HP Universal CMDB Configuration Manager

para los sistemas operativos Windows y Linux

Versión del software: 9.20

Guía de implantación

Fecha de publicación del documento: Junio de 2011
Fecha de lanzamiento del software: Junio de 2011

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

SECCIÓN I: INSTALACIÓN Y CONFIGURACIÓN

SECCIÓN II: APÉNDICES

Sección I

Instalación y configuración

1

Descripción general

Este capítulo incluye:

Componentes

HP Universal CMDB Configuration Manager es un conjunto de varios componentes:

- **HP Universal CMDB Foundation**

  HP Universal CMDB Foundation (UCMDB Foundation) es una base de datos de gestión de configuraciones (CMDB) para que las organizaciones de TI de empresa documenten, almacenen, y gestionen definiciones de servicios empresariales y las relaciones con infraestructuras asociadas.

  UCMDB Foundation implementa un modelo de datos, gestión de flujos de atos y capacidades de modelado de datos, además de proporcionar análisis de impacto, seguimiento de cambios y capacidades de generación de informes, con el fin de transformar datos de CMDB en información comprensible y que se puede accionar que le ayuda a responder preguntas críticas y solucionar problemas empresariales.

➤ **HP Universal CMDB Configuration Manager**

HP Universal CMDB Configuration Manager (Configuration Manager) introduce una nueva topología basada en políticas y un control de la configuración del inventario. Se ha creado específicamente para gestores y propietarios de configuraciones, y permite a estos usuarios realizar análisis exhaustivos, además de los datos de CI y el contenido de topología disponible en UCMBD, o a través de éste. Configuration Manager proporciona a los gestores y usuarios de configuraciones las herramientas necesarias para configurar fácilmente las políticas de topología y de configuración de inventarios, así como para determinar automáticamente su nivel de cumplimiento de los estándares de la organización.

Configuration Manager se implementa como un servidor adicional basado en Tomcat y se comunica con el servidor de UCMDB mediante el exhaustivo UCMDB SDK.

➤ **HP Discovery and Dependency Mapping Advanced Edition**

Gracias a su gran cantidad de contenido que se actualiza constantemente, el software HP Discovery and Dependency Mapping Advanced Edition (DDMA) es el método preferido por UCMDB para adquirir y mantener los datos de las infraestructuras de TI.

➤ **HP Operations Orchestration**

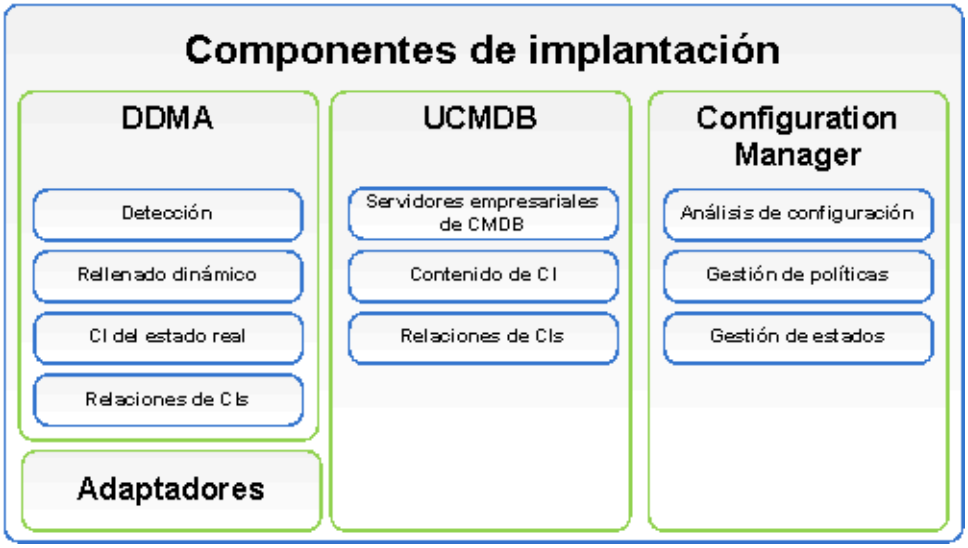
HP Operations Orchestration **(**OO) es una herramienta de creación y despliegue de flujos. Las intuitivas capacidades de arrastrar y conectar de OO Studio permiten a los usuarios diseñar, crear, compartir y personalizar flujos a personas con pocos conocimientos de programación, o ninguno. OO Studio admite la colaboración entre varios autores gracias a sus capacidades de control de versiones. Su potente depurador integrado permite probar los flujos en varios entornos, acelera el desarrollo de contenido y permite la validación de flujos, con el fin de lograr una ejecución estable y fiable.

OO Studio también permite a los usuarios desplegar flujos con suma facilidad. Además, les permite comparar y aumentar el nivel de los flujos en varios entornos (despliegue, pruebas, etapas y producción). Con Studio, los procesos estándar se pueden documentar y es posible generar documentación estructurada que soporte los requisitos que deben cumplirse.

➤ **Integración entre Configuration Manager y OO**

Configuration Manager brinda la posibilidad de ejecutar flujos de OO desde el propio marco de trabajo Configuration Manager. Hay dos métodos principales para ejecutar flujos de OO:

- ➤ **Integración de procesos**: permite abrir un RFC en una petición de un centro de servicios externo que alinea un CI específico con una política de configuración concreta.
- ➤ **Remedio de políticas**: permite desencadenar un flujo de OO que solucionar el problema de configuración. Por ejemplo, se puede asignar más memoria a un equipo host virtual.



Identificar el entorno

En esta guía se describe el proceso de despliegue de HP Universal CMDB Configuration Manager desde los distintos puntos de partida posibles:

Para Configuration Manager

➤ Si está instalada la versión 9.10 de Configuration Manager

Para obtener información sobre la actualización de Configuration Manager a la versión actual, consulte "Actualizar Configuration Manager" en la página 41.

➤ Si no está instalada la versión de Configuration Manager

Para obtener más información, consulte una de las siguientes fuentes:

- "Instalación de HP Universal CMDB Configuration Manager en plataformas Windows" en la página 19
- "Instalación de HP Universal CMDB Configuration Manager en plataformas Linux" en la página 45

Para UCMDB

➤ Si está instalada una versión de UCMDB anterior a la 9.03

Realice las siguientes operaciones:

➤ Actualice UCMDB a la versión 9.03. Para obtener más información, consulte la *Guía de implantación de HP Universal CMDB*, en formato PDF. El manual se puede descargar de www.hp.com/go/hpsoftwaresupport.

➤ Instale el paquete de actualización acumulada 2, que se puede obtener en el soporte de instalación de Configuration Manager o se puede descargar de www.hp.com/go/hpsoftwaresupport.

Para obtener información acerca de cómo configurar la preparación de la empresa, consulte "Configurar la base de datos o el esquema de usuario" en la página 20.

➤ Si está instalada la versión 9.03 de UCMDB

Instale el paquete de actualización acumulada 2, que se puede obtener en el soporte de instalación de Configuration Manager o se puede descargar de www.hp.com/go/hpsoftwaresupport.

Para obtener información acerca de cómo configurar la preparación de la empresa, consulte "Configurar la base de datos o el esquema de usuario" en la página 20.

➤ Si no está instalada ninguna versión de UCMDB

Realice una de las siguientes operaciones:

➤ Use Deployment Manager (sólo en sistemas Windows) para instalar UCMDB a la vez que Configuration Manager. Para obtener más información, consulte "Instalación de HP Universal CMDB Configuration Manager en plataformas Windows" en la página 19.

➤ Instale Configuration Manager en un sistema Linux siguiendo las instrucciones de "Instalación de HP Universal CMDB Configuration Manager en plataformas Linux" en la página 45.

Información general

En esta guía se tienen en cuenta los despliegues especiales de UCMDB que pueda tener en su entorno (por ejemplo, despliegue de alta disponibilidad) y proporciona los ajustes necesarios al procedimiento de despliegue de dichos despliegues.

Nota: se admite la instalación conjunta de UCMDB y Configuration Manager en el mismo servidor. Con fines de escalado en un entorno de producción, el software de HP recomienda instalar estos componentes en servidores independientes.

El uso de Configuration Manager requiere que UCMDB se configure con un modo de esquema consolidado y que se cree un estado en UCMDB (estado Autorizado). Estas configuraciones las realiza automáticamente el procedimiento de despliegue en ambas instalaciones (tanto si ya existe una instalación de UCMDB como si lo instala Deployment Manager).

Importante: si hace referencia a una instalación existente de UCMDB y su esquema no está consolidado, es posible que el paso de consolidación pueda tardar mucho tiempo (entre 20 y 60 minutos) en bases de datos densamente poblada (las que contienen más de 5 millones de CI).

Tenga en cuenta que si va a desplegar sólo Configuration Manager (es decir, si va a usar una instalación existente o actualizada de UCMDB), es preciso ejecutar el servidor de UCMDB para completar la instalación de Configuration Manager.

Matriz de soporte

Requisitos de sistema del servidor

CPU	Mínimo 4 core
Memoria (RAM)	Mínimo 4 GB
Plataforma	x64
Sistema operativo	Windows (64 bits) ➤ Windows 2003 Enterprise SP2 y R2 SP2 ➤ Windows 2008 Enterprise SP2 y R2 Linux ➤ Red Hat Enterprise Linux x86 (64 bits)
Base de datos	➤ Microsoft SQL Server 2005 SP2; 2005 con modo de compatibilidad 80 (ediciones Enterprise para todos) ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x, 11.x
Servidor web	➤ Microsoft IIS 7 ➤ Apache 2

HP Universal CMDB	➤ HP Universal CMDB, versión 9.03, con CUP 2 (instalación típica de CMDB) Para ver una lista completa de los requisitos del sistema, consulte la *Guía de implantación de HP Universal CMDB*, en formato PDF. **Nota:** ➤ Si el servidor de HP Universal CMDB se despliega junto con Configuration Manager, se requieren la edición Enterprise de Oracle y la opción de creación de particiones de Oracle. ➤ Si con anterioridad había instalado el servidor de HP Universal CMDB con la edición Standard de Oracle y tiene previsto añadir Configuration Manager a la instalación, antes es preciso que convierta la base de datos de la edición Standard en una base de datos de la edición Enterprise con la opción de creación de particiones habilitada.
LDAP (opcional)	➤ Active Directory ➤ SunONE 6.x
Tamaño mínimo recomendado del esquema de la base de datos (opcional)	2 GB

Requisitos del cliente

Sistema operativo	➤ Windows XP x86 (32 bits) ➤ Windows Vista x86 (32 y 64 bits) ➤ Windows 7 x86 (32 y 64 bits)
Explorador	➤ Microsoft Internet Explorer 7.0 y 8.0 ➤ Mozilla Firefox 3.x y 4
Complemento de explorador Flash Player	Flash Player 9, o posterior **Nota:** Flash Player se puede descargar de: http://www.adobe.com/products/flashplayer/.
Resolución de la pantalla	➤ 1024x768 (mínima) ➤ 1280x1024 (recomendada)
Calidad de color	Mínimo 16 bits

HP Operations Orchestration (opcional)

HP Operations Orchestration	➤ 7.51, 9.0

2

Instalación de HP Universal CMDB Configuration Manager en plataformas Windows

Importante: si desea conocer la versión más reciente de las instrucciones de instalación, lea las notas de la versión.

Este capítulo incluye:

Configuración previa a la instalación

Esta sección incluye:

Configurar la base de datos o el esquema de usuario

Nota: esta tarea se realiza automáticamente como parte del proceso de instalación de Configuration Manager; sin embargo, se puede realizar de forma manual si así lo desea.

Para trabajar con Configuration Manager, debe especificar un esquema de base de datos. Configuration Manager y UCMDB usan esquemas diferentes. Configuration Manager admite Microsoft SQL Server y Oracle Database Server. En esta tarea se describe cómo crear un esquema para Configuration Manager. Si va a instalar UCMDB, también tendrá que instalar una base de datos o esquema de usuario independientes. Para obtener más información, consulte la *Guía de implantación de HP Universal CMDB*, en formato PDF.

Nota: para conocer los requisitos de sistema de Microsoft SQL Server y Oracle Server, consulte "Requisitos de sistema del servidor" en la página 15.

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**: 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

Instalación de Configuration Manager en entornos UCMDB de alta disponibilidad

Para usar Configuration Manager en un entorno de alta disponibilidad de UCMDB, realice los siguientes pasos:

1 Apague el servidor de copia de seguridad (pasivo). Espere dos minutos después de apagarlo.

2 Instale la versión 9.20 de Configuration Manager.

a Use los datos del host equilibrador de carga.

b Instale Configuration Manager en un tercer servidor, no en los servidores de UCMDB.

3 Asegúrese de que UCMDB y Configuration Manager funcionan correctamente.

4 Inicie el servidor de copia de seguridad (pasivo) para proporcionar alta disponibilidad.

Nota: el modo de alta disponibilidad no se admite en la propia versión 9.20 de HP Universal CMDB Configuration Manager.

Instalar Configuration Manager

Deployment Manager puede instalar UCMDB, Configuration Manager y DDMA en distintas configuraciones (que se eligen y configuran en la página **Product Selection** del asistente de instalación):

- Instalar una instancia nueva de UCMDB.
- Instalar una instancia nueva de Configuration Manager y conectarla a una instancia nueva o existente de UCMDB.
- Integrar una instancia nueva de Configuration Manager en una instancia existente de OO.
- Instalar varias instancias de DDMA.

Nota:

- Deployment Manager proporciona la capacidad para instalar productos, componentes e integraciones en un equipo de destino. Sin embargo, no admite la desinstalación y modificación de productos ni la instalación de parches en productos instalados, por lo que estas operaciones se deben realizar manualmente.
- Una vez que se pulsa el botón **Next** en la página **Product Selection**, no es posible volver a dicha página y seleccionar de nuevo la configuración del despliegue. Si es preciso realizar cambios en dicha configuración, reinicie Deployment Manager.

Para instalar Configuration Manager:

1. Para iniciar la instalación, inserte el soporte de instalación de Configuration Manager en el equipo y busque el archivo **setup.exe**.
2. Haga doble clic en dicho archivo para ejecutar Deployment Manager.
3. Deshabilite el firewall de Windows en el equipo de destino mientras dure la instalación. Para obtener más información sobre el firewall, consulte el paso 6 de este procedimiento.

4 Acepte los términos del contrato de licencia para el usuario final y haga clic en **Next** para abrir la página **Product Selection**.

Nota: los términos del contrato de licencia se aplican a todos los productos seleccionados en la página **Product Selection** de Deployment Manager.

---

5 En la página **Product Selection**, seleccione los productos que se van a desplegar. Cuando haya finalizado, haga clic en **Next** para pasar a la página **Server Location**.

La página **Product Selection** le permite seleccionar los productos que desea instalar, así como especificar las opciones de configuración que se realizan durante el despliegue.

a Seleccione una opción de instalación de HP Universal CMDB Foundation.

Puede elegir cualquiera de las dos opciones de instalación siguientes:

➤ **Connect to an Existing Server**: al seleccionarla, esta opción conecta y configura Configuration Manager o Discovery and Dependency Mapping a una instancia existente de un servidor de UCMDB Foundation.

Nota: la versión de UCMDB de los servidores existentes debe ser la 9.03 con CUP 2, o cualquier versión posterior.

➤ **Install New Server**: al seleccionarla, esta opción instala, configura y conecta una instancia nueva de un servidor de UCMDB Foundation y configura y conecta Configuration Manager o DDMA a la instancia nueva del servidor de UCMDB Foundation.

b Active la casilla de **Configuration Manager** para instalar y configurar una instancia nueva de Configuration Manager.

Si lo desea, seleccione **Connect to an Existing HP Operation Orchestration instance**. Esta opción configura una integración entre Configuration Manager y Operations Orchestration rellenando Configuration Manager con los datos de conexión del servidor de OO.

c **HP Discovery and Dependency Mapping Advanced Edition.** Si se selecciona, esta opción instala y configura instancias nuevas de DDMA.

La opción **Number of DDMA instances** permite instalar varias instancias de DDMA. El número especificado en el campo de entrada indica el número de instancias de DDMA conectadas a una instancia individual del servidor de UCMDB.

Nota: Deployment Manager admite varios despliegues de instancias de DDMA en la misma DMZ. Deployment Manager admite un máximo de diez instancias de pruebas de detección en cada despliegue. Si se requieren más pruebas de detección, instálelas en varias fases de despliegue en grupos de diez.

---

6 Especifique la ubicación los servidores remotos y las credenciales de los equipos de destino en que se va a desplegar cada uno de los productos seleccionados en la página Ubicación de servidor. Cuando haya finalizado, haga clic en **Next** para pasar a la página **Connections**.

Opciones de despliegue

Seleccione una opción de despliegue para la ubicación de destino. Puede elegir cualquiera de las dos opciones siguientes:

- **Deploy on the local machine**: esta opción se usa cuando un producto se despliega en el mismo equipo que Deployment Manager. En ese caso, los campos de detalles del host remoto y de credenciales están deshabilitados.
- **Deploy on the following machine**: si se selecciona, es preciso especificar la dirección y el sistema operativo del host remoto. Las credenciales de usuario especificadas deben tener privilegios de administrador en el host remoto.

Nota: al especificar el nombre de host en el despliegue del producto, asegúrese de usar sólo letras (a-z), dígitos (0-9) y el signo de guión ('-').

La siguiente información es importante al especificar los detalles del equipo remoto:

- **WMI and SMB Protocols**: se usan para establecer conexión con el equipo remoto. Para que Deployment Manager se conecte correctamente con el equipo remoto, deben darse los siguientes requisitos.
  - **WMI Service**: el servicio WMI debe ejecutarse en el equipo remoto.
  - **Server Service**: para habilitar el protocolo SMB, el servicio de servidor debe ejecutarse en el equipo remoto.

➤ **Firewall de Windows**: el equipo remoto debe permitir conexiones de administración remotas. Ejecute el comando relevante en la consola del símbolo del sistema del equipo remoto:

Sistema operativo	Comando
Windows XP Windows Server 2003 Windows Server 2003 R2	netsh firewall set service RemoteAdmin enable
Windows Vista Windows 7 Windows Server 2008 Windows Server 2008 R2	netsh advfirewall firewall set rule group="windows management instrumentation (WMI)" new enable=Yes

Probar conexión

Haga clic en **Test Connection** para comprobar que tanto las credenciales como los detalles de la conexión son correctos y para analizar los recursos de los sistemas local y remoto.

Si el resultado de la prueba de conexión no es satisfactorio, Deployment Manager muestra un mensaje de error en el que se proporcionan detalles del error. Al pulsar el botón **Next**, se fuerza que se compruebe automáticamente la conexión de prueba.

La validación de los recursos del equipo se realiza en los siguientes elementos:

➤ **Plataforma de sistema operativo**: comprueba que el sistema operativo está certificado para el despliegue del producto.

➤ **Espacio en disco**: comprueba que hay suficiente espacio en el disco.

➤ **Memoria**: comprueba que hay suficiente memoria física.

➤ **Puertos**: comprueba que están disponibles los puertos requeridos.

La validación de los recursos que se realiza al probar la conexión varía en función de las matrices de productos compatibles.

Nota: si la prueba devuelve un error **Unknown**, compruebe que los siguientes servicios se ejecutan en el equipo host en que se va a realizar el despliegue:

- Servidor
- Instrumental de administración de Windows

Asegúrese de que Control de cuentas de usuario (UAC) está desactivado antes de hacer clic en **Next**.
Para obtener más información acerca de UAC, vaya a http://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx.

7 Configure las conexiones entre los productos seleccionados en la página **Connections**. Las opciones de conexión que aparecen en la página **Connections** reflejan los componentes seleccionados para su despliegue en la página **Product Selection**. Cuando haya finalizado, haga clic en **Next** para pasar a la página **Installation Configuration**.

- Integración de UCMDB con Configuration Manager

  Esta sección aparece al elegir instalar Configuration Manager con la opción **Connect to an Existing Server** y permite configurar la integración de Configuration Manager con UCMDB.

  Nota: para conectarse con una instancia existente de UCMDB es preciso instalar la versión 9.03 de UCMDB con CUP 2, o una versión posterior.

Especifique los siguientes detalles de UCMDB:

Campo	Definición
UCMDB Host Name/IP	Dirección de ubicación de despliegue de UCMDB. ➤ Si UCMDB está configurado en modo de alta disponibilidad, siga las instrucciones de "Instalación de Configuration Manager en entornos UCMDB de alta disponibilidad" en la página 21. ➤ Si UCMDB está instalado en el equipo local y Configuration Manager en un equipo remoto, el nombre de la instancia de UCMDB local debe ser el nombre de dominio completo, no localhost. ➤ Si UCMDB y Configuration Manager tienen nombres de dominio de DNS diferentes y se requiere integración con LW-SSO, debe especificar el nombre de dominio completo en el campo de entrada del host de UCMDB existente.
Protocol	Protocolo HTTP o HTTPS.
UCMDB HTTP(S) Port	Los valores predeterminados de los puertos HTTP o HTTPS son: **8080** para HTTP y **8443** para HTTPS.
Client Certificate File	Este campo aparece cuando se selecciona el protocolo HTTP. El archivo de certificado de UCMDB se debe colocar manualmente en el host de destino de Configuration Manager y se debe especificar la ruta de acceso completa al archivo, incluyendo el nombre de archivo, en el campo de entrada adyacente. Si UCMDB utiliza HTTPS, es preciso usar un intercambio de claves. Dicho intercambio no se valida en la prueba de conexión

Campo	Definición
Customer Name	El nombre de cliente predeterminado de UCMDB es **Default Client**. El valor del nombre de cliente se usa durante la configuración de la integración de UCMDB y Configuration Manager. La prueba de conexión no valida este valor. Si se especifica un valor incorrecto, el despliegue no se realizará.
JMX Port	El valor predeterminado es ***29601***.
UCMDB System User (JMX)	El usuario de sistema de UCMDB (JMX) se emplea para activar funciones de JMX como la creación de usuarios de integración de Configuration Manager y el despliegue del paquete de Configuration Manager. El valor predeterminado es **sysadmin**.
UCMDB System Password	La contraseña de usuario del sistema de UCMDB. El valor predeterminado es **sysadmin**.

Nota: Configuration Manager se configura con un repositorio de usuarios interno. Si desea usar un LDAP externo como repositorio de usuarios, debe configurar Configuration Manager para utilizarlo. Para obtener más información, consulte "Configuración del sistema" en la *Guía del usuario de HP Universal CMDB Configuration Manager.*

➤ Integración entre Configuration Manager y OO

Esta sección aparece al seleccionar la opción **Connect to an Existing HP Operation Orchestration instance** y permite configurar una integración de Configuration Manager con OO.

Especifique los siguientes detalles de OO:

Campo	Definición
OO Version	Las versiones válidas de OO son la 7.5 y la 9.0.
OO Host Name/IP	Host o dirección IP del equipo del servidor de OO.
OO Port Number	El número de puerto predeterminado es **8443**.
OO Username	El nombre de usuario predeterminado de OO es **admin**. El usuario se debe configurar como externo en OO.
OO Password	La contraseña predeterminada de OO es **admin**.

➤ Configuración de DDMA

Los siguientes campos aparecen al seleccionar la opción **Discovery and Dependency Mapping Advanced Edition instance** y permite configurar una conexión DDMA con UCMDB.

Especifique los siguientes detalles de DDMA:

Campo	Definición
Data Flow Probe Identifier	El valor predeterminado es el nombre de host del equipo de DDMA y este campo se rellena automáticamente. Este valor se puede cambiar.
Use Default Domain	De manera predeterminada esta opción está seleccionada y afecta al valor del nombre de dominio. Si desactiva esta casilla, puede cambiar el nombre predeterminado por otro valor.
Domain Name	El valor predeterminado se establece en **DefaultDomain**. Para habilitar este campo, desactive la casilla **Use Default Domain**.

Campo	Definición
Initial Heap Size in MB	El tamaño inicial de la memoria asignado al JVM del DDMA. El valor predeterminado es 256 MB.
Maximum Heap Size in MB	El tamaño máximo de la memoria asignado al JVM. El valor predeterminado es 512 MB.

8 Especifique los detalles del directorio de destino de los despliegues de los productos que seleccionó en la página **Installation Configuration**. Cuando haya finalizado, haga clic en **Next** para pasar a la página **Database Configuration**.

Se proporciona una ruta de acceso al directorio predeterminado de cada uno de los productos seleccionados. Si realiza el despliegue en un equipo local, podrá usar una opción para seleccionar una ruta de directorio distinta. Si la instalación la realiza en un equipo remoto, esta opción estará deshabilitada.

Nota: el directorio de instalación no debe contener espacios en su nombre y sólo puede usar letras (a-z), dígitos (0-9) y el signo de guión ('-').

---

9 Configure la conexión y el esquema de la base de datos de cada uno de los productos en la página **Database Configuration**. Cuando haya finalizado, haga clic en **Next** para pasar a la página **Ports Configuration**.

Puede configurar las siguientes bases de datos (esquemas):

- Esquema de UCMDB-CM
- Esquema de UCMDB

➤ Esquema de historial de UCMDB

Campo	Definición
Database Host Name/IP	La dirección de la ubicación del servidor de bases de datos.
Port	MSSQL y Oracle utilizan puertos predeterminados diferentes. El puerto predeterminado de la base de datos de Oracle es el 1521, mientras que el de la base de datos de MSSQL es el 1433.
SID (Oracle)	Nombre de la instancia de la base de datos de Oracle.
Admin Username (Oracle)	Escriba el nombre de usuario del administrador de Oracle según el servidor de Oracle.
Admin Password (Oracle)	Escriba la contraseña del administrador de Oracle según el servidor de Oracle.
Test Connection	Pruebe la conexión con el host de DB de destino utilizando las credenciales proporcionadas.
Schema Name (Oracle)	Escriba el nombre del esquema.
Schema Password (Oracle)	Escriba la contraseña del esquema. Este campo aparece al crear esquemas.
Default Tablespace (Oracle)	Escriba el nombre del espacio de tabla predeterminado.
Temporary Tablespace (Oracle)	Escriba el nombre del espacio de tabla temporal.
Database Name (MSSQL)	Escriba el nombre del esquema de base de datos que se va a usar o crear en el servidor de MSSQL.
Database Username (MSSQL)	Escriba el nombre de usuario del administrador de MSSQL según el servidor de MSSQL.
Database Password (MSSQL)	Escriba la contraseña del administrador de MSSQL según el servidor de MSSQL.

Nota:

- Si el espacio de tablas de UCMDB está lleno, el despliegue del producto se realizará correctamente, pero ni los productos ni los componentes funcionarán de forma satisfactoria
- No se admite la creación de un esquema UCMDB y la conexión de éste con un esquema del historial de UCMDB existente.
- Por motivos de seguridad, no se admite el uso de la autenticación NTLM al configurar esquemas de UCMDB con una base de datos MSSQL cuando UCMDB se instala de forma remota. Si se requiere autenticación NTLM, despliegue UCMDB localmente.

Modo de esquema

Configuration Manager requiere que UCMDB se configure con un modo de esquema consolidado y que se cree un estado de UCMDB.

Si hace referencia a una instalación existente de UCMDB y su esquema no está ya consolidado, es posible que el paso de consolidación automática pueda tardar mucho tiempo (entre 20 y 60 minutos) en bases de datos densamente pobladas (las que contienen más de 5 millones de CI).

Nota: las conexiones NTLM de Oracle Real Application Cluster (RAC) y SQL Server no se admiten como parte de esta instalación. Si dichas conexiones son obligatorias, en primer lugar instale Configuration Manager con una conexión de base de datos simple y cuando el proceso de instalación finalice, cambie la conexión desde la configuración del producto específico. Para ello, modifique el archivo **database.properties** en función de las especificaciones de la base de datos. Para obtener más información, consulte "Configuración avanzada de bases de datos (para Configuration Manager)" en la página 34.

Modo de configuración de bases de datos

Configuration Manager y UCMDB deben usar esquemas diferentes.

Configuration Manager permite al usuario configurar todas las bases de datos de un servidor de bases de datos Oracle o MSSQL.

Tipos de configuración

Puede conectarse con un esquema existente o crear un esquema. Si se conecta con un esquema existente, se anula su contenido.

Configuración de bases de datos

Este paso lo realiza Deployment Manager automáticamente. Para realizar este paso manualmente, consulte "Configurar la base de datos o el esquema de usuario" en la página 20.

Configuración avanzada de bases de datos (para Configuration Manager)

Las conexiones de las bases de datos se deben configurar y asociar con conexiones de URL estándar. Si se requieren características 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 para bases de datos tanto de Oracle como de Microsoft SQL Server, Se admiten las características de todos los controladores nativos, siempre que se puedan configurar con la dirección URL de la base de datos. La dirección URL se encuentra en el archivo **database.properties**.

Cuando finaliza el Asistente de Deployment Manager, se pueden realizar configuraciones adicionales tanto de los esquemas como de las bases de datos.

Campos de configuración de bases de datos

Dos tipos de bases de datos disponibles: Oracle y MSSQL. Los campos de entrada cambian en función del tipo de base de datos seleccionado.

10 Especifique los puertos de conexión de Configuration Manager en la página **Ports Configuration**. Cuando haya finalizado, haga clic en **Next** para pasar a la página **Users Configuration**.

Configuration Manager proporciona una configuración predeterminada de fábrica de los puertos que aparece en los campos de entrada de la página del Asistente de configuración de puertos.

Si un número de puerto entra en conflicto con una instalación existente, póngase en contacto con un gestor de TI antes de cambiarlo.

Campo	Definición
Application HTTP Port	8180
JMX HTTP Port	39900
Tomcat Port	8005
AJP Port	8009 (Apache Java Protocol)
Application HTTPS Port	8143
JMX Remote Port	39600

Haga clic en el botón **Revert to Default Values** para restablecer los puertos a los valores predeterminados que proporciona Deployment Manager.

11 Cree los siguientes usuarios en la página **Users Configuration**:

- Instancia de usuario de inicio de sesión inicial de UCMDB-CM con permisos de administrador.
- Usuario de integración en UCMDB: Configuration Manager crea usuarios de integración a petición en UCMDB con el fin de proporcionar soporte a la integración entre estos dos productos.

Cuando haya finalizado, haga clic en **Next** para pasar a la página **Security Configuration**.

12 Active LW-SSO global en una instancia nueva de UCMDB y Configuration Manager en la página **Configuration** de la seguridad. LW-SSO sólo se configura en las instancias nuevas de Configuration Manager o UCMBD, en función de lo que se haya seleccionado en la página **Product Selection**. Cuando haya finalizado, haga clic en **Next** para pasar a la página **Summary**.

LW-SSO es un marco de trabajo modular que se usa para validar distintos tipos de tokens de seguridad y autenticación (como LW-SSO y SAML2). LW-SSO se usa para conectar y usar información autenticada de distintos entornos en contextos de seguridad de aplicaciones dentro de un marco de trabajo de la seguridad o de la aplicación.

La configuración de LW-SSO varía en función de los componentes de producto que se seleccionen.

Si Configuration Manager se conecta con una instancia existente de UCMDB o de OO, LW-SSO sólo se configura en Configuration Manager. La cadena de LW-SSO se debe extraer de UCMDB o de OO, y se introduce en el campo de entrada Cadena de LW-SSO. Al establecer conexión con UCMDB y OO, compruebe que las cadenas de LW-SSO definidas en las instancias de UCMDB y OO coinciden.

Si se conecta una instancia nueva de Configuration Manager con una instancia existente de UCMDB, use el nombre de dominio completo como nombre de host de UCMDB.

Para extraer la cadena de LW-SSO de UCMDB:

a Abra UCMDB y seleccione **Administración** > **Administrador de configuración de infraestructura**.

b En la columna **Nombre**, seleccione el campo Cadena init de LW-SSO y haga doble clic en él.

c Copie la cadena del campo de entrada Valor actual.

d Pegue el valor en el campo de entrada Cadena de LW-SSO de la página **Security Configuration**.

Al conectar Configuration Manager a una instancia nueva de UCMDB, LW-SSO se configura automáticamente tanto en UCMDB como en Configuration Manager.

13 Revise los ajustes de instalación y configuración en la página **Summary**. Cuando haya finalizado, haga clic en **Next** para pasar a la página **Validation**.

La página **Summary** centraliza todos los detalles de la configuración y la entrada del usuario. Si es necesario, puede revisar el contenido del resumen haciendo clic en el botón **Back** de las páginas hasta llegar a la página que desee y, a continuación, ajustar la configuración del despliegue. Vuelva a la página **Summary** haciendo clic en **Next** tantas veces como sea necesario.

14 A continuación, Deployment Manager ejecuta una serie de acciones para comprobar que los equipos remotos tienen suficientes recursos del sistema, que los datos introducidos por el usuario son correctos y para validar los ajustes de la configuración de la base de datos. Estas validaciones indican si la configuración de las definiciones del usuario se ajustan a las limitaciones conocidas del entorno. El proceso de validación comienza automáticamente o, si vuelve de una página anterior de Deployment Manager y ha realizado cambios en la configuración, haga clic en **Run Validation** para comenzar el proceso de validación. Cuando haya finalizado, haga clic en **Deploy** para pasar a la página **Deployment**.

15 La página **Deployment** refleja el estado del proceso de despliegue mientras esté se está llevando a cabo. Dicho proceso incluye las instalaciones de los productos, los procedimientos de inicio y sus integraciones y conexiones con otros productos.

El proceso de despliegue finaliza una vez que todos los productos se inician correctamente.

Haga clic en **Details** para ver los detalles del progreso de despliegue, incluyendo los pasos que realiza Deployment Manager en el despliegue de todos los productos seleccionados.

Haga clic en **Cancel** para cancelar correctamente el despliegue, es decir, permitiendo que la acción activa del despliegue finalice antes de detener el despliegue.

Haga clic en **Abort** (disponible únicamente después de hacer clic en **Cancel**) para terminar correctamente la acción activa y el despliegue. La anulación del despliegue puede provocar que los productos estén en un estado indeterminado.

Validaciones

La siguiente tabla muestra una lista de las validaciones que realiza Deployment Manager.

Validación	Mensaje de error	Descripción
Comprobar credenciales de inicio de sesión	Credentials verification failed	Las credenciales de usuario proporcionadas no son correctas.
		No se pudo establecer conexión.
Comprobar la compatibilidad del sistema operativo	Target operating system platform is <Platform> Product <Product Name> supports the following platforms <Platform>	El sistema operativo de destino real no se corresponde con la lista de sistemas operativos certificados para el producto.
Comprobar la memoria	The assigned memory(<Memory> MB) exceeds the available memory (<Memory> MB) on <Target>	El equipo de destino no tiene suficiente memoria para todos los productos asignados
	<Memory> MB of memory are verified to be available on <Target Machine>	La validación se realizó correctamente.
Comprobar el espacio del disco	Assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target>	El equipo de destino no tiene suficiente espacio en disco para todos los productos asignados.
	<Memory> MB of disk space are verified to be available on drive <Target>	La validación se realizó correctamente.

Validación	Mensaje de error	Descripción
Comprobar que se han proporcionado todas las propiedades obligatorias	Missing the target storage device for the product: <Target>	No se ha definido el directorio de instalación del producto.
Comprobar que se ha definido un equipo de despliegue	No deployment machine is defined for <Product Name>	El producto no se ha configurado para desplegarlo en ningún equipo.
Comprobar credenciales de inicio de sesión	Credentials verification failed	Las credenciales de inicio de sesión no son correctas.
Comprobar que el UAC está deshabilitado	The UAC is enabled	El UAC está habilitado en el equipo de destino.
Comprobar los puertos libres	The required port number <Port> is already in use on <Target>	El puerto requerido en el equipo de destino ya está en uso.
Comprobar que el dispositivo de almacenamiento de destino existe	The target storage device <Device> does not exist on <Target>	El dispositivo de almacenamiento de destino seleccionado no existe en el equipo de destino.
Validar la existencia de un esquema	Schema <Name> does not exist/ already exist	El esquema del equipo de destino existe/no existe.
Validar la existencia de permisos del esquema	Validate <Permissions> schema tables user permissions existence	El usuario de DB no tiene suficientes permisos
Validar la existencia de tablas de esquema	Schema Tables <Tables> on the database: <Tables> already exist	Las tablas de esquema de la base de datos ya existen.
Validar la existencia de permisos de usuario de las tablas del esquema	The database user does not have the correct permissions	El usuario de la base de datos no tiene los permisos correctos.

Validación	Mensaje de error	Descripción
Comprobar la conexión UCMDB	Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error>	Error en la conexión de prueba a UCMDB con los ajustes de conexión dados.
	Existing UCMDB version must be 9.03 with CUP 2 or later.	La versión de UCMDB existente debe ser la 9.03 con CUP 2, o posterior.
Comprobar la conexión de DB	The host name/IP address validation failed	No se puede acceder al nombre de host/dirección IP de la base de datos especificados.
	The username or password validation failed	Las credenciales de usuario especificadas no son válidas.
	The port validation failed	No se puede acceder al puerto de la base de datos especificado.
	The SID validation failed	El SID de la base de datos especificado no existe en DB.
Comprobación de la instalación	The product is already installed	El producto ya está instalado en el host de destino

Actualizar Configuration Manager

El procedimiento de actualización comprueba y valida automáticamente los siguientes elementos antes de empezar:

- Que hay una conexión activa con el servidor de UCMDB.
- Que el parche de CUP 2 se ha instalado para UCMDB.
- Que el puerto de JMX es correcto.

Si alguno de estos elementos no se ha instalado o configurado correctamente, verá un mensaje de error que le informa de ello. Puede solucionar el problema indicado y, a continuación, realizar la actualización.

- Si se produce un error en la actualización porque no puede conectarse a UCMDB, compruebe que el servidor de UCMDB está en funcionamiento.
- Si se produce un error en la actualización debido a que no se ha instalado el parche, instale CUP 2 según las instrucciones que se encuentran en: http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045
- Si se produce un error en la actualización debido a un puerto de JMX de UCMDB incorrecto, seleccione el puerto de JMX correcto. Para ello, cambie la propiedad ucmdb.jmx.port en el archivo **upgrade.properties**, que se encuentra en la carpeta **<directorio de instalación de Configuration Manager>\utilities\Upgrade**.

Para realizar la actualización, siga estos pasos:

Nota: asegúrese de que el servidor de UCMDB está en funcionamiento al comenzar el proceso de actualización.

---

1. Realice una copia de seguridad de los esquemas de Configuration Manager y de UCMDB.
2. Busque el archivo **setup-win64.msi** en la subcarpeta Windows del soporte de instalación de Configuration Manager.
3. Haga doble clic en dicho archivo para ejecutar el Asistente de instalación de Configuration Manager.
4. Haga clic en **Next** para abrir la página del contrato de licencia para el usuario final.
5. Acepte los términos de la licencia y haga clic en **Next** para abrir la página **Customer Information**.
6. Introduzca sus datos y haga clic en **Next** para abrir la página **Setup Type**.
7. Seleccione la carpeta en la que se va a instalar Configuration Manager. Asegúrese de seleccionar una ubicación que no sea la que se utilizó para la versión anterior.

   De manera predeterminada, Configuration Manager se instala en el siguiente directorio: **c:\hp\cnc920**. Haga clic en **Next** para aceptar la ubicación predeterminada, o bien haga clic en **Browse** para seleccionar otra ubicación y, a continuación, haga clic en **Next**.

   Nota: el nombre del directorio de instalación no debe contener espacios.

   ---

8. Haga clic en **Next** para confirmar y comenzar la instalación.

   Cuando el Asistente de instalación finaliza, el Asistente de Post-instalación de Configuration Managerse inicia automáticamente.
9. Haga clic en **Next** hasta que se le pregunte si desea realizar una instalación nueva de Configuration Manager o desea realizar una actualización.
10. Seleccione **Upgrade** y haga clic en **Next**.

11 Cuando la instalación finalice, compruebe el archivo **post_installation.log** (que se encuentra en la carpeta **<directorio de instalación de Configuration Manager/tmp/log**) para asegurarse de que la instalación ha finalizado sin errores.

Si se produce un error durante el proceso de actualización, aparece un mensaje, lo que le permite cerrar el asistente. Si esto ocurre, póngase en contacto con el soporte técnico de HP.

12 Inicie el servicio de Configuration Manager.

Nota: después de realizar la actualización, es preciso volver a configurar SSL. Para obtener más información, consulte "Sistema de protección" en la página 93.

3

Instalación de HP Universal CMDB Configuration Manager en plataformas Linux

Importante: si desea conocer la versión más reciente de las instrucciones de instalación, lea las notas de la versión.

Este capítulo incluye:

Configuración previa a la instalación

Esta sección también incluye:

Requisitos previos

- Un mínimo de 400 MB de espacio libre en el disco
- Se recomienda la pantalla activa

Obtención del archivo setup.bin

El archivo de instalación de Linux (**setup.bin**) se encuentra en el soporte de instalación o en la imagen ISO que puede descargar del sitio web de HP. Acceda al archivo de una de las siguientes formas:

➤ Monte un DVD en la máquina Linux:

```
$ mkdir -p /mnt/cdrom
$ mount /dev/cdrom /mnt/cdrom
```

➤ Monte una imagen ISO como un dispositivo de bloqueo de bucle invertido:

```
$ mkdir -p /mnt/cdrom
$ mount -o loop cnc-<version>.iso /mnt/cdrom
```

➤ Copie el archivo **setup.bin** a una ubicación temporal de la máquina Linux.

Instalación de 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 tiene una pantalla activa, el Asistente de post-instalación aparece en la interfaz de usuario; en caso contrario, la información del asistente aparece en el modo de consola.

Nota: los pasos de esta guía se describen para el modo de consola; sin embargo, aparecen pasos equivalente si se usa el asistente de la interfaz de usuario.

Para instalar Configuration Manager:

1 Para instalar Configuration Manager en su posición actual, genere el siguiente comando:

```
chmod 755 setup.bin
$ /path/to/installation/kit/setup.bin
```

2 Se muestra un contrato de licencia de usuario final (CLUF) que debe aceptar. Desplácese hacia abajo haciendo clic en la barra espaciadora varias veces hasta que llegue al final del CLUF. Para aceptarlo y continuar con la instalación, escriba **Yes** y pulse **Entrar**.

HP Universal CMDB Configuration Manager se instala en la posición actual de la subcarpeta **cnc**.

Página de bienvenida

```
<============================>
Welcome
<============================>
Welcome to the HP Universal CMDB Configuration Manager
post installation wizard.
Enter [<C>ancel] [Ne<x>t]>
```

Pulse **Entrar** para pasar a la página siguiente.

Selección de proveedor de bases de datos

```
<============================>
Database Connection Configuration
<============================>
-------
Vendor:
-------
  ->1 - Oracle
    2 - Microsoft
Enter index number from 1 to 2 OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Pulse **Entrar** para seleccionar Oracle o escriba **2** y pulse **Entrar** para seleccionar Microsoft.

Nombre de host de base de datos

```
-------------
Set Hostname:
-------------
        Hostname: = "localhost"
Input the new Hostname: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Escriba el nombre de host de la base de datos y pulse **Entrar**. El valor predeterminado del nombre de host que se proporciona es **localhost**.

Puerto de base de datos

```
---------
Set Port:
---------
        Port: = "1521"
Input the new Port: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

El puerto predeterminado de Oracle es el 1521, mientras que el de es el 1433. Si desea usar otro número de puerto, escríbalo aquí y pulse **Entrar**.

Nombre de SID/DB

```
-----------
Set SID/DB:
-----------
        SID/DB: = "orcl"
Input the new SID/DB: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Para Oracle, este campo especifica el SID de la base de datos; en Microsoft, este campo especifica el nombre de la base de datos. Escriba un valor válido y pulse **Entrar**.

Nombre de usuario/esquema y contraseña

```
-------------
Set Username:
-------------
Input the Username: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Escriba el nombre de usuario de la base de datos y pulse **Entrar**.

```
Input the Password: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Escriba la contraseña del esquema y pulse **Entrar**.

Prueba de la conexión de la base de datos

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pulse **Entrar** para probar la conexión de la base de datos.

Dado que este asistente intenta crear tablas en el esquema de la base de datos, se recomienda encarecidamente probar la conexión de la base de datos. Si no desea probar la conexión, escriba **No** y pulse **Entrar**.

Cuando la prueba de conexión de la base de datos finaliza correctamente, se muestra el siguiente mensaje:

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pulse **Entrar** para continuar. Si se produce algún error en la prueba de conexión, se muestra un mensaje de error y se le solicitará que vuelva a realizar la prueba. Solucione el problema de conexión, vuelva a realizar la prueba y prosiga la instalación.

Nombre de host del servidor de aplicaciones

```
<============================>
Application Server Configuration
<============================>
Hostname:
----
Set
----
         = "myucmdbcmhost.mydomain"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

El valor predeterminado del nombre de host es el nombre de host real del equipo. Si va a realizar la instalación detrás de un equilibrador de carga o un proxy inverso, escriba aquí el nombre externo.

Personalización de los puertos del servidor de aplicaciones

```
-------------------
Select Customize ports
-------------------
        Customize ports = "No"
Choose [<Y>es]/[<N>o] for Customize ports OR [<C>ancel] [<B>ack]
[Ne<x>t]>
```

Si desea usar los puertos predeterminados en Configuration Manager, pulse **Entrar**. Si desea usar puertos personalizados, escriba **Yes** y pulse **Entrar**.
Los números de puerto predeterminados son:

Nombre de puerto	Número de puerto
HTTP	8180
HTTPS	8443
Gestión de Tomcat	8005
AJP	8009
JMX HTTP	39900
JMX RMI	39600

Si elige personalizar los puertos, en todos los puertos que se muestran arriba se le solicitará que introduzca un valor. Escriba el valor nuevo y pulse **Entrar** en cada uno de ellos:

```
HTTP port:
----
Set
----
         = "8180"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
HTTPS port:
----
Set
----
         = "8443"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
Tomcat port:
----
Set
----
         = "8005"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
AJP port:
----
Set
----
         = "8009"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX HTTP port:
----
Set
----
         = "39900"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX remote port:
----
Set
----
         = "39600"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Usuario administrativo inicial

```
<============================>
Users Credentials
<============================>
Initial Administrative User
Admin username:
----
Set
----
Input the  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Se crea un usuario administrativo inicial para que sea el administrador o superusuario del sistema para la conexión inicial. Escriba el nombre de usuario de administrador que desea usar y pulse **Entrar**.

```
Admin password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Escriba la contraseña del usuario administrador y pulse **Entrar**.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Para confirmar, vuelva a escribir la contraseña del usuario administrador y pulse **Entrar**.

Usuario de integración

```
Platform Integration User
Integration username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Seleccione el nombre de usuario de integración de UCMDB. Este usuario se crea en UCMDB durante este proceso de postinstalación. HP recomienda utilizar un nombre de usuario que deje claro que su objetivo es la integración (por ejemplo, cm_integration). Escriba el nombre de usuario seleccionado y pulse **Entrar**.

```
Integration password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Escriba la contraseña del usuario de integración y pulse **Entrar**.

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Para confirmar, vuelva a escribir la contraseña del usuario de integración y pulse **Entrar**.

Nombre de host del servidor de HP Universal CMDB

```
<============================>
HP UCMDB Connection Configuration
<============================>
Hostname:
----
Set
----
         = "localhost"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

Escriba el nombre de host del servidor UCMDB y pulse **Entrar**. Es probable que el nombre no sea el mismo que el del localhost predeterminado, ya que no se recomienda instalar UCMDB y Configuration Manager en el mismo equipo en los entornos de producción.

Puerto del servidor de HP Universal CMDB

```
Port:
----
Set
----
         = "8080"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pulse **Entrar** para aceptar el número de puerto predeterminado de 8080 para el servidor UCMDB o escriba un número de puerto y pulse **Entrar**.

Protocolo del servidor de HP Universal CMDB

```
Protocol:
  ->1 - HTTP
    2 - HTTPS
Enter index number from 1 to 2 OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pulse **Entrar** para usar HTTP o escriba 2 y pulse **Entrar** para usar HTTPS.

Nota: si selecciona HTTPS, tendrá que intercambiar claves con UCMDB. Para obtener más información, consulte "Sistema de protección" en la página 93. Este procedimiento configura HTTPS con un certificado autofirmado no seguro.

Cliente del servidor de HP Universal CMDB

```
Customer:
----
Set
----
         = "Default Client"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pulse **Entrar** para aceptar el nombre de cliente predeterminado para el servidor UCMDB o escriba un nombre de cliente y pulse **Entrar**.

Credenciales de Sysadmin del servidor de HP Universal CMDB

```
Administrative username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Introduzca el nombre de usuario sysadmin del servidor de UCMDB. Éste es el usuario que puede ejecutar métodos de JMX en el servidor de UCMDB. Éste es un usuario preexistente y no se crea durante la instalación. Obtenga las credenciales del usuario sysadmin de su administrador del servidor de UCMDB.

```
Administrative password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Escriba la contraseña de host del servidor UCMDB y pulse **Entrar**.

Comprobación de la conexión del servidor de HP Universal CMDB

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pulse **Entrar** para probar la conexión del servidor de UCMDB. Dado que este asistente intenta desplegar paquetes y configurar el servidor UCMDB, se recomienda encarecidamente que pruebe la conexión del servidor. Si no desea probar la conexión, escriba **No** y pulse **Entrar**.

Cuando la prueba de conexión del servidor finaliza correctamente, se muestra el siguiente mensaje:

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

Pulse **Entrar** para continuar. Si se produce un error en la prueba de conexión, se muestra un mensaje de error y se le solicitará que vuelva a ejecutar la prueba. Solucione el problema de conexión, vuelva a realizar la prueba y continúe con la instalación.

Resumen

El asistente muestra un resumen de todas las selecciones realizadas antes de ejecutarlas:

```
<============================>
Post Installation Actions Summary
<============================>
Post installation actions summary
Users
-----
HP Universal CMDB Configuration Management admin username: admin
HP Universal CMDB Platform integration username: cm_integration

Database
--------
Vendor: Oracle
Host: mydbhost.mydomain
Port: 1521
SID/DB: orcl
Encrypt password? Yes
Create schema objects? Yes

Application Server
------------------
hostname: myucmdbcmhost.mydomain
HTTP: 8180
HTTPS: 8443
Tomcat management: 8005
AJP: 8009
JMX HTTP: 39900
JMX remote: 39600
Debug: 7878

Windows Service
---------------
Create service? No

HP Universal CMDB Platform
-----
URL: http://myucmdb.mydomain:8080
Sysadmin username: sysadmin
Customer: Default Client

Enter [<C>ancel] [Back<b>] [Ne<x>t]>
```

Pulse **Entrar** para continuar con la fase de configuración. Mientras se está realizando la configuración aparece una barra de progreso. El asistente realiza las siguientes tareas:

1. Crea las tablas y los objetos de la base de datos.
2. Rellena la base de datos con los valores inicial y predeterminado
3. Crea el usuario administrativo inicial.
4. Crea el usuario de integración en el servidor de UCMDB.
5. Consolida el servidor de UCMDB.
6. Crea el estado autorizado en el servidor de UCMDB.
7. Despliega paquetes de Configuration Manager en el servidor de UCMDB.

Al finalizar la configuración, aparece el siguiente mensaje:

```
<============================>
Finish
<============================>
Post installation configuration has completed.
Enter [Finish<f>]>
```

Pulse **Entrar** para salir del asistente.

Opción de instalación silenciosa

Configuration Manager se puede instalar en modo silencioso. Así sólo se extraen los archivos del paquete de instalación, pero no se realiza ningún tipo de configuración después de la instalación. Para ejecutar la instalación en modo silencioso, ejecute el siguiente comando:

```
$ /path/to/installation/kit/setup.bin –silent
```

Ejecución del servidor de aplicaciones de Configuration Manager

Para ejecutar Configuration Manager, ejecute los siguientes comandos:

```
$ cd /path/to/installation/location
$ ./start-server-0.sh
```

Puede crear un script en el directorio **/etc/init.d** que inicie Configuration Manager automáticamente al iniciarse el equipo.

4

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 "Gestión 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 sobre los requisitos mínimos para ver correctamente Configuration Manager, consulte "Matriz de soporte" en la página 15.

Para obtener más información sobre cómo acceder a Configuration Manager de forma segura, consulte "Sistema de protección" en la página 93.

Para obtener información sobre cómo solucionar problemas de acceso a Configuration Manager, consulte "Solución de problemas" en la página 129.

Conectar a Configuration Manager

1. 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>/cnc, donde <**nombre o dirección IP del servidor**>.<**nombre de dominio**> representa el nombre de dominio completo (FQDN) del servidor de Configuration Manager y <**puerto**> representa el puerto seleccionado en la instalación.
2. Escriba el nombre de usuario y la contraseña que definió en el Asistente post-instalación de Configuration Manager.
3. Pulse **Conectar**. Tras iniciar sesión, el nombre de usuario aparece en la parte superior derecha de la pantalla.
4. (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 "Gestión 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 de 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.

5

Casos de usos adicionales

Este capítulo incluye:

Mover una instalación de Configuration Manager entre equipos

Este procedimiento se debe usar cuando se desea transferir una instalación de Configuration Manager de un equipo a otro manteniendo intacto el esquema de base de datos y estableciendo una conexión con el mismo servidor de UCMDB.

1. En la carpeta <**directorio de instalación de Configuration Manager**>**cnc****bin**, ejecute el siguiente comando: edit-server-0.bat.
2. Registre todos los parámetros que encuentre, incluso los puertos (por ejemplo, el puerto de JMX).
3. Detenga el servidor de Configuration Manager en el equipo de origen. (Si el equipo de origen está instalado en un sistema Windows, es preciso detener el servicio de Configuration Manager).

4 Instale Configuration Manager en el equipo de destino:

- ➤ En Windows: ejecute el archivo **setup-win64.msi** (que se encuentra en la carpeta **windows** del soporte de instalación).
- ➤ En Linux: siga las instrucciones que encontrará en "Instalación de Configuration Manager" en la página 46.

5 Cancele el Asistente post-instalación cuando comience.

6 Copie todos los archivos del directorio de instalación anterior del equipo de origen a la ubicación de la nueva instalación en el equipo de destino.

7 En el equipo de destino, cambie el nombre de host por el nombre de dicho equipo en **client-config.properties** y **resources.properties** (que se encuentran en la carpeta **conf**).

Nota: si el equipo de destino no está en el mismo dominio que el de origen, modifique también la referencia del dominio anterior, operación que debe realizar en el archivo **lwssofmconf.xml**.

---

8 En el equipo de destino, ejecute el archivo **bin/create-windows-service.bat** para crear el servicio de Windows. Configure el indicador **-h** para ver las opciones disponibles y use los parámetros registrados del servicio del equipo de origen (los que registró en el paso 2) como sea necesario. Para el parámetro de nombre de dominio, use server-0. Si se usan los valores predeterminados, el comando será:

c:\HP\cnc920\bin>create-windows-service.bat -j 39900 -n server-0 -r 39600

9 Inicie el servidor de Configuration Manager en el equipo de destino.

Cambiar los números de puerto después de la instalación

1. Detenga el servidor de Configuration Manager.
2. Realice una copia de seguridad del contenido de la carpeta <**directorio de instalación de Configuration Manager**>**servers****server-0**.
3. Elimine la carpeta <**directorio de instalación de Configuration Manager**>**servers****server-0**.
4. Ejecute el archivo de comandos **create-node.bat** con el indicador **-h** para ver las opciones disponibles. Pase todos los números de puerto necesarios a la utilidad.
5. En el equipo de destino, cambie el puerto por el nuevo número de puerto HTTP en **client-config.properties** y **resources.properties** (que se encuentran en la carpeta **conf**).
6. Ejecute la secuencia de comandos **edit-server-0.bat**, que se encuentra en la carpeta <**directorio de instalación de Configuration Manager**>**bin**.
7. (En sistemas Windows) En la ventana Propiedades de HP Universal CMDB Configuration Manager que se abre, haga clic en la ficha Java y cambie la configuración de **jmx.http.port** y **com.sun.management.jmxremote.port** por los nuevos números de puerto.
8. Inicie el servicio de Configuration Manager en el equipo de destino.

Copiar la configuración de un sistema a otro

1. En el equipo de origen, abra Configuration Manager. Vaya a **Sistema** > **Configuración** y haga clic en el botón **Exportar conjunto de configuración a un archivo zip**.

   Antes de realizar la exportación puede excluir determinadas partes de la configuración. Para ello, es preciso que desactive la casilla que hay junto a los elementos de configuración pertinentes.
2. Copie la configuración exportada al equipo de destino.
3. En el equipo de destino, abra Configuration Manager. Vaya a **Sistema** > **Configuración** y haga clic en el botón **Importar conjunto de configuración**.

Copias de seguridad y restauración de las mismas

Si se desea, es posible realizar una copia de seguridad de cualquier instalación de Configuration Manager, con el fin de poder recuperarse de cualquier tipo de error que, sin copia de seguridad, requeriría que se realizara una instalación completa nueva.

Copias de seguridad

Realice copias de seguridad de la siguiente información:

- Las subcarpetas **conf** y **security** del directorio de instalación de Configuration Manager. Esta operación se puede efectuar con el sistema en funcionamiento, no es preciso interrumpirlo.
- El esquema de base de datos.

Restauraciones (en un sistema Windows)

Este procedimiento se debe realizar en un sistema nuevo que no contenga ninguna instalación de Configuration Manager.

1. Instale Configuration Manager en el equipo de destino, para lo que debe ejecutar el archivo **setup-win64.msi** (que se encuentra en la carpeta **windows** del soporte de instalación) en modo silencioso, tal como se indica a continuación:

   ```
   msiexec /i setup-win64.msi TARGETDIR=path\to\install\dir /passive
   ```

2. Restaure los directorios **conf** y **security**. A la hora de realizar la restauración, use el mismo método que empleó para realizar la copia de seguridad. Sobrescriba los directorios que ha creado la instalación que realizó en el paso 1.
3. Restaure el esquema de base de datos. Si realiza la restauración en otro servidor de bases de datos, debe modificar la propiedad **url** del archivo **database.properties** (que se encuentra en el directorio **conf**) para que coincida con el nombre del nuevo servidor de bases de datos.
4. Emplee la utilidad **create-windows-service** (con el indicador **-h** para ver las opciones disponibles) para crear un servicio de Windows.
5. Inicie el servidor de Configuration Manager.

Restauraciones (en un sistema Linux)

1. Instale Configuration Manager en el equipo de destino, para lo que debe ejecutar el archivo **setup.bin** (que se encuentra en el soporte de instalación). Para obtener más información, consulte "Instalación de Configuration Manager" en la página 46, pero cancele la instalación en el primer paso del Asistente post-instalación. Se desplegarán todos los archivos, pero el sistema no estará configurado.
2. Restaure los directorios **conf** y **security**. A la hora de realizar la restauración, use el mismo método que empleó para realizar la copia de seguridad. Sobrescriba los que ha creado la instalación que realizó en el paso 1.
3. Restaure el esquema de base de datos. Si realiza la restauración en otro servidor de bases de datos, debe modificar la propiedad **url** del archivo **database.properties** (que se encuentra en el directorio **conf**) para que coincida con el nombre del nuevo servidor de bases de datos.
4. Inicie el servidor de Configuration Manager.

6

Configuración avanzada

Este capítulo incluye:

Opciones avanzadas de conexión de base de datos

Si necesita propiedades de conexión de 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**.

Nota: lleve a cabo las siguientes operaciones al realizar la configuración avanzada en un sistema Linux:

- Cambie las barras diagonales inversas (\) por barras diagonales (/) en las instrucciones.
- Sustituya **.bat** por **.sh** en las ejecuciones de archivos de comandos.

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

- **Autenticación de Windows (NTLM):** para aplicar la autenticación de 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. HP Universal CMDB 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.

Inicio de sesión único (SSO)

El inicio de sesión único entre Configuration Manager y UCMDB se realiza a través de la tecnología LWSSO de HP. Para obtener más información, consulte "Autenticación ligera de inicio de sesión único (LW-SSO): referencia general" en la página 125.

Esta sección incluye:

Habilitar LW-SSO entre Configuration Manager y UCMDB

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** > **UCMDB Foundation**). 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. Esta tarea se debe realizar manualmente, a menos que ya se haya realizado en la instalación de Deployment Manager.

Para habilitar LW-SSO:

1. En el directorio de instalación de Configuration Manager, edite el archivo **\conf\lwssofmconf.xml**.
2. Busque la siguiente sección:

   enableLWSSO enableLWSSOFramework="true"

   y verifique 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-->

Nota: la segunda instancia de DNSDomain sólo se debe incluir si Configuration Manager y otra aplicación se encuentran en dominios distintos.

Quite el carácter de comentario del principio e introduzca todos los dominios del servidor (en caso de ser necesario) en los elementos de DNSDomain (en lugar de Este valor se debe reemplazar por el dominio de la aplicación o Este valor se debe reemplazar por un dominio de otra aplicación. La lista debe incluir el dominio del servidor especificado en el paso 3 en la página 78.

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 **Invoke**.

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

11 Seleccione el método **setInitString**. Especifique el mismo initString que indicó para Configuration Manager en el paso 4 en la página 78 y haga clic en **Invoke**.

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 **Invoke**.

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

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

Configurar LW-SSO en Operations Orchestration

Si LW-SSO está habilitado en Configuration Manager y en Operations Orchestration (OO), a los usuarios que se hayan conectado a Configuration Manager se les permite iniciar sesión en Operations Orchestration a través de la capa web sin tener que especificar su nombre de usuario y contraseña (para administradores del sistema).

Nota:

- En el siguiente procedimiento, <OO_HOME> representa el directorio principal de Operations Orchestration.
- LW-SSO requiere que las cuentas usadas para conectarse a Operations Orchestration y Configuration Manager tienen el mismo nombre de cuenta (pero pueden tener distintas contraseñas).
- LW-SSO requiere que la cuenta de Operations Orchestration no sea interna.

Para configurar LW-SSO en Operations Orchestration:

1. Detenga el servicio RSCentral.
2. En **<OO_HOME>\Central\WEB-INF\applicationContext.xml**, habilite la importación entre LWSSO_SECTION_BEGIN y LWSSO_SECTION_END como se muestra a continuación:

```
<!--  LWSSO_SECTION_BEGIN-->
      <import resource="CentralLWSSOBeans.xml"/>
<!--  LWSSO_SECTION_END -->
```

3 En <**OO_HOME**>**Central****WEB-INF****web.xml**, habilite todos los filtros y asignaciones entre LWSSO_SECTION_BEGIN y LWSSO_SECTION_END como se muestra a continuación:

```
<!--  LWSSO_SECTION_BEGIN-->

<filter>
        <filter-name>LWSSO</filter-name>
        <filter-
    class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProx
    y
        </filter-class>
        <init-param>
            <param-name>targetBean</param-name>
            <param-value>dharma.LWSSOFilter</param-value>
        </init-param>
   .....
   </filter>
<!--  LWSSO_SECTION_END -->

<!--  LWSSO_SECTION_BEGIN-->
   <filter-mapping>
      <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
   </filter-mapping>
<!--  LWSSO_SECTION_END -->

<!--  LWSSO_SECTION_BEGIN-->
    <filter-mapping>
          <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
    <filter-mapping>
          <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
    pattern>/*</url-pattern>
          </filter-mapping>
<!--  LWSSO_SECTION_END -->
```

4 En <**OO_HOME**>**Central****conf****lwssofmconf.xml**, edite los dos siguientes parámetros:

- domain: nombre de dominio del servidor OO.
- initString: debe coincidir con el valor de initString en la configuración de OO LW-SSO (longitud mínima: 12 caracteres).
  Por ejemplo, smintegrationlwsso.

  Por ejemplo:

```
<webui>
<validation>
      <in-ui-lwsso>
       <lwssoValidation  id="ID000001">
            <domain>asia.hpqc.net</domain>
            <crypto cipherType="symmetricBlockCipher"
                                    engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                                    initString=" smintlwsso "></crypto>
       </lwssoValidation>
      </in-ui-lwsso>
</validation>
<creation>
       <lwssoCreationRef id="ID000002">
            <lwssoValidationRef refid="ID000001"/>
            <expirationPeriod>600000</expirationPeriod>
       </lwssoCreationRef>
</creation>
</webui>
```

5 Para que la configuración surta efecto, reinicie el servicio RSCentral.

Realizar una autenticación de Identity Manager

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

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

Esta tarea incluye los siguientes pasos:

➤ "Requisitos previos" en la página 83

➤ "Configurar HP Universal CMDB Configuration Manager para que acepte Identity Manager" en la página 83

Requisitos previos

El servidor Tomcat de Configuration Manager debe estar conectado a un servidor web (IIS o Apache) protegido mediante Identity Manager 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 Identity Manager

Para configurar Java Tomcat (AJP13) con IIS6:

1. Configure Identity Manager 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 de Identity Manager y cambie el puerto por el de Identity Manager:

bsf.server.url=http://< URL de Identity Manager>:< Puerto de Identity Manager >/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://<Configuration Manager URL>:
<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 este 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=<directorio de instalación de Configuration Manager>\servers
\server-0\logs\isapi.log
# Log level (debug, info, warn, error or trace)
log_level=info
# Ruta de acceso completa al archivo workers.properties
worker_file==<directorio de instalación de Configuration Manager>\tomcat
\conf\workers.properties.minimal
# Ruta de acceso completa al archivo uriworkermap.properties
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

---

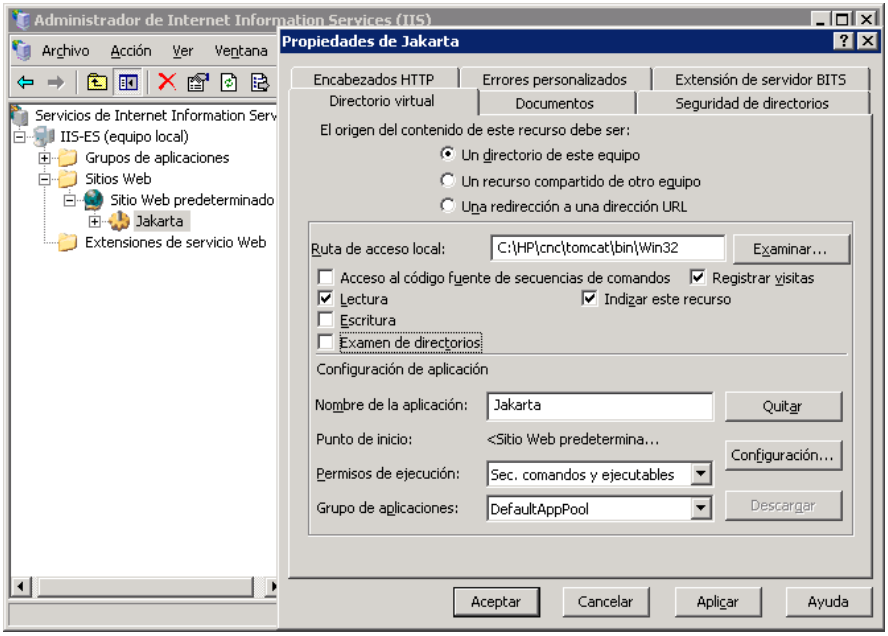
6 Cree el directorio virtual en el objeto de sitio web de la configuración de IIS.

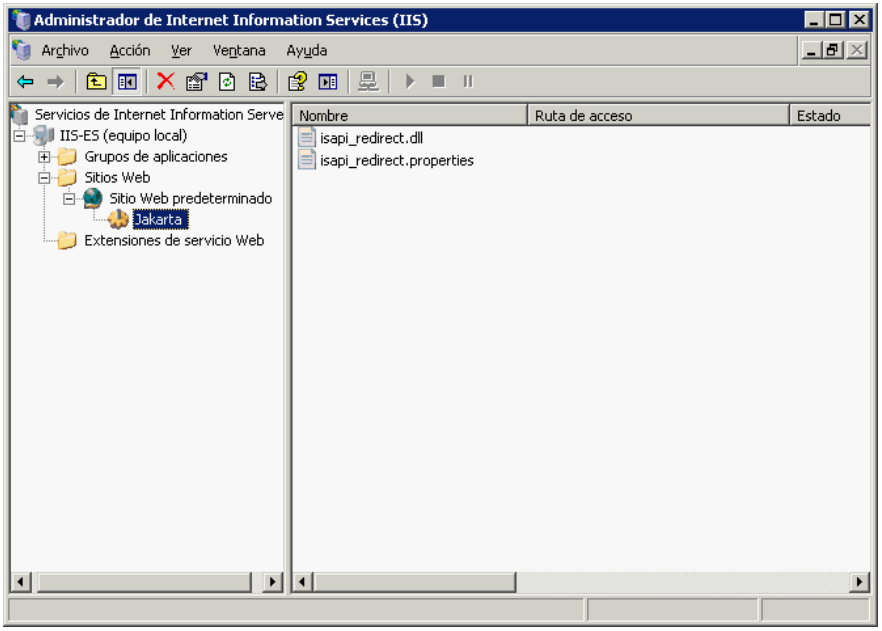
a En el menú Inicio de Windows, abra **Configuración** > **Panel de control** > **Herramientas administrativas** >**Administrador de Internet Information Services (IIS)**.

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:





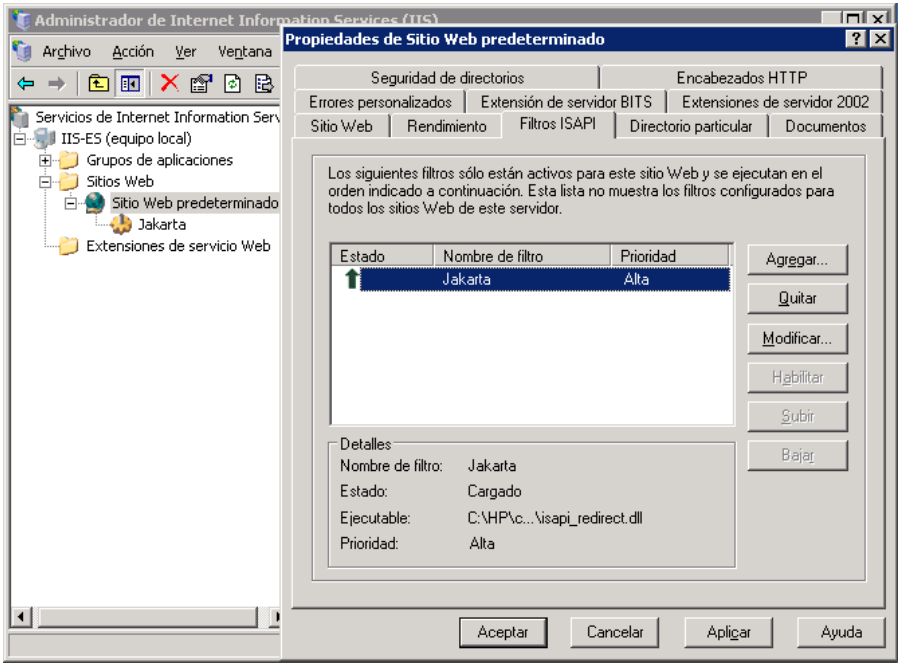
7 Agregue **isapi_redirect.dll** como filtro ISAPI.

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:



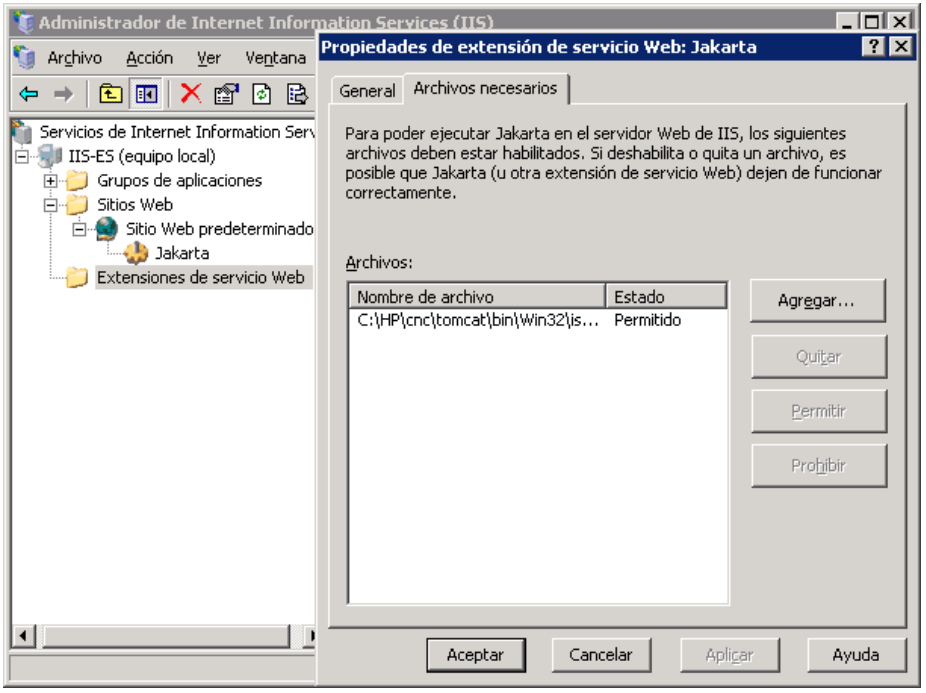
d Haga clic en el botón **Aplicar**.

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.

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 tanto IPv6 como IPv4. Para obtener más información, consulte la documentación del sistema operativo relevante.
2. Abra el archivo **client-config.properties**, que se encuentra en la carpeta <**directorio de instalación de Configuration Manager**>/**conf** y edite los siguientes valores:
   - Cambie el valor del parámetro **bsf.server.url** y asegúrese de que usa el nombre de host. Por ejemplo:

     bsf.server.url=http://mycomputer:8080/bsf

   - Cambie el valor del parámetro **bsf.server.services.url** y asegúrese de que la URL de Configuration Manager es la dirección del nombre de host. Por ejemplo:

     bsf.server.services.url=http://<nombre de host de Configuration Manager>:<Puerto de Configuration Manager>/bsf

3 Abra el archivo **servers\server-0\conf\server.xml** de Tomcat y edite los siguientes valores:

➤ Añada la dirección IPv6 al enlace SHUTDOWN agregando **address="[::]"** a la siguiente etiqueta:

<Server port="8005" shutdown="SHUTDOWN" **address="[::]"** >

➤ Duplique el conector HTTP. Para el segundo conector añada la dirección IPv6 [::]. Por ejemplo:

```
<Connector port="8180" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
<Connector port="8180" protocol="HTTP/1.1" address="[::]"
           connectionTimeout="20000"
           redirectPort="8443" />
```

➤ Duplique el conector AJP. Para el segundo conector añada la dirección IPv6 [::]. Por ejemplo:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"  address="[::]" />

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

4 Añada la variable de entorno al servidor: useIPv6="true":

Abra el archivo **edit_server-0.bat**, que se encuentra en la carpeta <**directorio de instalación de Configuration Manager**>/**bin**. En la ficha Java, añada la siguiente propiedad a las opciones de Java: -DuseIPv6.

5 Reinicie el servidor.

LDAP

LDAP se puede configurar en Configuration Manager. Para obtener más información, consulte "Configuración de sistema" en la *guía de usuario de HP Universal CMDB Configuration Manager*.

Sistema de protección

Esta sección incluye:

Nota: después de realizar la actualización, es preciso volver a configurar SSL. Para obtener más información, consulte "Actualizar Configuration Manager" en la página 41.

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.

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 96.

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 la secuencia de comandos **generate-keys.bat**, que crea el siguiente directorio: **cnc920\security\encrypt_repository** y genera la clave de cifrado.
3. Ejecute la utilidad **bin\encrypt-password** para cifrar la contraseña. Configure el indicador **-h** para ver las opciones disponibles.
4. Copie el resultado de la utilidad de cifrado de contraseñas y pegue el cifrado resultante en el archivo **conf\database.properties**.

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 95.

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.

Parámetro	Descripción
cipherType	El tipo de cifrado. Actualmente, sólo se admite **symmetricBlockCipher**.
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**.

Parámetro	Descripción
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.

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 7.0 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 el 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 por 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

Añada el certificado a los almacenes de confianza del cliente de Internet Explorer en el equipo (**Herramientas** > **Opciones de Internet** > **Contenido** > **Certificados**). Si no lo hace, se le solicitará que lo haga la primera vez que intente usar Configuration Manager.

Para obtener más información sobre el uso de certificados de cliente, consulte "Certificados de cliente" en la página 106.

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. Defina el protocolo de **bsf.server.url** como **https** y el puerto como **8443**.

5 Modificar el archivo server.xml

Abra el archivo **server.xml**, que se encuentra en **<directorio de instalación de Configuration Manager>\servers\server-0\conf**. Localice la sección que empieza por

Connector port="8443"

que aparece en los comentarios. Active la secuencia de comandos quitando el carácter de comentario y agregue los siguientes atributos al conector de HTTPS:

keystoreFile="<ubicación de archivo tomcat.keystore>" (véase el paso 2 en la página 99)
keystorePass="<contraseña>"

Convierta la siguiente línea en comentario:

<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />

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 la propiedad **bsf.server.url** se ha establecido en **https** y que el puerto es **8443**.

4 Modificar el archivo server.xml

Abra el archivo **server.xml**, que se encuentra en <**directorio de instalación de Configuration Manager**>**servers****server-0****conf**. 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" />
```

Convierta la siguiente línea en comentario:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

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.

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.

Por ejemplo: java/{os name}/lib.

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 muestra 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**.
2. Copie **hpcert.cer** al equipo servidor que se encuentra en la carpeta <**directorio de instalación de Configuration Manager**>**java****bin**.
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:

   <directorio de instalación de Configuration Manager>\java\bin\keytool.exe -import
   -alias hp -file hpcert.cer -keystore ..\lib\security\cacerts

4 Modifique el archivo **server.xml** (se encuentra en la carpeta **<directorio de instalación de Configuration Manager>\servers\server-0\conf**) como se indica a continuación:

   a Realice los cambios descritos en el paso 5 en la página 100.

   b Inmediatamente después, añada los siguientes atributos al conector de HTTPS:

   ```
   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 100.

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.

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 98 hasta el paso 6 en la página 100 o "Habilitar SSL en el equipo servidor con un certificado de una entidad de certificación" en la página 101 hasta el paso 5 en la página 102.

2 Escriba la siguiente URL en el explorador web: http://<Nombre o dirección IP de servidor de Configuration Manager>:8180/cnc.

Habilitar la autenticación de certificado de cliente

Esta tarea describe cómo configurar Configuration Manager para aceptar la autenticación de certificados 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 98.

2 Abra el siguiente archivo: **<directorio de instalación de Configuration Manager>\conf\lwssofmconf.xml.** Busque 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 98.
- Cambie **bsf.server.services.url** para usar el protocolo HTTP y cambie el puerto al puerto HTTP original.

Certificados de cliente

Esta sección incluye:

Información de certificados de cliente

En esta sección se describe la información de certificados de cliente y cómo extraer un identificador de usuario de un certificado de cliente.

- **Identificador de usuario**

  El identificador de usuario es la parte exclusiva de la información del certificado de cliente que se emplea para identificar la identidad del usuario.

➤ **Información básica de certificados de cliente**

La información básica de los certificados de cliente incluye:

Campo Certificado	Descripción
Versión	La versión del certificado codificado. Ejemplo: 1 (0x1)
Número de serie	Número entero positivo que asigna la entidad emisora de certificados a cada certificado. Ejemplo: 0 (0x0)
Algoritmo de firmas	El identificador del algoritmo usado por la entidad emisora de certificados para firmar el certificado. Ejemplo: md5WithRSAEncryption
Emisor	La entidad que ha firmado y generado el certificado. Ejemplo: CN=Emisor, C=US, ST=NY, L=Nueva York, O=Organización de trabajo, O=example.com
Validez	El intervalo de tiempo durante el que la entidad emisora de certificados garantiza que mantendrá la información sobre el estado del certificado: ➤ **No antes**. Especifica la fecha en que comienza el periodo de validez del certificado. Ejemplo: 25 nov. 04:34:49 2009 GMT ➤ **No después**. Especifica la fecha en que finaliza el periodo de validez del certificado. Ejemplo: 25 nov. 04:34:49 2010 GMT

Campo Certificado	Descripción
Sujeto	La entidad asociada con la clave pública almacenada en el campo de claves públicas del sujeto.
Información de clave pública del sujeto	Se usa para llevar la clave pública e identificar el algoritmo con el que se usa la clave (por ejemplo, RSA, DSA o Diffie-Hellman).

Para obtener más información, consulte el perfil del certificado de infraestructura de clave pública Internet X.509 y de la lista de revocación de certificados (CRL):

http://tools.ietf.org/html/rfc5280

➤ **Campo Sujeto**

El campo Sujeto (también denominado Nombre distintivo del sujeto o SubjectDN) identifica la entidad asociada con la clave pública.

El campo Sujeto contiene los siguientes atributos relevantes (también puede contener otros atributos):

Atributo de Sujeto	Descripción de atributos de Sujeto	Ejemplo
CN	Nombre común	CN=Bob BobFamily
emailAddress	Dirección de correo electrónico	*emailAddress=bob@example.com*
C	Nombre de país	C=EEUU
ST	Nombre de estado o provincia	ST=NY
L	Nombre de localidad	L=Nueva York
O	Nombre de organización	O=Organización de trabajo
OU	Nombre de unidad organizativa	OU=Gestores

Para recuperar el identificador de usuario del sujeto, puede utilizar todo el campo SubjectDN o el atributo SubjectDN.

➤ **Extensión de la información de certificados de cliente**

Las extensiones definidas para los certificados X.509 v3 proporcionan métodos para asociar los atributos adicionales con usuarios y claves públicos, y para gestionar las relaciones entre las entidades emisoras de certificados. Campo Nombre alternativo del sujeto puede contener el identificador de usuario.

➤ **Campo Nombre alternativo del sujeto**

La extensión del nombre alternativo del sujeto permite enlazar las identidades al sujeto del certificado. Estas identidades se pueden incluir junto con la identidad en el campo del sujeto del certificado, o en lugar de ella.

El campo Nombre alternativa del sujeto puede contener las siguientes identidades:

Identidad	Ejemplo
otherName	Otro nombre: Nombre principal= *bobOtherAltName@example.com*
rfc822Name	Nombre RFC822 =*bobRFC822AltName@example.com*
dNSName	Nombre DNS=example1.com
x400Address	
directoryName	Dirección del directorio: E=*bobDirAltName@example.com*, CN=bob, OU=Baladas de oro, O=Música de oro, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/
iPAddress	Dirección IP=192.168.7.1
registeredID	ID registrado=1.2.3.4

Para recuperar el identificador de usuario del nombre alternativo del sujeto, puede usar una de las identidades.

Configuración

Configuration Manager emplea LW-SSO para aprovechar el identificador de usuario de un certificado de cliente. El gestor de certificados de cliente usa los siguientes atributos para configurar LW-SSO para que haga uso del identificador del usuario:

Para hacer uso de la información de un certificado de cliente, se debe configurar Configuration Manager para recuperar el identificador de usuario.

Se deben decidir los siguientes elementos:

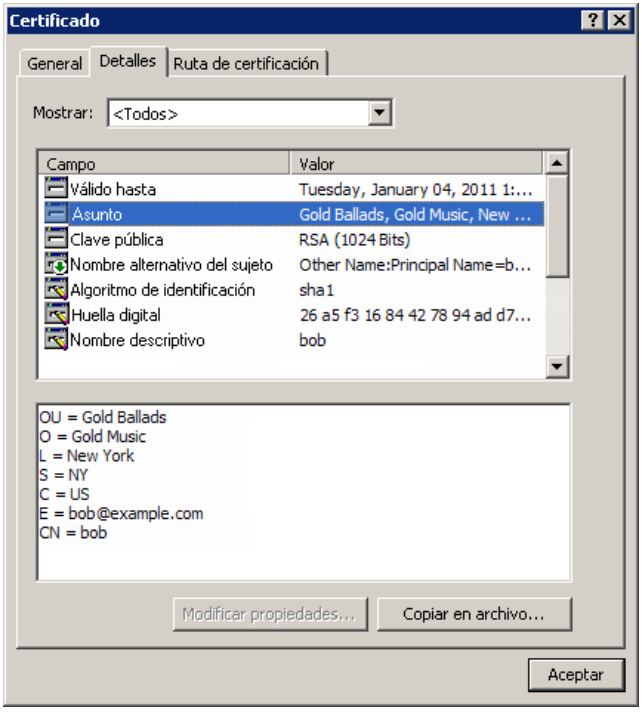
- ¿Qué campo se debe usar: SubjectDN o Nombre alternativo del sujeto?
- ¿Se debe usar todo el campo o sólo una parte del mismo?
- Si se usa una parte del campo de entrada, especifique un valor para el mismo: especifique el atributo de sujeto de SubjectDN o especifique la identidad de Nombre alternativo del sujeto.

El gestor de certificados de cliente usan los siguientes certificados para configurar LW-SSO:

Nombre de atributo	Descripción
enabled	Especifica si el gestor está habilitado o deshabilitado. **Importante**: se recomienda encarecidamente establecer explícitamente el valor como falso y habilitar el gestor sólo cuando se requiera la validación del certificado de cliente.
userIdentifierRetrieveField	El parámetro indica qué campo del certificado contiene el identificador de usuario. Las opciones son: **SubjectDN** o **SubjectAlternativeName**.
userIdentifierRetrieveMode	El parámetro userIdentifierRetrieveMode indica si el identificador de usuario se compone de todo el contenido del campo relevante, o sólo de una parte del mismo. Las opciones son: **EntireField** o **FieldPart**.
userIdentifierRetrieveFieldPart	Si el valor de **userIdentifierRetrieveMode** es **FieldPart**, el parámetro 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 **Nota**: Este atributo no puede estar vacío si en **userIdentifierRetrieveMode** se ha seleccionado **FieldPart**. Tampoco puede estar vacío si en **userIdentifierRetrievField** se ha seleccionado **SubjectAlternativeName**.

Ejemplos

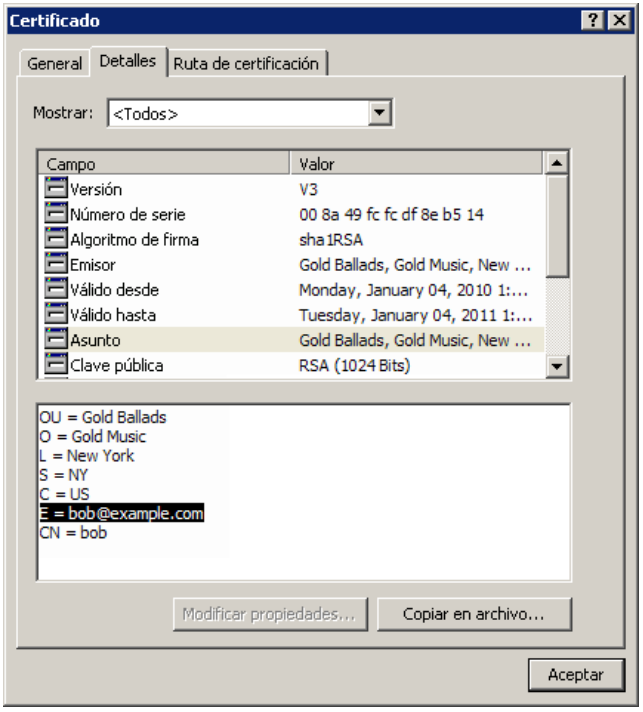
➤ **Asunto se usa para contener el identificador de usuario**



El siguiente ejemplo muestra cómo configurar el gestor para que tome el identificador de usuario de todo SubjectDN:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

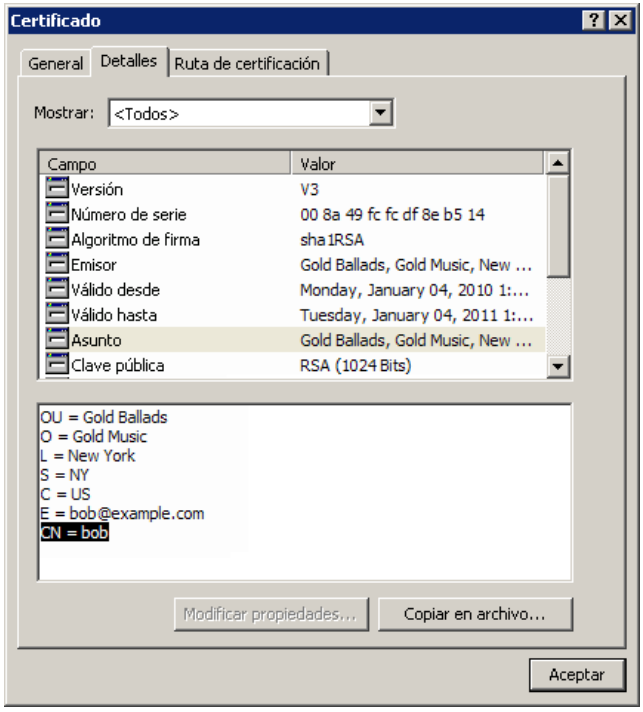
➤ **El campo Correo electrónico de Asunto se usa para contener el identificador de usuario**



Use los nombre de los campos que ve en la leyenda del certificado de cliente. El siguiente ejemplo muestra cómo configurar el gestor para que tome el identificador de usuario del campo de correo electrónico de Sujeto:

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

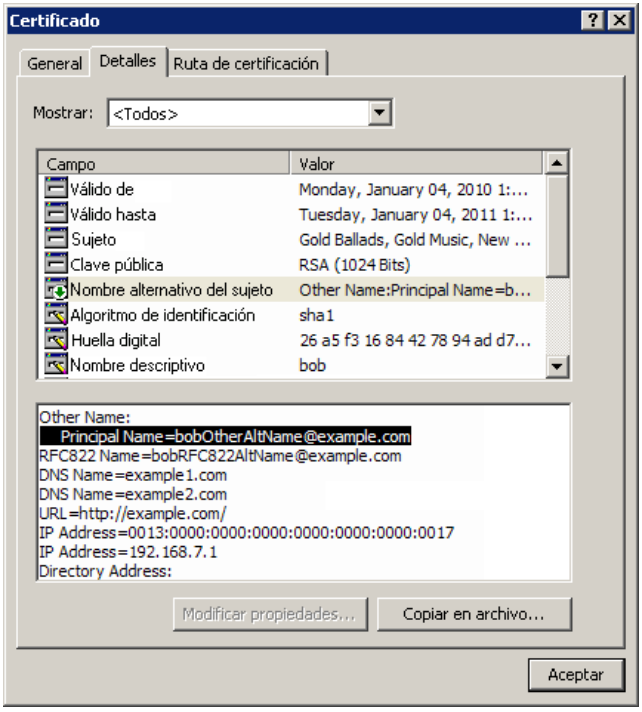
➤ **El campo Nombre personalizado de Asunto se usa para contener el identificador de usuario**



Use los nombre de los campos que ve en la leyenda del certificado de cliente. El siguiente ejemplo muestra cómo configurar el gestor para que tome el identificador de usuario del campo Nombre personalizado de Sujeto:

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

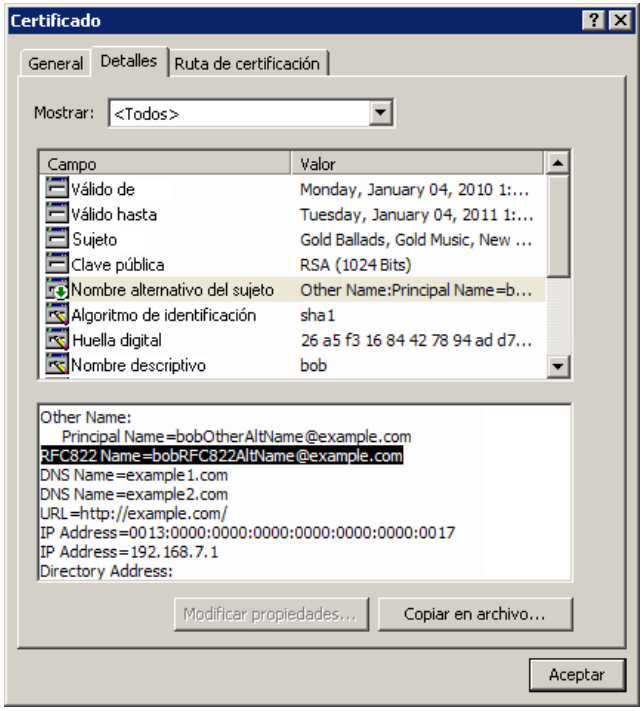
➤ **El campo Identidad de otherName de Nombre alternativo del sujeto se usa para contener el identificador de usuario**



Use el nombre de identidad que ve en la leyenda del certificado de cliente. El siguiente ejemplo muestra cómo configurar el gestor para que tome el identificador de usuario del campo Identidad de otherName de Nombre alternativo de sujeto:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

➤ **El campo Identidad de rfc822Name de Nombre alternativo del sujeto se usa para contener el identificador de usuario**



Use el nombre de identidad que ve en la leyenda del certificado de cliente. El siguiente ejemplo muestra cómo configurar el gestor para que tome el identificador de usuario del campo Identidad de rfc822Name de Nombre alternativo de sujeto:

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

Configurar Configuration Manager para que funcione con UCMDB mediante SSL

Configuration Manager se puede configurar para que funcione con UCMDB utilizando Capa de sockets seguros (SSL). En UCMDB, el conector SSL del puerto 8443 está habilitado de forma predeterminada.

Para exportar el certificado de servidor e importarlo en el almacén de confianza del cliente

1. Diríjase a **<directorio de instalación de UCMDB>bin\jre\bin** y ejecute el siguiente comando:

   keytool -export -alias hpcert -keystore <UCMDB server dir>
   \conf\security\server.keystore -storepass hppass -file <certificatefile>

2. Importe el certificado en el almacén de confianza de Configuration Manager (el almacén de confianza jre predeterminado):

   <CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias hpcert -keystore
   <CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file
   <certificatefile>

3. Defina las propiedades de conexión de UCMDB en Configuration Manager:

   Diríjase a **Sistema** > **Configuración** > **Integraciones** > **UCMDB Foundation**. En Estrategia de conexión, seleccione **HTTPS**; en el puerto del servidor de UCMDB, seleccione el puerto HTTPS de UCMDB y en la dirección URL de acceso a UCMDB seleccione https://<HostName>:8443.

4. Guarde el conjunto de configuración y actívelo. Reinicie Configuration Manager.

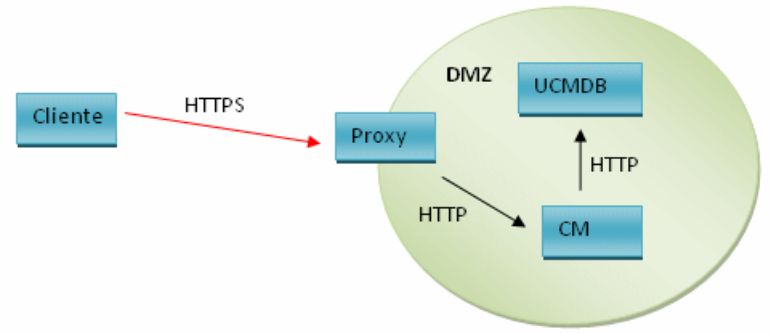
Para configurar Configuration Manager para que funcione con otros productos (como equilibradores de carga) que usan Capa de sockets seguros (SSL), importe el certificado de seguridad del producto en el almacén de confianza de Configuration Manager (almacén de confianza jre predeterminado), para lo que debe ejecutar el siguiente comando:

<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias> -keystore
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file <certificatefile>

Proxy inverso

Si Configuration Manager y UCMDB se encuentran en un DMZ, es aconsejable configurar el sistema para que funcione con un servidor proxy inverso. Los pasos de la configuración son los mismos que los que hay que seguir para configurar UCMDB para que funciones con un proxy inverso. Para habilitar el acceso a Configuration Manager es preciso asignar las rutas de acceso a **/cnc** y **/bsf** a las direcciones URL del servidor remoto en el que se instala Configuration Manager.

La siguiente imagen muestra el proceso de configuración de un proxy inverso para Configuration Manager:



Por ejemplo, si el proxy inverso es un servidor Apache, añada las siguientes líneas al archivo **Apache2.2\conf\extra\httpd-ssl.conf** y, a continuación, reinicie el servidor Apache:

```
ProxyPass /cnc http://<CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPassReverse /cnc http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPass /bsf http://< CM_HOSTNAME >:<CM_HTTP_PORT>/bsf
ProxyPassReverse /bsf http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/bsf
```

Es posible que los distintos tipos de proxy inverso puedan requerir diferentes pasos de configuración, por lo que si desea más información, debe consultar la documentación del servidor proxy.

Para configurar un proxy inverso para Configuration Manager:

Actualice el archivo **client-config.properties** en la carpeta **<directorio de instalación de Configuration Manager>\conf** como se indique a continuación:

```
bsf.server.url=https://<proxy-server-name>:443/bsf
```

El puerto HTTPS predeterminado del proxy Apache es el 443.

Sección II

Apéndices

A

Límites de capacidad

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

Número máximo de vistas	100
Número máximo de políticas	300
Número máximo de CI compuestos por vista	5000
Número máximo de usuarios concurrentes	50
Número máximo de CI compuestos en el módulo Análisis de configuración	1000

B

Autenticación ligera de inicio de sesión único (LW-SSO): referencia general

Este capítulo 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.

Para obtener información sobre cómo solucionar problemas de LW-SSO, consulte "LW-SSO: solución de problemas ylimitaciones" en la página 144.

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.

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

C

Solución de problemas

Este capítulo incluye:

Solución de problemas generales y limites

Limitaciones

Los tipos de CI que se crean en UCMDB no se ven hasta que se produce una desconexión de Configuration Manager y, posteriormente, se vuelve a establecer una conexión.

Solución de problemas

Problema. El atributo **name** del tipo de CI Nodo no se habilita como cambio monitorizado y no se copia al estado autorizado durante la autorización de CI. Esto sucede si la versión 9.20 de Configuration Managerse instala sin el Content Pack 9 para UCMDB.

Solución. Realice una de las siguientes operaciones:

- Establezca manualmente que el atributo **name** esté habilitado como cambio monitorizado en el Gestor de tipos de CI de UCMDB.
- Instale el Content Pack 9.

Problema. Al iniciar el servicio de Configuration Manager, recibe un mensaje de error que indica lo siguiente:

Windows could not start the HP Universal CMDB Configuration Manager on Local Computer. For more information, review the System Manager Event log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.r code 0.

Solución. Realice las siguientes operaciones:

1. Vaya a **<directorio de instalación de Configuration Manager>\cnc\bin** y ejecute el siguiente comando:

   edit-server-0.bat

2. Seleccione la ficha Inicio. En la lista desplegable Modo (en la parte inferior), seleccione **jvm**, en lugar de **exe**.
3. Seleccione la ficha Apagado. En el campo Clase, cambie el apellido de **Boostrap** a **Bootstrap**.
4. Haga clic en **Aceptar**.
5. Ejecute el servicio.

Deployment Manager: solución de problemas y limitaciones

Para solucionar los problemas de Deployment Manager, abra el registro de la sesión anterior, que se encuentra en el siguiente directorio:

%temp%\HP\ucmdb-dm\Workspace\Sessions

Directrices generales para volver a realizar despliegues

En la instalación, anote las advertencias y errores que aparezcan en la página **Validation** de Deployment Manager haciendo clic en el botón de detalles que se encuentra junto a cada uno de los componentes desplegados.

Una vez que se haya localizado un problema durante el despliegue y se haya encontrado una solución, lleve a cabo los siguientes pasos:

1. Desinstale los productos desplegados y reinicie la máquina.
2. Reinicie Deployment Manager y vuelva a introducir todas las configuraciones.

Errores durante el despliegue

Problema. Error de permisos durante el despliegue.

El registro de la sesión indica que hay un problema con los permisos de usuario de la base de datos al crear un esquema.

Solución. Para crear una base de datos, es preciso tener los permisos pertinentes. Asegúrese de que las credenciales de usuario utilizadas en el despliegue son suficientes para la creación de espacios de tabla y esquemas.

Problema. Error de configuración de esquema/base de datos en UCMDB.

El registro de la sesión indica que Deployment Manager no pudo crear un esquema o una base de datos.

Solución:

Nota: tenga en cuenta que no se puede crear un esquema de UCMDB y conectarlo a un esquema existente en el historial de UCMDB (independientemente del tipo de servidor de bases de datos).

Verifique que el esquema de UCMDB y el esquema del historial de UCMDB no usan el siguiente tipo de conexión:

- Esquema de UCMDB - Crear esquema
- Esquema de historial de UCMDB - Conectar con esquema existente

Problema. Error de configuración de esquema/base de datos en UCMDB.

El registro de la sesión indica que no se pudo crear el esquema.

Solución. Abra el archivo session.log y busque el siguiente mensaje: SQL error executing statement CREATE USER <schema name>

Al asignar un nombre al esquema de Oracle en la página **Database Configuration** de Deployment Manager, asegúrese de usar sólo letras (a-z), dígitos (0-9) y el signo de guión ('-').

Problema. El esquema no se puede crear porque no hay suficiente espacio.

Solución. Aumente la cantidad de espacio libre en el esquema o la base de datos. Use las interfaces de gestión estándar que proporcionan Oracle y Microsoft.

Problema. Se produjo el siguiente error en la configuración de la base de datos:
NT AUTHORITY\ANONYMOUS LOGON – Could not connect to database.

Al seleccionar un servidor de MSSQL con autenticación NTLM para la configuración de la base de datos de UCMDB, se produce un error de dicha configuración, lo que provoca un error en el despliegue.

Solución. Despliegue UCMDB en un equipo con localhost (el único lugar en que se admite la autenticación NTLM).

Problema. Error en la configuración de bases de datos de Configuration Manager al crear una base de datos.

El siguiente error puede aparecer en el panel de detalles de Deployment Manager:

> Failed to create Oracle schema due to error: ORA-01031: insufficient privileges

o

> Failed to create a schema to the database: machineName. Reason: ORA-01919: role 'RESOURCE' does not exist

Solución. Compruebe que el usuario de la base de datos tiene los siguientes privilegios:

- Conexión
- Recurso

Problema. No se pudo realizar el despliegue debido a que el equipo host de destino no tenía suficiente espacio en el disco.

Solución. Inicie sesión en el equipo host de destino y asegúrese de que hay suficiente espacio en el disco para que el despliegue se realice correctamente:

- UCMDB requiere 1 GB de espacio libre
- Configuration Manager requiere 1 GB de espacio libre
- DDMA requiere 1 GB de espacio libre

Nota: además de los requisitos específicos del producto, se requiere 1 GB adicional de espacio libre para la gestión de archivos temporales.

Problema. Error en la utilidad para realizar pings a UCMDB.

Esta utilidad se ejecuta desde el equipo de Configuration Manager y comprueba que la conexión con la instancia existente de UCMDB. Abra el archivo session.log y busque el siguiente mensaje:
Failed to test connection due to error: java.net.ConnectException: Connection refused: connect.

Solución:

- Compruebe que el firewall de Windows no bloquea el puerto 8080 del UCMDB de destino.
- Compruebe que se puede acceder al servidor de UCMDB desde el equipo de Configuration Manager, así como que el despliegue de UCMDB finaliza correctamente y que UCMDB está en funcionamiento.

La conexión con el equipo host no está disponible

Problema. RPC no está disponible o se ha producido un error desconocido.

Al pulsar el botón Probar conexión genera un error que indica que RPC no está disponible.

Solución. Corrija el nombre de host si es necesario y asegúrese de que tanto el servicio de WMI como los servicios de servidor se están ejecutando y de que el firewall de Windows no bloquea el acceso a la interfaz de WMI.

Deshabilite el firewall de Windows o añada la habilitación de excepciones de firewall al acceso a la administración remota.

Para ello, abra el panel de control de **Firewall** y seleccione **Reglas de entrada.** Habilite Archivo e impresoras, las reglas de WMI y el puerto 8080.

No se pudo probar la conexión

Problema. Acceso denegado.

El acceso se deniega debido a cualquiera de los siguientes motivos: el nombre de usuario o la contraseña son incorrectos, la configuración de DNS no es válida o el nombre de usuario empleado en el despliegue no tiene credenciales administrativas en el equipo host de destino.

Solución. Asegúrese de que las credenciales de usuario especificadas son correctas y que el usuario tiene credenciales administrativas en el equipo host.

Error al acceder a la aplicación

Problema. Tras un despliegue correcto no es posible acceder a la aplicación (UCMDB o Configuration Manager).

Solución. Compruebe que los siguientes servicios de UCMDB y Configuration Manager existen y están funcionando.

- Servicio **UCMDB_Server**
- Servicio **HPUCMDBCMoasisSNAPSHOTserver0**

Revise los registros de despliegue que se encuentran en el directorio Sessions, por si contuvieran errores.

LW-SSO está deshabilitado

Problema. El despliegue ha sido correcto, pero la funcionalidad LW-SSO está deshabilitada.

Solución. Asegúrese de que la cadena de inicialización de LW-SSO y el dominio son idénticos en UCMDB y Configuration Manager (y en OO si corresponde).

Revise la configuración de LW-SSO siguiendo los métodos que se indican a continuación:

- Configuration Manager: abra el archivo **lwssofmconf.xml** y compruebe el dominio y las definiciones de la cadena de inicialización. El archivo se encuentra en la carpeta **<directorio de instalación de Configuration Managery>\conf**.
- UCMDB: abra UCMDB y seleccione **Gestores** > **Administración** > **Gestor de configuración de infraestructura**.

Si tanto Configuration Manager como UCMDB residen en equipos host que tienen dominios DNS diferentes, asegúrese de que la configuración de **Dominios de confianza** incluye los dos dominios DNS y están habilitados en ambos productos.

Para recibir información adicional del despliegue, se puede habilitar Deployment Manager en modo de depuración. El modo de depuración proporciona información adicional sobre el despliegue.

Para habilitar el modo de depuración:

1. Después de ejecutar Deployment Manager, abra una ventana del explorador y escriba %temp% en la barra de direcciones.
2. Desplácese a la carpeta **hp\ucmdb-dm**.
3. Abra el archivo **ini** en un editor de textos y añada la siguiente propiedad a la última línea del archivo:

   –Ddebug.mode=true

4. Use **%temp%\HP\ucmdb-dm\ucmdb-dm.exe** para ejecutar Deployment Manager.

Acceso a Configuration Manager: Solución de problemas y limitaciones

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.

Solución de problemas

Problema. Tras cambiar el conjunto de configuración en **Sistema** > **Configuración**, 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:

```
<Directorio de instalación de Configuration Manager>\bin\export-cs.bat
<propiedades de base de datos> --history
```

donde <**propiedades de base de datos**> se puede especificar señalando 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 <directorio de instalación de Configuration Manager>\bin export-cs.bat -
p ..\conf\database.properties --history
```

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

```
<directorio de instalación de 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 <directorio de instalación de Configuration Manager>\bin export-cs.bat -p ..\conf\database.properties -i 491520 -f mydump.zip

3 Detenga el servicio de Configuration Manager.

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

<directorio de instalación de Configuration Manager>\bin\import-cs.bat <propiedades de base de datos> -i <nombre de 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 **Sistema** > **Configuración** > **Integraciones** > **UCMDB Foundation** > **UCMDB Foundation**, cambie la configuración y guárdela. 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:

   <Directorio de instalación de Configuration Manager>\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 <**directorio de instalación de Configuration Manager**>**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: **v<Directorio de instalación de Configuration Manager>\servers\server-0\conf\server.xml** y actualizando los puertos pertinentes:
  - HTTP (8180): línea 69
  - HTTPS (8443): líneas 71, 90

Problema. Recibe un mensaje de "memoria insuficiente".

Solución. Realice las siguientes acciones para cambiar los parámetros de inicio del servidor:

1 Ejecute el siguiente archivo por lotes:

<Directorio de instalación de Configuration Manager>/bin/edit-server-0.bat

2 Cambie las siguientes propiedades:

-Dapplication.ms=<tamaño inicial de bloque de memoria>
-Dapplication.mx=<tamaño máximo de bloque de memoria>

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 **Sistema** > **Configuración**.
- Ejecute una llamada JMX para ejecutar el cálculo del análisis sin conexión en la vista pertinente.

➤ Acceda a **Administración** > **Políticas**> **Políticas de configuración**. Pulse el botón **Recalcular análisis de política**. 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** > **UCMDB Foundation**, 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 "Inicio de sesión único (SSO)" en la página 77. 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** > **UCMDB Foundation** no funciona.

Solución. Siga estos pasos:

1. Diríjase a **Sistema** > **Configuración** > **Integraciones** > **UCMDB Foundation** > **UCMDB Foundation.**
2. Añada corchetes a la dirección IP de la URL de acceso a UCMDB. La dirección URL debe ser 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.

LW-SSO: solución de problemas ylimitaciones

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.

Solución de problemas

Problema: No se crean cookies de LW-SSO después de iniciar sesión.

- **Posible causa:** un dominio que no está vacío no está definido correctamente en el elemento LW-SSO de la configuración.
- **Posible solución**: asegúrese de que el dominio definido en el elemento LW-SSO de la configuración coincide con el dominio de la aplicación.
- **Posible causa:** un dominio que no está vacío y que se ha usado como parámetro en la función enableSSO no es correcto.
- **Posible solución**: asegúrese de que el dominio que se usa como parámetro en la función enableSSO coincide con el dominio de la aplicación.
- **Posible causa:** No ha accedido a la aplicación con el nombre de dominio completo (FQDN) en la dirección URL de inicio de sesión cuando hay un dominio definido en la configuración de LW-SSO (por ejemplo: http://192.168.12.13/WebApp).
- **Posible solución**: Asegúrese de que accede a la aplicación con el nombre de dominio completo en la dirección URL de conexión (por ejemplo: http://myserver.companydomain.com/WebApp).

Problema: LW-SSO no puede crear una cookie para la funcionalidad.

- **Posible causa:** un dominio no está definido correctamente en el elemento LW-SSO de la configuración.
- **Posible solución**: asegúrese de que el dominio definido en el elemento LW-SSO de la configuración coincide con el dominio de la aplicación.

Problema: el token LW-SSO no se ha validado.

- **Posible causa:** las dos aplicaciones tienen diferentes parámetros initString en el elemento crypto de la configuración (u otros parámetros criptográficos).
- **Posible solución**: use el mismo initString en las dos aplicaciones (además de todos los parámetros de crypto restantes del elemento de creación de LW-SSO).
- **Posible causa:** la diferencia, en hora GMT, entre las dos aplicaciones es superior a 15 minutos.
- **Posible solución**: asegúrese de que todas las aplicaciones que participan en una integración LW-SSO tienen la misma hora GMT con una diferencia máxima de 15 minutos.
- **Posible causa:** un dominio está vacío en el elemento LW-SSO de la configuración y usted accede a una segunda aplicación de otro equipo con el mismo dominio DNS.
- **Posible solución**: asegúrese de que el dominio definido en el elemento LW-SSO de la configuración coincide con el dominio de la aplicación.
- **Posible causa:** un dominio no está definido en el elemento LW-SSO de la configuración y usted accede a una segunda aplicación de otro equipo con el mismo dominio DNS.
- **Posible solución**: agregue un dominio al elemento LW-SSO y asegúrese de que en la definición de dicho dominio se ha establecido que coincide con el dominio de la aplicación.

Problema: LW-SSO no puede validar el token LW-SSO en un entorno con varios dominios

- **Posible causa:** en la configuración de una de las aplicaciones, uno de los dominios no está definido correctamente en el elemento LW-SSO.
- **Posible solución**: el dominio definido en el elemento LW-SSO de la configuración de la aplicación debe coincidir con el dominio de la aplicación en función de los dominios que están en uso.
- **Posible causa:** en la configuración de una de las aplicaciones, uno de los dominios no está definido correctamente en la configuración de trustedHosts (o la de protectedDomains).

- **Posible solución**: asegúrese de que los dominios de la configuración de trustedHosts (o la de protectedDomains) de las configuraciones de todas las aplicaciones están definidas correctamente.
- **Posible causa:** la cookie de la sesión de LW-SSO se bloquea o se deniega al usar Internet Explorer 6.x, 7.x o 8.x.
- **Posible solución**: agregue todos los servidores de LW-SSO a la zona "Intranet"/"De confianza" de las zonas de seguridad de Internet Explorer en el equipo (Herramientas > Opciones de Internet > Seguridad > Intranet local > Sitios > Opciones avanzadas). De esta forma se aceptarán todas las cookies.
- **Posible causa:** algunas aplicaciones tienen diferentes parámetros initString en el elemento crypto de la configuración (u otros parámetros criptográficos).
- **Posible solución**: use el mismo initString en todas las aplicaciones (además de todos los parámetros de crypto restantes del elemento de creación de LW-SSO).
- **Posible causa:** algunas aplicaciones tienen una diferencia, en hora GMT, superior a 15 minutos.
- **Posible solución**: asegúrese de que todas las aplicaciones que participan en una integración LW-SSO tienen la misma hora GMT con una diferencia máxima de 15 minutos.
- **Posible causa:** un vínculo de dominio múltiple va del recurso protegido (HTTPS) al no protegido (HTTP).
- **Posible solución**: al vincular un dominio a otro o trabajar con vínculos cruzados, asegúrese de que la primera petición de vínculo/trabajo cruzado va de un recurso protegido (HTTPS) a otro recurso protegido (HTTPS).

Compatibilidad con IPv6: solución de problemas y limitaciones

Limitaciones

- La dirección URL no puede contener una dirección IP.
- El sistema operativo debe admitir IPv6 y IPv4. Si la dirección IPv4 no está cerrada o no se admite, no podrá conectarse al servidor de Configuration Manager.
- Siempre que se cambia la hora en el servidor Tomcat de Configuration Manager es preciso reiniciar el servidor para actualizar la hora del mismo.

Solución de problemas

Problema. Tras configurar una conexión de UCMDB como una dirección IPv6 durante la instalación, la opción de menú **Administración > UCMDB Foundation** no funciona.

Solución. Realice las siguientes operaciones:

1. Diríjase a **Sistema > Configuración > Integraciones > UCMDB Foundation > UCMDB Foundation.**
2. Añada corchetes a la dirección IP del campo URL de acceso a UCMDB. La dirección URL debe ser similar a la siguiente: http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/.
3. Guarde el conjunto de configuración y actívelo.
4. Reinicie Configuration Manager.

Autenticación: solución de problemas y limitaciones

En esta sección se describen problemas conocidos relativos a la autenticación.

Problema: Durante la autenticación de una aplicación después de realizar la redirección a un punto de autenticación recibe el error 500.

- **Posible causa:** Las aplicaciones WAR y BSF.WAR de Configuration Manager tienen diferentes parámetros initString en el elemento crypto de la configuración (u otros parámetros de crypto).
- **Posible solución:**use el mismo initString en las dos aplicaciones (además de todos los parámetros de crypto restantes del elemento de creación de LW-SSO).

Problema: Durante la autenticación de una aplicación después de realizar la redirección a un punto de autenticación no ve el formulario de inicio de sesión.

Solución: La cookie de la sesión de autenticación de Configuration Manager se bloquea o se deniega al usar la versión 6.0, 7.0 o 8.0 de Internet Explorer. Agregue el servidor de Configuration Manager a la zona **Intranet/De confianza** de las zonas de seguridad de Internet Explorer en el equipo (**Herramientas** > **Opciones de Internet** > **Seguridad** > **Intranet local** > **Sitios** > **Opciones avanzadas**). De esta forma se aceptarán todas las cookies.

Problema: Después de la autenticación, recibe el error 403.

- **Posible causa:** un dominio no está definido correctamente en el elemento LW-SSO de la configuración de la aplicación.
- **Posible solución:** asegúrese de que el dominio definido en el elemento LW-SSO de la configuración de la aplicación coincide con el dominio de la aplicación.
- **Posible causa:** no ha accedido a la aplicación con el nombre de dominio completo (FQDN) en la dirección URL de inicio de sesión cuando hay un dominio definido en la configuración de LW-SSO (por ejemplo: http://192.168.12.13/WebApp).

➤ **Posible solución:** asegúrese de que accede a la aplicación con el nombre de dominio completo en la dirección URL de conexión (por ejemplo: http://myserver.companydomain.com/WebApp).

Problema: Después de la autenticación, aparece la página **Obtener detalles de usuario de Acegi**.

Solución: La cookie de la sesión de autenticación de Configuration Manager se bloquea o se deniega al usar la versión 6.0, 7.0 o 8.0 de Internet Explorer. Agregue el servidor de Configuration Manager a la zona **Intranet/De confianza** de las zonas de seguridad de Internet Explorer en el equipo (**Herramientas** > **Opciones de Internet** > **Seguridad** > **Intranet local** > **Sitios** > **Opciones avanzadas**). De esta forma se aceptarán todas las cookies.