HP Universal CMDB y Configuration Manager

Versión de software: 10.10

Guía del sistema de protección

Fecha de publicación del documento: Noviembre 2013

Fecha de lanzamiento del software: Noviembre 2013

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 es responsable de omisiones, errores técnicos o de edición contenidos en el presente documento.

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

Leyenda 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.

Aviso de copyright

Avisos de marcas comerciales

Adobe™ es una marca comercial de Adobe Systems Incorporated.

Microsoft® y Windows® son marcas comerciales registradas estadounidenses de Microsoft Corporation.

UNIX® es una marca comercial registrada de The Open Group.

Actualizaciones de la documentación

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

- Número de versión del software, que indica la versión del software.
- 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 buscar actualizaciones recientes o verificar que está utilizando la edición más reciente de un documento, visite: **http://h20230.www2.hp.com/selfsolve/manuals**

Este sitio requiere que esté registrado como usuario de HP Passport. Para registrarse y obtener un ID de HP Passport, visite: **http://h20229.www2.hp.com/passport-registration.html**

O haga clic en el enlace **New user registration** (Registro de nuevos usuarios) de la página de registro de HP Passport.

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

Soporte

Visite el sitio web HP Software Support Online en: **http://www.hp.com/go/hpsoftwaresupport**

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

HP Software Support Online brinda a los clientes la posibilidad de auto-resolución de problemas. Ofrece una forma rápida y eficaz de acceder a las herramientas de soporte técnico interactivo necesarias para gestionar su negocio. Como cliente preferente de soporte, puede beneficiarse de utilizar el sitio web de soporte para:

- Buscar los documentos de la Base de conocimiento que le interesen
- Enviar y realizar un seguimiento de los casos de soporte y las solicitudes de mejora
- Descargar revisiones de software
- Gestionar contratos de soporte
- 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

HP Software Solutions Now accede al sitio web HPSW Solution and Integration Portal. Este sitio le permite explorar las soluciones de productos HP que satisfacen sus necesidades de negocio e incluye una lista completa de integraciones entre productos HP, así como una lista de procesos ITIL. La URL de este sitio web es **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contenido

Capítulo 1: Introducción al sistema de protección

Este capítulo incluye:

Información general del sistema de protección

Esta sección presenta el concepto de aplicación HP Universal CMDB 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.

HP Universal CMDB 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 implementar un HP Universal CMDB más seguro (reforzado).

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

Es muy recomendable usar un proxy inverso con HP Universal CMDB para obtener una arquitectura segura. Para obtener más información sobre la configuración de un proxy inverso para utilizarlo con HP Universal CMDB, consulte "Utilización de un proxy inverso" en la página 39.

Si debe usar con HP Universal CMDB un tipo de arquitectura segura distinto del que se describe en este documento, póngase en contacto con el soporte técnico de HP para determinar cuál es la arquitectura más adecuada para usar.

Para obtener más información sobre el sistema de protección de Data Flow Probe, consulte "Sistema de protección de Data Flow Probe" en la página 72.

Nota:

- Los procedimientos del sistema de protección se basan en la suposición de que el usuario solo va a implementar las instrucciones que se proporcionan en estos capítulos y que no va a llevar a cabo otros pasos del sistema de protección documentados en otros lugares.
- Aunque los procedimientos del sistema de protección 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 los siguientes capítulos se van a llevar a cabo en equipos dedicados a HP Universal CMDB. El uso de los equipos para otros fines, además de para HP Universal CMDB, 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 informatizados.

Preparativos del sistema de protección

- 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 HP Universal CMDB en la red.
- Debe conocer a la perfección tanto el marco técnico como las capacidades de seguridad de HP Universal CMDB.
- Revise todas las directivas del sistema de protección
- Verifique que HP Universal CMDB funciona a la perfección antes de iniciar los procedimientos del sistema de protección.
- En todos los capítulos, siga los pasos del procedimiento del sistema de protección de forma cronológica. Por ejemplo, si decide configurar el servidor de HP Universal CMDB para que admita SSL, lea "Habilitar la comunicación de Capa de sockets seguros (SSL)" en la página 17 y, a continuación, siga todas las instrucciones cronológicamente.
- HP Universal CMDB no admite la autenticación básica con contraseñas en blanco. No utilice una contraseña en blanco cuando configure los parámetros de conexión de autenticación básica.

Sugerencia: Imprima los procedimientos del sistema de protección y vaya marcándolos a medida que los implemente.

Implementar UCMDB en una arquitectura segura

Se recomienda tomar varias medidas para desplegar los servidores de HP Universal CMDB de forma segura:

- **Arquitectura DMZ con un servidor de seguridad**

  La arquitectura segura a la que se hace referencia en este documento es una arquitectura DMZ típica que utiliza un dispositivo como servidor de seguridad. El concepto básico de dicha arquitectura es crear una separación completa y evitar el acceso directo entre los clientes de HP Universal CMDB y el servidor de HP Universal CMDB.

- **Explorador seguro**

  Internet Explorer y Firefox en un entorno Windows deben configurarse para controlar de forma segura las cookies, los applets y las secuencias de comandos Java.

- **Protocolo de comunicación SSL**

  El protocolo Capa de sockets seguros (SSL) protege la conexión entre el cliente y el servidor. Las direcciones URL que requieren una conexión SSL utilizan una versión segura (HTTPS) del protocolo de transferencia de hipertexto. Para obtener más información, consulte "Habilitar la comunicación de Capa de sockets seguros (SSL)" en la página 17.

- **Arquitectura de proxy inverso**

  Una de las soluciones más seguras y recomendadas sugiere desplegar HP Universal CMDB utilizando un proxy inverso. HP Universal CMDB es totalmente compatible con la arquitectura segura de proxy inverso. Para obtener más información, consulte "Utilización de un proxy inverso" en la página 39.

Acceso al sistema

Sistema de protección de acceso a Java JMX

Nota: El procedimiento que se describe aquí también se puede utilizar para JMX de Data Flow Probe.

Para garantizar que el puerto RMI de JMX es accesible solo cuando se proporcionan las credenciales de usuario, siga este procedimiento:

1. En el archivo **wrapper.conf** del servidor, que se encuentra en **C:\hp\UCMDB\UCMDBServer\bin**, ajuste lo siguiente:

   wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true

Esta configuración requiere que JMX solicite la autenticación.

- **Para JMX de Data Flow Probe**, realice lo siguiente:

  En los archivos **WrapperGateway.conf** y **WrapperManager.conf**, que se encuentran en **C:\hp\UCMDB\DataFlowProbe\bin**, ajuste lo siguiente:

  wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true

2. Cambie el nombre del archivo **jmxremote.password.template** (que se encuentra en: **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) a **jmxremote.password**.

   Nota: Para JMX de Data Flow Probe, este archivo se encuentra en: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

3. En **jmxremote.password**, agregue contraseñas para las funciones **monitorRole** y **controlRole**.

   Por ejemplo:

   monitorRole QED

   controlRole R&D

   asignaría la contraseña **QED** a **monitorRole** y la contraseña **R&D** a **controlRole**.

   Nota: Asegúrese de que solamente el propietario tenga permisos de lectura y escritura en **jmxremote.password**, ya que contiene las contraseñas en texto sin cifrar. El propietario del archivo debe ser el mismo usuario con el que se ejecuta el servidor UCMDB.

4. En el archivo **jmxremote.access** (que se encuentra en **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**), asigne acceso a **monitorRole** y **controlRole**.

   Por ejemplo:

   monitorRole readonly

   controlRole readwrite

   asignaría acceso de solo lectura a**monitorRole** y acceso de lectura o escritura a **controlRole**.

   Nota: Para JMX de Data Flow Probe, este archivo se encuentra en: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

5. Proteja los archivos de la siguiente manera:

   - **En Windows solamente:** Ejecute los siguientes comandos desde la línea de comandos para proteger los archivos:

     cacls jmxremote.password /P <nombre de usuario>:F

     cacls jmxremote.access /P <nombre de usuario>:R

     donde **<nombre de usuario>** es el propietario del archivo visible en las propiedades de ambos archivos. Abra las propiedades de esos archivos y asegúrese de que sean correctas y solo tengan un propietario.

   - **En sistemas operativos Solaris y Linux:** Ajuste los permisos de archivo para el archivo de contraseña ejecutando:

     chmod 600 jmxremote.password

6. **Para actualizaciones de Service Pack, migraciones de servidor y recuperación ante desastres:** Cambie la propiedad del archivo **jmxremote.access** (que se encuentra en **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) al sistema operativo que ejecuta la instalación de actualización o migración.

   Nota:

   - Para JMX de Data Flow Probe, este archivo se encuentra en: **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.
   - Antes de desinstalar el producto, edite los permisos de archivo para **<carpeta de instalación de UMCDB>\bin\jre\lib\management\jmxremote.password**, de forma que pueda editarlo el usuario con el que haya iniciado sesión.

Cambio del nombre de usuario o la contraseña del sistema en la consola JMX

La consola JMX utiliza usuarios del sistema, es decir, usuarios de varios clientes en un entorno multiempresa. Puede iniciar sesión en la consola JMX con cualquier nombre de usuario del sistema. El nombre y la contraseña predeterminados son **sysadmin/sysadmin**..

Puede cambiar la contraseña a través de la consola JMX o de la herramienta Administración de servidor.

Para cambiar el nombre de usuario o la contraseña predeterminados del sistema a través de la consola JMX:

1. Inicie un explorador web y escriba la siguiente dirección: **http://localhost.<nombre de dominio>:8080/jmx-console**.

2. Especifique las credenciales de autenticación de la consola de JMX.
3. Localice **UCMDB:service=Authorization Services** y haga clic en el vínculo para abrir la página de operaciones.
4. Localice la operación **resetPassword**.
   - En el campo **userName**, escriba **sysadmin**.
   - En el campo **password**, escriba una contraseña nueva.
5. Haga clic en **Invoke** para guardar el cambio.

Para cambiar el nombre de usuario o la contraseña predeterminados del sistema a través de la herramienta Administración de servidor:

1. **En Windows:** ejecute el siguiente archivo: **C:\hp\UCMDB\UCMDBServer\tools\server_management.bat.**

   En Linux: Ejecute **server_management.sh**, que se encuentra en la siguiente carpeta: **/opt/hp/UCMDB/UCMDBServer/tools/**.
2. Inicie sesión en la herramienta con las credenciales de autenticación: **sysadmin/sysadmin**.
3. Haga clic en el vínculo Usuarios.
4. Seleccione el usuario del sistema y haga clic en **Cambiar contraseña de usuario con sesión iniciada**.
5. Escriba la contraseña antigua y la contraseña nueva y haga clic en **Aceptar**.

Cambio del usuario del servicio del servidor de HP Universal CMDB

En una plataforma Windows, el servicio de HP Universal CMDB, que ejecuta todos los procesos y servicios de HP Universal CMDB, se instala cuando se ejecuta la utilidad de Configuración de servidores y bases de datos. De forma predeterminada, este servicio se ejecuta con el usuario del sistema local. Sin embargo, es posible que sea necesario asignar otro usuario para ejecutar el servicio (por ejemplo, si utiliza la autenticación NTLM).

El usuario asignado para ejecutar el servicio debe tener los siguientes permisos:

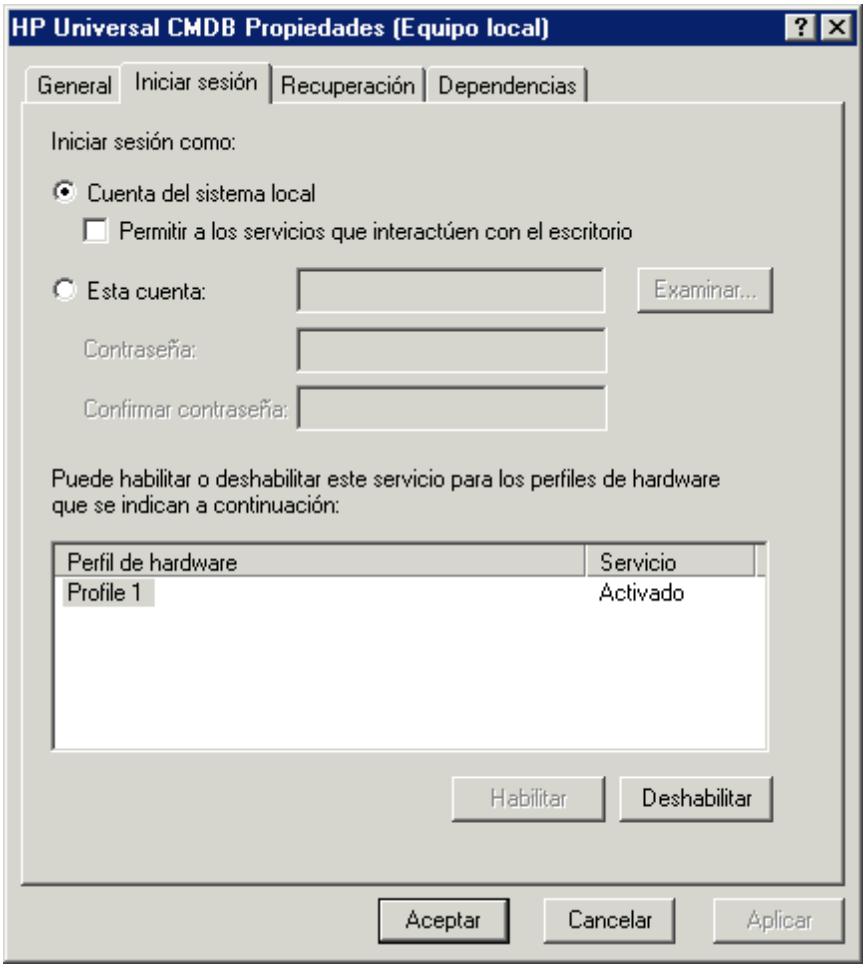
- permisos de base de datos suficientes (definidos por el administrador de bases de datos)
- permisos de red suficientes
- permisos de administrador en el servidor local

Para cambiar el usuario del servicio:

1. Deshabilite HP Universal CMDB a través del menú Inicio (**Inicio > Todos los programas > HP UCMDB > Detener HP Universal CMDB Server**) o deteniendo el servicio del servidor de HP Universal CMDB. Para obtener más información, consulte la sección que describe cómo iniciar y detener el servicio del servidor UCMDB en la *HP Universal CMDB – Guía de administración*.

2. En la ventana **Servicios** de Windows, haga doble clic en **UCMDB_Server**. Se abre el cuadro de diálogo **UCMDB_Server Propiedades (Equipo local)**.

3. Haga clic en la ficha Iniciar sesión.



4. Seleccione **Esta cuenta** y elija otro usuario en la lista de usuarios válidos en el equipo.

5. Introduzca la contraseña de Windows del usuario seleccionado y confírmela.

6. Haga clic en **Aplicar** para guardar la configuración y en **Aceptar** para cerrar el cuadro de diálogo.

7. Habilite HP Universal CMDB a través del menú Inicio (**Inicio > Todos los programas >HP UCMDB > Iniciar HP Universal CMDB Server**) o iniciando el servicio del servidor de HP

Universal CMDB. Para obtener más información, consulte la sección que describe cómo iniciar y detener el servicio del servidor UCMDB en la *HP Universal CMDB – Guía de administración*.

Cifrar la contraseña de la base de datos para Configuration Manager

La contraseña de base de datos de CM 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 para el cifrado de la contraseña de la base de datos de Configuration Manager" abajo

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\database.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 archivo ***directorio de instalación de Configuration Manager*>\security\encrypt_repository** y genera el archivo de cifrado.
3. Ejecute la utilidad **bin\encrypt-password.bat** 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 para el cifrado de la contraseña de la base de datos de Configuration Manager

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 de CM. Para obtener más información sobre el cifrado de la contraseña de la base de datos, consulte "Cifrar la contraseña de la base de datos para Configuration Manager" arriba.

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, solo se admite **archivo binario**.
binaryFileStorageName	Indica el lugar del archivo en el que se almacena la clave maestra.
cipherType	El tipo de cifrado. Actualmente, solo 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

Parámetro	Descripción
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, solo se admite **CBC**.
algorithmPaddingName	El algoritmo de relleno que se usa. Las siguientes opciones están disponibles: • **PKCS7Padding** (opción predeterminada) • **PKCS5Padding**
jceProviderName	El nombre del algoritmo de cifrado JCE. **Nota:** Solo es relevante cuando crytpSource es jce. Para lw, se usa engineName.

Capítulo 2: Habilitar la comunicación de Capa de sockets seguros (SSL)

Este capítulo incluye:

Habilitar SSL en el equipo servidor con un certificado autofirmado - UCMDB

En estas secciones se explica cómo configurar HP Universal CMDB para que admita la comunicación mediante el canal Capa de sockets seguros (SSL).

1. **Requisitos previos**

   a. Antes de iniciar el siguiente procedimiento, elimine el **server.keystore** antiguo que está ubicado en **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

   b. Coloque el almacén de claves de HP Universal CMDB (tipo JKS) en la carpeta **C:\hp\UCMDB\UCMDBServer\conf\security**.

2. **Generar un almacén de claves del servidor**

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

   - Desde **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, ejecute el siguiente comando:

     ```
     keytool -genkey -alias hpcert -keystore
     C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
     ```

     Se abre el cuadro de diálogo de la consola.

   - Escriba la contraseña del almacén de claves. Si la contraseña ha cambiado, ejecute la operación **changeKeystorePassword** de JMX, en **UCMDB:service=Security Services**. Si la contraseña no ha cambiado, utilice la contraseña **hppass** predeterminada.

   - Responda a la pregunta por su nombre y sus apellidos. Escriba el nombre del servidor web de HP Universal CMDB. 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 **server.keystore** con un certificado de servidor llamado **hpcert**.

   b. Exporte el certificado autofirmado a un archivo:

   Desde **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, ejecute el siguiente comando:

   ```
   keytool -export -alias hpcert -keystore
   C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <su
   contraseña> -file hpcert
   ```

3. **Colocar el certificado en el almacén de confianza del cliente**

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

   Nota: En **server.keystore**, no puede haber más de un certificado de servidor.

4. **Deshabilitar el puerto HTTP 8080**

   Para obtener más información, consulte "Habilitar o deshabilitar puertos HTTP/HTTPS" en la página 32.

Nota: Antes de cerrar el puerto HTTP, compruebe que la comunicación HTTPS funciona.

5. **Reiniciar el servidor**

6. **Mostrar HP Universal CMDB**

   Para comprobar que el servidor UCMDB es seguro, escriba la siguiente dirección URL en el explorador web: **https://<nombre o dirección IP de servidor UCMDB>:8443/ucmdb-ui**.

Habilitar SSL en el equipo servidor con un certificado autofirmado - Configuration Manager

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

Configuration Manager usa Tomcat 7.0.19 como servidor de aplicaciones.

1. **Requisitos previos** (no es relevante si va a instalar por primera vez)

   Antes de iniciar el siguiente procedimiento, elimine el antiguo archivo **tomcat.keystore** que se encuentra en la carpeta **<*directorio de instalación de Configuration Manager*>\java\windows\x86_64\lib\security** o la carpeta **<*directorio de instalación de Configuration Manager*>\java\linux\x86_64\lib\security** (la que sea relevante), si existe.

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 **<*directorio de instalación de Configuration Manager*>\java\windows\x86_64\bin** o **<*directorio de instalación de Configuration Manager*>\java\linux\x86_64\bin**, ejecute el comando siguiente:

     ```
     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.

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

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="8143"
   ```

   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 del archivo tomcat.keystore>"
   keystorePass="<contraseña>"
   ```

   (consulte el paso 2)

   Convierta la siguiente línea en comentario:

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

   Nota: No debe bloquear el puerto de la conexión HTTP. Si desea bloquear la comunicación HTTP, puede usar un servidor de seguridad para ello.

5. **Reiniciar el servidor**

   Reinicie el servidor de Configuration Manager.

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 del servidor o dirección IP de Configuration Manager>:8143/cnc**.

7. En Configuration Manager, vaya a **Configuración > Gestión de aplicaciones> Configuración de correo** y cambie el protocolo y el puerto en **Dirección URL completa de Configuration Manager**, de acuerdo a los valores indicados anteriormente.

8. En UCMDB, vaya a **Administrador de configuración de infraestructura > Configuración**

general y cambie el protocolo y el puerto en **URL de Configuration Manager**, de acuerdo a los valores indicados anteriormente.

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 - UCMDB

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, elimine el **server.keystore** antiguo, que está ubicado en **C:\hp\UCMDB\UCMDBServer\conf\security\server.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: **C:\hp\UCMDB\UCMDBServer\conf\security**.

   d. Abra el símbolo del sistema y cambie el directorio a **C:\hp\UCMDB\UCMDBServer\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 c:\hp\UCMDB\UCMDBServer\conf\securit
   y\<nombre de archivo pfx> -srcstoretype PKCS12 -destkeystore server.keyst
   ore
   ```

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

e. Escriba la contraseña del almacén de claves de destino. Debe ser la misma contraseña que la que se definió previamente en el método **changeKeystorePassword** de JMX, en Security Services. Si la contraseña no ha cambiado, utilice la contraseña **hppass** predeterminada.

> **Nota:** La contraseña del almacén de claves de origen debe ser la misma que la contraseña del almacén de claves de destino.

f. Después de generar el certificado, deshabilite el puerto HTTP 8080. Para obtener más información, consulte "Habilitar o deshabilitar puertos HTTP/HTTPS" en la página 32.

g. Si ha utilizado una contraseña distinta de **hppass** o la contraseña usada en el archivo **.pfx** ejecute el método **changeKeystorePassword** de JMX y asegúrese de que la clave tiene la misma contraseña.

> **Nota:** Antes de cerrar el puerto HTTP, compruebe que la comunicación HTTPS funciona.

3. **Reiniciar el servidor**

4. **Verificar la seguridad del servidor**

   Para verificar que el servidor UCMDB es seguro, escriba la siguiente dirección URL en el explorador web: **https://<nombre o dirección IP de servidor UCMDB>:8443/ucmdb-ui**.

> **Precaución:** En **server.keystore**, no puede haber más de un certificado de servidor.

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

En Configuration Manager, 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, elimine el antiguo archivo **tomcat.keystore** que se encuentra en la carpeta **<*directorio de instalación de Configuration Manager*>\java\windows\x86_64\lib\security** o la carpeta **<directorio de instalación de Configuration Manager>\java\linux\x86_64\lib\security** (la que sea relevante), si existe.

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.

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

   c. Abra el símbolo del sistema y cambie el directorio a ***<directorio de instalación de Configuration Manager>*\java\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 Config
      uration Manager>\conf\security\<nombre de archivo pfx> -srcstoretype PKCS
      12 -destkeystore tomcat.keystore
      ```

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

3. **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="8143"
   ```

   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" />
   ```

   Nota: No debe bloquear el puerto de la conexión HTTP. Si desea bloquear la comunicación HTTP, puede usar un servidor de seguridad para ello.

4. **Reiniciar el servidor**

   Reinicie el servidor de Configuration Manager.

5. **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 del servidor o dirección IP de Configuration Manager>:8143/cnc**.

6. En Configuration Manager, vaya a **Configuración > Gestión de aplicaciones> Configuración de correo** y cambie el protocolo y el puerto en **Dirección URL completa de Configuration Manager**, de acuerdo a los valores indicados anteriormente.

7. En UCMDB, vaya a **Administrador de configuración de infraestructura > Configuración general** y cambie el protocolo y el puerto en **URL de Configuration Manager**, de acuerdo a los valores indicados anteriormente.

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

Habilitar SSL en los equipos cliente - UCMDB

Si el certificado que usa el servidor web de HP Universal CMDB 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 explorador web no confía en la entidad de certificación, debe importar la ruta completa de confianza del certificado o importar el certificado que utiliza HP Universal CMDB de forma explícita en el almacén de confianza del explorador.

El siguiente ejemplo muestra cómo importar el certificado autofirmado **hpcert** en el almacén de confianza de Windows para Internet Explorer.

Para importar un certificado en el almacén de confianza de Windows:

1. Localice el certificado **hpcert** y cámbiele el nombre a **hpcert.cer**.

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

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

3. Siga las instrucciones para habilitar la confianza instalando el certificado con el Asistente para importación de certificados.

Nota: Otro método para importar en el explorador web el certificado que emite el servidor UCMDB consiste en iniciar sesión en UCMDB e instalar el certificado cuando se muestra la advertencia que indica que el certificado no es de confianza.

Habilitar SSL con un certificado de cliente - Configuration Manager

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 en la carpeta **<*directorio de instalación de Configuration Manager*>\java\windows\x86_64bin**.
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 -i
   mport
   -alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
   ```

4. Modifique el archivo **server.xml** (que se encuentra en **<*directorio de instalación de Configuration Manager*>\servers\server-0\conf**) de la manera siguiente:

   a. Realice los cambios que se describen en "Modificar el archivo server.xml" en la página 23.

   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 tal y como se describe en "Verificar la seguridad del servidor" en la página precedente.

Habilitar SSL en el SDK del cliente

Puede utilizar el transporte HTTPS entre el SDK del cliente y el SDK del servidor:

1. En el equipo cliente, en el producto que incrusta el SDK del cliente, localice la configuración de transporte y asegúrese de que está establecida en HTTPS y no en HTTP.

2. Descargue el certificado de CA o el certificado público autofirmado en el equipo cliente, e impórtelo en el almacén de confianza **cacerts** del JRE que va a conectarse al servidor.

   Use el siguiente comando:

   ```
   Keytool -import -alias <nombre de CA> -trustcacerts -file <ruta de certifica
   do público del servidor> -keystore <ruta al almacén cacerts de confianza del
   jre cliente (p. ej., x:\archivos de programa\java\jre\lib\security\cacerts)>
   ```

Habilitar la autenticación de certificados manual en el SDK

Este modo utiliza SSL y permite tanto la autenticación del servidor por parte de UCMDB como la autenticación de cliente por parte del cliente UCMDB-API. Tanto el servidor como el cliente UCMDB-API envían sus certificados a la otra entidad para su autenticación.

Nota: El siguiente método, que consiste en habilitar SSL en el SDK con autenticación mutua, es el más seguro de los métodos y, por lo tanto, es el modo de comunicación recomedado.

1. Proteja el conector del cliente UCMDB-API en UCMDB:

   a. Acceda a la consola JMX de UCMDB: Inicie un explorador web y escriba la siguiente dirección: **http://<nombre de equipo o dirección IP de UCMDB>:8080/jmx-console**. Es posible que deba iniciar sesión con un nombre de usuario y una contraseña (los valores predeterminados son sysadmin/sysadmin).

   b. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.

   c. Localice la operación **PortsDetails** y haga clic en **Invoke**. Anote el número de puerto de HTTPS con autenticación de cliente. El valor predeterminado es 8444 y debería estar habilitado.

   d. Vuelva a la página de operaciones.

   e. Para asignar el conector ucmdb-api al modo de autenticación mutua, llame al método **mapComponentToConnectors** con los siguientes parámetros:

      - **componentName**: ucmdb-api
      - **isHTTPSWithClientAuth**: true
      - Todos los demás indicadores: false

Se muestra el siguiente mensaje:

Operation succeeded. Component ucmdb-api is now mapped to: HTTPS_CLIENT_AUTH ports.

f. Vuelva a la página de operaciones.

2. Asegúrese de que el JRE que ejecuta el cliente UCMDB-API tiene un almacén de claves que contiene un certificado de cliente.

3. Exporte el certificado de cliente UCMDB-API de su almacén de claves.

4. Importe el certificado de cliente UCMDB-API exportado al almacén de confianza del servidor UCMDB.

   a. En el equipo donde está instalado UCMDB, copie el archivo del certificado de cliente UCMDB-API creado en el siguiente directorio en UCMDB:

   C:\HP\UCMDB\UCMDBServer\conf\security

   b. Ejecute el siguiente comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
   C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <
   certificado de cliente UCMDB-api> - alias ucmdb-api
   ```

   c. Introduzca la contraseña del almacén de confianza del servidor UCMDB (el valor predeterminado es **hppass**).

   d. Cuando se le pregunte **Trust this certificate?**, pulse **y** y, a continuación **Intro**.

   e. Asegúrese de que aparece el mensaje **Certificate was added to keystore**.

5. Exporte el certificado de servidor UCMDB de su almacén de claves.

   a. En el equipo donde está instalado UCMDB, ejecute el siguiente comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert
   -keystore
   C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore
   -file C:\HP\UCMDB\conf\security\server.cert
   ```

   b. Introduzca la contraseña del almacén de confianza del servidor UCMDB (el valor predeterminado es **hppass**).

   c. Compruebe que el certificado se crea en el siguiente directorio:

   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

6. Importe el certificado de UCMDB exportado en el JRE del almacén de confianza del cliente UCMDB-API.

7. Reinicie el servidor UCMDB y el cliente UCMDB-API.

8. Para conectar del cliente UCMDB-API al servidor UCMDB-API, use el siguiente código:

```
UcmdbServiceProvider provider = UcmdbServiceFactory.getServiceProvider
("https", <SOME_HOST_NAME>, <HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER
(default:8444>));
UcmdbService ucmdbService = provider.connect(provider.createCertificateCrede
ntials(<TheClientKeystore.
e.g: "c:\\client.keystore">, <KeystorePassword>), provider.createClientConte
xt(<ClientIdentification>));
```

Configurar la compatibilidad con CAC en UCMDB

En esta sección se describe cómo configurar la compatibilidad con las tarjetas de acceso común (CAC) en UCMDB.

Nota: La compatibilidad con CAC solo está disponible con Internet Explorer 8, 9 o 10.

1. Importe los certificados de CA raíz e intermedios en el almacén de confianza de UCMDB de la siguiente manera:

   a. En el equipo donde está instalado UCMDB, copie los archivos de certificado en el siguiente directorio en UCMDB:

      C:\HP\UCMDB\UCMDBServer\conf\security

      Nota: Si su certificado está en formato Microsoft p7b, es posible que tenga que convertirlo al formato PEM.

   b. Por cada certificado, ejecute el siguiente comando:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file
<certificado> - alias <alias de certificado>
```

   c. Introduzca la contraseña del almacén de confianza del servidor UCMDB (el valor predeterminado es **hppass**).

   d. Cuando se le pregunte **Trust this certificate?**, pulse **y** y, a continuación **Intro**.

   e. Asegúrese de que aparece el mensaje **Certificate was added to keystore**.

2. Abra la consola JMX iniciando el explorador web e introduzca la dirección del servidor de la siguiente manera: http://<IP o nombre de host del servidor UCMDB>:8080/jmx-console.

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

3. En UCMDB, haga clic en **UCMDB:service=Ports Management Services** para abrir la página de operaciones.

   - (Opcional) Haga clic en **ComponentsConfigurations**. Realice las siguientes operaciones:
     - Establezca **HTTPSSetPort** en **8444** y haga clic en **Invoke**.
     - Haga clic en **Back to MBean**.
   - Haga clic en **mapComponentToConnectors**. Realice las siguientes operaciones:
     - En el servicio mapComponentToConnectors, establezca **componentName** como **ucmdb-ui**.
     - Establezca solo **isHTTPSWithClientAuth** como **true** y haga clic en **Invoke**.
     - Haga clic en **Back to MBean**.
     - En el servicio mapComponentToConnectors, establezca **componentName** como **root**.
     - Establezca solo **isHTTPSWithClientAuth** como **true** y haga clic en **Invoke**.

4. En UCMDB, haga clic en **UCMDB:service=Security Services** para abrir la página de operaciones. En el servicio **loginWithCAC**, lleve a cabo los pasos descritos a continuación:

   - Establezca **loginWithCAC** como **true** y haga clic en **Invoke**.
   - Haga clic en **Back to MBean**.
   - (Opcional) Haga clic en **usernameField** para especificar el campo del certificado que UCMDB utilizará para extraer un nombre y haga clic en **Invoke**.

     Nota: Si no especifica un campo, se utiliza el valor predeterminado de PRINCIPAL_NAME_FROM_SAN_FIELD.

   - Haga clic en **Back to MBean**.
   - Haga clic en **pathToCRL** para establecer una ruta de acceso para la lista de revocación de certificados (CRL) sin conexión que debe utilizarse en caso de que la lista en línea (del certificado) no esté disponible. Finalmente, haga clic en **Invoke**.

Nota: Cuando se trabaja con una CRL local y hay una conexión a Internet en funcionamiento en el servidor UCMDB, se utiliza la CRL local. La validación de certificados (aunque no estén revocados) falla en las siguientes situaciones:

- Si se ha establecido la ruta de acceso a la CRL pero falta el archivo CRL en sí
- Si la CRL ha caducado
- Si la CRL tiene una firma incorrecta

Si no establece la ruta de una CRL sin conexión y el servidor UCMDB no puede acceder a la CRL en línea, se rechazarán todos los certificados que contengan una CRL o una URL de OCSP (como no se puede acceder a la URL, la comprobación de revocación falla). Para darle acceso a Internet al servidor UCMDB, quite la marca de comentario de las siguientes líneas en el archivo **wrapper.conf** y proporcione un proxy y puerto válidos:

```
#wrapper.java.additional.40=-Dhttp.proxyHost=<PROXY_ADDR>
#wrapper.java.additional.41=-Dhttp.proxyPort=<PORT>
#wrapper.java.additional.42=-Dhttps.proxyHost=<PROXY_ADDR>
#wrapper.java.additional.43=-Dhttps.proxyPort=<PORT>
```

- Haga clic en **Back to MBean**.
- (Opcional) Establezca **onlyCACCerts** como **true** y haga clic en **Invoke**.

  Establezca esta operación como **true** para aceptar únicamente certificados que provengan de un dispositivo CAC físico.

Ahora debería poder iniciar sesión en UCMDB con https://<IP o nombre de host del servidor UCMDB>.<nombre_dominio>:8444.

5. Configure UCMDB para que utilice la autenticación LW-SSO y reinicie el servidor UCMDB.

Para obtener más información sobre la autenticación LW-SSO, consulte "Habilitación del inicio de sesión en HP Universal CMDB con LW-SSO" en la página 99.

Cambiar la contraseña del almacén de claves del servidor

Después de instalar el servidor, se abre el puerto HTTPS y el almacén está protegido con una contraseña no segura (la contraseña predeterminada **hppass**). Si tiene previsto trabajar solamente con SSL, debe cambiar la contraseña.

A continuación se explica el procedimiento para cambiar únicamente la contraseña de **server.keystore**. Sin embargo, debe realizar el mismo procedimiento para cambiar la contraseña de **server.truststore**.

Nota: Debe realizar todos los pasos de este procedimiento.

1. Inicie el servidor UCMDB.
2. Ejecute el cambio de contraseña en la consola JMX:
   a. Inicie el explorador web y especifique la dirección del servidor, del siguiente modo: **http://<Nombre de host del servidor UCMDB>:8080/jmx-console**.

      Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

   b. En UCMDB, haga clic en **UCMDB:service=Security Services** para abrir la página de operaciones.

   c. Localice y ejecute la operación **changeKeystorePassword**.

      Este campo no debe estar vacío y debe tener al menos seis caracteres. La contraseña solo se cambia en la base de datos.
3. Inicie el servidor UCMDB.
4. Ejecute los comandos.

   Desde **C:\hp\UCMDB\UCMBServer\bin\jre\bin**, ejecute los siguientes comandos:

   a. Cambie la contraseña del almacén:

      keytool -storepasswd -new <Nueva_contraseña_almacén_de_datos> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <contraseña_actual_almacén_de_datos>

   b. El siguiente comando muestra la clave interna del almacén de claves. El primer parámetro es el alias. Guarde este parámetro para el siguiente comando:

      keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

   c. Cambie la contraseña de clave (si el almacén no está vacío):

      keytool -keypasswd -alias <alias> -keypass <contraseñaActual> -new <nuevaContraseña> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

   d. Escriba la contraseña nueva.
5. Inicie el servidor UCMDB.
6. Repita el procedimiento para el almacén de confianza del servidor.

Habilitar o deshabilitar puertos HTTP/HTTPS

Puede habilitar o deshabilitar los puertos HTTP y HTTPS desde la interfaz de usuario o desde la consola JMX.

Para habilitar o deshabilitar los puertos HTTP/HTTPS desde la interfaz de usuario:

1. Conéctese a HP Universal CMDB.
2. Seleccione **Administración> Administraciñon de configuración de infraestructura**.
3. Introduzca **http** o **https** en el cuadro **Filtro** (por Nombre) para mostrar la configuración de HTTP.
   - **Habilitar conexiones HTTP(S)**. **True**: el puerto está habilitado. **False**: el puerto está deshabilitado.
4. Reinicie el servidor para aplicar el cambio.

> **Precaución:** el puerto HTTPS se abre de forma predeterminada; si se cierra este puerto se impide el funcionamiento de **Server_Management.bat**.

Para habilitar o deshabilitar los puertos HTTP/HTTPS desde la consola JMX:

1. Inicie un explorador web y escriba la siguiente dirección: http://localhost.<nombre_dominio>:8080/jmx-console.
2. Especifique las credenciales de autenticación de la consola de JMX. Las credenciales predeterminadas son:
   - Nombre de inicio de sesión = **sysadmin**
   - Contraseña = **sysadmin**
3. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
4. Para habilitar o deshabilitar el puerto HTTP, localice la operación **HTTPSetEnable** y configure el valor.
   - **True:** el puerto está habilitado.
   - **False:** el puerto está deshabilitado.
5. Para habilitar o deshabilitar el puerto HTTPS, localice la operación **HTTPSSetEnable** y configure el valor.

- **True:** el puerto está habilitado.
- **False:** el puerto está deshabilitado.

6. Para habilitar o deshabilitar el puerto HTTPS con autenticación de cliente, localice la operación **HTTPSClientAuthSetEnable** y configure el valor.
   - **True:** el puerto está habilitado.
   - **False:** el puerto está deshabilitado.

Asignar los componentes web de UCMDB a los puertos

Puede configurar la asignación de cada componente de UCMDB a los puertos disponibles desde la consola JMX.

Para ver las configuraciones de los componentes actuales:

1. Inicie un explorador web y escriba la siguiente dirección: **http://localhost.<nombre de dominio>:8080/jmx-console**.
2. Especifique las credenciales de autenticación de la consola de JMX. Las credenciales predeterminadas son:

   Nombre de inicio de sesión = **sysadmin**

   Contraseña = **sysadmin**
3. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
4. Localice el método **ComponentsConfigurations** y haga clic en **Invoke**.
5. En cada componente, se muestran los puertos válidos y los puertos asignados actualmente.

Para asignar los componentes:

1. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
2. Localice el método **mapComponentToConnectors**.
3. Introduzca un nombre de componente en el cuadro Value. Seleccione **True** o **False** en cada uno de los puertos según su selección. Haga clic en **Invoke**. El componente seleccionado se asigna a los puertos seleccionados. Para buscar los nombres de componentes, llame al método **serverComponentsNames**.
4. Repita el proceso en cada componente relevante.

Nota:

- Cada componente debe asignarse al menos a un puerto. Si no asigna un componente a ningún puerto, se asigna de forma predeterminada al puerto HTTP.
- Si asigna un componente al puerto HTTPS y al puerto HTTPS con autenticación de cliente, solo se asigna la opción de autenticación de cliente (la otra opción es redundante en este caso).
- Si establece **isHTTPSWithClientAuth** como **true** para el componente UI de UCMDB, también debe establecerlo como **true** para el componente raíz.

También puede cambiar el valor asignado a cada uno de los puertos.

Para configurar los valores de los puertos:

1. Localice **UCMDB:service=Ports Management Services** y haga clic en el vínculo para abrir la página de operaciones.
2. Para configurar un valor en el puerto HTTP, localice el método **HTTPSetPort** e introduzca un valor en el cuadro **Value**. Haga clic en **Invoke**.
3. Para configurar un valor en el puerto HTTPS, localice el método **HTTPSSetPort** e introduzca un valor en el cuadro **Value**. Haga clic en **Invoke**.
4. Para configurar un valor en el puerto HTTPS con autenticación de cliente, localice el método **HTTPSClientAuthSetPort** e introduzca un valor en el cuadro **Value**. Haga clic en **Invoke**.

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.

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

   ```
   keytool -export -alias hpcert -keystore <directorio del servidor UCMDB>
   \conf\security\server.keystore -storepass hppass -file <archivocertificado>
   ```

2. Copie el archivo de certificado en una ubicación temporal en el equipo de Configuration Manager local.
3. Realice una nueva instalación o vuelva a configurar una instalación existente de Configuration Manager. Para obtener instrucciones, consulte las secciones relevantes en la publicación

interactiva de *HP Universal CMDB – Guía de implementación*.

En la pantalla de configuración de UCMDB, establezca el protocolo en HTTPS y elija el archivo de certificado que ha copiado en el paso 2.

4. Copie **hpcert.cer** al equipo servidor en la carpeta **<*directorio de instalación de Configuration Manager*>\java\windows\x86_64\bin**.

5. En el equipo servidor, importe el certificado 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 <directorio de instalación de
   Configuration Manager>\java\windows\x86_64\lib\security\cacerts
   ```

6. Copie **hpcert.cer** al equipo servidor en la carpeta **<*directorio de instalación de Configuration Manager*>\java\ windows\x86_64\lib\security**.

7. Cree un almacén de claves del servidor (tipo JKS) con un certificado autofirmado y una clave privada coincidente. **Desde la carpeta <*directorio de instalación de Configuration Manager*>\java\windows\x86_64\bin**, ejecute el siguiente comando:

   ```
   keytool –genkey –alias tomcat –keyalg RSA –keystore <directorio de instalaci
   ón de Configuration Manager>\java\windows\x86_64\lib\security\tomcat.keystore
   ```

   a. Introduzca una contraseña del almacén de claves.

   b. Para la pregunta `¿Cuál es su nombre y apellidos?`, introduzca el nombre del servidor web de Configuration Manager así como el resto de parámetros en función de su organización.

   c. Escriba una contraseña de la clave. Dicha contraseña DEBE coincidir con la contraseña del almacén de claves. Se creará un almacén de claves JKS llamado **tomcat.keystore** con un certificado de servidor llamado **hpcert**.

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

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

      ```
      Connector port="8143"
      ```

      que aparece como un comentario. Active la secuencia de comandos eliminando el carácter de comentario y agregue las siguientes líneas:

      ```
      keystoreFile="<directorio de instalación de Configuration Manager>\java\w
      indows\x86_64\lib\security\tomcat.keystore"
      keystorePass="password"
      truststoreFile="<directorio de instalación de Configuration Manager>\java
      ```

```
\windows\x86_64\lib\security\cacerts"
truststorePass="changeit" />
```

b. Convierta la siguiente línea en comentario:

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

9. Reinicie el servidor.

Para configurar Configuration Manager para que funcione con otros productos (como equilibradores de carga) que usan 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
<archivocertificado>
```

Habilitar el adaptador KPI de UCMDB para su uso con SSL

Puede configurar la información del adaptador KPI de UCMDB para que se envíe mediante Secure Sockets Layer (SSL).

1. Exporte el certificado de Configuration Manager:

```
<CM_JAVA_HOME>\bin\keytool -export -alias tomcat -keystore
<CM_JAVA_HOME>\lib\security\tomcat.keystore -storepass
<clave del almacén de datos> -file <nombre del archivo de certificado>
```

2. Importe el certificado que ha exportado de Configuration Manager al almacén de confianza de UCMDB de la siguiente manera:

```
<Dir. del servidor de UCMDB>\bin\jre\bin keytool -import -trustcacerts
-alias tomcat -keystore <Dir. del servidor de UCMDB>\bin\jre\lib
\security\cacerts -storepass changeit -file <archivocertificado>
```

3. Importe el certificado que ha exportado de Configuration Manager al almacén de confianza de la sonda de la siguiente manera:

   a. Abra el símbolo del sistema y ejecute el comando:

```
<dir. de DataFlowProbe>\bin\jre\bin\keytool.exe -import -v -keystore
<dir. de DataFlowProbe>\conf\security\hpprobeTrustStore.jks -file
<archivocertificado> -alias tomcat
```

   b. Escriba la contraseña del almacén de claves: logomania

c. Cuando se le pregunte **Trust this certificate?**, pulse **y** y, a continuación **Intro**.

Se muestra el siguiente mensaje:

Certificate was added to keystore.

Para obtener más información sobre el sistema de protección de Data Flow Probe, consulte "Sistema de protección de Data Flow Probe" en la página 72

4. Reinicie UCMDB, Data Flow Probe y Configuration Manager.

Configuración de la compatibilidad con SSL para UCMDB Browser

Nota: Las instrucciones que se proporcionan aquí son relevantes para UCMDB Browser, versión 1.95. Si está utilizando una versión posterior de UCMDB Browser que se ha actualizado por separado del resto del conjunto de productos UCMDB, consulte la sección sobre la configuración de la compatibilidad con SSL en la publicación *HP Universal CMDB Browser Installation and Configuration Guide* para esa versión.

Para instalar y configurar la compatibilidad con SSL en Tomcat:

1. Cree un archivo de almacenamiento de claves para almacenar la clave privada del servidor y el certificado autofirmado ejecutando uno de los siguientes comandos:
   - En Windows: **%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
   - En Unix: **$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

   Para ambos comandos, use el valor de contraseña **changeit** (para todos los otros campos del cuadro de diálogo de la consola que se abre, puede usar cualquier valor).

2. Elimine los comentarios de la entrada **SSL HTTP/1.1 Connector** de **$CATALINA_BASE/conf/server.xml**, donde **$CATALINA_BASE** es el directorio en el que ha instalado Tomcat.

   Nota: Para obtener una descripción completa de cómo configurar **server.xml** para utilizar SSL, consulte el sitio oficial de Apache Tomcat: http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

3. Reinicie el servidor Tomcat.

Para utilizar el protocolo HTTPS para la conexión con el servidor UCMDB:

1. En **ucmdb_browser_config.xml**, asigne el valor **https** a la etiqueta **<protocol>** y asigne el valor de puerto HTTPS del servidor UCMDB (8443 de forma predeterminada) a la etiqueta **<port>.**

2. Descargue el certificado público del Servidor UCMDB en el equipo de UCMDB Browser (si utiliza SSL en el Servidor UCMDB, el administrador de UCMDB puede proporcionarle este certificado) e impórtelo en el almacén de confianza **cacerts** del JRE que se va a conectar al servidor ejecutando el siguiente comando:

   "%JAVA_HOME%\bin\keytool" -import -alias ucmdb -trustcacerts -file <UCMDB-Server-certificate-file> -keystore "%JAVA_HOME%\jre\lib\security\cacerts"

   donde **<UCMDB-Server-certificate-file>** es la ruta de acceso completa al archivo de certificado público del Servidor UCMDB.

3. Reinicie el servidor Tomcat.

Capítulo 3: Utilización de un proxy inverso

Esta sección describe las ramificaciones de seguridad de un proxy inverso y contiene instrucciones para utilizar un proxy inverso con HP Universal CMDB y Configuration Manager. Se tratan los aspectos de seguridad de un proxy inverso, pero no otros aspectos como el almacenamiento en caché y el equilibrio de carga.

Este capítulo incluye:

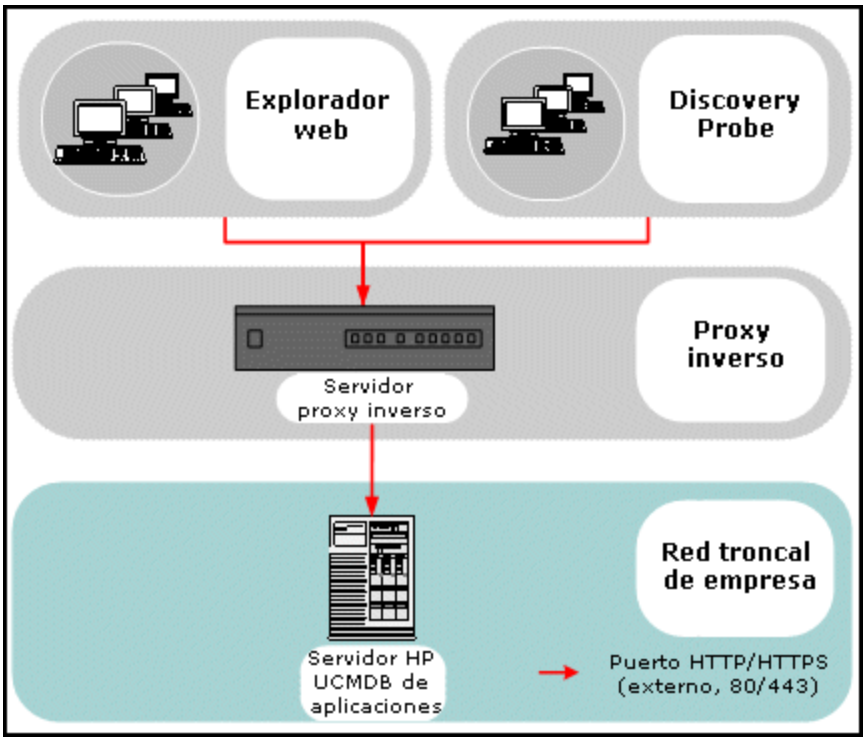
Información general del proxy inverso

Un proxy inverso es un servidor intermedio que se encuentra entre el equipo cliente y los servidores web. En el equipo cliente, el proxy inverso aparece como un servidor web estándar que atiende las solicitudes de protocolo HTTP del equipo cliente.

El equipo cliente envía solicitudes normales de contenido web utilizando el nombre del proxy inverso en lugar del nombre de un servidor web. El proxy inverso envía la solicitud a uno de los servidores web. Aunque el proxy inverso es el que envía la respuesta al equipo cliente, este percibe que ha sido enviada por el servidor web.

Se pueden tener varios proxies inversos, con diferentes direcciones URL, representando la misma instancia de UCMDB/CM. Como alternativa, se puede usar un solo servidor de proxy inverso para tener acceso a varios servidores de UCMDB/CM, estableciendo diferentes contextos de raíz para cada servidor de UCMDB/CM.

HP Universal CMDB y Configuration Manager admiten un proxy inverso en una arquitectura de DMZ. El proxy inverso es un mediador HTTP entre Data Flow Probe, el cliente web y el servidor de HP Universal CMDB/CM.



Nota:

- Los distintos tipos de proxy inverso requieren sintaxis de configuración diferentes. Para ver un ejemplo de una configuración de proxy inverso Apache 2.0.x, consulte "Ejemplo: configuración de Apache 2.0.x " en la página 42.
- Solamente es necesario establecer la configuración de la dirección URL front-end cuando se crea un vínculo directo a un informe mediante el Planificador.

Aspectos de seguridad de la utilización de un servidor proxy inverso

Un servidor proxy inverso funciona como un host defensivo. El proxy está configurado para ser el único equipo al que se dirigen directamente los clientes externos y, por lo tanto, oculta el resto de la red interna. El uso de un proxy inverso permite colocar el servidor de la aplicación en un equipo independiente en la red interna.

Esta sección trata sobre el uso de una red perimetral (DMZ) y un proxy inverso en un entorno de topología opuesta.

A continuación se exponen las principales ventajas de seguridad que supone el uso de un proxy inverso en dicho entorno:

- No se produce ninguna conversión de protocolos de DMZ. El protocolo de entrada y el protocolo de salida son idénticos (solo se produce un cambio de encabezado).
- Solo se permite el acceso HTTP al proxy inverso, lo que significa que los servidores de seguridad de inspección de paquetes con estado pueden proteger mejor la comunicación.
- Se puede definir en el proxy inverso un conjunto restringido y estático de solicitudes de redirección.
- La mayoría de las características de seguridad del servidor web están disponibles en el proxy inverso (métodos de autenticación, cifrado, etc.).
- El proxy inverso filtra las direcciones IP de los servidores reales, además de la arquitectura de la red interna.
- El único cliente accesible del servidor web es el proxy inverso.
- Esta configuración admite servidores de seguridad NAT (al contrario que otras soluciones).
- El proxy inverso requiere un número mínimo de puertos abiertos en el servidor de seguridad.
- El proxy inverso proporciona un buen rendimiento en comparación con otras soluciones defensivas.

Configuración de un proxy inverso

Esta sección describe cómo configurar un proxy inverso. En la versión de UCMDB 10.01, ninguna configuración es necesaria en UCMDB. En el proxy inverso, edite el archivo de configuración en función de la documentación del proxy inverso. Para ver un ejemplo, consulte "Ejemplo: configuración de Apache 2.0.x " en la página siguiente.

Para los trabajos planificados creados antes de UCMDB versión 10.01, también es necesario establecer la configuración en UCMDB de la siguiente manera:

Configurar un proxy inverso mediante la configuración de infraestructura

A continuación se explica el procedimiento para acceder a la configuración de infraestructura para configurar un proxy inverso. Esta configuración solo es necesaria cuando se crea un vínculo directo con un informe mediante el Planificador.

Para configurar un proxy inverso:

1. Seleccione **Administración > Administración de configuración de infraestructura > Configuración general**.
2. Cambie la configuración de **URL del frontend**. Introduzca la dirección; por ejemplo, **https://mi_servidor_proxy:443/**.

Nota: Tras realizar este cambio, no podrá acceder al servidor de HP Universal CMDB directamente a través de un cliente. Para cambiar la configuración del proxy inverso, utilice la

consola JMX en el equipo servidor. Para obtener más información, consulte "Configurar un proxy inverso mediante la consola JMX" a continuación.

Configurar un proxy inverso mediante la consola JMX

Puede realizar cambios en la configuración de proxy inverso mediante la consola JMX en el equipo servidor de HP Universal CMDB. Esta configuración solo es necesaria cuando se crea un vínculo directo con un informe mediante el Planificador.

Para cambiar la configuración de un proxy inverso:

1. En el equipo servidor de HP Universal CMDB, inicie el explorador web e introduzca la siguiente dirección:

   http://<nombre de equipo o dirección IP>.<nombre de dominio>:8080/jmx-console

   donde **<nombre de equipo o dirección IP>** es el equipo en el que está instalado HP Universal CMDB. Es posible que tenga que iniciar sesión con el nombre de usuario y la contraseña.

2. Haga clic en el vínculo **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.

   En el campo **setUseFrontendURLBySettings**, introduzca la dirección URL del servidor proxy; por ejemplo, `https://mi_servidor_proxy:443/`.

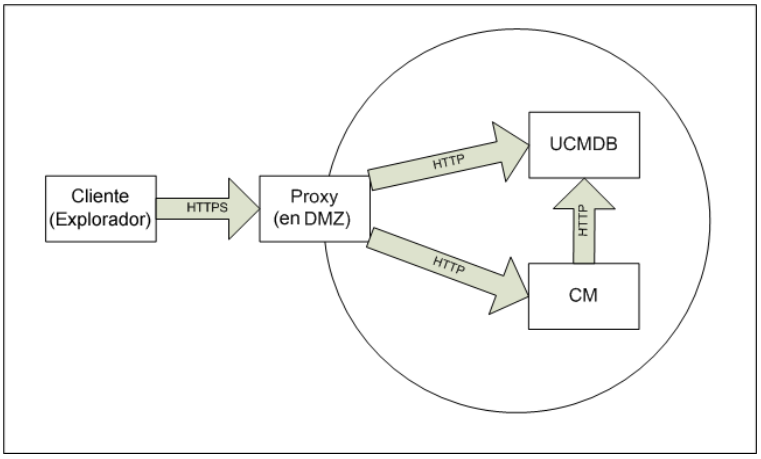
3. Haga clic en **Invoke**.

4. Para ver el valor de esta configuración, utilice el método **showFrontendURLInSettings**.

Ejemplo: configuración de Apache 2.0.x

Esta sección describe un ejemplo de archivo de configuración que admite el uso de un proxy inverso Apache 2.0.x cuando las Data Flow Probes y los usuarios de la aplicación se conectan a HP Universal CMDB.

El siguiente diagrama muestra el proceso de configuración de un proxy inverso para Configuration Manager y UCMDB.



Nota:

- En este ejemplo, el nombre DNS del equipo de HP Universal CMDB y el puerto es UCMDB_server.
- En este ejemplo, el nombre DNS y el puerto de HP Configuration Manger es UCMDB_CM_server.
- Solo deben realizar este cambio aquellos usuarios que tengan conocimientos de administración de Apache.

1. Abra el archivo **<directorio raíz del equipo Apache>\Webserver\conf\httpd.conf**.
2. Habilite los siguientes módulos:
   - **LoadModule proxy_module modules/mod_proxy.so**
   - **LoadModule proxy_http_module modules/mod_proxy_http.so**
3. Agregue las siguientes líneas al archivo **httpd.conf**:

```
ProxyRequests off
<Proxy *>
     Order deny,allow
     Deny from all
     Allow from all
</Proxy>

ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
```

```
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
```

4. Guarde los cambios.

Conexión de Data Flow Probe por proxy inverso o equilibrador de carga mediante autenticación mutua

Siga este procedimiento para conectar Data Flow Probe mediante proxy inverso o equilibrador de carga usando autenticación mutua. Este procedimiento se aplica a la siguiente configuración:

- Autenticación SSL mutua entre la sonda y un proxy inverso o un equilibrador de carga basado en un certificado de cliente proporcionado por la sonda y requerido por el proxy inverso o el equilibrador de carga.
- Una conexión SSL regular entre el proxy inverso o el equilibrador de carga y el servidor de UCMDB.

Nota: Las siguientes instrucciones utilizan el almacén de claves **cKeyStoreFile** como almacén de claves de la sonda. Es un almacén de claves del cliente predefinido que forma parte de la instalación de Data Flow Probe y contiene certificados autofirmados. Para obtener más información, consulte "Almacén de claves y almacén de confianza predeterminados de servidor y Data Flow Probe" en la página 88.

Se recomienda crear un nuevo almacén de claves único que contenga una clave privada recién generada. Para obtener más información, consulte "Crear un almacén de claves para Data Flow Probe" en la página 87.

Obtener un certificado de una entidad de certificación

Obtener el certificado raíz de la entidad de certificación e importarlo en las siguientes ubicaciones:

- almacén de confianza de Data Flow Probe
- certificados de la entidad de certificación de JVM de Data Flow Probe
- almacén de confianza del servidor de UCMDB
- almacén de confianza del proxy inverso

1. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de Data Flow Probe.

   a. Coloque el certificado raíz de la entidad de certificación en el siguiente directorio: <Directorio de instalación de Data Flow Probe>\conf\security\<nombre del archivo de certificado>.

   b. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de Data Flow ejecutando la siguiente secuencia de comandos:

   ```
   <directorio de instalación de Data Flow Probe>\bin\jre\bin\keytool.exe -i
   mport -trustcacerts -alias <SuAlias> -file C:\hp\UCMDB\DataFlowProbe\conf
   \security\<nombre del archivo de certificado> -keystore <directorio de in
   stalación de Data Flow Probe>\conf\security\hpprobeTrustStore.jks
   ```

   La contraseña predeterminada es: **logomania**.

2. Importe el certificado raíz de la entidad de certificación en las entidades de certificación de JVM de Data Flow Probe ejecutando la siguiente secuencia de comandos:

   ```
   <Directorio de instalación de Data Flow Probe>\bin\jre\bin\keytool.exe -impo
   rt -trustcacerts -alias <SuAlias> -file <Directorio de instalación de Data F
   low Probe>\conf\security\<nombre del archivo de certificado> -keystore <Dire
   ctorio de instalación de Data Flow Probe>\bin\jre\lib\security\cacerts
   ```

   La contraseña predeterminada es: **changeit**.

3. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de UCMDB.

   a. Coloque el certificado raíz de la entidad de certificación en el siguiente directorio: <Directorio de instalación de UCMDB>\conf\security\<nombre del archivo de certificado>.

   b. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de UCMDB ejecutando la siguiente secuencia de comandos:

   ```
   <Directorio de instalación de UCMDB>\bin\jre\bin\keytool.exe -import -tru
   stcacerts -alias <YourAlias> -file <Directorio de instalación de UCMDB>\c
   onf\security\<nombre de archivo de certificado> -keystore <Directorio de
   instalación de UCMDB>\conf\security\sever.truststore
   ```

   La contraseña predeterminada es: **hppass**.

4. Importe el certificado raíz de la entidad de certificación en el almacén de confianza de proxy inverso. Este paso depende del servidor.

Convertir el certificado en un almacén de claves Java

Obtenga el certificado del cliente (y la clave privada) para Data Flow Probe de la autoridad de certificación en el formato PFX/PKCS12 y conviértalo en un almacén de claves de Java ejecutando la siguiente secuencia de comandos:

```
<Directorio de instalación de Data Flow Probe>\bin\jre\bin\keytool.exe -importke
ystore -srckeystore <PFX keystore full path> -destkeystore <ruta completa del nu
evo almacén de claves de destino> -srcstoretype PKCS12
```

Se le pedirá el origen de las contraseñas del almacén de claves de origen y destino.

Para la contraseña del almacén de datos de origen utilice la misma contraseña que se usó para exportar el almacén de datos de PFX.

La contraseña del almacén de claves de destino predeterminado para el almacén de datos de Data Flow Probe es: **logomania**.

Nota: Si ha especificado una contraseña del almacén de claves de destino diferente de la contraseña del almacén de claves de Data Flow Probe (logomania), deberá proporcionar la nueva clave en formato cifrado en el archivo **<Directorio de instalación de Data Flow Probe>\conf\ssl.properties** (javax.net.ssl.keyStorePassword). Para obtener más información, consulte "Cifrar las contraseñas del almacén de claves y el almacén de confianza de la sonda" en la página 88.

Coloque el nuevo almacén de claves en el siguiente directorio: **<Directorio de instalación de Data Flow Probe>\conf\security**.

Precaución: No sobrescriba el archivo **hpprobeKeyStore.jks**.

Cambiar el archivo de propiedades de SSL para usar el almacén de claves recién creado

Establezca el almacén de claves que contiene el certificado de cliente en el archivo **<Directorio de instalación de Data Flow Probe>\conf\ssl.properties** en **javax.net.ssl.keyStore**.

Si la contraseña de su almacén de claves no es la contraseña predeterminada del almacén de claves de Data Flow Probe (logomania), actualice **javax.net.ssl.keyStorePassword** tras cifrarlo. Para obtener más información sobre el cifrado de la contraseña, consulte "Cifrar las contraseñas del almacén de claves y el almacén de confianza de la sonda" en la página 88.

Revisar la configuración de Data Flow Probe

Edite el archivo **<Directorio de instalación de Data Flow Probe>\conf\DataFlowProbe.properties** de la siguiente manera:

```
appilog.agent.probe.protocol = HTTPS

serverName = <dirección del servidor proxy inverso>
```

```
serverPortHttps = <el puerto HTTPS que el proxy inverso escucha para redirigir s
olicitudes a UCMDB>
```

Configurar UCMDB para trabajar usando SSL

Para obtener más información, consulte "Habilitar la comunicación de Capa de sockets seguros (SSL)" en la página 17.

Si se crea el certificado del servidor de UCMDB mediante la misma entidad de certificación que creó el resto de certificados de este procedimiento, el proxy inverso o el equilibrador de carga confía en el certificado de UCMDB.

Configurar compatibilidad con CAC en UCMDB por proxy inverso

En esta sección se describe cómo configurar la compatibilidad con las tarjetas de acceso común (CAC) en UCMDB mediante un proxy inverso.

1. Abra la consola JMX iniciando el explorador web e introduzca la dirección del servidor de la siguiente manera: http://<IP o nombre de host del servidor UCMDB>:8080/jmx-console.

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. En UCMDB, haga clic en **UCMDB:service=Ports Management Services** para abrir la página de operaciones.

   - (Opcional) Haga clic en **ComponentsConfigurations**. Realice las siguientes operaciones:
     - Establezca **HTTPSetPort** en **8080** y haga clic en **Invoke**.
     - Haga clic en **Back to MBean**.
   - Haga clic en **mapComponentToConnectors**. Realice las siguientes operaciones:
     - En el servicio mapComponentToConnectors, establezca **componentName** como **ucmdb-ui**.
     - Establezca solo **isHTTP** como **true** y haga clic en **Invoke**.
     - Haga clic en **Back to MBean**.
     - En el servicio mapComponentToConnectors, establezca **componentName** como **root**.
     - Establezca solo **isHTTP** como **true** y haga clic en **Invoke**.

3. En UCMDB, haga clic en **UCMDB:service=Security Services** para abrir la página de operaciones.

- Establezca **loginWithCAC** como **true** y haga clic en **Invoke**.
- Haga clic en **Back to MBean**.
- Establezca **withReverseProxy** como **true** y haga clic en **Invoke**.

  Este parámetro indica al servidor UCMDB que extraiga del encabezado UCMDB_SSL_CLIENT_CERT el nombre de usuario que se utilizará en UCMDB y el certificado que se empleará para la autenticación.
- Haga clic en **Back to MBean**.
- (Opcional) Establezca **onlyCACCerts** como **true** y haga clic en **Invoke**.

  Establezca esta operación como **true** para aceptar únicamente certificados que provengan de un dispositivo CAC físico.

4. Reinicie el servidor de UCMDB.

Ejemplo: configuración de Apache 2.4.4

En esta sección se presenta un ejemplo de archivo de configuración para Apache 2.4.4 (en el archivo **<directorio raíz del equipo Apache> \Webserver\conf\httpd.conf**

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
ServerName Apache_Server_Name:80
Include conf/extra/httpd-ssl.conf
```

En esta sección se presenta un ejemplo de archivo de configuración para Apache 2.4.4 con SSL (en el archivo **<directorio raíz del equipo Apache>\Webserver\conf\httpd.conf**):

```
Listen 8443<VirtualHost _default_:8443>
ServerName Apache_Server_Name:8443
SSLCACertificateFile "c:/Apache24/conf/ssl.crt"
SSLCARevocationFile "c:/Apache24/conf/ssl.crl"
#SSLCARevocationCheck chain|leaf|none
SSLCARevocationCheck leaf
RequestHeader set UCMDB_SSL_CLIENT_CERT %{SSL_CLIENT_CERT}e


ProxyRequests off
<Proxy *>
     Order deny,allow
     Deny from all
     Allow from all
</Proxy>

ProxyPass /mam http://UCMDB_server/mam
```

```
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
SSLVerifyClient require
SSLVerifyDepth  10
SSLOptions+ExportCertData
```

Capítulo 4: Administración de credenciales de Data Flow

Este capítulo incluye:

Información general de la administración de credenciales de Data Flow

Para realizar la detección o ejecutar la integración, debe configurar las credenciales de acceso al sistema remoto. Las credenciales se configuran en la ventana Configuración de Data Flow Probe y se guardan en el servidor de UCMDB. Para obtener más información, consulte la sección que describe la instalación de Data Flow Probe en la *HP Universal CMDB – Guía de Administración de Data Flow*.

El almacenamiento de credenciales se administra en el componente Confidential Manager. Para obtener más información, consulte "Confidential Manager" en la página 107.

Data Flow Probe puede acceder a las credenciales mediante el cliente de Confidential Manager. El cliente de Confidential Manager reside en Data Flow Probe y se comunica con el servidor de Confidential Manager, que reside en el servidor de UCMDB. La comunicación entre el cliente de Confidential Manager y el servidor de Confidential Manager está cifrada y el cliente de Confidential Manager necesita autenticación cuando se conecta al servidor de Confidential Manager.

La autenticación del cliente de Confidential Manager en el servidor de Confidential Manager se basa en un componente de LW-SSO. Antes de conectarse al servidor de Confidential Manager, el cliente de Confidential Manager envía primero una cookie LW-SSO. El servidor de Confidential Manager comprueba la cookie y, si la comprobación es satisfactoria, se inicia la comunicación con el cliente de Confidential Manager. Para obtener más información sobre LW-SSO, consulte "Configuración de LW-SSO" en la página 55.

La comunicación entre el cliente de Confidential Manager y el servidor de Confidential Manager está cifrada. Para obtener más información sobre la actualización de la configuración de cifrado, consulte "Configuración del cifrado de la comunicación de Confidential Manager" en la página 55.

Precaución: La autenticación de Confidential Manager utiliza la hora universal definida en el equipo (UTC). Para que la autenticación sea correcta, asegúrese de que la hora universal de Data Flow Probe y el servidor de UCMDB sean la misma. El servidor y la sonda se pueden ubicar en zonas horarias diferentes, ya que UTC es independiente de la zona horaria o de la configuración del horario de verano.

El cliente de Confidential Manager mantiene una memoria caché local de las credenciales. El cliente de Confidential Manager está configurado para descargar todas las credenciales del servidor de Confidential Manager y almacenarlas en una caché. Los cambios de credenciales se sincronizan automáticamente desde el servidor de Confidential Manager de forma continua. La

caché puede ser un sistema de archivos o una caché en memoria, en función de la configuración predefinida. Además, la caché está cifrada y no es posible tener acceso a ella de forma externa. Para obtener más información sobre la actualización de la configuración de caché, consulte "Configurar el modo de caché del cliente de Confidential Manager en la sonda" en la página 60. Para obtener más información sobre el cifrado de caché, consulte "Establecer la configuración de cifrado de caché del cliente de Confidential Manager en la sonda" en la página 61.

Para obtener más información sobre la solución de problemas, consulte "Cambiar el nivel de mensajes del archivo de registro del cliente de Confidential Manager" en la página 63.

Puede copiar la información de credenciales de un servidor UCMDB a otro. Para obtener más información, consulte "Exportar e importar la información de credenciales e intervalos en formato cifrado" en la página 62.

Nota: El archivo **DomainScopeDocument** (DSD) que se usaba para almacenar las credenciales en la sonda (en UCMDB versión 9.01 o anterior) ya no contiene ninguna información confidencial sobre credenciales. Ahora el archivo contiene una lista de sondas e información del intervalo de red. También contiene una lista de entradas de credenciales para cada dominio, donde cada entrada incluye únicamente el Id. de credencial y el intervalo de red (definido para esta entrada de credencial).

Esta sección incluye los siguientes temas:

Suposiciones básicas de seguridad

Tenga en cuenta la siguiente suposición de seguridad:

Ha protegido el servidor UCMDB y la consola JMX de la sonda para permitir el acceso solo a los administradores del sistema UCMDB únicamente.

Ejecución de Data Flow Probe en modo independiente

Cuando Puerta de enlace de sonda y Administrador de sonda se ejecutan como procesos independientes, el componente cliente de Confidential Manager pasa a formar parte del proceso Administrador. La información de credenciales está almacenada en la caché y solo la usa el Administrador de sonda. Para acceder al servidor de Confidential Manager en el sistema UCMDB, la solicitud del cliente de Confidential Manager la gestiona el proceso de la Puerta de enlace y desde ahí se reenvía al sistema UCMDB.

Esta configuración es automática cuando se configura la sonda en modo independiente.

Mantener la caché de credenciales actualizada

La primera vez que se conecta correctamente al servidor de Confidential Manager, el cliente de Confidential Manager descarga todas las credenciales relevantes (todas las credenciales configuradas en el dominio de la sonda). Una vez que se ha establecido la primera comunicación satisfactoria, el cliente de Confidential Manager mantiene una sincronización continua con el servidor de Confidential Manager. La sincronización diferencial tiene lugar en intervalos de un minuto y solo se sincronizan las diferencias entre el servidor de Confidential Manager y el cliente de Confidential Manager. Si se cambian las credenciales en el lado del servidor de UCMDB (por ejemplo, porque se agregan nuevas credenciales o se actualizan o eliminan las credenciales existentes), el cliente de Confidential Manager recibe una notificación inmediata del servidor de UCMDB y realiza una sincronización adicional.

Sincronización de todas las sondas con cambios de configuración

Para que la comunicación se realice correctamente, el cliente de Confidential Manager debe tener actualizada la configuración de autenticación del servidor de Confidential Manager (cadena init de LW-SSO) y la configuración de cifrado (cifrado de comunicación de Confidential Manager). Por ejemplo, si se cambia la cadena init en el servidor, la sonda debe conocer la nueva cadena init para poder realizar la autenticación.

El servidor de UCMDB monitoriza constantemente los cambios en la configuración de cifrado de comunicación de Confidential Manager y en la configuración de autenticación de Confidential Manager. Esta monitorización se realiza cada 15 segundos; si se ha producido algún cambio, se envía la configuración actualizada a las sondas. La configuración se pasa a las sondas de forma cifrada y se almacena en la sonda en un almacenamiento protegido. El cifrado de la configuración que se envía se realiza mediante una clave de cifrado simétrico. De forma predeterminada, el servidor de UCMDB y Data Flow Probe se instalan con la misma clave de cifrado simétrico predeterminada. Para una seguridad óptima, es muy recomendable cambiar esta clave antes de agregar credenciales al sistema. Para obtener más información, consulte "Generar o actualizar la clave de cifrado" en la página 65.

Nota: Debido al intervalo de monitorización de 15 segundos, es posible que el cliente de Confidential Manager en la sonda no esté actualizado con la configuración más reciente durante 15 segundos.

Si elige deshabilitar la sincronización automática de la configuración de comunicación y autenticación de Confidential Manager entre el servidor de UCMDB y Data Flow Probe, cada vez que actualice la configuración de comunicación y autenticación de Confidential Manager en el servidor de UCMDB, también debería actualizar todas las sondas con la nueva configuración. Para obtener más información, consulte "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" en la página 57.

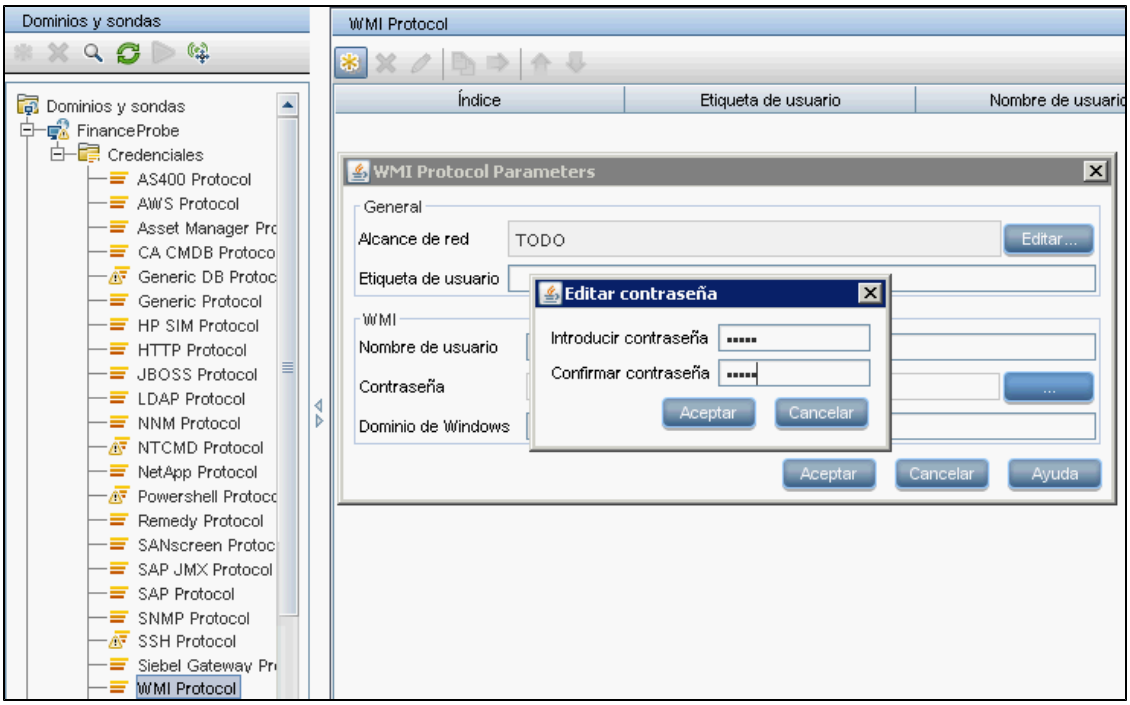
Almacenamiento protegido en la sonda

Toda la información confidencial (por ejemplo, la configuración de comunicación y autenticación de Confidential Manager y la clave de cifrado) se almacena en la sonda en el archivo **secured_ storage.bin** de almacenamiento protegido, que está ubicado en **C:\hp\UCMDB\DataFlowProbe\conf\security**. Este almacenamiento protegido se cifra mediante DPAPI, que se basa en la contraseña de usuario de Windows en el proceso de cifrado. DPAPI es un método estándar que se usa para proteger datos confidenciales, como certificados y claves privadas, en sistemas Windows. La sonda debería ejecutarse siempre con el mismo usuario de Windows para que, en caso de que cambie la contraseña, la sonda pueda seguir leyendo la información almacenada en almacenamiento protegido.

Visualización de información de credenciales

Nota: En esta sección se explica la visualización de información de credenciales cuando la dirección de datos es desde CMDB hasta HP Universal CMDB

Las contraseñas no se envían desde CMDB hasta la aplicación. Es decir, HP Universal CMDB muestra asteriscos (*) en el campo de contraseña, independientemente del contenido:



Actualización de credenciales

Nota: En esta sección se explica la actualización de credenciales cuando la dirección de los datos es desde HP Universal CMDB hasta CMDB.

- La comunicación que se realiza en este sentido no está cifrada, de manera que debería conectarse al servidor de UCMDB mediante https\SSL, o asegurarse de que la conexión se realice a través de una red de confianza.

  Aunque no se cifre la comunicación, las contraseñas no se envían como texto legible en la red. Se cifran mediante una clave predeterminada, por lo que es muy recomendable utilizar SSL para garantizar la confidencialidad durante la comunicación.

- Es posible utilizar caracteres especiales y caracteres que no sean del idioma inglés en las contraseñas.

Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager

Esta tarea describe la configuración de los parámetros de cifrado y la autenticación de cliente de Confidential Manager en el Servidor de UCMDB e incluye los siguientes pasos:

- "Configuración de LW-SSO" abajo
- "Configuración del cifrado de la comunicación de Confidential Manager" abajo

Configuración de LW-SSO

Este procedimiento describe cómo cambiar la cadena init de LW-SSO en el servidor de UCMDB. Este cambio se envía automáticamente a las sondas (como una cadena cifrada), a menos que la configuración del servidor UCMDB establezca que no se realice esta acción de forma automática. Para obtener más información, consulte "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" en la página 57.

1. En el servidor UCMDB inicie el explorador web e introduzca la siguiente dirección: **http://localhost:8080/jmx-console**.
2. Haga clic en **UCMDB-UI:name=LW-SSO Configuration** para abrir la página JMX MBEAN View.
3. Localice el método **setInitString**.
4. Introduzca una nueva cadena init de LW-SSO.
5. Haga clic en Invoke.

Configuración del cifrado de la comunicación de Confidential Manager

Este procedimiento describe cómo cambiar la configuración de cifrado de Confidential Manager en el Servidor de UCMDB. Esta configuración especifica el cifrado de la comunicación entre el cliente

de Confidential Manager y el servidor de Confidential Manager. Este cambio se envía automáticamente a las sondas (como una cadena cifrada), a menos que la configuración del servidor UCMDB establezca que no se realice esta acción de forma automática. Para obtener más información, consulte "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" en la página siguiente.

1. En el servidor UCMDB inicie el explorador web e introduzca la siguiente dirección: **http://localhost:8080/jmx-console.**
2. Haga clic en **UCMDB:service=Security Services** para abrir la página JMX MBEAN View.
3. Haga clic en el método **CMGetConfiguration**.
4. Haga clic en **Invoke**.

   Se muestra el archivo XML de la configuración de Confidential Manager actual.
5. Copie el contenido del archivo XML visualizado.
6. Regrese a la página JMX MBean View de **Security Services**.
7. Haga clic en el método **CMSetConfiguration**.
8. Pegue el XML copiado en el campo **Value**.
9. Actualice la configuración correspondiente relacionada con el transporte y haga clic en **Invoke**.

   Ejemplo:

```
<transport>
      <encryptTransportMode>true</encryptTransportMode>
      <CMEncryptionDecryption>
            <encryptDecryptInitString>radiohead</encryptDecryptInitStrin
            g>
            <cryptoSource>lw</cryptoSource>
            <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
            <cipherType>symmetricBlockCipher</cipherType>
            <engineName>AES</engineName>
            <algorithmModeName>CBC</algorithmModeName>
            <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
            <keySize>256</keySize>
            <pbeCount>20</pbeCount>
```

```
            <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
            <encodingMode>Base64Url</encodingMode>
            <useMacWithCrypto>false</useMacWithCrypto>
            <macType>hmac</macType>
            <macKeySize>256</macKeySize>
            <macHashName>SHA256</macHashName>
      </CMEncryptionDecryption>
</transport>
```

Para obtener más información sobre los valores que pueden actualizarse, consulte "Configuración de cifrado de Confidential Manager" en la página 69.

Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager manualmente en la sonda

Esta tarea incluye los siguientes pasos:

- "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" abajo
- "Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager en la sonda" en la página siguiente
- "Configurar el cifrado de la comunicación de Confidential Manager en la sonda" en la página siguiente

Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas

De forma predeterminada, el servidor UCMDB está configurado para enviar automáticamente la configuración de Confidential Manager/LW-SSO a todas las sondas. Esta información se envía como una cadena cifrada a las sondas, que descifran la información en cuanto la reciben. Puede configurar el servidor UCMDB para que no envíe automáticamente los archivos de configuración de Confidential Manager/LW-SSO a todas las sondas. En tal caso, es responsabilidad del usuario actualizar manualmente todas las sondas con la nueva configuración de CM/LW-SSO.

Para deshabilitar la sincronización automática de la configuración de Confidential Manager/LW-SSO:

1. En UCMDB, haga clic en **Administración > Administrador de configuración de infraestructura > Configuración general**.
2. Seleccione **Habilitar sincronización automática de la configuración de CM/LW-SSO y cadena init con sonda.**
3. Haga clic en el campo **Valor** y cambie **True** por **False**.
4. Haga clic en el botón **Guardar**.
5. Reinicie el servidor de UCMDB.

Establecer la configuración de autenticación y cifrado del cliente de Confidential Manager en la sonda

Este procedimiento es importante si la configuración del servidor de UCMDB establece que no se envíe automáticamente a las sondas la configuración de LW-SSO/Confidential Manager. Para obtener más información, consulte "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" en la página precedente.

1. En el equipo donde está instalada la sonda, inicie el explorador web e introduzca la siguiente dirección: **http://localhost:1977**.

   Nota: Si Administrador de sonda y Puerta de enlace de sonda se están ejecutando como procesos independientes, debe introducirse la dirección en el equipo que ejecuta el Administrador de sonda, del siguiente modo: **http://localhost:1978**.

2. Haga clic en **type=CMClient** para abrir la página JMX MBEAN View.
3. Localice el método **setLWSSOInitString** y proporcione la misma cadena init que se proporcionó en la configuración de LW-SSO de UCMDB.
4. Haga clic en el botón **setLWSSOInitString**.

Configurar el cifrado de la comunicación de Confidential Manager en la sonda

Este procedimiento es importante si la configuración del servidor de UCMDB establece que no se envíe automáticamente a las sondas la configuración de LW-SSO/Confidential Manager. Para más información, consulte "Deshabilitar la sincronización automática de la configuración de autenticación y cifrado del cliente de Confidential Manager entre el servidor y las sondas" en la página precedente.

1. En el equipo donde está instalada la sonda, inicie el explorador web e introduzca la siguiente dirección: **http://localhost:1977**.

   Nota: Si Administrador de sonda y Puerta de enlace de sonda se están ejecutando como procesos independientes, debe introducirse la dirección en el equipo que ejecuta el Administrador de sonda, del siguiente modo: **http://localhost:1978**.

2. Haga clic en **type=CMClient** para abrir la página JMX MBEAN View.

3. Actualice la siguiente configuración relacionada con el transporte:

   Nota: Debe actualizar la misma configuración que actualizó en el servidor UCMDB. Para ello, es posible que algunos de los métodos que actualice en la sonda requieran más de un parámetro. Para ver la configuración de sonda actual, haga clic en **displayTransportConfiguration** en la página JMX MBEAN View. Para obtener más información, consulte "Configuración del cifrado de la comunicación de Confidential Manager" en la página 55. Para obtener más información sobre los valores que pueden actualizarse, consulte "Configuración de cifrado de Confidential Manager" en la página 69.

   a. **setTransportInitString** cambia la configuración de **encryptDecryptInitString**.

   b. **setTransportEncryptionAlgorithm** cambia la configuración de Confidential Manager en la sonda según el siguiente mapa:

      - **Engine name** hace referencia a la entrada <engineName>
      - **Key size** hace referencia a la entrada <keySize>
      - **Algorithm padding name** hace referencia a la entrada <algorithmPaddingName>
      - **PBE count** hace referencia a la entrada <pbeCount>
      - **PBE digest algorithm** hace referencia a la entrada <pbeDigestAlgorithm>

   c. **setTransportEncryptionLibrary** cambia la configuración de Confidential Manager en la sonda según el siguiente mapa:

      - **Encryption Library name** hace referencia a la entrada <cryptoSource>
      - **Support previous lightweight cryptography versions** hace referencia a la entrada <lwJCEPBECompatibilityMode>

   d. **setTransportMacDetails** cambia la configuración de Confidential Manager en la sonda según el siguiente mapa:

- **Use MAC with cryptography** hace referencia a la entrada <useMacWithCrypto>
- **MAC key size** hace referencia a la entrada <macKeySize>

4. Haga clic en el botón **reloadTransportConfiguration** para que los cambios surtan efecto en la sonda.

Para obtener más información sobre las distintas opciones de configuración y sus posibles valores, consulte "Configuración de cifrado de Confidential Manager" en la página 69.

Configurar la caché del cliente de Confidential Manager

Esta tarea incluye los siguientes pasos:

- "Configurar el modo de caché del cliente de Confidential Manager en la sonda" abajo
- "Establecer la configuración de cifrado de caché del cliente de Confidential Manager en la sonda" en la página siguiente

Configurar el modo de caché del cliente de Confidential Manager en la sonda

El cliente de Confidential Manager almacena la información de credenciales en la caché y la actualiza cuando la información cambia en el servidor. La caché puede almacenarse en el sistema de archivos o en la memoria:

- **Cuando se almacena en el sistema de archivos**, incluso si se reinicia la sonda y no puede conectarse al servidor, la información de credenciales sigue estando disponible.
- **Cuando se almacena en la memoria**, si se reinicia la sonda, se borra la caché y toda la información se recupera nuevamente del servidor. Si el servidor no está disponible, la sonda no incluye ninguna credencial, por lo que no se puede ejecutar ninguna detección o integración.

Para cambiar esta configuración:

1. Abra el archivo **DataFlowProbe.properties** en un editor de texto. El archivo está ubicado en la carpeta **c:\hp\UCMDB\DataFlowProbe\conf**.
2. Localice el siguiente atributo:
com.hp.ucmdb.discovery.common.security.storeCMData=true
   - Para almacenar la información en el sistema de archivos, deje el valor predeterminado (**true**).
   - Para almacenar la información en la memoria, introduzca **false**.

3. Guarde el archivo **DataFlowProbe.properties**.

4. Reinicie la sonda.

Establecer la configuración de cifrado de caché del cliente de Confidential Manager en la sonda

Este procedimiento describe cómo cambiar la configuración de cifrado del archivo de caché del sistema de archivos del cliente de Confidential Manager. Tenga en cuenta que, al cambiar la configuración de cifrado de la caché del sistema de archivos del cliente de Confidential Manager, se vuelve a crear el archivo de caché del sistema de archivos. Este proceso de recreación requiere que se reinicie la sonda y se sincronice completamente con el servidor UCMDB.

1. En el equipo donde está instalada la sonda, inicie el explorador web e introduzca la siguiente dirección: **http://localhost:1977**.

   Nota: Si Administrador de sonda y Puerta de enlace de sonda se están ejecutando como procesos independientes, debe introducirse la dirección en el equipo que ejecuta el Administrador de sonda, del siguiente modo: **http://localhost:1978**.

2. Haga clic en **type=CMClient** para abrir la página JMX MBEAN View.

3. Actualice la siguiente configuración relacionada con la caché:

   Nota: Es posible que algunos de los métodos que actualice en la sonda requieran más de un parámetro. Para ver la configuración de sonda actual, haga clic en **displayCacheConfiguration** en la página JMX MBEAN View.

   a. **setCacheInitString** cambia la configuración de <encryptDecryptInitString> en la caché del sistema de archivos.

   b. **setCacheEncryptionAlgorithm** cambia la configuración de caché del sistema de archivos según el siguiente mapa:

      - **Engine name** hace referencia a la entrada <engineName>
      - **Key size** hace referencia a la entrada <keySize>
      - **Algorithm padding name** hace referencia a la entrada <algorithmPaddingName>
      - **PBE count** hace referencia a la entrada <pbeCount>
      - **PBE digest algorithm** hace referencia a la entrada <pbeDigestAlgorithm>

   c. **setCacheEncryptionLibrary** cambia la configuración de caché del sistema de archivos

según el siguiente mapa:

- **Encryption Library name** hace referencia a la entrada <cryptoSource>
- **Support previous lightweight cryptography versions** hace referencia a la entrada <lwJCEPBECompatibilityMode>

d. **setCacheMacDetails** cambia la configuración de caché del sistema de archivos según el siguiente mapa:

- **Use MAC with cryptography** hace referencia a la entrada <useMacWithCrypto>
- **MAC key size** hace referencia a la entrada <macKeySize>

4. Haga clic en el botón **reloadCacheConfiguration** para que los cambios surtan efecto en la sonda. Esto provoca el reinicio de la sonda.

> **Nota:** Asegúrese de que no haya ningún trabajo en ejecución en la sonda durante esta acción.

Para obtener más información sobre las distintas opciones de configuración y sus posibles valores, consulte "Configuración de cifrado de Confidential Manager" en la página 69.

Exportar e importar la información de credenciales e intervalos en formato cifrado

Puede exportar e importar la información de credenciales e intervalos de red en formato cifrado para copiar la información de credenciales de un servidor de UCMDB a otro. Por ejemplo, podría realizar esta operación durante la recuperación tras un bloqueo del sistema o durante la actualización.

- **Al exportar la información de credenciales**, debe introducir una contraseña (de su elección). La información de esta contraseña está cifrada.
- **Al importar la información de credenciales**, debe usar la misma contraseña que se definió al exportar el archivo DSD.

> **Nota:** El documento de credenciales exportado también contiene la información de intervalos definida en el sistema del que se exportó el documento. Durante la importación del documento de credenciales, también se importa la información de intervalos.

Para exportar la información de credenciales del servidor de UCMDB:

1. En el servidor UCMDB inicie el explorador web e introduzca la siguiente dirección: **http://localhost:8080/jmx-console**. Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. Haga clic en **UCMDB:service=DiscoveryManager** para abrir la página JMX MBEAN View.
3. Localice la operación **exportCredentialsAndRangesInformation**. Realice las siguientes operaciones:
   - Introduzca el Id. de cliente (el valor predeterminado es 1).
   - Introduzca un nombre para el archivo exportado.
   - Escriba la contraseña.
   - Establezca **isEncrypted=True** si desea cifrar el archivo exportado con la contraseña proporcionada o **isEncrypted=False** si no desea cifrar el archivo exportado (en cuyo caso no se exportan las contraseñas ni ninguna otra información confidencial).
4. Haga clic en **Invoke** para exportar.

   Cuando el proceso de exportación finaliza de forma satisfactoria, el archivo se guarda en la ubicación siguiente: **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.

Para importar la información de credenciales del servidor de UCMDB:

1. En el servidor UCMDB inicie el explorador web e introduzca la siguiente dirección: **http://localhost:8080/jmx-console**.

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.
2. Haga clic en **UCMDB:service=DiscoveryManager** para abrir la página JMX MBEAN View.
3. Localice la operación **importCredentialsAndRangesInformation**.
4. Introduzca el Id. de cliente (el valor predeterminado es 1).
5. Introduzca el nombre del archivo que se va a importar. Este archivo debe estar ubicado en la carpeta **c:\hp\UCMDB\UCMDBServer\conf\discovery\<customer_dir>**.
6. Escriba la contraseña. Debe ser la misma contraseña que la que se usó al exportar el archivo.
7. Haga clic en **Invoke** para importar las credenciales.

Cambiar el nivel de mensajes del archivo de registro del cliente de Confidential Manager

La sonda proporciona dos archivos de registro que contienen información relativa a la comunicación relacionada con Confidential Manager entre el servidor de Confidential Manager y el cliente de Confidential Manager. Estos archivos son:

- "Archivo de registro del cliente de Confidential Manager" abajo
- "Archivo de registro de LW-SSO" abajo

Archivo de registro del cliente de Confidential Manager

El archivo **security.cm.log** está ubicado en la carpeta **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

El registro contiene mensajes de información que intercambian el servidor de Confidential Manager y el cliente de Confidential Manager. De forma predeterminada, el nivel de registro de estos mensajes está establecido en INFO.

Para cambiar el nivel de registro de los mensajes al nivel DEBUG:

1. En el servidor del administrador de Data Flow Probe, vaya a **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Abra el archivo **security.properties** en un editor de texto.
3. Cambie la línea:

   ```
   loglevel.cm=INFO
   ```

   por:

   ```
   loglevel.cm=DEBUG
   ```

4. Guarde el archivo.

Archivo de registro de LW-SSO

El archivo **security.lwsso.log** está ubicado en la carpeta **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

El registro contiene mensajes de información relacionados con LW-SSO. De forma predeterminada, el nivel de registro de estos mensajes está establecido en INFO.

Para cambiar el nivel de registro de los mensajes al nivel DEBUG:

1. En el servidor del administrador de Data Flow Probe, vaya a **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Abra el archivo security.properties en un editor de texto.
3. Cambie la línea:

   ```
   loglevel.lwsso=INFO
   ```

   por:

```
loglevel.lwsso=DEBUG
```

4. Guarde el archivo.

Generar o actualizar la clave de cifrado

Puede generar o actualizar una clave de cifrado que se usará para cifrar o descifrar las configuraciones de comunicación y autenticación de Confidential Manager que intercambian el servidor de UCMDB y Data Flow Probe. Tanto en la generación como en la actualización, el servidor UCMDB crea una nueva clave de cifrado a partir de los parámetros suministrados (por ejemplo, longitud de clave, ciclos PBE adicionales, proveedor JCE) y la distribuye a las sondas.

La ejecución del método **generateEncryptionKey** da como resultado la generación de una nueva clave de cifrado. Esta clave solo se almacena en almacenamiento protegido y se desconocen tanto su nombre como sus detalles. Si vuelve a instalar una sonda Data Flow existente o conecta una nueva sonda al servidor de UCMDB, la nueva sonda no reconoce esta nueva clave generada. En tales casos, es preferible utilizar el método **changeEncryptionKey** para cambiar las claves de cifrado. De este modo, si se vuelve a instalar una sonda o se instala una nueva, se puede importar la clave existente (cuyo nombre y ubicación son conocidos) ejecutando el método **importEncryptionKey** en la consola JMX de la sonda.

Nota:

- La diferencia entre los métodos que se usan para crear una clave (**generateEncryptionKey**) y actualizar una clave (**changeEncryptionKey**) es que **generateEncryptionKey** crea una clave de cifrado nueva y aleatoria, mientras que **changeEncryptionKey** importa una clave de cifrado cuyo nombre proporciona el usuario.
- Solo puede haber una clave de cifrado en un sistema, independientemente del número de sondas instaladas.

Esta tarea incluye los siguientes pasos:

- "Generar una nueva clave de cifrado" abajo
- "Actualizar una clave de cifrado en un servidor de UCMDB" en la página 67
- "Actualizar una clave de cifrado en una sonda" en la página 68
- "Cambiar manualmente la clave de cifrado cuando Administrador de sonda y Puerta de enlace de sonda están instalados en equipos independientes" en la página 69
- "Definir varios proveedores JCE" en la página 69

Generar una nueva clave de cifrado

Puede generar una nueva clave que el servidor UCMDB y Data Flow Probe usarán para cifrar o descifrar. El servidor UCMDB reemplaza la clave antigua por la nueva clave generada y la

distribuye entre las sondas.

Para generar una nueva clave de cifrado mediante la consola JMX:

1. En el servidor UCMDB inicie el explorador web e introduzca la siguiente dirección: **http://localhost:8080/jmx-console**.

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. Haga clic en **UCMDB:service=DiscoveryManager** para abrir la página JMX MBEAN View.

3. Localice la operación generateEncryptionKey.

   a. En el cuadro del parámetro **customerId**, escriba 1 (el valor predeterminado).

   b. En **keySize**, especifique la longitud de la clave de cifrado. Los valores válidos son 128, 192 ó 256.

   c. En **usePBE**, especifique **True** o **False**:

      - **True:** usa ciclos hash PBE adicionales.
      - **False:** no usa ciclos hash PBE adicionales.

   d. En **jceVendor**, puede optar por utilizar un proveedor JCE no predeterminado. Si el cuadro esta vacío, se utiliza el proveedor predeterminado.

   e. En **autoUpdateProbe**, especifique **True** o **False**:

      - **True:** el servidor distribuye la nueva clave a las sondas automáticamente.
      - **False:** la nueva clave debe colocarse en las sondas manualmente.

   f. En **exportEncryptionKey**, especifique **True** o **False**.

      - **True:** además de crear la nueva contraseña y almacenarla en almacenamiento seguro, el servidor exporta la contraseña nueva al sistema de archivos (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). Esta opción le permite actualizar manualmente las sondas con la nueva contraseña.
      - **False:** la nueva contraseña no se exporta al sistema de archivos. Para actualizar las sondas manualmente, establezca **autoUpdateProbe** en False y **exportEncryptionKey** en True.

      Nota: Asegúrese de que la sonda está funcionando y conectada al servidor. Si la sonda deja de funcionar, la clave no puede llegar a la sonda. Si cambia la clave antes de que la sonda deje de funcionar, cuando vuelva a estar en funcionamiento, la clave se enviará de nuevo a la sonda. Sin embargo, si cambia

la clave más de una vez antes de que la sonda deje de funcionar, debe cambiar la clave manualmente a través de la consola JMX. (Seleccione **False** en **exportEncryptionKey**).

4. Haga clic en **Invoke** para generar la clave de cifrado.

Actualizar una clave de cifrado en un servidor de UCMDB

El método **changeEncryptionKey** se utiliza para importar la propia clave de cifrado en el servidor de UCMDB y distribuirla entre todas las sondas.

Para actualizar una clave de cifrado a través de la consola JMX:

1. En el servidor UCMDB inicie el explorador web e introduzca la siguiente dirección: **http://localhost:8080/jmx-console.**

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. Haga clic en **UCMDB:service=DiscoveryManager** para abrir la página JMX MBEAN View.

3. Localice la operación **changeEncryptionKey**.

   a. En el cuadro del parámetro **customerId**, escriba **1** (el valor predeterminado).

   b. En **newKeyFileName**, escriba el nombre de la nueva clave.

   c. En **keySizeInBits**, especifique la longitud de la clave de cifrado. Los valores válidos son 128, 192 ó 256.

   d. En **usePBE**, especifique **True** o **False**:

      - **True:** usa ciclos hash PBE adicionales.
      - **False:** no usa ciclos hash PBE adicionales.

   e. En **jceVendor**, puede optar por utilizar un proveedor JCE no predeterminado. Si el cuadro esta vacío, se utiliza el proveedor predeterminado.

   f. En **autoUpdateProbe**, especifique **True** o **False**:

      - **True:** el servidor distribuye la nueva clave a las sondas automáticamente.
      - **False:** la nueva clave debe distribuirse manualmente mediante la consola JMX de la sonda.

Nota: Asegúrese de que la sonda está funcionando y conectada al servidor. Si la sonda deja de funcionar, la clave no puede llegar a la sonda. Si cambia la clave antes de que la sonda deje de funcionar, cuando vuelva a estar en funcionamiento, la clave se enviará de nuevo a la sonda. Sin embargo, si cambia la clave más de una vez antes de que la sonda deje de funcionar, debe cambiar la clave manualmente a través de la consola JMX. (Seleccione **False** en **autoUpdateProbe**).

4. Haga clic en **Invoke** para generar y actualizar la clave de cifrado.

Actualizar una clave de cifrado en una sonda

Si opta por no distribuir una clave de cifrado del servidor de UCMDB a todas las sondas automáticamente porque le preocupa la seguridad, debe descargar la nueva clave de cifrado en todas las sondas y ejecutar el método **importEncryptionKey** en la sonda:

1. Coloque el archivo de clave de cifrado en el directorio **C:\hp\UCMDB\DataFlowProbe\conf\security**.

2. En el equipo donde está instalada la sonda, inicie el explorador web e introduzca la siguiente dirección: **http://localhost:1977**.

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

   Nota: Si Administrador de sonda y Puerta de enlace de sonda se están ejecutando como procesos independientes, debe introducirse la dirección en el equipo que ejecuta el Administrador de sonda, del siguiente modo: **http://localhost:1978**.

3. En el dominio Sonda, haga clic en **type=SecurityManagerService**.

4. Localice el método **importEncryptionKey**.

5. Escriba el nombre del archivo de clave de cifrado ubicado en **C:\hp\UCMDB\DataFlowProbe\conf\security**. Este archivo contiene la clave que se va a importar.

6. Haga clic en el botón **importEncryptionKey**.

7. Realice un reinicio de la sonda.

Cambiar manualmente la clave de cifrado cuando Administrador de sonda y Puerta de enlace de sonda están instalados en equipos independientes

1. En el equipo donde está instalado Administrador de sonda, inicie el servicio Administrador de sonda (**Inicio > Programas > HP UCMDB > Administrador de sonda**).
2. Importe la clave del servidor mediante la consola JMX de Administrador de sonda. Para obtener más información, consulte "Generar una nueva clave de cifrado" en la página 65.
3. Tras importar la clave de cifrado correctamente, reinicie los servicios Administrador de sonda y Puerta de enlace de sonda.

Definir varios proveedores JCE

Cuando se genera una clave de cifrado mediante la consola JMX, se pueden definir varios proveedores JCE mediante los métodos **changeEncryptionKey** y **generateEncryptionKey**.

Para cambiar el proveedor JCE predeterminado:

1. Registre los archivos jar del proveedor JCE en **$JRE_HOME/lib/ext**.
2. Copie los archivos jar en la carpeta $JRE_HOME:
   - En el servidor UCMDB: $JRE_HOME reside en: **c:\hp\UCMDB\UCMDBServer\bin\jre**
   - En Data Flow Probe: $JRE_HOME reside en: **c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. Agregue la clase de proveedor al final de la lista de proveedores en el archivo **$JRE_HOME\lib\security\java.security**.
4. Actualice los archivos **local_policy.jar** y **US_export_policy.jar** para incluir directivas JCE ilimitadas. Puede descargar estos archivos jar del sitio web de Sun.
5. Reinicie el servidor de UCMDB y Data Flow Probe.
6. Localice el campo de proveedor JCE en el método **changeEncryptionKey** o **generateEncryptionKey** y agregue el nombre del proveedor JCE.

Configuración de cifrado de Confidential Manager

Esta tabla contiene una lista de la configuración de cifrado que puede cambiarse mediante diversos métodos de JMX. Esta configuración de cifrado es importante para cifrar las comunicaciones entre el cliente de Confidential Manager y el servidor de Confidential Manager y para cifrar la caché del cliente de Confidential Manager.

Nombre de config. de Confidential Manager	Nombre de config. de Confidential Manager de la sonda	Descripción de la configuración	Valores posibles	Valor predet.
cryptoSource	Encryption Library name	Esta configuración define la biblioteca de cifrado que se va a usar.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBE CompatibilidadModo	Support previous lightweight cryptography versions	Esta configuración define si se admite la criptografía ligera anterior o no.	true, false	true
engineName	Engine name	Nombre del mecanismo de cifrado	AES, DES, 3DES, Blowfish	AES
keySize	Key size	Longitud de la clave de cifrado en bits	En AES: 128, 192 o 256; En DES: 64; En 3DES: 192; En Blowfish: cualquier número entre 32 y 448	256
algoritmo Relleno Nombre	Algorithm padding name	Estándares de relleno	PKCS7Padding, PKCS5Padding	PKCS7Padding
pbeCount	PBE count	Número de veces que hay que ejecutar el hash para crear la clave a partir de la contraseña (cadena init)	Cualquier número positivo	20
pbeDigest Algoritmo	PBE digest algorithm	Tipo de hash	SHA1, SHA256, MD5	SHA1
useMacWith Crypto	Use MAC with cryptography	Indicación sobre el uso de MAC con la criptografía	true, false	false
macKeySize	MAC key size	Depende del algoritmo MAC	256	256

Solución de problemas y limitaciones

Si cambia el nombre de dominio predeterminado en el servidor UCMDB, en primer lugar debe verificar que Data Flow Probe no está en ejecución. Tras aplicar el nombre de dominio predeterminado, debe ejecutar la secuencia de comandos **DataFlowProbe\tools\clearProbeData.bat** en Data Flow Probe.

Nota: La ejecución de la secuencia de comandos clearProbeData.bat causará un ciclo de detección en la sonda una vez que esta esté activa.

Capítulo 5: Sistema de protección de Data Flow Probe

Este capítulo incluye:

Modificar la contraseña cifrada de la base de datos PostgreSQL

Esta sección explica cómo modificar la contraseña cifrada para el usuario de la base de datos PostgreSQL.

1. Crear el formato cifrado de una contraseña (AES, clave de 192 bits)

   a. Acceda a la consola JMX de Data Flow Probe. Inicie un explorador web y escriba la siguiente dirección: **http://<nombre de equipo o dirección IP de Data Flow Probe>:1977**. Si ejecuta Data Flow Probe de forma local, introduzca **http://localhost:1977**.

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

Nota: Si no ha creado un usuario, utilice el nombre de usuario predeterminado sysadmin y la contraseña sysadmin para iniciar sesión.

b. Localice el servicio **Type=MainProbe** y haga clic en el vínculo para abrir la página de operaciones.

c. Localice la operación **getEncryptedDBPassword**.

d. En el campo **DB Password**, introduzca la contraseña que hay que cifrar.

e. Llame a la operación haciendo clic en el botón **getEncryptedDBPassword**.

El resultado de la llamada es una cadena de contraseña cifrada como, por ejemplo:

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61
,61
```

2. Detener Data Flow Probe

Inicio > Todos los programas > HP UCMDB > Detener Data Flow Probe

3. Ejecutar la secuencia de comandos set_dbuser_password.cmd

Esta secuencia de comandos está ubicada en la carpeta siguiente:
C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd

Ejecute la secuencia de comandos **set_dbuser_password.cmd** con la nueva contraseña como primer argumento y la contraseña de la cuenta raíz de PostgreSQL como segundo argumento.

Por ejemplo:

set_dbuser_password <mi_contraseña><contraseña_raíz>.

La contraseña debe introducirse sin cifrar (como texto sin formato).

4. Actualizar la contraseña en los archivos de configuración de Data Flow Probe

a. La contraseña debe estar cifrada en los archivos de configuración. Para recuperar el formato cifrado de la contraseña, utilice el método **getEncryptedDBPassword** de JMX, como se explica en el paso 1.

b. Agregue la contraseña cifrada a las siguientes propiedades del archivo **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

- **appilog.agent.probe.jdbc.pwd**

  Por ejemplo:

  ```
  appilog.agent.probe.jdbc.user = mamprobe
  appilog.agent.probe.jdbc.pwd =
  66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,
  61,61
  ```

- **appilog.agent.local.jdbc.pwd**
- **appilog.agent.normalization.jdbc.pwd**

5. Iniciar Data Flow Probe

   Inicio > Todos los programas > HP UCMDB > Iniciar Data Flow Probe.

Secuencia de comandos clearProbeData: uso

Para volver a crear la base de datos de usuario sin alterar su contraseña actual, ejecute la secuencia de comandos **clearProbeData.bat** para Windows o la secuencia de comandos **clearProbeData.sh** para Linux.

Después de ejecutar la secuencia de comandos:

- Revise el siguiente archivo para ver si hay errores: **C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log** para Windows, **/opt/hp/UCMDB/DataFlowProbe/runtime/log/probe_setup.log** para Linux.
- Elimine el archivo, ya que contiene la contraseña de la base de datos.

Nota: No ejecute esta secuencia de comandos a menos que se indique lo contrario en HP Software Support.

Configurar la contraseña cifrada de la consola JMX

Esta sección explica cómo cifrar la contraseña para el usuario de JMX. La contraseña cifrada se almacena en el archivo DataFlowProbe.properties. Los usuarios deben iniciar sesión para acceder a la consola JMX.

1. ### Crear el formato cifrado de una contraseña (AES, clave de 192 bits)

   a. Acceda a la consola JMX de Data Flow Probe. Inicie un explorador web y escriba la siguiente dirección: **http://<nombre de equipo o dirección IP de Data Flow Probe>:1977**. Si ejecuta Data Flow Probe de forma local, introduzca **http://localhost:1977**.

Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

Nota: Si no ha creado un usuario, utilice el nombre de usuario predeterminado sysadmin y la contraseña sysadmin para iniciar sesión.

b. Localice el servicio **Type=MainProbe** y haga clic en el vínculo para abrir la página de operaciones.

c. Localice la operación **getEncryptedKeyPassword**.

d. En el campo **Key Password**, introduzca la contraseña que hay que cifrar.

e. Llame a la operación haciendo clic en el botón **getEncryptedKeyPassword**.

El resultado de la llamada es una cadena de contraseña cifrada como, por ejemplo:

```
85,-9,-61,11,105,-93,-81,118
```

2. Detener Data Flow Probe

Inicio > Todos los programas > HP UCMDB > Detener Data Flow Probe

3. Agregar la contraseña cifrada

Agregue la contraseña cifrada a la siguiente propiedad del archivo **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

appilog.agent.Probe.JMX.BasicAuth.Pwd

Por ejemplo:

```
appilog.agent.Probe.JMX.BasicAuth.User=sysadmin
appilog.agent.Probe.JMX.BasicAuth.Pwd=12,-35,-37,82,-2,20,57,-40,38,80,-111,-99,-64,-5,35,-122
```

Nota: Para deshabilitar la autenticación, deje estos campos en blanco. De esta forma, los usuarios podrán abrir la página principal de la consola JMX de la sonda sin necesidad de autenticación.

4. Iniciar Data Flow Probe

Inicio >Todos los programas > HP UCMDB > Iniciar Data Flow Probe

Pruebe el resultado en un explorador web.

Configurar la contraseña de UpLoadScanFile

Esta sección explica cómo configurar la contraseña para **UpLoadScanFile**, utilizada para guardar la exploración de forma remota. La contraseña cifrada se almacena en el archivo **DataFlowProbe.properties**. Los usuarios deben iniciar sesión para acceder a la consola JMX.

1. **Crear el formato cifrado de una contraseña (AES, clave de 192 bits)**

   a. Acceda a la consola JMX de Data Flow Probe. Inicie un explorador web y escriba la siguiente dirección: **http://<nombre de equipo o dirección IP de Data Flow Probe>:1977**. Si ejecuta Data Flow Probe de forma local, introduzca **http://localhost:1977**.

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

   > **Nota:** Si no ha creado un usuario, utilice el nombre de usuario predeterminado sysadmin y la contraseña sysadmin para iniciar sesión.

   b. Localice el servicio **Type=MainProbe** y haga clic en el vínculo para abrir la página de operaciones.

   c. Localice la operación **getEncryptedKeyPassword**.

   d. En el campo **Key Password**, introduzca la contraseña que hay que cifrar.

   e. Llame a la operación haciendo clic en el botón **getEncryptedKeyPassword**.

   El resultado de la llamada es una cadena de contraseña cifrada como, por ejemplo:

   ```
   85,-9,-61,11,105,-93,-81,118
   ```

2. **Detener Data Flow Probe**

   Inicio > Todos los programas > HP UCMDB > Detener Data Flow Probe

3. **Agregar la contraseña cifrada**

   Agregue la contraseña cifrada a la siguiente propiedad del archivo **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties**.

   com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd

   Por ejemplo:

   ```
   com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile
   com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,77,-
   108,14,127,4,-89,101,-33,-31,116,53
   ```

4. **Iniciar Data Flow Probe**

   Inicio >Todos los programas > HP UCMDB > Iniciar Data Flow Probe

   Pruebe el resultado en un explorador web.

Acceso remoto a PostgreSQL Server

Esta sección explica cómo permitir/restringir el acceso a la cuenta de Data Flow Probe de PostgreSQL desde equipos remotos.

Nota:

- De forma predeterminada, el acceso está restringido.
- No puede acceder a la cuenta raíz de PostgreSQL desde equipos remotos.

Para permitir el acceso a PostgreSQL:

- Ejecute la siguiente secuencia de comandos en una ventana del símbolo del sistema:

  C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\enable_remote_user_access.cmd

Para restringir el acceso a PostgreSQL:

- Ejecute la siguiente secuencia de comandos en una ventana del símbolo del sistema:

  C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd

Habilitar SSL entre el servidor UCMDB y Data Flow Probe

Puede configurar la autenticación en Data Flow Probe y el servidor UCMDB con certificados. El certificado de cada componente se envía y se autentica antes de establecer la conexión.

Nota: El siguiente método, que consiste en habilitar SSL en Data Flow Probe es el más seguro de los métodos y, por lo tanto, es el modo de comunicación recomendado. Este método reemplaza el procedimiento de autenticación básica.

Esta sección incluye los siguientes temas:

- "Información general" en la página siguiente
- "Almacenes de claves y almacenes de confianza" en la página siguiente

- "Habilitar SSL con la autenticación de servidor (unidireccional)" abajo
- "Habilitar autenticación mutua de certificados (bidireccional)" en la página 81

Información general

UCMDB admite los siguientes modos de comunicación entre el servidor UCMDB y Data Flow Probe:

- **Autenticación del servidor.** Este modo utiliza SSL y la sonda autentica el certificado del servidor UCMDB. Para obtener más información, consulte "Habilitar SSL con la autenticación de servidor (unidireccional)" abajo.
- **Autenticación mutua.** Este modo utiliza SSL y permite tanto la autenticación del servidor por parte de la sonda como la autenticación de cliente por parte del servidor. Para obtener más información, consulte "Habilitar autenticación mutua de certificados (bidireccional)" en la página 81.
- **HTTP estándar.** Sin comunicación SSL. Es el modo predeterminado y el componente de Data Flow Probe de UCMDB no requiere ningún certificado. Data Flow Probe se comunica con el servidor a través del protocolo HTTP estándar.

Nota: La detección no puede utilizar cadenas de certificados cuando trabaja con SSL. Por lo tanto, si está utilizando cadenas de certificados, debe generar un certificado autofirmado para que Data Flow Probe pueda comunicarse con el Servidor de UCMDB.

Almacenes de claves y almacenes de confianza

El servidor UCMDB y Data Flow Probe utilizan almacenes de claves y almacenes de confianza:

- **Almacén de claves.** Un archivo que contiene entradas de claves (un certificado y su correspondiente clave privada).
- **Almacén de confianza.** Un archivo que contiene certificados que se utilizan para comprobar un host remoto (por ejemplo, cuando se usa la autenticación de servidor, el almacén de confianza de Data Flow Probe debería incluir el certificado del servidor UCMDB).

Limitación de la autenticación mutua

El almacén de claves de Data Flow Probe (como se define en **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**) debe contener 1 (una) sola entrada de clave.

Habilitar SSL con la autenticación de servidor (unidireccional)

Se utiliza SSL y la sonda autentica el certificado del servidor.

Esta tarea incluye:

- "Requisitos previos" abajo
- "Configuración del servidor UCMDB" abajo
- "Configuración de Data Flow Probe" en la página 81
- "Reiniciar los equipos" en la página 81

Requisitos previos

1. Compruebe que UCMDB y Data Flow Probe se estén ejecutando.

   Nota: Si la sonda está instalada en modo independiente, estas instrucciones hacen referencia a Puerta de enlace de sonda.

2. Si UCMDB o Data Flow Probe no están instalados en las carpetas predeterminadas, tenga en cuenta la ubicación correcta y cambie los comandos como corresponda.

Configuración del servidor UCMDB

1. **Exportar el certificado de UCMDB**

   a. Abra el símbolo del sistema y ejecute el comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <alias de almacén de claves> -keystore <ruta de acceso de archivo de almacén de claves> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   donde:

   - **alias de almacén de claves** es el nombre dado al almacén de claves.
   - **Ruta de acceso de archivo de almacén de claves** es la ruta de acceso completa de la ubicación del archivo de almacén de claves.

   Por ejemplo, para el archivo server.keystore listo para su uso, utilice el comando siguiente:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. Escriba la contraseña del almacén de claves. Por ejemplo, la contraseña del almacén de claves listo para su uso es **hppass**.

c. Compruebe que el certificado se creó en el siguiente directorio: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Proteja el conector de Data Flow Probe en UCMDB**

a. Acceda a la consola JMX de UCMDB: en el explorador web, introduzca la siguiente dirección URL: **http://<nombre de equipo o dirección IP de UCMDB>:8080/jmx-console**. Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

b. Seleccione el servicio: **Ports Management Services**.

c. Invoque el método **PortsDetails** y anote el número de puerto para HTTPS. (Valor predeterminado: 8443) Asegúrese de que el valor de la columna **Is Enabled** es **True**.

d. Vuelva a **Ports Management Services**.

e. Para asignar el conector de Data Flow Probe al modo de autenticación de servidor, invoque el método **mapComponentToConnectors** con los siguientes parámetros:

- **componentName**: mam-collectors
- **isHTTPS**: true
- **Todos los demás indicadores**: false

Se muestra el siguiente mensaje:

Operation succeeded. Component mam-collectors is now mapped to: Puertos HTTPS.

f. Vuelva a **Ports Management Services**.

g. Para asignar el conector de Confidential Manager al modo de autenticación de servidor, invoque el método **mapComponentToConnectors** con los siguientes parámetros:

- **componentName**: cm
- **isHTTPS**: true
- **Todos los demás indicadores**: false

Se muestra el siguiente mensaje:

Operation succeeded. Component cm is now mapped to: HTTPS ports.

3. **Copie el certificado de UCMDB a cada equipo de sonda**

Copie el archivo de certificado, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, en el equipo de UCMDB Server a la carpeta siguiente en cada uno de los equipos de Data Flow Probe **C:\HP\UCMDB\DataFlowProbe\conf\security**

Configuración de Data Flow Probe

Nota: Debe configurar cada equipo de Data Flow Probe.

1. **Importe el archivo server.cert, creado en** "Exportar el certificado de UCMDB " en la página 79**, al almacén de confianza de la sonda.**

   a. Abra el símbolo del sistema y ejecute el comando:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:
   \HP\UCMDB\DataFlowProbe\conf\security\hpprobeTrustStore.jks -file C:\HP\U
   CMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
   ```

   b. Escriba la contraseña del almacén de claves: logomania

   c. Cuando se le pregunte **Trust this certificate?**, pulse **y** y, a continuación **Intro**.

   Se muestra el siguiente mensaje:

   Certificate was added to keystore.

2. **Abra el archivo DataFlowProbe.properties ubicado en: C:\HP\UCMDB\DataFlowProbe\conf**

   a. Actualice la propiedad **appilog.agent.probe.protocol** a **HTTPS**.

   b. Actualice la propiedad **serverPortHttps** al número de puerto relevante. (Utilice el número de puerto del paso 2c de "Configuración del servidor UCMDB" en la página 79).

Reiniciar los equipos

Reinicie el servidor UCMDB y los equipos de sonda.

Habilitar autenticación mutua de certificados (bidireccional)

Este modo utiliza SSL y permite tanto la autenticación del servidor por parte de la sonda como la autenticación de cliente por parte del servidor. Tanto el servidor como la sonda envían sus certificados a la otra entidad para su autenticación.

Esta tarea incluye:

Requisitos previos

1. Compruebe que UCMDB y Data Flow Probe se estén ejecutando.

   Nota: Si la sonda está instalada en modo independiente, estas instrucciones hacen referencia a Puerta de enlace de sonda.

2. Si UCMDB o Data Flow Probe no están instalados en las carpetas predeterminadas, tenga en cuenta la ubicación correcta y cambie los comandos como corresponda.

Configuración del servidor UCMDB inicial

1. **Exportar el certificado de UCMDB**

   a. Abra el símbolo del sistema y ejecute el comando:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <alias de almacén de claves> -keystore <ruta de acceso de archivo de almacén de claves> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   donde:

   - **alias de almacén de claves** es el nombre dado al almacén de claves.
   - **Ruta de acceso de archivo de almacén de claves** es la ruta de acceso completa de la ubicación del archivo de almacén de claves.

   Por ejemplo, para el archivo server.keystore listo para su uso, utilice el comando siguiente:

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. Escriba la contraseña del almacén de claves. Por ejemplo, la contraseña del almacén de claves listo para su uso es **hppass**.

c. Compruebe que el certificado se creó en el siguiente directorio: **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Proteger el conector de Data Flow Probe en UCMDB**

a. Acceda a la consola JMX de UCMDB: en el explorador web, introduzca la siguiente dirección URL: **http://<nombre de equipo o dirección IP de UCMDB>:8080/jmx-console**. Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

b. Seleccione el servicio: **Ports Management Services**.

c. Invoque el método **PortsDetails** y anote el número de puerto para HTTPS con la autenticación del cliente. (Valor predeterminado: 8444) Asegúrese de que el valor de la columna **Is Enabled** es **True**.

d. Vuelva a **Ports Management Services**.

e. Para asignar el conector de Data Flow Probe al modo de autenticación mutua, invoque el método **mapComponentToConnectors** con los siguientes parámetros:

- **componentName**: mam-collectors
- **isHTTPSWithClientAuth**: true
- **Todos los demás indicadores**: false

Se muestra el siguiente mensaje:

Operation succeeded. Component mam-collectors is now mapped to: HTTPS_ CLIENT_AUTH ports.

f. Vuelva a **Ports Management Services**.

g. Para asignar el conector de Confidential Manager al modo de autenticación mutua, invoque el método **mapComponentToConnectors** con los siguientes parámetros:

- **componentName**: cm
- **isHTTPSWithClientAuth**: true
- **Todos los demás indicadores**: false

Se muestra el siguiente mensaje:

Operation succeeded. Component cm is now mapped to: HTTPS_CLIENT_AUTH ports.

3. **Copiar el certificado de UCMDB a cada equipo de sonda**

Copie el archivo de certificado, **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**, en el equipo del servidor UCMDB a la carpeta siguiente en cada uno de los equipos de Data Flow Probe: **C:\HP\UCMDB\DataFlowProbe\conf\security**

Configuración de Data Flow Probe

Nota: Debe configurar cada equipo de Data Flow Probe.

1. **Importe el archivo server.cert, creado en** "Exportar el certificado de UCMDB " en la página 82**, al almacén de confianza de la sonda.**

   a. Abra el símbolo del sistema y ejecute el comando:

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:
   \HP\UCMDB\DataFlowProbe\conf\security\hpprobeTrustStore.jks -file C:\HP\U
   CMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
   ```

   b. Escriba la contraseña del almacén de claves: logomania

   c. Cuando se le pregunte **Trust this certificate?**, pulse **y** y, a continuación **Intro**.

   Se muestra el siguiente mensaje:

   Certificate was added to keystore.

2. **Crear un nuevo archivo client.keystore**

   a. Abra el símbolo del sistema y ejecute el comando:

   ```
   c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool –genkey –alias <NombreSonda> -k
   eyalg RSA –sigalg SHA256withRSA –keysize 2048 –keystore c:\HP\UCMDB\DataF
   lowProbe\conf\security\client.keystore
   ```

   donde **NombreSonda** es el alias exclusivo de Data Flow Probe.

   Nota: Para asegurarse de que este alias es único, utilice el identificador del nombre de sonda que se dio a la sonda al definirla.

   b. Introduzca la contraseña del almacén de claves, de 6 caracteres como mínimo, y tome nota de la misma.

   c. Vuelva a introducir la contraseña para confirmarla.

   d. Pulse **Intro** tras responder a cada una de las siguientes preguntas:

   ¿Cuáles son su nombre y sus apellidos? [Desconocido]:

¿Cuál es el nombre de su unidad organizativa? [Desconocido]:

¿Cuál es el nombre de su organización? [Desconocido]:

¿Cuál es el nombre de su ciudad o localidad? [Desconocido]:

¿Cuál es el nombre de su estado o provincia? [Desconocido]:

¿Cuál es el código de dos letras de esta unidad? [Desconocido]:

e. Escriba **yes** cuando se le solicite **¿Es CN=Desconocido, OU=Desconocido, O=Desconocido, L=Desconocido, ST=Desconocido, C=Desconocido correcto?**

f. Pulse **Intro** tras responder a la siguiente pregunta:

Introduzca la contraseña de clave de <probekey> (RETURN si es la misma que la contraseña del almacén de claves):

g. Compruebe que el archivo se creó en la carpeta siguiente y asegúrese de que su tamaño es mayor que 0: **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

3. **Exportar el nuevo certificado de cliente**

a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias <NombreSonda> -keystore C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -file C:\hp\UCMDB\DataFlowProbe\conf\security\<NombreSonda>.cert
```

b. Cuando se le solicite, escriba la contraseña del almacén de claves. (La contraseña del paso 2b anterior).

Se muestra el siguiente mensaje:

Certificate stored in file <C:\hp\UCMDB\DataFlowProbe\conf\security\<NombreSonda>.cert>

4. **Abra el archivo DataFlowProbe.properties ubicado en: C:\HP\UCMDB\DataFlowProbe\conf**

a. Actualice la propiedad **appilog.agent.probe.protocol** a **HTTPS**.

b. Actualice la propiedad **serverPortHttps** al número de puerto relevante. (Utilice el número de puerto del paso 2c de "Configuración del servidor UCMDB inicial" en la página 82).

5. **Abra el archivo ssl.properties ubicado en: C:\HP\UCMDB\DataFlowProbe\conf\security**

a. Actualice la propiedad **javax.net.ssl.keyStore** a **client.keystore**.

b. Cifre la contraseña del paso 2b anterior:

i. Inicie Data Flow Probe (o asegúrese de que se está ejecutando).

ii. Acceda a la sonda JMX. Vaya a: **http://<nombre_host_sonda>:1977**

Por ejemplo, si ejecuta la sonda localmente, vaya a: **http://localhost:1977**.

iii. Pulse el vínculo **type=MainProbe**.

iv. Desplácese hasta la operación **getEncryptedKeyPassword**.

v. Introduzca la contraseña en el campo **Key Password**.

vi. Pulse el botón **getEncryptedKeyPassword**.

c. Copie y pegue la contraseña cifrada para actualizar la propiedad **javax.net.ssl.keyStorePassword**.

Nota: Los números se separan con comas. Por ejemplo: -20,50,34,-40,-50.)

6. **Copiar el certificado de sonda al equipo de UCMDB**

Copie el archivo **C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert** desde el equipo de Data Flow Probe al equipo de UCMDB en **C:\HP\UCMDB\UCMDBServer\conf\security\<NombreSonda>.cert**.

Configuración adicional del servidor UCMDB

1. **Agregue cada certificado de sonda al almacén de confianza de UCMDB**

Nota: Debe completar los pasos siguientes para cada certificado de sonda.

a. Abra el símbolo del sistema y ejecute el comando:

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore C:\hp
\UCMDB\UCMDBServer\conf\security\server.truststore -file C:\hp\UCMDB\UCMDB
Server\conf\security\<NombreSonda>.cert -alias <NombreSonda>
```

b. Escriba la contraseña del almacén de claves. Por ejemplo, la contraseña del almacén de claves listo para su uso es **hppass**.

c. Cuando se le pregunte **Trust this certificate?**, pulse **y** y, a continuación **Intro**.

Se muestra el siguiente mensaje:

Certificate was added to keystore

Reiniciar los equipos

Reinicie el servidor UCMDB y los equipos de sonda.

Controlar la ubicación del archivo domainScopeDocument

El sistema de archivos de la sonda contiene (de manera predeterminada) tanto la clave de cifrado como el archivo **domainScopeDocument**. Cada vez que se inicia la sonda, recupera el archivo **domainScopeDocument** del servidor y lo almacena en su sistema de archivos. Para evitar que usuarios no autorizados obtengan esas credenciales, puede configurar la sonda para que el archivo **domainScopeDocument** se almacene en la memoria de la sonda y no en su sistema de archivos.

Para controlar la ubicación del archivo domainScopeDocument:

1. Abra **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** y cambie:

   ```
   appilog.collectors.storeDomainScopeDocument=true
   ```

   por:

   ```
   appilog.collectors.storeDomainScopeDocument=false
   ```

   Las carpetas serverData de Puerta de enlace de sonda y Administrador de sonda ya no contienen el archivo **domainScopeDocument**.

   Para obtener más información sobre el uso del archivo **domainScopeDocument** para proteger DFM, consulte "Administración de credenciales de Data Flow" en la página 50.

2. Reinicie la sonda.

Crear un almacén de claves para Data Flow Probe

1. En el equipo donde está instalada la sonda, ejecute el siguiente comando:

   ```
   c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool –genkey –alias <NombreSonda> -keya
   lg RSA –sigalg SHA256withRSA –keysize 2048 –keystore c:\HP\UCMDB\DataFlowPro
   be\conf\security\client.keystore
   ```

2. Escriba una contraseña para el nuevo almacén de claves.

3. Introduzca la información cuando se le pida.

4. Cuando se le pregunte **Is CN=… C=… Correct?**, introduzca **yes** y, a continuación, pulse **Intro**.

5. Pulse **Intro** de nuevo para aceptar la contraseña del almacén de claves como la contraseña de clave.

6. Compruebe que **client.keystore** se crea en el siguiente directorio: **C:\HP\UCMDB\DataFlowProbe\conf\security**.

Cifrar las contraseñas del almacén de claves y el almacén de confianza de la sonda

Las contraseñas del almacén de claves y el almacén de confianza de la sonda se almacenan cifradas en **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. Este procedimiento explica cómo cifrar la contraseña.

1. Inicie Data Flow Probe (o compruebe que se está ejecutando).

2. Acceda a la consola JMX de Data Flow Probe: Inicie un explorador web y escriba la siguiente dirección: http://<Dirección IP o nombre del equipo de Data Flow Probe>:1977. Si está ejecutando Data Flow Probe localmente, escriba http://localhost:1977.

   Nota: Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña. Si no ha creado un usuario, utilice el nombre de usuario predeterminado sysadmin y la contraseña sysadmin para iniciar sesión.

3. Localice el servicio **Type=MainProbe** y haga clic en el vínculo para abrir la página de operaciones.

4. Localice la operación **getEncryptedKeyPassword**.

5. Introduzca la contraseña del almacén de claves o el almacén de confianza en el campo **Key Password** y llame a la operación haciendo clic en **getEncryptedKeyPassword**.

6. El resultado de la llamada es una cadena de contraseña cifrada como, por ejemplo:

   ```
   66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
   ```

7. Copie y pegue la contraseña cifrada en la línea correspondiente al almacén de claves o almacén de confianza en el siguiente archivo: **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties.**

Almacén de claves y almacén de confianza predeterminados de servidor y Data Flow Probe

Esta sección incluye los siguientes temas:

- "Servidor UCMDB" abajo
- "Data Flow Probe" abajo

Servidor UCMDB

Los archivos están ubicados en el siguiente directorio:
C:\HP\UCMDB\UCMDBServer\conf\security.

Entidad	Nombre de archivo/Término	Contraseña/Término	Alias
Almacén de claves del servidor	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Almacén de confianza del servidor	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	hpcert (entrada de confianza predeterminada)
Almacén de claves del cliente	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow Probe

Los archivos están ubicados en el siguiente directorio:
C:\HP\UCMDB\DataFlowProbe\conf\security.

Entidad	Nombre de archivo/Término	Contraseña/Término	Alias
Almacén de claves de la sonda	hpprobeKeyStore.jks (pKeyStoreFile)	logomania (pKeyStorePass)	hpprobe
Data Flow Probe utiliza el almacén de claves **cKeyStoreFile** como almacén de claves predeterminado durante el procedimiento de autenticación. Se trata de un almacén de claves de cliente que forma parte de la instalación de UCMDB.			
Almacén de confianza de la sonda	hpprobeTrustStore.jks (pTrustStoreFile)	logomania (pTrustStorePass)	hpprobe (entrada de confianza predeterminada)
La contraseña **cKeyStorePass** es la contraseña predeterminada de **cKeyStoreFile**.			

Capítulo 6: Autenticación de Lightweight Single Sign-On (LW-SSO) – Referencia general

Este capítulo incluye:

Información 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.

- **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 deben 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.

Requisitos del sistema de LW-SSO

Aplicación	Versión	Comentarios
Java	1.5 y posterior	
HTTP Servlets API	2.1 y posterior	
Internet Explorer	6.0 y posterior	El explorador debe tener habilitada las cookies en la sesión HTTP y la funcionalidad de redirección 302 de HTTP.
Firefox	2.0 y posterior	El explorador debe tener habilitada las cookies en la sesión HTTP y la funcionalidad de redirección 302 de HTTP.
Autenticaciones de JBoss	JBoss 4.0.3 JBoss 4.3.0	
Autenticaciones de Tomcat	Tomcat 5.0.28 independiente Tomcat 5.5.20 independiente	
Autenticaciones de Acegi	Acegi 0.9.0 Acegi 1.0.4	
Motores de servicios web	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

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** solo 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 solo 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 solo puedan generar tokens LW-SSO aquellas aplicaciones que usen marcos de autenticación sólidos y seguros.

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

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

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

  Además, en los casos en que un usuario inicie sesión en una aplicación (AppA) y seguidamente acceda a una segunda aplicación (AppB) que use la autenticación de contenedores o aplicaciones, si no se asigna el usuario, obligará al usuario a iniciar sesión manualmente en AppB y especificar un nombre de usuario. Si el usuario especifica un nombre de usuario distinto

del que se usó para iniciar sesión en AppA, puede producirse el siguiente comportamiento: si el usuario accede posteriormente a una tercera aplicación (AppC) desde AppA o AppB, accederá a ella usando los mismos nombres de usuario que se emplearon para iniciar sesión en AppA o AppB, respectivamente.

- **Gestor de identidades**. Se usa para la autenticación, todos los recursos sin proteger del Gestor de identidades se deben configurar con la opción **nonsecureURLs** en el archivo de seguridad de LW-SSO.
- **Modo de demostración de LW-SSO.**
  - El modo de demostración debe usarse exclusivamente con fines de demostración.
  - El modo de demostración debe usarse exclusivamente en redes no protegidas.
  - El modo de demostración no debe usarse en un entorno de producción. No debe usarse ninguna combinación del modo de demostración y el modo de producción.

Solución de problemas y limitaciones

En esta sección se describen los problemas y las limitaciones conocidas cuando se trabaja con la autenticación de LW-SSO.

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 solo 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 solo 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 solo 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 solo 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 (solo 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). Esta 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`

- Comportamiento de cookies de terceros en Internet Explorer:

  Microsoft Internet Explorer 6 contiene un módulo que admite la especificación P3P (Plataforma para preferencias de privacidad), lo que significa que las cookies procedentes de un dominio de terceros se bloquean, de forma predeterminada, en la zona de seguridad Internet. Las cookies de la sesión también se consideran cookies de terceros en Internet Explorer, por lo que se bloquean y provocan que LW-SSO deje de funcionar. Para obtener más información, consulte: `http://support.microsoft.com/kb/323752/en-us`.

  Para solucionar este problema, agregue la aplicación iniciada (o un subconjunto de dominio DNS como *.midominio.com) a la zona Intranet/Sitios de confianza del equipo (en Microsoft Internet Explorer, seleccione **Menú > Herramientas > Opciones de Internet > Seguridad > Intranet local > Sitios > Opciones avanzadas)** y se aceptarán las cookies.

  Precaución: La cookie de la sesión LW-SSO solo es una de las cookies utilizadas por la aplicación de terceros bloqueada.

- **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.

- **Modo de demostración.** En el modo de demostración, LW-SSO admite vínculos de una aplicación a otra pero no permite escribir una dirección URL en la ventana del explorador, porque no hay ningún encabezado de origen de referencia de HTTP en este caso.

Capítulo 7: Autenticación de inicio de sesión de HP Universal CMDB

Este capítulo incluye:

Configuración de un método de autenticación

Se puede realizar la autenticación:

- **En el servicio de HP Universal CMDB interno.**
- **Mediante el Protocolo ligero de acceso a directorios (LDAP).** Puede utilizar un servidor LDAP externo y dedicado para almacenar la información de autenticación en lugar de utilizar el servicio de HP Universal CMDB interno. El servidor LDAP debe residir en la misma subred que todos los servidores de HP Universal CMDB.

  Para obtener más información sobre LDAP, consulte la sección acerca de la asignación LDAP en la *HP Universal CMDB – Guía de administración*.

  El método de autenticación predeterminado utiliza el servicio de HP Universal CMDB interno. Si utiliza el método predeterminado, no es necesario realizar ningún cambio en el sistema.

  Estas opciones se aplican a los inicios de sesión que se realizan a través de los servicios web y a través de la interfaz de usuario.
- **Mediante LW-SSO.** HP Universal CMDB está configurado con LW-SSO. LW-SSO permite iniciar sesión en HP Universal CMDB y tener acceso automático a otras aplicaciones configuradas que se ejecutan en el mismo dominio, sin que sea necesario iniciar sesión en esas aplicaciones.

  Cuando se habilita el soporte de autenticación LW-SSO (está deshabilitado de forma predeterminada), hay que asegurarse de que las demás aplicaciones del entorno Single Sign-On tengan LW-SSO habilitado y funcionen con el mismo parámetro initString.

Habilitación del inicio de sesión en HP Universal CMDB con LW-SSO

Para habilitar LW-SSO en HP Universal CMDB, siga este procedimiento:

1. Para acceder a la consola JMX, introduzca la siguiente dirección en el explorador web: **http://<nombre_servidor>:8080/jmx-console**, donde **<nombre_servidor>>** equivale al nombre del equipo donde se ha instalado HP Universal CMDB.
2. En **UCMDB-UI**, haga clic en **name=LW-SSO Configuration** para abrir la página de operaciones.
3. Configure la cadena init mediante el método **setInitString**.
4. Configure el nombre de dominio del equipo en el que está instalado UCMDB mediante el método **setDomain**.
5. Llame al método **setEnabledForUI** con el parámetro establecido en **True.**
6. **Opcional**. Si desea trabajar usando la funcionalidad multidominio, seleccione el método **addTrustedDomains**, introduzca los valores del dominio y haga clic en **Invoke**.
7. **Opcional.** Si desea trabajar usando un proxy inverso, seleccione el método **updateReverseProxy**, ajuste el parámetro **Está habilitado el proxy inverso** en **True**, especifique una dirección URL para el parámetro **Reverse proxy full server URL** y haga clic en Invoke. Si desea acceder a UCMDB directamente y usando un proxy inverso, establezca la siguiente configuración adicional: seleccione el método **setReverseProxyIPs**, especifique la dirección IP para el parámetro ip/s de proxy inverso y haga clic en **Invoke.**
8. **Opcional**. Si desea acceder a UCMDB usando un punto de autenticación externo, seleccione el método **setValidationPointHandlerEnable**, establezca el parámetro **Is validation point handler enabled** en **True**, especifique la dirección URL para el punto de autenticación en el parámetro **Authentication point server** y haga clic en **Invoke.**
9. Para ver la configuración de LW-SSO cuando se guarda en el mecanismo de configuración, llame al método **retrieveConfigurationFromSettings**.
10. Para ver la configuración real de LW-SSO cargada, llame al método **retrieveConfiguration**.

Nota: No puede habilitar LW-SSO mediante la interfaz de usuario.

Configuración de una conexión segura con el protocolo SSL (Capa de sockets seguros)

Dado que en el proceso de inicio de sesión se pasa información confidencial entre HP Universal CMDB y el servidor LDAP, se puede aplicar un determinado nivel de seguridad al contenido. Para ello, es necesario habilitar la comunicación SSL en el servidor LDAP y configurar HP Universal CMDB para trabajar con SSL.

HP Universal CMDB admite SSL que utiliza un certificado emitido por una entidad de certificación (CA) de confianza.

La mayoría de servidores LDAP, incluido Active Directory, puede mostrar un puerto seguro para una conexión basada en SSL. Si utiliza Active Directory con una CA privada, debe agregar la CA a la lista de entidades de certificación de confianza en JRE.

Para obtener más información sobre la configuración de la plataforma HP Universal CMDB para permitir la comunicación mediante SSL, consulte "Habilitar la comunicación de Capa de sockets seguros (SSL)" en la página 17.

Para agregar una CA a la lista de entidades de certificación de confianza para mostrar un puerto seguro en una conexión basada en SSL:

1. Exporte un certificado de la CA e impórtelo en la JVM que utiliza HP Universal CMDB, siguiendo estos pasos:

   a. En el equipo servidor de UCMDB, acceda a la carpeta **UCMDBServer\bin\JRE\bin**.

   b. Ejecute el siguiente comando:

   ```
   Keytool -import -file <su archivo de certificado> -keystore C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

   Por ejemplo:

   ```
   Keytool -import -file c:\ca2ss_ie.cer -keystore C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

2. Seleccione **Administración > Configuración de infraestructura > General de LDAP**.

   Nota: También es posible establecer esta configuración mediante la consola JMX. Para obtener más información, consulte "Cómo habilitar y definir el método de autenticación LDAP mediante la consola JMX" en la página 103.

3. Localice **URL del servidor LDAP** e introduzca un valor, con el formato:

   ```
   ldaps://<host ldap>[:<puerto>]/[<DN de base>][??ámbito]
   ```

   Por ejemplo:

```
ldaps://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

Tenga en cuenta la **s** en **ldaps**.

4. Haga clic en **Guardar** para guardar el nuevo valor o en **Restaurar predeterm.** para reemplazar la entrada por el valor predeterminado (una dirección URL en blanco).

Uso de la consola JMX para probar las conexiones LDAP

Esta sección describe un método para probar la configuración de autenticación LDAP mediante la consola JMX.

1. Inicie un explorador web y escriba la siguiente dirección: **http://<nombre_servidor>:8080/jmx-console**, donde **<nombre_servidor>>** equivale al nombre del equipo donde se ha instalado HP Universal CMDB.

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. En **UCMDB**, haga clic en **UCMDB:service=LDAP Services** para abrir la página de operaciones.

3. Localice **testLDAPConnection.**

4. En el cuadro **Value** del parámetro **customer id**, introduzca el Id. de cliente.

5. Haga clic en **Invoke.**

   La página JMX MBEAN Operation Result indica si la conexión LDAP se ha establecido correctamente. Si se ha establecido correctamente, la página muestra además los grupos raíz de LDAP.

Cómo habilitar y definir el método de autenticación LDAP

Puede habilitar y definir el método de autenticación LDAP en un sistema HP Universal CMDB.

Nota:

- También puede establecer la configuración de autenticación LDAP mediante la consola JMX. Para obtener más información, consulte "Cómo habilitar y definir el método de autenticación LDAP mediante la consola JMX" en la página 103.
- Para ver un ejemplo de configuración de autenticación LDAP, consulte "Configuración de autenticación LDAP - Ejemplo" en la página 104.

Para habilitar y definir el método de autenticación LDAP en la interfaz de usuario de UCMDB:

1. Seleccione **Administración > Configuración de infraestructura > General de LDAP**.
2. Seleccione **URL del servidor LDAP** e introduzca el valor de la dirección URL de LDAP, con el formato:

   ```
   ldap://<host ldap>[:<puerto>]/[<DN de base>][??ámbito]
   ```

   Por ejemplo:

   ```
   ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
   ```

3. Seleccione la categoría **Definición de grupo LDAP**, localice **DN de base de grupos** e introduzca el nombre distintivo del grupo general.
4. Localice **DN de base de grupos raíz** e introduzca el nombre distintivo del grupo raíz.
5. Seleccione la categoría **General de LDAP**, localice **Habilitar sincronización de permisos de usuario** y compruebe que el valor está establecido en **True.**
6. Seleccione la categoría **Autenticación general para LDAP**, localice **Contraseña de usuario con derecho a búsqueda** y rellene la contraseña.
7. Seleccione la categoría **Opciones LDAP para clases y atributos**, localice **Objeto de clase de grupo** y rellene el nombre de clase de objeto (**grupo** para Microsoft Active Directory y **groupOfUniqueNames** para Oracle Directory Server).
8. Localice **Atributo de miembro de grupos** y rellene el nombre de atributo (**miembro** para Microsoft Active Directory y **uniqueMember** para Oracle Directory Server).
9. Localice **Clase de objeto de usuarios** y rellene el nombre de la clase de objeto(**usuario** para Microsoft Active Directory e **inetOrgPerson** para Oracle Directory Server).
10. Localice **Atributo UUID** y rellene el atributo de identificación exclusivo para un usuario de su servidor de directorio. Asegúrese de seleccionar un atributo que sea exclusivo en el servidor de directorio. Por ejemplo, cuando se usa SunOne/Oracle Directory Server, el atributo de UID no es exclusivo. En tal caso, utilice el atributo de dirección de correo electrónico o el nombre distintivo. El uso de un atributo que no sea exclusivo como atributo de identificación en UCMDB puede provocar un comportamiento incoherente durante el inicio de sesión.
11. Guarde los nuevos valores. Para reemplazar una entrada por el valor predeterminado, haga clic en **Restaurar predeterm.**
12. Si la configuración de infraestructura de **General de LDAPS**, **Se ha aplicado la distinción**

entre mayúsculas y minúsculas en la autenticación con LDAP, se establece en **True**, la autenticación distingue entre mayúsculas y minúsculas.

> **Precaución:** Cuando se cambia el valor de la configuración de esta infraestructura, todos los usuarios externos deben eliminar manualmente el administrador de UCMDB.

13. Asigne grupos de usuarios LDAP a grupos de usuario de UCMDB. Para obtener más información, consulte "Autenticación de inicio de sesión de HP Universal CMDB" en la página 98.

14. Si desea definir un conjunto predeterminado de permisos para usuarios de un grupo LDAP que no tiene una asignación de grupo, seleccione la categoría **General de LDAP**, localice **Grupo de usuarios asignado automáticamente** e introduzca el nombre del grupo.

15. **Importante:** Si está configurando LDAP en un entorno de alta disponibilidad, debe reiniciar el clúster para que los cambios entren en vigor.

> **Nota:** Cada usuario de LDAP tiene un nombre, un apellido y una dirección de correo electrónico guardados en el repositorio local. Si el valor de cualquiera de esos parámetros que se almacena en el servidor LDAP es diferente del valor del repositorio local, los valores del servidor LDAP sobrescribirán los valores locales en cada inicio de sesión.

Cómo habilitar y definir el método de autenticación LDAP mediante la consola JMX

Esta tarea describe cómo establecer la configuración de autenticación LDAP mediante la consola JMX.

> **Nota:**
>
> - En un entorno de alta disponibilidad, asegúrese de iniciar la sesión en la consola JMX del servidor Escritor.
> - También puede establecer la configuración de autenticación LDAP en UCMDB. Para obtener más información, consulte "Cómo habilitar y definir el método de autenticación LDAP" en la página 101.
> - Para ver un ejemplo de configuración de autenticación LDAP, consulte "Configuración de autenticación LDAP - Ejemplo" en la página siguiente.

Para establecer la configuración de autenticación LDAP:

1. Inicie un explorador web y escriba la siguiente dirección: **http://<nombre_servidor>:8080/jmx-console**, donde **<nombre_servidor>>** equivale al nombre del equipo donde se ha instalado HP Universal CMDB.

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. En **UCMDB**, haga clic en **UCMDB:service=LDAP Services** para abrir la página de operaciones.

3. Para ver la configuración de autenticación LDAP actual, localice el método **getLDAPSettings**. Haga clic en **Invoke**. Se muestra una tabla con toda la configuración de LDAP y sus valores.

4. Para cambiar los valores de la configuración de autenticación LDAP, localice el método **configureLDAP**. Introduzca los valores de configuración relevantes y haga clic en **Invoke**. La página JMX MBEAN Operation Result indica si la configuración de autenticación LDAP se ha actualizado correctamente.

   Nota: Si no introduce un valor en un parámetro de configuración, se conserva el valor actual.

5. Tras establecer la configuración LDAP, puede comprobar las credenciales de usuario LDAP:

   a. Localice el método **verifyLDAPCredentials**.

   b. Escriba el Id. de cliente, el nombre de usuario y la contraseña.

   c. Haga clic en **Invoke**.

      La página JMX MBEAN Operation Result indica si el usuario pasa la autenticación LDAP.

6. **Importante:** Si está configurando LDAP en un entorno de alta disponibilidad, debe reiniciar el clúster para que los cambios entren en vigor.

Nota: Cada usuario de LDAP tiene un nombre, un apellido y una dirección de correo electrónico guardados en el repositorio local. Si el valor de cualquiera de esos parámetros que se almacena en el servidor LDAP es diferente del valor del repositorio local, los valores del servidor LDAP sobrescribirán los valores locales en cada inicio de sesión.

Configuración de autenticación LDAP - Ejemplo

La tabla siguiente contiene un ejemplo de valores de configuración para la autenticación LDAP:

Opción	Valor
Clase de objeto de usuarios	user

Opción	Valor
Se ha aplicado la distinción entre mayúsculas y minúsculas en la autenticación con LDAP	false
Atributo de miembro de grupos	member
Resolución de nombre distintivo (DN)	true
Filtro de grupos raíz	(objectCategory=group)
Cadena de conexión de LDAP	ldap://myldap.example.com:389/OU=Users,OU=Dept,OU=US,DC=example,DC=com??sub
Usuario de búsqueda de LDAP	CN=John Doe,OU=Users,OU=Dept,OU=US,DC=example,DC=com
Objeto de clase de grupo	group
Use el algoritmo ascendente para buscar grupos principales	true
Atributo UUID	sAMAccountName
Atributo de nombre de grupos	cn
Filtro de base de grupo	(objectclass=group)
Filtro de usuarios	(&(sAMAccountName=*)(objectclass=user))
Número de reintentos de búsqueda	3
Atributo de nombre para mostrar de grupos	cn
Alcance de grupos raíz	sub
Atributo de nombre de usuario para mostrar	cn
Alcance de la búsqueda de grupos	sub
Habilitar autenticación LDAP	false
Habilitar la sincronización de LDAP	true
Grupo raíz	OU=Users,OU=Security Groups,DC=example,DC=com
Base de grupo	OU=AMRND,OU=Security Groups,DC=example,DC=com

Opción	Valor
Grupo predeterminado	AdminsGroup
Atributo de descripción de grupos	description

Recuperación de la configuración de LW-SSO actual en un entorno distribuido

Si UCMDB está incrustado en un entorno distribuido, por ejemplo, en un despliegue de BSM, lleve a cabo el siguiente procedimiento para recuperar la configuración de LW-SSO actual en el equipo de procesamiento.

Para recuperar la configuración de LW-SSO actual:

1. Inicie un explorador web y escriba la siguiente dirección: `http://localhost.<nombre_dominio>:8080/jmx-console.`

   Es posible que se le solicite un nombre de usuario y una contraseña.

2. Localice **UCMDB:service=Security Services** y haga clic en el vínculo para abrir la página de operaciones.

3. Localice la operación **retrieveLWSSOConfiguration**.

4. Haga clic en **Invoke** para recuperar la configuración.

Capítulo 8: Confidential Manager

Este capítulo incluye:

Información general de Confidential Manager

El marco Confidential Manager soluciona los problemas de administración y distribución de datos confidenciales en HP Universal CMDB y otros productos de HP Software.

Confidential Manager consta de dos componentes principales: el cliente y el servidor. Estos dos componentes son responsables de transferir datos de manera segura.

- El cliente de Confidential Manager es una biblioteca que las aplicaciones utilizan para acceder a datos confidenciales.
- El servidor de Confidential Manager recibe las solicitudes de los clientes de Confidential Manager, o de clientes de terceros, y realiza las tareas necesarias. El servidor de Confidential Manager es responsable de guardar los datos de forma segura.

Confidential Manager cifra las credenciales en el transporte, la caché del cliente, la persistencia y la memoria. Confidential Manager utiliza criptografía simétrica para transportar credenciales entre el cliente de Confidential Manager y el servidor de Confidential Manager mediante un secreto compartido. Confidential Manager utiliza diversos secretos para el cifrado de la caché, la persistencia y el transporte según la configuración.

Para obtener directrices detalladas sobre la administración del cifrado de credenciales en Data Flow Probe, consulte "Administración de credenciales de Data Flow" en la página 50.

Consideraciones de seguridad

- Puede utilizar los siguientes tamaños de clave en el algoritmo de seguridad: 128, 192 y 256 bits. El algoritmo se ejecuta con mayor rapidez con la clave más pequeña, pero es la menos segura. El tamaño de 128 bits es suficientemente seguro en la mayoría de los casos.
- Para aumentar la seguridad del sistema, utilice MAC: ajuste **useMacWithCrypto** en **true.** Para obtener más información, consulte "Propiedades de cifrado" en la página 110.
- Para aprovechar los proveedores de seguridad sólida de clientes, puede utilizar el modo JCE.

Configurar el servidor de HP Universal CMDB

Al trabajar con HP Universal CMDB, debe configurar el secreto y las propiedades de cifrado mediante los siguientes métodos de JMX:

1. En el equipo servidor de HP Universal CMDB, inicie el explorador web e introduzca la dirección del servidor, del siguiente modo: **http://<IP o nombre de host del servidor UCMDB>:8080/jmx-console.**

   Es posible que tenga que iniciar sesión con un nombre de usuario y una contraseña.

2. En UCMDB, haga clic en **UCMDB:service=Security Services** para abrir la página de operaciones.

3. Para recuperar la configuración actual, localice la operación **CMGetConfiguration**.

   Haga clic en **Invoke** para mostrar el archivo XML de configuración del servidor de Confidential Manager.

4. Para realizar cambios en la configuración, copie el XML al que llamó en el paso anterior en un editor de texto. Realice cambios conforme a la tabla de "Propiedades de cifrado" en la página 110.

   Localice la operación **CMSetConfiguration**. Copie la configuración actualizada en el cuadro **Value** y haga clic en **Invoke.** La nueva configuración se escribe en el servidor UCMDB.

5. Para agregar usuarios a Confidential Manager para la autorización y la réplica, localice la operación **CMAddUser**. Este proceso también es útil en el proceso de réplica. En la réplica, el servidor esclavo debe comunicarse con el servidor maestro mediante un usuario con privilegios.

   - **username**. El nombre de usuario.
   - **customer.** El valor predeterminado es ALL_CUSTOMERS.
   - **resource.** El nombre del recurso. El valor predeterminado es ROOT_FOLDER.
   - **permission.** Elija entre ALL_PERMISSIONS, CREATE, READ, UPDATE y DELETE. El valor predeterminado es ALL_PERMISSIONS.

   Haga clic en **Invoke**.

6. Si es necesario, reinicie HP Universal CMDB.

   En la mayoría de los casos no es necesario reiniciar el servidor. Es posible que deba reiniciar el servidor cuando cambie uno de los siguientes recursos:

   - Tipo de almacenamiento
   - Nombres de columnas o nombre de tabla de la base de datos

- El creador de la conexión de base de datos
- Las propiedades de conexión a la base de datos (es decir, dirección URL, usuario, contraseña, nombre de clase de controlador)
- Tipo de base de datos

Nota:

- Es importante que el servidor UCMDB y sus clientes tengan las misma propiedades de cifrado de transporte. Si se cambian estas propiedades en el servidor UCMDB, debe cambiarlas en todos los clientes. (Esto no es relevante para Data Flow Probe, ya que se ejecuta en el mismo proceso con el servidor UCMDB; es decir, no se requiere configuración de cifrado de transporte).
- La réplica de Confidential Manager no está configurada de forma predeterminada y puede configurarse en caso necesario.
- Si se habilita la réplica de Confidential Manager y cambia la propiedad **initString** de transporte o cualquier otra propiedad de cifrado del maestro, todos los esclavos deben adoptar los cambios.

Definiciones

Propiedades de cifrado de almacenamiento. Configuración que define cómo el servidor contiene y cifra los datos (si en una base de datos o en un archivo, qué propiedades de cifrado deben cifrar o descifrar los datos, etc.), cómo se almacenan las credenciales de forma segura, cómo se procesa el cifrado y conforme a qué configuración.

Propiedades de cifrado de transporte. La configuración de transporte define cómo el servidor y los clientes cifran el transporte entre sí, qué configuración se usa, cómo se transfieren las credenciales de forma segura, cómo se procesa el cifrado y conforme a qué configuración. Debe utilizar las mismas propiedades de cifrado para cifrar y descifrar el transporte, tanto en el servidor como en el cliente.

Réplicas y propiedades de cifrado de réplica. Los datos que Confidential Manager contiene de forma segura se replican de manera segura entre varios servidores. Estas propiedades definen cómo se transfieren los datos entre el servidor esclavo y el servidor maestro.

Nota:

- La tabla de base de datos que contiene la configuración del servidor de Confidential Manager se denomina: **CM_CONFIGURATION.**
- El archivo de configuración predeterminado del servidor de Confidential Manager está ubicado en app-infra.jar y se denomina **defaultCMServerConfig.xml.**

Propiedades de cifrado

La siguiente tabla describe las propiedades de cifrado. Para obtener más información sobre estos parámetros, consulte "Configurar el servidor de HP Universal CMDB" en la página 108.

Parámetro	Descripción	Valor recomendado
encryptTransportMode	Cifra los datos transportados: true, false	true
encryptDecrypt InitString	Contraseña de cifrado	Más de 8 caracteres
cryptoSource	Biblioteca de implementación de cifrado que se va a usar: • lw • jce • windowsDPAPI • lwJCECompatible	lw
lwJCEPBE CompatibilityMode	Admite versiones anteriores de criptografía ligera: • true • false	true
cipherType	El tipo de cifrado que utiliza Confidential Manager. Confidential Manager solo admite un valor: **symmetricBlockCipher**	symmetric BlockCipher
engineName	• AES • Blowfish • DES • 3DES • Null (sin cifrado)	AES
algorithmModeName	Modo de algoritmo de cifrado de bloque: • CBC	CBC

Parámetro	Descripción	Valor recomendado
algorithmPaddingName	Estándares de relleno: • PKCS7Padding • PKCS5Padding	PKCS7Padding
keySize	Depende del algoritmo (lo que admita **engineName**)	256
pbeCount	Número de veces que hay que ejecutar el hash para crear la clave a partir de **encryptDecryptInitString.** Cualquier número positivo.	1000
pbeDigestAlgorithm	Tipo de hash: • SHA1 • SHA256 • MD5	SHA256
encodingMode	Representación ASCII del objeto cifrado: • Base64 • Base64Url	Base64Url
useMacWithCrypto	Define si se utiliza MAC con la criptografía: • true • false	false
macType	Tipo de código de autenticación de mensajes (MAC): • hmac	hmac
macKeySize SHA256	Depende del algoritmo MAC	256
macHashName	El algoritmo MAC hash: • SHA256	SHA256

Capítulo 9: Protección de alta disponibilidad

Este capítulo incluye:

Autenticación de clústeres

Para habilitar la autenticación de clústeres:

1. En UCMDB, vaya a **Administración > Administrador de configuración de infraestructura**.

2. Busque la configuración **Habilitar autenticación al unirse a un clúster de alta disponibilidad** y establézcalo como **true**.

3. Indique un único almacén de claves de autenticación de servidores (certificado + claves pública y privada) en formato JKS. Este almacén de claves se coloca en todos los servidores y se utiliza para la autenticación al conectarse con un clúster de alta disponibilidad.

   Coloque el almacén de claves en la siguiente ubicación: **<carpeta de instalación de UCMDB>\conf\security** asígnele el nombre **cluster.authentication.keystore.**

   Nota: UCMDB viene con este almacén de claves preconfigurado de serie. Este almacén es el mismo para todas las instalaciones de UCMDB y, por lo tanto, no es seguro. Si desea autenticar solicitudes de unión de forma segura, elimine este archivo y cree otro.

4. Genere un almacén de claves para la autenticación de clústeres como se indica a continuación:

   a. Desde C:\hp\UCMDB\UCMDBServer\bin\jre\bin, ejecute el siguiente comando:

   ```
   keytool -genkey -alias hpcert –keystore <carpeta de instalación de UCMDB>
   \conf\security\cluster.authentication.keystore -keyalg RSA
   ```

   Se abrirá el cuadro de diálogo de la consola y se le indicará que introduzca una nueva contraseña para el almacén de claves.

   b. La contraseña predeterminada es **hppass**. Si desea usar otra contraseña, actualice el servidor ejecutando el siguiente método JMX: **UCMDB:service=High Availability Services: changeClusterAuthenticationKeystorePassword**

c. En el cuadro de diálogo de la consola, responda a la pregunta por su nombre y sus apellidos con el nombre del clúster.

d. Introduzca los parámetros restantes en función de los datos de su organización.

e. Escriba una contraseña de la clave. Dicha contraseña debe coincidir con la contraseña del almacén de claves.

Se creará un almacén de claves JKS en **<carpeta de instalación de UCMDB>\conf\security\cluster.authentication.keystore**

5. Sustituya el almacén de claves antiguo (**<carpeta de instalación de UCMDB>\conf\security\cluster.authentication.keystore**) en todos los servidores del clúster por el nuevo.

6. Reinicie todos los servidores del clúster.

Cifrado de mensajes de clúster

Utilice el cifrado de mensajes de clúster para cifrar todos los mensajes del clúster.

Para activar el cifrado de mensajes de clúster:

1. En UCMDB, vaya a **Administración > Administrador de configuración de infraestructura**.

2. Busque la configuración **habilitar cifrado de comunicación del clúster de alta disponibilidad** y establézcalo como **true**.

3. Proporcione una clave secreta para el cifrado simétrico en todos los servidores. La clave debe colocarse en un almacén de claves de tipo JCEKS en la siguiente ubicación **<carpeta de instalación de UCMDB>\conf\security\cluster.encryption.keystore**.

Nota: UCMDB viene con este almacén de claves preconfigurado de serie. Este almacén es el mismo para todas las instalaciones de UCMDB y, por lo tanto, no es seguro. Si desea cifrar los mensajes de clúster de forma segura, borre este archivo y cree otro siguiendo este procedimiento.

4. Desde **<carpeta de instalación de UCMDB>\bin\jre\bin**, ejecute el comando siguiente:

Keytool –genseckey –alias hpcert –keystore <carpeta de instalación de UCMDB>\conf\security\cluster.encryption.keystore –storetype JCEKS

5. Se le pedirá la contraseña del nuevo almacén. La contraseña predeterminada es “hppass”. Si desea usar otra contraseña, deberá actualizar el servidor ejecutando el siguiente método JMX:

UCMDB:service=High Availability Services: changeClusterEncryptionKeystorePassword

6. Sustituya el almacén de claves antiguo (**<carpeta de instalación de UCMDB>\conf\security\cluster.encryption.keystore**) de todos los servidores del clúster por este nuevo.

7. Reinicie los servidores.

Solución de problemas

Cada vez que se inicia el servidor, el servidor envía un mensaje de prueba al clúster para verificar si está conectado correctamente al clúster. Si hay un problema con la conexión, la transmisión del mensaje no se completa y el servidor se detiene para impedir que se atasque la totalidad del clúster.

Algunos ejemplos de configuración incorrecta de cifrado de clúster son:

- El cifrado está deshabilitado en un nodo cuando otro nodo lo habilitó.
- cluster.encryption.keystore falta o es incorrecto.
- Falta clave en el almacén de claves o es incorrecta.

Si el servidor se bloquea debido a un problema de configuración, el mensaje de error será:

```
2012-09-11 17:48:23,584 [Thread-14] FATAL - #### El servidor no pudo conectarse correctamente al clúster y se detuvo el servicio. Solucione el problema e inícielo nuevamente ####

2012-09-11 17:48:23,586 [Thread-14] FATAL -       Los problemas potenciales pueden ser: configuración de seguridad errónea (falta cluster.encryption.keystore o es incorrecta, la clave es incorrecta, o hay un cifrado deshabilitado en un clúster con cifrado habilitado)
```

Cambio de la clave en key.bin

En un entorno de alta disponibilidad con varios servidores, cambie la **clave** de **key.bin** como se indica a continuación:

1. Vaya al equipo escritor en la consola JMX. Puede elegir cualquier equipo del clúster y hacer clic en el vínculo **writer** en la parte superior de cada página.

2. En la sección UCMDB de la consola, haga clic en **UCMDB:service=Discovery Manager**.

3. Cambie la clave de una de las siguientes formas:

- Haga clic en **changeEncryptionKey** (esto importa la clave de cifrado existente)
- Haga clic en **Generateencryptionkey** (esto genera una clave de cifrado aleatorio)

4. En el equipo escritor, vaya al sistema de archivo y busque **key.bin** en: **C:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**

5. Copie **key.bin** desde la ubicación del equipo escritor en cada uno de los demás equipos del clúster en la carpeta: **C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_1** y cambie el nombre del archivo de destino (por ejemplo, **key_new.bin**).

6. En cada uno de los demás servidores (lectores), haga lo siguiente:

   a. Cambie el lector a escritor (puede hacerlo desde la consola JMX de alta disponibilidad) y espere a que el cambio se efectúe.

   b. Conéctese a la consola JMX del escritor actual y haga clic en **UCMDB:service=Discovery Manager**.

   c. Haga clic e invoque **changeEncryptionKey**, utilice los mismos detalles que haya introducido en el paso 3 (en **newKeyFileName**, utilice el nuevo nombre asignado en el paso 5).

   d. Compruebe que aparezca el siguiente mensaje: **Key was created successfully**.

Agradecemos sus comentarios.

Si desea hacer algún comentario sobre este documento, puede ponerse en contacto con el equipo de documentación por correo electrónico. Si en este sistema está configurado un cliente de correo electrónico, haga clic en el vínculo anterior para abrir una ventana de correo electrónico con la información siguiente en la línea del asunto:

Comentarios sobre Guía del sistema de protección (Universal CMDB y Configuration Manager 10.10)

Solo añada sus comentarios al correo electrónico y haga clic en Enviar.

Si no hay disponible ningún cliente de correo electrónico, copie la información anterior en un nuevo mensaje de un cliente de correo web y envíe sus comentarios a sw-doc@hp.com.