HP Universal CMDB 9.10 Configuration Manager

para el sistema operativo Windows

Guía de implantación

Fecha de publicación del documento: noviembre de 2010
Fecha de lanzamiento del software: noviembre de 2010

Avisos legales

Garantía

Las únicas garantías de los productos y servicios HP se exponen en el certificado de garantía que acompaña a dichos productos y servicios. El presente documento no debe interpretarse como una garantía adicional. HP no se responsabiliza de los errores u omisiones, ya sean técnicos o de redacción, que pueda contener el presente documento.

La información contenida en esta página está sujeta a cambios sin previo aviso.

Aviso de derechos limitados

Software informático confidencial. Es necesario disponer de una licencia válida de HP para su posesión, uso o copia. De conformidad con FAR 12.211 y 12.212, el gobierno estadounidense dispone de licencia de software informático de uso comercial, documentación del software informático e información técnica para elementos de uso comercial con arreglo a la licencia estándar para uso comercial del proveedor.

Avisos de propiedad intelectual

Actualizaciones de la documentación

La página de título de este documento contiene la siguiente información de identificación:

- Fecha de publicación del documento, que cambia cada vez que se actualiza el documento.
- Fecha de lanzamiento del software, que indica la fecha desde la que está disponible esta versión del software.

Para consultar las últimas actualizaciones o comprobar que está utilizando la edición más reciente de un documento, visite:

http://h20230.www2.hp.com/selfsolve/manuals

Este sitio requiere que se registre para obtener un HP Passport e inicie sesión.
Para obtener un ID de HP Passport, vaya a:

http://h20229.www2.hp.com/passport-registration.html

O bien, pulse el enlace **New users - please register** (Nuevos usuarios - registro) en la página de inicio de sesión de HP Passport.

Asimismo, recibirá ediciones actualizadas o nuevas si se suscribe al servicio de soporte del producto correspondiente. Para obtener más información, póngase en contacto con su representante de ventas de HP.

Soporte técnico

Visite el sitio web de HP Software Support en:

http://www.hp.com/go/hpsoftwaresupport

Este sitio web proporciona información de contacto y detalles sobre los productos, servicios y soporte técnico que ofrece HP Software.

El soporte en línea de HP Software proporciona capacidades de resolución de problemas por parte de los propios clientes. Ofrece una forma rápida y eficaz de acceder a las herramientas de soporte técnico interactivo necesarias para gestionar su negocio. Puede beneficiarse de ser un cliente preferente de soporte utilizando el sitio de soporte para:

- Buscar documentos de interés en la base de conocimientos
- Enviar y realizar el seguimiento de los casos de soporte y las solicitudes de mejora
- Descargar parches de software
- Gestionar contratos de soporte técnico
- Buscar contactos de soporte de HP
- Consultar la información sobre los servicios disponibles
- Participar en debates con otros clientes de software
- Investigar sobre formación de software y registrarse para recibirla

Para acceder a la mayor parte de las áreas de soporte es necesario que se registre como usuario de HP Passport. En muchos casos también será necesario disponer de un contrato de soporte. Para registrarse y obtener un ID de HP Passport, visite:

http://h20229.www2.hp.com/passport-registration.html

Para obtener más información sobre los niveles de acceso, visite:

http://h20230.www2.hp.com/new_access_levels.jsp

Tabla de contenido

1

Instalación y configuración

Este capítulo incluye:

Descripción general de Configuration Manager

HP Universal CMDB Configuration Manager (Configuration Manager) permite analizar y controlar los datos del CMS, además de proporcionar un entorno para controlar la infraestructura del CMS, que engloba muchos orígenes de datos y sirve varios productos y aplicaciones.

La implantación de Configuration Manager en un entorno de red empresarial es un proceso que requiere la planificación de los recursos y el diseño de la arquitectura del sistema. Antes de instalar Configuration Manager, revise la información de esta sección, incluidos los requisitos del sistema.

Requisitos del sistema de Configuration Manager

Requisitos de sistema del servidor

La siguiente tabla describe los requisitos del sistema para el servidor de Configuration Manager:

CPU	Intel Pentium 4 con un mínimo de 4 núcleos
Memoria (RAM)	Mínimo 4 GB
Plataforma	x64
Sistema operativo	Se admiten los siguientes sistemas operativos Windows de 64 bits: ➤ Windows 2003 Enterprise SP2 y R2 SP2 ➤ Windows 2008 Enterprise SP2 y R2

Base de datos	➤ Microsoft SQL Server 2005 SP2; 2005 con modo de compatibilidad 80; (ediciones Enterprise para todos) ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB versión 9.03 (instalación típica de CMDB) Para obtener una lista completa de los requisitos del sistema para esta versión, consulte la documentación de HP Universal CMDB.

Requisitos del cliente

La siguiente tabla describe los requisitos del cliente para ver Configuration Manager:

Explorador	➤ Microsoft Internet Explorer 7.0, 8.0. ➤ Mozilla Firefox 3.x
Complemento de explorador Flash Player	Flash Player 9 o superior
Resolución de la pantalla	➤ 1024x768 (mínima) ➤ 1280x1024 (recomendada)
Calidad de color	Mínimo 16 bits

Instrucciones de configuración recomendada

La siguiente tabla muestra las instrucciones de las opciones de configuración de Configuration Manager.

LDAP	Se admiten los siguientes entornos LDAP: ➤ Active Directory ➤ SunONE 6.x
Tamaño mínimo recomendado del esquema de base de datos	2 GB

Configuration Manager Límites de capacidad de

La siguiente tabla muestra los límites de capacidad de Configuration Manager.

Número máximo de vistas recomendado	100
Número máximo de políticas recomendado	300
Número máximo de CI compuestos por vista recomendado	5000
Número máximo de usuarios simultáneos recomendado	50

Configurar la base de datos o el esquema de usuario

Para trabajar con Configuration Manager, es preciso incluir un esquema de base de datos. Configuration Manager admite Microsoft SQL Server y Oracle Database Server. En esta tarea se describe cómo configurar las propiedades de conexión de la base de datos o del esquema de usuario de Configuration Manager a través del Asistente de instalación.

Nota: para conocer los requisitos de sistema de Microsoft SQL Server y Oracle Server, consulte "Requisitos de sistema del servidor" en la página 8.

Para configurar una base de datos:

1 Asigne una base de datos de Microsoft SQL Server o un esquema de usuario de Oracle Server.

➤ En **Microsoft SQL Server 2005**: active el aislamiento de instantáneas.

Ejecute el siguiente comando una vez cuando haya creado la base de datos:

```
alter database <ccm_database_name> set read_committed_snapshot on
```

Para obtener más información sobre la función de aislamiento de instantáneas de SQL Server, consulte http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

➤ En **Oracle**: conceda al usuario de Oracle sólo los roles **Connect** y **Resource**.
(Si se concede el privilegio **Select any table**, se produce un error en el procedimiento de rellenado del esquema.)

2 Verifique la siguiente información, ya que la necesitará durante el proceso de configuración:

✔	**Información necesaria**
	Puerto y nombre de host de la base de datos
	Nombre de usuario y contraseña de la base de datos
	Para MS SQL: nombre de la base de datos
	Para Oracle: SID

3 Ejecute el Asistente de instalación de Configuration Manager.
Para obtener más información, consulte "Instalar Configuration Manager" en la página 12.

Instalar Configuration Manager

En esta tarea se describe cómo instalar Configuration Manager en un servidor y cómo configurar la conexión de la base de datos y la integración de UCMDB. Si necesita ayuda durante la instalación, puede hacer clic en **Ayuda** en cualquiera de las páginas del asistente. Para obtener descripciones detalladas de las páginas del asistente, consulte "Asistente de configuración post- instalación de Configuration Manager" en la página 23.

Para instalar Configuration Manager:

1 En el directorio raíz del DVD de Configuration Manager, busque el archivo **install.bat**.

2 Haga doble clic en dicho archivo para ejecutar el Asistente de instalación de Configuration Manager.

3 Haga clic en **Siguiente** para abrir la página del contrato de licencia para el usuario final.

4 Acepte los términos de la licencia y haga clic en **Siguiente** para abrir la página de instalación de productos.

5. Seleccione los productos que desea instalar (UCMDB y Configuration Manager) y especifique la ubicación de la instalación. Si tiene una licencia personalizada de UCMDB, active la casilla. Haga clic en **Siguiente** para iniciar la instalación de UCMDB. Para obtener más información sobre la instalación de UCMDB, consulte la guía the *HP Universal CMDB Deployment Guide* PDF.
6. Cuando tanto la instalación como la post-instalación de UCMDB finalizan, se inicia automáticamente el Asistente de configuración post-instalación de Configuration Manager.
7. Haga clic en **Siguiente** en la página de bienvenida para abrir la página Configuración de conexión de base de datos.
8. Seleccione el tipo de base de datos (Oracle o Microsoft SQL Server) y escriba el nombre de usuario y la contraseña. Es aconsejable probar la conexión haciendo clic en el botón **Prueba**. Si el resultado de la prueba de conexión indica que es correcta, pulse **Siguiente** para abrir la página Configuración de servidor de aplicaciones.

Nota: tras finalizar el asistente es posible configurar opciones de conexión de la base de datos más avanzadas. Para obtener más información, consulte "Configurar las opciones avanzadas de conexión de la base de datos" en la página 15.

---

9. Escriba el nombre de host y pulse **Siguiente** para abrir la página Configuración de servicios de Windows.
10. Si desea instalar Configuration Manager como un servicio de Windows, active la casilla. Haga clic en **Siguiente** para abrir la página Credenciales de usuario.
11. Escriba el nombre de usuario y la contraseña tanto en Usuario administrativo como en Usuario de integración. Haga clic en **Siguiente** para abrir la página Configuración de conexión de HP UCMDB.

12 Si UCMDB ya está instalado en el propio equipo, o en otro, antes de continuar asegúrese de que el servidor de UCMDB está activo.

Si va a instalar UCMDB en otro equipo, asegúrese de que la casilla está activada y especifique los parámetros requeridos. Es aconsejable probar la conexión haciendo clic en el botón **Prueba**. Si el resultado de la prueba de conexión indica que es correcta, haga clic en **Siguiente** para abrir la página Resumen de acciones post-instalación.

13 Revise la información de dicha página. Si es correcta, haga clic en **Siguiente** para continuar con la post-instalación.

14 Para completar la post-instalación, haga clic en el botón **Finalizar** de la página Finalizar.

15 Si éste no es el primer inicio de UCMDB, tendrá que cambiar el tamaño de las columnas en UCMDB tal como se indica a continuación:

a Vaya a **Administración** > **Gestor de configuración de infraestructura**. Busque el valor **Raíz de objeto** y cámbielo a **datos**. Para que el cambio surta efecto, cierre la sesión de UCMDB y vuelva a iniciarla.

b Vaya a **Modelado** > **Gestor de tipo de CI**. Seleccione los **datos** del tipo de CI en el árbol y haga clic en la ficha Atributos. Edite el atributo **Etiqueta de usuario**, cambie el valor de **Tamaño de valor** a 900.

c Vuelva al **Gestor de configuración de infraestructura** y devuelva **Raíz de objeto** a su valor original. Para que el cambio surta efecto, cierre la sesión y vuelva a iniciarla.

16 Si Gestión de flujo de datos ya se ejecutaba en UCMDB, es posible que los datos del historial estén dañados. Para solucionar este problema, ejecute el siguiente procedimiento:

a Inicie un explorador web y escriba la siguiente dirección: http://<dirección de servidor de UCMDB>.<nombre_dominio>:8080/jmx-console.

Introduzca las credenciales de autenticación de la consola JMX, que de forma predeterminada son:

- Nombre de inicio de sesión = **sysadmin**
- Contraseña = **sysadmin**

b En **UCMDB**, seleccione **Servicios de base de datos de historial**.

c Seleccione el método **Fix902EndTimeRecords**.

d En el cliente de estado real, escriba **1** en Id. de cliente y haga clic en **Invocar**.

e Si la operación se ha realizado correctamente, aparece el mensaje "La base de datos del historial se ha actualizado correctamente".

f En el cliente de estado autorizado, escriba **100001** en Id. de cliente y haga clic en **Invocar**.

g Si la operación se ha realizado correctamente, aparece el mensaje "La base de datos del historial se ha actualizado correctamente".

Configurar las opciones avanzadas de conexión de la base de datos

Si necesita propiedades de conexión de la base de datos más avanzadas que admitan la implantación de su base de datos, puede configurarlas cuando haya finalizado la ejecución del Asistente de post-instalación. Configuration Manager admite todas las opciones de conexión de base de datos que admita el controlador JDBC del fabricante y se pueden configurar con la dirección URL de conexión de la base de datos. Para configurar conexiones más avanzadas, edite la propiedad **jdbc.url** en el archivo **<Directorio de instalación de Configuration Manager>\conf\database.properties**.

A continuación encontrará algunos ejemplos de opciones avanzadas de Microsoft SQL Server:

- **Autenticación Windows (NTLM):** para aplicar una autenticación Windows, añada la propiedad de dominio a la URL de su conexión JTDS en el archivo database.properties. Especifique el dominio Windows que desea autenticar.

  Por ejemplo:

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode=false;domain=myDomain
  ```

- **SSL.** Para obtener más información sobre cómo proteger la conexión de MS SQL Server con SSL, consulte http://jtds.sourceforge.net/faq.html.

A continuación encontrará algunos ejemplos de opciones avanzadas de Oracle Database Server:

- **URL de Oracle.** Especifique la dirección URL del controlador nativo de Oracle. Incluya un SID y nombre de servidor Oracle válidos. Asimismo, si está utilizando **Oracle RAC**, especifique los detalles de configuración de Oracle RAC.

Nota: para obtener más información sobre cómo configurar el formato de la dirección URL del JDBC Oracle nativo, consulte http://www.orafaq.com/wiki/JDBC#Thin_driver. Para obtener más información sobre cómo configurar la dirección URL de Oracle RAC, consulte http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

- **SSL.** Para obtener más información sobre cómo proteger la conexión de Oracle con SSL, consulte las siguientes explicaciones:
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

Configuración de base de datos: compatibilidad con MLU (Unidad multilingüe)

Esta sección describe la configuración de la base de datos necesaria para admitir la localización.

Configuración de Oracle Server

La siguiente tabla muestra los valores necesarios para Oracle Server:

Opción	Compatible	Se recomienda	Comentarios
Juego de caracteres	WE8ISO8859P1; UTF8,AL32UTF8	AL32UTF8	

Configuración de Microsoft SQL Server

La siguiente tabla muestra los valores necesarios para Microsoft SQL Server:

Opción	Compatible	Se recomienda	Comentarios
Intercalación	No diferencia mayúsculas de minúsculas. No admite criterio de ordenación binario ni diferencia mayúsculas de minúsculas. Sólo se admite un criterio de ordenación que no diferencia mayúsculas de minúsculas con una combinación de los valores de acento, kana o anchura.	Para seleccionar la intercalación, use el cuadro de diálogo Configuración de intercalación. No active la casilla Binario. Se debe seleccionar la sensibilidad del acento, la kana y la anchura de acuerdo con los requisitos relevantes del idioma de los datos. El idioma seleccionado debe ser el mismo que el de la configuración regional de Windows.	Se limita a la configuración regional de la intercalación y a las definiciones predeterminadas en inglés.
Propiedad de base de datos de intercalación	Valor predeterminado de servidor		

Nota:

Para todos los idiomas: **<Idioma>_CI_AS** es la opción mínima requerida. Por ejemplo, en japonés, si desea seleccionar las opciones Distinguir kana y Distinguir ancho, la opción recomendada es: **Japanese_CI_AS_KS_WS** o **Japanese_90_CI_AS_KS_WS**. Esta recomendación indica que los caracteres japoneses distinguen acentos, kana y anchura.

- **Distinguir acentos (_AS).** Distingue entre caracteres acentuados y sin acentuar. Por ejemplo, **a** no es igual que **á**. Si no se selecciona esta opción, a efectos de ordenación Microsoft SQL Server considera que las versiones acentuada y sin acentuar de las letras son idénticas.
- **Distinguir kana (_KS).** Distingue entre los dos tipos de caracteres kana japoneses: Hiragana y Katakana. Si no se selecciona esta opción, a efectos de ordenación Microsoft SQL Server considera que los caracteres Hiragana y Katakana son iguales.
- **Distinguir ancho (_WS).** Distingue entre un carácter de un solo byte y el mismo carácter cuando se representa como carácter de doble byte. Si no se selecciona esta opción, a efectos de ordenación Microsoft SQL Server considera que las representaciones de un solo byte y de doble byte son idénticas.

Habilitar Lightweight Single Sign-On

Algunos usuarios de Configuration Manager también tienen permiso para iniciar sesión en UCMDB. Por comodidad, Configuration Manager proporciona un enlace directo a la interfaz de usuario de UCMDB (seleccione **Administración** > **Abrir UCMDB**). Para usar un inicio de sesión único (que elimina la necesidad de iniciar sesión en UCMDB después de iniciar sesión en Configuration Manager), es preciso habilitar LW-SSO tanto en Configuration Manager como en UCMDB y asegurarse de que ambos funcionan con el mismo initString. En esta tarea se describe cómo habilitar LW-SSO en Configuration Manager y en UCMDB.

Para habilitar LW-SSO:

1 Abra el siguiente archivo del directorio de instalación de Configuration Manager: **\servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml**.

Nota: este archivo no existe antes de iniciar Configuration Manager.

---

2 Busque la siguiente sección:

```
enableLWSSO enableLWSSOFramework="true"
```

y compruebe que el valor es **true**.

3 Busque la siguiente sección:

```
lwssoValidation  id="ID000001">
<dominio> </dominio>
```

y especifique el dominio del servidor de Configuration Manager después de <**dominio**>.

4 Busque la siguiente sección:

```
<initString="Esta cadena se debe reemplazar"></crypto>
```

y reemplace "Esta cadena se debe reemplazar" por una cadena compartida que usen todas las aplicaciones de confianza que se integran con LW-SSO.

5 Busque la siguiente sección:

```
<!--multiDomain>
<trustedHosts>
<DNSDomain>Este valor se debe reemplazar por el dominio de la
aplicación</DNSDomain>
<DNSDomain>Este valor se debe reemplazar por un dominio de otra
aplicación</DNSDomain>
</trustedHosts>
</multiDomain-->
```

Quite el carácter de comentario del principio y especifique los dominios del servidor de Configuration Manager en los elementos de DNSDomain (en lugar de Este valor se debe reemplazar por el dominio de la aplicación). La lista debe incluir el dominio del servidor especificado en el paso 3 en la página 20.

6 Guarde el archivo con los cambios y reinicie el servidor.

7 Inicie un explorador web y escriba la siguiente dirección: http://<dirección de servidor de UCMDB>.<nombre_dominio>:8080/jmx-console.

Introduzca las credenciales de autenticación de la consola JMX, que de forma predeterminada son:

- Nombre de inicio de sesión = **sysadmin**
- Contraseña = **sysadmin**

8 En **UCMDB-UI**, seleccione **Configuración de LW-SSO** para abrir la página Vista de MBEAN de JMX.

9 Seleccione el método **setEnabledForUI**, elija el valor **true** y haga clic en **Invocar**.

10 Seleccione el método **setDomain**. Especifique el nombre del dominio del servidor de UCMDB y haga clic en **Invocar**.

11 Seleccione el método **setInitString**. Especifique el mismo initString que indicó para Configuration Manager en el paso 4 en la página 21 y haga clic en **Invocar**.

12 Si Configuration Manager y UCMDB se encuentran en dominios separados, seleccione el método **addTrustedDomains** y especifique los nombres de dominio de los servidores de UCMDB y Configuration Manager. Haga clic en **Invocar**.

13 Para ver la configuración de LW-SSO cuando se guarda en el mecanismo de configuración, seleccione el método **retrieveConfigurationFromSettings** y haga clic en **Invocar**.

14 Para ver la configuración real de LW-SSO cargada, seleccione el método **retrieveConfiguration** y haga clic en **Invocar**.

Compatibilidad con IPv6

Configuration Manager admite direcciones URL IPv6 sólo para las direcciones URL que utilizan los clientes.

Para trabajar con Configuration Manager utilizando una dirección IPv6:

1 Asegúrese de que el sistema operativo admite IPv6. Para obtener más información, consulte la documentación del sistema operativo relevante.

2 Abra el archivo **client-config.properties**, que se encuentra en el directorio **conf** del <**Directorio de instalación de Configuration Manager**>. Cambie el valor del parámetro **bsf.server.url** a la dirección IPv6, escrita entre corchetes. Por ejemplo:

```
bsf.server.url=http://[2620:0:a17:e008:d840:5b0f:2040:519c]:8080/bsf
```

2

Asistente de configuración post-instalación de Configuration Manager

Este capítulo incluye:

Descripción general de la configuración post-instalación de Configuration Manager

En este capítulo se proporcionan descripciones detalladas de las páginas del Asistente post-instalación de Configuration Manager y las tareas de configuración asociadas. Éste es el contenido que se abre al pulsar en **Ayuda** desde cualquiera de las páginas del asistente.

Página Conexión de base de datos

Esta sección incluye:

General

Las conexiones de las bases de datos se deben configurar asociadas con conexiones de URL estándar. Si se requieren características más avanzadas, como Oracle Real Application Cluster, configure una conexión estándar y, a continuación, edite manualmente el archivo **database.properties** para configurar las características avanzadas.

Configuration Manager usa controladores nativos tanto para Oracle como para Microsoft SQLServer, lo que significa que, en general, se admiten las características de todos los controladores nativos, siempre que dichas características se puedan configurar utilizando la dirección URL de la base de datos. La dirección URL se encuentra en el archivo **database.properties**.

Nota: la configuración de características avanzadas se debe realizar una vez que haya terminado el proceso posterior a la instalación y se haya establecido una configuración de trabajo.

Parámetros

Para configurar la conexión de la base de datos, defina los siguientes parámetros:

Parámetro	Valor recomendado	Descripción
Proveedor	<definido por el usuario>	Proveedor de base de datos Valores posibles: **Oracle** o **Microsoft** HP Universal CMDB se puede instalar con el mismo instalador que Configuration Manager o por separado. Si Configuration Manager y UCMDB se van a instalar en el mismo equipo con el mismo instalador, el valor predeterminado de este parámetro es el proveedor de base de datos seleccionado en el Asistente post-instalación de UCMDB. Los valores predeterminados sólo se definen cuando se instalan las dos aplicaciones con los mismos instaladores Si la instalación se va realizar con paquetes separados, aunque UCMDB se instale en el mismo equipo que Configuration Manager, los valores predeterminados NO aparecerán en el Asistente post-instalación.
Nombre de host	<definido por el usuario>	Nombre de host del servidor de bases de datos Si Configuration Manager y UCMDB se van a instalar en el mismo equipo, el valor predeterminado de este parámetro es el servidor de bases de datos seleccionado en el Asistente post-instalación de UCMDB. **Este valor es obligatorio.**

Parámetro	Valor recomendado	Descripción
Puerto	<definido por el usuario>	Puerto del agente de escucha de la base de datos Si Configuration Manager y UCMDB se van a instalar en el mismo equipo, el valor predeterminado de este parámetro es el puerto de la base de dato seleccionado en el Asistente post-instalación de UCMDB. En el caso de Oracle, el valor predeterminado es **1521**. En el caso de Microsoft SQL Server, el valor predeterminado es **1433**. **Este valor es obligatorio.**
SID/DB	<definido por el usuario>	Nombre del SID de Oracle o nombre de la base de datos de Microsoft SQL Server Si Configuration Manager y UCMDB se van a instalar en el mismo equipo, el valor predeterminado de este parámetro es el sid/db de base de datos seleccionado en el Asistente post-instalación de UCMDB. **Este valor es obligatorio.**
Nombre de usuario	<definido por el usuario>	Nombre de usuario utilizado para conectarse a la base de datos. **Este valor es obligatorio.**
Contraseña	<definido por el usuario>	Contraseña utilizada para conectarse a la base de datos.

Opciones

También están disponibles las siguientes opciones:

Parámetro	Valor recomendado	Descripción
Cifrar contraseña	<definido por el usuario>	Si se selecciona, esta opción cifra la contraseña en el archivo **database.properties**. Por seguridad, se recomienda cifrar las contraseñas almacenadas en archivos de texto.
Crear objetos de esquema	<definido por el usuario>	Si se selecciona, esta opción crea los objetos de esquema necesarios para ejecutar Configuration Manager. Esta opción sólo se debe anular cuando la instalación utilice un esquema existente que previamente se haya creado y llenado con objetos de Configuration Manager.

Probar

Nota: se recomienda encarecidamente probar las propiedades de la conexión antes de continuar.

Para probar las propiedades de la conexión, pulse **Probar**. El asistente intenta acceder a la base de datos y comprobar la conexión. El resultado de la prueba aparece a la derecha del botón **Probar**.

La base de datos genera varios mensajes de error. Dichos mensajes son explicativos (normalmente indican que se ha especificado un nombre de usuario o una contraseña incorrectos). Para poder continuar, el error se debe solucionar y se debe obtener un resultado satisfactorio en la prueba.

Página Servidor de aplicaciones

Esta sección incluye:

General

Configure el servidor de aplicaciones de Configuration Manager con los números de puerto predeterminados que se muestran a continuación.

Parámetros

Para configurar el servidor de aplicaciones de Configuration Manager, defina los siguientes parámetros:

Parámetro	Valor recomendado	Descripción
Nombre de host	<definido por el usuario>	Nombre externo del servidor de aplicaciones De manera predeterminada, este valor es el nombre de host completo del equipo que ejecuta el asistente (y Configuration Manager). En algunas implantaciones, este nombre debe ser distinto, como cuando se implanta un servidor web delante del servidor de aplicaciones de Configuration Manager.
Personalizar puertos	<definido por el usuario>	De manera predeterminada, esta opción no está seleccionada. Cuando se selecciona, es posible personalizar los números de puerto predeterminados del servidor de aplicaciones.

Parámetro	Valor recomendado	Descripción
Puerto HTTP	<definido por el usuario>	Puerto HTTP del servidor de aplicaciones de Configuration Manager Valor predeterminado: **8080** El valor predeterminado cuando se instala en el mismo equipo que HP Universal CMDB es **8180**
Puerto HTTPS	<definido por el usuario>	Puerto HTTPS del servidor de aplicaciones de Configuration Manager Valor predeterminado: **8443** El valor predeterminados cuando se instala en el mismo equipo que UCMDB es **8143**
Puerto de Tomcat	<definido por el usuario>	Puerto de gestión del servidor de aplicaciones de Configuration Manager Valor predeterminado: **8005**
Puerto AJP	<definido por el usuario>	Puerto AJP (Apache Java Protocol) del servidor de aplicaciones de Configuration Manager Valor predeterminado: **8009**
Puerto JMX HTTP	<definido por el usuario>	Puerto JMX HTTP del servidor de aplicaciones de Configuration Manager Valor predeterminado: **39900**
Puerto JMX remoto	<definido por el usuario>	Puerto JMX remoto del servidor de aplicaciones de Configuration Manager Valor predeterminado: **39600**

Página Configuración de servicios de Windows

Seleccione si desea instalar Configuration Manager como un servicio de Windows. Esta opción sólo está disponible cuando la instalación se realiza en un equipo con Windows.

El servicio de Windows se puede instalar manualmente con la utilidad **create-windows-service.bat**, que se encuentra en el directorio **cnc-home/bin**.

Página Credenciales de usuario

Esta sección incluye:

➤ "General" en la página 30

General

Configure los siguientes usuarios iniciales de Configuration Manager:

Parámetro	Valor recomendado	Descripción
Usuario Admin	<definido por el usuario>	Usuario administrativo de Configuration Manager (el "superusuario")
Usuario de integración	<definido por el usuario>	Usuario creado por Configuration Manager en HP Universal CMDB con fines de integración

---

Nota: debe proporcionar las credenciales de nombre de usuario y contraseña tanto a los usuarios administrativos como a los de integración.

Página Conexión de HP Universal CMDB

Esta sección incluye:

General

La selección de la conexión HP Universal CMDB es opcional.

Si Configuration Manager se instala en el mismo equipo que UCMDB en una instalación combinada, no es necesario introducir nada en esta página.

Si UCMDB no se instala en una instalación combinada, o si se instala en otro equipo (incluso cuando se realiza una conexión con UCMDB en el localhost), o bien si UCMDB se instala antes que Configuration Manager, UCMDB debe estar funcionando y el usuario debe introducir estas propiedades de conexión.

Nota: si la instalación se realiza usando una instancia remota de UCMDB, dicha instancia debe estar activa y funcionando. Si Configuration Manager y UCMDB se instalan en el mismo equipo, UCMDB debe estar inactivo mientras se ejecuta este asistente.

Parámetros

Para configurar la conexión de UCMDB, defina los siguientes parámetros:

Parámetro	Valor recomendado	Descripción
Usar HP UCMDB en otro host	<definido por el usuario>	Con esta opción se habilitan las restantes propiedades al instalar Configuration Manager y UCMDB en equipos distintos.
Nombre de host	<definido por el usuario>	Nombre del host en el que está instalado UCMDB
Puerto	<definido por el usuario>	Puerto que UCMDB escucha
Protocolo	<definido por el usuario>	HTTP o HTTPS
Cliente	<definido por el usuario>	Cliente de UCMDB
Nombre de usuario administrativo	<definido por el usuario>	Nombre de usuario de sysadmin en UCMDB
Contraseña administrativa	<definido por el usuario>	Contraseña de sysadmin en UCMDB

Probar

Nota: se recomienda encarecidamente probar las propiedades de la conexión antes de continuar.

Para probar las propiedades de la conexión, pulse **Probar**. El asistente intenta acceder a UCMDB y comprobar la conexión. El resultado de la prueba aparece a la derecha del botón **Probar**.

UCMDB genera distintos mensajes de error. Dichos mensajes son explicativos (normalmente indican que se ha especificado un nombre de usuario o una contraseña incorrectos). Para poder continuar, el error se debe solucionar y se debe obtener un resultado satisfactorio en la prueba.

Página Resumen

Se muestran todas las selecciones realizadas en la páginas anteriores del asistente. Confirme la exactitud de todas las selecciones y realice los cambios necesarios. Cuando todas las selecciones sean correctas, haga clic en **Siguiente** para que el asistente finalice las tareas de configuración.

Página Finalizar

Es la última página del Asistente de configuración post-in**stalación de Configuration Manager.** Las tareas de configuración posteriores a la instalación han finalizado. Pulse **Finalizar** para cerrar el asistente.

Nota: aunque todas las tareas hayan finalizado correctamente, se recomienda comprobar los registros ubicados en **cnc-home/tmp/chp/app.log**.

3

Configuración de LDAP

HP UCMDB Configuration Manager usa LDAP para gestionar usuarios, funciones y permisos. En este capítulo se describen los pasos necesarios para configurar LDAP y para solucionar los problemas que surjan.

Este capítulo incluye:

Descripción general de LDAP

Configuration Manager incluye un servidor LDAP interno (identificado en la interfaz de usuario como **Compartido**), pero también se puede conectar con un servidor LDAP de la organización. Configuration Manager usa estos servidores para buscarusuarios, grupos y funciones; para almacenar datos de personalización y para autenticar usuarios. Puede elegir cuáles de estas acciones usan el servidor LDAP de la organización y cuáles el servidor LDAP interno.

Una implantación típica usaría el servidor LDAP interno (compartido) para almacenar funciones y el LDAP externo (de la organización) para el resto de acciones.

Elección de proveedores

1. Inicie sesión en **Configuration Manager** como usuario administrador.
2. Vaya a **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** y seleccione SHARED o EXTERNAL en cada uno de los siguientes atributos según su preferencia en cuanto a proveedores (de manera predeterminada se selecciona SHARED):
   - ➤ Proveedor de autenticación
   - ➤ Proveedor de grupos
   - ➤ Proveedor de personalización
   - ➤ Proveedor de funciones
   - ➤ Proveedor de relaciones con funciones
3. Guarde el conjunto de configuración.

Conexión con un LDAP de la organización

Inicialmente, HP UCMDB Configuration Manager está configurado con un LDAP interno (compartido). Esta sección describe los pasos necesarios para conectar con un servidor LDAP de su organización.

Esta sección incluye:

- ➤ "Configurar la conexión LDAP" en la página 37
- ➤ "Configurar los proveedores de grupos y usuarios" en la página 37
- ➤ "Activar el conjunto de configuración" en la página 40
- ➤ "Asignar permisos a usuarios" en la página 41
- ➤ "Seleccionar el LDAP externo en Proveedor de autenticación" en la página 41
- ➤ "Importar el certificado LDAP" en la página 42

Configurar la conexión LDAP

En esta sección se explica cómo conectar Configuration Manager con un servidor LDAP externo. El servidor LDAP externo es el LDAP de la organización y contiene los usuarios de la organización.

1. Inicie sesión en **Configuration Manager** como usuario administrador.
2. Vaya a **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario externo** y actualice los siguientes atributos según las propiedades del LDAP de la organización:

   Conexión general de LDAP

   ldapHost: <Nombre de host LDAP>

   ldapPort: <Número de puerto LDAP>

   enableSSL: <true/false: usar conexión SSL con LDAP>

   useAdministrator: <true/false: utilizar usuario para conectar con LDAP>

   ldapAdministrator: <Nombre de usuario LDAP (se debe definir si **useAdministrator=true)**>

   ldapAdministratorPassword: <Contraseña de usuario LDAP (se debe definir si **useAdministrator=true**)>
3. Guarde el conjunto de configuración.

Configurar los proveedores de grupos y usuarios

Este procedimiento define el LDAP de la organización (repositorio externo) como proveedor de los grupos y usuarios. El LDAP interno (repositorio compartido) se sigue usando para la autenticación, pero los usuarios y grupos se recuperan del LDAP externo. Este modo se usa para probar la configuración del LDAP externo y asignar permisos a los usuarios de la organización.

Para definir los proveedores de grupos y usuarios:

1. Si no está en la página, vaya a **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario externo**. Asegúrese de que utiliza el borrador del conjunto de configuración que guardó en la sección "Configurar la conexión LDAP" en la página 37.

2. Actualice los siguientes atributos de acuerdo con sus propiedades LDAP organizativas:

   a **Búsqueda de usuarios**

   usersBase: <DN base para la búsqueda de usuarios>

   usersScope: <Ámbito para la búsqueda de usuarios>

   usersFilter: <Filtro para la búsqueda de usuarios>

   b **Clase objeto de usuarios** (depende del proveedor de LDAP)

   usersObjectClass: <Clase de objeto LDAP de usuarios>

   usersUniqueIDAttribute: <Atributo LDAP de Id. único de usuarios>

   Los siguientes atributos son opcionales:

   usersDisplayNameAttribute: <Atributo LDAP de nombre que se muestra de los usuarios>

   usersLoginNameAttribute: <Atributo LDAP de nombre de inicio de sesión de los usuarios>

   usersFirstNameAttribute: <Atributo LDAP de nombre de los usuarios>

   usersLastNameAttribute: <Atributo LDAP de apellidos de los usuarios>

   usersEmailAttribute: <Atributo LDAP de correo electrónico de los usuarios>

   usersPreferredLanguageAttribute: <Atributo LDAP de idioma preferido de los usuarios>

   usersPreferredLocationAttribute: <Atributo LDAP de ubicación preferida de los usuarios>

usersTimeZoneAttribute: <Atributo LDAP de zona horaria de los usuarios>

usersDateFormatAttribute: <Atributo LDAP de formato de fecha de los usuarios>

usersNumberFormatAttribute: <Atributo LDAP de formato de número de los usuarios>

usersWorkWeekAttribute: <Atributo LDAP de semana laboral de los usuarios>

usersTenantIDAttribute: <Atributo LDAP de Id. de titular de usuarios>

usersPasswordAttribute: <Atributo LDAP de contraseña de los usuarios>

c **Búsqueda de grupos**

groupsBase: <DN base para la búsqueda de grupos>

groupsScope: <Ámbito de LDAP para la búsqueda de grupos>

groupsFilter: <Filtro para la búsqueda de grupos>

rootGroupsBase: <DN base para la búsqueda de grupos raíz>

rootGroupsScope: <Ámbito de LDAP para la búsqueda de grupos raíz>

rootGroupsFilter: <Filtro para la búsqueda de grupos>

d **Clase objeto de grupos** (depende del proveedor de LDAP)

groupsObjectClass: <Clase de objeto LDAP de grupos>

groupsMembersAttribute: <Atributo LDAP de miembros de grupos>

Los siguientes atributos son opcionales:

groupsNameAttribute: <Atributo LDAP de nombre único de los grupos>

groupsDisplayNameAttribute: <Atributo LDAP de nombre que se muestra de los grupos>

groupsDescriptionAttribute: <Atributo LDAP de descripción de los grupos>

enableDynamicGroups: <Habilitar grupos dinámicos>

dynamicGroupsClass: <Clase de objeto LDAP de grupos dinámicos>

dynamicGroupsMemberAttribute: <Atributo LDAP de miembros de grupos dinámicos>

dynamicGroupsNameAttribute: <Atributo LDAP de nombre único de los grupos dinámicos>

dynamicGroupsDisplayNameAttribute: <Atributo LDAP de nombre para mostrar de los grupos dinámicos>

dynamicGroupsDescriptionAttribute: <Atributo LDAP de descripción de grupos dinámicos>

e **Jerarquía de grupos** (si el LDAP de la organización utiliza jerarquía de grupos)

enableNestedGroups: <Habilitar compatibilidad con grupos anidados>

maximalAllowedGroupsHierarchyDepth: <Profundidad de jerarquía de grupos máxima permitida>

f **Configuración avanzada**

ldapVersion: <Versión de LDAP>

baseDistinguishNameDelimiter: <Delimitador de DN base>

scopeDelimiter: <Delimitador de ámbito>

attributeValuesDelimiter: <Delimitador de valores de atributos de LDAP>

Guarde el borrador del conjunto de configuración.

Activar el conjunto de configuración

1 Vaya a **Administración** > **Administrador de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** y actualice las siguientes opciones:

Origen de UUM externo: Verdadero:

Proveedor de grupos: EXTERNAL

Proveedor de usuarios: EXTERNAL

2 Guarde el conjunto de configuración y actívela.

3 Cierre sesión y reinicie el servidor de **Configuration Manager**.

Asignar permisos a usuarios

Este procedimiento asigna la función **System Administrator** a los usuarios de la organización. Los usuarios que tengan la función **System Administrator** tendrán permisos para asignar las funciones pertinentes a los restantes usuarios de la organización.

1 Inicie sesión en **Configuration Manager** como usuario administrador.

2 Abra el módulo **Gestión de usuarios** (**Administracion** > **Gestión de usuarios**).

3 Confirme que ve los grupos y usuarios del LDAP de la organización.

4 Vaya al panel **Gestión de usuarios** > **Buscar usuarios** y busque los usuarios que servirán como administradores (por ejemplo: Nombre = j*, Apellido = Smith).

5 Añada la función **System Administrator** a los usuarios.

Seleccionar el LDAP externo en Proveedor de autenticación

Este procedimiento define el LDAP externo de la organización como proveedor de autenticación, con lo que los usuarios de la organización se utilizan para la autenticación.

1 Vaya a **Administración** > **Administrador de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** y actualice las siguientes opciones:

Proveedor de autenticación: EXTERNAL

2 Guarde el conjunto de configuración y actívelo.

3 Cierre sesión y reinicie el servidor de **Configuration Manager**.

4 Inicie sesión con uno de los usuarios de la organización a los que haya asignado el rol **System Administrator**.

Importar el certificado LDAP

Si se necesita un certificado para establecer conexión con el LDAP de la organización, lleve a cabo los siguientes pasos:

1. Exporte el certificado a un archivo.
2. Detenga el servicio Configuration Manager de Windows.
3. Ejecute el siguiente comando:

   <Instalación de Configuration Manager>\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias <certificate alias> -keystore <Instalación de Configuration Manager>\java\windows\x86_64\lib\security\cacerts -storepass changeit -file <ruta de archivo de certificado>

4. Inicie el servicio de Configuration Manager de Windows.

Configuración del LDAP interno (compartido)

Cambio de la contraseña del servidor LDAP interno (compartido) (opcional)

La contraseña del servidor LDAP interno (compartido) se puede cambiar por motivos de seguridad.

1. Conéctese a **HP Universal CMDB Configuration Manager**.
2. Abra una línea de comandos y desplácese hasta la carpeta **<Instalación de Configuration Manager>\ldap\serverRoot\bat**.
3. Ejecute **ldappasswordmodify -h localhost -p <ldap port> -D "cn=Directory Manager" -w <contraseña admin ldap> -c <contraseña admin ldap> -n <nueva contraseña admin ldap>**.
   - **a** La contraseña de admin ldap predeterminada es **ldapadmin**.
   - **b** El puerto predeterminado es **2389**.
   - **c** Confirme que el comando se ejecuta correctamente y, a continuación, realice los pasos siguientes.

4. En **UCMDB Configuration Manager**, seleccione **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario compartido**.
5. Actualice la contraseña en el atributo **ldapAdministratorPassword**.
6. Guarde el conjunto de configuración y actívela.
7. Cierre sesión de **UCMDB Configuration Manager**.
8. Reinicie el servidor de **UCMDB Configuration Manager**.

Configuración del puerto LDAP interno (compartido)

Es posible que otra aplicación ya use el puerto predeterminado, 2389. Para cambiar el puerto predeterminado use el siguiente procedimiento.

Para configurar el puerto LDAP interno:

1. Abra una línea de comandos y desplácese hasta la carpeta **<Instalación de Configuration Manager>\ldap\serverRoot\bat**.
2. Ejecute el siguiente comando:
   dsconfig -h localhost -p 2444 -D "cn=directory manager" -w <contraseña admin ldap> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:<nuevo puerto>

   La <contraseña de admin ldap> predeterminada es **ldapadmin**.
3. Confirme que no aparecen mensajes de error y, a continuación, realice los pasos siguientes.
4. Inicie sesión en HP Universal CMDB Configuration Manager.
5. En UCMDB Configuration Manager, seleccione A**dministración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario compartido** y actualice el número de puerto en el atributo **ldapPort**.
6. Guarde el conjunto de configuración y actívela.
7. Cierre sesión de UCMDB Configuration Manager.
8. Reinicie el servidor de UCMDB Configuration Manager.

Solución de problemas de LDAP

Problema: no se puede establecer comunicación con el servidor LDAP. En los registros aparece una excepción en la comunicación.

Solución: compruebe la configuración del host, del puerto de LDAP y del modo SSL:

a Compruebe que el host y el puerto de LDAP están configurados correctamente:
seleccione **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario externo** y compruebe la configuración de **ldapHost y ldapPort**.

b Compruebe que el modo SSL está configurado correctamente. Consulte al administrador del LDAP de la organización si el usuario administrador es obligatorio para la conexión LDAP. Seleccione **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario externo** y compruebe la configuración de **enableSSL**.

c Compruebe que está instalado el certificado de servidor apropiado. Ejecute el siguiente comando:

<Instalación de Configuration Manager>\java\windows\x86_64\bin\keytool.exe -list -trustcacerts [-alias <alias de certificado>] -keystore <Instalación de Configuration Manager>\java\windows\x86_64\lib\security\cacerts -storepass changeit

d Consulte al administrador de LDAP de la organización si el administrador es obligatorio para la conexión LDAP. Seleccione **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario externo** y compruebe las siguientes propiedades: **useAdministrator, ldapAdministrator y ldapAdministratorPassword**

Problema: no aparecen grupos en la pantalla de gestión de usuarios o grupos. En los registros no aparecen excepciones.

Solución: compruebe lo siguiente:

a Compruebe que los filtros de búsqueda de usuarios y grupos están configurados correctamente: Seleccione **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario externo** y modifique las siguientes propiedades: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope y rootGroupsFilter**

b Abra el explorador del cliente LDAP y busque los usuarios en el DNS base.

Problema: la interfaz de usuario funciona demasiado lentamente.

Solución: suele deberse a que hay demasiados grupos o usuarios configurados en el LDAP. Configure el DNS base y los filtros para reducir el número de grupos en el subconjunto pertinente, tal como se indica a continuación:

a Seleccione **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario externo**

b Modifique las siguientes propiedades: **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope y rootGroupsFilter**

Problema: algunos usuarios conocidos no aparecen en la ventana de gestión de grupos o usuarios.

Solución: La pantalla de gestión de usuarios y grupos sólo muestra los usuarios que pertenecen a algún grupo. Para ver los usuarios en la pantalla principal, colóquelos en los grupos pertinentes de LDAP.

Problema: el inicio de sesión tarda mucho tiempo.

Solución: es posible que el usuario pertenezca a demasiados grupos. Para optimizar el tiempo del inicio, cambie el filtro de búsqueda de grupos para que devuelva el menor número de grupos, lo que se puede hacer de la siguiente forma:

a Seleccione **Administración** > **Administración de servidores** > **Gestión de usuarios** > **Configuración de gestión de usuarios** > **Repositorio de usuario externo**

b Modifique la propiedad **groupsFilter**.

4

Autenticación de Lightweight Single Sign-On (LW-SSO): referencia general

Esta sección del incluye:

Descripción general de la autenticación LW-SSO

LW-SSO es un método de control de acceso que permite a los usuarios iniciar sesión una vez y obtener acceso a los recursos de diversos sistemas de software sin tener que volver a iniciar sesión. Las aplicaciones de un grupo configurado de sistemas de software confían en la autenticación, por lo que no se requiere ninguna autenticación adicional al moverse de una aplicación a otra.

La información de esta sección se aplica a las versiones 2.2 y 2.3 de LW-SSO.

Esta sección incluye los siguientes temas:

Caducidad del token LW-SSO

El valor de caducidad del token LW-SSO determina la validez de la sesión de la aplicación. Por lo tanto, su valor de caducidad debe ser, como mínimo, el mismo que el valor de caducidad de la sesión de la aplicación.

Configuración recomendada de la caducidad del token LW-SSO

Todas las aplicaciones que usen LW-SSO debe configurar la caducidad de tokens. El valor recomendado es 60 minutos. En el caso de las aplicaciones que no requieren un alto nivel de seguridad, se puede configurar un valor de 300 minutos.

Hora GMT

Todas las aplicaciones que participan en una integración LW-SSO deben utilizar la misma hora GMT con una diferencia máxima de 15 minutos.

Funcionalidad multidominio

La funcionalidad multidominio requiere que todas las aplicaciones que participan en la integración de LW-SSO configuren las opciones de trustedHosts (o las de **protectedDomains**) si son necesarias para realizar la integración con aplicaciones de diferentes dominios DNS. Además, también deben añadir el dominio correcto al elemento **lwsso** de la configuración.

Obtener la funcionalidad SecurityToken para URL

Para obtener información enviada como una **SecurityToken para URL** desde otras aplicaciones, la aplicación host debe configurar el dominio correcto en el elemento **lwsso** de la configuración.

Advertencias de seguridad de LW-SSO

En esta sección se describen advertencias de seguridad que son relevantes para la configuración de LW-SSO:

➤ **Parámetro InitString confidencial en LW-SSO.** LW-SSO utiliza una clave de cifrado simétrica para validar y crear un token LW-SSO. El parámetro **initString** de la configuración se utiliza para la inicialización de la clave secreta. Una aplicación crea un token y todas las aplicaciones que tengan el mismo parámetro initString validan el token.

Precaución:

- ➤ No es posible utilizar LW-SSO sin definir el parámetro **initString**.
- ➤ El parámetro **initString** es información confidencial y debe tratarse como tal en términos de publicación, transporte y persistencia.
- ➤ El parámetro **initString** sólo debe compartirse entre aplicaciones que se integren entre sí empleando LW-SSO.
- ➤ La longitud mínima del parámetro **initString** debe ser 12 caracteres.

➤ **Habilitar LW-SSO sólo si es estrictamente necesario.** LW-SSO debe estar deshabilitado, a menos que se requiera específicamente.

➤ **Nivel de seguridad de la autenticación.** La aplicación que usa el marco de autenticación más débil y genera un token LW-SSO en el que confían otras aplicaciones integradas determina el nivel de seguridad de la autenticación de todas las aplicaciones.

Se recomienda que sólo puedan generar tokens LW-SSO aquellas aplicaciones que usen marcos de autenticación sólidos y seguros.

- **Implicaciones del cifrado simétrico.** LW-SSO usa criptografía simétrica para generar y validar los tokens LW-SSO. Por consiguiente, todas las aplicaciones que usen LW-SSO pueden generar un token en el que confíen las demás aplicaciones que usen el mismo parámetro **initString**. El riesgo potencial es relevante cuando una aplicación que comparte un initString se encuentra en una ubicación que no es de confianza o cuando se puede acceder a ella desde dicha ubicación.

- **Asignación de usuarios (sincronización).** El marco LW-SSO no garantiza la asignación de usuarios entre las aplicaciones integradas. Por lo tanto, la aplicación integrada debe supervisar la asignación de usuarios.
  Se recomienda compartir el mismo registro de usuarios (como LDAP/AD) entre todas las aplicaciones integradas.

  Si no se asignan usuarios, pueden aparecer infracciones de seguridad y el comportamiento de la aplicación se puede resentir. Por ejemplo, el mismo nombre de usuario se puede asignar a los diferentes usuarios reales de las distintas aplicaciones.

  Además, en los casos en que un usuario inicie sesión en una aplicación (AppA) y seguidamente acceda a una segunda aplicación (AppB) que use la autenticación de contenedores o aplicaciones, si no se asigna el usuario, obligará al usuario a iniciar sesión manualmente en AppB y especificar un nombre de usuario. Si el usuario especifica un nombre de usuario distinto del que se usó para iniciar sesión en AppA, puede producirse el siguiente comportamiento: si el usuario accede posteriormente a una tercera aplicación (AppC) desde AppA o AppB, accederá a ella usando los mismos nombres de usuario que se emplearon para iniciar sesión en AppA o AppB, respectivamente.

- **Gestor de identidades**. Se usa para la autenticación, todos los recursos sin proteger del Gestor de identidades se deben configurar con la opción **nonsecureURLs** en el archivo de seguridad de LW-SSO.

Solución de problemas y limitaciones

Problemas conocidos

En esta sección se describen los problemas conocidos de la autenticación de LW-SSO.

- **Contexto de seguridad.** El contexto de seguridad de LW-SSO sólo admite un valor de atributo por nombre de atributo.

  Por lo tanto, si el token SAML2 envía más de un valor para el mismo nombre de atributo, el marco de LW-SSO sólo aceptará uno de ellos.

  De igual forma, si el token IdM está configurado para enviar más de un valor para el mismo nombre de atributo, el marco de LW-SSO sólo aceptará uno de ellos.

- **Funcionalidad de desconexión multidominio al utilizar Internet Explorer 7**. La funcionalidad de desconexión multidominio puede fallar en las siguientes condiciones:

  - El explorador usado es Internet Explorer 7 y la aplicación está invocando a más tres verbos de redireccionamiento HTTP 302 consecutivos en el procedimiento de desconexión.

  En ese caso, Internet Explorer 7 puede gestionar de forma incorrecta la respuesta de redirección HTTP 302 y mostrar una página de error **Internet Explorer no puede mostrar la página web** en su lugar.

  Como solución temporal, se recomienda reducir, en la medida de lo posible, el número de comandos de redirección de aplicaciones en la secuencia de desconexión.

Limitaciones

Tenga en cuenta las siguientes limitaciones al trabajar con la autenticación LW-SSO:

- **Acceso de los clientes a la aplicación**.

  Si se define un dominio en la configuración de LW-SSO:

  - Los clientes de la aplicación deben acceder a la aplicación con un nombre de dominio completo en la dirección URL de conexión, por ejemplo, http://myserver.**companydomain**.com/WebApp.
  - LW-SSO no admite direcciones URL con una dirección IP, por ejemplo, http://192.168.12.13/WebApp.
  - LW-SSO no admite direcciones URL sin un dominio, por ejemplo, http://myserver/WebApp.

  Si se define un dominio en la configuración de LW-SSO: el cliente puede acceder a la aplicación sin un nombre de dominio completo en la dirección URL de conexión. En ese caso, se crea una cookie de la sesión de LW-SSO específicamente para un equipo individual sin información de dominio. Por consiguiente, el explorador no delega la cookie a otro, por lo que no pasa a otros equipos ubicados en el mismo dominio DNS, lo que significa que LW-SSO no funciona en el mismo dominio.

- **Integración del marco LW-SSO.** Las aplicaciones sólo pueden usar y aprovechar las capacidades de LW-SSO si están integradas previamente en el marco de LW-SSO.

- **Compatibilidad con múltiples dominios**.
  - La funcionalidad multidominio se basa en el sitio de referencia HTTP. Por consiguiente, LW-SSO admite enlaces de una aplicación a otra y no permite escribir una URL en una ventana del explorador, salvo cuando ambas aplicaciones están en el mismo dominio.
  - No se admite el primer vínculo entre dominios que usen **HTTP POST**.

    La funcionalidad multidominio no admite la primera solicitud **HTTP POST** en una segunda aplicación (sólo se admite la solicitud **HTTP GET**). Por ejemplo, si la aplicación tiene un vínculo HTTP a una segunda aplicación, se admite una solicitud **HTTP GET**, pero no se admite una solicitud **HTTP FORM**. Todas las solicitudes a partir de la primera pueden ser **HTTP POST** o **HTTP GET**.
  - Tamaño del token LW-SSO:

    El tamaño de la información que LW-SSO puede transferir de una aplicación de un dominio a otra aplicación de otro dominio está limitada a 15 grupos/funciones/atributos (tenga en cuenta que cada elemento puede tener una longitud media de 15 caracteres).
  - Vinculación de un sitio protegido (HTTPS) a otro no protegido (HTTP) en un escenario multidominio:

    La funcionalidad multidominio no funciona al vincular una página protegida (HTTPS) a otra no protegida (HTTP). Ésta es una limitación del explorador en la que el encabezado del remitente no se envía al vincular un recurso protegido a otro no protegido. Por ejemplo, consulte: http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP
- **Token SAML2.**
  - La funcionalidad de desconexión no se admite cuando se usa el token SAML2.

    Por lo tanto, si el token SAML2 se usa para acceder a una segunda aplicación, los usuarios que se desconecten de la primera aplicación no se desconectarán de la segunda.

- La caducidad del token SAML2 no aparece reflejada en la gestión de sesiones de la aplicación.

  Por consiguiente, si el token SAML2 se usa para acceder a una segunda aplicación, la gestión de sesiones de cada aplicación se trata de forma independiente.

- **Dominio JAAS.** El dominio JAAS de Tomcat no es compatible.
- **Uso de espacios en directorios de Tomcat.** No se admite el uso de espacios en directorios de Tomcat.

  LW-SSO no se puede utilizar cuando una ruta de instalación de Tomcat (carpetas) incluye espacios (por ejemplo, Archivos de programa) y el archivo de configuración de LW-SSO se encuentra en la carpeta **common\classes** de Tomcat.

- **Configuración del equilibrador de carga.** Debe configurarse un equilibrador de carga implantado en LW-SSO para utilizar sesiones adheridas.

5

Autenticación del Gestor de identidades

Esta sección del incluye:

- Aceptar la autenticación del Gestor de identidades en la página 55
- Ejemplo de uso del conector Java para configurar el Gestor de identidades para Configuration Manager con IIS6 en un sistema operativo Windows 2003 en la página 57

Aceptar la autenticación del Gestor de identidades

Si usa un Gestor de identidades y tiene intención de agregar HP Universal CMDB Configuration Manager, debe realizar esta tarea.

En esta tarea se describe cómo configurar HP Universal CMDB Configuration Manager para que acepte la autenticación del Gestor de identidades.

Esta tarea incluye los siguientes pasos:

- "Requisitos previos" en la página 55
- "Configurar HP Universal CMDB Configuration Manager para que acepte el Gestor de identidades" en la página 56

Requisitos previos

El servidor Tomcat de Configuration Manager debe estar conectado a un servidor web (IIS o Apache) protegido mediante su Gestor de identidades a través de un conector Java de Tomcat (AJP13).

Para obtener instrucciones sobre la utilización de un conector Java de Tomcat (AJP13), consulte la documentación de Java de Tomcat (AJP13).

Configurar HP Universal CMDB Configuration Manager para que acepte el Gestor de identidades

Para configurar Java Tomcat (AJP13) con IIS6:

1. Configure el Gestor de identidades para que envíe un encabezado/devolución de llamada personalizados que contenga el nombre de usuario y solicite el nombre del encabezado.
2. Abra el archivo <**Directorio de instalación de Configuration Manager**>**conf****lwssofmconf.xml** y busque la sección que empieza por **in-ui-identity-management**.

   Por ejemplo:

   ```
   <in-ui-identity-management enabled="false">
       <identity-management>
         <userNameHeaderName>sm-user</userNameHeaderName>
       </identity-management>
   </in-ui-identity-management>
   ```

   a. Active la funcionalidad quitando el carácter de comentario.

   b. Reemplace **enabled**="**false**" por **enabled**="**true**".

   c. Reemplace **sm-user** por el nombre de encabezado que ha solicitado en el paso. 1
3. Abra el archivo <**Directorio de instalación de Configuration Manager**>**conf****client-config.properties** y edite las siguientes propiedades:

   a. Cambie **bsf.server.url** por la dirección URL del Gestor de identidades y cambie el puerto por el del Gestor de identidades:

   ```
   bsf.server.url=http://< URL de Gestor de identidades>:< Puerto de Gestor de identidades >/bsf
   ```

   b. Cambie **bsf.server.services.url** por el protocolo HTTP y cambie el puerto por el puerto original de Configuration Manager:

   ```
   bsf.server.services.url=http://<URL de Configuration Manager>:< Puerto de Configuration Manager>/bsf
   ```

Ejemplo de uso del conector Java para configurar el Gestor de identidades para Configuration Manager con IIS6 en un sistema operativo Windows 2003

En esta tarea de ejemplo se describe cómo instalar y configurar el conector Java para usarlo para configurar la gestión de identificación para usarla con Configuration Manager con IIS6 ejecutándose en un sistema operativo Windows 2003.

Para instalar el conector Java y configurarlo para IIS6 en Windows 2003:

1. Descargue la última versión del conector Java (por ejemplo, **djk-1.2.21**) del sitio web de Apache.
   a. Haga clic en **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/**.
   b. Seleccione la versión más reciente.
   c. Descargue el archivo **isapi_redirect.dll** del directorio **amd64**.
2. Almacene este archivo en <**Directorio de instalación de Configuration Manager**>**\tomcat\bin\win32**.
3. Cree un archivo de texto llamado **isapi_redirect.properties** en el directorio en que se encuentre isapi_redirect.dll.

   El contenido de dicho archivo es:

   ```
   # Configuration file for the Jakarta ISAPI Redirector

   # The path to the ISAPI Redirector Extension, relative to the website

   # This must be in a virtual directory with execute privileges

   extension_uri=/jakarta/isapi_redirect.dll

   # Full path to the log file for the ISAPI Redirector

   log_file=<Configuration Manager Install Directory>\servers\server-0\logs\isapi.log

   # Log level (debug, info, warn, error or trace)

   log_level=info

   # Full path to the workers.properties file
   ```

worker_file==<Directorio de instalación de Configuration Manager>\tomcat\conf\workers.properties.minimal

Full path to the uriworkermap.properties file

worker_mount_file==<Directorio de instalación de Configuration Manager>\tomcat\conf\uriworkermap.properties

4 Cree un archivo de texto llamado **workers.properties.minimal** en <**Directorio de instalación de Configuration Manager**>**tomcat****conf**.

El contenido de este archivo es:

workers.properties.minimal -

#

This file provides minimal jk configuration

properties needed to

connect to Tomcat.

#

Defining a worker named ajp13w and of type ajp13

Note that the name and the type do not have to

match.

worker.list=ajp13w

worker.ajp13w.type=ajp13

worker.ajp13w.host=localhost

worker.ajp13w.port=8009

#END

5 Cree un archivo de texto llamado **uriworkermap.properties** en <**Directorio de instalación de Configuration Manager**>**tomcat****conf**.

El contenido de este archivo es:

uriworkermap.properties - IIS

#

This file provides sample mappings for example:

```
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]

/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

Importante: tenga en cuenta que Configuration Manager debe tener dos reglas. La nueva sintaxis les permite unirse en una regla, como por ejemplo:

/cnc|/*=ajp13w

---

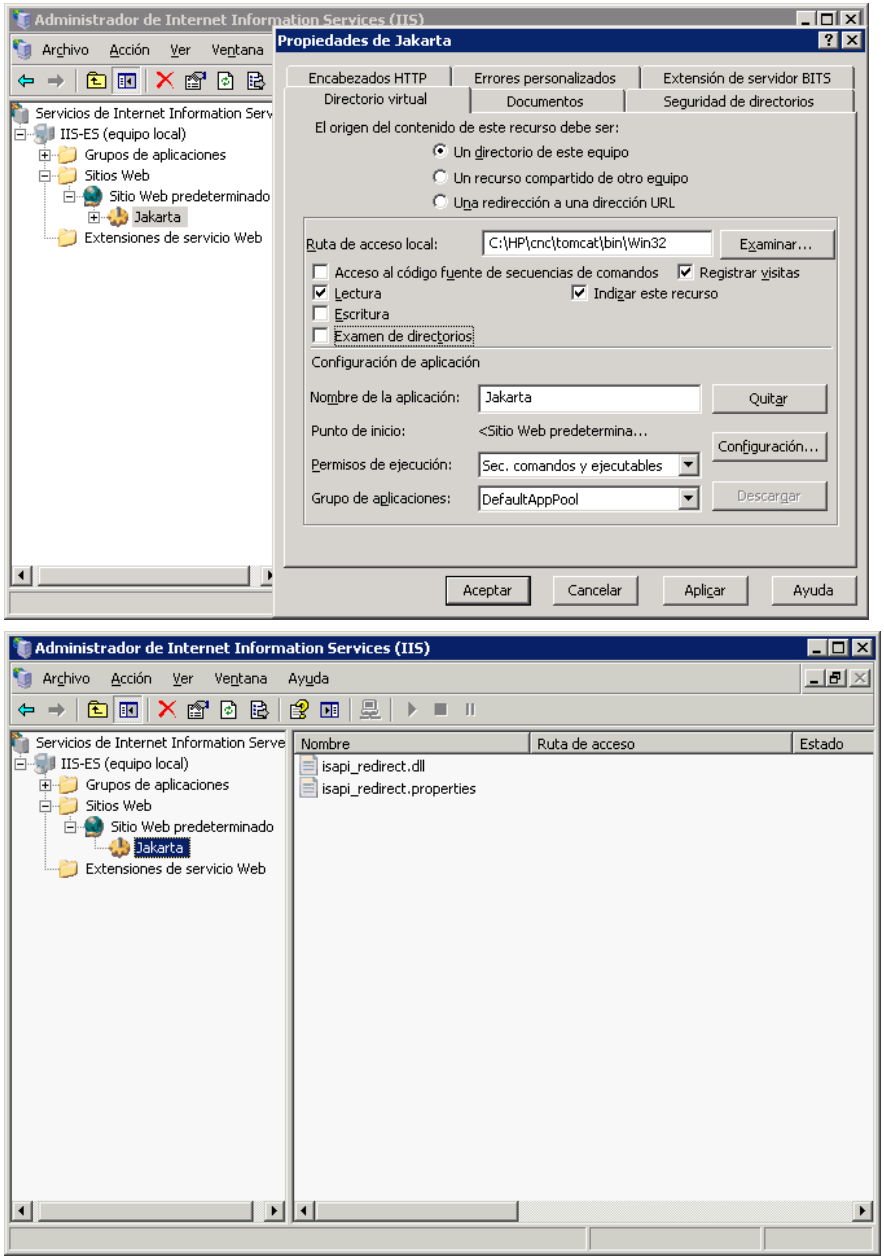
6 Cree el directorio virtual en el objeto de sitio web de la configuración de IIS.

a En el menú Inicio de Windows, abra **Configuración\Panel de control\Herramientas administrativas\Administrador de Internet Information Services (IIS)**.

b En el panel derecho, haga clic con el botón secundario en **<Nombre del equipo local>\Web Sites\<Nombre de su sitio web>** y seleccione **Nuevo\Directorio virtual**.

c Asigne al directorio el nombre de alias **Jakarta** y seleccione el directorio que contenga el archivo isapi_redirect.dll como ruta de acceso.

La ventana del Administrador de Internet Information Services (IIS) es similar a la siguiente:



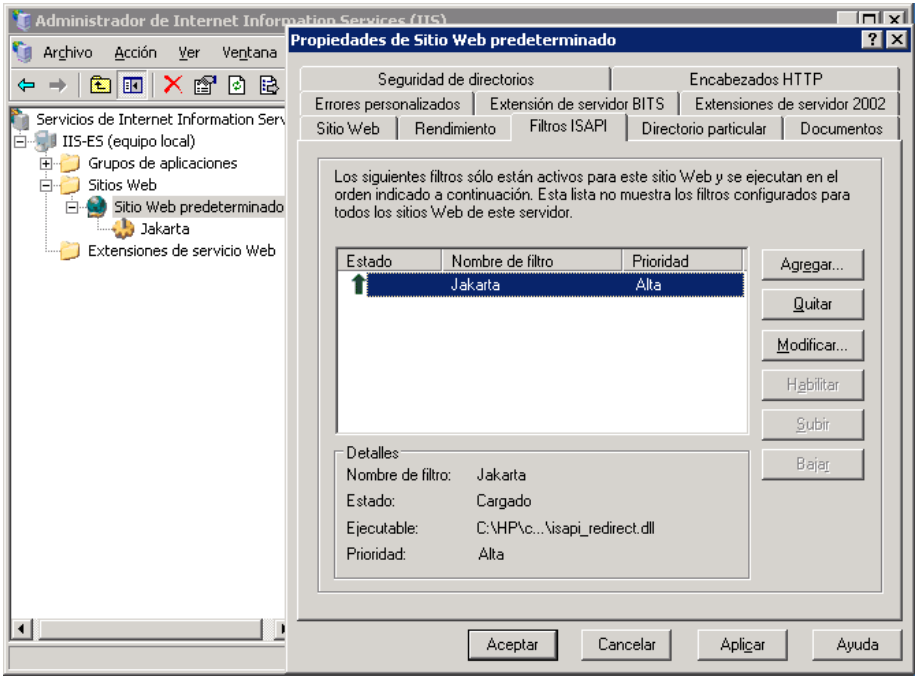
7 Agregue **isapi_redirect.dll** como filtro ISAPI.

a Haga clic con el botón secundario en **<Nombre de su sitio web>** y seleccione **Propiedades**.

b Seleccione la ficha **Filtros ISAPI** y haga clic en el botón **Agregar...**.

c Seleccione el nombre de filtro **Jakarta** y diríjase a **isapi_redirect.dll**. El filtro se ha agregado, pero sigue inactivo.

La ventana de configuración es similar a la siguiente:



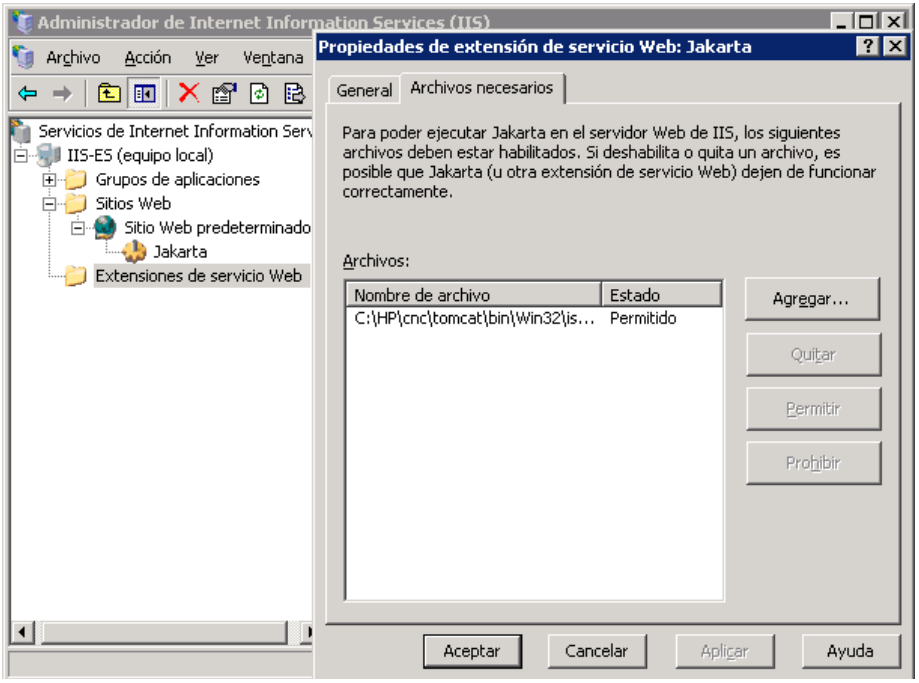
d Haga clic en el botón **Aplicar**.

8 Defina y permita la extensión del nuevo servicio web.

a Haga clic con el botón secundario en la entrada **<Nombre del equipo local>\Extensiones de servicio web** y seleccione el elemento de menú **Agregar extensión de servicio web nuevo...**

b Asigne a la extensión del nuevo servicio web el nombre **Jakarta** y diríjase al archivo **isapi_redirect.dll**.

Nota: antes de hacer clic en el botón **Aceptar**, active la casilla **Establecer el estado de extensión a Permitida**.



9 Reinicie el servidor web de IIS y acceda a la aplicación a través del servicio web.

6

Inicio de sesión en Configuration Manager

Este capítulo incluye:

Acceso a Configuration Manager

Para acceder a Configuration Manager, utilice un explorador web compatible, desde cualquier equipo con conexión de red (intranet o Internet) al servidor de Configuration Manager. El nivel de acceso que concede a un usuario depende de los permisos del mismo. Para obtener más detalles sobre los permisos de usuario, consulte "Administración de usuarios" en la guía de usuario de *HP Universal CMDB Configuration Manager*.

Para obtener más información sobre los requisitos del explorador web, así como los requisitos mínimos para ver Configuration Manager correctamente, consulte "Requisitos del sistema de Configuration Manager" en la página 8.

Para obtener más información sobre cómo acceder a Configuration Manager de forma segura, consulte "Sistema de protección" en la página 73.

Cómo acceder a Configuration Manager

En el explorador web, escriba la dirección URL del servidor de Configuration Manager, por ejemplo, **http://<nombre o dirección IP del servidor>.<nombre de dominio>:<puerto>** donde **<nombre o dirección IP del servidor>.<nombre de dominio>** representa el nombre de dominio completo del servidor de Configuration Manager y **<puerto>** representa el puerto seleccionado en la instalación.

Conectar a Configuration Manager

1. Escriba el nombre de usuario y la contraseña que definió en el Asistente post-instalación de Configuration Manager.
2. Pulse **Conectar**. Tras iniciar sesión, el nombre de usuario aparece en la parte superior derecha de la pantalla.
3. (Se recomienda) Conecte con el servidor LDAP de la organización y asigne funciones administrativas a los usuarios LDAP, con el fin de que los administradores de Configuration Manager puedan acceder al sistema. Para obtener más información sobre cómo asignar funciones a los usuarios en el sistema de Configuration Manager, consulte "Administración de usuarios" en la guía *HP Universal CMDB Configuration Manager User Guide*.

Desconectar

Cuando finalice una sesión, es aconsejable desconectarse del sitio web para evitar entradas sin autorización.

Para desconectarse:

Pulse **Desconectar** en la parte superior de la página.

Nota: el tiempo de expiración de sesión predeterminado es 30 minutos.

Acceso a la consola JMX desde Configuration Manager

Para solucionar problemas o modificar ciertas configuraciones, es posible que necesite acceder a la consola JMX.

Para acceder a la consola JMX:

1. Abra la consola JMX en http://<nombre o dirección IP del servidor>:<puerto>/cnc/jmx-console. El puerto es el configurado en la instalación de Configuration Manager.
2. Especifique las credenciales de usuario predeterminadas. Son las mismas que se han utilizado para conectarse a Configuration Manager.

Solución de problemas y limitaciones

Problema. Tras cambiar el conjunto de configuración en Administración de servidores, el servidor no se inicia.

Solución. Vuelva al conjunto de configuración anterior. Siga estos pasos:

1. Ejecute el siguiente comando para localizar el Id. del último conjunto de configuración activado:

   ```
   <HP Universal CMDB Configuration Manager>\bin\export-cs.bat
   <propiedades de base de datos> --history
   ```

   en donde se pueden especificar las **<propiedades de la base de datos>** apuntando a la ubicación del archivo **<Directorio de instalación de Configuration Manager\>conf\database.properties** o especificando cada una de las propiedades de la base de datos. Por ejemplo:

   ```
   cd <HP Universal CMDB Configuration Manager>\bin export-cs.bat -p
   ..\conf\database.properties --history
   ```

2 Ejecute el siguiente comando para exportar el último conjunto de configuración:

```
< HP Universal CMDB Configuration Manager>\bin\export-cs.bat
<propiedades de base de datos> <Id de conjunto de configuración>
<nombre de archivo de volcado>
```

donde <**Id de conjunto de configuración**> es el Id de conjunto de configuración del paso anterior y <**archivo de volcado**> es el nombre de un archivo temporal que se usa para almacenar el conjunto de configuración. Por ejemplo, para exportar un conjunto de configuración cuyo Id es **491520** al archivo **mydump.zip**, escriba:

```
cd <HP Universal CMDB Configuration installation home>\bin export-
cs.bat -p ..\conf\database.properties -i 491520 -f mydump.zip
```

3 Detenga el servicio HP Universal CMDB Configuration Manager.

4 Ejecute el siguiente comando para importar y activar el conjunto de configuración anterior:

```
< HP Universal CMDB Configuration Manager>\bin\import-cs.bat
<propiedades de base de datos> <nombre de archivo de volcado> --
activate
```

Problema. Error en la conexión UCMDB.

Solución. La causa puede ser cualquiera de las siguientes:

- El servidor de UCMDB no funciona. Reinicie Configuration Manager una vez que UCMDB esté totalmente activo (verifique que el estado del servidor de UCMDB es **En funcionamiento**).
- El servidor de UCMDB está en funcionamiento, pero las credenciales de conexión o la dirección URL de Configuration Manager es incorrecta. Inicie Configuration Manager. Vaya a Administración de servidores cambie la configuración de la conexión de UCMDB y guarde el conjunto de configuración nuevo. Active el conjunto de configuración y reinicie el servidor.

Problema. La configuración de la conexión LDAP es incorrecta.

Solución. Vuelva al conjunto de configuración anterior. Defina la configuración correcta de la conexión LDAP y active el conjunto de configuración nuevo.

Problema. Los cambios en el modelo de clase UCMDB no se detectan en Configuration Manager.

Solución. Reinicie el servidor de Configuration Manager.

Problema. El registro de Configuration Manager contiene el error **Se ha agotado el tiempo de espera para la ejecución de UCMDB**.

Solución. Esto sucede cuando la base de datos de UCMDB está sobrecargada. Para corregirlo, aumente el tiempo de espera de la conexión como se indica a continuación:

1. Cree un archivo jdbc.properties en la carpeta **UCMDBServer\conf**.
2. Escriba el siguiente texto: QueryTimeout=<número de segundos>.
3. Reinicie el servidor de UCMDB .

Problema. Configuration Manager no le permite añadir una vista que se va a gestionar.

Solución. Cuando se agrega una vista para gestionarla, se crea un TQL en UCMDB. Si se alcanza el límite máximo de TQL activos, la vista no se podrá agregar. Aumente el límite de TQL activos en UCMDB, para lo que debe cambiar los siguientes ajustes en el Gestor de configuración de infraestructura:

- Número máx. de TQL activos en el servidor
- Número máx. de TQL activos del cliente

Problema. El certificado del servidor HTTPS no es válido

Solución. La causa puede ser cualquiera de las siguientes:

- Se ha superado la fecha de validación del certificado. Tiene que obtener un certificado nuevo.
- La entidad emisora de certificados del certificado no es de confianza. Agregue dicha entidad emisora su lista Entidad emisora de certificados de raíz de confianza.

Problema. Al conectar desde la página de inicio de sesión de Configuration Manager, aparece un error de inicio de sesión o se accede a una página denegada.

Solución. La causa puede ser cualquiera de las siguientes:

- Es posible que el nombre no se haya definido en el proveedor de autenticación (LDAP externo/compartido). Agregue el usuario al sistema proveedor de autenticación.
- El usuario está definido, pero no tiene permiso de inicio de sesión en Configuration Manager. Conceda al usuario permiso de inicio de sesión. Como práctica recomendada, asigne el permiso de inicio de sesión al grupo raíz de todos los usuarios de Configuration Manager.
- Estas soluciones también se aplican en los casos en los que se produce un error de inicio de sesión cuando se viene de un inicio de sesión del sistema IDM.

Problema. El servidor de Configuration Manager no se inicia porque se han especificado unas credenciales incorrectas de la base de datos.

Solución. Si ha cambiado las credenciales de la base de datos y el servidor no se inicia, es posible que las credenciales sean erróneas. (**Nota**: el Asistente post-instalación no comprueba automáticamente las credenciales introducidas. Debe pulsar el botón **Probar** del asistente.) Debe volver a cifrar la contraseña de la base de datos y especificar nuevas credenciales en el archivo de configuración. Siga estos pasos:

1 En la línea de comandos, ejecute el siguiente comando para cifrar la contraseña actualizada de la base de datos:

<Carpeta de instalación de Configuration Manager (CnC)>\bin\encrypt-password.bat –p <contraseña>

que devuelve una contraseña cifrada.

2 Copie la contraseña cifrada (incluyendo el prefijo {CIFRADO}) en el parámetro **db.password** de <**carpeta de instalación de CnC**>**conf****database.properties**.

Problema. Si el DNS no se ha configurado correctamente, es posible que tenga que conectarse utilizando la dirección IP del servidor. Al introducir la dirección IP, se produce un segundo error de DNS.

Solución. Vuelva a reemplazar el nombre del equipo por la dirección IP. Por ejemplo:

Si inicia sesión con la siguiente dirección IP: http://16.55.245.240:8180/cnc/

y obtiene una dirección en la que el nombre del equipo muestra un error de DNS, como:
http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

reemplácela por:
http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

y vuelva a iniciar la aplicación en el explorador.

Problema. El servidor Tomcat de Configuration Manager no se inicia.

Solución. Pruebe a realizar una de las acciones siguientes:

- Ejecute el Asistente post-instalación y reemplace los puertos del servidor de Configuration Manager.
- Anule el otro proceso que ocupa los puertos de Configuration Manager.

- Cambie manualmente los puertos en los archivos de configuración de Configuration Manager editando el siguiente archivo: <**Carpeta de instalación de CnC**>**\servers\server-0\conf\server.xml** y actualizando los puertos pertinentes:
  - HTTP (8080): línea 69
  - HTTPS (8443): líneas 71, 90

Problema. Se encuentra un error de memoria insuficiente en el registro de Configuration Manager.

Solución. Aumente la memoria máxima de Java tanto como sea necesario.

Para cambiar el tamaño de la memoria en el servicio de Configuration Manager:

1. Vaya al directorio <**Carpeta de instalación de CnC**>**\cnc\bin** y ejecute el siguiente comando: edit-server-0.bat.
2. Seleccione la ficha **Java**.
3. Actualice los parámetros **Bloque de memoria inicial** y **Bloque de memoria máximo**.

Para cambiar el tamaño de la memoria en el archivo por lotes:

1. Vaya al directorio <**Carpeta de instalación de CnC**>**\cnc**, abra el archivo **start-server-0.bat** y edítelo
2. Busque la línea que comienza por **SET JAVA_OPTS=-Dcnc.home**.
3. Busque los comandos **-Xms** y **-Xmx**, y cámbielos en función de sus requisitos:

   -Xms<tamaño de bloque de memoria inicial> -Xmx<tamaño de bloque de memoria máximo>

   Por ejemplo: para establecer el bloque de memoria inicial en 100 MB y el bloque de memoria máxima en 800 MB, escriba:

   -Xms100m -Xmx800m

Problema. El Asistente post-instalación tarda mucho tiempo en terminar después de pulsar **Finalizar**.

Solución. En un sistema UCMDB que no se haya preconfigurado para el modo consolidado, la operación de consolidación del esquema puede tardar mucho tiempo (en función de la cantidad de datos). Espere 15 minutos. Si no se detecta progreso, anule el Asistente post-instalación y reinicie el proceso.

Problema. Los cambios en los CI en UCMDB no se reflejan en Configuration Manager.

Solución. Configuration Manager ejecuta un proceso de análisis asíncrono sin conexión. Es posible que el proceso no haya procesado aún los últimos cambios realizados en UCMDB. Para resolverlo, pruebe a realizar una de las acciones siguientes:

- Espere unos minutos. El intervalo predeterminado entre las ejecuciones de procesos de análisis es 10 minutos. Se puede configurar en el módulo Administrador de servidores.
- Para ejecutar el cálculo del análisis sin conexión en la vista pertinente, ejecute una llamada JMX.
- Vaya a Administración de directivas. Pulse el botón **Recalcular análisis de directiva**. Así se invoca el proceso de análisis sin conexión para todas las vistas (lo que puede tardar un tiempo). Es posible que también tenga que realizar un cambio artificial en una política y guardarlo.

Problema. Al hacer clic en **Administración** > **Abrir UCMDB**, aparece la página de inicio de sesión de UCMDB.

Solución. Para acceder a UCMDB sin tener que volver a conectarse, es preciso que habilite el inicio de sesión único. Para obtener más información, consulte "Habilitar Lightweight Single Sign-On" en la página 20. Además, asegúrese de que el usuario de Configuration Manager conectado está definido en el sistema de gestión de usuarios de UCMDB.

Problema. Al configurar una conexión UCMDB en el Asistente post-instalación como una dirección IPv6, el elemento de menú **Administración** > **Abrir UCMDB** no funciona.

Solución. Siga estos pasos:

1. Vaya a **Administración** > **Administración de servidores** > **Configuration Manager** > **Conexión de UCMDB**.
2. Añada corchetes a la dirección IP de la URL de acceso a UCMDB. La dirección URL debeser similar a la siguiente: http://[x:x:x:x:x:x:x:x]:8080/.
3. Guarde el conjunto de configuración y actívelo.
4. Reinicie Configuration Manager.

Cuando se trabaja con Configuration Manager se pueden aplicar las siguientes limitaciones:

- Siempre que se cambia la hora en el servidor Tomcat de Configuration Manager es preciso reiniciar el servidor para actualizar la hora del mismo.

7

Sistema de protección

Este capítulo incluye:

Sistema de protección de Configuration Manager

Esta sección presenta el concepto de aplicación Configuration Manager segura y explica la planificación y arquitectura necesarias para implementar la seguridad. Se recomienda encarecidamente leer esta sección antes de pasar a las secciones siguientes.

Configuration Manager se ha diseñado para poder formar parte de una arquitectura segura y, por consiguiente, puede afrontar el reto de enfrentarse a las amenazas de seguridad a las que pueda estar expuesto.

Las directrices del sistema de protección tienen que ver con la configuración necesaria para implantar un Configuration Manager más seguro (endurecido).

La información que se proporciona sobre el sistema de protección va dirigida principalmente a los administradores de Configuration Manager, quienes deben familiarizarse con la configuración y las recomendaciones del sistema de protección antes de iniciar los procedimientos de dicho sistema.

Éstas son las preparaciones recomendadas para proteger el sistema:

- Evalúe el riesgo de seguridad/estado de la seguridad de la red general y use las conclusiones que obtenga a la hora de decidir cuál es la mejor forma de integrar Configuration Manager en la red.
- Debe conocer a la perfección tanto el marco técnico como las capacidades de seguridad de Configuration Manager.
- Revise todas las directivas del sistema de protección
- Verifique que Configuration Manager funciona a la perfección antes de iniciar los procedimientos del sistema de protección.
- En todas las secciones, siga los pasos del procedimiento del sistema de protección de forma cronológica.

Importante:

- Los procedimientos del sistema de protección se basan en la asunción de que el usuario sólo va a implantar las instrucciones que se proporcionan en estas secciones y que no va a llevar a cabo otros pasos de protección documentados en otros lugares.
- Aunque los procedimientos se centran en una arquitectura distribuida concreta, ello no implica que ésta sea la arquitectura que mejor cubra las necesidades de su organización.
- Se supone que los procedimientos que se incluyen en las siguientes secciones se van a llevar a cabo en equipos dedicados a Configuration Manager. El uso de las máquinas para otros fines, además de para Configuration Manager, pueden generar resultados problemáticos.
- La información sobre el sistema de protección que se proporciona en esta sección no pretende ser una guía para la realización de evaluaciones de los riesgos de seguridad en sistemas computerizados.

Cifrar la contraseña de la base de datos

La contraseña de la base de datos se almacena en el archivo < **Directorio de instalación de Configuration Manager>\conf\database.properties**. Si desea cifrar la contraseña, nuestro algoritmo de cifrado predeterminado cumple los estándares de FIPS 140-2. Para cifrar la contraseña de la base de datos, active la casilla **Cifrar contraseña** de la página Configuración de base de datos del Asistente post-instalación de Configuration Manager.

El cifrado se logra por medio de una clave, ya que la contraseña se cifra a través de ella. Posteriormente, la propia clave se cifra mediante otra clave, que se conoce como clave maestra. Ambas claves se cifran con el mismo algoritmo. Para obtener más información sobre los parámetros que se usan en el proceso de cifrado, consulte "Parámetros de cifrado" en la página 83.

Precaución: Si cambia el algoritmo de cifrado, no se podrán volver a utilizar las contraseñas cifradas anteriormente.

Para cambiar el cifrado de la contraseña de la base de datos:

1. Abra el archivo < **Directorio de instalación de Configuration Manager>\conf\encryption.properties** y edite los siguientes campos:
   - **engineName.** Escriba el nombre del algoritmo de cifrado.
   - **keySize.** Especifique el tamaño de la clave maestra del algoritmo seleccionada.
2. Ejecute el script **generate-keys.bat**, que crea el siguiente directorio: **cnc\security\encrypt_repository**, y genera la clave de cifrado.
3. Vuelva a ejecutar el Asistente de post-instalación.

Habilitar SSL en el equipo servidor con un certificado autofirmado

En estas secciones se explica cómo configurar Configuration Manager para que admita la autenticación y el cifrado utilizando el canal Capa de sockets seguros (SSL).

Configuration Manager usa Tomcat 6.0 como servidor de aplicaciones.

Nota: las ubicaciones de todos los directorios y archivos dependen de su plataforma concreta, del sistema operativo y de las preferencias que se elijan durante la instalación.

---

1 Requisitos previos

Antes de iniciar el siguiente procedimiento, quite el archivo **tomcat.keystore** antiguo, que se encuentra en < **Directorio de instalación de Configuration Manager**>**java****lib****security****tomcat.keystore**.

2 Generar un almacén de claves del servidor

Cree un almacén de claves (tipo JKS) con un certificado autofirmado y una clave privada coincidente:

➤ Desde el directorio bin de la instalación de Java en <**Directorio de instalación de Configuration Manager**>, ejecute el siguiente comando:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore
..\lib\security\tomcat.keystore
```

Se abre el cuadro de diálogo de la consola.

➤ Escriba la contraseña del almacén de claves. Si la contraseña ha cambiado, cámbiela manualmente en el archivo.

➤ Responda a la pregunta, **¿Cuáles son su nombre y sus apellidos?** Escriba el nombre del servidor web de Configuration Manager. Introduzca los restantes parámetros en función de las necesidades de su organización.

➤ Escriba una contraseña de la clave. Dicha contraseña DEBE coincidir con la contraseña del almacén de claves.

Se crea un almacén de claves JKS llamado **tomcat.keystore** con un certificado de servidor llamado **hpcert**.

3 Colocar el certificado en el almacén de confianza del cliente

Después de generar **tomcat.keystore** y exportar el certificado de servidor para todos los clientes que necesiten comunicarse con Configuration Manager a través de SSL utilizando este certificado autofirmado, coloque este certificado en los almacenes de confianza del cliente.

Limitación: en **tomcat.keystore**, no puede haber más de un certificado de servidor.

---

4 Verificar los valores de configuración del cliente

Abra el archivo **client-config.properties**, que se encuentra en el directorio **conf** del <**Directorio de instalación de Configuration Manager**>. Seleccione el protocolo **https** y el puerto **8443**.

5 Modificar el archivo server.xml

Abra el archivo **server.xml**, que se encuentra en el directorio **conf** del <**Directorio de instalación de Configuration Manager**>. Localice la sección que empieza por

Connector port="8443"

que aparece en los comentarios. Active el script quitando el carácter de comentario y agregue las dos líneas siguientes:

keystoreFile="<ubicación de archivo tomcat.keystore>" (véase el paso 2 en la página 76)

keystorePass="<contraseña>"

6 Reiniciar el servidor

7 Verificar la seguridad del servidor

Para verificar que el servidor de Configuration Manager es seguro, escriba la siguiente URL en el explorador web:
https://<Nombre o dirección IP de servidor de Configuration Manager>:8443/cnc.

Sugerencia: si no logra establecer una conexión, pruebe a usar otro explorador o actualice el explorador a una versión más reciente.

Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación

Para usar un certificado generado por una entidad de certificación (CA), el almacén de claves debe estar en formato Java. El siguiente ejemplo explica cómo dar formato al almacén de claves en un equipo Windows.

1 Requisitos previos

Antes de iniciar el siguiente procedimiento, quite el archivo **tomcat.keystore** antiguo, que se encuentra en < **Directorio de instalación de Configuration Manager>\java\lib\security\tomcat.keystore**.

2 Generar un almacén de claves del servidor

a Genere un certificado firmado por CA e instálelo en Windows.

b Exporte el certificado a un archivo ***.pfx** (incluyendo las claves privadas) a través de Microsoft Management Console (**mmc.exe**).

➤ Escriba cualquier cadena como contraseña del archivo **pfx**. (Esta contraseña se solicita al convertir el tipo de almacén de claves a un almacén JAVA.)
El archivo **.pfx** ahora contiene un certificado público y una clave privada, y está protegido mediante contraseña.

c Copie el archivo **.pfx** que ha creado a la siguiente carpeta: **<Directorio de instalación de Configuration Manager>\java\lib\security**.

d Abra el símbolo del sistema y cambie el directorio a **<Directorio de instalación de Configuration Manager>\bin\jre\bin**.

➤ Cambie el tipo de almacén de claves de **PKCS12** a un almacén de claves **JAVA**, para lo que debe ejecutar el siguiente comando:

```
keytool -importkeystore -srckeystore <Directorio de instalación de Configuration Manager>\conf\security\<nombre de archivo pfx> -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

Se le solicitará la contraseña del almacén de claves de origen (**.pfx**). Ésta es la contraseña que introdujo al crear el archivo pfx en el paso b.

3 Verificar los valores de configuración del cliente

Abra el siguiente archivo: **<Directorio de instalación de Configuration Manager>\cnc\conf\client-config.properties** y verifique que en la propiedad **bsf.server.url** se selecciona **https** y el puerto es **8443**.

4 Modificar el archivo server.xml

Abra el siguiente archivo: **<Directorio de instalación de Configuration Manager>\conf\server.xml**. Localice la sección que empieza por

```
Connector port="8443"
```

que aparece en los comentarios. Active el script quitando el carácter de comentario y agregue las dos líneas siguientes:

```
keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />
```

5 Reiniciar el servidor

6 Verificar la seguridad del servidor

Para verificar que el servidor de Configuration Manager es seguro, escriba la siguiente URL en el explorador web: **https://<Nombre o dirección IP de servidor de Configuration Manager>:8443/cnc**.

Limitación: en **tomcat.keystore**, no puede haber más de un certificado de servidor.

Habilitar SSL con un certificado de cliente

Si el certificado que usa el servidor web de Configuration Manager lo genera una entidad de certificación (CA) conocida, es muy probable que el explorador web pueda validar el certificado sin tener que realizar más acciones.

Si el almacén de confianza del servidor no confía en el CA, importe el certificado de CA en el almacén de confianza del servidor.

El siguiente ejemplo demuestra cómo importar el certificado **hpcert** autofirmado en el almacén de confianza del servidor (cacerts).

Para importar un certificado en el almacén de confianza del servidor:

1. En el equipo cliente, localice el certificado **hpcert** y cámbielo de nombre por **hpcert.cer**.

   En el Explorador de Windows, el icono muestra que el archivo es un certificado de seguridad.

2. Haga doble clic en **hpcert.cer** para abrir el cuadro de diálogo Certificado de Internet Explorer e importe el archivo.

3 En el equipo del servidor, importe el certificado de CA en el almacén de confianza (cacerts) empleando la utilidad keytool con el siguiente comando:

```
keytool.exe -import -alias hp -file hp.cer -keystore ..\lib\security\cacerts
```

4 Modifique el archivo server.xml como se indica a continuación:

a Realice los cambios descritos en el paso 5 en la página 77.

b Inmediatamente después de realizarlos, agregue las siguientes líneas:

```
truststoreFile="../../java/lib/security/cacerts"
truststorePass="changeit" />
```

c Establezca clientAuth="true".

5 Compruebe la seguridad del servidor como se ha descrito en el paso 7 en la página 78.

Habilitar SSL sólo para autenticación

Esta tarea describe cómo configurar Configuration Manager para que admita sólo autenticación. Éste es el nivel de seguridad mínimo requerido para trabajar con Configuration Manager.

Para habilitar SSL para la autenticación:

1 Siga uno de los procedimientos para habilitar SSL en el equipo servidor, como se describe en "Habilitar SSL en el equipo servidor con un certificado autofirmado" en la página 76 hasta el paso 6 en la página 78 o "Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación" en la página 78 hasta el paso 5 en la página 80.

2 Escriba la siguiente URL en el explorador web: **http://<Nombre o dirección IP de servidor de Configuration Manager>: 8080/cnc**.

Habilitar la autenticación de certificado de cliente

Esta tarea describe cómo configurar Configuration Manager para aceptar la autenticación de certificados de cliente.

Para habilitar la autenticación de certificado de cliente:

1. Siga el procedimiento para habilitar SSL en el equipo servidor como se describe en "Habilitar SSL en el equipo servidor con un certificado autofirmado" en la página 76.
2. Abra el siguiente archivo: <**Directorio de instalación de Configuration Manager**>**\conf\lwssofmconf.xml.** Localice la sección que comienza por in-client certificate. Por ejemplo:

   ```
   <in-clientCertificate userIdentifierRetrieveField="SubjectDN"
   userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
   ```

   Active la funcionalidad del certificado de cliente quitando el carácter de comentario.
3. Extraiga el nombre de usuario del certificado siguiendo este procedimiento:
   a. El parámetro **userIdentifierRetrieveField** indica qué campo del certificado contiene el nombre de usuario. Las opciones son:
      - **SubjectDN**
      - **SubjectAlternativeName**

   b. El parámetro **userIdentifierRetrieveMode** indica si el nombre de usuario se compone de todo el contenido del campo relevante, o sólo de una parte del mismo. Las opciones son:
      - **EntireField**
      - **FieldPart**

   c. Si el valor de **userIdentifierRetrieveMode** es **FieldPart**, el parámetro **userIdentifierRetrieveFieldPart** indica la parte del campo relevante que constituye el nombre de usuario. El valor es una letra de código basada en una leyenda definida en el propio certificado.

4 Abra el siguiente archivo: **<Directorio de instalación de Configuration Manager>\conf\client-config.properties** y edite las siguientes propiedades:

- Cambie **bsf.server.url** para usar el protocolo HTTPS y cambie el puerto HTTPS al puerto descrito en "Habilitar SSL en el equipo servidor con un certificado autofirmado" en la página 76.
- Cambie **bsf.server.services.url** para usar el protocolo HTTP y cambie el puerto al puerto HTTP original.

Parámetros de cifrado

La siguiente tabla enumera los parámetros que se incluyen en el archivo **encryption.properties**, que se usa para el cifrado de la contraseña de la base de datos. Para obtener más información sobre cómo cifrar la contraseña de la base de datos, consulte "Cifrar la contraseña de la base de datos" en la página 75.

Parámetro	Descripción
cryptoSource	Indica la infraestructura que implanta el algoritmo de cifrado. Las opciones disponibles son: ➤ **lw.** Usa la implementación ligera de Bouncy Castle (opción predeterminada) ➤ **jce.** Java Cryptography Enhancement (infraestructura de criptografía Java estándar)
storageType	Indica el tipo de almacenamiento de claves. Actualmente, sólo se admite **archivo binario**.
binaryFileStorageName	Indica el lugar del archivo en el que se almacena la clave maestra.
cipherType	El tipo de cifrado. Actualmente, sólo se admite **symmetricBlockCipher**.

Parámetro	Descripción
engineName	El nombre del algoritmo de cifrado. Las siguientes opciones están disponibles: ➤ **AES.** American Encryption Standard. Este cifrado es compatible con FIPS 140-2. (opción predeterminada) ➤ **Blowfish** ➤ **DES** ➤ **3DES.** (compatible con FIPS 140-2) ➤ **Nulo**. Sin cifrado
keySize	El tamaño de la clave maestra. Dicho tamaño lo determina el algoritmo: ➤ **AES.** 128, 192 ó 256 (la opción predeterminada es 256) ➤ **Blowfish.** 0-400 ➤ **DES.** 56 ➤ **3DES.** 156
encodingMode	La codificación ASCII de los resultados del cifrado binario. Las siguientes opciones están disponibles: ➤ **Base64** (opción predeterminada) ➤ **Base64Url** ➤ **Hex**
algorithmModeName	El modo del algoritmo. Actualmente, sólo se admite **CBC**.
algorithmPaddingName	El algoritmo de relleno que se usa. Las siguientes opciones están disponibles: ➤ **PKCS7Padding** (opción predeterminada) ➤ **PKCS5Padding**
jceProviderName	El nombre del algoritmo de cifrado JCE. **Nota:** sólo es relevante cuando crytpSource es **jce**. Para **lw**, se usa engineName.