorio<br>action=promote | Obligatorio<br>action=export | Obligatorio<br>action=promote | Obligatorio<br>action=rollback |
| *Nodo LCM* | `LCM_CMS` | Obligatorio | | | |
| | `LCM_userName` | Obligatorio | | | |
| | `LCM_Password` | Obligatorio<br>Si está vacía, será necesaria en la consola. | | | |
| | `LCM_authentication` | Opcional: Predeterminado = `secEnterprise` | | | |
| | `LCM_SystemID` | Obligatorio para la autenticación SAP | | | |
| | `LCM_ClientID` | Obligatorio para la autenticación SAP | | | |
| *Origen (live o LCMBIAR)* | `importLocation` | Obligatorio | No aplicable | No aplicable | No aplicable |
| | `lcmbiarpassword` | Obligatorio (puede estar vacío) | No aplicable | No aplicable | No aplicable |
| | `Source_CMS` | No aplicable | Obligatorio | Obligatorio | No aplicable |
| | `Source_UserName` | No aplicable | Obligatorio | Obligatorio | No aplicable |
| | `Source_password` | No aplicable | Obligatorio<br>Si está vacía, será necesaria en la consola. | Obligatorio<br>Si está vacía, será necesaria en la consola. | No aplicable |
| | `Source_authentication` | No aplicable | Opcional<br>Predeterminado = `secEnterprise` | Opcional<br>Predeterminado = `secEnterprise` | No aplicable |
| | `Source_systemID` | No aplicable | Obligatorio para la autenticación SAP | Obligatorio para la autenticación SAP | No aplicable |

| Grupo de parámetros | Parámetro | LCMBIAR a Live | Live a LCMBIAR | Live a Live | Rollback |
|---|---|---|---|---|---|
| | `Source_clientID` | No aplicable | Obligatorio para la autenticación SAP | Obligatorio para la autenticación SAP | No aplicable |
| *Destino (Live o LCMBIAR)* | `Destination_CMS` | Obligatorio | No aplicable | Obligatorio | No aplicable |
| | `Destination_username` | Obligatorio | No aplicable | Obligatorio | No aplicable |
| | `Destination_password` | Obligatorio | No aplicable | Obligatorio | No aplicable |
| | `Destination_authentication` | Opcional<br>Predeterminado = `secEnterprise` | No aplicable | Opcional<br>Predeterminado = `secEnterprise` | No aplicable |
| | `Destination_systemID` | Obligatorio para la autenticación SAP | No aplicable | Obligatorio para la autenticación SAP | No aplicable |
| | `Destination_clientID` | Obligatorio para la autenticación SAP | No aplicable | Obligatorio para la autenticación SAP | No aplicable |
| | `ExportLocation` | No aplicable | Obligatorio | No aplicable | No aplicable |
| | `lcmbiarpassword` | No aplicable | Obligatorio (puede estar vacío) | No aplicable | No aplicable |
| *Relacionado con job* | `JOB_CUID` | No aplicable | Opcional | Opcional | Obligatorio |
| | `Override` | Opcional | No aplicable | No aplicable | No aplicable |
| | `forceOverride`<br>Disponible en SP4 | Opcional | No aplicable | No aplicable | No aplicable |
| | `Timeout`<br>Disponible en SP4 | Opcional | No aplicable | Opcional | No aplicable |
| *Relacionado con exportación* | `ExportDependencies` | No aplicable | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | No aplicable |
| | `ExportQuery` | No aplicable | Obligatorio | Obligatorio | No aplicable |

| Grupo de parámetros | Parámetro | LCMBIAR a Live | Live a LCMBIAR | Live a Live | Rollback |
|---|---|---|---|---|---|
| | `ExportQueriesTotal` | No aplicable | Opcional: Utilizar cuando tenga más de una consulta de exportación | Opcional: Utilizar cuando tenga más de una consulta de exportación | No aplicable |
| | `BatchJobQuery` | No aplicable | Opcional: Utilizar con consulta de exportación | Opcional: Utilizar con consulta de exportación | No aplicable |
| | `LimitQueryBatchSize` | No aplicable | Opcional | Opcional | No aplicable |
| *Relacionado con log* | `Consolelog` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | No aplicable |
| | `ResultFileName` | Opcional | Opcional | Opcional | No aplicable |
| | `LogFileName`<br>Disponible en SP4 | Opcional | Opcional | Opcional | No aplicable |
| *Selección de objetos* | `Selected_CUIDS` | Opcional | No aplicable | No aplicable | No aplicable |
| | `selectUser`<br>Disponible en SP4 | No aplicable | Opcional<br>Predeterminado =`All` | Opcional<br>Predeterminado =`All` | No aplicable |
| | `selectGroup`<br>Disponible en SP4 | No aplicable | Opcional<br>Predeterminado =`All` | Opcional<br>Predeterminado =`All` | No aplicable |
| *Seguridad* | `IncludeApplicationSecurity` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | No aplicable |
| | `IncludeSecurity` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | No aplicable |
| | `IncludeTopLevelSecurity` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | No aplicable |

| Grupo de parámetros | Parámetro | LCMBIAR a Live | Live a LCMBIAR | Live a Live | Rollback |
|---|---|---|---|---|---|
| *Comentarios* | `IncludeComments` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | Opcional<br>Predeterminado = `False` | No aplicable |
| *Tareas de federación* | `IncludeFederationJobsRelationship` | Opcional<br>Predeterminado = `True` | No aplicable | Opcional<br>Predeterminado = `True` | No aplicable |

## Información relacionada

Fichero LCMBIAR para un CMS live [página 641]
CMS live a fichero LCMBIAR [página 644]
CMS live de origen a CMS live de destino [página 647]
Lista de todos los parámetros de líneas de comando [página 651]

# 16.6.3.2 Fichero LCMBIAR para un CMS live

Al promover objetos desde un fichero LCMBIAR a CMS live, se hace referencia a un fichero de propiedades de la línea de comando que especifica una orden de promoción de la siguiente manera:

- Ubicación de importación y tipo de acción de promoción.
- Credenciales de inicio de sesión en el CMS que ejerce de host de la herramienta de gestión de promociones (llamada previamente herramienta de gestión de ciclo de vida LCM).
- Credenciales de inicio de sesión en el CMS de destino.
- Otros parámetros son necesarios para promocionar el CMS correctamente, por ejemplo, la contraseña LCMBIAR o sustituir la parametrización de objetos existentes si es necesario.

Puede incluir otros parámetros opcionales que pueden especificar necesidades de promoción concretas. Estos parámetros opcionales se describen en la sección Lista de todos los parámetros de líneas de comando [página 651].

El siguiente ejemplo muestra un caso para un fichero LCMBIAR de promoción a CMS live sin usar un fichero de las propiedades en la línea de comandos:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -action promote -LCM_CMS myCMS.mydomain.sap:6400 -LCM_userName
adminLCM -LCM_password my_adminpassword1 -
Destination_CMS myCMS.mydomain.sap:6400 -Destination_userName adminLCM
-Destination_password my_adminpassword1 -
importLocation "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\Samples\webi\WebISamples.lcmbiar" -
```

```
lcmbiarpassword
```

El siguiente ejemplo muestra un caso para un fichero LCMBIAR de promoción a CMS live con un fichero de las propiedades en la línea de comandos:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
LCM command line property file
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
importLocation=C:\Backup\CR.lcmbiar
lcmbiarpassword=validlcmbiarpassword
#
Destination_CMS=myCMS.mydomain.sap:6400
Destination_userName=adminLCM
Destination_password=my_adminpassword1
#
```

La siguiente tabla enumera los parámetros obligatorios necesarios para un fichero de propiedades correcto para un fichero LCMBIAR de promoción a un CMS live:

| Grupo de parámetros | Parámetro | Descripción |
|---|---|---|
| *Tipo de acción* | `action` | Operación que debe ejecutar el CLI.<br>Valor: exportar<br>Ejemplo: `action=export` |
| *Nodo LCM* | `LCM_CMS` | CMS para la herramienta de administración de promociones.<br>Valor: Libre de texto<br>Ejemplo: `LCM_CMS=myCMS.mydomain.sap:6400` |
| | `LCM_userName` | Nombre de usuario de cuenta que la herramienta debe utilizar para conectarse con el CMS herramienta de gestión de promociones<br>Valor: Libre de texto<br>Ejemplo: `LCM_userName=adminLCM` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `LCM_password` | Contraseña de la cuenta de usuario.<br>Valor: Libre de texto<br>Ejemplo: `LCM_password=my_adminpassword1` |
| *Fuente: Fichero LCMBIAR* | `importLocation` | Ubicación del fichero LCMBIAR que contiene los objetos que deben promoverse.<br>Valor: Libre de texto. Debe tener la extensión `<.lcmbiar>`<br>Ejemplo: `importLocation=C:\Backup\New.lcmbiar` |
| | `lcmbiarpassword` | Permite la encriptación y desencriptación de ficheros BIAR utilizando una contraseña.<br>Valor: Libre de texto<br>Ejemplo: `lcmbiar=validlcmbiarpassword` |
| *Destino: Live CMS* | `Destination_CMS` | CMS al que debe conectarse la herramienta.<br>Valor: Nombre CMS válido<br>Ejemplo: `Destination_CMS=myCMS.mydomain.sap:6400` |
| | `Destination_username` | Cuenta de usuario que la herramienta debe utilizar para conectarse al CMS de plataforma de BI.<br>Valor: Nombre de usuario válido<br>Ejemplo: `Destination_username=adminLCM` |

| Grupo de parámetros | Parámetro | Descripción |
|---|---|---|
| | `Destination_password` | Contraseña asociada para la cuenta de usuario.<br>Valor: Contraseña válida<br>Ejemplo: `Destination_password=my_adminpassword1` |

## Información relacionada

CMS live a fichero LCMBIAR [página 644]
CMS live de origen a CMS live de destino [página 647]
Lista de todos los parámetros de líneas de comando [página 651]

# 16.6.3.3 CMS live a fichero LCMBIAR

Al promover objetos desde un CMS live de origen a un fichero LCMBIAR, se hace referencia a un fichero de propiedades de la línea de comando que especifica una orden de promoción de la siguiente manera:

- Tipo de acción de promoción: exportar
- Credenciales de inicio de sesión en el CMS que ejerce de host de la herramienta de gestión de promociones (llamada previamente herramienta de gestión de ciclo de vida LCM).
- Credenciales de inicio de sesión en el CMS de origen.
- Directorio de destino para el fichero LCMBIAR.
- Otros parámetros necesarios para promover correctamente el CMS, por ejemplo, la contraseña LCMBIAR o parametrizaciones de seguridad.

Puede incluir otros parámetros opcionales que pueden especificar necesidades de promoción concretas. Estos parámetros opcionales se describen en la sección Lista de todos los parámetros de líneas de comando [página 651].

El siguiente ejemplo muestra un fichero de propiedades típico para un CMS de origen de promoción a un fichero LCMBIAR:

```
Go to
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\win64_x64\scripts>
Type
lcm_cli.bat -lcmproperty C:\LCMTEST\MyPropertyFile.properties
#
#action=export
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
```

```
#
Source_CMS=myCMS.mydomain.sap:6400
Source_userName=adminLCM
Source_password=my_adminpassword1
#
exportLocation=E:\LCMTEST\
lcmbiarpassword=
#
#Queries
#
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM
CI_INFOOBJECTS, CI_APPOBJECTS, CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID in (23)")
#
#When applicable...
#
exportDependencies=true
includeSecurity=true
#
#Options
#
consolelog=true
```

La siguiente tabla enumera los parámetros obligatorios necesarios para un fichero de propiedades correcto para un fichero LCMBIAR de promoción a un CMS live:

| Grupo de parámetros | Parámetro | Descripción |
|---|---|---|
| *Tipo de acción* | `action` | Operación que debe ejecutar el CLI.<br>Valor: exportar<br>Ejemplo: `action=export` |
| *Nodo LCM* | `LCM_CMS` | CMS para la herramienta de administración de promociones.<br>Valor: Libre de texto<br>Ejemplo: `LCM_CMS=myCMS.mydomain.sap:6400` |
| | `LCM_userName` | Nombre de usuario de cuenta que la herramienta debe utilizar para conectarse con el CMS herramienta de gestión de promociones<br>Valor: Libre de texto<br>Ejemplo: `LCM_userName=adminLCM` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `LCM_password` | Contraseña de la cuenta de usuario.<br>Valor: Libre de texto<br>Ejemplo:<br>`LCM_password=my_adminpassword1` |
| *Fuente: Live CMS* | `Source_CMS` | CMS al que debe conectarse la herramienta de gestión de promociones.<br>Valor: Libre de texto<br>Ejemplo:<br>`Source_CMS=myCMS.mydomain.sap:6400` |
| | `Source_userName` | Cuenta de usuario que debe utilizar la herramienta de gestión de promociones para conectarse a la plataforma de BI CMS.<br>Valor: Libre de texto<br>Ejemplo:<br>`Source_username=adminLCM` |
| | `Source_password` | Contraseña de la cuenta de usuario.<br>Valor: Libre de texto<br>Ejemplo:<br>`Source_password=my_adminpassword1` |
| *Destino: Fichero LCMBIAR* | `exportLocation` | Especifica la ubicación para colocar el fichero LCMBIAR después de exportar y embalar los objetos .<br>Valor: Libre de texto. Debe tener la extensión `<.lcmbiar>`<br>Ejemplo:<br>`exportLocation=C:\Backup\New.lcmbiar` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `lcmbiarpassword` | Permite la encriptación y desencriptación de ficheros BIAR utilizando una contraseña.<br>Valor: Libre de texto<br>Ejemplo: `lcmbiarpassword=validlcmbiarpassword` |
| *Relacionado con exportación* | `exportQuery` | Consulta al CMS de origen para que obtenga los objetos necesarios para exportar al fichero LCMBIAR.<br>Valor: Libre de texto. Utilice el formato de idioma de query CMS.<br>Ejemplo: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'`<br>**Nota**<br>Puede tener cualquier número de consultas en un archivo de propiedades, pero se deben denominar como exportQuery1, exportQuery2. |

## Información relacionada

Fichero LCMBIAR para un CMS live [página 641]
CMS live de origen a CMS live de destino [página 647]
Lista de todos los parámetros de líneas de comando [página 651]

# 16.6.3.4 CMS live de origen a CMS live de destino

Al promover objetos desde un CMS live de origen a uno de destino, se hace referencia a un archivo de propiedades de la línea de comando que especifica una orden de promoción de la siguiente manera:

- Tipo de acción de promoción: Promoción
- Credenciales de inicio de sesión en el CMS que ejerce de host de la herramienta de gestión de promociones (llamada previamente herramienta de gestión de ciclo de vida LCM).
- Credenciales de inicio de sesión en el CMS de origen.
- Credenciales de inicio de sesión en el CMS de destino.
- Otros parámetros necesarios para promover correctamente el CMS, por ejemplo, parámetros de seguridad o de dependencias.

Puede incluir otros parámetros opcionales que pueden especificar necesidades de promoción concretas. Estos parámetros opcionales se describen en la sección Lista de todos los parámetros de líneas de comando [página 651].

El siguiente ejemplo muestra un fichero de propiedades típico para un CMS de origen de promoción a un CMS de destino:

```
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
#
Source_CMS=myCMS1:myCMS2
Source_userName=adminLCM
Source_password=my_adminpassword1
Source_authentication=secEnterprise
#
Destination_CMS=myCMS1:myCMS2
Destination_userName=adminLCM
Destination_password=my_adminpassword1
Destination_authentication=secEnterprise
#
exportQuery1select*from CI_INFOOBJECTS where SI_NAME='Charting Samples' and
SI_KIND='Webi'
#
includeSecurity=false
#
exportDependencies=false
#
```

La siguiente tabla enumera los parámetros obligatorios necesarios para un fichero de propiedades correcto para un CMS de origen de promoción a un CMS de destino:

| Grupo de parámetros | Parámetro | Descripción |
|---|---|---|
| *Tipo de acción* | `action` | Operación que la línea de comando debe realizar.<br>Valor: Promover<br>Ejemplo: `action=promote` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| *Nodo LCM* | `LCM_CMS` | CMS para la herramienta de administración de promociones.<br>Valor: Libre de texto<br>Ejemplo: `LCM_CMS=myCMS.mydomain.sap:6400` |
| | `LCM_userName` | Nombre de usuario de cuenta que la herramienta debe utilizar para conectarse con el CMS herramienta de gestión de promociones<br>Valor: Libre de texto<br>Ejemplo: `LCM_userName=adminLCM` |
| | `LCM_password` | Contraseña de la cuenta de usuario.<br>Valor: Libre de texto<br>Ejemplo: `LCM_password=my_adminpassword1` |
| *Fuente: Live CMS* | `source_CMS` | CMS al que debe conectarse la herramienta de gestión de promociones.<br>Valor: Libre de texto<br>Ejemplo: `Source_CMS=myCMS.mydomain.sap:6400` |
| | `Source_username` | Cuenta de usuario que debe utilizar la herramienta de gestión de promociones para conectarse a la plataforma de BI CMS.<br>Valor: Libre de texto<br>Ejemplo: `Source_username=adminLCM` |
| | `Source_password` | Contraseña de la cuenta de usuario.<br>Valor: Libre de texto<br>Ejemplo: `Source_password=my_adminpassword1` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| *Destino: Live CMS* | `Destination_CMS` | CMS al que debe conectarse la herramienta.<br>Valor: Libre de texto<br>Ejemplo: `Destination_CMS=myCMS1:myCMS2` |
| | `Destination_username` | Cuenta de usuario que la herramienta debe utilizar para conectarse al CMS de plataforma de BI.<br>Valor: Libre de texto<br>Ejemplo: `Destination_username=adminLCM` |
| | `Destination_password` | Contraseña asociada para la cuenta de usuario.<br>Valor: Libre de texto<br>Ejemplo: `Destination_password=my_adminpassword1` |
| *Relacionado con exportación* | `exportQuery` | Queries que ejecuta la herramienta LCM para obtener los objetos necesarios para exportar al CMS destino.<br>Valor: Libre de texto. Utilice el formato de idioma de query CMS.<br>Ejemplo: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'`<br>**Nota**<br>Puede tener cualquier número de consultas en un archivo de propiedades, pero se deben denominar como exportQuery1, exportQuery2. |

## Información relacionada

Fichero LCMBIAR para un CMS live [página 641]
CMS live a fichero LCMBIAR [página 644]
Lista de todos los parámetros de líneas de comando [página 651]

# 16.6.3.5 Lista de todos los parámetros de líneas de comando

La siguiente tabla describe todos los parámetros de líneas de comando.

> **Nota**
>
> Al ejecutar dentro de una línea de comando, los parámetros tienen esta sintaxis `-<parameterName><space><parameterValue>`. Dentro de un fichero de propiedades, los parámetros tienen esta sintaxis `<parameterName>=<parameterValue>`.

| Grupo de parámetros | Parámetro | Descripción |
|---|---|---|
| *Archivo de propiedades* | `lcmproperty` | Hace referencia a los valores necesarios para la ejecución de un comando, que se guardan en un archivo.<br>Valor: La ruta completa de la ubicación en la que se ha guardado el archivo de propiedad<br>Ejemplo: `-lcmproperty C:\MyPropertyFile.properties` |
| *Tipo de acción* | `action` | Operación que debe ejecutar el CLI.<br>Valor: Promorcionar o exportar<br>Ejemplo: `action=promote` |
| *Nodo LCM* | `LCM_CMS` | CMS para la herramienta de administración de promociones.<br>Valor: Libre de texto<br>Ejemplo: `LCM_CMS=myCMS.mydomain.sap:6400` |
| | `LCM_userName` | Nombre de usuario de cuenta que la herramienta debe utilizar para conectarse con la herramienta de gestión de promociones CMS.<br>Valor: Libre de texto<br>Ejemplo: `LCM_userName=adminLCM` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `LCM_Password` | Contraseña de la cuenta de usuario.<br>Si está vacia, será necesaria en la consola.<br>Valor: Libre de texto<br>Ejemplo: `LCM_password=my_adminpassword1` |
| | `LCM_authentication` | Indica el tipo de autenticación que se utilizará.<br>Valor: secEnterprise, secWinAD, secLDAP,secSAPR3. Si no se especifica, se utilizará `secEnterprise` .<br>Ejemplo: `LCM_authentication=secEnterprise` |
| | `LCM_systemID`<br>**Nota**<br>Obligatorio para la autenticación SAP. | Necesario solo para la autenticación SAP.<br>Valor: ID del sistema<br>Ejemplo: `LCM_systemID=systemID` |
| | `LCM_clientID`<br>**Nota**<br>Obligatorio para la autenticación SAP. | Necesario solo para la autenticación SAP.<br>Valor: ID de cliente<br>Ejemplo: `LCM_clientID=clientID` |
| *Fuente: Fichero LCMBIAR* | `importLocation` | Ubicación del fichero LCMBIAR que contiene los objetos que deben promoverse.<br>Valor: Libre de texto. Debe tener la extensión `<.lcmbiar>`<br>Ejemplo: `importLocation=C:\Backup\New.lcmbiar` |
| | `lcmbiarpassword` | Permite la encriptación y desencriptación de ficheros BIAR utilizando una contraseña.<br>Valor: Libre de texto<br>Ejemplo: `lcmbiar=validlcmbiarpassword` |
| *Fuente: Live CMS* | `Source_CMS` | CMS al que debe conectarse la herramienta de gestión de promociones.<br>Valor: Libre de texto<br>Ejemplo: `Source_CMS=myCMS.mydomain.sap:6400` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `Source_UserName` | Cuenta de usuario que debe utilizar la herramienta de gestión de promociones para conectarse a la plataforma de BI CMS.<br>Valor: Libre de texto<br>Ejemplo: `Source_username=adminLCM` |
| | `Source_password` | Contraseña de la cuenta de usuario.<br>Valor: Libre de texto<br>Ejemplo: `Source_password=my_adminpassword1` |
| | `Source_authentication` | Indica el tipo de autenticación que se utilizará.<br>Valor: secEnterprise, secWinAD, secLDAP,secSAPR3. Si no se especifica, se utilizará `secEnterprise` .<br>Ejemplo: `Source_authentication=secEnterprise` |
| | `Source_systemID`<br>**Nota**<br>Obligatorio para la autenticación SAP. | Necesario solo para la autenticación SAP.<br>Valor: ID del sistema<br>Ejemplo: `Source_systemID=systemID` |
| | `Source_clientID`<br>**Nota**<br>Obligatorio para la autenticación SAP. | Necesario solo para la autenticación SAP.<br>Valor: ID del sistema<br>Ejemplo: `Source_clientID=clientID` |
| *Destino: Fichero LCMBIAR* | `exportLocation` | Especifica la ubicación para colocar el fichero LCMBIAR después de exportar y embalar los objetos .<br>Valor: Libre de texto. Debe tener la extensión `<.lcmbiar>`<br>Ejemplo: `exportLocation=C:\Backup\New.lcmbiar` |
| | `lcmbiarpassword` | Permite la encriptación y desencriptación de ficheros BIAR utilizando una contraseña.<br>Valor: Libre de texto<br>Ejemplo: `lcmbiarpassword=validlcmbiarpassword` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| *Destino: Live CMS* | `Destination_CMS` | CMS al que debe conectarse la herramienta.<br>Valor: Nombre CMS válido<br>Ejemplo: `Destination_CMS=myCMS.mydomain.sap:6400` |
| | `Destination_username` | Cuenta de usuario que la herramienta debe utilizar para conectarse al CMS de plataforma de BI.<br>Valor: Nombre de usuario válido<br>Ejemplo: `Destination_username=adminLCM` |
| | `Destination_password` | Contraseña asociada para la cuenta de usuario.<br>Valor: Contraseña válida<br>Ejemplo: `Destination_password=my_adminpassword1` |
| | `Destination_authentication` | Indica el tipo de autenticación que se utilizará.<br>Valor: secEnterprise, secWinAD, secLDAP, secSAPR3. Si no se especifica, se utilizará `secEnterprise` .<br>Ejemplo: `Destination_authentication=secEnterprise` |
| | `Destination_systemID`<br>**Nota**<br>Obligatorio para la autenticación SAP. | Necesario solo para la autenticación SAP.<br>Valor: ID del sistema<br>Ejemplo: `Destination_systemID=systemID` |
| | `Destination_clientID`<br>**Nota**<br>Obligatorio para la autenticación SAP. | Necesario solo para la autenticación SAP.<br>Valor: ID de cliente<br>Ejemplo: `Destination_clientID=clientID` |
| *Relacionado con job* | `JOB_CUID` | Le da la instrucción a la herramienta de que exorte todos los objetos del job al fichero LCMBIAR.<br>Valor: El CUID del job de gestión grabado. |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `Override` | Se utiliza para promocionar selectivamente objetos de un fichero LCMBIAR.<br><br>Si es `true`: Permite al usuario sustituir un job existente.<br><br>Si es `false`: Permite al usuario crear un job nuevo con el nombre `<JOB_NAME>_<TIME_STAMP>` .<br><br>Valor: Verdadero o falso<br><br>Ejemplo: `Override=true` |
| | `forceOverride`<br><br>Disponible en SP4 | Se utiliza para sustituir un job con el mismo nombre pero no con el mismo CUID.<br><br>Valor: Verdadero o falso<br><br>Ejemplo: `forceOverride=true` |
| | `Timeout`<br><br>Disponible en SP4 | Fija un timeout para promocionar una acción.<br><br>Valor: Tiempo en segundos<br><br>Ejemplo: `timeout=30` |
| *Relacionado con exportación* | `ExportDependencies` | Especifica las dependencia de objeto que agrupa la herramienta para la exportación. Aplicable sólo se utiliza junto al flag `Source_CMS` .<br><br>Valor: Verdadero o falso. Si no se especifica, el valor por defecto es `false`.<br><br>Ejemplo: `ExportDependencies=false` |
| | `ExportQuery` | Queries que ejecuta la herramienta LCM para obtener los objetos necesarios para exportar al CMS destino.<br><br>Valor: Libre de texto. Utilice el formato de idioma de query CMS.<br><br>Ejemplo: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'`<br><br>**Nota**<br><br>Puede tener cualquier número de consultas en un archivo de propiedades, pero se deben denominar como exportQuery1, exportQuery2. |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `ExportQueriesTotal` | Se utiliza para especificar la cantidad de queries de exportación que deben ejecutarse. Si tiene x queries de exportación y desea ejecutarlas todas, debe establecer este valor de parámetro en x.<br><br>Valor: Número entero positivo. Si no se especifica, el valor estándar es 1.<br><br>Ejemplo: `ExportQuery1=<your sql statement>`<br>`ExportQuery2=<your sql statement>`<br>`ExportQueriesTotal=2` |
| | `BatchJobQuery` | Se utiliza junto a `ExportQuery`. Crea e inicia un job para cada línea devuelta por el query de job. Las queries de exportación de jobs pueden utilizar "reservas-espacio" que hacen referencia a propiedades creadas en el query de job. El formato reserva-espacio es $b:PPTY$, mientras que en el nombre de propiedad no influyen mayúsculas ni minúsculas. Los <PPTY> válidos son:- "cuid" - "name" - "id"<br><br>Un error se produce si un reserva-espacio no se reconoce o crea por el query de job.<br><br>Valor: Libre de texto<br><br>Ejemplo: `batchJobQuery=SELECT si_cuid,si_name FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") AND SI_KIND='Folder' AND SI_NAME LIKE '%sample%' and SI_PARENTID=0`<br><br>`exportQuery1= SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'" ,"SI_CUID='$b:CUID$'")` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `LimitQueryBatchSize` | Limita la cantidad de objetos devueltos a 1,000 por defecto. Si este parámetro se establece en false, se devuelven todos los objetos de consulta.<br><br>**Nota**<br>También puede establecer explícitamente el nuevo límite para el número de objetos devueltos por la consulta con `select TOP <number>`<br><br>Valor: Verdadero o falso. Si no se especifica, el valor por defecto es verdadero.<br><br>Ejemplo: `LimitQueryBatchSize=true` |
| *Relacionadon con log* | `consolelog` | Se utiliza para visualizar el log completo del comando ejecutado por el usuario en el log de comandos.<br><br>Valor: Verdadero o falso. Si no se especifica, el valor por defecto es `false`.<br><br>Ejemplo: `consolelog=true` |
| | `ResultFileName` | El nombre del fichero en el sistema de ficheros local cuando se utiliza el parámetro `consolelog` .<br><br>Valor: Ruta del archivo de resultados de job<br><br>Ejemplo: `ResultFileName=C:\Logs\ResultFile.txt` |
| | `LogFileName`<br><br>Disponible en SP4 | Permite al usuario especificar una ruta fija para utilizarla en el archivo de log.<br><br>Valor: Ruta del archivo de log<br><br>Ejemplo: `LogFileName=C:\Logs\LogFile.log` |
| *Selección de objetos* | `Selected_CUIDS` | Permite al usuario promocionar selectivamente objetos (reports,usuarios,universos etc.) junto con sus dependencias desde un fichero LCMBIAR en vez de promocionar el fichero entero.<br><br>Valor: CUIDs de objetos en el archivo LCMBIAR que se deben promover selectivamente |
| | `selectUser`<br><br>Disponible en SP4 | Filtros utilizados en función de la autenticación externa (LDAP, SAPR3, WindowsAD...).<br><br>Valor: Todos, ninguno, excluirTP o soloTP. Si no se especifica, el valor por defecto es `all`.<br><br>Ejemplo: `selectUser=excludeTP` |

| Grupo de parámetros | Parámetro | Descripción |
| --- | --- | --- |
| | `selectGroup`<br>Disponible en SP4 | Filtra grupos de usuarios en función a a la autenticación externa (LDAP, SAPR3, WindowsAD...).<br>Valor: Todos, ninguno, excluir TO o soloTP. Si no se especifica, el valor por defecto es `all`.<br>Ejemplo: `selectGroup=onlyTP` |
| *Seguridad* | `IncludeApplicationSecurity` | Le da la instrucción a la herramienta de exportar o importar la seguridad asociada con aplicaciones seleccionadas.<br>Valor: Verdadero o falso. Si no se especifica, el valor por defecto es `false`.<br>Ejemplo: `IncludeApplicationSecurity=true` |
| | `IncludeSecurity` | Le da la instrucción a la herramienta de exportar o importar la seguridad asociada con objetos y usuarios seleccionados Si se utilizan niveles de acceso, también se exportarán/importarán.<br>Valor: Verdadero o falso. Si no se especifica, el valor por defecto es `false`.<br>Ejemplo: `IncludeSecurity=true` |
| *Comentarios* | `IncludeComments` | Le da la instrucción a la herramienta de exportar o importar los comentarios asociados con objetos seleccionados<br>Valor: Verdadero o falso. Si no se especifica, el valor por defecto es `false`.<br>Ejemplo: `IncludeComments=true` |
| *Tareas de federación* | `IncludeFederationJobsRelationship` | Indica a la herramienta que mantenga la relación de tareas de federación (listas de réplicas y conexiones remotas). Si se establece en false, los objetos replicados se convertirán en regulares y se eliminará el indicador de federación. Esto puede ser útil si el objeto replicado es el único objeto disponible y el objeto de origen ya no está disponible.<br>Valor: Verdadero o falso. Si no se especifica, el valor por defecto es `true`.<br>Ejemplo: `IncludeFederationJobsRelationship=false` |

## 16.6.3.6 Rollback

Puede anular la tarea promovida en el sistema de destino a través de la herramienta *Gestión de promociones*.

Si ha promovido una tarea mediante la herramienta *Gestión de promociones*, por ejemplo, para actualizar BI 4.2 SP07 a BI 4.3, y si desea anular esta modificación más adelante, puede utilizar los parámetros de la línea de comandos definidos en Parámetros de línea de comandos por escenario de promoción [página 637] y ejecutar la operación de rollback.

Al ejecutar la operación de rollback, debe indicar un archivo de propiedades que especifique el pedido promocional como sigue:

- Tipo de acción de promoción: rollback
- Credenciales de inicio de sesión en el CMS que ejerce de host de la herramienta de gestión de promociones (llamada previamente herramienta de gestión de ciclo de vida LCM).
- Credenciales de inicio de sesión en el CMS de origen.
- Credenciales de inicio de sesión en el CMS de destino.
- Otros parámetros necesarios para promover correctamente el CMS, por ejemplo, parámetros de seguridad o de dependencias.

Puede incluir otros parámetros opcionales que pueden especificar necesidades de promoción concretas. Estos parámetros opcionales se describen en Lista de todos los parámetros de líneas de comando [página 651].

Consultar el archivo de propiedades de muestra siguiente para realizar una operación de rollback:

```
#
action=rollback
job_cuid=AWWxyVk5fkFKjtQnRAygAYg
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
```

> **Nota**
>
> Encontrará el `job_cuid` de una tarea promovida en *Inicio de la CMC* > *Gestión de promociones* > *Propiedades*.

La siguiente tabla enumera los parámetros obligatorios necesarios para un fichero de propiedades correcto para un fichero LCMBIAR de promoción a un CMS live:

| Grupo de parámetros | Parámetro | Descripción |
|---|---|---|
| *Tipo de acción* | `action` | Operación que debe ejecutar el CLI.<br>Valor: rollback<br>Ejemplo: `action=rollback` |

| Grupo de parámetros | Parámetro | Descripción |
|---|---|---|
| *Relacionado con la tarea* | `job_cuid` | Indica a la herramienta que debe exportar todos los objetos de la tarea al archivo LCMBIAR.<br>Valor: El CUID del job de gestión grabado.<br>Ejemplo: `job_cuid=AWWxyVk5fkFKjtQnRAygAYg` |
| *Nodo LCM* | `LCM_CMS` | CMS para la herramienta de administración de promociones.<br>Valor: Libre de texto<br>Ejemplo: `LCM_CMS=myCMS.mydomain.sap:6400` |
| | `LCM_userName` | Nombre de usuario de cuenta que la herramienta debe utilizar para conectarse con el CMS herramienta de gestión de promociones<br>Valor: Libre de texto<br>Ejemplo: `LCM_userName=adminLCM` |
| | `LCM_password` | Contraseña de la cuenta de usuario.<br>Valor: Libre de texto<br>Ejemplo: `LCM_password=my_adminpassword1` |
| | `LCM_authentication` | Tipo de autentificación para la cuenta de usuario<br>Valor: Tipo de autentificación<br>Ejemplo: `secEnterprise` |

## 16.6.4 Ejemplo de archivo de propiedades

A continuación, se presenta un archivo de `propiedades` de ejemplo:

## Ejemplo

```
importLocation=C:/Backup/CR.lcmbiar
action=promote
LCM_CMS=<nombre CMS:número de puerto>
LCM_userName=<nombre de usuario>
LCM_password=<contraseña>
LCM_authentication=<autenticación>
LCM_systemID=<ID>
LCM_clientID=<ID cliente>
Destination_CMS=<nombre CMS:número de puerto>
Destination_userName=<nombre de usuario>
Destination_password=<contraseña>
Destination_authentication=<autenticación>
Destination_systemID=<ID>
Destination_clientID=<ID cliente>
lcmbiarpassword=<contraseña>
```

> **Nota**
>
> Si el archivo de `propiedades` no dispone de información personal, la CLI del LCM solicitará lo mismo en la consola.

# 16.7 Usar el Sistema de transporte y cambio mejorado

El Sistema de transporte y cambio (CTS) organiza y adapta los proyectos de desarrollo en ABAP Workbench y, a continuación, transporta los cambios entre los sistemas SAP de la arquitectura del sistema. El Sistema de transporte y cambio mejorado (CTS+) es un complemento del CTS que promueve contenido que no es de ABAP entre repositorios que no son de ABAP habilitados para el CTS+.

Los InfoObjects de la plataforma de BI pueden usar contenido de SAP Business Warehouse como origen de datos. La integración de CTS+ con la herramienta de administración de promociones permite gestionar el repositorio de la plataforma de BI, de modo parecido al repositorio de SAP Business Warehouse (BW), mediante el uso de solicitudes de transporte del CTS para promover tareas. El CTS+ ofrece la opción de transportar objetos que no son de SAP dentro de una arquitectura de sistema. Por ejemplo, los objetos creados en el sistema de desarrollo se pueden adjuntar a una solicitud de transporte o reenviar a otros sistemas de la misma arquitectura.

Para obtener más información sobre el Sistema de transporte y cambio, consulte Change and Transport System - Overview (BC-CTS)

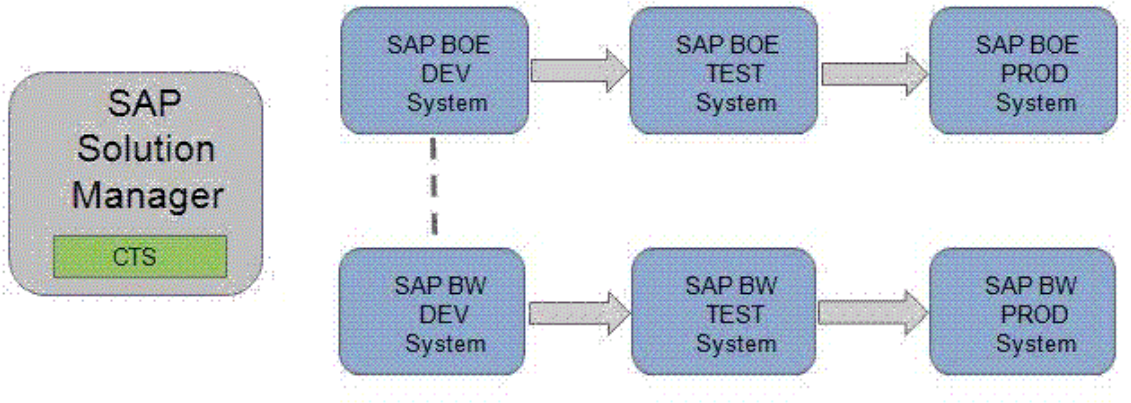
Para obtener más información sobre el CTS+ y transportes que no sean ABAP, consulte Transporting Non-ABAP Objects in Change and Transport System

## 16.7.1 Requisitos previos

A continuación se presentan los requisitos previos para transportar el contenido de Business Intelligence de un sistema a otro mediante CTS+:

1. Plataforma de BI 4.0 (o superior) está instalada.
2. SAP Solution Manager 7.1 o SAP Solution Manager 7.0 EHP1 (mínimo SP25) está instalado y se utiliza como controlador de dominio para CTS+, al menos para la configuración de sistemas SAP BusinessObjects.
   Para obtener más información sobre la configuración del dominio de transporte, consulte Configurar el dominio de transporte.
3. El complemento CTS está instalado en SAP Solution Manager (el complemento CTS se toma del conjunto de herramientas SL 1.0 SP02. Recomendamos el uso del último complemento CTS disponible).
   Para obtener más información sobre la instalación de complementos necesarios de CTS, consulte 1533059.
4. Los sistemas *SAP Business Warehouse 7.0* (SPS 24 o superior) están instalados. Para obtener más información, consulte 1369301.
5. La arquitectura de transporte de SAP Business Warehouse (SAP BW) está configurada en el Sistema de transporte y cambio (CTS).
6. 1692417 y 1860594 se han implementado en la máquina que aloja el servicio Web de despliegue.

## 16.7.2 Para configurar la plataforma de BI y de la integración CTS+




El Sistema de administración de transporte (TMS), que forma parte del Sistema de transporte y cambio, se utiliza para transportar cambios entre los sistemas SAP de una arquitectura. Gestiona los sistemas conectados, sus rutas y las importaciones en sus sistemas. Para obtener más información sobre el Sistema de administración de transporte, consulte Transport Management System (BC-CTS-TMS)

El CTS+ permite la recogida de archivos desde el exterior y su distribución en una arquitectura de transporte. La IU Web del Organizador de transporte, que forma parte del CTS+, administra las solicitudes de transporte y los objetos que contiene. Para obtener más información, consulte Transport Management System (BC-CTS-TMS)

Puede integrar la administración de promociones de la plataforma de BI con CTS+ y SAP BW con las solicitudes de transporte del CTS.

> **Nota**
>
> Para habilitar la integración de la plataforma de BI con SAP Solution Manager, tiene que definir el tipo de aplicación "BOLM" en la infraestructura de SAP Solution Manager.

Realice los pasos siguientes para integrar la plataforma de BI y CTS+:

1. Active el servicio web de exportación CTS.
2. Configure los ajustes de CTS en la herramienta de administración de promoción.
3. Configure el sistema de importación de la plataforma de BI en SAP Solution Manager.

## Información relacionada

Para activar el servicio Web de exportación CTS. [página 663]
Para configurar la configuración CTS+ en la herramienta de administración de promoción [página 664]
Para configurar la plataforma de BI y de la integración CTS+ [página 662]

# 16.7.2.1 Para activar el servicio Web de exportación CTS.

Para configurar la plataforma de BI, debe activar Servicio web de exportación CTS en la herramienta de administración web SOA.

1. Para iniciar la aplicación, introduzca el código de transacción SOAMANAGER en su SAP Solution Manager. Una vez que se ha realizado la autenticación necesaria, se abre la Consola de administración SOA en un explorador web.

   Para obtener más información sobre la administración SOA y la configuración de un punto final de servicio usando SAP Solution Manager 7.0, consulte Configurar un proveedor de servicios. Para SAP Solution Manager 7.1, consulte Configurar un proveedor de servicios.
2. En la ficha *Comunicación de escenarcio y aplicación* haga clic en *Configuración del servicio único*.

   El servicio web de exportación CTS se llama `EXPORT_CTS_WS`
3. En la ficha *Configuración*, cree o edite el punto final del servicio.
4. En la ficha *Seguridad*, configure el protocolo de transporte y el método de autenticación.
5. En la ficha *Ajustes de transporte*, defina la URL alternativa de acceso para un buen acceso al punto final del servicio.

## 16.7.2.2 Para configurar la configuración CTS+ en la herramienta de administración de promoción

En la siguiente sección se describen los pasos de configuración que se deben realizar en la CMC para configurar el CTS+ para su uso con la herramienta de administración de promociones.

1. En la página *Tareas de promoción*, haga clic en *Configuración de CTS* y haga clic en *Sistemas de BW*.
2. En la página *Sistemas BW*, haga clic en *Agregar* para agregar un sistema BW a la infraestructura.
3. En la página *Agregar sistema*, introduzca los siguientes detalles:
   - *SID de host BW*: especifique el ID de sistema (SID) del equipo SAP BW/ABAP del host.
   - *Nombre de host*: especifique la dirección IP del equipo host.
   - *Número de sistema*: introduzca el número de sistema del sistema host.
   - *Cliente*: hace referencia a los detalles del sistema del equipo cliente.
   - *Usuario* y *Contraseña*: especifique el nombre de usuario y la contraseña en el equipo cliente en estos campos.
   - *Idioma*: especifique el idioma en este campo.
4. Haga clic en *Aceptar* para agregar el sistema a la infraestructura.

   > **Nota**
   >
   > Una vez agregado el sistema BW a la infraestructura, puede usar *Editar* o *Eliminar* en la página *Sistemas BW* para modificar los sistemas de la infraestructura.

5. En la página *Tareas de promoción*, haga clic en *Configuración CTS* y haga clic en *Configuración del servicio Web*.
6. En la página *Configuración del servicio Web*, introduzca la dirección URL del servicio Web y los detalles del usuario.

   > **Nota**
   >
   > Si no conoce estos detalles, obténgalos del administrador de Solution Manager.

7. Haga clic en *Guardar* y *Cerrar* para finalizar la adición de la configuración del servicio Web.
8. Crear un archivo de asignación para el sistema CMS de administración de promociones de la plataforma de BI.

   Realice los siguientes pasos en el sistema de desarrollo de la plataforma de BI para crear un archivo de texto con detalles de conectividad para habilitar la asignación:

   a. En el CMS de la administración de promociones de la plataforma de BI, vaya al directorio raíz y cree una carpeta con el nombre **`LCM`** en la ruta `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/`
   b. Cree un archivo de texto con el nombre`LCM_SOURCE_CMS_SID_MAPPING.properties` e introduzca uno de los siguientes elementos en el archivo:
      - `<Nombre completo del sistema de origen de la plataforma SAP BI con dominio>@<número de puerto del CMS> = <nombre lógico para sistema de origen tal y como se usa en la configuración del CTS >`
      - `<Número de IP del sistema de origen de la plataforma SAP BI>@<número de puerto del CMS> = <nombre lógico para sistema de origen tal y como se usa en la configuración del CTS >`

Por ejemplo:

```
DEWDFTH04171S@6400=WJ3
10.208.112.177@6400=WJ3
DEWDFTH04171S.pgdev.sap.corp@6400=WJ3
```

> **Nota**
>
> En el caso de un entorno agrupado, copie el archivo `LCM_SOURCE_CMS_SID_MAPPING.properties` al sistema en el que se está ejecutando el Servidor de procesamiento de Adaptive.

Para obtener más información acerca de cómo realizar los pasos de configuración para sistemas no ABAP, consulte Realizar ajustes de transporte en la aplicación

## 16.7.2.3 Para configurar el sistema de importación de la plataforma de BI en SAP Solution Manager.

1. Inicie sesión en el sistema SAP Solution Manager.
2. Introduzca la transacción `stms` y pulse `Intro`.
3. Configure BOLM como el tipo de aplicación.
   a. Vaya a *Información general* > *Sistemas*.
   b. Vaya a *Extras* > *Tipo de aplicación* > *Configurar*.
   c. Seleccione *Nuevas entradas*.
   d. En el campo *Tipo de aplicación*, introduzca **`BOLM`**.
   e. Introduzca una descripción.
   f. En el campo *Detalles de soporte*, introduzca **`http://service.sap.com (ACH: BOJ-BIP-DEP)`**
   g. Haga clic en *Vista de tabla* > *Guardar*.
   h. Confirme la petición seleccionando *Sí*.
4. Para trabajar con idiomas distintos, puede mantener textos traducidos del siguiente modo:
   a. Elija *Ir a* > *Traducción*.
   b. Seleccione los idiomas a los cuales quiere traducir el texto.
   c. Introduzca los valores traducidos en los campos *Descripción* y *Datos relevantes*.
   d. Confirme el cuadro de diálogo.
   e. Seleccione *Continuar*.
   f. Haga clic en *Vista de tabla* > *Guardar*.
   g. Confirme la petición.

   Ahora el dominio TMS está listo para admitir el uso de contenido de BI en CTS.
5. En CTS+, defina el sistema de origen de la plataforma de BI como un sistema de exportación.

   > **Nota**
   >
   > Para más información sobre la creación de un sistema no ABAP como sistema de origen, consulte Definir y configurar sistemas no ABAP

6. En CTS+, lleve a cabo los siguientes pasos para configurar el sistema de importación de Plataforma de BI:

> **Nota**
>
> Puede definir un SID como referencia al sistema de importación de la plataforma de BI.

a. Cree un sistema no ABAP como sistema de importación.

   Para más información, consulte Definir y configurar sistemas no ABAP.

b. Especifique el método de implementación como *Otros* y anule la selección de todas las demás opciones.

c. Seleccione *Guardar*.

d. Confirme el cuadro de diálogo de distribución.
   Se muestra la vista de tabla para configurar los ajustes del sistema de importación.

e. Haga clic en *Editar* > *Entradas nuevas*.

f. En la pantalla "Cambiar vista CTS: Detalles de sistema para el manejo de tipos de aplicación", realice los siguientes pasos:

   1. En el campo *Método de despliegue*, seleccione *Deployer específico de la aplicación (EJB)*.
   2. En el campo *Desplegar URI*, introduzca el siguiente URI: **`http://<BOE web server name>:<Webserver port>/BOE/LCM/CTSServlet?&cmsName=<BOE destination name>:<CMSport>&authType=<BOE authentication type>`**
      donde
      - "nombre de servidor web BOE" es el nombre o dirección IP del equipo en el que se está ejecutando el servidor web de la Plataforma de BI.
      - "puerto de servidor web" es el número de puerto del servidor Web de la plataforma de BI.
      - "nombre de destino BOE" es el nombre del equipo en el que se está ejecutando el Servidor de administración central (CMS) de la plataforma de BI.
      - "puerto CMS" es el número del CMS destino.
      - "Tipo de autenticación BOE" es el tipo de autenticación de usuario para la importación de contenido de Business Intelligence. Los tipos de autenticación admitidos son secEnterprise, secLDAP, secWinAD y secSAPR3.
   3. En el campo *Usuario*, indique el nombre de usuario de la plataforma de BI.
   4. En el campo *Contraseña*, indique la contraseña de la plataforma BI.
   5. Seleccione *Guardar* para guardar la configuración.

Si necesita más de un sistema de importación, repita los pasos anteriores para crear todos los sistemas de destino que necesite. Para configurar rutas de transporte entre el sistema de origen y de destino después de crear los sistemas de destino, consulte Configurar rutas de transporte

## 16.7.2.4 Exportar desde la plataforma de BI a CTS+ con SSL

### 16.7.2.4.1 Para configurar SSL para CTS+

Para configurar SSL para CTS+ debe configurar SSL en el ABAP de servidor de aplicación. Para obtener más información, consulte Configuring the SAP Web AS for Supporting SSL.

### 16.7.2.4.2 Para configurar el certificado SSL por parte de cliente

Para configurar el certificado SSL por parte de cliente debe importar el certificado de servidor o el certificado CA de confianza al almacén de clave JVM.

1. Realice una copia de seguridad de los archivos `cacerts` del directorio `<INSTALLDIR>\win64_x64\sapjvm\jre\lib\security`.
2. Importe el certificado a Tomcat JVM que aloja el archivo `BOE.war` utilizando los parámetros siguientes:

```
<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file server.cer
-keystore cacerts
```

3. Reinicie Tomcat.

### 16.7.2.4.3 Para configurar el servicio Web de exportación + CTS.

Para configurar el servicio Web de exportación CTS + y activación de HTTPS (`EXPORT_CTS_WS`), puede crear un nuevo punto final de HTTPS.

> **Nota**
>
> Como alternativa, puede cambiar su punto final HTTP existente para utilizar HTTPS.

1. Utilice el código de transacción **`soamanager`**, y en la pestaña *Seguridad de proveedor*, bajo *Seguridad de comunicación*, seleccione *SSL sobre HTTP (seguridad de canal de transporte)* y en *Autenticación de canal de transporte*, seleccione *ID de usuario/Contraseña*.
2. En la ficha *Configuración de transporte*, bajo *Enlace de transporte*, seleccione *HTTPS* para *Protocolo calculado*.

### 16.7.2.4.4 Para configurar la gestión de promoción para SSL

> **→ Recuerde**
>
> Importe el certificado de servidor o la certificación CA probada al almacén de claves JVM.

1. En la CMC, en la ficha *Administración de promociones*, haga clic en *Configuración* > *Configuración CTS* > *Configuración de servicio Web*.
2. Compruebe que el parámetro *URL de servicio Web* incluye `https://` y el número de puerto configurado arriba.

> **Nota**
>
> *Promover mediante CTS* no se visualizará en la lista *Destino de tarea* o en el cuadro de diálogo *Sobrescribir* si la URL especificada no se puede alcanzar. Si el encaje SSL entre la administración de promociones y CTS+ falla, se registra un error en el archivo de registro de la CMC.

## 16.7.2.5 Importar desde CTS+ a la plataforma de BI con SSL

### 16.7.2.5.1 Para configurar Tomcat de la plataforma de BI para usar HTTPS

Para configurar la plataforma de BI para que Tomcat use HTTPS, debe seguir los pasos siguientes en el equipo en el que está instalada la plataforma de BI.

1. Cree una clave de servidor, un certificado y un almacén de claves.
   a. Ejecute `<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe` con los parámetros siguientes:

   ```
   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   serverkeystore.jks -storetype JKS
   keytool -certreq -keyalg RSA -alias server -file server.csr -keystore
   serverkeystore.jks
   ```

   b. Cuando se le solicite, introduzca la siguiente información:
      - Su nombre y apellidos
      - El nombre de la unidad organizacional
      - El nombre de la organización
      - El nombre de la ciudad o población
      - El nombre del estado o provincia
      - El código del país de dos letras para esta unidad

      Se visualizará un string formateado (por ejemplo, `CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA`). Escriba **`sí`** y pulse `Intro` para confirmar.
2. Envíe la solicitud de certificado de servidor a una autoridad de certificación (CA).
3. Importe el certificado de servidor firmado a un almacén de claves de servidor utilizando los parámetros siguientes:

   ```
   keytool -import -alias server -keystore serverkeystore.jks -trustcacerts
   -file server.crt
   ```

4. Configure el archivo de configuración de Tomcat `server.xml` para habilitar HTPPS y usar el almacén de claves que ha creado.
5. Reinicie Tomcat y pruebe la conexión accediendo a la siguiente URL en el explorador: `https://<SERVERNAME>:<SSLPORTNUMBER>`

### Información relacionada

Para configurar SSL para CTS+ [página 666]

## 16.7.2.5.2 Para configurar CTS+ para SSL

Para configurar CTS+ para SSL, debe crear un cliente SSL PSE e importar un certificado.

### Información relacionada

Para configurar SSL para CTS+ [página 666]

## 16.7.2.5.3 Actualizar los sistemas de prueba y producción en CTS+ para usar HTTPS

Para habilitar HTTPS en los sistemas de prueba y producción, ejecute los pasos siguientes:

1. Use el código de transacción STMS.
2. Haga clic en *Presentación general del sistema*.
3. Seleccione el sistema de prueba o producción y haga clic en *Ir a* > *Tipos de aplicación* > *Método de implementación* >.
4. Compruebe que el parámetro *Implementar URI* incluye `https://` y un número de puerto configurado.

## 16.7.3 Para promover una tarea usando CTS

En esta sección se describe el flujo de trabajo que admite la aplicación de la herramienta de gestión de promociones para promover objetos del Servidor de administración central (CMS) de la plataforma de BI desde el sistema de origen al sistema de destino mediante Cambiar sistema de transporte.. Para utilizar el CTS para promover una tarea, lleve a cabo estos pasos:

1. Inicie la herramienta de administración de promociones con la autenticación de SAP y cree una tarea.

   Para obtener más información sobre la creación de una nueva tarea, consulte la sección "Creación de una tarea" en los enlaces relacionados siguientes.

   > **Nota**
   >
   > Asegúrese de que selecciona "SAP" como tipo de autenticación en la pantalla de inicio de sesión en el sistema de origen.

2. En la lista desplegable *Destino*, seleccione la opción *Promover a través de CTS*.

3. Haga clic en *Crear*.
   Aparece la ventana *Agregar objetos desde el sistema*. Aquí las carpetas y subcarpetas se muestran en una estructura de árbol.
4. Desplácese a la carpeta de la que desee seleccionar el InfoObject.
5. Seleccione el InfoObject que desee agregar a la tarea y haga clic en *Agregar*. Si desea agregar un InfoObject y salir de la pantalla *Agregar objetos*, haga clic en *Agregar y cerrar*.
   El InfoObject se agrega a la tarea y se abre la pantalla *Promover tareas*.

   > **Nota**
   >
   > En la pantalla Tareas de promoción, puede hacer lo siguiente:
   > - Usar la opción *Agregar objetos* para agregar más InfoObjects a la tarea. Para obtener más información, consulte Agregar un InfoObject a una tarea.
   > - Utilice la opción *Administrar dependencias* para administrar las dependencias del objeto de información seleccionado. Las dependencias de SAP BW del objeto se muestran en la IU y el usuario puede seleccionarlas.
   > Para obtener más información, consulte Administrar dependencias de tareas.

6. Haga clic en *Promover*.
   Aparece la pantalla *Promover* que muestra el identificador, el responsable y una descripción breve de la solicitud de transporte predeterminada definida en ese momento.
7. Puede utilizar el hipervínculo *Solicitudes de transporte* para realizar lo siguiente:
   - Ver información detallada de la solicitud de transporte.
   - Cambiar los ajustes de la solicitud de transporte predeterminada.
   - Seleccionar otra solicitud de transporte.
   - Crear una solicitud de transporte.

   1. Haga clic en el hipervínculo *Solicitudes de transporte* para abrir la interfaz de usuario Web de *Organizador de transporte*.
   2. Si se le solicitan credenciales de inicio de sesión, inicie la sesión con unas credenciales de usuario válidas para el sistema de controlador de dominio del CTS.
   3. Actualice la pantalla *Promover* para ver las actualizaciones.

   Para obtener más información sobre cómo utilizar la IU de Web del *Organizador de transporte* , consulte IU de Web del Organizador de transporte
8. Para ver los detalles de las dependencias de los objetos de SAP BW, haga clic en el hipervínculo *Dependencias de segundo nivel*.

> **Nota**
>
> Al hacer clic en el hipervínculo *Dependencias de segundo nivel*, sólo se muestran los objetos bloqueados en una solicitud. Si la solicitud se ha liberado, no podrá ver ninguna dependencia. Asimismo, este hipervínculo permanece en gris si no hay ninguna dependencia de segundo nivel activa.

9. Haga clic en *Promover*.
10. Cierre la tarea.
    Se muestra la pantalla principal de la administración de promociones. Ahora el estado de la tarea que creó es *Exportada a CTS*.
11. Libere el objeto de la plataforma de BI en el sistema de destino a través de los pasos siguientes:
    a. Haga clic en el vínculo que aparece en la columna estado de la tarea que quiera promover.
       Aparece la ventana *Estado de promoción*.
    b. Haga clic en *Estado de solicitud*.
       Aparece la IU Web de *Organizador de transporte*.
    c. Si el estado de la solicitud es *Modificable*, haga clic en *Liberar* para liberar la solicitud de transporte del objeto de la plataforma de BI. Para obtener más información sobre cómo liberar solicitudes de transporte que contienen objetos no ABAP, consulte Liberar solicitudes de transporte con objetos no ABAP
    d. Cierre la IU Web del *Organizador de transporte*.
12. Para ver los dependencias de los objetos de SAP BW, haga clic en el hipervínculo *Lista de dependencias de BW*.

> **Nota**
>
> Le recomendamos que converse con el equipo de SAP BW para obtener actualizaciones sobre dependencias de SAP BW y su liberación cuando el equipo trabaje con esos objetos.

13. Cierre la ventana *Estado de promoción*.
14. Importe el objeto de la plataforma de BI en el sistema de destino a través de los pasos siguientes:
    a. Inicie sesión en el controlador de dominio del CTS+.
    b. Llame a la transacción **STMS** para acceder al sistema de administración de transporte.
    c. Haga clic en el icono de *Información general de importación*.
       Aparece la pantalla *Información general de importación* y podrá ver los elementos de la cola de importaciones de todos los sistemas.
    d. Seleccione el ID de sistema del sistema de gestión de promociones de destino.
       Puede ver la lista de solicitudes de transporte que se pueden importar en el sistema.
    e. Haga clic en *Actualizar*.
    f. Importe las solicitudes de transporte relevantes. Para obtener información adicional al respecto, consulte Importar solicitudes

       Para obtener información general sobre cómo importar solicitudes de transporte con contenido BOLM, consulte Importar solicitudes de transporte con objetos no ABAP
15. Si el objeto seleccionado tiene dependencias de SAP BW, lleve a cabo los pasos siguientes:
    a. Libere las dependencias de SAP BW en el sistema de destino a través de los pasos siguientes:
       1. Inicie sesión en el sistema de origen SAP BW.
       2. Llame a la transacción SE09. Aparece la pantalla *Organizador de transporte*.
       3. Haga clic en *Presentación*. Se muestra la solicitud de BW.

4. Haga clic en la solicitud de SAP BW y expándala para ver las tareas creadas para las dependencias.
5. Haga clic con el botón derecho en la solicitud asociada con el objeto de SAP BW principal y seleccione *Liberar directamente*. Repita este paso hasta liberar todas las tareas asociadas a cada objeto dependiente por separado.
6. Haga clic con el botón derecho en la solicitud asociada con el objeto de BW principal y seleccione *Liberar directamente*.
7. Actualice la pantalla hasta que todas las solicitudes estén liberadas.

> **Nota**
>
> Puede hacer doble clic en una solicitud para ver los registros de la misma.

b. Importe las dependencias de SAP BW en el sistema de destino a través de los pasos siguientes:
   1. Inicie sesión en el sistema de destino SAP BW.
   2. Llame a la transacción de STMS para acceder al sistema de administración de transporte.
   3. Haga clic en el icono de *Información general de importación*. Se abrirá la pantalla *Información general de importación*.
   4. Haga doble clic en el identificador del sistema para el destino de SAP BW. Puede ver la lista de solicitudes de transporte que se pueden importar en el sistema.
   5. Importe las solicitudes de transporte relevantes. Para obtener información adicional al respecto, consulte Importar solicitudes
      Para obtener más información acerca de transportes con Colas de importación, consulte Transportes con colas de importación

16. Inicie sesión en el sistema de destino para ver el estado de la tarea que ha promovido.

Para obtener información sobre CTS genérico, consulte Configurar sistemas de destino para otras aplicaciones

### Información relacionada

Crear una tarea [página 610]
Para gestionar las dependencias de una tarea [página 616]

## 16.8 Utilizar el asistente de gestión de promociones

El asistente de la gestión de promociones le permite copiar recursos de Business intelligence (BI) de un repositorio a otro fácilmente en pocos clics.

El asistente de gestión de promociones soporta los siguientes escenarios de promoción:

- Exportar un recurso BI de un sistema fuente a un fichero LCMBIAR.
- Replicar un recurso BI de un sistema fuente a un sistema de destino.
- Importar un fichero LCMBIAR a un sistema de destino.

Con el asistente de gestión de promociones puede promocionar todo el contenido de un repositorio o contenido selectivo de un repositorio sin utilizar la línea de comandos. La interfaz gráfica fácil de usar del asistente de administración de promociones le facilita el trabajo como administrador.

Para obtener más información sobre las mejores prácticas para el Asistente de administración de promociones, consulte la nota SAP 2531264.

> ⚠ Precaución
>
> El asistente de la gestión de promociones no admite restauración. Esto significa que después de promover recursos BI, no puede restaurar el sistema destino a su estado anterior.

> ⓘ Nota
>
> Asegúrese de revisar el valor de memoria antes de iniciar la promoción de objetos. El valor Xms necesita ser menor o igual al valor Xmx.

> ⓘ Nota
>
> Si tiene objetos QaaWs, deberá configurar el sistema destino de forma adecuada.

> → Sugerencias
>
> Para aumentar el rendimiento, desactive la auditoría y la supervisión en el CMC del sistema destino. Para obtener más información, consulte el Manual del administrador de la plataforma Business Intelligence > Auditoría.

## 16.8.1 Para excluir objetos de la promoción

Puede seleccionar los objetos de la lista que se proporciona a continuación y excluirlos de un job de promoción para grabar el espacio de disco y reducir el tiempo de migración.

Un job de promoción migra cada activo de BI de la fuente al sistema de destino. Como resultado, se migran también los activos fijos que son específicos del sistema de origen y no son útiles en el sistema de destino. Para excluir los activos de BI de la promoción, siga los siguientes pasos.

1. Vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
2. Abra *PromotionManagementWizard.ini* en un editor de texto.
3. Busque y localice la cadena *# Lista de tipos para excluir automáticamente de la exportación completa/selectiva.*
   Encontrará el código `-Dcom.sap.businessobjects.pmw.exclude.kind={}` debajo de la cadena.
4. Consulte la lista de objetos de debajo y añada los objetos que deben excluirse entre el `{}`.
5. Guarde el archivo.

Los objetos mencionados en el código se excluirán al ejecutar una tarea de promoción.

Consulte la tabla siguiente para ver la lista de objetos que se pueden excluir de una tarea de promoción.

| Atributos definidos por el cliente | Parámetro DFC | Debates | Objeto del RGPD |
|---|---|---|---|
| Trabajos de LCM | Anulaciones LCM | Historial de búsqueda LCM | Configuración LCM |

| | | | |
|---|---|---|---|
| HORIZONTAL | Conexión HORIZONTAL | LIVE Office | Configuración de MoN.MBEAN |
| Estado MON. ManagedEntity | MON.MonAppDataStore | Mon.Probe | Mon.Subscription |
| NotificationScheduleObject | Sustituir entrada | Status PlatformSearchApplication | PlatformSearchContentExtractor |
| PlatformSearchContentStore | PlatformSearchIndexEngine | PlatformSearchQueue | PlatformSearchScheduling |
| PlatformSearchSearchAgent | PlatformSearchServiceSession | TaskTemplate | VisualDifferenceComprator |
| XL.XcelsiusApplication | busobjectreporter | Explorador | Ampliaciones de Lumira |

## 16.8.2 Cuándo utilizar el asistente de gestión de promociones

Existen varias opciones diferentes disponibles para gestión de promociones. Esta tabla le ayuda a determinar si el asistente de gestión de promociones es la solución más apropiada para sus necesidades.

Diferentes opciones para gestión de promociones

| | **Asistente de gestión de promociones** | **Gestión de promociones utilizando la opción de línea de comandos** | **Gestión de promociones dentro de la consola de administración central** |
|---|---|---|---|
| Objetivo | Promoción excepcional | Automatización | Proyecto |
| Alcance de promoción | Número importante de recursos de BI | Número importante de recursos de BI | Unos pocos recursos de BI |
| Tarea | Ninguna posibilidad de crear una tarea que el servidor de tareas pueda volver a ejecutar | Posibilidad que el servidor de tareas cree una ejecución de tarea | Posibilidad que el servidor de tareas cree una ejecución de tarea |

> **Nota**
>
> Los ficheros LCMBIAR son compatibles con cada opción de gestión de promociones, independientemente de la opción de gestión de promociones seleccionada.

### 16.8.2.1 Definir las opciones de gestión de promociones

1. Especifique las opciones de gestión de promociones que necesita. La información que necesita está aquí:

| Configuración | Descripción |
| --- | --- |
| **Carpeta temporal** | ⓘ Nota<br>Asegúrese de asignar suficiente espacio libre en la carpeta temporal. La cantidad de espacio libre debe ser, al menos, el doble del espacio necesario. |
| **Ubicación de log** | La ubicación de log está definida de modo predeterminado. Puede modificar más tarde dicha ubicación. Las modificaciones se tienen en cuenta inmediatamente en las opciones de la gestión de promociones. |
| **Nivel de log** | Puede establecer el nivel de log en los siguientes niveles:<br>• Predeterminado<br>• Bajo<br>• Medio<br>• Alto<br>El nivel de log está establecido en Predeterminado a no ser que se modifique. |
| **Idioma** | Puede fijar el asistente de gestión de promociones en su idioma preferido. |

2. Haga clic en *Siguiente*.

## 16.8.3 Escenario

El asistente de gestión de promociones admite tres tipos de escenario de promoción:

- Sistema live a LCMBIAR: Copie objetos desde un CMS live a un fichero LCMBIAR.
- CMS live a promoción live: Copie objetos desde un sistema de origen CMS live a un sistema de destino CMS live.
- LCMBIAR a sistema live: Importe objetos de un fichero LCMBIAR a un sistema de destino CMS live.

### 16.8.3.1 Promocionar objetos desde un CMS live a un fichero LCMBIAR

Promocionar objetos desde un CMS live a un fichero LCMBIAR:

1. Seleccione *Exportar*.
2. Para definir el CMS de origen, realice una de las acciones siguientes:
   - Para utilizar el CMS central como el CMS de origen, marque la casilla *Convertir el CMS central en el CMS de origen*.
   - En la sección de origen, introduzca la información siguiente:

    - Nombre de CMS
    - Usuario
    - Contraseña
    - Autenticación
3. En el campo *Destino*, haga clic en *Seleccionar* para seleccionar la ubicación del fichero LCMBIAR.
4. (Opcional) Introduzca una contraseña para encriptar el fichero LCMBIAR.

> **Nota**
>
> Si encripta el fichero LCMBIAR, el proceso de promoción durará más.

5. Haga clic en *Siguiente* para seleccionar los objetos que desea exportar.

### 16.8.3.2 Promocionar objetos desde un sistema de origen CMS live a un sistema de destino CMS live

Para promocionar objetos desde un sistema de origen CMS live a un sistema de destino CMS live:

1. Seleccione *Promocionar*.
2. Para definir el CMS de origen, realice una de las acciones siguientes:
    - Para utilizar el CMS central como el CMS de origen, marque la casilla *Convertir el CMS central en el CMS de origen*.
    - En la sección de origen, introduzca la información siguiente:
        - Nombre de CMS
        - Usuario
        - Contraseña
        - Autenticación
3. Para definir el CMS de destino, realice una de las acciones siguientes:
    - Para utilizar el CMS central como el CMS de destino, marque la casilla *Convertir el CMS central en el CMS de destino*.
    - En la sección de *Destino*, introduzca la información siguiente:
        - Nombre de CMS
        - Usuario
        - Contraseña
        - Autenticación
4. Haga clic en *Siguiente* para seleccionar los objetos que desea copiar desde el sistema de origen en el sistema de destino.

### 16.8.3.3 Promocionar objetos de un fichero LCMBIAR a un sistema de destino CMS live

Para promocionar objetos desde un fichero LCMBIAR a un CMS live:

1. Seleccione *Importar*.
2. Para definir el CMS de destino, realice una de las acciones siguientes:
   - En la sección *Destino*, marque la casilla *Convertir el CMS central en el CMS de destino*.
   - En la sección de *Destino*, introduzca la información siguiente:
     - Nombre de CMS
     - Usuario
     - Contraseña
     - Autenticación
3. En la sección *Origen*, haga clic en *Seleccionar* para seleccionar el fichero LCMBIAR que desee importar.
4. (Opcional) Introduzca una contraseña para encriptar el fichero LCMBIAR.

   > **Nota**
   >
   > Si encripta el fichero LCMBIAR, el proceso de promoción durará más.

5. Haga clic en *Siguiente* para seleccionar los objetos que desea importar.

## 16.8.4 Objetos

El asistente de gestión de promociones admite dos tipos de promoción de contenido:

- Promoción de contenido completo
- Promoción de contenido parcial

La siguiente tabla explica cada tipo:

| Tipos de promoción de contenido | Contenido promocionado | Dependencias de contenido |
|---|---|---|
| Promoción de contenido completo | Promocione todos los siguientes contenidos del sistema fuente al sistema destino:<br>• Objetos (usuarios, documentos, universos, conexiones, etc.)<br>• Instancias<br>• Relaciones entre objetos<br>• Seguridad de objetos | Dado que todas las relaciones están actualizadas, las dependencias no deberán evaluarse. Vaya del actual paso Objetos directamente al paso Resumen. |

| Tipos de promoción de contenido | Contenido promocionado | Dependencias de contenido |
|---|---|---|
| Promoción de contenido parcial | Promocione el contenido que ha seleccionado del sistema fuente al sistema destino. El contenido puede ser el siguiente:<br>• Objetos (usuarios, documentos, universos, conexiones, etc.)<br>• Instancias<br>• Relaciones entre objetos<br>• Seguridad de objetos | Dado que no proporciona todos los contenidos del sistema fuente en el sistema destino, las dependencias deben evaluarse. |

## 16.8.4.1 Promocionar el contenido completo

Para promocionar el contenido completo del sistema fuente en el sistema destino:

1. Seleccione *Promoción de contenido completo*.

   Todos los objetos están seleccionados para la promoción.
2. Haga clic en *Siguiente* para revisar el contenido que ha seleccionado.

## 16.8.4.2 Sobre promocionar contenido selectivo

Antes de promocionar el contenido selectivo del sistema de origen en el sistema de destino, deberá definir las opciones de exportación. La definición de opciones de exportación le permite recuperar parametrizaciones especificadas en el sistema de destino que desea promocionar en el sistema de destino.

### 16.8.4.2.1 Sobre opciones de exportación

Si desea recuperar opciones especificadas en el sistema fuente y promocionarlas en el sistema destino, deberá definir los parámetros siguientes en Opciones de exportación:

- Instancias de objetos
- Dependencias de objetos
- Seguridad
- Comentario
- Tareas de federación
- Resolución de nombre de conflicto

**Instancias de objetos**

| Instancias de objetos | Descripción |
| --- | --- |
| Exporte todas las instancias de un objeto si el objeto está seleccionado. | Exporte los objetos seleccionados con todas sus instancias. |
| Exporte solo las instancias recurrentes de un objeto si el objeto está seleccionado. | Exporte los objetos seleccionados solo con sus instancias recurrentes.<br><br>Por ejemplo, si ha programado una actualización semanal y mensual para un documento, este documento y sus dos instancias recurrentes se exportarán durante la exportación. |
| No exporte instancias del objeto. | Exporte solo los objetos seleccionados. Sus instancias no se exportan. |

## Dependencias de objetos

| Dependencias de objetos | Descripción |
| --- | --- |
| Incluir dependencias al seleccionar objetos | Exporte los objetos seleccionados con todas sus dependencias.<br><br>**Nota**<br>La opción está marcada de manera predeterminada. |
| Excluir dependencias al seleccionar objetos | Exporte solo los objetos seleccionados sin todas sus dependencias. |

## Seguridad

| Seguridad | Descripción |
| --- | --- |
| Incluir seguridad de objeto | Exporte los objetos seleccionados con sus opciones de seguridad de objeto. |
| Incluir seguridad de usuario | Exporte los objetos seleccionados con sus opciones de seguridad de usuario. |
| Incluir seguridad de aplicación | Exporte los objetos seleccionados con sus opciones de seguridad de aplicación. |
| Incluir seguridad de nivel superior. | Exporte las opciones de seguridad definidas en la carpeta raíz.<br><br>**Precaución**<br>Esta opción sobrescribirá las opciones de seguridad definidas en el sistema destino. Debería utilizar esta opción con moderación. |

### Comentario

| Comentario | Descripción |
| --- | --- |
| Incluir comentarios | Exporte los objetos seleccionados con todos sus comentarios. |
| Preferencias del grupo de usuarios para la plataforma de lanzamiento | Si marca la casilla de selección, las preferencias del grupo de usuarios para la plataforma de lanzamiento de BI del sistema de origen y las preferencias predeterminadas se definen en el sistema de destino. |

### Preferencias de BI del grupo de usuarios

| Preferencias de BI del grupo de usuarios | Descripción |
| --- | --- |
| Sobrescribir las preferencias de BI de los grupos de usuarios | Si marca la casilla de selección, las preferencias del grupo de usuarios para la plataforma de lanzamiento de BI del sistema de origen y las preferencias predeterminadas se definen en el sistema de destino.<br>**Nota**<br>Si promueve un documento de Web Intelligence que usa personalización mediante archivo BIAR, asegúrese de habilitar esta opción para importar la personalización. |

### Tareas de federación

| Tareas de federación | Descripción |
| --- | --- |
| Incluir relación de tareas de federación | Importe los objetos seleccionados con sus relaciones de tareas de federación actualizadas. |

### Resolución de nombre de conflicto

| Resolución de nombre de conflicto | Descripción |
| --- | --- |
| Resolución de nombre de conflicto | Si un objeto seleccionado tiene el mismo nombre pero un BUID diferente que un objeto en el sistema destino, se creará una copia del objeto seleccionado en el sistema de destino.<br>Si no activa esta opción, el objeto seleccionado con el mismo nombre pero un CUID diferente no se copiará en el sistema destino. |

## 16.8.4.2.2 Promocionar contenido selectivo

Para promocionar el contenido selectivo del sistema fuente en el sistema destino:

1. Seleccione *Promoción de contenido selectivo*.
2. Para definir *Opciones de exportación*, haga clic en *Opciones*.
3. (Opcional) Marque *Aplicar filtro de tiempo* para filtrar objetos según un intervalo de fechas y horas.
4. Seleccione los objetos que desee exportar.
5. Para evaluar las dependencias de un objeto, marque la casilla asociada de debajo del icono de dependencias

   > **Nota**
   >
   > Por defecto, las casillas de dependencias se verifican todas. Si no desea evaluar las dependencias de un objeto, desmarque la casilla.

6. Haga clic en *Siguiente* para evaluar las dependencias.

## 16.8.5 Dependencias

Si selecciona promocionar contenido selectivo del sistema fuente al sistema destino, las dependencias del contenido selectivo pueden evaluarse. El paso de *Dependencias* proporciona un resumen de los objetos seleccionados identificados como dependencias.

Puede ver la información siguiente sobre las dependencias de los objetos seleccionados:

- Título
- CUID
- Fecha

Puede seleccionar objetos identificados como dependencias:

1. Dependiendo del nivel de detalle que desea ver, realice lo siguiente:
   - Haga clic en *Expandir todo* para ver los detalles de cada dependencia.
   - Haga clic en *Ocultar todo* para ver solamente los objetos dependientes.
2. Seleccione las dependencias que desee promocionar.

   > **Nota**
   >
   > Por defecto, las casillas de dependencias se verifican todas. Si no desea promocionar las dependencias de un objeto, desmarque la casilla.

3. Haga clic en *Siguiente* para revisar los objetos que ha seleccionado para la promoción.

## 16.8.6 Resumen

Antes de realizar la promoción, deberá revisar los objetos seleccionados para la promoción.

Puede ver la información siguiente sobre cada objeto:

- Título
- CUID
- Fecha

> ⚠ Precaución
>
> Asegúrese de que todos los objetos que desea copiar están incluidos porque una vez iniciada la promoción, no podrá cancelar el proceso de promoción. El asistente de la gestión de promociones no admite restauración.

Puede revisar objetos:

1. Dependiendo del nivel de detalle que desea revisar, realice lo siguiente:
   - Haga clic en *Expandir* para ver los detalles de cada objeto.
   - Haga clic en *Ocultar* para ver el nivel superior de cada objeto.

   > ⓘ Nota
   >
   > El nivel del detalle varía en el fichero CSV de resultados de promoción dependiendo de si selecciona *Expandir* u *Ocultar*.
2. Para garantizar que tiene suficiente espacio en su disco duro para la promoción, revise el *espacio temporal mínimo necesario*.
3. Haga clic en *Inicio* para promocionar objetos.

   Una vez iniciada la promoción, no podrá cancelar el proceso.

## 16.8.7 (Opcional) Fichero de propiedades

Puede configurar los parámetros siguientes en el fichero de propiedades del asistente de gestión de promociones:

- Configuración SSL
- Parámetros

El fichero de propiedades del asistente de gestión de promociones está ubicado en:`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

### 16.8.7.1 Configurar los ajustes de SSL

Si utiliza SSL, deberá configurar los ajustes SSL del asistente de gestión de promociones en

`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard`

1. Abra `PromotionManagementWizard.ini` en un editor de texto.

2. Para activar el modo SSL, elimine los comentarios de las líneas que comiencen por "-D".
3. Introduzca los valores para cada ajuste.

| Configuración | Valor |
|---|---|
| `-Dbusinessobjects.orb.oci.protocol` | El valor: ssl<br>**Nota**<br>La introducción de este valor habilita la comunicación SSL |
| `-DcertDir` | La ubicación de claves y certificados |
| `-DtrustedCert` | El nombre del archivo del certificado con confianza<br>**Nota**<br>Si especifica más de un archivo, separe las entradas con un punto y coma (por ejemplo, fileA;fileB). |
| `-DsslCert` | El certificado SDK |
| `-DsslKey` | La clave privada del certificado SDK. |
| `-Dpassphrase` | La ubicación del archivo que contiene la frase de contraseña de la clave privada |
| `-Dpsecert` | El fichero de certificados PSE |

**Precaución**

No agregue ni edite ninguna otra configuración o valor.

4. Grabe `PromotionManagementWizard.ini`

## Ejemplo: Ajustes de SSL en `PromotionManagementWizard.ini`

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/SSL
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dpsecert=temp.pse
```

## 16.8.7.2 Configurar parámetros

Dependiendo de sus necesidades, puede configurar opciones en el fichero de propiedad de asistente de gestión de promociones ubicado en:

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\PromotionManagementWizard
```

1. Abra `PromotionManagementWizard.ini` en un editor de texto.
2. Para activar las opciones, elimine los comentarios de las líneas que comiencen por "-D".
3. Introduzca los valores para cada parámetro.

| Parámetro | Valor |
|---|---|
| `-Dbusinessobjects.connectivity.directory` | La ubicación del directorio del servidor de conexión. |
| `-Dcom.businessobjects.mds.cs.ImplementationID` | `csEX`<br>**Nota**<br>No modifique ni edite este valor. |
| `-Xms8g` | El valor de la memoria está establecido por defecto en 8 Gb.<br>El valor Xms debe ser menor o igual al valor Xmx. |
| `-Xmx10g` | El valor de la memoria está establecido por defecto en 10 Gb.<br>10 Gb de memoria es suficiente para un repositorio de 65 000 objetos. |
| `-Dbobj.biar.suggestSplit=512` | Valor predeterminado (recomendado)<br>Se recomienda utilizar el parámetro `-Dbobj.biar.suggestSplit`.<br>Si promociona objetos de un CMS live a un fichero LCMBIAR, este ajuste le permite partir el fichero LCMBIAR en múltiples ficheros LCMBIAR. |
| `-Dbobj.biar.forceSplit=768` | Valor predeterminado (recomendado)<br>Si el parámetro `-Dbobj.biar.suggestSplit` no puede aplicarse, el parámetro `-Dbobj.biar.forceSplit` se aplica como solución de reserva. |
| `-Dcom.businessobjects.lcm.commit` | • KEEP_TS: Valor predeterminado. Este valor le permite conservar las fechas de modificación de la fuente. |

| Parámetro | Valor |
| --- | --- |
| | • LEGACY: Las fechas de modificación se corresponden con la fecha de ejecución en el sistema de destino. Se trata de un comportamiento existente anterior a 4.2 SP5. |
| `-Dcom.sap.businessobjects.pmw.exclude.list` | Este parámetro le permite excluir permanentemente objetos al promocionar objetos de un sistema fuente a un sistema de destino o al exportar un sistema fuente a un fichero LCMBIAR.<br><br>El valor (CUID) puede ser un objeto (documento, carpeta, etc.). Si se ha especificado una carpeta, todos los niveles inferiores de la carpeta se excluirán. |

4. Grabe `PromotionManagementWizard.ini`.

### Ejemplo: Opciones de asistente de gestión de promociones en `PromotionManagementWizard.ini`

```
-Dbusinessobjects.connectivity.directory=C:\Program Files (x86)\SAP
BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer
-Dcom.businessobjects.mds.cs.ImplementationID=csEX
-Xms2g
-Xmx10g
-Dbobj.biar.suggestSplit=512
-Dcom.businessobjects.lcm.commit=KEEP_TS
-Dcom.sap.businessobjects.pmw.exclude.list="c:/
PromotionManagementWizardExcludedItems.txt"
# Exclusion List AY2ygq4hFJhJmZMQNlQh8OI # Report Samples
AeN4lEu0h_tAtnPEjFYxwi8 # WebIntelligence Samples
```

## 16.8.8 Asistente de gestión de promociones en Linux

Puede ejecutar el asistente de gestión de promociones en Linux.

Antes de comenzar el asistente de gestión de promociones en Linux, asegúrese de que el tiempo de ejecución de Java está fijado en el sistema `PATH`.

Para iniciar el asistente de gestión de promociones en Linux, realice los pasos siguientes:

1. Abra un shell y vaya al directorio de instalación como el siguiente:

   `/usr/sap_bobj/enterprise_xi40`

2. Ejecute el siguiente comando:

   `./PromotionManagementWizard`

   Se inicia el asistente de gestión de promociones

   Para obtener más detalles sobre cómo usar la redirección X11 y SSH, consulte su documentación SO.

# 17 Administración de versión

## 17.1 Para administrar versiones distintas de un InfoObjeto

La aplicación de administración de versiones permite mantener versiones de los recursos de BI que existen en el repositorio de la plataforma de BI. Admite los sistemas de administración de versiones SubVersion y GIT. En esta sección, se describe cómo usar la función de administración de versiones en la herramienta de administración de promociones.

Para crear y administrar versiones diferentes de un InfoObject, complete estos pasos:

1. Inicie la herramienta de administración de promociones.
2. Haga clic con el botón derecho en una tarea, seleccione *Acciones VMS* y haga clic en *Agregar a VM*. (también puede hacer clic en la etiqueta *Acciones VMS* y luego en *Agregar a VM*.)

   > **Nota**
   >
   > Al hacer clic en *Agregar a VM*, se creará una versión base del objeto en el repositorio del VMS. La versión base es necesaria para proceder a la protección posteriormente.

3. Haga clic en *Proteger* para actualizar el documento que existe en el repositorio del VMS.
   Aparece el cuadro de diálogo *Proteger comentarios*.
4. Especifique el comentario y haga clic en *Aceptar*.
   Aparece el cambio en el número de versión del InfoObject seleccionado en las columnas VMS y del sistema de administración de contenidos.
5. Para obtener la versión más reciente del documento del VMS, seleccione el InfoObject que desee y haga clic en *Obtener versión más reciente*.
6. Para crear una copia de la versión más reciente, haga clic en *Crear copia*.
   Se crea una copia de la versión seleccionada.
7. Seleccione *Historial* para ver todas las versiones disponibles del recurso seleccionado.
   Aparece la ventana *Historial*. Aparecen las siguientes opciones:
   - *Obtener versión*: Si hay varias versiones y si necesita una versión determinada del recurso de BI, puede seleccionar el recurso adecuado y hacer clic en *Obtener versión*.
   - *Obtener copia de versión*: Esta opción permite obtener una copia de la versión seleccionada.
   - *Exportar copia de versión*: Esta opción permite obtener una copia de la versión seleccionada y guardarla en el sistema local.

### 17.1.1 derechos de acceso a la aplicación de administración de versión

En esta sección se describen los derechos de acceso a la aplicación de la aplicación de administración de versión.

- Puede configurar los derechos de acceso a la aplicación de administración de versión desde la CMC.
- Puede configurar los derechos granulares de la aplicación para varias funciones de la aplicación de administración de versión.

Para establecer los derechos específicos en la aplicación de administración de versión, lleve a cabo los siguientes pasos:

1. Conectar a la CMC y seleccionar *Aplicaciones*.
2. Haga doble clic en *Administración de versión*.
3. Haga clic en *Seguridad de usuario* y seleccione un usuario. Puede ver o asignar derechos de seguridad para el usuario seleccionado.
4. Están disponibles los siguientes derechos específicos de administración de versión:
   - Permitir protección
   - Permitir crear copia
   - Permitir eliminar revisión
   - Permitir obtener revisión
   - Permitir bloquear y desbloquear
   - Ver y versión de los objetos BOMM
   - Ver y versión de las vistas empresariales
   - Ver y versión de los calendarios
   - Ver y versión de las conexiones
   - Ver y versión de los perfiles
   - Ver y versión de QaaWS
   - Ver y versión de los objetos de informe
   - Ver y versión de los objetos de informe
   - Ver y versión de universos
   - Ver recursos eliminados
5. Si desea asignar derechos a un usuario seleccionado, seleccione el derecho adecuado y haga clic en *Asignar seguridad*.

## 17.1.2 Realización de una copia de seguridad y restauración de archivos de subversión

En esta sección se describen los procedimientos sugeridos para realizar copias de seguridad y recuperar archivos de subversión. Un plan de copia de seguridad y recuperación está formado por las precauciones que se deben tomar en el caso de fallo del sistema debido a un desastre natural o una catástrofe.

### 17.1.2.1 Para realizar una copia de seguridad de archivos de subversión

Realice los pasos siguientes para realizar una copia de seguridad de los archivos de subversión:

1. En Windows, vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise 4.0\CheckOut` o en Unix, vaya a `<INSTALLDIR>/sap_bobj/enterprise_40/Subversion/CheckOut`
2. Copie la carpeta `CheckOut` y almacénela en cualquier dispositivo de copia de seguridad.
3. Copie `<LCM_Repository>` y almacénelo en cualquier dispositivo de copia de seguridad.

### 17.1.2.2 Para restaurar archivos de subversión

Realice los pasos siguientes para restaurar archivos de subversión:

1. Restaure la carpeta CheckOut desde la ubicación en la que realizó anteriormente la copia de seguridad.

   > **Nota**
   >
   > En CMC, haga clic en *Aplicaciones* > *Administración de versiones* > *Configuración de VMS*, y asegúrese de que se ha introducido la ruta de desprotección correcta en el campo *Directorio de área de trabajo*.

2. Restaure el LCM_Repository desde la ubicación en la que realizó anteriormente la copia de seguridad.

   > **Nota**
   >
   > En CMC, haga clic en *Aplicaciones* > *Administración de versiones* > *Configuración de VMS*, y asegúrese de que se ha introducido la ruta de desprotección correcta en el campo *Ruta de instalación*.

## 17.2 Para administrar versiones distintas de recursos de BI

La aplicación de administración de versiones permite mantener diferentes versiones de los recursos de BI que existen en el repositorio de la plataforma de BI. Para facilitar esta función, la herramienta incluye el sistema de control de versiones SubVersion.

Para administrar versiones diferentes de tareas o InfoObjects, siga estos pasos:

1. Inicie sesión en la aplicación de la CMC y seleccione *Administración de versiones*.
2. En el panel izquierdo de la ventana *Administración de versiones*, seleccione la carpeta para ver la tarea o InfoObjects cuyas versiones desea administrar.
3. Seleccione los InfoObjects y haga clic en *Agregar a VM*.

   > **Nota**
   >
   > Al hacer clic en *Agregar a VM* se creará una versión base del objeto en el repositorio del Sistema de administración de versión (VMS). La versión base es necesaria para proceder a la protección posteriormente.

4. En los posteriores cambios del documento y de la versión del documento cambiado incrementalmente, haga clic en *Protección*. Esta acción actualizará el documento que existe en el repositorio de VMS.

   Aparece el cuadro de diálogo *Proteger comentarios*.

5. Especifique el comentario y haga clic en *Aceptar*.
   Aparece el cambio en el número de versión del InfoObject seleccionado en las columnas *Versión de VMS* y *Versión del CMS (Servidor de administración central)*.
6. Para obtener la versión más reciente del documento del VMS, seleccione el InfoObject que desee y haga clic en *Obtener versión más reciente*.
   La última versión del repositorio de VMS se importará al CMS.
7. Para crear una copia de la versión más reciente, haga clic en *Crear copia*.
   Se crea una copia de la versión seleccionada en el repositorio de VMS y CMS.
8. Seleccione *Historial* para ver todas las versiones disponibles para el InfoObject seleccionado.
   Aparece la ventana *Historial*. Aparecen las siguientes opciones:
   - *Obtener versión*: Si hay varias versiones y si necesita una versión determinada del recurso de BI, puede seleccionar el InfoObject adecuado y hacer clic en *Obtener versión*.
   - *Obtener copia de versión*: Esta opción permite obtener una copia de la versión seleccionada.
   - *Exportar copia de versión*: Esta opción permite obtener una copia de la versión seleccionada y guardarla en el sistema local.
   - *Comparar*: esta opción permite comparar la información de los metadatos de las dos versiones de una tarea. Para obtener más información, consulte «Comparar versiones distintas de la misma tarea».
9. Seleccione un InfoObject y haga clic en *Bloquear* para bloquear el InfoObject o *Desbloquear* para desbloquear el InfoObject, o *Eliminar* para eliminar todo el contenido versionado del repositorio de VMS. El contenido del CMS no se ve afectado.

   > **Nota**
   >
   > Si bloquea un InfoObject, no podrá realizar ninguna acción en él.

10. Cuando la versión del CMS es posterior a la versión de VMS, aparece un indicador junto al InfoObject. Al colocar el cursor en el indicador, se muestra la información sobre herramientas `La versión en el CMS es la más reciente`.
11. Para ver la lista de todos los recursos protegidos que existen en el VMS, pero no en el CMS, haga clic en *Ver recursos eliminados*.
    Haga clic en los recursos eliminados para ver el historial de dicho recurso. Puede seleccionar un recurso eliminado y hacer clic en *Obtener versión* para ver una versión determinada del recurso.

    Haga clic en *Eliminar* para sacar permanentemente el objeto del repositorio del VMS.

    > **Nota**
    >
    > Si utiliza *Obtener versión* , el recurso se mueve de la lista de archivos que faltan del VMS al CMS.

12. Seleccione un InfoObject y haga clic en para ver las propiedades del InfoObject.
    Como alternativa, puede hacer clic con el botón derecho en el InfoObject y realizar los pasos del 3 al 12.
13. Puede buscar activos de BI en la aplicación *Gestión de versiones*. Puede utilizar las opciones como *Buscar todos los campos*, *Buscar título*, *Buscar palabra clave* y *Buscar descripción* para realizar una búsqueda específica para obtener resultados más rápidos.

    > **Nota**
    >
    > La función de búsqueda en la aplicación *Gestión de versiones* es contextual. Esto significa que si selecciona una carpeta como *Auditoría* e introduce una cadena para buscar un documento, la

plataforma de BI busca el documento solo en la carpeta *Auditoría*. De forma similar, si selecciona *Todas las carpetas* y realiza una búsqueda, la plataforma de BI busca el InfoObjeto en cada carpeta.

## 17.3 Iniciar y detener la subversión manualmente en Unix

En Unix, la subversión no se inicia automáticamente después de reiniciar el equipo. Desde la plataforma de BI 4.1 SP2, puede ejecutar `<INSTALLDIR>/svn_startup.sh` para iniciar la subversión y `<INSTALLDIR>/svn_shutdown.sh` para detenerla.

> **Nota**
>
> `svn_shutdown.sh` solo funcionará si `svnserve` se inicia con `svn_startup.sh`

> **Restricción**
>
> Si el proceso de subversión se ejecuta antes de la instalación de la revisión SP2, `svn_shutdown.sh` no funcionará después de instalar la revisión. Para reiniciar la subversión, debe terminar manualmente el proceso `svnserve` y ejecutar `svn_startup.sh`.

## 17.4 Archivos requeridos para subversión en Solaris 10 y RedHat Linux 5

Los archivos siguientes son obligatorios para ejecutar la subversión.

> **Nota**
>
> Si cualquiera de los binarios siguientes no se encuentran antes de la instalación de la plataforma de BI 4.1 SP1, el usuario debe ejecutar `<INSTALLDIR>/sap_bobj/lcm_installer.sh <SUBVERSION_PASSWORD> <CMS_PASSWORD>` y reiniciar el servidor de procesamiento de Adaptive para que la administración de versiones funcione correctamente.

- En Solaris 10, debe instalar los paquetes `CSWlibiconv2` y `CSWlibgcc-s1` que contienen `libiconv.so.2` y `libgcc_s.so.1`

  > **→ Recuerde**
  >
  > Después de instalar los paquetes, compruebe que la ruta a estas blbliotecas se incluye en la variable de entorno del usuario `LD_LIBRARY_PATH`.

- En RedHat Linux 5, debe desplegar `libexpat.so.1`

## 17.5 Para utilizar la subversión Apache como el sistema de administración de versión

Puede fijar Apache SubVersion como su Sistema de administración de versión y configurar las opciones de la Consola de administración central.

1. En la CMC, seleccione *Aplicaciones*.
2. Haga doble clic en *VMS*.
   Aparece la pantalla Administración de versiones.
3. Seleccione *Configuración de VMS*.
4. En la lista desplegable *Sistemas de administración de versión*, seleccione *SubVersion*.
   El número de puerto del servidor, la contraseña, el nombre del repositorio, el nombre del servidor, el nombre de usuario, el nombre del directorio del área de trabajo y el nombre del directorio de instalación que se proporcionaron durante el proceso de instalación de la herramienta de administración de promociones se muestran en los campos correspondientes.
5. Modifique los campos según sea necesario.

   > **Nota**
   >
   > Compruebe que introduce la ruta de instalación que contiene el archivo `.exe`.

   En Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Subversion`

   En Unix: `<INSTALLDIR>/sap_bobj/enterprise_40/subversion/bin`
6. Seleccione *SVN*, *HTTP*, o *HTTPS*.

   > **Nota**
   >
   > Para obtener más información sobre la conexión a Subversion con HTTPS consulte la *Documentación de Apache Subversion*.
7. (Opcional) Haga clic en *Realizar un test de VMS* para validar la configuración de VMS.
8. Haga clic en *Guardar*.

   > **Nota**
   >
   > - Si desea que SubVersion sea su VMS predeterminado, seleccione *Usar como VMS predeterminado*.
   > - Si ha modificado los campos, reinicie el servidor de procesamiento de Adaptive.

## 17.6 Para utilizar Git como el sistema de administración de versión

Puede fijar Git como su Sistema de administración de versión y configurar las opciones de la Consola de administración central.

1. En la página de inicio de CMC, seleccione *Aplicaciones*.
2. Haga doble clic en *Administración de versión*.
   Visualizará *Configuración de VMS* en la pantalla *Configuración de administración de versiones*.
3. Seleccione *Git* desde la lista *Sistemas de administración de versión*.
   Se visualizará la *Configuración de Git* y los parámetros necesarios.
4. Seleccione un protocolo e introduzca el valor en los campos vacíos. Consulte la tabla siguiente para comprender más sobre cada campo.

| Términos de IU | Descripción |
|---|---|
| **Protocolo** | Seleccione Local si Git está instalado en su sistema local y seleccione HTTP(s) si Git está instalado en un servidor remoto. |
| **Nombre de usuario** | Introduzca el nombre de usuario del servidor donde Git está instalado. |
| **Contraseña** | Introduzca la contraseña para acceder al servidor donde está instalado Git. |
| **URL del servidor** | Introduzca el enlace al servidor donde esté instalado Git. |
| **Directorio del área de trabajo** | Introduzca la ruta del archivo en la que desea guardar el área de trabajo. |
| **Nombre de repositorio de servidor** | Introduzca un nombre para el repositorio de servidor. |
| **Ruta de instalación GIT** | Introduzca el directorio de instalación de Git. |

> **Nota**
>
> Si desea que Git sea su VMS predeterminado, seleccione *Usar como VMS predeterminado*.

5. (Opcional) Haga clic en *Probar VMS* para validar la configuración de VMS.
6. Seleccione *Guardar*.
7. Vaya a *Servidores* > *Lista de servidores* y seleccione *Reiniciar servidor* del menú contextual del *Servidor de procesamiento de Adaptative*.

Ha configurado correctamente Git como su sistema de administración de versión.

## 17.7 Configuración del sistema de administración de versiones predeterminada

Al reinicializar el CMS, se borran todos los ajustes de la aplicación. Los siguientes ajustes predeterminados son del sistema de administración de versiones:

| Parámetro | Valor |
|---|---|
| Nombre del servidor | `localhost` |
| Puerto del servidor | `3690` |
| Nombre de usuario | `LCM` |

| Parámetro | Valor |
| --- | --- |
| Contraseña | Introducido durante la instalación. |
| Ruta de instalación | En Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Subversion`<br>En Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/subversion/bin` |
| Nombre del repositorio | En Windows: `svn_repository`<br>En Unix: `LCM_repository` |
| Directorio del área de trabajo | En Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\CheckOut`<br>En Unix: `<INSTALLDIR>/sap_bobj/enterprise_xi40/CheckOut` |
| Protocolo | `SVN` |

## 17.8 Comparar versiones distintas del mismo trabajo

Puede ver las diferencias entre dos versiones de la misma tarea siguiendo estos pasos:

1. Inicie sesión en la aplicación de la CMC.
2. Desde la página de inicio de la CMC, seleccione *Administración de versiones*.
3. Desde la pantalla de administración de versiones, seleccione la tarea cuya versión se deba comparar.
4. Haga clic en *Historial*.
   Aparece la página Historial que muestra todas las versiones del InfoObject seleccionado.
5. Seleccione cualquiera de las dos versiones para la comparación.
6. Haga clic en *Comparar*.
   El proceso de comparación se inicia y las diferencias se resaltan en color naranja y los objetos perdidos, en color rojo.
7. Haga clic en *Guardar* para guardar el informe de diferencias.

## 17.9 Actualizar el contenido de subversión

Si dispone de contenido de subversión antiguo que se creó con una versión anterior de la plataforma de BI, puede actualizar el contenido a la versión más reciente con los siguientes pasos:

1. Inicie sesión en el VMS del equipo SAP BusinessObjects Enterprise 4.2.
2. Proteja los objetos. Por ejemplo, introduzca el administrador y los objetos invitados dos veces.
3. En la CMC, haga clic en *Usuarios* y verifique que `2` se muestra en el número de versión del VMS y del CMS.
4. Cierre sesión del VMS.
5. Vaya al símbolo del sistema, desplácese a `C:\Archivos de programa\Subversion\bin` y ejecute el comando de exportación: `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`
6. Copie el archivo `dumrepo` en el equipo de la plataforma de BI
7. Vaya a la petición de comandos del equipo de la plataforma de BI, desplácese a `C:\Archivos de programa (x86)\SAP` y ejecute los siguientes comandos:

   ```
   svnadmin.exe load "C:/Program Files (x86)/SAP BusinessObjects/SAPBusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo
   ```

   ```
   svnadmin.exe upgrade "C:/Program Files (x86)/SAP BusinessObjects/SAP BusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository"
   ```
8. Después de ejecutar correctamente los comandos, reinicie el SIA.
9. Inicie sesión en la CMC y haga clic en *Administración de versiones*.
10. Haga clic en *Usuarios* y verifique que la versión del VMS es `2`.
11. Seleccione el objeto *Administrador* y haga clic en *Obtener versión más reciente*.
12. El número de versión del VMS y del CMS es el mismo.

    Para obtener más información acerca de la actualización de Apache Subversion, consulte Apache Subversion, notas de la versión 1.10 .

## 17.10 Configurar subversión para servidores de tareas de procesamiento agrupadas

### 17.10.1 Opción A: Configurar el equipo de subversión antes de cualquier operación del sistema de administración de versiones

1. Verifique que el directorio de copia de trabajo no haya sido creado en `<INSTALLDIR>\CheckOut`
2. Cree un directorio para sus archivos de copia de trabajo de subversión y compártalo haciendo que sea de escritura desde otros equipos.
3. En la CMC, en la página de configuración del sistema de administración de versiones, cambie el *Nombre del servidor* de **`localhost`** a la dirección de su equipo principal.
4. Cambie el *Directorio del área de trabajo* a su compartición de copia de trabajo en el formato siguiente: `\\<HOSTNAME>\<SHARENAME>`

5. Detenga el Server Intelligence Agent (SIA) y cambie la cuenta de LocalSystem al administrador de sistema operativo.

> **Nota**
>
> LocalSystem no tiene acceso de red al directorio compartido.

6. Inicie el SIA.

> **Nota**
>
> Si el SIA ya se ha ejecutado en una cuenta con acceso de red al directorio compartido, solo tiene que reiniciar todos los servidores de tareas de procesamiento que almacenan el sistema de administración de versiones para que los pasos 3 y 4 tengan efecto.

## 17.10.2 Opción B: Configurar la subversión después de que el sistema de administración de versiones cree un directorio de copia de trabajo

1. Verifique que la subversión haya sido instalada como parte de la plataforma de BI.
2. Comparta el directorio de copia de trabajo que se encuentra en `<INSTALLDIR>\CheckOut` y haga que sea de escritura desde otros equipos.
3. Establezca el nombre del área de trabajo con uno de los métodos siguientes:
   - Realice una operación de sistema de administración de versiones (VMS) con el equipo principal. A continuación, inspeccione el directorio de copia de trabajo de la subversión para determinar el nombre del área de trabajo.
   - Calcule el nombre del área de trabajo eliminando el símbolo @ y sustituyendo los dos puntos por el carácter *B*. Por ejemplo, si el cluster se llama `ABCD-LCM:6400`, el sistema de administración de versiones utilizará `ABCD-LCMB6400` como nombre del área de trabajo.

> **Nota**
>
> La subversión almacena su repositorio en el directorio de copia de trabajo.

4. Cambie la dirección URL predeterminada de **`localhost`** en otro que cualquier equipo puede usar ejecutando el comando siguiente:

```
svn switch --relocate svn://localhost:3690/
svn_repository svn://<SUBVERSION_MACHINE>:3690/svn_repository \
\<SUBVERSION_SHARE>\CheckOut\<WORKSPACE_NAME>-LCMB6400\WORKSPACE
```

5. Cuando se le solicite, introduzca la contraseña del administrador del sistema operativo, el usuario y la contraseña.

> **Nota**
>
> De forma predeterminada, el usuario es LCM y la contraseña que se ha establecido durante la instalación.

6. En la CMC, en la página de configuración del sistema de administración de versiones, cambie el *Nombre del servidor* de **`localhost`** a la dirección de su equipo principal.

7. Cambie el *Directorio de área de trabajo* de **`localhost`** a la compartición de copia de trabajo: `\\<SUBVERSION_SHARE>\CheckOut`
8. Detenga el Server Intelligence Agent (SIA) y cambie la cuenta de LocalSystem al administrador de sistema operativo
9. Inicie el SIA.

> **Nota**
>
> Si el SIA ya se ha ejecutado en otra cuenta con acceso de red al directorio compartido, solo tiene que reiniciar todos los servidores de tareas de procesamiento que almacenan el VMS.

## 17.10.3 Configurar otros equipos de subversión

Para configurar otros equipos de subversión, detenga el Server Intelligence Agent (SIA) y cambie la cuenta de LocalSystem a otra cuenta con acceso de red para que este servidor de tareas de procesamiento pueda acceder al directorio compartido (por ejemplo, la cuenta de administrador del sistema operativo). A continuación, reinicie el SIA.

> **Nota**
>
> Si el SIA ya se ha ejecutado en otra cuenta con acceso de red al directorio compartido, solo tiene que reiniciar todos los servidores de tareas de procesamiento que almacenan el VMS.

# 18 Administración de aplicaciones

## 18.1 Desactivar el mensaje emergente GDPR

Desde el release 4.2 SP5 de la plataforma SAP BusinessObjects Business Intelligence, el mensaje emergente de descargo de responsabilidad GDPR (normativa de protección de datos global) es obligatorio para todos los usuarios cuando inician sesión en aplicaciones Web de la plataforma de BI como:

- Plataforma de lanzamiento de BI
- Consola de administración central
- Plataforma de lanzamiento de Fiori BI
- Abrir documento

Sabiendo que el mensaje de descargo de responsabilidad GDPR es obligatorio, tendrá la opción de desactivar su visualización.

> ⚠ Precaución
>
> El mensaje emergente de descargo de responsabilidad GDPR **no debería**, ni **puede** desactivarse de forma proactiva. Para asegurar el cumplimiento de la legislación GDPR UE, todos los usuarios deben aceptar activamente este mensaje antes de continuar.

### Desactivar el mensaje GDPR para los usuarios que inician sesión en la plataforma de lanzamiento de BI

1. En una instalación predeterminada de Tomcat, vaya al archivo de propiedades:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Ejemplo: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Cree un archivo nuevo denominado `<Infoview.properties>`y escriba `<properties file>` en la vía de acceso personalizado:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Ejemplo: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Cree una nueva entrada de propiedad para `<disclaimer.enabled>`y establézcala como `<false>`:
   `disclaimer.enabled=false`
4. Guarde el archivo.
5. Reinicie Tomcat.

## Desactivar el mensaje GDPR para los usuarios que inician sesión en CMC

1. En una instalación predeterminada de Tomcat, vaya al archivo de propiedades:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Ejemplo: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
2. Cree un nuevo archivo denominado `<CMCApp.properties>`y escriba `<properties file>` en la vía de acceso personalizado:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Ejemplo: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Cree una nueva entrada de propiedad para `<disclaimer.enabled>`y establézcala como `<false>`:
   `disclaimer.enabled=false`
4. Guarde el archivo.
5. Reinicie Tomcat.

## Desactivar el mensaje GDPR para los usuarios que inician sesión en la plataforma de lanzamiento de Fiori BI

1. En una instalación predeterminada de Tomcat, vaya al archivo de propiedades:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Ejemplo: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Cree un nuevo archivo denominado `<FioriBI.properties>`y escriba `<properties file>` en la vía de acceso personalizado:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Ejemplo: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`
3. Cree una nueva entrada de propiedad para `<disclaimer.enabled>`y establézcala como `<false>`:
   `disclaimer.enabled=false`
4. Guarde el archivo.
5. Reinicie Tomcat.

## Desactivar el mensaje GDPR para Open Document

1. En una instalación predeterminada de Tomcat, vaya al archivo de propiedades:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\default`
   Ejemplo: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\default`
2. Cree un nuevo archivo denominado `<OpenDocument.properties>`y escriba `<properties file>` en la vía de acceso personalizado:
   `<BOE_HOME>\Tomcat\webapps\BOE\WEB-INF\config\custom`
   Ejemplo: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEB-INF\config\custom`

3. Cree una nueva entrada de propiedad para `<disclaimer.enabled>`y establézcala como `<false>`: `disclaimer.enabled=false`
4. Guarde el archivo.
5. Reinicie Tomcat.

## 18.2 Administrar aplicaciones mediante la CMC

### 18.2.1 Información general

El área de administración de *Aplicaciones* de la CMC permite cambiar la apariencia y la funcionalidad de las aplicaciones Web como la CMC y la rampa de lanzamiento BI, sin necesidad de programación. También modificar el acceso a las aplicaciones para usuarios, grupos y administradores si cambia los derechos asociados a cada una.

En esta sección, encontrará información contextual, procedimientos e instrucciones sobre cómo administrar las distintas configuraciones. Las siguientes aplicaciones tienen configuraciones que pueden modificarse con la CMC:

- *Aplicación de alertas*
- *Edición de análisis para OLAP*
- *Analysis Office en tiempo de ejecución*
- *Configuración del servidor de autorizaciones*
- *Aplicaciones BEx Web*
- *Cockpit del administrador de BI*
- *Rampa de lanzamiento BI*
- *Áreas de trabajo de BI*
- *Consola de administración central*
- *Colaboración*
- *Aplicación Comentario BI*
- *Configuración de Crystal Reports*
- *Autentificación HANA*
- *Herramienta de diseño de información*
- *Aplicación Information Steward*
- *BI Admin Studio*
- *Herramienta de administración de multipropiedad*
- *Abrir documento*
- *Aplicación de búsqueda de plataformas*
- *Administración de promociones*
- *Aplicación de papelera de reciclaje*
- *Servicio Web RESTful*
- *SAP BusinessObjects Mobile*
- *SAP Analytics Cloud*

- *Herramienta de administración de traducciones*
- *Herramienta de diseño de universos*
- *Administración de versión*
- *Administración de versión*
- *Diferencia visual*
- *Web Intelligence*
- *Servicio Web*
- *Asistente de workflow*

## 18.2.2 Configuración común para aplicaciones

### 18.2.2.1 Configuración de derechos de usuario en aplicaciones

Puede usar los derechos para controlar el acceso de los usuarios a algunas funciones de las aplicaciones. El área *Aplicaciones* de la CMC sirve para asignar entidades de seguridad a la lista de control de acceso de una aplicación, ver los derechos con los que cuenta una entidad de seguridad y modificar los derechos de los que dispone la entidad de seguridad para una aplicación. Para obtener más información acerca de la administración de derechos, consulte el *Manual del administrador de laplataforma BI de SAP*.

### 18.2.2.2 Para definir el nivel de registro de seguimiento de la aplicación Web en la CMC

Para trazar otras aplicaciones web, debe configurar manualmente el archivo `BO_trace.ini` correspondiente.

1. En el área *Aplicaciones* de la CMC, haga clic con el botón derecho en la aplicación y seleccione *Configuración del registro de seguimiento*.

   > **Nota**
   >
   > Estas aplicaciones tienen configuraciones de registro de seguimiento: plataforma de lanzamiento de BI de Fiori, CMC, Open Document, administración de promociones, administración de versiones, diferencia visual, y servicio Web.

   Aparece el cuadro de diálogo *Configuración de registro de seguimiento*.
2. Seleccione la configuración de la lista *Nivel de registro*.
3. Haga clic en *Guardar y cerrar*.
4. Reinicie el servidor de aplicaciones Web.

El nuevo nivel de registro de seguimiento entrará en vigor después del siguiente inicio de sesión en la aplicación Web.

## Información relacionada

Niveles de registro de seguimiento [página 701]

### 18.2.2.2.1 Niveles de registro de seguimiento

Los siguientes niveles de registro de seguimiento están disponibles para los componentes de la plataforma de BI:

| Nivel | Descripción |
|---|---|
| No especificado | El nivel de registro de seguimiento se especifica mediante otros medios (normalmente un archivo `.ini`). |
| Ninguno | No ocurre ningún seguimiento. |
| Baja | El filtro de registro de seguimiento permite registrar mensajes de error e ignorar mensajes de advertencia y de estado. Los mensajes de estado importantes se registran para los mensajes de inicio del componente, de cierre, de inicio de la consulta, y de finalización de la consulta. Este nivel no es aconsejable para realizar depuraciones. |
| Medio | El filtro del registro de seguimiento está definido para incluir mensajes de error, de advertencia y la mayoría de los mensajes de estado. Los mensajes de estado no tan importantes o muy detallados están filtrados. Este nivel no incluye suficiente contenido para realizar depuraciones. |
| Alto | Ningún mensaje está filtrado. Este nivel es aconsejable para realizar depuraciones.<br>⚠ Precaución<br>Este nivel de registro de seguimiento afecta significativamente los recursos del sistema, incrementa el uso de la CPU y consume espacio de almacenamiento. |

## 18.2.3 Configuración específica de la aplicación

### 18.2.3.1 Administración de la configuración de la aplicación CMC

### 18.2.3.1.1 Autenticación y objetos de programa

Puede controlar los tipos de objetos de programa que los usuarios pueden ejecutar y puede configurar las credenciales necesarias para ejecutar objetos de programa.

Tenga en cuenta los posibles riesgos de seguridad asociados con la adición de los objetos de programa en el repositorio. El nivel de permisos de archivo para la cuenta con la que se ejecuta un objeto de programa determinará las modificaciones, si las hay, que puede efectuar el programa en los archivos.

## Habilitar o deshabilitar un tipo de objeto de programa

Como primer nivel de seguridad, puede configurar los tipos de objetos de programa disponibles para su uso.

## Autenticación de todas las plataformas

En el área de administración *Carpetas* de la CMC, debe especificar las credenciales de la cuenta con la que se ejecuta el programa. Esta función le permite configurar una cuenta de usuario específica para el programa y asignarle los derechos necesarios para que el objeto de programa se ejecute con esa cuenta.

O bien, los usuarios que agregan objetos de programa en Servicios de plataforma de información pueden asignar sus propias credenciales a un objeto de programa para que éste tenga acceso al sistema. De esta forma, el programa se ejecutará con esa cuenta de usuario y los derechos del programa se restringirán a los del usuario. Si decide no especificar ninguna cuenta de usuario para un objeto de programa, éste se ejecuta con la cuenta del sistema predeterminada que suele tener derechos localmente pero no en la red.

> ⓘ Nota
>
> De forma predeterminada, al programar un objeto de programa, la tarea falla si no se especifican las credenciales. Para proporcionar credenciales predeterminadas, seleccione *CMC* en el área de administración *Aplicaciones*. En el menú *Acciones*, haga clic en *Derechos del objeto de programa*. Haga clic en *Programar con las siguientes credenciales del sistema operativo* y proporcione un nombre de usuario y una contraseña predeterminados.

## Autenticación de programas de Java

Servicios de plataforma de información permite establecer la seguridad de todos los objetos de programa. Para los programas de Java, Servicios de plataforma de información fuerza el uso de un archivo de directivas Java, que contiene la configuración predeterminada coherente con los valores predeterminados de Java de código no seguro. Utilice la herramienta Java Policy Tool (disponible con Java Development Kit) para modificar el archivo de instrucciones Java con el fin de adaptarlo a sus necesidades específicas.

Esta herramienta tiene dos entradas base de código. La primera entrada apunta al SDK Java de SAP BusinessObjects Enterprise y permite que los objetos de programa tengan derechos totales en todos los archivos JAR de SAP BusinessObjects Enterprise. La segunda entrada base de código se aplica a todos los archivos locales. Utiliza la misma configuración de seguridad para el código no seguro que la predeterminada de Java para este tipo de código.

> **Nota**
>
> La configuración de las instrucciones Java son universales para todos los Servidores de tareas de programa que se ejecutan en el mismo equipo.

> **Nota**
>
> De forma predeterminada, el archivo de directivas Java se instala en el directorio del SDK Java del directorio raíz de instalación de Servicios de plataforma de información. Por ejemplo, una ubicación típica en Windows es: `C:\Archivos de programa\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`

### 18.2.3.1.1.1 Para habilitar o deshabilitar un tipo de objeto de programa

1. En el área *Aplicaciones*, seleccione *Consola de administración central*.
2. Haga clic en *Acciones* > *Derechos del objeto de programa* .
   Aparece el cuadro de diálogo *Derechos del objeto de programa*.
3. En el área *Permitir a los usuarios*, seleccione los tipos de objetos de programa que desea que los usuarios puedan ejecutar.

   Puede seleccionar *Ejecutar secuencias de comandos/binarios* o *Ejecutar programas de java*.

   Si ha seleccionado *Ejecutar programas de java*, puede activar o desactivar la casilla de verificación *Usar representación*. Esta opción proporciona al programa Java un token con el que se puede iniciar sesión en servicios de plataforma de información.
4. Haga clic en *Guardar y cerrar*.

> **Nota**
>
> Si actualiza a la plataforma de SAP BusinessObjects Business Intelligence 4.3 Support Package 3, los derechos del objeto de programa se rechazan para todos de forma predeterminada. Un usuario administrador (o cualquier usuario del grupo de administradores) puede activarlo.
>
> En *Ejecutar programas Java*, hay una casilla de verificación *Usar suplantación*. En 4.3 Support Package 3, se elimina la casilla de verificación *Usar suplantación*.

### 18.2.3.1.2 Registro de extensiones de procesamiento en el sistema

> **Nota**
>
> Esta función no se aplica a los documentos de Web Intelligence.

Antes de aplicar las extensiones de procesamiento a objetos particulares, es necesario que la biblioteca de códigos esté disponible en cada equipo que vaya a procesar las peticiones programadas o de vista

correspondientes. Al instalar la plataforma de BI se crea un directorio predeterminado para las extensiones de procesamiento en cada servidor de tareas, servidor de procesamiento y servidor de aplicaciones de informes (RAS). Se recomienda copiar las extensiones de procesamiento al directorio predeterminado en cada servidor. En Windows, el directorio predeterminado es `C:\Archivos de programa\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\ProcessExt`. En UNIX, es el directorio `sap_bobj/ProcessExt`.

> → Sugerencias
>
> Se puede compartir un archivo de extensión de procesamiento.

En función de la funcionalidad grabada en la extensión, copie la biblioteca en los equipos siguientes:

- Si la extensión de procesamiento intercepta solo peticiones programadas, copie la biblioteca en cada equipo que se ejecute como Servidor de tareas de Adaptive.
- Si la extensión de procesamiento solo intercepta peticiones de consulta, copie la biblioteca en cada equipo que se ejecute como un servidor de procesamiento de Crystal Reports o RAS.
- Si la extensión de procesamiento intercepta peticiones programadas y de consulta, copie la biblioteca en cada equipo que se ejecute como un servidor de tareas de Adaptive, servidor de procesamiento de Crystal Reports o RAS.

> ⓘ Nota
>
> Si la extensión de procesamiento es necesaria solo para solicitudes programadas o de consulta realizadas a un grupo de servidores en particular, solo deberá copiar la biblioteca en cada servidor de procesamiento del grupo.

## 18.2.3.1.2.1 Para registrar una extensión de procesamiento con el sistema

1. Vaya al área de administración *Aplicaciones* de la CMC.
2. Seleccione *Consola de administración central*.
3. Haga clic en *Acciones* > *Extensiones de procesamiento*.
   Aparecerá el cuadro de diálogo *Extensiones de procesamiento: CMC*.
4. En el campo *Nombre*, escriba un nombre para mostrar la extensión de procesamiento.
5. En el campo *Ubicación*, escriba el nombre del campo de la extensión de procesamiento junto con cualquier información adicional de ruta de acceso.
   - Si copió la extensión de procesamiento en el directorio predeterminado de cada uno de los equipos correspondientes, solo tiene que escribir el nombre (pero no la extensión del archivo).
   - Si copió la extensión de procesamiento en una subcarpeta situada debajo del directorio predeterminado, escriba la ubicación como: **`<subcarpeta>/<nombredearchivo>`**
6. Utilice el campo *Descripción* para agregar información acerca de la extensión de procesamiento.
7. Haga clic en *Agregar*.

> → Sugerencias
>
> Para eliminar una extensión de procesamiento, selecciónela en la lista *Extensiones existentes* y haga clic en *Eliminar*. (Asegúrese de que no haya tareas periódicas basadas en esta extensión de procesamiento porque fallará cualquier tarea futura basada en esta extensión de procesamiento.)

8. Haga clic en *Guardar y cerrar*.
   La extensión de procesamiento se registra con la CMC.

Ahora puede seleccionar esta extensión de procesamiento para aplicar su lógica a objetos particulares.

## 18.2.3.1.2.2 Compartir extensiones de procesamiento entre varios servidores

> ⓘ Nota
>
> Esta función no se aplica a los documentos o informes de Web Intelligence creados en SAP Crystal Reports para Enterprise.

Si desea agrupar todas las extensiones de procesamiento en una única ubicación, puede sobrescribir este directorio de extensiones de procesamiento predeterminado para cada servidor de tareas de Adaptive, servidor de procesamiento de Crystal Reports y RAS. En primer lugar, copie las extensiones de procesamiento en un directorio compartido de la unidad de red al que puedan tener acceso todos los servidores. Asigne, o monte, la unidad de red desde cada equipo del servidor.

> ⓘ Nota
>
> Las unidades asignadas en Windows son sólo válidas hasta que se reinicie el equipo.

Si los servidores se ejecutan en Windows y en UNIX, es necesario copiar una versión .dll y una versión .so de cada extensión de procesamiento en el directorio compartido. Además, la unidad de red compartida debe ser visible para los equipos de Windows y UNIX (a través de Samba o de algún otro sistema de archivos compartidos).

Finalmente, cambie la línea de comandos de cada servidor para modificar el directorio de extensiones de procesamiento predeterminado. Para modificar la línea de comandos, vaya a la ficha Servidores de la CMC, seleccione un servidor, y abra la página Propiedades. Agregue la ruta absoluta `-report_ProcessExtPath <>` a la línea de comandos. Reemplace `<ruta absoluta>` por la ruta a la nueva carpeta; para ello, utilice cualquier convención de ruta que sea adecuada para el sistema operativo en el que se ejecuta el servidor (por ejemplo, `M:\code\extensions`, `/home/shared/code/extensions`, etc.).

Para modificar el directorio predeterminado de las extensiones de procesamiento, utilice la CMC para detener el servidor. Después, abra las Propiedades del servidor para modificar la línea de comandos. Cuando haya acabado, vuelva a iniciar el servidor.

## 18.2.3.1.3 Administrar el acceso a la ficha CMC

### 18.2.3.1.3.1 Administración delegada y acceso a la ficha CMC

Normalmente, un administrador del sistema de la plataforma de BI administra un gran número de documentos, carpetas, usuarios, servidores y otros objetos. Sin embargo, los grandes entornos corporativos pueden superar los recursos de un único administrador. Un administrador del sistema que solo desee centrarse en tareas de alta prioridad puede crear administradores delegados y asignarles subconjuntos de tareas de administración (por ejemplo, la administración del contenido de un departamento o arrendatario). A diferencia de los administradores del sistema, los administradores delegados realizan un conjunto limitado de tareas y tienen menos derechos sobre los objetos del sistema.

La configuración predeterminada de la Consola de administración central permite a los usuarios acceder a todas las fichas CMC disponibles. El administrador del sistema puede administrar el acceso a la ficha CMC para controlar las fichas que son visibles para los principales (usuarios o grupos de usuarios). Para mejorar la experiencia del usuario y el flujo de trabajo del administrador delegado, un administrador del sistema también puede ocultar cualquier ficha CMC que el administrador delegado no vaya a usar.

> ⚠ Precaución
>
> La administración del acceso a la ficha CMC solo afecta al aspecto visual de la interfaz de usuario de la CMC. Ocultar las fichas CMC no es una medida de seguridad porque no configura o modifica los derechos de seguridad en los objetos de las fichas. Para garantizar que los usuarios no puedan realizar operaciones no autorizadas en objetos no autorizados (por ejemplo, administrar servidores a través del Administrador de configuración central o de software de terceros basado en el SDK de la plataforma de BI), debe configurar los derechos de seguridad adecuados en los objetos (como los objetos de servidor).

#### Información relacionada

Administrar el acceso a la ficha CMC para otros usuarios [página 708]
Administrar los permisos para configurar el acceso a la ficha CMC para otros usuarios o grupos de usuarios [página 709]

### 18.2.3.1.3.2 Trabajar con el acceso a la ficha CMC

#### 18.2.3.1.3.2.1 Administrar el acceso a la ficha CMC para otros usuarios

Un administrador del sistema siempre tiene acceso a todas las fichas CMC. Use las siguientes directrices para administrar las fichas CMC a las que los principales tienen acceso:

- Para obtener un proceso de administración simplificado y una necesidad reducida de mantenimiento y solución de problemas, se recomienda que los administradores administren el acceso a la ficha CMC en un nivel de grupo de usuario (en lugar de en un nivel de usuario).

- Para las fichas CMC que disponen de carpetas de nivel superior, un administrador debe conceder acceso a una ficha y conceder el derecho *Ver* en la carpeta de nivel superior de la ficha. Las siguientes fichas CMC admiten carpetas de nivel superior:
  - *Niveles de acceso*
  - *Calendarios*
  - *Categorías*
  - *Conexiones (Universo)*
  - *Claves criptográficas*
  - *Eventos*
  - *Federaciones*
  - *Carpetas*
  - *Bandejas de entrada*
  - *Conexión OLAP*
  - *Categorías personales*
  - *Carpetas personales*
  - *Perfiles*
  - *Listas de réplicas*
  - *Servidores y grupos*
  - *Almacenamiento temporal*
  - *Universos*
  - *Usuarios y grupos*
  - *Consulta de servicio web*
- Para mejorar la seguridad del sistema, solo los miembros del grupo de administradores pueden acceder a las siguientes fichas de la CMC. Como administradores del sistema, los miembros del grupo de administradores pueden acceder a cualquier ficha de CMC a pesar de los permisos de acceso a las fichas CMC. Los permisos de acceso a la ficha de la CMC están diseñados para controlar el acceso a las fichas de la CMC para administradores delegados; es decir, usuarios y no miembros del grupo de administradores.
  - *Auditoría*
  - *Autenticaciones*
  - *Claves criptográficas*
  - *Claves de licencia.*
  - *Supervisar*
  - *Sesiones*
  - *Configuración*
  - *Gestión de atributos de usuario*

> ⚠ Precaución
>
> La administración del acceso a la ficha CMC solo afecta al aspecto visual de la interfaz de usuario de la CMC. Ocultar las fichas CMC no es una medida de seguridad porque no configura o modifica los derechos de seguridad en los objetos de las fichas. Para garantizar que los usuarios no puedan realizar operaciones no autorizadas en objetos no autorizados (por ejemplo, administrar servidores a través del Administrador de configuración central o de software de terceros basado en el SDK de la plataforma de BI), debe configurar los derechos de seguridad adecuados en los objetos (como los objetos de servidor).

## 18.2.3.1.3.2.1.1 Administrar el acceso a la ficha CMC para otros usuarios

1. Inicie una sesión en la CMC.
2. En la ficha *Usuarios y grupos*, haga clic con el botón derecho en un principal y seleccione *Configuración de la ficha CMC*.

   > **Nota**
   >
   > Si el acceso a la ficha de la CMC no está restringido, se mostrará el mensaje siguiente: `Advertencia: el acceso a la ficha de la CMC no está restringido actualmente. Para restringir el acceso a CMC, haga clic en la ficha "Aplicación", seleccione "CMC," y establezca el acceso a la ficha CMC en restringido. Esta configuración tiene efecto una vez restringido el acceso a la ficha de la CMC.` Podrá seguir configurando el acceso a la ficha de la CMC. Sin embargo, la configuración no tendrá efecto hasta que se restrinja el acceso a la ficha CMC.

   En el cuadro de diálogo *Configurar el acceso a la ficha CMC*, se muestra una tabla:
   - □ o □ indica las fichas CMC a las que puede acceder el principal.
   - *Heredado* indica que el acceso a la ficha se heredó de sus grupos de usuarios principales.
   - *Explícito* indica que el acceso a la ficha se especificó explícitamente en el nivel principal.
3. Revise los derechos de acceso a la ficha CMC. Para modificar los derechos, puede usar los botones de la barra de herramientas:
   - Haga clic en *Conceder* para conceder explícitamente el acceso a una ficha.
   - Haga clic en *Denegar* para denegar explícitamente el acceso a una ficha.
   - Haga clic en *Heredar* para usar un derecho de acceso heredado.

   > **Nota**
   >
   > Hacer clic en los botones aplica los cambios en el principal inmediatamente.
4. Cuando haya terminado, haga clic en *Cerrar*.

El nuevo acceso a la ficha efectivo se muestra en la columna *Permisos* de la tabla.

### Información relacionada

Restringir el acceso a la ficha CMC [página 711]

## 18.2.3.1.3.2.1.2 Herencia del acceso a la ficha CMC

Los derechos de acceso a la ficha CMC y el permiso para configurar el acceso a la ficha CMC para otros usuarios o grupos de usuarios se aplican y heredan del mismo modo que otros derechos de seguridad de la plataforma de BI. Si los principales no tienen especificado explícitamente el acceso a la ficha, heredarán el acceso a la ficha de los grupos de usuarios de los que sean miembros.

Si un usuario es miembro de dos grupos de usuarios, el acceso a la ficha se calcula del mismo modo en que se calculan el resto de derechos de la plataforma de BI. Por ejemplo, si se concede el acceso a una ficha CMC en uno de los grupos y se deniega para el otro, el principal no podrá acceder a la ficha CMC.

> **Nota**
>
> - Modificar el derecho de acceso a la ficha CMC de un grupo de usuarios cambia el mismo acceso a la ficha para todos los usuarios o grupos de usuarios que heredan derechos desde el grupo de usuarios, si el acceso a la ficha CMC se configura en *Heredado*.
> - El acceso a la ficha que se configura en un nivel de usuario siempre sustituye el acceso a la ficha heredado de los grupos de usuarios.

## 18.2.3.1.3.2.1.3 Grupos de usuarios de administradores delegados

Puede crear un conjunto de grupos de usuarios de administradores delegados para simplificar la administración de la ficha CMC. Para evitar configurar el acceso individual a la ficha CMC, puede hacer que un usuario o grupo de usuarios existente sea miembro de un grupo de usuarios de administradores delegados. Se recomienda la siguiente configuración pero se puede modificar según necesidades empresariales específicas.

> **Nota**
>
> Ser miembro de varios grupos dará como resultado en la adición de derechos, si los derechos se configuran en *Heredado*.

| Grupo de usuarios de administradores delegados | Derechos recomendados |
|---|---|
| Administradores del sistema | Conceder acceso a todas las fichas. |
| Administradores de usuarios | Conceda el acceso a *Niveles de acceso*, *Carpetas*, *Bandejas de entrada*, *Carpetas personales*, *Categorías personales*, *Resultados de consulta*, *Sesiones* y *Usuarios y grupos*. Configure el resto de fichas en *Heredado*. |
| Administradores de contenido | Conceda el acceso a *Calendarios*, *Categorías*, *Eventos*, *Carpetas*, *Administrador de instancias*, *Categorías personales*, *Carpetas personales*, *Perfiles*, *Resultados de consulta* y *Universos*. Configure el resto de fichas en *Heredado*. |
| Administradores de servidores | Conceda el acceso a *Servidores* y *Aplicaciones.* Configure el resto de fichas en *Heredado*. |

## 18.2.3.1.3.2.1.4 Administrar los permisos para configurar el acceso a la ficha CMC para otros usuarios o grupos de usuarios

En un entorno corporativo grande, es posible que un administrador de sistemas necesite delegar la administración del acceso a la ficha CMC a un administrador delegado. De forma alternativa, en un

sistema de varios arrendatarios, cada arrendatario puede tener un administrador delegado responsable de la administración del acceso a la ficha CMC para otros usuarios y grupos de usuarios.

1. Inicie una sesión en la CMC.
2. En la ficha *Usuarios y grupos*, haga clic con el botón derecho en un principal y seleccione *Configuración de la ficha CMC*.
   En el cuadro de diálogo *Configurar el acceso a la ficha CMC*, se muestra *Permiso para configurar el acceso a la ficha CMC para otros usuarios o grupos de usuarios* para el principal.

   > **Nota**
   >
   > Si se concede este permiso, el principal podrá administrar el acceso a la ficha CMC (solo para las fichas a las que tenga acceso el principal) para los usuarios para los que el principal tiene el derecho *Modificar de forma segura los derechos*. Además, el principal podrá delegar más tarde la administración del acceso a la ficha CMC para otros usuarios al conceder el *Permiso para configurar el acceso a la ficha CMC para otros usuarios o grupos de usuarios* a los usuarios para los que el principal tiene el derecho *Modificar de forma segura los derechos*.

   - ☐ o ☐ indica si el principal tiene permiso para configurar las fichas CMC para los otros usuarios o grupos de usuarios.
   - *Heredado* indica que el permiso se heredó de sus grupos de usuarios principales.
   - *Explícito* indica que el permiso se especificó explícitamente en el nivel principal.
3. Revise los permisos para configurar el acceso a la ficha CMC para otros usuarios o grupos de usuarios.
   Para modificar los permisos, puede seleccionar una de las siguientes configuraciones de la lista:

   - Haga clic en *Conceder* para conceder explícitamente el permiso para administrar el acceso a la ficha CMC para otros usuarios o grupos de usuarios.
   - Haga clic en *Denegar* para denegar explícitamente el permiso para administrar el acceso a la ficha CMC para otros usuarios o grupos de usuarios.
   - Haga clic en *Heredar* para heredar el permiso para administrar el acceso a la ficha CMC para otros usuarios o grupos de usuarios.

   > **Nota**
   >
   > Seleccionar una configuración de la lista cambia el permiso del principal inmediatamente.
4. Cuando haya terminado, haga clic en *Cerrar*.

Se muestra el nuevo permiso efectivo.

## Información relacionada

Administración delegada y acceso a la ficha CMC [página 706]
Herencia del acceso a la ficha CMC [página 708]

## 18.2.3.1.3.2.1.5 Para agregar una ficha Personalización a un usuario o grupo de usuarios

El acceso a la ficha de la CMC se debe fijar en «Restringido» antes de que pueda agregar la ficha *Personalización* a un usuario o grupo de usuarios.

1. En la CMC, vaya al área de administración *Usuarios y grupos*.
2. Haga clic con el botón derecho en un usuario o grupo de usuarios y seleccione *Configuración de la ficha CMC*.

   Aparece el cuadro de diálogo *Configurar fichas de CMC*, que lista cada título de ficha de CMC y el nivel de permisos, para el grupo de usuarios.

   Si aparece el siguiente mensaje de advertencia en rojo en la parte superior del cuadro de diálogo, debe establecer el acceso de la ficha CMC en restringido antes de que pueda agregar una ficha *Personalización*:

   ```
   Advertencia: el acceso a la ficha CMC no está restringido actualmente. Para
   restringir el acceso a CMC, haga clic en la ficha "Aplicación", seleccione
   "CMC," y establezca el acceso a la ficha CMC en restringido. Esta configuración
   tiene efecto una vez restringido el acceso a la ficha CMC:
   ```
3. (En caso necesario) Para establecer el acceso a la ficha CMC en restringido:
   a. En el área de administración *Aplicaciones* de la CMC, haga clic con el botón derecho en *Consola de administración central* y seleccione *Configuración de acceso a ficha CMC*.
   b. En *acceso a la ficha CMC*, seleccione la opción *Restringido*, y haga clic en *Guardar y cerrar*.
4. En el cuadro de diálogo *Configurar fichas de CMC* para el grupo de usuarios, para cada ficha de CMC, seleccione *Concedido*, *Denegado*, o *Heredado* en la lista.
   Cada vez que cambie el permiso de una ficha, el cuadro de diálogo Configurar fichas de CMC actualiza el permiso del grupo de usuarios para configurar el acceso a la ficha para otros usuarios o grupos de usuarios.
5. Haga clic en *Cerrar*.

## 18.2.3.1.3.2.2 Restringir el acceso a la ficha CMC

Se recomienda configurar primero el acceso a la ficha CMC para los principales y, a continuación, restringir el acceso a la ficha CMC. Si se restringe el acceso a la ficha antes de configurarlo, los usuarios no podrán acceder a ninguna de las fichas CMC hasta que un administrador les conceda acceso.

Para garantizar la coherencia con versiones anteriores de la plataforma de BI, el acceso a la ficha CMC no se restringe inicialmente después de instalar la plataforma de BI y cualquier usuario que pueda acceder a la CMC podrá acceder a todas las fichas disponibles. Para evitar que los usuarios accedan a las fichas a las que no tienen derechos de acceso, un administrador del sistema puede restringir el acceso a la ficha CMC.

Puede eliminar la restricción de acceso a la ficha CMC en un caso urgente o para solucionar problemas de configuración de acceso a la ficha CMC (por ejemplo, si un administrador delegado no puede acceder a una ficha CMC importante).

1. Inicie una sesión en la CMC.
2. En la ficha *Aplicaciones*, haga clic con el botón derecho en *Consola de administración central* y seleccione *Configuración de acceso a la ficha CMC*.

Se muestra el cuadro de diálogo *Acceso a la ficha CMC*.

3. Configure la regla de acceso a la ficha CMC.
   - Para limitar el acceso de los usuarios a las fichas de las que tienen derechos, seleccione *Restringido*.
   - Para permitir que los usuarios accedan a todas las fichas, seleccione *Sin restringir*.
4. Al finalizar, haga clic en *Guardar y cerrar*.

La regla de acceso a la ficha CMC se aplica al sistema.

## Información relacionada

Solucionar problemas de acceso a la ficha CMC [página 712]

# 18.2.3.1.3.2.3 Solucionar problemas de acceso a la ficha CMC

Para evitar el acceso sin autorización o para solucionar el acceso limitado de un usuarios a las fichas CMC, puede solucionar los problemas de derechos de acceso a la ficha CMC de un usuario.

1. Inicie sesión en la CMC como administrador.

   > **Nota**
   >
   > Asegúrese de que tiene acceso a la ficha que desea solucionar y de que dispone del derecho *Modificar de forma segura los derechos* en el usuario.

2. En la ficha *Usuarios y grupos*, haga clic con el botón derecho en un principal y seleccione *Configuración de la ficha CMC*.
   Se muestra la ventana *Configurar el acceso a la ficha CMC*.
3. Revise el acceso a la ficha CMC efectivo. Puede conceder o denegar explícitamente el acceso a las fichas disponibles.

   Si el acceso a la ficha CMC es heredado, pero el acceso a la ficha efectiva no coincide con las necesidades del usuario:
   a. Recopile una lista de todos los grupos de usuarios de los que el principal seleccionado sea miembro.
   b. Repita los pasos 1 a 3 para cada grupo del que el usuario herede el acceso a la ficha.
   c. Corrija el acceso a la ficha CMC en el nivel de principal o bajo el nivel de grupo, según sea necesario.

   > **Nota**
   >
   > Realizar esta tarea en el nivel de grupo afecta al acceso a la ficha CMC de todos los usuarios que sean miembros de dicho grupo de usuarios, y de todos los usuarios que sean miembros de los grupos de usuarios heredados de este grupo de usuarios, siempre y cuando los usuarios tengan el acceso a la ficha CMC configurado en *Heredado*.

4. Cuando haya terminado, haga clic en *Cerrar*.

## Información relacionada

Administrar el acceso a la ficha CMC para otros usuarios [página 708]
Herencia del acceso a la ficha CMC [página 708]

## 18.2.3.2 Administración de la configuración de la rampa de lanzamiento BI

En esta sección se describe cómo puede gestionar las siguientes opciones en la rampa de lanzamiento BI:

- Modificar las opciones de visualización para la plataforma de BI.
- Configuración de los detalles de URL de RESTful en la Consola de administración central para el inicio de sesión en la rampa de lanzamiento BI.
- Definición de la visibilidad de la ficha Autenticación y el CMS en la rampa de lanzamiento BI.
- Configuración del vínculo de correo electrónico para la opción *Ponerse en contacto con el administrador* en la rampa de lanzamiento BI.

### 18.2.3.2.1 Configuración de los detalles de URL de RESTful URL en la CMC para el inicio de sesión en la plataforma de lanzamiento de BI tipo Fiori

Tras instalar o actualizar BI 4.2 SP4, debe configurar la URL del servicio web REST para que un usuario pueda iniciar sesión en la plataforma de lanzamiento de BI tipo Fiori.

Para configurar los detalles del servicio web RESTful en la CMC, realice los siguientes pasos:

1. Inicie sesión en la CMC como administrador.
2. Vaya a *Gestionar* > *aplicaciones* > *Servicios Web RESTful* > *Propiedades*.
3. Proporcione la URL WACS (nombre de host o nombre cualificado completo en el que se desplegó el servidor WACS).

### 18.2.3.2.2 Configuración de proxy para activar el Web Assistant en la rampa de lanzamiento BI de Fiori

Tras instalar o actualizar BI 4.2 SP5, debe configurar las parametrizaciones de proxy para que un usuario pueda acceder a la ayuda de la aplicación del Web Assistant en la rampa de lanzamiento BI de Fiori.

Para configurar las parametrizaciones de proxy para el Web Assistant en la rampa de lanzamiento BI de Fiori, realice los siguientes pasos:

**Requisitos previos:**

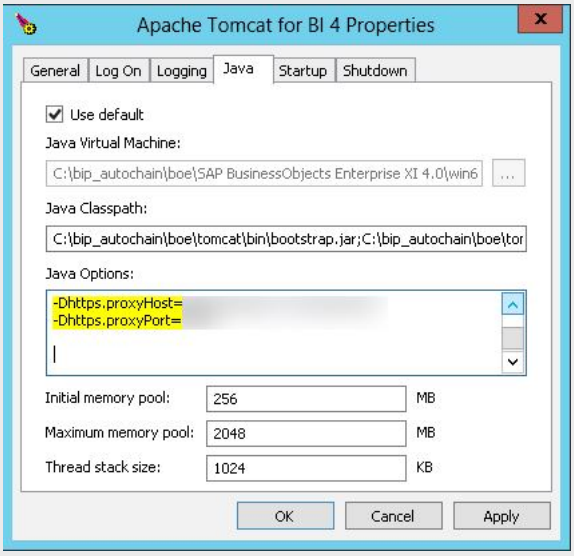
Está conectado a Internet.

1. Navegue a las propiedades del sistema del servidor Web.
2. Añada las propiedades `https.proxyHost` y `https.proxyPort`.

Ejemplo

SO: Windows, servidor Web: Tomcat 8.5

1. Navegue a *Windows* > *Tomcat*.
   Se abre la ventana *Propiedades de Apache Tomcat para BI 4*.
2. Seleccione la ficha *Java*.
3. En el campo de opciones de Java, añada las siguiente propiedades en la lista:
   `-Dhttps.proxyHost=<proxy_host>`
   `-Dhttps.proxyPort=<proxy_port>`
4. Reinicie Tomcat.




## 18.2.3.2.3 Configuración del vínculo de correo electrónico para la opción Ponerse en contacto con el administrador en la plataforma de lanzamiento de BI tipo Fiori

Para configurar el vínculo de correo electrónico para la opción *Ponerse en contacto con el administrador* en la plataforma de lanzamiento de BI tipo Fiori, siga los siguientes pasos:

1. Vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

Si tiene la versión de Tomcat instalada con la plataforma de BI, también puede acceder a la siguiente ubicación: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.

2. Cree un nuevo archivo con el bloc de notas y guarde el archivo con el siguiente nombre: 'FioriBI.properties'.
3. Modifique la siguiente propiedad en el archivo: `admin.user.email=administrator@bilp.com`, para incluir el ID de correo electrónico del administrador.

## 18.2.3.2.4 Definición de la visibilidad de la ficha Autenticación y el CMS en la plataforma de lanzamiento de BI tipo Fiori

Para definir la visibilidad de la ficha Autenticación y el CMS en la plataforma de lanzamiento de BI tipo Fiori, siga los siguientes pasos:

1. Vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

   Si usa el software Tomcat instalado con la plataforma de BI, también puede acceder a la siguiente ubicación: `C:\Program Files (x86)\SAP BusinessObjects\Tomcat\webapps\BOE\WEBINF\config\custom`.
2. Cree un nuevo archivo con el bloc de notas y guarde el archivo con el siguiente nombre: 'FioriBI.properties'.
3. Para incluir las opciones de autenticación en la pantalla de inicio de sesión de la plataforma de lanzamiento de BI, añada lo siguiente: `authentication.visible=true`.

   Sustituya <authentication> por los tipos de autenticación predeterminados: “secEnterprise, secLDAP, secWinAD, secSAPR3”.
4. Para cambiar el tipo de autenticación predeterminado, añada lo siguiente: `authentication.default=<authentication>`.
5. Para solicitar a los usuarios un nombre de CMS en la pantalla de inicio de sesión de la plataforma de lanzamiento de BI, añada lo siguiente: `cms.visible=true`.
6. Guarde y cierre el archivo.
7. Reinicie el servidor de aplicaciones Web.

## 18.2.3.2.5 Cambiar la configuración de visualización para la plataforma de BI

1. Vaya al área *Aplicaciones* de la CMC y haga doble clic en *Plataforma de lanzamiento de BI*.
   Aparece el cuadro de diálogo *Propiedades de la plataforma de lanzamiento de BI*.
2. Para habilitar los filtros para la programación, seleccione la casilla de verificación *Mostrar la ficha "Filtros" en la página Programar*.

   Esta configuración controla si los usuarios pueden introducir fórmulas de selección de grupos o registros al programar un informe de Crystal.

3. Haga clic en *Guardar y cerrar*.

## 18.2.3.3 Administrar la configuración de Web Intelligence

Las funciones a las que pueden acceder los usuarios para los documentos de Web Intelligence se controlan definiendo las propiedades de la aplicación Web Intelligence.

### 18.2.3.3.1 Para modificar la configuración de visualización de Web Intelligence

1. Vaya al área *Aplicaciones* de la CMC y seleccione *Web Intelligence*.
2. Haga clic en *Administrar* > *Propiedades.*
   Aparece el cuadro de diálogo *Propiedades*.
3. Defina cualquiera de las siguientes opciones de visualización.

| Opción | Descripción |
|---|---|
| *Opciones de visualización de datos modificados* > *Dimensiones y detalles* | Utilice las opciones de esta área para definir cómo aparecerán los datos agregados en los informes; cambie el estilo de fuente, color de texto y color de fondo. Una vista previa de celda muestra automáticamente los cambios. Al terminar, haga clic en *Aceptar*. |
| *Opciones de visualización de datos modificados* > *Valores fluctuantes (indicadores numéricos)* | Utilice las opciones de esta área para modificar y dar formato al encabezado de página; cambie el estilo de fuente, color de texto y color de fondo. Una vista previa de celda muestra automáticamente los cambios. Al terminar, haga clic en *Aceptar*. |
| *Propiedades de imagen incrustada* | Introduzca el tamaño máximo de imagen incrustada. |
| *Soporte para mapas geográficos*: | Habilite o deshabilite el soporte de mapas geográficos en Web Intelligence. |
| *Propiedades del modo de presentación rápida* | En los campos adecuados, introduzca el máximo de registros verticales, el máximo de registros horizontales, la anchura mínima de la página, la altura mínima de la página, el valor de relleno a la derecha y el valor de relleno inferior. |
| *Configuración del guardado automático* | Establezca el intervalo en el que se guardan automáticamente los documentos. Este intervalo se reinicia cada vez que un documento se guarda manualmente o automáticamente. El documento guardado automáticamente también se elimina al guardar un documento automáticamente. |
| *Actualización automática* | Habilita la actualización automática de los documentos de Web Intelligence cuando se selecciona la propiedad de documentos de Web Intelligence *Actualización automática*. |

| Opción | Descripción |
| --- | --- |
| | Para obtener más detalles, consulte el *Manual de actualización a SAP BusinessObjects Web Intelligence*. |
| *Fusión automática* | Habilita la fusión automática de dimensiones cuando la propiedad del documento de Web Intelligence *Fusión automática de dimensiones* está seleccionada.<br><br>Para obtener más detalles, consulte el *Manual de actualización a SAP BusinessObjects Web Intelligence*. |
| *Actualizar el documento automáticamente en Abrir configuración de derecho de seguridad* | Borre esta opción para habilitar que Web Intelligence actualice documentos automáticamente al abrirse, sin habilitar *Actualizar al abrir* en las propiedades del documento de Web Intelligence. Al seleccionar esta opción, se selecciona el derecho de seguridad *Documentos: deshabilitar la actualización automática al abrir*. |
| *Vista inteligente* | Esta opción determina la versión del documento que se muestra cuando los usuarios abren documentos en Web Intelligence.<br>• Ver instancia más reciente<br>La instancia más reciente del objeto se abre. Por ejemplo, si un documento se programa para que se actualice cada hora, y el documento se guardó y cerró por última vez hace cinco horas, se abre la instancia más reciente.<br>• Ver objeto<br>El documento se abre en el mismo estado en que estaba cuando se guardó por última vez, independientemente de cualquier actualización programada que se haya llevado a cabo. |
| *JavaScript* | Su selección aquí define la renderización de celdas con Leer contenido como HTML o Leer contenido como hipervínculo en documentos de Web Intelligence:<br>• *Deshabilitar JavaScript y habilitar hipervínculos y solo los elementos HTML utilizados por Web Intelligence*<br>Esta opción predeterminada permite hipervínculos y el conjunto limitado de elementos HTML necesario para funciones de Web Intelligence. Elimina JavaScript y los demás elementos HTML de los documentos.<br>• *Habilitar solo elementos HTML definidos en la página de elementos HTML autorizados*<br>Esta opción solo habilita los elementos y atributos HTML que especifica en la página *Elementos HTML autorizados*.<br>• *Habilitar JavaScript, elementos HTML e hipervínculos*<br>Esta opción habilita todo, JavaScript, elementos HTML e hipervínculos.<br><br>Siempre que cambie la opción, para ver las modificaciones en Web Intelligence, salga y vuelva a entrar en la aplicación.<br><br>⚠ Precaución<br>• Web Intelligence permite el código JavaScript/HTML integrado en las celdas de documentos gracias a las funciones de las fórmulas.<br>Este código se puede activar o desactivar en la Consola de administración central. Sin embargo, al autorizar JavaScript, HTMLs e hipervínculos, reconoce el riesgo de estar exponiéndose al cross-site scripting. El cross-site scripting permite a los atacantes alterar sitios web o ejecutar código en otros sistemas. Esta vulnerabilidad |

| Opción | Descripción |
| --- | --- |
| | afecta a productos como navegadores de Internet cuando están ejecutando scripts. La mayoría de los ataques de cross-site scripting son el resultado de una programación no segura en el sistema de destino.<br>• El código se puede ajustar mediante la autorización de etiquetas HTML y atributos *BI Admin Studio* > *Aplicaciones* > *Elementos HTML*.<br>Sin embargo, SAP no se hace responsable de la compatibilidad del código y sus posibles efectos secundarios. Por ejemplo, puede que sea necesario adaptar el código debido a actualizaciones del navegador, soporte de versión JavaScript o el modo en que el código se incrusta de forma dinámica en la página web. El código puede requerir ajustes para ejecutarse en ese nuevo contexto. |
| *Alineación de contenido para documentos nuevos* | Utilice estas opciones para definir si el contenido del documento nuevo debe alinearse de derecha a izquierda, de izquierda a derecha o si debe depender de la configuración regional de visualización preferida por el usuario y/o la configuración regional del producto. |
| *Features Toggle* | Utilice este campo de texto para introducir conmutadores para activar las funciones de vista previa. Estos conmutadores también se pueden utilizar en las notas SAP para modificar el comportamiento predeterminado. Esta lista de conmutadores debe introducirse como una lista con formato JSON. |

4. Haga clic en *Guardar y cerrar*.

> **Nota**
>
> Para revertir la selección a las variables de presentación predeterminadas, haga clic en *Restablecer*.

## 18.2.3.3.2 Servicios de Elementos personalizados

Los Elementos personalizados son visualizaciones cuya representación se delega a servicios de terceros mediante Web Intelligence.

En los documentos de Web Intelligence, los Ementos personalizados se integran y visualizan como cualquier otro elemento de informe (gráficos, tablas, etc.). Los servicios de Elementos personalizados deben configurarse primero en la CMC a fin de que los usuarios finales puedan visualizar Elementos personalizados en documentos de Web Intelligence.

Puesto que sus datos se transferirán entre el servidor BOE y el servidor de terceros de elementos personalizados, se recomienda desplegar el servidor de Elementos personalizados en su intranet. Si no es posible, se recomienda utilizar solamente HTTPS para acceder al servidor de Elementos personalizados.

> **Precaución**
>
> El servicio de elementos personalizados que despliega añade un código a Web Intelligence y puede generar problemas potenciales de seguridad como cross-site scripting. Cross-site scripting permite que acceda al código de ejecución y ejecutar scripts en equipos de otros usuarios. Un mensaje de advertencia de seguridad le pregunta por su consentimiento explícito antes de desplegar el servicio de elementos personalizados. Su consentimiento es obligatorio para desplegar el servicio de elementos personalizados.

## Migración

Al migrar un documento de Web Intelligence de un CMS a otro, el servicio de Elementos personalizados utilizado para crear contenido en este documento deberá ser creado de nuevo en el nuevo CMS con el mismo nombre. Si el servicio de Elementos personalizados no se vuelve a crear (con el mismo nombre) en el nuevo CMS, los Elementos personalizados del documento migrado ya no se podrán modificar.

## 18.2.3.3.2.1 Para añadir un servicio de elementos personalizados

Para que los usuarios finales puedan utilizar elementos personalizados, como administrador debe especificar primero el servicio de terceros que gestiona la representación. Por defecto, no hay ningún servicio de elementos personalizados activado. Esta configuración es opcional y se debe habilitar en la CMC.

Ha añadido la URL del servicio personalizado a la lista de URL de confianza. Si no lo ha hecho, consulte la sección Añadir URLs de confianza a la lista de URLs autorizados [página 724].

1. Abra la Consola de administración central.
2. Haga clic en *Aplicaciones*.
3. Haga clic con el botón derecho en *Web Intelligence*.
4. Haga clic en *Propiedades*.
5. Haga clic en *Elementos personalizados*.
6. Haga clic en *Añadir servicio*.
7. Asigne un nombre al servicio.

   > ⚠ Precaución
   >
   > El nombre del servicio se visualizará tal como está en los clientes Web Intelligence y debe ser único. No puede reutilizar un nombre de servicio que ya existe. Si modifica el nombre de un servicio, ya no se podrán modificar los elementos personalizados creados con este servicio en los documentos de Web Intelligence.

8. Indique una URL con el número de puerta.
9. Haga clic en *Probar*.
10. Seleccione un *Tipo de medio*.

    Web Intelligence puede consumir tanto tipos de medios HTML como de mapa de bits. El tipo de medio preferido es HTML (text/html), que permite interactuar entre clientes de Web Intelligence y una mejor experiencia del usuario. Los tipos de medios de mapa de bits pueden ser .PNG (imagen/png), .JPG (imagen/JPG) o .GIF (imagen/gif).

11. Introduzca el *DPI de imagen*.

    > ⓘ Nota
    >
    > Se trata de la resolución de las imágenes de mapa de bits generadas por el servicio. Se necesita un formato de mapa de bits para publicar informes de Web Intelligence con el formato PDF o Excel, en los que los elementos personalizados se representan como imágenes. Sin un formato de mapa de bits, estas publicaciones mostrarán un bloque vacío en lugar del elemento personalizado previsto.

12. Haga clic en *Aceptar*.

> **Nota**
>
> Puede utilizar varios servicios de elementos personalizados a la vez. Un solo servicio puede proporcionar varios elementos personalizados.

### Información relacionada

URLs que autorizan [página 723]

## 18.2.3.3.3 Actualización paralela del proveedor de datos

La actualización paralela del proveedor de datos mejora el rendimiento de la actualización de datos en documentos de Web Intelligence que contienen múltiples proveedores de datos.

Para actualizar consultas en paralelo, Web Intelligence distribuye todos los proveedores de datos en diferentes threads. Esta propiedad se activada de forma predeterminada y Web Intelligence puede actualizar hasta 64 consultas en paralelo. Los proveedores de datos basados en conexiones relacionales, OLAP y BICS se admiten, así como proveedores de datos personales (archivos de texto, FHSQL).

> **Restricción**
>
> No se admiten proveedores de datos Excel.

Puede reducir este valor en la consola de administración central si el hardware que ejecuta Web Intelligence no soporta esta carga de trabajo. Compruebe que su hardware tenga suficientes núcleos como para garantizar un rendimiento óptimo.

Están disponibles dos parámetros globales en la consola de administración central:

- *Máximo de consultas paralelas por documento*: Fije el número máximo de proveedores de datos que Web Intelligence puede actualizar en paralelo por documento. El valor predeterminado es 64.
- *Activar consultas paralelas para programación*. Active o desactive el procesamiento paralelo de consultas al programar documentos. Esta opción se activa de manera predeterminada.

También animamos a ajustar cada conexión a una base de datos con parámetros que permitan especifican el número de consultas que se pueden ejecutar en paralelo. Este parámetro, llamado máximo de consultas paralelas, está disponible:

- En la consola de administración central o herramienta de diseño de información para conexiones OLAP y BICS.
- En la herramienta de diseño de información o herramienta de diseño de universos para conexiones relacionales.

Para cada conexión, el número de proveedores de datos que se puede actualizar en paralelo está fijado en 4 por defecto. El administrador de la base de datos puede modificar este valor según el hardware de la base de datos. Sin embargo, para ficheros de texto, el valor por defecto se fija en 1.

## Ejemplo

En este ejemplo, todos los valores predeterminados se han guardado y cada conexión admite un máximo de 4 tareas de actualización paralelas.

| Conexión | Cantidad de proveedores de datos a actualizar |
|---|---|
| 2 conexiones OLAP | 6 (5 en conexión 1, 1 en conexión 2) |
| 1 conexión relacional | 2 |
| 1 conexión BICS | 2 |
| Ficheros Excel de un proveedor de datos personales | 2 |

Ambos ficheros Excel se actualizan secuencialmente pues no los admite la función de actualizar del proveedor de datos paralelo.

Cuatro de los proveedores de datos de la primera conexión OLAP se actualizan en paralelo en los threads 1, 2, 3 y 4. El quinto se pone en cola y se procesará después de que un proveedor de datos (o cualquier conexión) se haya actualizado, mientras que el que proviene de la segunda conexión OLAP se actualizará en el threar 5 puesto que es de una conexión diferente.

Los cuatro proveedores de datos de la primera conexión OLAP se actualizan en paralelo en los threads 5, 6, 7 and 8.

> **Nota**
>
> Siempre que la cantidad de proveedores de datos del mismo tipo sea superior al valor por defecto, se pondrán en cola y esperarán a que terminen otros proveedores de datos.

## Información relacionada

Modificar el número de proveedores de datos actualizados en paralelo por documento [página 721]
Modificar el número de proveedores de datos actualizados en paralelo para una conexión OLAP específica [página 722]

# 18.2.3.3.3.1 Modificar el número de proveedores de datos actualizados en paralelo por documento

1. En la página de inicio de la CMC, haga clic en *Servidores*.
2. Haga clic en *Servicios de Web Intelligence*.
3. Haga clic con el botón derecho del ratón en *Servidor de procesamiento de Web Intelligence* y haga clic en *Propiedades*.
4. En el campo de entrada *Máximo de consultas paralelas* introduzca un número.

   El rango de valores posibles es de 0 a 64.

> **Nota**
>
> Si introduce 0 desactiva la función de actualización de proveedor de datos paralelo.

### 18.2.3.3.3.2 Desactivar el procesamiento paralelo de consulta programación

1. En la página de inicio de la CMC, haga clic en *Servidores*.
2. Haga clic en *Servicios de Web Intelligence*.
3. Haga clic con el botón derecho del ratón en *Servidor de procesamiento de Web Intelligence* y haga clic en *Propiedades*.
4. Desmarque *Activar consultas paralelas para programación*.

### 18.2.3.3.3.3 Modificar el número de proveedores de datos actualizados en paralelo para una conexión OLAP específica

1. En la página de inicio, haga clic *conexiones OLAP*.
2. Vaya a la conexión que quiere configurar y haga clic con el botón derecho del ratón.
3. Seleccione *Organizar* > *Editar*.
4. En el campo de entrada *Máximo de consultas paralelas* introduzca un número.

   El rango de valores posibles es de 1 a 64.

   > **Nota**
   >
   > Si introduce 1 los proveedores de datos se actualizan secuencialmente.

### 18.2.3.3.4 Protección para exportaciones CSV

Web Intelligence proporciona una medida de seguridad para evitar la inyección de comandos cuando los usuarios abren un fichero CSV generado desde un documento en Microsoft Excel. Puede desactivar esta protección para exportaciones CSV.

Por defecto, Web Intelligence añade un espacio antes de los caracteres siguientes en la exportación a CSV o un archivo CSV:

- = (Igual)
- + (más)

- - (menos)
- @ (en)

El espacio adicional impide que valores con estos caracteres sean ejecutados como comandos, lo que podría ocasionar un problema de seguridad en su sistema.

### Información relacionada

Desactivar la protección para exportaciones CSV [página 723]

## 18.2.3.3.4.1 Desactivar la protección para exportaciones CSV

Si desea desactivar le medida de seguridad por defecto en Web Intelligence que evita la inyección de comandos cuando los usuarios abren un archivo CSV exportado en Microsoft Excel, modifique la clave de registro correspondiente.

Establezca el valor de la clave de registro `EscapeCharactersForCSVExport` como falso para desactivar la medida de seguridad. Por defecto, la clave de registro no está presente y su valor es verdadero, por lo que quizá tenga que crearla para establecer el valor como falso.

El cambio surte efecto después de que los usuarios de Web Intelligence cierren y vuelvan a abrir la aplicación.

Modifique la clave de registro de la siguiente manera:

- En Windows, en los equipos del cliente y del servidor, establezca la clave de registro como falsa: `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.
- En UNIX, en los equipos del servidor, en `$installdir/setup/boconfig.cfg`, establezca la clave de declaración de registro como falsa `HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects\Suite XI 4.0\default\WebIntelligence\EscapeCharactersForCSVExport`.

## 18.2.3.3.5 URLs que autorizan

Web Intelligence usa URLs para:

- Hipervínculos en el documento
- Hipervínculos en sugerencias de petición
- Imagen de fondo
- Fuente de datos OData
- Elementos personalizados o extensiones externas

Estos URLs pueden potencialmente crear amenazas de seguridad.

Como administrador, debe crear en la Consola de administración central una lista de URLs de confianza que los usuarios puedan utilizar. Esta lista controla el uso de estas URL en Web Intelligence.

### 18.2.3.3.5.1 Añadir URLs de confianza a la lista de URLs autorizados

Siempre que desee utilizar una URL en Web Intelligence como hipervínculo en el documento o una sugerencia de petición, una imagen de fondo, una fuente de datos OData o un nuevo servicio personalizado o extensión externa, primero debe autorizarlo.

1. En la pantalla de inicio de la Consola de administración central, haga clic en *Aplicaciones*.
2. Seleccione *Web Intelligence*.
3. En el menú contextual, seleccione *Propiedades*.
4. Seleccione la sección *Categoría de URLs autorizados*.
5. Haga clic en el botón *Añadir un URL nuevo* para añadir un URL de confianza.
6. En el campo *URL autorizado*, especifique un URL único, con su protocolo, nombre de host y puerto.

   > → Sugerencias
   >
   > Puede escribir el carácter * para autorizar cualquier URL para hipervínculo, imagen de fondo o fuente de datos OData. A continuación, debe hacer clic en la casilla de verificación *Acepto el riesgo* para confirmar que entiende el riesgo potencial para activar todos los URL.

7. Si el URL introducido es un URL para una extensión o un servicio de elemento personalizado al que se puede acceder a través de un proxy, puede marcar la casilla de selección *Si este URL se utiliza para un elemento personalizado o una extensión que requiere un proxy, introduzca su servidor y puerto* para fijar este servidor proxy y puerto.
8. Haga clic en *Aceptar*.

## 18.2.3.4 Administración de la configuración de Crystal Reports

### 18.2.3.4.1 Activación de la vista inteligente en Crystal Reports

1. Vaya al área *Aplicaciones* de la CMC y seleccione *Crystal Reports*.
2. Seleccione *Gestionar* > *propiedades*
   Aparece el cuadro de diálogo *Propiedades*.
3. Seleccione *Plataforma de lanzamiento de BI*.
4. Defina la siguiente opción de visualización:

| Opción | Descripción |
| --- | --- |
| *Vista inteligente* | Esta opción determina la versión del documento que se muestra cuando los usuarios abren un Crystal report.<br>• Ver instancia más reciente<br>La instancia correcta más reciente del objeto se abre. Por ejemplo, si un documento se programa para que se actualice cada hora, y el documento se guardó y cerró por última vez hace cinco horas, se abre la instancia correcta más reciente.<br>• Ver objeto<br>El documento se abre en el mismo estado en que estaba cuando se guardó por última vez, independientemente de cualquier actualización programada que se haya llevado a cabo. |

## 18.2.3.4.2 Habilitar la biblioteca de funciones de usuario Java para Crystal Reports para Enterprise

Puede visualizar y programar el informe que contiene la biblioteca de funciones de usuario Java (UFL). Siga los siguientes pasos:

1. Inicie sesión en CMC.
2. Seleccione *Aplicaciones* de la lista desplegable.
3. Seleccione *Configuración de Crystal Reports*.
4. En el panel izquierdo, bajo *Propiedades*, seleccione *Crystal Reports para Enterprise*.
5. Seleccione la opción *Añadir nuevas* e introduzca las siguientes propiedades:

| Propiedad | Valor | Información adicional |
| --- | --- | --- |
| classpath | Ruta de clase a las UFL Java. | • Use punto y coma como carácter separador para varios contenedores.<br>• Tiene que utilizar doble barra invertida (\\) o una barra (/) en su lugar.<br>Ejemplo: C:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\java\\lib\\MyFirstUFL.jar |
| ExternalFunctionLibraryClassNames.classname | El nombre plenamente cualificado de la UFL. | Ejemplo: samples.ufl.InternationalizationLibrary |

6. Reiniciar servicios relacionados con Crystal Reports.
   Ahora puede ejecutar la visualización y programación de workflows.

### 18.2.3.4.3 Habilitar la biblioteca de funciones de usuario .NET/COM para Crystal Reports para Enterprise

Puede visualizar y programar el informe que contiene la biblioteca de funciones de usuario .NET/COM (UFL). Siga los siguientes pasos:

1. Copie la versión de 64 bits de .Net UFL en `<Install Directory>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

   > **Nota**
   >
   > El diseñador de Crystal Reports para Enterprise es de 64 bits y, por lo tanto, requiere una .NET UFL de 64 bits, mientras que los servicios de Crystal Reports para Enterprise en Business Intelligence Platform son de 64 bits y, por lo tanto, requieren una .NET UFL de 64 bits.

2. Registrar y GAC los 64 bits con "regasm <dll> and “gacutil /if <dll>".
3. Inicie sesión en la CMC.
4. Seleccione *Aplicaciones* de la lista desplegable.
5. Seleccione *Configuración de Crystal Reports*.
6. En el panel izquierdo, bajo *Propiedades*, seleccione *Crystal Reports para Enterprise*.
7. Seleccione la opción *Añadir nuevas* e introduzca la siguiente propiedad:

| Categoría | Propiedad | Valor |
|---|---|---|
| Deje la columna vacía. | NonJavaExternalFunctionLibraries.managerDirectory | Ruta al archivo UFL de 64 bits.<br>• Tiene que utilizar doble barra invertida (\\) o una barra (/) en su lugar.<br>Ejemplo: C:\\Program Files (x86)\\SAP BusinessObjects\\SAP BusinessObjects Enterprise XI 4.0\\win64_x64). |

8. Reiniciar servicios relacionados con Crystal Reports.
   Ahora puede ejecutar la visualización y programación de workflows.

### 18.2.3.5 Administración de valores del servicio de alertas

En el área *Aplicaciones* de la CMC de la plataforma de BI, puede especificar los valores del sistema para las alertas.

Para la aplicación *Servicio de alertas*, puede controlar y definir el modo en que los usuarios del sistema acceden a las alertas mediante:

- La habilitación de la carpeta *Mis alertas* para los suscriptores de alertas
- La habilitación y el formato de mensajes de alerta enviados por correo electrónico

- La definición de un límite para el número de alertas en el sistema
- La definición de un periodo de vencimiento para los mensajes de alertas

## Información relacionada

Configuración de derechos de usuario en aplicaciones [página 700]

# 18.2.3.5.1 Para modificar las propiedades de destino de las alertas

1. En el área *Aplicaciones* de la CMC, haga doble clic en *Aplicación de envío de alertas*.
2. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Alertas*.
3. (Obligatorio) Realice una de las siguientes acciones:
   - Seleccione *Habilitar Mis alertas* para habilitar que los suscriptores de las alertas reciban notificaciones en *Mis alertas* en la plataforma de lanzamiento de BI.
   - Seleccione *Habilitar correo electrónico* para habilitar que los suscriptores de alertas reciban notificaciones por correo electrónico.
     Aparecen las opciones globales de correo electrónico para alertas.
4. Si ha seleccionado *Habilitar correo electrónico*, lleve a cabo las acciones siguientes:
   - En el cuadro *De*, introduzca la dirección de correo electrónico desde el que se enviarán las notificaciones de alerta.
     Los suscriptores recibirán correos electrónicos de alerta desde esta dirección de correo electrónico.
     Use una dirección de correo electrónico válida que el sistema reconozca.
   - En el cuadro *A*, introduzca la dirección de correo electrónico del suscriptor de la alerta.
     De forma predeterminada, todas las alertas del sistema se enviarán a esta dirección de correo electrónico.

     > → Sugerencias
     >
     > No especifique ninguna dirección de correo electrónico o destinatario. Use el marcador de posición *%SI_EMAIL_ADDRESS%*.
   - En el cuadro *cc*, introduzca la dirección de correo electrónico de cada destinatario que deba recibir copias de las alertas.
   - En el cuadro *Asunto*, introduzca un encabezado de asunto predeterminado para usarlo en los correos electrónicos que contengan alertas.
   - En el cuadro *Mensaje*, introduzca un mensaje predeterminado para incluirlo en los correos electrónicos que contengan alertas.
   - Seleccione *Agregar adjunto* para permitir que se incluyan datos adjuntos de forma predeterminada en los correos electrónicos que contengan alertas.
     Por ejemplo, seleccione esta opción para incluir informes de Crystal asociados con alertas desencadenadas.

- Si ha seleccionado *Agregar adjunto*, en *Nombre de archivo* seleccione *Generado automáticamente* o *Nombre específico* para indicar cómo nombrar los adjuntos de los correos electrónicos.

5. Haga clic en *Guardar y cerrar*.

### Información relacionada

Configuración de derechos de usuario en aplicaciones [página 700]
Administración de valores del servicio de alertas [página 726]

## 18.2.3.5.2 Modificar las propiedades predeterminadas del servicio de alertas

1. Vaya al área *Aplicaciones* de la CMC y seleccione *Aplicación de alertas*.
2. Haga clic en *Administrar* > *Propiedades* > *Configuración predeterminada*.
3. Configure los valores apropiados para las siguientes propiedades.

| Opción | Descripción |
|---|---|
| *Período de vencimiento* | Especifica durante cuánto tiempo se conservarán los mensajes de alerta en el sistema antes de eliminarlos. |
| *Número máximo de mensajes de alerta* | Especifica el número máximo límite de los mensajes de alerta que admite el sistema. Cuando se alcanza el umbral, el sistema eliminará el 20% de los mensajes de alerta, empezando por los mensajes más antiguos. |

4. Haga clic en *Guardar y cerrar*.

### Información relacionada

Administración de valores del servicio de alertas [página 726]

## 18.2.3.6 Administrar la configuración de la aplicación Comentario BI

Comentario BI es una aplicación que se ha introducido en el CMC. Permite a los usuarios documentarse para colaborar comentando cualquiera de los datos o estadísticas disponibles en un documento determinado.

Con Comentario BI los usuarios pueden publicar comentarios sobre datos/estadísticas dentro de los informes.

→ Recomendación

Por defecto, Comentario Bi crea y actualiza sus tablas en la base de datos de Auditoría.

> ⓘ Nota
>
> Para usar Comentario BI con la base de datos de auditoría en una plataforma que no sea de Windows, consulte el Manual de acceso de datos para configurar los controladores de ODBC.

Sin embargo, SAP le recomienda que configure una nueva base de datos para guardar los comentarios de la aplicación Comentario BI. Las bases de datos compatibles con Comentario BI son las mismas que las compatibles con Auditoría. Las bases de datos soportadas y los correspondientes JAR JDBC certificados para Comentario BI incluyen:

- IBM DB2 Workgroup Edition - db2jcc4.jar
- Microsoft SQL Server - sqljdbc4.jar
- MySQL - com.mysql.jdbc_5.1.5.jar
- Oracle - ojdbc6.jar
- SAP HANA - ngdbc.jar
- Sybase Adaptive Server Enterprise - jconn4.jar
- Sybase SQL Anywhere - jconn4.jar

> ⓘ Nota
>
> Independientemente de si elige configurar comentarios BI con base de datos de auditoría u otra base de datos soportada, para que comentarios BI funcione con la base de datos MySQL, tendrá que ubicar el fichero MySQL jdbc jar en la siguiente ubicación: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.
>
> Si configura Comentario BI con IBM DB2, necesitará un espacio de tabla temporal en el sistema con un tamaño de página de 8K, 16K o 32K. De forma predeterminada, el tamaño de la página es de 4K.

> ⓘ Nota
>
> Si la base de datos Auditoría no está configurada/habilitada por defecto, Comentario BI no está activa hasta que configure manualmente una nueva base de datos para Comentario BI.
>
> Si configura Comentario BI con base de datos de auditoría y borra la base de datos de auditoría, también se borran todos los comentarios almacenados en la base de datos de auditoría.
>
> La base de datos Auditoría utiliza o tipos de controladores de bases de datos ODBC o nativos. Para configurar una nueva base de datos para Comentario, necesita un Controlador JDBC.

> ⓘ Nota
>
> El tamaño de un comentario está limitado a 2000 UTF - 8 bytes de caracteres o 666 UTF-16 bytes de caracteres.

> ⓘ Nota
>
> No puede migrar comentarios con la Herramienta de federación.

> **Nota**
>
> Comentario BI no está soportado para las conexiones MaxDB.

> **Nota**
>
> Para borrar entradas de comentarios realizadas por el usuario, utilice la siguiente consulta:
>
> `DELETE from dba.COMMENTARY_MASTER where UserName ='<User Name>'`

## 18.2.3.6.1 Configurar una nueva base de datos de comentario BI

Ha creado una conexión JBDC.

> **Nota**
>
> Cuando configura una nueva base de datos de Comentario BI, el servicio de comentarios alojado en el servidor de procesamiento de Adaptative es responsable de escribir la información de Comentario en la base de datos. Los siguientes pasos deberán seguirse en cada equipo en el clúster donde se está ejecutando el Servicio Comentario.

Para crear una nueva conexión JDBC, realice los siguientes pasos:

1. Coloque el controlador jar JBDC para la base de datos que desee configurar en la siguiente ubicación: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

   > **Nota**
   >
   > Si actualiza a la plataforma SAP BusinessObjects Business Intelligence 4.2 Support Package 2 y ya tiene configurada una base de datos para Comentario BI de las versiones anteriores, debe mover el archivo de controlador de la base de datos de la carpeta "jdbc" de `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib\external>` a `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\BICommentaryService\lib>`.

2. Reinicie SIA.

Para configurar una nueva base de datos para Comentario BI, proceda de la forma siguiente:

1. Inicie una sesión en CMC.
2. Desde la página de inicio de CMC, seleccione *Aplicaciones* del menú desplegable.
3. En a lista *Nombre de aplicación* seleccione *Aplicación Comentario BI*.

   Aparece la ventana emergente *Comentario BI*. El botón de selección *Utilizar base de datos de auditoría* está seleccionado.
4. Seleccione el botón de selección *Utilizar otra base de datos que se soporte*.
5. Indicar el *Tipo*, *Nombre de base de datos*, *Host*, *Puerta*, *Nombre de usuario*, y *Contraseña* en el panel *Configurar base de datos del comentario*.

6. Seleccione *Guardar y cerrar*
7. Reinicie APS.

   Cualquier cambio realizado en la configuración de la base de datos de Comentario de BI solo se aplicará tras reiniciar el Servidor de procesamiento de Adaptive (APS).

   Valide la conexión seleccionando *Probar conexión*.

   > **Nota**
   >
   > Si actualiza a la plataforma de SAP BusinessObjects Business Intelligence 4.3 Support Package 3 y ya había configurado una base de datos para Comentario de BI para JDBC desde las versiones anteriores, el campo de contraseña ahora estará en blanco al seleccionar *Probar conexión*, *Guardar y cerrar* o *Guardar*.

   Puede seleccionar borrar o limpiar comentarios más antiguos verificando la casilla de selección *Borrar comentarios más antiguos que* y especificando el número de días.

   > **Nota**
   >
   > Debe reiniciar todos los servidores APS que albergan un servicio Comentario BI para que las modificaciones tengan efecto.

Ahora ya ha configurado una nueva base de datos para almacenar comentarios de la aplicación Comentario BI.

## 18.2.3.7 Gestionar las opciones de la aplicación BI Admin Studio

> **Nota**
>
> Para acceder a BI Admin Studio, debe formar parte del grupo de administradores.

Si deniega derechos de acceso concretos como: *Permitir el acceso al cockpit de administración de BI*, *Permitir el acceso a la supervisión* y *Permitir el acceso a Diferencia visual*, es posible que no pueda acceder a la aplicación específica en BI Admin Studio.

| Specific Rights for BI Admin Studio | Implicit Value |
|---|---|
| Allow access to BI Admin Cockpit | Granted |
| Allow access to Monitoring | Granted |
| Allow access to Visual Difference | Granted |
| Visual Difference - Create comparison | Granted |
| Visual Difference - Delete comparison | Granted |
| Visual Difference - Rerun comparison | Granted |
| Visual Difference - View comparison | Granted |

Si se deniegan los derechos de *Diferencia visual*, también podrá restringir el uso de la aplicación VD.

## 18.2.3.8 Administrar la integración de aplicaciones de colaboración

Esta guía es específica para los administradores de la plataforma de BI que integrarán la plataforma de BI con una aplicación de colaboración de SAP Jam.

Utilice el área de *Aplicaciones* de la Consola de administración central (CMC) en la plataforma de BI para activar y configurar la colaboración.

Se necesita la siguiente configuración adicional en el agente de Enterprise de la aplicación de colaboración:

- Establecer una conexión HTTPS con un proveedor de servicios
- Cumplir con los requisitos previos para la autenticación

Después de configurar SAP Jam, los alimentadores de la aplicación de colaboración estarán disponibles en la plataforma de lanzamiento de BI.

SAP Jam no soporta Microsoft Internet Explorer 11.

### 18.2.3.8.1 Requisitos previos de colaboración

Los requisitos previos de colaboración se tienen que cumplir antes de integrar la plataforma de BI con una aplicación de colaboración.

- La plataforma de BI debe estar instalada con al menos un Servidor de administración central (CMS).
- La aplicación de colaboración (SAP Jam) se tiene que configurar en la Consola de administración central (CMC).
- Se debe definir una organización de Enterprise de la aplicación de colaboración (SAP Jam).
- Los usuarios de SAP Jam deben pertenecer a la organización de Enterprise.
- Se necesita un agente de Enterprise de SAP Jam para proporcionar usuarios que utilicen un servicio de directorios LDAP/AD.

### 18.2.3.8.2 Configuración de la plataforma de BI

#### 18.2.3.8.2.1 Opciones de configuración de colaboración

Aparecen opciones de colaboración en *Propiedades:*Cuadro de diálogo *Colaboración* en la Consola de administración central (CMC) de la plataforma de BI.

Para acceder a *Propiedades:*Cuadro de diálogo *Colaboración*, en la ficha *Aplicaciones* en la CMC, haga clic en *Colaboración*, y seleccione *Administrar* > *Propiedades*.

| Opción | Descripción |
| --- | --- |
| *Habilitar colaboración* | Seleccione esta casilla de verificación y seleccione *SAP Jam*. |
| *URL de conexión* | Escriba el URL a la aplicación de colaboración. |
| *ID de proveedor de identidades único* | Introduzca un valor único para el despliegue de la plataforma de BI.<br>Este valor se asociará al certificado que se usa para configurar la integración en la consola de administración de la aplicación de colaboración. La aplicación que reafirma una identidad para un inicio de sesión único debe configurarse como una aplicación administrativa modelo. |
| *Certificado Base64 de proveedor de identidades* | Al hacer clic en *Generar*, se crea un certificado en esta casilla. Use este certificado en la consola de administración de la aplicación de colaboración para generar una clave de consumidor OAuth.<br>Este certificado establece la relación de confianza entre la aplicación de colaboración y la plataforma de BI. El proveedor de identidad externa se identifica con un certificado X509, que se usa para firmar todas las reafirmaciones de identidad. El certificado debe estar codificado como Base64. |
| *Clave de consumidor OAuth* | Indique la clave de consumidor OAuth generada en la consola de administración de aplicación de colaboración. |
| *Conectando con proxy* | Marque esta casilla de selección para habilitar conexiones mediante proxy, e indique información acerca del host de proxy en las casillas *Host de proxy HTTP* y *Puerto*.<br>Para permitir conexiones entrantes de los servidores de la aplicación de colaboración a la red corporativa, debe tener un proxy inverso en el DMZ.<br>Para agregar un certificado de confianza de un proveedor de certificados SSL al proxy inverso, debe tener un nombre de dominio o subdominio para el proxy inverso.<br>*Host proxy HTTP*: En la configuración de proxy inverso, escriba una dirección externa a la que pueda acceder la aplicación de colaboración. Por ejemplo, utilice `https://<ReverseProxy>/`, en que `<ReverseProxy>` es el dominio o subdominio del proxy inverso.<br>La aplicación de colaboración usa esta dirección para enviar información a la plataforma de BI. El proxy inverso utiliza esta dirección para redirigir la información que recibe de la aplicación de colaboración al equipo que contiene el agente de Enterprise de la aplicación de colaboración.<br>*Puerto*: El agente de Enterprise de la aplicación de colaboración se configura para escuchar desde el puerto 8443. |

## 18.2.3.8.2.2 Habilitación y configuración de la colaboración en la CMC

Esta tarea necesita una conexión válida a la consola de administración de la aplicación de colaboración (SAP Jam). Necesitará pasar y recuperar los detalles de seguridad desde la consola.

Por motivos de seguridad, las siguientes cuentas predeterminadas no pueden enviar o programar contenido en SAP Jam:

- Invitado
- SMAdmin
- Administrador
- WaaWSServletPrincipal

1. En la Consola de administración central (CMC) de la plataforma de BI, vaya al área *Aplicaciones*, y haga doble clic en *Colaboración*.
2. En el cuadro de diálogo *Propiedades:Colaboración*, seleccione la casilla de verificación *Habilitar colaboración* y seleccione *SAP Jam*.
3. En el cuadro *URL de conexión*, escriba la dirección URL para la aplicación de colaboración.
4. En el cuadro *ID de proveedor de identidades único*, escriba un valor de proveedor de identidades único para el despliegue de la plataforma de BI.

   Anote el valor del proveedor de identidades; lo usará para configurar la aplicación de colaboración.
5. Haga clic en *Generar* (r *Regenerar*, si ya se ha creado un certificado antes).
   El certificado aparece en el cuadro *Certificado Base64 del proveedor de identidades*. Usará el certificado para configurar la aplicación de colaboración.
6. En el cuadro *Clave de consumidor OAuth*, introduzca una clave de consumidor OAuth válido.
7. Si está conectado a través de proxy al servidor que ejecuta SAP Jam, lleve a cabo las siguientes acciones:
   a. Seleccione la casilla de verificación *Conectando con proxy*.
   b. En el cuadro *Host proxy http*, escriba el nombre del host proxy del servidor.
   c. En el cuadro *Puerto*, introduzca el número de puerto del servidor.
8. Haga clic en *Guardar y cerrar*.

## 18.2.3.8.3 Configuración de SAP Jam

### 18.2.3.8.3.1 Registro de un IDP de confianza de SAML nuevo para SAP Jam

Debe registrar cada usuario con una dirección de correo electrónico única que se corresponda con la dirección de correo electrónico de Enterprise del usuario en la plataforma de lanzamiento de BI. Las direcciones de correo electrónico se asignarán entre la plataforma de BI y SAP.

Antes de poder registrar un nuevo IDP de confianza SAML:

- Se debe agregar y configurar la empresa en SAP.
- Debe disponer de una cuenta de usuario de SAP válida asociada a su empresa en SAP.
- Debe disponer de derechos de administración de su empresa en SAP y derechos de administración completos en la plataforma de BI y la plataforma de lanzamiento de BI.
- La plataforma de lanzamiento de BI debe estar registrada como un cliente OAuth que actúe como un representante de la plataforma de lanzamiento en SAP.

SAP Jam no soporta Microsoft Internet Explorer 11.

1. En la esquina derecha superior de la consola de administración central (CMC) en la plataforma de BI, seleccione *Administrador* y después seleccione *Administración*.
   Se visualizará información sobre su empresa, incluyendo la licencia SAP. Apunte o tome nota de la información.
2. Desde el menú *Administración*, seleccione *ID de confianza de SAML* y haga clic en *Registrar su proveedor de identidad*.

   Debe registrar el IDP que ha creado en la plataforma de lanzamiento de BI.
3. En el cuadro *ID de IDP*, introduzca el valor del proveedor de identidad único que se creó al configurar SAP en la plataforma de BI.

   Si no dispone del valor, póngase en contacto con el administrador de aplicaciones externas.

   Introduzca, por ejemplo, **`<NombreEmpresa>_<IDSistema>_<Cliente>`**.
4. En el cuadro *URL de inicio de sesión único*, introduzca la URL que proporciona acceso directo a SAP.

   SAP usa esta dirección URL para el inicio de sesión único con el proveedor de identidades único.
5. En el cuadro *URL de cierre de sesión único*, escriba la dirección URL para mostrar después de cerrar sesión en SAP.

   SAP usa esta dirección URL para el cierre de sesión único con el proveedor de identidades único.
6. En el cuadro *Formato de ID de nombre predeterminado*, introduzca el formato del ID de nombre para usar en las solicitudes de autenticación.
7. En el cuadro *Calificador de nombre SP de la política de ID de nombre predeterminado*, introduzca el calificador de nombre SP para usar en las solicitudes de autenticación.
8. En la lista *Alcance de la aserción permitida*, seleccione *Usuarios en mi empresa*.

   Esta opción especifica el conjunto de usuarios para los que SAP aceptará aserciones desde IDP.
9. En el cuadro *Certificado X509 (Base64)*, introduzca el valor del certificado Base64 que se generó al configurar SAP en la plataforma de BI.

   Si no dispone del valor, póngase en contacto con el administrador de aplicaciones externas.
10. Haga clic en *Registrar*.

## 18.2.3.8.3.2 Creación de un cliente OAuth desde SAP Jam

Antes de poder crear un calve de consumidor OAuth:

- Se debe agregar y configurar la empresa en SAP Jam.
- Debe disponer de una cuenta de usuario de SAP Jam válida asociada a la empresa en SAP Jam.
- Debe disponer de derechos de administración de la empresa en SAP Jam y derechos de administración completos en la plataforma de BI y en la plataforma de lanzamiento de BI.
- La plataforma de lanzamiento de BI debe estar registrada con SAP Jam como un cliente OAuth que actúe como un representante de la plataforma de lanzamiento en SAP Jam.
- Cada usuario debe estar registrado en SAP Jam con una dirección de correo electrónico única que se corresponda a la dirección de correo electrónico de Enterprise del usuario en la plataforma de lanzamiento de BI. Las direcciones de correo electrónico se asignarán entre la plataforma de BI y SAP Jam.

SAP Jam no soporta Microsoft Internet Explorer 11.

1. En SAP Jam, desde el menú *Administrator* (Administrador) de la esquina superior derecha, seleccione *Admin*.

Aparecerá información sobre su empresa, incluyendo la licencia SAP Jam

2. Desde el menú *Administración*, seleccione *Clientes OAuth* y haga clic en *Agregar cliente OAuth*.
3. En el cuadro de diálogo *Registrar un cliente OAuth nuevo*, en el cuadro *Nombre*, introduzca el valor de proveedor de identidad único que se creó al configurar SAP Jam en la plataforma de BI.

   Si no dispone del valor, póngase en contacto con el administrador de aplicaciones externas.

   SAP Jam muestra el nombre de la aplicación como un hipervínculo (a esta dirección URL) cuando realiza una acción en nombre de un usuario.

   Introduzca, por ejemplo, **`<Nombre Empresa>_<IDSistema>_<Cliente>_<Aplicación>`**
4. En el cuadro *Integration URL*, introduzca la URL para la plataforma de lanzamiento de BI.

   SAP Jam muestra el nombre de la aplicación como un hipervínculo a esta URL cuando realiza una acción en nombre de un usuario.
5. En el cuadro *Certificado X509 (Base64)*, introduzca el valor del certificado Base64 que se generó al configurar SAP Jam en la plataforma de BI.

   Si no dispone del valor, póngase en contacto con el administrador de aplicaciones externas.

   Si deja este cuadro en blanco, SAP Jam proporciona un secreto de consumidor.
6. Haga clic en *Guardar*.

Se genera la clave de consumidor OAuth. Tome nota del valor de la clave de consumidor OAuth para que lo use el administrador de la plataforma de BI.

## 18.2.3.9 Administración del servicio de notificaciones push en SAP BusinessObjects Mobile

El servidor SAP BusinessObjects Mobile pasa notificaciones a dispositivos iOS de usuarios de la aplicación SAP BusinessObjects Mobile. Las notificaciones se pasan en los escenarios siguientes:

- Cuando los documentos BI descargados en un dispositivo de usuario tienen una actualización o una nueva instancia disponible en el servidor.
- Cuando un documento nuevo llega a la Bandeja de entrada de usuario BI.
- Cuando la plataforma de BI o el administrador BOE envía un mensaje.

Las notificaciones se pasan automáticamente al dispositivo desde el servidor Mobile mediante Apple Push Notification Server (APNS). Los usuarios no tienen que conectarse al servidor para recibir las notificaciones push. Un usuario puede recibir notificaciones push incluso cuando la aplicación no se ejecuta en el sistema. La "Configuración de notificaciones" debe estar activa en la aplicación. Para más información sobre cómo configurar notificaciones push, consulte *Despliege del servidor Mobile y manual de configuración* para el servidor Mobile 4.2.

> **Nota**
>
> A fin de activar las notificaciones push en Mobile, BIMobileService se debe ejecutar en la APS.
>
> Dado que BIMobileService no consume mucha memoria, puede ejecutarlo junto otros servicios en la APS.

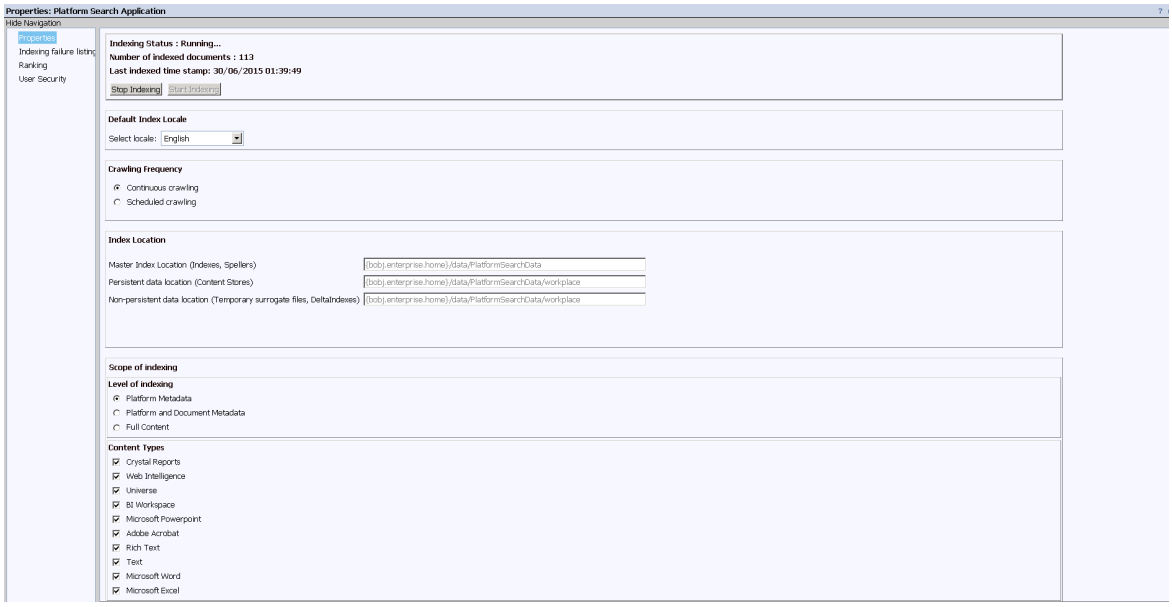
## 18.2.3.10 Administración de la configuración de Búsqueda de plataforma

En el área *Aplicaciones* de la CMC de la plataforma de BI, puede especificar los valores del sistema para la aplicación de búsqueda en plataforma.

### 18.2.3.10.1 Configurar las propiedades de aplicaciones en la CMC

Para configurar las propiedades de la aplicación de búsqueda en plataforma, complete esos pasos:

1. Vaya al área *Aplicaciones* de CMC.
2. Seleccione la *aplicación de búsqueda en plataforma*.
3. Haga clic en *Administrar* > *Propiedades*. Aparece el cuadro de diálogo *Propiedades de la aplicación de búsqueda en plataforma*.




4. Configurar los ajustes de búsqueda de la plataforma:

| Opción | Descripción |
|---|---|
| Estadísticas de búsqueda | Búsqueda de plataforma ofrece las siguientes estadísticas de búsqueda:<br>• Estado de indexación: muestra el estado del proceso de indexación.<br>• Cantidad de documentos indexados: muestra el número de documentos indexados.<br>• Cronomarcador de última indexación: muestra la fecha y la hora de la última indexación del documento. |

| Opción | Descripción |
| --- | --- |
| Iniciar/detener indexación | Las opciones Iniciar o detener indexación permiten iniciar o detener el proceso de indexación cuando desee alternar de la inspección continua a la inspección programada, o por motivos de mantenimiento.<br><br>Para detener la indexación, haga clic en *Detener indexación*. |
| Configuración regional del índice predeterminada | La búsqueda de plataformas usa la configuración regional especificada en la CMC para indexar todos los documentos de BI no localizados. Una vez que se localiza el documento, se usa el analizador de idioma correspondiente para la indexación.<br><br>La búsqueda se basa en la configuración regional del producto del cliente, y la ponderación se proporciona en la configuración regional del producto del cliente.<br><br>Puede configurar la ponderación en las propiedades de configuración de la CMC. |
| Frecuencia de inspección | Puede indexar todo el repositorio de la plataforma de BI mediante las opciones siguientes:<br>• Inspección continua: con esta opción, la indexación es continua cuando se indexa el repositorio, siempre que se agrega, modifica o elimina un objeto. Permite ver o trabajar con el contenido de la plataforma de BI más actualizado. Por defecto, la inspección continua actualiza constantemente el repositorio con las acciones que realice. La inspección continua trabaja sin la intervención del usuario y reduce el tiempo necesario para indexar un documento.<br>• Inspección programada: con esta opción, la indexación se basa en la programación definida con las opciones de programación.<br>Para obtener información acerca de la programación de un objeto, consulte la sección *Programar un objeto* de la Búsqueda de plataformas de la *Ayuda online de la CMC de la plataforma de SAP BusinessObjects Business Intelligence*.<br><br>**Nota**<br>• Si selecciona *Inspección programada* y define la *Periodicidad* con una opción que no sea *Ahora*, la búsqueda de plataformas muestra la marca de fecha y hora cuando se programa el documento para que se indexe a continuación.<br>• Si selecciona *Inspección programada*, el botón *Iniciar indexación* se activa y el botón *Detener indexación* se desactiva.<br>• Una vez completada la programación, el botón *Detener indexación* se desactiva. |

| Opción | Descripción |
| --- | --- |
| Ubicación de índice | Los índices se almacenan en carpetas compartidas en las siguientes ubicaciones:<br>• Ubicación del índice maestro (índices y corrector ortográfico): los índices maestros y el corrector ortográfico que se almacenan en esta ubicación. Durante una búsqueda, los resultados iniciales se recuperar mediante el Índice maestro y los índices de corrector ortográfico se usan para recuperar sugerencias. En un despliegue de la plataforma de BI en clúster, esta ubicación debe estar en un sistema de archivos compartido al que se pueda acceder desde todos los nodos del clúster.<br>• Ubicación de datos persistentes (almacenes de contenido): el almacén de contenido se encuentra en esta ubicación. Se crea desde la ubicación de índice maestro y permanece en sincronización con ella. El almacén de contenido se usa para generar facetas y procesar los resultados iniciales que se generan desde la ubicación del índice maestro. En un despliegue de la plataforma de BI en clúster, los almacenes de contenido se generan en cada nodo.<br>La ubicación de datos persistentes es la única ubicación de índice que se ve afectada por el entorno en clúster ya que contiene carpetas de almacén de contenido. Si un equipo tiene un único servicio de búsqueda, existirá una sola ubicación de contenido. Por ejemplo, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores.<br>Sin embargo, si en un entorno agrupado existen varios servicios de búsqueda, cada servicio tendrá una única ubicación de almacén de contenido. Por ejemplo, si existen dos instancias de un servidor que se están ejecutando, las ubicaciones del almacén de contenido serán las siguientes:<br>1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nombre de servidor>\ContentStores.<br>2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nombre de servidor 1>\ContentStores.<br>• Ubicación de datos no persistentes (archivos temporales, índices Delta): en esta ubicación, los índices Delta se crean y almacenan temporalmente antes de fusionarse con el índice maestro. Los índices desde esta ubicación se eliminan cuando se han fusionado con el índice maestro. Además, los archivos suplentes (fuera de los extractores) se crean en esta ubicación y se almacenan temporalmente hasta que se convierten en índices delta.<br>**Nota**<br>• La ubicación del índice maestro tiene que ser una ubicación compartida.<br>• Debe hacer clic en *Detener indexación* para modificar la ubicación del índice.<br>• Si modifica la ubicación de un índice, debe copiar el contenido en una nueva ubicación, de lo contrario la información de indexación se perderá.<br>• Los archivos de indexación pueden almacenar información personal y confidencial, especialmente cuando seleccione indexar el contenido del documento. Debe permitir solo a un usuario del sistema acceder a la carpeta compartida y debe almacenar las carpetas compartidas en un entorno encriptado para evitar el robo de datos. |

| Opción | Descripción |
| --- | --- |
| Nivel de indexación | Puede ajustar el contenido de la búsqueda definiendo el nivel de indexación de los modos siguientes:<br>• Metadatos de plataforma: solo se crea un índice para la información de los metadatos de la plataforma, como títulos, palabras clave y descripciones de los documentos. De forma predeterminada se selecciona esta opción.<br>• Metadatos de plataforma y documento: este índice incluye los metadatos de la plataforma, así como los metadatos del documento. Los metadatos del documento incluyen la fecha de creación, la fecha de modificación y el nombre del autor.<br>• Contenido completo: este índice incluye los metadatos de plataforma, metadatos de documentos y otro contenido como:<br>  • El contenido real del documento<br>  • El contenido de las solicitudes y LOV<br>  • Diagramas, gráficos y etiquetas<br>**Nota**<br>La indexación completa de contenido no es compatible con documentos de Analysis Office y Lumira. Solo la indexación de metadatos es compatible con documentos de Analysis Office y Lumira.<br>**Nota**<br>Al modificar el nivel de indexación, se inicializa la indexación para que se actualice todo el repositorio de la plataforma de BI. |

| Opción | Descripción |
| --- | --- |
| Tipos de contenido | Puede seleccionar los siguientes tipos de contenido para la indexación:<br>• Crystal Reports<br>• Web Intelligence<br>• Universo<br>• Área de trabajo de BI<br>• Analysis Office<br>• Lumira<br>• Microsoft PowerPoint<br>• Adobe Acrobat<br>• Texto enriquecido<br>• Texto<br>• Microsoft Word<br>• Microsoft Excel<br><br>El filtro del tipo de contenido no se aplica para la indexación de metadatos de la plataforma. Independientemente de los tipos de contenido que seleccione, la indexación de metadatos de la plataforma tiene lugar para todos los tipos de objeto soportados y los resultados de la búsqueda en la plataforma de lanzamiento de BI devuelven todos los objetos para la palabra clave relacionada con los metadatos de la plataforma.<br><br>El filtro del tipo de contenido es relevante para la indexación de metadatos de la plataforma (autor, cabecera, pie de página, etc. del documento) y la indexación de contenido (gráficas, gráficos, tabla con un informe). Según el nivel de indexación y los tipos de contenido que seleccione, la plataforma busca índices para los metadatos del documento y el contenido para los tipos de objetos seleccionados del repository y solo aquellos objetos que aparezcan en los resultados de la búsqueda de la plataforma de lanzamiento de BI, al buscar palabras clave relacionadas con los metadatos y contenido del documento. |
| Regenerar índice | Esta opción elimina el índice existente y vuelve a indexar todo el repositorio.<br><br>Puede seleccionar la opción *Regenerar índice* tanto si la indexación se está ejecutando o está detenida. El índice existente se elimina al guardar las modificaciones realizadas en la página de propiedades. Sin embargo, si la indexación está detenida, el índice no se vuelve a generar hasta que reinicia la indexación.<br><br>Si no desea que la búsqueda en plataforma vuelva a indexar los documentos, debe anular la selección de *Regenerar índice* antes de hacer clic en *Iniciar indexación*. |

| Opción | Descripción |
| --- | --- |
| Documentos excluidos de la indexación | La opción *Documentos excluidos de la indexación* excluye de la indexación los documentos. Por ejemplo, puede que no desee que se puedan buscar informes de Crystal extremadamente grandes para asegurar que los recursos del servidor de aplicaciones de informes no se sobrecargan. De igual modo, puede que no desee que se indexen publicaciones con cientos de informes personalizados.<br><br>Al excluir documentos concretos, puede evitar que la Búsqueda de plataforma acceda a ellos. Es importante tener en cuenta que si un documento ya se ha indexado antes de ponerlo en esta categoría, se podrán seguir realizando búsquedas en él. Para asegurar que los documentos del grupo *Documentos excluidos de la indexación* no se puedan buscar, debe volver a crear el índice.<br><br>De forma predeterminada, solo la cuenta del administrador tiene control completo de la opción *Documentos excluidos de la indexación*. Otros usuarios con los siguientes derechos solo pueden agregar documentos al grupo *Documentos excluidos de la indexación*:<br>• Derechos de visualización y edición en la categoría<br>• Editar el documento directamente |
| Otra configuración: Omitir instancia | Por defecto, las instancias de documentos se seleccionan para indexar. Esto provoca un aumento del tamaño del índice, que a su vez aumenta el consumo del espacio en disco. El tamaño de la carpeta "Lucene Index Engine" dentro de la carpeta PlatformSearchData aumenta considerablemente a causa de la indexación de un gran número de instancias en el repository. Si hay millones de documentos (o más) y muchos de ellos también tienen un gran número de instancias existentes (junto con instancias programadas generadas en intervalos regulares) en el sistema, el tamaño de la carpeta "Lucene Index Engine" aumentará demasiado, incluso si el nivel de indexación se fija en "Metadatos de plataforma".<br><br>La opción Búsqueda de plataforma omite instancia le permite controlar la indexación de instancias activando o desactivando mediante la casilla de selección "Otra configuración: Omitir instancia" en la página de propiedades "Aplicación de búsqueda de plataforma" en CMC.<br><br>**Nota**<br>• Si Activa/Desactiva Omitir instancia, tendrá que reiniciar el servidor de tratamiento de adaptación de búsqueda de plataforma. Esta modificación afectará a todos los niveles de indexación.<br>• Si modifica Omitir instancia y desea que se apliquen las modificaciones a todas las instancias existentes (por ejemplo, seleccionar para indexar), tendrá que reestructurar el índice. |

| Opción | Descripción |
| --- | --- |
| Objetos excluidos de la indexación | La opción *Objetos excluidos de la indexación* excluye de la indexación los objetos. Por ejemplo, puede que no desee que se puedan buscar determinados objetos para asegurar que los recursos del servidor de aplicaciones de informes no se sobrecargan.<br><br>Al excluir objetos concretos, puede evitar que la Búsqueda de plataforma acceda a ellos. Es importante tener en cuenta que si un objeto ya se ha indexado antes de ponerlo en esta categoría, se podrán seguir realizando búsquedas en él. Para asegurar que los documentos del grupo *Objetos excluidos de la indexación* no se puedan buscar, debe volver a crear el índice.<br><br>Lista de objetos que se pueden excluir de la indexación:<br>• CrystalReport<br>• Webi<br>• LCMJob<br>• Universe<br>• Excel<br>• PDF<br>• PowerPoint<br>• Rtf<br>• Txt<br>• Word<br>• AFDashboardPage<br>• ObjectPackage<br>• QaaWS<br>• Perfil<br>• Evento<br>• Debates<br>• InformationDesigner<br>• MDAnalysis<br>• Publicación<br>• Documentos agnósticos<br>• Analytic<br>• Hipervínculo<br>• Programa<br>• pQuery<br>• DSL.MetaDataFile<br>• Acceso directo<br>• DataDiscoveryAlbum<br>• AO.Workbook<br>• VISI.Story<br>• VISI.Dataset |

| Opción | Descripción |
| --- | --- |
| | • VISI.Lums<br>• VISILums<br>• Usuario<br>• UserGroup |

5. Haga clic en *Guardar y cerrar*.

> **Nota**
>
> Si el usuario no selecciona la opción *Regenerar índice* y cambia el nivel de indexación o selecciona o deselecciona extractores, entonces el índice se actualiza incrementalmente desde el principio sin eliminar el índice existente.

## 18.2.3.11 Configuración la integración Web BEx

Las aplicaciones Web BEx son aplicaciones basadas en Web de Business Explorer (BEx) de SAP Business Warehouse (BW) para el análisis de datos, informes y aplicaciones analíticas en la Web.

Business Explorer es la suite de Business Intelligence de SAP NetWeaver que proporciona herramientas de informes y análisis flexibles para análisis estratégicos y soporte en la toma de decisiones. Estas herramientas incluyen funciones de consulta, informes y análisis. Como empleado con derechos de acceso, puede evaluar los datos históricos o actuales en varios niveles de detalle y desde distintas perspectivas; tanto en la Web como en Microsoft Excel.

Los usuarios acceden a los datos desde SAP NetWeaver Portal o desde la plataforma de lanzamiento de BI de la plataforma de SAP BI. Los autores de aplicaciones BEx Web pueden ejecutar las aplicaciones Web directamente en la plataforma de lanzamiento de BI desde diseñador de aplicación BEx Web.

Para integrar aplicaciones Web BEx en la plataforma de BI, lleve a cabo los siguientes pasos de configuración:

1. Configure un servidor para las aplicaciones Web BEx en la Consola de administración central (CMC).

   Puede usar un servidor general o uno independiente para las aplicaciones Web BEx.

   > **→ Sugerencias**
   >
   > Se recomienda configurar un servidor independiente para las aplicaciones Web BEx ya que muchos otros servicios usan normalmente el servidor general.

2. Configure los ajustes del servidor.
3. Compruebe la conexión al sistema de BW.
4. Para asegurarse de que los autores pueden ejecutar aplicaciones web BEx directamente en la Plataforma de lanzamiento de BI desde BEx Web Application Designer, establezca la configuración apropiada en la tabla *Portales conectados* (**RSPOR_T_PORTAL**) en el sistema BW.

Después de la configuración del servidor de la Plataforma de BI, los usuarios pueden abrir las aplicaciones Web BEx en la Plataforma de lanzamiento de BI. Pueden navegar por los datos aquí y guardar las aplicaciones BEx Web como marcadores en los favoritos del explorador Web.

**⚠ Restricción**

La integración es aplicable a partir de las siguientes versiones de SAP NetWeaver:

SAP NetWeaver 7.0 Enhancement Package 1 pila de support packages 8
SAP NetWeaver 7.3 pila de support packages 1

Ya que la pila Java de SAP NetWeaver no es necesaria para esta integración, se aplican las siguientes restricciones:

No se admite la emisión de información.
Ya que el portal y la administración de conocimiento de SAP NetWeaver no se necesitan, la integración de documentos y el uso de motivos de portal no se admiten en las aplicaciones Web BEx.
No se admite el item de Web *Informe*. Le recomendamos que use SAP Crystal Reports para la generación de informes con formato.
Para crear versiones de impresión de aplicaciones Web BEx, se usa la biblioteca de exportación para SAP Business Explorer. Servicios de documentos de Adobe (ADS) no están disponibles.
Las aplicaciones Web BEx que están integradas en la plataforma de BI solo pueden contener orígenes de datos almacenados en el sistema principal de BW. En la administración del sistema, se define el sistema que se configura como el sistema principal de BW en la plataforma de BI.
El inicio de de sesión único entre la plataforma de BI y el sistema SAP NetWeaver BW no está habilitado. Para cada sesión de la Plataforma de BI, se solicita a los usuarios de las aplicaciones Web BEx que inicien sesión en el sistema principal de BW correspondiente.
No se admite la interfaz informe-informe desde y hacia aplicaciones Web BEx. Los comandos correspondientes no se ejecutarán.
No se admiten los dashboards basados en queries BEx o en vistas de queries y creados con SAP BusinessObjects Dashboards.

Para obtener más información sobre las funciones de las aplicaciones BEx Web, consulte el SAP Help Portal enhttp://help.sap.com: *SAP NetWeaver 7.3* > *Biblioteca de SAP NetWeaver: vista orientada a la función* > *Business Warehouse* > *SAP Business Explorer* > *BEx Web* > *Análisis e informes: aplicaciones BEx Web*.

Para obtener más información sobre cómo acceder y guardar aplicaciones BEx Web en la plataforma de lanzamiento de BI, consulte el *Manual del usuario de la plataforma de lanzamiento de BI* en http://help.sap.com.

## Información relacionada

Iniciar un servidor para aplicaciones Web BEx [página 746]
Iniciar un servidor independiente para aplicaciones Web BEx [página 746]
Configuración de los ajustes del servidor [página 746]
Comprobar la conexión al sistema BW [página 747]
Configuración de una conexión entre BEx Web Application Designer y la plataforma de BI [página 748]

## 18.2.3.11.1 Iniciar un servidor para aplicaciones Web BEx

Antes de poder realizar esta tarea, el Servidor de procesamiento de Adaptive tiene que estar Detenido.

1. Inicie sesión en la Consola de administración central (CMC).
2. Seleccione *Servidores*.
3. Expanda el nodo *Categorías de servicio* y elija *Analysis Services*.
4. Seleccione el *Servidor de procesamiento de Adaptive* y seleccione *Seleccionar servicios* del menú contextual.
5. Mueva *Servicio de aplicaciones Web BEx* de la lista *Servicios disponibles* a la lista Servicios al lado derecho.
6. Reinicie el servicio de aplicaciones Web BEx reiniciando el servidor de procesamiento de Adaptive.

## 18.2.3.11.2 Iniciar un servidor independiente para aplicaciones Web BEx

1. Inicie sesión en la Consola de administración central (CMC).
2. Seleccione *Servidores*.
3. Expanda el nodo *Categorías de servicio* y elija *Analysis Services*.
4. Seleccione el *Servidor de procesamiento de Adaptive* y seleccione *Clonar servidor* del menú contextual.
5. Introduzca un nombre para el servidor (**`AdaptiveProcessingServer`**, por ejemplo) y seleccione el nodo necesario del cuadro *Clonar a nodo*.
6. Seleccione el servidor clonado y seleccione *Seleccionar servicios* del menú contextual.
7. Seleccione *Servicio de aplicaciones Web BEx* de la lista *Servicios disponibles* y muévalo a la lista Servicios del lado derecho.
8. Inicie el servicio de aplicaciones Web BEx iniciando el nuevo servidor de procesamiento de Adaptive.

## 18.2.3.11.3 Configuración de los ajustes del servidor

1. Inicie sesión en la Consola de administración central (CMC).
2. Seleccione *Servidores*.
3. Expanda el nodo *Categorías de servicio* y elija *Analysis Services*.
4. Seleccione el servicio que aloja el servicio de aplicaciones Web BEx y seleccione *Propiedades* en el menú contextual.
5. En *Configuración del servicio de aplicaciones web BEx* en el área *Servicio de aplicaciones web BEx*, establezca los siguientes ajustes:
   a. Compruebe (y cambie si es necesario) el número máximo de sesiones de cliente.
   b. En el *Sistema principal de SAP BW*, introduzca el nombre de la conexión OLAP al sistema BW que ha creado en la plataforma de BI. El nombre predeterminado es *SAP_BW*.
   c. Introduzca el nombre del *Destino RFC del servidor de JCo* que ha especificado en el sistema BW en *Configuración de conexiones RFC* (código de transacción **`sm59`**).

d. Introduzca el nombre del *Host de gateway del servidor de JCo* que ha definido en el sistema BW en *Configuración de conexiones RFC* (código de transacción **sm59**).
e. Introduzca el nombre del *Servicio de gateway del servidor de JCo* que ha definido en el sistema BW en *Configuración de conexiones RFC* (código de transacción **sm59**).
f. Compruebe (y cambie si es necesario) el *Recuento de conexiones con el servidor de JCo*.

6. Seleccione *Guardar y cerrar*
7. Seleccione el servidor que aloja el servicio de aplicaciones Web BEx y seleccione *Reiniciar servidor* en el menú contextual.

   Tiene que reiniciar el servidor para aplicar la configuración seleccionada.

> ⓘ Nota
>
> Antes de reiniciar el servidor deberá haber creado el destino RFC en el sistema ABAP.

### Información relacionada

Crear un destino RFC en el sistema ABAP [página 748]

## 18.2.3.11.4 Comprobar la conexión al sistema BW

1. Inicie sesión en la Consola de administración central (CMC).
2. Seleccione *Conexiones OLAP*.
3. Compruebe si se ha establecido una conexión con el sistema BW. Si no, haga clic en el botón *Nueva conexión* para configurar una. El nombre predeterminado de la conexión es **SAP_BW**. Puede introducir un nombre diferente.
4. Asegúrese de que ha seleccionado *Predefinida* en *Autenticación* y de que ha introducido el usuario y la contraseña.

> ⓘ Nota
>
> Esta cuenta de usuario es necesaria para el destino RFC del servidor de JCo, que permite la integración de BEx Web Application Designer, el sistema BW y la plataforma de BI.

> → Sugerencias
>
> Para proteger la conexión, asegúrese de que sólo los administradores tienen derecho de acceso a la conexión.
>
> 1. Para ello, haga clic con el botón derecho en la conexión al sistema BW (nombre predeterminado **SAP_BW**) y seleccione *Seguridad de usuario*.
> 2. Defina la configuración de seguridad necesaria y, si es posible, otorgue derechos de acceso sólo a los administradores.

## 18.2.3.11.5 Configuración de una conexión entre BEx Web Application Designer y la plataforma de BI

Para asegurarse de que los autores pueden ejecutar aplicaciones web BEx directamente en la Plataforma de lanzamiento de BI desde BEx Web Application Designer, debe establecer la configuración apropiada en la tabla *Portales conectados* (**RSPOR_T_PORTAL**) en el sistema BW.

1. En el sistema BW, llame la transacción **SM30** (*Mantenimiento de vista de tabla*).
2. En *Tabla/Vista*, introduzca **RSPOR_T_PORTAL**.
3. Seleccione *Mantener*.
4. Para crear una nueva entrada, seleccione *Nuevas entradas*.
5. Configure los siguientes ajustes:
   a. Para garantizar la integración entre el sistema BW y la plataforma de BI, debe crear un destino RFC en la transacción **SM59**. Introduzca este destino RFC en *Destino*.
   b. Seleccione *Portal estándar*. Esto garantiza que las aplicaciones Web de Web Application Designer se podrán llamar siempre en la plataforma de BI.
   c. En *Prefijo URL*, introduzca la dirección URL del servidor de contenedor de aplicación Web (WACS) de la Plataforma de BI, incluyendo el protocolo, el nombre de host y el puerto, por ejemplo: **http://<wacs><dominio>:<puerto>**.
   d. En *Plataforma*, seleccione *BOE*.
   e. Seleccione *Usar biblioteca de exportación SAP (PDF)* si desea que se active la biblioteca de exportación para SAP Business Explorer, lo que permitirá la exportación de archivos PDF, PostScript y PCL desde aplicaciones web BEx.
6. Guarde los cambios.

### Información relacionada

Crear un destino RFC en el sistema ABAP [página 748]

## 18.2.3.11.5.1 Crear un destino RFC en el sistema ABAP

Para integrar el sistema BW y la plataforma de BI necesita un destino RFC. Este destino RFC permite que el sistema BW y la plataforma de BI se comuniquen entre sí.

1. Llame a *Configuración de conexiones RFC* (código de transacción **SM59**).
2. Elija *Crear*.
3. Mantener el destino RFC:
   a. Introduzca un nombre para el destino RFC.
   b. Seleccione *T para conexión TCP/IP* como tipo de conexión.
   c. Introduzca una descripción.

      Puede hacer que la descripción del destino RFC dependa del idioma.

d. En *Configuración técnica*, seleccione *Programa de servidor registrado* como tipo de activación.
e. En *Configuración técnica*, introduzca el Id. del programa.

   El ID del programa debe ser idéntico al ID de programa (Destino RFC de Servidor JCo) que especificó al crear el destino para este sistema BW en el servidor de la Plataforma de BI.
f. En *Configuración técnica*, en *Opciones de Gateway*, introduzca el host de gateway y el servicio de gateway que la plataforma de BI usa para comunicarse con el sistema BW.

4. En la página de la ficha *Inicio de sesión y seguridad*, active la opción *Enviar vale de inicio de sesión SAP*.
5. Guarde los cambios.

### Información relacionada

Configuración de los ajustes del servidor [página 746]

## 18.2.3.12 Configurar el inicio de sesión único de SAP HANA

En el área *Aplicaciones* de la CMC en la plataforma de BI, puede configurar el inicio de sesión único (SSO) de las conexiones de base de datos de SAP HANA. SSO se implementa mediante SAML (Security Assertion Markup Language).

Cuando haya establecido una sesión de la plataforma de BI, podrá generar un vale SAML que se pueden usar para iniciar sesión en SAP HANA sin la necesidad que el usuario proporcione una contraseña.

Este es el flujo de trabajo básico involucrado en la conexión a los orígenes de datos de SAP HANA:

1. Un administrador configura confianza entre SAP HANA y la plataforma de BI en la CMC.
2. Un usuario inicia sesión en la plataforma de BI sin ningún proveedor de autenticación admitido.
3. Con tal que los ID de usuario de SAP HANA y la plataforma de BI coincidan, la plataforma de BI puede generar una aserción SAML que SAP HANA puede aceptar para establecer una conexión para el usuario actual. El ID de usuario que pasa a SAP HANA es el ID de usuario de la plataforma de BI para el usuario que inició sesión.
4. Una aplicación de cliente de la plataforma de BI crea una conexión SAP HANA.

> **Nota**
>
> Antes de configurar el inicio de sesión único a SAP HANA con SAML, debe configurar SSL en el equipo de SAP HANA. Consulte la documentación de SAP HANA para obtener más detalles.

### 18.2.3.12.1 Configuración de conexión de SAP HANA

La tabla siguiente resume la configuración disponible en el CMC para configurar la conexión de SAP HANA.

| Parámetro | Descripción |
| --- | --- |
| *Nombre de host de HANA* | Proporciona el nombre del host de SAP HANA. |
| *Puerto de HANA* | Proporciona el número de puerto para el host de SAP HANA. |
| *ID de proveedor de identidades único* | Un nombre único en una instalación HANA en concreto. La instalación HANA aceptará vales debidamente firmados desde el nombre del proveedor de identidades para inicios de sesión. |
| *Certificado Base64 de proveedor de identidades* | Cuando hace clic en *Generar*, se crea un certificado en el campo *Certificado Base64 de proveedor de identidades*. Copie este certificado al archivo `trust.pem` en el despliegue de SAP HANA. Este certificado establece la relación de confianza entre SAP HANA y la plataforma de BI. El proveedor de identidad externa se identifica con un certificado X509, que se usa para firmar todas las reafirmaciones de identidad. El certificado debe estar codificado como Base64. |
| *Número de instancia de HANA* | El número de instancia de su sistema SAP HANA. |
| *Base de datos de HANA* | Proporciona el nombre del host de la base de datos de arrendatario de SAP HANA. |

## 18.2.3.12.2 Crear una conexión SAP HANA

1. Obtenga los parámetros de base de datos relevantes de SAP HANA.
   a. Abra la aplicación SAP HANA Studio.
   b. Abra la página de propiedades del sistema, y busque la URL para la conexión de la base de datos.
   c. Registre el nombre del equipo host, el número de puerto, el número de instancia y el nombre de la base de datos de arrendatario.

      Necesitará esta información en el paso 2.
2. Configure una conexión SAP HANA en la plataforma de BI.
   a. Vaya al área *Aplicaciones* de la CMC y haga doble clic en *Autenticación HANA*.
   b. En el cuadro de diálogo *Autenticación HANA*, haga clic en el botón *Crear una conexión*.
      Se abre el cuadro de diálogo *Crear una conexión de autenticación HANA*.
   c. Seleccione un *Tipo de conexión*.

      > **Nota**
      >
      > Debería elegir *SAP HANA* para una conexión JDBC y *SAP HANA HTTP* para una conexión HTTP.

   d. Introduzca el número de puerto, el nombre de máquina host, el número de instancia y el nombre de la base de datos de arrendatarios que había registrado en el paso 1.
   e. En el campo *ID único del proveedor de identidad*, especifique el valor que se usará para el despliegue de la plataforma de BI.
   f. Introduzca el *nombre del proveedor de servicios*.

      > **Nota**
      >
      > Puede verificar la configuración de Nombre del proveedor de servicios en HANA navegando a `indexserver.ini -> Autenticación -> saml_service_provider_name`. También puede

> modificar el valor en HANA introduciendo el código mencionado a continuación: `ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') SET ('authentication', 'saml_service_provider_name') = 'DEV00' WITH RECONFIGURE;` En el código, DEV 00 es el nombre del proveedor de servicios y puede introducirlo según su elección. La práctica recomendad para denominar el proveedor de servicios es combinar el ID de sistema (DEV) y el número de instancia (00).

g. Seleccione *Conexión segura*.

> **Nota**
>
> Debe seleccionar *Conexión segura* para establecer una conexión segura JDBD o HTTPS.
>
> - Para establecer una conexión HTTPS, deberá seleccionar *SAP HANA HTTP* como el *Tipo de conexión* y seleccionar *Conexión segura*.
> - Para establecer una conexión JDBC, deberá seleccionar *SAP HANA* como el *Tipo de conexión* y seleccionar *Conexión segura*.

h. Haga clic en *Volver a generar*.
Se crea un certificado en el cuadro *Certificado Base64 del proveedor de identidades*.

3. Configure el despliegue de SAP HANA.
   a. Inicie sesión en el sistema SAP HANA.
   b. Expanda *Configuración de confianza y de SSL* y seleccione *Gestión PSE*.
   c. Seleccione el archivo PSE de la lista desplegable respecto a *Gestionar PSE*.
   d. Seleccione *Importar certificados*.
   e. Pegue el certificado generado en el paso anterior en la plataforma de BI.
   f. Seleccione *Importar*
   g. Inicie SAP HANA Studio.
   h. En la vista *Sistemas* , expanda su sistema SAP HANA. Consulte la Guía de administración SAP HANA One.
   i. Abra (Editor de seguridad) desde la carpeta Seguridad.
   j. Seleccione (Importar proveedor de identidades SAML para archivo de certificado).
   k. Seleccione su proveedor de identidades desde la lista de *proveedores de identidades SAML* .
   l. Seleccione (desplegar).
   m. Navegue al usuario de HANA en la vista *Sistemas* .
   n. Abra el usuario de HANA en el área Editores.
   o. En la etiqueta *Usuario* , marque *SAML* como autenticación y seleccione *Configurar*.
   p. En el asistente *Configurar identidades SAML externas* , seleccione *Añadir*.
   q. Seleccione su proveedor de identidades.
   r. Seleccione Aceptar.
   s. Seleccione su proveedor de identidades e introduzca el nombre de usuario de la plataforma de BI que está asignado al usuario HANA.
   t. Seleccione Aceptar.
   u. Seleccione (desplegar).
   v. Reinicie el sistema SAP HANA.
      1. Abra el menú contextual de su sistema SAP HANA.
      2. Seleccione *Configuración y supervisión*.

3. Seleccione *Reiniciar sistema*.

4. Pruebe la configuración de SAP HANA .
   a. Vaya al área *Aplicaciones* de la CMC y haga doble clic en *Autenticación HANA*.
   b. En el cuadro de diálogo *Autenticación HANA*, abra la conexión que creó en el paso 2.
      Se abre el cuadro de diálogo *Editar una conexión de autenticación HANA*.
   c. En *Probar la conexión para este usuario*, introduzca un nombre de usuario y haga clic en el botón *Probar conexión* para verificar que la configuración de la conexión es correcta.

      Por ejemplo, introduzca el nombre de usuario **`Administrador`**. Si la configuración no es válida, se muestra un mensaje de error. Puede llevar a cabo estos pasos de resolución de problemas:
      - Asegúrese de que no hay ningún otro certificado en el archivo `trust.pem` que contenga un Asunto o Emisor con el mismo valor de propiedad de CN. Para ver los componentes del certificado, busque en Internet un «decodificador de certificados x509» para encontrar un decodificador de certificados.
      - Intente estos comandos para comprobar la configuración de HANA:

        ```
        select * from "SAML_PROVIDERS"
        select user_name, is_saml_enabled from users where user_name =
        '<UserName>'
        select * from "PUBLIC"."SAML_USER_MAPPINGS"
        ```

      - Si aparece un error de autenticación SAML al configurar SSO en SAP HANA, pruebe a ejecutar estos pasos:
        1. En el archivo `indexserver.ini`, fije el parámetro `sslCreateSelfSignedCertificate` en **`false`**.
        2. En el mismo archivo, fije los parámetros `sslKeyStore` y `sslTrustStore` para que utilicen rutas absolutas.
        3. Regenere los archivos `key.pem` y `trust.pem`.

Si el archivo `key.pem` no existe en el directorio `.ssl`, significa que SAP HANA no se configuró correctamente para usar SSL.

## 18.2.3.12.3 Configurar la conexión SAP HANA HTTPS

La configuración de SAP HANA HTTPS incluye añadir el servidor SAP HANA y el certificado CA del servidor SAP HANA en TrustStore o en la ubicación de su elección.

> **Nota**
>
> Debe exportar el certificado de servidor de SAP HANA desde el sistema SAP HANA antes de agregar el certificado al TrustStore o a otra ubicación.

### Añadir el certificado en TrustStore

1. Vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.

2. Ejecute el comando: `..\..\bin\keytool -importcert -file "<absolute path of the certificate>" -alias CertifcateAliasName -keystore cacerts -storepass changeit`.
3. El servidor SAP HANA y el certificado CA del servidor SAP HANA se almacenan en TrustStore.

> **Nota**
>
> Si el archivo de keystore está ubicado en la ubicación estándar `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`, las modificaciones realizadas en el archivo de keystore se pierden después de un upgrade del support package 4 al 5 de la Plataforma de SAP Business Intelligence. Por lo tanto, se recomienda que añada el certificado en una ubicación diferente.

### Añadir el certificado en una ubicación diferente

1. Vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`.
2. Ejecute el comando: `keytool -importcert -file "C:\certificate\HANASERVERCertificate " -alias CertificateAliasName -keystore C:\certificate\cacerts -storepass changeit`.

   > **Nota**
   >
   > La ubicación definida arriba es solo un ejemplo. Puede añadir la ubicación que desee.

3. Para que el servidor APS identifique la ubicación de los archivos, ejecute el comando:

   ```
   -Djavax.net.ssl.trustStore= cacerts_PATH
   -Djavax.net.ssl.trustStorePassword= Password
   ```

   > **Nota**
   >
   > cacerts_PATH y Password son solo ejemplos del acceso al almacén de claves y contraseña de certificado. Puede añadir cualquier acceso y contraseña que desee.

## 18.2.3.13 Administrar parametrizaciones SAP Lumira

Para el área de "Aplicaciones" de CMC, puede administrar los derechos relacionados con la adquisición de datos y la funcionalidad de compartir contenido de SAP Lumira para cada usuario o grupo de usuarios.

Para administrar derechos para SAP Lumira, realice los pasos siguientes:

1. De la página de inicio CMC, seleccione *Aplicaciones* > *SAP Lumira* > *Seguridad de usuario*.
2. Seleccione el usuario o grupo para el que desee fijar los derechos.
3. Seleccione *Asignar seguridad*.
4. Seleccione *Avanzado*.
5. Seleccione *Agregar o eliminar derechos*.
6. Defina los derechos que el usuario necesita tener para SAP Lumira.
7. Haga clic en *Aplicar*.

## 18.2.3.14 Administración de la configuración de SAP Analytics Cloud

### 18.2.3.14.1 Enviar objetos de hub a SAP Analytics Hub

Puede añadir activos de BI a una nueva categoría *Objeto de hub* y acceder a los mismos objetos de BI desde SAP Analytics Hub.

Cree un *cliente OAuth* en SAP Analytics Cloud y anote los valores de parámetros como *URL de arrendatario de SAP Analytics Cloud*, *URL de token*, *ID de cliente OAuth* y *Secreto*. Puede consultar el tema *Gestión de clientes OAuth* en la ayuda de SAP Analytics Cloud en SAP Help Portal para aprender a crear un cliente OAuth.

SAP Analytics Hub le permite acceder a sus objetos de BI locales y en la nube desde una única plataforma. Debe configurar una relación de confianza entre la plataforma de BI y SAP Analytics Cloud, que hace de proveedor de identidades de SAP Analytics Hub, para que la plataforma de BI puede cargar objetos de BI en SAP Analytics Hub.

> **Nota**
>
> No se admiten las publicaciones en la categoría *Objeto de hub*.

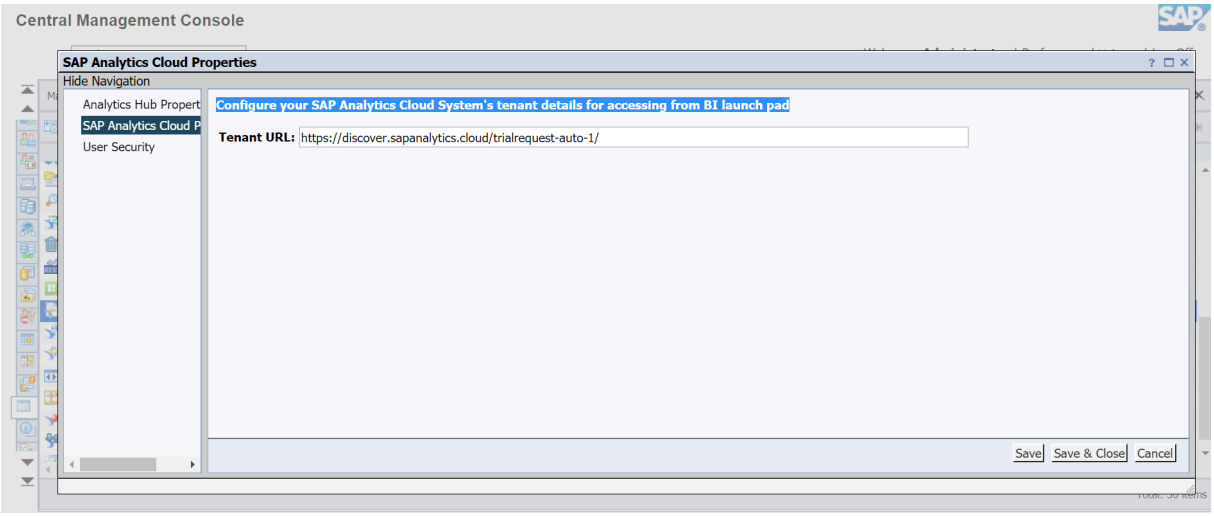
1. Inicie sesión en la CMC y vaya a *Aplicaciones* > *SAP Analytics Cloud*.
2. Seleccione *Permitir que la plataforma de BI inserte objetos de BI en SAP Analytics Hub*.
3. Introduzca los siguientes parámetros:
   - *URL de arrendatario de SAP Analytics Cloud*
   - *URL de token*
   - *ID de cliente OAuth*
   - *Secreto*
4. Seleccione *Guardar y cerrar*.

Ha configurado correctamente las opciones de SAP Analytics Cloud en la plataforma de BI para cargar los objetos de BI de la categoría *Objeto de hub* en SAP Analytics Hub.

### 18.2.3.14.2 Configurar la configuración de la URL del arrendatario de SAP Analytics Cloud

Ahora puede configurar los datos del arrendatario del sistema SAP Analytics Cloud para acceder a él desde el mosaico de SAC en las aplicaciones de la plataforma de lanzamiento de BI.

> **Nota**
>
> Por defecto, la URL se configura en la URL de cuenta de prueba de SAP Analytics.




## 18.2.3.15 Configuración del servidor de autorizaciones

La aplicación Configuración del servidor de autorización es para cualquier recurso de base de datos al que se pueda acceder a través del protocolo o mecanismo del Servidor de autorización.

### Soporte OAuth SSO de extremo a extremo: soporte de servidor OAuth único y múltiple

En la Consola de administración central, la aplicación *Configuración del servidor de autorización* le permite configurar y administrar servidores de autorización en la plataforma de BI. Dentro de la aplicación, el administrador es responsable de registrar y gestionar las configuraciones mediante los objetos de referencia de autorización. Cada configuración del servidor de autorización tiene un objeto de referencia de autorización. Puede crear configuraciones de servidor de autorización para recursos agnósticos, Google Drive, Microsoft Drive u OData.

Para crear una configuración del servidor de autorización, rellene los campos obligatorios en *Introducir información de configuración para un servidor de autorización*.

El *Alcance de autorización* se puede definir en función de sus necesidades para ayudarle a controlar a qué tienen acceso los usuarios finales, ya sea online u offline.

## 18.2.3.15.1 Para configurar un servidor de autorizaciones

Puede configurar un servidor de autorizaciones.

1. Lance e inicie sesión en la Consola de administración central como administrador.
2. En la página de inicio, seleccione *Aplicaciones* en la columna *Gestionar*.

3. En la página *Aplicaciones*, haga doble clic en *Configuración del servidor de autorizaciones*.
4. En el diálogo *Configuraciones del servidor de autorizaciones*, realice una de las siguientes acciones:
   - Seleccione *Gestionar* > *Nueva configuración del servidor de autorizaciones*
   - Seleccione el icono de la barra de herramientas *Crear una nueva configuración del servidor de autorizaciones*
5. Rellene los siguientes parámetros en el diálogo *Crear una nueva configuración del servidor de autorizaciones*:
   - *Nombre de referencia*
     Seleccione una cadena aleatoria unívoca e introduzca la misma para identificar la configuración, reconocer y elegir la configuración en diferentes flujos de trabajo y así conseguir la autorización basada en SSO.
   - *Descripción* (opcional)
     Introduzca una declaración o palabra clave cualquiera para describir e identificar fácilmente la configuración a partir de la lista de configuraciones disponibles.
   - **Campos específicos de OpenID Connect**
     Los siguientes campos son específicos de la autenticación de OpenID Connect y no son necesarios para el SSO de autorización:
     - Casilla de selección *Habilitado para la autenticación "OpenID Connect"*
     - *URI emisor*
     - *URI de juegos de claves web JSON (jwks_uri)*
     - *Algoritmo de firma de token ID*
   - *Punto de acceso de autorización*
     Introduzca el URL del servidor de autorización con el que puede obtener la adjudicación de autorización.
   - *Punto de acceso de token*
     Introduzca el URL del servidor de autorización con el que puede solicitar un token de acceso intercambiando el código de autorización.
   - *ID de cliente*
     Introduzca el nombre de la aplicación que se utiliza para registrar la infraestructura BI con el servidor de autorización.
   - *Secreto de cliente*
     Introduzca el código secreto específico correspondiente a la aplicación que se utiliza para registrar la infraestructura BI con el servidor de autorización.
   - *Redireccionamiento URL*
     Introduzca el URL del punto de acceso de la infraestructura BI al que el servidor de autorización debe enviar el código de autorización una vez validada la autorización.
   - *Punto de acceso de revocación* (opcional)
     Introduzca el URL del servidor de autorización con el que la aplicación puede solicitar la revocación de todos los tokens de acceso emitidos anteriormente mediante un token de actualización específico.
   - *Alcance de autorización*
     Introduzca los alcances de autorización admitidos por el servidor de autorización para definir los límites para el acceso de la aplicación (infraestructura BI) a diferentes recursos API disponibles.

     > **Nota**
     >
     > La implementación de la plataforma de BI de SSO OAuth se basa en el acceso offline. Si la finalidad de configurar el servidor de autorización en la plataforma de BI es actualizar datos o acceder

> a recursos sin tener que validar la autorización cada vez, deberá configurar este campo con el parámetro de alcance necesario junto con un parámetro obligatorio (por ejemplo, "refresh_token" u "offline_access" según el proveedor del servidor de autorización).

- *Tipo de recurso*
  Seleccione el tipo de recurso deseado en la lista disponible de tipos de recurso admitidos por la plataforma de BI. La siguiente es la lista actual de tipos de recursos admitidos en la plataforma de BI para configurar y acceder a través del servidor de autorización correspondiente:
  - *Agnóstico* (valor predeterminado)
    No es específico de un proveedor o protocolo, para indicar un recurso al que se puede acceder con una autorización válida concedida por un servidor de autorización.
  - *GoogleDrive*
    Para indicar que la configuración es del servidor de autorización de Google que se puede utilizar para acceder a Google Drive para diferentes escenarios de la plataforma de BI. Solo puede existir una configuración del tipo GoogleDrive en el sistema.
  - *Microsoft Drive*
    Para indicar que la configuración es del servidor de autorización de Microsoft que se puede utilizar para acceder a Microsoft Drive para diferentes escenarios de la plataforma de BI. Solo puede existir una configuración del tipo Microsoft Drive en el sistema.
  - *OData*
    No es específico de un proveedor. Sirve para indicar que la configuración está relacionada con un recurso al que se puede acceder a través del protocolo OData con una autorización concedida por un servidor de autorización. Como ocurre con GoogleDrive, solo puede existir una configuración del tipo OData en el sistema.

> **Nota**
>
> El parámetro *Tipo de recurso* no tiene nada que ver con el estándar OAuth 2.0. Sin embargo, esto se introduce en la configuración para evitar cualquier posible ambigüedad en la identificación de determinados recursos en la plataforma de BI. Por lo tanto, las configuraciones correspondientes se pueden elegir fácilmente y utilizar en determinados escenarios para conseguir la autorización.

- *Tipo de acceso*
  Este parámetro es específico de la configuración de autorización del tipo *GoogleDrive*. Se rellenará automáticamente cuando el valor del campo *Tipo de recurso* sea *GoogleDrive*.
- *Parámetros personalizados* (opcional)
  Introduzca los parámetros personalizados necesarios para enviar al solicitar la autorización. Dependerán de los requisitos personalizados (si son necesarios) del servidor de autorización que se configura.

> **Nota**
>
> El nombre del parámetro personalizado debe ser unívoco en la configuración.
>
> En cualquier configuración de autorización se permite configurar un máximo de cinco parámetros personalizados.

6. Después de rellenar todos los parámetros necesarios, seleccione *OK* para validar los detalles y guardar la configuración.

La configuración se guardará como un objeto de sistema en el repositorio con el tipo *AuthorizationReference*. Puede consultar la configuración en todos los escenarios admitidos con su *Nombre de referencia*.

## 18.2.3.15.2 Para probar la configuración del servidor de autorizaciones

Puede probar la configuración del servidor de autorizaciones.

1. Una vez que haya guardado la configuración del servidor de autorizaciones, lance la rampa de lanzamiento BI e inicie sesión para probar la configuración.

   > **Nota**
   >
   > Actualmente no se puede probar la configuración desde la CMC.
   >
   > Inicie sesión como administrador o con cualquier cuenta de usuario de la plataforma de BI que no esté restringida a utilizar la configuración de autorización guardada antes.
   >
   > Utilice el método de inicio de sesión actual configurado para la rampa de lanzamiento BI (por ejemplo, Enterprise o cualquier método de autenticación).

2. Seleccione el icono de usuario.
3. En el menú desplegable que aparece, seleccione *Opciones*.
4. En el diálogo *Opciones*, seleccione *Tokens de autorización* en la sección *Cuenta de usuario*.
5. Seleccione *Generar* en la columna *Gestionar tokens*.
6. De acuerdo con la política de su organización y la configuración de autorización de su servidor de autorizaciones, la validación de la cuenta se realizará en función de los certificados configurados en el sistema o se le pedirá que introduzca el nombre de usuario, la contraseña y/o la autenticación de varios factores acorde con las opciones de configuración.
7. Una vez que se hayan validado las credenciales o el certificado, la plataforma de BI debería haber recibido el token de actualización. Debería haberse almacenado de forma segura en el repository de la plataforma de BI. Cuando se haya realizado, debería ver las siguientes modificaciones en la pestaña *Tokens de autorización*:
   - En la columna *Fecha de vencimiento*, debería ver el valor de vencimiento del token emitido por el servidor de autorización. Si su servidor de autorización emite un token sin vencimiento, el valor de la columna se actualizará como *Sin vencimiento*.
   - En la columna *Gestionar tokens*, debería ver el botón *Eliminar* junto al botón *Generar*.
     - El botón *Eliminar* sirve para borrar el token emitido por el servidor de autorización y este borrado no se limita solamente a borrar el token de almacenamiento del repository de la plataforma de BI. También se puede propagar al servidor de autorizaciones según la configuración y el soporte.
     - Si el parámetro opcional *Punto de acceso de revocación* se rellena con el URL adecuado conforme a la compatibilidad del servidor de autorizaciones con él, el token emitido también se revocará para el servidor de autorizaciones, junto con el borrado del almacenamiento del repository de la plataforma de BI.
8. Si el token se emite y la columna *Fecha de vencimiento* se actualiza según el vencimiento del token emitido, significa que la configuración funciona y está lista para que la utilicen el desarrollador y el usuario final de BI.

## 18.2.3.16 Configuración de clasificación de información

En la plataforma de BI, puede configurar el servidor de directivas de Azure de su organización para permitir que su infraestructura de BI tenga la capacidad de clasificar el contenido de BI. Estas capacidades de clasificación se pueden aplicar mediante etiquetas de sensibilidad definidas por el administrador de Azure Policy Server de su organización.

> **Nota**
>
> Esta opción de integración para configurar el servidor de directivas solo es compatible con Microsoft Azure Information Protection Platform.
>
> La versión SAP BusinessObjects BI 4.3 SP04 incluye una opción de integración para la plataforma de protección de información de Microsoft Azure. Sin embargo, es importante tener en cuenta que la aplicación para configurar los detalles del servidor de políticas de Azure en la plataforma de BI no está habilitada de forma predeterminada; se envía como una función oculta. Para hacer visible esta función oculta, consulte 3409349.

Esta función de la información solo está disponible en la plataforma Windows.

### 18.2.3.16.1 Para configurar la clasificación de información

1. Inicie sesión en la *Consola de administración central* como administrador.
2. Vaya a *Aplicaciones*.
3. Haga clic con el botón derecho en la aplicación *Configuración de clasificación de información*.
4. Seleccione *Configuración para clasificación de información*.
5. Marque la casilla de selección *Activar clasificación de información* para activar la configuración y los campos.
6. Introduzca la URL de token del campo *URL del servidor de directivas* de Azure Policy Server de su organización.
   El formato de URL debe ser `https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token`.
7. Introduzca los valores *ID de cliente* y *Secreto de cliente* de su aplicación de cliente en Azure.
   Están activados para el modo de autorización de flujo de credenciales de cliente para acceder al servidor de políticas de Azure de su organización.
8. Haga clic en *Guardar y probar configuración* para probar la conexión.
9. Si la prueba de configuración es correcta, haga clic en *Guardar* o *Guardar y cerrar*.

> **Nota**
>
> No marque la casilla de selección relacionada con *Activado para la autenticación de certificado*, ya que este modo de configuración de autenticación no es compatible.

## 18.3 Administración de aplicaciones mediante propiedades de la capa semántica

Las opciones de configuración de biblioteca de la capa semántica dimensional (DSL) se pueden establecer en tiempo de ejecución para modificar el comportamiento del acceso directo HANA de BW a través de conexiones BICS en herramientas BI, como, por ejemplo, Web Intelligence, herramienta de diseño de información, Dashboards, y Crystal Reports para Enterprise. Estas opciones se especifican mediante opciones de línea de comandos Java del tipo:

-DoptionName=optionValue

Actualizar y modificar esta configuración puede ser compleja:

- Las opciones de línea de comandos deben estar definidas para todos los procesos Java que ejecutan DSL. No hay una ubicación común para realizar modificaciones.
- Cada proceso Java DSL se debe reiniciar para que la revisión de las configuraciones surta efecto. Las modificaciones no se aplican al instante.

Para simplificar la tarea administrativa de actualizar las opciones de configuración DSL BICS, se ha incorporado un nuevo mecanismo en el que las opciones se pueden guardar en un fichero. Las modificaciones en el fichero propagarán la configuración de la nueva opción a todos los procesos DSL que leen el fichero.

El nombre y el valor de la opción se guardan en un fichero como XML válido para java.util.Propertes tal como define http://java.sun.com/dtd/properties.dtd

Al iniciar por primera vez este nuevo mecanismo ejecutando el DSL, se generan de forma automática los dos ficheros siguientes:

- DSLBICSConfiguration.xml o DSLConfiguration.xml - este fichero contiene todas las opciones disponibles y sus valores por defecto. Este fichero no se debe modificar.
- DSLBICSConfiguration_custom.xml o DSLConfiguration_custom.xml - este fichero contiene todas las opciones con valores especificados por el administrador.

> **Nota**
>
> - Los archivos DSLBICSConfiguration.xml y DSLBICSConfiguration_custom.xml files se usan para gestionar el comportamiento del acceso directo de BW mediante las conexiones BICS.
> - Los archivos DSLBICSConfiguration.xml y DSLBICSConfiguration_custom.xml files se usan para gestionar el comportamiento del acceso directo de HANA.

El fichero `DSLBICSConfiguration_custom.xml` y `DSLConfiguration_custom.xml` contiene todas las configuraciones de opciones especificadas mediante línea de comandos y configuraciones estándar para otras opciones. Posteriormente a su generación inicial, el fichero `DSLBICSConfiguration_custom.xml` o `DSLConfiguration.xml` puede modificarse para añadir o modificar valores de opción. El mecanismo no actualiza este fichero tras su generación inicial. El mecanismo actualiza el fichero `DSLBICSConfiguration.xml` con las nuevas opciones disponibles o si hay una evolución para un valor estándar.

Para modificar cualquiera de las propiedades estándar, utilice el fichero de configuración personalizada para grabar configuraciones nuevas para propiedades globales o específicas de aplicación. Por defecto, los ficheros del directorio se encuentran en: `SAP BusinessObjects Enterprise XI 4.0\java\lib`

No modifique las propiedades en el fichero de configuración estándar.

## 18.4 Administración de aplicaciones mediante las propiedades de BOE.war

### 18.4.1 El archivo BOE WAR

Puede modificar la configuración de las aplicaciones Web de la Plataforma de BI si sobrescribe las propiedades predeterminadas del archivo BOE.war. Este archivo se despliega en el equipo que aloja el servidor de aplicaciones Web. Para obtener información detallada sobre cómo se despliega el archivo, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

Las propiedades contenidas en el archivo BOE.war controlan las especificaciones para el comportamiento de inicio de sesión predeterminado, los métodos de autenticación predeterminados y la configuración para el inicio de sesión único. Se pueden especificar dos tipos de propiedades:

- Propiedades globales: estas propiedades afectan a todas las aplicaciones Web contenidas en el archivo BOE.war.
- Propiedades específicas de la aplicación: configuración de propiedad que sólo afecta a una aplicación Web específica.

Para modificar alguna de las propiedades predeterminadas, use el directorio de configuración personalizado para guardar la configuración nueva, tanto para las propiedades globales como para las específicas de una aplicación. De forma predeterminada, el directorio se encuentra en: `C:\Archivos de programas (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

No modifique las propiedades del directorio `config\default`.

> **Nota**
>
> En algunos servidores de aplicaciones Web, como la versión de Tomcat en paquete con la plataforma de BI, puede acceder al archivo BOE.war directamente. En este escenario, puede configurar los ajustes personalizados directamente sin tener que anular el despliegue del archivo WAR. Si no puede acceder directamente a las aplicaciones Web desplegadas, debe anular el despliegue, personalizar y volver a desplegar el archivo. Para obtener más información, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

#### 18.4.1.1 Propiedades de BOE.war globales

En la siguiente tabla se muestra la configuración que se incluye en el archivo `global.properties` predeterminado para BOE.war.

Para sobrescribir la configuración, cree un nuevo archivo en `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

| Parámetro | Valores predeterminados | Descripción |
| --- | --- | --- |
| `persistentcookies.enabled` | `persistentcookies.enabled=true` | Habilita o deshabilita las cookies persistentes en la página del inicio de sesión de la aplicación Web. |
| `siteminder.authentication` | `siteminder.authentication=secLDAP` | Especifica qué método de autenticación usar con SiteMinder. Las únicas opciones son secLDAP y secwinAD. |
| `siteminder.enabled` | `siteminder.enabled=false` | Habilita y deshabilita la autenticación con SiteMinder. |
| `sso.enabled` | `sso.enabled=false` | Habilita y deshabilita el inicio de sesión único (SSO) en la Plataforma de BI. |
| `sso.sap.primary` | `sso.sap.primary=false` | Configúrelo en `true` si desea usar el SSO de SAP como el mecanismo de inicio de sesión único principal de la aplicación. Sólo se aplica a los casos en los que se usan el SSO de SAP y SiteMinder. |
| `max.tree.children.threshold` | `max.tree.children.threshold=200` | Especifica el umbral en el que el control de la lista de árbol no mostrará todos los nodos, y mostrará un mensaje "demasiados secundarios". |
| `trusted.auth.shared.secret` | Ninguno | Especifica el nombre de la variable de sesión que se usa para recuperar el secreto para la autenticación de confianza. Sólo se aplica si se usa la sesión Web para pasar el secreto compartido. |
| `trusted.auth.user.param` | Ninguno | Especifica la variable usada para recuperar el nombre de usuario para la autenticación de confianza y se puede establecer en uno de los valores siguientes:<br>• `Header`<br>• `URL Parameter`<br>• `Cookie`<br>• `Session` |
| `trusted.auth.user.retrieval` | Ninguno | Especifica el método usado para recuperar el nombre de usuario para la autenticación de confianza y se puede establecer en uno de los valores siguientes:<br>• `"REMOTE_USER"`<br>• `"HTTP_HEADER"`<br>• `"COOKIE"`<br>• `"QUERY_STRING"`<br>• `"WEB_SESSION"`<br>• `"USER_PRINCIPAL"`<br>Establecer en vació para deshabilitar la autenticación de confianza. |
| `trusted.auth.user.namespace.enabled` | `trusted.auth.user.namespace.enabled=false` | Habilita y deshabilita el enlazado dinámico de alias a cuentas de usuario existentes. Si la propiedad se configura en `true`, la autenticación con confianza usa el enlace de alias para autenticar usuarios en |

| Parámetro | Valores predeterminados | Descripción |
| --- | --- | --- |
| | | la plataforma de BI. Con el enlazado de alias, el servidor de aplicaciones puede trabajar como un proveedor de servicios SAML por lo que se habilita la autenticación de confianza para proporcionar el SSO de SAML en el sistema. Si se establece en `false`, la autenticación de confianza usa la coincidencia de nombres para autenticar usuarios. |
| `vintela.enabled` | `vintela.enabled=false`<br>`idm.realm=YOUR_REALM`<br>`idm.princ=YOUR_PRINCIPAL`<br>`idm.allowUnsecured=true`<br>`idm.allowNTLM=false`<br>`idm.logger.name=simple`<br>`idm.logger.props=error-log.properties` | Se usa para habilitar o deshabilitar la configuración de Vintela para la autenticación de Windows AD. |
| `pinger.showWarningDialog.cmc` | `pinger.showWarningDialog.cmc=true` | Especifica si mostrar o no el cuadro de diálogo de advertencia con el mensaje que indica que la sesión actual caducará pronto en la CMC. |
| `pinger.showWarningDialog.bilaunchpad` | `pinger.showWarningDialog.bilaunchpad=true` | Especifica si mostrar o no el cuadro de diálogo de advertencia con el mensaje que indica que la sesión actual caducará pronto en la plataforma de lanzamiento de BI. |
| `pinger.warningPeriod.pingIncrementsInSeconds` | `pinger.warningPeriod.pingIncrementsInSeconds=15` | Especifica la frecuencia con la que se envía una solicitud de servidor Web mientras se muestra el mensaje de advertencia de caducidad. Es importante para sincronizar el cuadro de diálogo de advertencia en las aplicaciones. |
| `pinger.warningPeriod.lengthInMinutes` | `pinger.warningPeriod.lengthInMinutes=5` | Especifica cuánto tiempo se debe mostrar la advertencia antes de que caduque. |
| `logoff.on.websession.expiry` | `logoff.on.websession.expiry=true` | Especifica si todas las sesiones de la aplicación cerrarán sesión cuando la sesión caduque. |
| `pinger.enabled` | `pinger.enabled=true` | Habilita o deshabilita el mecanismo de mensajería de advertencia de caducidad de sesión. |
| `system.com.sap.bip.jcomanager.destinations.maxsize` | `system.com.sap.bip.jcomanager.destinations.maxsize=1000` | Especifica el número máximo de caracteres de las conexiones Java en caché. |
| `httpproxy.username` | `httpproxy.username=myusername` | Especificar el nombre de usuario para iniciar sesión en el servidor proxy HTTP. |
| `httpproxy.password` | `httpproxy.password=mypassword` | Especificar la contraseña para iniciar sesión en el servidor proxy HTTP. |
| `logon.embed.secret` | Ninguno | Un secreto compartido entre un portal que incrusta aplicaciones de la plataforma de BI y el servidor de aplicaciones de la plataforma de BI, |

| Parámetro | Valores predeterminados | Descripción |
| --- | --- | --- |
| | | que se usa para determinar si las aplicaciones de la plataforma de BI se pueden incrustar de forma segura en otras páginas. |
| `logon.embed.timeout` | `logon.embed.timeout=300` | El número de segundos tras los que las aplicaciones de la plataforma de BI, como por ejemplo la plataforma de lanzamiento de BI, rechazarán las incrustaciones en el portal. Asegúrese de que el reloj del sistema del servidor Web de la plataforma de BI y los equipos del servidor de portal se encuentran en este número de segundos. |
| `iview.autologoff` | `iview.autologoff=true` | Establezca en `true` para habilitar un cierre de sesión inmediato para iViews de SAP NetWeaver Technology Platform. |
| `pinger.showWarningDialog` | `pinger.showWarningDialog=true` | Especifica si mostrar o no el cuadro de diálogo de advertencia con el mensaje que indica que la sesión actual caducará pronto. No se aplica para la CMC ni la plataforma de lanzamiento de BI. |
| `ure.request.queue.timeout.seconds` | `ure.request.queue.timeout.seconds=20` | El número de segundos que esperará una solicitud para varias solicitudes anteriores esperadas antes de no agotar el tiempo de espera<br><br>Si los usuarios realizan acciones de navegación o expansión de carpetas en el control de la lista de árbol en la plataforma de lanzamiento de BI, las solicitudes AJAX se ponen en la cola. La interfaz de usuario espera a que se completen estas solicitudes antes de dar control al usuario. La configuración determina en número de segundos que esperará la interfaz de usuario para cada solicitud, si se retrasa en la consulta de back end. |
| | | |
| `enable.safe.html` | `enable.safe.html=true` | Activa la utilización de URLs de página Web seguras en los URL de módulo de páginas Web para el área de trabajo BI. |
| | | |
| `upload.file.maxsize.in MB` | `upload.file.maxsize.in MB = 0` | Especifica el tamaño máximo de archivo para cargar archivos en Megabytes. Si el valor predeterminado, es decir, 0, está establecido, se pueden cargar archivos de cualquier tamaño. |
| `upload.file.allowed.formats` | Ninguno | Especifica los formatos de archivo permitidos para cargar archivos. Para obtener más información, consulte 2296060. |

| Parámetro | Valores predeterminados | Descripción |
| --- | --- | --- |
| `upload.file.maxsize.in MB=0` | Ninguno | El tamaño máximo de archivo para carga de documento local se expresa en MegaBytes y debe ser un número entero, por ejemplo: 10 etc. |
| `upload.file.allowed.fo rmats=` | Ninguno | Esta propiedad se utiliza para controlar diferentes clases de archivos permitidos para cargar el documento local. Consulte la Nota SAP 2296060 para obtener la lista de formatos de archivo admitidos.<br><br>Si define varios formatos, separe cada formato de archivo seguido de una coma como txt, doc, xls. |
| `offlinehelp.enabled=fa lse` | Ninguno | Fije el indicador offlineHelp en verdadero para habilitar la ayuda offline. Por defecto, este valor está fijado en falso. |
| `offlinehelp.url=` | Ninguno | La url offlinehelp.url se consumirá mientras el usuario haya fijado el indicador offline en verdadero |

## 18.4.1.2 Propiedades de la plataforma de lanzamiento de BI

En la siguiente tabla se muestra la configuración que se incluye en el archivo `bilaunchpad.properties` predeterminado para el archivo BOE.war. Para sobrescribir la configuración, cree un nuevo archivo en `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

| Parámetro | Descripción |
| --- | --- |
| `app.name` | Especifica el nombre de visualización de la aplicación. El nombre aparece en la página de título de la aplicación Web y en la pantalla de inicio de sesión. Valor predeterminado: `app.name=BI launch pad` |
| `app.name.short` | Especifica el nombre de visualización de la aplicación. El nombre aparece en la página de título de la aplicación Web y en la pantalla de inicio de sesión. Valor predeterminado: `app.name.short=BI launch pad` |
| `app.url.name` | Especifica el nombre de la dirección URL de la aplicación, precedida del carácter «/». Valor predeterminado: `app.url.name=/BI` |
| `authentication.default` | Especifica el método de autenticación predeterminado que se usa para autenticar usuarios en la aplicación. Puede usar cualquiera de las siguientes opciones para esta configuración: |

<table>
<tr><th>Parámetro</th><th>Descripción</th></tr>
<tr><td></td><td>
<table>
<tr><th>Autenticación</th><th>Valor de configuración</th></tr>
<tr><td>Enterprise</td><td>secEnterprise</td></tr>
<tr><td>LDAP</td><td>secLDAP</td></tr>
<tr><td>Windows AD</td><td>secWinAD</td></tr>
<tr><td>SAP</td><td>secSAPR3</td></tr>
<tr><td>PeopleSoft</td><td>secpsenterprise</td></tr>
<tr><td>JD Edwards</td><td>secPSE1</td></tr>
<tr><td>Siebel</td><td>secSiebel7</td></tr>
<tr><td>EBS de Oracle</td><td>secOraApps</td></tr>
</table>
Valor predeterminado:<br>authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>Especifica si los usuarios que inician sesión en la plataforma de lanzamiento de BI tienen la opción de ver y cambiar el método de autenticación. Valor predeterminado: authentication.visible=false</td></tr>
<tr><td>Authentication.VisibleList</td><td>Especifica la visibilidad de la lista de los tipos de autenticación disponibles en la pantalla de inicio de sesión. La siguiente es la lista de los tipos de autenticación disponibles: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7. De la lista, puede seleccionar activar o desactivar los tipos de autenticación incluyendo o excluyendo los tipos de autenticación deseados de la Authentication.VisibleList. Valor predeterminado: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7</td></tr>
<tr><td>sap.system.client.visible<br>authentication.sapSystem<br>authentication.sapClient</td><td>Especifica la visibilidad de los campos Sistema SAP y Cliente SAP cuando selecciona el tipo de autenticación «SAP». Valor predeterminado: sap.system.client.visible=true. Cuando sap.system.client.visible se fija en sap.system.client.visible=false, puede especificar los valores para el Sistema SAP y el Cliente SAP en el archivo de propiedades utilizando los parámetros authentication.sapSystem y authentication.sapClient respectivamente.</td></tr>
<tr><td>cms.default</td><td>Especifica el nombre del CMS predeterminado. Valor predeterminado: cms.default=[name of host machine]</td></tr>
</table>

| Parámetro | Descripción |
| --- | --- |
| `cms.visible` | Especifica si los usuarios que inician sesión en la plataforma de lanzamiento de BI tienen la opción de ver y cambiar el nombre del CMS. Valor predeterminado: `cms.visible=true` |
| `dialogue.prompt.enabled` | Especifica si se debe preguntar a los usuarios cuando navegan fuera de una página de entrada en un cuadro de diálogo. Valor predeterminado: `dialogue.prompt.enabled=false` |
| `logontoken.enabled` | Especifica si se debe habilitar o no la creación de identificadores para la sesión después de que un usuario inicie sesión en la plataforma de lanzamiento de BI. El identificador se almacenará en una cookie. Valor predeterminado: `logontoken.enabled=false` |
| `SMTPFrom` | Habilita o deshabilita el campo *Desde* al programar un objeto en un destino. Valor predeterminado: `SMTPFrom=true`<br><br>Cuando el valor se establece en `false`, el campo *De* no se visualiza y el sistema intenta recuperar el valor de correo electrónico *De* en la orden siguiente:<br><br>1. Primero, del informe predeterminado para un objeto de informe.<br>2. Segundo, de la dirección electrónica del perfil de usuario del usuario registrado.<br>3. Para finalizar, desde el valor predeterminado del servidor de tareas. |
| `url.exit` | Especifica la dirección URL que volverá a dirigir a los usuarios después de finalizar la sesión de la plataforma de lanzamiento de BI. Esta configuración solo se aplica a los usuarios que han iniciado sesión en la aplicación a través de un proceso de verificación externo. |
| `disable.locale.preference` | Habilita o deshabilita al usuario para ver y modificar las preferencias locales de visualización para la plataforma de lanzamiento de BI. Valor predeterminado: `disable.locale.preference=false` |
| `extlogon.allow.logoff` | Habilita o deshabilita el cierre de sesión automático de un usuario una vez que ha cerrado la sesión de la plataforma de lanzamiento de BI. Configúrelo en false si desea que la sesión no finalice automáticamente cuando los usuarios cierren la sesión de la plataforma de lanzamiento de BI. Valor predeterminado: `extlogon.allow.logoff=true` |
| `logon.allowInsecureEmbedding` | Especifica si permitir que otras páginas incluyan esta aplicación (como marco) sin dar paso a un token incrustado válido. Valor predeterminado: `logon.allowInsecureEmbedding=false` |

| Parámetro | Descripción |
| --- | --- |
| `sso.types.and.order` | Especifica una lista delimitada por comas de tipos SSO a habilitar, y el orden en que se ejecutarán.<br><br>Una lista vacía indica que se debe usar la ordenación heredada.<br><br>Si la lista está especificada, se ignorarán las opciones heredadas.<br><br>Opciones válidas: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO`, y `siteminder`.<br><br>Si no se desea ninguno, especifique: `none` |
| `allowed.cms` | Para asegurarse que el inicio de sesión sea seguro y evitar una falsificación de la solicitud por parte del servidor, puede crear una lista blanca de IPs o nombres de CMS válidos, junto con los números de puertos. Ha iniciado la sesión en la aplicación solamente si el valor introducido durante el inicio de sesión coincide exactamente con el valor en la lista blanca.<br><br>Introduzca la lista de nombres de CMS o IPs junto con el número de puerto en la propiedad allowed.cms. Por ejemplo, `allowed.cms =<cms name or IP>:<port number>.` En el caso de que tenga múltiples CMSs a los que conectarse, introduzca los valores separados por coma (,) como se muestra a continuación: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>`<br><br>**Nota**<br>• Para iniciar sesión utilizando el nombre de CMS o IP, añada la propiedad `allowed.cms`.<br>• Ya que el número de puerto es opcional en la pantalla de inicio de sesión, puede seleccionar omitirlo en la lista blanca. Estará iniciando la sesión en el puerto predeterminado. Sin embargo, si el número de puerto está presente en la lista blanca y no se introduce durante el inicio de sesión, el inicio de sesión falla.<br><br>Los siguientes son escenarios que no requieren el uso de la lista blanca: |

| Parámetro | Descripción |
| --- | --- |
| | • Si el valor de `cms.visible` se fija en falso y un CMS se fija para `cms.default`<br>• Si el CMS se establece como cluster e inicia la sesión con el nombre de cluster. Si intenta iniciar sesión con un cluster específico (CMS), el nombre de CMS debe estar presente en la propiedad `allowed.cms`.<br>• Si el inicio de sesión se hace mediante SAP Single Sign-On. |

## 18.4.1.3 Propiedades de la rampa de lanzamiento BI de Fiori

En la siguiente tabla se muestra la configuración que se incluye en el archivo `FioriBI.properties` predeterminado para el archivo BOE.war. Para sobrescribir la configuración, cree un nuevo archivo en `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

> **Nota**
>
> En BI 4.2 SP5, el archivo "Bing.properties" se renombra como "FioriBI.properties". Al actualizar o realizar el upgrade a BI 4.2 SP5 de cualquier versión anterior, tendrá que modificar manualmente el nombre del archivo de propiedades de la rampa de lanzamiento BI de Fiori de "Bing.properties" a "FioriBI.properties", para mantener las configuraciones existentes para la rampa de lanzamiento BI de Fiori.

| Parámetro | Descripción |
| --- | --- |
| `app.name` | Especifica el nombre de visualización de la aplicación. El nombre aparece en la página de título de la aplicación Web y en la pantalla de inicio de sesión. Valor por defecto: `app.name=BI launch pad` |
| `app.name.short` | Especifica el nombre de visualización de la aplicación. El nombre aparece en la página de título de la aplicación Web y en la pantalla de inicio de sesión. Valor por defecto: `app.name.short=BI launch pad` |
| `app.url.name` | Especifica el nombre de la dirección URL de la aplicación, precedida del carácter «/». Valor por defecto: `app.url.name=/BILaunchpad` |
| `authentication.default` | Especifica el método de autenticación predeterminado que se usa para autenticar usuarios en la aplicación. Puede usar cualquiera de las siguientes opciones para esta configuración:<br>**Autenticación** — **Valor de configuración**<br>Enterprise — `secEnterprise` |

| Parámetro | Descripción |
|---|---|
| | <table><tr><th>Autenticación</th><th>Valor de configuración</th></tr><tr><td>LDAP</td><td>secLDAP</td></tr><tr><td>Windows AD</td><td>secWinAD</td></tr><tr><td>SAP</td><td>secSAPR3</td></tr><tr><td>PeopleSoft</td><td>secpsenterprise</td></tr><tr><td>JD Edwards</td><td>secPSE1</td></tr><tr><td>Siebel</td><td>secSiebel7</td></tr><tr><td>EBS de Oracle</td><td>secOraApps</td></tr></table> Valor por defecto: `authentication.default=secEnterprise` |
| `authentication.visible` | Especifica si los usuarios que inician sesión en la rampa de lanzamiento de BI de Fiori tienen la opción de ver y cambiar el método de autenticación. Valor por defecto: `authentication.visible=false` |
| `Authentication.VisibleList` | Especifica la visibilidad de la lista de los tipos de autenticación disponibles en la pantalla de inicio de sesión. La siguiente es la lista de los tipos de autenticación disponibles: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. De la lista, puede seleccionar activar o desactivar los tipos de autenticación incluyendo o excluyendo los tipos de autenticación deseados de la `Authentication.VisibleList`. Valor por defecto: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7` |
| `sap.system.client.visible`<br>`authentication.sapSystem`<br>`authentication.sapClient` | Especifica la visibilidad de los campos *Sistema SAP* y *Cliente SAP* cuando selecciona el tipo de autenticación «SAP». Valor predeterminado: `sap.system.client.visible=true`. Cuando `sap.system.client.visible` se fija en `sap.system.client.visible=false`, puede especificar los valores para el Sistema SAP y el Cliente SAP en el archivo de propiedades utilizando los parámetros `authentication.sapSystem=` y `authentication.sapClient=` respectivamente. |
| `cms.default` | Especifica el nombre del CMS predeterminado. Valor por defecto: `cms.default=[name of host machine]` |
| `cms.visible` | Especifica si los usuarios que inician sesión en la rampa de lanzamiento de BI de Fiori tienen la opción de ver y cambiar el nombre del CMS. Valor por defecto: `cms.visible=true` |

| Parámetro | Descripción |
| --- | --- |
| `dialogue.prompt.enabled` | Especifica si se debe preguntar a los usuarios cuando navegan fuera de una página de entrada en un cuadro de diálogo. Valor por defecto: `dialogue.prompt.enabled=false` |
| `logontoken.enabled` | Especifica si se debe habilitar o no la creación de identificadores para la sesión después de que un usuario inicie sesión en la plataforma de lanzamiento de BI. El identificador se almacenará en una cookie. Valor por defecto: `logontoken.enabled=false` |
| `SMTPFrom` | Habilita o deshabilita el campo *Desde* al programar un objeto en un destino. Valor por defecto: `SMTPFrom=true`<br><br>Cuando el valor se establece en `false`, el campo *De* no se visualiza y el sistema intenta recuperar el valor de correo electrónico *De* en la orden siguiente:<br><br>1. Primero, del informe predeterminado para un objeto de informe.<br>2. Segundo, de la dirección electrónica del perfil de usuario del usuario registrado.<br>3. Para finalizar, desde el valor predeterminado del servidor de tareas. |
| `url.exit` | Especifica la dirección URL que volverá a dirigir a los usuarios después de finalizar la sesión de la rampa de lanzamiento de BI de Fiori. Esta configuración solo se aplica a los usuarios que han iniciado sesión en la aplicación a través de un proceso de verificación externo. |
| `disable.locale.preference` | Habilita o deshabilita al usuario para ver y modificar las preferencias locales de visualización para la rampa de lanzamiento de BI de Fiori. Valor por defecto: `disable.locale.preference=false` |
| `extlogon.allow.logoff` | Habilita o deshabilita el cierre de sesión automático de un usuario una vez que ha cerrado la sesión de la rampa de lanzamiento de BI de Fiori. Configúrelo en false si desea que la sesión no finalice automáticamente cuando los usuarios cierren la sesión de la plataforma de lanzamiento de BI. Valor por defecto: `extlogon.allow.logoff=true` |
| `logon.allowInsecureEmbedding` | Especifica si permitir que otras páginas incluyan esta aplicación (como marco) sin dar paso a un token incrustado válido. Valor por defecto: `logon.allowInsecureEmbedding=false` |
| `sso.types.and.order` | Especifica una lista delimitada por comas de tipos SSO a habilitar, y el orden en que se ejecutarán.<br><br>Una lista vacía indica que se debe usar la ordenación heredada.<br><br>Si la lista está especificada, se ignorarán las opciones heredadas. |

| Parámetro | Descripción |
| --- | --- |
| | Opciones válidas: `vintela`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `trustedX509`, `sapSSO`, y `siteminder`.<br><br>Si no se desea ninguno, especifique: `none` |
| `allowed.cms` | Para asegurarse que el inicio de sesión sea seguro y evitar una falsificación de la solicitud por parte del servidor, puede crear una lista blanca de IPs o nombres de CMS válidos, junto con los números de puertos. Ha iniciado la sesión en la aplicación solamente si el valor introducido durante el inicio de sesión coincide exactamente con el valor en la lista blanca.<br><br>Introduzca la lista de nombres de CMS o IPs junto con el número de puerto en la propiedad allowed.cms. Por ejemplo, `allowed.cms =<cms name or IP>:<port number>.` En el caso de que tenga múltiples CMS a los que conectarse, introduzca los valores separados por coma (,) como se muestra a continuación: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>`<br><br>**Nota**<br>• Para iniciar sesión utilizando el nombre de CMS o IP, añada la propiedad `allowed.cms`.<br>• Ya que el número de puerto es opcional en la pantalla de inicio de sesión, puede seleccionar omitirlo en la lista blanca. Estará iniciando la sesión en el puerto predeterminado. Sin embargo, si el número de puerto está presente en la lista blanca y no se introduce durante el inicio de sesión, el inicio de sesión falla.<br><br>Los siguientes son escenarios que no requieren el uso de la lista blanca:<br>• Si el valor de `cms.visible` se fija en falso y un CMS se fija para `cms.default`<br>• Si el CMS se establece como cluster e inicia la sesión con el nombre de cluster. Si intenta iniciar sesión con un cluster específico (CMS), el nombre de CMS debe estar presente en la propiedad `allowed.cms`. |

| Parámetro | Descripción |
| --- | --- |
| | • Si el inicio de sesión se hace mediante SAP Single Sign-On. |
| upload.file.maxsize.inMB=0 | El tamaño máximo de archivo para carga de documento local se expresa en MegaBytes y debe ser un número entero, por ejemplo: 10 etc. |
| upload.file.allowed.formats= | Esta propiedad se utiliza para controlar diferentes clases de archivos permitidos para cargar el documento local. Consulte la Nota SAP 2296060 para obtener la lista de formatos de archivo admitidos.<br><br>Si define varios formatos, separe cada formato de archivo seguido de una coma como txt, doc, xls. |
| app.custom.banner.message | Especifica el mensaje del banner en la plataforma de lanzamiento de BI. |
| logon.webssoauthnetication.framework=None | Esta propiedad se utiliza para habilitar el flujo de trabajo de autenticación SSO web. Los valores posibles son Ninguno, OpenId y SAML. |
| openid.restful.url= | Esta propiedad se utiliza para establecer la dirección URL Restful que se proporciona en la CMC. Por ejemplo: `http://<hostname>:<portNo>/biprws` |

## 18.4.1.4 Propiedades de OpenDocument

En la siguiente tabla se muestra la configuración que se incluye en el archivo `opendocument.properties` predeterminado para el archivo BOE.war. Para sobrescribir la configuración, cree un nuevo archivo en `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

| Parámetro | Descripción |
| --- | --- |
| `app.name` | Especifica el nombre de visualización de la aplicación. El nombre aparece en la página de título de la aplicación Web y en la pantalla de inicio de sesión. Predeterminado: `app.name=SAP BusinessObjects OpenDocument` |
| `app.name.short` | Especifica el nombre de visualización de la aplicación. El nombre aparece en la página de título de la aplicación Web y en la pantalla de inicio de sesión. Predeterminado: `app.name.short=OpenDocument` |
| `authentication.default` | Especifica el método de autenticación predeterminado que se usa para autenticar usuarios en la aplicación. Puede usar cualquiera de las siguientes opciones para esta configuración: |

<table>
<tr><th>Parámetro</th><th>Descripción</th></tr>
<tr><td></td><td>
<table>
<tr><th>Autenticación</th><th>Valor de configuración</th></tr>
<tr><td>Enterprise</td><td>secEnterprise</td></tr>
<tr><td>LDAP</td><td>secLDAP</td></tr>
<tr><td>Windows AD</td><td>secWinAD</td></tr>
<tr><td>SAP</td><td>secSAPR3</td></tr>
<tr><td>PeopleSoft</td><td>secpsenterprise</td></tr>
<tr><td>JD Edwards</td><td>secPSE1</td></tr>
<tr><td>Siebel</td><td>secSiebel7</td></tr>
<tr><td>EBS de Oracle</td><td>secOraApps</td></tr>
</table>
Valor predeterminado:<br>authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>Especifica si los usuarios que inician sesión en OpenDocument tienen la opción de ver y cambiar el método de autenticación. Predeterminado: authentication.visible=false</td></tr>
<tr><td>Authentication.VisibleList</td><td>Especifica la visibilidad de la lista de los tipos de autenticación disponibles en la pantalla de inicio de sesión. La siguiente es la lista de los tipos de autenticación disponibles: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7. De la lista, puede seleccionar activar o desactivar los tipos de autenticación incluyendo o excluyendo los tipos de autenticación deseados de la Authentication.VisibleList. Valor predeterminado: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7</td></tr>
<tr><td>sap.system.client.visible<br>authentication.sapSystem<br>authentication.sapClient</td><td>Especifica la visibilidad de los campos Sistema SAP y Cliente SAP cuando selecciona el tipo de autenticación «SAP». Valor predeterminado: sap.system.client.visible=true. Cuando sap.system.client.visible se fija en sap.system.client.visible=false, puede especificar los valores para el Sistema SAP y el Cliente SAP en el archivo de propiedades utilizando los parámetros authentication.sapSystem= y authentication.sapClient= respectivamente.</td></tr>
<tr><td>cms.default</td><td>Especifica el nombre del CMS predeterminado. Predeterminado: cms.default=[name of host machine]</td></tr>
</table>

| Parámetro | Descripción |
| --- | --- |
| `cms.visible` | Especifica si los usuarios que inician sesión en OpenDocument tienen la opción de ver y cambiar el nombre del CMS. Predeterminado: `cms.visible=true` |
| `logontoken.enabled` | Especifica si se debe habilitar o no la creación de identificadores para la sesión después de que un usuario inicie sesión en OpenDocument. El identificador se almacenará en una cookie. Predeterminado: `logontoken.enabled=false` |
| `extlogon.allow.logoff` | Habilita o deshabilita el cierre de sesión automático de un usuario una vez que ha cerrado la sesión de OpenDocument. Configúrelo en false si desea que la sesión no finalice automáticamente cuando los usuarios cierren la sesión de OpenDocument. Predeterminado: `extlogon.allow.logoff=true` |
| `SAPLogonToken.enabled` | Especifica si se va a permitir que los tokens de inicio de sesión de SAP del Servicio Web RESTful se autentiquen ante la plataforma de BI. El token de inicio de sesión de SAP se especifica mediante el valor X-SAP-LogonToken en el encabezado de solicitud tras un inicio de sesión correcto con la dirección URL del Servicio Web RESTful. Predeterminado: `SAPLogonToken.enabled=true` |
| `logon.allowInsecureEmbedding=false` | Especifica si permitir que otras páginas incluyan esta aplicación (como marco) sin dar paso a un token incrustado válido. Predeterminado: `logon.allowInsecureEmbedding=false` |
| `sso.types.and.order` | Especifica una lista delimitada por comas de tipos SSO a habilitar, y el orden en que se ejecutarán.<br><br>Una lista vacía indica que se debe usar la ordenación heredada.<br><br>Si la lista está especificada, se ignorarán las opciones heredadas.<br><br>Opciones válidas: `serializedSession`, `sapLogonToken`, `trustedIIS`, `trustedHeader`, `trustedParameter`, `trustedCookie`, `trustedSession`, `trustedUserPrincipal`, `trustedVintela`, `vintela`, `infoview`, `trustedX509`, `sapSSO`, y `siteminder`.<br><br>Si no se desea ninguno, especifique: `none` |
| `allowed.cms` | Para asegurarse que el inicio de sesión sea seguro y evitar una falsificación de la solicitud por parte del servidor, puede crear una lista blanca de IPs o nombres de CMS válidos, junto con los números de puertos. Ha iniciado la sesión en la aplicación solamente si el valor introducido durante el |

| Parámetro | Descripción |
| --- | --- |
| | inicio de sesión coincide exactamente con el valor en la lista blanca.<br><br>Introduzca la lista de nombres de CMS o IPs junto con el número de puerto en la propiedad allowed.cms. Por ejemplo, `allowed.cms =<cms name or IP>:<port number>.` En el caso de que tenga múltiples CMSs a los que conectarse, introduzca los valores separados por coma (,) como se muestra a continuación: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>`<br><br>**Nota**<br>• Para iniciar sesión utilizando el nombre de CMS o IP, añada la propiedad `allowed.cms`.<br>• Ya que el número de puerto es opcional en la pantalla de inicio de sesión, puede seleccionar omitirlo en la lista blanca. Estará iniciando la sesión en el puerto predeterminado. Sin embargo, si el número de puerto está presente en la lista blanca y no se introduce durante el inicio de sesión, el inicio de sesión falla.<br><br>Los siguientes son escenarios que no requieren el uso de la lista blanca:<br>• Si el valor de `cms.visible` se fija en falso y un CMS se fija para `cms.default`<br>• Si el CMS se establece como cluster e inicia la sesión con el nombre de cluster. Si intenta iniciar sesión con un cluster específico (CMS), el nombre de CMS debe estar presente en la propiedad `allowed.cms`.<br>• Si el inicio de sesión se hace mediante SAP Single Sign-On. |

## 18.4.1.5 Propiedades de la CMC

En la siguiente tabla se muestra la configuración que se incluye en el archivo `cmc.properties` predeterminado para BOE.war. Para sobrescribir la configuración, cree un nuevo archivo en `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

| Parámetro | Descripción |
| --- | --- |
| `app.url.name` | Especifica el nombre de la dirección URL de la aplicación, precedida del carácter «/». Valor predeterminado: `app.url.name=/CMC` |
| `authentication.default` | Especifica el método de autenticación predeterminado que se usa para autenticar usuarios en la aplicación. Puede usar cualquiera de las siguientes opciones para esta configuración:<br><br>**Autenticación** / **Valor de configuración**<br>Enterprise: `secEnterprise`<br>LDAP: `secLDAP`<br>Windows AD: `secWinAD`<br>SAP: `secSAPR3`<br>PeopleSoft: `secpsenterprise`<br>JD Edwards: `secPSE1`<br>Siebel: `secSiebel7`<br>EBS de Oracle: `secOraApps`<br><br>Valor predeterminado: `authentication.default=secEnterprise` |
| `authentication.visible` | Especifica si los usuarios que inician sesión en la CMC tienen la opción de ver y cambiar el método de autenticación. Predeterminado: `authentication.visible=false` |
| `Authentication.VisibleList` | Especifica la visibilidad de la lista de los tipos de autenticación disponibles en la pantalla de inicio de sesión. La siguiente es la lista de los tipos de autenticación disponibles: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`. De la lista, puede seleccionar activar o desactivar los tipos de autenticación incluyendo o excluyendo los tipos de autenticación deseados de la `Authentication.VisibleList`. Valor predeterminado: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7` |
| `sap.system.client.visible`<br>`authentication.sapSystem`<br>`authentication.sapClient` | Especifica la visibilidad de los campos *Sistema SAP* y *Cliente SAP* cuando selecciona el tipo de autenticación «SAP». Valor predeterminado: `sap.system.client.visible=true`. Cuando `sap.system.client.visible` se fija en `sap.system.client.visible=false`, puede especificar los valores para el Sistema SAP y el |

| Parámetro | Descripción |
| --- | --- |
| | Cliente SAP en el archivo de propiedades utilizando los parámetros `authentication.sapSystem=` y `authentication.sapClient=` respectivamente. |
| `cms.default` | Especifica el nombre del CMS predeterminado. Valor predeterminado: `cms.default=[name of host machine]` |
| `cms.visible` | Especifica si los usuarios que inician sesión en la CMC tienen la opción de ver y cambiar el nombre del CMS. Valor predeterminado: `cms.visible=true` |
| `dialogue.prompt.enabled` | Especifica si se debe preguntar a los usuarios cuando navegan fuera de una página de entrada en un cuadro de diálogo. Valor predeterminado: `dialogue.prompt.enabled=false` |
| `logontoken.enabled` | Especifica si se debe habilitar o no la creación de identificadores para la sesión después de que un usuario inicie sesión en la CMC. El identificador se almacenará en una cookie. Valor predeterminado: `logontoken.enabled=false` |
| `SMTPFrom` | Habilita o deshabilita el campo *Desde* al programar un objeto en un destino. Valor predeterminado: `SMTPFrom=true`<br><br>Cuando el valor se establece en `false`, el campo *De* no se visualiza y el sistema intenta recuperar el valor de correo electrónico *De* en la orden siguiente:<br><br>1. Primero, del informe predeterminado para un objeto de informe.<br>2. Segundo, de la dirección electrónica del perfil de usuario del usuario registrado.<br>3. Para finalizar, desde el valor predeterminado del servidor de tareas. |
| `ulr.exit` | Especifica la dirección URL que volverá a dirigir a los usuarios después de finalizar la sesión de CMC. Esta configuración solo se aplica a los usuarios que han iniciado sesión en la aplicación a través de un proceso de verificación externo. |
| `allowed.cms` | Para asegurarse que el inicio de sesión sea seguro y evitar una falsificación de la solicitud por parte del servidor, puede crear una lista blanca de IPs o nombres de CMS válidos, junto con los números de puertos. Ha iniciado la sesión en la aplicación solamente si el valor introducido durante el inicio de sesión coincide exactamente con el valor en la lista blanca.<br><br>Introduzca la lista de nombres de CMS o IPs junto con el número de puerto en la propiedad allowed.cms. |

| Parámetro | Descripción |
| --- | --- |
| | Por ejemplo, `allowed.cms =<cms name or IP>:<port number>.` En el caso de que tenga múltiples CMSs a los que conectarse, introduzca los valores separados por coma (,) como se muestra a continuación: `allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>`<br><br>**Nota**<br>• Para iniciar sesión utilizando el nombre de CMS o IP, añada la propiedad `allowed.cms`.<br>• Ya que el número de puerto es opcional en la pantalla de inicio de sesión, puede seleccionar omitirlo en la lista blanca. Estará iniciando la sesión en el puerto predeterminado. Sin embargo, si el número de puerto está presente en la lista blanca y no se introduce durante el inicio de sesión, el inicio de sesión falla.<br><br>Los siguientes son escenarios que no requieren el uso de la lista blanca:<br>• Si el valor de `cms.visible` se fija en falso y un CMS se fija para `cms.default`<br>• Si el CMS se establece como cluster e inicia la sesión con el nombre de cluster. Si intenta iniciar sesión con un cluster específico (CMS), el nombre de CMS debe estar presente en la propiedad `allowed.cms`.<br>• Si el inicio de sesión se hace mediante SAP Single Sign-On. |

## 18.5 Personalizar los puntos de acceso de inicio de sesión de la plataforma de lanzamiento de BI y OpenDocument

Puede personalizar la página de inicio de sesión para las aplicaciones Web de la plataforma de lanzamiento de BI y OpenDocument. Por ejemplo, puede personalizar la página de inicio de sesión para usar un logotipo u hoja de estilo corporativa de la empresa, o puede crear una página de inicio de sesión personalizada que permita la autenticación de confianza.

Para personalizar la página de inicio de sesión, modifique el archivo `custom.jsp` almacenado en las áreas de aplicación de la Plataforma de lanzamiento de BI y OpenDocument de la aplicación Web `BOE.war`, y vuelva a desplegar la aplicación Web `BOE.war` en el sistema de la Plataforma de BI. Los usuarios acceden al punto de acceso de inicio de sesión personalizado desplazándose a una única dirección URL.

Para trabajar con estos ejemplos, debe conocer el despliegue de las aplicaciones Web de la Plataforma de BI. Para obtener más información, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 18.5.1 Ubicaciones de la plataforma de lanzamiento de BI y OpenDocument

Las aplicaciones Web de la plataforma de lanzamiento de BI y OpenDocument se empaquetan en el archivo Web `BOE.war`. La ubicación del archivo `BOE.war` se define en el archivo `BOE.properties`.

El archivo `BOE.properties` se encuentra aquí en los sistemas Windows:

- `<DIR_INSTALACIÓN_BOE>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

El archivo `BOE.properties` se encuentra aquí en los sistemas UNIX:

- `<DIR_INSTALACIÓN_BOE>/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

Las siguientes tablas definen la ubicación de los archivos comunes dentro del archivo Web `BOE.war` para las aplicaciones de la plataforma de lanzamiento de BI y OpenDocument.

Ubicaciones del archivo de la Plataforma de lanzamiento de BI

> **Nota**
>
> La aplicación Web de la plataforma de lanzamiento de BI se conocía como InfoView.

| Tipo de archivo | Ubicación |
|---|---|
| Secuencia de comandos de inicio de sesión personalizado | `WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp` |
| Directorio para archivos adicionales | `WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources` |
| Dirección URL de inicio de sesión personalizado | `http://<nombreservidor>:<puerto>/BOE/BI/custom.jsp` |

Ubicaciones del archivo de OpenDocument

| Tipo de archivo | Ubicación |
|---|---|
| Secuencia de comandos de inicio de sesión personalizado | `WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp` |
| Directorio para archivos adicionales | `WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources` |

| Tipo de archivo | Ubicación |
| --- | --- |
| Dirección URL de inicio de sesión personalizado | `http://<nombreservidor>:<puerto>/BOE/OpenDocument/opendoc/custom.jsp` |

## 18.5.2 Definir una página de inicio de sesión personalizada

Puede personalizar el punto de entrada a la página de inicio de sesión de la Plataforma de BI. Por ejemplo, puede crear una página de inicio de sesión personalizada que muestre el logotipo de la empresa y use una hoja de estilo corporativa.

Edite el archivo `custom.jsp` para personalizar la experiencia de inicio de sesión para los usuarios y coloque los archivos de compatibilidad en la carpeta `noCacheCustomResources`.

Este ejemplo muestra cómo crear una página de inicio de sesión personalizada que vuelva a dirigir al usuario a la página de inicio de sesión estándar.

1. Cree un archivo que contenga el código de inicio de sesión personalizado y guárdelo como `custom.js` en la carpeta `noCacheCustomResources`.

   Este ejemplo define una función que vuelva a dirigir al usuario a la página de inicio de sesión estándar, `logon.faces`.

   ```
   function load() {window.location =  "logon.faces";}
   ```

2. Edite el archivo `custom.jsp` para personalizar la página de inicio de sesión.

   Este ejemplo muestra un mensaje de bienvenida y un hipervínculo que llama al método `load` definido en el archivo `custom.js`.

   ```
   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    "http://www.w3.org/TR/html4/loose.dtd">
   <%@ page language=  "java" contentType=  "text/html;charset=utf-8"%>
   <html>
     <head> <title>Welcome</title>
     </head>
     <body>
       <script type=  "text/javascript" src=  "noCacheCustomResources/
   custom.js"></script>
       <p>Welcome to ABC corporation.</p>
       <a href= "javascript:load()">Enter</a>
     </body>
   </html>
   ```

3. Vuelva a desplegar la aplicación Web `BOE.war` y reinicie el servidor Web.

## 18.5.3 Agregar una autenticación de confianza al inicio de sesión

Para habilitar la autenticación de confianza, configure el usuario de confianza como un atributo de sesión en el archivo `custom.jsp` y modifique la configuración de la autenticación en una copia del archivo

`global.properties`. Los valores de la copia personalizada del archivo `global.properties` sobrescriben los valores predeterminados.

> **Nota**
>
> No se debe habilitar la autenticación de confianza sin HTTPS por motivos de seguridad. Activar la autenticación de confianza sin https se considera una infracción de seguridad, ya que el URL queda expuesto a usuarios no autorizados. Para evitar una brecha de seguridad, la información del usuario se puede validar con un certificado válido. Para obtener más información, consulte 1388240

1. Edite el archivo `custom.jsp` para configurar un atributo de sesión que defina el usuario de confianza.

   ```
   request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
   ```

2. Cree una copia personalizada del archivo `global.properties` copiando `WEB-INF\config\default\global.properties` en `WEB-INF\config\custom\global.properties`.
3. Modifique `WEB-INF\config\custom\global.properties` para habilitar el inicio de sesión único (SSO).

   ```
   sso.enabled=true
   ```

4. Modifique `WEB-INF\config\custom\global.properties` para configurar los parámetros de autenticación de confianza, incluyendo la variable de sesión de usuario de confianza, y el secreto compartido.

   Sustituya `"..."` por el secreto compartido del sistema.

   ```
   trusted.auth.user.param=TrustedUserAttribute
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.shared.secret="..."
   ```

   Para obtener más detalles, consulte el tema relacionado sobre configurar autenticación de confianza para aplicaciones Web.
5. Vuelva a desplegar la aplicación Web y reinicie el servidor Web.
6. En la CMC, habilite la autenticación de confianza.

   En la ficha *Autenticación*, haga doble clic en *Enterprise* y, a continuación, seleccione la casilla de verificación *La autenticación de confianza está habilitada*.

## Información relacionada

Habilitación de la autenticación de confianza [página 262]
Configurar la autenticación de confianza para la aplicación Web [página 269]

# 18.6 Personalización de interfaces de usuario de aplicación

Algunas interfaces de usuario de aplicación se pueden personalizar a través de la CMC.

En la Consola de administración central puede personalizar el aspecto de algunas aplicaciones. Por ejemplo, puede cambiar los elementos de la interfaz de usuario.

## 18.6.1 Web Intelligence

### 18.6.1.1 Personalizar los elementos de interfaz de Web Intelligence por grupos de usuario y carpetas

La personalización le permite ocultar varios elementos de interfaz para simplificar la forma en que los usuarios finales interactúan con la aplicación, dependiendo de los grupos de usuarios y las carpetas que contengan documentos de Web Intelligence. Puede ocultar tipos de orígenes de datos, cambiar al modo de edición, desactivar la función de actualización automática, etc.

Por defecto están habilitados todos los elementos de la interfaz. Si quiere ocultarlos, puede hacerlo en la Consola de administración central. La siguiente tabla detalla los elementos de la interfaz de usuario que puede ocultar.

| Lista de funciones | Descripción |
|---|---|
| *Modo* | Oculta los modos disponibles a los que puede acceder el usuario a través del botón desplegable.<br>• Lectura<br>Para ocultar el modo lectura del botón desplegable.<br>• Diseño<br>Para ocultar los modos de diseño y estructura del botón desplegable.<br>• Datos<br>Para ocultar el modo de datos del botón desplegable.<br>Si están desactivados todos los modos, los documentos solo pueden abrirse en modo de lectura. |
| *Ubicación* | Oculta una categoría completa de fuentes de datos. Las categorías que puede desactivar son:<br>• Repositorio de plataforma BI<br>• Local (solo disponible en el cliente enriquecido)<br>• Servicios Web<br>• Google Drive<br>• Microsoft OneDrive |

| Lista de funciones | Descripción |
| --- | --- |
| *Fuente de datos* | En el modo de diseño puede restringir las fuentes de datos disponibles en los cuadros de diálogo *Seleccionar una fuente de datos* y *Modificar fuente*.<br><br>Los orígenes de datos que puede desactivar son:<br><br>• Universos<br>• Documentos de Web Intelligence<br>• Archivos de Excel<br>• Archivos de texto<br>• SAP BW<br>• Vistas SAP HANA<br>• Consultas SQL manuales<br>• OData<br>• Hoja de cálculo de Google |
| *Consulta* | • Actualizar<br>En el modo de lectura, oculta la sección *Datos* de la barra de herramientas. En el modo de diseño, oculta el menú desplegable *Actualizar*, el comando *Actualizar todo* y el botón *Ejecutar* junto con su menú desplegable en el panel de consulta.<br>• Actualización avanzada<br>En el modo de diseño, oculta el comando *Actualización avanzada* del menú desplegable *Actualizar*.<br>• Actualización automática<br>Oculta la opción *Actualización automática* del modo de presentación.<br>• Cambiar fuente<br>En el modo de diseño, oculta la capacidad de modificar las fuentes de datos del documento. |
| *Datos* | En el modo de datos, oculta las funciones de Combinar cubos. |
| *Análisis* | • Explorar<br>En los modos de lectura y diseño, oculta la casilla de verificación *Explorar* de la sección Analizar de la barra de herramientas y los filtros de exploración de la *barra de filtros*. Además, en el informe no se visualizan como hipervínculos los valores que se pueden explorar, y se ocultan las acciones y los iconos de exploración disponibles para estos valores.<br>En el modo de diseño, oculta los filtros de exploración del panel *Crear* en *Filtros de datos*.<br>• Seguir los cambios de datos<br>En los modos de lectura y diseño, ocultar *Seguimiento de modificaciones de datos* y *Mostrar modificaciones* de la barra de herramientas. |

| Lista de funciones | Descripción |
|---|---|
| *Documentos* | • *Nuevo*, *Abrir*, *Guardar*, *Favoritos*, *Modo de presentación*.<br>Oculta los botones correspondientes de la barra de herramientas.<br>• Comentarios<br>En los modos de lectura y diseño, ocultar la ficha *Comentarios* del panel lateral y el comando *Comentarios* del menú contextual.<br>• Elementos compartidos<br>En el modo de diseño, ocultar la ficha *Elementos compartidos* en el panel lateral y el comando *Elementos compartidos* en la sección *Insertar* de la barra de herramientas. |
| *Exportar a* | En cualquier modo, oculta la posibilidad de exportar informes de documentos y cubos a:<br>• Excel<br>• PDF<br>• HTML<br>• TXT<br>• CSV |
| *Generar enlace* | En el modo de diseño, oculta la capacidad de crear un enlace OpenDocument y generar enlaces OData para consultas y elementos de informe individuales de menús contextuales. |
| *Programar y publicar* | Oculta la posibilidad de programar y publicar documentos en TXT, XLS, PDF, HTML, MHTML y CSV. |

## 18.6.1.1.1 Interfaz de personalización

Puede seleccionar carpetas individuales para que los documentos que contienen se beneficien automáticamente de la personalización. Basta con seleccionar una o más carpetas del área *Carpetas personalizadas* e ir a la ficha *Funciones* para iniciar la personalización. De forma predeterminada, la personalización se aplica a todos los documentos de la carpeta que ha seleccionado.

La ficha *Funciones* reúne todas las funciones que puede habilitar o deshabilitar. Utilice las casillas de selección dedicadas para activarlas o desactivarlas.

## 18.6.1.1.2 Reglas de personalización

Los reglas siguientes se utilizan para definir las personalizaciones a aplicar a un usuario:

- Si el usuario pertenece a diferentes grupos, solo se aplica la personalización definida para el grupo cuyo ID es el más bajo. No se aplica la personalización definida para los otros grupos que contienen el usuario.
- Para la estructura de carpeta anidada, la carpeta inmediatamente superior del documento que se ha añadido en la lista de carpetas personalizadas define las personalizaciones para el documento para los elementos de interfase de usuario, las propiedades y las extensiones.

- La personalización definida para las carpetas por defecto se aplica a los documentos almacenados en los Documentos personales y las Bandejas de entrada personales, y a los documentos para los que la carpeta superior no está personalizada.
- La personalización definida para los elementos de interfase de usuario que tienen prioridad por encima de la personalización definida para las propiedades como propiedades solo es un acceso directo para activar todos los elementos de interfase usuario.
- Escenario: Cuando los elementos de personalización se muestran como una lista de árbol y deshabilita un nodo en un sistema. Aquí, si actualiza este sistema con una versión más reciente del producto que tiene posiciones nuevas en los nodos, estas posiciones se activan por defecto incluso si el nodo superior está desactivado.

### 18.6.1.1.3 Personalizar la apariencia de la interfaz de Web Intelligence

Puede personalizar la apariencia de la interfaz de usuario de Web Intelligence ocultando elementos, subelementos y funciones del menú para un grupo de usuarios seleccionado y una carpeta de documentos.

1. Conéctese a la CMC como administrador.
2. En la lista *Organizar*, seleccione *Usuarios y grupos*.
3. En la lista *Jerarquía de grupo*, seleccione un grupo de usuarios.
4. En la lista *Acciones*, seleccione *Personalización*.
5. En la sección *Carpetas personalizadas*, realice una de las siguientes acciones:

| Opción | Descripción |
|---|---|
| **Para definir una personalización predeterminada** | 1. Seleccione *Carpetas por defecto* en la sección *Carpetas personalizadas*. |
| **Para añadir las carpetas de documentos para las que desea aplicar la personalización para el grupo de usuarios seleccionado** | 1. Haga clic en *Añadir carpeta*.<br>2. Seleccione las carpetas.<br>Las carpetas se muestran en la sección *Carpetas personalizadas*. |
| **Para evitar volver a definir la misma personalización para otras carpetas** | 1. En la sección *Carpetas personalizadas*, seleccione la carpeta a partir de la que quiera copiar la personalización.<br>2. En la lista desplegable, haga clic en *Duplicar personalización*.<br>3. Seleccione la carpeta para la que desee definir la personalización.<br>4. Haga clic en *Pegar personalización*.<br>5. Vaya al paso 7. |
| **Para eliminar la personalización de una carpeta específica** | 1. En la sección *Carpetas personalizadas*, seleccione la carpeta en cuestión.<br>2. En la lista desplegable, haga clic en *Eliminar carpeta*.<br>3. Vaya al paso 7. |

| Opción | Descripción |
| --- | --- |
| | **Nota**<br>No puede eliminar *carpetas predeterminadas*. |

6. Marque o desmarque posiciones de la ficha *Funciones* para mostrarlas u ocultarlas en Web Intelligence.

   Si desmarca todos los elementos secundarios de un elemento principal, este también se desmarca y oculta en Web Intelligence. Para obtener más información, consulte Personalizar los elementos de interfaz de Web Intelligence por grupos de usuario y carpetas [página 783].
7. Haga clic en *Guardar y cerrar*.

Al guardar la personalización, todos los usuarios del grupo seleccionado verán estas modificaciones la próxima vez que inicien sesión en la plataforma de lanzamiento de BI y abran Web Intelligence.

> **Nota**
>
> Le recomendamos que inicie sesión en la plataforma de lanzamiento de BI como usuario del grupo que acaba de personalizar, inicie Web Intelligence, y verifique que la interfaz se corresponde con los ajustes de configuración.

## 18.6.1.2 Alineación de contenido de Web Intelligence

Seleccione cómo se alineará el contenido del documento (de izquierda a derecha o de derecha a izquierda) cuando los usuarios crean documentos de Web Intelligence.

Para la interfaz de Cliente enriquecido, la alineación de contenido se determina según las configuraciones regionales establecidas en las preferencias de la plataforma de lanzamiento de BI:

- El sistema usa alineación de derecha a izquierda solo si las dos configuraciones regionales de visualización preferida y de producto están establecidas en idiomas de derecha a izquierda.
- En los demás casos, la alineación de contenido es de izquierda a derecha.

> **Nota**
>
> Para obtener información sobre cómo establecer configuraciones regionales, consulte el *Manual del usuario de la plataforma de lanzamiento de Business Intelligence*.

> **Nota**
>
> La alineación de contenido solo se aplica a la hora de creación de documentos y no afecta a los documentos existentes.

## 18.6.1.3 Habilitar puntos de extensión de la interfaz de usuario de Web Intelligence

Puede configurar derechos de Web Intelligence para permitir a grupos de usuarios seleccionados acceder a extensiones de interfaz personalizadas. Consulte *Guía de desarrollo SAP BusinessObjects BI para Web Intelligence y layer semántico BI* para más información acerca de paquetes de extención y las llamadas API de servicios REST que están disponibles.

### 18.6.1.3.1 Habilitar puntos de ampliación de interfaz de usuario de Web Intelligence

- Ha creado y desplegado la extensión adecuada en la instalación. Despliegue una ampliación para cada función de ampliación (por ejemplo, Botón personalizado o Guardar como HTML).
- Ha añadido la extensión a la lista de URL de confianza. Si no lo ha hecho, consulte la sección Añadir URLs de confianza a la lista de URLs autorizados [página 724].

1. Inicie sesión en la CMC como administrador.
2. En la lista *Organizar*, seleccione *Ususarios y grupos*.
3. En la lista *Jerarquía de grupo*, seleccione un grupo de usuarios.
4. En la lista *Acciones*, seleccione *Personalización*
5. Haga clic en la ficha *Ampliaciones* y realice una de las siguientes acciones:

| Opción | Descripción |
|---|---|
| **Para agregar una ampliación OSGi desplegada en la plataforma de BI y su servidor de aplicación** | Seleccione las ampliaciones personalizadas que desea que utilicen los usuarios. |
| **Para agregar una ampliación no OSGi desplegada en el servidor de aplicación de la plataforma de BI o en un servidor de aplicación externo** | 1. Haga clic en *Agregar*.<br>2. Introduzca la dirección URL de la ampliación.<br>Es la URL del fichero JSON.<br>**Nota**<br>Sustituya todos los espacios en blanco de la URL con **`20`**.<br>Ejemplos:<br>• Servidor de aplicaciones de Apache Tomcat:<br>`http://myserver/webiextension/extension/SAP/RayLight_Embedded/extension.json`<br>• Servidor de aplicaciones externo:<br>`http://www.mysite.org/documents/web/extension/Custom%20Button/extension.json`<br>3. Seleccione *Fijar información proxy si es necesaria* en su servidor de aplicación e introduzca nombre de servidor y número de puerto. |

| Opción | Descripción |
| --- | --- |
| | 4. Seleccione *Ninguna autenticación* o *Autenticación básica* si lo requiere su servidor de aplicaciones e introduzca su nombre de usuario y la contraseña.<br>5. Haga clic en *Aceptar* y seleccione la extensión.<br>6. Haga clic en *Grabar*. |
| **Para modificar información detallada de una extensión.** | Haga clic en *Modificar*. |
| **Para eliminar una extensión de CMC.** | Haga clic en *Eliminar*. |

6. Haga clic en *Guardar y cerrar*.

Las extensiones hablitadas están disponibles para el grupo de usuarios seleccionado al abrir un documento ubicado en la carpeta seleccionada. Los puntos de ampliación están disponibles para todos los clientes de aplicación de Web Intelligence: web, Java Applet y Cliente enriquecido.

## 18.6.2 Plataforma de lanzamiento de BI

### 18.6.2.1 Activar valores en las peticiones de limpieza en el cuadro de diálogo Programación

Al programar un documento de Web Intelligence basado en una consulta BEx que contenga peticiones SAP BW, los usuarios de la plataforma de lanzamiento BI pueden borrar un valor de petición de forma que se obtenga mediante una variable de fuente de datos de SAP BW cuando se ejecute un documento o fíjelo antes de ejecutar el job de planificación.

El procedimiento siguiente le permite visualizar dos botones en la interfaz de usuario:

- *Utilizar valor dinámico*: Deje que la fuente de datos SAP BW procese el valor.
- *Utilizar valor constante*: Introducir un valor fijo.

1. Realice una de las acciones siguientes en la carpeta `<InstallDir>\<WebAppServer>\webapps\BOE\WEB-INF\config\custom`:
   - Si en la carpeta se encuentra el fichero `AnalyticalReporting.properties`, abra el fichero en un editor de texto.
   - Si en la carpeta no existe un fichero llamado `AnalyticalReporting.properties`, cree un fichero con ese nombre y ábralo en un editor de texto.
2. Realice una de las siguientes acciones en el fichero `AnalyticalReporting.properties`:
   - Si el fichero ya existía, busque la propiedad `bex.dynamic_variable.schedule` en el fichero y compruebe que tiene el valor fijado en `true`.
   - Si usted ha creado el fichero `AnalyticalReporting.properties`, añada `bex.dynamic_variable.schedule=true` al final del fichero.
3. Grabe y cierre el fichero y, a continuación, reinicie el servidor de aplicaciones web.

## 18.7 Configurar los servicios Web RESTful de la plataforma de BI en el servidor Web.

Para personalizar la configuración para los servicios Web RESTful, siga los siguientes pasos:

1. Copie el archivo: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\default\biprws.properties` to `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps \biprws\WEB-INF\config\custom\biprws.properties` y a continuación ábralo para editarlo.
   Modifique los parámetros como sea necesario.

```
global properties | biprws.properties | hosts | biprws.properties
1  #-----------------------------------------------------Default CMS Configuration-----------------------------------------------------
2  CMS_Default=
3  #-----------------------------------------------------System Property Configuration-------------------------------------------------
4  Default_Number_Of_Objects_On_One_Page=
5  Enterprise_Session_Token_Timeout_In_Minutes=
6  Session_Pool_Size=
7  Session_Pool_Timeout_In_Minutes=
8  #-----------------------------------------------------Logger properties-------------------------------------------------------
9  LogLevel=
10 #-----------------------------------------------------Trusted Authentication Configuration------------------------------------------
11 Retrieving_Method=
12 User_Name_Parameter=
13 Trusted_Auth_Shared_Secret=
14 # ------------------------------------------------------ SSO Related Default Global Core Web Properties ------------------------------------------------------
15 # Vintela single sign on properties
16 sso.enabled=
17 idm.realm=
18 idm.princ=
19 idm.keytab=
20 idm.allowUnsecured=
21 idm.allowNTLM=
22 idm.logger.name=
23 idm.logger.props=
```

   A continuación hay una tabla donde se describen las propiedades según se muestra en la captura de pantalla.

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| `CMS_Default` | El usuario también puede proporcionar el nombre del CMS y su número de puerto, o el nombre del clúster.<br>Ejemplo:<br>`CMS_HOST_NAME:CMS_PORT_NUMBER`<br>O<br>`@CMS_CLUSTER_NAME` | 0 |
| `Default_Number_Of_Objects_On _One_Page` | El número de entradas que se mostrará por página. Puede sobrescribir esta configuración con el parámetro `&pageSize=<m>` en el SDK de servicios Web RESTful. | 50 |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| `Enterprise_Session_Token_Timeout_In_Minutes)` | La hora de vencimiento hasta la que un token de inicio de sesión será válido. Pasada esta hora, tiene que generar un nuevo token de inicio de sesión. | 60 |
| `Session_Pool_Size` | El número de sesiones de caché que se pueden almacenar en cualquier momento. El grupo de sesión copia en caché las sesiones del servicio Web RESTful activo. De este modo, se pueden volver a usar cuando un usuario envía otra solicitud que use el mismo token de inicio de sesión en el encabezado de la solicitud HTTP. | 1000 |
| `Session_Pool_Timeout_In_Minutes` | El tiempo en minutos en que caducarán las sesiones en caché. | 2 |
| `LogLevel` | Permite el registro y configura el nivel de gravedad y detalle en *Ninguno* (solo se registran los eventos críticos), *Bajo* (mensajes de solicitud de arranque, apagado, inicio y finalización), *Medio* (mensajes de error, advertencia y la mayoría de los mensajes de estado) o *Alto* (no se excluye nada). Se utiliza solamente para depurar. El uso de la CPU puede aumentar, repercutiendo en el rendimiento).<br><br>Las opciones de menú disponibles son:<br>• `Unspecified`<br>• `None`<br>• `Low`<br>• `Medium`<br>• `High` | No especificado |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| Log_Location | La ubicación del archivo de log que registre los logs de utilización del equipo donde se aloja la plataforma de BI.<br><br>**Nota**<br>• Se creará una nueva carpeta en caso de que se proporcione la ruta de archivo a una carpeta que no existe.<br>• La ubicación del archivo de log se fija como ubicación predeterminada si la ubicación no está especificada en el archivo biprws.properties. | No especificado |
| `Retrieving_Method` | El menú que establece qué método de consulta se utilizará para recuperar tokens de inicio de sesión con autenticación con confianza al utilizar el servicio web RESTful de API 107/iniciosesión/confianza.<br>• `HTTP_HEADER` se utiliza para consultas GET con el encabezado de solicitud aceptar=aplicación/xml (o aplicación/json).<br>• `QUERY_STRING` se utiliza para agregar un nombre de inicio de sesión al final de la consulta de la dirección URL mediante el servicio web RESTful de API, por ejemplo /iniciosesión/confianza/?usuario=johndoe.<br>• `COOKIE` se utiliza cuando el nombre de inicio de sesión se recupera desde una cookie del explorador web. El dominio, el nombre, el valor y la ruta se deben almacenar en la cookie | `HTTP_HEADER` |
| `User_Name_Parameter` | La etiqueta que se utiliza para identificar el usuario de confianza para recuperar el token de inicio de sesión. | `X-SAP-TRUSTEDUSER` |

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| `Trusted_Auth_Shared_Secret` | El valor de cadena generado al seguir los pasos mencionados en la sección Generación de un valor de secreto compartido [página 411]. | No especificado |
| `Basic_Auth_Supported` | Activa la autenticación básica en el servidor web Tomcat. Los valores posibles son `True` y `False`. | No especificado |
| `Basic_Auth_Type` | Fija la autenticación en `secEnterprise`, `secLDAP`, `secSAPR3` o `secWinAD` para admitir la autenticación básica. | `secEnterprise` |

2. Reinicie Tomcat.

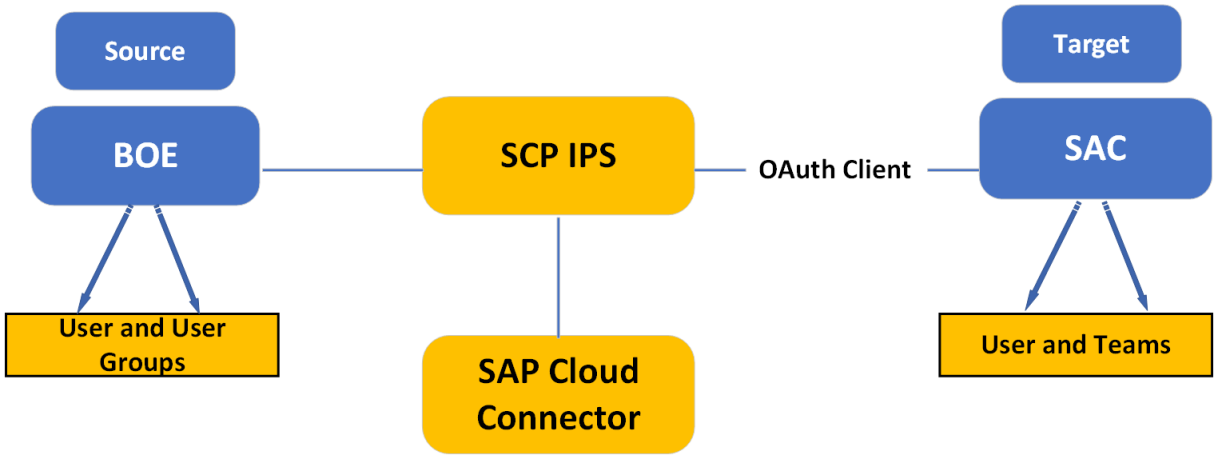
## 18.8 Gestión híbrida de usuarios

SAP se centra en la primera estrategia de nube, y los clientes también se mueven con mayor rapidez hacia soluciones híbridas en las que gestionan activos entre el entorno local y la nube. Es imprescindible que proporcionamos los servicios de la plataforma de BI de SAP BusinessObjects que lo permitan.

Esto se consigue exponiendo APIs de aprovisionamiento de usuarios (internos) basados en el sistema para la gestión de identidades entre dominios (SCIM), que pueden ser consumidos por SAP Cloud Platform Identity Provisioning Service (SCP IPS) para proporcionar a los usuarios empresariales de plataforma de BI otros sistemas de SCIM admitidos que utilicen Identity Provisioning Service (IPS) (especialmente SAP Analytics Cloud).

Con SCP IPS y la plataforma de BI SAP BusinessObjects 4.2 SP06 o superior, ahora los usuarios empresariales de la plataforma de BI pueden obtener cualquier sistema SCIM destino compatible.

La siguiente ilustración describe el escenario híbrido y cómo habilitar los servicios entre On-Premise y la nube.



## 18.9 Proporcionar SAP Analytics Cloud a los usuarios locales

Para proporcionar entidades (usuarios, grupos, roles) de un sistema a otro de su empresa, primero debe añadir y configurar estos sistemas como sistemas de origen y destino en la interfaz de usuario de Aprovisionamiento de identidades.

Puede proporcionar los usuarios del local (BOE) a SAP Analytics Cloud a través de SAP Cloud Platform Identity Provisioning Service (SCP IPS) en unos cuantos pasos sencillos.

1. Establecer conexión entre el sistema local y la nube
2. Crear credenciales de cliente de OAuth en SAP Analytics Cloud
3. Configurar el sistema fuente
4. Configurar el sistema de destino
5. Proporcionar SAP Analytics Cloud a sus usuarios y grupos de usuarios
6. Ver usuarios aprovisionados y grupos de usuarios

### 18.9.1 Establecer conexión entre el sistema local y la nube

Puede establecer una conexión entre el sistema local y la nube (Identity Provisioning System) mediante el conector SAP Cloud (sistema IPS).

El conector de la nube está instalado.

1. Inicie la página de administración del SAP Cloud Connector e inicie sesión en: `https://<HCC HOST>:8443`.

   > **Nota**
   >
   > Sustituya `<HCC HOST>` por el nombre de host del sistema en el que está instalado el conector de la nube.

2. 
3. En el panel de navegación, seleccione *Conector*, a continuación haga clic en el icono + (*Añadir subcuenta*).

   Aparece el diálogo *Añadir subcuenta*.
4. Introduzca la siguiente información para su cuenta IPS:

   > **Nota**
   >
   > Es necesario tener la autorización para *gestionar conexiones locales* para el usuario de la subcuenta en IPS. El *host de la región* y el *nombre de la subcuenta* se encuentran en la sección *Soporte - Información de la cuenta* en IPS.

   a. *Host de región*: Seleccione el host de su región de la lista.
   b. *Nombre de subcuenta*: Añada el nombre de su cuenta. Por ejemplo, dd00bb33.
   c. (Opcional) *Nombre de visualización*: Añada un nombre para la cuenta.
   d. *Usuario de subcuenta*: Añada su nombre de usuario de subcuenta (S-User).
   e. *Contraseña*: Añada su contraseña de S-User.

f. *ID de ubicación*: Deje en blanco para utilizar la ubicación por defecto.
g. (Opcional) *Descripción*: Añada una descripción para el conector de la nube.

5. Haga clic en *Guardar*.
6. En el panel de navegación, en *DisplayName*, seleccione *Cloud a On-Premise*.

   *DisplayName* es el nombre del arrendatario del conector de la nube.

7. En la ficha *Control de acceso*, haga clic en el icono + (Añadir).

   Aparece la ventana de diálogo *Editar asignación del sistema*.

8. Agregue la información de asignación del sistema solicitada para su sistema de la plataforma de BI, el servidor de aplicaciones Web (p. ej., Tomcat) alojando biprws:
   a. *Tipo de back end*: Seleccione Otro sistema SAP de la lista desplegable.
   b. *Protocolo*: Seleccione HTTP de la lista desplegable.
   c. (Opcional) *Host virtual*: El host virtual y la puerta estándar son el host y la puerta internos. Puede renombrar el host y la puerta para que el nombre de host y puerta internos no estén expuestos.
   d. (Opcional) *Puerta virtual*: Este es el número de puerta utilizado por el host virtual.
   e. *Host interno*: Este es el nombre de host para WAS (por ejemplo, Tomcat) que aloja Restful Web Service (biprws).
   f. *Puerta interna*: Número de puerta utilizado por el host interno. (Puerta en la que se despliegan los servicios Web de BIP RESTful; por ejemplo, biprws.)
   g. *SAProuter*: Deje este campo vacío.
   h. *Tipo principal*: Seleccione la opción Ninguno de la lista desplegable.
   i. *Nombre de socio SNC*: Deje este campo vacío.
   j. (Opcional) *Descripción*: Añada una descripción del sistema.
9. Marque la casilla de selección *Verificar host interno* y haga clic en *Guardar*.
10. Seleccione el sistema que ha añadido a la lista *Asignación virtual a sistema interno*.
11. En el área *Recursos accesibles* haga clic en el icono + (Añadir).

    Aparece la ventana diálogo *Agregar recurso*.

12. Añada la siguiente información de recurso para su cuenta:
    a. *Vía de acceso URL*: /biprws/sbop/internal/v2/scim.
    b. *Habilitado*: Asegúrese de que la casilla de selección esté marcada.
    c. *Política de acceso*: Seleccione el botón de selección *Vía de acceso y todas las subvías de acceso*.
    d. (Opcional) *Descripción*: Añada una descripción para el recurso.
13. Haga clic en *Guardar*.

> **Nota**
>
> El estado junto al host virtual debe aparecer en verde.

## 18.10 Crear credenciales de cliente OAuth en SAP Analytics Cloud

Para crear credenciales de cliente OAuth en SAP Analytics Cloud, siga los siguientes pasos:

1. Iniciar sesión en SAP Analytics Cloud.
2. En el menú principal, vaya a *Sistema > Administración > Integración de aplicación*.
3. Haga clic en *Cliente OAuth nuevo*.
4. Proporcione un nombre de su elección.
5. Seleccione *Acceso a API* como *Propósito*.
6. Seleccione *Aprovisionamiento de usuario* en Acceso.
7. Haga clic en *Agregar*.

   En esta lista de *Clientes configurados*, seleccione el cliente que acaba de añadir.

   > **Nota**
   >
   > Seleccione el icono ✎ (Editar) para ver el ID generado y la clave secreta de OAuthClient (contraseña). Estas credenciales son necesarias cuando se configura el sistema destino.
   >
   > El ID de cliente OAuth corresponde a su nombre de usuario en los detalles de configuración del sistema destino en SCP IPS, y el secreto se corresponde con su contraseña.

## 18.11 Configurar el sistema fuente

Debe configurar los detalles del sistema fuente de los que desea proporcionar usuarios y grupos de usuarios en SAP Cloud Platform Identity Provisioning Service (SCP IPS).

1. Inicie sesión en SCP IPS.
2. En la página de inicio, seleccione el mosaico *Sistemas fuente*.
3. Haga clic en el icono + (Añadir) situado en la parte inferior del panel izquierdo.
4. En el cuadro combinado *Tipo*, seleccione el tipo de sistema que desea utilizar.
5. Añada un nombre para su sistema. (Asegúrese de que no se haya duplicado el nombre de otro sistema).
6. (Opcional) Introduzca una descripción para su sistema para distinguirlo fácilmente en la lista más tarde.
7. Haga clic en *Guardar*.

   El nuevo sistema aparece en el panel de la izquierda.

   *Precaución*: Si no guarda el sistema en este punto, las propiedades y las transformaciones por defecto no aparecerán.
8. Haga clic en el icono ✎ (Editar) para ver las transformaciones y para añadir propiedades de configuración.
9. Agregue la siguiente información:
   a. *Autenticación*: BasicAuthentication.
   b. *Host*: <nombre de host y puerta BOE>.
   c. *ips.delta.read*: Habilitado:
   d. *ips.full.read.force.count*: 2.
   e. *ips.trace.faied.entity.content*: verdadero.
   f. *Contraseña*: <contraseña del usuario administrador BOE>.
   g. *Tipo de proxy*: OnPremise.

h. *scim.group.filter*: <ID de grupo de usuarios o CUID>.

   Por ejemplo, `scim.group.filter: groupId eq "4214"`.

i. *scim.user.filter*: <ID de usuario o CUID>.

   Por ejemplo, `scim.filter.filter: userId in "8077"` o `scim.user.filter: userCuid in "AQ.rQ1V1FR9JmQoQa0xYfII"`.

j. *Tipo*: HTTP.

k. *URL*: http://host name: port/biprws/sbop/internal/v2/scim.

l. *Usuario*: Administrador.

> **Nota**
>
> - Puede proporcionar los detalles del sistema local desde cero o importando un archivo existente con la información de configuración.
> - Puede definir determinadas restricciones o condiciones alrededor del sistema fuente mediante transformaciones.
> - Al seleccionar un destino de conectividad, debe ser compatible con el tipo de sistema relevante. El destino debe especificar todas las opciones de conexión necesarias para el escenario de aprovisionamiento de identidad.
> - El nombre de host/puerto especificado en el campo URL debe coincidir con el nombre/puerto de host virtual especificado en el conector de la nube.

10. Si omite el campo *Nombre de destino*, podrá abrir la ficha *Propiedades* para introducir todas las propiedades de conexión y configuración necesarias para su escenario de aprovisionamiento.
11. Puede modificar su transformación de sistema estándar (si es necesario).
12. Guarde los cambios.

> **Nota**
>
> Al final de la URL de aprovisionamiento de identidad, aparece una cadena separada por guiones. Este es el ID único generado automáticamente del sistema que se acaba de crear.

## 18.12 Configurar el sistema destino

Antes de empezar, asegúrese de haber creado las credenciales de cliente OAuth en SAP Analytics Cloud.

1. Haga clic en la ficha *Sistema destino* en la página de inicio.
2. En la ficha *Detalles* , introduzca el nombre del sistema SAP Analytics Cloud, la URL de SAP Analytics Cloud y el/los sistema(s) fuente.

   > **Nota**
   >
   > Los sistemas fuente que ya se han configurado aparecen aquí por defecto.

3. Haga clic en la ficha *Propiedades*.
4. Agregue la siguiente información:
   a. *Autenticación*: BasicAuthentication.

b. *csrf.token.path*: api/v1/scim/Users?count=1.
c. *ips.trace.failed.entity.content*: verdadero.
d. *OAuth2TokenService URL*: <OAuthClientTokenURL>.
e. *Contraseña*: <Secreto generado durante la configuración del cliente de OAuth>.
f. *Tipo proxy*: Internet.
g. *scim.api.csrf.protection*: enabled.
h. *Tipo*: HTTP.
i. *URL*: URL de SAP Analytics Cloud.
j. *Usuario*: <OAuth Client ID>.

## 18.13 Proporcionar SAP Analytics Cloud a sus usuarios y grupos de usuarios

Una vez que haya configurado los sistemas fuente y de destino mediante el servicio de provisión de identidad de SAP Cloud Platform, puede aprovisionarlos desde la ficha *Jobs* de la ventana *Detalles del sistema fuente*.

Los usuarios de la plataforma de BI que se aprovisionarán deben tener direcciones de correo electrónico configuradas.

1. Haga clic en el mosaico *Sistema fuente*.
2. Haga clic en *Jobs*.
3. En *Jobs* para el *Tipo de job*: *Leer job*, seleccione la acción *Ejecutar ahora*.

   > **Nota**
   >
   > Si ha modificado los usuarios o grupos de usuarios en BOE, seleccione *Volver a sincronizar tarea* para asegurarse de que los cambios se actualizan en SAP Analytics Cloud.

4. Para visualizar el progreso, seleccione *Logs de job* en el panel izquierdo y visualice el *Estado* de los jobs iniciados.
5. Para visualizar los detalles de la ejecución del job, haga clic en la fila correspondiente.

   Se abre la ventana *Detalles de ejecución de job* con el estado de las acciones.

## 18.14 Visualizar usuarios aprovisionados en SAP Analytics Cloud

1. Vaya al menú principal > *Seguridad* > *Equipos*.
2. Vaya a la página *Equipos*.
3. Seleccione su grupo de usuarios BOE.
4. Haga clic en *Miembros del equipo* para ver la lista de usuarios que se han aprovisionado de BOE a SAP Analytics Cloud.

> **Nota**
>
> También puede ver la lista de usuarios del menú *Usuarios* en *Seguridad*.

## 18.15 Plantillas de muestra

Puede utilizar las siguientes plantillas para aprovisionar un usuario o grupo(s) de usuarios.

**Configuración del sistema fuente de muestra**

```
{ "connectorTypeString": "SCIM", "accessMode": "READ",
"alias": "SBOP_10.47.228.194",
"relatedSystems": [
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SBOP_43",
"state": "ENABLED",
"transformation": {
"user": {
"condition": "($.memberOf contains '7741') || ($.memberOf contains '7962') ||
($.id contains '8077') || ($.id contains '8081')",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
{
"targetPath": "$.meta",
"type": "remove"
}
]
},
"group": {
"condition": "$.id contains '7741' || $.id contains '7962'",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
```

```
{
"targetPath": "$.meta",
"type": "remove"
}
]
}
},
"properties": {
"Type": "HTTP",
"User": "Administrator",
"ips.full.read.force.count": "2",
"Authentication": "BasicAuthentication",
"host": "adept6991435:6400",
"scim.group.filter": "groupId eq \"7741,7962\" or groupCuid eq
\"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ\"",
"ProxyType": "OnPremise",
"ips.delta.read": "enabled",
"ips.trace.failed.entity.content": "true",
"URL": "http://adept6991435:6405/biprws/sbop/internal/v2/scim",
"Password": "Password1",
"scim.user.filter": "groupId eq \"7741\" and groupCuid eq
\"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ\" and userId in \"8077\" or
userCuid in \"AQ.rQ1V1FR9JmQoQa0xYfII\""
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```


### Transformación de muestra


```
{
"connectorTypeString": "SAP_ANALYTICS_CLOUD",
"accessMode": "WRITE",
"destinationName": " ",
"alias": "https://idcsac.jp1.sapanalytics.cloud",
"relatedSystems": [
"SBOP_43"
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SAC-Machine",
"state": "ENABLED",
"transformation": {
"user": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"sourceVariable": "entityIdTargetSystem",
"targetPath": "$.id"
},
{
"sourcePath": "$.userName",
"targetPath": "$.userName"
},
{
"sourcePath": "$.name",
"targetPath": "$.name"
```

```
},
{
"sourcePath": "$.displayName",
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.active",
"optional": true,
"targetPath": "$.active"
},
{
"sourcePath": "$.emails",
"preserveArrayWithSingleElement": true,
"targetPath": "$.emails"
},
{
"condition": "$.emails[0].length() > 0",
"constant": true,
"targetPath": "$.emails[0].primary"
},
{
"constant": [
"PROFILE:sap.epm:BI_Admin"
],
"preserveArrayWithSingleElement": true,
"targetPath": "$.roles"
},
{
"sourcePath": "$.groups",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.groups"
},
{
"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
"optional": true,
"targetPath": "$['urn:scim:schemas:extension:enterprise:1.0']['manager']
['managerId']",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
},
"group": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"condition": "$.displayName EMPTY false",
"sourcePath": "$.displayName",
"targetPath": "$.id"
},
{
"condition": "$.id EMPTY false",
"sourcePath": "$.id",
"targetPath": "$.id"
},
{
"sourcePath": "$.displayName",
```

```
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.roles",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.roles"
},
{
"sourcePath": "$.members[*].value",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.members[?(@.value)]",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
}
}
},
"properties": {
"Type": "HTTP",
"User": "<exampleusername>",
"Authentication": "BasicAuthentication",
"OAuth2TokenServiceURL": "https://oauthasservices-
gf097393f.jp1.hana.ondemand.com/oauth2/api/v1/token",
"csrf.token.path": "/api/v1/scim/Users?count=1",
"ProxyType": "Internet",
"ips.trace.failed.entity.content": "true",
"URL": "https://idcsac.jp1.sapanalytics.cloud",
"scim.api.csrf.protection": "enabled",
"Password": "<examplepassword>"
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```

# 19 Administrar conexiones y universos

## 19.1 Administrar conexiones

Una conexión es un conjunto con nombre de parámetros que define cómo una o más aplicaciones de SAP BusinessObjects pueden acceder a las bases de datos OLAP o relacionales. Los detalles de las conexiones, como el nombre del servidor, la base de datos, el nombre de usuario y la contraseña, se pueden almacenar con seguridad en el repositorio de la plataforma de BI en la carpeta Conexiones.

Los diseñadores definen los universos en función de las conexiones. Los usuarios de las aplicaciones de consulta, análisis y generación de informes acceden a la base de datos mediante el universo sin necesidad de conocer las estructuras de datos subyacentes en la base de datos.

Puede crear conexiones con las siguientes aplicaciones:

- La herramienta de diseño de universos: las conexiones se almacenan en el repositorio.
- La herramienta de diseño de información: las conexiones pueden crearse localmente y después publicarse en el repositorio o crearse y editarse directamente en el repositorio.

> ⓘ Nota
>
> Para obtener información sobre cómo administrar las conexiones de orígenes de datos OLAP, consulte el *SAP BusinessObjects Analysis, edition for OLAP Administrator Guide* (Manual del administrador de SAP BusinessObjects Analysis, edición para OLAP).

Puede otorgar derechos para que los usuarios puedan crear, editar y eliminar conexiones.

Puede conceder acceso a las conexiones de universo a los usuarios y permitirles crear y ver documentos que usan universos y conexiones.

### Información relacionada

Administración de la configuración de seguridad para los objetos en la CMC [página 136]
Derechos de conexión [página 1153]

## 19.1.1 Para eliminar una conexión de universo

> → Sugerencias
>
> También se pueden eliminar las conexiones en la herramienta de diseño de universos y en la herramienta de diseño de información.

1. En el área *Conexiones*, seleccione una conexión de universo en la lista.
2. Haga clic en *Administrar* > *Eliminar*.

## 19.2 Administrar universos

Un universo es un conjunto de objetos de metadatos organizados que permiten a los usuarios de negocios analizar los datos corporativos en un lenguaje no técnico y después informar sobre ellos. Estos objetos incluyen dimensiones, indicadores, jerarquías, atributos, cálculos predefinidos, funciones y consultas. La capa de objetos de metadatos se crea en un esquema de base de datos relacional o un cubo de OLAP, de forma que los objetos se asignan directamente a las estructuras de la base de datos. Un universo incluye conexiones a orígenes de datos de forma que los usuarios de las herramientas de consulta y análisis puedan conectarse a un universo y ejecutar consultas y crear informes usando los objetos de un universo sin tener que conocer las estructuras de datos subyacentes en la base de datos.

Se pueden crear universos con las herramientas siguientes:

- La herramienta de diseño de universos. Los universos que se crean con esta herramienta se distinguen por la extensión .unv y, por consiguiente, se denominan universos .unv. Los universos .unv se definen en una conexión segura y se almacenan en la carpeta Universos del repositorio.
- La herramienta de diseño de información. Los universos creados con esta herramienta se basan en la nueva capa semántica. Se distinguen por la extensión .unx y, en consecuencia, se denominan universos .unx. Los universos .unx se crean localmente y se publican en la carpeta Universos del repositorio. Los diseñadores pueden definir la seguridad del sistema mediante el editor de seguridad de la herramienta de diseño de información.

Puede otorgar a los usuarios derechos de aplicación y derechos de universos para que puedan crear, editar y eliminar universos, así como diseñar la seguridad sobre los universos.

Puede otorgar derechos de universo a los usuarios para que puedan crear y ver documentos que usan documentos.

### Información relacionada

Administración de la configuración de seguridad para los objetos en la CMC [página 136]
Herramienta de diseño de universos [página 1158]
Derechos de universo (.unv) [página 1149]
Herramienta de diseño de información [página 1159]
Derechos de universos (.unx) [página 1150]

## 19.2.1 Para eliminar universos

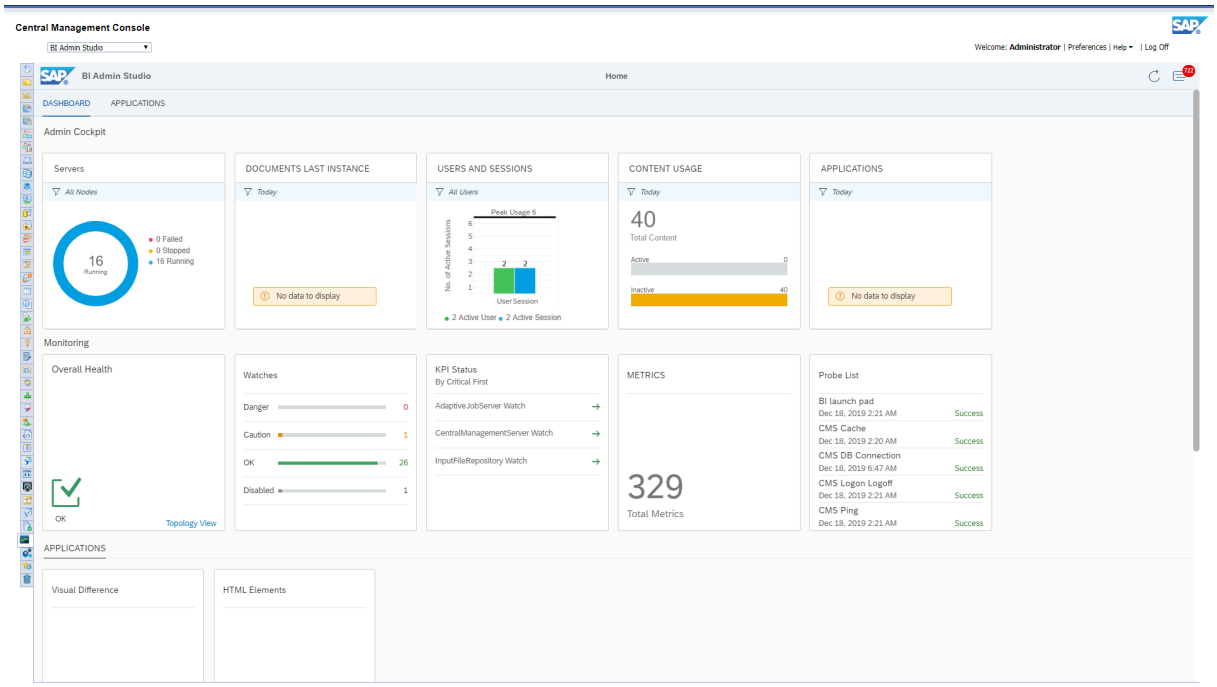
> → Sugerencias
>
> También se pueden eliminar universos en la herramienta de diseño de información.

1. En el área *Universos* de la CMC, seleccione un universo en la lista.
2. Haga clic en *Administrar* > *Eliminar*.
3. Cuando se le pida confirmación, haga clic en *Aceptar*.

# 20 BI Admin Studio

BI Admin Studio es una aplicación en la CMC que combina Supervisión, Alertas y Cockpit de administración, antes conocido como Cockpit del administrador de BI.

La aplicación consta de dos fichas *Cuadro de mandos empresarial* y *Aplicaciones*.




## Cuadro de mandos empresarial

La ficha *Cuadro de mandos empresarial* proporciona una vista única de los cuadro de mandos empresariales disponibles en *Cockpit de administración* y *Supervisión*. Puede hacer clic en cada cuadro de mandos empresarial para obtener información detallada sobre el mismo. Por ejemplo, puede seleccionar el cuadro de mandos empresarial *Servidores* para obtener la lista de servidores que tienen los *Estados* como *En ejecución*, *Detenido*y *Error*, junto con sus detalles como *Nombre de servidor*, *PID*y *Tipo*. Para obtener más información sobre el cockpit de administración, consulte Cockpit de administración [página 807] y para averiguar más sobre Supervisión, consulte Supervisión [página 811].

### Aplicaciones

Puede acceder *Diferencia visual* y *Elementos HTML autorizados* desde la ficha *Aplicaciones*. Para obtener más información sobre la *Diferencia visual*, consulte Diferencia visual [página 835] y para averiguar más sobre los *Elementos HTML*, consulte Autorización de elementos HTML [página 838].

### Alertas

Puede seleccionar para acceder al panel de notificaciones para alertas. Desde el panel de notificaciones, puede seleccionar la opción *A la página de alertas* para saber más sobre las alertas que ha creado.

## 20.1 Cockpit de administración

El cockpit de administración es una aplicación nueva que se ha añadido al CMC. Permite al administrador recopilar datos básicos acerca del entorno BI. Supone derivar Business Intelligence de los datos de su entorno Business Intelligence. Con el cockpit de administración puede obtener información de servidores, tareas programadas, usuarios y sesiones, utilización del contenido y aplicaciones.

> **Nota**
>
> Los siguientes requisitos son necesarios para asegurar que el cockpit de administración pueda utilizarse correctamente.
>
> - Monitoring Service debe estar activado.
> - La auditoría y el evento relevante deben estar activados, de modo que se tomen los datos correctos.
> - El servicio web RESTful de la plataforma BI debe ser accesible a los clientes.
> - WACS debe estar en ejecución, a no ser que el servicio Web RESTful esté desplegado en Tomcat.
> - Si configura SSL para la CMC, asegúrese de configurar también SSL para WACS, a menos que el servicio Web RESTful se implemente en Tomcat.
> - Debe estar activado el acceso a dominios cruzados.
> - Los usuarios deben pertenecer al grupo Administradores o a cualquier subgrupo del mismo para acceder al cockpit de administración.

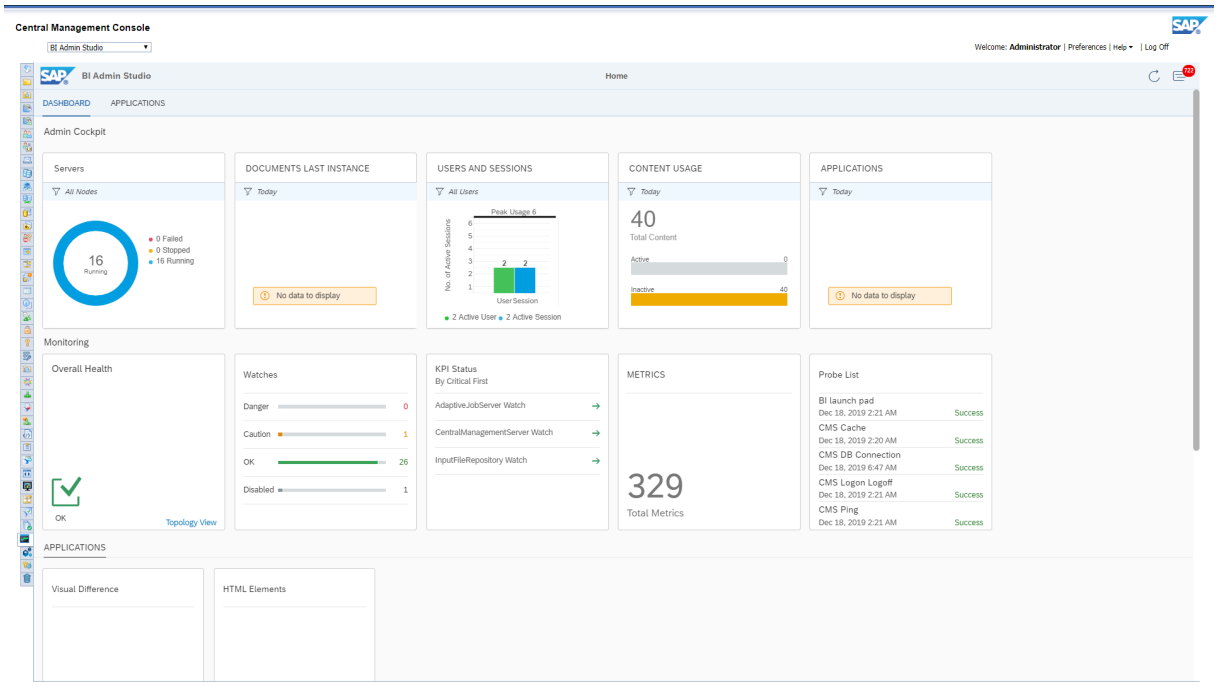
### 20.1.1 Cockpit de administración

El cockpit de administración ofrece un análisis completo de los datos relacionados con los siguientes componentes en una visualización gráfica:

- Servidores

- Última instancia de documento
- Usuarios y sesiones
- Utilización del contenido
- Aplicación

> **Nota**
>
> La base de datos de auditoría debe estar habilitada para ver el análisis en *Utilización del contenido* y *Aplicación*.




Puede actualizar los datos que aparecen en cada página del cockpit de administración haciendo clic en en la esquina superior derecha de la página de inicio.

## 20.1.2 BI en servidores

El cockpit de administración le ayuda a obtener datos en tiempo real sobre el estado y datos relacionados de todos los servidores de su entorno BI.

La página de inicio le proporciona los siguientes detalles:

- Número total de servidores
- Número de servidores con errores
- Número de servidores parados

Puede filtrar los datos que aparecen en la cascada *Servidores* seleccionando el clúster de servidores deseado.

Al hacer clic en el mosaico *Servidores* , se le dirige a una página de servidores que tiene los detalles del número total de servidores, de servidores que producen errores y de servidores detenidos. Los servidores también proporcionan el *estado*, *nombre del servidor*, *PID* (identificador de proceso), *tipo*, *estado* y *hora de última modificación* para cada servidor que produce errores.

Dentro de la página *Servidores* puede filtrar datos según clústeres de servidores específicos seleccionado el clúster de servidores específico.

Puede ver más detalles sobre el servidor que produce errores seleccionando la fila correspondiente. Ello le dirige a una nueva página que detalla el motivo del error Puede reiniciar el servidor que produce errores desde dentro de la página, seleccionando *INICIAR*.

## 20.1.3 BI en instancias de documento

Puede utilizar el cockpit de administración para obtener datos acerca del estado y los detalles relacionados de todas las instancias de documentos programados en su entorno BI.

La página inicial proporciona la información siguiente:

- Cantidad total de la última instancia de cada documento programado.
- Cantidad de la última instancia en ejecución de cada documento programado.
- Cantidad de las últimas instancias que producen errores de cada documento programado.
- Cantidad de las últimas instancias pendientes de cada documento programado.

En el mosaico *Última instancia de documentos* puede filtrar datos de un intervalo de tiempo específico seleccionando el intervalo de tiempo deseado del menú desplegable. Los intervalos de tiempo disponibles son:

- Hoy
- Últimos 7 días
- Últimos 30 días
- Trimestre
- Año

Al hacer clic en el mosaico *Última instancia del documento*, se le dirige a la página Últimas instancias que contiene los detalles de la cantidad total de la última instancia de cada documento programado desglosadas por estado: En ejecución, error y pendiente. La etiqueta *Estadísticas* proporciona los detalles que puede ver en las secciones *Documentos con la mayoría de instancias* e *Instancias con el tiempo de ejecución más prolongado*. La página de Instancias de documento también le proporciona el *Nombre de la instancia*, *Estado*, *Tipo*, *Propietario* y *Hora de fin* da cada estado de error.

Puede exportar los datos vistos en la página *Últimas instancias* como fichero .CSV haciendo clic en el botón de enlace de exportación. También puede exportar exportar instancias seleccionadas eligiendo la casilla de selección correspondiente y luego *Exportación seleccionada* de la lista desplegable de exportación.

Puede ver más detalles sobre la instancia que produce errores seleccionando la fila correspondiente. Puede reiniciar el job desde la página, seleccionando *EJECUTAR*.

En la etiqueta de estadísticas, hay habilitado un nuevo filtro de gráfico que permite filtrar y visualizar los principales documentos 5, 10, 15 y 20.

## 20.1.4 BI en usuarios y sesiones

El cockpit de administración le ayuda a obtener datos acerca de usuarios y sesiones en su entorno BI.

Por ejemplo, la página de inicio le proporciona los siguientes detalles:

- Número de usuarios activos
- Número de sesiones activas

En el mosaico *Usuarios y sesiones* puede filtran los datos para:

- Todos los usuarios
- Usuarios con nombre
- Usuarios simultáneos

Al hacer clic en el mosaico *Usuarios y sesiones* se le dirige a la página Usuarios y sesiones que tiene los detalles de todos los usuarios, usuarios principales y estadísticas. La etiqueta Estadísticas proporciona detalles relacionados con los usuarios más activos y los usuarios más inactivos.

La página Usuarios y sesiones también proporciona el *nombre de usuario*, *sesiones totales*, *último inicio de sesión*y *sesión de ejecución más larga*.

Puede ver más detalles sobre un usuario en concreto seleccionando la fila correspondiente. Ello le dirige a una nueva página que detalla las principales sesiones de ese usuario. Puede finalizar cualquier sesión de un usuario en particular desde la página seleccionando la sesión deseada y eligiendo *FINALIZAR SESIÓN*.

## 20.1.5 BI en Utilización del contenido

El cockpit de administración le ayuda a obtener datos acerca de la utilización de contenido en su entorno BI.

Por ejemplo, la página de inicio le proporciona los siguientes detalles:

- Número de documentos activos
- Número de documentos inactivos

En el mosaico *Utilización de contenido* puede filtrar datos de un intervalo de tiempo específico seleccionando el intervalo de tiempo deseado del menú desplegable.

> **Nota**
>
> Si ha borrado algún contenido activo y datos de filtro para un período específico, la posición borrada todavía aparece listada en contenido activo, si es que estaba activa durante el período seleccionado.

Los intervalos de tiempo disponibles son:

- Hoy
- Últimos 7 días
- Últimos 30 días
- Trimestre
- Año

Al hacer clic en el mosaico *Utilización del contenido* se le dirige a una página de Utilización del contenido que tiene los detalles de Contenido activo, Contenido inactivo y Estadísticas. La etiqueta Estadísticas le

proporciona detalles relacionados con Bandejas de entrada con más Contenido inactivo, Universos son más contenido y Carpetas con más contenido.

Puede exportar los datos vistos en la página *Utilización del contenido* en un fichero csv seleccionando el botón de enlace de exportación. También puede seleccionar exportar las tareas seleccionadas eligiendo la casilla de selección correspondiente *Exportación seleccionada* del desplegable de exportación.

La página de Utilización del contenido también le proporciona el *Nombre del contenido*, *Tipo*y *Tiempo de ejecución*.

En la etiqueta de estadísticas, hay habilitado un nuevo filtro de gráfico que permite filtrar y visualizar los principales documentos 5, 10, 15 y 20.

### 20.1.6 BI en aplicaciones

El cockpit de administración le proporciona datos sobre el número de aplicaciones, ordenadas por el nombre de aplicación en su entorno BI.

En el mosaico *Aplicación* pude filtrar datos de un intervalo de tiempo específico seleccionando el intervalo de tiempo deseado del menú desplegable. Los intervalos de tiempo disponibles son:

- Hoy
- Últimos 7 días
- Últimos 30 días
- Trimestre
- Año

Al hacer clic en el mosaico *Aplicaciones* se le dirige a una página de Aplicaciones que tiene los detalles relacionados con *Todas las aplicaciones* y *Aplicaciones principales*.

La etiqueta *Aplicaciones principales* muestra una lista de las 5 aplicaciones principales, con el mayor número de documentos creados en el intervalo de tiempo seleccionado. La página Aplicaciones también le proporciona el *Nombre de aplicación*, *Número de usuarios* y *Número de artefactos*.

## 20.2 Supervisión

La aplicación de supervisión proporciona la capacidad de capturar métricas históricas y de tiempo de ejecución de los servidores de la plataforma de BI para la generación de informes y notificaciones. La aplicación de supervisión ayuda a los administradores del sistema a identificar si una aplicación funciona de forma normal y si los tiempos de respuesta son los esperados. Al proporcionar métricas empresariales clave, la aplicación de supervisión proporciona una mejor perspectiva de la plataforma de BI.

La supervisión le permite llevar a cabo las tareas siguientes:

- Comprobar el rendimiento de cada servidor: Esto es posible con la ayuda de vigilancias, que muestran el estado de cada servidor como semáforos. El administrador del sistema puede definir umbrales para las vigilancias, recibir alertas cuando se crucen los umbrales y ayudar a emprender acciones en caso de fallo o corte de suministro.

- Ver indicadores de rendimiento claves (KPI) críticos del sistema: esto ayuda en una supervisión de actividad y recurso. Estos KPI se muestran en la página de cuadro de mandos de la aplicación de supervisión.
- Visualice el despliegue completo de la plataforma de BI (tanto en formato gráfico como de tabla) en función de los grupos de servidores, las categorías de servicio y los nodos de Enterprise.
- Visualice los errores recientes en la pantalla del cuadro de mandos.
- Compruebe la disponibilidad del sistema y el tiempo de respuesta: Con el uso de métricas, se pueden simular flujos de trabajo para comprobar si los servidores y servicios del despliegue de la plataforma de BI funcionan como se ha previsto. Al analizar el tiempo de circuito de estas medidas en intervalos periódicos, el administrador del sistema puede evaluar el patrón de uso del sistema.
- Analizar la carga y el período máximo para el CMS: Esto ayuda al administrador del sistema a determinar si se requieren más licencias o recursos del sistema.
- Integración con otras aplicaciones empresariales: La aplicación de supervisión de la plataforma de BI se puede integrar con otras aplicaciones empresariales, como SAP Solution Manager e IBM Tivoli Monitoring.
- Realice un seguimiento del valor de métrica del *nivel de auditoría* en el *Servidor de administración central* cuando *Fijar eventos* esté seleccionado como *Desactivado* (valor de métrica 1). Aquí se puede crear una lista de seguimiento. Cuando el valor de métrica es 1, se envía una alerta de prueba en la lista de seguimiento junto con una alerta de correo electrónico.

Para más información sobre la manera de utilizar la aplicación de supervisión, incluidos los detalles sobre métricas y vigilancias, consulte la *Ayuda en línea de la CMC de la plataforma de SAP BusinessObjects Business Intelligence*.

### Información relacionada

Acerca del apéndice de métrica de servidor [página 1199]

## 20.2.1 Términos de supervisión

En la siguiente lista se proporcionan los términos que se relacionan con la aplicación de supervisión:

### Tendencia

Registrar o mostrar datos históricos para buscar tendencias.

### Cuadro de mandos

La página Cuadro de mandos proporciona una vista centralizada del administrador del sistema para supervisar el rendimiento de todos los servidores. Proporciona información en tiempo real de los KPI del sistema, las alertas recientes, las vigilancias y los gráficos correspondientes basados en los estados de vigilancia.

## Vigilancia

Las vigilancias proporcionan el estado en tiempo real y la tendencia histórica de los servidores y los flujos de trabajo en el entorno de la plataforma de BI. Los usuarios pueden asociar umbrales y alertas con vigilancias. Puede crear una vigilancia usando datos de pruebas, servidores, SAPOSCOL o métricas derivadas.

## Métrica derivada

Las métricas derivadas son métricas que crea al combinar dos o más métricas existentes en una ecuación matemática. Puede crear una métrica según los requisitos del usuario y, a continuación, crear una supervisión utilizando esta métrica.

## Métrica topológica

Las métricas topológicas le proporcionan el estado neto de cada categoría de servicio en la plataforma de BI. Por ejemplo, el servicio de Crystal Reports ofrece el estado combinado de todas las vigilancias relacionadas con los servidores de Crystal Reports.

## Estado

Estos son los valores del estado:

- "0": Indica que la métrica está en mal estado.
- "1": Indica que el estado de la métrica se está deteriorando y que necesita atención inmediata.
- "2": Indica que la métrica está en buen estado.

## KPI

Los KPI (indicadores de rendimiento clave) son métricas estándar de la plataforma de BI. Proporcionan información sobre programaciones y sesiones de inicio de sesión. Por ejemplo, un número más lato de *RunningJobs* indica un buen rendimiento en los servidores. Además, un número más elevado de *PendingJobs* indica un rendimiento bajo y una carga del sistema elevada.

## Medida

Las métricas supervisan los distintos servicios y simulan las distintas funcionalidades de los componentes de los componentes de la plataforma de BI. Al programar métricas para que se ejecuten en intervalos

determinados, el administrador del sistema puede realizar el seguimiento de la disponibilidad y el rendimiento de los servicios clave que proporciona la plataforma de BI. Asimismo, estos datos pueden usarse para planificar la capacidad del sistema.

### Semáforo

Un semáforo es un icono que muestra el color verde, ámbar, o rojo para indicar el estado de una vigilancia en un momento en concreto. Los usuarios pueden seleccionar configurar dos o tres estados para una vigilancia.

### Gráfico de tendencias

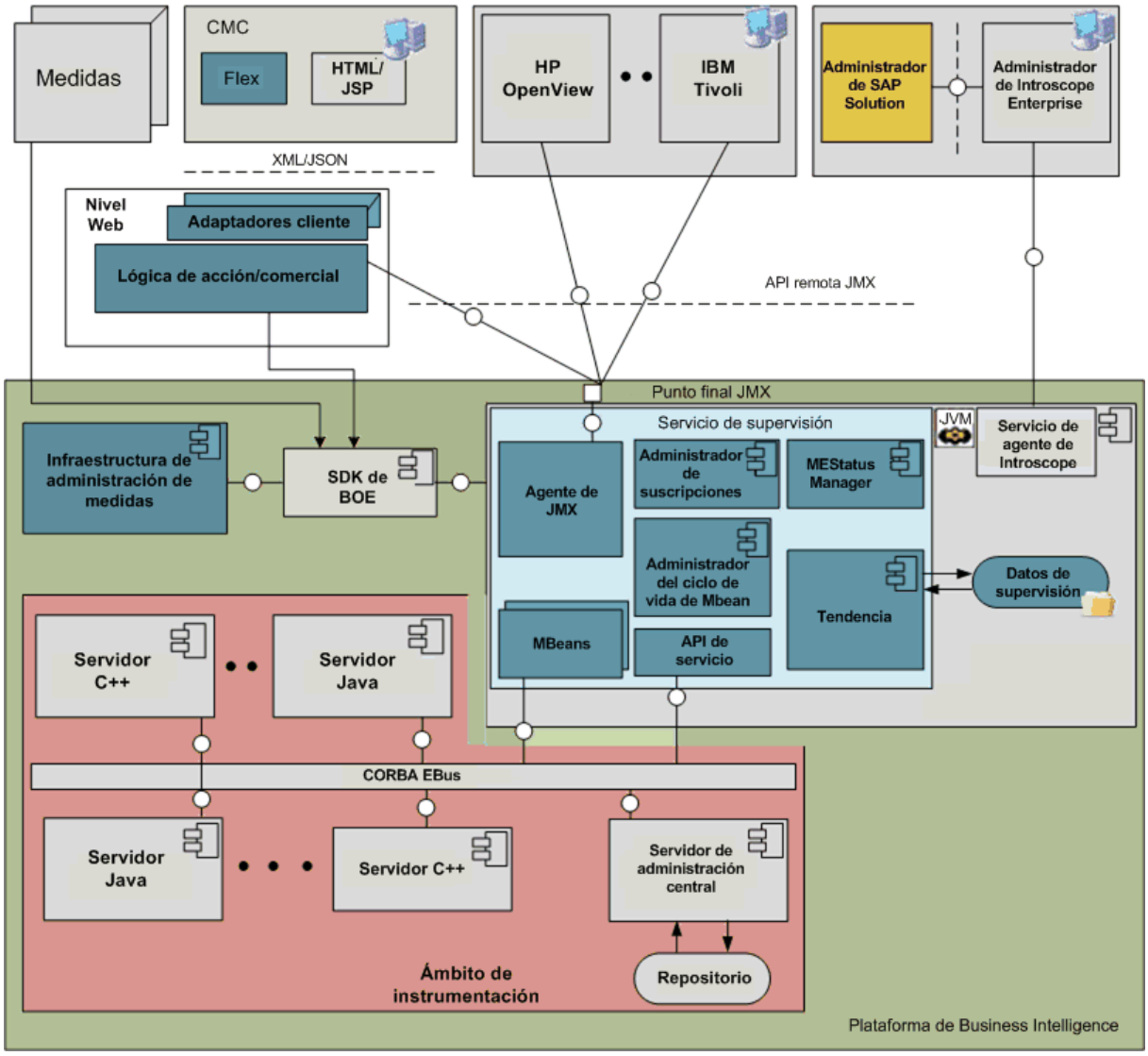
Un gráfico de tendencias es una representación gráfica de los datos de medidas históricos generados por las medidas y los servidores. Ayuda a los administradores del sistema a supervisar el sistema en distintos intervalos de tiempo, y evalúa el patrón de uso del sistema.

### Alerta

Una alerta es una notificación generada por la aplicación de supervisión, cuando se infringe un valor de umbral definido por el usuario para las diferentes medidas aplicadas a una vigilancia. Puede optar por recibir las alertas por correo electrónico o bien verlas en la página *Cuadro de mandos*.

## 20.2.1.1 Arquitectura

En esta sección se proporciona información general de nivel elevado de la arquitectura de supervisión y se explica brevemente las funciones de los componentes. A continuación se representa gráficamente la arquitectura de supervisión:




A continuación se enumeran los componentes de alto nivel de la arquitectura:

- Servidor de procesamiento de Adaptive (APS)
- Servidor/agente de extensiones de administración Java (JMX)
- MBeans
- Clientes JMX
- Consolas de administración
- Base de datos de tendencias

El servicio de supervisión se aloja en un servidor de procesamiento de Adaptive. La aplicación se basa en la tecnología JMX.

El servicio de supervisión proporciona los principales servicios disponibles en la aplicación de supervisión. El servicio de supervisión proporciona los siguientes servicios:

- Proporciona el servicio de agente JMX.
- Crea dinámicamente MBeans para los servidores SAP BusinessObjects.

- Proporciona Lifecycle Management para los MBeans.
- Proporciona un mecanismo para registrar medidas nuevas.
- Permite a los usuarios crear condiciones de umbral complejas usando las medidas de los servidores.
- Proporciona un mecanismo de notificación de umbrales y envía alertas.
- Almacena datos históricos.

El Servicio de programación de métrica que se aloja en el Servidor de tareas de Adaptive administra la ejecución y programación de métricas. Por consiguiente, el Servidor de tareas de Adaptive debe ejecutarse para que la métrica se ejecute.

La aplicación de supervisión expone un punto final de URL JMX o RMI (Invocación de método remoto). Otras aplicaciones como SAP Solution Manager e IBM Tivoli Monitoring pueden conectarse a la aplicación de supervisión y acceder a las métricas de la plataforma de BI mediante una API remota de JMX. La aplicación de supervisión utiliza la base de datos Memoria de datos de auditoría (ADS) para almacenar datos históricos para la elaboración de tendencias. Si desea obtener más información sobre el esquema de la base de datos, consulte Esquema de base de datos de tendencias [página 1235].

## 20.2.2 Configurar la compatibilidad de la base de datos para la supervisión

En esta sección se describe cómo configurar la supervisión, y generar un informe sobre los datos de supervisión.

> **Nota**
>
> Solo las supervisiones con la opción *Guardar en base de datos de tendencias* seleccionada escriben información de seguimiento en la base de datos de tendencias.

Hay dos opciones de base de datos para registrar información de supervisión: información de registro mediante el Almacén de datos de auditoría (ADS), o cualquier otra base de datos compatible con la plataforma mediante el controlador JDBC.

> **Nota**
>
> La base de datos Apache Derby es obsoleta en la versión de BI 4.3. Para más información sobre datos de migración y copias de seguridad, consulte 2912759.

Puede utilizar el almacén de datos de auditoría (ADS) predeterminado, a menudo conocido como la base de datos de auditoría. Esta es la base de datos relacional en la que el CMS almacena datos de auditoría. Puede usar el ADS incluido con la plataforma de BI, o cualquier otra base de datos admitida que haya configurado como base de datos de auditoría.

Otras bases de datos admitidas son:

- DB2
- SQL Server
- My SQL
- Oracle
- Base de datos SAP HANA

- SQL Anywhere
- Sybase

El uso de la base de datos de auditoría permite que los usuarios generen informes a partir de los datos de auditoría junto con la información de supervisión. La captura de datos en una base de datos relacional proporciona una capacidad de recuperación y copia de seguridad, y la disponibilidad en tiempo real de los datos.

### Información relacionada

Configuración para usar la base de datos de auditoría [página 817]

## 20.2.2.1 Configuración para usar la base de datos de auditoría

Si desea usar la base de datos de auditoría para sus datos de supervisión, tendrá que llevar a cabo los siguientes pasos de configuración adicionales:

- Antes de BI 4.3, si tenía datos existentes en la base de datos Derby de tendencias, tendrá que migrar la base de datos Derby a la base de datos de auditoría y, a continuación, configurar la plataforma de BI para registrar información de supervisión en la base de datos de auditoría. Estos son los pasos de alto nivel que debe seguir. Para obtener más detalles, consulte los temas relacionados.
  1. Migrar la base de datos Derby.
  2. Configurar los archivos SBO y agregar nombres de alias.
  3. Cambiar a la base de datos de auditoría.
  4. Reinicie el servidor de procesamiento de Adaptive que aloja el servicio de supervisión.
  5. En el cuadro de mandos de supervisión, asegúrese de que todo funciona correctamente. Verifique que estas tablas de supervisión se han creado en la base de datos:

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA
     MOT_TREND_DETAILS
- Si no tiene datos en la base de datos de tendencias, es decir, si tiene una instalación nueva, no tiene que migrar la base de datos; solo tiene que configurar la plataforma de BI para registrar información de supervisión en la base de datos de auditoría. Estos son los pasos de alto nivel que debe seguir. Para obtener más detalles, consulte los temas relacionados.
  1. Verifique que la base de datos de auditoría esté en funcionamiento, y que la auditoría funcione correctamente.
  2. Crear tablas de supervisión en el ADS.
  3. Configurar los archivos SBO y agregar nombres de alias.
  4. Cambiar a la base de datos de auditoría.
  5. Reinicie el servidor de procesamiento de Adaptive que aloja el servicio de supervisión.
  6. En el cuadro de mandos de supervisión, asegúrese de que todo funciona correctamente. Verifique que estas tablas de supervisión se han creado en la base de datos:

MOT_MES_DETAILS
MOT_MES_METRICS
MOT_TREND_DATA
MOT_TREND_DETAILS

> **Nota**
>
> Si registra datos de supervisión en la base de datos de auditoría, y desea generar informes a partir de estos datos, tendrá que desarrollar un universo personalizado.

### Información relacionada

Configurar archivos SBO [página 819]
Adición del nombre del alias en el archivo SBO [página 822]
Cambiar a la base de datos de auditoría. [página 822]
Crear tablas de supervisión en el ADS [página 818]

## 20.2.2.1.1 Crear tablas de supervisión en el ADS

Siga estos pasos para preparar la base de datos de auditoría de destino:

1. Después de instalar la `plataforma de BI`, los DDL relacionados con todas las bases de datos de auditoría del CMS admitidas están disponibles en la ubicación <Dir Instalación>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB. Encontrará siete archivos distintos (extensión .sql) con el respectivo nombre de base de datos. Por ejemplo: `Oracle.sql` para Oracle, `Sybase ASE.sql` para Sybase ASE Database, etc.
2. Vaya a la base de datos de destino (en este caso la base de datos de destino es la base de datos en la que se ha configurado la auditoría del CMS) y ejecute el archivo .sql. Se crean las cuatro tablas de supervisión siguientes: `MOT_TREND_DETAILS`, `MOT_TREND_DATA`, `MOT_MES_DETAILS` y `MOT_MES_METRICS`. Los índices necesarios también se crean junto con las tablas.

Si todas las tablas se crean con los tipos de datos correctos que se mencionan en el archivo .sql, se crea el esquema de base de datos necesario para la aplicación de supervisión.

## 20.2.2.1.2 Para restaurar contenidos en la base de datos de destino

Es necesario realizar los pasos siguientes para restaurar el contenido de la base de datos de destino:

1. Habilitar la inserción de identidad.

   Las tablas de supervisión contienen varias columnas IDENTITY. Se trata de columnas que generan sus valores de forma automática. Algunas bases de datos (por ejemplo, MS SQL Server y Sybase ASE) no permiten la inserción explícita de valores en dichas columnas. Durante la migración de datos, sin embargo,

también se deben migrar los valores de la columna Identity. Por este motivo, los usuarios deben habilitar la inserción explícita de estos valores mediante el siguiente comando de SQL: `SET IDENTITY_INSERT <NOMBRE DE TABLA> ON`.

2. Importar el archivo de volcado CSV en la tabla de destino

   Todo el software que proporcionan los clientes de la base de datos permite a los usuarios importar los datos de CSV a la tabla mediante una opción de menú o un comando. El usuario debe usar esta opción para importar los datos del archivo CSV a la tabla correspondiente. Importar los archivos de datos en tablas nuevas en el orden siguiente:

   1. `MOT_TREND_DETAILS`
   2. `MOT_TREND_DATA`
   3. `MOT_MES_DETAILS`
   4. `MOT_MES_METRICS`

3. Deshabilitar la inserción de identidad.

   Una vez importados los datos, el usuario debe deshabilitar la inserción de identidad en la tabla mediante el siguiente comando de SQL:`SET IDENTITY_INSERT <NOMBRE DE TABLA> OFF`

   Los usuarios deben deshabilitar la inserción de identidad en una tabla tras la importación de datos para habilitar la inserción de identidad en la tabla siguiente. Esto sucede porque solo se puede habilitar la operación de inserción de identidad en una tabla a la vez.

Habilitar o deshabilitar la inserción de identidad solo se aplica a MS SQL Server y Sybase ASE. Para otras bases de datos como Oracle, MaxDb, DB2, MySQL o SQL Anywhere no es necesario. Puede importar los datos directamente a las tablas.

## 20.2.2.1.3 Configurar archivos SBO

De forma interna, la aplicación de supervisión usa las bibliotecas del servidor de conexión y se necesita la configuración de SBO para que el servidor de conexión establezca la conectividad con el controlador de base de datos. Se debe especificar el controlador de base de datos y su ubicación en el archivo SBO para establecer la conectividad.

> **Nota**
>
> La aplicación de supervisión hace referencia al nombre de conexión de auditoría y utiliza JDBC si se usa `<hostName>.<Portnum>.<dbName>`, de lo contrario, ODBC. Los archivos SBO del servidor de conexión deben configurarse de forma correspondiente para que la aplicación de supervisión se pueda conectar a la base de datos de auditoría.

> **Nota**
>
> Para las bases de datos Oracle, solo se soportan las conexiones JDBC.

## Ejemplo

- Si el campo Nombre de conexión configurado en la página Auditoría de la CMC es `<hostName>.<Portnum>.<dbName>`, el JAR del controlador se debe configurar en: `dataAccess\connectionServer\jdbc\<dbType>.sbo`.
- Si el campo Nombre de conexión configurado en la página Auditoría de la CMC es un DNS ODBC, el controlador se debe configurar en: `<Dir_Instal>\dataAccess\connectionServer\odbc\<tipoBd>.sbo`.
- Si la base de datos que se usa para la auditoría es SAP HANA, el archivo en el que se debe configurar el controlador es: `<Dir_Instal>\dataAccess\connectionServer\odbc\newdb.sbo`.
- Si la base de datos que se usa para la auditoría es MS SQL Server, el archivo en el que se debe configurar el controlador es: `<Dir_Instal>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- Si la base de datos que se usa para la auditoría es servidor DB2, el servidor de conexión no contendrá un archivo `db2iseries.sbo` compatible.
  De manera perdeterminada la aplicación de monitorización utiliza el modo de conexión ODBC para conectarse a la base de datos de auditoría DB2. Para trabajar en este modo, primero deberá añadir y configurar el sistema DNS (para el servidor DB2) en el equipo en el que se esté ejecutando la aplicación de monitorización. Consulte los siguiente enlaces para obtener información sobre cómo habilitar y configurar la conexión ODBC para DB2:
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024166.htm
  - http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024200.htm

> **Nota**
>
> Si no configura el sistema DSN para DB2 fallará la tendencia de monitorización.

## Configurar archivos SBO

Normalmente, las bibliotecas ODBC están configuradas en los archivos SBO y solo se tienen que agregar los nombre de alias. Si este no es el caso, siga estos ejemplos para llevar a cabo la configuración en el archivo SBO:

## Ejemplo

- Si la versión de base de datos que se usa para la auditoría es SAP HANA, la configuración en el SBO debe ser:

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
    <Aliases>
        <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
        <Alias>Hana</Alias>
    </Aliases>
    <Libraries>
        <Library Platform="MSWindows">dbd_wnewdb</Library>
        <Library Platform="MSWindows">dbd_newdb</Library>
```

```
    </Libraries>
    <Parameter Name="Driver Name">HDBODBC</Parameter>
</DataBase>
```

- Si la versión de base de datos que se usa para la auditoría es MS SQL Server 2008, la configuración en el SBO debe ser:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
    <Libraries>
        <Library>dbd_wmssql</Library>
        <Library>dbd_mssql</Library>
    </Libraries>
    <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
    <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
    <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
    <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- id="li_9D4EB94F9752458BB21A940C0A892C6D">Si la versión de la base de datos utilizada para la auditoría es MySQL 5, el SBO deberá tener esta entrada:

```
<DataBase Active="Yes" Name="MySQL 5">
    <JDBCDriver>
        <ClassPath>
            <Path>C:\mysqljdbcdriver.jar</Path>
              </ClassPath>
        <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
        <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE$/$DATABASE$</
Parameter>
    </JDBCDriver>
    <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
    <Parameter Name="Force Execute">Always</Parameter>
    <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

- Si la versión de base de datos que se usa para la auditoría es Oracle, la configuración en el SBO debería ser:

```
<DataBase Active="Yes" Name="Oracle 11">
        <Aliases>
           <Alias>Oracle</Alias>
        </Aliases>
      <JDBCDriver>
            <ClassPath>

<Path>C:\app\Administrator\product\11.2.0\client_64\jdbc\lib\ojdbc6.jar</Path>
             </ClassPath>
                <Parameter Name="JDBC Class">oracle.jdbc.OracleDriver</
Parameter>
                <Parameter Name="URL Format">jdbc:oracle:thin:@//$DATASOURCE$/
$DATABASE$</Parameter>
       </JDBCDriver>
       <Parameter Name="Extensions">oracle11,oracle,jdbc</Parameter>
        <Parameter Name="Escape Character">/</Parameter>
         <Parameter Name="Force Execute">Always</Parameter>
         <Parameter Name="Catalog Separator">.</Parameter>
</DataBase>
```

Para obtener más información acerca de la configuración del controlador en archivos SBO, consulte el *Manual de acceso a datos*.

## 20.2.2.1.4 Adición del nombre del alias en el archivo SBO

Además de configurar el controlador, los usuarios también deben agregar un alias en el SBO, en la versión de base de datos que se usa para la auditoría. En la siguiente tabla se muestra una lista de los nombres del alias que se deben usar para bases de datos específicas.

| Nombre de DB | Nombre del alias que se usará en SBO |
|---|---|
| SAP HANA | Hana |
| Microsoft SQL Server | MS SQL Server |
| My SQL | MySQL |
| SAP Max DB | MaxDB |
| IBM DB2 | DB2 |
| Sybase SQL Anywhere | Sybase SQL Anywhere |
| Sybase Adaptive Server Enterprise | Sybase Adaptive Server Enterprise |
| Oracle | Oracle |

Se deben usar los nombres especificados, ya que la aplicación de supervisión busca estos nombres en el SBO.

### Ejemplo

Si la base de datos que se usa para la auditoría es MS SQL Server 2008, se debe agregar el alias al SBO tal y como se muestra:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
        <Aliases>
        <Alias>MS SQL Server</Alias>
        </Aliases>
            <Libraries>
                <Library>dbd_wmssql</Library>
                <Library>dbd_mssql</Library>
            </Libraries>
            <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
            <Parameter Name="CharSet Table" Platform="Unix">datadirect</
Parameter>
            <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
            <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
   </DataBase>
```

## 20.2.2.1.5 Cambiar a la base de datos de auditoría.

Cambiar la base de datos para que la información de tendencias de supervisión se almacene en la base de datos de auditoría.

1. En el área *Administrar* en la página de inicio de la CMC, haga clic en *Aplicaciones*.
2. Haga clic en *BI Admin Studio*.

3. Luego, haga clic en *Propiedades de supervisión.*
4. Haga doble clic en *Aplicación de supervisión* para abrir la página de propiedades.
5. En el área *Configuración de la base de datos de tendencias*, seleccione *Usar base de datos de auditoría*.

> **Nota**
>
> Si está utilizando una base de datos Oracle para auditorías, es preciso especificar como conexión JDBC el *Nombre de conexión* de *base de datos ADS* en la página de auditoría de la CMC. Especifique el nombre de conexión como sigue: `<server_name>,<port>,<service_name>`.

> **Nota**
>
> Para asegurarse de que las tablas de supervisión se creen correctamente, otorgue los permisos siguientes para la cuenta de usuario de la base de datos:
>
> EJECUTAR
> CREAR SECUENCIA
> CREAR DESENCADENADOR

## 20.2.2.2 Configuración de la base de datos de supervisión mediante JDBC

Ha creado una conexión JBDC. Para crear una nueva conexión JDBC, realice los siguientes pasos:

1. Coloque el controlador jar JBDC para la base de datos que desee configurar en la siguiente ubicación: `<INSTALL_DIR\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\MON.MonitoringService\lib>`.

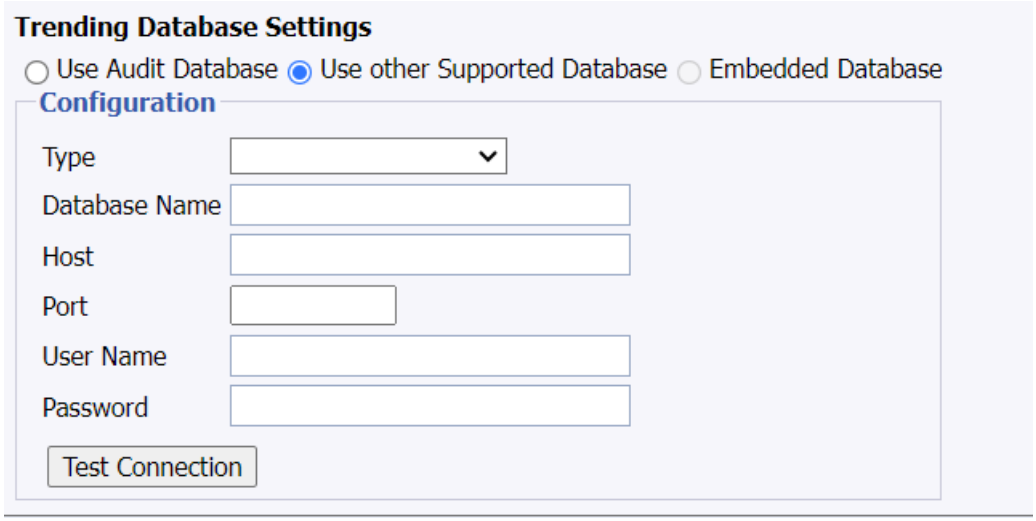
   > **Nota**
   >
   > En los despliegues clusterizados, debe copiar el controlador JDBC en el sistema que aloja los servicios de supervisión.

2. Reinicie SIA.

Para configurar una nueva base de datos para Supervisión BI, proceda de la forma siguiente:

1. Inicie una sesión en la CMC.
2. En la página de inicio de CMC, seleccione *Aplicaciones* en el menú desplegable.
3. Haga clic con el botón derecho en *BI Admin Studio* y seleccione *Propiedades de supervisión*.

   Aparece la ventana emergente *Propiedades de la aplicación de supervisión*. El botón de selección *Utilizar base de datos de auditoría* está seleccionado.
4. Seleccione el botón de selección *Utilizar otra base de datos que se soporte*.
5. Introduzca el *tipo*, el *nombre de la base de datos*, el *host*, la *puerta*, el *nombre de usuario* y la *contraseña*.




6. **Opcional:** Añada el número de días tras los que la plataforma debe borrar los datos del historial de supervisión con la propiedad *Borrar todo el historial anterior a X días*.
7. Seleccione *Guardar y cerrar*.
8. Reinicie el servidor de procesamiento de Adaptive.

   Valide la conexión seleccionando *Probar conexión*.

> **Nota**
>
> Debe reiniciar todos los servidores APS que albergan un servicio Supervisión BI para que las modificaciones tengan efecto.

Ahora ya ha configurado una nueva base de datos para almacenar comentarios de la aplicación Supervisión BI.

## 20.2.3 Propiedades de configuración

En esta sección se describen las propiedades de la aplicación de supervisión y cómo puede modificarlas.

Para ver las propiedades de configuración de la aplicación supervisión:

1. En la página de inicio de la CMC, haga clic en *Aplicación*.
2. Haga clic con el botón derecho en *BI Admin Studio* y seleccione *Propiedades de supervisión*. A continuación se describen las propiedades configurables:

| Sección | Campo | Descripción |
|---|---|---|
| | *Habilitar aplicación de supervisión* | Seleccione esta opción para activar las funcionalidades de supervisión. Si deselecciona esta opción, se desactivarán todas las funciones de supervisión excepto las medidas. La tendencia de medidas también se desactivará. |

| Sección | Campo | Descripción |
| --- | --- | --- |
| | *URL de punto final de agente JMX predeterminado (IIOP)* | Contiene la dirección URL de punto final de agente JMX que utiliza el protocolo IIOP. Esta dirección URL se genera automáticamente si habilita la supervisión y reinicia el servidor. Es el protocolo predeterminado para el servicio de supervisión. Se trata de un campo de sólo lectura. |
| RMI | *Habilitar protocolo RMI para JMX* | Esta opción está desactivada de forma predeterminada. Si activa esta opción, debe proporcionar el número de puerto RMI. Este puerto se usará tanto para la entrada de registro RMI como para el puerto de conector de RMI. Este puerto debe estar disponible para el servicio; de lo contrario, el servicio no se podrá iniciar. Tras proporcionar el número de puerto RMI, reinicie el servidor. Una vez reiniciado el servidor, se genera el URL del punto final del agente JMX RMI. Se trata de una propiedad de solo lectura que contiene el URL del punto final del agente JMX usando el protocolo RMI. Use este URL para conectarse a la supervisión desde otros clientes. |
| Indicadores de host | *Habilitar indicadores de host* | Esta opción está desactivada de forma predeterminada. Si habilita esta opción, debe proporcionar la ruta a la instalación del binario SAPOSCOL.<br><br>Para habilitar la métrica de host, es necesario instalar SAPOSCOL. Para más información sobre cómo instalar SAPOSCOL, consulte «Instalar SAPOSCOL». |
| Configuración de la base de datos de tendencias | *Usar base de datos de auditoría* | Seleccione esta opción para almacenar el historial de tendencias de las métricas en la base de datos de auditoría de la Memoria de datos de auditoría (ADS).<br><br>**Nota**<br><br>Para que funcione, se debe haber configurado la Memoria de datos de auditoría. |
| | *Utilizar otra base de datos permitida* | Marque esta opción para almacenar el historial de tendencias de supervisión/métricas en una base de datos compatible que deberá haber configurado. |
| | *Borrar todo el historial anterior a X días* | Especifica cuánto tiempo, en días, se deben conservar los datos del historial. |

| Sección | Campo | Descripción |
|---|---|---|
| Otros parámetros | *Intervalo de actualización de métrica (segundos)* | El intervalo mínimo que puede especificar son 15 segundos. Este intervalo regula lo siguiente:<br>• El cálculo de subscripción de las vigilancias: las reglas de precaución y peligro se calculan de manera continua con un intervalo de tiempo especificado.<br>• Cálculo del estado de vigilancia: el estado de vigilancia se calcula de forma continua con un intervalo de tiempo mencionado en el periodo de actualización de métrica si la configuración de Evento de la vigilancia se selecciona con las siguientes opciones: *Cambiar el estado de vigilancia cada vez que se evalúa una precaución o un peligro como verdadero*.<br>• Periodo de tendencia: el modo de historial para los gráficos se registra de forma continua en el intervalo de tiempo especificado. |
| | *Intervalo de actualización automática de IU de supervisión (segundos)* | Este intervalo se usará en la interfaz de usuario de supervisión (incluyendo el cuadro de mandos, la lista de vigilancias y las medidas) para llevar a cabo la actualización automática. El intervalo mínimo es 15 segundos. La actualización automática no afecta a la duración en modo Live en gráficos que, de manera predeterminada, se establece en 15 segundos. |
| | *Frecuencia del recordatorio de alerta (días)* | Especifica el número de días antes de que se genere un recordatorio de alertas. |

3. Haga clic en *Guardar*.

> **Nota**
>
> Si modifica cualquiera de estas propiedades excepto la habilitación y la deshabilitación de la aplicación de supervisión, debe reiniciar los servidores de procesamiento Adaptive que alojan los servicios de supervisión.

## Instalación de SAPOSCOL

Para instalar SAPOSCOL, lleve a cabo los pasos siguientes:

1. Descargue`SAPHOSTAGENT710_XX.SAR` del SAP Marketplace (http://service.sap.com).
2. Extraiga `SAPHOSTAGENT710_XX.SAR` ejecutando el comando `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR`.
3. Instale `saphostexec` ejecutando el comando `saphostexec.exe -install`. Una vez que saphostexec está instalado como un servicio, se inicia SAPOSCOL.
4. Compruebe el estado de SAPOSCOL ejecutando el comando `saposcol -s`.

## 20.2.3.1 Dirección URL de punto final JMX

La aplicación de supervisión expone una dirección URL de punto final JMX mediante la cual otros clientes pueden conectarse usando una API remota JMX. De forma predeterminada, la conectividad de JMX se proporciona sobre transporte IIOP (Internet Inter-Orb Protocol) o CORBA (Common Object Request Broker Architecture). Esta dirección URL de conexión se muestra en la página de propiedades de la aplicación de supervisión. Al poderse conectar sobre IIOP, no hay por qué preocuparse de los servidores de seguridad ni tener que mostrar puertos. Los puertos CORBA están disponibles de forma predeterminada. Los archivos jar enumerados en la tabla siguiente son necesarios en el extremo de cliente JMX para poder establecer la conexión:

| Archivos jar |
| --- |
| activation-1.1.jar |
| axiom-api-1.2.5.jar |
| axiom-impl-1.2.5.jar |
| axis2-adb-1.3.jar |
| axis2-kernel-1.3.jar |
| cecore.jar |
| celib.jar |
| cesession.jar |
| commons-logging-1.1.jar |
| corbaidl.jar |
| ebus405.jar |
| log4j.jar |
| logging.jar |
| monitoring-plugins.jar |
| monitoring-sdk.jar |
| stax-api-1.0.1.jar |
| wsdl4j-1.6.2.jar |
| wstx-asl-3.2.1.jar |
| XmlSchema-1.3.2.jar |
| TraceLog.jar |
| ceaspect.jar |
| aspectjrt.jar |

Otra opción es conectarse mediante el puerto RMI predeterminado. Para obtener más información sobre cómo conectarse mediante el puerto RMI, consulte Propiedades de configuración [página 824]

## 20.2.3.2 Configuración SSL JMX

Ahora puede lograr una comunicación segura entre JConsole y BOE a través de la configuración de SSL JMX.

1. Inicie sesión en la CMC.
2. Vaya a *Aplicaciones* > *BI Admin Studio* > *Propiedades de supervisión*.
3. En *RMI*, active la opción *Habilitar protocolo RMI para JMX*.
4. Indique el número de puerta RMI.

   7777
5. Active la opción *Habilitar SSL para protocolo RMI para JMX*.
6. Haga clic en *Guardar* y *Cerrar*.
7. Reinicie el *Servidor de procesamiento de Adaptive*.

> **Nota**
>
> Se reinicia el servidor que aloja el servicio de supervisión.

### 20.2.3.2.1 Generar certificado

1. Abra la petición de comandos en modo Administrador o una sesión de terminal, y navegue hasta esta ubicación:

   **Windows**:

   ```
   INSTALLDIR\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
   ```

   **Linux / Unix:**

   ```
   INSTALLDIR/sap_bobj/enterprise_xi40/<PLATFORM>_x64/sapjvm/bin
   ```
2. Ejecute el comando para generar un certificado: `keytool -genkeypair -alias serverkey -keyalg RSA -keysize 2048 -keystore serverkeystore`
3. Introduzca toda la información necesaria para crear un certificado.
4. 4. Una vez la ejecución sea correcta, crea un archivo de certificado por nombre en el mismo directorio de ubicación sapjvm: `serverkeystore`

### 20.2.3.2.2 Añadir un archivo de almacén de certificados al servicio de supervisión

1. En CMC, vaya a *Servidores* > *Lista de servidores*.
2. Seleccione *Servidor de procesamiento de Adaptive* (Servicio de supervisión del host de servidor).
3. Seleccione *Propiedades*.
4. Vaya a la sección *Configuración SSL JMX*.

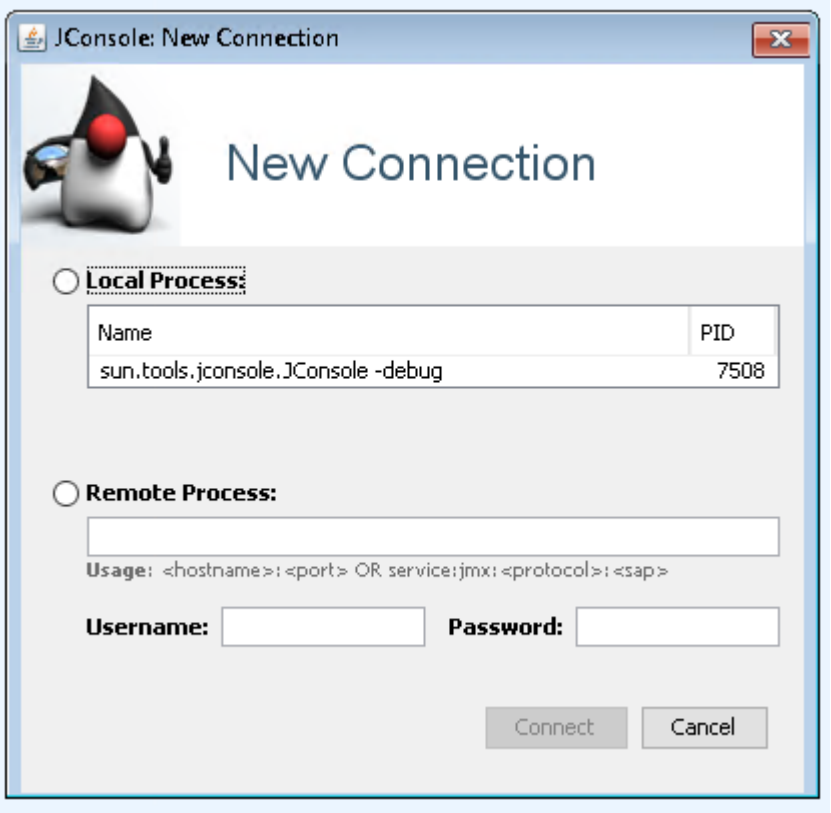
5. En la *Ubicación del archivo del almacén de certificados*, introduzca la ruta de la *Ubicación del archivo Keystore del certificado*.
6. Introduzca la información de *Contraseña de acceso a clave privada*.

   Contraseña1

## 20.2.3.2.3 Conexión con JConsole

1. Ejecute el comando para lanzar `JCONSOLE.exe` en la petición de comandos (`jconsole.exe -J-Djavax.net.ssl.trustStore="<Path of Certificate Keystore file location >" -J-Djavax.net.ssl.trustStorePassword=<PasswordDetail>`)

   ```
   jconsole.exe -J-Djavax.net.ssl.trustStore="C:\Program Files
   (x86)\SAP BusinessObjects\SAP BusinessObjects
   Enterprise XI 4.0\win64_x64\sapjvm\bin\serverkeystore" -J-
   Djavax.net.ssl.trustStorePassword=Password1
   ```
2. Una vez ejecutado el comando anterior, lance el visor JConsole tal como se muestra a continuación.

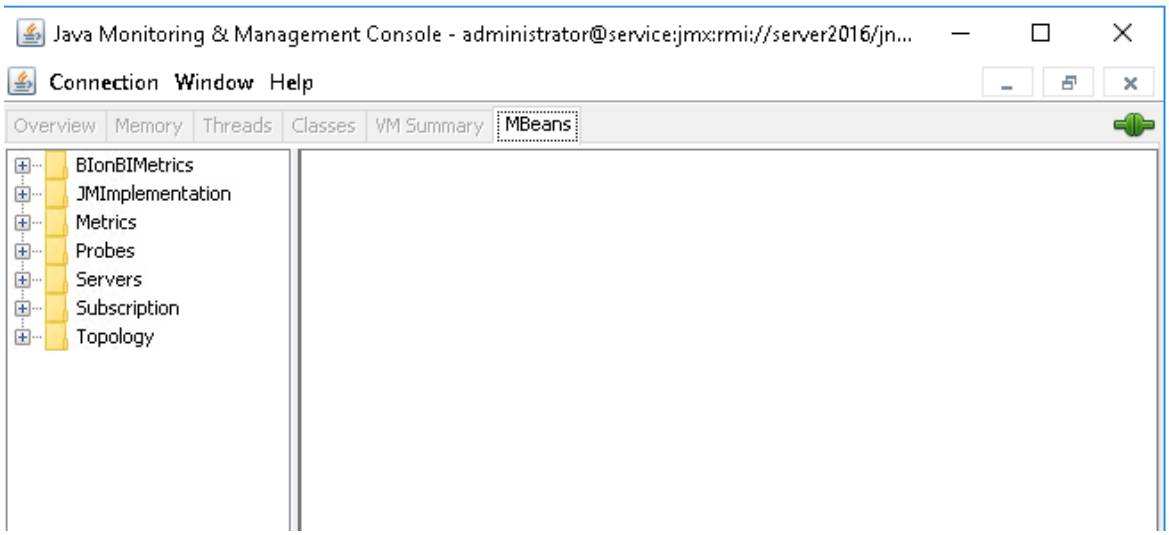



3. Haga clic en el botón de selección *Proceso remoto* para habilitar el campo.
4. Indique el *URL de punto final de agente RMI JMX*, y el *Nombre de usuario* asociado y *Contraseña*.

   El formato *URL de punto final de agente RMI JMX* es: `service:jmx:rmi://<HostName>/jndi/rmi://<HostName>:<RMI Port Number>/<hostname>:<CMS Port>`.

   `service:jmx:rmi://server2016/jndi/rmi://server2016:7777/server2016:6400`.

5. Haga clic en *Conectar*.
6. Se ha iniciado el visor JConsole *JAVA Monitoring & Management Console*.




7. En el visor JConsole, puede navegar a diferentes secciones como BIonBIMetrics, Métricas, Pruebas, Servidores y Topología para recuperar los datos relacionados.

## 20.2.3.3 Autenticación HTTPS para métricas de supervisión

Se admite la autenticación del servidor HTTPS para métricas de supervisión, y se requiere la configuración siguiente antes del uso:

1. Importar el certificado del servidor en el almacén de confianza del cliente. Esto permite que el cliente (la métrica) verifique la identidad del servidor. Ejecute este comando:
   ```
   <RAÍZ_INSTAL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\lib>
   keytool -import -alias ca -keystore "<RAÍZ_INSTAL>\SAP BusinessObjects
   Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security\cacerts" –file ca.cer
   ```
   `ca.cer` es el certificado autofirmado o el certificado de la autoridad de certificados (normalmente un CA interno) que ha generado el certificado del servidor. Si el certificado del servidor se ha generado por un CA reconocido, no es necesario importarlo, y se puede saltar este paso. Esto se debe a que el certificado del servidor se verificará con en CA, la clave pública del cual ya está en el almacén de confianza de forma predeterminada.
2. Modifique la *URL base* en la configuración de la métrica de la plataforma de lanzamiento de BI en `https://<URL>/BOE/BI`, dónde <URL> se refiere al host del nombre usado en el certificado.

Autenticación de cliente HTTPS para métricas de supervisión no admitida.

## 20.2.3.4 Cifrado de contraseña para métricas

Al usar métricas, para asegurar que las contraseñas están cifradas, debe agregar el parámetro `true` a cada parámetro de contraseña de prueba de supervisión al crear la métrica a través de la línea de comandos. Para obtener más información y un ejemplo de sintaxis, consulte el tema *Administrar métricas mediante la línea de comandos* en la ayuda de la CMC.

## 20.2.4 Integración con otras aplicaciones

Las soluciones Enterprise como IBM Tivoli Monitoring, se integran con la aplicación de supervisión como clientes JMX que se conectan a través de la dirección URL de punto final JMX. Tras la integración, las medidas de SAP BusinessObjects pueden verse desde la interfaz de usuario del cliente.

### 20.2.4.1 Integración de la aplicación de supervisión con SAP Solution Manager

Para integrar la aplicación de supervisión con SAP Solution Manager, debe tener instalado y en funcionamiento Wily Introscope en el sistema. SAP Solution Manager debe estar configurado para la estación de trabajo Introscope. Lleve a cabo los siguientes pasos durante la instalación de la plataforma de BI:

1. En el paso «Configurar conectividad con Introscope Enterprise Manager», indique el nombre del host y los datos del puerto. Se instalará un agente de Introscope en `C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wily` cuando se instale la plataforma de BI.
2. Lance la estación de trabajo Wily Introscope y haga clic en *Nuevo investigador*. Puede ver la métrica de servidores SAP BusinessObjects y métricas virtuales en la sección JMX del agente configurado.

> **Nota**
>
> Puede configurar el agente de Wily Introscope (IS) seleccionando *CMC* > *Servidores* > *Nodo de servidor* > *Marcadores de posición*. El host y el puerto de IS Enterprise Manager se configuran también aquí para que el agente de IS se comunique con la aplicación de supervisión. Para obtener más información, consulte *Administrar servidores* en el Manual de ayuda de CMC.
>
> Para que las métricas JMX estén disponibles en IS, asegúrese de que los servicios del agente de IS y de supervisión están disponibles en la instancia de AdaptiveProcessingServer.
>
> Si habilita la instrumentación de IS, la instrumentación de código se habilita automáticamente.

## 20.2.5 Soporte de clúster para el servidor de supervisión

La aplicación de supervisión admite clústeres, lo que proporciona capacidad de conmutación.

Con la compatibilidad de clúster, solo estará activo un único servicio en un momento dado, y el resto de servicios permanecerán pasivos. Si hay dos servicios de supervisión s1 y s2 en un entorno de clúster, solo uno de ellos está disponible. Ambos s1 y s2 intentan convertirse en activos, pero cuando uno de ellos lo consigue, el otro servicio se convierte en inactivo o pasivo.

El servicio pasivo comprueba periódicamente la disponibilidad del servicio activo (cada minuto). Si el servicio activo no está disponible, el servicio pasivo intenta inmediatamente activarse.

> **Nota**
>
> Se recomienda que el servicio de supervisión se aloje en una instancia Adaptive Processing Server (APS) independiente para evitar fallos o un bajo rendimiento del APS.

## 20.2.6 Solución de problemas

Esta sección proporciona soluciones paso a paso de una amplia gama de problemas que pueden ocurrir en el trabajo con la aplicación de supervisión.

### 20.2.6.1 Cuadro de mandos

#### El vínculo de supervisión no se muestra en la página de la CMC

- Compruebe si el usuario dispone de los derechos de acceso adecuados.
- Asegúrese de que el usuario se agrega a los grupos Usuario o administrador de supervisión o cualquier otro grupo que forme parte de dichos grupos.

#### Los indicadores de rendimiento de claves (KPI) no están visibles en el cuadro de mandos de supervisión

- Compruebe que las métricas necesarias están visibles seleccionando *Propiedades de servidor del CMS* > *Métricas*.
- Asegúrese de que el Servidor de administración central responde según lo esperado.

### 20.2.6.2 Alertas

#### No se pueden recibir alertas en la página Alertas

- Compruebe que la opción *Habilitar mis alertas* esté seleccionada en las propiedades de aplicación de alertas.
- Asegúrese de que dispone de los derechos de acceso adecuados para recibir alertas.
- Compruebe si las alertas recientes son visibles en el cuadro de mandos de supervisión.

> **Nota**
>
> Puede enviar un documento de Crystal Reports al ID de correo electrónico que configuró para probar si el SMTP funciona según lo esperado.

### No se reciben notificaciones de correo electrónico

- Compruebe que la opción *Habilitar correo electrónico* esté seleccionada en las propiedades de aplicación de alertas.
- Compruebe que la configuración de la dirección de correo electrónico es la adecuada para recibir alertas de correo electrónico.
- Compruebe si el servidor SMTP está funcionando.
- Asegúrese de que la instancia del servidor de tareas de Adaptive está habilitada.
- Compruebe la configuración SMTP en el destino de instancia del servidor de tareas de Adaptive.

## 20.2.6.3 Lista de vigilancia

### No se pueden recibir los datos históricos para la vigilancia

- Compruebe el intervalo de sondeo en la página *Propiedades* de la aplicación de supervisión.
- Compruebe el archivo de traza en la carpeta de inicio de sesión.
- Compruebe que la hora del sistema del servidor y el cliente es la misma en una zona horaria específica.

### Ocurrió un error al recuperar los datos sincronizados en directo

Compruebe que la instancia del servidor de procesamiento de Adaptive se está ejecutando.

### La ficha de la lista de vigilancia está deshabilitada

- Compruebe si el servicio de supervisión está en funcionamiento.
- Compruebe si hay mensajes de error en los registros del servicio de supervisión.
- Compruebe si los servidores y sus métricas están visibles en jConsole.

## 20.2.6.4 Medidas

### No se pueden programar medidas

- Compruebe si la instancia de AdaptiveJobServer que almacena el servicio de programación de métrica se está ejecutando.
- Asegúrese de que el CUID de informe, que se usa para documentos de Crystal Reports y Web Intelligence, sea el correcto.

- Asegúrese de que el usuario dispone de derechos administrativos o es miembro del grupo Administrador.
- Compruebe si el usuario dispone de los derechos adecuados para abrir, actualizar, exportar documentos de Crystal Reports o Web Intelligence que se usan en las medidas correspondientes.

### El estado de la programación de la medida es pendiente

- Compruebe si la instancia ProbeSchedulingService está instalada.
- Compruebe si la instancia de AdaptiveJobServer que almacena el servicio de programación de métrica se está ejecutando.

### Ocurrió un error al recuperar los datos de tendencias de la base de datos

Compruebe que la instancia AdaptiveProcessingServer se está ejecutando.

### probeRun.bat no se ejecuta correctamente

- Compruebe si `java_home` está configurado.
- Compruebe si se han introducido los parámetros correctos en el símbolo del sistema.

> **Nota**
>
> Introduzca **`probeRun.bat -help`** en el símbolo del sistema para comprobar si todos los parámetros son correctos.

## 20.2.6.5 Métrica

### Las métricas de host no aparecen

- Asegúrese de que SAPOSCOL se está ejecutando.
- Asegúrese de que la opción *Habilitar métricas del host* está seleccionada en la página *Propiedades* de la aplicación de supervisión.
- Reinicie la instancia AdaptiveProcessingServer para que los cambios sean efectivos.
- Asegúrese de que la *Ruta a la instalación del binario SAPOSCOL* es correcta.

### Ocurrió un error al recuperar el cliente JMX

Compruebe que la instancia AdaptiveProcessingServer se está ejecutando.

### El valor de la métrica SAPOSCOL es cero en la página Métrica

- Asegúrese de que SAPOSCOL se está ejecutando.
- Ejecute los siguiente en el host en el que está instalado SAPOSCOL:
  1. `saposcol -s` para comprobar el estado
  2. `saposcol -m` para obtener una instantánea de los datos recopilados por SAPOSCOL

## 20.2.6.6 Gráfico

### Las gráficas muestran momentos distintos para los modos historial y en directo

Asegúrese de que la hora del sistema del servidor y el cliente son las mismas en una zona horaria específica.

# 20.3 Diferencia visual

La diferencia visual permite ver las diferencias entre dos versiones de un LCMBIAR o de un objeto o ambos. Puede usar esta función para determinar la diferencia entre archivos u objetos para desarrollar y mantener diferentes tipos de informe. Esta función ofrece un estado de comparación entre las versiones de origen y de destino. Por ejemplo, si una versión anterior del informe del usuario es preciso y la versión actual no es precisa, puede comparar y analizar el archivo para evaluar el problema.

### Página de inicio

La página de inicio de la diferencia visual consta de las siguientes fichas y paneles:

- Nueva comparación: esta ficha permite crear una nueva comparación de objetos
- Buscar comparaciones: este campo permite buscar los objetos que ya se han comparado
- Panel Comparaciones: en este panel se muestra una lista las fichas de filtros y diferencias
- Comparaciones: Panel Diferencias: esta panel muestra en una lista los objetos comparados con el nombre de la comparación, la Fecha y hora, y el estado de las diferencias

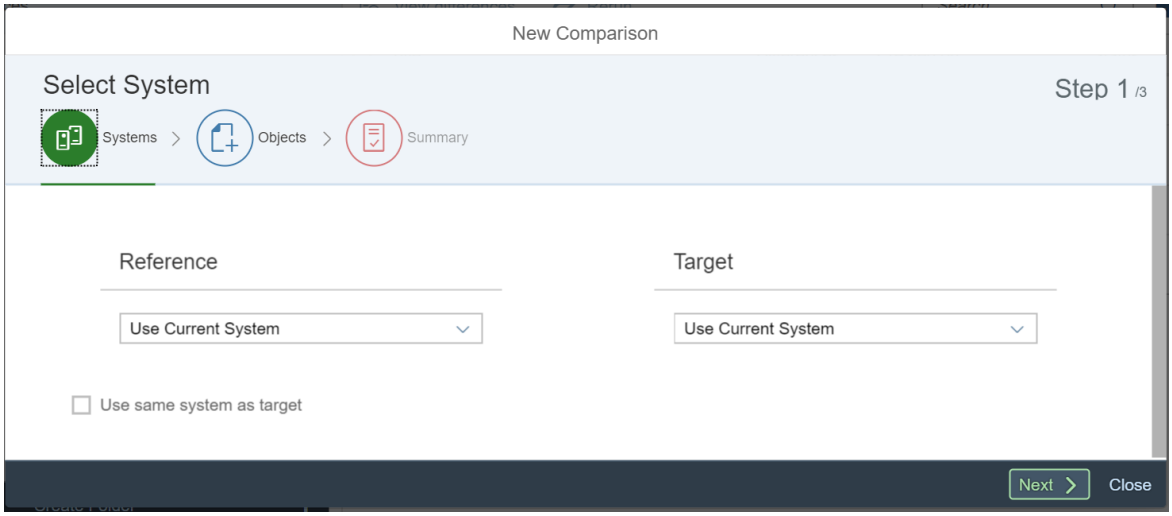
## 20.3.1 Comparar objetos o archivos con diferencia visual

Para comparar archivos con la diferencia visual, siga los siguientes pasos:

1. Inicie sesión en la aplicación de la CMC.
2. En la página de inicio de la CMC, en la ficha *Administrar*, haga clic en el vínculo *Diferencia visual*.
   Aparecerá la página Diferencia visual. Los archivos comparados se almacenan en la carpeta "Diferencias" o en cualquiera de las subcarpetas creadas por el usuario.

   > **Nota**
   >
   > Para crear una subcarpeta, seleccione Create Folder +

3. Seleccione + para crear una comparación nueva.
   Se visualiza el asistente *nueva comparación*.




4. Seleccione el sistema de *referencia* y de *destino* de la lista desplegable.
   Puede conectarse a cualquiera de los siguientes sistemas de referencia y de destino:

   > **Nota**
   >
   > Si se agrega un objeto en el sistema de administración de versiones (VMS), recibirá la opción de selección de versiones en el siguiente paso.

   - CMS
   - Sistema de archivos locales
5. En la pantalla *Selección de objetos* busque y seleccione el objeto o un archivo del sistema de *referencia* y *de destino* .
6. Modifique el *nombre de la comparación*, si es necesario.
7. Seleccione *Comparar* para comparar los objetos.

   > **Nota**
   >
   > - Puede comprobar las diferencias al seleccionar la primera comparación y, a continuación, *Visualizar las diferencias*. Las diferencias se resaltan en color naranja y los objetos perdidos se resaltan en color rojo.

> - Puede ejecutar de nuevo la comparación mediante la selección de la primera comparación y, a continuación, *Volver a ejecutar*

El proceso de comparación se inicia inmediatamente.

También puede usar la opción de filtro para ver los objetos comparados por tipo y con diferencias o con atributos comunes.

## 20.3.2 Comparar objetos o archivos con el sistema de administración de versiones

Puede comparar tareas de administración de promociones o carpetas en un sistema de administración de versiones mediante la opción de diferencia visual.

Para comparar objetos en un sistema de administración de versiones, siga los siguientes pasos:

1. Inicie la sesión en la aplicación de la CMC.
2. En la página de inicio de la CMC, en la ficha *Administrar*, haga clic en el vínculo *Diferencia visual*.
   Aparecerá la página Diferencia visual. Los archivos comparados se almacenan en la carpeta "Diferencias" o en cualquiera de las subcarpetas creadas por el usuario.

   > ⓘ Nota
   >
   > Para crear una subcarpeta, haga clic en el icono Carpeta.

3. Haga clic en *Nueva comparación*.
   Aparecerá la pantalla *Diferencia visual: Comparaciones*.
4. Seleccione *Iniciar sesión en VMS* desde *Seleccionar sistema* en Referencia.
5. Introduzca las credenciales de inicio de sesión en VMS y haga clic en *Iniciar sesión*.
   Aparecerá el cuadro de diálogo *Selección automática de sistema de destino*.
6. Haga clic en *No* si quiere establecer un sistema de destino diferente, o haga clic en *Sí* para establecer el mismo sistema de destino que el sistema de referencia.
7. Haga clic en el botón *Examinar* para seleccionar los objetos o trabajos que desea comparar desde los sistemas de referencia y de destino.
8. Haga clic en *Agregar*.
   Los objetos seleccionados para la comparación aparecen en una lista en el panel *Nueva comparación*.
   Puede comparar los archivos inmediatamente o programar la comparación para otro momento más tarde.
   Para comparar los archivos, continúe con el siguiente paso.
9. Haga clic en *Comparar* para comparar las tareas o carpetas.
   El proceso de comparación se inicia inmediatamente y las diferencias, si las hubiera, se muestran en el *visor de Diferencia visual*. Las diferencias se resaltan en color naranja y los objetos perdidos se resaltan en color rojo.
   También puede usar la opción de filtro para ver los objetos comparados por tipo y con diferencias o con atributos comunes.
10. Haga clic en *Guardar* para guardar el informe de diferencias.
11. Especifique la ubicación en la que desea guardar el informe y haga clic en *Aceptar*.

## 20.4 Autorización de elementos HTML

Para permitir que los usuarios se beneficien de las capacidades de elementos HTML de confianza y proteger su organización frente a otros, especifique una lista de elementos HTML autorizados.

Cuando un usuario abre un documento que contiene una celda con la propiedad Leer como HTML o Leer como hipervínculo en el visor HTML de Web Intelligence o el visor interactivo, el visor puede interpretar el HTML. Este comportamiento depende del modo que haya definido el renderizado de estas celdas en las propiedades de visualización Web Intelligence y los elementos HTML que autoriza.

Cuando especifica los elementos HTML autorizados y un documento en el modo de lectura contiene un elemento no autorizado, solo se retiene el texto del elemento, no la etiquetas de los elementos o sus atributos. En un documento que contiene un elemento autorizado y ambos atributos autorizados y no autorizados, solo se retienen el elemento y los atributos autorizados.

Para autorizar solo elementos HTML específicos en las propiedades de visualización de Web para JavaScript, seleccione *Activar solo elementos HTML en la página de elementos HTML autorizados* y especifique los elementos HTML en la página *Elementos HTML autorizados*.

Por defecto, solo están autorizados los elementos HTML para Web Intelligence para que funcionen correctamente. Puede agregar elementos o eliminarlos de la lista predeterminada.

⚠ Precaución

- Web Intelligence permite el código JavaScript/HTML integrado en las celdas de documentos gracias a las funciones de las fórmulas.
  Este código se puede activar o desactivar en la Consola de administración central. Sin embargo, al autorizar JavaScript, HTMLs e hipervínculos, reconoce el riesgo de estar exponiéndose al cross-site scripting. El cross-site scripting permite a los atacantes alterar sitios web o ejecutar código en otros sistemas. Esta vulnerabilidad afecta a productos como navegadores de Internet cuando están ejecutando scripts. La mayoría de los ataques de cross-site scripting son el resultado de una programación no segura en el sistema de destino.
- El código se puede ajustar con una lista de etiquetas y atributos HTML autorizados. Sin embargo, SAP no se hace responsable de la compatibilidad del código y sus posibles efectos secundarios. Por ejemplo, puede que sea necesario adaptar el código debido a actualizaciones del navegador, soporte de versión JavaScript o el modo en que el código se incrusta de forma dinámica en la página web. Desde un punto de vista técnico, a partir de la versión 4.3, la aplicación se ejecuta como una Aplicación de página única. No existe una separación técnica entre el informe y la página web global. El código puede requerir ajustes para ejecutarse en ese nuevo contexto
- Eliminar los elementos de la lista predeterminada acumula las funciones de Web Intelligence así que la desaconsejamos.

Puede autorizar:

- El elemento `<a>` con el atributo `href` para agregar una referencia.
- Un conjunto de atributos para todos los elementos en su lista asociando el elemento * con la lista de atributos.
  No puede autorizar todos los atributos asociados con un elemento.
- Los elementos que contengan JavaScript, como `<script>`, `<onClick>` y `<onMouseEnter>`.
  No puede autorizar las palabras clave JavaScript.

## Ejemplo

Elementos HTML autorizados

| Elemento | Atributos |
|---|---|
| * | estilo, clase, id |
| img | src |
| vínculo | ref |

La tabla siguiente muestra cómo Web Intelligence muestra los elementos HTML en documentos como resultado de las autorizaciones.

Impacto de autorizaciones para elementos HTML

| HTML original | HTML final | Explicación |
|---|---|---|
| `<link title="SAP" ref="www.sap.com">` | `<link ref="www.sap.com">` | El elemento `<link>` y el atributo `ref` están autorizados de manera que el enlace muestre un enlace activo en el documento.<br><br>El atributo `title` está autorizado de manera que se elimina del documento. |
| `<img src="datasource" id="I1">` | `<img src="datasource" id="I1">` | El elemento `<img>` y los atributos asociados `src` están autorizados y el atributo `id` está autorizado para todos los elementos de manera que queda el HTML original. |
| `<div title="datasource" id="D1">` | Eliminado. | El elemento `<div>` no está autorizado de manera que el elemento y los atributos asociados se eliminan del documento. |
| `<p> ...as shown in the picture below: <img src="../picture.jpg" alt="Mountain"> </p>` | `...as shown in the picture below:<img src="../picture.jpg">` | El elemento `<p>` no está autorizado, así que se elimina. Solo permanece el texto incluido en el elemento `<p>`.<br><br>El elemento `<img>` y el atributo asociado `src` están autorizados así que permanecen.<br><br>El atributo `alt` está autorizado de manera que se elimina del documento. |

Para modificar la configuración de visualización de Web Intelligence [página 716]Modificar la lista de elementos HTML autorizados [página 840]

## 20.4.1 Modificar la lista de elementos HTML autorizados

Especifique los elementos HTML de confianza que desee autorizar y ofrezca protección contra posibles elementos malintencionados modificando la lista de elementos HTML autorizados.

Web Intelligence sólo autoriza los elementos que defina en la página *Elementos HTML autorizados* cuando la propiedad de visualización JavaScript *Activar sólo elementos HTML definidos en la página de elementos HTML autorizados* está activa en las propiedades de Web Intelligence.

1. Vaya a CMC y seleccione *BI Admin Studio*.
2. En la *Página de inicio de la consola de administración central*, desplácese hacia abajo hasta los *Elementos HTML*.
3. Modifique la lista como se describe en la siguiente tabla:

| Modificación | Pasos |
|---|---|
| **Para añadir un elemento** | Haga clic en *Añadir un elemento nuevo* e introduzca el elemento y los atributos asociados que deben autorizarse.<br>**Nota**<br>• Para autorizar ciertos atributos para todos los elementos HTML, introduzca * como elemento y añada los atributos.<br>• Cuando intenta añadir un elemento HTML que ya estaba en la lista, sólo se añadirán a la lista los atributos nuevos para el elemento. |
| **Para editar un elemento** | Haga clic en el elemento y luego, en *Editar el elemento seleccionado.* |
| **Para eliminar un elemento** | Haga clic en el elemento y luego, en *Borrar el elemento seleccionado.* |
| **Para recuperar la lista estándar de elementos HTML autorizados** | Haga clic en *Reinicializar.*<br>La lista estándar contiene sólo los elementos necesarios para que Web Intelligence funcione correctamente. |

# 21 Reporting CMS

## 21.1 Reporting CMS

Antes de iniciar la generación de informes en CMS deberá poseer los conocimientos básicos sobre los conceptos siguientes:

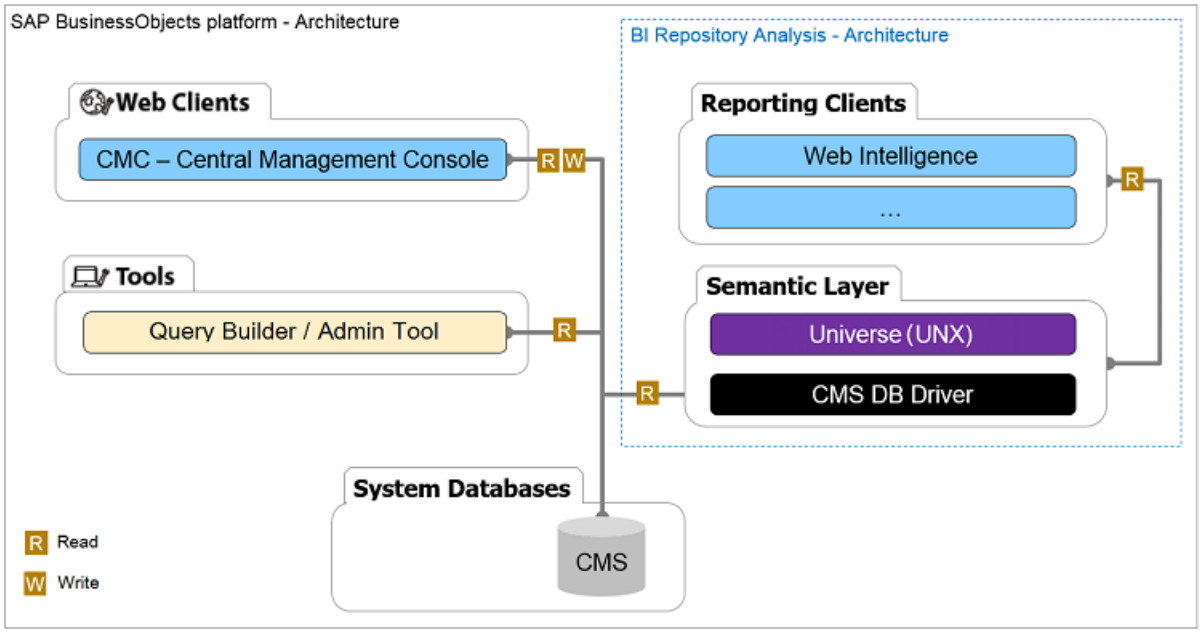
- la arquitectura de la plataforma SAP BusinessObjects
- la estructura de la base de datos del sistema CMS
- propiedades y relaciones de InfoObjects

### Información relacionada

La arquitectura de la plataforma SAP BusinessObjects [página 841]
La estructura de la base de datos del sistema CMS [página 842]

## 21.1.1 La arquitectura de la plataforma SAP BusinessObjects

El esquema está diseñado para ayudarle a entender la arquitectura de la plataforma SAP BusinessObjects.




La siguiente tabla le proporciona más información sobre los componentes de la plataforma SAP BusinessObjects.

Los componentes de la plataforma SAP BusinessObjects

| Componentes | Descripción |
| --- | --- |
| CMC - Consola de administración central | Una herramienta basada en Web que se utiliza para configurar los ajustes de seguridad y gestionar las siguientes opciones:<br>• Usuario<br>• Contenido<br>• Servidor |
| Base de datos del sistema CMS | Base de datos que almacena la siguiente información de la plataforma BI:<br>• Usuario<br>• Servidor<br>• Documento<br>• Configuración<br>• Autenticación<br>La base de datos del sistema CMS se actualiza en el Servidor de administración central (CMS) y se puede consultar como repositorio del sistema. |
| Creador de gráficos (también llamado Herramientas de administración) | Herramienta basada en Web que se utiliza para consultar el repositorio de BusinessObjects y obtener la información necesaria que no se puede encontrar en el CMC. |
| Análisis del repositorio de BI | Esta solución utiliza la capa semántica de la plataforma de BI, el universo (UNX) y el controlador de BD de CMS para consultar el CMS. |

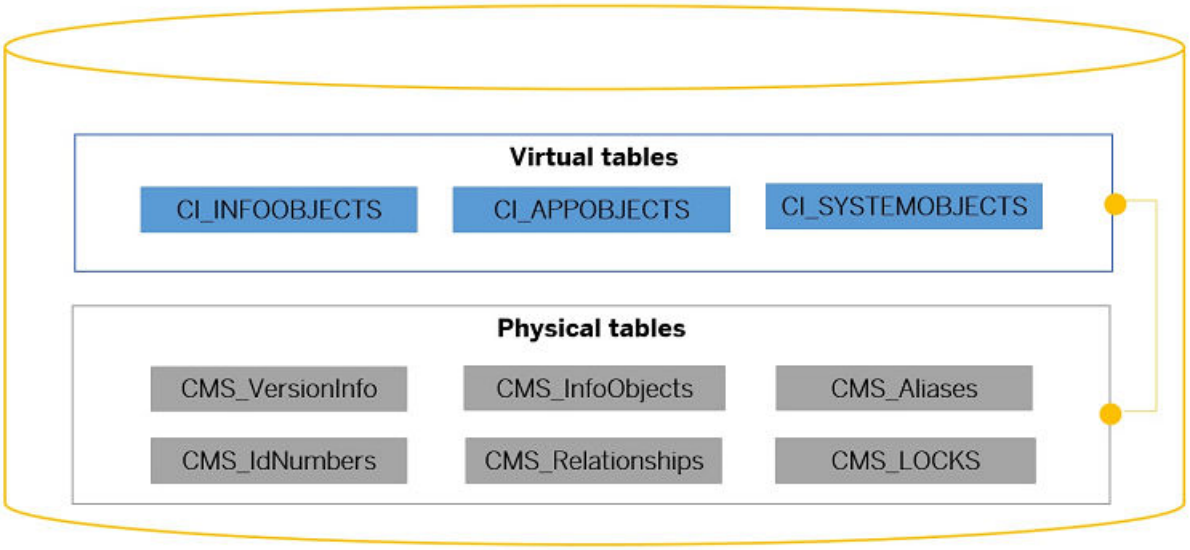
## 21.1.2 La estructura de la base de datos del sistema CMS

La base de datos del sistema CMS se actualiza en el Servidor de administración central (CMS) y se puede consultar como repositorio del sistema. El sistema CMS es una base de datos que almacena información sobre la plataforma BI en forma de InfoObjects.

La base de datos del sistema CMS incluye dos tipos de tabla:

- Tabla de base de datos física: los metadatos de CMS se almacenan en las tablas de bases de datos físicas.
- Tabla virtual: el servidor CMS explora los InfoObjects de las tablas virtuales.

El siguiente esquema le proporciona un resumen de la estructura de base de datos del sistema CMS.




Para más información sobre la estructura de base de datos del sistema CMS, consulte los temas relacionados.

## Información relacionada

Tablas de bases de datos físicas [página 843]
Tablas virtuales [página 844]

# 21.1.2.1 Tablas de bases de datos físicas

Los metadatos de CMS se almacenan en seis tablas de bases de datos físicas.

Tablas de bases de datos físicas

| Tabla física | Descripción |
|---|---|
| CMS_VersionInfo | Incluye la versión actual de SAP BusinessObjects Enterprise (BOE) |
| CMS_InfoObjects | Tabla principal en el repository de sistema. Cada fila almacena un único InfoObject. |
| CMS_Aliases | Asigna los alias de usuario a el ID de usuario correspondiente. Un usuario tiene un alias para cada dominio de seguridad en el que el usuario es un miembro. Sin embargo, un usuario solo tiene un ID de usuario. |
| CMS_IdNumbers | Genera IDs de objeto e IDs de tipo únicos. |

| Tabla física | Descripción |
| --- | --- |
| CMS_Relationships | Almacena las relaciones entre InfoObjects. |
| CMS_LOCKS | Tabla auxiliar de CMS_RELATIONS |

### 21.1.2.2 Tablas virtuales

El servidor CMS explora los InfoObjects de tres tablas virtuales.

Tablas virtuales

| Tabla virtual | Descripción |
| --- | --- |
| Tabla de InfoObjects | Incluye InfoObjects que el usuario final puede visualizar, como:<br>• Documentos de informe<br>• Programas<br>• Accesos directos<br>• Carpetas<br>• Categorías<br>• Bandejas de entrada |
| Tabla de objetos de aplicación | Incluye InfoObjects que utilizan documentos, como:<br>• Universos<br>• Conexiones<br>• Sobrecargas |
| Tabla de objetos de sistema | Incluye InfoObjects que la plataforma de BI utiliza para funcionar, como:<br>• Usuarios<br>• Grupos<br>• Claves de licencia |

## 21.1.3 Acerca de InfoObjects

Antes de consultar los metadatos de InfoObject, deberá comprender claramente los conceptos siguientes:

- propiedades de InfoObject
- relaciones entre InfoObjects

Si entiende cómo los InfoObjects están organizados en el repositorio CMS, podrá explorar el repositorio rápida y fácilmente y resolver los problemas relacionados con el repositorio CMS.

## Información relacionada

Propiedades de InfoObject [página 845]
Relaciones entre InfoObjects [página 845]

# 21.1.3.1 Propiedades de InfoObject

La tabla siguiente incluye las propiedades más importantes para InfoObjects y sus descripciones.

Propiedades de InfoObject

| Propiedades de InfoObject | Descripción |
|---|---|
| SI_NAME | Nombre del objeto |
| SI_KIND | Clase de objeto |
| SI_OWNER | Nombre de usuario del propietario |
| SI_OWNERID | ID de usuario del propietario |
| SI_CHILDREN | Número de hijos |
| SI_CUID | Los CUID son identificadores únicos de clúster que identifican un InfoObject de forma unívoca. |
| SI_UNIVERSE | Los universos (UNV) utilizados por el documento |

# 21.1.3.2 Relaciones entre InfoObjects

Los InfoObjects están organizados en tres jerarquías:

- Jerarquía de carpetas
- Jerarquía de usuarios/grupos de usuarios
- Jerarquía de servidores/grupos de servidores

El CMS y las aplicaciones cliente utilizan la jerarquía de carpetas para navegar por los InfoObjects.

Para más información sobre las relaciones entre InfoObjects, consulte los temas relacionados.

## Información relacionada

Jerarquía de carpetas [página 846]
Carpetas raíz [página 846]

### 21.1.3.2.1 Jerarquía de carpetas

La jerarquía de carpetas es una lista plana de un superior de InfoObjeto. Todos los InfoObjetos deben tener un superior definido en la propiedad SI_PARENTID.

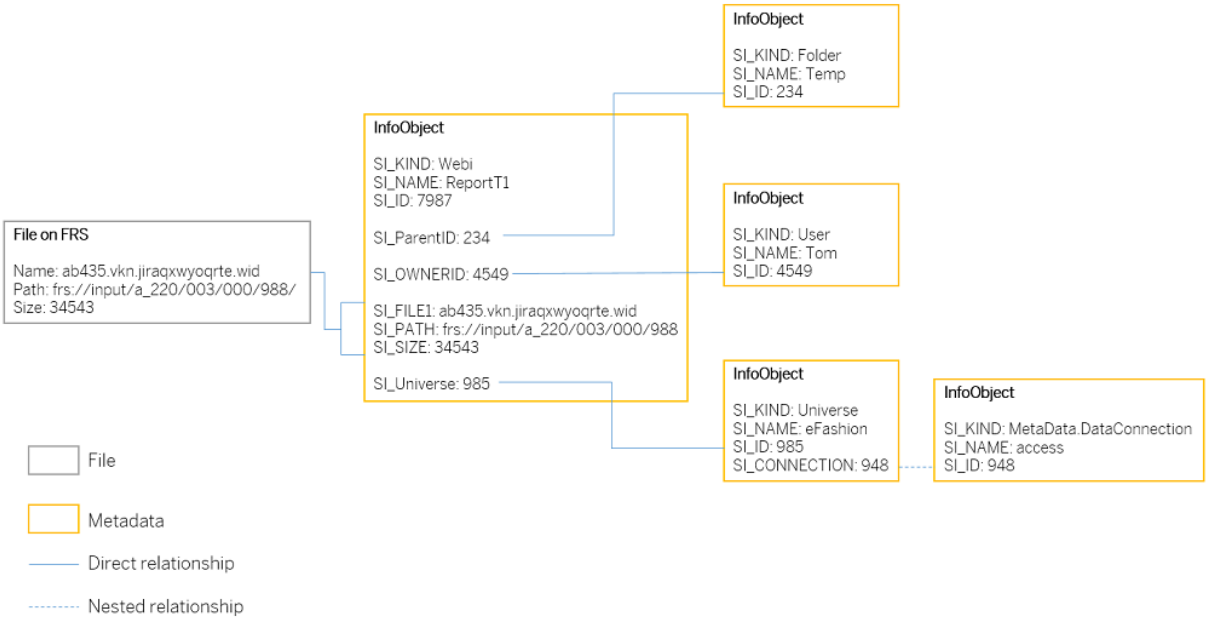
CMS usa la propiedad ID superior para crear la jerarquía de carpetas que es virtual. De hecho, la jerarquía no corresponde al modo en que los InfoObjetos se almacenan en el repositorio.

### 21.1.3.2.2 Carpetas raíz

La carpeta principal en la jerarquía del repositorio del CMS es la carpeta de cluster CMS. Las carpetas raíz se pueden encontrar en un nivel inferior en la carpeta de cluster CMS. Las carpetas raíz son virtuales y no corresponden a nada en el sistema de ficheros.

Los InfoObjetos se organizan en carpetas raíz para CMS y las aplicaciones cliente para encontrarlas de manera rápida y sencilla. Por ejemplo, las aplicaciones cliente pueden navegar por la colección de InfoObjetos primero utilizando la carpeta raíz InfoObjetos, después la propiedad ID superior y las propiedades ID inferiores. El mismo tipo de InfoObjetos normalmente se pueden encontrar en la misma carpeta raíz.

El diagrama siguiente le ayudará a entender las relaciones entre InfoObjetos.




Como puede ver, la estructura del InfoObjeto permite a los InfoObjetos tener un número infinito de relaciones y relaciones anidadas.

## 21.2 Resumen de gestión de informes de CMS

Como administrador, debe entender y optimizar la utilización de la plataforma de business intelligence.
El kit de ejemplo de la gestión de informes de CMS incluye el controlador de base de datos CMS que

permite visualizar e informar de los objetos de metadatos de la base de datos CMS. Ahora puede utilizar un universo y clientes de gestión de informes nativos para consultar los objetos de metadatos de la base de datos de repository de CMS. Estos objetos de metadatos incluyen información de la plataforma de Business Intelligence, como:

- Conexiones
- Documentos
- Programas
- Universos
- Usuarios

Puede importar el ejemplo de gestión de informes de CMS que contiene los objetos predefinidos para ayudarle a crear informes y dashboards con las siguientes aplicaciones de análisis de datos y gestión de informes de SAP BusinessObjects:

- SAP BusinessObjects Web Intelligence
- SAP Crystal Reports para Enterprise

Para iniciar la gestión de informes de forma rápida y fácil en el CMS, puede trabajar con el kit de ejemplo de gestión de informes de CMS. A continuación las fases principales para crear un informe de CMS.

- Importe el ejemplo de gestión de informes de CMS: La Gestión de promociones se utiliza en la CMC para importar el ejemplo de gestión de informes de CMS.
- Cree un informe CMS: Con SAP BusinessObjects Web Intelligence, puede crear un informe CMS con el mismo universo de muestra CMS que una fuente de datos.

Consulte la Información relacionada para obtener el procedimiento global que ofrece un resumen más detallado del proceso de creación.

### Información relacionada

Kit de ejemplo de la gestión de informes de CMS
Crear un informe CMS
Importación del kit de ejemplo de gestión de informes de CMS con Gestión de promociones [página 849]

## 21.3 Conexión de la base de datos CMS

Un controlador de base de datos CMS se utiliza para establecer una conexión segura con la base de datos CMS. Puede utilizar la conexión estándar disponible en el ejemplo de la gestión de informes CMS o puede establecer su propia conexión CMS.

Para la conexión de base de datos de CMS, debe utilizar una conexión relacional. La siguiente tabla describe los parámetros de una conexión relacional.

Parámetros para una conexión relacional

| Parámetro | Descripción |
| --- | --- |
| *Modo de autenticación* | El método que se usa para autenticar las credenciales de inicio de sesión del usuario al acceder al origen de datos:<br>• *Usar el nombre de usuario, contraseña e ID del sistema especificados*: Usa los parámetros *Nombre de usuario* y *Contraseña* definidos para la conexión. Puede acceder a la fuente de datos desde un sistema On-Premise o un sistema distante.<br>**Nota**<br>Compruebe que el usuario tenga derechos para ver el contenido de esta sesión.<br>• *Utilizar token de sesión*: Utiliza la sesión de usuario actual. Solamente puede ver el contenido para el que está autorizado y trabajar con él. Solamente puede acceder a la fuente de datos desde un sistema On-Premise.<br>**Nota**<br>Por motivos de seguridad, este modo de autenticación es la elección recomendada. |
| *ID del sistema* | El nombre de CMS si *Modo de autenticación* es *Usar el nombre de usuario y contraseña especificados*. |
| *Nombre de usuario* | El nombre de usuario para acceder al origen de datos si *Modo de autenticación* es *Usar el nombre de usuario y contraseña especificados*. |
| *Contraseña* | La contraseña para acceder al origen de datos si *Modo de autenticación* es *Usar el nombre de usuario y contraseña especificados*. |

## 21.4 Kit de ejemplo de la gestión de informes de CMS

Debe utilizar el kit de ejemplo de gestión de informes de CMS para empezar a crear documentos para la gestión de informes de CMS. El controlador de base de datos de CMS está integrado en la plataforma de Business Intelligence y el ejemplo de gestión de informes de CMS se encuentra en la ubicación siguiente:

`<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI on BI`.

Este ejemplo incluye:

- Conexión (plataforma BI database.cns del sistema CMS)

- Universo (plataforma BI database.unx del sistema CMS)
- Ejemplo de Web Intelligence

Encontrará más información de la gestión de informes de CMS en SAP Community network.

## Información relacionada

Importación del kit de ejemplo de gestión de informes de CMS con Gestión de promociones [página 849]

# 21.4.1 Importación del kit de ejemplo de gestión de informes de CMS con Gestión de promociones

Antes de empezar, compruebe que tenga acceso al ejemplo de gestión de informes de CMS que se encuentra en la ubicación siguiente:

```
<INSTALLDIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\BI
on BI
```

La herramienta Gestión de promociones se utiliza en la Consola de administración central (CMC) para importar el ejemplo de gestión de informes de CMS.

1. En la Consola de administración central, haga clic en *Gestión de promociones*.
2. Haga clic en *Importar* > *Importar archivo*.
3. Seleccione *Sistema de archivos*.
4. Haga clic en *Seleccionar archivo* para seleccionar el ejemplo.
5. En el panel *Job nuevo*, seleccione *Conectar a nuevo CMS* para el campo *Destino*.
6. Indique los parámetros de inicio de sesión y luego haga clic en *Inicio de sesión* > *Crear*.
7. En el panel *Tareas de promoción*, haga clic con el botón derecho en el ejemplo y luego seleccione *Promocionar*.
8. En el cuadro de diálogo *Promocionar*, haga clic en *Promocionar*.

Cuando el *Estado de promoción* del ejemplo de gestión de informes de CMS sea *Éxito*, significa que ha importado el ejemplo con éxito a su sistema Business Intelligence 4.2. Para utilizar el universo de ejemplo para la gestión de informes de CMS, vea el tema relacionado.

## Información relacionada

Kit de ejemplo de la gestión de informes de CMS [página 848]

## 21.4.2 El universo de ejemplo de CMS

El universo de ejemplo de CMS incluye un universo predefinido que permite escenarios de gestión de informes comunes. Según sus necesidades de análisis y gestión de informes, puede tratar y ampliar el universo predefinido. También puede buscar una lista de consultas predefinidas en el panel *Consultas*. Estas consultas puede servir como programa de aprendizaje para las funciones de universo.

En la tabla se recogen algunas de las consultas más útiles y lo que significan.

Consultas útiles para ejecutar en el universo CMS

| Consulta | Descripción |
|---|---|
| Detalle de la relación de usuario ejemplo | Permite ver a qué grupo pertenece un usuario. |
| FolderPath de ejemplo (universo) | Permite buscar la ubicación de un universo. |
| Relaciones de ScheduleInfo de ejemplo | Permite visualizar las acciones programadas por los usuarios. |
| Propiedades QT de ejemplo con filtro (servidor) | Permite visualizar las propiedades de un InfoObjeto. |

## 21.4.3 Ampliación del universo de ejemplo de CMS

Puede crear un universo vinculado para ampliar el universo de ejemplo de CMS. Un universo vinculado es un universo .UNX que contiene un vínculo a un universo principal en CMS.

En este caso, el universo de ejemplo de CMS actúa como universo principal, de modo que el universo vinculado puede utilizar la infraestructura de datos y la capa empresarial del universo de ejemplo de CMS como módulos prefabricados. Una vez ha creado el universo vinculado, puede grabar la infraestructura de datos y la capa empresarial heredadas del universo de ejemplo de CMS como nuevos archivos, de forma que tengan un ciclo de vida independiente del universo de ejemplo de CMS.

Puede utilizar la conexión de base de datos CMS del universo de ejemplo de CMS u otra conexión compatible con la base de datos CMS.

Puede añadir tablas, crear combinaciones vinculando las tablas de infraestructura de origen de datos con los nuevos y añadir nuevos componentes a la capa empresarial de la misma forma que lo hace para cualquier otro universo. Cualquier cambio en los componentes principales se propaga automáticamente al universo vinculado cuando se verifica en el CMS.

# 21.5 Creación de un informe en el CMS

Con SAP BusinessObjects Web Intelligence, puede crear un informe en el CMS con el universo de muestra CMS como fuente de datos.

1. Abra Web Intelligence y haga clic en el icono *Nuevo* de la barra de herramientas *Archivo*.

2. Seleccione el universo de muestra CMS.

   Si utiliza el Cliente enriquecido de Web Intelligence, haga clic en *Seleccionar* .

   Se abre el *Panel de consulta*
3. Seleccione y arrastre las dimensiones y las medidas que desee incluir en la consulta al área de ventana *Objetos del resultado*.
4. Seleccione los objetos sobre los que desea definir filtros de búsqueda y arrástrelos al panel *Filtros de consulta*. Para crear un filtro rápido en un objeto, seleccione el objeto en el área de ventana *Objetos de resultado* y haga clic en el icono *Agregar un filtro rápido* de la barra de herramientas *Objetos de resultado*.
5. Haga clic en *Ejecutar consulta*.

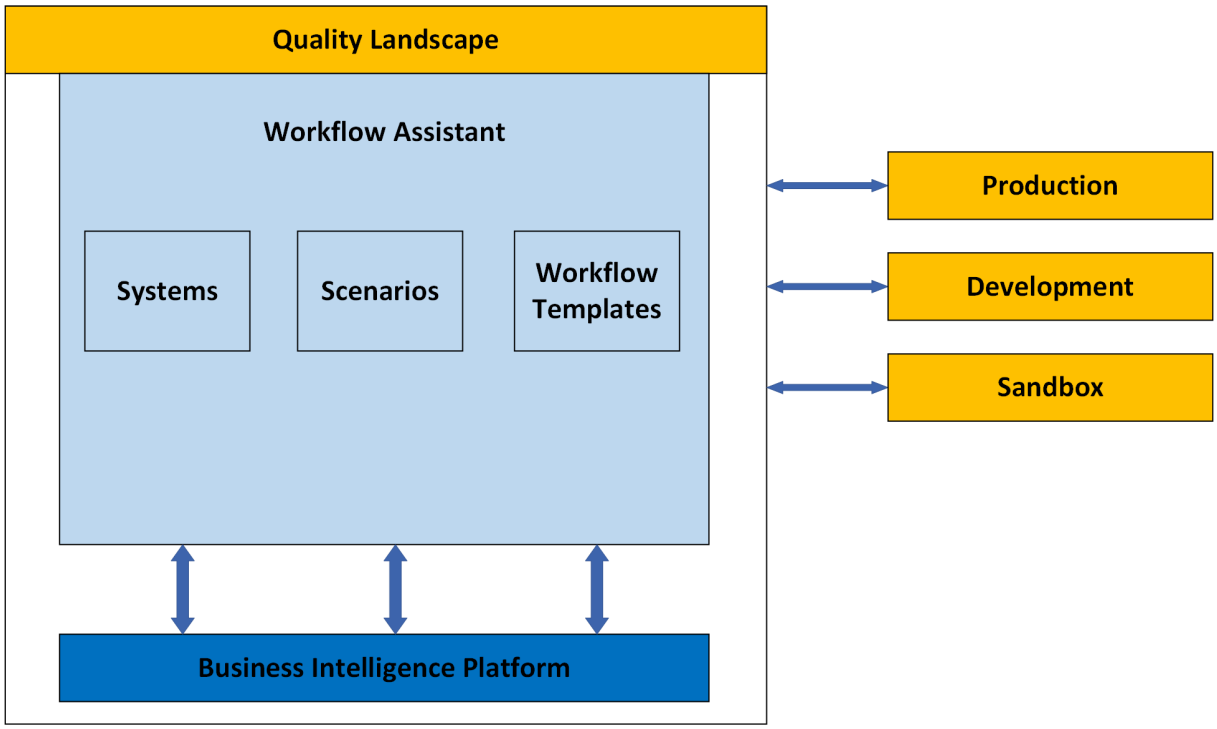
# 22 Asistente de workflow

El framework de automatización y los servicios de agente ahora están fusionados en un servicio llamado servicio de asistente de workflow. El asistente de workflow es una aplicación de la Consola de administración central (CMC) para la administración de sistemas BI y la automatización de tareas de BI.

> **Nota**
>
> Ahora, la funcionalidad del framework de automatización de la consola de administración de BI se alcanza mediante el asistente de workflow. El URL de la consola de administración de BI `(http://<systemName>:<portNo>/BOE/BIAdminConsole)` y el servicio de cola de mensajes están obsoletos.

El asistente de workflow muestra el contenido en forma de fichas: *Escenarios*, *Plantillas de workflow* y *Sistemas*. Desde estas fichas, puede desglosar la sección relevante para obtener información más detallada y funciones.

El asistente de workflow implementa un concepto basado en roles para que los usuarios solo puedan acceder a aquellas fichas para las que están autorizados.




## Acerca de los sistemas

Sistema hace referencia a uno o más equipos de BI para los que tiene autorización de acceso. Administración del sistema es una aplicación que permite acceder y administrar las infraestructuras de BI de manera

centralizada. Para utilizar las funcionalidades del asistente de workflow, es imprescindible que antes registre las infraestructuras de BI con la aplicación Administración del sistema.

### Acerca del asistente de workflow

El Asistente de workflow ofrece la funcionalidad de simplificar las tareas de BI complejas y repetitivas.

> Ejemplo
>
> Tenga en cuenta que debe realizar las siguientes tareas de BI en orden:
>
> 1. Iniciar sesión en la plataforma de BI.
> 2. Modificar el origen de determinados documentos de Web Intelligence de `.unv` a `.unx`.
> 3. Actualizar los documentos de Web Intelligence.
> 4. Salir de la plataforma de BI.

El esfuerzo manual se reduce con el asistente de workflow. Puede crear un escenario con plantillas de tarea y de workflow, guardar este escenario, ejecutar y visualizar los resultados.

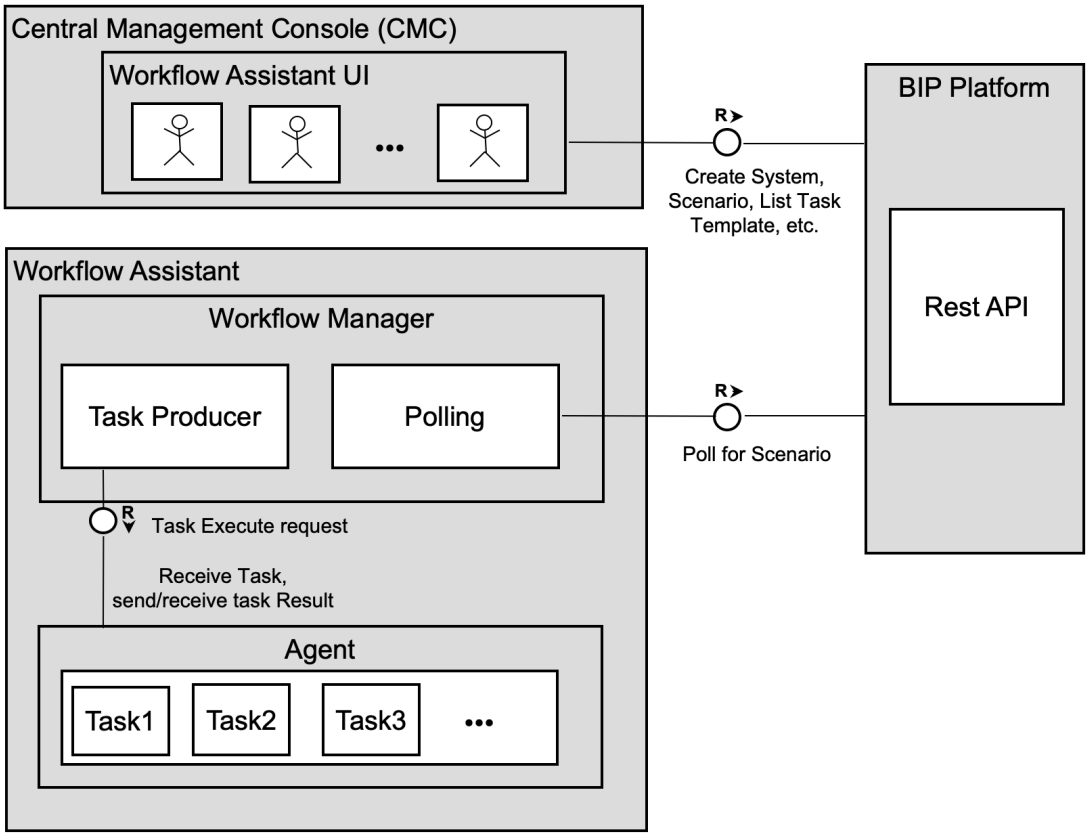
## 22.1 Audiencia de destino

Este manual se ha previsto para determinados usuarios de la plataforma Business Intelligence (BI) y determinados desarrolladores de la plataforma de BI.

- Los usuarios de la plataforma de BI que usan este manual deben tener derechos para acceder a la Consola de administración central (CMC) y al asistente de workflow. Estos usuarios tienen el rol de administradores o administradores delegados.
- Los desarrolladores de la plataforma de BI que utilicen este manual deben estar familiarizados con el trabajo en SDK Java y poder crear esquemas JSON para los requisitos personalizados mediante Task Template SDK.

## 22.2 Comprender la arquitectura

El siguiente diagrama le ayuda a comprender la arquitectura del asistente de workflow y las conexiones entre sus componentes.




Glosario de términos utilizados en el diagrama anterior:

| Término | Definición |
|---|---|
| IU de asistente de workflow | Una IU para crear plantillas de workflow y escenarios que pueden ejecutarse en cualquier sistema concreto. |
| Administrador de workflow | Un administrador de workflow consulta escenarios desde la plataforma, gestiona la ejecución de los escenarios y guarda los resultados. |
| Agente | Se trata de un proceso ligero para ejecutar las tareas dentro de los escenarios. |

## 22.3 Glosario

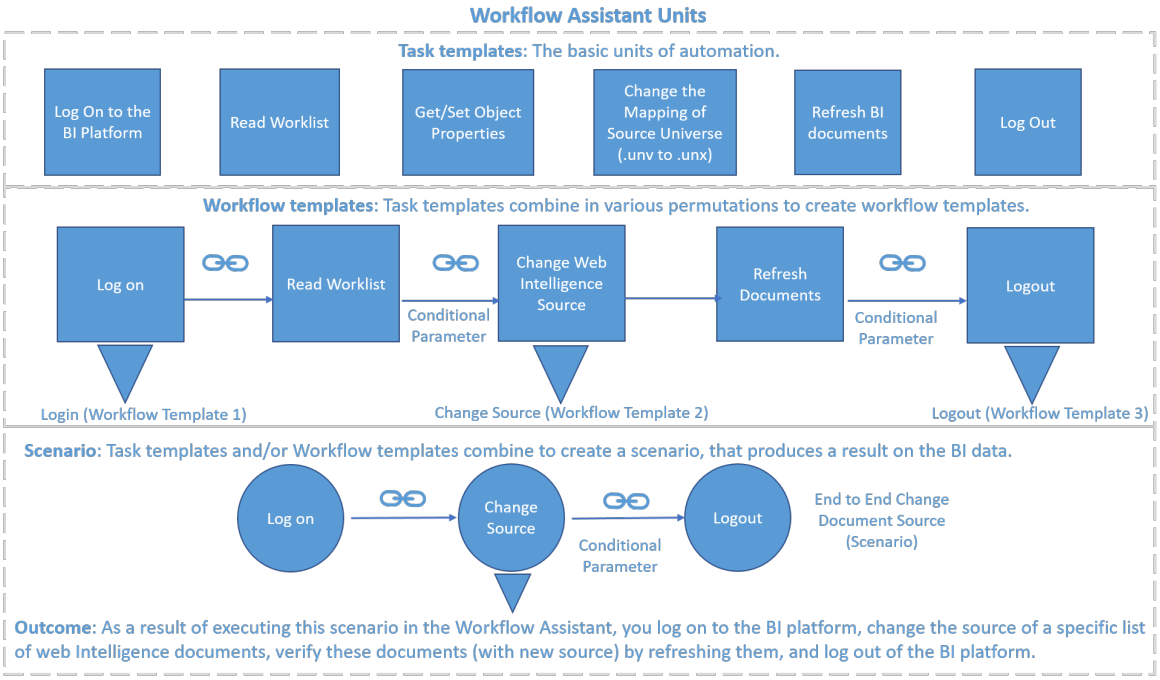
El asistente de workflow tiene su propio vocabulario especializado.

Términos de uso frecuente en el asistente de workflow

| Término | Definición |
| --- | --- |
| Plantilla para tarea estándar | La unidad básica de automatización indicada por defecto en la aplicación. Estas unidades pueden utilizarse en escenarios o plantillas de workflow.<br><br>Por ejemplo, una tarea simple como iniciar sesión en la plataforma de BI, actualizar documentos de BI, leer datos, modificar la asignación del universo de origen de documentos de Web Intelligence (de unv a unx), añadir usuarios a la infraestructura o cerrar la sesión. |
| Plantilla para tarea personalizada | Una plantilla de tarea (unidad base de automatización) que crean los desarrolladores para satisfacer requisitos personalizados.<br><br>**Restricción**<br><br>No puede crear una plantilla para tarea personalizada con la IU del asistente de workflow. Requiere el SDK de la plantilla de tarea. |
| Plantilla de flujo de trabajo | Un grupo lógico de plantillas de tarea ordenadas en la secuencia requerida para conseguir el resultado de un workflow. |
| Plantilla para workflow estándar | Plantillas de workflow predefinidas en el asistente de workflow. Los administradores pueden utilizar de inmediato las plantillas para workflow estándar cuando crean escenarios para sus diversos requisitos de automatización de BI. |
| Plantilla para workflow personalizado | Una plantilla de workflow creada por los administradores para satisfacer sus requisitos personalizados. Se crea en el asistente de workflow agrupando plantillas para tareas estándar o personalizadas. |
| Escenario | Entidad ejecutable que se crea con plantillas para tareas o workflow en la secuencia deseada. |

| Término | Definición |
| --- | --- |
| Parámetros condicionales | El enlace de conexión entre plantillas para tareas o workflow, que dirige el flujo de control, se basa en una de las siguientes condiciones:<br>• Continuar (estándar)<br>• Si correcto<br>• Si erróneo<br>• Si éxito parcial<br>**Nota**<br>Un parámetro condicional también le permite insertar un *"Retraso"*(en segundos) para garantizar que la siguiente tarea del escenario no se inicie hasta un tiempo después de que haya finalizado la ejecución de la tarea anterior.<br>**→ Recuerde**<br>El asistente de workflow tiene en cuenta el valor del parámetro condicional: "Continuar", solo si la tarea anterior ha finalizado con cualquiera de los tres estados: "Éxito", "Éxito parcial" o "Error". Si la tarea anterior tiene el estado "Error" o "No ejecutada", el estado del nodo siguiente se fija automáticamente en "No ejecutada". |

Esta ilustración le ayudará a comprender la interconexión entre algunos de los términos anteriores:




## 22.4 Acerca de la instalación y la actualización

Según si instala desde cero o si actualiza una instalación existente, el acceso a la funcionalidad de back end será distinto.

Al realizar **una instalación nueva** de la plataforma SAP BusinessObjects BI (instalación predeterminada), se obtiene acceso total al asistente de workflow en los equipos en los que ha instalado y configurado la plataforma de BI. Esto incluye el acceso a la aplicación Asistente de workflow en la CMC y la funcionalidad de back end (servicio de asistente de workflow).

Sin embargo, ahora al actualizar de la plataforma de BI SP5 o posterior a 4.3, está disponible la funcionalidad completa del asistente de workflow, aunque todavía tendrá que ver la nota SAP mencionada en Restricciones. Tras instalar la actualización, ejecute el workflow de instalación "Modificar" para obtener los servicios de back end. Para obtener más información sobre la instalación Modificar, consulte la *Guía de actualización del support package* que se ha publicado en la página de la plataforma de SAP Business Intelligence del SAP Help Portal.

> **Nota**
>
> El asistente de workflow forma parte del archivo BOE.war. Tras actualizar de la plataforma de BI 4.2 SP4 o anterior a 4.2 SP5 y la versión anterior, la aplicación web se implementa solo si se ha seleccionado la funcionalidad *Aplicaciones web Java* al instalar la versión existente.

> **Precaución**
>
> No debe instalar el asistente de workflow en varios equipos dentro de sistemas, ya que no se permite la agrupación en clústeres del asistente de workflow.

Ahora el asistente de workflow admite los sistemas operativos AIX y Solaris.

> **⚠ Restricción**
>
> - Para las plataformas de AIX y Solaris, al instalar la versión de BI 4.3 en 4.2 SP05 o versiones posteriores, el asistente de workflow se instala por defecto. Sin embargo, se necesita una reparación para obtener los servicios back end.
> - Al actualizar de la plataforma de BI 4.2 SP4 o anterior a 4.2 SP5 o posterior, fíjese que algunas de las carpetas no aparecen en el asistente de workflow. Para obtener más información, consulte 2882649

## 22.5 Configurar el asistente de workflow

Al instalar el asistente de workflow como parte de la instalación de la plataforma de BI, se obtiene el servicio de forma predeterminada en la configuración.

Luego puede configurar la autenticación de confianza para comenzar a utilizar el asistente de workflow.

### 22.5.1 Configuración básica

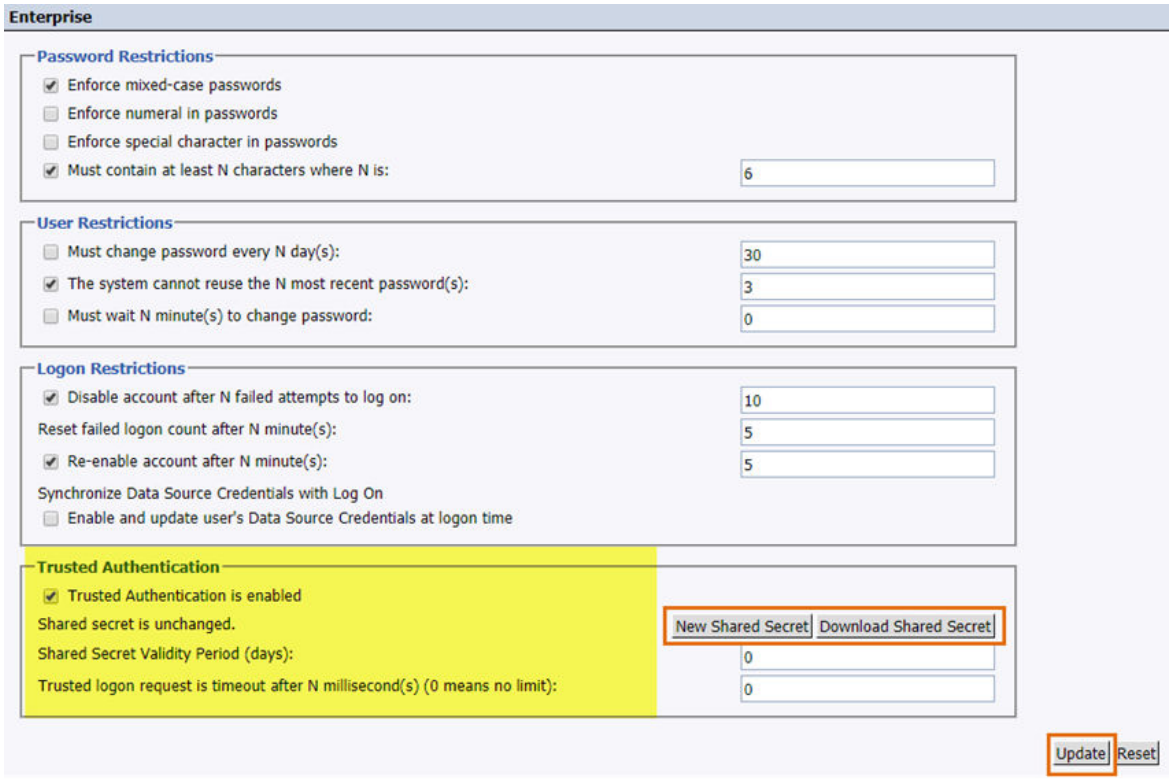
#### 22.5.1.1 Configurar la autenticación de Enterprise para el asistente de workflow

Ha instalado el asistente de workflow como parte de la instalación de la plataforma de BI en su configuración.

Para configurar la autenticación de confianza (Enterprise) para el asistente de workflow, siga este procedimiento:

1. Inicie sesión en la Consola de administración central (CMC) conectándose al CMS del nodo maestro.
2. Seleccione *Autenticación* en el menú desplegable y haga doble clic en *Enterprise*.

El diálogo "Enterprise" aparece como se muestra a continuación:




3. En la sección "Autenticación de confianza", asegúrese de activar *Autenticación de confianza*.
4. Seleccione *Nuevo secreto compartido*.
   Se genera la clave de secreto compartido.
5. Seleccione *Descargar secreto compartido*.
6. Seleccione *Actualizar*.
7. Guarde la clave de secreto compartido generada (TrustedPrincipal.conf):
   a. En Windows, en `INSTALLDIR\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.
   b. En Linux, en `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`.
   c. En AIX, en `<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/`.
   d. En Solaris, en `<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/`.

> **Nota**
>
> Para obtener más información sobre cómo crear certificados de autenticación de confianza con distintas opciones, consulte el tema Habilitación de la autenticación de confianza [página 262].

## 22.5.1.2 Crear un usuario predeterminado para el servicio back end del asistente de workflow

1. Cree un usuario nuevo en el asistente de workflow con el nombre **WAUser**.

2. Asigne los derechos adecuados yendo a la carpeta `Asistente de workflow` y otorgando el control completo de la cuenta **WAUser**.

   El servicio back end del asistente de workflow empieza con la cuenta **WAUser**.

   Si la cuenta **WAUser** no existe, el asistente de workflow se inicia con la cuenta de *administrador*.

   > ⓘ Nota
   >
   > No es obligatorio que el nuevo usuario forme parte del grupo de usuarios *Administrador*.

### 22.5.1.3 Iniciar el servicio de asistente de workflow

El tema proporciona instrucciones para iniciar el *servicio del asistente de workflow*.

1. Configure la autenticación de Enterprise para el asistente de workflow. Consulte Configurar la autenticación de Enterprise para el asistente de workflow [página 858] para obtener más información.
2. Para iniciar el *servicio de asistente de workflow*:
   a. En Windows, inicie el *Administrador de configuración central* (CCM) y el *servicio del asistente de workflow*.
   b. En Unix, vaya a `<INSTALLDIR>/AdminConsole/WorkflowAssistant/startWfAssistant.sh`.

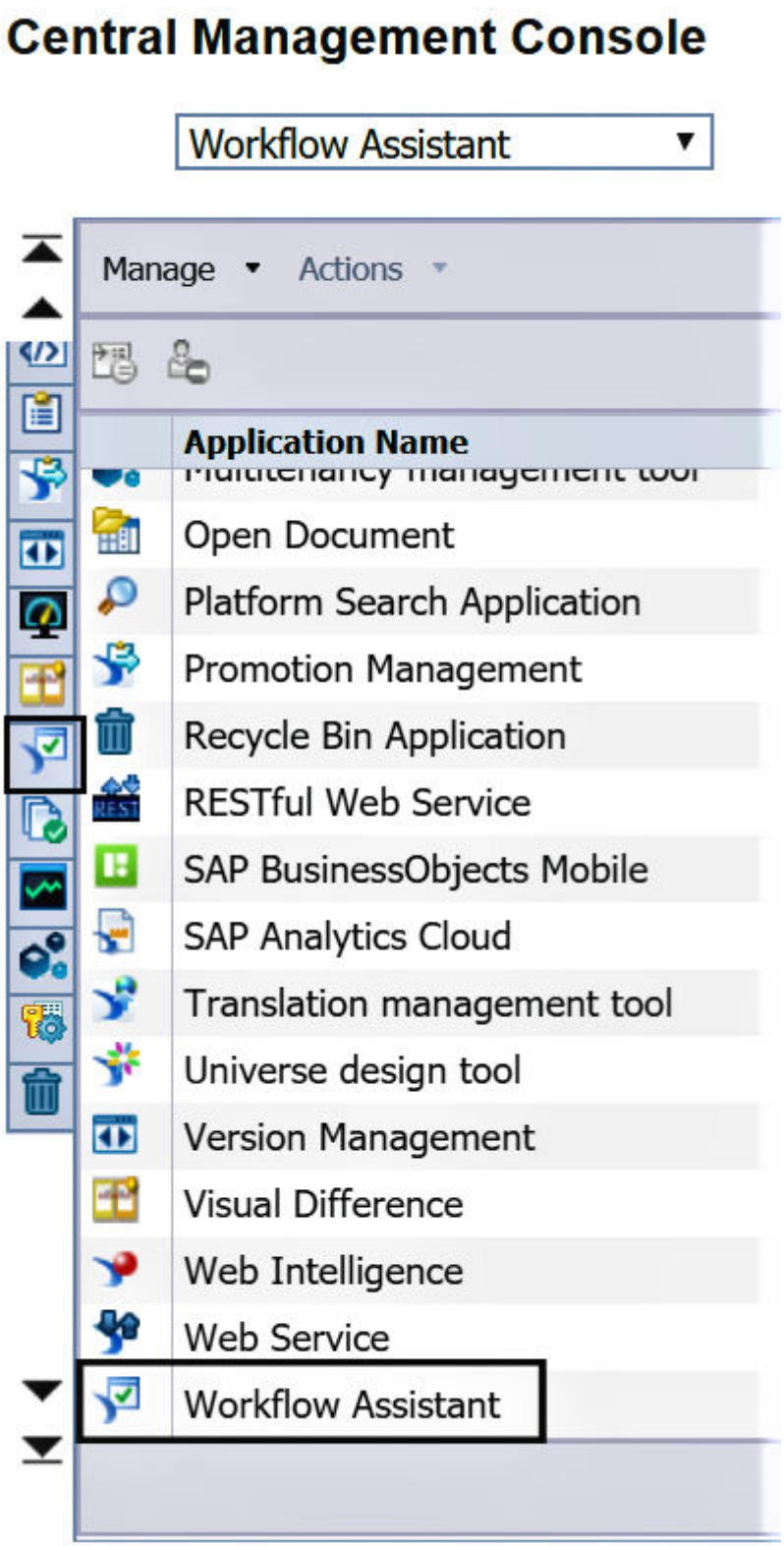
   Ahora puede utilizar el *asistente de workflow* y ejecutar escenarios.

   > ⓘ Nota
   >
   > Para asegurarse de que el asistente de workflow se haya iniciado correctamente, verifique el contenido del archivo `message.properties` en `<BOE-Install-Directory>\AdminConsole\WorkflowAssistant\service-logs`. El contenido de `message.properties` debe ser:
   >
   > ```
   > STATUS_WFM=success
   >
   > MESSAGE_AGENT=Agent - Started\!\!
   >
   > STATUS_AGENT=success
   >
   > MESSAGE_WFM=Workflow Assistant - Started\!\!
   > ```

## 22.6 Gestión de derechos del asistente de workflow mediante la Consola de administración central

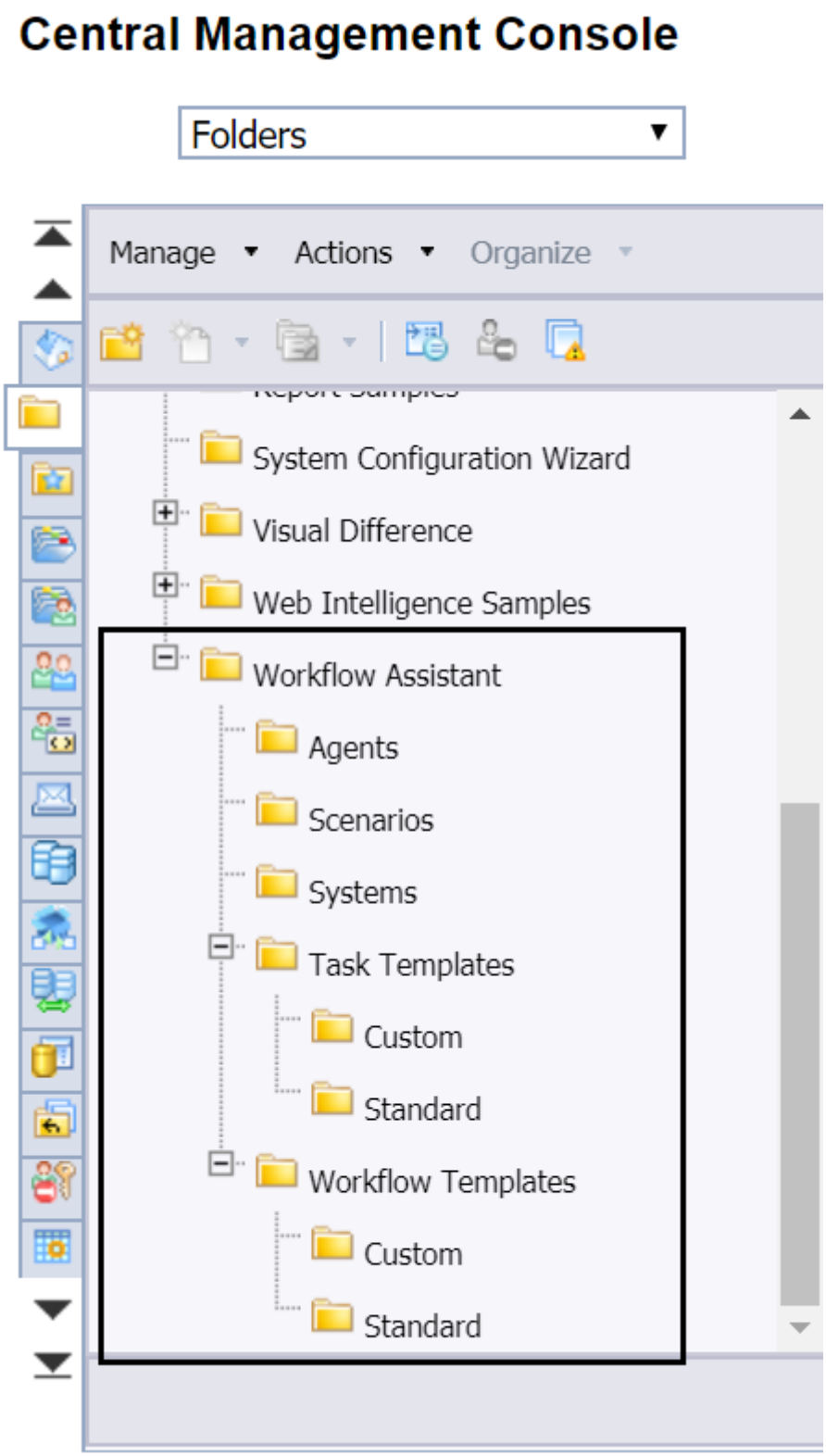
Puede administrar la seguridad del asistente de workflow mediante la Consola de administración central.

El *asistente de workflow* aparece entre las *Aplicaciones* de la *Consola de administración central*.




Puede visualizar y administrar los derechos de acceso y las opciones de seguridad globales para las siguientes entidades en el asistente de workflow:

- Sistemas
- Escenarios
- Plantillas de tarea
- Plantillas de workflow




Para obtener información sobre cómo gestionar las opciones de seguridad de los objetos de la CMC, consulte el tema Gestión de las opciones de seguridad de objetos de la CMC.

> **Nota**
>
> - Puede controlar el acceso a una funcionalidad del asistente de workflow como *Sistemas*, *Escenarios*, *Plantillas de tarea* y *Plantillas de workflow* asignando derechos en el nivel de carpeta u objeto al usuario, aunque la falta de derechos no afecta a la interfaz de usuario. Esto significa que un usuario debe tener el derecho *Añadir objetos a esta carpeta* en la carpeta *Escenario* para crear un escenario.
> - Por ejemplo, el usuario puede ver una opción para crear un escenario en el asistente de workflow incluso aunque no tenga derechos para la carpeta *Escenario* de la CMC. Si aun así el usuario intenta crear y guardar un escenario en la carpeta *Escenario*, el sistema mostrará un mensaje de error.

## Gestión de derechos de aplicación

Con los derechos específicos de aplicación adecuados, puede rechazar o realizar las siguientes tareas en el asistente de workflow:

- Para rechazar *Crear plantilla de tarea*, vaya a la carpeta Plantilla de tarea y rechace *Añadir objetos a la carpeta*.
- Para rechazar *Crear plantilla de workflow*, vaya a la carpeta Plantilla de workflow y rechace *Añadir objetos a la carpeta*.
- Para rechazar *Crear escenario*, vaya a la carpeta Escenario y rechace *Añadir objetos a la carpeta*.
- Para rechazar *Editar plantilla de tarea*, vaya a la carpeta Plantilla de tarea y rechace *Editar objetos*.
- Para rechazar *Editar plantilla de tarea que posee el usuario*, vaya a la carpeta Plantilla de tarea y rechace *Editar objetos que posee el usuario*.
- Para rechazar *Editar plantilla de workflow*, vaya a la carpeta Plantilla de workflow y rechace *Editar objetos*.
- Para rechazar *Editar plantilla de workflow que posee el usuario*, vaya a la carpeta Plantilla de workflow y rechace *Editar objetos que posee el usuario*.
- Para rechazar *Editar escenario*, vaya a la carpeta Escenario y rechace *Editar objetos*.
- Para rechazar *Editar escenario que posee el usuario*, vaya a la carpeta Escenario y rechace *Editar objetos que posee el usuario*.
- Para rechazar *Ver plantilla de tarea*, vaya a la carpeta Plantilla de tarea y rechace *Ver objetos*.
- Para rechazar *Ver plantilla de tarea que posee el usuario*, vaya a la carpeta Plantilla de tarea y rechace *Ver objetos que posee el usuario*.
- Para rechazar *Ver plantilla de workflow*, vaya a la carpeta Plantilla de workflow y rechace *Ver objetos*.
- Para rechazar *Ver plantilla de workflow que posee el usuario*, vaya a la carpeta Plantilla de workflow y rechace *Ver objetos que posee el usuario*.
- Para rechazar *Ver escenario*, vaya a la carpeta Escenario y rechace *Ver objetos*.
- Para rechazar *Ver escenario que posee el usuario*, vaya a la carpeta Escenario y rechace *Ver objetos que posee el usuario*.
- Para rechazar *Borrar plantilla de tarea*, vaya a la carpeta Plantilla de tarea y rechace *Borrar objetos*.
- Para rechazar *Borrar plantilla de tarea que posee el usuario*, vaya a la carpeta Plantilla de tarea y rechace *Borrar objetos que posee el usuario*.
- Para rechazar *Borrar plantilla de workflow*, vaya a la carpeta Plantilla de workflow y rechace *Borrar objetos*.
- Para rechazar *Borrar plantilla de workflow que posee el usuario*, vaya a la carpeta Plantilla de workflow y rechace *Borrar objetos que posee el usuario*.

- Para rechazar *Borrar escenario*, vaya a la carpeta Escenario y rechace *Borrar objetos*.
- Para rechazar *Borrar escenario que posee el usuario*, vaya a la carpeta Escenario y rechace *Borrar objetos que posee el usuario*.
- Para rechazar *Ejecutar escenario para todas las combinaciones*, vaya al escenario indicado y rechace *Añadir objetos a la carpeta*.
- Para rechazar *Ejecutar escenario que posee el usuario para todas las combinaciones*, vaya al escenario indicado y rechace *Añadir objetos a la carpeta que posee el usuario*.
- Para rechazar *Crear infraestructura*, vaya a la carpeta Infraestructura y rechace *Añadir objetos a la carpeta*.
- Para rechazar *Editar y ver infraestructura*, vaya a la carpeta Infraestructura y rechace *Editar objetos* y *Ver objetos*.
- Para rechazar *Borrar infraestructura*, vaya a la carpeta Infraestructura y rechace *Borrar objetos*.
- Para rechazar *Añadir credenciales de usuario en infraestructura*, vaya a la carpeta Infraestructura y rechace *Añadir objetos a la carpeta*.

> **Nota**
>
> Todos los derechos mencionados arriba se pueden aplicar de forma individual a la plantilla de tarea / la plantilla de workflow / el escenario.

## 22.7 Trabajar con el asistente de workflow

El asistente de workflow es una aplicación de la CMC que permite automatizar las tareas de administración de BI repetitivas y complejas. En las siguientes secciones, aprenderá a automatizar las tareas de administración de BI.

### 22.7.1 Acerca de las plantillas para tareas estándar

Las plantillas para tareas estándar se suministran integradas (listas para usar) con el asistente de workflow. Al crear escenarios o plantillas de workflow, puede utilizar estas plantillas de tarea.

| Plantilla para tarea estándar | Descripción |
|---|---|
| *Iniciar sesión* | Establece una sesión con el servidor de la plataforma de BI de destino. |
| *Actualizar documentos* | Abre y actualiza la lista de documentos proporcionados a través de la operación `<Programar ahora>`.<br>**Nota**<br>Para documentos con peticiones, los valores predefinidos deben indicarse en los documentos antes de la ejecución. |

| Plantilla para tarea estándar | Descripción |
| --- | --- |
| *Cambiar origen de Web Intelligence* | Cambia la asignación del universo de origen para su lista de documentos de .unv a .unx, de .unx a .unx o de .unv a .bex. |
| *Añadir/Eliminar usuario y grupo de usuarios* | Añade o elimina usuarios y grupos de usuarios a la infraestructura de BI.<br>**Nota**<br>Esta plantilla de tarea corresponde a la `<funcionalidad Importar>` de la plataforma de BI. Para obtener información sobre la funcionalidad Importar, consulte el tema Para añadir usuarios o grupos de usuarios en masa. |
| *Obtener propiedades* | Devuelve los valores de determinadas propiedades para los InfoObjetos consultados. |
| *Definir propiedades* | Fija los valores de determinadas propiedades para los InfoObjetos indicados en la CMS. |
| *Leer pool de trabajo* | Lee los archivos .CSV como entrada y devuelve los valores separados por comas que pueden consumir las tareas siguientes. Utilice esta plantilla de tarea cuando las plantillas de workflow deban consumir un gran número de valores (datos en masa) en el escenario y no sea factible que los valores se introduzcan manualmente mediante el panel de entrada del asistente de workflow. |
| *Consultar pool de trabajo* | Consulta las tablas de CMS e indica la salida en formato CSV. |
| *Guardar salida* | Guarda los valores obtenidos del *Parámetro de salida* de una tarea en un archivo CSV del CMS. |
| *Establecer propiedades del servidor* | Fija los valores de determinadas propiedades para los servidores indicados |
| *Cerrar sesión* | Finaliza la sesión de la tarea con el servidor de la plataforma de BI de destino. |

## 22.7.1.1 Iniciar sesión

## Parámetros para la plantilla de la tarea de inicio de sesión

Parámetros de entrada

| Nombre | Tipo | Descripción |
|---|---|---|
| Sistema | Cadena | Nombre de la infraestructura registrada en el asistente de workflow |

# 22.7.1.2 Actualizar documentos

## Parámetros para actualizar documentos

Parámetro de entrada

| Nombre | Tipo | Descripción |
|---|---|---|
| *Documentos | CSV | Identificadores de documentos (ID/CUID) para documentos que deben actualizarse. Un usuario también puede seleccionar documentos del Explorador de repositorio mediante la ayuda para entradas.<br>Formato CSV: ID o CUID |

Parámetros de salida

| Nombre | Tipo | Descripción |
|---|---|---|
| SuccessfullyRefreshedDocuments | CSV | Documentos que se han actualizado correctamente.<br>Formato CSV: ID, CUID |
| UnsuccessfullyRefreshedDocuments | CSV | Documentos que no se han actualizado correctamente.<br>Formato CSV: ID, CUID |
| Todos | CSV | Lista de documentos procesados.<br>Formato CSV: ID, CUID |

# 22.7.1.3 Cambiar origen de Web Intelligence

## Parámetros para modificar el origen de Web Intelligence

Parámetros de entrada

| Nombre | Tipo | Descripción |
|---|---|---|
| *Documento | CSV | Indique el CUID del documento de Web Intelligence para el que desea sustituir UNV por UNX, UNX por UNX o UNV por BEx. Un usuario también puede seleccionar documentos desde el Repository Explorer mediante la ayuda para entradas o asignando una salida de una tarea a otra.<br>Formato CSV: ID o CUID |
| *UniverseMapping | CSV | Asignación de universos (UNV, UNX, BEx) basados en ID o CUID. Un usuario también puede asignar los universos mediante la pantalla Asignación de universos en la ayuda para entradas.<br>Formato CSV (para UNV-UNX): unv_cuid, unx_cuid o unv_id, unx_id<br>Formato CSV (para UNX-UNX): src_cuid,dest_cuid,type<br>Formato CSV (para UNV-BEx): src_cuid,dest_cuid,type,technical_name |
| Acción de documento | Cadena | Para modificar la fuente sin guardar el documento, asigne el valor: "Test"<br>Para modificar la fuente y guardar el documento, asigne el valor: "Change" |

Parámetros de salida

| Nombre | Tipo | Descripción |
|---|---|---|
| Éxito | CSV | Documentos para los que la fuente se ha modificado correctamente.<br>Formato CSV: ID, CUID |

| Nombre | Tipo | Descripción |
| --- | --- | --- |
| Error | CSV | Documentos para los que la fuente no se ha podido modificar.<br>Formato CSV: ID, CUID |
| Todos | CSV | Lista de documentos de entrada.<br>Formato CSV: ID, CUID |

**Restricción**

- Solo el .UNV creado en la consulta .BEx puede sustituirse por otra consulta .BEx.
- No se admiten consultas BEx con peticiones.
- La asignación solo tiene lugar cuando los objetos de universo tienen un tipo similar y el nombre más próximo con los objetos de consulta BEx.
- Los objetos de universo creados con etiquetas no se asignan.

## 22.7.1.4 Añadir/Eliminar usuario y grupo de usuarios

### Parámetros para añadir/eliminar usuario y grupo de usuarios

Parámetros de entrada

| Nombre | Tipo | Descripción |
| --- | --- | --- |
| *Datos | CSV | Información específica del usuario.<br>Consulte los siguientes datos CSV de muestra. Para obtener más información sobre los datos CSV, consulte el tema *Para añadir usuarios o grupos de usuarios en masa* en el *Manual del administrador de la plataforma de Business Intelligence*.<br>`command,group,user,fullname,password,mail,profileName,profileValue`<br>`Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue` |

> **Nota**
>
> También puede crear un archivo CSV sin una cabecera CSV y utilizarlo como entrada para el escenario.
>
> La contraseña seleccionada en el archivo CSV debe cumplir con la política de contraseñas.

> **→ Sugerencias**
>
> Puede utilizar comas consecutivas para omitir un campo de entrada.

## 22.7.1.5 Obtener propiedades

### Parámetros para obtener propiedades

Parámetros de entrada

| Nombre | Tipo | Descripción |
|---|---|---|
| *InfoObjeto | CSV | Valores CSV para InfoObjetos. El prefijo "si_" no se debe indicar para utilizar las propiedades.<br>Formato CSV: ID o CUID |
| *Propiedad | CSV | Valores CSV de propiedades. El prefijo "si_" no se debe indicar para utilizar las propiedades.<br>Para los InfoObjetos de un usuario, la propiedad permitida es "property;data". |

Parámetros de salida

| Nombre | Tipo | Descripción |
|---|---|---|
| Éxito | CSV | Lista de InfoObjetos para los que el valor de propiedad se ha buscado o asignado correctamente.<br>Formato CSV: ID o <propiedad buscada> |
| Error | CSV | Lista de InfoObjetos para los que el valor de propiedad no se ha buscado o asignado correctamente.<br>Formato CSV: ID, CUID |

| Nombre | Tipo | Descripción |
| --- | --- | --- |
| Todos | CSV | Lista de todos los InfoObjetos procesados.<br>Formato CSV: ID, CUID |

## 22.7.1.6 Definir propiedades

### Parámetros para definir propiedades

Parámetros de entrada

| Nombre | Tipo | Descripción |
| --- | --- | --- |
| *InfoObjeto | CSV | Valores CSV para InfoObjetos. El prefijo "si_" no se debe indicar para utilizar las propiedades.<br>Formato CSV: ID o CUID |
| *Propiedad | CSV | Valores CSV de propiedades.<br>Para los InfoObjetos de un usuario, la propiedad permitida es "property;data". |

Parámetros de salida

| Nombre | Tipo | Descripción |
| --- | --- | --- |
| Éxito | CSV | Lista de InfoObjetos para los que el valor de propiedad se ha obtenido o definido correctamente.<br>Formato CSV: ID o <propiedad buscada> |
| Error | CSV | Lista de InfoObjetos para los que el valor de propiedad no se ha obtenido o definido correctamente.<br>Formato CSV: ID, CUID |
| Todos | CSV | Lista de todos los InfoObjetos procesados.<br>Formato CSV: ID, CUID |

## 22.7.1.7 Establecer propiedades del servidor

### Parámetros para establecer las propiedades del servidor

Parámetros de entrada

| Nombre | Tipo | Descripción |
|---|---|---|
| *Servidor | CSV | Identificadores (ID/CUID) para servidores que deben modificarse. Un usuario también puede seleccionar servidores del Explorador de repositorio mediante la ayuda para entradas.<br>Formato CSV: ID o CUID |
| *Propiedad | CSV | Valores CSV con propiedad y valor. Por ejemplo: `hostname;new value`.<br>Propiedades admitidas: Nombre de host |

Parámetros de salida

| Nombre | Tipo | Descripción |
|---|---|---|
| Éxito | CSV | Lista de servidores para los que el valor de propiedad se ha definido correctamente.<br>Formato CSV: ID |
| Error | CSV | Lista de servidores para los que el valor de propiedad no se ha definido correctamente.<br>Formato CSV: ID |
| Todos | CSV | Lista de todos los servidores procesados.<br>Formato CSV: ID |

## 22.7.1.8 Leer pool de trabajo

## Parámetros para leer pool de trabajo

Parámetros de entrada

| Nombre | Tipo | Descripción |
|---|---|---|
| *Archivo | CSV | Archivo CSV con los datos necesarios para la lectura. Un usuario también puede seleccionar un archivo CSV del Explorador de repositorio mediante la ayuda para entradas.<br><br>Formato CSV: <Cabecera1>, <Cabecera2>, ..<CabeceraN><br><br>**Nota**<br>Para conocer mejor los formatos de datos y los delimitadores en CSV, consulte Trabajar con datos CSV [página 879]. |

Parámetros de salida

| Nombre | Tipo | Descripción |
|---|---|---|
| Valores | CSV | La lista de valores leídos del archivo de entrada y que se devuelven en formato separado por comas. |

# 22.7.1.9 Guardar salida

## Parámetros para la tarea guardar salida

Parámetros de entrada

| Nombre | Tipo | Descripción |
|---|---|---|
| *Parámetro | CSV | Asigna la salida obtenida con la tarea anterior. |
| *Nombre del archivo | Cadena | Especifica el nombre de archivo donde se guardará la salida. |
| *Seleccionar carpeta de destino | Cadena | Seleccione la carpeta donde se debe guardar el archivo. |

| Nombre | Tipo | Descripción |
|---|---|---|
| *Opciones de guardado | Cadena | Para sobrescribir un archivo que existe con el mismo nombre, seleccione el valor: *Sobrescribir*.<br>Para cambiar el nombre de un archivo que tenga el mismo nombre con el sufijo _1, _2... seleccione el valor: *Cambiar nombre*. |

> **Nota**
>
> **Parámetro de salida:**
>
> La salida obtenida es un archivo en CMS. De ahí que no haya ningún parámetro disponible para el consumo.

## 22.7.1.10 Cerrar sesión

### Parámetros para tarea de salida de sesión

Parámetro de entrada

| Nombre | Tipo | Descripción |
|---|---|---|
| Token de sesión | Cadena | Token de sesión (generado a causa de la entrada al sistema) |

## 22.7.2 Acerca de las plantillas de workflow estándar

Las plantillas para workflow estándar se suministran integradas (listas para usar) con el asistente de workflow. Al crear escenarios, puede utilizar estas plantillas de workflow.

Plantillas de workflow estándar disponibles en el asistente de workflow

| Nombre de plantilla | Descripción |
|---|---|
| Inicio de sesión | Establece una sesión con el servidor de la plataforma de BI de destino. |
| Actualizar documentos | Actualiza la lista indicada de documentos de Web Intelligence. |

| Nombre de plantilla | Descripción |
|---|---|
| Cambiar propiedad del documento | Consulta el propietario del documento y asigna el mismo propietario a otro documento. |
| Cambiar tipo de licencia de usuario | Consulta la lista de usuarios a partir de condiciones específicas de usuario y modifica el tipo de licencia. |
| Cambiar origen de Web Intelligence y verificar los documentos | Modifica la asignación del universo de origen de .unv a .unx, .unx a .unx o .unv a .bex y valida los documentos para documentos de Web Intelligence en masa. |
| Agregar/Eliminar usuarios | Permite que un administrador añada o elimine usuarios y grupos. |
| Cerrar sesión | Finaliza la sesión de la tarea con el servidor de la plataforma de BI de destino. |

## 22.7.3 Acerca de las plantillas para tareas personalizadas

Puede utilizar las plantillas de tarea estándar del asistente de workflow para diseñar plantillas de workflow y ejecutar escenarios. Si las plantillas estándar no son suficientes para cubrir sus necesidades, puede desarrollar una plantilla de tarea propia y un complemento para el asistente de workflow.

Cree su propia plantilla de tarea personalizada con el SDK de plantilla de tarea personalizado que proporciona una API para que los desarrolladores implementen plantillas nuevas de tarea. Para obtener más información, consulte Cómo crear una plantilla de tarea personalizada en el Framework de automatización de BI.

## 22.7.4 Gestión de plantillas de workflow

Puede crear, editar y borrar plantillas de workflow personalizadas del asistente de workflow.

### 22.7.4.1 Creación de plantillas de workflow personalizadas

Las plantillas de workflow personalizadas se crean con plantillas de tarea estándar o personalizadas.

1. En la página de inicio, seleccione *Asistente de workflow* .
2. En la página *Asistente de workflow*, seleccione la ficha *Plantillas de workflow*.
3. Elija el icono + (*Añadir*) en la parte superior derecha de las *Plantillas de workflow*.
4. En la zona de diseño *Crear plantilla de workflow*, seleccione el icono > (*Expandir*) que aparece delante de las categorías *Estándar* y *Personalizada* de las plantillas de tarea del panel izquierdo.

5. Arrastre y suelte las plantillas de tarea necesarias en el área de diseño de la derecha de la página.
6. Cambie el nombre de la plantilla de tarea que ha soltado en la zona de diseño.
7. (Opcional) Seleccione el icono (*Enlace*) que aparece entre dos plantillas de tarea y seleccione el valor necesario para los parámetros condicionales en la lista que aparece.

   Aquí, también puede insertar el `<Retraso temporal>` requerido (en segundos).
8. (Opcional) Defina valores para los parámetros de entrada, se utilizarán como valores predefinidos cuando la plantilla de workflow se utilice en un escenario.
9. Seleccione *Guardar*.
10. En el diálogo *Guardar plantilla de workflow*, introduzca un nombre (obligatorio) para su plantilla de workflow y, si es necesario, añada una descripción.
11. Seleccione *Guardar* en el diálogo *Guardar plantilla de workflow*.

    La nueva plantilla de workflow inicia el listado en la vista *Plantillas de workflow* del asistente de workflow.

    > **Nota**
    >
    > Las modificaciones de las plantillas de workflow existentes no afectan a los escenarios existentes.

## 22.7.4.2 Edición de plantillas de workflow personalizadas

Las plantillas de workflow personalizadas se editan en el asistente de workflow.

1. En la ficha *Plantillas de workflow* del asistente de workflow, seleccione (*Más*) y luego *Editar*.
2. En la pantalla *Editar plantilla de workflow*, realice las modificaciones necesarias en la plantilla de workflow añadiendo/eliminando las plantillas de tarea, modificando los valores de los parámetro de entrada o modificando los parámetros condicionales entre plantillas de tarea.
3. Seleccione *Guardar como*.
4. En el diálogo *Guardar plantilla de workflow*, realice las modificaciones que necesite en la plantilla de workflow.
5. Seleccione *Guardar*.

   Las modificaciones de la plantilla de workflow se guardan y vuelve a la página de inicio del asistente de workflow.

## 22.7.4.3 Borrado de plantillas de workflow personalizadas

Las plantillas de workflow personalizadas se borran en el asistente de workflow.

1. En la ficha *Plantillas de workflow* del asistente de workflow, seleccione (*Más*) y luego *Borrar*.
2. Seleccione *Borrar* en la advertencia que aparece.

   La plantilla de workflow borrada ya no aparece en la lista de la ficha *Plantillas de workflow* del asistente de workflow.

## 22.7.5 Gestión de escenarios y visualización de resultados

Los escenarios se crean conectando plantillas de tarea y plantillas de workflow. En el asistente de workflow se gestionan escenarios y se ven resultados.

### 22.7.5.1 Crear escenarios

Este tema explica cómo puede crear escenarios en el asistente de workflow.

1. En la página de inicio de la CMC, seleccione *Asistente de workflow*.

   Los escenarios disponibles se detallan en la página que aparece.
2. Haga clic en el icono + (*Crear carpeta o escenario*) y seleccione *Escenario*.
3. En la página *Crear escenario*, seleccione el icono > (*Expandir*) que aparece delante de las categorías *Estándar* y *Personalizado* de las plantillas de tarea en el panel izquierdo.

   > ⓘ Nota
   >
   > Puede consultar la descripción de la tarea pasando el ratón por encima del nombre de la plantilla de tarea.
4. Arrastre y suelte las plantillas de workflow necesarias en el área de diseño de la derecha de la página.
5. (Opcional) Seleccione el icono (*Enlace*) que aparece entre dos plantillas de tarea y seleccione el valor necesario para los parámetros condicionales en la lista que aparece.

   Aquí, también puede insertar el `<Retraso temporal>` requerido (en segundos).
6. Haga clic en una plantilla de workflow en el área de diseño.

   Aparece el panel de entrada a la derecha del área de diseño.
7. En el panel de entrada de la derecha, seleccione > (*Expandir*) para ver los campos de parámetro de entrada para cada plantilla de tarea y realizar las selecciones de valor necesarias en los campos.

   > ⚠ Precaución
   >
   > - Asegúrese de que ninguno de los valores de entrada que indique para los parámetros de la plantilla incluya sus datos personales y cumpla con las directrices del Reglamento General de Protección de Datos (GDPR). Para obtener más información del GDPR, consulte el tema Protección de datos y privacidad [página 178].

   > ⓘ Nota
   >
   > Encontrará más información de los parámetros en la información del parámetro. Para obtener más información sobre la info de parámetro, consulte Acerca de la información de parámetro [página 880].
8. Seleccione *Guardar*.

   > → Recuerde
   >
   > Es obligatorio especificar entradas para cada plantilla de tarea en un escenario antes de ejecutar un escenario. Sin embargo, también puede utilizar la opción *Ejecutar con parámetro* para especificar las entradas.

9. En el cuadro de diálogo *Guardar escenario*, proporcione la información necesaria en las fichas *Guardar escenario* y *Notificar por correo electrónico*.
   a. En la ficha *Guardar escenario*, introduzca un nombre (obligatorio) para el escenario, añada una descripción y seleccione una ubicación en la que se guardará el escenario.
   b. En la ficha *Notificar por correo electrónico*, seleccione el pulsador de conmutación para activarla. Se visualizan las opciones, tal como se muestra en la imagen

      Only On ☐ Success ☐ Partial Success ☐ Failure

      siguiente.
   c. Seleccione una o más opciones. La selección será el criterio que se aplicará para lanzar una notificación por correo electrónico.
   d. Puede *Utilizar la configuración estándar* o desactivarla con el pulsador de conmutación. Estas opciones predeterminadas se definen en la CMC. Consulte el *Manual del administrador de Business Intelligence* para aprender a definir las opciones predeterminadas para los destinos de correo electrónico.
   e. Si desmarca *Utilizar la configuración estándar*, indique *De, A*, *CC* (opcional), y dirección de correo electrónico *BCC* (opcional), *Asunto*y *Mensaje*. También puede añadir los marcadores de posición a cada campo.
10. Seleccione *Guardar* o *Guardar y ejecutar*.

    El escenario nuevo se incluye en la vista *Escenarios* del *asistente de workflow* y en función de los criterios seleccionados en la ficha *Notificar por correo electrónico*, se enviará el correo electrónico.

## 22.7.5.1.1 Proporcionar parámetros de entrada

Al crear modelos de workflow en el *asistente de workflow*, puede añadir valores de entrada durante el tiempo de diseño y el tiempo de ejecución. Esto significa que puede añadir los valores de entrada al crear y ejecutar un escenario. Hay dos maneras de añadir valores de entrada a un *escenario*:

1. Ayuda para entradas
2. Asignación de la salida de una tarea como entrada de otra tarea

### Ayuda para entradas

Puede seleccionar un objeto como documento y pool de trabajo en el explorador del repositorio con la *ayuda para entradas*. Por ejemplo, en un escenario para actualizar el documento, puede seleccionar un documento seleccionando el icono *Ayuda para entradas* en el campo *Documentos*.

### Asignación de la salida de una tarea como entrada de otra tarea

Puede proporcionar la salida de la primera tarea como la entrada para la segunda tarea al ejecutar un escenario. Tiene que escribir @ en un campo de entrada para ver la lista de valores obtenida de la primera tarea.

- El formato de un valor de entrada es **@<WorkflowTemplate>.<TaskTemplate>.<OutputParameter>**.
- La lista de valores de entrada muestra solo los valores compatibles obtenidos de la primera tarea. Si el campo de entrada acepta CSV como el tipo de datos, por ejemplo, se visualizan los valores de entrada de la tarea anterior que se encuentran en formato CSV.

> **Nota**
>
> Los parámetros de entrada soportan el fichero CSV como entrada. Para obtener más información, consulte Trabajar con datos CSV [página 879].

## 22.7.5.1.2 Trabajar con datos CSV

La mayoría de las plantillas de tarea estándar admiten valores de parámetro de entrada en formato CSV. Por ejemplo, la plantilla de tarea *Actualización de documento* admite el formato CSV para el campo de entrada *Documentos*. Esto significa que puede seleccionar un archivo CSV formado por datos con el formato **nombre, CUID y estado** como entrada para *Documentos*.

> **Nota**
>
> Si el campo de entrada de tarea acepta **CUid** y selecciona un archivo CSV que contiene otros parámetros, incluido **CUId**, el campo de entrada solo consume los valores de la columna **CUID** del archivo CSV. Para ver un ejemplo, consulte los datos CSV siguientes:
>
> nombre, CUID, estado;
>
> Elaboración de gráficos, AW4AVT1AUhVAogA6P7OQv9c, éxito;
>
> Informe de ventas, BW3AVT1AUhVAogA743QCDsD, éxito;
>
> En este ejemplo, el campo de entrada consume AW4AVT1AUhVAogA6P7P7OQv9c y BW3AVT1AUhVAogA743QCDsD e ignora los demás valores.

### Delimitador de columna y de fila

El delimitador de columna admitido es **,**. El delimitador de fila es **;**. Una columna y un delimitador de fila en un campo de entrada separan los datos en formato de columna y de fila. Para ver un ejemplo, consulte los datos CSV siguientes:

nombre, CUID, estado;

Elaboración de gráficos, AW4AVT1AUhVAogA6P7OQv9c, éxito;

Informe de ventas, BW3AVT1AUhVAogA743QCDsD, éxito;

Aquí, la coma significa que **nombre, CUID y estado** son columnas, mientras que el punto y coma indica el fin de la fila.

> **Nota**
>
> Si un archivo CSV es una entrada para la plantilla de tarea *Leer pool de trabajo*, el delimitador de columna es **,**. El delimitador de fila es **;** o una línea nueva.

> **Precaución**
>
> Un valor de los datos CSV no puede contener una coma o un punto y coma.

## 22.7.5.1.3 Acerca de la información de parámetro

Puede ver la información de parámetro tras expandir y seleccionar cualquiera de los parámetros del panel de entrada de un escenario. Por ejemplo, en la plantilla de tarea Actualizar documentos, hay un campo de entrada Documentos. Al seleccionar el campo de entrada de documento, se visualiza la información de parámetro.

La información de parámetro se compone de dos secciones:

1. Parámetro de entrada
2. Parámetro de salida

### Parámetro de entrada

El parámetro de entrada explica el tipo de entrada necesario para el campo seleccionado. Es específico del campo de entrada dentro de la plantilla de tarea.

### Parámetros de salida

Los parámetros de salida explican los distintos resultados obtenidos de la tarea. Son específicos de toda la tarea y no solo de un solo campo de entrada.

## 22.7.5.2 Edición de escenarios

Los escenarios se editan en el asistente de workflow.

1. En la ficha *Escenarios* del asistente de workflow, seleccione (*Más*) y luego *Editar*.

   Aparece la pantalla "Editar escenario".
2. En la pantalla *Editar escenario* realice las modificaciones necesarias en el escenario añadiendo/eliminando las plantillas de tarea/workflow o modificando los valores de los parámetros de entrada de las plantillas.

3. Seleccione *Guardar*.

   Aparece el diálogo "Guardar escenario".
4. En el diálogo *Guardar escenario*, modifique el nombre del escenario según sea necesario y seleccione *Guardar*.

   Se guardan las modificaciones del escenario y vuelve a la página de inicio del asistente de workflow.

## 22.7.5.3 Borrado de escenarios

Los escenarios se borran en el asistente de workflow.

1. En la ficha *Escenarios* del asistente de workflow, seleccione ⋯ (*Más*) y luego *Borrar*.
2. Seleccione *Borrar* en la advertencia que aparece.

   La escenario borrado ya no aparece en la lista de la ficha *Escenarios* del asistente de workflow.

## 22.7.5.4 Ejecución de escenarios y visualización de resultados

Los escenarios se ejecutan en datos BI y los resultados se ven en el asistente de workflow.

1. En la vista *Escenarios* del asistente de workflow, seleccione ⋯ (*Más*) y seleccione *Ejecutar* o *Ejecutar con parámetro*.

   *Ejecutar con parámetro* abre un diálogo que muestra todos los parámetros de entrada del escenario donde puede modificar valores o definir valores que falten.

   > **Nota**
   >
   > Los valores definidos en este diálogo de parámetros no se guardan con el escenario, solo se utilizan para la instancia en ejecución.

   El escenario (mosaico o elemento de lista) empieza a visualizar el nuevo estado como En ejecución o Pendiente. Una vez finalizada la ejecución, el estado se actualiza para visualizar el valor relevante (`<Éxito/Éxito parcial/Error/Pendiente/Error/En ejecución con error>`).
2. Para ver los resultados del escenario (mientras se ejecuta o tras ejecutarse correctamente), seleccione ⋯ (*Más*) y *Ver resultados*.

   > **Nota**
   >
   > Seleccione la opción Ver historial para verificar los resultados de las ejecuciones anteriores de un escenario.
3. En la página *Resultados*, expanda los resultados para ver los detalles de ejecución y finalización de cada plantilla de flujo de trabajo y plantilla de tarea del escenario. Una vez que haya visualizado los resultados, puede volver a la pantalla principal con el botón < (*Atrás*).

> **Nota**
>
> Seleccione la opción Exportar para guardar los resultados del escenario en formato PDF.

> **Nota**
>
> 1. Establezca un tiempo máximo para que una tarea responda a un agente añadiendo el tiempo (en segundos) con el valor clave task_time_out en el archivo wfmanager_conf.properties. Por defecto, el valor clave task_time_out está fijado en 86400, es decir, un día.
>
> 2. El valor task_time_out está fijado para todos los agentes en el asistente de workflow.

### 22.7.5.5 Detener escenarios

Puede detener un escenario mientras la ejecución de la tarea esté en curso.

**Requisitos previos:**

Puede continuar con los pasos siguientes solo cuando un escenario tiene el estado En ejecución o Pendiente.

- En la vista Escenarios, seleccione *Más* del escenario.
- Seleccione Detener.

> **Nota**
>
> La opción Detener no detiene el escenario de forma inmediata. Tras marcar la opción Detener, finaliza la tarea que se está ejecutando actualmente y, a continuación, se detiene el escenario. Es decir, solo se quedan sin ejecutar las tareas pendientes del escenario.

## 22.7.6 Comprensión de los estados de las plantillas de tarea, plantillas de workflow y escenarios

Posibles estados de artefacto (plantilla de tarea/plantilla de workflow/escenario) con descripciones

| Estado | Descripción |
|---|---|
| Creado (C) | Cuando se crea un artefacto, pero aún no se ha ejecutado ni una vez. |
| Pendiente (P) | Cuando se lanza un artefacto para la ejecución y está en cola para ejecutarse. |
| En ejecución (R) | Cuando se ejecuta un artefacto. |

| Estado | Descripción |
| --- | --- |
| Éxito (S) | Cuando todos los elementos procesados se ejecutan correctamente. Por ejemplo, los documentos procesados se actualizan correctamente tras la tarea Actualizar documento.<br><br>**Nota**<br>Basta con que una sola plantilla de workflow de un escenario no se ejecute correctamente, para que el escenario global no alcance el estado "Éxito". |
| Éxito parcial (PS) | Cuando solo se ejecutan con éxito algunos de los elementos procesados. Por ejemplo, cuando no se pueden actualizar algunos documentos tras la tarea Actualizar documento, el estado cambia a Éxito parcial. |
| Error (F) | Cuando ningún elemento se ejecuta correctamente. |
| Error (E) | Cuando un artefacto detecta un error o excepciones durante la ejecución. |
| En ejecución con error (RE) | Cuando un artefacto detecta un error en el servidor, pero continúa ejecutándose. |
| No ejecutado | Cuando una plantilla de tarea o de workflow de un escenario no se ejecuta a causa de la configuración de parámetros condicionales.<br><br>Por ejemplo, si el administrador decide fijar la condición `<Si correcto>` entre dos plantillas de workflow, por lo que el flujo de ejecución no llega a la siguiente plantilla de workflow si la anterior ha fallado. En este caso, las dos plantillas de workflow siguientes conservan el estado `<No ejecutado>`. |

**Nota**

Estas son las leyendas de las tablas:

- TTS: Estado de plantilla de tarea
- WFTS: Estado de la plantilla de workflow
- SS: Estado de escenario

Matriz de estado: Estado de plantillas de tarea y estado de la plantilla de workflow resultante

| TTS1 | TTS2 | TTS3 | TTS4 | TTS5 | WFTS |
| --- | --- | --- | --- | --- | --- |
| S | S | S | E | NE | E (Error) |
| S | S | S | PS | NE | PS (Éxito parcial) |
| S | S | PS | F | NE | F (Error) |
| S | PS | F | R | NE | R (En ejecución) |
| S | E | NE | NE | NE | E (Error) |

| TTS1 | TTS2 | TTS3 | TTS4 | TTS5 | WFTS |
|---|---|---|---|---|---|
| S | E | RE | NE | NE | RE (En ejecución con error) |

La siguiente matriz explica cómo el estado de cada plantilla de workflow afecta al estado global del escenario.

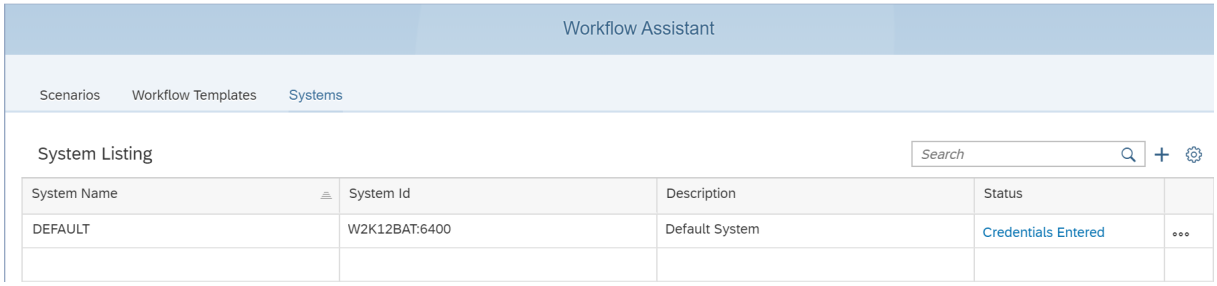
Matriz de estado: Estado de plantillas de workflow y estado del escenario resultante

| WFTS1 | WFTS2 | WFTS3 | WFTS4 | WFTS5 | SS |
|---|---|---|---|---|---|
| S | S | S | E | NE | E (Error) |
| S | S | S | PS | NE | PS (Éxito parcial) |
| S | S | PS | F | NE | F (Error) |
| S | PS | F | R | NE | R (En ejecución) |
| S | E | NE | NE | NE | E (Error) |
| S | E | RE | NE | NE | RE (En ejecución con error) |

## 22.7.7 Trabajar con sistemas

La ficha *Sistemas* le permite registrar varias infraestructuras de BI. *Sistemas* le proporciona acceso a las infraestructuras de BI registradas.

**Instantánea de la ficha** *Sistemas*




En la ficha *Sistemas* puede realizar las acciones siguientes:

- Añadir (registrar) un sistema nuevo

  > → Recuerde
  >
  > Es obligatorio registrar los sistemas en esta ficha para poder utilizarlos en otras vistas como *Escenarios* y *Plantillas de workflow*.

- Modificar (editar o borrar) un sistema existente
- Conectarse (o desconectarse) al sistema introduciendo las credenciales (`User Name, Password, Authentication`)

> **Nota**
>
> El sistema en el que ha instalado el asistente de workflow aparece en la ficha *Sistemas* como sistema "predeterminado". Sin embargo, para conectarse a esta infraestructura, debe introducir sus credenciales.

- Personalizar las columnas que se muestran en la vista Sistemas

## 22.7.7.1 Registrar sistema BI nuevo

Para conectarse al sistema BI autorizado y utilizar las funciones del asistente de workflow, es imprescindible registrar (añadir) antes los sistemas BI en el asistente de workflow.

Para registrar sistemas, siga el procedimiento que se indica a continuación:

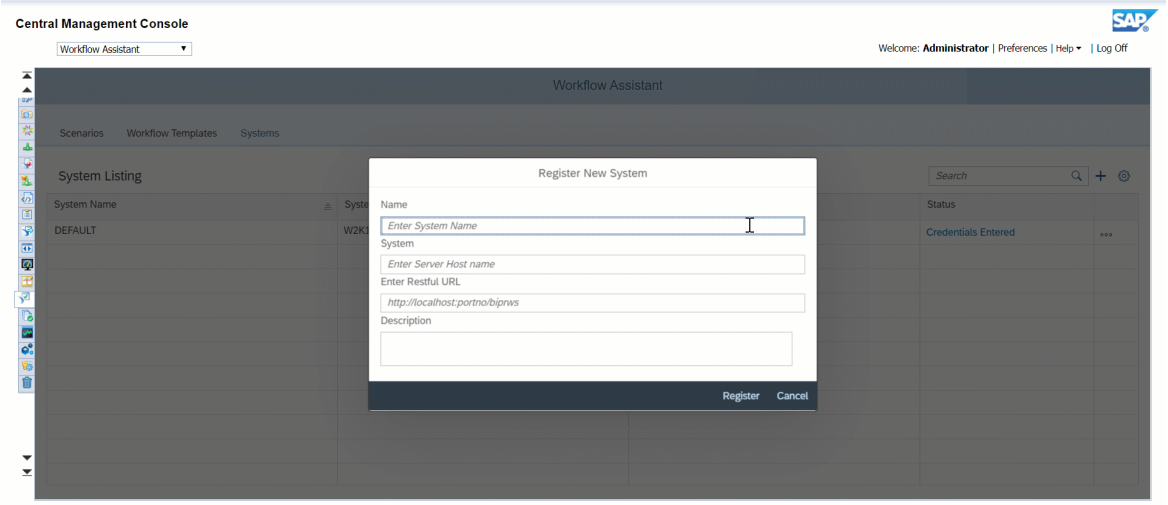
1. Inicie sesión en el asistente de workflow.
2. En la página *Inicio*, vaya a la ficha *Sistemas*.

   Esta vista detalla los sistemas registrados disponibles.
3. Seleccione el icono + (*Añadir*).

   Aparece el diálogo "Registrar sistema nuevo".
4. Para `<Nombre>`, introduzca un alias con el que identificar el sistema.
5. Para `<el Sistema>`, introduzca el nombre de host del servidor o la dirección IP que identifica el equipo o el clúster de equipos.
6. Para `<URL de RestFul>`, introduzca el URL de servicios Web RESTful para el servidor de la plataforma BI. Opcionalmente, puede añadir una `<Descripción>` para el sistema.
7. Seleccione *Registrar*.

   > **Nota**
   >
   > Puede registrar el mismo sistema BI con nombres diferentes, pero se recomienda registrar un sistema BI una sola vez en la vista Sistemas.

   El sistema registrado se añade a su lista de sistemas en la tabla Listado de sistemas.



## 22.7.7.2 Modificar sistemas BI existentes

La vista Sistemas le permite modificar los sistemas registrados.

Para modificar un sistema existente, siga el siguiente procedimiento:

1. Inicie sesión en el asistente de workflow y vaya a la ficha *Sistemas*.
2. En la vista Sistemas, seleccione (*Más*) → *Editar* para el sistema listado que desea modificar.

   Aparecerá el diálogo *Editar sistema*.
3. Modifique el `<Nombre>` (alias), el `<Sistema>`, el `<URL de RestFul>` o la `<Descripción>` según sus necesidades, y seleccione *Finalizado*.

   Las modificaciones se empiezan a reflejar en la tabla "Listado de sistema".

   > **Nota**
   >
   > Para borrar un sistema, seleccione (*Más*) → *Borrar* para el sistema listado que desee eliminar y confirme el borrado en el diálogo que aparece.

## 22.7.7.3 Conexión con los sistemas de BI registrados

Puede conectarse a sus sistemas registrados con el campo `<Estado>` que aparece en la tabla Lista de sistemas. La conexión a un sistema BI es esencial para utilizar los sistemas en los escenarios del asistente de workflow.

Para conectarse a un sistema de BI añadido, siga el siguiente procedimiento:

1. Inicie sesión en el asistente de workflow y vaya a la ficha *Sistemas*.
2. En el campo `<Estado>` de los sistemas registrados a los que aún no esté conectado, seleccione la cadena del indicador (*No se han indicado credenciales*).

   Aparece el diálogo "Introducir credenciales".
3. Introduzca sus credenciales para el sistema BI (en función de la autorización que le haya concedido el administrador de la plataforma): `<Nombre de usuario>`, `<Contraseña>` y `<Autenticación>`. A continuación, seleccione *Guardar*.

   El asistente de workflow valida las credenciales y actualiza el `<Estado>` de su infraestructura de BI a *Credenciales introducidas* si la validación es correcta. De lo contrario, se muestra un mensaje de error y el `<estado>` se conserva inalterado.

## 22.7.7.4 Personalización de la vista de sistemas

Puede personalizar el aspecto de la vista Listado de sistemas modificando la visibilidad de los campos (columnas) en la vista.

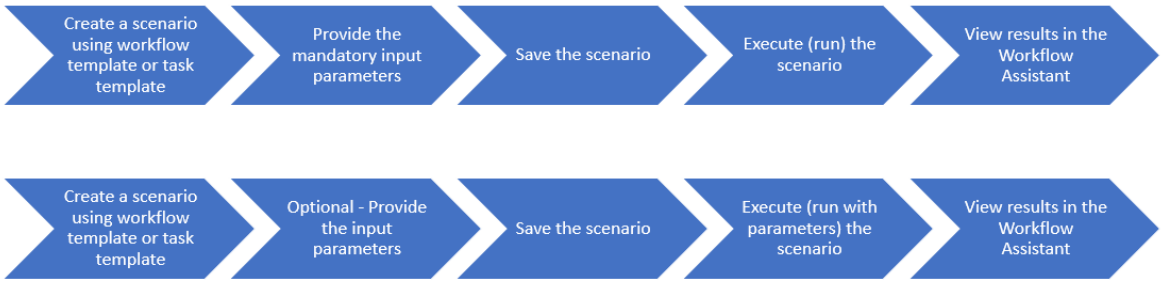
Para ocultar/mostrar columnas específicas de la vista Sistemas, proceda como sigue:

1. Inicie sesión en el asistente de workflow y vaya a la ficha *Sistemas*.
2. Seleccione (*Opciones*) y desmarque las columnas (cabeceras de campo) que quiera ocultar en la tabla Listado de sistemas.

   Las columnas desmarcadas ya no aparecerán en la tabla Listado de sistemas.
3. Para volver a incluir una columna oculta en la vista, seleccione *Opciones* y vuelva a marcar los encabezados de campo requeridos.

## 22.7.8 Flujo de proceso integral del asistente de workflow

Ver una representación visual.




# 22.8 Verificación de archivos de log

Este tema explica cómo puede verificar los archivos de log del asistente de workflow.

## Asistente de workflow

Para el asistente de workflow, debe seleccionar el nivel de trace en el archivo *WorkflowAssistant_Trace.ini* en `<INSTALLDIR>\AdminConsole\WorkflowAssistant`. Los archivos de trace también se pueden configurar con el archivo **_Trace.ini** configurando las siguientes variables de entorno:

- `BO_TRACE_CONFIGDIR`, para definir el nombre de la carpeta de archivos de configuración de registro, por ejemplo: `C:\BOTraces\config`
- `BO_TRACE_CONFIGFILE`, para definir el nombre del archivo de configuración, por ejemplo `BO_trace.ini`
- `BO_TRACE_LOGDIR`, para definir el nombre de la carpeta de registros, por ejemplo: `C:\BOTraces`

> **Nota**
>
> En el nombre del archivo `INI` se distingue entre mayúsculas y minúsculas.

Cree el archivo de configuración `BO_Trace.ini` del siguiente modo:

```
sap_log_level = log_info;
sap_trace_level = trace_debug;
```

Puede verificar los logs predeterminados en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`.

# 23 Papelera de reciclaje

## 23.1 Papelera de reciclaje

### Sobre la Papelera de reciclaje

La Papelera de reciclaje es una nueva aplicación en CMC. Cuando el usuario borra un elemento del sistema BOE, se desplaza a la Papelera de reciclaje, donde se almacena temporalmente hasta que se vacía la Papelera de reciclaje. Ello da la oportunidad al usuario de recuperar informes/carpetas borrados de forma accidental y restaurarlos a las ubicaciones originales.

Con la aplicación de Papelera de reciclaje, el administrador puede:

- Iniciar la restauración de cualquier elemento borrado (como informes y carpetas)
- Borrar permanentemente un elemento de la Papelera de reciclaje
- Realizar la limpieza automática de la Papelera de reciclaje

Si la papelera de reciclaje está habilitada, puede reciclar los siguientes tipos de InfoObjeto:

- Contenido de carpeta personal
- Eventos
- Calendarios
- Contenido de carpeta pública
- Universos
- Conexiones
- Categorías públicas
- Categorías personales
- Bandejas de entrada
- Perfiles
- Roles personalizados

### 23.1.1 Restaurar un elemento de la Papelera de reciclaje

La Pepelera de reciclaje muestra una lista de elementos borrados. Para restaurar un elemento de la Papelera de reciclaje, proceda de la forma siguiente:

1. Inicie una sesión en la CMC.
2. Desde el panel *Administrar* de la página inicial de CMC, seleccione *Papelera de reciclaje*.

3. Haga clic con el botón derecho sobre el elemento que quiera restaurar y seleccione *Restaurar* del menú contextual.
4. Seleccione *Aceptar*.

   Puede navegar a la ubicación del elemento restaurado para confirmar la operación de restauración.

   > **Nota**
   >
   > Si restaura un elemento desde la Papelera de reciclaje y ya existe otro elemento con el mismo nombre en la ubicación de restauración, el elemento se graba en ella con el nombre siguiente: "<nombre de elemento> restaurado(1, 2, ...)".
   >
   > Cuando de borra la carpeta superior de un elemento de la Papelera de reciclaje, se vuelve a crear la carpeta superior al restaurar el elemento. Sin embargo, la carpeta superior solo contiene el/los elemento(s) que se haya(n) restaurado desde la Papelera de reciclaje.
   >
   > No puede abrir/navegar desde la Papelera de reciclaje.
   >
   > Si borra un elemento de una carpeta y posteriormente el administrador restringe los derechos de modificación de esta carpeta, cuando intente restaurar el elemento de vuelta en la carpeta original, el elemento se restaurará en la carpeta original.

Ha restaurado correctamente un elemento de la Papelera de reciclaje.

## 23.1.2 Borrar permanentemente un elemento de la Papelera de reciclaje

Como administrador, tiene el derecho de borrar permanentemente elementos de la Papelera de reciclaje o de vaciarla.

Para borrar permanentemente un elemento de la Papelera de reciclaje, proceda de la forma siguiente:

1. Inicie una sesión en CMC.
2. Desde el panel *Administrar* de la página inicial de CMC, seleccione *Papelera de reciclaje*.
3. Haga clic con el botón derecho sobre el elemento que quiera borrar y seleccione *Borrar* del menú contextual.
4. Seleccione *Aceptar*.

Ha borrado correctamente un elemento de la Papelera de reciclaje.

## 23.1.3 Habilitar limpieza automática de la Papelera de reciclaje

Puede ejecutar la limpieza automática periódica de la Papelera de reciclaje.

Para habilitarla, proceda de la forma siguiente:

1. Inicie una sesión en CMC.

2. Desde el panel *Administrar* de la página inicial de CMC, seleccione *Aplicaciones*.
3. Desde la página *Aplicaciones*, seleccione la aplicación *Papelera de reciclaje*.

   Se are la ventana de diálogo *Propiedades: Papelera de reciclaje*.
4. Seleccione la ventana de diálogo Limpieza automática de archivos borrados y especifique (en días) es tiempo de espera del sistema antes de limpiar automáticamente un elemento borrado.
5. Seleccione *Guardar y cerrar*.

Ha habilitado correctamente la limpieza automática de la Papelera de reciclaje.

# 24 Auditoría

## 24.1 Introducción

La auditoría le permite conservar un registro de eventos importantes ocurridos en los servidores y aplicaciones, que proporciona una idea de la información a la que se accede, cómo se accede y modifica y quién realiza estas operaciones. Esta información se registra en una base de datos denominada Almacenamiento de datos de auditoría (ADS). Una vez que los datos se encuentren en el ADS, podrá diseñar informes personalizados en función de sus necesidades. Puede buscar universos e informes de muestra en SAP Community http://community.sap.com/.

A efectos de este capítulo, "auditor" es un sistema responsable de registrar o almacenar información de un evento y "auditado" es el sistema responsable de realizar un evento auditable. En algunas ocasiones, un solo sistema puede realizar ambas funciones.

### Cómo funcionan las auditorías

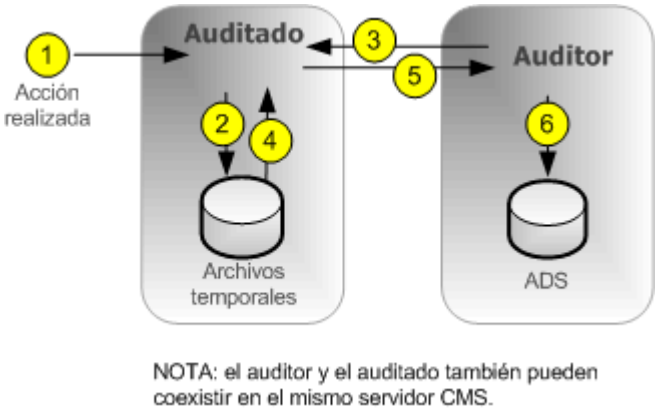
El Servidor de administración central (CMS) actúa como el sistema auditor, mientras que cada servidor o aplicación que activa un evento auditable actúa como auditado. Cuando se activa un evento auditado, el servidor responsable generará un registro y lo almacenará en un archivo temporal local. A intervalos regulares, el CMS se comunica con los auditados para solicitar estos registros y graba los datos en el ADS.

Asimismo, el CMS supervisa la sincronización de los eventos de auditoría que se producen en los distintos equipos. Cada auditado proporciona una marca de tiempo de los eventos de auditoría que registra. Para asegurarse de que las marcas de tiempo de los eventos de los distintos servidores son coherentes, el CMS envía periódicamente su hora del sistema a los auditados. A continuación, éstos la comparan con la de sus relojes internos. Si existe una diferencia, corrigen la hora registrada para los siguientes eventos de auditoría.

Según el tipo de auditado, el sistema usa uno de los siguientes flujos de trabajo para registrar los eventos.

### Auditoría del servidor

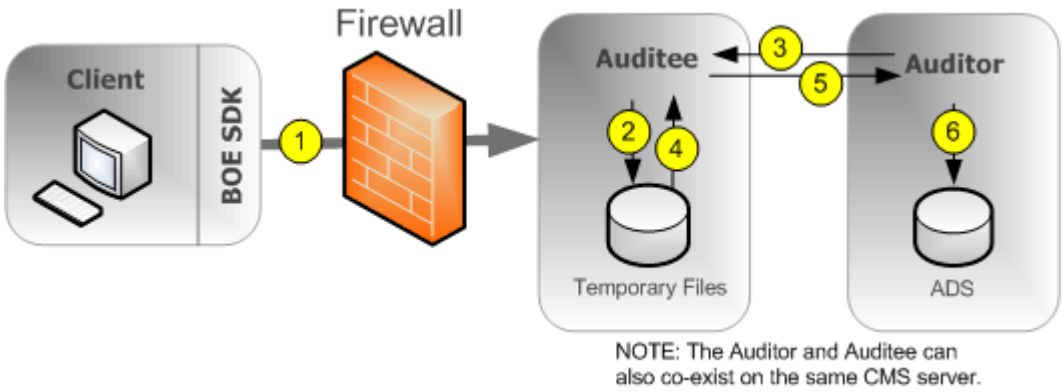
En el caso de eventos generados por el servidor, el CMS puede actuar como auditado o como auditor.




1. El servidor realiza un evento auditable.
2. El auditado escribe los eventos en un archivo temporal. Los pasos 1 y 2 pueden aparecer varias veces antes del paso 3.
3. A intervalos regulares, el auditor sondea al auditado y solicita un lote de eventos de auditoría.
4. El auditado recupera los eventos de los archivos temporales.
5. El auditado transmite los eventos al auditor.
6. El auditor graba los eventos en el ADS e indica al auditado que elimine los eventos de los archivos temporales.

## Auditoría con inicio de sesión de cliente para clientes conectados mediante CORBA

Esto incluye aplicaciones como SAP BusinessObjects Web Intelligence.



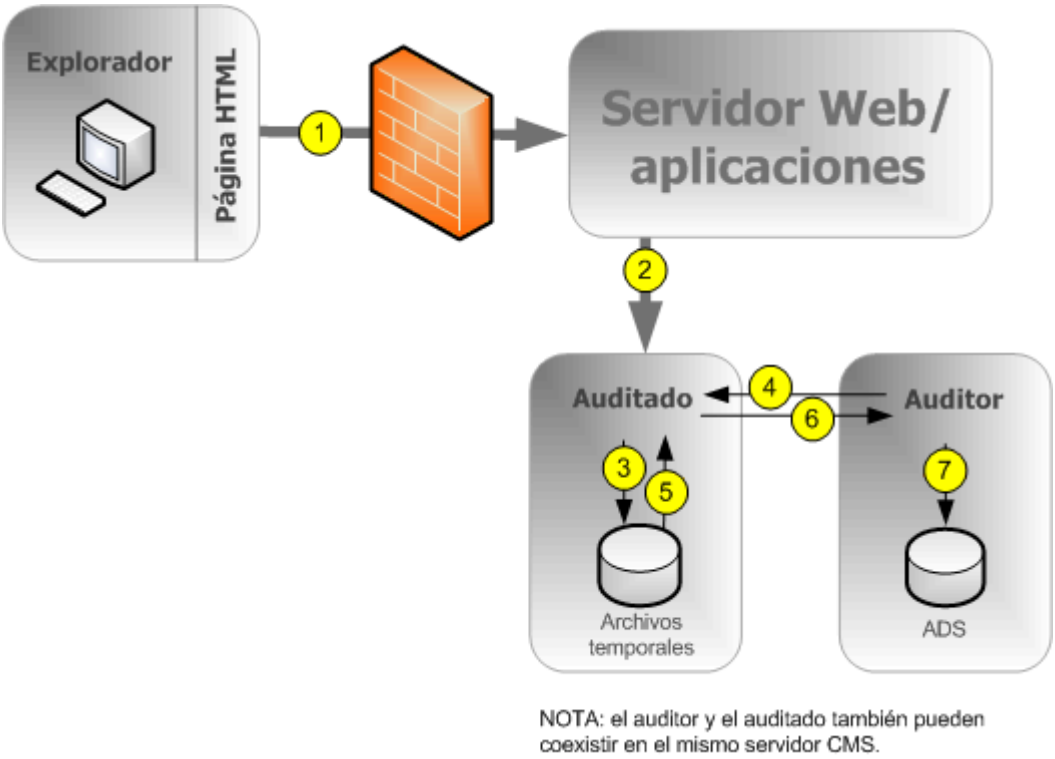

1. El cliente se conecta al CMS, que actuará como auditado. El cliente proporciona su dirección IP y nombre de equipo, que el auditor comprueba.

> **Nota**
>
> Debe abrirse un puerto en el servidor de seguridad entre el cliente y el CMS. Puede encontrar más información sobre servidores de seguridad en el capítulo de seguridad del *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*.

2. El auditado escribe los eventos en un archivo temporal. Los pasos 1 y 2 pueden aparecer varias veces antes del paso 3.
3. A intervalos regulares, el auditor sondea al auditado y solicita un lote de eventos de auditoría.
4. El auditado recupera los eventos de los archivos temporales.
5. El auditado transmite los eventos al auditor.
6. El auditor graba los eventos en el ADS e indica al auditado que elimine los eventos de los archivos temporales.

## Auditoría con inicio de sesión de cliente para clientes conectados mediante HTTP

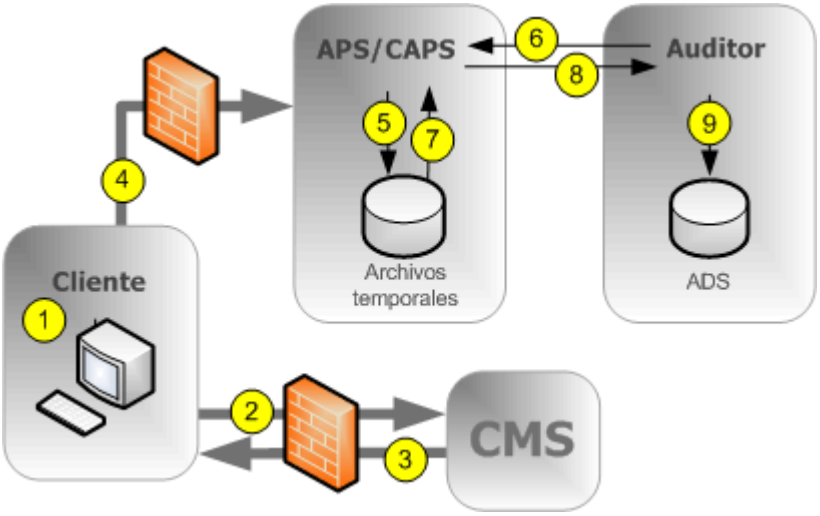
Esto incluye aplicaciones como la rampa de lanzamiento de BI, la Consola de administración central, SAP BusinessObjects Web Intelligence, etc.




1. El explorador se conecta al servidor de aplicaciones Web y los datos de inicio de sesión se envían a este.
2. El SDK de la plataforma de BI envía la solicitud de inicio de sesión al auditado (CMS), junto con la dirección IP y el nombre del equipo del explorador.
3. El auditado escribe los eventos en un archivo temporal. Los pasos del 1 al 3 pueden aparecer varias veces antes del paso 4.
4. A intervalos regulares, el auditor sondea al auditado y solicita un lote de eventos de auditoría.
5. El auditado recupera los eventos de los archivos temporales.
6. El auditado envía los eventos al auditor.
7. El auditor graba los eventos en el ADS e indica al auditado que elimine los eventos de los archivos temporales.

## Auditoría sin inicio de sesión para clientes conectados mediante CORBA

Este flujo de trabajo se aplica a eventos de auditoría de SAP BusinessObjects Web Intelligence al conectarse a través de CORBA.



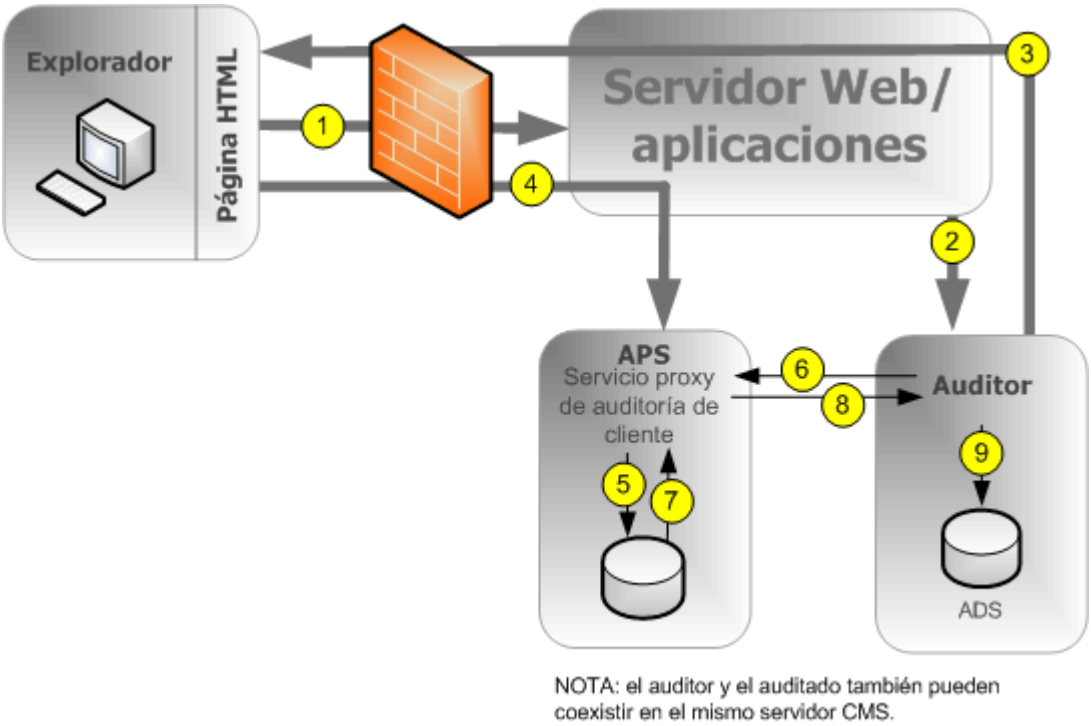

1. El usuario realiza una operación que se pueda auditar.
2. El cliente se pone en contacto con el CMS para comprobar si la operación está configurada para auditarse.
3. Si la acción está definida para auditarse, el CMS comunica esta información al cliente.
4. El cliente envía la información de evento al servicio proxy de auditoría de cliente (CAPS) que está alojado en un servidor de procesamiento de Adaptive.

   > **Nota**
   >
   > Debe abrirse un puerto en el servidor de seguridad entre cada cliente y cualquier servidor de procesamiento de Adaptive que aloje un CAPS, y también entre cada cliente y el CMS. Puede encontrar más información sobre servidores de seguridad en el capítulo de seguridad del *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*.

5. El CAPS graba los eventos en un archivo temporal. Los pasos del 1 al 5 pueden aparecer varias veces antes del paso 6.
6. A intervalos regulares, el auditor sondea el CAPS y solicita un lote de eventos de auditoría.
7. El CAPS recupera los eventos de los archivos temporales.
8. El CAPS envía la información de evento al auditor.
9. El auditor graba los eventos en el ADS e indica al CAPS que elimine los eventos de los archivos temporales.

## Auditoría sin inicio de sesión para clientes conectados mediante HTTP

Este flujo de trabajo se aplica a eventos de auditoría de SAP BusinessObjects Web Intelligence (excepto para eventos de inicio de sesión) al conectarse a través de HTTP.




1. El usuario inicia un evento potencialmente auditable. La aplicación cliente se pone en contacto con el servidor de aplicaciones Web.
2. La aplicación Web comprueba si el evento está configurado para auditarse.

   > **Nota**
   >
   > En el diagrama, se muestra el CMS auditor con el que se contacta, pero es posible ponerse en contacto con cualquier CMS del clúster para obtener esta información.

3. El CMS devuelve la información de configuración de auditoría al servidor de aplicaciones Web, que devuelve esta información a la aplicación cliente.
4. Si el evento está configurado para auditarse, el cliente envía la información de evento al servidor de aplicaciones Web, que la envía al servicio de proxy de auditoría de cliente (CAPS), alojado en un servidor de procesamiento de Adaptive (APS).
5. El CAPS graba los eventos en un archivo temporal. Los pasos del 1 al 5 pueden aparecer varias veces antes del paso 6.
6. A intervalos regulares, el auditor sondea el CAPS y solicita un lote de eventos de auditoría.
7. El CAPS recupera los eventos de los archivos temporales.
8. El CAPS envía la información de evento al auditor.
9. El auditor graba los eventos en el ADS e indica al CAPS que elimine los eventos de los archivos temporales.

## Clientes que admiten la auditoría

Las siguientes aplicaciones cliente admiten la auditoría:

- Edición de Analysis para OLAP (AOLAP)

- Plataforma de lanzamiento de BI (BILP)
- Administrador de vistas empresariales (BVM)
- Administrador de configuración central (CCM)
- Consola de administración central (CMC)
- OpenDocument
- Herramienta de diseño de información (IDT)
- Live Office (LO)
- SAP BusinessObjects Mobile
- Herramienta de administración de traducciones (TMT)
- Cliente enriquecido de Web Intelligence (WIRC)
- Aplicación Lumira Desktop (Discovery)
- Aplicación Lumira Designer

> **Nota**
>
> Al menos una instancia de CAPS se debe ejecutar para poder recopilar eventos de auditoría desde los clientes de la lista anterior.

Los clientes que no aparecen en la lista anterior no generan eventos directamente, pero se pueden auditar algunas acciones que realizan los servidores como resultado de las operaciones de las aplicaciones cliente.

## Coherencia de auditoría

En la mayoría de los casos, cuando la auditoría está correctamente instalada, configurada y protegida y se usan las versiones correctas de todas las aplicaciones cliente, la auditoría registrará de forma correcta y coherente todos los eventos del sistema indicados. No obstante, es importante tener presente que determinadas condiciones del sistema y del entorno pueden afectar negativamente a la auditoría.

Siempre hay un retardo entre el momento en que se produce un evento y su transferencia final a ADS. Estos retardos pueden ampliarse debido a la indisponibilidad del CMS o la base de datos de auditoría o a una pérdida de conectividad de la red.

Como administrador del sistema, debe trabajar para evitar cualquiera de las siguientes situaciones, que podrían provocar registros de auditoría incompletos:

- Una unidad en la que se almacenan los datos de auditoría alcanza su capacidad máxima. Debe asegurarse de que haya mucho espacio de disco disponible para la base de datos de auditoría y los archivos temporales del auditado.
- Un servidor de auditado se elimina de forma inadecuada de la red antes de que pueda transmitir todos los eventos de auditoría. Debería asegurarse de que al eliminar un servidor de la red, quede suficiente tiempo para que los eventos de auditoría se contabilicen en la base de datos de auditoría.
- La eliminación o modificación de los archivos temporales del auditado.
- Una anomalía de disco o hardware.
- La destrucción física de un equipo host de auditado o auditor.

También existen algunas condiciones que impiden que los eventos de auditoría lleguen al auditor de CMS. Entre estos vínculos se incluyen:

- Usuarios con versiones de cliente anteriores.
- La transmisión de la información de auditoría se puede bloquear si los servidores de seguridad están configurados incorrectamente.

> **Nota**
>
> Eventos generados por aplicaciones de cliente que contienen información enviada desde el lado del cliente; en otras palabras, fuera del área de confianza del sistema. Así, en algunas condiciones es posible que esta información no sea tan fiable como la información registrada por los servidores del sistema.

> **Nota**
>
> Si desea eliminar un servidor del despliegue, primero debe desactivar el servidor, pero mantenerlo en funcionamiento y conectado a la red hasta que todos los eventos de los archivos temporales hayan podido transferirse a la base de datos de auditoría. La métrica del servidor *Número actual de eventos de auditoría en cola* mostrará la cantidad de eventos de auditoría que están esperando para ser transferidos. Cuando esta métrica alcance cero, puede detener el servidor. La ubicación de los archivos temporales se define mediante la reserva-espacio `%DefaultAuditingDir%` de dicho nodo. Consulte el capítulo sobre la administración del servidor para obtener más información sobre los marcadores de posición.

> **Nota**
>
> Si va a usar la auditoría de cliente, es aconsejable que cree un servidor de procesamiento de Adaptive para el servicio proxy de auditoría de cliente. Así, conseguirá el mejor rendimiento. Para mejorar la tolerancia a errores del sistema, puede considerar también la posibilidad de ejecutar el CAPS en más de un APS.

### Vínculos relacionados

Marcadores de posición de servidor y nodo [página 1218]

## 24.2 Página de auditoría de la CMC

La página *Auditoría* de la CMC tiene las siguientes áreas:

- *Resumen de estado*
- *Definir eventos*
- *Definir detalles de eventos*
- *Configuración*

## 24.2.1 Estado de auditoría

En el *Resumen de estado de Auditoría* se muestra un conjunto de métricas que ayudan a optimizar la configuración de la auditoría y avisarle de los problemas que puedan afectar a la integridad de los datos de auditoría. El resumen de estado está en la parte superior de la página *Auditoría* de la Consola de administración central.

El resumen también mostrará las advertencias bajo las siguientes circunstancias:

- La conexión a la base de datos del Almacén de datos de auditoría (ADS) no está disponible.
- No existe un Servicio proxy de auditoría de cliente ejecutándose o disponible, lo que evita que se recopilen los eventos de cliente.
- Un auditado tiene eventos que no se pueden recuperar (se identificará el servidor o servidores afectados). Por lo general, esto indica que no se ha detenido o apagado correctamente un servidor y todavía tiene eventos en los archivos temporales.

> **Nota**
>
> Las métricas del resumen de estado están marcadas en verde, amarillo, o rojo para indicar el estado de la función de auditoría.

### Métricas del estado de auditoría

| Métrica | Detalles |
|---|---|
| Última actualización de ADS | La fecha y hora en que el CMS auditor finalizó el sondeo de los auditados para los eventos de auditoría. |
| Utilización de subproceso de auditoría | El porcentaje del ciclo de sondeo que el CMS auditor pasa recopilando datos de los auditados; el restante es el tiempo gastado descansando entre sondeos.<br><br>Si alcanza el 100%, la cifra se mostrará en color amarillo e indicará que el auditor todavía sigue recopilando datos de los auditados cuando debe comenzar el siguiente sondeo. Esto puede provocar retrasos en los eventos que llegan al ADS.<br><br>Si esto ocurre de forma repetida o frecuente, se recomienda actualizar la implementación para permitir que la base de datos del ADS reciba los datos a una tasa más alta (por ejemplo, conexiones de red más rápidas o hardware de base de datos más potente), o disminuir el número de eventos de auditoría que el sistema sigue. |
| Duración del último ciclo de sondeos | Duración del último ciclo de sondeos en segundos. Esto indica el retraso máximo de los datos de eventos para acceder al ADS durante el ciclo de sondeo anterior. |

| Métrica | Detalles |
| --- | --- |
| | • Si se encuentra por debajo de los 20 minutos (1200 segundos), la figura aparecerá con el fondo en color verde.<br>• Si se encuentra entre los 20 minutos y las 2 horas (72000 segundos), aparecerá con un fondo en color amarillo.<br>• Si se encuentra por encima de las 2 horas, aparecerá con un fondo de color rojo.<br><br>Si este estado continúa y considera que el retraso es demasiado largo, se recomienda actualizar la implementación para permitir que la base de datos del ADS reciba los datos a una tasa más alta (por ejemplo, conexiones de red más rápidas o hardware de base de datos más potente), o disminuir el número de eventos de auditoría que el sistema sigue. |
| Auditor de CMS | El nombre del CMS que actúa actualmente como auditor. |
| Nombre de la conexión de base de datos del ADS | El nombre de la conexión de base de datos que el CMS usa actualmente para conectarse al Almacén de datos de auditoría (ADS). Para los servidores de SQL Anywhere, SQL Server y SAP HANA, será el nombre de la conexión ODBC. Para otros tipos de bases de datos, será el nombre de la base de datos y el puerto de conexión, seguido del nombre de servidor. |
| Nombre de usuario de la base de datos del ADS | El nombre de usuario que el CMS auditor usa para iniciar sesión en la base de datos del ADS. |

## 24.2.2 Configurar eventos de Auditoría

La página Auditoría de CMC se puede usar para activar la auditoría y seleccionar los eventos que se auditarán en todo el sistema.

Si no está interesado en ciertos eventos o detalles de éstos, puede dejarlos sin seleccionar para conseguir que aumente el rendimiento del sistema.

> **Nota**
>
> Los eventos de auditoría se introducen en la base de datos de auditoría en modo de lote en contraposición a un evento a la vez. El tamaño de lote actualmente está fijado en 1000 eventos de auditoría.

> **Nota**
>
> Si seleccionó no configurar la conexión ADS al instalar la plataforma de BI, deberá configurar una conexión a la base de datos antes de configurar los eventos de auditoría. Sin una conexión, los eventos se seguirán recogiendo, pero una vez conectados, los eventos se escribirán al ADS. Para desactivar la auditoría, el

nivel debe estar establecido en desactivado. Consulte *Ajustes de configuración del almacén de datos de auditoría*.

## 24.2.2.1 Para configurar eventos de auditoría

Para configurar los eventos de auditoría, lleve a cabo los siguientes pasos:

1. En la Consola de administración central, seleccione la ficha *Auditoría*.
   Aparecerá la página *Auditoría*.
2. Establezca el botón deslizante *Definir eventos* en el nivel de auditoría deseado, donde cada nivel de auditoría corresponda a un valor de métrica específico.
   - *Desactivado* - 1
   - *Mínimo* - 2
   - *Predeterminado* - 3
   - *Finalizado* - 4
   - *Personalizado* - 0

   La siguiente tabla muestra las distintas configuraciones para el control deslizante y los eventos capturados en cada nivel.

| Nivel de auditoría | Eventos capturados |
|---|---|
| *Off* | Ninguno |
| *Mínimo* | • Iniciar sesión<br>• Cerrar sesión<br>• Modificación de derechos<br>• Nivel de acceso personalizado modificado<br>• Modificación de auditoría |
| *Valor predefinido* | Eventos *mínimos*, más:<br>• Visualizar<br>• Actualizar<br>• Petición<br>• Crear<br>• Eliminar<br>• Modificar<br>• Guardar<br>• Buscar<br>• Editar<br>• Ejecutar<br>• Entregar |
| *Finalizado* | Eventos *mínimos* y *predeterminados*, más:<br>• Desencadenar<br>• Exploración fuera del ámbito.<br>• Página obtenida |

| Nivel de auditoría | Eventos capturados |
| --- | --- |
| | • Configuración de la Administración de promociones<br>• Restauración<br>• Adición de VMS<br>• Recuperación de VMS<br>• Protección de VMS<br>• Desprotección de VMS<br>• Exportación de VMS<br>• Bloqueo de VMS<br>• Desbloqueo de VMS<br>• Eliminación de VMS<br>• Conexión de cubo<br>• Sesión MDAS<br><br>**Nota**<br>Puede ver más eventos cuando los add-ons están instalados. |
| *Personalizar* | Seleccione un conjunto personalizado de eventos. |

> **Nota**
>
> Cuando *Definir eventos* está fijado como *Predeterminado*, el valor del *Nivel de auditoría* es 3.
>
> Cuando *Definir eventos* está fijado como *Off*, el valor del *Nivel de auditoría* cambia de 3 a 1.

3. Seleccione *Personalizado*, haga clic en los eventos que desea capturar de la lista situada debajo del botón deslizante *Definir eventos*.
4. Haga clic en los detalles opcionales en *Definir detalles del evento* que desea guardar con los eventos, cuantos menos detalles se registren mejor será el rendimiento del sistema.

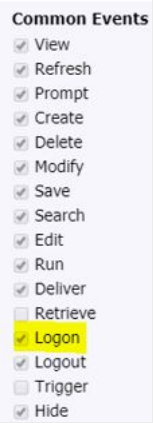
| Detalle | Descripción |
| --- | --- |
| *Consulta* | Si está definido, el detalle del evento *Consulta* (ID de detalle 25) se registra para cualquier evento que consulte una base de datos. |
| *Detalles de la ruta de la carpeta* | Si está configurado, se capturarán los siguientes detalles:<br>• *Ruta de la carpeta del objeto (ID de detalle 71)*<br>• *Nombre de la carpeta principal (ID de detalle 72*<br>• *Ruta de la carpeta del contenedor (ID de detalle 64)* |
| *Detalles de derechos* | Si está configurado, se capturarán los siguientes detalles:<br>• *Derecho agregado (ID de detalle 55)*<br>• *Derecho eliminado (ID de detalle 56)*<br>• *Derecho modificado (ID de detalle 57)* |
| *Detalles de grupo de usuarios* | Si está configurado, se capturarán los siguientes detalles:<br>• *Nombre de grupo de usuarios (ID de detalle 16)*<br>• *ID de grupo de usuarios (ID de detalle 15)* |

| Detalle | Descripción |
| --- | --- |
| *Detalles del valor de propiedad* | Si está configurado, se captura el detalle del evento *Valor de propiedad* (ID de detalle 29) cuando se actualicen las propiedades de un objeto. Esto se genera únicamente para los eventos de CMC, de la plataforma de lanzamiento de BI o de eventos de SharePoint. |

5. Haga clic en *Guardar*.

> **Nota**
>
> Para la auditoría de clientes, el sistema puede tardar hasta 2 minutos desde que se realizan las modificaciones para empezar a registrar datos para eventos nuevos. Asegúrese de permitir este retraso al implementar cambios en el sistema.

## 24.2.2.2 Grabación detallada del evento ampliado en tabla detallada de auditoría

> **Nota**
>
> - Debería tener conocimientos suficientes referentes a Página de auditoría de la CMC [página 898], especialmente *Eventos comunes, Fijar detalles de evento, Detalles de grupo de eventos*, e *Inicio de sesión* para poder utilizar la información proporcionada más adelante.
> - *Inicio de sesión* es un evento que proporciona detalles de un usuario que accede a la aplicación.
>
> 
> 
>
> - *Detalles de grupo de usuarios* proporciona información sobre los grupos de usuarios asociados con un usuario para cada evento.
>
>
> 

El registro de detalles del grupo de usuarios en la tabla AUDIT_EVENT_DETAIL es parcialmente dependiente de las selecciones realizadas bajo *Eventos comunes* y *Fijar detalles de evento* en la página de Auditoría. Considere

un escenario en el que ha seleccionado *Inicio de sesión* pero no *Detalles de grupo de usuarios* en la página *Auditoría*. En este escenario, los detalles del grupo de usuarios aún están registrados para el evento *Inicio de sesión* en la tabla AUDIT_EVENT_DETAIL. Vea la tabla siguiente para comprender el comportamiento en BI 4.2 Support Package 5.

| Inicio de sesión | Detalles de grupo de usuarios | Comportamiento |
|---|---|---|
| Seleccionado | Seleccionado | Detalles de grupos de usuarios están registrados para todos los eventos seleccionados bajo Evento común. |
| Seleccionado | No seleccionado | Los detalles de grupo de usuarios están registrados solo para eventos de Inicio de sesión. |
| No seleccionado | No seleccionado | No están registras los detalles del grupo de usuarios. |
| No seleccionado | Seleccionado | Los detalles de grupos de usuarios están registrados para todos los eventos seleccionados excepto Inicio de sesión. |

## 24.2.3 Opciones de configuración de memoria de datos de auditoría

Si seleccionó no configurar una base de datos de auditoría al instalar la plataforma de BI o desea cambiar la ubicación o los ajustes de la base de datos, puede usar los siguientes pasos para configurar la conexión al ADS.

Aquí también puede configurar el tiempo que se retendrán los eventos de auditoría en la base de datos.

Si ha llevado a cabo una actualización desde una versión anterior de SAP BusinessObjects Enterprise XI 3.x y tiene instalada la versión 3.x de Business Objects Metadata Manager (BOMM), se recomienda configurar el ADS para que use la misma base de datos o espacio de tabla que BOMM.

> **Nota**
>
> Si usa un grupo de trabajo DB2 9.7 existente como la base de datos de auditoría, asegúrese de que la cuenta de la base de datos está configurada para disponer de un tamaño de página de más de 8 KB.

### 24.2.3.1 Configurar los ajustes de la base de datos del Almacén de datos de auditoría

1. En la Consola de administración central, seleccione la ficha *Auditoría*.
2. En el área *Configuración*, en el encabezado *Base de datos ADS*, seleccione el tipo de base de datos que ha establecido para los datos de auditoría.

3. En el campo *Nombre de conexión*, introduzca el nombre de la conexión que ha configurado para la base de datos de auditoría.

| Tipo de base de datos | Nombre de conexión |
|---|---|
| IBM DB2 | nombre de servicio |
| Microsoft SQL Server | DSN ODBC |
| MySQL | `<serverhostname>,<port>,<databasename>` |
| Oracle | Nombre de servicio TNS |
| SAP HANA | ODBC DSN |
| SAP MaxDB | `<serverhostname>,<port>,<databasename>` |
| Sybase Adaptive Server Enterprise | Nombre de servicio |
| Sybase SQL Anywhere | ODBC DSN |

   a. Si usa una base de datos de Microsoft SQL con autenticación de Windows, habilite la opción *Autenticación de Windows*.

4. En los campos *Nombre de usuario* y *Contraseña*, introduzca el nombre de usuario y la contraseña que desea que use el CMS auditor al iniciar sesión en la base de datos.
5. En el campo *Eliminar eventos de más de (días)*, introduzca el número de días que desea que la información permanezca en la base de datos. (Valor mínimo 1, valor máximo 109.200)

> ⚠ Precaución
>
> Los datos mayores al número de días establecidos aquí se eliminarán permanentemente del ADS y no se podrán recuperar. Es posible que se plantee mover registros periódicamente a una base de datos de archivos si desea conservar registros a largo plazo.

6. En el caso de que la conexión de la base de datos se pierda, si desea volver a conectar manualmente el CMS auditor a la base de datos, no seleccione la opción *Reconexión automática de ADS*.

> ⓘ Nota
>
> Si no se selecciona, tendrá que volver a establecer una conexión al ADS manualmente si se pierde la conexión. Realice esta acción reiniciando el CMS o habilitando *Reconexión automática de ADS*. Los eventos se registrarán y se mantendrán almacenados en archivos temporales hasta que se vuelva a conectar el ADS.

7. Haga clic en *Guardar*.
8. Reiniciar todos los CMS en el clúster.

> ⓘ Nota
>
> El *Resumen de estado* en la parte superior de la página muestra los valores de ADS actuales, que pueden ser distintos de los valores en la sección *Base de datos ADS* hasta que se hayan reiniciado los CMS.

## 24.3 Eventos de auditoría

En la siguiente tabla se muestran todos los eventos de auditoría del sistema, y ofrece una breve descripción de cada una. Una lista de tipos de servicio que crea los siguientes eventos.

| Evento | |
|---|---|
| Descripción de modificación de auditoría y servidores y clientes que generan el tipo de evento | Se modifica la configuración de auditoría del sistema.<br>• Servicio de administración central |
| Crear | Se agrega un nuevo objeto al sistema.<br>• Servicio de comentario de BI<br>• Servicio de administración central<br>• Servicio de visualización y modificación de Crystal Reports<br>• Desktop Intelligence<br>• Servicio del motor de información<br>• Administración de ciclo de vida<br>• Web Intelligence<br>• Servicio común de Web Intelligence<br>• Descripción, servidores y clientes que generan el servicio principal de Web Intelligence<br>• Servicio de procesamiento de Web Intelligence |
| Conexión de cubo | Se lleva a cabo una operación de conexión de cubo OLAP.<br>• Servicio de análisis multidimensional<br>• Aplicaciones de análisis |
| Nivel de acceso personalizado modificado | Se ha modificado la información para privilegios.<br>• Servicio de administración central |
| Eliminar | Se elimina un objeto del sistema.<br>• Servicio de comentario de BI<br>• Servicio de administración central<br>• Servicio de administración de ciclo de vida |
| Entregar | Se envía/entrega un objeto a un destino.<br>• Servicio de programación de actualización de autenticaciones<br>• Servicio de administración central<br>• Servicio de programación de Crystal Reports para Enterprise<br>• Servicio de programación de Crystal Reports<br>• Desktop Intelligence<br>• Servicio de programación de entrega de destino<br>• Servicio de programación de búsqueda en plataforma<br>• Servicio de programación de métrica<br>• Servicio de programación de programa |

| Evento | |
|---|---|
| | • Servicio de programación de consulta de seguridad<br>• Servicio de programación para importar usuarios y grupos<br>• Servicio de programación y publicación de Web Intelligence |
| Exploración fuera del objeto | Un usuario de un documento de Web Intelligence ha profundizado un nivel de detalle fuera de los datos cargados anteriormente del informe.<br>• Web Intelligence<br>• Servicio de procesamiento de Web Intelligence<br>• Servicios comunes de Web Intelligence<br>• Servicios principales de Web Intelligence<br>• Servicio del motor de información |
| Editar | El contenido de un objeto se ha cambiado.<br>• Aplicación de espacios de trabajo de BI<br>• Desktop Intelligence<br>• Servicio del motor de información<br>• Web Intelligence<br>• Servicio común de Web Intelligence<br>• Servicio central de Web Intelligence<br>• Servicio de procesamiento de Web Intelligence |
| Configuración de LCM | Los detalles de configuración de la consola de administración de ciclo de vida (LCM) han cambiado.<br>• Gestión del ciclo de vida |
| Iniciar sesión | Un usuario inicia sesión en el sistema.<br>• Servicio de administración central |
| Cerrar sesión | Un usuario se desconecta del sistema.<br>• Servicio de administración central |
| Modificar | Las propiedades de archivo de un objeto han cambiado.<br>• Web Intelligence<br>• Gestión del ciclo de vida<br>• Servicio de administración central<br>• Servicio de comentario de BI |
| Sesión MDAS | Se lleva a cabo una operación de servicios de análisis multidimensional<br>• Servicio de análisis multidimensional |
| Página obtenida | Un cliente de SAP BusinessObjects Web Intelligence recupera información adicional del repositorio.<br>• Servicio de procesamiento de Web Intelligence |

| Evento | |
|---|---|
| | • Servicios comunes de Web Intelligence<br>• Servicios principales de Web Intelligence<br>• Servicio del motor de información |
| Petición | Se introduce la información para una petición de objeto.<br>• Servicio de caché de Crystal Reports<br>• Servicio de programación de Crystal Reports para Enterprise<br>• Servicio de programación de Crystal Reports<br>• Desktop Intelligence<br>• Servicio del motor de información<br>• Live Office<br>• Web Intelligence<br>• Servicio común de Web Intelligence<br>• Servicio central de Web Intelligence<br>• Servicio de procesamiento de Web Intelligence |
| Actualizar | Los datos de un objeto se actualizan desde la base de datos a petición de un usuario.<br>• Servicio de caché de Crystal Reports<br>• Servicio de programación de Crystal Reports para Enterprise<br>• Servicio de programación de Crystal Reports<br>• Desktop Intelligence<br>• Servicio del motor de información<br>• Live Office<br>• Web Intelligence<br>• Servicio común de Web Intelligence<br>• Servicio central de Web Intelligence<br>• Servicio de procesamiento de Web Intelligence |
| Recuperar | Se recupera un objeto desde el repositorio.<br>• Servicio de administración central<br>• Desktop Intelligence |
| Modificación de derechos | La información de seguridad cambia para un usuario, grupo u objeto.<br>• Servicio de administración central |
| Rollback | El administrador de ciclo de vida se usa para invertir un objeto a una versión anterior.<br>• Gestión del ciclo de vida |
| Ejecutar | Se ejecuta una tarea.<br>• Servicio de programación de actualización de autenticaciones |

| Evento | |
|---|---|
| | • Servicio de programación de Crystal Reports para Enterprise<br>• Servicio de programación de Crystal Reports<br>• Desktop Intelligence<br>• Servicio de programación de entrega de destino<br>• Servicio de programación de LCM<br>• Administración de ciclo de vida<br>• Servicio de programación de búsqueda en plataforma<br>• Servicio de programación de métrica<br>• Servicio de programación de programa<br>• Servicio de programación de publicación<br>• Servicio de réplica<br>• Servicio de programación de consulta de seguridad<br>• Servicio de programación para importar usuarios y grupos<br>• Servicio de programación de diferencia visual<br>• Servicio de programación y publicación de Web Intelligence |
| Guardar | Se guarda un objeto después de que se actualice o cambie.<br>• Edición de análisis para OLAP<br>• Servicio de caché de Crystal Reports<br>• Servicio de programación de Crystal Reports para Enterprise<br>• Servicio de programación de Crystal Reports<br>• Servicio de visualización y modificación de Crystal Reports<br>• Desktop Intelligence<br>• Servicio del motor de información<br>• Administración de ciclo de vida<br>• Servicio de análisis multidimensional<br>• SAP BusinessObjects Mobile<br>• Web Intelligence<br>• Servicio común de Web Intelligence<br>• Servicio central de Web Intelligence<br>• Servicio de procesamiento de Web Intelligence |
| Buscar | Se lleva a cabo una búsqueda.<br>• Servicio de búsqueda<br>• Explorador<br>• Administración de ciclo de vida |
| Desencadenar | Se desencadena un evento de archivo.<br>• Servicio de eventos<br>• Servicio de administración central |

| Evento | |
|---|---|
| Vista | Se visualiza un objeto.<br>• Aplicaciones de análisis<br>• Edición de análisis para OLAP<br>• Plataforma de lanzamiento de BI<br>• Aplicación de espacios de trabajo de BI<br>• Servicio de comentario de BI<br>• Consola de administración central<br>• Servicio de caché de Crystal Reports<br>• Servicio de visualización y modificación de Crystal Reports<br>• Desktop Intelligence<br>• Servicio del motor de información<br>• Abrir documento<br>• SAP BusinessObjects Mobile<br>• Web Intelligence<br>• Servicio común de Web Intelligence<br>• Servicio central de Web Intelligence<br>• Servicio de procesamiento de Web Intelligence |
| Adición de VMS | Se agrega un objeto al sistema de administración central de LCM.<br>• Gestión del ciclo de vida |
| Protección de VMS | Se protege un objeto en el sistema de administración de versiones de LCM.<br>• Gestión del ciclo de vida |
| Desprotección de VMS | Se desprotege un objeto del sistema de administración de versiones de LCM.<br>• Gestión del ciclo de vida |
| Exportación de VMS | Se exporta un recurso del VMS.<br>• Gestión del ciclo de vida |
| Bloqueo de VMS | Se bloquea un recurso en el VMS.<br>• Gestión del ciclo de vida |
| Desbloqueo de VMS | Se desbloquea un objeto en el VMS.<br>• Gestión del ciclo de vida |
| Recuperación de VMS | Se recupera un objeto desde el sistema de administración de versiones de LCM.<br>• Gestión del ciclo de vida |
| Eliminación de VMS | Se elimina un objeto desde el sistema de administración de versiones de LCM.<br>• Gestión del ciclo de vida |

## Eventos por tipo de servicio

| Tipo de servicio | Tipos de eventos generados |
|---|---|
| Aplicaciones de análisis | • Vista<br>• Conexión de cubo |
| Servicio de programación de actualización de autenticaciones | • Entregar<br>• Ejecutar |
| Plataforma de lanzamiento de BI de Fiori | Vista |
| Servicio de comentario de BI | • Crear<br>• Eliminar<br>• Vista<br>• Modificar<br>• Ocultar |
| Servicio de administración central | • Modificación de auditoría<br>• Crear<br>• Nivel de acceso personalizado modificado<br>• Eliminar<br>• Entregar<br>• Inicio de sesión<br>• Cerrar sesión<br>• Modificar<br>• Recuperar<br>• Modificación de derechos<br>• Desencadenar |
| Consola de administración central | Vista |
| Servicio de programación de Crystal Reports | • Entregar<br>• Solicitar<br>• Actualizar<br>• Ejecutar<br>• Guardar |
| Servicio de caché de Crystal Reports | • Petición<br>• Actualizar<br>• Guardar<br>• Vista |
| Servicio de programación de Crystal Reports para Enterprise | • Entregar<br>• Solicitar<br>• Actualizar<br>• Ejecutar<br>• Guardar |

| Tipo de servicio | Tipos de eventos generados |
| --- | --- |
| Servicio de programación de Crystal Reports | • Entregar<br>• Solicitar<br>• Actualizar<br>• Ejecutar<br>• Guardar |
| Servicio de visualización y modificación de Crystal Reports | • Crear<br>• Guardar<br>• Vista |
| Desktop Intelligence (cliente) | • Entregar<br>• Solicitar<br>• Recuperar<br>• Ejecutar |
| Proceso de programador de Desktop Intelligence | • Entregar<br>• Ejecutar |
| Servicio de programación de entrega de destino | • Entregar<br>• Ejecutar |
| Servicio de eventos | Desencadenar |
| Servicio del motor de información | • Crear<br>• Exploración fuera del objeto<br>• Editar<br>• Página obtenida<br>• Petición<br>• Actualizar<br>• Guardar<br>• Vista |
| Servicio de programación de LCM | Ejecutar |
| Servicio de LCM | • Crear<br>• Eliminar<br>• Configuración de LCM<br>• Modificar<br>• Rollback<br>• Ejecutar<br>• Guardar<br>• Adición de VMS<br>• Protección de VMS<br>• Desprotección de VMS<br>• Eliminación de VMS<br>• Exportación de VMS<br>• Bloqueo de VMS |

| Tipo de servicio | Tipos de eventos generados |
| --- | --- |
| | • Recuperación de VMS<br>• Desbloqueo de VMS<br>• Buscar |
| Live Office | • Petición<br>• Actualizar |
| Servicio de análisis multidimensional | • Conexión de cubo<br>• Sesión MDAS<br>• Guardar |
| OpenDocument | Vista |
| Servicio de programación de búsqueda en plataforma | • Entregar<br>• Ejecutar |
| Servicio de búsqueda de plataforma | Buscar |
| Servicio de programación de métrica | • Entregar<br>• Ejecutar |
| Servicio de programación de programa | • Entregar<br>• Ejecutar |
| Servicio de programación de publicación | Ejecutar |
| Servicio de réplica | Ejecutar |
| SAP BusinessObjects Design Studio versión 1.3 y posterior | • Inicio de sesión<br>• Cierre de sesión |
| Servicio de programación de consulta de seguridad | • Ejecutar<br>• Entregar |
| Servicio de programación para importar usuarios y grupos | • Ejecutar<br>• Entregar |
| Servicio de programación de diferencia visual | Ejecutar |
| Aplicación Web Intelligence | • Crear<br>• Exploración fuera del objeto<br>• Editar<br>• Modificar<br>• Petición<br>• Actualizar<br>• Guardar<br>• Vista |
| Servicio común de Web Intelligence | • Crear<br>• Exploración fuera del objeto<br>• Editar |

| Tipo de servicio | Tipos de eventos generados |
| --- | --- |
| | • Página obtenida<br>• Petición<br>• Actualizar<br>• Guardar<br>• Vista |
| Servicio central de Web Intelligence | • Crear<br>• Exploración fuera del objeto<br>• Editar<br>• Página obtenida<br>• Petición<br>• Actualizar<br>• Guardar<br>• Vista |
| Servicio de procesamiento de Web Intelligence | • Crear<br>• Exploración fuera del objeto<br>• Editar<br>• Página obtenida<br>• Petición<br>• Actualizar<br>• Guardar<br>• Vista |
| Servicio de programación y publicación de Web Intelligence | • Entregar<br>• Ejecutar |

## Propiedades y detalles de eventos

Cada evento que la plataforma de BI registra incluye un conjunto de propiedades y detalles de eventos.

Siempre se generarán propiedades de eventos con un evento, a pesar de que algunos pueden no disponer de valores si la información no se aplica a un evento específico. En ADS, las propiedades de eventos se incluyen en la tabla que almacena el evento, de modo que se pueden usar para ordenar o agrupar eventos al crear informes.

Los detalles de eventos registran información adicional sobre el evento que no se incluyen en las propiedades del evento. Si un detalle de evento no es importante para un evento específico, no se generará ese detalle del evento. Existe un conjunto de detalles de eventos comunes que se pueden generar para todos los tipos de evento cuando son importantes. También existen conjuntos de detalles de eventos adicionales que se generan para tipos específicos de eventos. Por ejemplo, los eventos Petición registran los valores introducidos para la petición en un detalle de evento, pero ningún otro tipo de evento genera un detalle de evento de valor de petición. En ADS, los detalles de almacenan en una tabla separada que se vincula al evento principal.

En algunos casos, los detalles de evento pueden contener varios valores. Estos detalles se pueden agrupar mediante el ID de grupo. Consulte el tema relacionado para obtener más información sobre los ID de grupo.

Se registrarán los datos multilingües (como nombres de objeto o carpeta) en el idioma predeterminado para la configuración regional del CMS del auditor.

### Información relacionada

Auditing Data Store Tables [página 1227]

## 24.3.1 Audit events and details

The following sections list all of the event types, followed by a description of any properties and event details that are unique to those events. At the beginning of the section is a list of the properties and details that are common to all event types.

> **Nota**
>
> Some client programs do not have their own unique events, and rely on the common and platform events to capture relevant information about their operations.

### Universal event Properties and Details

The following tables show what properties and event details are recorded for all events.

> **Nota**
>
> The properties in this table are columns in the ADS_EVENT table in the Auditing Data Store.

| Event Property | Description |
|---|---|
| Event_ID | A unique identifier for the event. |
| Client_Type_ID | Identifier for the type of application that performed the event |
| Service_Type_ID | Shows the ID of the type of service or application that triggered the event. |
| Start_Time | The start date and time when the event started (in GMT). |
| Duration | Duration of the event in milliseconds.<br>Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`. |
| Session_ID | ID of the session during which the event was triggered. |
| Event_Type_ID | Type of event (for example, 1002 for view). |

| Event Property | Description |
| --- | --- |
| Status_ID | Records if the action succeeds or fails ("0" = succeeded, "1" = failed). Some events will have additional status types, these are detailed with the descriptions of those events. |
| Object_ID | CUID of the object affected (if applicable). CUID of the alerting event for Trigger events.<br>**Nota**<br>All objects not saved in the CMS repository will have an ID of 0. These objects could be documents that have not yet been saved to the CMS database, or are stored locally on a client machine for example. You will need to use the Object_Name property to differentiate these objects. |
| User_ID | CUID of the User that performed the event. |
| User_Name | The user-name of the user the performed the event. |
| Object_Name | Name of the affected object (if applicable). Name of the alerting event for Trigger events. |
| Object_Type_ID | CUID of object type (for example document, folder, and so on). |
| Object_Folder_Path | Full folder path to where the affected object is located in the CMS repository. For example, `Sales/North America/East Coast` |
| Folder_ID | The CUID of the folder where the object is stored. |
| Top_Folder_Name | Name of the top level folder the affected object is stored in. For example, if object is located in `Sales/North America/East Coast` then the value would be `Sales`. |
| Top_Folder_ID | The CUID of the top level folder where the affected object is located. For example, if object is located in `Sales/North America/East Coast` then the value would be the CUID of the folder `Sales`. |
| Cluster ID | The CUID of the CMS cluster that recorded the event. |
| Action_ID | A unique identifier that can be used to tie together a sequence of events initiated by a single user action. |

**Nota**

The properties in this table are columns in the ADS_EVENT_DETAIL_TYPE_STR table in the Auditing Data Store.

| Event Detail | ID | Description |
| --- | --- | --- |
| Error | 1 | Only recorded if the action fails; the text of any error messages that result from the attempt. |

| Event Detail | ID | Description |
|---|---|---|
| Element ID | 2 | Name of an object that resides in a container object (Live Office document or Dashboard for example). |
| Element Name | 3 | ID generated for an object that resides in a container object (Live Office document or Dashboard for example). |
| Element Type ID | 5 | The type of object in a container object that is being viewed or modified. Only generated if applicable. |
| Parent Document ID | 12 | • For a document instance: the CUID of the parent document.<br>• For parent documents: its own CUID. |
| Universe ID | 13 | CUID of the Universe used by the document or object. An event detail will be generated for each Universe if more than one is used. |
| Universe Name | 14 | The name of the Universe used by the document/object. An event detail will be generated for each Universe if more than one is used. |
| User Group Name | 15 | The user group name that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group. |
| User Group ID | 16 | The user group ID that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group. |

## Common Events

The following event types are common to all SAP BusinessObjects servers and clients.

*View*

User viewed a document / object.

- Event Type ID: 1002

| Event Detail | ID | Description |
|---|---|---|
| Size | 17 | Size of the object (in bytes) that is the subject of the event. |

| Event Detail | ID | Description |
|---|---|---|
| Container ID | 32 | The CUID of the container object (a dashboard, for example) that the object resides in (if applicable). |
| Container Type | 33 | The application type of the container for the object (if applicable). |

> **Nota**
>
> If you are using a search service then during document indexing you may notice a large number of View events generated by the "System Account" user. This is caused by the search indexing service opening documents in order to build the search index.

### *Refresh*

An object was refreshed from the database.

- Event Type ID: 1003

| Event Detail | ID | Description |
|---|---|---|
| Size | 17 | Size of the object (in bytes) that is the subject of the event.<br>**Nota**<br>For View on Demand Crystal Reports this will be set to 0. |
| Number of Rows | 63 | The number of records the database server returned.<br>**Nota**<br>For View on Demand Crystal Reports this will be set to 0. |
| Query | 25 | Records the SQL query used to refresh the data (optional, set in CMC). |
| Universe Object Name | 31 | The name of the universe the document or object uses. An event detail will be generated for each universe accessed by the document or object. |
| Document Scope | 36 | Records information on the intended scope of the document from its publishing settings (for example: Country=USA, Role=Manager). Only applicable to publishing workflows. |
| Publication Instance ID | 37 | ID of this instance of the publication. Only applicable to publishing workflows. |

| Event Detail | ID | Description |
|---|---|---|
| Live Office Object Type | 10701 | Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents. |

### *Prompt*

A value was entered for a prompt.

- Event Type ID: 1004

| Event Detail | ID | Description |
|---|---|---|
| Prompt name | 26 | The name assigned to the prompt ("Date" for example). A separate detail will be generated for each prompt in a document or object, and they will be grouped. |
| Prompt value | 27 | The value entered for a prompt. A separate detail will be generated for each value entered. These can be grouped together and related back to the prompt name. |
| Document Scope | 36 | Information on the intended scope of the document (for example: Country=USA, Role=Manager). |
| Publication Instance ID | 37 | ID of this instance of the publication. Only applies to publishing workflows. |
| Name at Design Time | 90 | The name of the Dashboards document at the time it was designed. This is only generated for Dashboards refreshes, or a Dashboards or Live Office document that includes a prompt. |
| Live Office Object Type | 10701 | Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents where the embedded object includes a prompt. |

### *Create*

User created an object.

- Event Type ID: 1005

| Event Detail | ID | Description |
|---|---|---|
| Size | 17 | Size of the object (in bytes) that is the subject of the event. |

| Event Detail | ID | Description |
|---|---|---|
| Overwrite | 21 | Records if the document or object is new or overwrites an existing object (0=New document or object, 1=overwrite of existing document or object). |
| Refresh on Open | 23 | Records if the document or object is set to be automatically refreshed on open (0=No refresh, 1=Refresh on open). Only generated if applicable. |
| Description | 24 | Records any information in the document or object's description field. |

### *Delete*

User deleted an object.

- Event Type ID: 1006

### *Modify*

User modified a file property or the file properties of an object.

- Event Type ID: 1007

| Event Detail | ID | Description |
|---|---|---|
| Property Name | 28 | The name of the property that was modified. An event detail will be generated for each modified property. |
| Property Value | 29 | The new value for any modified property of the document or object. An event detail will be generated for each modified property. |
| Old Property Value | 120 | A user's old email address. |
| New Property Value | 121 | The same user's new email address. |

### *Save*

Saving or exporting a document or object locally, remotely, or to the CMS repository, in either its existing format or a different format.

- Event Type ID: 1008
- Statuses:
  - "0" indicates the object was successfully saved locally
  - "1" indicates the attempt failed
  - "2" indicates the object was successfully saved or exported to a repository
  - "3" indicates the object was successfully saved or exported to a new format

| Event Detail | ID | Description |
|---|---|---|
| Size | 17 | Size of the object (in bytes) that was saved or exported. |
| File Name | 18 | The full name the document or object was saved under. If the file is saved locally by a client application, the name will also include the file path. |
| Overwrite | 21 | Records if the document or object is new or overwrites an existing file. "0"=New document or object, "1"=overwrite of existing document or object. |
| Format | 22 | Specifies the format of the document saved/exported, displayed as the common three-letter file extension ("doc" for a Microsoft Word file, or "pdf" for an Adobe PDF file, for example). |
| Refresh on Open | 23 | Records if the document or object is set to be automatically refreshed on open ("0"=No refresh, "1"=Refresh on open). Only recorded if applicable. |

### *Search*

A search was conducted.

- Event Type ID: 1009

| Event Detail | ID | Description |
|---|---|---|
| Keyword | 19 | The keywords of the conducted search. |
| Category | 20 | Category used in the search (if applicable). |
| Number of Rows | 63 | The number of rows returned by the search. |

### *Edit*

User edited the content of an object.

- Event Type ID: 1010

| Event Detail | ID | Description |
|---|---|---|
| Size | 17 | Size of the object (in bytes) that is the subject of the event. |
| Query | 25 | If the edit modifies an SQL query, records the new query. (This setting is optional and can be selected in the CMC Auditing page.) |
| Universe Object Name | 31 | The name of the universe the document or object uses. A separate |

| Event Detail | ID | Description |
|---|---|---|
| | | detail will be generated for each universe accessed by the document or object. |
| Container ID | 32 | The CUID of the container (a dashboard for example) that uses the object (if applicable). |
| Container Type | 34 | The application type of the container for the object (if applicable). |
| Container Folder Path | 64 | Folder path for the container of the object (if applicable). |

### *Run*

A job was run.

- Event Type ID: 1011
- Statuses:
  - "0" indicates the job was successful
  - "1" indicates the job failed
  - "2" indicates the job failed but will be reattempted
  - "3" indicates the job was cancelled

| Event Detail | ID | Description |
|---|---|---|
| Size | 17 | Size of the document (in bytes) that was run. |
| Document Scope | 36 | Information on the intended scope of the document (for example: Country=USA, Role=Manager). |

### *Deliver*

An object was delivered.

- Event Type ID: 1012

| Event Detail | ID | Description |
|---|---|---|
| Size | 17 | Size of the object (in bytes) that was delivered. |
| Destination Type | 35 | The destination of the document or object instance. For example, email, FTP, unmanaged disk, inbox, or printer. |
| Document Scope | 36 | Information on the intended scope of the document (for example: Country=USA, Role=Manager) |
| Publication Instance ID | 37 | ID of this instance of the document or object. |

| Event Detail | ID | Description |
|---|---|---|
| Domain | 38 | Records the SMTP server domain name for documents/objects distributed by email (if applicable). |
| Host Name | 39 | Records the name of the SMTP or FTP host for documents/objects distributed by email or FTP (if applicable). |
| Port | 40 | Records the SMTP or FTP server domain port for documents/objects distributed by email or FTP (if applicable). |
| From address | 41 | Records the sender's address for documents/objects distributed by email (if applicable). |
| To address | 42 | Records the recipient's address for documents/objects distributed by email (if applicable). Will also specify if the address is included in the To, CC, or BCC fields. An event detail will be generated for each intended recipient. |
| File Name | 18 | Records the file name of documents/objects distributed by email or FTP, or written directly to a disk that is not part of the Business Objects deployment. |
| Account Name | 45 | This records one of the following:<br>• For *Inbox* delivered objects, a list of BusinessObjects user account names.<br>• For *FTP* delivered objects, the FTP account name.<br>• For *Unmanaged Disk* delivered objects, the login account used.<br>• For *SMTP* delivered objects, the login account used for the SMTP server. |
| Printer Name | 46 | The name of the printer the document or object was delivered to (if applicable). |
| Number of copies | 47 | The number of copies of the document or object printed (if applicable). |
| Recipient Name | 48 | User name or names of the recipient or recipients of the document or object. An event detail will be generated for each intended recipient. |
| Alerting Event ID | 92 | The CUID of the Alerting event. This is generated only if the event was prompted by an alert. |

| Event Detail | ID | Description |
|---|---|---|
| Alerting Event Name | 93 | The name of the alerting event. This is generated only if the event was prompted by an alert. |
| Delivery Type | 75 | Indicates how the delivery was initiated:<br>• "0" indicates scheduled<br>• "1" indicates sent to a destination<br>• "2" indicates published<br>• "3" indicates an alert was triggered |

### *Retrieve*

An object is retrieved from the CMS.

- Event Type ID: 1013

### *Logon*

A user logs on.

- Event Type ID: 1014
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "1" indicates a failed logon attempt
  - "2" indicates a named-user license logon was successful
  - "3" indicates a non-user (system) login was successful
- Event Type ID: 123
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "2" indicates a named-user license logon was successful

| Event Detail | ID | Description |
|---|---|---|
| Concurrent User Count | 50 | The number of users on the system at the time the event was triggered. |
| Client hostname reported by client | 51 | Hostname of client as reported by client. |
| Client hostname resolved by server | 52 | Hostname of client as resolved by server. If the client hostname cannot be resolved, no value is recorded. |
| Client IP address reported by client | 53 | IP address of client as reported by the client. |
| Client IP address resolved by server | 54 | IP address of client as resolved by the server. If the client IP cannot be resolved, no value is recorded. |
| Authentication Type | 122 | Authentication type is valid for the vlaues secEnterprise, secLDAP, secWinAD, secSAPR3 |
| User Type | 123 | Type of the user. |
| Session Count | 125 | Count of the session is recorded. |
| Tenant ID | 126 | The ID of the tenant is recorded. |

| Event Detail | ID | Description |
| --- | --- | --- |
| Concurrent Tenant Session | 127 | The count of the concurrent session of the tenant is recorded. |

*Logout*

A user logs off.

- Event Type ID: 1015

| Event Detail | ID | Description |
| --- | --- | --- |
| Concurrent User Count | 50 | The number of concurrent users on the system at the time the event was triggered. |

*Trigger*

A file event is triggered.

- Event Type ID: 1016

| Event Detail | ID | Description |
| --- | --- | --- |
| File Name | 18 | The name of the file that was being monitored and triggered the event. |

## 24.3.1.1 Eventos de la plataforma

Los siguientes eventos son específicos de la plataforma de BI.

### Modificación de derechos

Se han modificado el derecho o los derechos de un objeto.

- ID de tipo de evento: 10003

| Detalles del evento | ID | Descripción |
| --- | --- | --- |
| Derechos agregados | 55 | El tipo de derecho agregado, el ámbito del nuevo derecho (qué objetos) y el tipo de objeto al que se aplica. La información se estructurará según el siguiente ejemplo: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`. |
| Derechos eliminados | 56 | El tipo de derecho eliminado, el ámbito del nuevo derecho (qué objetos) |

| Detalles del evento | ID | Descripción |
|---|---|---|
| | | y el tipo de objeto al que se aplica. La información se estructurará según el siguiente ejemplo: `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`. |
| Derechos modificados | 57 | El tipo de derecho modificado, el ámbito del nuevo derecho (qué objetos) y el tipo de objeto al que se aplica. La información se estructurará según el siguiente ejemplo: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`. |
| Principal | 118 | El ID de un usuario o grupo de usuarios (principal) para el que se han modificado los derechos de seguridad. |
| Nombre principal | 119 | El nombre de un usuario o grupo de usuarios (principal) para el que se han modificado los derechos de seguridad. |

## Nivel de acceso personalizado modificado

Se ha modificado un nivel de acceso personalizado.

- ID de tipo de evento: 10004

| Detalles del evento | ID | Descripción |
|---|---|---|
| Derechos agregados | 55 | El tipo de derecho agregado, el ámbito del nuevo derecho (qué objetos) y el tipo de objeto al que se aplica. La información se estructurará según el siguiente ejemplo: `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types` |
| Derechos eliminados | 56 | El tipo de derecho eliminado, el ámbito del nuevo derecho (qué objetos) y el tipo de objeto al que se aplica. La información se estructurará según el siguiente ejemplo: |

| Detalles del evento | ID | Descripción |
| --- | --- | --- |
| | | `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`. |
| Derechos modificados | 57 | El tipo de derecho modificado, el ámbito del nuevo derecho (qué objetos) y el tipo de objeto al que se aplica. La información se estructurará según el siguiente ejemplo: `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`. |
| Principal | 118 | El ID de un usuario o grupo de usuarios (principal) para el que se han modificado los derechos de seguridad. |

## Modificación de auditoría

Se ha realizado un cambio en la configuración de auditoría del sistema.

- ID de tipo de evento: 10006

| Detalles del evento | ID | Descripción |
| --- | --- | --- |
| ID de tipo de evento | 58 | Registra el ID del tipo de evento de auditoría que se habilitó o deshabilitó. Si se habilitan o deshabilitan varios tipos de eventos en una acción, se generará un detalle de evento para cada tipo de evento. |
| Acción | 59 | Registra los eventos de auditoría que he habilitaron o deshabilitaron. |
| Nuevo nivel de auditoría | 60 | Si se cambia el nivel de auditoría del detalle, se registra la nueva configuración del nivel (por ejemplo, desconectado, mínimo o predeterminado). |
| Nivel de auditoría antiguo | 61 | Si se cambia el nivel de auditoría del detalle, se registra la configuración del nivel anterior (por ejemplo, desconectado, mínimo o predeterminado). |
| Opción de auditoría | 62 | Si se habilita o deshabilita un detalle opcional, el detalle modificado |

| Detalles del evento | ID | Descripción |
| --- | --- | --- |
| | | se registra y si está habilitado o deshabilitado. Si se habilitan o deshabilitan varios detalles en una única acción, se generará un registro de detalles para cada detalle modificado. |
| Conexión ADS | 78 | Si se cambia la conexión al almacén de datos de auditoría, se registra la nueva configuración de la conexión con el siguiente formato: `DBType=Oracle,DBName=MyADS,Username=USR1,Password="*****",SSO=off,DBReconnect=on`. Sólo se registrarán los detalles cambiados. Por ejemplo, si sólo se ha actualizado el nombre de usuario, sólo se registrará `Username="nuevo"`.<br>**Nota**<br>La información de la contraseña siempre se ocultará con * en la base de datos. |
| Intervalo de eliminación automática | 105 | Este detalle registrará los cambios del campo *Eliminar eventos más antiguos que* en la página Auditoría de la CMC. Esto rige la cantidad de días que la información de auditoría se conservará en el ADS. |

## 24.3.1.2 Eventos de comentario

Los siguientes derechos son específicos del **comentario BI** en la plataforma de Business Intelligence.

### Añadir comentario

Este evento se genera al agregar un nuevo comentario, duplicar un comentario y al agregar comentarios en masa. Cuando añade un comentario, solo se registra el ID de documento principal. En caso de duplicación o adición masiva de comentarios, se registran todos los detalles del evento mencionados en la tabla siguiente.

ID de tipo de evento: 11001

| Detalles del evento | ID | Descripción |
|---|---|---|
| ID de documento principal | 12 | Registra el ID del objeto. |
| Descripción | 24 | Registra cualquier información adicional en el evento. |
| Tamaño | 17 | Tamaño del objeto (en bytes) que es el asunto del evento. |
| Nombre de archivo | 18 | Registra el nombre de archivo del objeto. |

## Obtener comentario

El evento se genera al visualizar un comentario.

ID de tipo de evento: 11002

| Detalles del evento | ID | Descripción |
|---|---|---|
| ID de documento principal | 12 | Registra el ID del objeto. |
| Tamaño | 17 | Tamaño del objeto (en bytes) que es el asunto del evento. |

## Modificar comentario

El evento se genera al editar un comentario existente.

ID de tipo de evento: 11003

| Detalles del evento | ID | Descripción |
|---|---|---|
| ID de documento principal | 12 | Registra el ID del objeto. |

## Borrar comentario

El evento se genera al borrar un comentario existente.

ID de tipo de evento: 11004

| Detalles del evento | ID | Descripción |
|---|---|---|
| ID de documento principal | 12 | Registra el ID del objeto. |

### Ocultar comentario

El evento se genera al ocultar un comentario.

ID de tipo de evento: 11005

| Detalles del evento | ID | Descripción |
|---|---|---|
| ID de documento principal | 12 | Registra el ID del objeto. |

## 24.3.1.3 Eventos de SAP BusinessObjects Web Intelligence

Los siguientes eventos son específicos del componente de SAP BusinessObjects Web Intelligence.

### Exploración fuera del ámbito

El usuario ha explorado fuera del ámbito del informe.

- ID de tipo de evento: 10201

| Detalles del evento | ID | Descripción |
|---|---|---|
| Instancia de objeto | 11 | Registra si el evento es el resultado de una actualización programada o un usuario que visualiza el objeto ("0" = resultado de un usuario visualizando el objeto, "1" = resultado de una actualización programada del objeto). |
| Número de filas | 63 | El número de filas que devuelve el servidor de base de datos. |
| Consulta | 25 | Registra la consulta usada para actualizar los datos (opcional, establecido en la CMC). |
| Nombre del objeto del universo | 31 | El nombre del universo que usa el documento. Se registra una instancia para cada universo al que accede el documento. |

| Detalles del evento | ID | Descripción |
|---|---|---|
| ID de universo | 32 | El CUID del universo que usa el documento. Se registra una instancia para cada universo al que accede el documento. |

## Página obtenida

La página del documento de Web Intelligence se ha recuperado.

- ID de tipo de evento: 10202

| Detalles del evento | ID | Descripción |
|---|---|---|
| Nombre de informe de Web Intelligence | 10220 | Registra el nombre del informe del documento Web Intelligence visualizado. |
| Tipo de salida | 10221 | El formato de salida del documento visualizado, por ejemplo:<br>• `xml.ro` para Web Intelligence<br>• `pdf` para Adobe Acrobat<br>• `xls` para Microsoft Excel<br>• `text/xml` cuando se desconoce |
| Número de página | 10222 | Registra el número de la página del informe Web Intelligence visualizado.<br>NB:<br>• "0" cuando no se puede recuperar (por ejemplo, pdf)<br>• "-1" en caso de error |

## Estadísticas BW

> **Nota**
>
> Estos eventos de auditoría se envían directamente a SAP BW. Se listan a continuación para su referencia como eventos Web Intelligence, pero no se almacenan en la memoria de datos de auditorías de la plataforma de BI. Están disponibles a partir de SP03 4.2.

| Opción | Valores posibles | Descripción |
| --- | --- | --- |
| Nombre largo<br>`sap.sal.bics.postBWstatistics`<br>Nombre corto<br>`postBWstatistics`<br>Valor predeterminado: `false` | `true`<br>`false` | Activa los siguientes eventos de estadísticas BW:<br>• 20100: Recoge miembros de características BEx<br>• 20101: Recoge resultados de consulta BEx<br>• 20102: Envía variables BEx<br>• 20103: Abre una consulta BEx utilizando la API BICS.<br>• 20104: Sincroniza con BW<br>• 20105: Establece el string de entrada de la variable |

## 24.3.1.4 SAP BusinessObjects Analysis, edición para eventos OLAP

### Sesión MDAS

Se lleva a cabo una operación de sesión MDAS

- ID de tipo de evento: 10300
- Estados:
  - "0" = Se ha abierto una nueva sesión correctamente.
  - "1" = Error en una nueva sesión.
  - "2" = Se ha cerrado una sesión existente.

### Conexión de cubo MDAS

Se lleva a cabo una operación de conexión de cubo.

- ID de tipo de evento: 10301
- Estados:
  - "0" = Se ha abierto una nueva conexión correctamente.
  - "1" = Error en una nueva conexión.
  - "2" = Se ha cerrado una conexión existente.

| Detalles del evento | ID | Descripción |
| --- | --- | --- |
| ID de conexión | 94 | El identificador único de la conexión. |
| Nombre de conexión | 95 | El nombre de la conexión. |
| Tipo de proveedor | 96 | El tipo de proveedor para el cubo. |

| Detalles del evento | ID | Descripción |
|---|---|---|
| Nombre de cubo | 97 | El nombre completo del cubo que se ha usado. |

## 24.3.1.5 Eventos de la consola de la administración de promociones de SAP BusinessObjects

Los siguientes eventos son únicos para el componente Administración de promociones para SAP BusinessObjects.

### Detalles comunes de la Herramienta de administración de promociones de SAP BusinessObjects

Todos los eventos de la administración de promociones tendrán los siguientes detalles de eventos adicionales.

| Detalles del evento | ID | Descripción |
|---|---|---|
| Clúster de elemento | 6 | El CUID de los clústeres afectados cuando la consola de administración de promociones realiza una operación en objetos ubicados en diferentes clústeres. Se generará un detalle de evento para cada clúster afectado. |
| Comentario de elemento | 7 | Información adicional en el objeto. |
| Elemento principal | 8 | Si el elemento es un elemento principal, este detalle se establecerá en "1"; si se trata de un elemento dependiente, se establecerá en "0". |
| Estado del elemento | 9 | Si el elemento de operación falla, este detalle se establecerá en "1"; de lo contrario será "0". |
| Funcionamiento | 10 | Describe el tipo de operación a realizar (por ejemplo, agregar, eliminar o modificar). |

### Configuración de la Herramienta de administración de promociones de SAP BusinessObjects

La configuración de la administración de promociones cambia.

- ID de tipo de evento: 10900

| Detalles del evento | ID | Descripción |
|---|---|---|
| Configuración | 100 | Un usuario visualiza la configuración de la herramienta de administración de promociones. La configuración se muestra como pares de valores separados por comas, por ejemplo: configuración de restauración=enabled, puerto=900. |
| Configuración anterior | 101 | Si se modifica la configuración de la herramienta de administración de promociones para un objeto, se registran los ajustes de configuración anteriores. Usa el mismo formato que Configuración. |
| Configuración posterior | 102 | Si se modifica la configuración de la herramienta de administración de promociones para un objeto, se registran los ajustes de configuración nuevos. Usa el mismo formato que Configuración. |
| Tipo de VMS | 10900 | El tipo de sistema de administración de versiones. |

## Restauración

Un objeto se ha restaurado a una versión anterior del sistema de administración de versiones (VMS).

- ID de tipo de evento: 10901

## Adición de VMS

Se agrega un recurso al VMS.

- ID de tipo de evento: 10902

| Detalles del evento | ID | Descripción |
|---|---|---|
| Versión | 104 | Registra el número de versión del documento en el Sistema de administración de versiones. |

## Recuperación de VMS

Se recupera un recurso del VMS.

- ID de tipo de evento: 10903

| Detalles del evento | ID | Descripción |
|---|---|---|
| Restaurar objeto eliminado | 103 | Indica si un objeto recuperado se ha eliminado del sistema. "0" indica que el objeto no se ha eliminado; "1" indica que el objeto se ha eliminado. |
| Versión | 104 | Registra el número de versión del documento en el VMS. |

## Protección de VMS

Se registra un recurso en el VMS.

- ID de tipo de evento: 10904

| Detalles del evento | ID | Descripción |
|---|---|---|
| Versión | 104 | Registra el número de versión del documento en el VMS. |

## Desprotección de VMS

Se da de baja un recurso del VMS.

- ID de tipo de evento: 10905

| Detalles del evento | ID | Descripción |
|---|---|---|
| Versión | 104 | Registra el número de versión del documento en el VMS. |

## Exportación de VMS

Se exporta un recurso del VMS.

- ID de tipo de evento: 10906

| Detalles del evento | ID | Descripción |
|---|---|---|
| Versión | 104 | Registra el número de versión del documento en el VMS. |

## Bloqueo de VMS

Se bloquea un recurso del VMS para evitar que los usuarios lo editen.

- ID de tipo de evento: 10907

| Detalles del evento | ID | Descripción |
|---|---|---|
| Versión | 104 | Registra el número de versión del documento en el VMS. |
| Bloqueado por | 10901 | El nombre de usuario del usuario que realizó la acción. |

## Desbloqueo de VMS

Se desbloquea un recurso del VMS, lo que permite que los usuarios lo editen.

- ID de tipo de evento: 10908

| Detalles del evento | ID | Descripción |
|---|---|---|
| Versión | 104 | Registra el número de versión del documento en el VMS. |
| Desbloqueado por | 10902 | El nombre de usuario del usuario que realizó la acción. |

## Eliminación de VMS

Se elimina un recurso del VMS.

- ID de tipo de evento: 10909

| Detalles del evento | ID | Descripción |
|---|---|---|
| Versión | 104 | Registra el número de versión del documento en el Sistema de administración de versiones. |

# 25 Eventos

## 25.1 Acerca de Eventos

Los eventos se parecen a los indicadores o a los puntos de verificación que proporcionan información sobre eventos o acciones que ocurren en el servidor. La programación basada en eventos proporciona control adicional sobre los objetos de programación: puede configurar eventos de modo que los objetos se procesen sólo después de que se produzca un evento especificado.

A continuación tiene una lista de eventos que están disponibles en CMC:

### Eventos de Crystal Reports

Los eventos Crystal Report solo lanzan un informe si el informe que espera en el evento está programado y listo para ser ejecutado. Los eventos Crystal Reports se pueden basar en un nuevo archivo y los informes se pueden programar para esperar al lanzamiento del evento.

### Eventos personalizados

Los Evento personalizados también se llaman "eventos manuales". Cada evento personalizado tiene dos propiedades: el nombre del evento y la descripción correspondiente. Los Eventos personalizados se utilizan para lanzar alertas a una Bandeja de entrada de usuario BI y al ID de correo electrónico del usuario. Los Eventos personalizados también le proporcionan la opción de programar objetos basados en el lanzamiento de objetos, configurando las opciones necesarias.

### Eventos de supervisión

Los eventos de supervisión son sistemas generados por el sistema que relacionan con el estado general. La supervisión es una aplicación incorporada en CMC, que permite a los administradores supervisar el estado del sistema. Lo aspectos más importantes de la supervisión son las vigilancias y las métricas.

Las vigilancias le permiten fijar umbrales para más de 250 métricas del sistema. Recibe una notificación cuando se violan los umbrales fijados.

> Ejemplo
>
> Si tiene una vigilancia que supervisa el espacio de disco que consume el FRS de salida, se le notifica cuando el consumo alcanza el volumen de espacio de disco especificado.

## Eventos de sistema

Existen dos tipos de eventos de sistema:

- **Eventos basados en archivos**
  Los Eventos basados en archivos se basan en cualquier archivo ubicado en una vía de acceso. Por ejemplo, si un archivo está ubicado en una de las vías de acceso del servidor, puede ejecutar informes basando la programación en la vía de acceso de un archivo. Desde una perspectiva empresarial, si considera que las tablas para la realización de informes se deben cargar casa mes/semana/día, poner un archivo en la vía de acceso una vez se han cargado los informes, lanza un sistema de eventos basado en archivos.
- **Eventos basados en programación**
  Los Eventos basados en programación se utilizan para ejecutar informes en objetos BI de manera secuencial. Esta definición de evento consta de tres acciones: éxito, error y éxito o error. Esto se debe a que el estado de un objeto en ejecución, que en cualquier momento, puede ser de éxito o error.

## Notificaciones de usuario

Los administradores utilizan los eventos de notificación de usuario para notificar a usuarios finales BI, que están utilizando la plataforma de lanzamiento, sobre eventos importantes. Los administradores solo pueden notificar a usuarios seleccionados sobre mensajes críticos y otra información relacionada en el momento programado (por ejemplo, una parada del sistema). El mensaje de alerta aparece como ventana emergente de notificación en la pantalla de la plataforma de lanzamiento BI cuando el usuario inicia sesión.

## Eventos BW

En el sistema BW, el *Evento desencadenador de BOE*, un tipo de proceso en una cadena de procesos, lanza eventos BW para la plataforma BI. Cada evento BW comprende un nombre de evento y su descripción. Los eventos BW se utilizan para configurar una programación basada en eventos de informes que se basan en una fuente de datos BW. Un sistema BW lanza un evento BW cuando se modifican datos en el sistema. Los eventos BW también pueden lanzar alertas a una Bandeja de entrada BI y al ID de correo electrónico del usuario.

# 25.1.1 Notificaciones de usuario

La capacidad de notificación permite a un Administrador enviar mensajes de alerta del CMC al usuario. Utilizando esta función, los administradores pueden notificar a usuarios seleccionados sobre mensajes críticos y otra información relacionada (por ejemplo, una parada del sistema). El mensaje de alerta aparece como ventana emergente de notificación en la esquina superior derecha de la pantalla de la plataforma de lanzamiento BI cuando el usuario inicia sesión.

## 25.1.1.1 Editar un Evento de notificación

El evento de notificación en un plug in programable. Al crear un evento de notificación, se pide al administrador que especifique la fecha y la hora de "Inicio" y "Fin". El servidor de tarea adaptativo es responsable de la programación, creando una instancia de programación cuando llega la hora de "Inicio" especificada de la notificación. El AJS pasa la alerta a la bandeja de entrada de alertas de la plataforma de lanzamiento. Estas notificaciones aparecen en la esquina superior derecha de la pantalla de la plataforma de lanzamiento de BI.

Para crear un evento de notificación proceda de la forma siguiente:

1. Inicie una sesión en la CMC.
2. Desde la página de inicio de CMC, seleccione *Eventos* del menú desplegable.
3. Desde el panel *Eventos* de la derecha, haga clic con el botón derecho en *Notificaciones de usuario* y navegue a *Nuevo* > *Nueva notificación*.

   Aparece la ventana emergente *Nueva notificación*.
4. Para programar un evento de notificación proceda de la forma siguiente:
   a. Seleccione el huso horario correspondiente del menú desplegable *Huso horario*.
   b. Fije la correspondiente *Fecha/Hora de inicio*.
   c. Fije la correspondiente *Fecha/Hora de fin*.

   > **Nota**
   >
   > - La hora de *Finalización* no puede ser anterior a la de *Inicio*.
   > - La diferencia entre la hora de *Inicio* y *Finalización* no puede ser mayor de 14 días.
   > - Independientemente del huso horario seleccionado, la hora de *Inicio* no puede ser anterior a la hora del servidor CMS. Si la hora de *Inicio* es anterior a la del servidor CMS, la notificación no se lanzará.

   d. En el cuadro *Título de notificación*, especifique el título de la notificación.

   > **Nota**
   >
   > El *Título de notificación* no puede tener más de 256 caracteres.

   e. En la casilla *Descripción*,indique una descripción adecuada de la notificación.

   > **Nota**
   >
   > La *Descripción* no puede tener más de 1024 caracteres.

   > **Nota**
   >
   > Puede seleccionar mandar la notificación al correo electrónico del usuario, marcando la casilla de selección *Enviar este mensaje como notificación al ID de usuario del correo electrónico*
5. Seleccione *Aceptar*.

Ha editado correctamente un evento de notificación.

> **Nota**
>
> En la página Propiedades de notificación, el tiempo creado y modificado refleja el tiempo ded servidor del CMS
>
> El administrador puede deshabilitar la emergencia automática del banner en la plataforma de lanzamiento BI modificando el archivo `BIlaunchpad.properties` y deshabilitando el sondeo configurando el campo `Notification.enabled` en `false`. Para que el sondeo de notificaciones se ejecute por defecto, se debe habilitar la propiedad `pinger.enabled` del archivo `global.properties`. Si el sondeo y el ping no están habilitados, la ventana emergente de notificación solo aparece cuando el usuario actualiza la página, accede por primera vez o vuelve a acceder cuando la notificación está activa.
>
> El sondeo tiene lugar una vez cada 3 minutos en la rampa de lanzamiento BI.

## 25.1.1.2 Seleccionar una Audiencia de notificación

La función de notificación le permite seleccionar la audiencia necesaria para cada notificación que crea.

Para seleccionar la audiencia para una notificación, proceda de la forma siguiente:

1. Haga clic con el botón derecho sobre la notificación que ha creado y seleccione *Administrar suscriptores* en el menú contextual.

   Aparece la ventana emergente *Administrar suscriptores*.
2. Seleccione *Añaadir* del panel *Lista de suscriptores*.

   Aparece la ventana emergente *Añadir suscriptores*.
3. Seleccione los usuarios/grupos de usuarios a los que quiere notificar.
4. Haga clic en *Agregar suscripciones predeterminadas*.

   Aparece la ventana emergente *Añadir suscriptores*.
5. Seleccione *Guardar y cerrar* de la ventana emergente *Administrar suscriptores*.

Ha seleccionado correctamente la audiencia para una notificación.

> **Nota**
>
> - No puede modificar la lista de suscripción después de lanzar la notificación.
> - Ahora puede enviar notificaciones a los usuarios de OpenDocument.

## 25.1.1.3 Editar un Evento de notificación

Para editar un evento de notificación proceda de la forma siguiente:

1. Inicie una sesión en CMC.
2. Desde la página de inicio de CMC, seleccione *Eventos* del menú desplegable.
3. Desde el panel *Eventos* de la izquierda, seleccione *Notificaciones de usuario*.

4. Haga clic con el botón derecho sobre la notificación que quiera editar y seleccione *Editar evento* del menú contextual.

   Aparecerá el cuadro de diálogo *Editar evento*.
5. Editar los parámetros necesarios del evento de notificación.

   > **Nota**
   >
   > Puede editar los siguientes parámetros de un evento de notificación:
   > - Zona horaria
   > - Fecha/Hora de inicio
   > - Fecha/Hora de fin
   > - Título de la notificación
   > - Descripción
   > - Administrar suscriptores
6. Seleccione *Aceptar*.

Ha editado correctamente un evento de notificación.

> **Nota**
>
> Si edita un evento de notificación navegando a *Eventos* > *Notificaciones de usuario* > *Propiedades*, la notificación no se lanza hasta que seleccione *Aceptar* en la página *Editar evento*.

# 26 Búsqueda de plataforma

## 26.1 Información de Búsqueda de plataforma

Búsqueda de plataforma permite buscar contenido en el repositorio dentro de la plataforma de BI. Refina los resultados de búsqueda agrupándolos en categorías y clasificándolos en función de su importancia.

En esta versión de la plataforma de BI, la búsqueda de plataforma tiene las siguientes funciones:

- Buscar contenido de la plataforma de BI.
- Sugerir una consulta para crear un documento si no puede encontrar un documento actual.
- Admitir la indexación continua y basada en programaciones.
- Admitir la indexación en un entorno de agrupación en clúster.
- Configurar y modificar el nivel de indexación.
- Proporcionar opciones de configuración de búsqueda avanzada.
- Admitir la búsqueda e indexación multilingües.
- Proporcionar una sintaxis de búsqueda avanzada.
- Admitir metadatos, contenido y restricciones dinámicas.
- Admitir la corrección automática según la carga del sistema.

> **Nota**
>
> El índice no migra al migrar de una versión anterior a una versión nueva.

### 26.1.1 SDK de la Búsqueda de plataforma

La búsqueda de plataformas admite un SDK público que funcione como interfaz entre la aplicación cliente y Búsqueda de plataforma. Está abierto al público para ayudarle a personalizar el servicio de búsqueda e integrarlo con su aplicación.

Al enviar un parámetro de solicitud de búsqueda mediante la aplicación cliente al nivel de SDK, el nivel de SDK convierte el parámetro de solicitud al formato codificado XML y lo pasa al servicio de búsqueda de plataformas.

Para obtener más información acerca de la API de búsqueda de plataforma, consulte el *Manual de consulta de la API Java de la plataforma de Business Intelligence*.

### 26.1.2 Entorno agrupado

La búsqueda de plataforma puede compartir la carga en varios nodos de un entrono en clúster. El despliegue en el entrono en clúster optimiza los recursos y mejora el rendimiento del servidor.

La búsqueda de plataforma admite la agrupación en clúster horizontal y vertical para las funciones de búsqueda e indexación. Con los entornos en clúster, se optimiza el rendimiento de los procesos de búsqueda e indexación.

Para obtener más información sobre cómo configurar la ubicación del índice de búsqueda de plataforma en un entorno agrupado, consulte esta nota SAP.

### Equilibrio de carga

La Búsqueda de plataforma admite el equilibrio de carga tanto para la indexación como para la búsqueda. En un entorno agrupado, las solicitudes de indexación y búsqueda pueden ejecutarse en varios nodos para compartir la carga. Cada nodo funciona independientemente para indexar el contenido y crear índices delta. No obstante, sólo un nodo del clúster actuará como índice maestro y fusionará los índices delta en el índice maestro. Todos los nodos tienen acceso al índice maestro. Esto permite las solicitudes de búsqueda simultáneas.

### Recuperación tras fallos

El mecanismo de conmutación por error garantiza que los usuarios puedan seguir buscando y usando la operación de indexación sin que se interrumpa. Cuando un nodo del clúster deja de estar disponible debido a un error técnico o a actividades relacionadas con el mantenimiento, otro nodo asume automáticamente el proceso de indizar y buscar solicitudes.

## 26.2 Configuración de la búsqueda de plataforma

### 26.2.1 Desplegar OpenSearch

La búsqueda de plataformas admite el estándar OpenSearch, lo que permite que las aplicaciones cliente usen el estándar o formato de OpenSearch para comunicarse con la búsqueda de plataformas. OpenSearch no se instala de forma predeterminada con la suite de SAP BusinessObjects Business Intelligence, por lo que los usuarios deben implementarlo manualmente como archivo WAR independiente (`opensearch.war`) en un servidor de aplicaciones como Tomcat o usando la herramienta WDeploy. El instalador copia este archivo en el directorio `<DIRINSTALACIÓN>\warfiles\OpenSearch`.

> **Nota**
>
> Los programas cliente debe seguir los estándares OpenSearch para comunicarse con la búsqueda de plataforma.

> **Nota**
>
> Al instalar la plataforma de BI, el servidor de aplicaciones de Tomcat se instala de forma predeterminada.

### 26.2.1.1 Despliegue manual

Para desplegar OpenSearch en un entorno de la plataforma de BI, lleve a cabo los pasos siguientes:

1. Vaya a la siguiente ubicación: `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\`.
2. Copie la carpeta OpenSearch en `<DIRINSTALACIÓN>\tomcat\webapps\`.
3. Cambie los parámetros de configuración en el archivo `OpenSearch\WEB-INF\config.properties`:
   - CMS: nombre del CMS con número de puerto: `<Nombre CMS>:<Número puerto>`.
   - OpenDocURL: la dirección URL de la aplicación: `http://<tomcathost>:<connector port>/BOE/OpenDocument/opendoc/openDocument.jsp`.
   - Proxy.rpurl: el nombre del servidor proxy inverso es necesario si desea usar un proxy inverso.
   - Proxy.opendoc.rpurl: el nombre del servidor proxy inverso de opendoc es necesario si desea usar el proxy inverso.
4. Reinicie el servidor de aplicaciones de Tomcat para desplegar OpenSearch.

### 26.2.1.2 Despliegue con WDeploy

Para Windows, los comandos se mencionan como `wdeploy.bat <parameters>`. Para UNIX, los comandos se mencionan como `wdeploy.sh <parameters>`.

1. Actualice el archivo `config.<ApplicationServer>` ubicado en `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf` con los parámetros de servidor de aplicaciones Web necesarios (por ejemplo, el directorio de instalación, el nombre de la instancia, el puerto administrativo, el nombre de usuario administrador y la contraseña de administrador).
2. Modifique los parámetros siguientes en el archivo `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties`:
   a. Para el parámetro `CMS`, indique `<CMSName>:<Port>`.
   b. Para el parámetro `OpenDocURL`, indique la dirección URL de la aplicación OpenDocument.

      La dirección URL debería ser `http://<WebApplicationServerHost>:<ConnectorPort>/BOE/OpenDocument/opendoc/openDocument.jsp`.
   c. (Necesario para proxy inverso) Para el parámetro `Proxy.rpurl`, indique el nombre del servidor proxy inverso.
   d. (Necesario para proxy inverso) Para el parámetro `Proxy.opendoc.rpurl`, indique el nombre del servidor proxy inverso de la aplicación OpenDocument.
3. Ejecute el comando de despliegue `wdeploy.bat <WebApplicationServer> -Dapp_source_tree=<ParentFolderOpenSearchWebApp> -DAPP=OpenSearch` desde `<InstallDir>\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
   Por ejemplo, el siguiente comando despliega OpenSearch en un servidor de aplicaciones Web de WebSphere 7:

   ```
   wdeploy.bat websphere7 -Dapp_source_tree="<InstallDir>\SAP BusinessObjects
   Enterprise XI 4.0\warfiles" -DAPP=OpenSearch deploy
   ```
4. Reinicie el servidor de aplicaciones Web.

## 26.2.2 Configuración del proxy inverso

Para implementar las aplicaciones Web en un servidor de aplicaciones Web ubicado detrás de un servidor proxy inverso, configure el servidor proxy inverso para que asigne las solicitudes de dirección URL entrantes al archivo WAR correcto:

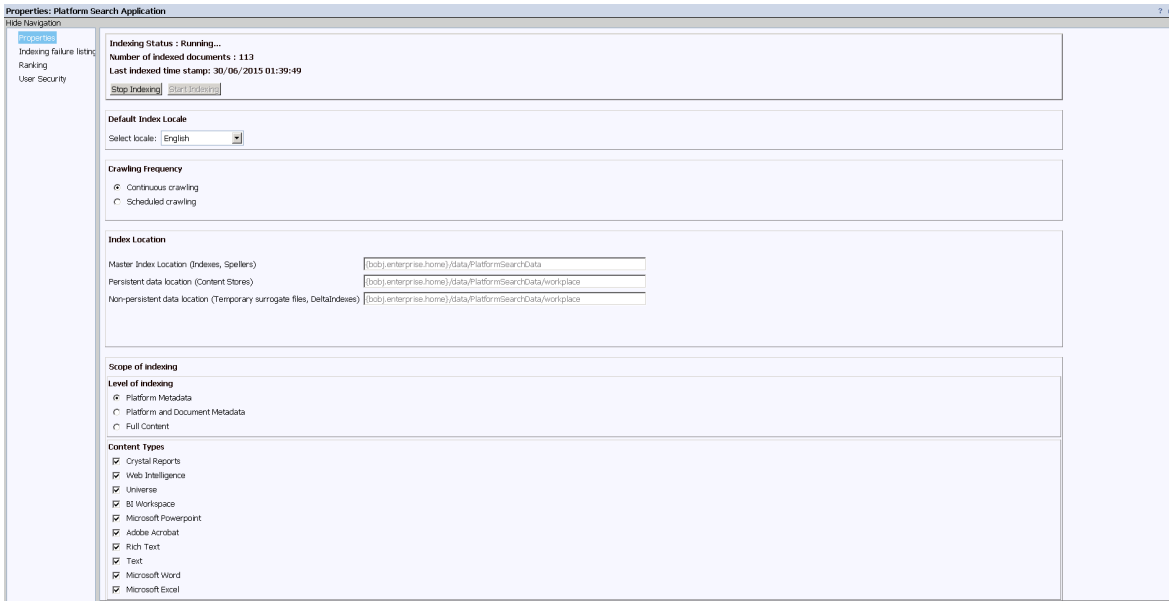
Para ilustrar los pasos del proceso de configuración, hemos usado como ejemplo un servidor proxy inverso de Apache 2.2. Para configurar el servidor proxy inverso de Apache 2.2 para OpenSearch:

1. Configure el proxy inverso y realice los cambios en el archivo`WEB-INF\config.properties` de OpenSearch.
2. Habilite los siguientes parámetros de contexto y cambie los valores en consecuencia.
   - `proxy.rpurl`: es la dirección URL del proxy inverso para OpenSearch (como `http://machineIPAddress/RP/OpenSearch/`).
   - `proxy.opendoc.rpurl`: es la dirección URL del proxy inverso para Open Doc (como `http://machineIPAddress/RP/BOE/`).
3. Actualice el archivo `httpd.conf` que se encuentra en la carpeta de instalación del proxy inverso de Apache con la configuración siguiente:
   - `ProxyPass /RP/BOE/OpenDocument/ http://<host de Tomcat>:<puerto de conector>/BOE/OpenDocument/`
   - `ProxyPass /RP/OpenSearchRP/ http://<host de Tomcat>:<puerto de conector>/OpenSearch/`
   - `ProxyPassReverseCookiePath /BOE /RP/BOE`
   - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`
4. Reinicie el servidor proxy inverso de Apache 2.2.

## 26.2.3 Configurar las propiedades de aplicaciones en la CMC

Para configurar las propiedades de la aplicación de búsqueda en plataforma, complete esos pasos:

1. Vaya al área *Aplicaciones* de CMC.
2. Seleccione la *aplicación de búsqueda en plataforma*.
3. Haga clic en *Administrar* > *Propiedades*. Aparece el cuadro de diálogo *Propiedades de la aplicación de búsqueda en plataforma*.




4. Configurar los ajustes de búsqueda de la plataforma:

| Opción | Descripción |
|---|---|
| Estadísticas de búsqueda | Búsqueda de plataforma ofrece las siguientes estadísticas de búsqueda:<br>• Estado de indexación: muestra el estado del proceso de indexación.<br>• Cantidad de documentos indexados: muestra el número de documentos indexados.<br>• Cronomarcador de última indexación: muestra la fecha y la hora de la última indexación del documento. |
| Iniciar/detener indexación | Las opciones Iniciar o detener indexación permiten iniciar o detener el proceso de indexación cuando desee alternar de la inspección continua a la inspección programada, o por motivos de mantenimiento.<br>Para detener la indexación, haga clic en *Detener indexación*. |
| Configuración regional del índice predeterminada | La búsqueda de plataformas usa la configuración regional especificada en la CMC para indexar todos los documentos de BI no localizados. Una vez que se localiza el documento, se usa el analizador de idioma correspondiente para la indexación.<br>La búsqueda se basa en la configuración regional del producto del cliente, y la ponderación se proporciona en la configuración regional del producto del cliente.<br>Puede configurar la ponderación en las propiedades de configuración de la CMC. |

| Opción | Descripción |
| --- | --- |
| Frecuencia de inspección | Puede indexar todo el repositorio de la plataforma de BI mediante las opciones siguientes:<br>• Inspección continua: con esta opción, la indexación es continua cuando se indexa el repositorio, siempre que se agrega, modifica o elimina un objeto. Permite ver o trabajar con el contenido de la plataforma de BI más actualizado. Por defecto, la inspección continua actualiza constantemente el repositorio con las acciones que realice. La inspección continua trabaja sin la intervención del usuario y reduce el tiempo necesario para indexar un documento.<br>• Inspección programada: con esta opción, la indexación se basa en la programación definida con las opciones de programación.<br>Para obtener información acerca de la programación de un objeto, consulte la sección *Programar un objeto* de la Búsqueda de plataformas de la *Ayuda online de la CMC de la plataforma de SAP BusinessObjects Business Intelligence*.<br>**Nota**<br>• Si selecciona *Inspección programada* y define la *Periodicidad* con una opción que no sea *Ahora*, la búsqueda de plataformas muestra la marca de fecha y hora cuando se programa el documento para que se indexe a continuación.<br>• Si selecciona *Inspección programada*, el botón *Iniciar indexación* se activa y el botón *Detener indexación* se desactiva.<br>• Una vez completada la programación, el botón *Detener indexación* se desactiva. |

| Opción | Descripción |
| --- | --- |
| Ubicación de índice | Los índices se almacenan en carpetas compartidas en las siguientes ubicaciones:<br>• Ubicación del índice maestro (índices y corrector ortográfico): los índices maestros y el corrector ortográfico que se almacenan en esta ubicación. Durante una búsqueda, los resultados iniciales se recuperar mediante el Índice maestro y los índices de corrector ortográfico se usan para recuperar sugerencias. En un despliegue de la plataforma de BI en clúster, esta ubicación debe estar en un sistema de archivos compartido al que se pueda acceder desde todos los nodos del clúster.<br>• Ubicación de datos persistentes (almacenes de contenido): el almacén de contenido se encuentra en esta ubicación. Se crea desde la ubicación de índice maestro y permanece en sincronización con ella. El almacén de contenido se usa para generar facetas y procesar los resultados iniciales que se generan desde la ubicación del índice maestro. En un despliegue de la plataforma de BI en clúster, los almacenes de contenido se generan en cada nodo.<br>La ubicación de datos persistentes es la única ubicación de índice que se ve afectada por el entorno en clúster ya que contiene carpetas de almacén de contenido. Si un equipo tiene un único servicio de búsqueda, existirá una sola ubicación de contenido. Por ejemplo, {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Server Name>\ContentStores.<br>Sin embargo, si en un entorno agrupado existen varios servicios de búsqueda, cada servicio tendrá una única ubicación de almacén de contenido. Por ejemplo, si existen dos instancias de un servidor que se están ejecutando, las ubicaciones del almacén de contenido serán las siguientes:<br>1. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nombre de servidor>\ContentStores.<br>2. {bobj.enterprise.home}\data\PlatformSearchData\workspace\<Nombre de servidor 1>\ContentStores.<br>• Ubicación de datos no persistentes (archivos temporales, índices Delta): en esta ubicación, los índices Delta se crean y almacenan temporalmente antes de fusionarse con el índice maestro. Los índices desde esta ubicación se eliminan cuando se han fusionado con el índice maestro. Además, los archivos suplentes (fuera de los extractores) se crean en esta ubicación y se almacenan temporalmente hasta que se convierten en índices delta.<br>**Nota**<br>• La ubicación del índice maestro tiene que ser una ubicación compartida.<br>• Debe hacer clic en *Detener indexación* para modificar la ubicación del índice.<br>• Si modifica la ubicación de un índice, debe copiar el contenido en una nueva ubicación, de lo contrario la información de indexación se perderá.<br>• Los archivos de indexación pueden almacenar información personal y confidencial, especialmente cuando seleccione indexar el contenido del documento. Debe permitir solo a un usuario del sistema acceder a la carpeta compartida y debe almacenar las carpetas compartidas en un entorno encriptado para evitar el robo de datos. |

| Opción | Descripción |
| --- | --- |
| Nivel de indexación | Puede ajustar el contenido de la búsqueda definiendo el nivel de indexación de los modos siguientes:<br>• Metadatos de plataforma: solo se crea un índice para la información de los metadatos de la plataforma, como títulos, palabras clave y descripciones de los documentos. De forma predeterminada se selecciona esta opción.<br>• Metadatos de plataforma y documento: este índice incluye los metadatos de la plataforma, así como los metadatos del documento. Los metadatos del documento incluyen la fecha de creación, la fecha de modificación y el nombre del autor.<br>• Contenido completo: este índice incluye los metadatos de plataforma, metadatos de documentos y otro contenido como:<br>  • El contenido real del documento<br>  • El contenido de las solicitudes y LOV<br>  • Diagramas, gráficos y etiquetas<br>**Nota**<br>La indexación completa de contenido no es compatible con documentos de Analysis Office y Lumira. Solo la indexación de metadatos es compatible con documentos de Analysis Office y Lumira.<br>**Nota**<br>Al modificar el nivel de indexación, se inicializa la indexación para que se actualice todo el repositorio de la plataforma de BI. |

| Opción | Descripción |
| --- | --- |
| Tipos de contenido | Puede seleccionar los siguientes tipos de contenido para la indexación:<br>• Crystal Reports<br>• Web Intelligence<br>• Universo<br>• Área de trabajo de BI<br>• Analysis Office<br>• Lumira<br>• Microsoft PowerPoint<br>• Adobe Acrobat<br>• Texto enriquecido<br>• Texto<br>• Microsoft Word<br>• Microsoft Excel<br><br>El filtro del tipo de contenido no se aplica para la indexación de metadatos de la plataforma. Independientemente de los tipos de contenido que seleccione, la indexación de metadatos de la plataforma tiene lugar para todos los tipos de objeto soportados y los resultados de la búsqueda en la plataforma de lanzamiento de BI devuelven todos los objetos para la palabra clave relacionada con los metadatos de la plataforma.<br><br>El filtro del tipo de contenido es relevante para la indexación de metadatos de la plataforma (autor, cabecera, pie de página, etc. del documento) y la indexación de contenido (gráficas, gráficos, tabla con un informe). Según el nivel de indexación y los tipos de contenido que seleccione, la plataforma busca índices para los metadatos del documento y el contenido para los tipos de objetos seleccionados del repository y solo aquellos objetos que aparezcan en los resultados de la búsqueda de la plataforma de lanzamiento de BI, al buscar palabras clave relacionadas con los metadatos y contenido del documento. |
| Regenerar índice | Esta opción elimina el índice existente y vuelve a indexar todo el repositorio.<br><br>Puede seleccionar la opción *Regenerar índice* tanto si la indexación se está ejecutando o está detenida. El índice existente se elimina al guardar las modificaciones realizadas en la página de propiedades. Sin embargo, si la indexación está detenida, el índice no se vuelve a generar hasta que reinicia la indexación.<br><br>Si no desea que la búsqueda en plataforma vuelva a indexar los documentos, debe anular la selección de *Regenerar índice* antes de hacer clic en *Iniciar indexación*. |

| Opción | Descripción |
| --- | --- |
| Documentos excluidos de la indexación | La opción *Documentos excluidos de la indexación* excluye de la indexación los documentos. Por ejemplo, puede que no desee que se puedan buscar informes de Crystal extremadamente grandes para asegurar que los recursos del servidor de aplicaciones de informes no se sobrecargan. De igual modo, puede que no desee que se indexen publicaciones con cientos de informes personalizados.<br><br>Al excluir documentos concretos, puede evitar que la Búsqueda de plataforma acceda a ellos. Es importante tener en cuenta que si un documento ya se ha indexado antes de ponerlo en esta categoría, se podrán seguir realizando búsquedas en él. Para asegurar que los documentos del grupo *Documentos excluidos de la indexación* no se puedan buscar, debe volver a crear el índice.<br><br>De forma predeterminada, solo la cuenta del administrador tiene control completo de la opción *Documentos excluidos de la indexación*. Otros usuarios con los siguientes derechos solo pueden agregar documentos al grupo *Documentos excluidos de la indexación*:<br>• Derechos de visualización y edición en la categoría<br>• Editar el documento directamente |
| Otra configuración: Omitir instancia | Por defecto, las instancias de documentos se seleccionan para indexar. Esto provoca un aumento del tamaño del índice, que a su vez aumenta el consumo del espacio en disco. El tamaño de la carpeta "Lucene Index Engine" dentro de la carpeta PlatformSearchData aumenta considerablemente a causa de la indexación de un gran número de instancias en el repository. Si hay millones de documentos (o más) y muchos de ellos también tienen un gran número de instancias existentes (junto con instancias programadas generadas en intervalos regulares) en el sistema, el tamaño de la carpeta "Lucene Index Engine" aumentará demasiado, incluso si el nivel de indexación se fija en "Metadatos de plataforma".<br><br>La opción Búsqueda de plataforma omite instancia le permite controlar la indexación de instancias activando o desactivando mediante la casilla de selección "Otra configuración: Omitir instancia" en la página de propiedades "Aplicación de búsqueda de plataforma" en CMC.<br><br>**Nota**<br>• Si Activa/Desactiva Omitir instancia, tendrá que reiniciar el servidor de tratamiento de adaptación de búsqueda de plataforma. Esta modificación afectará a todos los niveles de indexación.<br>• Si modifica Omitir instancia y desea que se apliquen las modificaciones a todas las instancias existentes (por ejemplo, seleccionar para indexar), tendrá que reestructurar el índice. |

| Opción | Descripción |
| --- | --- |
| Objetos excluidos de la indexación | La opción *Objetos excluidos de la indexación* excluye de la indexación los objetos. Por ejemplo, puede que no desee que se puedan buscar determinados objetos para asegurar que los recursos del servidor de aplicaciones de informes no se sobrecargan.<br><br>Al excluir objetos concretos, puede evitar que la Búsqueda de plataforma acceda a ellos. Es importante tener en cuenta que si un objeto ya se ha indexado antes de ponerlo en esta categoría, se podrán seguir realizando búsquedas en él. Para asegurar que los documentos del grupo *Objetos excluidos de la indexación* no se puedan buscar, debe volver a crear el índice.<br><br>Lista de objetos que se pueden excluir de la indexación:<br>• CrystalReport<br>• Webi<br>• LCMJob<br>• Universe<br>• Excel<br>• PDF<br>• PowerPoint<br>• Rtf<br>• Txt<br>• Word<br>• AFDashboardPage<br>• ObjectPackage<br>• QaaWS<br>• Perfil<br>• Evento<br>• Debates<br>• InformationDesigner<br>• MDAnalysis<br>• Publicación<br>• Documentos agnósticos<br>• Analytic<br>• Hipervínculo<br>• Programa<br>• pQuery<br>• DSL.MetaDataFile<br>• Acceso directo<br>• DataDiscoveryAlbum<br>• AO.Workbook<br>• VISI.Story<br>• VISI.Dataset |

| Opción | Descripción |
| --- | --- |
| | • VISI.Lums<br>• VISILums<br>• Usuario<br>• UserGroup |

5. Haga clic en *Guardar y cerrar*.

> **Nota**
>
> Si el usuario no selecciona la opción *Regenerar índice* y cambia el nivel de indexación o selecciona o deselecciona extractores, entonces el índice se actualiza incrementalmente desde el principio sin eliminar el índice existente.

## 26.3 Uso de la búsqueda de plataforma

### 26.3.1 Indexación de contenido en el repositorio CMS

La indexación es un proceso continuo que conlleva las siguientes tareas secuenciales:

1. Inspección: se trata de un mecanismo que sondea el repositorio del CMS e identifica los objetos que están publicados, se han modificado o eliminado. Se puede llevar a cabo de dos modos: inspección continua y programada.
   Para obtener más información acerca de la inspección continua y programada, consulte el tema *Configurar las propiedades de aplicación* en Temas relacionados.
2. Extracción: la extracción es un mecanismo para llamar a los extractores según el tipo de documento. Existe un extractor dedicado para cada tipo de documento disponible en el repositorio. Los tipos de documentos nuevos pueden ser susceptibles de búsqueda definiendo nuevos complementos de extractor. Cada uno de estos extractores es suficientemente escalable para extraer el contenido de documentos grandes que contienen muchos registros.
   Se admiten los extractores siguientes:
   - Extractor de metadatos
   - Extractor del informe de Crystal
   - Extractor de Web Intelligence
   - Extractor de universos
   - Extractores agnósticos (documentos de MS Office 2003 y 2007 y documentos PDF)

   Para obtener más información sobre los tipos de documentos que se pueden buscar, consulte el tema *Tipos de contenido que se pueden buscar* en Temas relacionados.
3. Indexación: se trata de un mecanismo que indexa todo el contenido extraído mediante una biblioteca de terceros denominada Apache Lucene Engine. El tiempo que tarda en realizarse la indexación varía en función del número de objetos del sistema y el tamaño y tipo de documentos.
   Para la ejecución correcta de la indexación, deben ejecutarse y activarse los siguientes servidores:
   - Servidor del repositorio de archivos de entrada (IFRS)

- Servidor del repositorio de archivos de salida (OFRS)
- Servidor de administración central (CMS)
- El servidor de procesamiento de Adaptive (APS) que aloja el servicio de búsqueda de plataforma

Si el tipo de objeto se selecciona como informe de Web Intelligence o Crystal, se deben ejecutar el servidor de procesamiento de Web Intelligence o el servidor de aplicaciones de informes de Crystal y deben estar habilitados para los tipos de objetos respectivos seleccionados.

4. Almacén de contenido: contiene información como el ID, el CUID, el nombre, la clase y la instancia extraída del índice principal en un formato que puede leerse cómodamente. Esto acelera el proceso de búsqueda.

### Información relacionada

Configurar las propiedades de aplicaciones en la CMC [página 945]
Tipos de contenido que se puede buscar [página 956]

## 26.3.2 Lista de errores de indexación

La lista de errores de indexación proporciona una lista de documentos que no se pueden indexar. La búsqueda de plataforma ofrece tres intentos de indexar un documento. Si un documento no se puede indexar, se enumera en la lista de errores de indexación.

Para ver la lista de errores de indexación, complete estos pasos:

1. Vaya al área "Aplicaciones" de la CMC.
2. Seleccione la *aplicación de búsqueda en plataforma*.
3. Elija *Acciones > listado de errores de indexación*.

   Aparece el cuadro de diálogo "Aplicación de búsqueda en plataforma" donde se muestra una lista de documentos con los detalles siguientes:
   - Título: muestra el título del documento que no se ha logrado indexar.
   - Tipo: muestra el nombre del tipo de documento, como Crystal Report y Web Intelligence, y la ubicación del documento.
   - Tipo de error: muestra el código de error y el motivo del error de indexación del documento. Haga clic en el hipervínculo Más información para averiguar más sobre el seguimiento de pila de la causa del error.
   - Hora de último intento: muestra la fecha y hora del último intento de indexar un documento.

## 26.3.3 Búsqueda de resultados

### 26.3.3.1 Búsqueda previa

#### 26.3.3.1.1 Consultas sugeridas

Al usar la búsqueda de plataforma, un usuario puede estar intentando encontrar respuestas a preguntas específicas, en lugar de buscar un objeto específico. Estas preguntas puede que se respondan o no en informes disponibles en el repositorio de la plataforma de BI.

Búsqueda de plataforma analiza la estructura de los universos y de los informes existentes del repositorio y compara esta información con la solicitud de búsqueda que ha proporcionado el usuario para sugerir nuevas consultas de SAP BusinessObjects Web Intelligence que pueden ayudar a los usuarios a encontrar las respuestas a sus preguntas.

Para crear informes potenciales, Búsqueda de plataforma relaciona las palabras de todos los universos para dimensión, indicador, condición y filtro.

La aplicación de Búsqueda de plataforma busca coincidencias en la información siguiente sobre los universos o los documentos existentes de Web Intelligence:

- Los indicadores en los universos que coinciden con las palabras de la entrada de búsqueda. Cuando un indicador coincide con uno de los términos de búsqueda, dicho indicador se utilizará en el documento de Web Intelligence resultante.
- Los nombres de dimensión en los universos que coinciden con las palabras de la entrada de búsqueda. Cuando un nombre de dimensión coincide con uno de los términos de búsqueda, el documento de Web Intelligence resultante desglosa la información de esta dimensión.
- Los filtros de consulta se pueden usar para centrar los datos mostrados en el documento. Estos filtros de consulta se generan mediante el análisis de la entrada de búsqueda.
  - Si el nombre de una condición de universo coincide con uno de los términos de búsqueda, la condición se utiliza como el filtro.
  - Si hay valores de campo en documentos existentes de Web Intelligence cuyos nombres coincidan con los términos de búsqueda, se creará un filtro a partir de la dimensión del informe histórico con el valor coincidente, usando un "igual a" como operador de condición.

Si la aplicación de búsqueda de plataforma ha realizado suficientes coincidencias de modo que el documento resultante contendrá dos campos de resultado y un filtro, se considera que la consulta está lista para ejecutarse. En este caso, el usuario puede hacer clic para ver el informe completado.

Si no hay un número suficiente de coincidencias entre los universos y el documento, puede editar la consulta antes de ejecutarla.

La búsqueda de plataforma sugiere varias consultas si varios universos coinciden con a entrada de búsqueda o si aparece la misma palabra en dos coincidencias distintas, como en el nombre de una dimensión y como un valor de filtro.

## 26.3.3.1.2 Tipos de contenido que se puede buscar

En el contenido publicado en la plataforma de BI se pueden realizar búsquedas con Búsqueda de plataforma. Los tipos de objeto se enumeran a continuación con el contenido indexado correspondiente:

| Tipo de objeto | Contenido indexado |
|---|---|
| Crystal Reports 2020 | Título, descripción, fórmula de selección, datos guardados, campos de texto de cualquier sección, valores de parámetro y subinformes. |
| Documentos de Web Intelligence | Título, descripción, nombre de los filtros de universo usados en el informe, datos guardados, constantes en la condición de filtro definida localmente en el informe, nombre de los indicadores de universo usados en el informe, nombre de los objetos de universo usados en el informe, datos del conjunto de registros y texto estático de las celdas. |
| Documentos de Microsoft Excel (2003 y 2007) | Datos de todas las celdas que no estén vacías, campos de la página Resumen de las propiedades del documento (título, asunto, autor, compañía, categoría, palabras clave y comentarios), y texto en las cabeceras y pies de página del documento.<br><br>Para las celdas que utilizan cálculos o fórmulas, se puede buscar el valor posterior a la evaluación. Para los valores numéricos o de fecha/hora, se pueden realizar búsquedas en los datos sin formato. |
| Documentos de Microsoft Word (2003 y 2007) | Texto de todos los párrafos y tablas, campos de la página Resumen de las propiedades del documento (título, asunto, autor, compañía, categoría, palabras clave y comentarios), texto en las cabeceras y pies de página del documento y texto numérico. |
| Archivos RTF, PDF. PPT y TXT | Se puede buscar en todo el texto de estos archivos. |
| LCMJob, ObjectPackage, consulta de servicios Web (QaaWS), perfil, debates, InformationDesigner, widgets para la plataforma de SAP BusinessObjects BI, MDAnalysis, publicaciones, analítica e hipervínculo | El contenido de los metadatos se puede buscar. |

| Tipo de objeto | Contenido indexado |
| --- | --- |
| Eventos | Todos los eventos como eventos personalizados, eventos del sistema, eventos de Crystal Reports y eventos de supervisión admiten búsquedas. Si un evento está asociado con un origen, la búsqueda de plataforma recupera el origen junto con el evento.<br><br>**Nota**<br>La búsqueda de plataforma admite eventos para Crystal Reports para Enterprise. |
| Área de trabajo BI | • El título, la descripción y el contenido de los siguientes módulos BIW están indexados:<br>  • Módulo de texto<br>  • Módulo de página Web<br>  • Módulo de la lista de navegación<br>  • Módulo de visor<br>• El título y la descripción de un módulo compuesto están indexados.<br>• Solo está indexado el título de un módulo de plantilla de área de trabajo.<br>• En el caso de un módulo de grupo, el título y los metadatos de los módulos dentro del mismo están indexados.<br>• El título, la descripción y el CUID de los módulos de InfoObject en BIW están indexados.<br><br>**Nota**<br>Ya que solo están indexados el título y la descripción de un módulo de InfoObject incrustado, intentar buscar el contenido del InfoObject no devolverá referencias al módulo incrustado. Por ejemplo, si un CR está insertado en BIW, están indexados el título y la descripción. Intentar buscar en contenido del CR no devolverá referencias al módulo incrustado.<br>• Si un BIW contiene varias fichas y subfichas, también están indexados el título y el contenido de cada ficha y subficha. |

| Tipo de objeto | Contenido indexado |
| --- | --- |
| CR Next Gen | Título, descripción, fórmula de selección, datos guardados, campos de texto de cualquier sección, valores de parámetro y subinformes.<br><br>No se admites los siguientes objetos en un informe de CR Next Gen:<br><br>• Informe de tabla de referencias cruzadas<br>• Extracción de datos del gráfico<br>• Extracción de imágenes y metadatos asociados<br>• OLE incrustado (por ejemplo, un documento Word incrustado en CR)<br><br>Además, no es posible leer datos de página por página desde un informe CR Next Gen. |
| Universo | Se puede buscar en el contenido de los datos.<br><br>**Nota**<br><br>De forma predeterminada, la opción de indexación de universos está habilitada. Si nota que las consultas usadas por la búsqueda de plataforma para indexar contenido de universo tarda mucho tiempo en ejecutarse, y esto tiene impacto en el rendimiento del servidor de la base de datos, le recomendamos que deshabilite la opción de indexación de universos en la Consola de administración central (CMC). `Select distinct SampleColumnName from SampleTableName LIMIT 1000` es un ejemplo de la consulta que utiliza la búsqueda de plataformas al indexar contenido de universos.<br><br>Siga estos pasos para deshabilitar la indexación de universos:<br><br>1. Inicie sesión en la Consola de administración central (CMC).<br>2. Elija *Aplicaciones*.<br>3. Navegue a las aplicaciones de búsqueda en plataforma y elija *Propiedades*.<br>4. Navegue a los tipos de contenido y desmarque *Universo*.<br>5. Seleccione *Guardar y cerrar*. |
| Documento Lumira | Solo se puede buscar el contenido de los metadatos. |
| Documento de Analysis Office | Solo se puede buscar el contenido de los metadatos. |

> **Nota**
>
> El tamaño máximo admitido para los documentos agnósticos (MS Office 2003 y 2007 y documentos PDF) es de 15 MB.

## 26.3.3.2 Buscar

Cuando un usuario busca una palabra clave desde la rampa de lanzamiento BI o cualquier desde otra aplicación que usa el SDK de búsqueda de plataforma, se comprueba el índice maestro para buscar los términos de búsqueda. En función de los derechos de visualización del usuario, el motor de búsqueda muestra solo los documentos para los que el usuario dispone de derechos de acceso.

> **Nota**
>
> Cuando se busca en la CMC en un entorno con una base de datos de CMS grande, la búsqueda puede fallar. Para obtener más información, verifique la nota SAP 2156647 La búsqueda en la CMC es muy lenta o no devuelve resultados.

## 26.3.3.3 Búsqueda posterior

### 26.3.3.3.1 Facetas

La búsqueda de plataforma refina los resultados de la búsqueda agrupándolos en categorías o facetas de tipos de objetos similares y clasificándolos según el número de apariciones de la categoría entre los resultados devueltos para el concepto de búsqueda. Las facetas permiten navegar al resultado exacto.

La búsqueda de plataforma genera facetas de los metadatos de InfoObject, metadatos de documentos y contenido de documentos. Muestra solo las facetas que tienen más de dos documentos que coinciden con una consulta específica. Las facetas aparecen de forma dinámica según los documentos que coinciden con la consulta de búsqueda y se clasifican por recuento de documentos.

Los documentos se agrupan en las facetas o categorías genéricas siguientes:

- Personal o pública (como HR, Corporativo o Finanzas): Se basa en las categorías de documentos de la plataforma de BI.
- Tipo de documento: se basa en el tipo de documento, como Web Intelligence, Crystal Reports, Microsoft Word (2003 y 2007), Microsoft Excel (2003 y 2007).
- Universo y conexiones: Se basa en el origen de contenido.
- Fecha: Incluye la última fecha actualizada: (año, trimestre y mes).
- Hora: Incluye la hora de actualización más reciente, por ejemplo: 24 horas y última semana.
- Autor: Es el nombre del usuario que creó el documento.

> **Nota**
>
> Al trabajar con las configuraciones regionales en hebreo o árabe, si busca objetivos de contenido en la rampa de lanzamiento BI, los resultados de búsqueda no muestran facetas.

## 26.3.3.3.2 Normalización de la clasificación de resultados de la búsqueda

Para clasificar un documento, la función Búsqueda de plataforma tiene en cuenta el lugar de repetición del término buscado. Agrupa el contenido en las categorías siguientes en función de la repetición del contenido en el documento:

1. Metadatos de plataforma
2. Metadatos de documento
3. Metadatos de contenido
4. Contenido

Puede configurar el peso de estas categorías en la CMC.

### 26.3.3.3.2.1 Personalización del peso para clasificar los resultados de la búsqueda

La función Búsqueda de plataforma le permite establecer pesos (de importancia) para el contenido agrupado en categorías en función de la repetición del contenido en el documento, de manera que pueda establecer un valor mayor para la categoría que quiera a fin de recuperar más rápidamente los resultados de la búsqueda que estén relacionados.

Para definir el peso, siga estos pasos:

1. En el área *Administrar* de la CMC, haga clic en *Aplicaciones*.
2. Abra la *aplicación de búsqueda de plataforma*.
3. Elija *Clasificación*.

   Se muestran las ponderaciones de distintas categorías de contenidos como metadatos de plataforma, metadatos de documento, metadatos de contenido y contenido. La *Configuración regional de usuario* es la configuración regional establecida en las preferencias de la plataforma de lanzamiento de BI.
4. Establecer las ponderaciones para satisfacer los requisitos.
5. Seleccione *Guardar*.

En un escenario de actualización, si se tiene que aplicar una clasificación para documentos que ya están indexados, tiene que volver a crear el índice. Para obtener más información, consulte la información sobre volver a crear el índice en la sección Configurar las propiedades de aplicaciones en la CMC [página 945].

## 26.3.3.3.3 Compatibilidad con varios idiomas

La búsqueda de plataforma ofrece compatibilidad multilingüe para indexar contenido, recuperar resultados de búsqueda y conseguir sugerencias en el idioma deseado. Para indexar todos los documentos no localizados de la plataforma de BI usa la configuración local establecida en la *Configuración regional del índice predeterminada* en la CMC.

Una vez localizado el InfoObject, la función Búsqueda de plataforma usa el analizador del idioma correspondiente para indexar el documento.

La búsqueda se basa en la configuración regional establecida como configuración regional de producto del cliente. Al recuperar los resultados de la búsqueda, la función Búsqueda de plataforma concede más peso a la configuración regional de producto del cliente. Puede configurar las ponderaciones en la CMC.

#### 26.3.3.3.4 Sugerencias

La búsqueda de plataforma ofrece sugerencias para las consultas de búsqueda deletreadas de forma incorrecta. Si la consulta de búsqueda original no ofrece ningún resultado, la búsqueda de plataforma sugiere los términos más probables según el contenido indexado.

Las sugerencias aparecen como palabras clave con un hipervínculo. Haga clic en un hipervínculo para ver una lista de documentos que contenga la palabra clave que puede coincidir con la consulta original. Estas sugerencias se determinan de forma algorítmica según los diferentes factores objetivos.

Si existen varios términos que puedan coincidir con la solicitud original, la búsqueda de plataforma aporta tres sugerencias principales en el idioma configurado como la *Configuración regional de índice* en la aplicación de la CMC.

> **Nota**
>
> La búsqueda de plataforma no genera sugerencias en estos casos:
>
> - Si las consultas de búsqueda contienen menos de tres letras
> - Para la búsqueda con atributos, como el Tipo: Crystal Report
> - Para metadatos y contenido del universo
> - Para idiomas de varios bytes, como chino, japonés o coreano

## 26.4 Integración de Búsqueda de plataforma con la búsqueda de SAP NetWeaver Enterprise

SAP NetWeaver Enterprise Search 7.20 y posterior puede usar el servicio de búsqueda basado en OpenSearch (RSS y ATOM). Puede delegar solicitudes de búsqueda a sistemas de proveedor de servicio de búsqueda. En este caso, OpenSearch es el proveedor de servicios, SAP NetWeaver Enterprise Search es el consumidor de resultados de búsqueda y SAP BusinessObjects Platform Search es el proveedor del servicio de búsqueda.

Si un usuario envía una solicitud de búsqueda, SAP NetWeaver Enterprise Search reenvía la solicitud de búsqueda directamente al proveedor de OpenSearch. El proveedor responde a la solicitud de búsqueda y envía la respuesta a SAP NetWeaver Enterprise Search. A continuación, se fusiona con los resultados recibidos de los conectores del objeto de búsqueda en un resultado de búsqueda y se muestra en la interfaz de usuario.

Para integrar SAP NetWeaver Enterprise Search y la búsqueda de plataforma, debe llevar a cabo los siguientes pasos:

1. Cree un conector en SAP NetWeaver Enterprise Search.
2. Importar una función de usuario en la plataforma de BI.

## 26.4.1 Creación de un conector en SAP NetWeaver Enterprise Search

Puede usar un conector de objeto de búsqueda del tipo OpenSearch para integrar proveedores de búsqueda externos que proporcionen una función de búsqueda disponible a través de OpenSearch.

Para crear in conector en SAP NetWeaver Enterprise Search, necesita los siguientes requisitos previos:

1. La dirección URL del servicio de descripción de OpenSearch.
2. El servicio de descripción de OpenSearch debe estar disponible sólo en formato RSS o ATOM.

Lleve a cabo los siguientes pasos para crear un conector en SAP NetWeaver Enterprise Search:

1. Inicie la cabina de administración y seleccione Crear.
2. Seleccione OpenSearch como el tipo de conector del objeto de búsqueda.
3. Pulse *Siguiente*.
4. Introduzca la dirección URL del servicio de descripción de OpenSearch del proveedor de OpenSearch.
5. Seleccione una de las siguientes configuraciones de autenticación para iniciar la dirección URL del servicio de descripción:
   - Sin autenticación: no se lleva a cabo ninguna autenticación
   - SAP Authentication Assertion Ticket: este usuario se usa para la autenticación a través de SSO.
   - Usuario/contraseña: un usuario predefinido se usa para la autenticación.
6. Seleccione Iniciar dirección URL de búsqueda desde la configuración de OpenSearch.
   El servicio de descripción de OpenSearch se valida para obtener un servicio de búsqueda más adecuado. El sistema introduce automáticamente un valor para la plantilla URL de búsqueda y la descripción asociada.
7. Seleccione una de las siguientes configuraciones de autenticación para configurar un conector:
   - Sin autenticación: no se lleva a cabo ninguna autenticación
   - SAP Authentication Assertion Ticket: este usuario se usa para la autenticación a través de SSO.
   - Usuario/contraseña: un usuario predefinido se usa para la autenticación.
8. Pulse *Siguiente*.
   Aparece un cuadro de diálogo de resumen que muestra los valores introducidos para este conector de objeto de búsqueda.
9. Seleccione *Anterior* para modificar la configuración o en *Cancelar* para omitir todos los datos introducidos.
10. Seleccione *Finalizar* para guardar la configuración.

## 26.4.2 Importar una función de usuario en la plataforma de BI.

Lleve a cabo los siguientes pasos para importar una función de usuario en la plataforma de BI:

> **Nota**
>
> El administrador debe disponer de los detalles de usuario, la información del sistema, la información del host de la aplicación y las credenciales del usuario.

1. Diríjase al área *Autenticación* de la CMC.
2. Seleccione *SAP*.
3. Especifique lo siguiente en la ficha *Sistemas de derechos*:
   - Sistema
   - Cliente
   - Servidor de aplicaciones
   - Número de sistema
   - Nombre de usuario
   - Contraseña
   - Idioma
4. Seleccione *Actualizar*.
5. Elija la ficha *Importar función* e importe las funciones de usuario.
6. Seleccione *Actualizar*.
7. Seleccione *Administrar* > *Seguridad de usuario* en la CMC para asignar los derechos de usuario adecuados.

## 26.5 Buscar desde SAP NetWeaver Enterprise Search

Para buscar resultados desde SAP NetWeaver Enterprise Search, lleve a cabo los siguientes pasos:

1. Inicie sesión en la aplicación SAP NetWeaver Enterprise Search.
2. Seleccione *Búsqueda avanzada*.
3. Seleccione el conector que se creó para la búsqueda de plataforma.
4. Busque una palabra clave.

   Los resultados consolidados para la palabra clave contienen los resultados de la búsqueda de plataforma si existe una coincidencia en la palabra clave.

## 26.6 Auditoría

Se realiza una auditoría de todos los eventos de las solicitudes de búsqueda enviados desde una aplicación cliente que use el Servicio de búsqueda de plataforma y de la respuesta de búsqueda. Para la búsqueda de plataforma, se implementa la auditoría en el nivel de servicio.

El servicio de búsqueda de plataforma debe ejecutarse con un servicio de proxy de auditoría de cliente en el mismo servidor para enviar eventos de auditoría.

Hay un ID de tipo de evento 1009 para la búsqueda de plataforma y cuatro ID de tipo de detalles de evento específicos de búsqueda de plataforma:

- Palabra clave buscada (ID: 19)
- Número de resultados de la búsqueda (ID: 63)

- Búsqueda de faceta (ID: 20)
- Excepción de búsqueda (ID: 1)

Aparte de los detalles de evento anteriores, existen algunos detalles de evento estándar, como sessionCuid y userCuid, que se admiten con cualquier auditoría de cualquier módulo de la Plataforma de BI.

A continuación se explica, mediante un ejemplo, cómo funciona la auditoría en la Búsqueda de plataforma.

Si busca la palabra clave "Ventas", el número total de resultados de búsqueda podría ser 5. En este caso, se auditarán los eventos siguientes:

- ID de tipo de evento 1009
- ID de tipo de detalle de evento 19 con el valor de ventas
- ID de tipo de detalle de evento 63 con el valor 5
- CUID de sesión
- CUID de usuario
- Estado con el valor 0, que indica un estado de operación correcta
- Hora de inicio
- Duración
- ID de objeto con el valor 0 ya se trata de un servicio de auditoría

Si se generan facetas y se selecciona una o varias facetas, se realiza una auditoría de los eventos siguientes:

- ID de tipo de evento 1009
- ID de tipo de detalle de evento 19 con el valor de ventas
- ID de tipo de detalle de evento 63 con el valor 5
- ID del tipo de detalle de evento 20 con una cadena separada por comas de aspectos
- CUID de sesión
- CUID de usuario
- Estado con el valor 0, que indica un estado de operación correcta
- Hora de inicio
- Duración
- ID de objeto con el valor 0 ya se trata de un servicio de auditoría

Si existe una excepción de búsqueda debido a una entrada no válida (por ejemplo *"a"), se auditan los siguientes detalles de evento:

- ID de tipo de evento 1009
- ID de tipo de detalle de evento 19 con el valor de ventas
- ID del tipo de detalle de evento 63 con el valor 0
- ID del tipo de detalle de evento 1 con el mensaje de excepción
- CUID de sesión
- CUID de usuario
- Estado con el valor 1, que indica un estado de operación incorrecta
- Hora de inicio
- Duración
- ID de objeto con el valor 0 ya se trata de un servicio de auditoría

## 26.7 Solución de problemas

### 26.7.1 Corrección automática

La búsqueda de plataforma dispone de su propio mecanismo de recuperación automática. Supervisa de manera continua el uso de memoria del servicio de búsqueda y detiene automáticamente la indexación cuando el uso de memoria supera el valor del umbral. Se inicia automáticamente cuando el uso de memoria se reduce a un límite considerable. Sin embargo, los usuarios pueden continuar con la búsqueda durante este proceso, pero no se pueden indizar para un periodo específico de tiempo. De forma predeterminada, la Búsqueda de plataforma configura el número de documentos que se pueden indexar en cualquier momento, según el tipo de documento. La indexación se inicia en base a los recursos del sistema como la CPU y memoria.

### 26.7.2 Escenarios de problemas

Esta sección proporciona soluciones paso a paso para una amplia gama de problemas que se pueden producir al recuperar resultados de búsqueda con la búsqueda de plataforma.

#### No es posible recuperar los resultados de búsqueda del documento recientemente agregado que contiene la palabra clave

- Compruebe si Búsqueda de plataforma admite el tipo de documento al que corresponde el documento enviado. Si no se admite el tipo de documento, no se indexará el documento.
  Para obtener más información acerca de los tipos de documento admitidos, consulte el tema *Tipos de documento en los que se pueden realizar búsquedas* en los Temas relacionados que se enumeran a continuación.
- Marque la opción seleccionada para *Frecuencia de inspección*. Si la *Frecuencia de inspección* está configurada en *Inspección continua*, los documentos se recuperan inmediatamente para su indexación. Si la *Frecuencia de inspección* está configurada en *Inspección programada*, la indexación se ejecuta solo durante el periodo de tiempo programado.
  Para obtener más información acerca de la opción *Frecuencia de inspección*, consulte el tema *Configurar las propiedades de aplicación* en los Temas relacionados que se enumeran a continuación.
- Compruebe la lista de errores de indexación para verificar si se ha indexado el documento correctamente. Si el documento aparece en esta lista, deberá modificarlo y volver a enviarlo para que la búsqueda de plataforma use el documento para su indexación.

  > ⓘ Nota
  >
  > Puede modificar el documento agregando o eliminando un campo y guardándolo de nuevo a continuación. De este modo se actualiza la marca de hora del documento en el repositorio de la plataforma de BI y se inicia de nuevo la indexación del documento.

  Para obtener más información acerca de los documentos que no se pueden indexar, consulte el tema *Listado de fallos de indexación* en los Temas relacionados que se enumeran a continuación.

- Compruebe los registros de seguimiento del servidor de procesamiento de Adaptive que contienen información acerca del error de indexación.
  1. Vaya al directorio `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\logging\`, que contiene el registro de seguimiento de APS con una extensión .glf.
  2. Abra el archivo de registro de rastreo y busque el SI_ID de documento que se debe indexar.

     > **Nota**
     >
     > Puede encontrar el SI_ID de documento en las propiedades del documento.

## No se pueden recuperar documentos de Crystal Reports

La búsqueda de plataforma indexa el contenido de Crystal Reports solo para Crystal Reports 2020. No indexa el contenido de Crystal Reports para Enterprise.

Sin embargo, si usa Crystal Reports para Enterprise puede buscar metadatos de documentos como el título, descripción y palabra clave, que forman parte de las propiedades del documento.

Si el documento contiene contenido que se puede indexar, deberá seguir el mismo procedimiento que se enumera en la sección antes mencionada *No es posible recuperar los resultados de búsqueda del documento agregado recientemente que contiene la palabra clave*.

## La búsqueda de SAP NetWeaver Enterprise no puede recuperar resultados de la plataforma de BI

- Compruebe si la búsqueda de plataforma recupera los resultados de búsqueda mediante la plataforma de lanzamiento de BI para encontrar si el problema se debe a la búsqueda de plataforma y la integración de la búsqueda de SAP NetWeaver Enterprise.
- Compruebe si OpenSearch se despliega correctamente en el servidor de aplicaciones Web. Los pasos específicos para validar el despliegue de OpenSearch depende del tipo de servidor de aplicaciones Web que se usa.
- Compruebe si el conector se crea o configura correctamente en la configuración de la búsqueda de SAP NetWeaver Enterprise. Debe usar el conector correcto para que la búsqueda de SAP NetWeaver Enterprise federe los resultados de la búsqueda de plataforma.
- Compruebe si la comunicación es correcta entre los equipos que ejecutan la búsqueda de SAP NetWeaver Enterprise y la plataforma de BI respectivamente. En el caso de problemas de red en un entorno distribuido, la búsqueda de SAP NetWeaver Enterprise puede fallar al federar los resultados.
- Compruebe si los usuarios de SAP NetWeaver Enterprise Search se agregan a la plataforma de BI con los derechos adecuados. Para validar los derechos de usuario, vaya al área *Autenticación* de la CMC y seleccione *SAP*.

## Información relacionada

Lista de errores de indexación [página 954]
Configurar las propiedades de aplicaciones en la CMC [página 945]
Tipos de contenido que se puede buscar [página 956]

# 27 Federación

## 27.1 Federación

Federación es una herramienta de réplica entre sitios para trabajar con varios despliegues de la plataforma de BI en un entorno global.

El contenido se puede crear y administrar desde un despliegue de la plataforma de BI y se puede replicar en otros despliegues de la plataforma de BI entre sitios geográficos con una programación repetitiva. Puede realizar tareas de réplica unidireccional y bidireccional.

Las ventajas de Federación incluyen la capacidad para:

- Reducir el tráfico de red
- Crear y administrar contenido desde un solo sitio
- Aumentar el rendimiento para los usuarios finales

Cuando se replica contenido con Federación, se puede:

- Simplificar las necesidades de administración para varios despliegues.
- Proporcionar una directiva de derechos coherentes entre varias oficinas para las organizaciones globales.
- Obtener información más rápidamente y procesar los informes en los sitios remotos donde se encuentran los datos.
- Ahorrar tiempo mediante la recuperación de datos locales y dispersos más rápidamente
- Sincronizar el contenido de varias implementaciones sin escribir código personalizado.

Federación permite disponer de modelos de seguridad, ciclos de vida, tiempos de prueba y despliegue independientes, así como distintos propietarios y administradores empresariales. Por ejemplo, puede delegar las funciones de administración que limiten al administrador de aplicaciones de ventas realizar modificaciones en una aplicación de recursos humanos.

Puede replicar varios objetos con Federación, como se describe en la siguiente tabla.

| Categoría | Tipos de objeto que puede replicar | Notas adicionales |
|---|---|---|
| Vistas empresariales | Administrador de vistas empresariales, DataConnection, LOV, infraestructura de datos, etc. | Se admiten todos los objetos, aunque no en el nivel individual. |
| Informes | Crystal Reports, Web Intelligence y Dashboard Design | Se admiten el complemento y las plantillas del cliente completo. |
| Objetos de terceros | Archivos Excel, PDF, PowerPoint, Word, texto, texto enriquecido y Shockwave Flash | |
| Usuarios | usuarios, grupos, bandejas de entrada, favoritos y categoría personal | |
| Plataforma de Business Intelligence | Carpetas, eventos, categorías, calendarios, niveles de acceso, | |

| Categoría | Tipos de objeto que puede replicar | Notas adicionales |
|---|---|---|
| | hipervínculos, accesos directos, programas, perfiles, paquetes de objetos, agnóstico | |
| Universo | Universo, conexiones y sobrecarga de universo | |

En los siguientes escenarios se presentan dos ejemplos de cómo su organización puede usar Federación.

**Escenario 1: Venta al detalle (diseño centralizado)**

La tienda ACME desea enviar un informe de ventas mensuales a las demás tiendas con el método de réplica unidireccional. El administrador del sitio de origen crea un informe que los administradores de cada sitio de destino replican y ejecutan según la base de datos de dicha tienda.

> → Sugerencias
>
> Las instancias localizadas se pueden devolver al sitio de origen que mantenga la información replicada de cada objeto. Por ejemplo, aplicará el logotipo adecuado, la información de conexión de base de datos, etc.

**Escenario 2: Programación remota (acceso distribuido)**

Los datos están en el sitio de origen. Las tareas de réplica pendientes se envían al sitio de origen para que se ejecuten. A continuación, las tareas de réplica completadas de devuelven a los sitios de destino para su visualización. Por ejemplo, los datos de un informe pueden no estar disponibles en el sitio de destino, pero el usuario puede configurar los informes para que se ejecuten en el sitio de origen antes de que el informe completado se devuelva al sitio de destino.

## 27.2 Términos de Federación

La siguiente lista de términos presenta las palabras y frases relacionadas con Federación y puede ayudarle en su exploración y uso.

| | |
|---|---|
| Aplicación BI | Agrupación lógica de contenido de Business Intelligence (BI) relacionado con una finalidad y unos destinatarios específicos. Una aplicación BI no es un objeto. Un despliegue de la plataforma de BI puede alojar varias aplicaciones de BI, cada una con distintos modelos de seguridad, ciclos de vida, líneas temporales de pruebas y despliegue, así como propietarios empresariales y administradores independientes. |
| Sitio de destino | Un sistema de la plataforma de BI que extrae el contenido replicado de la plataforma de BI desde un sitio de origen. |
| Local | Sistema local donde está conectado un usuario o administrador. Por ejemplo, el administrador de un sitio de destino se considera «local» respecto al sitio de destino. |
| Instancias completadas ejecutadas localmente | Instancias que se procesan en el sitio de destino y, a continuación, se envían de vuelta al sitio de origen. |

| | |
|---|---|
| Múltiples sitios de origen | Más de un sitio puede servir de sitio de origen. Por ejemplo, varios centros de desarrollo suelen tener varios sitios de origen. No obstante, solo puede haber un sitio de origen por réplica. |
| Réplica unidireccional | Los objetos se replican solo en una dirección: desde el sitio de origen al sitio de destino. Las actualizaciones efectuadas en un sitio de destino permanecen en dicho sitio de destino. |
| Sitio de origen | El sistema de la Plataforma de BI en el que se origina el contenido. |
| Remoto | Sistema que no es local para un usuario. Por ejemplo, el sitio de origen se considera «remoto» para los usuarios y administradores del sitio de destino. |
| Conexión remota | Un objeto que contiene información que se usa para conectarse a un despliegue de la Plataforma de BI, incluidos el nombre de usuario y la contraseña, el nombre del CMS, la dirección URI de WebService y las opciones de limpieza. |
| Programación remota | Solicitudes de programación que se envían desde el sitio de destino al sitio de origen. Los informes de los sitios de destino se pueden programar de forma remota, lo cual envía la instancia del informe de vuelta al sitio de origen para su procesamiento. A continuación, la instancia completada se devuelve al sitio de destino. |
| Réplica | Proceso de copia de contenido de un sistema de la Plataforma de BI a otro. |
| Tarea de réplica | Objeto que contiene información acerca de la programación de la réplica, el contenido que se va a replicar y cualquier condición especial que deba aplicarse al replicar contenido. |
| Lista de réplicas | Lista de los objetos que se van a replicar. Una lista de réplicas hace referencia a otros contenidos, como usuarios, grupos, informes, etc., en el despliegue de la Plataforma de BI para replicarlos conjuntamente. |
| Objeto de réplica | Objeto que se replica de un sitio de origen en un sitio de destino. Todos los objetos replicados en un sitio de destino se etiquetarán con un icono de replicación. Si hay un conflicto, los objetos se etiquetarán con un icono de conflicto. |
| Paquete de réplica | Creado durante la transferencia, el paquete de réplica contiene objetos de una tarea de réplica. Puede contener todos los objetos definidos en la lista de réplica, como en el caso de un entorno en constante cambio o de una réplica inicial. O puede contener un subconjunto de la lista de réplicas si los objetos cambian con poca frecuencia en comparación con la programación de la tarea de réplica. El paquete de réplica se implementa como archivo de recursos de aplicación BI (BIAR). |
| Actualización de réplica | Todos los objetos de una lista de réplicas se actualizan independientemente de la versión de la última modificación. |
| Réplica bidireccional | Actúa del mismo modo que la réplica unidireccional, pero la bidireccional también envía los cambios en ambas direcciones. Las actualizaciones del sitio de origen se replican en cada sitio de destino. Las actualizaciones y los objetos nuevos de un sitio de destino se envían al sitio de origen. |

## 27.3 Administrar derechos de seguridad

Federación replica el contenido entre despliegues independientes y requiere la colaboración con otros administradores. Por lo tanto, es necesario entender la seguridad antes de empezar a usar la federación.

Los administradores de despliegues independientes deben coordinarse entre sí antes de habilitar la Federación. Después de replicar el contenido, los administradores pueden cambiarlo.

Son necesarios determinados derechos en los despliegues de origen y destino para realizar determinadas tareas.

- Derechos necesarios en el sitio de origen
- Derechos necesarios en el sitio de destino
- Derechos necesario para los objetos específicos de la federación
- Escenarios de federación

> → Sugerencias
>
> Se recomienda leer este capítulo antes de habilitar la federación.

### 27.3.1 Derechos necesarios en el sitio de origen

En esta sección se describen las acciones del sitio de origen y los derechos necesarios de la cuenta de usuario que se conecta al sitio de origen. Esta es la cuenta que se introduce en el objeto de conexión remota en el sitio de destino.

| Acción | Descripción | Derechos necesarios |
|---|---|---|
| Réplica unidireccional | Realiza la réplica únicamente desde el sitio de origen al sitio de destino.<br>ⓘ Nota<br>«Se requieren derechos de visualización» y «réplica» en todos los objetos que se replican, incluidos los objetos que los cálculos de dependencia replican automáticamente. | • Derechos de «visualización» y «réplica» en todos los objetos que desea replicar<br>• Derecho a «Ver» en la lista de réplicas |
| Réplica bidireccional | Realiza la réplica desde el sitio de origen al sitio de destino y desde el sitio de destino al de origen. | • Derechos de «visualización» y «réplica» en todos los objetos que desea replicar<br>• Derecho a «Ver» en la lista de réplicas<br>• Derechos de «modificación» en los objetos de usuario para replicar los cambios de contraseña |

| Acción | Descripción | Derechos necesarios |
| --- | --- | --- |
| Programación | Permite que tenga lugar la programación remota en el sitio de origen desde el sitio de destino. | • Derecho «Programar» para todos los objetos que desea programar de forma remota. |

## Información relacionada

Derechos necesarios en el sitio de destino [página 972]

# 27.3.2 Derechos necesarios en el sitio de destino

En esta sección se describen las acciones que se aplican en el sitio de destino y los derechos necesarios de la cuenta de usuario que ejecuta la tarea de réplica. Esta es la cuenta del usuario que ha creado la tarea de réplica.

> **Nota**
>
> Al igual que otros objetos programables, puede programar la tarea de réplica en nombre de otro usuario.

| Acción | Descripción | Derechos necesarios |
| --- | --- | --- |
| Todos los objetos | Replica los objetos independientemente de la réplica unidireccional o bidireccional. | • «Derechos de visualización», «adición», «edición» y «modificación» en todos los objetos<br>• Derecho «Modificar contraseña de usuario», para todos los objetos de usuario |
| Primera réplica | La primera vez que ejecute la tarea de replicación, no habrá aún objetos en el sitio de destino. Por lo tanto, la cuenta de usuario en la que se ejecuta la tarea de réplica debe tener derechos para todas las carpetas de nivel superior y en los objetos a los que agregará contenido. | • Derechos «Ver», «Agregar», «Editar» y «Modificar derechos» en todas las carpetas de nivel superior y objetos predeterminados |

## Información relacionada

Derechos necesarios en el sitio de origen [página 971]

## 27.3.3 Derechos específicos de Federación

Esta sección describe los escenarios específicos de Federación.

| Acción | Descripción | Derechos necesarios |
|---|---|---|
| Limpieza de objetos | La limpieza de objetos elimina los objetos del sitio de destino. | • La cuenta con la que se ejecuta la tarea de réplica necesita derechos de «eliminación» en todos los objetos que se puedan eliminar. |
| Desactivar la limpieza para determinados objetos | Cuando determinados objetos se replican desde el sitio de origen, puede que no desee eliminarlos desde el sitio de destino si se han eliminado en el sitio de origen. Puede asegurarse de ello por medio de los derechos. Por ejemplo, seleccione esta opción cuando los usuarios del sitio de destino empiecen a usar un objeto independientemente de los usuarios del sitio de origen.<br><br>Por ejemplo, en un universo replicado en el que los usuarios del sitio de destino crean sus propios informes locales con este universo, puede que no desee perder el universo en el sitio de destino si se elimina desde el sitio de origen. | • Deniegue los derechos de «Eliminar» de la cuenta de usuario en la que se ejecuta la tarea de réplica en los objetos que desea mantener. |
| Réplica bidireccional sin modificaciones en el sitio de origen | En determinadas circunstancias puede que opte por la réplica bidireccional pero que no desee que algunos objetos del sitio de origen se modifiquen, incluso si se cambian en el sitio de destino. Los motivos para ello pueden ser: si el objeto es especial y solo lo deben cambiar los usuarios del sitio de origen; o si desea habilitar la programación remota pero no desea que los cambios se propaguen hacia atrás.<br><br>**Nota**<br>Para la programación remota puede crear una tarea que solo controle los objetos para la programación remota. No obstante, en este caso los objetos ascendientes se siguen replicando, | • Denegar los derechos de «edición» de la cuenta de usuario que se usa para conectarse en el objeto de conexión remota. |

| Acción | Descripción | Derechos necesarios |
|---|---|---|
| | incluidos el informe, la carpeta que contiene el informe y la carpeta principal de esa carpeta. Los cambios realizados en el sitio de destino se replican en el sitio de origen y los cambios realizados en el sitio de origen se replican al sitio de destino. | |

## 27.3.4 Réplica de la seguridad en un objeto

Para mantener los derechos de seguridad de un objeto, debe replicar tanto el objeto como su usuario o grupo al mismo tiempo. De no hacerlo, ya deben existir en el sitio al que se está efectuando la réplica y tener identificadores únicos (CUID) idénticos en cada sitio.

Si un objeto se replica y el usuario o grupo no se replica, o no existe todavía en el sitio al que se esté efectuando la réplica, se perderán sus derechos.

### Ejemplo

El Grupo A y el Grupo B tienen derechos asignados en el Objeto A. El Grupo A tiene derechos de «visualización» y el Grupo B tiene derechos de «denegar visualización». Si la tarea de réplica solo replica el Grupo A y el Objeto A, en el sitio de destino, el Objeto A solo tendrá los derechos «Ver» del Grupo A asociado a él.

Cuando se replica un objeto, existe un posible riesgo de seguridad si no se replican todos los grupos con derechos explícitos sobre el objeto. En el ejemplo anterior se destaca un posible riesgo. Si el Usuario A pertenece al Grupo A y al Grupo B, el usuario no tendrá permiso para ver el Objeto A en el sitio de origen. Sin embargo, el Usuario A se replicará en el sitio de destino, ya que pertenece a ambos grupos. Una vez allí, como el Grupo B no se ha replicado, el usuario A tendrá derecho a ver el Objeto A en el sitio de destino, pero no podrá ver el Objeto A en el sitio de origen.

Los objetos que hacen referencia a otros objetos que no están incluidos en una tarea de réplica o aquellos que no se encuentran aún en el sitio de destino, se muestran en un archivo de registro. El archivo de registro muestra que el objeto hacía referencia al objeto que no se ha replicado y que ha eliminado su referencia.

La seguridad en un objeto para un usuario o grupo concreto solo se replica desde el sitio de origen al sitio de destino. Puede configurar la seguridad en objetos replicados del sitio de destino, pero dichos ajustes no se replicarán en el sitio de origen.

## 27.3.5 Réplica de la seguridad mediante niveles de acceso

Para persistir, los derechos se deben definir por niveles de acceso. El objeto, usuario o grupo y el nivel de acceso se deben replicar al mismo tiempo o ya deben existir en el sitio en el que se está realizando la réplica.

Los objetos que asignan derechos explícitos a un usuario o grupo que no están incluidos en una tarea de réplica o que no están en el sitio de destino, aparecen en su archivo de registro, que muestra que el objeto que tenía derechos asignados que no se han replicado y que los derechos se han eliminado.

Además, puede optar por replicar automáticamente los «niveles de acceso» que se usan en un objeto importado. Esta opción está disponible en la lista de réplicas.

> ⓘ Nota
>
> Los niveles de acceso predeterminados no se replican pero las referencias se mantienen.

## 27.4 Opciones de tipos y modos de réplica

En función de la selección del tipo de réplica y modo de réplica, puede crear una opción de tarea de réplica de entre cuatro distintas:

- réplica unidireccional,
- réplica bidireccional,
- actualizar a partir de origen o
- actualizar a partir de destino.

### 27.4.1 Réplica unidireccional

Con la réplica unidireccional, sólo se puede replicar el contenido en una dirección, del sitio de origen a un sitio de destino. Cualquier cambio efectuado en los objetos del sitio de origen de la lista de réplicas se envía al sitio de destino. No obstante, los cambios efectuados en los objetos de un sitio de destino no se envían al sitio de origen.

La réplica unidireccional es ideal para despliegues con un despliegue central de la Plataforma de BI donde los objetos se crean, modifican y administran. Otros despliegues utilizan el contenido del despliegue central.

Para crear una réplica unidireccional, seleccione las opciones siguientes:

- Tipo de réplica = réplica unidireccional
- Modo de réplica = réplica normal

### 27.4.2 Réplica bidireccional

La réplica bidireccional permite replicar contenido en ambas direcciones entre los sitios de origen y de destino. Los cambios efectuados en los objetos del sitio de origen se replican en los sitios de destino y los cambios realizados en un sitio de destino se replican en el sitio de origen.

> **Nota**
>
> Para realizar la programación remota y replicar las instancias ejecutadas localmente de vuelta al origen, debe elegir el modo de réplica bidireccional.

Si dispone de varios despliegues de la Plataforma de BI en los que el contenido se crea, modifica, administra y usa en ambas ubicaciones, la réplica bidireccional es la opción más eficaz. También contribuye a sincronizar los despliegues.

Para crear una réplica bidireccional, seleccione las opciones siguientes:

- Tipo de réplica = réplica bidireccional
- Modo de réplica = réplica normal

### Información relacionada

Programación remota e instancias ejecutadas localmente [página 1000]

## 27.4.3 Actualizar a partir de origen o Actualizar a partir de destino

Cuando se replica el contenido en los modos de réplica unidireccional o bidireccional, los objetos de la lista de réplicas se replican en un sitio de destino. Sin embargo, no todos los objetos se replican necesariamente cada vez que se ejecuta la tarea de réplica.

Federación dispone de un motor de optimización concebido para ayudar a concluir las tareas de réplica con mayor rapidez. Usa una combinación de la versión y la marca de tiempo del objeto para determinar si el objeto se ha modificado desde la última réplica. La comprobación se realiza en objetos seleccionados específicamente en la lista de réplicas y en los objetos replicados durante la comprobación de dependencia.

Sin embargo, en algunos casos el motor de optimización no encontrará objetos y éstos no se replicarán. En estos casos puede usar «Actualizar a partir de origen» y «Actualizar a partir de destino» para forzar a la tarea de réplica a replicar el contenido y sus dependencias independientemente de su marca de tiempo.

"Actualizar a partir de origen" solo envía el contenido del sitio de origen a los de destino. "Actualizar a partir de destino" solo envía el contenido de los sitios de destino al de origen.

### Ejemplo

Los siguientes tres ejemplos muestran escenarios que usan «Actualizar a partir de origen» y «Actualizar a partir de destino» en los que faltarán determinados objetos debido a la optimización.

**Escenario 1:** La adición de objetos que contienen otros objetos en un área que se replica.

La Carpeta A se replica del sitio de origen al sitio de destino. Ahora existe en ambos sitios: Un usuario mueve o copia la Carpeta B con el Informe B a la Carpeta A del sitio de origen. Durante la siguiente réplica, Federación

verá que la marca de tiempo de la Carpeta B ha cambiado y la replicará al sitio de destino. Sin embargo, la marca de tiempo del Informe B no cambia. Por ello, faltará en una tarea de réplica unidireccional o bidireccional normal.

Para garantizar que el contenido de la Carpeta B se replica correctamente, debe usarse una tarea de réplica con «Actualizar a partir de origen» una vez. Después, la tarea de réplica unidireccional o bidireccional normal lo replicará correctamente. Si invertimos este ejemplo y la Carpeta B se mueve o copia al sitio de destino, debe usarse «Actualizar a partir de destino».

**Escenario 2:** La adición de nuevos objetos mediante LifeCycle Manager o la línea de comandos BIAR.

Cuando se agregan objetos a un área que se replica mediante el LifeCycle Manager o la línea de comandos BIAR, puede que el objeto no se seleccione con una tarea de réplica unidireccional o bidireccional normal. Esto ocurre porque los relojes internos de los sistemas de origen y de destino pueden no estar sincronizados cuando se usa LifeCycle Manager o la línea de comandos BIAR.

> ⓘ Nota
>
> Tras importar objetos nuevos a un área que se replica en el sitio de origen, se recomienda ejecutar una tarea de réplica «Actualizar a partir de origen». Tras importar objetos nuevos a un área que se replica en el sitio de destino, se recomienda ejecutar una tarea de réplica «Actualizar a partir de destino».

**Escenario 3:** Entre réplicas programadas.

Si agrega objetos a un área que se replica y no puede esperar hasta la siguiente réplica programada, puede usar las tareas de réplica «Actualizar a partir de origen» y «Actualizar a partir de destino». Si selecciona el área a la que se han agregado objetos, puede replicar el contenido rápidamente.

> ⓘ Nota
>
> Este escenario puede resultar costoso para listas de réplicas grandes, por lo que se recomienda no usar esta opción con frecuencia. Por ejemplo, no es necesario crear tareas de réplica para actualizar en modo de origen a destino programadas para cada hora. Estos modos se deben utilizar en programaciones tipo «Ejecutar ahora» o poco frecuentes.

> ⓘ Nota
>
> En algunos casos no se puede usar la resolución de conflictos, entre ellos: «Actualizar a partir de origen»: "Tiene preferencia el sitio de destino" está bloqueado o «Actualizar a partir de destino»: "Tiene preferencia el sitio de origen" está bloqueado.

## 27.5 Replicar usuarios y grupos de terceros

En Federación, puede replicar usuarios y grupos de terceros, específicamente usuarios y grupos de Active Directory (AD) y LDAP.

> → Sugerencias
>
> Lea esta sección si piensa replicar estos tipos de usuarios y grupos o su contenido personal, como carpetas de favoritos o bandejas de entrada.

## Asignar usuarios y grupos

1. Asigne los usuarios y grupos en el sitio de origen para que Federación los replique correctamente.
2. Replique los usuarios y grupos asignados en el sitio de destino.

> **Nota**
>
> No asigne grupos y usuarios por separado en el sitio de destino. Si lo hace, tendrán identificadores únicos (CUID) distintos en los sitios de destino y de origen y Federación no podrá encontrar las coincidencias con los usuarios o grupos.

## Ejemplo

El administrador asigna el Grupo A al Usuario A en los sitios de origen y de destino. Tanto el Grupo A como el Usuario A tienen identificadores únicos distintos en los sitios de origen y de destino. Durante la réplica, Federación no puede asignarlos y el Grupo A o el Usuario A no se replican debido a un conflicto de alias.

> **Nota**
>
> Antes de replicar usuarios y grupos de terceros, es necesario configurar el sitio de destino para usar la autenticación AD o LDAP. No obstante, también debe configurar el sitio de destino para que use AD o LDAP con el fin de que se comunique con el servidor de directorios o el controlador de dominio.

> **Nota**
>
> Después de replicar un grupo AD o LDAP por primera vez, los usuarios de este grupo no pueden iniciar sesión hasta que se haya actualizado el gráfico de grupo AD/LDAP. Esto se produce de forma automática aproximadamente cada 15 minutos. Para actualizar el gráfico de grupo AD/LDAP manualmente, vaya a la página *Autenticación* de la CMC, haga doble clic en *Windows AD* o *LDAP*, y, a continuación, haga clic en *Actualizar*.

> **Nota**
>
> Tenga cuidado al replicar grupos de terceros. Cuando se agregan usuarios nuevos al grupo en el servidor de directorio, podrán iniciar sesión en ambos sitios. Esta cuestión de seguridad sobre la autenticación AD o LDAP es independiente de Federación.
>
> Si inicia sesión en los sitios de destino y de origen por separado o bien la pertenencia a grupos se actualiza en ambos sitios mediante el botón de actualización de la página de autenticación de CMC, se creará una cuenta de usuario en ambos sitios. Las cuentas tendrán distintos identificadores únicos y Federación no podrá replicarlas correctamente.
>
> Es importante crear la cuenta en un sitio y, después, replicarla en el otro.

## 27.6 Replicar universos y conexiones de universos

Al usar Federación para replicar universos entre despliegues de la Plataforma de BI, es importante planear con antelación. Un objeto de universo no puede funcionar sin una conexión de universo subyacente.

Los objetos de conexión de universo contienen información necesaria para conectarse a una base de datos de informes. Para que funcione correctamente, los objetos de conexión de universo deben contener información válida y permitir que se establezca una conexión de base de datos.

> **Nota**
>
> Si usa la réplica bidireccional y replica un universo desde el sitio de origen al sitio de destino sin la conexión de universo, en las réplicas posteriores el universo del sitio de origen puede sobrescribir o eliminar su relación con la conexión de universo en el sitio de origen. Para evitarlo, replique siempre las conexiones de universo con los universos.

Para garantizar que las conexiones de universos dependientes se replican con los universos, seleccione siempre las siguientes opciones al crear o modificar la lista de réplicas que contenga los universos:

- *Incluir conexiones utilizadas por universos seleccionados*
- *Incluir universos requeridos por universos seleccionados*

> **Nota**
>
> Si se ha sobrescrito o eliminado la relación de un universo con su conexión de universo, abra el universo en Universe Designer y en *Archivo* > *Parámetros* modifique la información de conexión.

En los dos ejemplos siguientes se demuestra el proceso de replicar universos y sus conexiones de universos relacionadas.

### Ejemplo

Al replicar universos y conexiones de universo, debe asegurarse de que el entorno de conectividad en el sitio de origen coincide con el entorno de conectividad en el sitio de destino.

Por ejemplo, si la conexión de universo usa una conexión ODBC denominada «PruebaODBC», debe haber una conexión ODBC correctamente configurada y denominada «PruebaODBC» en el entorno de destino. La conexión ODBC puede resolverse en la misma base de datos o en otra diferente. Para garantizar que los universos que usan esta conexión no se encuentran con problemas de conectividad, los esquemas de las bases de datos deben ser los mismos.

### Ejemplo

Si desea que el universo replicado en el sitio de destino use una base de datos distinta de la que usa el universo en el sitio de origen, replique la conexión de universo, pero haga que la información de conectividad en el sitio de destino apunte a la base de datos deseada.

Por ejemplo, si la conexión de universo en el sitio de origen usa una conexión ODBC denominada «Prueba» que apunta a «Base de datos A», asegúrese de que dispone de una conexión ODBC en el sitio de destino también denominada «Prueba» pero que apunte a «Base de datos B».

## 27.7 Administración de listas de réplicas

La lista de réplicas incluye contenido, como usuarios, grupos e informes, en el despliegue de la plataforma de BI, que se pueden replicar conjuntamente. Se accede a las listas de réplicas desde la CMC.

Los tipos de contenido que se pueden replicar se explican en la siguiente tabla.

| Categoría | Objetos compatibles |
|---|---|
| Objetos de repositorio | Objetos que incluyen vistas empresariales, conexión de datos, listas de valores, infraestructura de datos, etc.<br>**Nota**<br>Se admiten todos los objetos, aunque no en el nivel individual. |
| Informes | Informes de Crystal, documentos de Web Intelligence y objetos de Cuadros de mandos.<br>**Nota**<br>Se admiten el complemento y las plantillas del cliente completo. |
| Objetos de terceros | Excel, PDF, PowerPoint, Word, archivos de texto, archivos de texto enriquecido o archivos de Shockwave. |
| Usuarios | Usuarios, grupos, bandejas de entrada, favoritos o categoría personal. |
| Plataforma de Business Intelligence | Carpetas, eventos, categorías, calendarios, funciones personalizadas, hipervínculos, accesos directos, programas, perfiles, paquetes de objetos o agnóstico. |
| Universos | Universos, conexiones o sobrecarga de universos. |

**Nota**

Los siguientes objetos deben crearse en el sitio de origen y, a continuación, replicarse al sitio de destino. Si crea estos objetos en el sitio de destino y, a continuación, los replica en el sitio de origen, no funcionarán en el sitio de origen.

- Vistas empresariales
- Elementos empresariales
- Infraestructuras de datos
- Conexiones de datos
- Listas de valores
- Sobrecargas de universos

## 27.7.1 Creación de listas de réplicas

Las listas de réplicas están situadas en el área Listas de réplicas de la CMC. Puede organizar las listas de réplicas en carpetas y subcarpetas de su creación.

### 27.7.1.1 Para crear una carpeta de lista de réplicas

1. Vaya al área *Listas de réplicas* de la CMC.
2. Haga clic en *Listas de réplicas*.
3. Haga clic en *Administrar* > *Nueva* > *Carpeta*.
   Aparece el cuadro de diálogo *Crear carpeta*.
4. Escriba un nombre de carpeta y haga clic en *Aceptar*.
   Ahora puede crear listas de réplicas en esta carpeta.

### 27.7.1.2 Crear una lista de réplicas

1. Vaya al área *Listas de réplicas* de la CMC.
2. Seleccione la carpeta en la que desea guardar la nueva lista de réplicas.
3. Haga clic en *Gestionar* > *Nuevo* > *Nueva lista de réplicas*.
   Aparece el cuadro de diálogo *Nueva lista de réplicas*.
4. Escriba el título y la descripción de la lista de réplicas.
5. Para obtener opciones avanzadas, haga clic en el enlace *Propiedades de lista de réplicas*.

   Esto le permite especificar las dependencias que quiere que se repliquen automáticamente desde del sitio de origen al sitio de destino.
6. Seleccione las opciones necesarias, tal como se describe en la tabla.

| Opciones de objeto de dependencia | Definición |
|---|---|
| Incluir carpetas personales para usuarios seleccionados | Replica las carpetas personales y su contenido del usuario seleccionado. |
| Incluir categorías personales para usuarios seleccionados | Replica las categorías personales del usuario seleccionado. |
| Incluir universos para informes seleccionados | Replica cualquier universo del que dependan los objetos de informe seleccionados. |
| Incluir miembros de los grupos de usuarios seleccionados | Replica los usuarios del grupo seleccionado. |
| Incluir universos requeridos por universos seleccionados | Replica los universos que dependen de otros universos. |
| Incluir bandejas de entrada para usuarios seleccionados | Replica la bandeja de entrada y su contenido del usuario seleccionado. |

| Opciones de objeto de dependencia | Definición |
|---|---|
| Incluir grupos de usuarios para universos seleccionados | Replica los grupos de usuarios asociados a las sobrecargas de un universo. |
| Incluir niveles de acceso establecidos en objetos seleccionados | Replica los niveles de acceso usados en cualquiera de los objetos seleccionados. |
| Incluir documentos para categorías seleccionadas | Replica cualquier documento, incluidos Word, Excel y PDF, que se incluyan en las categorías seleccionadas. |
| Incluir perfiles para los usuarios y grupos de usuarios seleccionados | Replica los perfiles asociados con los usuarios o grupos de usuarios seleccionados. |
| Incluir conexiones usadas por universos seleccionados | Replica los objetos de conexión de universos usados por los objetos seleccionados. |

> **Nota**
>
> Algunos objetos de la plataforma de BI dependen de otros objetos. Por ejemplo: un documento de Web Intelligence depende del universo subyacente por su estructura y contenido. Si replica un documento de Web Intelligence pero no selecciona el universo que usa, la réplica no funcionará en el sitio de destino a menos que el universo ya se haya replicado allí. Sin embargo, si activa *Incluir universos para informes seleccionados*, Federación replica los universos de los que depende el informe automáticamente.

7. Haga clic en *Siguiente*.
8. Seleccione uno o varios objetos para agregarlos a la lista de réplicas.
   - Use los botones de flecha para agregar o eliminar objetos de la carpeta *Objetos disponibles*.
   - O bien, haga clic en *Objetos del repositorio* en *Replicar todo* para replicar todos los objetos Vista empresarial, Elementos empresariales, Infraestructura de datos, Conexión de datos, Lista de valores y objetos del repositorio, incluidas las imágenes y funciones del informe.

> **Nota**
>
> No se pueden replicar las carpetas del nivel superior situadas en la carpeta *Objetos disponibles*.

9. Haga clic en *Guardar y cerrar*.

## 27.7.2 Modificar listas de réplicas

Después de crear una lista de réplicas, puede modificar sus propiedades u objetos.

### 27.7.2.1 Para modificar las propiedades de una lista de réplicas

1. Vaya al área *Listas de réplicas* de la CMC.
2. Seleccione la *Lista de réplicas* que desea modificar.

3. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades generales*.
4. Modifique el título y la descripción. También puede modificar el resto de áreas de la lista de réplicas mientras el cuadro de diálogo *Propiedades generales* está abierto.
5. Si desea modificar las opciones de dependencia, haga clic en *Propiedades de la lista de réplica* de la lista de navegación.
6. Haga clic en *Guardar y cerrar*.

### Información relacionada

Creación de listas de réplicas [página 981]

## 27.7.2.2 Para modificar en una lista de réplicas

1. Vaya al área *Listas de réplicas* de la CMC.
2. Seleccione una *lista de réplicas*.
3. Haga clic en *Acciones* > *Administrar lista de réplicas*.
   Aparece el cuadro de diálogo *Administrar lista de réplica* con una lista de objetos incluida en la lista de réplicas.
4. Agregue o elimine objetos según convenga.
5. Haga clic en *Guardar y cerrar*.

### Información relacionada

Creación de listas de réplicas [página 981]

# 27.8 Administrar conexiones remotas

Los objetos de conexión remota contienen la información necesaria para conectarse a un despliegue remoto de la Plataforma de BI.

> **Nota**
>
> El objeto de conexión remota se crea en un despliegue de la plataforma de BI del sitio de destino. La conexión remota es el sitio de origen.

Puede ver las conexiones remotas en el área *Federación* de la CMC.

## 27.8.1 Crear conexiones remotas

Una conexión remota de Federación se conecta a un despliegue remoto de la Plataforma de BI. Para establecer una conexión al sitio de origen en el que se encuentra el contenido que se va a replicar, primero debe crear una conexión remota en el sitio de destino.

Puede crear carpetas y subcarpetas para organizar las conexiones remotas.

### 27.8.1.1 Para crear una carpeta de conexión remota

1. Vaya al área *Federación* de la CMC.
2. Haga clic en *Conexiones remotas*.
3. Haga clic en *Administrar* > *Nueva* > *Carpeta*.
   Aparece un cuadro de diálogo *Crear carpeta*.
4. Escriba un nombre de carpeta y haga clic en *Aceptar*.
   Ahora puede crear conexiones remotas en esta carpeta.

### 27.8.1.2 Para crear una conexión remota

Para conectarse a un despliegue remoto de la Plataforma de BI, debe crear una conexión remota en Federación.

1. Vaya al área *Federación* de la CMC.
2. Haga clic en *Conexiones remotas*.
3. Haga clic en *Administrar* > *Nuevo* > *Nueva conexión remota*.
   Aparece el cuadro de diálogo *Nueva conexión del sistema remoto*.
4. Escriba un título, una descripción y los campos relacionados según sea necesario:

   > **Nota**
   >
   > Todos los campos son obligatorios, excepto «Descripción» y «Limitar el número de objetos de limpieza».

| Campo | Descripción |
|---|---|
| Título | Nombre del objeto de conexión remota. |
| Descripción | Descripción del objeto de conexión remota. (Opcional) |

| Campo | Descripción |
| --- | --- |
| URI del servicio Web del sistema remoto | Dirección URL de los servicios Web de Federación, que se despliega automáticamente en el servidor de aplicaciones Java. Puede usar cualquier servicio Web de federación de la plataforma de BI, tanto si se trata del sitio de origen o de destino, o de otro despliegue. Use este formato:<br>**`http://<aplicación_suservidor_equipo_nombre>:<puerto>/dswsbobje`**.<br>Ejemplo: **`http://<miequipo.midominio.com>:<8080>/dswsbobje`** |
| CMS del sistema remoto | Nombre del CMS al que desea conectarse y al que se puede tener acceso por medio de los servicios Web de Federación. Se tratará como el CMS del sitio de origen. El formato es: **`Nombre_CMS:puerto`**.<br>Ejemplo: **`<miequipo>:6400`**<br>**Nota**<br>Si usa el puerto predeterminado 6400, la especificación del puerto es opcional. |
| Nombre de usuario | El nombre de usuario que se usa para conectarse al sitio de origen.<br>**Nota**<br>Asegúrese de que el nombre de usuario que está usando tiene derechos de visualización en la lista de réplicas del despliegue del sitio de origen. |
| Contraseña | La contraseña de la cuenta de usuario para conectarse al sitio de origen. |
| Autenticación | El tipo de autenticación de cuenta para conectarse al sitio de origen. Las opciones son: Enterprise, AD o LDAP. |
| Frecuencia de limpieza (en horas) | La frecuencia con la que las tareas de réplica que usan este objeto de conexión remota realizan una limpieza de objetos. Especifique únicamente números enteros positivos. La unidad son horas. Valore predeterminado = 24. |
| Limitar el número de objetos de limpieza a | El número de objetos que limpia una tarea de réplica. (Opcional) |

5. Haga clic en *Aceptar*.

## 27.8.2 Modificar conexiones remotas

Después de crear una conexión remota, puede modificar sus propiedades y opciones de seguridad.

Para modificar una conexión remota:

1. Vaya al área *Federación* de la CMC.
2. Haga clic en *Conexiones remotas*.

3. Haga doble clic en la conexión remota que desea modificar.
   Aparece el cuadro de diálogo *Propiedades de la conexión remota*. Puede modificar las siguientes propiedades:
   - *Título*
   - *Descripción*
   - *URI del servicio Web del sistema remoto*
   - *CMS del sistema remoto*
   - *Nombre del usuario*
   - *Contraseña*
   - *Autenticación*
   - *Frecuencia de limpieza (en horas)*
   - *Limitar el número de objetos de limpieza a*
4. Especifique los cambios.
5. Haga clic en *Guardar y cerrar*.

## 27.9 Administración de tareas de réplica

Una tarea de réplica es un tipo de objeto que se ejecuta en una programación y que se usa para replicar el contenido entre dos despliegues de la Plataforma de BI en federación.

> **Nota**
>
> Los objetos replicados en un sitio de destino se marcarán con un icono de réplica, tal y como se muestra aquí: Si existe un conflicto, un objeto se marcará con un icono de conflicto, como se muestra aquí:

Puede ver una lista de tareas de réplica en la carpeta *Conexión remota* del área *Federación* de la CMC.

### 27.9.1 Creación de tareas de réplica

Se necesita una tarea de réplica para replicar el contenido entre dos despliegues de la Plataforma de BI en federación. Cada tarea de réplica debe tener únicamente una conexión remota y una lista de réplicas asociada a ella.

#### 27.9.1.1 Para crear una tarea de réplica

1. Vaya al área *Federación* de la CMC.
2. Haga clic en *Conexiones remotas*.
3. Seleccione una *Conexión remota* para que albergue la nueva tarea de réplica.

> **⚠ Precaución**
>
> La CMC debe poder conectarse a los servicios web en el URI de conexión remota para continuar usando el asistente.

4. Haga clic en *Administrar* > *Nuevo* > *Nueva tarea de réplica*.
   Aparecerá un cuadro de diálogo *Nueva tarea de réplica*.
5. Escriba un título y una descripción para la tarea de réplica.
6. Haga clic en *Siguiente*.
   Aparece una lista de listas de réplicas disponibles en el sitio de origen.
7. Seleccione la *lista de réplicas* que desee usar con la tarea de réplica.
8. Haga clic en *Siguiente*.
9. Seleccione las opciones de configuración tal y como se describe en la siguiente tabla.

| Opción | Descripción |
|---|---|
| *Habilitar limpieza de objetos en destino* | Fuerza a la tarea de réplica a eliminar los objetos replicados en el sitio de destino en caso de que el objeto que lo originó se haya eliminado del sitio de origen.<br>**ⓘ Nota**<br>La limpieza de objetos no eliminará los objetos replicados por medio de dependencias u objetos seleccionados en la lista de réplicas. |
| *Réplica unidireccional* | Especifica que un objeto solo se replica desde el sitio de origen al sitio de destino. Cualquier cambio efectuado después de la réplica en el objeto en el sitio de origen se replica en el sitio de destino, pero los cambios realizados en el sitio de destino no se replican en el sitio de origen. |
| *Réplica bidireccional* | Especifica que los objetos se replican en ambas direcciones; desde del sitio de origen hacia el sitio de destino y desde el sitio de destino hacia el sitio de origen. Los cambios efectuados en estos objetos tras la réplica en uno de los sitios se replican automáticamente en el otro. |
| *El sitio de origen tiene prioridad* | Especifica que en las ocasiones en las que se detecta un conflicto entre un objeto del sitio de origen y su versión replicada en el sitio de destino, la versión del sitio de origen tiene prioridad. |
| *Sin resolución automática de conflictos* | Especifica que no se realiza ninguna acción para resolver los conflictos detectados. |
| *El sitio de destino tiene prioridad* (solo disponible con la réplica bidireccional) | Especifica que en las ocasiones en las que se detecta un conflicto entre un objeto del sitio de origen y su versión replicada del sitio de destino, la versión del sitio de destino tiene prioridad. |
| *Réplica normal* | Especifica que la tarea de réplica actúa de forma normal. |

| Opción | Descripción |
| --- | --- |
| *Actualizar a partir de origen* | Replica todo el contenido del sitio de origen al sitio de destino tanto si ha cambiado como si no. Puede replicar toda la lista de réplicas o solo una parte. |
| *Actualizar a partir de destino* (solo disponible con la réplica bidireccional) | Replica todo el contenido desde el sitio de destino al sitio de origen tanto si ha cambiado como si no. Puede replicar toda la lista de réplicas o solo una parte. |
| *Replicar todos los objetos* (solo visible con la réplica bidireccional) | Replica toda la lista de réplicas.<br>**Nota**<br>Se trata de la opción más completa, pero es la que más tarda en realizarse. |
| *Replicar programaciones remotas* (solo visible con la réplica bidireccional) | Replica las instancias remotas pendientes desde el sitio de destino al sitio de origen y fuerza a las instancias completadas del sitio de origen al sitio de destino. |
| *Replicar plantillas de documento* | Replica todos los objetos que no sean instancias (que se ejecutan localmente o informes marcados para la programación remota). Esto incluye usuarios, grupos, carpetas, informes, etc. |
| *Replicar instancias completadas ejecutadas localmente* | Replica las instancias completadas solo desde el sitio de destino al sitio de origen. |

10. Haga clic en *Aceptar*.

## 27.9.2 Programación de tareas de réplica

Después de crear una tarea de réplica, puede programarla para que se ejecute una vez o de forma periódica. También puede programar varias tareas de réplica en un sitio de destino desde un sitio de origen.

> **Nota**
>
> Si programa varias tareas de réplica en un sitio de destino, sólo se podrá conectar una tarea de réplica al sitio de origen cada vez. Todas las demás tareas de réplica que intenten conectarse se establecerán con un estado pendiente y permanecerán pendientes hasta que puedan conectarse automáticamente al sitio de origen.

### 27.9.2.1 Para programar una tarea de réplica

1. Vaya al área *Federación* de la CMC.
2. Seleccione la *tarea de réplica* que desea programar.
3. Haga clic en *Acciones* > *Programaciones*.
4. Seleccione las opciones de programación pertinentes.

## 27.9.3 Modificar las tareas de réplica

Después de crear una tarea de réplica en Federación, puede modificar sus propiedades.

### 27.9.3.1 Para modificar una tarea de réplica

1. Vaya al área *Federación* de la CMC.
2. Haga clic en la carpeta *Conexiones remotas*.
3. Seleccione el objeto de *conexión remota* que contiene la *tarea de réplica* que va a modificar.
4. Seleccione la *tarea de réplica* que desea modificar.
5. Haga clic en *Administrar* > *Administrar las propiedades del objeto*.
6. Vea y edite *Propiedades*, *Programación*, *Historial*, *Lista de réplicas* y *Seguridad de usuario*, según sea necesario.

| Secciones | Descripción |
|---|---|
| Propiedades | Modifique el nombre, la descripción y otras propiedades generales y opciones de la tarea de réplica. |
| Programación | Establezca que la tarea de réplica se ejecute según una programación periódica. |
| Historial | Vea y administre todas las instancias de la tarea de réplica. |
| Lista de réplicas | Cambie la lista de réplicas seleccionada. |
| Seguridad de usuario | Establezca derechos sobre la tarea de réplica. |

## 27.9.4 Visualización de un registro después de una tarea de réplica

Cada vez que se ejecuta una tarea de réplica, Federación genera automáticamente un archivo de registro que se crea en el sitio de destino. Los archivos de registro usan estándares XML 1.1 y requieren un explorador Web que admita XML 1.1.

Para ver un registro de réplicas:

1. Vaya al área *Federación* de la CMC.
2. Haga clic en *Todas las tareas de réplica*.
3. Seleccione una *Tarea de réplica* de la lista.
4. Haga clic en *Propiedades*.
   Se abre la página *Propiedades* de la tarea de réplica.
5. Haga clic en *Historial*.
6. Haga clic en *Hora de la instancia* del archivo de registro para ver las tareas de réplica correctas o haga clic en el estado *Error* para ver un archivo de registro de las tareas de réplica con error.

7. Seleccione la instancia pertinente para ver el archivo de registro.
   El archivo de registro se genera en formato XML y usa un formulario XSL para dar formato a la información en una página HTML.

   Puede tener acceso al registro XML desde el equipo que ejecuta el Agente de inteligencia de servidor que contiene el servidor de tareas de Adaptive. Puede encontrar el archivo de registro en esta ubicación:

   - En Windows: `<DirInstal>\SAP BusinessObjects XI 4.0\logging`
   - En Unix: `<DirInstal>/sap_bobj/logging`

## 27.10 Administración de la limpieza de objeto

En federación, debe realizar limpiezas de objetos en todo el ciclo de vida del proceso de réplica para asegurarse de que todos los objetos que elimina del sitio de origen también se eliminan del sitio de destino.

La limpieza de objetos implica dos elementos: una conexión remota y una tarea de réplica. Un objeto de conexión remota define opciones de limpieza generales y una tarea de réplica lleva a cabo la limpieza cuando transcurre el intervalo apropiado.

### 27.10.1 Cómo usar la limpieza de objetos

Las tareas de réplica que usan la misma conexión remota colaboran durante la limpieza de objetos. Esto significa que la tarea de réplica limpiará los objetos de su lista de réplicas, así como los objetos dentro de otras listas de réplica que usen la misma conexión remota. Una conexión remota sólo se considera igual si el objeto principal de la tarea de réplica es el mismo objeto de conexión remota.

#### Ejemplo

Las Tareas de réplica A y B replican el Objeto A y el Objeto B. Ambas replican desde el mismo sitio de origen y usan la misma conexión remota. Si el sitio de origen elimina el Objeto B, la Tarea de réplica A verá que el Objeto B se ha eliminado. Aunque lo replique la Tarea de réplica B, el Objeto B también se eliminará del sitio de destino. Cuando la Tarea de réplica B lo ejecute, no necesitará ejecutar una limpieza de objetos.

> **Nota**
>
> Sólo se eliminan los objetos del sitio de destino durante la limpieza de objetos. Si elimina un objeto del sitio de origen que forma parte de una réplica, el objeto se eliminará del sitio de destino. Sin embargo, si un objeto se elimina del sitio de destino, no se eliminará del sitio de origen durante la limpieza de objetos, aunque la tarea de réplica se encuentre en modo de réplica bidireccional.
>
> Los objetos que se eliminan o eliminan de la lista de réplicas no se eliminan del sitio de destino. Para eliminar correctamente un objeto especificado en una lista de réplicas, debe eliminarlo del sitio de destino y del sitio de origen. Los objetos que se replican mediante cálculos de dependencia no se eliminan.

## 27.10.2 Límites de la limpieza de objetos

En el objeto de conexión remota, puede definir el número de objetos que una tarea de réplica limpiará cada vez. La Federación hace automáticamente el seguimiento de dónde acaba el trabajo de limpieza. De este modo, la próxima vez que ejecute una tarea de réplica, iniciará la siguiente tarea de limpieza en ese punto.

> → Sugerencias
>
> Para finalizar una tarea de réplica más rápido, limite el número de objetos de la limpieza.

### Ejemplo

Las tareas de réplica A y B replican el Objeto A y el Objeto B. Ambos objetos se replican desde el mismo sitio de origen y usan la misma conexión remota.

Si el sitio de origen elimina el Objeto B y el límite de objetos está establecido en 1, la próxima vez que se ejecute la Tarea de réplica A, sólo comprobará si el Objeto A se ha eliminado. De esta forma, la eliminación del Objeto B no se comprueba y no se eliminará.

A continuación, se ejecuta la Tarea de réplica B que inicia la limpieza de objetos donde terminó la Tarea de réplica A. Comprobará si el Objeto B se ha eliminado y lo eliminará del sitio de destino. Puede encontrar esta opción en las propiedad del objeto de conexión remota «Limitar el número de objetos de limpieza a:»

> ⓘ Nota
>
> Si no selecciona esta opción, todas las tareas de réplica que usan esta conexión remota comprobarán todos los objetos para su posible limpieza.

## 27.10.3 Frecuencia de la limpieza de objetos

Puede establecer la frecuencia con la que una tarea de réplica realizará una limpieza de objetos en el campo «Frecuencia de limpieza» de la conexión remota.

> ⓘ Nota
>
> Debe introducir un número entero positivo, que representa el número de horas que debe esperarse entre los procesos de limpieza de objetos.

### Ejemplo

Las Tareas de réplica A y B replican el Objeto A y el Objeto B. Ambos objetos se replican desde el mismo sitio de origen y usan la misma conexión remota.

Si se elimina el Objeto B del sitio de origen y se cumplen todas las condiciones que se enumeran a continuación, la tarea de réplica comprobará si se ha eliminado el Objeto A.

- El límite de objetos es 1
- La frecuencia de limpieza es de 150 horas
- Se ejecuta la Tarea de réplica A a continuación

Puesto que el límite de objetos está establecido en 1, el Objeto B no se comprobará ni eliminará en el sitio de destino.

La siguiente limpieza tiene lugar 150 horas después de que la Tarea de réplica A hiciera la comprobación inicial. Aunque las tareas de réplica A y B se pueden ejecutar varias veces antes del límite de 150 horas, ninguna intentará ejecutar una limpieza de objetos. Después de las 150 horas, se ejecutará la siguiente tarea de réplica e intentará limpiar. A continuación, determinará que el Objeto B se eliminó en el sitio de origen y lo eliminará en el sitio de destino.

### Activación y desactivación de opciones

Cada tarea de réplica puede participar en la limpieza de objetos. Use la opción «Activar limpieza de objetos en destino» en una tarea de réplica para indicarle si debe ejecutar la limpieza de objetos. En algunos casos, puede tener tareas de réplica de alta prioridad que no desea que participen en la limpieza de objetos, de modo que pueda ejecutarlas lo antes posible. Para ello, desactive la limpieza de objetos.

### Información relacionada

Límites de la limpieza de objetos [página 991]

## 27.11 Administrar la detección y resolución de conflictos

En Federación, se puede producir un conflicto si se cambian las propiedades de un objeto en el sitio de origen y en el de destino. Se comprueban las propiedades de nivel superior y las anidadas de un objeto en busca de conflictos. Por ejemplo, se puede producir un conflicto si un informe o el nombre de un informe se modifican tanto en el sitio de origen como en el de destino.

Algunas situaciones no crean conflictos. Por ejemplo, si se modifica el nombre de un informe en el sitio de origen y la descripción de la versión replicada se modifica en el sitio de destino, los cambios se fusionan y no se produce ningún conflicto.

### 27.11.1 Resolución de conflictos de réplica unidireccional

En la réplica unidireccional hay dos opciones de resolución de conflictos.

## El sitio de origen tiene prioridad

Si se produce un conflicto durante la réplica unidireccional, el objeto del sitio de origen tiene prioridad. Cualquier cambio de los objetos de un sitio de destino se sobrescribe con la información del sitio de origen. Por ejemplo, si se modifica un informe en el sitio de origen y en el de destino, la modificación del sitio de destino se sobrescribirá con la versión del sitio de origen después de la siguiente tarea de réplica.

> ⓘ Nota
>
> Puesto que el conflicto se resuelve automáticamente, no se genera en el archivo de registro y no aparece en la lista de objetos en conflicto.

## Sin resolución automática de conflictos

Si se produce un conflicto y se selecciona «Sin resolución automática de conflictos», el conflicto no se resuelve, no se genera en un archivo de registro y no aparece en la lista de objetos en conflicto.

Los administradores pueden tener acceso a una lista de todos los objetos replicados que están en conflicto en el área Federación de la CMC. Los objetos en conflicto se agrupan según la conexión remota que usaron para conectarse al sitio de origen. Para tener acceso a estas listas, vaya a la carpeta Errores de replicación del área Federación de la CMC y seleccione la conexión remota pertinente. Todos los objetos replicados en un sitio de destino se etiquetarán con un icono de réplica. Si hay un conflicto, los objetos se etiquetarán con un icono de conflicto. También aparece un mensaje de advertencia en la página *Propiedades*.

> ⓘ Nota
>
> La lista se actualiza cuando se completa una tarea de réplica que usa una conexión remota. Contiene todos los objetos en conflicto para todas las tareas de réplica que usan su conexión remota específica.

> ⓘ Nota
>
> Un usuario con acceso a la CMC y a las instancias de la tarea de réplica puede tener acceso al registro XML guardado en el directorio de archivos de registro. El icono del objeto del sitio de destino se marca para indicar un conflicto. Durante el procesamiento se crea un registro de conflictos.

Abdul modifica el Informe A en el sitio de origen. María modifica la versión replicada en el sitio de destino. La próxima vez que se ejecute la tarea de réplica, el informe estará en conflicto ya que ha cambiado en ambos sitios y no se resolverá.

El informe de destino se mantiene y los cambios en el informe de origen no se replican. Las tareas de réplicas posteriores se comportarán de la misma forma hasta que el conflicto se resuelva. No se replica ningún cambio en el sitio de origen hasta que no se resuelve manualmente el conflicto.

> ⓘ Nota
>
> En este caso, no se replica el objeto entero. No se transferirán los demás cambios que puedan no estar en conflicto.

**Para resolver manualmente un conflicto dispone de tres opciones:**

1. Crear una tarea de réplica que replique únicamente los objetos en conflicto. Debe usar el mismo objeto de conexión remota y lista de réplicas.
   Para mantener los cambios del sitio de origen, cree una tarea de réplica. A continuación, configure el modo de réplica en «Actualizar a partir de origen» y configure Resolución automática de conflictos en «El sitio de origen tiene prioridad».
   Para conservar los cambios del sitio de destino, cree una tarea de réplica con Tipo de réplica = «Réplica bidireccional», Modo de réplica = «Actualizar a partir de destino» y Resolución automática de conflictos = «El sitio de destino tiene prioridad»

   > ⓘ Nota
   >
   > En modo de réplica, establezca «Actualizar a partir de origen » o «Actualizar a partir de destino» para seleccionar solo los objetos en conflicto en la lista de réplicas. De este modo, los demás objetos no se replican. A continuación, programe la tarea de réplica para que se ejecute y ésta replicará los objetos seleccionados y resolverá los conflictos según lo especificado.

2. Crear una tarea de réplica que replique únicamente los objetos en conflicto. Será necesario que use el mismo objeto de conexión remota. Sin embargo, a diferencia de la opción 1, puede crear una nueva lista de réplicas en el sitio de origen. Use únicamente los objetos en conflicto y cree una nueva tarea de réplica que usará esta lista de réplicas en concreto.
   Para conservar los cambios del sitio de origen, establezca Resolución automática de conflictos en «El sitio de origen tiene prioridad».
   Para conservar los cambios del sitio de destino, establezca Resolución automática de conflictos en «El sitio de destino tiene prioridad» y Tipo de réplica en «Réplica bidireccional».
3. Para las tareas de réplica unidireccionales, solo puede eliminar el objeto en el sitio de destino. La próxima vez que se ejecute la tarea de réplica, replicará el objeto del sitio de origen al sitio de destino.

   > ⓘ Nota
   >
   > Tenga cuidado al eliminar un objeto porque otros objetos que dependen de él pueden eliminarse, dejar de funcionar o perder la seguridad. Las opciones 1 y 2 son las recomendadas.

## 27.11.2 Resolución de conflictos de réplica bidireccional

En los conflictos de réplica bidireccionales, dispone de dos opciones para detectar el conflicto:

- El sitio de origen tiene prioridad
- El sitio de destino tiene prioridad
- Sin resolución automática de conflictos

### El sitio de origen tiene prioridad

Si se produce un conflicto, el sitio de origen tendrá prioridad y sobrescribirá los cambios en el sitio de destino.

## Ejemplo

Lucía cambia el nombre de un informe por Informe A. Malik modifica el nombre de la versión replicada en el sitio de destino por Informe B. Después de ejecutar la siguiente tarea de réplica, la versión replicada del sitio de destino revertirá a Informe A.

No se generará un conflicto en el archivo de registro y no aparecerá en la lista de objetos conflictivos porque el conflicto se ha resuelto según las instrucciones del usuario en el sitio de origen.

## El sitio de destino tiene prioridad

Si se produce un conflicto, el sitio de destino conservará sus cambios y los sobrescribirá en el sitio de origen.

## Ejemplo

Kamal modifica el nombre de un informe por Informe A. Pedro modifica el nombre de la versión replicada en el sitio de destino por Informe B. Cuando se ejecuta la tarea de réplica, se detecta un conflicto. El nombre del informe de destino permanece como Informe B.

En la réplica bidireccional, los cambios también se envían al sitio de origen. En este escenario, el sitio de origen se actualiza y se cambia el nombre del informe por Informe B. Esto no genera ningún conflicto en el archivo de registro y no aparecerá en la lista de objetos en conflicto porque el conflicto se resolvió según las instrucciones del usuario.

## Sin resolución automática de conflictos

Cuando se selecciona «Sin resolución automática de conflictos», los conflictos no se resuelven. El conflicto se indicará en el archivo de registro para el administrador, que puede resolverlo manualmente.

> ⓘ Nota
>
> Se marca el icono de un objeto para indicar que existe un conflicto.

> ⓘ Nota
>
> Aunque los cambios se replican tanto en el sitio de origen como en el de destino en la réplica bidireccional, sólo las versiones del sitio de destino se marcarán con un icono de conflicto.

> ⓘ Nota
>
> Un usuario con acceso a la CMC y a las instancias de la tarea de réplica puede tener acceso al registro XML emitido en el directorio de archivos de registro. El icono del objeto del sitio de destino se marca para indicar un conflicto. Durante el procesamiento se crea un registro de conflictos.

El administrador puede tener acceso a una lista de todos los objetos replicados que están en conflicto en el área Federación de la CMC. Los objetos en conflicto se agrupan según la conexión remota que usaron para conectarse al sitio de origen. Para acceder a estas listas, vaya a *CMC* > *Federación* > *Errores de replicación* > *Conexión remota*.

> **Nota**
>
> La lista se actualiza cuando se completa una tarea de réplica que usa una conexión remota. Contiene todos los objetos en conflicto para todas las tareas de réplica que usan su conexión remota específica. Todos los objetos replicados en un sitio de destino se etiquetarán con un icono de replicación. Si hay un conflicto, los objetos se etiquetarán con un icono de conflicto.

## Ejemplo

Miguel modifica el Informe A en el sitio de origen. Damián modifica la versión replicada en el sitio de destino. La próxima vez que se ejecute la tarea de réplica, el informe estará en conflicto ya que ha cambiado en ambos sitios y no se resolverá.

El informe de destino se conserva y los cambios en el informe de origen no se replican. Las tareas de réplica posteriores se comportarán de la misma forma hasta que el conflicto se resuelva. Los cambios en el sitio de origen no se replicarán hasta que el conflicto se resuelva manualmente por parte del administrador o un administrador delegado.

> **Nota**
>
> En este caso, no se replica el objeto entero. No se replicarán los demás cambios que no estén en conflicto.

> **Nota**
>
> Un usuario con acceso a la CMC y a las instancias de la tarea de réplica puede tener acceso al registro XML emitido en el directorio de archivos de registro. El icono del objeto del sitio de destino se marca para indicar un conflicto. Durante el procesamiento se crea un registro de conflictos.

El administrador puede tener acceso a una lista de todos los objetos replicados que están en conflicto en el área Federación de la CMC. Los objetos en conflicto se agrupan según la conexión remota que usaron para conectarse al sitio de origen. Para acceder a estas listas, vaya a *CMC* > *Federación* > *Errores de replicación* > *Conexión remota*.

> **Nota**
>
> La lista se actualiza cuando se completa una tarea de réplica que usa una conexión remota. Contiene todos los objetos en conflicto para todas las tareas de réplica que usan su conexión remota específica. Todos los objetos replicados en un sitio de destino se etiquetarán con un icono de replicación. Si hay un conflicto, los objetos se etiquetarán con un icono de conflicto.

**Para resolver manualmente un conflicto dispone de tres opciones:**

1. Crear una tarea de réplica que replique únicamente los objetos en conflicto. Debe usar el mismo objeto de conexión remota y lista de réplicas.

Para mantener los cambios del sitio de origen, cree una tarea de réplica. A continuación, configure el modo de réplica en «Actualizar a partir de origen» y configure Resolución automática de conflictos en «El sitio de origen tiene prioridad».
Para conservar los cambios del sitio de destino, cree una tarea de réplica y configure Tipo de réplica en «Réplica bidireccional», Modo de réplica en «Actualizar a partir de destino» y Resolución automática de conflictos en «El sitio de destino tiene prioridad».

> **Nota**
>
> En modo de réplica, establezca «Actualizar a partir de origen »o «Actualizar a partir de destino» para seleccionar sólo los objetos en conflicto en la lista de réplicas. De este modo, los demás objetos no se replican. A continuación, programe la tarea de réplica para que se ejecute y ésta replicará los objetos seleccionados y resolverá los conflictos según lo especificado.

2. Crear una tarea de réplica que replique únicamente los objetos en conflicto. Será necesario que use el mismo objeto de conexión remota. Sin embargo, a diferencia de la opción 1, puede crear una nueva lista de réplicas en el sitio de origen. Utilice solo los objetos en conflicto y cree una tarea de réplica, que utilizará esta lista de réplicas en concreto.
   Para conservar los cambios del sitio de origen, establezca Resolución automática de conflictos en: «El sitio de origen tiene prioridad».
   Para conservar los cambios del sitio de destino, establezca Resolución automática de conflictos en: «El sitio de destino tiene prioridad» y Tipo de réplica en: «Réplica bidireccional».
3. Elimine el objeto del sitio que no se desee que se encuentre.

> **Nota**
>
> Tenga cuidado al eliminar un objeto porque otros objetos que dependen de él pueden eliminarse, dejar de funcionar o perder la seguridad. Las opciones 1 y 2 son las recomendadas.

Para conservar los cambios del sitio de destino, puede eliminar el objeto en el sitio de origen. La próxima vez que se ejecute la tarea de réplica, replicará el objeto del sitio de destino al sitio de origen.

> **Nota**
>
> Tenga cuidado al eliminar una copia del sitio de origen, ya que otros sitios de destino que repliquen ese objeto pueden ejecutar su tarea de réplica antes de que la copia se haya vuelto a replicar. Ello hará que los otros sitios de destino eliminen su copia, que no estará disponible hasta que la copia se haya devuelto.

Para mantener los cambios del sitio de origen, puede eliminar el objeto en el sitio de destino.

## 27.12 Uso de servicios Web en Federación

Federación usa servicios Web para enviar objetos y sus cambios entre los sitios de origen y de destino. Los servicios Web específicos de Federación se instalan e implementan automáticamente en la instalación de la plataforma de BI. Sin embargo, quizá quiera modificar propiedades o personalizar despliegues en los servicios Web para mejorar la funcionalidad, tal como se describe en esta sección.

→ Sugerencias

Para mejorar la administración y funcionalidad de los archivos, habilite el almacenamiento en caché de archivos en la federación.

## 27.12.1 Variables de sesión

Si transfiere una gran cantidad de archivos de contenido en una tarea de réplica, es posible que quiera aumentar el tiempo de espera de la sesión de los servicios Web de Federación.

La propiedad se encuentra en el archivo `dsws.properties`:

```
<Directorio de instalación del servidor de aplicaciones>\dswsbobje\Web-INF\classes
```

Por ejemplo:

```
C:\Archivos de programa\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\classes
```

Para activar una variable de sesión, introduzca:

```
session.timeout = x
```

Donde «x »es el tiempo deseado; «x» se mide en segundos. Si no se especifica, el valor predeterminado es 1200 segundos o 20 minutos.

Las nuevas propiedades surten efecto solo después de que la aplicación Web modificada se vuelva a desplegar en el equipo que ejecuta el servidor de aplicaciones Web. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web. Para obtener información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 27.12.2 Memoria caché de archivos

El almacenamiento en caché de archivos permite que los servicios Web controlen datos adjuntos muy grandes sin almacenarlos en el búfer de memoria. Si no se activa con tamaños de transferencia grandes, es posible que se use la memoria de la máquina virtual Java y que falle la réplica.

ⓘ Nota

El almacenamiento en caché de archivos reduce el rendimiento, ya que los servicios Web procesan en archivos en lugar de hacerlo en memoria. Puede usar una combinación de ambas opciones y enviar las transferencias grandes a un archivo y las más pequeñas a la memoria.

Para habilitar el almacenamiento en caché de archivos, modifique el archivo `Axis2.xml` ubicado en:

```
<Directorio de instalación del servidor de aplicaciones>\dswsbobje\Web-Inf\conf
```

Por ejemplo:

```
C:\Archivos de programa\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
```

Especifique los siguientes datos:

```
<parameter name="cacheAttachments" locked="false">true</parameter>
```

```
<parameter name="attachmentDIR" locked="false">temp directory</parameter>
```

```
<parameter name="sizeThreshold" locked="false">4000</parameter>
```

> **Nota**
>
> El tamaño de umbral se mide en bytes.

Las nuevas propiedades surten efecto solo después de que la aplicación Web modificada se vuelva a desplegar en el equipo que ejecuta el servidor de aplicaciones Web. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web. Para obtener información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 27.12.3 Despliegue personalizado

Los servicios Web de Federación pueden desplegarse automáticamente y requieren que estén activados los servicios «federation», «biplatform» y «session». Para desactivar Federación o cualquier otro servicio Web, modifique el correspondiente archivo `service.xml` de servicios Web.

Los servicios Web de la Plataforma de BI se encuentran ubicados en:

```
<Directorio de instalación del servidor de aplicaciones>\dswsbobje\WEB-INF\services
```

Ejemplo:

```
C:\Archivos de programa\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\services
```

Para desactivar los servicios Web:

- Agregue la propiedad «activate» en la etiqueta de nombre de servicio del archivo `service.xml` y establézcala como false
- Reinicie el servidor de aplicaciones Java

Por ejemplo, para desactivar Federación:

El archivo `services.xml` se encuentra en:

```
C:\Archivos de programa\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswsbobje\WEB-INF\services\federator\META-INF
```

Cambie el nombre de servicio de:

```
<service name="Federator">
```

Hasta:

```
<service name="Federator" activate="false">
```

Las nuevas propiedades surten efecto solo después de que la aplicación Web modificada se vuelva a desplegar en el equipo que ejecuta el servidor de aplicaciones Web. Use WDeploy para volver a desplegar el archivo WAR en el servidor de aplicaciones Web. Para obtener información acerca del uso de WDeploy, consulte el *Manual del despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 27.13 Programación remota e instancias ejecutadas localmente

En esta sección se explica la programación remota, las instancias ejecutadas localmente y el uso compartido de instancias. Estas funciones permiten que los informes se ejecuten donde se encuentran los datos y envíen las instancias completadas a las ubicaciones adecuadas.

### 27.13.1 Programación remota

Con Federación se puede programar un informe en el sitio de destino y procesarlo después en el de origen. La instancia completada se devolverá al sitio de destino.

Para habilitar la programación remota, programe un informe como lo hace habitualmente y active la opción «Ejecutar en el sitio de origen». Para activar esta opción, haga clic en *Programar* > *Programando grupo de servidores* > *Ejecutar en el sitio de origen*. Una vez creadas las instancias programadas se colocan en la etapa pendiente.

Durante la programación remota, se descartará la información enviada al sitio de destino y la instancia de informe permanecerá en la etapa pendiente.

Cuando la siguiente tarea de réplica que administra el informe se active para la programación remota, copiará la instancia en el sitio de origen para su procesamiento. La instancia permanece en un estado pendiente hasta que el programador la procese. Mientras tanto, la tarea de réplica que la ha enviado devolverá cualquier instancia y cambios de objeto que se hayan completado anteriormente.

Una vez procesada la instancia en el sitio de origen, cambia a estado completado. Cuando la siguiente tarea de réplica que administra el informe se active para programación remota, ésta utiliza la instancia completada para actualizar la copia en el sitio de destino. Una vez actualizada, la instancia en el sitio de destino estará completa.

> **Nota**
>
> Una tarea de réplica se tiene que ejecutar dos veces para devolver una instancia completada.

#### Ejemplo

1. Tomás programa el Informe A para programación remota.
2. Se crea el Informe A en el sitio de destino y se encuentra en el estado pendiente.
3. Se ejecuta la Tarea de réplica A. En primer lugar, replica los cambios del sitio de origen al de destino (incluidas las instancias completadas anteriormente). A continuación, copia la instancia en estado pendiente al sitio de origen, así como los cambios que se replicarán del sitio de destino al sitio de origen.
4. En el sitio de origen, el programador toma la instancia que está en estado pendiente y la envía para procesarla al servidor de tareas adecuado. A continuación, la instancia se procesa y se coloca en el sitio de origen con el estado completado.
5. Se ejecuta de nuevo la Tarea de réplica A. Cuando replica contenido del sitio de origen al de destino, se selecciona la instancia completada Informe A y los cambios se aplican a la versión del destino.

6. Una vez terminada la tarea, la versión del destino estará completa.

La programación remota solo funciona con tareas de réplica bidireccionales. Se debe activar «Replicar programaciones remotas». Esta opción se encuentra en la página *Propiedades de la tarea de réplica* del área «Filtros de réplica». En algunos escenarios se pueden replicar algunas tareas programadas de forma remota con más frecuencia que otros objetos de la lista de réplicas. Para ello, cree dos tareas de réplica. Active una tarea con «Replicar programaciones remotas» para una tarea de réplica que solo se centre en la programación remota. Active la otra tarea con «Replicar plantillas de documento» o «Replicar todos los objetos (sin filtro)».

> **Nota**
>
> Cuando se activa la programación remota, las instancias completadas y las que han fallado aparecen en los sitios de origen y de destino.
>
> Si un usuario del sitio de destino programa un informe para la programación remota y el usuario no existe en el sitio de origen, la instancia fallará en el sitio de origen. El propietario de la instancia que ha fallado será la cuenta de usuario del objeto de conexión remota que se utiliza para la conexión con el origen.
>
> Una tarea de réplica solo se puede configurar para la programación remota, pero siempre replica los objetos ascendientes de la instancia de informe. Esto significa que si hay cualquier cambio entre réplicas, la tarea replica el informe real, la carpeta de informes real, etc. Si no desea que estos cambios del sitio de destino se repliquen en el sitio de origen, puede usar derechos de seguridad para controlar los cambios que se replicarán.

### Información relacionada

Administrar derechos de seguridad [página 971]

## 27.13.2 Instancias ejecutadas localmente

Las instancias ejecutadas localmente son instancias de un informe que se procesan a partir de informes en el sitio de destino. Con Federación, puede replicar las instancias completadas del sitio de destino en el sitio de origen.

Para que una tarea de réplica replique las instancias completadas y las que han fallado del sitio de destino en el de origen, haga clic en *Propiedades de la tarea de réplica* > *Filtros de réplica* > *Replicar instancias completadas ejecutadas localmente*.

En algunos casos puede desear que una tarea de réplica sólo replique instancias ejecutadas localmente. Para ello, active «Replicar instancias completadas ejecutadas localmente».

> **Nota**
>
> Cuando se activan las instancias ejecutadas localmente en una tarea de réplica, se replican en el sitio de origen tanto las instancias completadas como las que han dado error. Así pues, habrá copias tanto en el sitio de origen como en el de destino.
>
> Las instancias pendientes nunca se replican.

> Si el propietario de una instancia ejecutada localmente no existe en el sitio de origen, el propietario será la cuenta de usuario usada para conectarse al objeto de conexión remota.

## 27.13.3 Uso compartido de instancias

Cuando se activan la programación remota y las instancias ejecutadas localmente en una tarea de réplica, se puede producir el uso compartido de instancias si un sitio de origen con varios sitios de destino replica el mismo informe.

### Ejemplo

El Informe A se origina en el sitio de origen mientras que los sitios de destino A y B lo replican. El uso compartido de instancias se produce en ambos sitios de destino:

- Las tareas de réplica activadas con «Replicar programaciones remotas» y/o «Replicar instancias completadas ejecutadas localmente» replican el informe A con la misma tarea de réplica que anteriormente
- Programan que el informe A en el sitio de destino «se ejecute en el origen» y/o se ejecute localmente

Si ambos sitios de destino A y B replican el Informe A y sus correspondientes tareas de réplica replican programaciones remotas y/o replican instancias ejecutadas localmente, todas las instancias que se procesaron en el sitio de destino A y/o en el sitio de origen en nombre del sitio de destino A se compartirán con el sitio de destino B.

De forma similar, todas las instancias procesadas en el sitio de destino B y/o procesadas en el sitio de origen también se compartirán con el sitio de destino A. Por último, el sitio de origen y los sitios de destino A y B tendrán un conjunto idéntico de instancias.

El uso compartido de instancias es ideal en muchos casos. Por ejemplo, cuando usuarios de otros sitios necesitan tener acceso a información de sus despliegues de igual nivel. En ese caso, para evitar que los usuarios vean las réplicas en el sitio local, asegúrese de haber establecido los derechos de seguridad adecuados. Por ejemplo, en un objeto de informe, aplique los derechos de manera que los usuarios solo puedan ver las instancias de las que son propietarios.

> ⓘ Nota
>
> Todos los objetos deben cumplir las normas de seguridad de la Plataforma de BI. Para garantizar que los usuarios y grupos solo pueden ver las instancias aplicables, se recomienda establecer los derechos de modo que los usuarios solo vean las instancias de las que son propietarios. Por ejemplo, en un objeto de informe, aplique los derechos de manera que los usuarios solo puedan ver las instancias de las que son propietarios.

### Información relacionada

Administrar derechos de seguridad [página 971]

## 27.14 Importar y promover contenido replicado

En algunos casos, puede optar por importar o promover el contenido replicado de un sistema de la Plataforma de BI a otro. En esta sección se analizan estas funciones de Federación.

> ⓘ Nota
>
> Las migraciones de objetos las realizan mejor los miembros del grupo Administradores; concretamente, la cuenta de usuario Administrador. Para migrar un objeto, es posible que también deban migrarse muchos objetos relacionados. Es posible que no pueda obtener para una cuenta de administrador delegado los derechos de seguridad necesarios para todos los objetos.

### 27.14.1 Importar contenido replicado

Si usa el Administrador de ciclo de vida para importar contenido de un despliegue de la Plataforma de BI a otro, el Administrador de ciclo de vida no importará información específica de la réplica asociada a los objetos replicados que se importan. Ello significa que tras la importación el objeto actúa como si nunca se hubiera replicado. Esto es específico de los objetos replicados en un sitio de destino y se describe en el siguiente escenario.

#### Ejemplo

La Plataforma de BI A es un sitio de destino de un proceso de federación. El Informe A, un informe replicado en el Sistema A, se importa desde el Sistema A a la Plataforma de BI B mediante el Administrador de ciclo de vida.

**Resultado:** cuando el Informe A se copia en la Plataforma de BI B, no contiene información replicada. El Informe A ya no estará marcado con un icono de réplica. Si el objeto estaba en conflicto en la Plataforma de BI A, no lo estará en el Sistema B. Básicamente se trata como un objeto originado desde el Sistema B.

> ⓘ Nota
>
> El CUID puede ser el mismo o no, en función de las opciones de importación seleccionadas en el Administrador de ciclo de vida.

## 27.14.2 Importar contenido replicado y continuar la réplica

Después de haber importado el contenido replicado, puede incluir los objetos importados en un proceso de Federación. Existen dos escenarios: tratar el sistema en el que residen los objetos importados como sitio de origen o tratarlo como sitio de destino. Para tratar este sistema como sitio de origen, continúe con Federación como lo hace normalmente.

Para tratar el sistema como sitio de destino y replicar los objetos importados del sitio de origen, debe:

- Asegurarse de que los CUID de los objetos se conservan al usar LifeCycle Manager.
- Asegurarse de que la primera tarea de réplica tenga la resolución de conflictos establecida en «Tiene preferencia el sitio de origen» o bien «Tiene preferencia el sitio de destino».

> → Sugerencias
>
> En lugar de importar el objeto mediante LifeCycle Manager de un sitio de destino a otro, es más eficaz y recomendable usar únicamente Federación para replicar el objeto.

### Ejemplo

El Informe A se creó en el Sistema A de la Plataforma de BI. El Sistema X usó Federación para replicar el Informe A del Sistema A en el Sistema X. A continuación, el Administrador de ciclo de vida importó el Informe A del Sistema X al Sistema Y.

**Plan:** el Sistema Y quiere configurar Federación en el Sistema A y conservar el Informe A como parte de la réplica. El Sistema Y es el destino y el Sistema A es el origen.

**Acción:** al importar el Informe A del Sistema X al Sistema Y, debe conservarse el CUID del Informe A. Además, cuando se ejecuta la primera tarea de réplica, ésta intentará replicar el Informe A. Puesto que el objeto ya existe en el Sistema Y, la réplica causará un conflicto Para especificar la versión que se utilizará, debe configurar el modo de resolución de conflictos en «Tiene preferencia el sitio de origen» o bien «Tiene preferencia el sitio de destino».

> ⓘ Nota
>
> En este ejemplo, se recomienda que en lugar de importar el objeto mediante LifeCycle Manager de un sitio de destino a otro, se use únicamente Federación para replicar el objeto. El Informe A se replicará desde el Sistema A en el Sistema Y y no es necesario usar LifeCycle Manager para importar del Sistema X al Sistema Y.

## 27.14.3 Promover contenido desde un entorno de prueba

En cualquier organización, con frecuencia se realizan pruebas antes de pasar algo a un entorno de producción. Es normal probar Federación entre sistemas de la Plataforma de BI en un entorno de desarrollo o de prueba antes de configurar Federación en los equipos de producción. Una vez creados los sitios de origen y de destino, así como el contenido en un entorno de prueba, puede promover esta configuración a los equipos de producción con los siguientes pasos:

1. Use LifeCycle Manager para promover el contenido del sitio de origen en el entorno de prueba al equipo de producción que actuará como sitio de origen.

   > **Nota**
   >
   > El objeto de lista de réplicas no se puede seleccionar mientras se usa LifeCycle Manager.

2. Cree la lista de réplicas en el sitio de origen en el entorno de producción e incluya el contenido que desee.
3. Elija entre estas dos opciones:
   - A) Cree un objeto de conexión remota y las tareas de réplica adecuadas en los equipos de producción que actuarán como sitios de destino.
   - B) Use LifeCycle Manager para importar la conexión remota y las tareas de réplica del sitio de destino de Dev/QA a los equipos de producción que actuarán como sitios de destino. A continuación, edite las conexiones remotas importadas para que indiquen el equipo de producción que actuará como sitio de origen.

### 27.14.4 Volver a dirigir un sitio de destino

Actualmente, después de replicar un objeto desde un sitio de origen, se debe replicar siempre desde dicho sitio de origen y no se puede replicar desde otra Plataforma de BI si el objeto de conexión remota se edita para apuntar al nuevo sistema. Cualquier intento de replicar un objeto replicado desde un sistema distinto de la Plataforma de BI que no sea el objeto de conexión, no se podrá replicar. Para replicar un objeto de un sitio de origen distinto, elimínelo primero del sitio de destino.

> **Nota**
>
> Una vez que se copia un objeto replicado, el CUID de la copia cambia y esta no contendrá ninguna información replicada.

## 27.15 Procedimientos recomendados

Puede usar Federación para optimizar el rendimiento de una tarea de réplica.

Si hay un gran número de objetos en una única tarea de réplica, puede realizar unos pasos adicionales para asegurarse de que se ejecuta correctamente. Normalmente, se deben poder replicar hasta 32.000 objetos en cada tarea de réplica. No obstante, es posible que algunos despliegues requieran configuraciones con tamaños de réplica menores o mayores.

**1) Obtener un proveedor de servicios Web dedicado**

En Federación, el contenido replicado se envía usando servicios Web. En una instalación predeterminada de la plataforma de BI, todos los servicios Web usan el mismo proveedor de servicios Web. Las tareas de réplica de mayor tamaño utilizan durante más tiempo el proveedor de servicios Web y ralentizan su respuesta a otras solicitudes de servicio Web así como a cualquiera de las aplicaciones que sirve.

Si tiene pensado replicar un gran número de objetos a la vez, o ejecutar varias tareas de réplica en secuencia, puede considerar la posibilidad de desplegar los servicios Web de Federación en su propio servidor de aplicaciones Java utilizando su propio proveedor de servicios Web.

Para ello, use el instalador de la Plataforma de BI para instalar los servicios Web. Ya debe tener en ejecución un servidor de aplicaciones Java. Si no es así, instale la opción Componentes de nivel Web completa, que instalará los servicios Web y Tomcat.

> **Nota**
>
> Debe proporcionar información para un CMS existente (por ejemplo, el nombre de host, el puerto y la contraseña de administrador).

> **Nota**
>
> Deberá utilizar este nuevo URI del proveedor de servicios Web en el campo URI de conexión remota.

**2) Aumentar la memoria disponible del servidor de aplicaciones Java**

Aumente la memoria disponible del servidor de aplicaciones Java si con una sola tarea de réplica se replican numerosos objetos o si se comparte el servidor de aplicaciones con otras aplicaciones.

Si ha desplegado la plataforma de BI y Tomcat, la memoria disponible es, de forma predeterminada, 1 GB. Para aumentar la memoria disponible para Tomcat:

**En Windows:**

1. Haga clic en *Inicio* > *Programas* > *Tomcat* > *Configuración de Tomcat*.
2. Seleccione *Java*.
3. En el cuadro *Opciones de Java*, busque `-Xmx1024M`
4. Aumente el valor de `-Xmx1024M` al tamaño que desee.

## Ejemplo

Para aumentar la memoria a 2 GB, introduzca: `-Xmx2048M`

**En Unix:**

1. En `<directorio_instalación_BOE>/setup/`, abra `env.sh` con su editor de textos preferido. Aumente el parámetro `-Xmx1024m` al tamaño que desee.
2. Busque las siguientes líneas

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxMetaspaceSize=256m"
 fi
 export JAVA_OPTS
 # fi
```

> **Nota**
>
> En BI 4.2 Support package 5 puede utilizar el parámetro MaxMetaspaceSize para definir tamaño de la memoria metaspace en contraposición al parámetro MaxPermSize.
>
> - Si está actualizando desde versiones anteriroes a BI 4.2 Support package 5 a BI 4.2 Support package, deberá editar manualmente el parámetro para todos los servidores existentes.
> - Si está realizando una instalación por primera vez de BI 4.2 Support Package 5, el parámetro se sustituirá por defecto.

3. Aumente el parámetro `-Xmx1024m` al tamaño que desee.

## Ejemplo

Para aumentar la memoria a 2 GB, introduzca: `-Xmx2048m`

> **→ Sugerencias**
>
> Para otros servidores de aplicaciones Java, consulte su documentación para aumentar la memoria disponible.

**3) Reducir el tamaño de los archivos BIAR que se crean.**

Federación usa servicios Web para replicar contenido entre el sitio de origen y el de destino. Los objetos se agrupan y comprimen archivos BIAR con el fin de obtener un transporte más eficaz.

Al replicar una gran cantidad de objetos, configure el servidor de aplicaciones Java para que cree archivos BIAR de menor tamaño. Federación empaquetará y comprimirá los objetos de varios archivos BIAR de menor tamaño de modo que el número de objetos que desea replicar no estará limitado.

Para reducir el tamaño de los archivos BIAR creados, agregue los siguientes parámetros Java al servidor de aplicaciones Java:

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

`bobj.biar.suggestSplit` sugiere un tamaño adecuado del archivo BIAR, que intentará cumplir. El nuevo valor sugerido es 90 MB.

`bobj.biar.forceSplit` forzará que un archivo BIAR se detenga en un determinado tamaño. El nuevo valor sugerido es 100 MB.

> **Nota**
>
> No necesita cambiar la configuración de tamaño archivo BIAR predeterminada a menos que el servidor de aplicaciones se quede sin memoria y su tamaño de pila máximo ya no se pueda incrementar más.

**Para Tomcat en Windows:**

1. Para abrir la herramienta *Configuración de Tomcat*, haga clic en *Inicio* > *Programas* > *Tomcat* > *Configuración de Tomcat* >.

2. Seleccione *Java*.
3. En el cuadro *Opciones de Java*, agregue las siguientes líneas al final:

```
-Dbobj.biar.suggestSplit=90
-Dbobj.biar.forceSplit=100
```

**Para Tomcat en Unix/Linux:**

1. Abra env.sh con su editor de textos preferido. Se encuentra en `<directorio_instalación_BOE>/setup/`
2. Busque las siguientes líneas:

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ];
then
JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
export JAVA_OPTS
 # fi
```

Agregue los parámetros de tamaño de archivo BIAR que desee.

Ejemplo: `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m` **-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"**

Para otros servidores de aplicaciones Java, consulte su documentación para agregar propiedades del sistema Java.

**4) Aumentar el tiempo de espera de socket.**

El servidor de tareas de Adaptive se encarga de ejecutar la tarea de réplica. Durante la ejecución de la tarea de réplica, el servidor de tareas de Adaptive establece una conexión con el sitio de origen. Al recibir una gran cantidad de información del sitio de origen, es importante que no se agote el tiempo de espera del socket que utiliza el servidor de tareas de Adaptive para recibir información.

El valor predeterminado es 90 minutos. Puede aumentar el tiempo de espera de socket si es necesario.

**Para aumentar el tiempo de espera de socket en el servidor de tareas de Adaptive:**

1. Abra la Consola de administración central (CMC)
2. Desplácese a la sección *Servidor* y seleccione *Servidor de tareas de Adaptive*.
3. Haga clic en *Propiedades*.
4. Agregue «Parámetros de línea de comandos» al final de:
   - **Windows:** `-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<timeout in minutes>`
   - **Unix:** `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<timeout in minutes>`

## Información relacionada

Solución de problemas de mensajes de error [página 1010]
Uso de servicios Web en Federación [página 997]

Limitaciones de la versión actual [página 1009]

## 27.15.1 Limitaciones de la versión actual

Federación es una herramienta flexible. Sin embargo, determinadas limitaciones pueden repercutir en su rendimiento durante la producción. En esta sección se destacan las áreas que puede modificar para optimizar las operaciones de Federación.

- Número máximo de objetos
  Cada tarea de réplica replica objetos entre despliegues de la Plataforma de BI. Se recomienda que el número máximo de objetos que se repliquen en una sola tarea de réplica sea de 100.000. Aunque una tarea de réplica puede funcionar con más de 100.000 objetos, Federación sólo admite la réplica de hasta 100.000 objetos.
- Derechos
  En Federación los derechos sólo se replican desde el sitio de origen al de destino. Se recomienda que los derechos de usuario comunes a ambos despliegues se establezcan en el sitio de origen y se repliquen en los sitios de destino con réplica bidireccional. Los derechos de usuario de un sitio específico se administrarán de la forma habitual en un despliegue de la Plataforma de BI en el sitio donde reside el usuario.
- Vistas empresariales y objetos asociados
  La Plataforma de BI puede almacenar vistas empresariales, elementos empresariales, infraestructuras de datos, conexiones de datos y listas de valores (LOV). Estos objetos se utilizan para mejorar la funcionalidad de Crystal Reports.
  Si estos objetos se crean primero en el sitio de destino y, a continuación, se replican en el sitio de origen con la réplica bidireccional, es posible que no funcionen correctamente y que sus datos no aparezcan en Crystal Reports.
  Se recomienda crear las vistas empresariales, los elementos empresariales, las infraestructuras de datos, las conexiones de datos y las LOV en el sitio de origen y, a continuación, replicarlos en el sitio de destino. Actualice los objetos del sitio de destino o del sitio de origen (si lo permiten los permisos) y los cambios se replicarán entre uno y otro correctamente.
- Sobrecargas de universos
  La Plataforma de BI puede almacenar sobrecargas de universos. Si las sobrecargas de universos se crean primero en el sitio de destino y, a continuación, se replican en el sitio de origen con la réplica bidireccional, es posible que no funcionen correctamente.
  Para resolverlo, primero cree las sobrecargas de universos en el sitio de origen y replíquelas en el sitio de destino. En segundo lugar, establezca seguridad en las sobrecargas de universos en el sitio de origen y replíquelas en el sitio de destino.
- Limpieza de objetos
  Con la limpieza de objetos se eliminan los objetos que se han eliminado en el otro sitio. La limpieza de objetos actualmente sólo se lleva a cabo desde el sitio de origen en el sitio de destino.
- Archivos de registro de Federación
  Los archivos de registro de Federación se escriben en archivos XML que usan estándares XML 1.1. Para ver los archivos de registro con un explorador, éste debe admitir XML 1.1.

## Información relacionada

Administración de la limpieza de objeto [página 990]

# 27.15.2 Solución de problemas de mensajes de error

Esta sección contiene mensajes de error que se pueden presentar en muy contadas ocasiones al usar Federación. Estos mensajes aparecerán en los registros de tareas de réplica o en el área de funcionalidad de un informe.

## 1) GUID no válido

Ejemplo de error: `ERROR 2008-01-10T00:31:08.234Z El GUID ASXOOFyvy0FJnRcD0dZNTZg (encontrado en la propiedad SI_PARENT_CUID en el número de objeto 1285) no es un GUID válido`.

Este error significa que va a replicar un objeto cuyo objeto principal no se replica con él y que no existe en el sitio de destino. Por ejemplo, se replica un objeto, pero no la carpeta que lo contiene. Puede que el objeto principal no se replique porque la cuenta que replica los objetos no disponga de suficientes derechos en el objeto principal.

## 2) Crystal Reports que no muestran datos en el sitio de origen

Este error se puede producir si el informe de Crystal utiliza una vista empresarial, un elemento empresarial, una infraestructura de datos, una conexión de datos o una lista de valores (LOV) que se ha creado originalmente en el sitio de destino y, a continuación, se replica en el sitio de origen.

## 3) Las sobrecargas de universo no se aplican correctamente

Este error se puede producir si el informe utiliza un universo que contiene una sobrecarga de universos que se ha creado en el sitio de destino y se replica al sitio de origen.

## 4) Memoria insuficiente de Java

Ejemplo de error: `java.lang.OutOfMemoryError`.

Se puede producir si el servidor de aplicaciones Java se ha quedado sin memoria al procesar una tarea de réplica. Puede que la tarea de réplica sea demasiado grande o que el servidor de aplicaciones Java no disponga de suficiente memoria.

Incremente la memoria disponible del servidor de aplicaciones Java mediante el traslado de los servicios Web de Federación a un equipo dedicado, o reduzca la cantidad de objetos que se replican en una tarea de réplica.

## 5) Tiempo de espera de socket

Ejemplo de error: `Error communicating with origin site.` (Error al comunicar con el sitio de origen.) `Read timed out.` (Tiempo de espera de lectura agotado.)

La información que se envía desde el sitio de origen al servidor de tareas de Adaptive en el sitio de destino dura más que el tiempo de espera asignado. Aumente el tiempo de espera de socket en el servidor de tareas de Adaptive o reduzca el número de objetos que está replicando en la tarea de réplica.

## 6) Límite de consulta

Ejemplo de error: `SDK error occurred at the destination site.` (Ocurrió un error del SDK en el sitio de destino.) `Not a valid query.` (No es una consulta válida.) `(FWB 00025) …...Query string is larger than query length limit.` (La cadena de consulta es mayor que el límite de longitud de consulta.)

Este error puede aparecer si replica demasiados objetos a la vez y Federación envía una consulta que es demasiado grande como para que el CMS se ocupe de ella. Los objetos del sitio de origen se enviarán al sitio de destino. No obstante, los cambios que se deban enviar al sitio de origen no se enviarán. Los conflictos se resuelven del modo especificado; sin embargo, no se establecerán las marcas de conflicto de resolución manual en el objeto. Los objetos enviados en el sitio de destino seguirán funcionando correctamente.

Para resolver este problema, reduzca el número de objetos que replica en cada tarea de réplica.

## 7) Se agota el tiempo de espera de la tarea de réplica

Ejemplo de error: `No es posible programar el objeto con el intervalo de tiempo especificado`.

Este mensaje puede aparecer si se ha agotado el tiempo de la tarea de réplica mientras se espera que termine otra tarea de réplica. Esto puede suceder si hay varias tareas de réplica que se conectan al mismo sitio de origen simultáneamente. Se intentará volver a ejecutar la tarea de réplica con error en la siguiente hora programada.

Para resolver este problema, programe la tarea de réplica con error en una hora que no esté en conflicto con otras tareas de réplica que se conectan al mismo sitio de origen.

## 8) Límite de réplica

Ejemplo de error: `SDK error occurred at the destination site.` (Ocurrió un error del SDK en el sitio de destino.) `Database access error.` (Error de acceso a la base de datos.) `…. Internal Query Processor Error:` (Error del procesador de consultas interno:) `El procesador de consultas se quedó sin espacio de pila durante la optimización de consultas. Error al ejecutar la consulta en ExecWithDeadlockHandling.`

Este mensaje puede aparecer si ha excedido el número de objetos admitidos que se pueden replicar a la vez. Para resolver este problema, reduzca el número de objetos que replica en la tarea de réplica y ejecútela de nuevo.

## 9) Objeto descartado

Ejemplo de error: `Se encontró un error al comprobar los derechos de seguridad` o `Se encontró un error al empaquetar el objeto`.

Este mensaje puede mostrarse si un objeto se descarta del paquete de réplica. Se puede producir cuando Federación consulta un objeto que necesita réplica pero antes comprueba los derechos y empaqueta el objeto.

## 10) Servidor de procesamiento de Adaptive

Ejemplo de error: `Se ha producido un error en Servidor de procesamiento de Adaptive`.

Este error se puede producir cuando Federación carga demasiadas clases y no hay suficiente memoria para procesar la tarea de réplica.

Para solucionar este problema, debe realizar estos dos pasos:

1. En los argumentos de la línea de comandos del servidor de procesamiento de Adaptive, agregue la siguiente línea: `-javaArgs "XX:MaxMetaspaceSize=256m"`.

   > **Nota**
   >
   > En BI 4.2 Support package 5 puede utilizar el parámetro MaxMetaspaceSize para definir tamaño de la memoria metaspace en contraposición al parámetro MaxPermSize.
   >
   > - Si está actualizando desde versiones anteriroes a BI 4.2 Support package 5 a BI 4.2 Support package, deberá editar manualmente el parámetro para todos los servidores existentes.
   > - Si está realizando una instalación por primera vez de BI 4.2 Support Package 5, el parámetro se sustituirá por defecto.

2. Agregue los siguientes parámetros al servidor de aplicaciones Java al que se conecte para Federación, con el fin de reducir el tamaño de los archivos BIAS que utilice:
   - `-Dbobj.biar.suggestSplit=100m`
   - `-Dbobj.biar.forceSplit=100m`

## 11) Servidores de procesamiento de Adaptive

Se ha añadido un nuevo argumento Java `-XX:MetaspaceSize` a la línea de comandos APS en combinación con el `-XX:MaxMetaspaceSize` existente para mejorar la experiencia de inicialización y evitar la recopilación total de desechos no deseados dentro del proceso de Java relativo a Servidor(es) de procesamiento de Adaptive.

Las pruebas en una MV con recursos mínimos de RAM, un APS por defecto y Todos los servicios, incluidos estos valores para MetaSpace y MaxMetaSpace, parecen permitir que el APS se inicie e inicialice un poco más rápido que la configuración predeterminada. Hay cero "Recopilaciones de desecho totales" notificadas.

Para obtener más información sobre *Ajuste de opciones de servidores de procesamiento para evitar la recopilación de desecho total (GC total) con MetaSpace*, consulte la Nota SAP 3001317.

## 12) Espacio de administrador de objetos

Ejemplo de error: `No se pudo crear el paquete de inserción. Se ha producido una excepción de entrada/salida: "No queda espacio en el dispositivo."`

Esto sucede cuando el directorio temporal que usa Federación no tiene suficiente espacio en disco. Para solucionar este problema, libere espacio adicional en el directorio temporal o use otra ubicación para el directorio temporal.

Para especificar una ubicación distinta para el directorio temporal en el sitio de origen, agregue la siguiente línea a los archivos de configuración del servidor de aplicaciones Java: `-Dbobj.tmp.dir=<TempDir>`.

Para especificar una ubicación distinta para el directorio temporal en el sitio de destino, agregue la siguiente línea a los argumentos de la línea de comandos del Servidor de procesamiento de Adaptive: `-javaArgs «-Dbobj.tmp.dir=<TempDir>»`.

En los ejemplos anteriores, `<DirectorioTemporal>` es la ubicación del directorio temporal que desea utilizar.

## 13) Error de universo

Ejemplo de error: `Error interno ocurrido al llamar la API processDPCommands`

Se produce cuando falta una relación de conexión de universo a universo en un universo que se ha replicado o no válida. Para solucionar este problema, ejecute la tarea de réplica con la opción *Actualizar a partir de origen* seleccionada y compruebe que se replica su conexión de universo.

También puede abrir el universo en Universe Designer, editar la conexión del universo y volver a transferirlo.

## Información relacionada

Procedimientos recomendados [página 1005]

Limitaciones de la versión actual [página 1009]

# 28 Configuración suplementaria para entornos ERP

## 28.1 Configuración para la integración de SAP NetWeaver

### 28.1.1 Integración con SAP Business Warehouse (BW)

#### 28.1.1.1 Información general

En esta sección se muestra cómo configurar BW para habilitar y administrar la publicación de informes desde la aplicación SAP Business Warehouse a la plataforma de BI.

Antes de empezar esta sección, asegúrese de que ha completado la configuración del complemento de autenticación de SAP en la CMC.

**Información relacionada**

Configurar la autenticación SAP [página 338]

##### 28.1.1.1.1 Configuración de carpetas y seguridad en la plataforma de BI

Al definir un sistema de derechos en la plataforma de BI, el sistema crea una estructura de carpetas lógica para que coincida con el sistema SAP. Al importar funciones y publicar contenido en la plataforma de BI, se crean las carpetas correspondientes. Como administrador, no debe crear estas carpetas. Se crean como resultado de la definición de un sistema de derechos al configurar el complemento de autenticación de SAP, al importar funciones en la CMC y al publicar contenido en la plataforma de BI.

> **Nota**
>
> El administrador de la Plataforma de BI es el responsable de asignar los derechos adecuados a dichas carpetas:
>
> - *Carpeta de nivel superior de SAP*
>  Asegúrese de que el grupo Todos tiene acceso limitado a la carpeta de nivel superior de SAP.
> - *Carpetas de ID de sistema*
>  Asigne los derechos siguientes al principal Publicador en la CMC:

> **Nota**
>
> La publicación principal no está disponible hasta que se publique el contenido.

- Agregar objetos a la carpeta
- Ver objetos
- Editar objetos
- Modificar los derechos de los usuarios para los objetos
- Eliminar objetos

> **→ Sugerencias**
>
> Para facilitar la administración de derechos, puede crear un nivel de acceso Publicador personalizado que incluya estos derechos y, luego, otorgar al principal Publicador este nivel de acceso en las carpetas de Id. del sistema relevantes.

### Información relacionada

Uso de niveles de acceso [página 141]
Cómo funcionan los derechos en la Plataforma de BI [página 127]

## 28.1.1.1.2 Descripción de los patrones de seguridad predeterminados de las carpetas

Al publicar contenido en la plataforma de BI desde SAP, la plataforma crea automáticamente la jerarquía de funciones, carpetas e informes restante. El sistema organiza los informes en carpetas denominadas en función del ID del sistema y el número de cliente, y según el nombre de la función.

- El sistema crea carpetas de nivel superior, es decir, las carpetas SAP, 2.0 y de sistema (`<SID>`), al definir un sistema de derechos.
- El sistema crea carpetas Función (importadas como grupos en la plataforma de BI) según sea necesario, cuando se publica una función desde BW.
- El sistema crea una carpeta Contenido para cada función en la que se publica el contenido.
- La seguridad se establece en cada objeto del informe; de esta forma, los usuarios sólo ven los informes que pertenecen a su función.

El administrador es el responsable de asignar los derechos a los miembros de las diferentes funciones. Este módulo de administración de contenidos permite administrar las funciones de publicación de informes desde SAP BW. Puede identificar roles del sistema SAP BW con un sistema determinado de la plataforma de BI, publicar informes y sincronizar informes entre SAP BW y un despliegue de la plataforma de BI.

### Carpetas Contenido

La plataforma de BI importa un grupo para cada función que se agrega al sistema de derechos, tal como se definió en la CMC.

Para garantizar que se conceden los derechos predeterminados adecuados a todos los miembros de una función con contenido, otorgue los derechos apropiados en el puesto de trabajo de administración de contenido para cada sistema de derechos que se haya definido en la plataforma de BI. Para iniciar el Trabajo de administración de contenido, ejecute la transacción /CRYSTAL/RPTADMIN:

1. En el Puesto de trabajo de administración de contenido, expanda *Enterprise system* (Sistema Enterprise) y, a continuación, *Available systems* (Sistemas disponibles).
2. Haga doble clic en el sistema que desee.
3. Haga clic en la ficha *Layout* (Diseño).
4. Defina *Default security policy for reports* (Directiva de seguridad predeterminada para informes) como *View* (Vista).
5. Defina *Default security policy for role folders* (Directiva de seguridad predeterminada para carpetas de función) como *View On Demand* (Vista bajo demanda).
6. Haga clic en *OK*.

Esta configuración se refleja en la plataforma de BI para todas las funciones de contenido. Es decir, funciones en las que se ha publicado contenido. Los miembros de estas funciones ahora podrán ver instancias programadas de los informes publicados en otras funciones, así como actualizar informes publicados en funciones de las que son miembros.

> **Nota**
>
> Se recomienda que mantenga independientes las actividades de las funciones. Por ejemplo, mientras que se puede publicar con la función de administrador, es mejor que solo se publique con los roles de editor. Además, el cometido de las funciones de publicación es tan sólo definir los usuarios que pueden publicar contenido. De esta forma, las funciones de publicación no deben incluir contenido alguno; los publicadores deben publicar en funciones con contenido a las que puedan acceder los miembros de funciones normales.

## 28.1.1.1.3 Programación basada en eventos BW

Ahora puede programar objetos basados en eventos BW en la plataforma de BI. Debe establecer un canal de comunicación de confianza entre el sistema SAP NetWeaver Business Warehouse (BW) y la plataforma de BI para activar la programación basada en eventos BW.

### 28.1.1.1.3.1 Crear y configurar eventos BW

Siga los pasos a continuación para crear un evento BW:

1. Inicie sesión en CMC.
2. Vaya a *Eventos* > *Eventos BW*.

3. Seleccione para crear un evento nuevo.
4. Introduzca el *Nombre de evento* y la *Descripción*.
5. Seleccione *Crear*.
   Acaba de crear un evento BW nuevo.

## 28.1.1.1.3.2 Añadir eventos BW al programar informe

Siga los siguientes pasos para añadir un evento BW al programar informes:

1. En **CMC**, vaya a *Carpetas* y seleccione un informe.
2. En el menú contextual del informe, seleccione *Programar*.
3. En el panel *Navegación* , vaya a *Eventos* > *Eventos BW* >.
4. Seleccione un evento de *Eventos disponibles*.
5. Añádalo a Eventos y espere a utilizar >>.
6. En el panel *Navegación* , vaya a *Frecuencia*.
7. Especifique los parámetros *Ejecutar objeto*, *Cantidad de reintentos permitidos* e *intervalo de reintento en segundos*.
8. Seleccione *Programar*.

   Una vez se haya desencadenado el evento, el status de programación cambiará a **En ejecución** de **Pendiente**.

   > **Nota**
   >
   > El status de programación se mantiene como **Pendiente** si cualquier evento definido en *Eventos a los que esperar* no se desencadena.

## 28.1.1.1.3.3 Integrar la plataforma de BI y el sistema ABAP

Este tema explica cómo activar la programación basada en eventos BW.

Siga los siguientes pasos:

1. Configure HTTPS/SSL para cualquier servidor de aplicación admitido en la plataforma de BI y añada la clave de secreto compartida en `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container\bin`. Consulte el tema Para configurar HTTPS/SSL [página 527] para WACS y Configuración SSL en Tomcat [página 410] para Tomcat.

   > **Nota**
   >
   > Puede remitirse a SAP Product Availability Matrix (PAM) para obtener más información sobre servidores de aplicación compatibles.

2. Exporte el certificado de servidor de plataforma de BI desde un navegador a un sistema local. Puede descargar los certificados desde el navegador Chrome siguiendo los siguientes pasos:
1. Vaya a http://<hostname>:<port_number>/biprws. Para obtener más información acerca del número de puerto específico para cada aplicación, consulte el tema. Configurar la URL básica para servicios Web RESTful [página 540]
2. Abra las herramientas de desarrollador del navegador Chrome pulsando F12.
3. Navegue a la etiqueta *Seguridad* y seleccione *Ver certificado*.
   Aparece el asistente `Certificado` .
4. En el asistente `Certificado` , vaya a la etiqueta *Detalles* y seleccione *Copiar a archivo*.
   Aparece el *Asistente de exportación de certificados*
5. Seleccione *Siguiente*.
6. En la página *Exportar formato de archivo* , seleccione el formato *Base-64 encoded X.509 (.CER)* y luego, *Siguiente*.
7. Especifique un nombre para el archivo de certificado y guárdelo localmente.
3. Descargue el certificado de sAP NetWeaver BW.
1. Inicie SAP NetWeaver BW.
2. Vaya a la transacción *STRUSTSSO2*.
3. Navegue a *Sistema PSE* > *Sujeto* > *Certificado propio* >.
4. Seleccione *Descargar*.
5. Especifique una ruta de archivo y seleccione el formato de archivo como *Base64*.
6. Seleccione .

El certificado de sistema SAP NetWeaver BW se descarga en la ubicación especificada.

4. Importe el certificado de plataforma de BI al sistema SAP NetWeaver BW.
1. Vaya a la transacción *STRUSTSSO2*.
2. Cambie al modo *Editar* .
3. Seleccione la carpeta *SSL client SSL Client (Standard)*.
4. Seleccione *Importar*.
5. Cargue el certificado de sistema SAP NetWeaver BW y seleccione *Añadir a lista de certificados*.
   El certificado se añade a la *lista de certificados*.
6. Guarde la transacción.
5. Importe el certificado de sistema SAP NetWeaver BW a la plataforma de BI. Consulte el paso 12 del tema Para configurar HTTPS/SSL [página 527] para obtener más información sobre cómo importar certificados.
6. Crear un usuario en la plataforma de BI

> **Nota**
>
> Debe asegurarse de que el nombre de usuario en la plataforma de BI sea el mismo que en el sistema SAP NetWeaver BW. Por ejemplo, si el nombre de sistema SAP NetWeaver BW es MySystem, deberá crear un usuario en la plataforma de BI con el nombre MySystem.

7. Crear un destino HTTP en el sistema SAP NetWeaver BW
1. Vaya a la transacción *SM59*.
2. Seleccione *Conexiones HTTP con servidor externo*.
3. Seleccione .

4. En la ventana *Desitno RFC* , cambie a la etiqueta Opciones técnicas e introduzca *Host*, *Puerta*, y *Prefijo de ruta* como `<hostname>`, `<port_number>`, y `/biprws` respectivamente.
5. Cambie a la etiqueta *Inicio de sesión y seguridad* y seleccione *Activo* respecto a *SSL*.
6. Seleccione *DEFAULT SSL Client (Standard)* como el *Certificado SSL*.
7. Seleccione *Guardar*.
8. Seleccione la conexión de test Connection Test para realizar tests con la conexión HTTP. El resultado de test de conexión aparece y muestra el texto de status como Correcto.

> **Nota**
>
> La conexión HTTP entre SAP NetWeaver BW y la plataforma de BI no es posible si no se cumplen las condiciones mencionadas a continuación.
>
> - El sistema BW debería actualizarse para admitir las versiones TLS 1.1 y TLS 1.2.
> - El sistema BW debería admitir los mismos conjuntos de cifrado que se admiten en la plataforma de BI.

9. Cree una cadena de procesos en el sistema SAP NetWeaver BW.
1. Vaya a la transacción *RSPC*.
2. Abra el menú contextual de *Cadenas de procesos* y seleccione *Crear componente de visualización*.
3. En la ventana *Creación de una agrupación* , especifique el *componente de aplicación* y la *descripción explicativa*.
   Se crea un componente SAP NetWeaver BW.
4. En el menú contextual del componente de aplicación, seleccione *Crear cadena de procesos*.
5. Especifique el nombre y la descripción y seleccione .
   Después de especificar el nombre de la nueva cadena de procesos, se abre el diálogo `Insertar proceso de inicio` . Le permite insertar un proceso de inicio para la cadena de procesos.
6. Especifique la *variante de proceso*y *la descripción explicativa*, y luego, .
   Aparece la ventana Actualizar proceso de inicio.
7. Seleccione *Editar condiciones* y luego, *Inmediato* para ejecutar la cadena de procesos inmediatamente.
8. Seleccione *Grabar* en la ventana `Hora de inicio` .
9. Seleccione *Grabar* en la ventana `Actualizar proceso de inicio` .
10. En la ventana `Insertar proceso de inicio` , seleccione .
    Se ha creado la cadena de procesos.
10. Configure el tipo de proceso en la cadena de procesos.
1. Seleccione la cadena de procesos creada después del paso anterior desde la columna *Cadenas de procesos*.
2. Despliegue la carpeta *Cargar proceso y tratamiento posterior* y seleccione *Evento de desencadenador en plataforma de BI SAP BOBJ para intercambio de datos BW*.
   Se abre el diálogo `Insertar evento de desencadenador en plataforma de BI SAP BOBJ para intercambio de datos BW` .
3. En *Insertar evento de desencadenador en plataforma de BI SAP BOBJ para intercambio de datos BW*, seleccione .
4. Introduzca las *Variantes de proceso* y la *Descripción explicativa*.
5. Seleccione .
   Aparece la ventana `Actualización de proceso` .

6. Seleccione respecto a *Destino* para seleccionar un destino.
7. Seleccione respecto a *Evento* para seleccionar un evento.
8. Guarde los cambios.
9. Seleccione en el diálogo `Insertar evento de desencadenador en plataforma de BI SAP BOBJ para intercambio de datos BW`.
   Se ha creado el tipo de proceso.
11. Active la cadena de procesos y ejecútela.

La acción desencadena el evento BW mencionado en el tipo de proceso.

## 28.1.1.2 Configuración del Publicador de BW

La publicación de BW permite publicar informes de Crystal (archivos .rpt) de forma individual o por lotes desde BW a la plataforma de BI.

En Windows puede configurar el Publicador de BW de dos formas:

- Inicie el Publicador de BW mediante un servicio que se encuentre en un equipo que aloje la plataforma de BI. El servicio del Publicador de BW iniciará instancias del Publicador de BW según sea necesario.
- Iniciar el Publicador de BW mediante un gateway de SAP local para crear instancias del Publicador de BW.

Debe seleccionar el método de configuración basado en los requisitos de su sitio, tras considerar las ventajas e inconvenientes de cada configuración. Cuando haya configurado el Publicador de BW en la plataforma de BI, debe configurar la publicación en el puesto de trabajo de administración de contenido.

## 28.1.1.3 Configuración del Publicador de BW como servicio

En esta sección se explica cómo habilitar la publicación de informes de BW en la plataforma de BI mediante el Publicador de BW como servicio.

### 28.1.1.3.1 Distribuir la instalación del Publicador de BW

En esta sección se explica la distribución del servicio Publicador de BW y cómo separar el Publicador de BW de otros componentes de la Plataforma de BI.

Puede equilibrar la carga de publicación de BW si instala los servicios del Publicador de BW en dos equipos independientes del mismo sistema de la Plataforma de BI.

Al instalar el Publicador de BW en los equipos que alojan la plataforma de BI, debe configurarlos de forma que usen el mismo ID de programa, SAP Gateway Host y servicio de Gateway. Después de crear un destino RFC que use este ID de programa, BW equilibra la carga de publicación entre los equipos que alojan la plataforma de BI. Además, si un Publicador de BW deja de estar disponible, BW sigue usando el Publicador de BW restante.

Puede agregar un nivel adicional de redundancia del sistema a cualquier configuración que incluya varios servidores de aplicaciones BW. Configure cada servidor de aplicaciones BW para que ejecuten SAP Gateway. Para cada uno, instale un servicio de Publicador de BW independiente en un equipo que aloje la plataforma de BI. Configure cada servicio de publicación de BW para que utilicen el host de gateway y el servicio de gateway de un servidor de aplicaciones BW independiente. En esta configuración, la publicación desde BW puede continuar aunque falle un Publicador de BW o un servidor de aplicaciones.

Si desea separar el Publicador de BW de los demás componentes de la Plataforma de BI, instale BW con SAP Gateway independiente.

En este caso, debe instalar SAP Gateway local en el mismo equipo que el Publicador de BW. Además, el Publicador de BW necesita tener acceso al SDK de la Plataforma de BI y al motor de impresión de SAP Crystal Reports. Por tanto, si instala el Publicador de BW y SAP Gateway local en un equipo dedicado, también debe instalar el servidor SIA.

## 28.1.1.3.2 Iniciar el Publicador de BW: UNIX

Ejecute la secuencia de comandos del Publicador de BW para crear una o varias instancias del publicador con el fin de atender las solicitudes de publicación. Se recomienda que inicie una instancia del publicador.

Una vez iniciado el Publicador de BW, se establece una conexión con el servicio SAP Gateway que se especificó al ejecutar el programa de instalación de la plataforma de BI.

## 28.1.1.3.3 Iniciar el Publicador de BW: Windows

En Windows, use el Administrador de configuración central™ (CCM, Central Configuration Manager) para iniciar el servicio de publicación de BW. Al iniciar este servicio, se crea una instancia del publicador para atender las solicitudes de publicación del sistema BW. Si incrementa el volumen de solicitudes de publicación, el Publicador de BW automáticamente genera publicadores adicionales para satisfacer la demanda.

## 28.1.1.3.4 Configurar un destino para el Servicio de publicación de BW

Para habilitar el Publicador de BW, debe configurar un destino RFC en el servidor BW para que se comunique con el Servicio del publicador de BW. Si tiene un clúster de BW, configure el destino RFC en cada servidor, mediante la instancia central de BW como Host de gateway en cada caso.

Si desea publicar en varios despliegues de la plataforma de BI desde BW, cree un destino RFC independiente para el servicio del Publicador de BW en cada despliegue de la plataforma de BI. Debe usar Id. de programa exclusivos para cada destino, pero los mismos host y servicio de gateway.

### 28.1.1.3.5 Configuración del Publicador de BW con un gateway de SAP local

> **Nota**
>
> No use esta configuración si la plataforma de BI está instalada en UNIX. Si se utiliza este método en UNIX podría producirse un comportamiento impredecible del sistema.

Para habilitar la publicación de informes desde BW a la plataforma de BI, mediante usando un Gateway de SAP local, siga este procedimiento:

- Instalación de un gateway de SAP local [página 1023].
- Configuración de un destino para el Publicador de BW [página 1023].

### 28.1.1.3.6 Instalación de un gateway de SAP local

Debe instalar un gateway de SAP local en el equipo donde instaló el Publicador de BW. Se recomienda que un administrador de SAP BASIS realice la instalación de uno de estos gateways de SAP.

Para obtener instrucciones actualizadas de instalación de un gateway de SAP local, consulte las instrucciones de instalación de SAP incluidas en el CD de presentación del producto.

Para obtener una lista detallada de entornos comprobados, consulte la Matriz de disponibilidad de productos (PAM) en http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540. La PAM incluye los requisitos específicos de versión y Service Pack para los servidores de aplicaciones, los sistemas operativos, los componentes SAP, etc.

Una vez instalado el gateway de SAP, use `regedit` para verificar las entradas del registro `TMP` y `TEMP` bajo la clave secundaria `HKEY_CURRENT_USER\Environment`. Ambas entradas del registro deben contener el mismo valor de cadena, que debe ser una ruta de acceso absoluta válida al directorio. Si el valor de cualquiera de las entradas contiene la variable `%USERPROFILE%`, reemplácela por una ruta de acceso absoluta al directorio. Normalmente, el valor de ambas entradas del Registro está establecido en `C:\WINDOWS\TEMP`

### 28.1.1.4 Configuración de un destino para el Publicador de BW

Para habilitar el Publicador de BW, debe configurar un destino RFC para proporcionar a BW la ubicación del equipo en la que ha instalado el gateway de SAP local y el Publicador de BW.

### 28.1.1.5 Configuración de publicación en el Puesto de trabajo de administración de contenido

Este módulo de administración de contenidos permite administrar las funciones de publicación de informes desde SAP BW. Puede identificar roles del sistema SAP BW con un sistema determinado de la plataforma de

BI, publicar informes y sincronizar informes entre SAP BW y un despliegue de la plataforma de BI. Cuando haya configurado la autenticación SAP y el Publicador de BW Publisher, lleve a cabo las funciones descritas en esta sección para habilitar la publicación. Estas instrucciones le permitirán:

- Establecer las autorizaciones indicadas para los distintos usuarios del Puesto de trabajo de administración de contenido.
- Configurar las conexiones a la plataforma de BI en la que se publica contenido.
- Definir las funciones que se pueden publicar en cada plataforma de BI.
- Publicar el contenido desde BW a la plataforma de BI.

### 28.1.1.6 Usuarios que pueden acceder al Puesto de trabajo de administración de contenido

Existen tres tipos de usuarios que pueden tener acceso al Puesto de trabajo de administración de contenido:

- Consumidores de contenido: pertenecen a las funciones relacionadas con contenido y pueden ver los informes. Ellos no tienen autorización para hacer otra cosa que no sea ver informes.
- Publicadores de contenido de la Plataforma de BI: pueden ver, publicar, modificar y, opcionalmente, eliminar informes desde BW.
- Administradores de la Plataforma de BI: pueden realizar todas las tareas en el Puesto de trabajo de administración de contenido. Estas tareas incluyen la definición de los sistemas de la Plataforma de BI, la publicación y el mantenimiento de informes.

### 28.1.1.7 Creación de funciones en BW para los publicadores de contenido designados

Al configurar BW para su integración con la plataforma de BI, valore si la estructura de funciones actual le permite designar rápidamente usuarios concretos de BW como publicadores de contenido o administradores del sistema para los sistemas de la plataforma de BI.

Es conveniente etiquetar de forma descriptiva las nuevas funciones que se creen. Como ejemplos de nombres de funciones descriptivos podríamos tener `PUBLICADORES_DE_CONTENIDO_DE_BOE` y `ADMINISTRADORES_DEL_SISTEMA_DE_SBOP`.

> → Sugerencias
>
> Puede asignar a un usuario administrativo derechos totales de administración del sistema o un subconjunto de dichos derechos.

Para modificar los derechos de estas nuevas funciones (o de cualquier función existente) que se conceden en la plataforma de BI, en primer lugar debe configurar la autenticación SAP e importar las funciones. Después puede modificar los derechos de cada función importada mediante la Consola de administración central.

Para obtener información detallada sobre la creación de funciones, consulte la documentación de SAP. Para obtener más información sobre el uso de las funciones en la administración de contenido, consulte las siguientes secciones:

- Importación de funciones de SAP [página 346].
- Configuración de carpetas y seguridad en la plataforma de BI [página 1015].
- Descripción de los patrones de seguridad predeterminados de las carpetas [página 1016].

### 28.1.1.8 Configuración de acceso al Puesto de trabajo de administración de contenido

Para cada tipo de usuario que tenga acceso al Puesto de trabajo de administración de contenido, deberá aplicar el conjunto de autorizaciones apropiado dentro de BW. Las autorizaciones se enumeran en las siguientes tablas.

Autorizaciones para usuarios administrativos

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| S_TCODE | RFC_NAME | /CRYSTAL/CE_SYNCH, SH3A, SUNI |
| | ACTVT | Ejecutar (16) |
| | TCD | /CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH |
| S_TABU_CLI | CLIIDMAINT | X |
| S_TABU_DIS | ACTVT | Cambiar, mostrar (02, 03) |
| | DICBERCLS | &NC& |
| | JOBACTION | DELE, RELE |
| | JOBGROUP | ' ' |
| S_RS_ADMWB | ACTVT | Ejecutar (16) |
| | RSADMWBOBJ | WORKBENCH |
| | ACTVT | Crear, cambiar, mostrar, eliminar (01, 02, 03, 06) |
| ZCNTADMJOB | ACTVT | Crear, eliminar (01, 06) |
| ZCNTADMRPT | ACTVT | Mostrar, eliminar, activar, mantener, comprobar (03, 06, 07, 23, 39) |

Autorizaciones para los publicadores de contenido

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | /CRYSTAL/CE_SYNCH, SH3A, SUNI |
| | ACTVT | Ejecutar (16) |
| | TCD | /CRYSTAL/RPTADMIN |
| S_BTCH_JOB | JOBACTION | DELE, RELE |
| | JOBGROUP | ' ' |
| | ACTVT | Ejecutar (16) |
| | RSADMWBOBJ | WORKBENCH |
| ZCNTADMCES | ACTVT | Mostrar (03) |
| ZCNTADMJOB | ACTVT | Crear, eliminar (01, 06) |
| ZCNTADMRPT | ACTVT | Mostrar, activar, mantener, comprobar (03, 07, 23, 39)<br>Eliminar (opcional) (06)<br>Editar (opcional) (02) |

Conceder a los publicadores de contenido el derecho a eliminar informes en el Puesto de trabajo de administración de contenido de BW es opcional. Sin embargo, tenga en cuenta que si se elimina un informe en BW, también se elimina en la plataforma de BI. Si los publicadores no disponen de derechos suficientes para eliminar informes en la plataforma, se produce un error.

## Autorizaciones para los consumidores de contenido

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SH3A, SUNI |
| | ACTVT | Ejecutar (16) |
| | TCD | /CRYSTAL/RPTADMIN |
| S_RS_ADMWB | ACTVT | Ejecutar (16) |
| | RSADMWBOBJ | WORKBENCH |

| Objeto de autorización | Campo | Valores |
|---|---|---|
| | ACTVT | Mostrar (03) |

## 28.1.1.9 Definir un sistema de la Plataforma de BI

Debe crear una definición de sistema en el puesto de trabajo de administración de contenido para cada sistema de la Plataforma de BI en el que desee publicar informes.

### 28.1.1.9.1 Agregar un sistema de la Plataforma de BI

1. Ejecute la transacción `/crystal/rptadmin` para acceder al Puesto de trabajo de administración de contenido.
2. En el panel *Operaciones*, seleccione *Sistema Enterprise*.
3. Haga doble clic en *Agregar nuevo sistema*.
4. En la ficha *Sistema*:
   - Escriba un nombre descriptivo en el campo *Alias*. Evite utilizar espacios o caracteres especiales, puesto que estos caracteres necesitan un tratamiento especial cuando se usa el nombre del alias al configurar portales Enterprise Portal.
   - Escriba el nombre del equipo donde se ejecuta el CMS. Si ha configurado el CMS para que utilice un puerto distinto del predeterminado, escriba **`CMSNAME:PORT`**.
   - Seleccione *Sistema predeterminado* si desea publicar informes en este sistema desde cualquier función que no se haya asignado explícitamente a ningún sistema de la Plataforma de BI. Solo un sistema de la Plataforma de BI puede ser el predeterminado.
     En la lista de todos los sistemas disponibles, el sistema predeterminado tiene una marca de verificación verde.
5. Haga clic en *Guardar*.
6. En la ficha *Destinos RFC*, agregue cada uno de los destinos RFC asociados a este sistema.

   Para agregar un destino, haga clic en el botón *Insertar fila*. En la lista que aparece, haga doble clic en el nombre del destino RFC.

   > **Nota**
   >
   > Un sistema de la Plataforma de BI tener varios destinos para agregar redundancia del sistema. Consulte «Distribuir la instalación del Publicador de BW».

7. Seleccione la casilla de verificación junto al nombre de destino que ha agregado, y haga clic en *Verificar definición BOE*.

   Esta prueba comprueba que BW puede ponerse en contacto con la publicación de BW especificado y que puede iniciar sesión en este sistema con la cuenta de usuario de derechos de Crystal.
8. En la ficha *HTTP*:

- En el campo *Protocolo*, escriba **`http`** o **`https`**, en caso de que el servidor Web conectado a la plataforma de BI esté configurado para HTTPS.
- En el campo *Host y puerto de servidor Web*, escriba el nombre de dominio o dirección IP completos del servidor Web que aloja la plataforma de lanzamiento de BI. Para una instalación que usa un servidor de aplicaciones Java, incluya el número de puerto. Por ejemplo, escriba **`boserver01.businessobjects.com:8080`**.
- En el campo *Ruta*, escriba **`SAP`**
  Esta ruta es, básicamente, la ruta virtual que usa el servidor web al hacer referencia a la subcarpeta `sap` del contenido web de la plataforma de BI. Proporcione un valor alternativo solo si ha personalizado el entorno Web y la ubicación de los archivos de contenido Web de la plataforma. No incluya una barra inclinada al comienzo ni al final de esta entrada.
- En el campo *Aplicación de visor*, escriba el nombre de la aplicación del visor.
  Para usar el visor de la plataforma de BI predeterminado que utiliza la versión Java de la plataforma de lanzamiento de BI, escriba **`openDocument.jsp`**
  Si se instaló la plataforma de BI en Windows usando la configuración predeterminada `ASP.NET`, para usar el explorador predeterminado, escriba **`report/report_view.aspx`**

9. En la ficha *Idiomas*, seleccione los idiomas de los informes que se publicarán en este sistema.
10. En la ficha *Funciones*, agregue las funciones con contenido que desee asociar a este sistema de la plataforma de BI.

    Consulte «Importar funciones SAP».
11. Haga clic en el botón *Insertar fila*.

    Aparece una lista de las funciones disponibles para agregar a este sistema.

    > **Nota**
    >
    > Cada función se puede publicar solo en un sistema de la plataforma de BI. Si las funciones que desea agregar a este sistema de la plataforma de BI no aparecen en la lista, haga clic en *Cancelar* para volver a la ficha *Funciones* y haga clic en *Reasignar funciones*.
12. Seleccione las funciones que desea publicar en este sistema y haga clic en *Aceptar*.
13. En la ficha *Diseño*, seleccione la configuración de seguridad predeterminada para las carpetas de funciones e informes publicadas en este sistema de la plataforma de BI.

    > **Nota**
    >
    > Automáticamente se crea una carpeta en la plataforma de BI para cada función publicada en dicho sistema. Esta carpeta contiene los accesos directos a los informes publicados en esa función.

    > **Nota**
    >
    > Una vez configurado un sistema de la Plataforma de BI, si cambia los niveles de seguridad predeterminados aquí, no afectará a los niveles de seguridad de las carpetas de funciones publicadas ni de los informes. Para cambiar los niveles de seguridad predeterminados de todas las funciones y el contenido publicado en la plataforma, elimine las carpetas de funciones y los accesos directos en el sistema. (De esta forma, no se eliminarán los informes reales.) Cambie la configuración de seguridad aquí y vuelva a publicar las funciones y los informes.
14. Haga clic en *Aceptar* en la parte inferior para guardar la configuración y crear el sistema de la plataforma de BI en el puesto de trabajo de administración de contenido.

Ahora puede publicar informes en la plataforma de BI desde BW.

## Información relacionada

Distribuir la instalación del Publicador de BW [página 1021]
Importación de funciones de SAP [página 346]

## 28.1.1.10 Publicación de informes mediante el Puesto de trabajo de administración de contenido

Después de haber guardado un informe en BW, puede publicarlo utilizando el Puesto de trabajo de administración de contenido. Puede usar este Puesto de trabajo para publicar informes independientes o puede publicar todos los informes guardados en una función concreta. Sólo un usuario que tenga autorizaciones adecuadas en un editor de contenido de Crystal (consulte Crear y aplicar autorizaciones [página 1044]) puede usar el Puesto de trabajo de administración de contenido para publicar y mantener informes.

## 28.1.1.11 Publicación de funciones o informes

1. Ejecute la transacción `/crystal/rptadmin` para acceder al Puesto de trabajo de administración de contenido.
2. En el panel *Operaciones*, seleccione *Publicar informes*.
3. Para buscar contenido guardado en el sistema BW, haga doble clic en *Seleccionar informes y funciones para publicar*.
   Aparece un cuadro de diálogo diseñado para ayudarle a filtrar las funciones y los informes disponibles.
4. Desde la lista, seleccione los sistemas con contenido que desee mostrar.

   > **Nota**
   >
   > La lista contiene todos los sistemas disponibles definidos en este sistema BW.

5. Después, filtre los resultados para limitar el número de informes y funciones que se mostrarán. Utilice estas opciones:
   - *Versión del objeto*
     Si selecciona "A: activo", se muestran todos los informes que se pueden publicar. Si selecciona la opción en blanco, se muestran todos los informes. (Las opciones restantes son términos reservados de SAP.)
   - *Estado del objeto*
     Seleccione "ACT Activo, ejecutable" para mostrar solo los informes publicados. Seleccione "INA Inactivo, no ejecutable" para mostrar solo los informes que no se han publicado. Deje el campo en blanco para que se muestren todos los informes. (Las opciones restantes son términos reservados de SAP.)
   - *Filtro de la función*
     Si escribe texto en este cuadro, solo se mostrarán las funciones que coincidan con lo escrito aquí. Use el símbolo * como carácter comodín. Por ejemplo, para mostrar todas las funciones que empiecen con la letra d, escriba "d*".

- *Descripción del informe*
  Si escribe texto en este cuadro, solo se mostrarán las funciones que coincidan con las descripciones escritas aquí. Use el símbolo * como carácter comodín para que coincida con cualquier número de caracteres. Use el símbolo + como carácter comodín para que coincida con 0 o 1 carácter. Por ejemplo, para mostrar todos los informes cuya descripción contenga la palabra ingresos, escriba *ingreso*.

6. Haga clic en *Aceptar*.
   La lista de informes que coincidan con los criterios aparece en el panel de la derecha.
   Los informes se ordenan en una jerarquía: plataforma del sistema BI > Funciones en ese sistema > Informes guardados en la función.
   Cada elemento de la jerarquía se etiqueta con un punto rojo, amarillo o verde. Los elementos más altos de la jerarquía reflejan el estado de los elementos que contienen, con la condición menos favorable filtrada en la parte superior de la jerarquía. Por ejemplo, si un informe de una función es amarillo (activo), pero el resto de los informes son verdes (publicados), la función se muestra en color amarillo (activo).
   - Verde: el elemento está completamente publicado. Si el elemento es un sistema de la Plataforma de BI o una función, se publican todos los informes de ese elemento.
   - Amarillo: el elemento está activo, pero no publicado. Si el elemento es un informe, está disponible para su publicación. Si el elemento es una función o un sistema de la Plataforma de BI, todo el contenido estará activo y al menos un elemento que contiene la función o el sistema no se habrá publicado.
   - Rojo: el elemento corresponde a contenido de SAP y no está disponible para su publicación mediante el Puesto de trabajo de administración de contenido. El contenido no estará disponible para su publicación hasta que se haya activado mediante el Puesto de trabajo de administración de contenido de BW.
7. Seleccione los informes que desee publicar.
   Para publicar todos los informes de una función, selecciónela. Para publicar todas las funciones de un sistema de la Plataforma de BI, selecciónelo.

   > **Nota**
   >
   > Al seleccionar una función (o un sistema), se seleccionan todos los informes contenidos en esa función (o sistema). Para borrar esta selección, desactive la casilla de verificación de la función (o sistema) y haga clic en Actualizar.

8. Haga clic en *Publicar*.

   > **Nota**
   >
   > Los informes publicados en el fondo se procesan a medida que se liberan recursos del sistema. Para usar esta opción, haga clic en *En el fondo* en vez de en *Publicar*.

9. Haga clic en *Actualizar* para actualizar la presentación del estado de los sistemas de la Plataforma de BI, las funciones y los informes del puesto de trabajo de administración de contenido.

   > **→ Sugerencias**
   >
   > Para ver un informe, haga clic con el botón derecho en el informe y seleccione *Ver*. Para ver las consultas usadas por el informe, haga clic con el botón derecho en el informe y seleccione *Consultas utilizadas*.

> **Nota**
>
> Si desea sobrescribir un informe después de publicarlo en la plataforma de BI, haga clic en *Sobrescribir*.

### Información relacionada

Programación de publicaciones en el fondo [página 1031]

## 28.1.1.12 Programación de publicaciones en el fondo

La publicación de informes en el fondo, ya sea inmediatamente o como trabajo programado, conserva los recursos del sistema. Se recomienda que se publiquen los informes en el fondo para mejorar la respuesta del sistema.

La publicación de informes periódica, como trabajos programados, sincroniza la información del informe entre BW y el despliegue de la plataforma de BI. Se recomienda que programe todos los informes (o las funciones que los contengan). También puede sincronizar manualmente las funciones y los informes mediante la opción de estado de actualización de la operación Mantenimiento del informe. Consulte Actualización del estado de los informes [página 1031] para obtener más detalles.

## 28.1.1.13 Actualización de la información del sistema para los informes publicados

El Publicador de BW utiliza la información del sistema SAP especificada aquí para actualizar el origen de datos de los informes publicados. Si prefiere una configuración de equilibrio de carga, puede elegir el uso del servidor de aplicaciones de BW local o la instancia de BW central.

## 28.1.1.14 Mantenimiento de informes

Las tareas de mantenimiento de informes incluyen información de sincronización sobre informes entre la plataforma de BI y BW (Actualizar estado), la eliminación de informes no deseados (Eliminar informes) y la actualización de informes migrados de versiones anteriores de la plataforma (Posterior a la migración).

### 28.1.1.14.1 Actualización del estado de los informes

Si realiza un cambio en un informe publicado en un sistema de la plataforma de BI (como cambiar la función en la que se publica un informe), el cambio no se refleja en BW hasta que sincronice la plataforma de BI y BW.

Puede programar una tarea de publicación para sincronizar periódicamente la plataforma de BI y BW (consulte Programación de publicaciones en el fondo [página 1031] ) o puede actualizar manualmente el estado del informe mediante la herramienta de mantenimiento de informes.

#### 28.1.1.14.2 Eliminar informes

Si se elimina un informe publicado desde BW mediante el puesto de trabajo de administración de contenido, también se elimina en la plataforma de BI. Solo los usuarios con las autorizaciones necesarias para eliminar informes en BW y en el sistema de la Plataforma de BI pueden eliminar informes.

> **Nota**
>
> Si un usuario tiene derechos para eliminar un informe en BW, pero no los tiene en el sistema de la Plataforma de BI en el que está publicado el informe, se puede originar un error.

### 28.1.1.15 Configuración del identificador de solicitud http de SAP

Para habilitar la presentación de informes en BW, debe configurar BW para que use el identificador de solicitud http incluido como parte del Puesto de trabajo de administración de contenido. A continuación, cuando un usuario de BW abre un informe de Crystal desde SAPGUI, BW puede redirigir la solicitud de vista a través de Internet adecuadamente.

Utilice la transacción SICF para acceder a la lista de host virtuales y servicios activos del sistema de BW. Cree un nuevo nodo denominado `ce_url` en BW en la jerarquía `default_host` y agregue `/CRYSTAL/CL_BW_HTTP_HANDLER` a la lista de indentificadores. Quizá deba activar este servicio manualmente después de crearlo.

### 28.1.1.16 Configuración para procesar datos de SAP

#### 28.1.1.16.1 Procesar informes programados en modo por lotes de SAP

Para las instalaciones de Windows, se pueden ejecutar informes programados en la plataforma de BI mediante el modo por lotes de SAP. Los controladores InfoSet y Open SQL pueden ejecutar informes utilizando el modo por lotes o en segundo plano de SAP cuando las variables de entorno específicas se configuran como 1. Las variables de entorno correspondientes son:

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE` (para el controlador InfoSet)
- `CRYSTAL_OPENSQL_FORCE_BATCH_MODE` (para el controlador Open SQL)

Sin embargo, se recomienda usar esta función solo cuando se dispone de una instalación distribuida de la plataforma de BI. Cuando estas variables de entorno se configuran en 1, los controladores ejecutan informes

con el modo por lotes de SAP, independientemente del componente de generación de informes que ejecute el informe. Por tanto, si crea estas variables de entorno como variables de entorno del sistema en un equipo que ejecute una combinación de servidores de la Plataforma de BI, los controladores ejecutarán todos los informes en modo por lotes (incluidas las solicitudes de informes a petición desde el servidor de procesamientos de Crystal Reports y el servidor de aplicaciones de informes).

Para garantizar que los controladores solo ejecutan los informes programados en modo por lotes (informes ejecutados por el Servidor de tareas de Adaptive), evite configurar las variables de entorno de sistema en equipos que ejecuten combinaciones de servidores de la plataforma de BI. En su lugar, siga estos pasos para personalizar las variables de entorno para cada Servidor de tareas de Adaptive.

> **Nota**
>
> Los usuarios de SAP que programan informes en la plataforma de BI pueden necesitar autorizaciones adicionales en SAP.

### Información relacionada

Programar un informe en modo por lotes usando una consulta Open SQL [página 1059]

## 28.1.1.16.2 Para procesar informes programados en modo por lotes de SAP

1. Cree una secuencia de comandos por lotes (archivo `.bat`) en un editor de texto como Bloc de notas, con el siguiente contenido:

   ```
   @echo off
   set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
   set CRYSTAL_OPENSQL_FORCE_BATCH_MODE=1
   %*
   ```

   Esta secuencia de comandos establece las variables de entorno como 1 y, a continuación, ejecuta los parámetros enviados a la secuencia de comandos desde la línea de comandos.
2. Guarde el archivo como `jobserver_batchmode.bat` en una carpeta en cada equipo del Servidor de tareas de Adaptive.
3. Inicie sesión en la Consola de administración central (CMC).
4. Seleccione *Servidores*.
5. Expanda el nodo *Categorías de servicio* y elija *Analysis Services*.
6. Seleccione el *Servidor de procesamiento de Adaptive* y elija *Propiedades* en el menú contextual. Aparecerá la página *Propiedades*.
7. En la página *Propiedades*, busque el campo *Parámetros de línea de comandos*.

   Este es el comando de inicio del Servidor de tareas de Adaptive. Por ejemplo:

   ```
   "\\SERVER01\C$\Archivos de programa\SAO Business Objects\SAP BusinessObjects
   Enterprise\win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01
   -objectType BusinessObjects Enterprise.Report -lib procReport -restart
   ```

8. Indique antes del comando predeterminado la ruta de acceso completa al archivo `jobserver_batchmode.bat` guardado en el equipo del Servidor de tareas de Adaptive.

   En este ejemplo, el archivo por lotes se encuentra en un equipo de nombre SERVER01 como:

   ```
   C:\Crystal Scripts\jobserver_batchmode.bat
   ```

   El nuevo comando de inicio del Servidor de tareas de Adaptive es:

   ```
   "\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$
   \Program Files\SAP Business Objects\SAP
   BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe" -service -name
   SERVER01.report  -ns SERVER01
   -objectType BusinessObjects Enterprise.Report -lib procReport  -restart
   ```

   Este nuevo comando de inicio inicia en primer lugar el archivo por lotes. A su vez, el archivo por lotes establece las variables de entorno necesarias antes de ejecutar el comando de inicio original del Servidor de tareas de Adaptive. De esta forma se garantiza que las variables de entorno disponibles para el Servidor de tareas de Adaptive son distintas de las variables de entorno disponibles para los servidores responsables de los informes a petición (el servidor de procesamiento de Crystal Reports y el servidor de aplicaciones de informes).
9. Haga clic en *Guardar y cerrar*.
10. Haga clic con el botón derecho en el Servidor de tareas de Adaptive y seleccione *Iniciar* en el menú contextual.

   > **Nota**
   >
   > Si el Servidor de tareas de Adaptive no se inicia, compruebe el nuevo comando de inicio.

## 28.1.1.17 Configurar para los transportes de SAP

### 28.1.1.17.1 Información general

La plataforma de BI incluye estos transportes:

- Transporte de conectividad Open SQL
- Transporte de conectividad de InfoSet
- Transporte de definición de seguridad de filas
- Transporte de definición de clúster
- Transporte del Puesto de trabajo de administración de contenido
- Transporte de personalización de parámetros de consultas BW
- Transporte MDX
- Transporte ODS

Existen dos conjuntos diferentes de transportes: transportes compatibles con Unicode y transportes ANSI. Si ejecuta un sistema BASIS 6.20 o posterior, utilice los transportes compatibles con Unicode. Si ejecuta un sistema BASIS anterior a la versión 6.20, utilice los transportes ANSI. Todos los transportes instalados se encuentran en el siguiente directorio del medio de distribución del producto: `\Collaterals\Add-Ons\SAP\Transports\`.

> **Nota**
>
> Cuando realice la comprobación de búsqueda de posibles conflictos de instalación, asegúrese de que no existe ninguno de estos nombres de objeto en el sistema SAP. Los objetos usan un espacio de nombre `/crystal/` de forma predeterminada, de modo que no es necesario que cree el espacio de nombre. Si crea el espacio de nombres `/crystal/` manualmente, se solicitarán las claves de reparación de licencia a las que no tiene acceso.

## 28.1.1.17.2 Configurar transportes

Para configurar los componentes Acceso a datos o Publicador de BW de la plataforma de BI, debe importar los transportes adecuados en el sistema de SAP. Estos componentes usan el contenido de estos archivos de transporte al comunicarse con el sistema de SAP.

Los procedimientos de instalación y configuración que precisa el sistema SAP debe efectuarlos un experto en BASIS familiarizado con el sistema de cambio y transporte y que disponga de derechos de administración en el sistema SAP. El procedimiento exacto de importación de archivos de transporte varía en función de la versión de BASIS que se ejecute. Para obtener detalles específicos sobre el procedimiento, consulte su documentación de SAP.

Cuando implementa el componente de acceso a datos por primera vez, de forma predeterminada todos los usuarios pueden acceder a las tablas de SAP. Para determinar los datos de SAP a los que pueden acceder los usuarios, use el Editor de definición de seguridad.

Después de importar los transportes, debe configurar los niveles adecuados de acceso del usuario. Cree las autorizaciones necesarias y aplíquelas por medio de perfiles o funciones a los usuarios de SAP que diseñarán, ejecutarán o programarán informes de Crystal.

### Información relacionada

Crear y aplicar autorizaciones [página 1044]

## 28.1.1.17.2.1 Tipos de transportes

Existen dos conjuntos diferentes de transportes: transportes compatibles con Unicode y transportes ANSI. Si ejecuta un sistema BASIS 6.20 o posterior, utilice los transportes compatibles con Unicode. Si ejecuta un sistema BASIS anterior a la versión 6.20, utilice los transportes ANSI. Todos los transportes instalados se encuentran en el siguiente directorio de distribución del producto: `\Collaterals\Add-Ons\SAP\Transports\`. El archivo `transports.txt` enumera los archivos de transporte Unicode compatibles y ANSI.

A continuación se describen los tipos de transporte:

- Transporte de conectividad Open SQL

El transporte de conectividad Open SQL permite que el controlador Open SQL se conecte al sistema SAP y elabore informes en él.

- Transporte de definición de seguridad de filas
  Este transporte proporciona el Editor de definición de seguridad, una herramienta que actúa como interfaz gráfica con las tablas /crystal/auth en el transporte de conectividad Open SQL.
- Transporte de definición de clúster
  Este transporte proporciona la herramienta de definición de clústeres. Permite crear un repositorio de metadatos para las definiciones de clúster de datos ABAP. Estas definiciones proporcionan al controlador Open SQL la información que precisa para elaborar informes con estos clústeres de datos.

  > **Nota**
  >
  > Los clústeres de datos ABAP no son lo mismo que las tablas de clústeres. Estas tablas ya se encuentran definidas en DDIC.

- Transporte de conectividad de InfoSet
  Este transporte permite al controlador InfoSet acceder a los InfoSets y consultas de SAP.
- Transporte del Puesto de trabajo de administración de contenido
  Este transporte proporciona la funcionalidad de administración de contenido a los sistemas BW. Sólo está disponible como transporte compatible con UNICODE.
- Transporte de personalización de parámetros de consultas BW
  Este transporte proporciona soporte para los valores de parámetros personalizados y predeterminados de informes basados en consultas BW.
- Transporte de conectividad BW MDX
  Este transporte permite que el controlador MDX Query tenga acceso a cubos y consultas BW. Este transporte es compatible con BW 3.0B parche 27 o posterior y BW 3.1C parche 21 o posterior.
- Transporte de conectividad ODS
  Este transporte permite que el controlador ODS Query tenga acceso a los datos ODS. Este transporte es compatible con BW 3.0B parche 27 o posterior y BW 3.1C parche 21 o posterior.

## 28.1.1.17.2.2 Comprobar la existencia de conflictos

El contenido de los archivos de transporte se registra automáticamente en el espacio de nombres de SAP BusinessObjects al importar los archivos. El espacio de nombres de SAP BusinessObjects se reserva para esta finalidad en las últimas versiones de R/3 y MYSAP ERP. Sin embargo, los nombres de algunos objetos como los objetos de autorización, las clases de autorización y los objetos heredados puede que no contengan los prefijos apropiados. Antes de importar los archivos de transporte se recomienda que compruebe estos tipos de objetos por si existen conflictos.

Si el grupo de funciones, alguno de los módulos de funciones o cualquier otro objeto ya existen en el sistema de SAP, debe resolver el espacio de nombres antes de importar los archivos de transporte de SAP BusinessObjects. Consulte la documentación de la plataforma SAP NetWeaver para conocer los procedimientos apropiados para su versión de SAP.

## 28.1.1.17.2.3 Importar los archivos de transporte

Consulte el archivo `transports_EN.txt` que se encuentra en el siguiente directorio del medio de distribución del producto: `\Collaterals\Add-Ons\SAP\Transports\` . Este archivo de texto indica los nombres exactos de los archivos que constituyen cada transporte. (Los directorios `cofiles` y `data` incluidos en el directorio `transports` corresponden a los directorios .../`trans/cofiles` y .../`trans/data` del servidor SAP.)

Debe importar el transporte de conectividad Open SQL antes de importar los transportes de definición de seguridad de filas o de definición de clústeres. Los demás transportes pueden importarse en cualquier orden.

> **Nota**
>
> Después de copiar los archivos del CD al servidor, debe comprobar que tienen habilitado el permiso de escritura antes de importar los transportes. Si los archivos son de sólo lectura, la importación fallará.

> **Nota**
>
> Debido a que los transportes son archivos binarios, en instalaciones de UNIX debe agregar los archivos por FTP en modo Binario (para evitar daños en los archivos). Además, debe contar con permiso de escritura en el servidor UNIX.

## 28.1.1.17.2.4 Transportes

### 28.1.1.17.2.4.1 Transporte de conectividad Open SQL

El transporte de conectividad Open SQL permite que los controladores se conecten al sistema SAP y elaboren informes en él.

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/BC | Paquete | Clase Development |
| /CRYSTAL/OPENSQL | Grupo de funciones | Funciones Open SQL |
| /CRYSTAL/OSQL_AUTH_FORMS | Programa | Programa de ayuda |
| /CRYSTAL/OSQL_EXECUTE | Programa | Programa de ayuda |
| /CRYSTAL/OSQL_TYPEPOOLPROG | Programa | Programa de ayuda |
| /CRYSTAL/OSQL_TYPEPOOLS | Programa | Programa de ayuda |
| /CRYSTAL/OSQL_UTILS | Programa | Programa de ayuda |
| ZSSI | Clase de objeto de autorización | Objetos de autorización de informes |

| Objeto | Tipo | Descripción |
|---|---|---|
| ZSEGREPORT | Objeto de autorización | Objeto de autorización de informes |
| /CRYSTAL/OSQL_CLU_ACT-KEY_ENTRY | Tabla | Metadatos de clúster |
| /CRYSTAL/OSQL_FCN_PARAM | Tabla | Metadatos de función |
| /CRYSTAL/OSQL_FCN_PARAM_FIELD | Tabla | Metadatos de función |
| /CRYSTAL/OSQL_FIELD_ENTRY | Tabla | Metadatos de tabla |
| /CRYSTAL/OSQL_OBJECT_ENTRY | Tabla | Metadatos de tabla |
| /CRYSTAL/OSQL_RLS_CHK_ENTRY | Tabla | Metadatos de RLS |
| /CRYSTAL/OSQL_RLS_FCN_ENTRY | Tabla | Metadatos de RLS |
| /CRYSTAL/OSQL_RLS_VAL_ENTRY | Tabla | Metadatos de RLS |
| ZCLUSTDATA | Tabla | Metadatos de clúster |
| ZCLUSTID | Tabla | Metadatos de clúster |
| ZCLUSTKEY | Tabla | Metadatos de clúster |
| ZCLUSTKEY2 | Tabla | Metadatos de clúster |
| /CRYSTAL/AUTHCHK | Tabla | Metadatos de RLS |
| /CRYSTAL/AUTHFCN | Tabla | Metadatos de RLS |
| /CRYSTAL/AUTHKEY | Tabla | Metadatos de RLS |
| /CRYSTAL/AUTHOBJ | Tabla | Metadatos de RLS |
| /CRYSTAL/AUTHREF | Tabla | Metadatos de RLS |
| ZSSAUTHCHK | Tabla | Metadatos de RLS antiguos |
| ZSSAUTHOBJ | Tabla | Metadatos de RLS antiguos |
| ZSSAUTHKEY | Tabla | Metadatos de RLS antiguos |
| ZSSAUTHREF | Tabla | Metadatos de RLS antiguos |
| ZSSAUTH FCN | Tabla | Metadatos de RLS antiguos |

## 28.1.1.17.2.4.2 Transporte de conectividad de InfoSet

Este transporte permite al controlador InfoSet acceder a los InfoSets. Este transporte es compatible con R/3 4.6c y posteriores. No importe este transporte si ejecuta SAP R/3 4.6a o anteriores.

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/BC | Paquete | Clase Development |
| /CRYSTAL/FLAT | Grupo de funciones | Funciones de ajuste de InfoSet |
| /CRYSTAL/QUERY_BATCH | Programa | Ejecución del modo por lotes |
| /CRYSTAL/QUERY_BATCH_STREAM | Programa | Ejecución del modo por lotes en secuencia. |

## 28.1.1.17.2.4.3 Transporte de definición de seguridad de filas

Este transporte proporciona el Editor de definición de seguridad, una herramienta que actúa como interfaz gráfica con las tablas /CRYSTAL/AUTH en el transporte de conectividad Open SQL.

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/BC | Paquete | Clase Development |
| /CRYSTAL/TABMNT | Grupo de funciones | Grupo de funciones en vista de mantenimiento de tablas para restricciones de funciones |
| /CRYSTAL/RLSDEF | Programa | Programa principal |
| /CRYSTAL/RLS_INCLUDE1 | Programa | Programa de inclusión que contiene las definiciones de módulos |
| /CRYSTAL/RLS_INCLUDE2 | Programa | Programa de inclusión que contiene las definiciones de subrutinas |
| TDDAT [/CRYSTAL/AUTHFCN] | Contenido de tabla | Definición de mantenimiento de tablas |
| TVDIR [/CRYSTAL/AUTHFCN] | Contenido de tabla | Definición de mantenimiento de tablas |
| /CRYSTAL/AUTHFCNS | Definición de objeto de mantenimiento y transporte | Definición de mantenimiento de tablas |
| /CRYSTAL/RLS | Transacción | Transacción de programa principal |

| Objeto | Tipo | Descripción |
| --- | --- | --- |
| /CRYSTAL/RLSFCN | Transacción | Transacción de ayuda llamada internamente por el programa principal |

### 28.1.1.17.2.4.4 Transporte de definición de clúster

Este transporte proporciona la herramienta de definición de clústeres. Permite crear un repositorio de metadatos para las definiciones de clúster de datos ABAP. Estas definiciones proporcionan al controlador Open SQL la información que precisa para elaborar informes con estos clústeres de datos.

> **Nota**
>
> Los clústeres de datos ABAP no son lo mismo que las tablas de clústeres. Estas tablas ya se encuentran definidas en DDIC.

| Objeto | Tipo | Descripción |
| --- | --- | --- |
| ZCIMPRBG | Programa | Programa principal |
| ZCRBGTOP | Programa | Programa de inclusión |
| ZCDD | Transacción | Transacción de programa principal |

### 28.1.1.17.2.4.5 Transporte del Puesto de trabajo de administración de contenido

Este transporte proporciona la funcionalidad de administración de contenido a los sistemas BW. solo está disponible como transporte compatible con Unicode.

| Objeto | Tipo | Descripción |
| --- | --- | --- |
| /CRYSTAL/BC | Paquete | Clase Development |
| /CRYSTAL/CL_BW_HTTP_HANDLER | Clase | Gestor de peticiones HTTP compatibles con varios CE |
| /CRYSTAL/OBJECT_STATUS_DOM | Dominio | Actividad de informe |
| /CRYSTAL/OBJ_POLICY_DOM | Dominio | Seguridad de objetos CE |
| /CRYSTAL/OBJECT_STATUS | Elemento de datos | Actividad de informe |

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/OBJ_POLICY | Elemento de datos | Seguridad de objetos CE |
| /CRYSTAL/CE_SYNCH | Grupo de funciones | Talones del Publicador |
| /CRYSTAL/CA_MSG | Clase de mensaje | Mensajes de estado |
| /CRYSTAL/CE_SYNCH_FORMS | Programa | Componente de programa |
| /CRYSTAL/CONTENT_ADMIN | Programa | Componente de programa |
| /CRYSTAL/CONTENT_AD-MIN_CLASS_D | Programa | Componente de programa |
| /CRYSTAL/CONTENT_AD-MIN_CLASS_I | Programa | Componente de programa |
| /CRYSTAL/CONTENT_ADMIN_CTREE | Programa | Componente de programa |
| /CRYSTAL/CONTENT_ADMIN_FORMS | Programa | Componente de programa |
| /CRYSTAL/CONTENT_ADMIN_MODU-LES | Programa | Componente de programa |
| /CRYSTAL/CONTENT_ADMIN_PAIS | Programa | Componente de programa |
| /CRYSTAL/CONTENT_ADMIN_PBOS | Programa | Componente de programa |
| /CRYSTAL/CONTENT_AD-MIN_TAB_FRM | Programa | Componente de programa |
| /CRYSTAL/CONTENT_ADMIN_TOP | Programa | Componente de programa |
| /CRYSTAL/PUBLISH_WORKER | Programa | Componente de programa |
| /CRYSTAL/PUBLISH_WORKER_DISP | Programa | Componente de programa |
| /CRYSTAL/PUBLISH_WORKER_DISP_I | Programa | Componente de programa |
| /CRYSTAL/PUBLISH_WOR-KER_FORMS | Programa | Componente de programa |
| /CRYSTAL/PUBLISH_WORKER_PROC | Programa | Componente de programa |
| /CRYSTAL/PUBLISH_WOR-KER_PROC_I | Programa | Componente de programa |
| /CRYSTAL/PUBLISH_WOR-KER_SCREEN | Programa | Componente de programa |
| /CRYSTAL/CA_DEST | Tabla | Estado de aplicación |

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/CA_JOB | Tabla | Estado de aplicación |
| /CRYSTAL/CA_JOB2 | Tabla | Estado de aplicación |
| /CRYSTAL/CA_LANG | Tabla | Estado de aplicación |
| /CRYSTAL/CA_PARM | Tabla | Estado de aplicación |
| /CRYSTAL/CA_ROLE | Tabla | Estado de aplicación |
| /CRYSTAL/CA_SYST | Tabla | Estado de aplicación |
| /CRYSTAL/MENU_TREE_ITEMS | Estructura | Estado de aplicación |
| /CRYSTAL/REPORT_ID | Tabla | Estado de aplicación |
| /CRYSTAL/RPTADMIN | Transacción | Transacción de programa principal |
| /CRYSTAL/EDIT_REPORT | Programa | Ajuste de edición de informes |
| /CRYSTAL/EDIT_REPORT | Grupo de funciones | Funciones de edición de informes |
| ZSSI | Clase de objeto de autorización | Autorizaciones de Crystal |
| ZCNTADMCES | Objeto de autorización | Operaciones de CE |
| ZCNTADMRPT | Objeto de autorización | Operaciones de informe |
| ZCNTADMJOB | Objeto de autorización | Operaciones de tareas en fondo |

## 28.1.1.17.2.4.6 Transporte de conectividad ODS

Este transporte permite que el controlador ODS Query tenga acceso a los datos ODS. Este transporte es compatible con BW 3.0B parche 27 o posterior y BW 3.1C parche 21 o posterior.

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/BC | Paquete | Clase Development |
| /CRYSTAL/ODS_REPORT | Grupo de funciones | Funciones ODS |

## 28.1.1.17.2.4.7 Transporte de personalización de parámetros de consultas BW

Este transporte proporciona soporte para los valores de parámetros personalizados y predeterminados de informes basados en consultas BW.

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/BC | Paquete | Clase Development |
| /CRYSTAL/PERS_VAR | Estructura | Definición de variable |
| /CRYSTAL/PERS_VALUE | Estructura | Definición de valor |
| /CRYSTAL/PERS | Grupo de funciones | Funciones de personalización |

## 28.1.1.17.2.4.8 Transporte de conectividad BW MDX

Este transporte permite que el controlador MDX Query tenga acceso a cubos y consultas BW. Este transporte es compatible con BW 3.0B parche 27 o posterior y BW 3.1C parche 21 o posterior.

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/BC | Paquete | Clase Development |
| /CRYSTAL/MDX | Grupo de funciones | Funciones MDX |
| /CRYSTAL/MDX_STREAM_LAYOUT | Definición de tabla | Estructura de conjunto de datos |
| /CRYSTAL/CX_BAPI_ERROR | Clase | Excepción |
| /CRYSTAL/CX_METADATA_ERROR | Clase | Excepción |
| /CRYSTAL/CX_MISSING_STREA-MINFO | Clase | Excepción |
| /CRYSTAL/CX_NO_MORE_CELLS | Clase | Excepción |
| /CRYSTAL/CX_NO_MORE_MEMBERS | Clase | Excepción |
| /CRYSTAL/CX_NO_MORE_PROPER-TIES | Clase | Excepción |
| /CRYSTAL/CX_SAVE_SESSION_STATE | Clase | Excepción |
| /CRYSTAL/MDX_APPEND_DATA | Clase | Procesador de conjunto de datos |

| Objeto | Tipo | Descripción |
|---|---|---|
| /CRYSTAL/MDX_READER_BASE | Clase | Procesador de conjunto de datos |
| /CRYSTAL/MDX_READ_DIMENSIONS | Clase | Procesador de conjunto de datos |
| /CRYSTAL/MDX_READ_MEASURES | Clase | Procesador de conjunto de datos |
| /CRYSTAL/MDX_READ_PROPERTIES | Clase | Procesador de conjunto de datos |
| /CRYSTAL/MDX_AXIS_LEVELS | Tipo de tabla | Estructura de metadatos |
| /CRYSTAL/MDX_PROPERTY_KEYS | Tipo de tabla | Estructura de metadatos |
| /CRYSTAL/MDX_PROPERTY_VALUES | Tipo de tabla | Estructura de metadatos |
| /CRYSTAL/MDX_STREAM_LA-YOUT_TAB | Tipo de tabla | Estructura de metadatos |

## 28.1.1.18 Información general sobre las autorizaciones

En esta sección se proporciona una lista de las autorizaciones de SAP que, según nuestra experiencia y nuestro entorno de prueba, son necesarias para realizar tareas comunes de la Plataforma de BI en un entorno SAP integrado. Pueden ser necesarios otros objetos o campos de autorización, en función de la implementación individual.

En cada objeto de autorización debe crear una autorización y definir los valores de campo correspondientes. A continuación, debe aplicar las autorizaciones apropiadas a los perfiles (o funciones) de los usuarios SAP. En las siguientes secciones se describen las autorizaciones necesarias y se indican los valores de campo necesarios. Para obtener detalles sobre el procedimiento específicos para su versión de SAP, consulte la documentación de SAP.

> ⓘ Nota
>
> La información de esta sección solo se indica a modo de orientación.

> ⓘ Nota
>
> El objeto de autorización ZSEGREPORT pertenece a la clase de objetos ZSSI, que se instala durante la importación de los archivos de transporte de integración de SAP necesarios para realizar consultas de Open SQL.

### 28.1.1.18.1 Crear y aplicar autorizaciones

Debe crear y aplicar las autorizaciones necesarias para que cada usuario acceda a la información mediante la integración de Desktop Intelligence para SAP. El procedimiento exacto para crear, configurar y aplicar

autorizaciones depende de la versión de SAP instalada. En esta sección se proporciona una lista de las autorizaciones de SAP que, según nuestra experiencia y en nuestros entornos de prueba, son necesarios al llevar a cabo tareas comunes al usar la plataforma de BI integrada en un entorno ABAP de SAP NetWeaver. Pueden ser necesarios otros objetos o campos de autorización, en función de la implementación individual.

### Información relacionada

Configuración de publicación en el Puesto de trabajo de administración de contenido [página 1023]

## 28.1.1.19 Acciones en BW

Esta sección explica varias acciones en BW.

### 28.1.1.19.1 Acciones dentro de Crystal Reports

#### 28.1.1.19.1.1 Crear un nuevo informe desde una consulta en una función BW

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_USER_AGR | ACT_GROUP | **<FUNCIÓN_USUARIO>*** |
| | ACTVT | 01, 02, 06 |
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | RS_PERS_BOD |
| | ACTVT | 16 |
| S_CTS_ADMI | CTS_ADMFCT | TABL |
| S_RS_COMP | RSINFOAREA | **<AREA_INFO>**** |
| | RSINFOCUBE | **<CUBO_INFO>**** |
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<ID_COMP>**** |
| S_RS_COMP1 | RSZCOMPID | **<ID_COMP>**** |

| Objeto de autorización | Campo | Valores |
|---|---|---|
| | RSZCOMPTP | REP |
| | RSZOWNER | **<PROPIETARIO_CONSULTA>*** |
| | ACTVT | 16 |

* **<FUNCIÓN_USUARIO>** indica el nombre de cualquier función a la que pertenezca el usuario. Puede introducir varios valores en este campo.

* **<PROPIETARIO_CONSULTA >**indica el nombre del propietario de la consulta. Si especifica un nombre, sólo puede realizar informes sobre las consultas con dicho propietario. Introduzca * para realizar informes sobre las consultas con cualquier propietario.

** En **< AREA_INFO>**, **<CUBO_INFO>** o **<ID_COMP>**, * indica cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

## 28.1.1.19.1.2 Abrir un informe existente desde una función BW

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SUSO, SUNI. RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, / CRYSTAL/PERS, RSOB |
| | ACTVT | 16 |
| S_RS_COMP | RSINFOAREA | **<AREA_INFO>*** |
| | RSINFOCUBE | **<CUBO_INFO>*** |
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<ID_COMP>*** |
| S_RS_COMP1 | RSZCOMPID | **<ID_COMP>*** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<PROPIETARIO_CONSULTA>*** |
| | ACTVT | 16 |

* **<PROPIETARIO_CONSULTA>** indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

** En **< AREA_INFO>**, **<CUBO_INFO>** o **<ID_COMP>**, * indica cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

### 28.1.1.19.1.3 Obtener una vista previa o actualizar un informe

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RS_COMP | RSINFOAREA | **<AREA_INFO>**** |
| | RSINFOCUBE | **<CUBO_INFO>**** |
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<ID_COMP>**** |
| S_RS_COMP1 | RSZCOMPID | **<ID_COMP>**** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<PROPIETARIO_CONSULTA>*** |
| | ACTVT | 16 |

* **<PROPIETARIO_CONSULTA>** indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

** En **< AREA_INFO>**, **<CUBO_INFO>** o **<ID_COMP>**, * indica cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

### 28.1.1.19.1.4 Verificar la base de datos (actualizar las definiciones de tabla en un informe)

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RS_COMP | RSINFOAREA | **<AREA_INFO>**** |
| | RSINFOCUBE | **<CUBO_INFO>**** |

| Objeto de autorización | Campo | Valores |
|---|---|---|
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<ID_COMP>**** |
| S_RS_COMP1 | RSZCOMPID | **<ID_COMP>**** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<PROPIETARIO_CONSULTA>*** |
| | ACTVT | 16 |

* **<PROPIETARIO_CONSULTA>** indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

** En **< AREA_INFO>**, **<CUBO_INFO>** o **<ID_COMP>**, * indica cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

## 28.1.1.19.1.5 Establecer la ubicación del origen de datos

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RS_COMP | RSINFOAREA | **<AREA_INFO>**** |
| | RSINFOCUBE | **<CUBO_INFO>**** |
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<ID_COMP>**** |
| S_RS_COMP1 | RSZCOMPID | **<ID_COMP>**** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<PROPIETARIO_CONSULTA>*** |
| | ACTVT | 16 |

* **<PROPIETARIO_CONSULTA>** indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

** En **< AREA_INFO>**, **<CUBO_INFO>** o **<ID_COMP>**, * indica cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

### 28.1.1.19.1.6 Guardar un informe en una función BW

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_USER_AGR | ACT_GROUP | **<USER_ROLE>** * |
| | ACTVT | 01, 02, 06 |
| S_CTS_ADMI | CTS_ADMFCT | TABL |

* **<FUNCIÓN_USUARIO>** indica el nombre de cualquier función a la que pertenezca el usuario. Puede introducir varios valores en este campo.

### 28.1.1.19.1.7 Preparar un informe para su traducción al guardarlo en BW

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_USER_AGR | ACT_GROUP | **<FUNCIÓN_USUARIO>*** |
| | ACTVT | 01 |
| S_CTS_ADMI | CTS_ADMFCT | TABL |

* **<FUNCIÓN_USUARIO>** indica el nombre de cualquier función a la que pertenezca el usuario. Puede introducir varios valores en este campo.

### 28.1.1.19.1.8 Guardado de un informe y publicación simultánea en la plataforma de BI

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_USER_AGR | ACT_GROUP | **<FUNCIÓN_USUARIO>*** |
| | ACTVT | 01 |
| S_CTS_ADMI | CTS_ADMFCT | TABL |
| S_RS_COMP | RSINFOAREA | **<AREA_INFO>** *** |
| | RSINFOCUBE | **<CUBO_INFO>** *** |

| Objeto de autorización | Campo | Valores |
|---|---|---|
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<ID_COMP>** *** |
| S_RS_COMP1 | RSZCOMPID | **<ID_COMP>** *** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<PROPIETARIO_CONSULTA>** ** |
| | ACTVT | 16 |

* **<FUNCIÓN_USUARIO>** indica el nombre de cualquier función a la que pertenezca el usuario. Puede introducir varios valores en este campo.

** **<PROPIETARIO_CONSULTA>** indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

*** En **< AREA_INFO>** , **<CUBO_INFO>** o **<ID_COMP>** , * indica cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

## 28.1.1.19.1.9 Iniciar BEx Query Designer™

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RS_COMP | RSINFOAREA | **<INFO_AREA>**** |
| | RSINFOCUBE | **<INFO_CUBE>**** |
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<COMP_ID>**** |
| S_RS_COMP1 | RSZCOMPID | **<COMP_ID>**** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<QUERY_OWNER>*** |
| | ACTVT | 16 |
| S_CTS_ADMI | CST_ADMFCT | TABL |

* **<QUERY_OWNER >**indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

** Para **<INFO_AREA>**, **<INFO_CUBE>**, o **<COMP_ID>**, introduzca * para indicar cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

## 28.1.1.19.2 Acciones dentro de la plataforma de lanzamiento de BI

### 28.1.1.19.2.1 Inicio de sesión en la plataforma de BI con credenciales SAP

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_ADMI_FCD | S_ADMI_FCD | ST0R, ST0M |

### 28.1.1.19.2.2 Ver un informe de SAP BW a petición

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST, RSOB, SUNI |
| | ACTVT | 16 |
| S_RS_COMP | RSINFOAREA | **<AREA_INFO>**** |
| | RSINFOCUBE | **<CUBO_INFO>**** |
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<ID_COMP>**** |
| S_RS_COMP1 | RSZCOMPID | **<ID_COMP>**** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<PROPIETARIO_CONSULTA>*** |
| | ACTVT | 16 |
| S_RS_ODSO | RSINFOAREA | **<AREA_INFO>**** |
| | RSODSOBJ | 0CRM_OLVM |

| Objeto de autorización | Campo | Valores |
|---|---|---|
| | RSODSPART | DATA |
| | ACTVT | 03 |

* **<PROPIETARIO_CONSULTA>** indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

** En **< AREA_INFO>**, **<CUBO_INFO>** o **<ID_COMP>**, * indica cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

## 28.1.1.19.2.3 Actualizar un informe desde el visor

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RS_COMP | RSINFOAREA | **<INFO_AREA>**** |
| | RSINFOCUBE | **<INFO_CUBE>**** |
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<COMP_ID>**** |
| S_RS_COMP1 | RSZCOMPID | **<COMP_ID>**** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<QUERY_OWNER>*** |
| | ACTVT | 16 |
| S_RS_ODSO | RSINFOAREA | **<INFO_AREA>**** |
| | RSODSOBJ | 0CRM_OLVM |
| | RSODSPART | DATA |
| | ACTVT | 03 |

* **<QUERY_OWNER >**indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

** Para **<INFO_AREA>**, **<INFO_CUBE>**, o **<COMP_ID>**, introduzca * para indicar cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

## 28.1.1.19.2.4 Programar un informe

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST, RSOB, SUNI |
| | ACTVT | 16 |
| S_RS_COMP | RSINFOAREA | **<AREA_INFO>**** |
| | RSINFOCUBE | **<CUBO_INFO>**** |
| | RSZCOMPTP | REP |
| | RSZCOMPID | **<ID_COMP>**** |
| S_RS_COMP1 | RSZCOMPID | **<ID_COMP>**** |
| | RSZCOMPTP | REP |
| | RSZOWNER | **<PROPIETARIO_CONSULTA>*** |
| | ACTVT | 16 |
| S_RS_ODSO | RSINFOAREA | **<AREA_INFO>**** |
| | RSODSOBJ | 0CRM_OLVM |
| | RSODSPART | DATA |
| | ACTVT | 03 |

* **<PROPIETARIO_CONSULTA>** indica el nombre del propietario de la consulta desde la que crea el informe. Si introduce el nombre de un propietario, sólo puede elaborar informes sobre consultas con dicho propietario. Introduzca * para indicar cualquier propietario.

** En **< AREA_INFO>**, **<CUBO_INFO>** o **<ID_COMP>**, * indica cualquier valor. Si indica un valor específico, sólo puede elaborar informes sobre consultas que contienen dichas áreas de información, cubos de información e Id. de componentes.

### 28.1.1.19.2.5 Leer listas de selección dinámicas en parámetros del informe

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST, RSOB |
| | ACTVT | 16 |

### 28.1.1.19.3 Acciones dentro de SAP Netweaver (ABAP)

### 28.1.1.19.3.1 Desde Crystal Reports con el controlador Open SQL

En esta sección se explican las diferentes acciones en SAP NetWeaver (ABAP) desde Crystal Reports mediante el controlador Open SQL.

### 28.1.1.19.3.2 Iniciar sesión en un servidor SAP

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST, /CRYSTAL/OPENSQL |
| | ACTVT | 16 |

### 28.1.1.19.3.3 Crear un nuevo informe

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST, /CRYSTAL/OPENSQL |
| | ACTVT | 16 |

| Objeto de autorización | Campo | Valores |
|---|---|---|
| ZSEGREPORT | ACTVT | 01 |

### 28.1.1.19.3.4 Abrir u obtener una vista previa de un informe existente

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST, /CRYSTAL/OPENSQL |
| | ACTVT | 16 |
| ZSEGREPORT | ACTVT | 02 |

### 28.1.1.19.3.5 Verificar la base de datos (actualizar las definiciones de tabla en un informe)

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_ADMI_FCD | S_ADMI_FCD | ST0R, ST0M |
| ZSEGREPORT | ACTVT | 02 |
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | /CRYSTAL/OPENSQL |
| | ACTVT | 16 |

### 28.1.1.19.3.6 Establecer la ubicación del origen de datos

| Objeto de autorización | Campo | Valores |
|---|---|---|
| ZSEGREPORT | ACTVT | 02 |
| S_RFC | RFC_TYPE | FUGR |

| Objeto de autorización | Campo | Valores |
|---|---|---|
| | RFC_NAME | /CRYSTAL/OPENSQL |
| | ACTVT | 16 |

## 28.1.1.19.4 Acciones dentro de Crystal Reports mediante el controlador InfoSet y los informes de InfoSet

### 28.1.1.19.4.1 Iniciar sesión en un servidor SAP

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST |
| | ACTVT | 16 |

### 28.1.1.19.4.2 Crear un nuevo informe desde un InfoSet en SAP Netweaver (ABAP)

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | /CRYSTAL/FLAT, SKBW, AQRC |
| | ACTVT | 16 |
| S_CTS_ADMI | CTS_ADMFCT | TABL |

> **Nota**
>
> Agregue además suficientes autorizaciones para ver filas de datos. Por ejemplo, P_ORIG o P_APAP.

#### Información relacionada

Establecer la ubicación del origen de datos [página 1057]

### 28.1.1.19.4.3 Verificar la base de datos (actualizar las definiciones de tabla en un informe)

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_ADMI_FCD | S_ADMI_FCD | ST0R, ST0M |

### 28.1.1.19.4.4 Establecer la ubicación del origen de datos

| Objeto de autorización | Campo | Valores |
|---|---|---|
| P_ABAP | REPID | AQTGSYSTGENERATESY, SAPDBPNP |
| | COARS | 2 |

## 28.1.1.19.5 Acciones dentro de Crystal Reports mediante el controlador InfoSet y la generación de informes de una consulta ABAP

### 28.1.1.19.5.1 Iniciar sesión en un servidor SAP

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST |
| | ACTVT | 16 |

### 28.1.1.19.5.2 Crear un nuevo informe desde una consulta ABAP en SAP Netweaver

| Objeto de autorización | Campo | Valores |
|---|---|---|
| P_ABAP | REPID | AQTG02==========P6, SAPDBPNP |
| | COARS | 2 |
| S_ADMI_FCD | S_ADMI_FCD | ST0R, ST0M |
| S_TABU_DIS | ACTVT | 03 |
| | GROUP | Nombre del grupo de tablas |

## 28.1.1.19.5.3 Verificar la base de datos

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_ADMI_FCD | S_ADMI_FCD | ST0R, ST0M |
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SKBW |
| | ACTVT | 16 |

## 28.1.1.19.5.4 Establecer la ubicación del origen de datos

| Objeto de autorización | Campo | Valores |
|---|---|---|
| P_ABAP | REPID | AQTG02==========P6, SAPDBPNP |
| | COARS | 2 |
| S_ADMI_FCD | S_ADMI_FCD | ST0R, ST0M |
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SKBW |
| | ACTVT | 16 |
| S_TABU_DIS | ACTVT | 03 |
| | GROUP | Nombre del grupo de tablas |

## 28.1.1.19.6 Acciones dentro de la plataforma de BI

### 28.1.1.19.6.1 Programar un informe en modo de cuadro de diálogo (con una consulta Open SQL)

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_USER_GRP | CLASS | |
| | ACTVT | 03 |
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST, RFC1, /CRYSTAL/OPENSQL |
| | ACTVT | 16 |
| ZSEGREPORT | ACTVT | 02 |

> **Nota**
>
> El valor de CLASS es BLANK.

### 28.1.1.19.6.2 Programar un informe en modo por lotes usando una consulta Open SQL

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_USER_GRP | CLASS | |
| | ACTVT | 03 |
| S_RFC | RFC_TYPE | FUGR |
| | RFC_NAME | SYST, RFC1, /CRYSTAL/OPENSQL, SH3A |
| | ACTVT | 16 |
| S_BTCH_JOB | JOBGROUP | ' ' |
| | JOBACTION | RELE |
| ZSEGREPORT | ACTVT | 02 |

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_BTCH_ADM | BTCADMIN | Y |

> **Nota**
>
> El valor de CLASS es BLANK.

## 28.1.1.19.6.3 Sistema de acceso condicionado de Crystal

| Objeto de autorización | Campo | Valor |
|---|---|---|
| Autorización de acceso a archivos (S_DATASET) | Actividad (ACTVT) | Lectura, escritura (33, 34) |
| | Nombre físico del archivo (FILENAME) | * (indica Todos) |
| | Nombre del programa ABAP (PROGRAM) | * |
| Comprobación de autorización para acceso RFC (S_RFC) | Actividad (ACTVT) | 16 |
| | Nombre del RFC que debe protegerse (RFC_NAME) | BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SECURITY |
| | Tipo del objeto RFC que debe protegerse (RFC_TYPE) | Grupo de funciones (FUGR) |
| Mantenimiento principal de usuarios: grupos de usuarios (S_USER_GRP) | Actividad (ACTVT) | Creación o generación, y visualización (03) |
| | Grupo de usuarios en mantenimiento principal de usuarios (CLASS) | * <br> **Nota** <br> Para obtener una mayor seguridad, es posible que prefiera indicar de forma explícita los grupos de usuarios cuyos miembros necesiten acceso a la plataforma de BI. |

## 28.1.1.19.6.4 Ejecución y diseño de consultas BW BeX

Al crear un informe a partir de un universo basado en una consulta BW BeX, si se incluye una dimensión de fecha, el administrador del sistema debe otorgar la autorización `S_RS_IOBJ` al usuario que diseñe el universo y al usuario que ejecute el informe.

| Objeto de autorización | Campo | Valores |
|---|---|---|
| S_RS_IOBJ | ACTVT | 03 |
| | RSIOBJ | |
| | RSIOBJ_CAT | |
| | RSIOBJ_PART | |

## 28.2 Configurar para la integración de JD Edwards

### 28.2.1 Configurar el inicio de sesión único (SSO) para SAP Crystal Reports

De forma predeterminada, la plataforma de BI se configurará para permitir que los usuarios de SAP Crystal Reports accedan a los datos de JD Edwards EnterpriseOne mediante el inicio de sesión único (SSO).

#### 28.2.1.1 Desactivar el SSO para JD Edwards y SAP Crystal Reports

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. Seleccione *crdb_pseone*.
5. Haga clic en *Eliminar*.
6. Haga clic en *Guardar y cerrar*.
7. En la página *Servidores* en la CMC, seleccione *Servicios de Crystal Reports* y haga clic en *Reiniciar servidor*.

#### 28.2.1.2 Activar el SSO para JD Edwards y SAP Crystal Reports

Si ha desactivado el SSO para JD Edwards y SAP Crystal Reports y desea volver a activarlo.

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. En *Usar contexto de SSO para conexión de base de datos con los siguientes controladores*, escriba *crdb_pseone*.

5. Haga clic en *Agregar*.
6. Haga clic en *Guardar y cerrar*.
7. En la página *Servidores* en la CMC, seleccione *Servicios de Crystal Reports* y haga clic en *Reiniciar servidor*.

## 28.2.2 Configuración del Nivel de socket seguro para integraciones de JD Edwards

Puede usar el protocolo Nivel de socket seguro (SSL) para todas las comunicaciones de red entre los clientes y los servidores del despliegue de la plataforma de BI y JD Edwards EnterpriseOne.

El uso de los datos de JD Edwards EnterpriseOne con la plataforma de BI necesita que se realicen algunos cambios en la configuración del SSL. Como sucede con la configuración SSL de otros servidores y clientes de la Plataforma de BI, almacene la siguiente clave y los archivos de certificado en una ubicación segura (bajo el mismo directorio) a la que puedan acceder los equipos del despliegue de la Plataforma de BI.

- El archivo de certificado de confianza (cacert.der).
- El archivo de certificado de servidor generado (servercert.der).
- El archivo de claves del servidor (server.key).
- El archivo de frase de acceso (passphrase.txt).

### 28.2.2.1 Para habilitar la conectividad de datos de JD Edwards EnterpriseOne con SSL

> **Nota**
>
> Todos los valores que se describen en el siguiente procedimiento distinguen entre mayúsculas y minúsculas.

1. Copie el certificado SSL en `C:\SSLCert`.
2. Inicie el Administrador de configuración central (CCM).
3. Detenga el Agente de inteligencia de servidor (SIA).
4. Haga doble clic en SIA para abrir el cuadro de diálogo *Propiedades*.
5. Haga clic en la ficha *Protocolo*.
6. Seleccione *Habilitar SSL*.
7. Para la *Carpeta de certificados SSL*, elija el directorio que contiene los certificados SSL: `C:\SSLCert`.
8. Para el *Archivo del certificado SSL del servidor*, seleccione `servercert.der`.
9. Para los *Archivos de certificados de confianza SSL*, seleccione `cacert.der`.
10. Para el *Archivo de clave privada SSL*, seleccione `server.key`.
11. Para el *Archivo de contraseña de clave privada SSL*, seleccione `passphrase.txt`.
12. Haga clic en *Aplicar*.
13. Inicie Server Intelligence Agent.

Debe reiniciar los servidores de generación de informes de la plataforma de BI (como el servidor de tareas de Adaptive) antes de que estos cambios surtan efecto.

#### 28.2.2.2 Archivo de propiedades de configuración de SSL

El archivo de propiedades `sslconf.properties` contienen toda la información para los certificados y claves necesarias que usa la plataforma de BI. Por ejemplo:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

El archivo `sslconf.properties` se debe colocar en la carpeta en la que está instalada la plataforma de BI, `C:\Archivos de programa\Business Objects\BusinessObjects 13.0`, de forma predeterminada.

## 28.3 Configurar para la integración de PeopleSoft Enterprise

### 28.3.1 Configurar el inicio de sesión único (SSO) para SAP Crystal Reports y PeopleSoft Enterprise

De forma predeterminada, la plataforma de BI se configurará para permitir que los usuarios de SAP Crystal Reports accedan a los datos de PeopleSoft Enterprise mediante el inicio de sesión único (SSO).

#### 28.3.1.1 Desactivar el SSO para PeopleSoft Enterprise y SAP Crystal Reports

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. Seleccione *crdb_psenterprise*.
5. Haga clic en *Eliminar*.
6. Haga clic en *Guardar y cerrar*.
7. En la página *Servidores* en la CMC, seleccione *Servicios de Crystal Reports* y haga clic en *Reiniciar servidor*.

### 28.3.1.2 Activar el SSO para PeopleSoft Enterprise y SAP Crystal Reports

Si ha desactivado el SSO para PeopleSoft Enterprise y SAP Crystal Reports y desea volver a activarlo.

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. En *Usar contexto de SSO para conexión de base de datos con los siguientes controladores*, escriba *crdb_psenterprise*.
5. Haga clic en *Agregar*.
6. Haga clic en *Guardar y cerrar*.
7. En la página *Servidores* en la CMC, seleccione *Servicios de Crystal Reports* y haga clic en *Reiniciar servidor*.

## 28.3.2 Configuración de la comunicación de Capa de sockets seguros (SSL)

Puede usar el protocolo Nivel de socket seguro (SSL) para todas las comunicaciones de red entre clientes y servidores del despliegue de la Plataforma de BI.

Como sucede con la configuración SSL de otros servidores y clientes de la Plataforma de BI, almacene la siguiente clave y los archivos de certificado en una ubicación segura (bajo el mismo directorio) a la que puedan acceder los equipos del despliegue de la Plataforma de BI.

- El archivo de certificado de confianza (cacert.der).
- El archivo de certificado de servidor generado (servercert.der).
- El archivo de claves del servidor (server.key).
- El archivo de frase de acceso (passphrase.txt).

### 28.3.2.1 Archivo de propiedades de configuración de SSL

El archivo de propiedades `sslconf.properties` contiene toda la información para los certificados y claves necesarias que usan los componentes de la plataforma de BI de SAP. Por ejemplo:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

El archivo `sslconf.properties` se debería colocar en la carpeta donde esté instalado el producto de la plataforma de BI: `C:\Archivos de programa\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\`, de forma predeterminada.

### 28.3.2.2 Para activar SSL en el Servidor de consultas de PeopleSoft

> **Nota**
>
> Todos los valores que se describen en el siguiente procedimiento distinguen entre mayúsculas y minúsculas.

1. Copie el certificado SSL en `C:\SSLCert`.
2. Inicie el Administrador de configuración central (CCM).
3. Detenga el Agente de inteligencia de servidor (SIA).
4. Haga doble clic en SIA para abrir el cuadro de diálogo *Propiedades*.
5. Haga clic en la ficha *Protocolo*.
6. Seleccione *Habilitar SSL*.
7. Para la *Carpeta de certificados SSL*, elija el directorio que contiene los certificados SSL: `C:\SSLCert`.
8. Para el *Archivo del certificado SSL del servidor*, seleccione `servercert.der`.
9. Para los *Archivos de certificados de confianza SSL*, seleccione `cacert.der`.
10. Para el *Archivo de clave privada SSL*, seleccione `server.key`.
11. Para el *Archivo de contraseña de clave privada SSL*, seleccione `passphrase.txt`.
12. Haga clic en *Aplicar*.
13. Inicie Server Intelligence Agent.

Debe reiniciar los servidores de generación de informes de la plataforma de BI (como el servidor de tareas de Adaptive) antes de que estos cambios surtan efecto.

### 28.3.2.3 Para activar el Puente de seguridad con SSL

> **Nota**
>
> Todos los valores que se describen en el siguiente procedimiento distinguen entre mayúsculas y minúsculas.

1. Copie el certificado SSL en `C:\SSLCert`.
2. Inicie el Administrador de configuración central (CCM).
3. Detenga el Agente de inteligencia de servidor (SIA).
4. Haga doble clic en SIA para abrir el cuadro de diálogo *Propiedades*.
5. Haga clic en la ficha *Protocolo*.
6. Seleccione *Habilitar SSL*.
7. Para la *Carpeta de certificados SSL*, elija el directorio que contiene los certificados SSL: `C:\SSLCert`.
8. Para el *Archivo del certificado SSL del servidor*, seleccione `servercert.der`.
9. Para los *Archivos de certificados de confianza SSL*, seleccione `cacert.der`.
10. Para el *Archivo de clave privada SSL*, seleccione `server.key`.

11. Para el *Archivo de contraseña de clave privada SSL*, seleccione `passphrase.txt`.
12. Haga clic en *Aplicar*.
13. Inicie Server Intelligence Agent.

## 28.3.3 Sintonización del rendimiento para sistemas de PeopleSoft

Para garantizar un rendimiento óptimo al crear informes a partir de consultas de PeopleSoft, es importante entender cómo Crystal Reports y la plataforma de BI ejecutan las consultas.

Cada vez que actualice o ejecute un informe basado en una consulta de PeopleSoft, se establece una conexión con un servidor PeopleSoft:

- En entornos PeopleSoft Enterprise (PeopleTools 8.46 o posterior), se establece una conexión con el *Servidor de analíticas de PeopleSoft*.
- En entornos PeopleSoft Enterprise (PeopleTools 8.21-8.45), se establece una conexión con el *Servidor de aplicaciones de PeopleSoft*.

### 28.3.3.1 Recomendaciones

En una implementación óptima, uno o varios Servidores de analíticas o aplicaciones de PeopleSoft se configuran para que traten únicamente solicitudes de informes. En cada uno de estos servidores, los parámetros para las instancias mín. y máx. controlan el número de solicitudes de informe que se pueden procesar al mismo tiempo. Esta configuración presenta las siguientes ventajas:

- No hay ningún conflicto entre las solicitudes de informe y otras solicitudes transaccionales en el servidor PeopleSoft.
- Es posible realizar el mantenimiento en el servidor que controla las solicitudes de informe sin inhabilitar el servidor que controla las solicitudes transaccionales.

En un entorno en el que el mismo Servidor de analíticas o de aplicaciones de PeopleSoft controla las solicitudes de informes y las transaccionales, debe configurar la plataforma de BI para que no ejecute más de un informe al mismo tiempo. De lo contrario, los usuarios no podrán realizar ninguna solicitud transaccional si todos los procesos PSANALYTICSRV o PSAPPSRV se utilizan para ejecutar informes.

> **Nota**
>
> Para obtener información sobre cómo limitar el número de tareas programadas de informe y de visualización de informes a petición, consulte "Administrar y configurar servidores" del *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*.

> **Nota**
>
> No es posible configurar el sistema para que limite el número de usuarios de Crystal Reports que pueden intentar acceder al mismo tiempo al servidor.

Si aparecen problemas de rendimiento, utilice la herramienta de configuración Psadmin para determinar si las solicitudes se ponen en cola. Además, supervise los recursos del sistema en el equipo del Servidor de

analíticas o aplicaciones de PeopleSoft. Si se está utilizando memoria virtual debido a la falta de memoria física, el procesamiento también puede ralentizarse.

### 28.3.3.2 Servidores PeopleSoft

En un Servidor de analíticas de PeopleSoft, el proceso que actualiza o ejecuta los informes es el proceso PSANALYTICSRV. En un Servidor de aplicaciones de PeopleSoft, el proceso que actualiza o ejecuta los informes es el proceso PSAPPSRV. El número de procesos PSANALYTICSRV o PSAPPSRV disponibles determina el número de informes que se pueden ejecutar simultáneamente.

Un archivo de configuración típico del Servidor de analíticas o aplicaciones de PeopleSoft contiene la información siguiente:

```
Min Instances=3
Max Instances=5
```

En este ejemplo, un mínimo de tres procesos PSANALYTICSRV o PSAPPSRV está disponible en cualquier momento con la capacidad de incrementarse hasta cinco procesos. No significa necesariamente que siempre se puedan ejecutar cinco informes al mismo tiempo; los procesos también se pueden utilizar para controlar otras tareas en el sistema. Si no hay ningún proceso PSANALYTICSRV o PSAPPSRV disponible para controlar una solicitud, ésta se pone en cola hasta que haya algún proceso disponible.

> **Nota**
>
> El archivo de configuración para Servidores de *aplicaciones* de PeopleSoft también suele incluir el parámetro `Tiempo de espera de servicio`, que especifica cuánto tiempo esperarán en cola las solicitudes a que haya un proceso disponible. Si ningún proceso queda disponible dentro del tiempo especificado en el parámetro, finalizará el tiempo de espera de la solicitud.

## 28.4 Configurar para la integración de Siebel

### 28.4.1 Configurar Siebel para la integración con la plataforma SAP BI

La integración de la plataforma de BI proporciona un vínculo a Crystal Reports que permite incrustar el contenido de la suite de BusinessObjects Business Intelligence en una aplicación de Siebel. Una vez instalado y configurado, el nuevo elemento de menú permite a los usuarios iniciar la plataforma de BI desde la aplicación de Siebel.

De forma predeterminada, los archivos necesarios se instalan en la siguiente carpeta: `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.

### 28.4.1.1 Importar el proyecto de integración a la Plataforma de BI

1. Inicie Siebel Tools.
2. Haga clic en *Herramientas* > *Importar desde archivo*.
3. Cuando se le solicite un archivo, desplácese a la carpeta Archivos de Siebel de la instalación del producto de integración.

   De forma predeterminada, es: `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\`.
4. Vaya a la subcarpeta adecuada (Siebel 7.7 o Siebel 8.0) y seleccione el archivo `BusinessObjectsEnterprise.sif`.
   Aparece el asistente de importación.
5. Haga clic en *Merge the object definition from the archive file with the definition in the repository* (Fusionar la definición del objeto del archivo de almacenamiento con la definición del repositorio).
6. Siga las instrucciones que vayan apareciendo en las ventanas del asistente para finalizar la importación del proyecto de integración.
   El proyecto de integración se agrega al repositorio.
7. Bloquee el proyecto de *BusinessObjects Integration*.

## 28.4.2 Crear el elemento de menú Crystal Reports

1. En Siebel Tools (Herramientas de Siebel), bloquee el proyecto *Menu* (Menú).
2. En el explorador de objetos, seleccione el objeto *Menu Item* (Elemento de menú).

   > **Nota**
   >
   > Si el objeto Menu (Menú) no aparece en el explorador de objetos, haga clic en *View (Ver)* > *Options (Opciones)* en Siebel Tools (Herramientas de Siebel), haga clic en la ficha *Object Explorer* (Explorador de objetos) y seleccione el objeto *Menu* (Menú).
3. En la lista *Menus* (Menús), seleccione el menú *Generic Web* (Web genérica).
4. Haga clic en el encabezado de lista *Menu Items* (Elementos de menú).
5. Haga clic en *Editar* > *Nuevo registro*.
6. Defina como corresponde el nuevo elemento de menú. A continuación, se indican los valores recomendados:
   - Name (Nombre): View (Vista) - Crystal Reports
   - Command (Comando): Crystal Reports
   - Comentarios: menú de informes integrado de SAP BusinessObjects
   - Inactive (Inactivo): False(falso)
7. Utilice un número de posición para seleccionar una ubicación para el elemento de menú en el menú View (Vista).

   Le resultará más sencillo elegir un número de posición si ordena los elementos de menú por posición.

8. Ahora puede agregar registros de configuración regional para localizar el título según corresponda.

Recompile la aplicación Siebel. Consulte Recompilar la aplicación de Siebel [página 1069].

## 28.4.2.1 Recompilar la aplicación de Siebel

Al instalar la plataforma de BI y hacer que su comando esté disponible para los usuarios a través de un elemento de menú de Siebel, debe recompilar la aplicación de Siebel mediante los procedimientos normales. Para obtener más información, consulte el manual de Siebel.

Después de recompilar la aplicación Siebel, regenere los archivos JavaScript. En Siebel 7.7 y posterior, es posible regenerar automáticamente los archivos JavaScript como parte del proceso de recopilación.

Dado que los pasos necesarios para compilar el repositorio Siebel se realizan en la estación de trabajo Siebel Tools, debe desplegar los JavaScripts resultantes desde la estación de trabajo Siebel Tools en el servidor Siebel. Normalmente, aunque depende de dónde se ha instalado Siebel, puede encontrar los archivos JavaScript generados en la siguiente ubicación:

```
C:\sea77\tools\PUBLIC\ENU\<srf1096416329_444>
```

El nombre de la carpeta del ejemplo **`<srf1096416329_444>`** se ha generado mediante Siebel Tools y corresponde únicamente al archivo de repositorio resultante.

Los archivos JavaScript deben desplegarse en el servidor Siebel, normalmente en la siguiente ubicación, dependiendo de dónde se ha instalado Siebel:

```
C:\sea77\SWEApp\PUBLIC\ENU\<srf1096416329_444>
```

Asegúrese de no modificar el nombre de carpeta generado con Siebel Tools.

Además, debe actualizar los archivos de configuración Siebel en el servidor Siebel para autorizar el servicio. Localice el archivo de configuración correcto en el servidor Siebel. Por ejemplo, si está ejecutando una versión en inglés del Siebel Call Center (Centro de llamadas Siebel), utilice `uagent.cfg`. De forma predeterminada, el archivo se encuentra en `C:\sea77\siebsrvr\bin\ENU\uagent.cfg` para Siebel 7.7.

Agregue la siguiente línea al final de la sección SWE del archivo de configuración:

```
ClientBusinessService<NUMBER> = BusinessObjects Integration Service
```

Los números de `ClientBusinessService` son consecutivos. Si no hay ningún otro ClientBusinessService en la sección SWE, defina **`<NUMBER>`** como 0. De lo contrario, defina **`<NUMBER>`** como el siguiente valor en orden ascendente.

Para Siebel 8.x o superior:

1. Inicie sesión en Siebel Tools y localice el objeto de aplicación *Siebel Universal Agent* en el Explorador de objetos.
2. Expanda los objetos de aplicación para ver el objeto *Application User Prop*.
3. Cree un nuevo registro para cada servicio empresarial que se declarará, configurando las propiedades Nombre y Valor de cada uno del siguiente modo:
   - Nombre = ClientBusinessServiceX
   - Valor = BusinessObjects Integration

Ahora creará el elemento de menú Crystal Reports que llama al comando Siebel importado.

## 28.4.3 Conocimiento contextual

El Conocimiento contextual es una función que presenta al usuario los informes que probablemente sean pertinentes para desempeñar su tarea actual. En este caso, los usuarios que acceden a Crystal Reports directamente desde una aplicación de cliente de Siebel podrán ver de forma automática los informes que se han asignado a los datos de Siebel incorporados.

### 28.4.3.1 Para configurar el conocimiento contextual

Antes de configurar la sensibilidad al contexto, asegúrese de que ha realizado los siguientes pasos.

- Se ha instalado el producto de integración de Siebel
- Siebel configurado para integrar con la Plataforma de BI

1. Abra la Consola de administración central (CMC).
2. Haga clic en *Autenticación*.
3. Haga doble clic en *Siebel*.
   Aparecerá la interfaz de asignación de Siebel.
4. Haga clic en *Dominios*.
   Aparece la interfaz de asignación de dominio.
5. Escriba el nombre del dominio que se corresponde con el servidor de Siebel que desea utilizar.
6. Cierre la interfaz de asignación de Siebel.
7. Abra la plataforma de lanzamiento de BI.
8. Cree una nueva carpeta bajo `PublicFolders\Siebel` con el mismo nombre que el dominio Siebel en la CMC.
9. Coloque todos los informes diseñados para incorporar información de Siebel en esta carpeta.

### 28.4.3.2 Para especificar la dirección URL para el conocimiento contextual

1. Una vez que haya regenerando los archivos JavaScript de la aplicación, vaya a la carpeta Archivos de Siebel de la instalación de la Plataforma de BI que, de forma predeterminada, se encuentra en `C:\Archivos de programa\Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files\`.
2. Copie el archivo `BusinessObjectsEnterpriseServer.html`. A continuación, localice la carpeta pública en la que el programa genbscript generó los nuevos archivos JavaScript y coloque una copia de `BusinessObjectsEnterpriseServer.html` en la subcarpeta de idioma adecuada.

   Por ejemplo, si ha generado los archivos JavaScript de una aplicación en la carpeta `c:\sea752\SWEApp\PUBLIC\ENU` en el servidor de Siebel, copie el archivo `BusinessObjectsEnterpriseServer.html` en la carpeta `c:\sea752\SWEApp\PUBLIC\ENU`.

3. Abra el archivo `BusinessObjectsEnterpriseServer.html` de la carpeta public en un editor de texto como el Bloc de notas y localice esta línea:

   ```
   Var userDomain = "SIEB78"
   ```

   ```
   var destAddr = "http://<servidor SAP BusinessObjects>:8080/BOE/BI/logon/siebelStart.do"
   ```

> **Nota**
>
> Si modifica la variable `<userDomain>` o `<destAddr>`, debe borrar las páginas Web en caché del navegador para garantizar que el navegador señale a la dirección de destino correcta.

> **Nota**
>
> La variable userDomain distingue entre mayúsculas y minúsculas.

## 28.4.3.3 Para verificar el conocimiento contextual

1. En Herramientas de Siebel, haga clic en *Depurar* > *Inicio*.
2. Desplácese a una pantalla cualquiera y haga clic en el menú *View* (Ver).
   El nuevo elemento de menú de Crystal Reports aparecerá en el menú.
3. Haga clic en el elemento de menú *Crystal Reports*.
   La plataforma de BI abre la ventana plataforma de lanzamiento de BI, que requiere el nombre de usuario y la contraseña para conectarse. Esto solo se requiere la primera vez que se inicia sesión antes del tiempo de espera de la sesión. El nombre de dominio configurado en HTML y la autenticación de Siebel ya deben estar cumplimentados.

> **Nota**
>
> Este paso es sólo para verificar la instalación hasta este punto. No puede iniciar sesión en la plataforma de BI mediante la autenticación de Siebel hasta que haya asignado las responsabilidades de Siebel a la plataforma de BI.

## 28.4.3.4 Agregar carpetas a la Plataforma de BI

La integración de la plataforma de BI para Siebel necesita que se agreguen algunas carpetas a la plataforma de lanzamiento de BI para habilitar completamente la función de conocimiento contextual.

Para que funcione, la carpeta contextual debe tener la estructura siguiente: `Carpetas públicas\Siebel\<Nombre de dominio>`. Como parte de la función de conocimiento contextual, solo aparecerán los informes que estén almacenados en la subcarpeta `<Nombre de dominio>` y que se hayan configurado en el sistema de Siebel para asociarlos con el componente empresarial de BusinessObjects específico. El `<Nombre de dominio>` que se utilice debe ser el mismo nombre de dominio que se ha configurado para Siebel en la configuración de la autenticación y el mismo que el valor configurado en el archivo`BusinessObjectsEnterpriseServer.html` de la parte de Siebel.

> **Nota**
>
> Para completar los pasos de esta sección se requiere Siebel Tools (Herramientas de Siebel).

## 28.4.4 Configurar el inicio de sesión único (SSO) para SAP Crystal Reports y Siebel

De forma predeterminada, la Plataforma de BI se configurará para permitir que los usuarios de SAP Crystal Reports accedan a los datos de SAP mediante el inicio de sesión único (SSO).

### 28.4.4.1 Desactivar el SSO para Siebel y Crystal Reports

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. Seleccione *crdb_siebel*.
5. Haga clic en *Eliminar*.
6. Haga clic en *Guardar y cerrar*.
7. Reinicie SAP Crystal Reports.

### 28.4.4.2 Activar el SSO para Siebel y SAP Crystal Reports

Si ha desactivado el SSO para Siebel y SAP Crystal Reports y desea volver a activarlo.

1. En la consola de administración central (CMC), haga clic en *Aplicaciones*.
2. Haga doble clic en *Configuración de Crystal Reports*.
3. Haga clic en *Opciones de inicio de sesión único*.
4. En *Usar contexto de SSO para inicio de sesión en base de datos...* escriba *crdb_siebel*.
5. Haga clic en *Agregar*.
6. Haga clic en *Guardar y cerrar*.
7. Reinicie los servidores de SAP Crystal Reports.

## 28.4.5 Configuración de la comunicación de Capa de sockets seguros (SSL)

Puede usar el protocolo Nivel de socket seguro (SSL) para todas las comunicaciones de red entre clientes y servidores de los despliegues de Siebel y de la Plataforma de BI.

Como sucede con la configuración SSL de otros servidores y clientes de la Plataforma de BI, almacene la clave y los archivos de certificado siguientes en un directorio seguro al que puedan tener acceso los equipos de su despliegue de Siebel.

- El archivo de certificado de confianza (cacert.der).
- El archivo de certificado de servidor generado (servercert.der).
- El archivo de claves del servidor (server.key).
- El archivo de frase de acceso (passphrase.txt).

### Archivo de propiedades de configuración de SSL

El archivo de propiedades `sslconf.properties` contiene toda la información de los certificados y las claves necesarios que utilizan los componentes de BusinessObjects XI Integration para Siebel. Por ejemplo:

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

El archivo `sslconf.properties` se debe colocar en la carpeta en la que está instalado del producto de la `plataforma de BI, `C:\Archivos de programa (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`, de forma predeterminada.

## 28.4.5.1 Habilitar conectividad de datos Siebel con SSL

> **Nota**
>
> Todos los valores que se describen en el siguiente procedimiento distinguen entre mayúsculas y minúsculas.

1. Copie el certificado SSL en `C:\SSLCert`.
2. Inicie el Administrador de configuración central (CCM).
3. Detenga el Agente de inteligencia de servidor (SIA).
4. Haga doble clic en SIA para abrir el cuadro de diálogo *Propiedades*.
5. Haga clic en la ficha *Protocolo*.
6. Seleccione *Habilitar SSL*.
7. Para la *Carpeta de certificados SSL*, elija el directorio que contiene los certificados SSL: `C:\SSLCert`.
8. Para el *Archivo del certificado SSL del servidor*, seleccione `servercert.der`.
9. Para los *Archivos de certificados de confianza SSL*, seleccione `cacert.der`.
10. Para el *Archivo de clave privada SSL*, seleccione `server.key`.
11. Para el *Archivo de contraseña de clave privada SSL*, seleccione `passphrase.txt`.
12. Haga clic en *Aplicar*.

13. Inicie Server Intelligence Agent.

Debe reiniciar los servidores de generación de informes de la plataforma de BI (como el servidor de tareas de Adaptive) antes de que estos cambios surtan efecto.

# 29 Administrar y configurar registros

## 29.1 Registro de seguimientos para componentes

### Registros

La plataforma de BI genera mensajes de nivel de sistema y los escribe en archivos de registro. Los administradores del sistema pueden usar estos archivos de registro para supervisar el rendimiento o para depurar errores.

### Seguimientos

La plataforma de BI también genera seguimientos (registros de eventos que ocurren durante la operación de un componente controlado) y los recoge en archivos de registro con la extensión `.glf`. El rango de eventos seguidos va de mensajes de estado a errores graves de excepción. El personal y los desarrolladores de soporte SAP pueden usar seguimientos para informar sobre el rendimiento de componentes de la plataforma de BI (servidores y aplicaciones Web) y la actividad de los componentes supervisados.

Al configurar el nivel de registro de seguimiento de un componente, se determina el tipo y la verbosidad de la información enviada al archivo de registro. El nivel de registro de seguimiento es un filtro que elimina seguimientos por debajo de un umbral especificado. Al controlar un registro de seguimiento de componente, puede determinar si la instancia actual de un componente o si su configuración se debe modificar para operar bajo una carga de trabajo aumentada.

> **Nota**
>
> Puede ver archivos de registro de la plataforma de BI usando cualquier editor de textos.

## 29.2 Niveles de registro de seguimiento

Los siguientes niveles de registro de seguimiento están disponibles para los componentes de la plataforma de BI:

| Nivel | Descripción |
|---|---|
| No especificado | El nivel de registro de seguimiento se especifica mediante otros medios (normalmente un archivo `.ini`). |
| Ninguno | No ocurre ningún seguimiento. |

| Nivel | Descripción |
| --- | --- |
| Baja | El filtro de registro de seguimiento permite registrar mensajes de error e ignorar mensajes de advertencia y de estado. Los mensajes de estado importantes se registran para los mensajes de inicio del componente, de cierre, de inicio de la consulta, y de finalización de la consulta. Este nivel no es aconsejable para realizar depuraciones. |
| Medio | El filtro del registro de seguimiento está definido para incluir mensajes de error, de advertencia y la mayoría de los mensajes de estado. Los mensajes de estado no tan importantes o muy detallados están filtrados. Este nivel no incluye suficiente contenido para realizar depuraciones. |
| Alto | Ningún mensaje está filtrado. Este nivel es aconsejable para realizar depuraciones.<br>**⚠ Precaución**<br>Este nivel de registro de seguimiento afecta significativamente los recursos del sistema, incrementa el uso de la CPU y consume espacio de almacenamiento. |

## 29.3 Configurar el seguimiento para los servidores

Un mensaje de registro es un registro permanente de eventos y estado de un sistema de software. Los seguimientos de un despliegue controlado de la plataforma de BI se escriben en un archivo de registro específico `.glf` y se almacenan en el directorio de registro.

- En Windows, la ubicación predeterminada es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\logging`
- En Unix, la ubicación predeterminada es `<DIRINSTALACIÓN>/sap_bobj/logging`

El nombre del archivo de registro `.glf` incluye un identificado breve, el nombre del servidor, y el número de referencia, por ejemplo, `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. Se crea un nuevo archivo de registro para el servidor supervisado cuando el tamaño del archivo de registro se aproxima al umbral de diez megabytes. Además, se actualizan cinco archivos de registro al mismo tiempo. A medida que se crean nuevos archivos de registro, se eliminan los archivos de registro antiguos.

Puede calibrar la severidad e importancia de los seguimientos recopilados en el archivo de registro si se configura el nivel de registro de seguimiento para un servidor específico o un grupo de servidores.

> **ⓘ Nota**
>
> Para modificar los niveles de registro de seguimiento para servidores o grupos de servidores específicos, utilice el Servicio de registro de seguimiento en la Consola de administración central (CMC). Para modificar otros parámetros, cambie manualmente el nivel de registro de seguimiento y otra configuración en el archivo `BO_trace.ini`.

## 29.3.1 Configurar un nivel de registro en la CMC

Puede ajustar el nivel de registro de seguimiento para un servidor sin afectar la configuración de seguimiento.

1. En el área *Servidores* de la CMC, acceda al servidor.
   - Seleccione un servidor desde una categoría específica.
   - Haga clic en *Lista de servidores* del panel de navegación para acceder a la lista completa de servidores, y seleccione un servidor.
2. Haga clic con el botón derecho en el servidor seleccionado y seleccione *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
3. En el área *Servicio de registro de seguimiento*, seleccione la configuración de la lista *Nivel de registro*.
4. Haga clic en *Guardar y cerrar*.

El nuevo nivel de registro de seguimiento surte efecto de forma inmediata.

Para especificar un directorio de salida distinto para archivos de registro, incluya el parámetro `-loggingPath <directorio_destino>` en el área *Parámetros de la línea de comandos*. Reinicie el servidor para que la configuración se aplique.

### Información relacionada

Niveles de registro de seguimiento [página 701]

## 29.3.2 Configurar el nivel de registro para varios servidores en la CMC

1. En el área *Servidores* de la CMC, acceda a varios servidores.
   - Seleccione servidores desde una categoría específica.
   - Haga clic en *Lista de servidores* del panel de navegación para acceder a la lista completa de servidores. Mantenga pulsado `Ctrl` y haga clic en varios servidores para seleccionarlos.
2. Haga clic con el botón derecho en los servidores seleccionados y seleccione *Editar servicios comunes*.
   Aparece el cuadro de diálogo *Editar servicios comunes*.
3. En el área *Servicio de registro de seguimiento*, seleccione la configuración de la lista *Nivel de registro*.
4. Haga clic en *Aceptar*.

El nuevo nivel de registro de seguimiento surte efecto de forma inmediata.

Para especificar un directorio de salida distinto para archivos de registro, incluya el parámetro `-loggingPath <directorio_destino>` en el área *Parámetros de la línea de comandos*. Reinicie el servidor para que la configuración se aplique.

## Información relacionada

Niveles de registro de seguimiento [página 701]

## 29.3.3 Para configurar el seguimiento del servidor mediante el archivo BO_trace.ini

El archivo `BO_trace.ini` solo registra los errores y aserciones de forma predeterminada.

1. Abra el archivo `BO_trace.ini`.
   - En Windows, la ubicación predeterminada es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - En Unix, la ubicación predeterminada es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/conf/`
2. Quite los comentarios de las líneas de la sección «Sintaxis y configuración de seguimiento».
3. Modificar los parámetros de seguimiento del servidor. Los parámetros siguientes se utilizan para configurar el seguimiento del servidor:

| Parámetro | Valores posibles | Descripción |
|---|---|---|
| **`sap_log_level`** | **`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`** | Determina el nivel de gravedad de los mensajes de registro. La gravedad del registro predeterminado es **`log_error`**.<br><br>El registro de severidad sigue una jerarquía, con **`log_information`** al más alto nivel y **`log_none`** al más bajo. Si se establece un nivel de seguridad de registro, se visualizarán todos los mensajes de dicho nivel e inferiores. Por ejemplo, si establece el nivel de gravedad del registro en **`log_warning`**, messages including **`log_warning`**, **`log_error`**, y **`log_fatal`** se escribirán en el archivo de registro.<br><br>**Nota**<br>**`log_information`** y **`log_warning`** se pueden acortar a **`log_info`** y **`log_warn`**. |

| Parámetro | Valores posibles | Descripción |
| --- | --- | --- |
| `sap_trace_level` | `trace_debug` `trace_path` `trace_information` `trace_error` `trace_none` | Determina el nivel de gravedad de los mensajes de seguimiento. La gravedad del seguimiento predeterminado es `trace_error`.<br><br>El seguimiento de gravedad sigue una jerarquía, con `trace_debug` al más alto nivel y `trace_none` al más bajo. Si se establece un nivel de seguridad de seguimiento, se visualizarán todos los mensajes de dicho nivel e inferiores. Por ejemplo, si establece el nivel de gravedad de seguimiento en `trace_path`, los mensajes con `trace_path`, `trace_information`, y `trace_error` se escribirán en el archivo de registro.<br><br>**Nota**<br>`trace_information` se puede acortar como `trace_info`. |

4. Guarde y cierre el archivo `BO_trace.ini`.

El archivo `BO_trace.ini` se lee a menudo. Las modificaciones al archivo `BO_trace.ini` surtirán efecto al cabo de cinco minutos de haberlas guardado. Si reinicia el CMS, las modificaciones al archivo `BO_trace.ini` surtirán efecto inmediatamente.

## Ejemplo

Archivo `BO_trace.ini`

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

## 29.3.3.1 Configurar el seguimiento para un servidor específico

El archivo `BO_trace.ini` especifica parámetros de seguimiento para los servidores de la plataforma de BI. La configuración afecta a todos los servidores administrados. Los administradores pueden usar el archivo `BO_trace.ini` para configurar parámetros se seguimiento específicos para un servidor concreto.

> ⚠ Precaución
>
> La nueva configuración de nivel de registro de seguimiento en la CMC para un servidor específico sobrescribirá cualquier configuración de `BO_trace.ini`.

1. Abra el archivo `BO_trace.ini`.
   - En Windows, la ubicación predeterminada es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - En Unix, la ubicación predeterminada es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/conf/`
2. Use una instrucción `if` para especificar la configuración de seguimiento de un servidor específico. Por ejemplo:

   ```
   if (process == "aps_MySIA.ProcessingServer") {
     sap_log_level=log_warning;
     sap_trace_level=trace_path;
   }
   ```

   > → Sugerencias
   >
   > El proceso se debe especificar para la configuración de seguimiento para aplicar a un servidor específico.

3. Guarde y cierre el archivo `BO_trace.ini`.

La configuración modificada se implementará en cinco minutos.

## 29.4 Configurar el seguimiento para las aplicaciones Web

Los seguimientos de un despliegue controlado de la plataforma de BI se escriben en un archivo de registro específico `.glf` y se almacenan en un directorio en el equipo que aloja la carpeta de aplicaciones Web.

- En Windows, la ubicación predeterminada es `C:\Windows\System32\config\systemprofile\SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>\` For example, `C:\Windows\System32\config\systemprofile\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\`
- En Unix, la ubicación predeterminada es `$userHome/SBOPWebapp_<APLICACIÓN>_<DIRECCIÓN IP>_<PUERTO>/` Por ejemplo, `$userHome/SBOPWebapp_CMC_192.0.2.0_8080/`

De forma predeterminada, el nivel de registro de seguimiento de las aplicaciones Web en la CMC está definido con el valor *No especificado*. La configuración del registro de seguimiento está disponible para las aplicaciones siguientes en la CMC:

- Consola de administración central
- Rampa de lanzamiento de BI
- Abrir documento
- Servicio Web

> **Nota**
>
> Para modificar los niveles de registro de seguimiento para servidores o grupos de servidores específicos, utilice el Servicio de registro de seguimiento en la Consola de administración central (CMC). Para modificar otros parámetros, cambie manualmente el nivel de registro de seguimiento y otra configuración en el archivo `BO_trace.ini`. Este archivo se despliega junto con los archivos `BOE.war` y `dswsbobje.war` en el servidor de aplicaciones Web.

Antes de configurar el archivo `BO_trace.ini`, debe usar la herramienta WDeploy para anular el despliegue de las aplicaciones Web existentes del servidor de aplicaciones Web. Después de configurar `BO_trace.ini`, se debe volver a configurar junto con las aplicaciones Web en el servidor de aplicaciones Web. Para obtener más información sobre el uso de WDeploy para preparar, desplegar y anular el despliegue de las aplicaciones Web, consulte el *Manual de despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.

## 29.4.1 Para definir el nivel de registro de seguimiento de la aplicación Web en la CMC

Para trazar otras aplicaciones web, debe configurar manualmente el archivo `BO_trace.ini` correspondiente.

1. En el área *Aplicaciones* de la CMC, haga clic con el botón derecho en la aplicación y seleccione *Configuración del registro de seguimiento*.

   > **Nota**
   >
   > Estas aplicaciones tienen configuraciones de registro de seguimiento: plataforma de lanzamiento de BI de Fiori, CMC, Open Document, administración de promociones, administración de versiones, diferencia visual, y servicio Web.

   Aparece el cuadro de diálogo *Configuración de registro de seguimiento*.
2. Seleccione la configuración de la lista *Nivel de registro*.
3. Haga clic en *Guardar y cerrar*.
4. Reinicie el servidor de aplicaciones Web.

El nuevo nivel de registro de seguimiento entrará en vigor después del siguiente inicio de sesión en la aplicación Web.

### Información relacionada

Niveles de registro de seguimiento [página 701]

## 29.4.2 Para configurar el seguimiento del servidor mediante el archivo `BO_trace.ini`

El archivo `BO_trace.ini` se despliega con los archivos `BOE` y `dswsbobje .war` en el servidor de aplicaciones Web. Puede usar `BO_trace.ini` para especificar parámetros de seguimiento para las aplicaciones Web de la plataforma de BI. Debido a que este archivo no siempre es accesible, debe anular el despliegue de la aplicación Web afectada desde el servidor de aplicaciones Web.

1. Use WDeploy para anular el despliegue de la aplicación Web desde el servidor de aplicaciones Web. Para obtener más información sobre el uso de WDeploy para deshacer el despliegue de las aplicaciones Web, consulte el *Manual de despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.
   - Si utiliza el servidor de aplicaciones Web Tomcat proporcionado con la instalación plataforma de BI, no es necesario no desplegar las aplicaciones Web. Puede modificar los archivos directamente.
     - El archivo de configuración de seguimiento para el archivo `BOE.war` está disponible en `<DIRINSTALACIÓN>\Tomcat\webapps\BOE\WEB-INF\TraceLog`
     - El archivo de configuración de seguimiento para el archivo `dswsbobje.war` está disponible en `<DIRINSTALACIÓN>\Tomcat\webapps\dswsbobje\WEB-INF\conf`

   > **Nota**
   >
   > Si utiliza el servidor de aplicaciones Web Tomcat en paquete, sáltese el paso 2.

2. Acceda a una versión desplegada anteriormente del archivo `BO_trace.ini`:
   - La ubicación predeterminada de una versión desplegada previamente del archivo de configuración para el archivo `BOE.war` es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
   - La ubicación predeterminada de una versión desplegada previamente del archivo de configuración para el archivo `dswsbobje.war` es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
3. Abra el archivo `BO_trace.ini`.
   - En Windows, la ubicación predeterminada es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - En Unix, la ubicación predeterminada es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/conf/`
4. Modificar los parámetros de seguimiento del servidor. Los parámetros siguientes se utilizan para configurar el seguimiento del servidor:

| Parámetro | Valores posibles | Descripción |
|---|---|---|
| **`sap_log_level`** | **`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`** | Determina el nivel de gravedad de los mensajes de registro. La gravedad del registro predeterminado es **`log_error`**.<br><br>El registro de severidad sigue una jerarquía, con **`log_information`** |

| Parámetro | Valores posibles | Descripción |
| --- | --- | --- |
| | | al más alto nivel y **log_none** al más bajo. Si se establece un nivel de seguridad de registro, se visualizarán todos los mensajes de dicho nivel e inferiores. Por ejemplo, si establece el nivel de gravedad del registro en **log_warning**, messages including **log_warning**, **log_error**, y **log_fatal** se escribirán en el archivo de registro.<br><br>ⓘ Nota<br>**log_information** y **log_warning** se pueden acortar a **log_info** y **log_warn**. |
| **sap_trace_level** | **trace_debug** **trace_path** **trace_information** **trace_error** **trace_none** | Determina el nivel de gravedad de los mensajes de seguimiento. La gravedad del seguimiento predeterminado es **trace_error**.<br><br>El seguimiento de gravedad sigue una jerarquía, con **trace_debug** al más alto nivel y **trace_none** al más bajo. Si se establece un nivel de seguridad de seguimiento, se visualizarán todos los mensajes de dicho nivel e inferiores. Por ejemplo, si establece el nivel de gravedad de seguimiento en **trace_path**, messages including **trace_path**, **trace_info**, y **trace_error** se escribirán en el archivo de registro.<br><br>ⓘ Nota<br>**trace_information** se puede acortar como **trace_info**. |

5. Guarde y cierre el archivo `BO_trace.ini`.
6. Use WDeploy para desplegar el archivo `.war` en el equipo que aloja el servidor de aplicaciones Web.

La configuración de seguimiento modificada tiene efecto después del siguiente inicio de sesión en la aplicación Web.

## 29.4.2.1 Configurar el seguimiento para una aplicación Web específica

El archivo `BO_trace.ini` se despliega junto con los archivos `BOE` y `dswsbobje .war` en el servidor de aplicaciones Web. Puede usar `BO_trace.ini` para especificar parámetros de seguimiento para las aplicaciones Web de la plataforma de BI. Debido a que este archivo no siempre es accesible, debe anular el despliegue de la aplicación Web afectada desde el servidor de aplicaciones Web. Las siguientes son aplicaciones Web y los archivos `.war` asociados a las mismas:

| Aplicación web | Archivo WAR | Ubicación previa al despliegue |
|---|---|---|
| Consola de administración central | `BOE.war` | `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog` |
| Plataforma de lanzamiento de BI | `BOE.war` | `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog` |
| Abrir documento | `BOE.war` | `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog` |
| Servicio Web | `dswsbobje.war` | `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf` |

1. Use WDeploy para anular el despliegue de la aplicación Web desde el servidor de aplicaciones Web. Para obtener más información sobre el uso de WDeploy para deshacer el despliegue de las aplicaciones Web, consulte el *Manual de despliegue de aplicaciones Web de la plataforma SAP BusinessObjects Business Intelligence*.
   - Si utiliza el servidor de aplicaciones Web Tomcat proporcionado con la instalación plataforma de BI, no es necesario no desplegar las aplicaciones Web. Puede modificar el archivo directamente.
     - El archivo de configuración de seguimiento para el archivo `BOE.war` está disponible en `<DIRINSTALACIÓN>\Tomcat\webapps\BOE\WEB-INF\TraceLog`
     - El archivo de configuración de seguimiento para el archivo `dswsbobje.war` está disponible en `<DIRINSTALACIÓN>\Tomcat\webapps\dswsbobje\WEB-INF\conf`

   > **Nota**
   >
   > Si utiliza el servidor de aplicaciones Web Tomcat en paquete, sáltese el paso 2.

2. Acceda a una versión desplegada anteriormente del archivo `BO_trace.ini`:

- La ubicación predeterminada de una versión desplegada previamente del archivo de configuración para el archivo `BOE.war` es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
- La ubicación predeterminada de una versión desplegada previamente del archivo de configuración para el archivo `dswsbobje.war` es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`

3. Abra el archivo `BO_trace.ini`.
   - En Windows, la ubicación predeterminada es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - En Unix, la ubicación predeterminada es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/conf/`
4. Use una instrucción `if` para especificar la configuración de seguimiento de una aplicación Web específica. Por ejemplo:

```
if (device_name == "Webapp_opendocument_trace") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

El proceso se debe especificar para la configuración de seguimiento para aplicar a un servidor de aplicaciones Web. Las siguientes aplicaciones Web están disponibles después de la instalación inicial:

| Aplicación Web | Nombre de dispositivo |
|---|---|
| Plataforma de lanzamiento de BI | **`WebApp_BIlaunchpad`** |
| Servidor de administración central | **`WebApp_CMC`** |
| OpenDocument | **`WebApp_OpenDocument`** |

Los parámetros siguientes se utilizan para configurar el seguimiento del servidor de aplicaciones Web:

| Parámetro | Valores posibles | Descripción |
|---|---|---|
| **`sap_log_level`** | **`log_information`** **`log_warning`** **`log_error`** **`log_fatal`** **`log_none`** | Determina el nivel de gravedad de los mensajes de registro. La gravedad del registro predeterminado es **`log_error`**.<br><br>El registro de severidad sigue una jerarquía, con **`log_information`** al más alto nivel y **`log_none`** al más bajo. Si se establece un nivel de seguridad de registro, se visualizarán todos los mensajes de dicho nivel e inferiores. Por ejemplo, si establece el nivel de gravedad del registro en **`log_warning`**, los mensajes con **`log_warning`**, **`log_error`**, y **`log_fatal`** se escribirán en el archivo de registro. |

| Parámetro | Valores posibles | Descripción |
| --- | --- | --- |
| | | **Nota**<br>`log_information` y `log_warning` se pueden acortar a `log_info` y `log_warn`. |
| `sap_trace_level` | `trace_debug` `trace_path` `trace_information` `trace_error` `trace_none` | Determina el nivel de gravedad de los mensajes de seguimiento. La gravedad del seguimiento predeterminado es `trace_error`.<br>El seguimiento de gravedad sigue una jerarquía, con `trace_debug` al más alto nivel y `trace_none` al más bajo. Si se establece un nivel de seguridad de seguimiento, se visualizarán todos los mensajes de dicho nivel e inferiores. Por ejemplo, si establece el nivel de gravedad de seguimiento en `trace_path`, messages including `trace_path`, `trace_info`, y `trace_error` se escribirán en el archivo de registro.<br>**Nota**<br>`trace_information` se puede acortar como `trace_info`. |

5. Guarde y cierre el archivo `BO_trace.ini`.
6. Use WDeploy para desplegar el archivo `.war` en el equipo que aloja el servidor de aplicaciones Web.

## 29.5 Configurar el seguimiento para las aplicaciones de cliente de la plataforma de BI

El seguimiento se puede activar en los clientes siguientes:

- Herramienta de diseño de universos
- Herramienta de diseño de información
- Cliente enriquecido de Web Intelligence

Puede configurar el seguimiento para estos componentes editando los archivos .ini para cada uno de los tipos de clientes. Estos archivos .ini funcionan igual que el archivo BO_trace.ini descrito en otra parte de este

capítulo. Consulte en Para configurar el seguimiento del servidor mediante el archivo BO_trace.ini [página 1078] información detallada sobre cómo modificar el archivo .ini.

Los archivos se deben ubicar en los directorios de funcionamiento configurados para estas aplicaciones (`<DIRINSTAL>\SAP BusinessObjects` de forma predeterminada). Si no existen, es probable que deba crearlos. Los archivos tienen los nombres siguientes:

- Herramienta de diseño de universos: `designer_trace.ini`.
- Herramienta de diseño de información: `BO_Trace.ini`
- Cliente enriquecido de Web Intelligence: `WebIRichClient_trace.ini`

Consulte la documentación de estos productos para obtener más información.

## 29.6 Configuración del seguimiento de mensajes de error ampliado

Para algunas aplicaciones, por ejemplo SAP BusinessObjects Web Intelligence, puede activar el seguimiento para generar archivos de log que contengan información ampliada sobre cualquier mensaje de error que emita la aplicación.

> **Nota**
>
> Estos archivos de log están diseñados para que los técnicos de SAP Support los utilicen. El formato de archivo de log es JSON.

Activa los archivos de log de la información ampliada del mensaje de error modificando el siguiente archivo en la instalación de SAP BusinessObjects BI: `extended_info.properties`.

## 29.7 Para habilitar los archivos de registro de información de ampliación de mensajes de error

Desea obtener información ampliada sobre los mensajes de error que emite una aplicación. Para ello, debe habilitar los archivos de registro de información de ampliación de mensajes de error.

> **Nota**
>
> En SAP BusinessObjects BI Suite versión 4.2 SP5, esta funcionalidad solo es compatible con SAP BusinessObjects Web Intelligence.

1. Abra el siguiente archivo en su instalación de SAP BusinessObjects BI: `extended_info.properties`.

   La ubicación predeterminada es:
   - En Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`
   - En UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`

2. Defina los parámetros según proceda:

| Parámetro | Valores posibles | Descripción |
|---|---|---|
| `output.format` | • Json<br>• ninguno | Controla el formato de los archivos generados.<br>**Nota**<br>Si define este formato como ninguno, no se genera ningún archivo. |
| `output.size` | `<size><unit>`, donde `<size>` es un entero positivo y `<unit>` es "g" para gigabytes o "m para megabytes.<br>**Nota**<br>La unidad predeterminada es kilobytes. | El tamaño total de todos los archivos que puede generar una aplicación. Cuando se supera el tamaño, se eliminan los archivos antiguos. |

Los archivos de registro se generan en la misma carpeta que los archivos trace. La ubicación predeterminada es:

- En Windows: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging\`
- En UNIX: `<INSTALLDIR>/sap_bobj/logging/`

El nombre de los archivos es `<nombre_aplicación>_<id_error>_exinfo.<formato>`

El nombre de la aplicación es el nombre de la aplicación que emitió el error. El ID de error se genera de forma aleatoria. El formato de archivo es el formato especificado en el archivo de configuración.

> **Nota**
> La única extensión de archivo posible es `.json`

Se genera un archivo de registro independiente para cada mensaje emitido por la aplicación especificada.

# 30 Integración en SAP Solution Manager

## 30.1 Información general de la integración

La funciones de compatibilidad se han agregado a la plataforma de BI para habilitar la integración en SAP Solution Manager. Los siguientes componentes de SAP Solution Manager™ se pueden usar para proporcionar compatibilidad para el despliegue de la Plataforma de BI:

- Directorio horizontal de soluciones
- Solution Manager Diagnostics
- Introscope por CA Wily
- SAP Passport

> **Nota**
>
> Para acceder a SAP Support Portal para SAP BusinessObjects, vaya a: https://support.sap.com/home.html

## 30.2 Lista de comprobación de la integración de SAP Solution Manager

La siguiente tabla resume los componentes necesarios para habilitar SAP Solution Manager para que proporcione compatibilidad para la plataforma de BI.

| Soporte de SAP Solution Manager | Necesario para la plataforma de BI |
|---|---|
| registro SLD | • SAPHOSTAGENT debe estar instalado para habilitar el registro de los servidores de la Plataforma de BI.<br>**Nota**<br>La plataforma de BI registrará automáticamente los servidores si SAPHOSTAGENT ya está instalado.<br>• Debe crear un archivo connect.key para el proveedor de datos que informa de los servidores back-end.<br>• (Opcional) Para el registro de SLD con WebSphere 6.1 o 7, la herramienta de registro SLDREG debe estar instalada en cada servidor de aplicaciones Web de WebSphere. Para obtener más información, consulte la Nota SAP 1482727.<br>• (Opcional) Para el registro de SLD con SAP NetWeaver 7.2, instale SLDREG en todos los hosts de NetWeaver. Consulte la documentación de SAP 1018839 para obtener más información.<br>• (Opcional) para el registro de SLD con Apache Tomcat, se debe instalar SLDREG en cada servidor de Tomcat. Para obtener más información, consulte la Nota de SAP 1508421. |
| Integración SMD | • Debe descargar e instalar el agente SMD (DIAGNOSTICS.AGENT) en todos los host de los servidores de la Plataforma de BI.<br>• La cuenta de usuario SMAdmin debe estar habilitada en la plataforma de BI. |
| Instrumentación del rendimiento | • El agente de Introscope se debe configurar para conectarse a Enterprise Manager. Use el instalador de la Plataforma de BI o los marcadores de posición del nodo de la CMC para configurar las conexiones.<br>• El agente SMD debe estar instalado.<br>• La plataforma de BI debe estar configurada para conectarse al agente SMD. Use el instalador de la Plataforma de BI o los marcadores de posición del nodo de la CMC para configurar las conexiones. |
| SAP Passport | • Debe descargar e instalar la herramienta cliente SAP Passport. |

## 30.3 Administrar el registro del directorio horizontal del sistema

### 30.3.1 Registro de la plataforma de BI en la infraestructura horizontal del sistema

El directorio horizontal del sistema (SLD) es un repositorio central de información horizontal del sistema que es importante para la administración del ciclo de vida del software. El SLD contiene una descripción de la arquitectura del sistema, los componentes del sistema y software que ya están instalados. Los proveedores de datos SLD registran el sistema en el servidor SLD y mantiene la información actualizada. La aplicaciones de administración y empresariales acceden a la información almacenada en el SLD para realizar tareas en un entorno de cálculo colaborativo.

El proveedor de datos del directorio horizontal del sistema (SLD-DS) es la aplicación responsable de registrar los servidores de la Plataforma de BI en el servidor SLS. Se proporciona un proveedor de datos específico para cada instalación de la plataforma para generar informes de los siguientes componentes:

- Servidores de la Plataforma de BI
- Aplicaciones y servicios Web alojados en el servidor de aplicaciones Web de WebSphere.

> **Nota**
>
> SAP NetWeaver tiene un proveedor SLD-DS incrustado que registra el servidor de aplicaciones de NetWeaver, así como aplicaciones y servidores Web alojados. Este SLD-DS es importante para los despliegues de la Plataforma de BI integrados dentro de un entorno SAP NetWeaver.

El SLD-DS que informa sobre los servidores de la Plataforma de BI necesita que el programa SLDREG esté instalado y configurado. El programa SLDREG se instala al instalar la herramienta SAPHOSTAGENT. Para obtener más información sobre cómo acceder e instalar SAPHOSTAGENT, consulte la sección Preparación del *Manual de instalación de la plataforma SAP BusinessObjects Business Intelligence*. Una vez instalado SLDREG, debe crear un archivo `connect.key` para permitir que se conecte al servidor SLD.

Para obtener información sobre cómo configurar el proveedor de datos específico para WebSphere, consulte el *Manual del despliegue de aplicaciones Web*.

Durante la instalación de la plataforma de BI, la información necesaria para registrar la plataforma de BI se almacena en un archivo de configuración. Este archivo contiene información que usa el SLD DS para conectarse a la base de datos de la Plataforma de BI.

### 30.3.1.1 Crear un archivo de connect.key para el proveedor de datos SLD

Antes de crear un archivo `connect.key` para el proveedor de datos SLD, debe descargar e instalar SAPHOSTAGENT. Consulte la sección Preparación del *Manual de instalación de la plataforma SAP BusinessObjects Business Intelligence* para obtener más detalles.

> **Nota**
>
> El archivo `connect.key` es necesario para el registro de SLD con el proveedor de datos que informa sobre los servidores de la Plataforma de BI.

1. Abra una consola de línea de comandos.
2. Desplácese a la ruta de instalación SAPHOSTAGENT predeterminada.
   - En Windows: `Archivos de programa\SAP\hostctrl\exe`
   - En Unix: `/usr/sap/hostctrl/exe`
3. Ejecute el siguiente comando:

   ```
   sldreg -configure connect.key
   ```
4. Introduzca los siguientes detalles de configuración
   - Nombre del usuario
   - Contraseña

- Host
- Número de puerto
- Especifique para usar HTTP

La herramienta `sldreg` creará un archivo connect.key que el proveedor de datos usará automáticamente para llevar la información al servidor de SLD.

## 30.3.2 ¿Cuándo se desencadena el registro de SLD?

El proveedor de datos invoca el proceso de registro de SLD que informa de los servidores back-end de la Plataforma de BI en los siguientes escenarios:

- Se reinicia un nodo del servidor en el despliegue de la Plataforma de BI.
- Se agrega un nuevo servidor o nodo al despliegue.
- Se elimina un servidor o nodo

> **Nota**
>
> Su un servidor o nodo se elimina, el proceso de registro de SLD no modifica los contenidos en el servidor SLD. Para actualizar el servidor SLD si un servidor o nodo está eliminado, elimine el sistema desde SLD y vuelva a enviarlo reiniciando la plataforma de BI.

El proveedor de datos para el registro SLD de WebSphere se puede invocar manualmente o configurar para que se ejecute en un intervalo especificado, por ejemplo, cada 24 horas. para obtener más información acerca de la configuración de este proveedor de datos, consulte la Nota de SAP 482727.

## 30.3.3 Limpieza SLD antes de instalaciones de patch

Los datos de versiones anteriores de la plataforma de BI se acumulan en el servidor SLD tras la instalación del patch y dificultan el diagnóstico del producto con SAP Solution Manager. Para evitar este problema, siga los pasos mencionados antes en la máquina base antes de iniciar una instalación de patch:

> **Nota**
>
> La función está disponible para la versión 4.2 SP3 y versiones superiores.

1. Vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
2. Ejecute el archivo de lote bobjsldds.bat con parámetros clean (`-clean`).

   > **Nota**
   >
   > El sistema crea un archivo xml con parámetros predefinidos que se introduce en el servidor SLD para limpieza. La limpieza se refleja tras reinicializar SIA.

## 30.3.4 Iniciar sesión en la conectividad SLD

### Archivo de configuración del proveedor de datos

Un archivo de configuración que se usa para el registro de SLD se crea para los despliegues de la Plataforma de BI. El archivo, `sldparserconfig.properties`, se encuentra en el siguiente directorio: `<DIRINSTALACIÓN>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.

### Iniciar sesión en la conectividad SLD

La conectividad entre el servidor SLD y el proveedor de datos en el despliegue de la Plataforma de BI se controla a través de la herramienta `sldreg` y el archivo `connect.key`.

> **Nota**
>
> El nombre del archivo de registro se especifica como una propiedad en el archivo `sldparserconfig.properties`.

El archivo de registro para el proveedor de datos SLD que informa de los servidores back-end de la Plataforma de BI se encuentra, de forma predeterminada, en la siguiente ubicación: `<DIRINSTALACIÓN>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`. El archivo se sobrescribe cada vez que el proveedor de datos se ejecuta.

Los archivos de registro para `sldreg` se encuentran, de forma predeterminada, en la siguiente ubicación: `<DIRINSTALACIÓN>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. Los nombres del archivo de registro sldreg no se puede modificar y usa el siguiente formato: `sldreg_<<Timestamp>>.log`.

Se crea un nuevo archivo de registro cada vez que el proveedor de datos llama a sldreg.

## 30.3.5 Nombre de host virtual

Cuando se reinicia el *agente de inteligencia de servidor*, un fichero de datos de proveedor se genera para cada nodo. El archivo se alimenta en el System Landscape Directory y posteriormente,utilizados por SAP Solution Manager. En la plataforma de business Intelligence 4.2 Support package 4 y anterior, el nombre de host físico se ha agregado al fichero de proveedor de datos. En la plataforma Business Intelligence 4.2 Support package 5 puede definir un nombre de host virtual en el fichero *sldparserconfig.properties* para asegurar que el fichero de proveedor de datos consume el nombre de host virtual.

> **Nota**
>
> Por defecto, el fichero de proveedor de datos toma el nombre de host física si el fichero «sldparserconfig.properties» no contiene ningún nombre de host virtual.

Siga los pasos siguientes para añadir el nombre de host virtual en sldparserconfig.properties:

1. Vaya a `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
2. Edite el fichero sldparserconfig.properties.
3. Agregue los parámetros siguientes: `virtualHostName = <Virtual Hostname>`.
4. Guarde el archivo.
5. Reinicie el *agente de inteligencia de servidor* para asegurar las modificaciones las consumen el fichero de proveedor de datos.

> **Nota**
>
> Las modificaciones también se pueden consumir ejecutando el comando dado abajo:
>
> En Windows: `runbobjsldds.bat -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` at `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bobj-sld-ds`.
>
> En Unix: `runbobjsldds.sh -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>` at `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bobj-sld-ds`.

## 30.4 Administrar agentes de Solution Management Diagnostics

### 30.4.1 Información general de Solution Manager Diagnostics (SMD)

El componente Solution Manager Diagnostics (SMD) de un SAP Solution Manager proporciona todas las funcionalidades para analizar y supervisar de forma central una arquitectura horizontal del sistema completa: El servidor SMD puede supervisar la plataforma de BI si está instalado el agente SMD. El agente SMD (`DIAGNOSTICS.AGENT`) recopila información para el SMD que se puede usar para el análisis de la causa raíz. La información recopilada y enviada al servidor SMD incluye configuraciones del servidor back-end y la ubicación de los archivos de registro.

### 30.4.2 Trabajar con agentes SMD

La plataforma de BI no instala el agente SMD. El agente, `DIAGNOSTICS.AGENT`, está disponible para la descarga desde la siguiente ubicación: https://support.sap.com/swdc.

La información sobre la instalación y configuración del agente está disponible en: http://service.sap.com/diagnostics

### Directrices para trabajar con el agente SMD

A continuación se proporcionan directrices para el uso con el agentes SMD para supervisar la plataforma de BI:

- El orden de instalación del sistema supervisado y el agente no es importante. Puede seleccionar instalar el agente SMD antes o después de instalar y desplegar la plataforma de BI.
- Al instalar un agente SMD, tome nota del nombre de host y el puerto de escucha. Son importantes para la configuración de la plataforma de BI como un sistema supervisado. Si ha instalado el agente antes que el sistema supervisado, puede proporcionar la información de configuración durante la configuración de la instalación de la Plataforma de BI. Esta información también se puede proporcionar más tarde a través de los marcadores de posición en la Consola de administración central del despliegue.
- Si los servidores back-end se despliegan en un sistema distribuido, debe instalar un agente SMD en cada equipo que alije un servidor back-end.
- Para obtener la instrumentación del rendimiento para servidores que no sean de Java, es necesario el agente SMD.
- Debe activar la cuenta de usuario SMAdmin para habilitar el acceso del servidor SMD al CMS.

## 30.4.3 Cuenta de usuario SMAdmin

Cada despliegue de la Plataforma de BI dispone de una cuenta de usuario creada para facilitar la integración SMD. El servidor SMD usa esta cuenta de sólo lectura para iniciar sesión en el CMS y para recopilar la configuración del servidor y otra información acerca del despliegue.

La cuenta SMAdmin está desactivada de forma predeterminada.

### 30.4.3.1 Activar la cuenta SMAdmin

1. En el área de administración *Usuarios y grupos* de la CMC, seleccione *Lista de usuarios*.
   Aparece la lista de usuarios.
2. Localice la cuenta de usuario *SMAdmin*.
3. Haga clic en *Administrar* > *Propiedades*.
   Aparece el cuadro de diálogo *Propiedades*.
4. Desactive el cuadro *La cuenta está desactivada*.
5. Haga clic en *Guardar y cerrar*.

## 30.5 Administrar la instrumentación del rendimiento

### 30.5.1 Instrumentación del rendimiento para la plataforma de BI

Puede usar CA Wily Introscope como parte de SAP Solution Manager para medir la instrumentación del rendimiento de la Plataforma de BI. Al instalar la plataforma, se proporcionan los siguientes recursos para el despliegue

- Agente de Introscope: los agentes de Introscope recopilan las métricas del rendimiento desde los servidores back-end Java de la Plataforma de BI. Los agentes también recopilan información desde el entorno de cálculo. Los agentes informan de estas métricas a Enterprise Manager.
- Los archivos proporcionados para facilitar el proceso de instrumentación. Se proporciona un conjunto de archivos para la instrumentación de servidores que no sean Java y otro conjunto de archivos para la instrumentación de servidores Java. Al final de SAP Solution Manager, es necesario el componente Enterprise Manager (EM). EM actúa como el repositorio central para todos los datos y métricas de rendimiento de Introscope recopiladas en un entorno de aplicaciones. El EM procesa los datos de rendimiento y los hace disponibles para los usuarios para la supervisión y diagnóstico de la producción.

### 30.5.2 Configurar la instrumentación del rendimiento para la plataforma de BI

Existen dos modos de configurar la instrumentación del rendimiento para los flujos de trabajo que se ejecutan en servidores back-end de la Plataforma de BI.

1. Durante la configuración de la instalación de la plataforma de BI. Deberá conocer el nombre de host y el puerto de escucha para el agente SMD. Para obtener más información, consulte el *Manual de instalación de la plataforma SAP BusinessObjects Business Intelligence*. Si selecciona esta opción, la instrumentación se ejecutará de forma predeterminada cuando haya finalizado el despliegue del sistema supervisado.
2. Después de instalar la plataforma de BI, puede proporcionar la información de configuración para el agente SMD a través de marcadores de posición en las propiedades del nodo de la Consola de administración central (CMC).

> **Nota**
>
> Para obtener la instrumentación para los flujos de trabajo de servidores que no son Java, debe tener instalado el agente de SMD (`DIAGNOSTICS.AGENT`).

#### Información relacionada

Trabajar con agentes SMD [página 1094]

### 30.5.2.1 Configurar nodos para la instrumentación

Use las siguientes instrucciones si no proporcionó la información de configuración para el agente SMD y el administrador de Enterprise durante la configuración de la instalación para la plataforma de BI.

1. Vaya al área *Servidores* en la CMC.
2. En el panel de navegación, haga clic en *Nodos*.
   Se muestran todos los nodos disponibles.
3. Haga clic con el botón derecho en el nodo en el que desea realizar la instrumentación y seleccione *Marcadores de posición*.
   Aparece el cuadro de diálogo Marcadores de posición.
4. Modifique el valor para los siguientes marcadores de posición.

| Marcador de posición | Descripción |
|---|---|
| %IntroscopeAgentEnableInstrumentation% | Habilita o deshabilita la instrumentación en servidores Java. Se establecerá en habilitado so ha proporcionado detalles de configuración para Enterprise Manager durante la configuración de la instalación. Configúrelo en `true` para habilitar la instrumentación. |
| %IntroscopeAgentEnterpriseManagerHost% | Nombre de host para el equipo en el que está instalado Enterprise Manager. |
| %IntroscopeAgentEnterpriseManagerPort% | Puerto de escucha que usa Enterprise Manager. |
| %IntroscopeAgentEnterpriseManagerTransport% | Protocolo de comunicación que usa Enterprise Manager. Los protocolos admitidos incluyen TCP, SSL, HTTP Tunnel y HTTPS. |
| %NCSInstrumentLevelThreshold% | Se usa para configurar el nivel de instrumentación para servidores que no sean Java. Configúrelo en «0» si desea desactivar la instrumentación. Seleccione cualquier valor por encima de «0» para activar la instrumentación. |
| %SMDAgentHost% | El nombre de host del equipo en el que está instalado el agente SMD (`DIAGNOSTICS.AGENT`). |
| %SMDAgentPort% | El puerto de escucha que usa el agente SMD. |

5. Haga clic en *Guardar y cerrar*.
6. Reinicie el nodo.

Después de reiniciar el nodo, los nuevos valores proporcionados se propagarán a todos los servidores administrados.

## 30.5.3 Instrumentación del rendimientos para el nivel Web

Los datos de instrumentación para los componentes de nivel Web no se incluyen en la plataforma de BI.

## 30.5.4 Archivos de registro de instrumentación

Una vez configurado el despliegue de la Plataforma de BI para ejecutar la instrumentación, se registran los mensajes en ubicaciones específicas. Comprobar los archivos de registro es un modo de verificar el estado de la instrumentación.

Para obtener la instrumentación de los servidores back-end Java, se ubica un archivo de registro en el siguiente directorio: `<DIRINSTALACIÓN>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs` . Se crea una archivo `.log` independiente para cada proceso Java. La carpeta también contiene archivos `AutoProbe.log` que especifican los métodos que se han cargado para la instrumentación.

Para obtener la instrumentación de servidores back-end que no son Java, los archivos de registro se ubican en el siguiente directorio: `<DIRINSTALACIÓN>/SAP BusinessObjects Enterprise XI 4.0/logging/`. En Unix, los archivos se encuentran en el directorio `<sap_bobj>\logging\`. Los archivos de registro relacionados con la instrumentación para servidores que no sean Java se guardan como archivos `.trc`.

Para obtener la instrumentación en servidores de aplicaciones Web, se ubica un archivo de registro en el siguiente directorio: `<DIRINSTALACIÓN>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs`. Aparecen dos tipos de archivos de registro en esta carpeta: `Introscope.log` y `Autoprobe.log`.

# 30.6 Seguimiento con SAP Passport

Además del seguimiento de los componentes de la Plataforma de BI, como servidores y aplicaciones Web, el mecanismo de seguimiento admite el seguimiento de una acción específica. Un análisis de seguimiento de principio a fin analiza el rendimiento de una única transacción. La consolidación de toda la información de seguimiento para una acción específica permite al personal se soporte técnico de SAP ver todos los datos de seguimiento sin que se distraigan por la información de seguimiento de otras acciones.

Para obtener más información, visite1861180.

## SAP Passport

El mecanismo que admite el seguimiento back-end para la plataforma de BI es una herramienta denominada SAP Passport™. La herramienta cliente SAP Passport inyecta un identificador único en todas las solicitudes HTTP para un flujo de trabajo concreto, y dicho identificador se reenvía a todos los servidores que se usan en el flujo de trabajo. El personal de soporte técnico de SAP puede unir un seguimiento de principio a fin para el flujo de trabajo con el uso de este identificador único.

> **Nota**
>
> Los niveles de registro de seguimiento especificados en la CMC y el archivo de configuración `BO_trace.ini` se usan si son superiores que los niveles especificados en la herramienta cliente de SAP Passport, `SAPClientPlugin.exe`.

Puede encontrar Passport en los registros para los servidores back-end, aplicaciones Web y registros de servicios Web.

La herramienta cliente SAP Passport no se instala como parte de la plataforma de BI. Para acceder y descargar la herramienta, vaya a https://support.sap.com/swdc.

# 31 Administración de líneas de comandos

## 31.1 Scripts de Unix

En esta sección se ofrece información detallada de las herramientas administrativas y scripts que se incluyen en la distribución Unix de la plataforma de BI. Esta sección se proporciona principalmente como referencia. Los conceptos y los procedimientos de configuración se describen más detalladamente en este manual.

> **Nota**
>
> Solo el usuario que ha instalado la plataforma de BI tiene los derechos para ejecutar los shell scripts en la plataforma de BI.

La distribución de Unix de la plataforma de BI incluye una serie de scripts que, juntos, proporcionan todas las opciones de configuración disponibles en la versión Windows del Administrador de configuración central (CCM). Hay otras secuencias de comandos que proporcionan opciones específicas de Unix o sirven de plantillas para sus propias secuencias de comandos. Además, existen otras secuencias de comandos secundarias que usa la plataforma de BI. Cada secuencia de comandos se describe a continuación y se indican las opciones de línea de comandos donde sea aplicable:

> **Nota**
>
> Al introducir parámetros de línea de comandos Unix, debe omitir o multiplicar caracteres shell especiales de escape. Por ejemplo, si se utiliza el signo de exclamación «!» en una contraseña, debe omitir el signo de exclamación de la forma siguiente: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

### 31.1.1 Utilidades de secuencia de comandos

En esta sección se describen las secuencias de comandos administrativas que sirven de ayuda para trabajar con la plataforma de BI en UNIX. En el resto de esta sección se describen los conceptos de las tareas que puede realizar con estos scripts. En esta sección de referencia se proporcionan las principales opciones de línea de comandos y sus argumentos.

#### 31.1.1.1 ccm.sh

La secuencia de comandos `ccm.sh` se instala en el directorio `<DIRINSTALACIÓN>/sap_bobj>` de la instalación. Esta secuencia de comandos proporciona una versión de línea de comandos del Administrador de configuración central. En esta sección se enumeran las opciones de línea de comandos y se proporcionan ejemplos.

> **Nota**
>
> Los argumentos entre corchetes [ ] son opcionales.

> **Nota**
>
> Si no está seguro del nombre de Server Intelligence Agent, consulte las propiedades del comando del archivo `ccm.config` y use el valor que aparece después de la opción `-name`.

> **Nota**
>
> La secuencia de comandos `ccm.sh` solo puede iniciarla el usuario que realizó la instalación de la plataforma de BI.

- Los argumentos indicados mediante **`<otra información de autenticación>`** se proporcionan en la segunda tabla.

| Opción de CCM | Argumentos válidos | Descripción |
|---|---|---|
| `-help` | n/d | Mostrar la ayuda de la línea de comandos. |
| `-start` | `all` o **`<sianame>`** | Iniciar cada Server Intelligence Agent como un proceso. La opción `all` inicia todos los nodos del equipo, incluyendo los nodos que pertenecen a clústeres distintos. |
| `-stop` | `all` o **`<sianame>`** | Detenga todos Server Intelligence Agents finalizando su ID de proceso correspondiente. La opción `all`inicia todos los nodos en la máquina, incluyendo cualquier nodo que pertenezca a clusters diferentes. |
| `-restart` | `all` o **`<sianame >`** | Detener cada Server Intelligence Agent mediante la terminación de su ID de proceso; a continuación, se inicia cada SIA. La opción `all` inicia todos los nodos del equipo, incluyendo los nodos que pertenecen a clústeres distintos. |
| `-managedstart` | **`<nombre del servidor completamente cualificado><[otra información de autenticación]>`** | Inicie un servidor. |

| Opción de CCM | Argumentos válidos | Descripción |
|---|---|---|
| `-managedstop` | **`<nombre del servidor completamente cualificado><[otra información de autenticación]>`** | Detenga un servidor. |
| `-managedrestart` | **`<nombre del servidor completamente cualificado><[otra información de autenticación]>`** | Detenga un servidor e inícielo. |
| `-managedforceterminate` | **`<nombre del servidor completamente cualificado><[otra información de autenticación]>`** | Detener el servidor inmediatamente sin finalizar las solicitudes de procesamiento actuales. |
| `-enable` | **`<nombre del servidor completamente cualificado><[otra información de autenticación]>`** | Habilitar un servidor iniciado de modo que se registre con el sistema y empiece a escuchar en el puerto adecuado. Utilice la forma completa del nombre de servidor. |
| `-disable` | **`<nombre del servidor completamente cualificado><[otra información de autenticación]>`** | Deshabilitar un servidor de modo que deje de responder a las solicitudes de la plataforma de BI pero permanece iniciado como un proceso. Utilice la forma completa del nombre de servidor. |
| `-display` | **`< [otra información de autenticación] >`** | Informa del estado actual de todos los servidores del clúster, incluyendo los nombres de servidor, los nombres de host, los ID de proceso y descripciones, tanto si se ejecutan o si están habilitados o deshabilitados. |

En la siguiente tabla se describen las opciones que componen el argumento indicado mediante **`<[otra información de autenticación]>`**.

> **Nota**
>
> Para obtener una protección mejorada, siempre debe proporcionar las credenciales de una cuenta con autenticación Enterprise. Otros tipos de autenticación no se admiten.

| Opción de autenticación | Argumentos válidos | Descripción |
|---|---|---|
| `-cms` | `<cmsname:port#>` | Especificar el CMS con el que desea conectar. Si no se especifica, el valor predeterminado del CCM es el equipo local y puerto predeterminado (6400). |
| `-username` | `<nombreusuario>` | Especifique la cuenta que proporciona derechos administrativos a la plataforma de BI. Si no se especifica, se intenta la cuenta Administrator predeterminada. |
| `-password` | `<password>` | Especificar la contraseña correspondiente. Si no se especifica, se intenta con una contraseña en blanco.<br>**Nota**<br>Para especificar el argumento `-password` también se debe especificar el argumento `-username`. |

El CCM lee las cadenas de inicio y otros valores de configuración del archivo `ccm.config`.

## Información relacionada

ccm.config [página 1104]

# 31.1.1.1.1 Ejemplos

Estos dos comandos inician y habilitan todos los servidores de la plataforma de BI. El Servidor de administración central (CMS) se inicia en el equipo local y el puerto predeterminado (6400):

```
ccm.sh -start all
ccm.sh -enable all
```

Estos dos comandos inician y habilitan todos los servidores de la plataforma de BI. El CCM habilitará todos los servidores en el clúster, en el que el CMS ejecuta el equipo MACHINE01 y el puerto 6701:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

Estos dos comandos inician y habilitan todos los servidores de la plataforma de BI con una cuenta administrativa especificada denominada `SysAdmin`y la contraseña proporcionada:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

Este único comando inicie sesión con una cuenta administrativa especificada para deshabilitar un servidor de tareas de Adaptive que se ejecuta en un segundo equipo:

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

## 31.1.1.1.2 ccm.config

Este archivo de configuración define las cadenas de inicio y otros valores que utiliza el CCM cuando ejecuta sus comandos. Este archivo lo mantiene el propio CCM y otras utilidades de secuencia de comandos de la plataforma de BI. Este archivo normalmente se edita sólo cuando es necesario modificar la línea de comandos de un Server Intelligence Agent. Es altamente recomendable que lleve a cabo una copia de seguridad de este archivo antes de editarlo manualmente.

### Información relacionada

Información general de las líneas de comandos [página 1111]

## 31.1.1.2 cmsdbsetup.sh

La secuencia de comandos `cmsdbsetup.sh` se instala en el directorio `<sap_bobj>` de la instalación. La secuencia de comandos proporciona un programa basado en texto que permite realizar las siguientes tareas.

- Configurar una base de datos del sistema CMS
- Reiniciar una base de datos del sistema del CMS
- Copiar datos de otro origen de datos
- Cambiar la clave de clúster
- Cambiar el nombre del clúster

> **Nota**
>
> Antes de ejecutar esta secuencia de comandos, realice la copia de seguridad de la base de datos del sistema CMS actual y de todos los contenidos de los repositorios de archivos de entrada y salida. Para obtener información, consulte «Copia de seguridad y restauración del sistema». También asegúrese de ver servidores de administración central de clustering en el capítulo «Actualización de servidores» del *manual de usuario de la plataforma de BI SAP* para obtener más información acerca de clústers CMS y configurar la base de datos de CMS.

La secuencia de comandos le pedirá el nombre del Server Intelligence Agent (SIA). Para comprobar el nombre del SIA, consulte las propiedades de SIA en el archivo `ccm.config`. El nombre actual del SIA aparece después de la opción `-name`. O, puede usar la opción 8 con el archivo `serverconfig.sh`.

### Información relacionada

Agrupar Servidores de administración central [página 435]
Presentación general de la copia de seguridad y de la restauración [página 558]

## 31.1.1.3 serverconfig.sh

La secuencia de comandos `serverconfig.sh` se instala en el directorio `<sap_bobj>` de la instalación. Esta secuencia de comandos proporciona un programa basado en texto que permite realizar las siguientes operaciones.

- Agregar un nodo
- Eliminar un nodo
- Modificar un nodo
- Mover un nodo
- Realizar la copia de seguridad de la configuración del servidor
- Restaurar la configuración del servidor
- Modificar la configuración de nivel Web
- Listar todos los nodos

### 31.1.1.3.1 Agregar/eliminar/modificar/enumerar nodos en UNIX

1. Vaya al directorio `<DIRINSTALACIÓN>/sap_bobj` de la instalación.
2. Utilice el siguiente comando:

   ```
   ./serverconfig.sh
   ```

   La secuencia de comandos muestra una lista de opciones:

   1. Agregar un nodo
   2. Eliminar un nodo
   3. Modificar un nodo
   4. Mover un nodo
   5. Realizar la copia de seguridad de la configuración del servidor
   6. Restaurar la configuración del servidor
   7. Modificar la configuración de nivel Web

8. Listar todos los nodos
3. Escriba el número que corresponda a la acción que desea realizar.
4. Si va a agregar, eliminar o modificar un servidor, proporcione a la secuencia de comandos la información adicional que solicite.

## 31.1.2 Plantillas de secuencia de comandos

### 31.1.2.1 startservers

La secuencia de comandos `startservers` se instala en el directorio `<DIRINSTALACIÓN>/sap_bobj>` de la instalación. Esta secuencia de comandos sirve como plantilla para sus propias secuencias de comandos: Se proporciona como ejemplo para mostrar el modo en que puede crear su propia secuencia de comandos que inicie los servidores de BusinessObjects Enterprise mediante la ejecución de una serie de comandos CCM. Para obtener información detallada acerca de cómo escribir comandos del CCM para los servidores, consulte ccm.sh [página 1100].

### 31.1.2.2 stopservers

La secuencia de comandos `stopservers` se instala en el directorio `<DIRINSTALACIÓN>/sap_bobj>` de la instalación. Esta secuencia de comandos sirve como plantilla para sus propias secuencias de comandos: Se proporciona como ejemplo para mostrar el modo en que puede crear su propia secuencia de comandos que inicie los servidores de BusinessObjects Enterprise mediante la ejecución de una serie de comandos CCM. Para obtener información detallada acerca de cómo escribir comandos del CCM para los servidores, consulte ccm.sh [página 1100].

## 31.1.3 Secuencias de comandos usadas por la plataforma de BI

Estas secuencias de comandos secundarias se ejecutan a menudo en la tarea de fondo si ejecuta las utilidades de la secuencia de comandos principal de la plataforma de BI y no tiene que ejecutarlas usted mismo.

#### bobjrestart.sh

Esta secuencia de comandos se ejecuta internamente por el CCM para administrar nodos del agente de Server Intelligence. No ejecute esta secuencia de comandos.

## env.sh

La secuencia de comandos `env.sh` se instala en el directorio `<sap_bobj/setup>` de la instalación. Esta secuencia de comandos configura las variables del entorno de la plataforma de BI necesarias para algunas otras secuencias de comandos. Las secuencias de comandos de la plataforma de BI ejecutan env.sh según sea necesario. Consulte el *Manual de instalación de la plataforma SAP BusinessObjects Business Intelligence* para obtener más información.

## env-locale.sh

La secuencia de comandos `env-locale.sh` se utiliza para convertir las cadenas del lenguaje de secuencia de comandos entre distintos tipos de codificación (por ejemplo, UTF8, EUC o Shift-JIS). Esta secuencia de comandos la ejecuta `env.sh` según sea necesario.

## initlaunch.sh

La secuencia de comandos `initlaunch.sh` ejecuta `env.sh` para configurar las variables del entorno de la plataforma de BI y, a continuación, ejecuta los comandos que haya agregado como argumento de línea de comandos para la secuencia de comandos. La secuencia de comandos se ha concebido principalmente para su uso como herramienta de depuración de SAP BusinessObjects.

## postinstall.sh

La secuencia de comandos `postinstall.sh` se instala en el directorio `<DIRSECUENCIACOMANDOS>` de la instalación. No necesita ejecutar esta secuencia de comandos.

## setup.sh

La secuencia de comandos `setup.sh` se instala en el directorio raíz de la instalación. Esta secuencia de comandos proporciona un programa basado en texto que permite configurar la instalación de la plataforma de BI. La secuencia de comandos se ejecuta automáticamente cuando se instala la plataforma de BI. Le pide la información que se necesita para configurar la plataforma de BI por primera vez.

Para obtener detalles completos sobre cómo responder a la secuencia de comandos de configuración al instalar la plataforma de BI consulte el *Manual de instalación de la plataforma SAP BusinessObjects Business Intelligence*.

### setupinit.sh

La secuencia de comandos `setupinit.sh` se instala en el directorio `<sap_bobj/init>` de la instalación. Esta secuencia de comandos copia las secuencias de comandos de control de ejecución en los directorios `rc#` para el inicio automatizado. Si desea que los servidores de la plataforma de BI se inicien y se detengan con el equipo dónde están instalados, ejecute esta secuencia de comandos cuando finalice la secuencia de comandos `setup.sh`.

> **Nota**
>
> Debe disponer de privilegios de root para ejecutar esta secuencia de comandos.

## 31.2 Secuencias de comandos de Windows

En esta sección se ofrece información detallada de las herramientas y secuencias de comandos administrativas que se incluyen en la distribución la plataforma de BI. Esta sección se proporciona principalmente como referencia. Los conceptos y los procedimientos de configuración se describen más detalladamente en este manual.

La distribución de Windows de la plataforma de BI incluye la versión de Windows del Administrador de configuración central (CCM). Además de interactuar con la GUI, puede seleccionar ejecutar ejecutable del CCM desde la línea de comandos con opciones para administrar servidores.

### 31.2.1 ccm.exe

El archivo ejecutable `ccm.exe` se instala en el directorio `<DIRINSTALACIÓN>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64` de la instalación. Puede ejecutar el ejecutable directamente desde la línea de comandos para realizar determinadas operaciones. En esta sección se enumeran las opciones de línea de comandos y se proporcionan ejemplos.

> **Nota**
>
> Se debe ejecutar un Agente de inteligencia de servidor (SIA) y el Servidor de administración central (CMS) antes de usar las opciones de línea de comandos de `ccm.exe` para interactuar con un servidor individual.

> **Nota**
>
> Los argumentos entre corchetes [ ] son opcionales.

> **Nota**
>
> Los argumentos indicados mediante **`<otra información de autenticación>`** se proporcionan en la segunda tabla.

| Opción de CCM | Argumentos válidos | Descripción |
|---|---|---|
| `-help` | n/d | Mostrar la ayuda de la línea de comandos. |
| `-managedstart` | `todo` o **`<nombre del servidor completo> <[otra información de autenticación]>`** | Inicie un servidor. |
| `-managedstop` | `todo` o **`<nombre del servidor completo> <[otra información de autenticación]>`** | Detenga un servidor. |
| `-managedrestart` | `todo` o **`<nombre del servidor completo> <[otra información de autenticación]>`** | Detenga un servidor e inícielo. |
| `-managedforceterminate` | `todo` o **`<nombre del servidor completo> <[otra información de autenticación]>`** | Detener el servidor inmediatamente sin finalizar las solicitudes de procesamiento actuales. |
| `-enable` | `todo` o **`<nombre del servidor completo> <[otra información de autenticación]>`** | Habilitar un servidor iniciado de modo que se registre con el sistema y empiece a escuchar en el puerto adecuado. |
| `-disable` | `todo` o **`<nombre del servidor completo> <[otra información de autenticación]>`** | Deshabilitar un servidor de modo que deje de responder a las solicitudes de la plataforma de BI pero permanece iniciado como un proceso. |
| `-display` | **`< [otra información de autenticación]>`** | Informa del estado actual de todos los servidores del clúster, incluyendo los nombres de servidor, los nombres de host, los ID de proceso y descripciones, tanto si se ejecutan o si están habilitados o deshabilitados. |

En la siguiente tabla se describen las opciones que componen el argumento indicado mediante **`<[otra información de autenticación]>`**.

> **Nota**
>
> Siempre debe proporcionar las credenciales de una cuenta don autenticación Enterprise.

| Opción de autenticación | Argumentos válidos | Descripción |
|---|---|---|
| `-cms` | **`<nombrecms:númeropuerto>`** | Especificar el CMS con el que desea conectar. Si no se especifica, el valor predeterminado del CCM es el equipo local y puerto predeterminado (6400). |
| `-username` | **`<nombreusuario>`** | Especifique la cuenta que proporciona derechos administrativos a la plataforma de BI. Si no se especifica, se intenta la cuenta Administrator predeterminada. |
| `-password` | **`<contraseña>`** | Especificar la contraseña correspondiente. Si no se especifica, se intenta con una contraseña en blanco.<br>**Nota**<br>Para especificar el argumento `-password` también se debe especificar el argumento `-username`. |
| `-authentication` | **`<tipo de autenticación>`** | Especifique el tipo de autenticación. Sólo se admite **`secEnterprise`**. |

El CCM lee las cadenas de inicio y otros valores de configuración del archivo `ccm.config`.

## 31.2.1.1 Ejemplos

Los siguiente ejemplos asumen que un Server Intelligence Agent (SIA) y el Servidor de administración central (CMS) se inician y ejecutan. Antes de usar las opciones de línea de comandos de `ccm.exe` para interactuar con un servidor individual, puede usar el siguiente comando de Windows para iniciar el servicio del SIA:

```
net start "Server Intelligence Agent (NODENAME)"
```

El SIA también se puede detener mediante `net stop "Server Intelligence Agent (NODENAME)"`.

Este comando inicia todos los servidores de la plataforma de BI:

```
ccm.exe -managedstart all
```

Este comando inicia el Servidor de tareas de Adaptive. El CMS se inició en el puerto 6701, en lugar de hacerlo en el puerto predeterminado:

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

Este comando habilita un servidor de tareas de Adaptive con una cuenta administrativa especificada denominada `SysAdmin`:

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

Este comando inicia la sesión con una cuenta administrativa especificada para deshabilitar un servidor de tareas de Adaptive que se ejecuta en un segundo equipo:

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

## 31.3 Líneas de comandos de los servidores

### 31.3.1 Información general de las líneas de comandos

En esta sección se enumeran las opciones de línea de comandos que controlan el comportamiento de cada servidor de la plataforma de BI.

Al iniciar o configurar un servidor a través de la consola de administración central (CMC), el servidor se inicia, o reinicia, con una línea de comandos predeterminada que incluye un conjunto típico de opciones y valores. En la mayoría de los casos, no es necesario modificar las líneas de comandos predeterminadas directamente. Además, puede manipular las opciones más habituales mediante las distintas pantallas de configuración de servidor en la CMC. Para referencia, en esta sección se ofrece una lista completa de las opciones de línea de comandos que admite cada servidor. Se puede modificar la línea de comandos de cada servidor si es necesario personalizar aún más el comportamiento de la plataforma de BI.

En esta sección, los valores indicados entre corchetes [ ] son opcionales.

> **Nota**
>
> La siguiente tabla enumera las opciones de línea de comandos disponibles. Los servidores de la plataforma de BI usan un número de opciones internas que no están enumeradas en estas tablas. Estas opciones internas no se deben modificar.

#### 31.3.1.1 Para ver o modificar la línea de comandos de un servidor

1. Use la consola de administración central (CMC) para detener el servidor.
2. Haga clic con el botón derecho en el servidor y seleccione *Propiedades*.
3. En la pantalla *Propiedades*, modifique la línea de comandos para el servidor y haga clic en *Guardar y cerrar*.
4. Inicie el servidor.

## 31.3.2 Opciones estándar para todos los servidores

Estas opciones de línea de comandos se aplican a todos los servidores de la plataforma de BI, a menos que se indique lo contrario. Consulte en el resto de esta sección las opciones específicas de cada tipo de servidor.

| Opción | Argumentos válidos | Comportamiento |
|---|---|---|
| `-requestPort` | `<port >` | Especificar el puerto en el que escucha el servidor. El servidor registra este puerto con el CMS. Si no se especifica, el servidor selecciona los puertos libres superiores a 1024.<br>**Nota**<br>Este puerto lo utilizan los diferentes servidores para fines distintos. Antes de realizar el cambio, consulte la sección sobre cómo cambiar los números de puerto del servidor predeterminados en el *Manual del administradorde la plataforma de SAP BusinessObjects Business Intelligence*. |
| `-loggingPath` | `<ruta absoluta >` | Especifique la ruta en la que se crean los archivos de registro. |

### 31.3.2.1 Manejo de señales de UNIX

En UNIX las subrutinas de la plataforma de BI manejan las siguientes señales:

- `SIGTERM` da como resultado un apagado correcto del servidor (código de salida = 0).
- `SIGSEGV`, `SIGBUS`, `SIGSYS`, `SIGFPE` y `SIGILL` dan como resultado un apagado rápido (código de salida = 1).

## 31.3.3 Servidor de administración central

En esta sección se proporcionan las opciones de línea de comandos específicas al CMS. La ruta predeterminada al servidor en Windows es `<DIRINSTALACIÓN>\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

La ruta predeterminada al servidor en UNIX es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/<plataforma>/boe_cmsd`.

| Opción | Argumentos válidos | Comportamiento |
|---|---|---|
| `-threads` | `<número>` | Especifica el número de subprocesos de trabajo que inicializa y usa el CMS. El valor puede estar entre 12 y 150, y de forma predeterminada se establece en 50. |
| `-reinitializedb` | | Provocar que el CMS elimine la base de datos del sistema y la vuelva a crear únicamente con los objetos de sistema predeterminados. Todos los datos existentes en la base de datos se pierden cuando se vuelve a crear. |
| `-quit` | | Obligar al CMS a salir después de procesar la opción `-reinitializedb`. |
| `-receiverPool` | `<número>` | Especificar el número de subprocesos que el CMS crea para recibir las solicitudes de cliente. Un cliente puede ser otro servidor de Business Objects, el Asistente para la publicación de informes, Crystal Reports o una aplicación cliente personalizada que haya creado. El valor predeterminado es 5. Normalmente no es necesario aumentar este valor a menos que se cree una aplicación personalizada con muchos clientes. |
| `-maxobjectsincache` | `<número>` | Especificar el número máximo de objetos que el CMS almacena en su caché de memoria. Al aumentar el número de objetos se reduce el número de llamadas de base de datos necesarias y se mejora el rendimiento de CMS en gran medida. Sin embargo, colocar demasiados objetos en la memoria puede dar como resultado que al CMS le quede poca memoria para procesar las consultas. El valor predeterminado es 100000. |

| Opción | Argumentos válidos | Comportamiento |
|---|---|---|
| -ndbqthreads | <número> | Especificar el número de subprocesos de trabajo de CMS que envían solicitudes a la base de datos. Cada subproceso tiene una conexión a la base de datos, por lo que se debe tener cuidado de no exceder la capacidad de la base de datos. En la mayoría de los casos, el valor máximo que se debe configurar es 20. |
| -oobthreads | <número> | Si el clúster incluye más de ocho miembros de clúster de CMS, asegúrese de que la línea de comandos para cada CMS incluye esta opción. Especifique el número de servicios de CMS en el clúster. Esta opción garantiza que el clúster puede admitir una carga elevada. |

## Información relacionada

Opciones estándar para todos los servidores [página 1112]

## 31.3.4 Servidor de procesamiento de Crystal Reports y servidor de caché de Crystal Reports

El servidor de procesamiento de Crystal Reports y el servidor de caché de Crystal Reports se controlan de forma similar desde la línea de comandos. Las opciones de línea de comandos determinan si el servidor se inicia como un servidor de procesamiento, como un servidor de caché o como ambos. Las opciones que se aplican únicamente a un tipo de servidor se indican a continuación.

Las rutas predeterminadas a los servidores en Windows son:

- <INSTALLDIR>\SAP BusinessObjects Business Intelligence platform 4.0 \win64_x64\cacheserver.exe.
- <INSTALLDIR>\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe.

Las rutas predeterminadas a los servidores en UNIX son:

- <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_cachesd.
- <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_procd.

| Opción | Argumentos válidos | Comportamiento |
|---|---|---|
| -cache | | Activar la funcionalidad de servidor de caché. |
| -deleteCache | | Eliminar el directorio de caché cada vez que se inicie y detenga el servidor. |
| -report_ProcessExtPath | **<rutaAbsoluta>** | Especificar el directorio predeterminado para las extensiones de procesamiento. |

## Información relacionada

Opciones estándar para todos los servidores [página 1112]

# 31.3.5 Servidores de tareas

En esta sección se proporcionan las opciones de línea de comandos específicas de los servidores de tareas de Adaptive.

La ruta predeterminada al servidor en Windows es `<DIRINSTALACIÓN>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe`.

La ruta predeterminada al servidor en UNIX es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/<PLATAFORMA>/boe_jobsd`.

| Opción | Argumentos válidos | Comportamiento |
|---|---|---|
| -dir | **<rutaAbsoluta>** | Especificar el directorio de datos del Servidor de tareas. |
| -maxJobs | **<número>** | Configurar el número máximo de trabajos simultáneos que puede gestionar el servidor. El valor predeterminado es cinco. |

| Opción | Argumentos válidos | Comportamiento |
|---|---|---|
| `-requestJSChildPorts` | **`<límiteInferior-límiteSuperior>`** | Especificar el intervalo de puertos que los procesos secundarios deben utilizar en un entorno de servidor de seguridad. Por ejemplo, `6800-6805` limita los procesos secundarios a seis puertos.<br>**Nota**<br>Para que esta opción surta efecto, también debe especificar la configuración `-requestPort`. |
| `-report_ProcessExtPath` | **`<rutaAbsoluta>`** | Especificar el directorio predeterminado para las extensiones de procesamiento. Para obtener más detalles, consulte el *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*. |

### Información relacionada

Opciones estándar para todos los servidores [página 1112]

## 31.3.6 Servidor de procesamiento de Adaptive

El servidor de procesamiento de Adaptive usa parámetros definidos por el equipo virtual Java de SAP (SAP JVM). Consulte la documentación de SAP JVM para obtener más información.

## 31.3.7 Servidor de aplicaciones de informes

En esta sección se proporcionan las opciones de línea de comandos específicas al Servidor de aplicaciones de informes (RAS).

La ruta predeterminada al servidor en Windows es `<DIRINSTALACIÓN>\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe`.

La ruta predeterminada al servidor en UNIX es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/<PLATAFORMA>/ras/boe_crystalrasd`.

| Opción | Argumentos válidos | Comportamiento |
| --- | --- | --- |
| `-ipport` | **`<puerto>`** | Especifique el número de puerto para recibir las solicitudes TCP/IP al ejecutar en modo independiente (fuera de la plataforma de BI) |
| `-report_ProcessExtPath` | **`<rutaAbsoluta>`** | Especificar el directorio predeterminado para las extensiones de procesamiento. Para obtener más detalles, consulte el *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*. |
| `-ProcessAffinityMask` | **`<máscara>`** | Utilice una máscara para especificar exactamente las CPU que utilizará RAS cuando se ejecute en un equipo con varios procesadores.<br><br>La máscara tiene el formato `0xffffffff`, donde cada `f` representa un procesador y la lista de procesadores se lee de derecha a izquierda (es decir, la última `f` representa el primer procesador). Por cada `f`, sustituya 0 (no se permite el uso de la CPU) o `1` (se permite el uso de la CPU).<br><br>Por ejemplo, si ejecuta RAS en un equipo con cuatro procesadores y desea utilizar los procesadores tercero y cuarto, utilice la máscara `0x1100`. Para los procesadores segundo y tercero utilice `0x0110`.<br><br>**Nota**<br>RAS utiliza los primeros procesadores permitidos en la cadena, hasta el máximo especificado en la licencia. Si dispone de una licencia de dos procesadores, `0x1110` tiene el mismo efecto que `0x0110`.<br><br>**Nota**<br>El valor predeterminado de la máscara es `-1`, que significa lo mismo que `0x1111`. |

## Información relacionada

Opciones estándar para todos los servidores [página 1112]

# 31.3.8 Servidor de procesamiento de Web Intelligence

En esta sección se muestran las opciones de línea de comandos específicas del servidor de procesamiento de Web Intelligence.

La ruta predeterminada al servidor en Windows es `<DIRINSTALACIÓN>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

La ruta predeterminada al servidor en UNIX es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/<PLATAFORMA>/WIReportServer`.

| Opción | Argumentos válidos | Comportamiento |
|---|---|---|
| `-ConnectionTimeoutMinutes` | **`<minutos>`** | Especifique el número de minutos antes de que el servidor supere el tiempo de espera. |
| `-MaxConnections` | **`<número>`** | Especifique el número máximo de conexiones simultáneas que el servidor permite de una vez. |
| `-DocExpressEnable` | | Permite el almacenamiento en caché de documentos de Web Intelligence cuando se está viendo el documento. |
| `-DocExpressRealTimeCachingEnable` | | Permite el almacenamiento en caché en tiempo real de documentos de Web Intelligence. |
| `-DocExpressCacheDurationMinutes` | **`<minutos>`** | Especifique el tiempo (en minutos) que se almacena el contenido en caché. |
| `-DocExpressMaxCacheSizeKB` | **`<kilobytes>`** | Especifique el tamaño de la caché de documentos. |
| `-EnableListOfValuesCache` | | Permite el almacenamiento en caché por sesiones de usuarios de listas de valores |
| `-ListOfValuesBatchSize` | **`<número>`** | Especifique el número máximo de valores que se pueden devolver por lote de listas de valores. |

| Opción | Argumentos válidos | Comportamiento |
| --- | --- | --- |
| -UniverseMaxCacheSize | **<número>** | Especifique el número de universos que se va a almacenar en memoria caché. |
| -WIDMaxCacheSize | **<número>** | Especifique el número máximo de documentos de Web Intelligence que se pueden almacenar en caché. |

## Información relacionada

Opciones estándar para todos los servidores [página 1112]

## 31.3.9 Servidores del repositorio de archivos de entrada y de salida

En esta sección se proporcionan las opciones de línea de comandos específicas a los Servidores del repositorio de archivos de entrada y salida.

La ruta predeterminada a los servidores en Windows es `<DIRINSTALACIÓN>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`

La ruta predeterminada al programa que proporciona ambos servidores en UNIX es: `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/<plataforma>/boe_filesd`. De forma predeterminada, el agente de Server Intelligence iniciará una instancia de `boe_filesd` para el servidor del repositorio de archivos de entrada y una instancia para el servidor del repositorio de archivos de salida.

| Opción | Argumentos válidos | Comportamiento |
| --- | --- | --- |
| `-rootDir` | `<absolutepath>` | Configurar el directorio raíz de las distintas carpetas y archivos que administra el servidor. Las rutas de archivo que se utilizan para hacer referencia a archivos del Servidor del repositorio de archivos se interpretan como relativas a este directorio raíz.<br><br>**Nota**<br>Todos los Servidores del repositorio de archivos de entrada y todos los de salida deben compartir el mismo directorio raíz. De lo contrario, hay riesgos de que existan instancias incoherentes. Adicionalmente, el directorio raíz de entrada no debe ser el mismo que el directorio raíz de salida. Se recomienda replicar los directorios raíz mediante una matriz RAID o una solución de hardware alternativa. |
| `-tempDir` | `<rutaAbsoluta>` | Definir la ubicación del directorio temporal que el FRS utiliza para transferir archivos. Utilice esta opción de línea de comandos si desea controlar la ubicación del directorio temporal del FRS o si el nombre de directorio temporal predeterminado que genera el FRS excede el límite de ruta del sistema operativo (lo que impediría que se iniciara el FRS).<br><br>**Nota**<br>No especifique un directorio existente para esta opción. El directorio especificado se vaciará cuando se inicie el FRS y se quitará cuando se cierre el FRS. Si utiliza un directorio existente, se vaciará y quitará. |
| `-maxidle` | `<minutos>` | Especificar el número de minutos que transcurrirán para que se limpie una sesión inactiva. |
| `-legacymode` | | Permitir que las versiones antiguas de SDK o clientes anteriores a la versión 4.0, accedan por completo a la plataforma BI. |

| Opción | Argumentos válidos | Comportamiento |
| --- | --- | --- |
| `-vsaFileLoc` | `<absolutepath>` | Fije la vía de acceso absoluta para archivo de la biblioteca de adaptador de la búsqueda de virus.<br>**Nota**<br>Todos los Servidores del repositorio de archivos de entrada y todos los de salida deben compartir el mismo directorio raíz. De lo contrario, hay riesgos de que existan instancias incoherentes. |

## Información relacionada

Opciones estándar para todos los servidores [página 1112]

# 31.3.10 Servidor de eventos

En esta sección se proporcionan las opciones de línea de comandos específicas para el Servidor de eventos.

La ruta predeterminada al servidor en Windows es `<DIRINSTALACIÓN>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe`.

La ruta predeterminada al servidor en UNIX es `<DIRINSTALACIÓN>/sap_bobj/enterprise_xi40/<plataforma>/boe_eventsd`.

| Opción | Argumentos válidos | Comportamiento |
| --- | --- | --- |
| `-cleanup` | `<minutos>` | Especificar la frecuencia (en minutos) con la que el servidor limpia los proxy de escucha. El valor representa la cantidad de tiempo que se tarda en realizar dos limpiezas. Por ejemplo, si especifica un valor de 10, los proxys se limpiarán cada cinco minutos. |

## Información relacionada

Opciones estándar para todos los servidores [página 1112]

# 32 Herramienta de diagnóstico del repositorio

## 32.1 Resumen de la herramienta de diagnóstico del repositorio

La herramienta de diagnóstico del repositorio (RDT) es una herramienta que analiza, diagnostica y repara las incoherencias que se pueden producir entre la base de datos de sistema del Servidor de administración central (CMS) y el almacén de archivos de los Servidor del repositorio de archivos (FRS) o incoherencias que se puedan producir en los metadatos de los InfoObjects almacenados en la base de datos de CMS.

Durante las operaciones normales, no es habitual que la base de datos del sistema de CMS presente incoherencias. No obstante, se pueden producir durante eventos inesperados, como la recuperación de desastres, la restauración de copias de seguridad o interrupciones en la red. Durante estos eventos, la base de datos del sistema de CMS se puede interrumpir al realizar una tarea. Esto puede provocar incoherencias con los objetos de la base de datos del sistema de CMS.

La RDT analiza la base de datos del sistema de CMS e identifica incoherencias en dichos objetos, como informes, usuarios, grupos de usuarios, carpetas, servidores, universos, conexiones de universo y otros objetos.

La RDT busca tres tipos de incoherencias.

- Incoherencias de objeto a archivo.
  Estas incoherencias se pueden producir entre InfoObjects de la base de datos del CMS y los archivos correspondientes de los repositorios de archivos. Por ejemplo, un archivo que esté almacenado en FRS puede que no tenga un objeto correspondiente dentro de la base de datos del sistema de CMS.
- Incoherencias de metadatos de InfoObject.
  Hay incoherencias que pueden existir en la definición de objeto de un InfoObject (metadatos) en la base de datos del CMS. Por ejemplo, un InfoObject puede hacer referencia a otro InfoObject que no existe en la base de datos del CMS.
- Inconsistencias en la relación.
  Se producen inconsistencias cuando existe una relación entre dos InfoObjects pero se ha borrado uno de ellos. Solo se procesan las relaciones EnterpriseNode-Server, Service-Server, ServiceContainer-Server.

La RDT lleva a cabo dos funciones, según los parámetros que proporcione al ejecutar la herramienta:

- Analiza la base de datos del sistema de CMS y el almacén de archivos de FRS, informa de las incoherencias y crea un archivo de registro en formato XML con las acciones sugeridas para reparar las incoherencias.
- Analiza y repara las incoherencias identificadas en la base de datos del sistema de CMS e informa de todas las acciones realizadas y los cambios efectuados en formato XML.

## 32.2 Uso de la herramienta de diagnóstico del repositorio

La Herramienta de diagnóstico del repositorio (RDT) está disponible en cualquier equipo con un Administrador de configuración central (CCM) instalado en él. Esta herramienta de la línea de comandos analiza, diagnostica y repara las incoherencias que se puedan producir entre la base de datos del sistema del Servidor de administración central (CMS) y el almacén de archivos de los Servidor del repositorio de archivos (FRS), o las incoherencias que se puedan producir en los metadatos de un InfoObject.

Se recomienda realizar una copia de seguridad de la base de datos del CMS y del almacén de archivos FRS y ejecutar la RDT en la versión de copia de seguridad mientras los servicios de la plataforma de BI están inactivos. Si no es posible, se puede ejecutar la RDT en una base de datos activa.

Si desea ejecutar la RDT en una base de datos activa, tenga en cuenta las siguientes consideraciones:

- La RDT usará una conexión de base de datos mientras se ejecuta.
- La RDT solo comprobará la coherencia de la base de datos hasta el punto en el que se empezó a ejecutar. Las incoherencias que se produzcan mientras se ejecuta la RDT no se registrarán o corregirán.
- Se recomienda que el equipo host que ejecuta la RDT tenga más memoria disponible que las recomendaciones normales del sistema para el procesamiento de las transacciones de la RDT:
  - Una base de datos de 50.000 InfoObjects o inferior debe tener 350 MB adicionales disponibles para el procesamiento
  - Una base de datos de 50.000 a 400.000 InfoObjects debe tener 1,7 GB adicionales disponibles para el procesamiento
  - Una base de datos de 400.000 a 1.000.000 InfoObjects debe tener 4 GB adicionales disponibles para el procesamiento
- La RDT no se tiene que ejecutar desde el servidor del CMS. Si se ejecuta desde un equipo separado ayuda a reducir el impacto en el rendimiento del sistema.
- La herramienta puede tener un impacto moderado en el rendimiento de la base de datos mientras se ejecuta.

La RDT no necesita el servicio del CMS para ejecutarse, la RDT se ejecuta directamente en la base de datos del CMS.

### 32.2.1 Para usar la herramienta de diagnóstico del repositorio

1. Si ejecuta la herramienta en un equipo Windows, abra una ventana del símbolo del sistema y ejecute el siguiente comando.

   `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe <arguments>`, donde `<arguments>` es la lista de los parámetros que desea especificar.
2. Si ejecuta la herramienta en un equipo UNIX, abra un shell compatible /usr/bin/sh y ejecute el siguiente comando.

   `.<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_reposcan.sh <arguments>`, donde `<platform>` es «linux64_x64», «solaris_sparcv9», «hpux_ia64» o «aix_rs6000_64», y `<arguments>` es la lista de los parámetros que desea especificar.

> **Nota**
>
> Al introducir parámetros de línea de comandos Unix cabe la posibilidad de que tenga que omitir o multiplicar caracteres de shell especiales de escape. Por ejemplo, si se utiliza el signo de exclamación «!» en una contraseña, quizá deba omitir el signo de exclamación de la forma siguiente: `./ccm.sh -display -username Administrator -password Abc\!defgh123 -cms cmsname`.

La herramienta de diagnóstico del repositorio analiza las incoherencias del repositorio. Según los parámetros que especifique, diagnostica y registra incoherencia o repara incoherencias y registra la acción que ha realizado.

`Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml` elabora una lista de las inconsistencias que encuentra la herramienta. Si la herramienta ha reparado las discrepancias que encuentra, también crea el archivo `Repo_Repair_aaaa_mm_dd_hh_mm_ss.xml`. Este archivo detallas los objetos que se reparan y los archivos huérfanos que se eliminan. Si existen incoherencias que no se pueden reparar, también se mostrarán en la lista.

La ruta a los archivos de registro se puede especificar mediante el parámetro `outputdir`. Si este parámetro no se especifica, el directorio predeterminado para los archivos de registro es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\reposcan` en Windows y `./sap_bobj/enterprise_xi40/reposcan`en Unix.

> **Nota**
>
> La aplicación también proporciona un archivo XSL predeterminado que se usa con el archivo XML para producir una página HTML. El archivo XSL se almacena en `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\reposcan` en Windows y `./sap_bobj/enterprise_xi40/reposcan` en Unix.

Para obtener una lista de los mensajes de advertencia y las acciones recomendadas que la RDT realiza cuando encuentra incoherencias, consulte *Incoherencias en metadatos de CMS* e *Incoherencias entre el CMS y el FRS*.

### Información relacionada

Incoherencias en los metadatos de CMS [página 1133]
Incoherencias entre el CMS y el FRS [página 1133]

## 32.2.2 Parámetros de la Herramienta de diagnóstico del repositorio

La RDT acepta los parámetros de la siguiente tabla:

> **Nota**
>
> Los argumentos de la línea de comandos anulan las entradas del archivo de parámetros al ejecutarse.

> **Nota**
>
> Para las opciones de parámetro de base de datos SAP HANA, consulte la nota SAP 1916845.

Parámetros generales

| Parámetro | Opcional u obligatorio | Descripción |
|---|---|---|
| `dbdriver` | Obligatorio | El tipo de controlador utilizado para conectarse a la base de datos del CMS. Los valores aceptados son:<br>• `db2databasesubsystem`<br>• `maxdbdatabasesubsystem`<br>• `mysqldatabasesubsystem`<br>• `oracledatabasesubsystem`<br>• `sqlserverdatabasesubsystem`<br>• `sybasedatabasesubsystem`<br>• `sqlanywheredatabasesubsystem` |
| `connect` | Obligatorio | Los detalles de conexión utilizados para conectarse a la base de datos del CMS.<br>Por ejemplo: `-connect "UID=root;PWD=<password>;DSN=<dsn>;HOSTNAME=<hostname>;PORT=<portnumber>"` |

| Parámetro | Opcional u obligatorio | Descripción |
| --- | --- | --- |
| `dbkey` | Obligatorio | Introduzca la clave de clúster para el despliegue de la plataforma de BI.<br><br>Si no sabe la clave de clúster, reiníciela siguiendo estos pasos:<br><br>**Nota**<br>Si el equipo se encuentra en un clúster, se deberán llevar a cabo estos pasos para todos los miembros del clúster. Realice una copia de seguridad de la base de datos del CMS y del almacén de datos antes de continuar.<br><br>1. Ejecute el Administrador de configuración central (CCM).<br>2. En el CCM, haga clic con el botón derecho en Server Intelligence Agent (SIA) y haga clic en *Detener*. No vaya al paso 3 hasta que el estado del SIA sea «Detenido».<br>3. Haga clic con el botón derecho del ratón en el SIA y elija *Propiedades*.<br>4. En la ficha Configuración, haga clic en *Cambiar* junto a *Configuración de clave de clúster del CMS*.<br>5. Se muestra un mensaje de advertencia. Haga clic en Sí para continuar.<br>6. En el cuadro de diálogo *Cambiar clave de clúster*, introduzca la misma clave de ocho caracteres en los campos *Nueva clave de clúster* y *Confirmar nueva clave de clúster*.<br><br>**Nota**<br>El RDT no se ejecutará si el parámetro `dbkey` se omite, o si la clave de clúster es incorrecta.<br><br>**Nota**<br>La clave de clúster mostrada en el CCM está cifrada y no se puede usar en el parámetro `dbkey`.<br><br>Si desea obtener más información sobre las claves de clúster, consulte la sección sobre «seguridad de la plataforma de BI» que encontrará en el *Manual del administrador de la plataforma de Business Intelligence de SAP BusinessObjects*. |
| `inputfrsdir` | Obligatorio | La ruta de acceso de archivos del Servidor del repositorio de archivos de entrada.<br><br>**Nota**<br>La cuenta de usuario con la que se ha iniciado sesión se utiliza para ejecutar la herramienta de la línea de comandos. Debe tener control total en la ubicación del archivo. |

| Parámetro | Opcional u obligatorio | Descripción |
| --- | --- | --- |
| `outputfrsdir` | Obligatorio | La ruta de acceso de archivos del Servidor del repositorio de archivos de salida.<br><br>**Nota**<br>La cuenta de usuario con la que se ha iniciado sesión se utiliza para ejecutar la herramienta de la línea de comandos. Debe tener control total en la ubicación del archivo. |
| `outputdir` | Opcional | La ruta de archivo donde la RDT escribe los archivos de registro.<br><br>El valor predeterminado es `<DIRINSTALACIÓN>\SAP BusinessObjects Enterprise XI 4.0\reposcan` en Windows y `./sap_bobj/enterprisexi_40/reposcan`en Unix. |
| `count` | Opcional | El número de errores aproximados que se explorarán. Contribuye a garantizar un rendimiento óptimo. El número superior es 2e31 - 1. Un valor de 0 se interpreta como el repositorio entero.<br><br>El valor predeterminado es 1000. |
| `repair` | Opcional | Indica a la RDT que repare todas las incoherencias que pueda encontrar. El comportamiento predeterminado es que sólo se informe de las incoherencias pero no se realice ninguna reparación. Si el parámetro `-repair` existe en la línea de comandos, el RDT informa y repara todas las incoherencias.<br><br>**Precaución**<br>Este proceso eliminará los archivos u objetos huérfanos en la base de datos del repositorio. |
| `scanfrs` | Opcional | Especifica si la RDT busca incoherencias en el CMS y el FRS. |
| `scancms` | Opcional | Especifica si la RDT busca incoherencias entre InfoObjects en el CMS. |
| `submitterid` | Opcional | Especifica el ID de usuario para reemplazar ID que faltan o no son válidos para los objetos programados. Si no se proporciona ningún valor, la RDT no reemplaza los ID no válidos. Si el ID de usuario proporcionado no existe en el CMS, la RDT solicita un ID válido.<br><br>Este parámetro sólo se usa cuando la RDT funciona en modo de reparación. |

| Parámetro | Opcional u obligatorio | Descripción |
| --- | --- | --- |
| `startid` | Opcional | Especifica el objeto de la base de datos del CMS por el que se iniciará el análisis. Por ejemplo, si ya ha analizado 500 objetos del repositorio, puede establecer **`-startid=501`** para iniciar un nuevo análisis en el objeto 501.<br><br>El valor predeterminado es **`1`**. |
| `optionsfile` | Opcional | Especifica la ruta de acceso a un archivo de parámetros. El archivo de parámetros es un archivo de texto que enumera cada una de las opciones de la línea de comandos y sus valores. El archivo debe tener un parámetro por línea.<br><br>**Nota**<br><br>Con esta opción, puede establecer todos los parámetros en un archivo de texto como se describe anteriormente. Utilice esta opción para indicar al archivo de parámetros sin necesidad de especificar los parámetros en la línea de comandos. |
| `syscopy` | Opcional | Este parámetro se usa al copiar la base de datos del repositorio. Debe ejecutar la herramienta en la copia creada recientemente, que actualizará la copia para evitar que forme clústeres con los servidores del sistema de origen. Si la copia no va a tener la capacidad de comunicarse con el sistema de origen, no es necesario. Se debe usar únicamente con los parámetros obligatorios, y no se debe combinar con otros parámetros opcionales de esta lista.<br><br>**Nota**<br><br>No ejecute la RDT con el parámetro `syscopy` en su sistema de origen. |
| `trace` | Opcional | Este parámetro genera seguimientos (registros de eventos que ocurren durante la operación de un componente controlado) y los recoge en archivos de registro con la extensión .glf en la ubicación: `<SAP_BOBJ_INST_DIR>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\logging` |

| Parámetro | Opcional u obligatorio | Descripción |
| --- | --- | --- |
| `scankind` | Opcional | Introduzca el tipo de infoObjeto que desee analizar en busca de inconsistencias.<br><br>**Ejemplo**<br>SI_KIND: informes de Web Intelligence y Crystal<br><br>Entre los infoObjetos admitidos que se pueden analizar en busca de inconsistencias se incluyen:<br><br>• carpeta<br>• crystalreport<br>• acceso directo<br>• usuario<br>• usergroup<br>• calendario<br>• conexión<br>• categoría<br>• objectpackage<br>• publicación<br>• pdf<br>• rtf<br>• txt<br>• nota<br>• Word<br>• Excel<br>• arrendatario<br>• perfil<br>• programa<br>• agnóstico<br>• universo<br>• hipervínculo<br>• fullclient<br>• PowerPoint<br>• scopebatch<br>• metadata.dataconnection<br>• webi<br>• qaaws<br>• lcmjob<br>• sobrecarga<br>• xcelsius |

| Parámetro | Opcional u obligatorio | Descripción |
| --- | --- | --- |
| | | • biwidgets<br>• mon.probe<br>• LiveOffice<br>• mdanalysis<br>• visualdiff<br>• ao.workbook<br>• dsl.metadatafile<br>• afdashboardpage<br>• ao.presentation<br>• ccis.dataconnection<br>• platformsearchqueue<br>• metadata.businessview<br>• platformsearchindex<br>• platformsearchcontentstore<br>• platformsearchcontentsurrogate<br><br>**Nota**<br>El xml resultado de scankind muestra la lista de inconsistencias con respecto a los InfoObjetos. En otras palabras, los objetos de archivo afectados no están en la lista. |
| `scandays` | Opcional | Introduzca la cantidad de días para los que RepoScan debe comprobar si hay inconsistencias.<br><br>**Ejemplo**<br>Cualquier número real diferente de 0.<br><br>**Nota**<br>Esta opción funciona según el tiempo del sistema actual. |

La relación no se escanea durante los escaneos parciales. Se producen escaneos parciales si se utiliza una de las tres opciones siguientes:

- startid
- scankind
- scandays

Inconsistencias en las relaciones

| Mensaje de advertencia | Incoherencia | Sugerencia | Acción |
|---|---|---|---|
| `Relation '<Name>' from object ID <ID> has an invalid target (Object ID = <ID>)` | El límite de una relación ya no existe. | Permitir que la aplicación elimine la relación. | Relación eliminada. |

Los siguientes parámetros se usan si se está ejecutando Repository Diagnostic Tool en un CMS agrupado activo.

Uso de la RDT en un CMS agrupado en clúster

| Parámetro | Opcional u obligatorio | Descripción |
|---|---|---|
| `requestport` | Opcional | El número de puerto que usa la RDT para comunicarse con el CMS. Acepta números enteros y positivos. De forma predeterminada, la herramienta usa el valor del sistema operativo del equipo en el que se ejecuta la RDT. |
| `numericip` | Opcional | Indica si la RDT utiliza la dirección IP numérica en vez del nombre de host para la comunicación entre el CMS y el equipo en el que se ejecuta la RDT. Los valores aceptables son **`True`** y **`False`**.<br>El valor predeterminado es **`False`**. |
| `ipv6` | Opcional | El nombre ipv6 del equipo en el que se ejecuta la RDT. Acepta una cadena.<br>El valor predeterminado es el nombre de host del equipo en el que se ejecuta la RDT. |
| `port` | Opcional | El nombre ipv4 del equipo en el que se ejecuta la RDT. Acepta una cadena.<br>El valor predeterminado es el nombre de host del equipo en el que se ejecuta la RDT. |
| `threads` | Opcional | El número de subprocesos que se utilizarán. Acepta números enteros y positivos.<br>El valor predeterminado es **`12`**. |

Los siguientes parámetros se utilizan cuando la RDT usa SSL para comunicarse con la base de datos del CMS que analiza.

Usar la RDT con SSL

| Parámetro | Opcional u obligatorio | Descripción |
|---|---|---|
| `protocol` | Opcional | Especifica si la herramienta se debe ejecutar en modo SSL.<br>El único valor aceptado es **`ssl`**. |
| `ssl_certdir` | Opcional | El directorio que contiene los certificados SSL. |
| `ssl_trustedcertificate` | Opcional | El nombre de archivo del certificado. |
| `ssl_mycertificate` | Opcional | El nombre de archivo del certificado firmado. |
| `ssl_mykey` | Opcional | Nombre del archivo que contiene la clave SSL privada. |
| `ssl_mykey_passphrase` | Opcional | Nombre del archivo que contiene la contraseña de SSL. |

## Ejemplo

El siguiente ejemplo de Windows busca en el CMS y el FRS ambos tipos de incoherencias y repara las que encuentra.

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect «UID=root;PWD=<Password1>;DSN=<myDsn>;HOSTNAME=<myHostname>;PORT=<3306>»
-inputfrsdir «C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Input»
-outputfrsdir    «C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects
Enterprise XI 4.0\FileStore\Output»
-dbkey <cluster key>
-repair
```

## Ejemplo

Ejemplo de Unix:

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Password1>;DSN=<myDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <cluster key>
```

## 32.3 Incoherencias entre el CMS y el FRS

En la siguiente tabla se describen las incoherencias que puede haber en una base de datos del Servidor de administración central (CMS) y los servidores del repositorio de archivos (FRS) que reconoce la herramienta de diagnóstico del repositorio (RDT).

- Mensaje de advertencia
  El mensaje de advertencia que se escribe en los archivos de registro de análisis y reparación.
- Incoherencia
  Una explicación de la incoherencia que la RDT encuentra para el objeto.
- Sugerencia
  La acción que la RDT recomienda cuando encuentra una incoherencia. Se halla en el archivo de registro de análisis.
- Acción
  La acción que la RDT realiza para reparar una incoherencia. Se halla en el archivo de registro de reparación.

| Mensaje de advertencia | Incoherencia | Sugerencia | Acción |
|---|---|---|---|
| `<Nombre de objeto>` objeto `<Tipo de objeto>` (ID de objeto = `<ID>`) hace referencia a archivos que no existen en el FRS (`<Nombre de archivo>`). | El objeto existe en la base de datos del CMS, pero no hay un archivo correspondiente en el FRS. | Permite que la aplicación elimine este objeto. Cualquier objeto que sea descendiente de este objeto también será eliminado. | Objeto eliminado del repositorio. |
| El archivo `<Nombre de archivo>` existe en el FRS de entrada o de salida, pero no hay un InfoObject correspondiente en el repositorio. | El archivo existe en el FRS, pero no hay un archivo correspondiente en la base de datos del CMS. | Permite que la aplicación elimine este archivo no vinculado. | No se realiza ninguna acción. |
| `<Tipo de objeto>` Objeto `<Nombre de objeto>` (ID de objeto = `<ID>`) tiene un tamaño de archivo `<Nombre de archivo>`. El tamaño de archivo almacenado es `<Tamaño>` bytes, que no concuerda con el tamaño real del archivo de `<Tamaño>` bytes. | El tamaño del archivo no coincide con el tamaño de archivo del InfoObject. | Permitir que la aplicación actualice el objeto con el tamaño de archivo correcto. | Actualiza el objeto para obtener el tamaño de archivo correcto. |
| Este directorio no contiene archivos. | La carpeta FRS está vacía. | Permitir que la aplicación elimine el directorio. | Elimina la carpeta vacía. |

## 32.4 Incoherencias en los metadatos de CMS

En la siguiente tabla se describen las incoherencias que se pueden producir en los metadatos de los objetos que están en una base de datos de sistema del Servidor de administración central (CMS) que reconoce la Herramienta de diagnóstico del repositorio (RDT).

- Mensaje de advertencia
  El mensaje de advertencia que se escribe en los archivos de registro de análisis y reparación.
- Incoherencia
  Una explicación de la incoherencia que la RDT encuentra para el objeto.
- Sugerencia
  La acción que la RDT recomienda cuando encuentra una incoherencia. Se halla en el archivo de registro de análisis.
- Acción
  La acción que la RDT realiza para reparar una incoherencia. Se halla en el archivo de registro de reparación.

| Mensaje de advertencia | Incoherencia | Sugerencia | Acción |
|---|---|---|---|
| `<Tipo de objeto>` Objeto `<Nombre de objeto>` (ID de objeto = `<ID>`) Objeto superior que falta (ID de objeto superior = `<ID>`). | Al objeto le falta un ID de objeto principal o el que tiene no es válido. | Permite que la aplicación mueva el objeto a la carpeta "Reparación BOE". | Mueve el objeto y sus objetos secundarios a la carpeta Reparación BOE. |
| `<Tipo de objeto>` Objeto `<Nombre de objeto>` (ID de objeto = `<ID>`) falta el objeto de propietario (ID de objeto de propietario = `<ID>`). | Al objeto le falta un ID de objeto de propietario o el que tiene no es válido. | Permitir que la aplicación asigne el objeto al administrador. | Asigna el objeto al administrador. |
| `<Tipo de objeto>` Objeto `<Nombre de objeto>` (ID de objeto: `<ID>`), falta objeto remitente (ID de objeto remitente = `<ID >`). | Al objeto le falta un ID de objeto remitente o el que tiene no es válido. | La recomendación que muestra la RDT depende de si ha proporcionado un valor para el parámetro `-submitterid`.<br>• Si proporciona este parámetro, la recomendación es «Permitir que la aplicación actualice el objeto con el ID de remitente proporcionado».<br>• Si no proporciona este parámetro, la recomendación es «Reprograme el objeto o envíe un ID de usuario para reemplazar el ID de remitente no válido». | Si proporciona un valor para el parámetro `-submitterid` , la RDT aplica el valor para el ID de remitente del objeto.<br>Si no proporciona ningún valor para este parámetro, la RDT no realiza ninguna acción. Al reprogramar el objeto, el CMS aplica un nuevo ID. |
| `<Tipo de objeto>` Objeto '`<Nombre de objeto>`' (ID de objeto = `<ID>`) la propiedad de la última instancia correcta se refiere a un objeto que no se | Falta la última instancia correcta del objeto o no es válida. | Permitir que la aplicación vuelva a calcular la propiedad. | Vuelve a calcular la propiedad. |

| Mensaje de advertencia | Incoherencia | Sugerencia | Acción |
|---|---|---|---|
| encuentra (ID de objeto de la última instancia correcta = <ID>). | | | |
| <Tipo de objeto> Objeto '<Nombre de objeto'> (ID de objeto = <ID>)' objeto de calendario que falta (ID de objeto de calendario = <ID>). | El objeto hace referencia a un calendario que no existe. | Vuelva a programar el objeto con un calendario existente. Esta aplicación no puede realizar ninguna acción. | No se realiza ninguna acción. |
| <Tipo de objeto> Objeto '<Nombre de objeto>' (ID de objeto = <ID>)' Grupo de servidores de programación obligatorio que falta (ID de objeto de grupo de servidores = <ID>). | El servidor preferido no existe. | Reprograme el objeto y elija un grupo de servidores existente. Esta aplicación no puede realizar ninguna acción. | No se realiza ninguna acción. |
| <Tipo de objeto> Objeto '<Nombre de objeto>' (ID de objeto = <ID>)' Lista de eventos pendientes que contiene objetos que faltan (ID de objeto de evento = <ID>). | El evento o los eventos que espera este objeto no existen. | Vuelve a programar el objeto para esperar los objetos de evento existentes. Esta aplicación no puede realizar ninguna acción. | No se realiza ninguna acción. |
| <Tipo de objeto> Objeto '<Nombre de objeto>' (ID de objeto = <ID>)' Lista de eventos a desencadenar que contiene objetos que faltan (ID de objeto de evento = <ID>). | Este objeto desencadena un evento que no existe. | Permitir que la aplicación elimine los eventos que faltan de la lista de eventos que activar del objeto. | Elimina los eventos que faltan de la lista de objetos de eventos a desencadenar. |
| <Tipo de objeto> Objeto '<Nombre de objeto>' (ID de objeto = <ID>)' Lista de control de acceso que hace referencia a un principal que falta (ID de objeto principal = <ID>). | Entrada de control de acceso huérfana. | Permitir que la aplicación elimine de la lista de control de acceso del objeto el objeto principal que falta. | Elimina el objeto principal que falta de la lista de control de acceso del objeto. |
| <Tipo de objeto> Objeto '<Nombre de objeto>' (ID de objeto = <ID>)' Lista de control de acceso que hace referencia a un nivel de acceso que falta (ID de objeto de nivel de acceso = <ID>). | Entrada de control de acceso huérfana. | Permitir que la aplicación elimine de la lista de control de acceso del objeto el objeto principal que falta. | Elimina el nivel de acceso que falta de la lista de control de acceso del objeto. |
| <Tipo de objeto> Objeto <Nombre de objeto> (ID de objeto = <ID>) tiene varias carpetas de favoritos | Una cuenta de usuario específica tiene varias carpetas Favoritos. | Permitir que la aplicación consolide varias carpetas en una sola carpeta Favoritos. | Todas las carpetas de favoritos se han consolidado en una única carpeta Favoritos. |

| Mensaje de advertencia | Incoherencia | Sugerencia | Acción |
|---|---|---|---|
| `<Tipo de objeto>` Objeto`<Nombre de objeto>` (ID de objeto = `<ID>`) contiene entradas de archivo de entrada no válidas (`<Archivos>`). | El objeto contiene entradas no válidas en la lista de archivos de entrada. | Permitir que la herramienta quite las entradas no válidas del objeto de su lista de grupos de servidores. | Elimina las entradas no válidas de la lista de archivos de entrada de objetos. |
| `<Tipo de objeto>` Objeto`<Nombre de objeto>` (ID de objeto = `<ID>`) contiene entradas de archivo de entrada no válidas (`<Archivos>`) | El objeto contiene entradas no válidas en la lista de archivos de salida. | Permitir que la herramienta quite las entradas no válidas del objeto de su lista de grupos de servidores. | Elimina las entradas no válidas de la lista de archivos de salida de objetos. |
| `<Tipo de objeto>` Objeto '`<Nombre de objeto>`' (ID de objeto = `<ID>`)' Grupo de servidores de programación obligatorio que falta (ID de objeto de grupo de servidores = `<ID>`). | Falta el objeto en el grupo de servidores de caché requerido. | Reprograme el objeto y elija un grupo de servidores existente. | No se realiza ninguna acción. |
| `<Tipo de objeto>` Objeto '`<Nombre de objeto>`' (ID de objeto = `<ID>`)' Grupo de servidores de programación obligatorio que falta (ID de objeto de grupo de servidores = `<ID>`). | Falta el objeto en el grupo de servidores de procesamiento requerido. | Reprograme el objeto y elija un grupo de servidores existente. | No se realiza ninguna acción. |
| `<Tipo de objeto>` Objeto `<Nombre de objeto>` (ID de objeto = `<ID>`)' Lista de perfiles que contiene objetos que faltan (ID de objeto de perfil = `<ID>`). | El objeto contiene objetos que faltan en la lista de perfiles. | Actualice la publicación con perfiles existentes. Esta aplicación no puede realizar ninguna acción. | No se realiza ninguna acción. |

## 32.5 Gestionar SDK restaurado dentro de BOE WebApp

Para activar la parte BIPRWS WebApp de la aplicación web BOE en 4.3 SP03, fije el indicador en *verdadero* en la siguiente ubicación:

```
<BOE_INST_DIR>\SAP BusinessObjects\tomcat\webapps\BOE\WEB-
INF\internal\Global.properties
```

Fije `use.boe.internal.biprws=true`

Cuando el indicador se fija en verdadero, las aplicaciones internas no dependen de la dirección URL de la aplicación Restful o de la marca de ruta relativa establecida en la CMC.

La función es ventajosa, ya que ayuda a evitar lo siguiente:

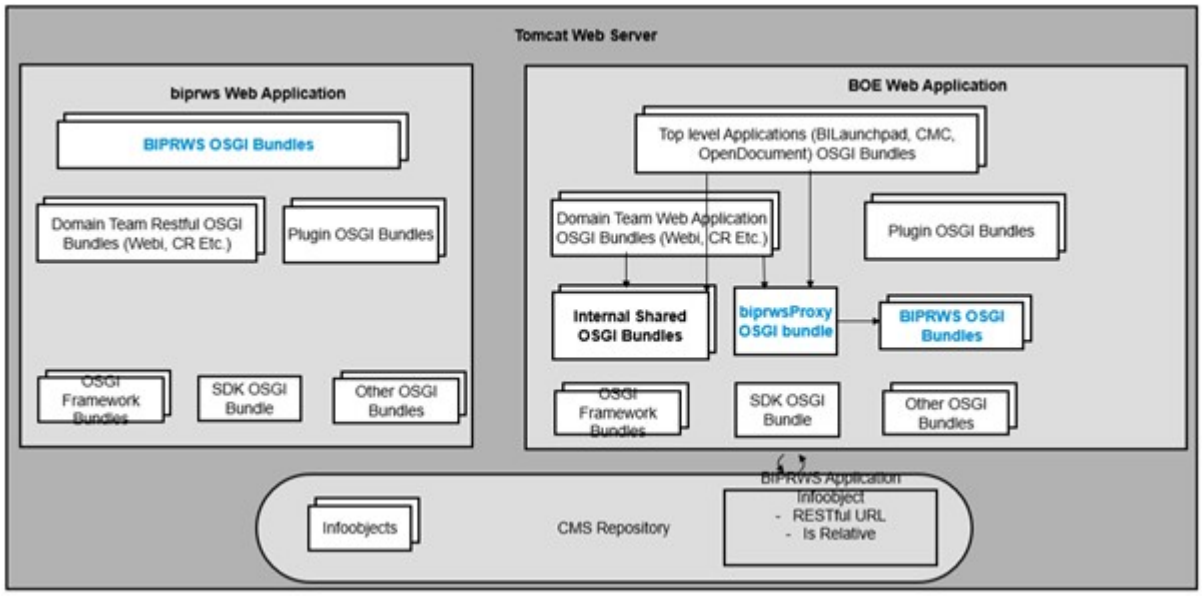
- Problemas de CORS (Cross-Origin Resource Sharing).
- Problemas de conectividad del sistema interno y externo.
- Ping de BOE WebApp para mantener la sesión activa.
- Problemas relacionados con el proxy ya que no hay una configuración independiente para BIPRWS y BOE.
- Problemas relacionados con el clúster de aplicaciones web.

La implementación existente con la aplicación web BOE funciona sin problemas después de la actualización.

**Grabación en log**:

Una vez que BIPRWS se fusiona en la aplicación web BOE, los logs se generan como parte de la ubicación del registro de la aplicación CMC o de la rampa de lanzamiento BI.

**Arquitectura**:



# 33 Seguridad estricta de transporte HTTP (HSTS)

## 33.1 Configuración de HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) es un mecanismo de políticas para proteger a los sitios web contra ataques man-in-the-middle como ataques de degradación de protocolo y secuestro de cookies.

Permite a los servidores web declarar que los navegadores web (u otros agentes de usuario conformes) deben interactuar automáticamente con él utilizando solo conexiones HTTPS. Esto proporciona seguridad de la capa de transporte (TLS/SSL), a diferencia del uso de HTTP inseguro.

HSTS es un protocolo de seguimiento de estándares IETF y se especifica en RFC 6797.

El servidor comunica la política HSTS al agente de usuario a través de un campo de cabecera de respuesta HTTP llamado "Strict-Transport-Security".

1. Esta política especifica un período durante el cual el agente de usuario solo debe acceder al servidor de forma segura.
2. Los sitios web que usan HSTS a menudo no aceptan texto claro HTTP, ya sea rechazando conexiones sobre HTTP o redirigiendo sistemáticamente a los usuarios a HTTPS (aunque esto no es requerido por la especificación).
   Esto es para asegurarse de que un agente de usuario que no sea capaz de realizar TLS no pueda conectarse al sitio.
3. La protección solo se aplica después de que un usuario haya visitado el sitio al menos una vez confiando en el principio de confianza en el primer uso.

**Cómo funciona**

Cuando un usuario introduce o selecciona una URL para el sitio que especifica HTTP, la URL se actualiza automáticamente a HTTPS sin realizar una solicitud HTTP. Esto evita que se produzca el ataque HTTP man-in-the-middle.

En 4.3 SP03, SAP BOE admite el acuerdo HSTS.

Antes de configurar HSTS, su servidor de aplicación debe estar configurado con SSL.

Para activar el soporte HSTS, siga los pasos que se indican a continuación:

1. Detenga Tomcat.
2. Navegue a `E:\Program Files (x86)\SAP BusinessObjects\tomcat\webapps\BOE\WEB-INF\config\default`
3. Abra el archivo Global.properties y establezca los parámetros siguientes.
   1. `hsts.enabled` Verdadero/Falso. Valor predeterminado fijado en falso.
   2. `hsts.Include.SubDomains` Verdadero /Falso: afecta a todos los subdominios del nombre de dominio.

   3. `hsts.MaxAge.Seconds` = 31536000.
   4. Predeterminado = 365 días.
4. Guarde los cambios.

# 34 Apéndice de derechos

## 34.1 Acerca del apéndice de derechos

En este apéndice de derechos se enumera y describe la mayoría de los derechos que se pueden configurar en distintos objetos en el sistema de la plataforma de BI. En los casos en que se necesita más de un derecho para realizar una tarea en un objeto, también proporciona información acerca de los derechos adicionales que se requieren y los objetos sobre los que debe tener esos derechos. Para obtener más información acerca de la configuración de derechos, consulte el capítulo *Configuración de derechos* en *Manual de administrador de la plataforma de SAP BusinessObjects Business Intelligence*.

## 34.2 Derechos generales

Los derechos de esta sección se aplican a varios tipos de objeto. Muchos de estos derechos también tienen derechos de propietario equivalentes. Los derechos de propietario son derechos que solo se aplican al propietario del objeto en el que se comprueban los derechos.

Los siguientes derechos solo se aplican a objetos que se pueden programar:

- El derecho *Programar el documento que debe ejecutarse*.
- El derecho*Programar en nombre de otros usuarios*.
- El derecho *Programar para destinos*.
- El derecho *Ver instancias de documento*.
- El derecho *Eliminar instancias*.
- El derecho *Poner en pausa y reanudar instancias de documento*.
- El derecho *Reprogramar instancias*.

| Derecho | Descripción |
|---|---|
| *Ver objetos* | Permite ver objetos y sus propiedades. Si no dispone de este derecho sobre un objeto, el objeto estará oculto en el sistema de la plataforma de BI. Este derecho es un derecho básico requerido para todas las tareas. |
| *Agregar objetos a la carpeta* | Permite agregar objetos a una carpeta. Este derecho también se aplica a objetos que se comportan como carpetas, como bandejas de entrada, carpetas de `favoritos` o paquetes de objetos. |
| *Editar objetos* | Permite editar el contenido del objeto y las propiedades de objetos y carpetas. |

| Derecho | Descripción |
| --- | --- |
| *Modificar los derechos de los usuarios para los objetos* | Permite modificar la configuración de seguridad para un objeto. |
| *Modificar de forma segura los derechos que tienen los usuarios sobre los objetos que son propiedad del usuario* | Permite conceder derechos o niveles de acceso que ya tiene sobre un objeto a otros usuarios. Para ello, necesita este derecho sobre el usuario y el objeto propiamente dicho. Para obtener más información acerca de este derecho, consulte el capítulo «Configuración de derechos» del *Manual del administrador de la plataforma SAP BusinessObjects Business Intelligence*. |
| *Definir grupos de servidor para procesar tareas* | Permite especificar el grupo de servidores que se usará cuando se procesen los objetos. Este derecho solo se aplica a objetos para los que se pueden especificar servidores de procesamiento.<br><br>Para especificar un grupo de servidores, también necesitará el derecho *Editar objetos* sobre el objeto. |
| *Eliminar objetos* | Permite eliminar objetos y sus instancias. |
| *Copiar objetos en otra carpeta* | Permite crear copias de objetos en otras carpetas del CMS. Para hacerlo, también necesita el derecho *Agregar objetos a la carpeta* sobre la carpeta de destino.<br><br>**Nota**<br>Cuando se copia un objeto, la seguridad explícita en él no se copia; el nuevo objeto hereda la configuración de seguridad de la carpeta de destino, pero debe restablecer la seguridad explícita. |
| *Repetir contenido* | Permite replicar objetos a otro sistema en un despliegue federado. |
| *Programar el documento que debe ejecutarse* | Permite programar objetos. |
| *Programar en nombre de otros usuarios* | Permite programar objetos para otros usuarios o grupos. El usuario o grupo para el que se programa el objeto se convierte en propietario de la instancia del objeto.<br><br>Para programar un objeto para otros usuarios o grupos, también necesitará los siguientes derechos:<br>• Este derecho sobre el usuario o grupo.<br>• El derecho *Programar el documento que debe ejecutarse* sobre el objeto. |
| *Programar para destinos* | *Programar para destinos* es el superior derecha de *Planificación para FTP, SMTP, bandeja de entrada de BI,* |

| Derecho | Descripción |
| --- | --- |
| | *SFTP* y *Sistema de archivos*. Debería seleccionar *Programar para destinos* junto con la combinación con el nivel inferior específico para programar un objeto para un determinado destino. Por ejemplo, debería seleccionar los derechos *Programar para destinos Programar para FTP* para programar un objeto para un destino FTP. Si está actualizando la infraestructura de BI de 4.2 SP04 o anterior para BI 4.2 SP05 o posterior, consulte 2675734, 2642221, 2626550 para más información sobre la resolución de problemas.<br><br>Para programar el objeto para otros destinos, también necesitará los siguientes derechos:<br><br>• El derecho *Programar el documento que debe ejecutarse* sobre el objeto que se va a programar.<br>• El derecho *Agregar objetos a la carpeta* sobre la bandeja de entrada del destinatario (si desea programar en un destino de bandeja de entrada).<br>• El derecho *Copiar objetos en otra carpeta* sobre el objeto que se va a programar (si desea enviar una copia a un destino de bandeja de entrada en lugar de un acceso directo).<br><br>**Nota**<br><br>Si el derecho *Programar en destino* está asignada mediante roles *Nivel de acceso* como *Control total* o *Programar* en BI 4.2 SP04 o anterior, tras la actualización a BI 4.2 SP05 revisión 03 o posterior, el destino de nivel inferior como, por ejemplo, *Programar FTP, SMTP, SFTP, bandeja de entrada de BI* y *Sistema de archivos* también están garantizados. Para *Niveles de acceso* como *Ver a petición* y roles *personalizados* existentes en BI 4.2 SP04 o anterior, tras la actualización a BI 4.2 SP05 revisión 03 o posterior, el destino del hijo derechos no se concede de manera predeterminada. Debería otorgar los derechos manualmente. Por tanto, el job de programación de repetición creado en BI 4.2 SP04 o anterior programará objetos correctamente en BI 4.2 SP05 revisión 03 o posterior. |
| *Programar para FTP* | Le permite programar un objeto para un destino FTP. |
| *Programar para SFTP* | Le permite programar un objeto para un destino SFTP. |
| *Programar para SMTP* | Le permite programar un objeto para un destino SMTP. |
| *Programar para sistema de ficheros* | Le permite programar un objeto para un destino de sistema de ficheros. |
| *Programar para bandeja de entrada de BI* | Le permite programar un objeto para un destino de bandeja de entrada de BI. |

| Derecho | Descripción |
| --- | --- |
| *Ver instancias de documento* | Permite ver instancias de objeto. Este derecho es un derecho básico requerido para todas las tareas que se realizan en instancias de objeto. |
| *Eliminar instancias* | Permite eliminar únicamente instancias de objeto. Si dispone del derecho *Eliminar objetos*, no necesita este derecho para eliminar instancias. |
| *Poner en pausa y reanudar instancias de documento* | Permite poner en pausa o reanudar las instancias de objeto que se están ejecutando. |
| *Reprogramar instancias* | Permite reprogramar instancias de objeto. |
| *Añadir comentarios: Comentario BI* | Permite que un usuario añada comentarios a un documento utilizando Comentario BI. |
| | |
| | |
| | |
| *Borrar comentarios: Comentario BI* | Permite que un usuario borre comentarios de un documento utilizando Comentario BI. |
| | |
| *Borrar comentarios que el usuario ha creado con Comentario BI* | Permite que un usuario borre comentarios que él mismo ha creado de un documento utilizando Comentario BI. |
| | |
| *Modificar comentarios: Comentario BI* | Permite que un usuario modifique comentarios de un documento utilizando Comentario BI. |
| | |
| *Borrar comentarios que el usuario ha creado con Comentario BI* | Permite que un usuario modifique comentarios que él mismo ha creado de un documento utilizando Comentario BI. |
| | |
| *Ver comentarios: Comentario BI* | Permite que un usuario vea comentarios de un documento utilizando Comentario BI. |
| | |
| *Ver comentarios que el usuario ha creado con Comentario BI* | Permite que un usuario vea comentarios que él mismo ha creado de un documento utilizando Comentario BI. |
| *Ocultar comentarios: Comentario BI* | Permite que un usuario oculte comentarios de un documento mediante Comentario BI. |
| *Ocultar comentarios que el usuario ha creado: Comentario BI* | Permite que un usuario oculte comentarios que ha creado de un documento mediante Comentario BI. |
| | |
| | |

| Derecho | Descripción |
| --- | --- |
| *Añadir comentarios no filtrados: Comentario BI* | Permite que un usuario migre los comentarios junto con el documento. |

## 34.2.1 Derechos de destino

Cada destino está asociado a un derecho de destino específico. El administrador de BOE debe garantizar que los usuarios tienen los derechos de destino deseados.

Antes, cuando un usuario tenía un derecho *Programar para destinos*, podía programar en todos los destinos disponibles. A partir de la versión SP05, se han concedido a los usuarios derechos de destino individuales en los que *Programar para destinos* solo se corresponde con *Ubicación de Enterprise por defecto*.

Se han introducido derechos nuevos en Derechos generales para cada destino:

- Programar para sistema de archivos
- Programar para FTP
- Programar para bandeja de entrada
- Programar para SFTP
- Programar para SMTP
- Programar para Google Drive

Para obtener más información sobre los *Derechos generales*, consulte Derechos generales [página 1140].

Para proporcionar estas opciones de destino al efectuar la programación, el administrador debe conceder los respectivos derechos de destino individuales. Consulte 2621878. Si el usuario tiene un derecho solo en *Programar para destinos*, no podrá programar en el FTP, la bandeja de entrada, SFTP, SMTP ni el sistema de archivos de destino.

Si se ha asignado el derecho *Programar para destinos* en una versión anterior mediante el nivel de acceso, como los roles Control total o Programación, después de una actualización a la versión 4.2 SP05 también se concederán derechos adicionales (introducidos recientemente). De este modo, la programación se efectuará correctamente en cualquier destino.

Si se asigna mediante el nivel de acceso *Ver a petición*, cualquier rol personalizado o asignado directamente (derecho individual, no por cualquier rol), solo se podrá programar en *Ubicación de Enterprise por defecto* (los demás destinos fallarán).

Para obtener más información, consulte Opciones de destino y Propiedades de destino de correo electrónico.

## 34.3 Derechos para tipos de objeto específicos

### 34.3.1 Derechos de carpeta

Para facilitar la administración de derechos, se recomienda establecer derechos en las carpetas, de modo que sus contenidos hereden la configuración de seguridad. Los derechos de carpeta incluyen lo siguiente:

- Derechos generales que se aplican al objeto de carpeta.
- Derechos específicos de tipo dirigidos a los contenidos de la carpeta (como el derecho *Imprimir datos del informe* sobre los informes de Crystal).

### 34.3.2 Categorías

Los derechos de esta sección son derechos generales con un significado específico en el contexto de las categorías públicas y personales.

> **Nota**
>
> Los objetos en las categorías no heredan los derechos establecidos en las categorías.

| Derecho | Descripción |
|---|---|
| *Agregar objetos a la carpeta* | Permite crear categorías nuevas dentro de categorías.<br>Este derecho no es necesario para agregar objetos a una categoría. |
| *Editar objetos* | Permite hacer lo siguiente:<br>• Modificar las propiedades de la categoría.<br>• Mover la categoría a otra categoría como subcategoría.<br>• Agregar objetos a la categoría.<br>• Eliminar objetos de la categoría.<br>Para mover una categoría a otra categoría como subcategoría, necesitará también los siguientes derechos:<br>• El derecho *Eliminar objetos* sobre la categoría original.<br>• El derecho *Agregar objetos a la carpeta* sobre la categoría de destino. |
| *Eliminar objetos* | Permite eliminar la categoría. |

### 34.3.3 Informes de Crystal

Los derechos de esta sección solo se aplican a los informes de Crystal.

> **Nota**
>
> Estos derechos solo se aplican cuando los informes de Crystal se encuentran en el entorno de la plataforma de BI. Cuando se descargan los informes de Crystal al disco local, estos derechos no tienen efecto. Para impedir este comportamiento, puede denegar el derecho *Descargar archivos asociados con el objeto* en el informe de Crystal.

| Derecho | Descripción |
|---|---|
| *Imprimir datos del informe* | Permite imprimir el informe. |
| *Actualizar datos del informe* | Permite actualizar datos del informe. |
| *Exportar datos del informe* | Permite exportar datos del informe en cualquier formato mientras ve el informe en línea en el visor de Crystal Reports.<br><br>Para exportar datos del informe en formato RPT, también necesitará el derecho *Descargar archivos asociados con el objeto*. |
| *Descargar archivos asociados con el objeto* | Este derecho permite hacer lo siguiente:<br>• Exportar el informe en formato RPT.<br>• Abra el informe en Crystal Reports Designer.<br>• Programe el informe en formato RPT para destinos externos. |

## 34.3.4 Documentos de Web Intelligence

Los derechos de esta sección solo se aplican a documentos de Web Intelligence.

| Derecho | Descripción |
|---|---|
| *Utilizar lista de valores* | Permite usar listas de valores. |
| *Exportar datos del informe* | Permite a un usuario exportar datos de informes al formato de texto, CSV, Excel, PDF o HTML. Este comando también permite utilizar el comando Imprimir que genera un archivo PDF que se puede imprimir. |
| *Script de consulta - Activar visualización (SQL, MDX...)* | Permite ver secuencias de comandos de consulta (SQL y MDX). |
| *Secuencia de comandos de consulta - Activar edición (SQL, MDX...)* | Permite tratar secuencias de comandos de consulta (SQL y MDX). También permite tratar fuentes de datos de SQL manual (FHSQL). |
| *Actualizar los datos del informe* | Permite actualizar datos del documento. |

| Derecho | Descripción |
| --- | --- |
| *Editar consulta* | Permite editar consultas en el documento. |
| *Actualizar lista de valores* | Permite actualizar listas de valores para peticiones cuando se crea la petición o cuando se visualiza el documento. Para ello, también necesita el derecho *Usar listas de valores* sobre el documento. |
| *Enviar a* | Permite enviar documentos a Scheduler, a una bandeja de entrada de la plataforma de BI o enviarlos como hipervínculos en correos electrónicos. Este derecho también permite a los usuarios del cliente enriquecido de Web Intelligence enviar documentos como datos adjuntos en correos electrónicos. |

## 34.3.5 Usuarios y grupos

Puede configurar derechos sobre usuarios y grupos como lo hace sobre otros objetos en el entorno de la plataforma de BI. Los derechos de esta sección son derechos específicos de tipo que solo se aplican a objetos de usuario y grupo o bien derechos generales con un significado específico en el contexto de usuarios y grupos.

> **Nota**
>
> Los usuarios y subgrupos pueden heredar derechos de la pertenencia al grupo.

> **Nota**
>
> El creador de una cuenta de usuario se considera el propietario de la cuenta. Sin embargo, una vez creada la cuenta de usuario, el usuario para el que se crea la cuenta también se considera propietario.

| Derecho | Descripción |
| --- | --- |
| *Editar objetos* | Permite hacer lo siguiente:<br>• Editar propiedades para el usuario o grupo.<br>• Administrar la pertenencia al grupo.<br>Para agregar un usuario o grupo a otro grupo, necesita tener este derecho sobre el usuario o grupo y sobre el grupo de destino. |
| *Cambiar contraseña de usuario* | Permite hacer lo siguiente:<br>• Cambiar la contraseña de la cuenta de usuario. Para hacerlo, también necesitará el derecho *Editar objetos* sobre su cuenta de usuario. |

| Derecho | Descripción |
| --- | --- |
| | • Cambiar la contraseña de la cuenta de otro usuario. Para ello, también necesita el derecho *Editar objetos* y el derecho *Modificar los derechos de los usuarios para los objetos* sobre la cuenta de usuario.<br><br>**Nota**<br>Este derecho no afecta a las siguientes configuraciones de contraseña de usuario:<br>*La contraseña nunca caduca*<br>*El usuario debe cambiar la contraseña la próxima vez que se conecte*<br>*El usuario no puede cambiar la contraseña*<br><br>**Nota**<br>Este derecho no se aplica a las credenciales de origen de datos para universos de SAP Business Objects. |
| *Suscribirse a publicaciones* | Permite agregar el usuario a publicaciones como destinatario. |
| *Programar en nombre de otros usuarios* | Permite programar objetos en nombre del usuario, de modo que éste se convierte en propietario de la instancia de objeto. Para ello, también necesitará el derecho *Programar en nombre de otros usuarios* sobre el objeto. |
| *Agregar o editar atributos de usuario* | Permite cambiar el valor de la dirección de correo electrónico de un usuario o los atributos de usuario personalizados.<br><br>Este derecho se aplica a los usuarios. |
| *Agregar o editar atributos de usuario (derecho de propietario)* | Permite al propietario de un objeto de usuario cambiar el valor de la dirección de correo electrónico del usuario o los atributos de usuario personalizados.<br><br>Este derecho se aplica a los usuarios. |
| *Modificar preferencias en objetos que son propiedad del usuario* | Muestra el menú *Preferencias* en un objeto de aplicación.<br><br>Sin este derecho de acceso, el usuario no puede fijar las preferencias personales en ninguna aplicación, por lo que no le aparecerá el menú Preferencias en las aplicaciones. Por ejemplo, sin este derecho, los usuarios no pueden seleccionar la unidad de medida (pulgadas o milímetros) que utilizarán en los informes de Web Intelligence o en la aplicación de la plataforma de lanzamiento de BI. |

## 34.3.6 Niveles de acceso

Los derechos de esta sección solo se aplican a los niveles de acceso.

| Derecho | Descripción |
| --- | --- |
| *Usar el nivel de acceso para la asignación de seguridad* | Permite asignar el nivel de acceso cuando se agrega principales a las listas de control de acceso para objetos. Para ello, también necesita el derecho *Modificar los derechos de los usuarios para los objetos* o el derecho *Modificar de forma segura los derechos de los usuarios para los objetos* en el principal y el objeto. En los casos en que se concede el derecho *Modificar de forma segura los derechos de los usuarios para los objetos*, también debe disponer de idéntico nivel de acceso concedido a sí mismo en el objeto. |

## 34.3.7 Derechos de universo (.unv)

Los derechos de esta sección se aplican a los universos creados con la herramienta de diseño de universos, o los universos .unv. Los derechos enumerados son derechos específicos de tipo que solo se aplican a universos o bien derechos generales con un significado específico en el contexto de los universos.

> **Nota**
>
> Los derechos de universo solo se aplican al importar universos del CMS en la aplicación herramienta de diseño de universos. Los derechos no se aplican cuando el universo se guarda en el disco local.

| Derecho | Descripción |
| --- | --- |
| *Agregar objetos a la carpeta* | Permite agregar conjuntos de restricciones u objetos al universo. Para ello, también necesita el derecho *Editar restricciones de acceso*. |
| *Ver objetos* | Permite acceder y ver el universo. |
| *Editar objetos* | Este derecho permite hacer lo siguiente:<br>• Editar el universo en la CMC como en la herramienta de diseño de universos.<br>• Bloquee o desbloquee el universo.<br>Para desbloquear un universo, también necesita el derecho *Desbloquear universo*. |
| *Eliminar objetos* | Permite eliminar el universo. |
| *Traducir objetos* | Permite guardar los nombres de objeto de universos traducidos con la herramienta de administración de traducciones. |

| Derecho | Descripción |
| --- | --- |
| | **Nota**<br>Asimismo puede guardar traducciones si se le ha concedido explícitamente el derecho *Editar objetos* y no se le ha denegado explícitamente el derecho *Traducir objetos*. |
| *Nueva lista de valores* | Este derecho permite hacer lo siguiente:<br>• Asociar nuevas listas de valores a objetos.<br>• Editar listas de valores existentes.<br>**Nota**<br>Este derecho no impide crear listas de valores en cascada. |
| *Imprimir universo* | Permite imprimir el universo. |
| *Mostrar valores de tabla u objeto* | Permite ver los valores asociados a tablas u objetos en el universo. |
| *Editar restricciones de acceso* | Permite editar restricciones de acceso (sobrecargas) para el universo. |
| *Desbloquear universo* | Permite hacer lo siguiente:<br>• Desbloquear el universo si está bloqueado por otro usuario.<br>• Exportar el universo del CMS.<br>Para desbloquear un universo, también necesita el derecho *Editar objetos*. |
| *Acceso a datos* | Permite recuperar datos del universo y actualizar documentos basados en el universo. Para ello, también necesita tener este derecho sobre la aplicación herramienta de diseño de universos, el documento y la conexión de universo. |
| *Crear y editar consultas basadas en universo* | Permite crear documentos y editar consultas basadas en el universo. |

## 34.3.8 Derechos de universos (.unx)

Los derechos de esta sección se aplican a los universos creados con la herramienta de diseño de información, o los universos .unx. Los derechos enumerados son derechos específicos de tipo que solo se aplican a universos o bien derechos generales con un significado específico en el contexto de los universos.

> **Nota**
>
> Los derechos de universo se aplican solo a los universos publicados en un repositorio. Estos derechos no se aplican cuando el universo se guarda en una carpeta local.

| Derecho | Descripción |
| --- | --- |
| *Ver objetos* | Permite acceder y ver el universo. |
| *Editar objetos* | Permite volver a publicar el universo. |
| *Eliminar objetos* | Permite eliminar el universo. |
| *Recuperar universo* | Permite recuperar un universo publicado y editar los recursos subyacentes (capa comercial e infraestructura de datos) en la herramienta de diseño de información.<br>**Nota**<br>Asimismo debe disponer del derecho de la aplicación herramienta de diseño de información *Recuperar universo*. |
| *Editar perfiles de seguridad* | Permite insertar, editar y eliminar perfiles de seguridad para el universo en el editor de seguridad de la herramienta de diseño de información.<br>**Nota**<br>Este derecho no es necesario para ver perfiles de seguridad o para cambiar las opciones de agregación del perfil de seguridad. |
| *Asignar perfiles de seguridad* | Permite asignar y desasignar perfiles de seguridad a los usuarios y grupos en el editor de seguridad de la herramienta de diseño de información. |
| *Acceso a datos* | Permite recuperar datos del universo y actualizar documentos basados en el universo.<br>En la herramienta de diseño de información, este derecho permite obtener una vista preliminar del conjunto de resultados del panel de consulta. |
| *Crear y editar consultas basadas en este universo* | Permite crear y editar consultas basadas en el universo.<br>En la herramienta de diseño de información, este derecho le permite abrir el panel de consulta y ejecutar una consulta sobre el universo. |
| *Guardar para todos los usuarios* | Permite guardar el universo para todos los grupos. |

| Derecho | Descripción |
| --- | --- |
| | **Nota**<br>Asimismo se le debe haber concedido el derecho de la aplicación herramienta de diseño de información *Guardar para todos*. |

## 34.3.9 Niveles de acceso a objeto de universo

Cuando los diseñadores crean un universo usando la herramienta de diseño de universos o una capa comercial con la herramienta de diseño de información, asignan un nivel de acceso a objeto a cada objeto del universo. Los niveles de acceso a objeto son:

Público (predeterminado)
Controlado
Restringido
Confidencial
Privado

Una vez que el objeto se publica en el repositorio, puede conceder acceso a los objetos del universo en función de los niveles de acceso a objeto asignados en la aplicación. Por ejemplo, puede conceder acceso Público al grupo Todos. Esto permite a los usuarios del grupo Todos ver los objetos del universo designado como Público.

Cada nivel de acceso a objeto concede más acceso a los objetos que el anterior. Público es el nivel inferior. Las entidades de seguridad que cuentan con acceso Público solo pueden ver los objetos designados como Público. Las entidades de seguridad que cuentan con acceso Controlado pueden ver objetos designados como Público o Controlado. Privado es la configuración de nivel superior y concede a las entidades de seguridad acceso a todos los niveles de acceso a objeto; en otras palabras, a todos los objetos del universo.

> **Nota**
> La configuración de seguridad de nivel de acceso a objeto anula cualquier configuración de seguridad que herede el universo.

> **Nota**
> Para los universos .unx, las configuraciones de seguridad de nivel de acceso a objeto se tienen en cuenta con la seguridad de objeto definida por el perfil de seguridad. Para obtener más información sobre los perfiles de seguridad, consulte el *Manual del usuario de la herramienta de diseño de información*.

### Información relacionada

Asignación de niveles de acceso a objeto de universo [página 1153]

### 34.3.9.1 Asignación de niveles de acceso a objeto de universo

Para establecer la seguridad del nivel de acceso a objeto de universo, es necesario tener el derecho *Modificar los derechos de los usuarios para los objetos* sobre el universo.

1. En el área *Universos* del CMS, seleccione el universo.
2. Haga clic en *Acción* > *Seguridad del universo*.
3. En el cuadro de diálogo *Seguridad del universo*, para el usuario o grupo, seleccione el nivel de acceso a objeto en la lista *Seguridad de nivel de objetos*.

## 34.3.10 Derechos de conexión

Los derechos de esta sección son derechos específicos de tipo que se aplican a conexiones de universo o bien derechos generales con un significado específico en el contexto de las conexiones de universo. Estos derechos se aplican a las conexiones publicadas en el repositorio.

### Derechos de conexión relacionales

| Derecho | Descripción |
|---|---|
| *Ver objetos* | Permite ver la conexión. |
| *Editar objetos* | Permite editar los parámetros de las conexiones. |
| *Descargar la conexión localmente* | Permite usar universos creados en la conexión del cliente enriquecido de Web Intelligence en el modo de desconexión.<br><br>Permite usar el controlador de middleware local de la herramienta de diseño de información. Para ello, seleccione la opción de middleware local de las preferencias de la herramienta de diseño de información; de lo contrario, las consultas a la base de datos usarán el middleware del servidor.<br><br>Este derecho también es necesario para editar una conexión segura en la herramienta de diseño de información. |
| *Eliminar objetos* | Permite eliminar la conexión. |
| *Copiar objetos en otra carpeta* | Permite copiar la conexión de un carpeta en otra. |
| *Acceso a datos* | Permite recuperar contenido de la base de datos especificada en la conexión. |

| Derecho | Descripción |
| --- | --- |
| | En la herramienta de diseño de información, este derecho permite examinar datos de tablas de la conexión y los editores de infraestructura de datos. También permite obtener una vista preliminar del conjunto de resultados en el panel de consulta. |
| *Usar conexiones para los procedimientos almacenados* | Permite usar los procedimientos almacenados en la base de datos especificada para la conexión de universo.<br>**Nota**<br>Este derecho se aplica solo a los universos .unv. |
| *Usar conexión para scripts SQL Free-Hand* | Permite ejecutar scripts SQL en la conexión. |

### Derechos de conexiones OLAP

| Derecho | Descripción |
| --- | --- |
| *Ver objetos* | Permite ver la conexión. |
| *Editar objetos* | Permite editar los parámetros de la conexión en el editor de conexión de la herramienta de diseño de información. |
| *Eliminar objetos* | Permite eliminar la conexión. |
| *Copiar objetos en otra carpeta* | Permite copiar la conexión de un carpeta en otra. |
| *Descargar la conexión localmente* | Permite usar universos creados en la conexión del cliente enriquecido de Web Intelligence en el modo de desconexión. |

## 34.3.11 Aplicaciones

## 34.3.11.1 CMC

| Derecho | Descripción |
| --- | --- |
| *Conectarse a la CMC Web y ver este objeto en la CMC* | Permite que el usuario se conecte a la CMC |
| *Permitir acceso al Administrador de instancias* | Permite que el usuario se conecte al Administrador de instancias |

| Derecho | Descripción |
| --- | --- |
| *Permitir acceso a Relationship Query* | Permite que el usuario efectúe consultas de relaciones en la CMC |
| *Permitir acceso a Security Query* | Permite que el usuario efectúe consultas de seguridad en la CMC |

## 34.3.11.2 Plataforma de lanzamiento de BI tipo Fiori

| Derecho | Descripción |
| --- | --- |
| *Inicio de sesión en la nueva plataforma de lanzamiento de BI tipo Fiori* | Permite que el usuario inicie sesión en la plataforma de lanzamiento de BI tipo Fiori. |
| *Organizar* | Permite que un usuario mueva y copie objetos, añada objetos a la carpeta `Favoritos` y cree accesos directos a los objetos |
| *Enviar a bandeja de entrada de Business Objects* | Permite al usuario enviar objetos a las bandejas de entrada de BI de los destinatarios. |
| *Enviar a destino de correo electrónico* | Permite al usuario enviar objetos a destinatarios a través de correo electrónico. |
| *Enviar a ubicación de archivo* | Permite al usuario enviar objetos a una ubicación de archivos. |
| *Enviar a ubicación FTP* | Permite al usuario enviar objetos a una ubicación FTP. |
| *Enviar a ubicación SFTP* | Permite al usuario enviar objetos a una ubicación SFTP. El destino SFTP tiene propiedades similares a la página destino FTP con una opción de huella adicional que el usuario tiene que proporcionar. Cada servidor SFTP tiene la opción de huella en las propiedades. La coincidencia o validación de la huella se realiza en el back end con el CMS. |

### 34.3.11.2.1 Derechos para aplicaciones de colaboración

Estos derechos de acceso se aplican a SAP Jam cuando la aplicación está configurada en la plataforma de BI.

| Derecho | Descripción |
| --- | --- |
| *Comentar en documentos propiedad del usuario* | Permite al usuario comentar en los documentos e instancias de su propiedad |
| *Ver comentarios en documentos propiedad del usuario* | Permite al usuario ver comentarios en los documentos e instancias de su propiedad |
| *Modificar preferencias en objetos que son propiedad del usuario* | Muestra el menú *Preferencias* en un objeto de aplicación<br><br>Sin este derecho de acceso, el usuario no puede fijar las preferencias personales en ninguna aplicación, por lo que no le aparecerá el menú *Preferencias* en las aplicaciones. Por ejemplo, sin este derecho, los usuarios no pueden seleccionar la unidad de medida (pulgadas o milímetros) que utilizarán en los informes de la aplicación. |

## 34.3.11.3 BI workspaces

| Derecho | Descripción |
| --- | --- |
| *Crear y editar área de trabajo de BI* | Enables a user to create new BI workspaces and to edit existing BI workspaces |
| *Crear y editar módulos* | Enables a user to create new modules and to edit existing modules |
| *Editar áreas de trabajo de BI* | Enables a user to edit existing BI workspaces (but does not enable a user to create new workspaces) |
| *Change preferences for objects that the user owns* | Displays the *Preferences* menu in an application object<br><br>Without this access right, a user cannot set personal preferences in any application and no *Preferences* menu will appear in applications. For example, without this right, users cannot select the unit of measurement (inches or millimeters) to use in reports in the Web Intelligence or BI launch pad application. |

## 34.3.11.4 Web Intelligence

Los derechos de esta sección solo se aplican a la aplicación Web Intelligence, incluido cliente enriquecido, y pueden afectar a los visores y a los paneles de consulta en dicha aplicación.

| Derecho | Descripción |
| --- | --- |
| Datos: Habilitar el seguimiento de datos | Permite que el usuario realice un seguimiento de datos modificados. |
| Datos: Habilitar el formato de datos modificados | Permite que el usuario seleccione el formato para datos modificados. |
| General: Habilitar acceso al cliente de escritorio | Permite que un usuario utilice el escritorio Web Intelligence (cliente enriquecido). |
| Escritorio: Exportar documentos | En el cliente enriquecido de Web Intelligence, permite que un usuario exporte documentos al repositorio de la plataforma de BI. |
| Escritorio: Guardar documentos para todos los usuarios | En el cliente enriquecido de Web Intelligence, permite al usuario guardar documentos localmente sin necesidad de seguridad. |
| Documentos: Deshabilitar la actualización automática al abrir | Evita que los documentos se actualicen automáticamente cuando se abren. |
| Documentos: Habilitar el almacenamiento automático | Permite que los documentos se guarden automáticamente si el administrador activó esta función en la CMC. |
| Documentos: Activar creación | Permite que el usuario cree documentos nuevos. |
| General: Editar las preferencias de Web Intelligence | Editar las preferencias de Web Intelligence |
| General: Habilitar acceso al cliente web | Permite que un usuario utilice el mandante web Web Intelligence. |
| Consulta: Editar script generado a partir de universo | En el panel de consulta, permite que un usuario edite los scripts de consulta SQL o MDX generados desde el universo. |
| Consulta: Editar SQL manual | Permite al usuario editar secuencias de comandos de consultas de SQL manual. |
| Consulta: Ver script generado a partir de universo | En el panel de consulta, permite que un usuario visualice los comandos de consulta SQL o MDX generados desde el universo. |
| Consulta: Visualizar el SQL manual | Permite a un usuario visualizar secuencias de comandos de consulta del SQL manual. |
| Generación de informes: Crear y editar saltos | Permite que el usuario cree y edite saltos. |
| Generación de informes: Crear y editar reglas de formato condicionales | Permite que el usuario cree y edite reglas de formato condicionales. |
| Generación de informes: Crear y editar cálculos predefinidos | Permite que el usuario cree y edite saltos cálculos predefinidos. |
| Generación de informes: Crear y editar controles de entrada y grupos | Permite que el usuario cree y edite controles de entrada. |
| Generación de informes: Crear y editar filtros y consumir controles de entrada | Permite que el usuario cree y edite filtros de informe y utilizar los controles de entrada. |
| Generación de informes: Crear y editar ordenaciones y clasificaciones | Permite que el usuario cree y edite ordenaciones y clasificaciones. |

| Derecho | Descripción |
| --- | --- |
| Generación de informes: Crear fórmulas, variables, grupos y referencias | Permite al usuario crear fórmulas, variables, grupos y referencias. |
| Generación de informes: Habilitar modificación de documento | Permite que el usuario edite el formato de informes. Sin este derecho de acceso, el modo Diseño no estará disponible. |
| Generación de informes: Objetos fusionados | Permite que el usuario sincronice datos mediante dimensiones fusionadas en informes y en el administrador de datos. |
| Generación de informes: Insertar y eliminar informes, tablas, gráficos y celdas | • Permite que el usuario inserte y elimine informes, tablas, gráficos y celdas.<br>• Permite asimismo el flujo de trabajo duplicado (copiar/pegar). |

## 34.3.11.5 Herramienta de diseño de universos

| Derecho | Descripción |
| --- | --- |
| *Comprobar integridad del universo* | Permite que el usuario verifique la integridad del universo. |
| *Actualizar ventana Estructura* | Permite que el usuario actualice la ventana de estructuras. |
| *Utilizar Lista de tablas* | Permite que el usuario vea datos de la base de datos mediante el explorador de tablas. |
| *Aplicar límites del universo* | Permite que el usuario aplique límites del universo predefinidos a los usuarios de un universo importado. |
| *Vincular universo* | Permite que el usuario vincule dos universos y comparta componentes. |
| *Crear, modificar o eliminar conexiones* | Permite crear, modificar y eliminar conexiones de universos almacenadas en el repositorio de la plataforma de BI o almacenadas como conexiones personales o compartidas. |
| *Modificar preferencias en objetos que son propiedad del usuario* | Muestra el menú *Preferencias* en un objeto de aplicación.<br>Sin este derecho de acceso, el usuario no puede fijar las preferencias personales en ninguna aplicación, por lo que no le aparecerá el menú *Preferencias* en las aplicaciones. Por ejemplo, sin este derecho, los usuarios no pueden seleccionar la unidad de medida (pulgadas o milímetros) que utilizarán en los informes de Web Intelligence o en la aplicación de la plataforma de lanzamiento de BI. |

## 34.3.11.6 Herramienta de diseño de información

| Derecho | Descripción |
|---|---|
| *Administrar perfiles de seguridad* | Permite al usuario abrir el editor de seguridad<br><br>Para trabajar con los perfiles de seguridad, necesita también derechos sobre el universo. |
| *Compartir proyectos* | Permite al usuario compartir un proyecto local y sincronizar un proyecto compartido con el proyecto local |
| *Crear, modificar o eliminar conexiones* | • Permite al usuario crear y eliminar conexiones seguras desde la vista de recursos publicados<br>• Permite al usuario editar conexiones en el editor de conexiones<br>• Permite al usuario publicar conexiones en un repositorio |
| *Publicar universos* | Permite al usuario publicar universos en un repositorio |
| *Recuperar universos* | Permite al usuario recuperar universos publicados en un proyecto local que va a editarse |
| *Guardar para todos los usuarios* | Permite al usuario guardar para todos los usuarios al recuperar universos |
| *Calcular estadísticas* | Permite al usuario seleccionar tablas y columnas con las que calcular y publicar estadísticas |
| *Modificar preferencias en objetos que son propiedad del usuario* | Muestra el menú *Preferencias* en un objeto de aplicación<br><br>Sin este derecho de acceso, el usuario no puede fijar las preferencias personales en ninguna aplicación, por lo que no le aparecerá el menú *Preferencias* en las aplicaciones. Por ejemplo, sin este derecho, los usuarios no pueden seleccionar la unidad de medida (pulgadas o milímetros) que utilizarán en los informes de Web Intelligence o en la aplicación de la rampa de lanzamiento de BI. |

## 34.3.11.7 Alertas

| Derecho | Descripción |
|---|---|
| *Desencadenar alertas* | Permite que un usuario desencadene eventos de alertas. Para desencadenar una alerta para un documento, se necesitan los siguientes derechos adicionales: |

| Derecho | Descripción |
| --- | --- |
| | • Derechos de "visualización" y "programación" del documento<br>• Derechos de "visualización" y "activación" del evento correspondiente |
| *Suscribirse a objetos* | Permite que un usuario se suscriba a un evento de alertas. Para suscribirse a un documento, se necesitan los siguientes derechos adicionales:<br>• Derecho de "visualización" sobre el evento correspondiente<br>• Derecho de "suscripción" sobre la cuenta propia del usuario<br>Para suscribirse a una alerta de un documento, se necesitan los siguientes derechos adicionales:<br>• Derecho de "visualización" sobre el documento<br>• Derecho de "visualización de instancia" sobre el documento<br>• Derecho de "visualización" sobre el evento correspondiente<br>• Derecho de "suscripción" sobre la cuenta propia del usuario |
| *Modificar preferencias en objetos que son propiedad del usuario* | Muestra el menú *Preferencias* en un objeto de aplicación<br>Sin este derecho de acceso, el usuario no puede fijar las preferencias personales en ninguna aplicación, por lo que no le aparecerá el menú *Preferencias* en las aplicaciones. Por ejemplo, sin este derecho, los usuarios no pueden seleccionar la unidad de medida (pulgadas o milímetros) que utilizarán en los informes de Web Intelligence o en la aplicación de la rampa de lanzamiento de BI. |

## 34.3.11.8 SAP BusinessObjects Mobile

| Derecho | Descripción |
| --- | --- |
| *Conexión a la aplicación SAP BusinessObjects Mobile* | Permite que el usuario inicie sesión en la plataforma de BI desde la aplicación móvil y ver documentos. |
| *Suscribirse a alertas de documentos* | Permite que el usuario se suscriba a alertas de documentos e instancias periódicas. |

| Derecho | Descripción |
| --- | --- |
| | Dado que el usuario necesita disponer del derecho de aplicación "Administrar perfiles de seguridad" para poder abrir el Editor de seguridad, este método de prueba de perfiles está limitado. Los usuarios deberán cancelar la suscripción a alertas explícitamente si no desea recibirlas.<br><br>Para suscribirse a alertas de documentos y a instancias periódicas para programas, el usuario debe disponer del acceso "Control total" a la carpeta `System Events`, en *Eventos* en la CMC. |
| *Guardar documentos en el almacén local del dispositivo* | Permite que el usuario guarde documentos en un dispositivo móvil.<br><br>Si el usuario disponía previamente del derecho "Guardar documentos localmente en el dispositivo" (incluso si ya no dispone de él ahora) y ha guardado documentos en el dispositivo móvil, los documentos siguen existiendo en el dispositivo pero no se sincronizarán durante la sincronización. |
| *Enviar documentos desde el dispositivo como un mensaje de correo electrónico* | Permite que el usuario envíe informes en un mensaje de correo electrónico. |
| *Modificar preferencias en objetos que son propiedad del usuario* | Muestra el menú *Preferencias* en un objeto de aplicación.<br><br>Sin este derecho de acceso, el usuario no puede fijar las preferencias personales en ninguna aplicación, por lo que no le aparecerá el menú *Preferencias* en las aplicaciones. Por ejemplo, sin este derecho, los usuarios no pueden seleccionar la unidad de medida (pulgadas o milímetros) que utilizarán en los informes de Web Intelligence o en la aplicación de la rampa de lanzamiento de BI. |

Para obtener más información, consulte el *Manual de despliegue e instalación de SAP BusinessObjects Mobile*.

## 34.3.11.9 Cockpit de administración de BI

| Derechos | Descripción |
| --- | --- |
| Permitir el acceso al cockpit de administración de BI | Le permite acceder al cockpit de administración de BI en CMC |
| Permitir el acceso a la supervisión | Le permite acceder a la supervisión en el cockpit de administración de BI |
| Permitir el acceso a la diferencia visual | Le permite acceder a la diferencia visual en el cockpit de administración de BI |

| Derechos | Descripción |
| --- | --- |
| Diferencia visual - Crear comparación | Le permite crear comparaciones nuevas entre objetos info en la diferencia visual |
| Diferencia visual - Eliminar comparación | Le permite borrar las comparaciones anteriores en la diferencia visual |
| Diferencia visual - Volver a ejecutar comparación | Le permite ejecutar de nuevo las comparaciones creadas anteriormente en la diferencia visual |
| Diferencia visual - Ver comparación | Le permite ver una comparación en la diferencia visual |

# 35 Apéndice de propiedades de servidor

## 35.1 Acerca del apéndice de propiedades de servidor

En este apéndice de propiedades de servidor se enumeran y describen las propiedades que se pueden configurar para cada servidor de la plataforma de BI.

### 35.1.1 Propiedades comunes de los servidores

Las propiedades de servidor descritas en esta sección se aplican a todos los tipos de servidores.

Propiedades de puerto de solicitud

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Nombre del servidor* | El nombre del servidor. | El valor predeterminado es el nombre del nodo en el que se encuentra el nodo más el nombre del servidor. |
| *ID, CUID* | El ID reducido y el ID de clúster único del servidor. Sólo lectura. | Estos valores se generan automáticamente. |
| *Nodo* | El nombre del nodo en el que se encuentra el servidor. | Estos valores se especifican durante la instalación. |
| *Descripción* | La descripción del servidor | El valor predeterminado es el nombre del servidor. |
| *Parámetros de la línea de comandos* | Los parámetros de la línea de comandos para el servidor. | El valor predeterminado depende del tipo de servidor. |
| *Puerto de solicitud* | Especifica el puerto desde el que el servidor recibe las solicitudes. En un entorno con servidores de seguridad, configure el servidor para que solo escuche las solicitudes en los puertos que estén abiertos en el servidor de seguridad. Si especifica un puerto para el servidor, compruebe que el puerto no esté siendo usado por otro proceso.<br>**Nota**<br>Si se activa *Asignar automáticamente*, el servidor se enlaza a un puerto asignado dinámicamente. Esto significa que se asigna automáticamente un número de puerto al servidor cada vez que éste se reinicia. | De forma predeterminada, *Asignar automáticamente* se establece en **TRUE** y *Puerto de solicitud* está vacío. |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Asignar automáticamente* | Especifica si el servidor se vincula a un puerto asignado dinámicamente cuando el servidor se reinicia. Para enlazar el servidor a un puerto específico, establezca *Asignar automáticamente* como **FALSE** y especifique un *Puerto de solicitud* válido. | El valor predeterminado es **TRUE**. |

Propiedades de inicio automático

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Iniciar automáticamente este servidor cuando se inicie Server Intelligence Agent* | Especifica si el servidor se inicia automáticamente cuando Server Intelligence Agent (SIA) se inicia o reinicia.<br><br>Si este valor se establece en **FALSE** y el SIA se inicia o reinicie, el servidor permanece detenido. | El valor predeterminado es **TRUE**. |

Propiedades del identificador de host

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Asignar automáticamente* | Especifica si el servidor se vincula a una interfaz de red que se asigna automáticamente. Si se establece el valor **FALSE**, el servidor se vincula a una interfaz de red específica. Si se establece el valor en **TRUE**, el servidor acepta solicitudes en la primera dirección IP disponible. En equipos multibase, se puede especificar una interfaz de red determinada para enlazar si establece este valor en **FALSE** y proporciona un nombre de host o dirección IP válida. | El valor predeterminado es **TRUE**. |
| *Nombre de host* | El nombre de host de la interfaz de red a la que se enlaza el servidor. Si se especifica un nombre de host, el servidor acepta solicitudes en odas las direcciones IP asociadas con el nombre de host. | De forma predeterminada, *Asignar automáticamente* se establece en **TRUE** y el *Nombre de host* está vacío. |
| *Dirección IP* | La dirección IP de la interfaz de red a la que se vincula el servidor. Se admiten los protocolos IPv4 e IPv6. Si se especifica una dirección IP, el servidor acepta solicitudes solo en la dirección IP. | De forma predeterminada, *Asignar automáticamente* se establece en **TRUE** y la *Dirección IP* está vacía. |

Propiedades de la plantilla de configuración

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Usar plantilla de configuración* | Especifica si se va a usar una plantilla de configuración. | El valor predeterminado es **FALSE**. |
| *Restaurar valores predeterminados del sistema* | Especifica si se restaurará la configuración predeterminada original para este servidor. | El valor predeterminado es **FALSE**. |
| *Establecer plantilla de configuración* | Especifica si se usará la configuración del servicio actual como plantilla de configuración para todos los servicios del mismo tipo. Si se establece como **TRUE**, todos los servicios del mismo tipo que ha especificado para *Usar plantilla de configuración* se vuelven a configurar inmediatamente para usar la configuración del servicio actual. | El valor predeterminado es **FALSE**. |

Propiedades del servicio de registro de seguimiento

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Nivel de registro* | Especifica la gravedad mínima de los mensajes que desea registrar y determina la cantidad de información que se almacena en el archivo de registro del servidor.<br>Los niveles de umbral de registro posibles son:<br>• *No especificado*<br>• *Ninguno*<br>• *Bajo*<br>• *Mediano*<br>• *Alto* | El valor predeterminado es **`No especificado`**. |

## 35.1.2 Propiedades de servicios principales

La categoría de servicios principales incluye los siguientes servidores:

- Servidor de tareas de Adaptive
- Servidor de procesamiento de Adaptive
- Servidor de administración central
- Servidor de eventos
- Servidor del repositorio de archivos de entrada
- Servidor del repositorio de archivos de salida
- Servidor de contenedor de aplicación Web

### Propiedades del servidor de tareas de Adaptive

Propiedades generales

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Directorio temporal* | Especifica el directorio donde se crean los archivos temporales cuando es necesario. Se pueden producir problemas de rendimiento si este directorio no dispone de espacio en disco adecuado. Para obtener un mejor rendimiento, compruebe que este directorio esté en un disco local.<br>**Nota**<br>Debe reiniciar el servidor para que los cambios se apliquen. | %DefaultDataDir% |

El servidor de tareas de Adaptive puede alojar diferentes servicios. Cada servicio tiene las propiedades siguientes:

Propiedades de servicio

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Número máximo de tareas simultáneas* | Especifica el número de procesos independientes simultáneos (procesos secundarios) que permite el servidor. Puede ajustar el número máximo de tareas según su entorno de informes.<br><br>El valor predeterminado es adecuado para la mayoría de los escenarios de generación de informes. La configuración ideal para su entorno de informes depende de la configuración del hardware, el software de base de datos y los requisitos de informes. | 5 |
| *Número máximo de solicitudes secundarias* | Especifica el número de tareas que el elemento secundario procesará antes del reinicio. | 100 |

## Propiedades del servidor de procesamiento de Adaptive

Propiedades generales

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tiempo de espera de inicio del servicio (segundos)* | Especifica el período de tiempo, en segundos, que el servidor esperará a que se inicien los servicios.<br><br>Si un servicio no se inicia en el tiempo especificado, existen dos motivos posibles:<br><br>• El servicio ha fallado, por ejemplo, porque no se ha podido encontrar un recurso necesario, como una base de datos, o se ha producido un conflicto de puertos en el servicio.<br>• El servicio no se pudo iniciar en el tiempo especificado, por ejemplo, porque el sistema es demasiado lento.<br><br>Para encontrar el motivo, consulte el archivo de registro del servidor. Si el servicio no se pudo iniciar en el tiempo especificado, considere la posibilidad de aumentar este valor. | 1200 |

Propiedades del servicio proxy de auditoría de cliente

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del servicio de token de seguridad

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del servicio Insight to Action

| Métrica | Descripción | |
|---|---|---|
| *Número máximo de conexiones activas por sesión de usuario* | El número máximo de conexiones con el servidor de SAP disponible para un usuario durante un tiempo dado. Cuando un usuario abra un informe o cuadro de mandos con capacidad de RRI, se establecerá una conexión con el servidor de SAP para determinar los destinos RRI disponibles. | 20 |
| *Número máximo de conexiones inactivas por sesión de usuario* | El número de conexiones inactivas para mantener abiertas y volver a usar en siguientes solicitudes de RRI. Si se aumenta esta configuración, se asignarán recursos del sistema adicionales. | 20 |
| *Tiempo de espera máximo de conexión (en segundos)* | La cantidad de tiempo que el marco Insight to Action debe esperar una respuesta desde el servidor SAP antes de que se agote el tiempo de espera (en segundos). | 30 |

Propiedades del servicio de publicación

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tamaño del conjunto de subprocesos* | Especifica el número de subprocesos de procesamiento de lotes de alcance se pueden ejecutar al mismo tiempo. Si el valor de esta propiedad está configurado en «0», el tamaño de grupo de subgrupo se determina mediante una fórmula basada en el número de núcleos de CPU en el equipo actual. | 0 |

Propiedades del servicio de traducción

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del servicio de supervisión

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del servicio de búsqueda de plataforma

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del servicio de publicación posterior al procesamiento

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

## Propiedades del servidor de administración central

> **Nota**
>
> Al modificar alguna de estas propiedades de servidor, debe reiniciar el servidor para que los cambios surtan efecto.

Propiedades del servicio de administración central

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Puerto del servidor de nombres* | Especifica el puerto en el que el CMS escucha las solicitudes de servicio de nombres. | 6400 |
| *Conexiones a la base de datos del sistema solicitadas* | Especifica el número de conexiones de base de datos del sistema de CMS que el CMS intenta establecer. Si el servidor no puede establecer todas las conexiones de base de datos solicitadas, el CMS sigue funcionando pero con un menor rendimiento, ya que pueden atenderse menos solicitudes simultáneas a la vez. El CMS intentará establecer conexiones adicionales, hasta que se haya establecido el número solicitado de conexiones.<br><br>La métrica del CMS *Conexiones de base de datos del sistema establecidas* muestra el número actual de conexiones establecidas. | 14 |
| *Reconectar automáticamente a la base de datos del sistema* | Especifica si el CMS intenta automáticamente volver a establecer una conexión a la base de datos del CMS si se produce una interrupción del servicio. Si este valor se establece como **FALSE**, se podrá comprobar la integridad de la base de datos del CMS antes de reanudar las operaciones; se debe reiniciar el CMS para volver a establecer la conexión a la base de datos. | **TRUE** |

Propiedades del servicio de inicio de sesión único

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Expiración del inicio de sesión único (segundos)* | Especifica el tiempo, en segundos, que es válida una conexión de inicio de sesión único a un origen de datos. Esto se aplica a usuarios de Windows AD que ejecutan informes configurados para SSO de Windows AD en el origen de datos. | 86400 |

## Propiedades del servidor de eventos

Propiedades del servicio de eventos

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Intervalo de sondeo de eventos (segundos)* | Especifica la frecuencia de desencadenamiento de los sondeos de servidor para un archivo, en segundos. | 10<br><br>El intervalo de valores permitidos es de 1 a 1200 segundos. |
| *Intervalo de limpieza (minutos)* | Especifica la frecuencia con que se ejecuta la utilidad de limpieza, en minutos. | 20 |

## Propiedades del servidor del repositorio de archivos de entrada

Propiedades del servicio de almacenamiento de archivos de entrada

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Directorio de almacenamiento de archivos* | Especifica el directorio donde se almacenan los objetos del repositorio de archivos.<br>**Nota**<br>Se pueden producir problemas de rendimiento si este directorio no dispone de espacio en disco adecuado. | %DefaultInputFRSDir/% |
| *Directorio temporal* | Especifica el directorio donde se crean los archivos temporales cuando es necesario.<br>**Nota**<br>Se pueden producir problemas de rendimiento si este directorio no dispone de espacio en disco adecuado. Para garantizar un mejor rendimiento, se recomienda que el *Directorio temporal* se encuentre en el mismo sistema de archivos que el *Directorio del almacén de archivos*. | %DefaultInputFRS-Dir/temp% |
| *Tiempo máximo de inactividad (minutos)* | Especifica el período de tiempo que el servidor espera antes de cerrar las conexiones inactivas. Si se configura un valor demasiado bajo, la solicitud de un usuario se puede cerrar prematuramente. Si se configura un valor que sea demasiado alto, puede provocar un consumo excesivo de los recursos del sistema, como el tiempo de procesamiento y el espacio de disco. | 10 |
| *Número máximo de reintentos para acceder al archivo* | Especifica el número de veces que el servidor intenta acceder a un archivo. | 1 |
| *Ubicación de archivos de adaptador de la búsqueda de virus* | Especifica la vía de acceso absoluta de la ubicación de archivos de adaptador de la búsqueda de virus. | |

## Propiedades del servidor del repositorio de archivos de salida

Propiedades del servicio de almacenamiento de archivos de salida

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Directorio de almacenamiento de archivos* | Especifica el directorio donde se almacenan los objetos del repositorio de archivos.<br>**Nota**<br>Se pueden producir problemas de rendimiento si este directorio no dispone de espacio en disco adecuado. | %DefaultOutputFRSDir/% |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Directorio temporal* | Especifica el directorio donde se crean los archivos temporales cuando es necesario.<br>**Nota**<br>Se pueden producir problemas de rendimiento si este directorio no dispone de espacio en disco adecuado. | %DefaultOutputFRS-Dir/temp% |
| *Tiempo máximo de inactividad (minutos)* | Especifica el período de tiempo que el servidor espera antes de cerrar las conexiones inactivas. Si se configura un valor demasiado bajo, la solicitud de un usuario se puede cerrar prematuramente. Si se configura un valor que sea demasiado alto, puede provocar un consumo excesivo de los recursos del sistema, como el tiempo de procesamiento y el espacio de disco. | 10 |
| *Número máximo de reintentos para acceder al archivo* | Especifica el número de veces que el servidor intenta acceder a un archivo. | 1 |

## Propiedades del servidor de contenedor de aplicaciones Web

Propiedades generales

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Tiempo de espera de inicio del servicio (segundos)* | Lo que esperará el WACS a que sus servicios alojados se inician antes de que se agote el tiempo de espera. Si se consume el tiempo de espera, el WACS no proporcionará servicios que no se hayan iniciado todavía. En un equipo lento, considere la posibilidad de especificar un valor mayor.<br>Si especifica un valor demasiado pequeño y el WACS no se inicia antes de que se agote el tiempo de espera, restaure la configuración predeterminada del WACS mediante el Administrador de configuración central (CCM). | 1200 |

Propiedades del servicio de registro de seguimiento

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Nivel de registro* | Permite el registro y configura el nivel de gravedad y detalle en Ninguno (solo se registran los eventos críticos), Bajo (mensajes de solicitud de arranque, apagado, inicio y finalización), Medio (mensajes de error, advertencia y la mayoría de los mensajes de estado) o Alto (no se excluye nada). Utilizar solo para la depuración. El uso de la CPU puede aumentar, repercutiendo en el rendimiento).<br><br>Las opciones de menú disponibles son:<br>• *No especificado*<br>• *Ninguno*<br>• *Bajo*<br>• *Mediano*<br>• *Alto* | No especificado |

Propiedades del servicio Business Process BI

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del servicio de Query Builder

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Servicio Web RESTful: propiedades de la configuración de la propiedad del sistema

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Mostrar pila de errores* | Cuando está habilitado, el registro de errores incluye los mensajes de error del servicio Web RESTful para su depuración. De lo contrario no se debe usar o cuando existe una preocupación de seguridad en la que se desvelan detalles de la plataforma de BI. | No seleccionado |
| *Número predeterminado de objetos en una página* | El número de entradas que se mostrará por página. Los desarrolladores pueden sobrescribir esta configuración con el parámetro &pageSize=<m> en el SDK de los servicios Web RESTful. | 50 |
| *Tiempo de espera del token de la sesión de Enterprise (minutos)* | La hora de vencimiento hasta la que un token de inicio de sesión será válido. Pasada esta hora, se debe generar un nuevo token de inicio de sesión. | 60 |
| *Tamaño del conjunto de sesiones* | Se trata del número de sesiones en caché que se almacenará en un momento dado que se usa para mejorar el rendimiento del servidor. El grupo de sesión copia en caché las sesiones del servicio Web RESTful activo. De este modo, se pueden volver a usar cuando un usuario envía otra solicitud que use el mismo token de inicio de sesión en el encabezado de la solicitud HTTP. | 1000 |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Tiempo de espera del conjunto de sesiones (minutos)* | El tiempo en minutos en que caducará las sesiones en caché. | 2 |
| *Habilitar autenticación HTTP Basic* | Si esta configuración no está habilitada, las solicitudes del servicio Web RESTful deben usar un token de inicio de sesión. Cuando esta configuración está habilitada, los usuarios deben proporcionar su nombre y contraseña la primera vez que realicen una solicitud de servicio Web RESTful. Cuando esté habilitada, aparece el menú desplegable *Esquema de autenticación predeterminada para HTTP Basic*. | No seleccionado |
| *Esquema de autenticación predeterminada para HTTP Basic* | Cuando está seleccionada *Habilitar autenticación HTTP Basic*, es posible que se seleccione uno de los cuatro tipos de autenticación. Tenga en cuenta que los nombres y contraseña se transmiten en texto no cifrado a menos que se usen las opciones HTTPS.<br>Los valores aceptados son:<br>• *secEnterprise*<br>• *secDAP*<br>• *SAPR3*<br>• *secWinAD* | En blanco. Sin embargo, si se activa *Habilitar autenticación HTTP Basic*, por defecto *secEnterprise*. |

Servicio Web RESTful: propiedades de la configuración de uso compartido de recursos de origen cruzado

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Permitir orígenes* | Esta configuración sirve para permitir que los usuarios con exploradores competentes CORS accedan a páginas con secuencias de comandos java que deben acceder a varios nombres de dominio. Agregar cada nombre de dominio y separarlos por comas. Por ejemplo, http://origin1.server.com:8080, http://origin2.server.com:8080. De forma predeterminada, los exploradores pueden acceder a todos los dominios (*). | * (un asterisco) |
| *Antigüedad máxima (minutos)* | Este es el tiempo máximo que los exploradores pueden almacenar solicitudes HTTP. | 1440 |

Servicio Web RESTful: propiedades de la configuración de autenticación de confianza

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Recuperando método* | Esta configuración es un menú que establece qué método de consulta se utilizará para recuperar tokens de inicio de sesión con autenticación con confianza al utilizar el servicio web RESTful de API `/iniciosesión/confianza`.<br>• *HTTP_HEADER* se utiliza para consultas GET con el encabezado de solicitud aceptar=aplicación/xml (o aplicación/json).<br>• *QUERY_STRING* se utiliza para agregar un nombre de inicio de sesión al final de la consulta de la dirección URL mediante el servicio web RESTful de API, por ejemplo /iniciosesión/confianza/?usuario=johndoe.<br>• *COOKIE* se utiliza cuando el nombre de inicio de sesión se recupera desde una cookie del explorador web. El dominio, el nombre, el valor y la ruta se deben almacenar en la cookie. | **HTTP_HEADER** |
| *Parámetro de nombre de usuario* | Esta es la etiqueta que se utiliza para identificar el usuario de confianza para recuperar el token de inicio de sesión. | **X-SAP-TRUSTED-USER** |

Propiedades del servicio de aplicación Web BOE

| Tipo de propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tipo de autenticación* | El tipo de autenticación que se usa para autenticar a los usuarios que inician sesión en la plataforma de lanzamiento de BI.<br>Los valores aceptados son:<br>• *AD Kerberos*<br>• *SSO de AD Kerberos*<br>• *Enterprise*<br>• *LDAP* | *Enterprise* |
| *Dominio predeterminado de AD* | El dominio de Active Directory predeterminado se utiliza para que los usuarios no necesiten proporcionar un dominio cuando inicien sesión. Por ejemplo, si el dominio predeterminado se establece como «mydomain» y un usuario inicia sesión con el nombre«user», la autoridad de inicio de sesión de Active Directory intenta autenticar«user@mydomain.com». | En blanco |
| *Nombre Principal de Servicio* | Los clientes usan un nombre principal de servicio (SPN) para identificar de forma exclusiva una instancia de un servicio. El servicio de autenticación Kerberos utiliza un SPN para autenticar un servicio. | En blanco |
| *Archivo Keytab* | La ruta completa a un archivo keytab. Un archivo keytab permite configurar filtros de Kerberos sin mostrar la contraseña de la cuenta de usuario en el equipo de la aplicación Web. | En blanco |

Propiedades de servicios Web SDK y QaaWS

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Habilitar inicio de sesión único Kerberos de Active Directory* | Indica si se habilitará el inicio de sesión único Kerberos de AD para Servicios Web SDK y QaaWS. | **FALSE** |

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Dominio predeterminado de AD* | El dominio predeterminado de Active Directory que se usará para que los usuarios no tengan que proporcionar un dominio cuando inicien la sesión. | En blanco |
| *Nombre Principal de Servicio* | Los clientes usan un nombre principal de servicio (SPN) para identificar de forma exclusiva una instancia de un servicio. El servicio de autenticación Kerberos utiliza un SPN para autenticar un servicio. | En blanco |
| *Archivo Keytab* | La ruta completa a un archivo keytab. Un archivo keytab permite configurar filtros de Kerberos sin mostrar la contraseña de la cuenta de usuario en el equipo de la aplicación Web. | En blanco |

Propiedades de configuración de HTTP

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Enlazar a todas las direcciones IP* | Indica si se enlazará a todas las interfaces de red. Si el servidor tiene varias NIC y desea enlazar a una interfaz de red específica, desactive esta propiedad. | **TRUE** |
| *Enlazar a nombre de host o dirección IP* | Especifica la interfaz de red (dirección IP o nombre de host) en la que se proporciona el servicio HTTP. Solo puede especificar un valor si desactiva *Enlazar a todas las direcciones IP*. | `localhost` |
| *Puerto HTTP* | El puerto en el que se proporciona el servicio HTTP. | 6405<br>El rango de valores permitidos está comprendido entre 1 y 65535. |
| *Tamaño máximo de encabezado HTTP* | El tamaño máximo permitido en bytes de encabezados HTTP de solicitud y respuesta. | 32768 |

Propiedades de configuración de HTTP mediante proxy

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Habilitar HTTP mediante proxy* | Indica si se habilita el conector HTTP mediante proxy en el WACS. Normalmente se activa en despliegues con un proxy inverso. | **FALSE** |
| *Enlazar a todas las direcciones IP* | Indica si el puerto de HTTP mediante proxy se enlazará a todas las interfaces de red. | **TRUE** |
| *Enlazar a nombre de host o dirección IP* | Especifica la interfaz de red (dirección IP o nombre de host) en la que se proporciona el servicio HTTP mediante proxy. Solo puede especificar un valor si desactiva *Enlazar a todas las direcciones IP*. | `localhost` |
| *Puerto HTTP* | El puerto en el que se proporciona el servicio HTTP en un despliegue de proxy inverso. Solo puede especificar un valor si activa *Habilitar HTTP mediante proxy*. | 6406<br>El rango de valores permitidos está comprendido entre 1 y 65535. |
| *Nombre de host de proxy* | La dirección IPv4, la dirección IPv6, el nombre de host o el nombre de dominio completo del servidor proxy. Solo puede especificar un valor si activa *Habilitar HTTP mediante proxy*. | En blanco |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Puerto de proxy* | El puerto del servidor de reenvío o proxy inverso. Solo puede especificar un valor si activa *Habilitar HTTP mediante proxy*. | 0<br>El rango de valores permitidos está comprendido entre 1 y 65535. |
| *Tamaño máximo de encabezado HTTP* | El tamaño máximo permitido en bytes de encabezados HTTP de solicitud y respuesta. | 32768 |

Propiedades de configuración de HTTPS

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Habilitar HTTPS* | Indica si se activan las comunicaciones HTTPS/SSL. | **FALSE** |
| *Enlazar a nombre de host o dirección IP* | Especifica la interfaz de red (dirección IP o nombre de host) en la que se proporciona el servicio HTTPS. Solo puede especificar un valor si activa *Habilitar HTTPS*. | `localhost` |
| *Puerto HTTPS* | El puerto en el que se proporciona el servicio HTTPS. Solo puede especificar un valor si activa *Habilitar HTTPS*. | 443<br>El rango de valores permitidos está comprendido entre 1 y 65535. |
| *Nombre de host de proxy* | La dirección IPv4, la dirección IPv6, el nombre de host o el nombre de dominio completo del servidor proxy. Solo puede especificar un valor si activa *Habilitar HTTPS*. | En blanco |
| *Puerto de proxy* | El puerto del servidor de reenvío o proxy inverso. Solo puede especificar un valor si activa *Habilitar HTTPS*. | 0<br>El rango permitido de valores está comprendido entre 1 y 65535. |
| *Protocolo* | El protocolo de cifrado que se utilizará. Solo puede especificar un valor si activa *Habilitar HTTPS*. | TLS<br>Los valores permitidos son TLS o SSL. |
| *Tipo de almacén de certificados* | El tipo de almacén de certificados que contiene sus certificados y claves privadas. En la mayoría de los casos será *PCKS12*. Solo puede especificar un valor si activa *Habilitar HTTPS*. | PKCS12<br>Los valores permitidos son PKCS12 o JKS. |
| *Ubicación del archivo de almacén de certificados* | La ruta de acceso completa al archivo de certificados. Solo puede especificar un valor si activa *Habilitar HTTPS*. | En blanco |
| *Contraseña de acceso a clave privada* | Los almacenes de certificados PKCS12 y los almacenes de claves de Java tienen claves privadas que están protegidas con contraseña, para prevenir el acceso no autorizado o el robo. Introduzca aquí la contraseña que ha especificado al generar el almacén de certificados, de modo que WACS pueda acceder a las claves privadas desde el almacén de certificados. Solo puede especificar un valor si activa *Habilitar HTTPS*. | En blanco |

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Alias de certificado* | El alias del certificado dentro del almacén de certificados. Si no se especifica y se usa un almacén de certificados que contiene varios certificados, se empleará el primer certificado del almacén. En la mayoría de los casos no es necesario especificar un valor. Solo puede especificar un valor si activa *Habilitar HTTPS*. | En blanco |
| *Habilitar la autenticación de cliente* | Si se habilita la autenticación de cliente, solo los clientes que tengan claves almacenadas en el archivo de lista de certificados de confianza pueden obtener servicios del WACS. Los demás clientes se rechazan. Solo puede habilitar la autenticación de cliente si activa *Habilitar HTTPS*. | **FALSE** |
| *Ubicación del archivo de certificados de confianza* | La ruta de acceso completa al archivo de lista de certificados de confianza. Solo puede especificar un valor si activa *Habilitar HTTPS* y *Habilitar la autenticación de cliente*. | En blanco |
| *Contraseña de acceso a clave privada de lista de certificados de confianza* | La contraseña que protege el acceso a las claves privadas en el archivo de lista de certificados de confianza. Solo puede especificar un valor si activa *Habilitar HTTPS* y *Habilitar la autenticación de cliente*. | En blanco |
| *Tamaño máximo de encabezado HTTP* | El tamaño máximo permitido en bytes de encabezados HTTP de solicitud y respuesta. | 32768 |

Propiedades de simultaneidad (por conector)

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Cantidad máxima de solicitudes simultáneas* | El número de solicitudes HTTP o HTTPS simultáneas que cada conector (HTTP, HTTP mediante proxy o HTTPS) puede procesar simultáneamente. | **150**<br>El rango de valores permitidos está comprendido entre 1 y 1000. |

Propiedades de configuración de Active Directory

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Ubicación del archivo Krb5.ini* | La ruta completa a un archivo `krb5.ini` que almacena propiedades de configuración Kerberos. | En blanco |
| *Ubicación del archivo bscLogin.conf* | La ruta completa a un archivo `bscLogin.conf`. | En blanco |

## 35.1.3 Propiedades de los servicios de conectividad

La categoría del servicio de conectividad contiene los siguientes servicios:

- Servicio de conectividad nativa (alojado en el servidor independiente)
- Servicio de conectividad nativa (de 32 bits alojado en el servidor independiente)
- Servicio de conectividad de Adaptive (alojado en APS)

Todos los servicios comparten la misma configuración.

Propiedades del servicio de acceso a datos de Excel

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tiempo de espera de limpieza del acceso a datos de Excel (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de realizar una limpieza de la sesión del cliente. | El valor predeterminado es 1200 segundos. |
| *Tiempo de espera de intercambio de acceso a datos de Excel (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de permutar la sesión del cliente en el disco duro. Se recomienda especificar un valor inferior al valor de la propiedad *Tiempo de espera de limpieza de acceso a datos de Excel (en segundos)*. | El valor predeterminado es 600 segundos. |

Propiedades de operación del servicio

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| | **→ Recuerde**<br>No tiene que reiniciar el servidor una vez cambiadas las siguientes propiedades de operación del servicio. | |
| *Grupo de conexiones* | Activa o desactiva el grupo de conexiones.<br>Los valores posibles son:<br>• Activado con tiempo de espera<br>• Activado sin tiempo de espera<br>• Desactivado<br>**Nota**<br>El grupo de conexiones es una funcionalidad de la memoria caché que mantiene las conexiones en un estado reutilizable para mejorar el rendimiento del servidor. | Activado con tiempo de espera |
| *Tiempo de espera del grupo de conexiones* | Especifica el tiempo de inactividad máximo para las conexiones del grupo (en minutos).<br>**Nota**<br>Esta propiedad equivale al parámetro `Max Pool Time` del archivo `cs.cfg`. Desactivar el grupo equivale a que `Max Pool Time` se establezca en `0`. Activar el grupo sin tiempo de espera equivale a que `Max Pool Time` se establezca en `-1`. Consulte el *Manual de acceso a los datos* para obtener más información. | `60` |
| *Tiempo de espera de inactividad de objeto transitorio* | Especifica cuántos minutos se conserva en el servidor un objeto temporal no usado. El objeto se elimina posteriormente y se recuperan sus recursos. | `60` |

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Intervalo de cronómetro del objeto transitorio* | Especifica el tiempo entre comprobaciones de actividad (en minutos). A intervalos regulares, el servidor busca los objetos candidatos a ser eliminados. | **5** |
| *Activar bloque de HTTP* | Activa o desactiva el bloque de HTTP.<br>**Nota**<br>El bloque de HTTP sólo es pertinente para el despliegue de nivel 3. Influye sobre el rendimiento de apertura y actualización del documento ya que mayores respuestas implican menores recorridos de ida y vuelta al analizar grandes documentos. Desactivar el bloque de HTTP equivale a que *Tamaño del bloque HTTP* se establezca en **0**. | Activado |
| *Tamaño del bloque HTTP* | Especifica el tamaño de las respuestas HTTP emitidas por el servidor (en kilobytes). | **64** |

Propiedades de seguimiento de bajo nivel

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| **Recuerde**<br>No tiene que reiniciar el servidor una vez cambiadas las siguientes propiedades de seguimiento de bajo nivel. | | |
| *Activar seguimiento de tareas* | Activa el seguimiento de las tareas del servidor de conexión.<br>**Nota**<br>Requiere que la propiedad *Nivel de registro* esté establecida en *Alto*. | Deshabilitado |
| *Activar seguimiento de middleware* | Activa el seguimiento de cualquier middleware. Para realizar el seguimiento de middleware concreto, deberá configurar el archivo `cs.cfg` y reiniciar el servidor.<br>**Nota**<br>Requiere que la propiedad *Nivel de registro* esté establecida en *Alto*. | Deshabilitado |

Propiedades de orígenes de Active Data

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| **Precaución**<br>Deberá reiniciar el servidor una vez cambiadas las siguientes propiedades de orígenes de datos activos. | | |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Origen de datos activo* | Permite seleccionar los orígenes de datos para los que desea obtener conexiones. Esta propiedad funciona como filtro para los controladores. Especifique los orígenes de datos activos para cargar los controladores que desea usar.<br><br>**⚠ Precaución**<br>El servidor predeterminado debe cargar todos los controladores disponibles. Use esta configuración para especializar algún servidor. Resulta especialmente útil cuando se despliegan varios servidores CORBA en su red.<br><br>**→ Recuerde**<br>Sólo se cargan los controladores para los orígenes de datos seleccionados. El resto se omiten. Si no selecciona ningún origen de datos, el servidor carga todos los controladores disponibles.<br><br>**ⓘ Nota**<br>Compruebe en la métrica del servidor que hayan activado los orígenes de datos seleccionados. Las capas de red y las bases de datos se muestran en *Métrica del servicio de conexión*. | Sin marca de verificación |
| *Capa de red* | Especifica la capa de red que usa la conexión.<br><br>**ⓘ Nota**<br>Sólo se tiene en cuenta el nombre sin localizar. Puede consultar la lista de capas de red disponibles en el archivo `driver.cfg`, ubicado en el directorio `<directorio-instalación-connectionserver>\connectionServer`. | • `ODBC` para servidores CORBA nativos<br>• `JDBC` para servidores CORBA de Adaptive |
| *Base de datos* | Especifica la base de datos que usa la conexión.<br><br>**ⓘ Nota**<br>Sólo se tiene en cuenta el nombre sin localizar. Los nombres de las bases de datos pueden ser expresiones regulares si son cadenas ASCII puras. Los modelos usan la sintaxis regexp de GNU. Utilice el patrón `.*` para hacer coincidir cualquier carácter. Por ejemplo, la expresión `MS SQL Server.*$` significa que todas las bases de datos de MS SQL Server están en uso. Para obtener más información acerca de las expresiones regulares, consulte el sitio Web de PERL en http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions . | El campo está vacío hasta que se especifique un nombre de base de datos. |

Propiedades del servicio de acceso a datos personalizados

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tiempo de espera de limpieza de acceso a datos personalizados (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de realizar una limpieza de la sesión del cliente. | El valor predeterminado es 1200 segundos. |
| *Tiempo de espera de intercambio de acceso a datos personalizados (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de permutar la sesión del cliente en el disco duro. Se recomienda especificar un valor inferior al valor de la propiedad *Tiempo de espera de limpieza de acceso a datos personalizados (en segundos)*. | El valor predeterminado es 600 segundos. |

Propiedades del servicio de inicio de sesión único

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Expiración del inicio de sesión único (segundos)* | Especifica el tiempo, en milisegundos, que una conexión de inicio de sesión único es válida antes de expirar. | El valor predeterminado es 86400 segundos. |

Propiedades del servicio de administración de promociones

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del servicio ClearCase de administración de promociones

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del servicio de diferencia visual

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

## Información relacionada

Propiedades comunes de los servidores [página 1163]

# 35.1.4 Propiedades de los servicios de Crystal Reports

La categoría de servicios de Crystal Reports incluye los siguientes servidores:

- Servidor de caché de Crystal Reports
- Servidor de procesamiento de Crystal Reports
- Propiedades del servidor de aplicaciones de informes de Crystal Reports 2020
- Servidor de procesamiento de Crystal Reports 2020

## Propiedades del servidor de caché de Crystal Reports

Cualquier propiedad que se aplique a los servidores de caché de Crystal Reports y a los servidores de procesamiento de Crystal Reports se debe establecer en el mismo valor. Por ejemplo, si establece la configuración *Actualización del visor siempre proporciona datos actuales* como **TRUE** en el servidor de caché, debe establecer la misma propiedad en **TRUE** en el servidor de procesamiento.

> **Nota**
>
> Al modificar alguna de estas propiedades de servidor, debe reiniciar el servidor para que los cambios surtan efecto.

Propiedades del servicio de caché de Crystal Reports

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Actualización del visor siempre proporciona datos actuales* | Especifica si, en el momento que los usuarios actualizan un informe explícitamente, todas las páginas en caché se omiten y se recuperan nuevos datos directamente de la base de datos.<br>**Nota**<br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. Para especificar un valor en el objeto de informe, seleccione el informe en la CMC y haga clic en *Configuración predeterminada* > *Viendo grupo de servidores*. | El valor predeterminado es **FALSE**. |
| *Compartir datos del informe entre clientes* | Especifica si los datos de informe se comparten entre clientes distintos.<br>**Nota**<br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. | El valor predeterminado es **TRUE**. |
| *Tiempo de espera de la conexión inactiva (minutos)* | Especifica el período de tiempo, en minutos, que el servidor de caché de Crystal Reports espera una solicitud de una conexión inactiva. Por lo general no hay necesidad de modificar el valor predeterminado. | El valor predeterminado es 20 minutos. |
| *Tiempo de espera de caché de seguridad (minutos)* | Especifica la cantidad de tiempo en minutos que el servidor usa la información almacenada en caché de las credenciales de inicio de sesión, de los parámetros de los informes y de conexión de la base de datos para atender solicitudes antes de consultar al CMS. | El valor predeterminado es 20 minutos. |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Datos a petición más antiguos facilitados a los clientes (segundos)* | Especifica el período de tiempo, en segundos, que el servidor usa datos en caché para cumplir las solicitudes de los informes a petición.<br><br>Si el servidor recibe una solicitud que se puede procesar con los datos generados para procesar una anterior y el tiempo transcurrido desde que se generaron dichos datos es menor que el valor configurado aquí, el servidor de procesamiento volverá a utilizar estos datos para procesar la solicitud posterior. Volver a utilizar los datos de este modo mejora de manera significativa el rendimiento del sistema cuando varios usuarios necesitan la misma información.<br><br>Al configurar este valor, tenga en cuenta lo importante que resulta para los usuarios recibir datos actualizados. Si es muy importante que todos los usuarios reciban datos nuevos (quizás porque los datos importantes cambian con mucha frecuencia), es posible que tenga impedir este tipo de utilización de los datos configurando el valor en 0.<br><br>**Nota**<br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. | El valor predeterminado es 0 segundos. |
| *Tamaño de caché máximo (KB)* | Especifica la cantidad de espacio en el disco duro (en KB) que se utiliza para guardar en caché los informes. Puede ser necesario un tamaño de caché grande si el servidor necesita administrar grandes cantidades de informes, o bien informes que son especialmente complejos. | El valor predeterminado es 256000 KB. |
| *Directorio de archivos de la caché* | Especifica la ubicación del directorio de archivos de la caché. | `%DefaultDataDir%/CrystalReportsCachingServer/temp` |
| *Argumentos VM Java* | Especifica los argumentos de la línea de comandos que pueden proporcionarse a la JVM. | El valor predeterminado es un valor vacío. |
| *Nombre DLL* | Especifica el nombre del complemento de tipo de documento que está cargado actualmente.<br><br>Esta propiedad es de solo lectura. | rasprocReport |

## Propiedades del servidor de procesamiento de Crystal Reports

Cualquier propiedad que se aplique a los servidores de caché de Crystal Reports y a los servidores de procesamiento de Crystal Reports se debe establecer en el mismo valor. Por ejemplo, si establece la configuración *Actualización del visor siempre proporciona datos actuales* como **TRUE** en el servidor de caché, debe establecer la misma propiedad en **TRUE** en el servidor de procesamiento.

> **Nota**
>
> Al modificar alguna de estas propiedades de servidor, debe reiniciar el servidor para que los cambios surtan efecto.

Propiedades del servicio de procesamiento de Crystal Reports

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tiempo de espera de la tarea inactiva (minutos)* | Especifica el período de tiempo, en minutos, que el servidor de procesamiento de Crystal Reports espera entre solicitudes para una tarea determinada. | El valor predeterminado es 20 minutos. |
| *Número máximo de tareas de ciclo de vida por proceso secundario* | Especifica el número máximo de tareas que cada proceso secundario puede administrar por vida útil. | El valor predeterminado es 1000. |
| *Actualización del visor siempre proporciona datos actuales* | Especifica si, en el momento que los usuarios actualizan un informe explícitamente, todas las páginas en caché se omiten y se recuperan nuevos datos directamente de la base de datos. Especifica si los datos de informe se comparten entre clientes distintos.<br>**Nota**<br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. Para especificar un valor en el objeto de informe, seleccione el informe en la CMC y haga clic en *Configuración predeterminada* > *Viendo grupo de servidores* >. | El valor predeterminado es **FALSE**. |
| *Compartir datos del informe entre clientes* | Especifica si los datos de informe se comparten entre clientes distintos. Especifica si los datos de informe se comparten entre clientes distintos.<br>**Nota**<br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. | El valor predeterminado es **TRUE**. |
| *Tiempo de espera de la conexión inactiva (minutos)* | Especifica el período de tiempo, en minutos, que el servidor de procesamiento de Crystal Reports espera una solicitud de una conexión inactiva. Por lo general no hay necesidad de modificar el valor predeterminado. | El valor predeterminado es 20 minutos. |
| *Número máximo de tareas simultáneas (0 para automático)* | Especifica el número máximo de tareas independientes permitidas para ejecutarse simultáneamente en el servidor de procesamiento de Crystal Reports. Si el valor de esta propiedad se establece en «0», el servidor aplica un valor adecuado, según la CPU y la memoria del equipo en el que se ejecuta el servidor. | El valor predeterminado es 0. |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Datos a petición más antiguos facilitados a los clientes (segundos)* | Especifica el período de tiempo, en segundos, que el servidor usa datos en caché para cumplir las solicitudes de los informes a petición.<br><br>Si el servidor recibe una solicitud que se puede procesar con los datos generados para procesar una anterior y el tiempo transcurrido desde que se generaron dichos datos es menor que el valor configurado aquí, el servidor de procesamiento volverá a utilizar estos datos para procesar la solicitud posterior. Volver a utilizar los datos de este modo mejora de manera significativa el rendimiento del sistema cuando varios usuarios necesitan la misma información.<br><br>Al configurar este valor, tenga en cuenta lo importante que resulta para los usuarios recibir datos actualizados. Si es muy importante que todos los usuarios reciban datos nuevos (quizás porque los datos importantes cambian con mucha frecuencia), es posible que tenga impedir este tipo de utilización de los datos configurando el valor en 0.<br><br>**Nota**<br><br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. | El valor predeterminado es 0. |
| *Número máximo de procesos secundarios iniciados previamente* | Especifica el número máximo de procesos secundarios iniciados previamente que permite el servidor. Si este valor es demasiado bajo, el servidor crea procesos secundarios tan pronto como se realizan las solicitudes y el usuario puede experimentar latencia. Si el valor es demasiado alto, los procesos secundarios inactivos pueden malgastar innecesariamente los recursos del sistema. | El valor predeterminado es 1 proceso secundario. |
| *Directorio temporal* | Especifica el directorio donde se crean los archivos temporales cuando es necesario.<br><br>**Nota**<br><br>Se pueden producir problemas de rendimiento si este directorio no dispone de espacio en disco adecuado. | %DefaultDataDir%/CrystalReportsProcessingServer/temp |
| *Ruta de clase de Java* | El nombre y la ruta de las clases Java que necesita el servidor. | %CommonJavaLibDir%/procCR.jar |
| *Argumentos VM secundarios Java* | Especifica los argumentos de la línea de comandos que se proporcionan a los procesos secundarios que crea el servidor. | Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%,Dcom.businessobjects.mds.cs.ImplementationID=csEX |

Propiedades del servicio de inicio de sesión único

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Expiración del inicio de sesión único (segundos)* | Especifica el tiempo, en milisegundos, que una conexión de inicio de sesión único es válida antes de expirar. | El valor predeterminado es 86400 segundos. |

## Propiedades del servidor de aplicaciones de informes de Crystal Reports 2020

> **Nota**
>
> Al modificar alguna de estas propiedades, debe reiniciar el servidor para que los cambios surtan efecto.

Propiedades del servicio de visualización y modificación de Crystal Reports 2020

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Permitir que las tareas de informe permanezcan conectadas a la base de datos hasta que se cierre la tarea de informe* | Especifica si la tarea de informe permanecerá conectada a la base de datos hasta que se haya ejecutado el proceso. | El valor predeterminado es **FALSE**. |
| *Tamaño de datos de exploración (registros)* | Especifica el número de registros distintos devueltos de la base de datos cuando se explore mediante los valores de un campo determinado. Los datos se recuperan en primer lugar de la caché del cliente (si está disponible) y, a continuación, de la caché del servidor. Si los datos no se encuentran en ninguna de las dos cachés, se recuperan de la base de datos. | El valor predeterminado es 100 registros. |
| *Tiempo de espera de la conexión inactiva (minutos)* | Especifica el período de tiempo, en minutos, que el servidor de aplicaciones de informes (RAS) espera solicitudes de un cliente inactivo antes de que se agote el tiempo de espera.<br><br>La configuración de un valor demasiado bajo puede provocar que la solicitud de un usuario se cierre prematuramente y la configuración de un valor demasiado puede afectar a la escalabilidad del servidor (por ejemplo, si el objeto `ReportClientDocument` no se cierra explícitamente, el servidor estará esperando innecesariamente a que se cierre una tarea inactiva). | El valor predeterminado es 30 minutos. |
| *Tamaño de lote (registros)* | Especifica la cantidad de filas del conjunto de resultados que la base de datos devuelve durante cada transferencia de datos.<br><br>Por ejemplo, si se solicitan 500 registros y la propiedad de tamaño de lote se configura como 100 registros, los datos se devolverán en 5 lotes independientes de 100 filas. Para mejorar el rendimiento del RAS, debe conocer el entorno de red, la base de datos y el tipo de las solicitudes para establecer el tamaño de lote adecuado. | El valor predeterminado es 100 registros. |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Número de registros de la base de datos para leer al previsualizar o actualizar un informe (-1 para ilimitado)* | Especifica el número de registros de base de datos que se leerán al visualizar o actualizar un informe. Esta configuración limita el número de registros que el servidor recupera de la base de datos cuando un usuario ejecuta una consulta o un informe. Esta configuración resulta útil cuando se desea impedir que los usuarios ejecuten informes a petición que contengan consultas que devuelvan conjuntos de registros excesivamente grandes.<br><br>Es preferible programar dicho tipo de informe, tanto para que los informes estén más rápidamente a disposición de los usuarios como para reducir la carga de la base de datos de estas consultas grandes. | El valor predeterminado es 20000 registros. |
| *Número máximo de tareas de informe simultáneas (0 para ilimitado)* | Especifica el número máximo de tareas independientes permitidas para ejecutarse simultáneamente en el RAS. | El valor predeterminado es 75 trabajos. |
| *Datos a petición más antiguos facilitados a un cliente (en minutos)* | Especifica el período de tiempo, en minutos, que un informe a petición servirá datos de informe en caché. | El valor predeterminado es 20 minutos. |
| *Directorio temporal* | Especifica el directorio donde se crean los archivos temporales cuando es necesario.<br><br>**Nota**<br>Se pueden producir problemas de rendimiento si este directorio no dispone de espacio en disco adecuado. | `%DefaultDataDir%/CrystalReportsRasServer/temp` |

Propiedades del servicio de inicio de sesión único

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Expiración del inicio de sesión único (segundos)* | Especifica el tiempo, en milisegundos, que una conexión de inicio de sesión único es válida antes de expirar. | El valor predeterminado es 86400 segundos. |

## Propiedades del servidor de procesamiento de Crystal Reports 2020

**Nota**

Al modificar alguna de estas propiedades, debe reiniciar el servidor para que los cambios surtan efecto.

Propiedades del servicio de procesamiento de Crystal Reports 2020

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Tiempo de espera de la tarea inactiva (minutos)* | Especifica el período de tiempo, en minutos, que el servidor de procesamiento de Crystal Reports espera entre solicitudes para una tarea determinada. | El valor predeterminado es 20 minutos. |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Número máximo de tareas de ciclo de vida por proceso secundario* | Especifica el número máximo de tareas que cada proceso secundario puede administrar por vida útil. | El valor predeterminado es 1000. |
| *Actualización del visor siempre proporciona datos actuales* | Especifica si, en el momento que los usuarios actualizan un informe explícitamente, todas las páginas en caché se omiten y se recuperan nuevos datos directamente de la base de datos. Especifica si los datos de informe se comparten entre clientes distintos.<br><br>**Nota**<br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. Para especificar un valor en el objeto de informe, seleccione el informe en la CMC y haga clic en *Configuración predeterminada* > *Viendo grupo de servidores*. | El valor predeterminado es **FALSE**. |
| *Compartir datos del informe entre clientes* | Especifica si los datos de informe se comparten entre clientes distintos. Especifica si los datos de informe se comparten entre clientes distintos.<br><br>**Nota**<br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. | El valor predeterminado es **TRUE**. |
| *Tiempo de espera de la conexión inactiva (minutos)* | Especifica el período de tiempo, en minutos, que el servidor de procesamiento de Crystal Reports espera una solicitud de una conexión inactiva. Por lo general no hay necesidad de modificar el valor predeterminado. | El valor predeterminado es 20 minutos. |
| *Número máximo de tareas simultáneas (0 para automático)* | Especifica el número máximo de tareas independientes permitidas para ejecutarse simultáneamente en el servidor de procesamiento de Crystal Reports. Si el valor de esta propiedad se establece en «0», el servidor aplica un valor adecuado, según la CPU y la memoria del equipo en el que se ejecuta el servidor. | El valor predeterminado es 0. |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Datos a petición más antiguos facilitados a los clientes (segundos)* | Especifica el período de tiempo, en segundos, que el servidor usa datos en caché para cumplir las solicitudes de los informes a petición.<br><br>Si el servidor recibe una solicitud que se puede procesar con los datos generados para procesar una anterior y el tiempo transcurrido desde que se generaron dichos datos es menor que el valor configurado aquí, el servidor de procesamiento volverá a utilizar estos datos para procesar la solicitud posterior. Volver a utilizar los datos de este modo mejora de manera significativa el rendimiento del sistema cuando varios usuarios necesitan la misma información.<br><br>Al configurar este valor, tenga en cuenta lo importante que resulta para los usuarios recibir datos actualizados. Si es muy importante que todos los usuarios reciban datos nuevos (quizás porque los datos importantes cambian con mucha frecuencia), es posible que tenga impedir este tipo de utilización de los datos configurando el valor en 0.<br><br>**Nota**<br><br>Esta propiedad se puede establecer en un objeto de informe y puede variar de un informe a otro; los valores especificados en el objeto de informe anulan la configuración del servidor. | El valor predeterminado es 0. |
| *Número máximo de procesos secundarios iniciados previamente* | Especifica el número máximo de procesos secundarios iniciados previamente que permite el servidor. Si este valor es demasiado bajo, el servidor crea procesos secundarios tan pronto como se realizan las solicitudes y el usuario puede experimentar latencia. Si el valor es demasiado alto, los procesos secundarios inactivos pueden malgastar innecesariamente los recursos del sistema. | El valor predeterminado es 1 proceso secundario. |
| *Directorio temporal* | Especifica el directorio donde se crean los archivos temporales cuando es necesario.<br><br>**Nota**<br><br>Se pueden producir problemas de rendimiento si este directorio no dispone de espacio en disco adecuado. | %DefaultDataDir%/CrystalReports2020ProcessingServer/temp |
| *Permitir que las tareas de informe permanezcan conectadas a la base de datos hasta que se cierre la tarea de informe* | Especifica si la tarea de informe permanecerá conectada a la base de datos hasta que se cierre la tarea. | El valor predeterminado es FALSE. |

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Registros de base de datos leídos al previsualizar o actualizar (0 para ilimitados)* | Especifica el número de registros de base de datos que se leerán al visualizar o actualizar un informe. Esta configuración limita el número de registros que el servidor recupera de la base de datos cuando un usuario ejecuta una consulta o un informe. Esta configuración resulta útil cuando se desea impedir que los usuarios ejecuten informes a petición que contengan consultas que devuelvan conjuntos de registros excesivamente grandes.<br><br>Es preferible programar dicho tipo de informe, tanto para que los informes estén más rápidamente a disposición de los usuarios como para reducir la carga de la base de datos de estas consultas grandes. | El valor predeterminado es 20000. |

Propiedades del servicio de inicio de sesión único

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Expiración del inicio de sesión único (segundos)* | Especifica el tiempo, en milisegundos, que una conexión de inicio de sesión único es válida antes de expirar. | El valor predeterminado es 86400 segundos. |

## 35.1.5 Propiedades de los servicios de análisis

La categoría de servicios de análisis incluye el servidor de procesamiento de Adaptive:

Propiedades del servicio de análisis multidimensional

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Máximo de sesiones del cliente* | Especifica el número máximo de sesiones de MDAS que se pueden abrir simultáneamente en el servidor.<br><br>Cuando el número de sesiones abiertas alcanza este valor, cualquier otro intento de iniciar sesiones de MDAS hará que se muestre un mensaje de error «Servidor no disponible». Puede cambiar este valor para optimizar el rendimiento de MDAS, dependiendo de sus necesidades y del hardware disponible, aunque el aumento de este valor podría producir problemas de rendimiento tanto para MDAS como para la base de datos. El valor predeterminado es 15 sesiones es una estimación conservadora. Para las instalaciones en las que las consultas de usuario son pequeñas, se puede aumentar este valor considerablemente, mientras que en las instalaciones en las que las consultas de usuario son grandes se requerirá un valor menor. | El valor predeterminado es 15. El intervalo válido es de 1 a 100. |
| *Número máximo de celdas devuelto por una consulta* | Especifica el número de celdas que se devuelven al usuario en una única consulta. No se permite al usuario ejecutar una consulta que devuelva un número extremadamente grande de celdas, que consume una gran cantidad de memoria. Si la consulta del usuario supera este límite de celda, el usuario recibe un mensaje de error. | El valor predeterminado es 100 000 celdas. |

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Número máximo de miembros devuelto al filtrar* | Especifica el número de miembros recuperados cuando se filtra por miembro. Si se recuperan muchos miembros, se puede consumir una gran cantidad de memoria. | El valor predeterminado es 100000 miembros. |

Propiedades del servicio de aplicaciones Web BEx

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Máximo de sesiones del cliente* | El número máximo de sesiones de cliente permitidas en el servicio. | El valor predeterminado es 15 sesiones. |
| *Sistema maestro de SAP BW* | El nombre de la conexión OLAP al sistema BW que ha creado en la plataforma de BI. | El valor predeterminado es SAP_BW. |
| *Destino RFC del servidor JCo* | El nombre del destino RFS del servidor JCo que ha introducido en el sistema BW. | De forma predeterminada, este valor está vacío. |
| *Host de puerta de enlace del servidor JCo* | El nombre del host de puerta de enlace del servidor JCo que ha definido en el sistema BW. | De forma predeterminada, este valor está vacío. |
| *Servicio de puerta de enlace del servidor JCo* | El nombre del Servicio de puerta de enlace del servidor JCo que ha definido en el sistema BW. | De forma predeterminada, este valor está vacío. |
| *Recuento de conexión del servidor JCo* | Especifica el número de programas creados automáticamente que se pueden utilizar para gestionar llamadas desde ABAP a Java para el servicio. | El valor predeterminado es 3 conexiones. |

## 35.1.6 Propiedades de los servicios de federación de datos

La categoría de servicios de federación de datos incluye el servidor de procesamiento de Adaptive:

Propiedades del servicio de federación de datos

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Máx. de conexiones* | Especifica el número máximo de conexiones permitidas en el servidor. | El valor predeterminado es 32767. |
| *Tamaño del grupo en ejecución* | Especifica el número máximo de consultas que pueden ejecutarse en paralelo en un momento determinado. | El valor predeterminado es 10. |
| *Tiempo de espera de inactividad de la conexión* | Especifica la cantidad de tiempo en segundos tras la cual se cierra una conexión inactiva. | El valor predeterminado es 10800 segundos. |
| *Tiempo de espera de inactividad de la instrucción* | Especifica la cantidad de tiempo en segundos tras la cual se cierra una declaración de consulta inactiva. | El valor predeterminado es 600 segundos. |

## 35.1.7 Propiedades de los servicios de Web Intelligence

La categoría de servicios de Web Intelligence incluye los siguientes servidores:

- Servidor de procesamiento de Adaptive

- Servidor de procesamiento de Web Intelligence

## Configuración del servidor de procesamiento de Adaptive

Parámetros de la línea de comandos

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Expandir al nivel | Especifica el nivel del que se recuperan los datos de las consultas BEx.<br><br>De forma predeterminada, las jerarquías no se expanden a ningún nivel dado. El nivel predeterminado siempre es el nivel 00. Puede cambiar este comportamiento agregando este parámetro a la línea de comandos, pero si establece un valor demasiado alto, Web Intelligence recuperará todos los datos de la jerarquía, lo que puede incidir en el rendimiento y la estabilidad del sistema. | **`-Dsap.sl.bics.expandToLevel=n`**<br><br>n puede ser cualquier entero entre 0 y 99. Si n=0 o si este parámetro no se especifica, las jerarquías no usarán el parámetro Expandir al nivel. |
| Selección variable de opción de selección | Especifica la opción de selección para selección variable.<br><br>Si esta propiedad se fija en intervalo, el cuadro de texto no estará disponible y los usuario sólo podrán introducir valores de inicio y de fin en el cuadro de diálogo Peticiones.<br><br>Si esta propiedad está fijada en multivalor, la casilla de texto "Escribir un valor" está disponible y los usuarios pueden introducir manualmente valores para las variables Opción de selección BW.<br><br>**Nota**<br>La propiedad no actualiza instalaciones locales de Cliente enriquecido de Web Intelligence. Véase "Manual de instalación del Cliente enriquecido de Web Intelligence" para información sobre la actualización de un registro local para tales instalaciones. | **`-Dsap.sl.bics.variableComplexSelectionMapping=n`**<br><br>dónde n puede ser o un intervalo o un multivalor.<br><br>**Nota**<br>Antes de BI 4.1 SP05, el valor por defecto para esta opción era intervalo. Si añade esta propiedad a las opciones del servidor de procesamiento de Adaptive y lo fija en un multivalor, deberá realizar las siguiente acciones en los documentos existentes:<br>• Un documento se debe purgar.<br>• Los valores por defecto para peticiones de consulta se deben modificar de manera que sea compatible con la selección de multivalor. |

Propiedades del servicio de supervisión de Web Intelligence

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Habilitar supervisión* | Especifica si está habilitada la supervisión para el servicio. | **TRUE** |
| *Supervisar el retraso del bucle del subproceso (segundos)* | Especifica la cantidad de tiempo, en segundos, entre los intentos que el servicio realiza para hacer ping en los clientes. | 300 |

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tiempo de espera predeterminado de limpieza de recursos supervisados (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de realizar una limpieza de la sesión del cliente. | 1200 |
| *Tiempo de espera predeterminado de intercambio de recusas supervisados (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de permutar la sesión del cliente en el disco duro. Se recomienda especificar un valor inferior al valor de la propiedad Tiempo de espera de limpieza de los recursos supervisados. | 600 |
| *Habilitar creación de perfil de servicio* | | **TRUE** |
| *Habilitar control de actividad de servicio* | | **TRUE** |

Propiedades del Servicio de visualización

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tiempo de espera de limpieza del motor de visualización (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de realizar una limpieza de la sesión del cliente. | 1200 |
| *Tiempo de espera de permuta del motor de visualización (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de permutar la sesión del cliente en el disco duro. Es aconsejable especificar un valor inferior al valor de la propiedad *Tiempo de espera de limpieza del motor de visualización (en segundos)*. | 600 |

Propiedades del Servicio Rebean

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del Servicio de recuperación de documentos

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| Sin propiedades de configuración | | |

Propiedades del Servicio de puente DSL

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tiempo de espera para la limpieza del motor DSLBridge (en segundos)* | Especifica la cantidad de tiempo en segundos que el servicio espera que un cliente esté inactivo antes de realizar una limpieza de la sesión del cliente. | 1200 |

## Propiedades del servidor de procesamiento de Web Intelligence

Las propiedades del servidor de procesamiento de Web Intelligence están agrupadas en los siguientes servicios:

- Motor de información
- Núcleo de Web Intelligence
- Procesamiento de Web Intelligence
- Común de Web Intelligence

Los valores de umbral se describen en tablas independientes.

Propiedades del Servicio del motor de información

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Habilitar caché de lista de valores* | Especifica si el almacenamiento en caché está habilitado para las listas de valores en el servidor de procesamiento de Web Intelligence. | **TRUE** |
| *Tamaño de lote de lista de valores (entradas)* | Especifica el número máximo de entradas (o valores) de cada lote de lista de valores. | 1000 |
| *Tamaño máximo de ordenación personalizada (entradas)* | Especifica el número máximo de entradas en la ordenación personalizada. | 100 |
| *Tamaño máximo de la caché de universos (Universos)* | Especifica el número de universos que se puede almacenar en memoria caché en el servidor de procesamiento de Web Intelligence. | 20 |
| *Tamaño máximo de lista de valores (entradas)* | Especifica el número máximo de entradas (o valores) de cada lista de valores. | 50000 |

Propiedades del Servicio principal de Web Intelligence

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Tiempo de espera antes del reciclaje (segundos)* | Especifica el tiempo, en segundos, que el servidor está inactivo antes de que el Server Intelligence Agent (SIA) detenga y reinicie el servidor cuando el número total de documentos procesados está por encima del valor especificado con la propiedad *Número máximo de documentos antes del reciclaje*. | 1200 |
| *Tiempo de espera de documento inactivo (segundos)* | Especifica el período de tiempo, en segundos, antes de que se intercambie la sesión del servidor de procesamiento de Web Intelligence. Por lo tanto, cuando el cliente no genera solicitudes durante este período de tiempo, la sesión se intercambiará al disco duro, con lo que se liberarán recursos para una sesión activa. | 300<br>El intervalo válido es de 100 a 10000 segundos. |
| *Intervalo de sondeo del servidor (segundos)* | Especifica el intervalo, en segundos, que deben transcurrir antes de que el servidor sondee nuevas solicitudes de subproceso. Cuando el servidor se encuentra en la fase de sondeo, lleva a cabo acciones de limpieza, como el intercambio de documentos no utilizadas para mantener la memoria del servidor debajo del umbral de memoria superior. | 120 |
| *Número máximo de documentos por usuario* | Especifica el número máximo de sesiones activas (documentos de Web Intelligence) que se pueden asociar a un usuario en un momento determinado. Por lo tanto, si es 5, el usuario puede usar hasta 5 sesiones activas a la vez. | 5<br>El intervalo válido es de 1 a 20. |

| Propiedad | Descripción | Valor predeterminado |
|---|---|---|
| *Número máximo de documentos antes del reciclaje* | Especifica el número de documentos de Web Intelligence que se pueden procesar antes de que se considere el servidor para reciclaje. Si se ha alcanzado el número de documentos procesados y el servidor está inactivo, éste se cierra y el Server Intelligence Agent (SIA) inicia una nueva instancia del servidor. No obstante, habrá un retado antes de que se inicie una nueva instancia del servidor. El retardo se define mediante la propiedad *Tiempo de espera antes del reciclaje*. | 50 |
| *Habilitar errores de tamaño máximo de asignación de documentos* | Especifica si la propiedad `<Conexiones máximas>` está restringida. Si esta propiedad está activada, el servidor reconoce el valor establecido para la propiedad `<Conexiones máximas>`; de lo contrario, la propiedad se descarta. | **TRUE** |
| *Tiempo de espera de la conexión inactiva (minutos)* | Especifica el período de tiempo, en minutos, que el servidor espera una solicitud de una conexión inactiva. Si se configura un valor demasiado bajo, una solicitud se puede cerrar prematuramente. Si se configura un valor demasiado alto, las solicitudes se pueden asignar a la cola mientras el servidor espera a que se cierren las solicitudes inactivas. | 20 |
| *Conexiones máximas* | Especifica el número máximo de sesiones simultáneas que se pueden abrir de una vez. Se trata de un número aproximado; esta configuración no cuenta las sesiones inactivas que se han intercambiado o la sesión que se crea para analizar el número de sesiones. Si se alcanza este límite y no hay disponible ningún servidor para controlar la solicitud, el usuario recibirá un mensaje de error.<br><br>**Nota**<br>La propiedad `<Habilitar errores de tamaño máximo de asignación de documentos>` se debe activar para que el servidor reconozca esta propiedad. | 200<br><br>El intervalo válido es de 5 a 65535. |
| *Habilitar análisis de memoria* | Especifica si está habilitado el análisis de la memoria. Si está propiedad está activada, el servidor activa y reconoce las siguientes propiedades:<br>• `<Umbral máximo de la memoria>`<br>• `<Umbral superior de la memoria>`<br>• `<Umbral inferior de la memoria>`<br><br>Cuando la memoria de proceso del servidor está por encima de `<Umbral superior de la memoria>`, la única operación que se permite es el almacenamiento de documentos. Cuando la memoria de proceso está por encima de `<Umbral máximo de la memoria>`, se detendrán y fallarán todas las operaciones. | **TRUE** |
| *Umbral inferior de la memoria (MB)* | Especifica el umbral inferior para el consumo de memoria. | **3500** |
| *Umbral superior de la memoria (MB)* | Especifica el umbral superior para el consumo de memoria. | **4500** |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Umbral máximo de la memoria (MB)* | Especifica el umbral máximo para el consumo de memoria. | **6000** |
| *Habilitar supervisión del servicio APS* | Habilita la supervisión del servidor por parte del servicio PJS, alojado en el servidor de procesamiento de Adaptive. | **TRUE** |
| *Reintentar recuento del fallo de ping del servicio APS* | Especifica el número de veces que el servidor intentará alcanzar el servicio APS antes de decidir que no puede hacerlo. | 3 |
| *Período de umbral de supervisión del servicio APS* | Especifica el periodo de retraso entre los intentos de alcanzar el servicio APS. | 300 |
| *Habilitar informes de la actividad actual* | Especifica si los seguimientos completos se generan en los archivos del registro del servidor.<br>**Nota**<br>Esta propiedad debería habilitarse solo para la depuración cuando se solucionan problemas. Establézcala en **FALSO** durante las operaciones normales. | **FALSE** |

Propiedades del Servicio de procesamiento de Web Intelligence

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Habilitar el uso de la URL HTTP* | Especifica si el servidor puede acceder a archivos almacenados en una ubicación remota. | **TRUE** |
| *Valor de proxy* | Especifica la dirección del servidor proxy de la red. Solo es necesario especificar un valor si la red tiene un servidor proxy y el usuario está intentado acceder a los archivos que se encuentran en una ubicación remota. | En blanco |

Propiedades del Servicio común de Web Intelligence

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Tiempo de espera de la caché (minutos)* | Especifica el período de tiempo, en minutos, antes de que se borre el contenido de la caché de documentos. El tiempo de espera depende de la fecha de acceso más reciente por documento. | 4370 |
| *Intervalo de limpieza de caché de documentos (minutos)* | Especifica el intervalo de tiempo, en minutos, que se explora la caché de documentos y se comprueba con las configuraciones `<Tamaño máximo de caché de documentos>`, `<Espacio de reducción máximo de la caché de documentos>` y `<Número máximo de documentos en la caché>`. | 120 |
| *Deshabilitar uso compartido de caché* | Especifica si está deshabilitado el uso compartido de la caché. De forma predeterminada, el uso compartido de la caché está habilitado, lo que significa que todas las instancias del servidor de procesamiento de Web Intelligence compartirán la misma caché. No obstante, si prefiere disponer de una caché por instancia de servidor de procesamiento de Web Intelligence, debe habilitar esta propiedad. | **FALSE** |

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Habilitar caché de documentos* | Especifica si está habilitada la caché de documentos. Si esta propiedad está habilitada, la caché se puede cargar previamente con documentos de Web Intelligence programados. | **TRUE** |
| *Habilitar almacenamiento en caché en tiempo real* | Especifica si está habilitada la caché en tiempo real. Si esta propiedad está habilitada, la caché se puede cargar dinámicamente. Por lo tanto, el servidor de procesamiento de Web Intelligence almacena en caché los documentos de Web Intelligence cuando se ven. El servidor también almacena en caché los documentos cuando se ejecutan como una tarea programada, si se ha activado el almacenamiento en caché previo en el documento. | **TRUE** |
| *Tamaño máximo de caché de documentos (KB)* | Especifica el tamaño máximo de la caché de documentos. Una vez alcanzado este límite, se borrará la caché de documentos según la propiedad `<Espacio de reducción máximo de la caché de documentos>`. | 1000000 |
| *Espacio de reducción máximo de la caché de documentos (porcentaje)* | Especifica el porcentaje de la caché que se vacía para permitir que las acciones y los resultados más recientes se almacenen en la caché. Los documentos con la «última hora de acceso» más antigua se purgarán. | 70 |
| *Tamaño máximo de secuencia de caracteres (MB)* | Especifica el tamaño máximo de la secuencia de caracteres enviada al cliente de Web Intelligence.<br>**Nota**<br>Si se supera la propiedad *Tamaño máximo de secuencia de caracteres*, no se creará el documento de Web Intelligence y el cliente recibirá un mensaje de error. | 5<br>El intervalo válido es de 1 a 4095 MB. |
| *Tamaño máximo de secuencia binaria (MB)* | Especifica el tamaño máximo, en MB, de un flujo binario enviado al cliente de Web Intelligence.<br>**Nota**<br>Si se supera la propiedad *Tamaño máximo de secuencia binaria*, no se creará el documento de Web Intelligence y el cliente recibirá un mensaje de error. | 50<br>El intervalo válido es de 1 a 4095 MB. |
| *Directorio de imágenes* | Especifica la ubicación del directorio de imágenes. | En blanco |
| *Directorio de caché de salida* | Especifica la ubicación de la caché. | En blanco |

Propiedades generales

| Propiedad | Descripción | Valor predeterminado |
| --- | --- | --- |
| *Expiración del inicio de sesión único (segundos)* | Especifica el tiempo, en milisegundos, que una conexión de inicio de sesión único es válida antes de expirar. | 86400 |

## Información relacionada

Configuración de los umbrales de memoria del servidor de Web Intelligence [página 1197]

# 35.1.7.1 Configuración de los umbrales de memoria del servidor de Web Intelligence

En las siguientes secciones se describe lo que sucede en un servidor de Web Intelligence cuando se alcanza un umbral de memoria máxima, superior o inferior.

## Umbral inferior de la memoria

Si se alcanza el límite `<Umbral inferior de la memoria>`, el servidor volcará los documentos inactivos al disco duro y asignará memoria adicional para los documentos que están activos. Cada usuario puede tener hasta un documento activo en lugar de `<Documentos máximos por usuario>`.

## Umbral superior de la memoria

Si se alcanza el `<Umbral superior de la memoria>`, se llevarán a cabo las siguientes acciones de servidor para liberar recursos y proteger el servidor:

- El servidor rechazará conexiones nuevas y llamadas de clientes nuevos. Sólo se permitirá la opción para *Guardar* documentos de Web Intelligence. Los usuarios que soliciten una acción, recibirán un mensaje `Servidor ocupado` y se les notificará que deben guardar los cambios pendientes.
- El servidor activará la limpieza del sistema para liberar suficientes recursos de modo que la cantidad de memoria asignada esté por debajo del límite establecido por la propiedad `<Umbral superior de la memoria>`.
- El servidor intenta cerrar los documentos de solo lectura.
- Si no se ha liberado suficiente memoria durante la limpieza del sistema, el servidor comenzará a cerrar los documentos que están en el modo *Edición*. El servidor comenzará a cerrar los documentos basado en el protocolo LIFO, por el que el documento activo más reciente se purgará de la memoria en primer lugar. El servidor seguirá cerrando documentos hasta que se alcance un nivel seguro; este nivel se basa en el siguiente cálculo: `<Umbral superior de la memoria>` - (20%*(`<Umbral superior de la memoria>`)). Por ejemplo, si la propiedad Umbral superior de la memoria está configurada en 4500 MB, el nivel seguro será:

  ```
  4500MB - .20*4500MB = 3600MB
  ```

  El servidor no puede cerrar documentos cuando se está ejecutando una llamada de cliente. Cualquier documento que se actualiza o exporta a otro formato, o cualquier otra operación que requiera tiempo, no se cerrará cuando el servidor alcance este valor umbral. Si el servidor no puede recuperar suficiente memoria y aún está por encima del `<Valor umbral superior de la memoria>`, se reinicializará.

## Umbral máximo de la memoria

Si se alcanza el límite de <Umbral máximo de la memoria>, se anulan todas las operaciones actuales. Se terminarán todas las llamadas de cliente. Una vez se termina una llamada, se cerrará el documento correspondiente.

# 36 Apéndice de métricas de servidor

## 36.1 Acerca del apéndice de métrica de servidor

En este apéndice, a menos que se indique lo contrario, el término "servidor" se refiere a un servidor de SAP BusinessObjects y no al equipo en el que está instalado o se ejecuta la plataforma de BI.

Las métricas del servidor no están disponibles en los servidores que no están en funcionamiento.

Además de las medidas descritas en este apéndice, la aplicación de supervisión también puede supervisar estos estados de servidor:

| Estado de servidor | Descripción |
|---|---|
| *Estado* | El estado indica el estado general de un servidor. Estos son los posibles valores:<br>• 0 = Rojo (peligro)<br>• 1 = Ámbar (precaución)<br>• 2 = Verde (positivo) |
| *Estado de servidor habilitado* | Este estado indica si un servidor está activado o desactivado. Estos son los posibles valores:<br>• 0 = Desactivado<br>• 1 = Activado |
| *Estado de servidor en ejecución* | Este estado indica el estado de ejecución de un servidor. Estos son los posibles valores:<br>• 0 = DETENIDO<br>• 1 = INICIO<br>• 2 = INICIALIZANDO<br>• 3 = EN EJECUCIÓN<br>• 4 = EN DETENCIÓN<br>• 5 = ERRÓNEO<br>• 6 = RUNNING_WITH_ERRORS<br>• 7 = RUNNING_WITH_WARNINGS |

### 36.1.1 Métricas de servidor común

Las siguientes métricas describen el equipo en el que se está ejecutando el servidor especificado.

Métricas específicas del equipo

| Métrica | Descripción |
|---|---|
| *Nombre de equipo* | El nombre de host del equipo en el que se ejecuta el servidor. |
| *Sistema operativo* | El sistema operativo del equipo en el que se ejecuta el servidor. |
| *Tipo de CPU* | El tipo de unidades de procesamiento central del equipo en el que se ejecuta el servidor. Esta métrica no está disponible en los servidores de procesamiento de Adaptive o los servidores de contenedor de aplicación Web (WACS). |
| *CPU* | El número de CPU disponibles para el servidor. En hardware con más de un núcleo, esta métrica puede indicar el número de CPU lógicas en lugar del número de procesadores físicos. Esta métrica no está disponible en los servidores de procesamiento de Adaptive o los servidores de contenedor de aplicación Web (WACS). |
| *Número de núcleos* | Muestra el número de núcleos en una máquina, donde se aloja el servidor de la plataforma de BI. |
| *RAM (MB)* | La cantidad de memoria en megabytes disponible en el equipo en el que se ejecuta el servidor. Esta métrica no está disponible en los servidores de procesamiento de Adaptive o los servidores de contenedor de aplicación Web (WACS). |
| *Hora local* | La hora local. |
| *Tamaño del disco (GB)* | El tamaño del disco en el que está instalada la plataforma de BI, en gigabytes. Esta métrica no está disponible en los servidores de procesamiento de Adaptive o los servidores de contenedor de aplicación Web (WACS). |
| *Espacio en disco utilizado (GB)* | La cantidad de espacio usado, en gigabytes, en el disco en el que está instalada la plataforma de BI. Esto incluye el espacio en disco que otros programas del equipo usan y no únicamente el espacio usa la plataforma de BI. Esta métrica no está disponible en los servidores de procesamiento de Adaptive o los servidores de contenedor de aplicación Web (WACS). |

Las métricas siguientes describen el servidor de SAP BusinessObjects especificado.

Métricas específicas del servidor

| Métrica | Descripción |
|---|---|
| *Servidor de nombres* | Nombre y número de puerto del servidor CMS en el que este servidor publica su dirección. |
| *Nombre registrado* | El nombre interno del servidor. No es el nombre que aparece en la pantalla *Servidores* de la CMC. |
| *Versión* | La versión del servidor. |
| *Hora de inicio* | La hora a la que se inició por última vez el servidor. |
| *PID* | El número ID de proceso único del servidor. El PID es generado por el sistema operativo del equipo en el que se ejecuta el servidor. Este PID se puede usar para identificar el servidor específico. |
| *Nombre de host* | Una lista separada por comas de los nombres de host que está usando el servidor. |
| *Dirección IP de host* | Una lista separada por comas de las direcciones IP cuyas solicitudes escucha el servidor. |

| Métrica | Descripción |
| --- | --- |
| *Puerto de solicitud* | El puerto del que el servidor recibe solicitudes de otros servidores. Si el servidor escucha solicitudes en más de una dirección IP, el puerto de solicitud del servidor será siempre el mismo. Si algún proceso usa este puerto de solicitud, el servidor no se iniciará. Asegúrese de que ningún otro proceso use este puerto. |
| *Subprocesos del servidor ocupado* | El número de subprocesos de servidor que están atendiendo actualmente una solicitud. Si este número es el mismo que el tamaño máximo del conjunto se subprocesos del servidor, esto indica que el sistema no puede procesar las solicitudes adicionales en paralelo y que puede que las nuevas solicitudes tengan que esperar a que los subprocesos ocupados estén disponibles. |

Métricas de auditorías

| Métrica | Descripción |
| --- | --- |
| *Número actual de eventos de auditoría en cola* | El número de eventos de auditoría que ha registrado un auditado pero que todavía no ha recuperado el auditor de CMS. Si este número aumenta sin límite, podría indicar que la auditoría no está correctamente configurada o que el sistema tiene un elevado nivel de carga y genera eventos de auditoría más rápido de lo que el auditor puede recuperarlos.<br><br>**Nota**<br><br>Al detener un servidor, primero deshabilítelo y espere a que esta métrica alcance «0». Si no lo hace, es posible que en la cola permanezcan eventos de auditoría, que no llegarán al almacén de datos de auditoría hasta que el servidor se reinicie y el CMS los sondee. |

Registro de métricas de servicio

| Métrica | Descripción |
| --- | --- |
| *Directorio de registro* | Los archivos de registro para el servidor están disponibles en esta ubicación. |

## 36.1.2 Métricas del servidor de administración central

En la tabla siguiente se describe la métrica del servidor que aparece en la pantalla *Métricas* para servidores de administración central (CMS).

Métricas del servidor de administración central

| Métrica | Descripción |
| --- | --- |
| *Se ha establecido la conexión a la base de datos de auditoría* | Indica si el CMS está correctamente conectado a la base de datos de auditoría. El valor «1» indica que hay conexión. El valor «0» indica que no hay conexión a la base de datos de auditoría. Si el CMS es un auditor, el valor debería ser «1». Si es «0», investigue el motivo por el que no se puede establecer una conexión a la base de datos de auditoría. |
| *Auditor de CMS* | Indica si el CMS actúa como un auditor. El valor «1» indica que el CMS actúa como auditor. El valor «0» indica que el CMS no actúa como auditor. |

| Métrica | Descripción |
| --- | --- |
| *Nombre de la conexión de la base de datos de auditoría* | El nombre de la conexión de la base de datos de auditoría. No es necesariamente el nombre de la propia base de datos de auditoría. Si esta métrica está vacía, indica que no puede establecerse una conexión a la base de datos de auditoría. |
| *Nombre de usuario de la base de datos de auditoría* | El nombre de la cuenta de usuario empleada para la conexión a la base de datos de auditoría. |
| *La base de datos de auditoría se ha actualizado por última vez el* | La fecha y hora en la que se inició correctamente el CMS para recuperar eventos de un auditado por última vez. Si el CMS es un auditor, esta métrica debe mostrar una hora cercana a la hora que se carga la página «Métricas». Si este valor es más de dos horas antes de la hora a la que se carga la página, puede indicar que la auditoría no está funcionando correctamente. |
| *Duración del último ciclo de sondeo del subproceso de auditoría (en segundos)* | La duración del último ciclo de sondeo en segundos. Indica el retraso máximo de los datos de eventos para acceder a la base de datos de auditoría durante el ciclo de sondeo anterior.<br>• Un valor inferior a 20 minutos indica un sistema en buen estado.<br>• Un valor entre 20 minutos y 2 horas indica un sistema ocupado.<br>• Un valor superior a 2 horas indica un sistema muy ocupado. Si este estado persiste y considera que el retraso es excesivo, es recomendable actualizar el despliegue en todas las bases de datos de auditoría para recuperar datos a mayor velocidad o bien reducir el número de eventos de auditoría que sigue el sistema. |
| *Utilización de subproceso de auditoría* | El porcentaje del ciclo de sondeo que el CMS auditor invierte en la recopilación de datos de los auditados. El tiempo restante es el de las pausas entre sondeos.<br>Si este valor alcanza el 100%, el auditor seguirá recopilando datos de los auditados cuando el siguiente sondeo deba empezar. Esto puede provocar retrasos en los eventos que llegan a la base de datos de auditoría. Si el uso de subprocesos llega con frecuencia al 100% y permanece en este nivel durante varios días, es recomendable actualizar el despliegue para permitir que la base de datos de auditoría reciba datos a mayor velocidad o bien reducir el número de eventos de auditoría que sigue el sistema. |
| *Servidores CMS agrupados* | Una lista separada por punto y coma de los nombres de host y números de puerto de los Servidores de administración central en ejecución del clúster. |
| *Número de sesiones establecidas por usuarios simultáneos* | El número total de sesiones para los usuarios con licencia simultánea. |
| *Número de sesiones establecidas por usuarios con nombre* | El número total de sesiones para usuarios con licencia con nombre. |
| *Número máximo de sesiones de usuario desde el inicio* | El número máximo de sesiones de usuario simultáneas que ha administrado el CMS desde que se inició. |
| *Número de sesiones establecidas por los servidores* | El número de sesiones simultáneas que han creado los servidores de la plataforma de BI con el CMS. Si este número es mayor que 250, cree un CMS adicional. |

| Métrica | Descripción |
| --- | --- |
| *Número de sesiones establecidas por todos los usuarios* | El número de sesiones de usuario simultáneas que administra el CMS cuando se carga la pantalla *Métricas*. Cuanto mayor sea este número, mayor será el número de usuarios que usan este sistema. Si este número es mayor que 250, cree un CMS adicional. |
| *Tareas con errores* | El número de tareas con errores en el sistema. |
| *Tareas pendientes* | Número de tareas programadas pero que no están listas para ejecutarse porque el tiempo o el evento programados no ha llegado. |
| *Tareas en ejecución* | El número de tareas en ejecución actualmente. |
| *Tareas completadas* | El número de tareas completadas en el sistema. |
| *Tareas en espera* | El número de tareas del sistema que están programadas y esperando recursos disponibles. |
| *Licencias de usuario simultáneas* | El número de licencias de usuario simultáneas según lo indicado en el código clave. |
| *Licencias de usuario con nombre* | El número de licencias de usuarios con nombre según lo indicado en el código clave. |
| *Fecha de compilación* | La fecha de compilación del CMS. |
| *Nombre de conexión de la base de datos del sistema* | El nombre de la conexión de la base de datos de sistema de CMS. No es necesariamente el nombre de la propia base de datos de sistema de CMS. |
| *Nombre de servidor de base de datos del sistema* | El nombre del servidor donde se ejecuta la base de datos de sistema de CMS. No es necesariamente el nombre de la propia base de datos de sistema de CMS. |
| *Nombre de usuario de base de datos del sistema* | El nombre de la cuenta de usuario empleada para la conexión a la base de datos de sistema de CMS. |
| *Nombre de origen de datos* | El nombre de la conexión de la base de datos de sistema de CMS. |
| *Número de compilación* | El número de compilación del CMS. Este número se puede usar para identificar la versión de la plataforma SAP BusinessObjects Business Intelligence que tiene instalada. |
| *Versión del producto* | La versión del producto del CMS. |
| *Versión del recurso* | La versión del recurso del CMS. |
| *Tiempo promedio de respuesta de confirmación desde el inicio (mseg)* | La cantidad total de tiempo en milisegundos que necesitó el CMS para realizar operaciones de confirmación desde que se inició el servidor. Un tiempo de respuesta mayor que 1000 milisegundos puede indicar la necesidad de ajustar el CMS o la base de datos de sistema de CMS. |
| *Tiempo promedio de respuesta de consulta desde el inicio (mseg)* | La cantidad total de tiempo en milisegundos que necesitó el CMS para realizar operaciones de consulta desde que se inició el servidor. Un tiempo de respuesta mayor que 1000 milisegundos puede indicar la necesidad de ajustar el CMS o la base de datos de sistema de CMS. |
| *Tiempo de respuesta de confirmación más prolongado desde el inicio (mseg)* | La mayor cantidad de tiempo en milisegundos que necesitó el CMS para realizar operaciones de confirmación desde que se inició el servidor. Un tiempo de respuesta mayor que 10000 milisegundos puede indicar la necesidad de ajustar el CMS o la base de datos de sistema de CMS. |

| Métrica | Descripción |
| --- | --- |
| *Tiempo de respuesta de consulta más prolongado desde el inicio (mseg)* | La mayor cantidad de tiempo en milisegundos que necesitó el CMS para realizar operaciones de consulta desde que se inició el servidor. Un tiempo de respuesta mayor que 10000 milisegundos puede indicar la necesidad de ajustar el CMS o la base de datos de sistema de CMS. |
| *Número de confirmaciones desde el inicio* | El número de confirmaciones enviadas a la base de datos de sistema de CMS desde que se inició el servidor. |
| *Número de consultas desde el inicio* | El número total de consultas de base de datos desde que se inició el servidor. Un número elevado puede indicar un sistema más activo o con elevado nivel de carga. |
| *Número de inicios de sesión de usuario desde el inicio* | El número de inicios de sesión de usuario desde que se inició el servidor. Un número elevado puede indicar un sistema más activo o con elevado nivel de carga. |
| *Conexiones de base de datos del sistema establecidas* | El número de conexiones a la base de datos de sistema de CMS que pudo establecer el CMS. Si se pierde una conexión a la base de datos, el CMS intentará restaurarla. Si el número de conexiones de base de datos establecidas es considerablemente inferior al número de conexiones de la base de datos del sistema que especifica la propiedad *Conexiones a la base de datos del sistema solicitadas* (área *Servicio de administración central* de la pantalla *Propiedades*), es posible que indique que el CMS no puede establecer conexiones adicionales, y que el sistema no funciona de forma óptima. Una posible solución es configurar el servidor de la base de datos para permitir más conexiones de base de datos para el CMS. |
| *Conexiones de bases de datos del sistema en uso* | El número de conexiones a la base de datos de sistema de CMS que está usando el CMS. El número de conexiones que se usan actualmente puede ser menor o igual que el número de conexiones establecidas a la base de datos de sistema. Si el número de conexiones establecidas y el número de conexiones usadas son iguales durante algún tiempo, es posible que se esté produciendo un cuello de botella. El rendimiento del CMS puede mejorar aumentando el valor de la propiedad *Conexiones a la base de datos del sistema solicitadas* en la pantalla *Propiedades*. Ajustando la base de datos de sistema de CMS también se puede mejorar el rendimiento. |
| *Solicitudes de base de datos del sistema pendientes* | El número de solicitudes para la base de datos de sistema de CMS que esperan una conexión disponible. Si este número es elevado, considere aumentar el valor de la propiedad *Conexiones a la base de datos del sistema solicitadas*. Ajustando la base de datos de sistema de CMS también se puede mejorar el rendimiento. |
| *Número de objetos de la caché del sistema del CMS* | El número total de objetos que se encuentran actualmente en la caché del sistema de CMS. |
| *Número de objetos de la BD del sistema del CMS* | El número total de objetos que se encuentran actualmente en la base de datos de sistema de CMS. |
| *Cuentas de usuario simultáneo existentes* | El número total de usuarios existentes con licencia simultánea en el clúster. |
| *Cuentas de usuario con nombre existentes* | El número total de usuarios existentes con licencia con nombre en el clúster. |

## 36.1.3 Métrica del servidor de conexión

Las siguientes métricas son específicas del servidor de conexión.

Métricas de servicios de conectividad

| Métrica | Descripción |
| --- | --- |
| *Orígenes de datos* | Enumera en una tabla los orígenes de datos activados mediante la página *Propiedades*. Muestra la siguiente información para cada capa de red y par de base de datos:<br>• *Estado* (*Cargado* o *Error*): el estado actual del controlador<br>• *Conexiones disponibles: número de conexiones en grupo que se pueden utilizar*<br>• *Tareas (CORBA): número de tareas que se están procesando (despliegue de dos niveles)*<br>• *Tareas (HTTP): número de tareas que se están procesando (despliegue de nivel Web)*<br>**Nota**<br>Para obtener más información sobre los grupos de conexiones, consulte el *Manual de acceso a los datos*. |

## 36.1.4 Métricas del servidor de eventos

En la tabla siguiente se describen las métricas del servidor que aparecen en la pantalla *Métricas* para los servidores de eventos.

Métricas de servicios de eventos

| Métrica | Descripción |
| --- | --- |
| *Lista de archivos monitorizados* | Una tabla que enumera los archivos que el Servidor de eventos supervisa. La columna «Nombre de archivo» muestra el nombre y la ruta del archivo. La columna «Última hora de notificación» muestra la última fecha y hora en que el servidor realizó un sondeo y encontró que el archivo existe. |
| *Archivos monitorizados* | Número total de archivos que están siendo monitorizados por el servidor de eventos. |

## 36.1.5 Métricas del servidor del repositorio de archivos

En la tabla siguiente se describen las métricas de servidor que aparecen en la pantalla *Métricas* para servidores del repositorio de archivos de entrada y de salida.

Métricas del servicio de almacenamiento de archivos

| Métrica | Descripción |
| --- | --- |
| *Archivos activos* | El número de archivos del servidor del repositorio de archivos al que se está accediendo actualmente. |

| Métrica | Descripción |
| --- | --- |
| *Datos escritos (MB)* | El número total de megabytes escritos en archivos en el servidor. |
| *Datos enviados (MB)* | El número total de megabytes leídos de archivos en el servidor. |
| *Lista de archivos activos* | Una tabla que muestra los archivos del servidor del repositorio de archivos a los que se está accediendo actualmente. |
| *Conexiones activas* | El número total de conexiones activas desde clientes y con otros servidores. |
| *Espacio en disco disponible en el directorio raíz (GB)* | La cantidad total de espacio disponible en el disco que contiene el archivo ejecutable del servidor, en gigabytes. |
| *Espacio en disco libre en el directorio raíz (GB)* | La cantidad total de espacio libre en el disco que contiene el archivo ejecutable del servidor, en gigabytes. |
| *Espacio en disco total en el directorio raíz (GB)* | El espacio en el disco total disponible que contiene el archivo ejecutable del servidor, en gigabytes. |
| *Espacio en disco disponible en el directorio raíz (%)* | La cantidad de espacio disponible en el disco que contiene el archivo ejecutable del servidor. |

## 36.1.6 Métricas del servidor de procesamiento de Adaptive

En la tabla siguiente se describe la métrica del servidor que aparece en la pantalla *Métricas* para servidores de procesamiento de Adaptive.

Métricas del servidor de procesamiento de Adaptive

| Métrica | Descripción |
| --- | --- |
| *Subprocesos en el nivel de transporte* | El número total de subprocesos en todos los grupos de subprocesos del nivel de transporte. |
| *Tamaño del conjunto de subprocesos del nivel de transporte* | El número total de subprocesos compartidos del nivel de transporte. Cualquiera de los servicios alojados en el servidor de procesamiento de Adaptive puede usar estos subprocesos. |
| *Procesadores disponibles* | Número de procesadores disponibles para la Máquina virtual Java (JVM) en la que se ejecuta el servidor. |
| *Memoria máxima (MB)* | La cantidad máxima de memoria en megabytes que intentará usar la máquina virtual Java. |
| *Memoria libre (MB)* | La cantidad de memoria en megabytes disponible para que la JVM asigne nuevos objetos. |
| *Memoria total (MB)* | La cantidad total de memoria en megabytes en la máquina virtual Java. Este valor puede variar a lo largo del tiempo en función del entorno del host. |
| *Porcentaje de uso de CPU (últimos 5 minutos)* | El porcentaje de tiempo total de CPU que ha usado el servidor durante los últimos cinco minutos. Por ejemplo, si un único subproceso utiliza una CPU completa de un sistema compuesto por cuatro CPU, el porcentaje de uso es del 25%. Se tienen en cuenta todos los procesadores asignados a la JVM. Un valor superior al 80% puede indicar un cuello de botella de CPU. |

| Métrica | Descripción |
| --- | --- |
| *Porcentaje de uso de CPU (últimos 15 minutos)* | El porcentaje de tiempo total de CPU que ha usado el servidor durante los últimos 15 minutos. Por ejemplo, si un único subproceso utiliza una CPU completa de un sistema compuesto por cuatro CPU, el porcentaje de uso es del 25%. Se tienen en cuenta todos los procesadores asignados a la JVM. Un valor superior al 70% puede indicar un cuello de botella. |
| *Porcentaje de sistema detenido durante GC (últimos 5 minutos)* | Porcentajes de sistema detenido mientras se ejecutaban recopilaciones de desecho (GC) durante los últimos cinco minutos. En este estado, se impide que todos los servicios de APS se ejecuten mientras la máquina virtual realiza una fase crítica de recopilación de desechos que requiere un acceso exclusivo.<br><br>En condiciones normales se devolverá generalmente un valor bajo de un único dígito, incluso con carga. Un valor de dos dígitos prologando en el tiempo puede indicar un problema de bajo rendimiento y será necesario investigarlo. |
| *Porcentaje de sistema detenido durante GC (últimos 15 minutos)* | Porcentajes de sistema detenido mientras se ejecutaban recopilaciones de desecho (GC) durante los últimos 15 minutos. En este estado, se impide que todos los servicios de APS se ejecuten mientras la máquina virtual realiza una fase crítica de recopilación de desechos que requiere un acceso exclusivo.<br><br>En condiciones normales se devolverá generalmente un valor bajo de un único dígito, incluso con carga. Un valor de dos dígitos prologando en el tiempo puede indicar un problema de bajo rendimiento y será necesario investigarlo. |
| *Número de errores de página durante GC (últimos 5 minutos)* | El número de errores de página producidos mientras se ejecutaban recopilaciones de desecho durante los últimos cinco minutos. Un valor mayor que 0 indica un sistema con elevado nivel de carga y baja memoria. |
| *Número de errores de página durante GC (últimos 15 minutos)* | El número de errores de página producidos mientras se ejecutaban recopilaciones de desecho durante los últimos 15 minutos. Un valor mayor que 0 indica un sistema con elevado nivel de carga y baja memoria. |
| *Número de GC completos* | El número de recopilaciones de desecho completas desde que se inició el servidor. Un rápido aumento de este valor puede indicar que el sistema tiene un bajo nivel de memoria. |
| *Recuento de contenciones de bloqueo de JVM* | El número de objetos sincronizados que tienen subprocesos que están esperando para acceder. Un valor considerablemente mayor que 0 puede indicar la presencia de subprocesos que no se volverán a ejecutar. Inicie un volcado de subprocesos para obtener más información sobre la causa del problema. |
| *Información de depuración de JVM* | Información de depuración sobre SAP Java Virtual Machine, incluido el estado, puerto y cliente adjunto, si lo hubiere. |
| *Información de versión de JVM* | Información de versión sobre SAP Java Virtual Machine. |
| *Contador de subprocesos interbloqueados de JVM* | El número de subprocesos que están interbloqueados. Un valor mayor que 0 indica la presencia de subprocesos que no se volverán a ejecutar. Inicie un volcado de subprocesos para obtener más información sobre la causa del problema. |
| *Marcas de seguimiento JVM* | Las marcas de seguimiento actualmente activadas para la JVM. Indica el nivel de seguimiento de la JVM. |
| *Servicios* | Una lista separada por comas de los servicios que aloja el servidor. |

Métricas del servicio de puente DSL

| Métrica | Descripción |
| --- | --- |
| *DSLServiceMetrics.queryCount* | El número de solicitudes de datos que están abiertas entre los clientes y el servicio |
| *DSLServiceMetrics.activeConnectionCount* | El número de conexiones que están abiertas actualmente entre los clientes y el servicio |
| *DSLServiceMetrics.activeSessionCount* | El número de sesiones que están abiertas actualmente entre los clientes y el servicio |
| *DSLServiceMetrics.activeOLAPConnection Count* | El número de conexiones que están abiertas actualmente entre los clientes OLAP y el servicio. |

Métricas del servicio proxy de auditoría de cliente

| Métrica | Descripción |
| --- | --- |
| *Número de eventos de auditoría recibidos desde el inicio del servidor* | El número de eventos de auditoría de cliente que el servicio recibió desde que se inició. Esta métrica se puede usar para verificar que la auditoría de cliente se ha configurado correctamente. Los valores superiores a «0» indican que los eventos de auditoría de los clientes se dirigen correctamente a través de este servicio de auditoría de cliente. |

Métricas del servicio de búsqueda en plataforma

| Métrica | Descripción |
| --- | --- |
| *Número de intentos de extracción correctos desde el inicio del servicio* | El número de intentos correctos para extraer documentos desde que se iniciara el servicio de búsqueda en plataforma. |
| *Fecha y hora de última actualización del índice* | La fecha y la hora en que se actualizó el índice por última vez. |
| *Fecha y hora de última generación del almacén de contenido* | La fecha y la hora en la que se generó el último almacén de contenido. |
| *Número de intentos de extracción erróneos desde el inicio del servicio* | El número de intentos erróneos para la extracción de documentos desde que se iniciara el servicio de búsqueda en plataforma. |
| *Servicio disponible* | TRUE si el servicio está disponible; de lo contrario, FALSE. |
| *Indexación en ejecución* | TRUE si la indexación se está ejecutando; de lo contrario, FALSE. |
| *Número de documentos indexados* | Muestra el número de documentos que se han indexado desde que se iniciara el servicio. |

Métricas del Servicio de análisis multidimensional

| Métrica | Descripción |
| --- | --- |
| *Recuento de sesiones* | El número actual se conexiones de los clientes de MDAS al servidor. |
| *Recuento de cubos* | El número de orígenes de datos que se están usando para suministrar datos a las conexiones que no han agotado el tiempo de espera. |
| *Recuento de consultas* | El número de solicitudes de datos que están abiertas entre los clientes MDAS y el servidor. |

Métricas del servicio de federación de datos

| Métrica | Descripción |
| --- | --- |
| *Número de consultas en ejecución* | El número total de consultas en ejecución (que consuman memoria o no). |

| Métrica | Descripción |
| --- | --- |
| *Número de conexiones* | El número total de conexiones de usuario al motor de consulta de la federación de datos. |
| *Total de bytes transferidos desde los orígenes de datos* | La cantidad de datos leídos desde los orígenes de datos (en bytes). |
| *Total de registros transferidos desde los orígenes de datos* | El número total de filas leídas desde los orígenes de datos. |
| *Total de bytes producidos por la ejecución de consulta* | La cantidad de datos producidos como salida de consultas (en bytes). |
| *Total de registros producidos por la ejecución de consulta* | El número total de filas producidas como salida de consultas. |
| *Número de consultas que consumen memoria* | El número total de consultas en ejecución que consumen memoria. |
| *Total de bytes de memoria usados por la ejecución de consulta* | La cantidad de memoria usada actualmente por las consultas en ejecución (en bytes). |
| *Total de bytes de disco usados por la ejecución de consulta* | La cantidad de disco usado actualmente por las consultas en ejecución (en bytes). |
| *Número de consultas que usan disco* | El número total de consultas en ejecución que usan disco. |
| *Número de consultas que esperan recursos* | El número total de consultas en ejecución que esperan actualmente para la ejecución. |
| *Número de subprocesos activos* | El número total de subprocesos activos que se usan para la ejecución de solicitudes. |
| *Total de bytes de memoria usados por la caché de metadatos* | La cantidad de memoria usada para el almacenamiento en caché de metadatos, estadísticas y configuración de conectores (en bytes). |
| *Número de consultas erróneas* | El número total de consultas erróneas (excepción elevada). |
| *Número de consultas en el paso de análisis de consulta* | El número total de consultas en ejecución que actualmente se encuentran en el paso de análisis. |
| *Número de consultas en el paso de optimización de consulta* | El número total de consultas en ejecución que se encuentran actualmente en el paso de optimización. |
| *Número de consultas en el paso de ejecución de consulta* | El número total de consultas en ejecución que se encuentran actualmente en el paso de ejecución. |
| *Número de conectores cargados* | El número total de conectores cargados en el servicio. |
| *Número de conexiones activas a conectores cargados* | El número total de conexiones activas a conectores cargados en el servicio. |
| *El servicio de federación de datos está disponible* | *TRUE* si el servicio está disponible. De lo contrario, *FALSE*. |

Métricas de servicios de conectividad

| Métrica | Descripción |
| --- | --- |
| *Orígenes de datos* | Enumera en una tabla las fuentes de datos activadas en la página *Propiedades*. Muestra la siguiente información para cada capa de red y par de base de datos:<br>• Estado («Cargado» o «Fallo»): el estado actual del controlador<br>• Conexiones disponibles: número de conexiones en grupo que se pueden utilizar<br>• Tareas (CORBA): número de tareas que se están procesando (despliegue de dos niveles)<br>• Tareas (CORBA): número de tareas que se están procesando (despliegue de dos niveles)<br>Para obtener más información sobre los grupos de conexiones, consulte el *Manual de acceso a los datos*. |

Métricas del servicio de supervisión

| Métrica | Descripción |
| --- | --- |
| *Tiempo promedio de cálculo del estado de vigilancia de los últimos 15 ciclos (mseg)* | El tiempo promedio necesario para calcular el estado de vigilancia de los últimos 15 ciclos para esta instancia del servicio de supervisión. |
| *Número de métricas creadas de usuario* | El número total de métricas creadas por el usuario del clúster, para todos los usuarios. |
| *Número de vigilancias* | El número total de vigilancias del clúster, incluidas las vigilancias habilitadas y deshabilitadas. |
| *serviceBean.monitoringAppPropEnabled* | TRUE si la aplicación de supervisión está habilitada. De lo contrario, FALSE. Esta métrica coincide con la configuración de la página de propiedades de la aplicación de supervisión de la CMC. |
| *Intervalo de actualización de medidas de supervisión (segundos)* | El intervalo de actualización que esta instancia del servicio de supervisión usa actualmente. Al iniciar el servicio, esta métrica se inicializa con la configuración de la página de propiedades de la aplicación de supervisión de la CMC en dicho momento de modo que, en otros momentos, es posible que la métrica sea distinta de la configuración actual de la página de la CMC. |
| *Servicio disponible* | TRUE si el servicio de supervisión está activo. De lo contrario, FALSE. Solo un servicio de supervisión está activo en el clúster. |
| *Número de métricas de tendencia* | El número total de métricas que se registran actualmente en la base de datos de supervisión. |

Métricas del servicio de aplicaciones Web BEx

| Métrica | Descripción |
| --- | --- |
| *Recuento de sesiones* | Un recuento del número total de sesiones activas dentro de un servicio de aplicaciones Web BEx. |

## 36.1.7 Métricas del Servidor de contenedor de aplicación Web

En la tabla siguiente se describen las métricas del servidor que aparecen en la pantalla *Métricas* de los servidores de contenedor de la aplicación web.

> **Nota**
>
> Los servidores de contenedor de la aplicación web también disponen de todas las métricas descritas en la sección "Métricas del servidor de procesamiento de Adaptive".

Métricas del Servidor de contenedor de aplicación Web

| Métrica | Descripción |
|---|---|
| *Lista de conectores WACS en ejecución* | Una lista con todos los conectores en ejecución en el servidor. Si no ve todos los conectores (HTTP, HTTPS y HTTP mediante proxy), quiere decir que el conector no está habilitado o que ha tenido errores durante el inicio. |
| *Conectores WACS con error al inicio* | Indica si se han producido errores en los conectores. Si es verdadero, como mínimo un conector tiene un error al iniciarse. Si es falso, todos los conectores se están ejecutando. No ejecute un servidor cuando uno o varios conectores no se han podido iniciar; debe solucionar el problema del servidor para garantizar que todas las conexiones se inician correctamente. |

### Información relacionada

Métricas del servidor de procesamiento de Adaptive [página 1206]

## 36.1.8 Métricas del servidor de tareas de Adaptive

Métricas del servidor de tareas

| Métrica | Descripción |
|---|---|
| *Solicitudes de tareas recibidas* | El número de tareas que se deberían haber ejecutado en el servidor. |
| *Tareas simultáneas* | El número de tareas que se están ejecutando actualmente en el servidor. Si este número es elevado, el servidor está ocupado. |
| *Número máximo de tareas* | El número máximo de tareas simultáneas ejecutadas a la vez en el servidor. Este número no se reduce nunca hasta el reinicio del servidor. |
| *Creaciones de tareas incorrectas* | El número de tareas que no se han ejecutado correctamente en el servidor. |
| *Directorio temporal* | El directorio donde se crean los archivos temporales. Se puede especificar en la pantalla*Propiedades* del servidor.<br><br>Se pueden producir problemas si este directorio no dispone de espacio en disco adecuado. |

| Métrica | Descripción |
| --- | --- |
| *Configuración predeterminada de destino del sistema de archivos válida* | *TRUE* si el servidor es capaz de enviar documentos al destino del sistema de archivos especificado en la pantalla *Destino* para el servidor. De lo contrario, *FALSE*. |
| *Configuración predeterminada de destino de FTP válida* | *TRUE* si el servidor es capaz de enviar documentos al destino de servidor FTP especificado en la pantalla *Destino* para el servidor. De lo contrario, *FALSE*. |
| *Configuración predeterminada de destino de SFTP válida* | *TRUE* si el servidor es capaz de enviar documentos al destino de servidor SFTP especificado en la pantalla *Destino* para el servidor. De lo contrario, *FALSE*.<br><br>Puede detectar problemas si el fingerprint no se ajusta correctamente al servidor SFTP. |
| *Configuración predeterminada de destino de bandeja de entrada válida* | *TRUE* si el servidor es capaz de enviar objetos al destino de bandeja de entrada especificado en la pantalla *Destino* para el servidor. De lo contrario, *FALSE*. |
| *Configuración predeterminada de destino de correo electrónico válida* | *TRUE* si el servidor es capaz de enviar objetos al destino de correo electrónico especificado en la pantalla *Destino* para el servidor. De lo contrario, *FALSE*. |
| *Servicios de programación* | Una tabla que muestra los servicios que se están ejecutando en el servidor. |
| *Secundarios* | Una tabla que muestra los procesos secundarios que se están ejecutando en el servidor. |

En la siguiente tabla se describen las métricas para cada servicio de programación que se está ejecutando en el servidor.

Métricas del servicio de programación

| Métrica | Descripción |
| --- | --- |
| *Servicio de programación* | El nombre del servicio. |
| *Solicitudes de tareas recibidas* | El número de tareas que se deberían haber ejecutado en el servicio. |
| *Tareas simultáneas* | El número de tareas simultáneas que se están ejecutando actualmente en el servicio. Si este número es elevado, el servicio está ocupado. |
| *Número máximo de tareas* | El número máximo de tareas simultáneas ejecutadas a la vez en el servicio. |
| *Número máximo de tareas simultáneas permitidas* | El número de procesos independientes simultáneos (procesos secundarios) que permite el servicio.<br><br>Se puede especificar en la pantalla*Propiedades* del servidor. |
| *Creaciones de tareas incorrectas* | El número de tareas que no se han ejecutado correctamente en el servicio. |

En la siguiente tabla se describen las métricas para cada proceso secundario que se está ejecutando en el servidor.

Métricas de elementos secundarios

| Métrica | Descripción |
| --- | --- |
| *Servicio de programación* | El nombre del proceso secundario. |
| *PID* | El identificador del proceso secundario. |

| Métrica | Descripción |
| --- | --- |
| *Solicitudes de tareas recibidas* | El número de tareas que se deberían haber ejecutado en el proceso secundario. |
| *Tareas simultáneas* | El número de tareas simultáneas que se están ejecutando actualmente en el proceso secundario. Por lo general este número debe ser «1». |
| *Número máximo de tareas* | El número máximo de tareas simultáneas ejecutadas a la vez en el proceso secundario. |
| *Número máximo de tareas permitidas* | El número de tareas simultáneas que permite el proceso secundario. |
| *Errores comunes* | El número de errores producidos en la comunicación con el servidor de tareas de Adaptive principal. Si este número es elevado, el proceso secundario se reiniciará. |
| *Inicializando* | *TRUE* si el proceso secundario se encuentra en el proceso de inicialización. De lo contrario, *FALSE*. |
| *Cerrando* | *TRUE* si el proceso secundario se encuentra en el proceso de cierre. De lo contrario, *FALSE*. |

## 36.1.9 Métricas de Crystal Reports Server

En la siguiente tabla se describen las métricas del servidor que aparecen en la pantalla *Métricas* para el procesamiento de Crystal Reports y los servidores de procesamiento de Crystal Reports 2020.

Métricas del servidor de procesamiento de Crystal Reports

| Métrica | Descripción |
| --- | --- |
| *Tareas abiertas* | Tabla que lista las tareas que se están ejecutando en el servidor. La tabla incluye el ID y el nombre del documento, el nombre del usuario que ejecuta la tarea, la fecha en la que se accedió al documento por última vez y el tiempo durante el que la tarea se ha estado ejecutando. |
| *Número de solicitudes atendidas* | El número total de solicitudes que el servidor ha servido desde que se inició. |
| *Número de tareas abiertas* | Número de tareas actuales que el servidor y sus procesos secundarios están procesando. |
| *Tipo de objeto* | El tipo de InfoObject con el que trabaja principalmente el servidor. El valor de esta métrica no cambia. |
| *Tiempo de procesamiento promedio (ms)* | El tiempo promedio, en milisegundos, que el servidor ha dedicado al procesamiento de las últimas 500 solicitudes que el servidor ha recibido. Si este número es normalmente alto y sigue aumentando, plantéese crear servidores adicionales en otros equipos. |
| *Tiempo de procesamiento máximo (ms)* | Tiempo máximo en milisegundos que el servidor ha dedicado a procesar una de las últimas 500 solicitudes. Si este número es normalmente alto y sigue aumentando, plantéese crear servidores adicionales en otros equipos. |
| *Tiempo de procesamiento mínimo (ms)* | Tiempo mínimo en milisegundos que el servidor ha dedicado a procesar una de las últimas 500 solicitudes. Si este número es normalmente alto y sigue aumentando, plantéese crear servidores adicionales en otros equipos. |

| Métrica | Descripción |
| --- | --- |
| *Número de solicitudes en cola* | El número de solicitudes que están a la espera de procesarse o que se están procesando. Si este número es normalmente alto y sigue aumentando, plantéese crear servidores adicionales en otros equipos. |
| *Nombre DLL del objeto* | Nombre del complemento de procesamiento para el servidor: El valor de esta métrica no cambia. |
| *Número de conexiones abiertas* | El número de conexiones actualmente abiertas entre el servidor y los clientes. |
| *Tasa de error de solicitud* | Número de solicitudes que el servidor no ha podido procesar como porcentaje de las últimas 500 solicitudes que el servidor ha recibido. |
| *Datos transferidos (KB)* | La cantidad total de datos, en kilobytes, que se han transferido a los clientes desde que se inició el servidor. |
| *Número de solicitudes con errores* | El número de solicitudes que el servidor no ha podido finalizar desde que se inició el servidor. |
| *Número máximo de procesos secundarios* | El número máximo de procesos secundarios simultáneos que se permiten en el servidor. |

En la siguiente tabla se describen las métricas del servidor que aparecen en la pantalla *Métricas* para los servidores de caché de Crystal Reports.

Métricas del servidor de caché de Crystal

| Métrica | Descripción |
| --- | --- |
| *Tasa de aciertos de la caché (%)* | El porcentaje de solicitudes, después de las últimas 500 solicitudes, que se han atendido con los datos almacenados en la memoria caché. |
| *Servidores de procesamiento conectados* | Tabla que enumera los servidores de procesamiento de Crystal Reports en el despliegue. La tabla lista el nombre del servidor y el número de conexiones actualmente abiertas con el servidor. |
| *Número de solicitudes atendidas* | El número total de solicitudes que el servidor ha servido desde que se inició. |
| *Tipo de objeto* | El tipo de InfoObject con el que trabaja principalmente el servidor. El valor de esta métrica no cambia. |
| *Tiempo de procesamiento promedio (ms)* | El tiempo promedio, en milisegundos, que el servidor ha dedicado al procesamiento de las últimas 500 solicitudes que el servidor ha recibido. Si este número es normalmente alto y sigue aumentando, plantéese crear servidores adicionales en otros equipos. |
| *Tiempo de procesamiento máximo (ms)* | Tiempo máximo en milisegundos que el servidor ha dedicado a procesar una de las últimas 500 solicitudes. Si este número es normalmente alto y sigue aumentando, plantéese crear servidores adicionales en otros equipos. |
| *Tiempo de procesamiento mínimo (ms)* | Tiempo mínimo en milisegundos que el servidor ha dedicado a procesar una de las últimas 500 solicitudes. Si este número es normalmente alto y sigue aumentando, plantéese crear servidores adicionales en otros equipos. |
| *Número de solicitudes en cola* | El número de solicitudes que están a la espera de procesarse o que se están procesando. Si este número es normalmente alto y sigue aumentando, plantéese crear servidores adicionales en otros equipos. |
| *Nombre DLL del objeto* | Nombre del complemento de procesamiento para el servidor: El valor de esta métrica no cambia. |

| Métrica | Descripción |
| --- | --- |
| *Tamaño de memoria caché* | La cantidad de datos, en kilobytes, que el servidor está almacenando en caché en el disco. |
| *Número de conexiones abiertas* | El número de conexiones actualmente abiertas entre el servidor y los clientes. |
| *Datos transferidos (KB)* | La cantidad total de datos, en kilobytes, que se han transferido a los clientes desde que se inició el servidor. |

En la siguiente tabla se describen las métricas del servidor que aparecen en la pantalla *Métricas* para los servidores de aplicaciones de informes de Crystal Reports 2020.

Métricas del servidor de aplicaciones de informes de Crystal Reports 2020

| Métrica | Descripción |
| --- | --- |
| *metric_currentdoccount*<br>**Nota**<br>Esta métrica aparece como «document_s_» en la página de supervisión de la CMC. | El número de documentos que el servidor está procesando actualmente. |
| *metric_totaldoccount*<br>**Nota**<br>Esta métrica aparece como «document_s_» en la página de supervisión de la CMC. | El número de documentos que el servidor ha procesado desde que se inició. |
| *metric_currentagentthreadcount*<br>**Nota**<br>Esta métrica aparece como «agent thread_s_» en la página de supervisión de la CMC. | El número de subprocesos que el servidor está procesando actualmente. |
| *metric_totalagentthreadcount*<br>**Nota**<br>Esta métrica aparece como «agent thread_s_» en la página de supervisión de la CMC. | El número de subprocesos que el servidor ha procesado desde que se inició. |

## 36.1.10 Métricas del servidor de Web Intelligence

Métricas del servicio de procesamiento de Web Intelligence

| Métrica | Descripción |
|---|---|
| *Tamaño de caché (KB)* | La cantidad actual de datos en kilobytes que están almacenados en la memoria caché. |
| *Número de documentos obsoletos en caché* | Número de documentos eliminados de la caché porque eran demasiado antiguos, desde que se inició el servidor. |
| *Recuento del marcador alto de caché* | Número de veces que la memoria caché ha alcanzado el tamaño máximo permitido en el servidor desde que se inició. |
| *Uso de CPU (%)* | Porcentaje de tiempo de CPU total invertido por el servidor desde que se inició. |
| *Tiempo total de CPU (segundos)* | Tiempo de CPU total, en segundos, invertido por el servidor desde que se inició. |
| *Recuento del umbral superior de memoria* | Número de veces que se ha alcanzado el umbral superior de memoria en el servidor desde que se inició. |
| *Recuento máximo del umbral de memoria* | Número de veces que se ha alcanzado el umbral máximo de memoria en el servidor desde que se inició. |
| *Tamaño de la memoria virtual (MB)* | Cantidad total de memoria en megabytes que se ha asignado al servidor. |
| *Número actual de llamadas de cliente* | Número actual de llamadas CORBA que el servidor está procesando. |
| *Número de errores remotos de extensión* | Número de veces que el servidor no ha podido conectarse a un servicio de extensión remota alojado por un Servidor de procesamiento de Adaptive. |
| *Número actual de tareas* | Número actual de tareas que el servidor está ejecutando. |
| *Número total de llamadas de cliente* | Número total de llamadas CORBA que el servidor ha recibido desde que se inició. |
| *Número total de tareas* | Número total de tareas que se han ejecutado en el servidor desde que se inició. |
| *Tiempo de inactividad (segundos)* | Tiempo en segundos que ha transcurrido desde la última solicitud que el servidor ha recibido del cliente. |
| *Número actual de sesiones activas* | Número actual de sesiones capaces de aceptar solicitudes de los clientes. |
| *Número de documentos abiertos en el caché* | Número de documentos para los cuales el último resultado de solicitud ha sido leído directamente desde el caché. |
| *Número de documentos* | Número de documentos actualmente abiertos en el servidor. |
| *Número actual de sesiones* | Número actual de sesiones creadas en el servidor. |
| *Número de permutas de documentos* | Número de documentos para los que un subproceso de limpieza ha programado solicitudes de permuta. |
| *Número de documentos permutados* | Número de documentos que se han permutado con solicitudes de permuta. |
| *Número de tiempos de espera de sesiones* | Número de sesiones que ha superado el tiempo de espera desde que se inició el servidor. |
| *Número total de sesiones* | Número de sesiones que se han creado en el servidor desde que se inició. |
| *Número de usuarios* | Número total de usuarios conectados al servidor. |

| Métrica | Descripción |
| --- | --- |
| *Número de subprocesos activos* | Número de subprocesos que atienden solicitudes recibidas por el servidor (conjunto de subprocesos asíncronos). |
| *Número total de subprocesos* | Número total de subprocesos que se han creado desde que el servidor se inicializó (conjunto de subprocesos asíncronos). |

# 37 Apéndice del marcador de posición del servidor y del nodo

## 37.1 Marcadores de posición de servidor y nodo

A excepción de *%SERVER_FRIENDLY_NAME%* y *%SERVER_NAME%*, estos marcadores de posición se aplican a todos los servidores en el mismo nodo.

> **Nota**
>
> Los siguientes marcadores de posición pueden editarse en el nodo. Hallará sus descripciones y valores determinados en la tabla anterior. Los marcadores de posición que no aparecen en esta lista son de solo lectura.
>
> - *%DefaultAuditingDir%*
> - *%DefaultDataDir%*
> - *%DefaultLoggingDir%*
> - *%IntroscopeAgentEnableInstrumentation%*
> - *%IntroscopeAgentEnterpriseManagerHost%*
> - *%IntroscopeAgentEnterpriseManagerPort%*
> - *%IntroscopeAgentEnterpriseManagerTransport%*
> - *%NCSInstrumentLevelThreshold%*
> - *%SMDAgentHost%*
> - *%SMDAgentPort%*

> **Precaución**
>
> Los marcadores de posición que no sean los previstos para la edición no deben cambiarse de ninguna manera. El administrador del sistema debe asegurarse de que solo la persona adecuada del grupo de administradores (que está prevista para la gestión de nodos) tenga los derechos de edición en el nodo. Todos los demás usuarios, incluidos los demás miembros del grupo de administradores, deben estar restringidos para ver/administrar los objetos Nodo aplicando los derechos de seguridad adecuados. En caso de que alguno de los valores de marcador de posición esté dañado accidentalmente y no aparezca CMS, consulte la siguiente nota SAP.

> **Nota**
>
> Consulte el siguiente artículo de la base de conocimientos de SAP 3278916 para saber cómo restringir los marcadores de posición que se modifican para evitar posibles interferencias con fines maliciosos con la infraestructura de BI.

Marcadores de posición

| Marcador de posición | Descripción | Valores predeterminados |
|---|---|---|
| *%AuditingDatabaseConnection%* | La conexión de la base de datos de auditoría usada por el CMS. | Este valor se especifica durante la instalación. |
| *%AuditingDatabaseDriver%* | El tipo de controlador de base de datos que se usa para establecer la conexión con la base de datos de auditoría. | En Windows, el valor predeterminado es sqlserverauditdbss. |
| *%BINDIR%* | La carpeta en la que están ubicados los binarios de 64 bits de la plataforma SAP BusinessObjects Business Intelligence. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/` |
| *%BINDIR32%* | La carpeta en la que están ubicados los binarios de 32 bits de la plataforma SAP BusinessObjects Business Intelligence. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/` |
| *%CACHESERVER_EXE%* | El nombre del ejecutable para el servidor de caché de Crystal Reports. | En Windows, `crcache.exe`. En UNIX, `boe_crcached.bin`. |
| *%CMS_EXE%* | El nombre del ejecutable para el servidor de administración central. | En Windows, `cms.exe`. En UNIX, `boe_cmsd`. |
| *%CONNECTIONSERVER32_EXE%* | El nombre del ejecutable para el servidor de conexión de 32 bits. | En Windows, `ConnectionServer32.exe`. En UNIX, `ConnectionServer32`. |
| *%CONNECTIONSERVER_DIR%* | La carpeta raíz del servidor de conexión. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer` |
| *%CONNECTIONSERVER_EXE%* | El nombre del ejecutable para el servidor de conexión de 64 bits. | En Windows, `ConnectionServer.exe`. En UNIX, `ConnectionServer`. |
| *%CRCPP_BINDIR%* | El directorio donde se encuentran los binarios del servidor de Crystal Reports C++. | En Windows, `<INSTALLDIR>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. En UNIX, el directorio será similar a: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`. |

| Marcador de posición | Descripción | Valores predeterminados |
|---|---|---|
| *%CRCPP_DefaultWorkingDir%* | El directorio de trabajo predeterminado para los servidores de Crystal Reports C++ 2011. | En Windows, `<INSTALLDIR>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86`. En UNIX, el directorio será similar a: `<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`. |
| *%CRYSTALRAS_EXE%* | El nombre del ejecutable para el servidor de aplicaciones de informes. | En Windows, `crystalras.exe`. En UNIX, `boe_crystalrasd`. |
| *%CR_ODBCINI%* | El nombre y la ruta en donde está ubicado el archivo `.odbc.ini`. | En UNIX, `<INSTALLDIR>/bobje/odbc.ini`. En Windows, es una cadena vacía. |
| *%CommonJavaBundlesDir%* | La carpeta donde se encuentran los paquetes OSGI compartidos. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bundles`. |
| *%CommonJavaLibDir%* | La carpeta donde se encuentran las bibliotecas Java comunes. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib`. |
| *%DLLEXT%* | La extensión predeterminada de un archivo `.dll` o `.so`. | En Windows, `.dll`. En UNIX, `.so`. |
| *%DLLPATH%* | El nombre de la variable de entorno en el equipo en el que está instalada la plataforma SAP BusinessObjects Business Intelligence que especifica los directorios donde el intérprete buscará los archivos ejecutables. | En Windows, «Ruta». En UNIX, «LD_LIBRARY_PATH». |
| *%DLLPATH32%* | En sistemas de 32 bits de Solaris, el nombre de la variable de entorno en el equipo en el que está instalada la plataforma SAP BusinessObjects Business Intelligence que especifica los directorios donde el intérprete buscará los archivos ejecutables. | En equipos Solaris, «LD_LIBRARY_PATH_32». Este marcador de posición es una cadena vacía en otros sistemas operativos. |
| *%DLLPATH64%* | En sistemas de 64 bits de Solaris, el nombre de la variable de entorno en el equipo en el que está instalada la plataforma SAP BusinessObjects Business Intelligence que especifica los directorios donde el intérprete buscará los archivos ejecutables. | En equipos Solaris, «LD_LIBRARY_PATH_64». Este marcador de posición es una cadena vacía en otros sistemas operativos. |

| Marcador de posición | Descripción | Valores predeterminados |
|---|---|---|
| *%DLLPREFIX%* | El prefijo predeterminado de un archivo `.dll` o `.so`. | En UNIX, «lib». Este marcador de posición es una cadena vacía en los equipos de Windows. |
| *%DLLPRELOAD%* | El nombre de la variable de entorno LD_PRELOAD para la plataforma. | En UNIX *LD_PRELOAD*. Este marcador de posición es una cadena vacía en los equipos de Windows. |
| *%DLLPRELOAD32%* | El nombre de la variable de entorno LD_PRELOAD en sistema AIX de 32 bits. | En AIX, *LDR_PRELOAD*. Este marcador de posición es una cadena vacía en otros equipos. |
| *%DLLPRELOAD64%* | El nombre de la variable de entorno LD_PRELOAD en sistema AIX de 64 bits. | En AIX, *LDR_PRELOAD64*. Este marcador de posición es una cadena vacía en otros equipos. |
| *%DP%* | El delimitador de ruta. | En Windows, «;». En UNIX, «:». |
| *%DefaultAuditingDir%* | El directorio donde se graban los archivos temporales de auditoría. Para conseguir un rendimiento óptimo, esta ubicación debe estar en la unidad local del servidor. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Auditing`. En UNIX, `<INSTALLDIR>/sap_bobj/data/Auditing/`. |
| *%DefaultDataDir%* | El directorio temporal que usa el servidor de tareas. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Data`. En UNIX, `<INSTALLDIR>/sap_bobj/data/`. |
| *%DefaultInputFRSDir%* | La carpeta raíz del servidor del repositorio de archivos de entrada. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input`. En UNIX, `<INSTALLDIR>/sap_bobj/data/frsinput`. |
| *%DefaultLoggingDir%* | La ubicación donde se almacenan los archivos de registro. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\logging`. En UNIX, `<INSTALLDIR>/sap_bobj/logging`. |
| *%DefaultOutputFRSDir%* | La carpeta raíz del servidor del repositorio de archivos de salida. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output`. En UNIX, `<INSTALLDIR>/sap_bobj/data/frsoutput`. |
| *%DefaultWorkingDir%* | El directorio de trabajo para los servidores de 64 bits. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>`. |

| Marcador de posición | Descripción | Valores predeterminados |
|---|---|---|
| *%DefaultWorkingDir32%* | El directorio de trabajo para los servidores de 32 bits. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>`. |
| *%EPM_LD_PRELOAD_ONCE%* | El nombre de la variable de entorno LD_PRELOAD_ONCE para la plataforma. | $LD_PRELOAD_ONCE$ |
| *%EVENTSERVER_EXE%* | El nombre del ejecutable para el servidor de eventos. | En Windows, `EventServer.exe`. En UNIX, `boe_eventsd`. |
| *%EXEEXT%* | La extensión predeterminada de los archivos ejecutables. | En Windows, `.exe`. Este marcador de posición no está disponible en UNIX. |
| *%EXEPATH%* | El nombre de la variable de entorno en el equipo en el que está instalada la plataforma SAP BusinessObjects Business Intelligence que especifica los directorios donde el intérprete buscará los archivos ejecutables. | En Windows, «Ruta». En UNIX, «RUTA». |
| *%EnterpriseDir%* | La ubicación en la que está instalada la plataforma SAP BusinessObjects Business Intelligence de 64 bits. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40`. |
| *%EnterpriseDir32%* | La ubicación en la que está instalada la plataforma SAP BusinessObjects Business Intelligence de 32 bits. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40`. |
| *%ExternalJavaLibDir%* | La carpeta donde se encuentran las bibliotecas Java externas de terceros. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib\external`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/external`. |
| *%FILESERVER_EXE%* | El nombre del ejecutable para el servidor de archivos. | En Windows, `fileserver.exe`. En UNIX, `boe_filesd`. |
| *%HOARD_PATH%* | La ubicación del administrador de memoria. | De forma predeterminada, está vacío. |
| *%HOARD_PRELOAD%* | Especifica si se debe precargar el administrador de memoria. | De forma predeterminada, está vacío. |
| *%INSTALLROOTDIR%* | La carpeta en la que está instalada la plataforma SAP BusinessObjects Business Intelligence de 64 bits. | Este valor se especifica durante la instalación. |

| Marcador de posición | Descripción | Valores predeterminados |
|---|---|---|
| *%INSTALLROOTDIR32%* | La carpeta en la que está instalada la plataforma SAP BusinessObjects Business Intelligence de 32 bits. | Este valor se especifica durante la instalación. |
| *%IntroscopeAgentEnableInstrumentation%* | Indica si está habilitada la instrumentación para servidores Java usando Introscope Agent Enterprise Manager. | Los valores posibles son TRUE o FALSE, según si Introscope Agent Enterprise Manager se ha habilitado al instalar la plataforma SAP BusinessObjects Business Intelligence. |
| *%IntroscopeAgentEnterpriseManagerHost%* | El nombre del host de Introscope Agent Enterprise Manager al que se envían los datos de instrumentación. | Este valor se especifica durante la instalación. |
| *%IntroscopeAgentEnterpriseManagerPort%* | El puerto de Introscope Agent Enterprise Manager al que se envían los datos de instrumentación. | Este valor se especifica durante la instalación. |
| *%IntroscopeAgentEnterpriseManagerTransport%* | El transporte que se usa al enviar datos de instrumentación a Introscope Agent Enterprise Manager. Los valores permitidos son:<br>• TCP<br>• HTTP<br>• HTTPS<br>• SSL | TCP |
| *%IntroscopeAgentEnterpriseManagerTransportHTTP%* | La clase que se usa al enviar datos de instrumentación a Introscope Agent Enterprise Manager mediante HTTP. | com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory |
| *%IntroscopeAgentEnterpriseManagerTransportHTTPS%* | La clase que se usa al enviar datos de instrumentación a Introscope Agent Enterprise Manager mediante HTTPS. | com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory |
| *%IntroscopeAgentEnterpriseManagerTransportSSL%* | La clase que se usa al enviar datos de instrumentación a Introscope Agent Enterprise Manager mediante SSL. | com.wily.isengard.postofficehub.link.net.SSLSocketFactory |
| *%IntroscopeAgentEnterpriseManagerTransportTCP%* | La clase que se usa al enviar datos de instrumentación a Introscope Agent Enterprise Manager mediante TCP. | com.wily.isengard.postofficehub.link.net.DefaultSocketFactory |
| *%IntroscopeDir%* | La carpeta en la que está instalado Introscope Agent Enterprise Manager. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\wily`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/wily`. |
| *%JAVAW_EXE%* | El nombre del archivo ejecutable para la máquina virtual Java que no tiene ventana de consola. | En Windows, `javaw.exe`. En UNIX, `java`. |
| *%JAVA_EXE%* | El nombre del archivo ejecutable para la máquina virtual Java. | En Windows, `java.exe`. En UNIX, `java`. |

| Marcador de posición | Descripción | Valores predeterminados |
|---|---|---|
| *%JOBSERVERCHILD_EXE%* | El nombre del ejecutable para el servidor de tareas secundario de Adaptive. | En Windows, `JobServerChild.exe`. En UNIX, `boe_jobcd`. |
| *%JOBSERVER_EXE%* | El nombre del ejecutable para el servidor de tareas de Adaptive. | En Windows, `JobServer.exe`. En UNIX, `boe_jobsd`. |
| *%JdkBinDir%* | La carpeta donde se encuentran los binarios de JDK. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin`. En UNIX, `<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/bin`. |
| *%JreBinDir%* | La carpeta donde se encuentran los binarios de JRE. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin`. En UNIX, `<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/jre/bin`. |
| *%JVM_ARCH_ENVIRONMENT%* | Indica si el equipo se ejecuta en la JVM de 32 bits o de 64 bits. | Para los equipos UNIX de 32 bits, el valor predeterminado es «-d32». Para los equipos UNIX de 64 bits, el valor predeterminado es «-d64». En los equipos Windows, es una cadena vacía. |
| *%JVM_HEADLESS_MODE%* | El argumento de línea de comando que especifica si la JVM funciona en modo desatendido. | En Windows, -Djava.awt.headless=false. En UNIX, -Djava.awt.headless=true |
| *%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%* | Los parámetros de la línea de comandos que especifican qué hace la JVM cuando detecta errores de falta de memoria. | "-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError" |
| *%JVM_SHARED_MEMORY_SEGMENT%* | Los parámetros de la línea de comandos que habilitan las extensiones de JVM y definen el número de instancia de JVM. | De forma predeterminada, este marcador de posición está vacío. |
| *%LANGUAGEPACKSDIR%* | La carpeta donde están instalados los paquetes de idioma del despliegue. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/`. |
| *%LANGUAGEPACKSDIR32%* | La carpeta en la que se instalan los paquetes de idiomas del despliegue en sistemas de 32 bits. | . En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\Languages`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/`. |

| Marcador de posición | Descripción | Valores predeterminados |
|---|---|---|
| *%LSTDir%* | La carpeta en la que se almacenan los archivos de configuración LST. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\lst`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/lst`. |
| *%MDAS_JVM_OS_STACK_SIZE%* | Especifica el tamaño de pila de la JVM para el servicio de análisis multidimensional. | De forma predeterminada, este marcador de posición está vacío. |
| *%NCSInstrumentLevelThreshold%* | El nivel de umbral del registro de seguimiento de la biblioteca NCS. | De forma predeterminada, este valor es 0. |
| *%PAGESERVER_EXE%* | El nombre del ejecutable para el servidor de procesamiento de Crystal Reports 2020. | En Windows, `crproc.exe`. En UNIX, `boe_crprocd.bin`. |
| *%PJSContainerDir%* | La carpeta donde se encuentran los JARS del contenedor de APS. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/container`. |
| *%PJSServicesDir%* | La carpeta donde se encuentran los JARS del servicio de APS. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/services`. |
| *%Platform%* | El sistema operativo del equipo que ejecuta la plataforma SAP BI. | El sistema operativo del equipo que ejecuta la plataforma SAP BI. |
| *%Platform32%* | El sistema operativo del equipo que ejecuta la plataforma SAP BI de 32 bits. | El sistema operativo del equipo que ejecuta la plataforma SAP BI. |
| *%RasBinDir%* | La carpeta raíz del servidor de aplicaciones de informes. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras`. |
| *%SERVER_FRIENDLY_NAME%* | El nombre completo del servidor. | El nombre completo del servidor. |
| *%SERVER_NAME%* | El nombre completo del servidor. | El nombre completo del servidor. |
| *%SMDAgentHost%* | El nombre del host del agente SMD al que se envían los datos de instrumentación. | Este valor se especifica durante la instalación. |
| *%SMDAgentPort%* | El puerto del agente SMD al que se envían los datos de instrumentación. | Este valor se especifica durante la instalación. |

| Marcador de posición | Descripción | Valores predeterminados |
|---|---|---|
| *%TRACE_CONFIGFILE_INI%* | El nombre y ruta del archivo `BO_Trace.ini`. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/BO-trace.ini`. |
| *%WarFilesDir%* | La ubicación de los archivos de aplicación Web. | En Windows, `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps`. En UNIX, `<INSTALLDIR>/sap_bobj/enterprise_xi40/warfiles/webapps`. |
| *%WEBI_LD_PRELOAD%* | El nombre de la variable de entorno LD_PRELOAD para la plataforma. | $LD_PRELOAD$ |
| *%WEBISERVER_EXE%* | El nombre del ejecutable para el servidor de procesamiento de Web Intelligence. | En Windows, `wireportserver.exe`. En UNIX, `WIReportServer`. |
| *%WEBI_LD_PRELOAD_ONCE%* | El nombre de la variable de entorno LD_PRELOAD_ONCE para la plataforma. | $LD_PRELOAD_ONCE$ |

## Información relacionada

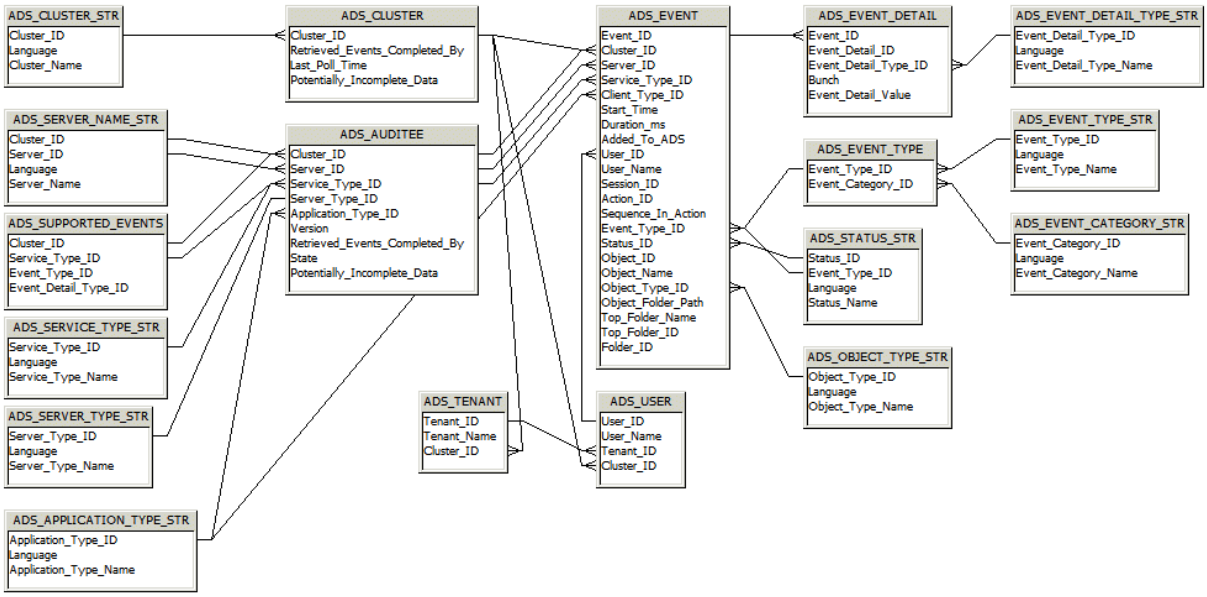
Ver y editar los marcadores de posición de un nodo [página 506]

# 38 Apéndice del esquema del almacén de datos de auditoría

## 38.1 Información general

Este apéndice es una referencia para los diseñadores de informes que accedan o elaboren informes de las tablas Almacén de datos de auditoría. En el siguiente diagrama y explicaciones de la tabla se muestran las tablas donde se registrarán los datos de auditoría y cómo se relacionan dichas tablas.

## 38.2 Diagrama del esquema




## 38.3 Auditing Data Store Tables

### ADS_APPLICATION_TYPE_STR table

This table provides a multilingual dictionary of client application-type names.

| Column Name | Type | Description |
|---|---|---|
| Application_Type_ID | Character (64) | The application-type CUID for the application. |
| Language | Character (10) | Code for the language in which the application type is recorded; for example `<EN>`, or `<DE>`. |
| Application_Type_Name | Character (255) | The text name of the application type; Crystal Reports or Web Intelligence for example. |

## ADS_AUDITEE table

This table records property information for all auditee servers that are part of the deployment.

| Column Name | Type | Description |
|---|---|---|
| Cluster_ID | Character (64) | The GUID for the cluster the auditee belongs to. |
| Server_ID | Character (64) | CUID of the server that triggered the event. If the event is client-triggered, will record the CUID of the adaptive processing server that processed the event. |
| Service_Type_ID | Character (64) | Service-type CUID of the service that triggered the event. Client-triggered events will record an application-type CUID. |
| Server_Type_ID | Character (64) | The server-type CUID for the server that triggered the event. |
| Application_Type_ID | Character (64) | The application-type CUID for the client that triggered the event. For server events, the ID of the service-type will be recorded. |
| Version | Character (64) | The version of the server or client that triggered the event at the time it was recorded. |
| Retrieved_Events_Completed_By | Datetime | The last time the Auditor CMS polled this auditee for its temporary files. This indicates that all events from this auditee competed prior to this date/time are in the ADS. |
| State | Integer | The state (Running, Not Running, Deleted) that the auditee was in. |
| Potentially_Incomplete_Data | Integer | Shows if this auditee may have events that were not transferred to the ADS. |

## ADS_CLUSTER table

This table records information on any clusters that contain Auditees.

| Column Name | Type | Description |
|---|---|---|
| Cluster_ID | Character (64) | The GUID of the cluster. |

| Column Name | Type | Description |
|---|---|---|
| Retrieved_Events_Completed_By | Datetime | Shows how current the auditing information in the database for that cluster is. Records the oldest retrieved auditing timestamp for all currently running auditee servers at any given moment. This indicates all events completed prior to this date are in the ADS. |
| Last_Poll_Time | Datetime | The last time the auditor CMS polled the auditees in this cluster. |
| Potentially_Incomplete_Data | Integer | Indicates potentially incomplete audit information within the cluster: "0" = all servers have transferred data normally; and "1" = at least one running or non-running server in the cluster has its *Potentially Incomplete Data* flag set, meaning that one auditee has events that haven't transferred to the ADS. |

## ADS_CLUSTER_STR table

This table provides a reference record of the different clusters in your deployment.

| Column Name | Type | Description |
|---|---|---|
| Cluster_ID | Character (64) | A unique ID of the cluster. |
| Language | Character (10) | Code for the language setting for the cluster, for example, `<EN>`, or `<DE>`. |
| Cluster_Name | Character (255) | The name of the cluster. |

## ADS_EVENT table

This table records the basic properties for each event, and is the central linking point for other tables in the schema.

| Column Name | Type | Description |
|---|---|---|
| Event_ID | Character (64) | A unique ID generated for the event. |
| Cluster_ID | Character (64) | The GUID of the auditee's cluster. This is recorded because multiple clusters may use the same ADS. |
| Server_ID | Character (64) | The CUID of the server that triggered the event. |
| Service_Type_ID | Character (64) | • The CUID of the service-type that triggered the event. Services on a server will record their service-type CUID.<br>• Client applications (BI launch pad or Web Intelligence for example) will record their application-type CUID. |
| Client_Type_ID | Character (64) | Records the Client Type ID of the client that established the session. |

| Column Name | Type | Description |
|---|---|---|
| Start_Time | Datetime | The date and time (UTC) when the event operation started (including milliseconds). |
| Duration_ms | Integer | Duration of operation in milliseconds.<br>Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`. |
| Added_to_ADS | Datetime | The date and time (UTC) when the event was recorded in the ADS. |
| User_ID | Character (64) | The CUID of the user who performed the action. |
| User_Name | Character (255) | The name associated with the ID of the user who performed the action. Recorded in the Auditor CMS's default language. |
| Session_ID | Character (64) | GUID of the session during which the event was triggered. If there is no associated session, the field will be null. |
| Action_ID | Character (64) | ID of the user action that triggered the event. Used to group events that result from a single user action. |
| Sequence_In_Action | Integer | For multi-server (or client and multi-server) events, the server or client application in the sequence that triggered the event. In all scheduling workflows the sequence ID will always be 0. |
| Event_Type_ID | Integer | Type of event (View or Save, for example). |
| Status_ID | Integer | Status of the operation (for example, "0" = succeeded, "1" = failed). |
| Object_ID | Character (64) | CUID of the object that the operation was performed on. |
| Object_Name | Character (255) | The name of the object the operation was performed on. Recorded in the Auditor CMS's default language. |
| Object_Type_ID | Character (64) | CUID of object-type that the operation was performed on. |
| Object_Folder_Path | Character (255) | The full folder path (for example `Country/Region/City`) for the object the operation was performed on. Recorded in the Auditor CMS's default language. If the folder path cannot be determined this, value will be set to null. |
| Folder_ID | Character (64) | The CUID of the folder for the object the operation was performed. |
| Top_Folder_Name | Character (255) | Name of top level folder for the object. For example, if the object is located in `Country/Region/City` then `Country` will be recorded. |
| Top_Folder_ID | Character (64) | The CUID of the top-level folder where the object resides. For example, if object is located in `Country/Region/City` then the CUID of the `Country` folder will be recorded. |

## ADS_EVENT_CATEGORY_STR Table

This table provides a multilingual dictionary of event category names.

| Column Name | Type | Description |
| --- | --- | --- |
| Event_Category_ID | Integer | The event-category ID. |
| Language | Character (10) | Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`. |
| Event_Category_Name | Character (255) | The name of the event category. |

## ADS_EVENT_DELETES

Do not use or report off of this table. It is intended for internal system use, and may be removed in future releases.

## ADS_EVENT_DETAIL table

This table records event detail properties.

| Column Name | Type | Description |
| --- | --- | --- |
| Event_Detail_ID | Integer | GUID for the event detail. |
| Event_ID | Character (64) | Parent event GUID. |
| Event_Detail_Type_ID | Integer | Type of event detail. |
| Bunch | Integer | If the detail is part of a series, this is used to tie them together.<br>For example, if a report had prompts for State and Country, a user may enter "USA" for the Country prompt, and "California" and "Nevada" for the State prompt. This would produce event details with two bunches. Bunch 1 would consist of:<br>• Prompt Name: Country<br>• Prompt Value: USA<br>Bunch 2 would consist of:<br>• Prompt Name: State<br>• Prompt Value: California<br>• Prompt Value: Nevada |
| Event_Detail_Value | Character (long-text) | The value of the event detail. |

## ADS_EVENT_DETAIL_TYPE_STR table

This table provides a multilingual dictionary of event detail type names.

| Column Name | Type | Description |
|---|---|---|
| Event_Detail_ID | Integer | The event detail-type ID for the event detail. |
| Language | Character (10) | Code for the language that the event detail name is recorded in; for example `<EN>`, or `<DE>`. |
| Event_Detail_Type_Name | Character (255) | The text name of the event detail type. |

## ADS_EVENT_TYPE table

This table provides a reference record for the different categories of events.

| Column Name | Type | Description |
|---|---|---|
| Event_Type_ID | Integer | The unique identifier for the type of event. |
| Event_Category_ID | Integer | Category of event. For example, common, Web Intelligence, or Life-Cycle Management. |

## ADS_EVENT_TYPE_STR Table

This table provides a multilingual dictionary of event type names.

| Column Name | Type | Description |
|---|---|---|
| Event_Type_ID | Integer | The event-type ID for the event. |
| Language | Character (10) | Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`. |
| Event_Type_Name | Character (255) | The text name of the event type; View or Logon for example. |

## ADS_OBJECT_TYPE_STR Table

This table provides a multilingual dictionary of event object names.

| Column Name | Type | Description |
|---|---|---|
| Object_Type_ID | Character (64) | Object-type CUID of the object |
| Language | Character (10) | Code for the language that the object type name is recorded in; for example `<EN>`, or `<DE>`. |
| Object_Type_Name | Character (255) | Name of the object type. |

## ADS_SERVER_NAME_STR table

This table provides a multilingual dictionary of server names. Values will be updated when servers are renamed.

| Column Name | Type | Description |
|---|---|---|
| Cluster_ID | Character (64) | The GUID of the cluster that the server belongs to. |
| Server_ID | Character (64) | The CUID of the server. |
| Language | Character (10) | Code for the language of the server name; for example `<EN>`, or `<DE>`. |
| Server_Name | Character (255) | The name of the server. |

## ADS_SERVICE_TYPE_STR table

This table provides a multilingual dictionary of service-type names.

| Column Name | Type | Description |
|---|---|---|
| Service_Type_ID | Character (64) | The service-type or service-category CUID for the service. |
| Language | Character (10) | Code for the language the service-type name is recorded in, for example `<EN>`, or `<DE>`. |
| Service_Type_Name | Character (255) | The name of the service-type. |

## ADS_STATUS_STR Table

This table provides a multilingual dictionary of event status names.

| Column Name | Type | Description |
|---|---|---|
| Status_ID | Integer | The numerical representation of the operation's status. |
| Event_Type_ID | Integer | ID of the event's event-type. For example, 1002 for View. |
| Language | Character (10) | Code for the language that the event status is recorded in; for example `<EN>`, or `<DE>`. |
| Status_Name | Character (255) | A text description of the event's status; Succeeded or Failed, for example. |

## ADS_SUPPORTED_EVENTS table

This table records a list of supported events and associated event details for each type of service or client application.

| Column Name | Type | Description |
|---|---|---|
| Cluster_ID | Character (64) | The cluster GUID that the service belongs to. |
| Service_Type_ID | Character (64) | Service-type CUID of the service that triggered the event. If the event is triggered by a client application, then an application-type CUID is recorded. |
| Event_Type_ID | Integer | ID for the type of event recorded (ID of Save, for example). |
| Event_Detail_Type_ID | Integer | CUID that identifies the type of event detail captured for that event (File Path, for example). |

## ADS_TENANT Table

This table records the relationship between tenant names and tenant IDs.

| Column Name | Type | Description |
|---|---|---|
| Cluster_ID | Character (64) | The GUID of the cluster. |
| Tenant_ID | Character (64) | The CUID of the tenant. |
| Tenant_Name | Character (255) | The name of the tenant. |

## ADS_USER Table

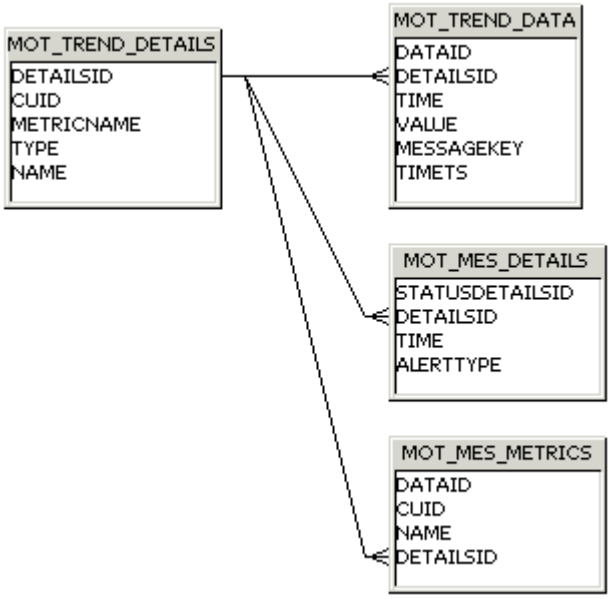
This table records the relationship between users and tenants.

| Column Name | Type | Description |
|---|---|---|
| Cluster_ID | Character (64) | The GUID of the cluster. |
| User_ID | Character (64) | The CUID of the user. |
| User_Name | Character (255) | The name of the user. |
| Tenant_ID | Character (64) | The CUID of the tenant. |

# 39 Apéndice del esquema de base de datos de supervisión

## 39.1 Esquema de base de datos de tendencias

En el diagrama de la base de datos de tendencias y las explicaciones de la tabla se muestran las tablas donde se registrarán los datos de las métricas, medidas y vigilancias así cómo se relacionan dichas tablas.




### MOT_TREND_DETAILS

Esta tabla registra la información sobre las entidades, las medidas y las vigilancias gestionadas. Por ejemplo, los CUID y los nombres de medidas.

| Nombre de columna | Tipo | Clave | Descripción |
|---|---|---|---|
| DetailsId | INTEGER | Clave primaria<br>Generado automáticamente | |
| CUID | VARCHAR(64) | No disponible | CUID de InfoObject que expone la métrica o está relacionado con la métrica |

| Nombre de columna | Tipo | Clave | Descripción |
|---|---|---|---|
| MetricName | VARCHAR(255) | No disponible | Nombre de métrica |
| Tipo | VARCHAR(32) | No disponible | Uno de "Suscripción", "ManagedEntityStatus", o "Métrica" |
| Nombre | VARCHAR(255) | No disponible | Nombre de la vigilancia si el tipo es "ManagedEntityStatus". Sin embargo, predeterminado para la misma cadena que en Tipo, excepto en todas las mayúsculas; por ejemplo, "MÉTRICA" o "SUSCRIPCIÓN". |

## MOT_TREND_DATA

Esta tabla registra los datos de tendencias de métricas, vigilancias y medidas. Por ejemplo, la hora y el valor de la métrica.

| Nombre de columna | Tipo | Clave | Descripción |
|---|---|---|---|
| DataId | INTEGER | Clave primaria<br>Generado automáticamente | |
| DetailsId | INTEGER | Clave externa (desde DETALLES_TEND_MOT) | |
| Hora o TimeT | ENTERO GRANDE o NÚMERO o FIJO<br>Fecha Unix Epoch | No disponible | Hora a la que se recopilan los datos |
| Valor | FLOTAR o DOBLE o NÚMERO | No disponible | Valor de la medida/suscripción |
| Clave de mensaje | VARCHAR(32) | No disponible | Clave de mensaje de error o nulo si correcto. Para la vigilancia, también puede ser "watchEnabled" o "watchDisabled". Se trata de una "clave" porque se usa para recuperar mensajes localizados antes de mostrar la IU. |
| Ts | FECHA Y HORA o FECHA Y HORA | No disponible | Hora en la que se escribe la fecha en la base de datos |

## MOT_MES_DETAILS

Esta tabla registra información sobre las infracciones de suscripción y la información de entrega de alertas. Por ejemplo, la hora de la infracción y la hora de la entrega de alertas.

| Nombre de columna | Tipo | Clave | Descripción |
|---|---|---|---|
| StatusDetailsId | INTEGER | Clave primaria<br>Generado automáticamente | |
| DetailsId | INTEGER | Clave externa (desde DETALLES_TEND_MOT) | |
| Hora | ENTERO GRANDE o NÚMERO<br>Fecha Unix Epoch | No disponible | Hora a la que se recopilan los datos |
| AlertType | ENTERO PEQUEÑO o NÚMERO | No disponible | Tipo de entrega de la notificación de suscripción (por ejemplo, correo electrónico) |

## MOT_MES_METRICS

Esta tabla registra información sobre vigilancias y las métricas que pertenecen a las ecuaciones de vigilancia. Todas las métricas que pertenezcan a la vigilancia tendrán una entrada en esta tabla.

| Nombre de columna | Tipo | Clave | Descripción |
|---|---|---|---|
| DataId | INTEGER | Clave primaria<br>Generado automáticamente | |
| DetailsId | INTEGER | Clave externa (desde DETALLES_TEND_MOT) | |
| CUID | VARCHAR(64) | No disponible | CUID de la vigilancia |
| Nombre | VARCHAR(255) | No disponible | Nombre de la vigilancia |

# 40 Apéndice de la hoja de cálculo de copia del sistema

## 40.1 Hoja de cálculo de copia del sistema

| Propiedad | Valor |
|---|---|
| Clave de clúster. | |
| Nombres de los nodos. | |
| El nombre del equipo y la carpeta de instalación de la plataforma de BI para cada equipo en el despliegue. | |
| La contraseña de administrador de la plataforma de BI. | |
| Las conexiones de base de datos CMS, los nombres de usuario y las contraseñas asociados con las conexiones para cada equipo del despliegue. | |
| Las conexiones de base de datos de auditoría, los nombres de usuario y las contraseñas asociados con las conexiones para cada equipo del despliegue. | |
| Para cada equipo del despliegue, los detalles de cualquier otra conexión cliente de base de datos para cada equipo del sistema de origen que los universos y los informes usan. | |
| Para cada equipo del despliegue, los tipos de cliente de base de datos y las versiones. | |
| La versión, el paquete de compatibilidad y el nivel de la revisión. | |
| Las ubicaciones de almacén de archivos para cada FRS de entrada y FRS de salida del despliegue. | |
| Si piensa copiar Gestión de promociones, la ubicación de la carpeta de la base de datos de Gestión de promociones y las carpetas de subversión. | |
| Si tiene pensado copiar la base de datos de supervisión, la carpeta de la base de datos de supervisión. | |
| La ruta de la carpeta de capa semántica. | |

# Limitaciones de responsabilidad y aspectos legales

## Hiperenlaces

Algunos enlaces se clasifican con un icono y/o con un texto al pasar el puntero del ratón. Estos enlaces proporcionan información adicional.
Acerca de los iconos:

- Enlaces con el icono Está entrando en una página Web que no está alojada por SAP. Al usar este tipo de enlaces, manifiesta su acuerdo (a no ser que se indique expresamente lo contrario en sus contratos con SAP) con lo siguiente:
  - El contenido del sitio al que se accede a través del enlace no es documentación SAP. No puede realizar ninguna reclamación de producto contra SAP en base a esta información.
  - SAP no manifiesta su acuerdo o desacuerdo con el contenido del sitio al que se accede a través del enlace, ni garantiza su disponibilidad o exactitud. SAP no es responsable de ningún daño causado por el uso de este contenido a menos que los daños se hayan causado por una imprudencia grave o por una conducta fraudulenta dolosa por parte de SAP.
- Enlaces con el icono Está dejando la documentación para este producto o servicio de SAP en concreto y está entrando en un sitio Web alojado por SAP. Al usar este tipo de enlaces, manifiesta su acuerdo (a no ser que se indique expresamente lo contrario en sus contratos con SAP) a no realizar ninguna reclamación de producto contra SAP en base a esta información.

## Vídeos alojados en plataformas externas

Algunos vídeos pueden dirigir a plataformas de hospedaje de vídeos de terceros. SAP no puede garantizar la disponibilidad futura de vídeos almacenados en estas plataformas. Además, cualquier anuncio u otro contenido alojado en estas plataformas (p. ej., vídeos sugeridos o la navegación a otros vídeos alojados en el mismo sitio), no se encuentra bajo el control o la responsabilidad de SAP.

## Beta y otras funciones experimentales

Las funciones experimentales no forman parte del alcance de la entrega oficial que SAP garantiza para futuras versiones. Esto significa que SAP puede modificar las funciones experimentales en cualquier momento, por cualquier motivo y sin previo aviso. Las funciones experimentales no están previstas para su uso productivo. No podrá mostrar, probar, examinar, evaluar las funciones experimentales o realizar cualquier otro uso de ellas en un entorno operativo en directo o con datos que no estén suficientemente fundamentados.
El propósito de las funciones experimentales es obtener de manera anticipada comentarios que permitan a los clientes y partners influir en el producto futuro en consecuencia. Al proporcionar su opinión (p. ej. en la Comunidad SAP), acepta que los derechos de propiedad intelectual de las contribuciones o de las tareas derivadas seguirán siendo propiedad exclusiva de SAP.

## Código de ejemplo

Cualquier codificación de software y/o fragmentos de código son ejemplos. No están previstos para su uso productivo. El código de ejemplo tiene el único propósito de explicar y permitir la visualización de las reglas de sintaxis y de redacción SAP no garantiza la exactitud ni la integridad de los códigos de ejemplo. SAP no es responsable de ningún error o daño causado por el uso de código de ejemplo a menos que los daños se hayan causado por una imprudencia grave o por una conducta fraudulenta dolosa por parte de SAP.

## Lenguaje sin sesgos

SAP apoya una cultura de diversidad e inclusión. Siempre que sea posible, utilizamos un lenguaje imparcial en nuestra documentación para referirnos a personas de todas las culturas, etnias, géneros y habilidades.

www.sap.com/contactsap

© 2024 SAP SE o una empresa filial de SAP. Reservados todos los derechos.

Queda prohibida la reproducción o transmisión de cualquier parte de esta publicación, en cualquier forma o para cualquier fin, sin el permiso expreso de SAP SE o de una empresa filial de SAP. La información que aquí se incluye puede modificarse sin previo aviso.

Algunos productos de software comercializados por SAP SE y sus distribuidores contienen componentes de software con derechos de autor de otros proveedores de software. Las especificaciones de productos en cada país pueden ser diferentes.

SAP SE o una empresa filial de SAP SE proporcionan estos materiales con fines meramente informativos, sin manifestación ni garantía de ningún tipo. Ni SAP SE ni sus empresas filiales se hacen responsables de los errores u omisiones en relación con los materiales. Las únicas garantías para los productos y servicios de SAP SE o de sus empresas filiales son aquellas especificadas en las cláusulas expresas de garantía que acompañan a dichos productos y servicios, si las hubiera. Nada de lo que se incluye en este documento debe interpretarse como garantía adicional.

SAP y los productos y servicios de SAP mencionados, así como sus respectivos logotipos, son marcas comerciales o marcas registradas de SAP SE (o de una empresa filial de SAP) en Alemania y en otros países. Todos los nombres y servicios de productos son las marcas comerciales de sus respectivas empresas.

Consulte https://www.sap.com/spain/about/legal/trademark.html para obtener información y avisos adicionales sobre marcas comerciales.

THE BEST RUN SAP