Hewlett Packard Enterprise

Operations Orchestration

Versión de software: 10.60
Sistemas operativos Windows y Linux

Guía de seguridad y protección

Fecha de publicación del documento: Mayo de 2016

Fecha de lanzamiento del software: Mayo de 2016

Avisos legales

Garantía

Las únicas garantías de los productos y servicios Hewlett Packard Enterprise se exponen en el certificado de garantía que acompaña a dichos productos y servicios. El presente documento no debe interpretarse como una garantía adicional. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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 en los EE.UU. de Microsoft Corporation.

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

Este producto incluye una interfaz de la biblioteca de compresión de uso general 'zlib' con Copyright © 1995-2002 Jean-loup Gailly y Mark Adler.

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: https://softwaresupport.hp.com/.

Este sitio requiere que se registre para obtener un HP Passport y que inicie sesión. Para registrarse y obtener un Id. de HP Passport, haga clic en **Register** en el sitio HP Software Support o haga clic en **Create account** en 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 HPE para obtener más información.

Contenido

Introducción

Bienvenido a la Guía de seguridad y protección de HPE OO.

Esta guía está diseñada para servir de ayuda a los profesionales de TI que despliegan y gestionan instancias de HPE Operations Orchestration (HPE OO) de un modo seguro. Nuestro objetivo es ayudarle a que tome unas decisiones fundadas sobre las distintas capacidades y funciones que HPE OO proporciona para satisfacer las necesidades de seguridad empresariales actuales.

Los requisitos de seguridad empresariales están en continua evolución y esta guía debe considerarse como un esfuerzo de HPE por satisfacer estos rigurosos requisitos. Si existen necesidades de seguridad adicionales que no se tratan en esta guía, abra una incidencia de soporte con el equipo de soporte técnico de HPE para documentarlas y las incluiremos en futuras ediciones de esta guía.

Panorama técnico del sistema

HPE OO es una aplicación a nivel de empresa basada en la tecnología Java 2 Enterprise Edition (J2EE). La tecnología J2EE proporciona un enfoque basado en componentes sobre el diseño, desarrollo, ensamblado y despliegue de aplicaciones empresariales.

Actualizaciones de seguridad

Entre OO 10.20 y 10.50, se han realizado las siguientes actualizaciones de seguridad:

- Cuando la casilla **Habilitar captura de credenciales de usuarios que han iniciado sesión** está seleccionada en Central, HPE OO capturará de forma temporal (de un modo seguro) las credenciales del usuario que ha iniciado sesión cuando este usuario ejecute flujos en el depurador remoto. Un mensaje advierte que se pueden capturar las credenciales.
- En HPE OO 10.5x, la opción predeterminada es que no hay un rol predeterminado. Esto proporciona al administrador un mayor control de la autorización de usuario porque los usuarios solo obtienen roles que están expresamente asignados a ellos o a su grupo LDAP.
- Cuando HPE OO tiene varias configuraciones LDAP, si el administrador marca una de ellas como la predeterminada, los usuarios que forman parte de ella no necesitarán seleccionar un dominio tras iniciar sesión.
- HPE OO 10.5x protege la información confidencial (por ejemplo, las contraseñas) durante la ejecución. Si una variable está marcada como confidencial en Studio, se recuperará en formato cifrado cuando se utilice en scriptlets.

Entre HPE OO 10.10 y 10.20, se han realizado las siguientes actualizaciones de seguridad:

- Ya es posible conceder permisos para cuentas del sistema en HPE OO. Esto permite al administrador controlar qué usuarios pueden ver las cuentas del sistema y ejecutar flujos que las utilizan. Esta función es útil para clientes que tengan varias organizaciones y deseen ocultar algunas cuentas del sistema de determinados usuarios.

  Para obtener más información, consulte "Content Management Enhancements - Apply Permissions to Multiple Roles" en *OO 10.20 Release Notes*.

- Ya es posible aplicar permisos a varios roles en el cuadro de diálogo Editar permisos. En versiones anteriores, solo era posible seleccionar un rol a la vez.

  Para obtener más información, consulte "Content Management Enhancements - Permissions for System Accounts" en *OO 10.20 Release Notes*.

- Cuando se actualiza una instalación de OO a partir de una versión 10.x anterior, se actualiza el almacén de confianza SSL para que incluya los certificados raíz de confianza actualizados tal como los publicó Oracle. Ello incluye la eliminación de certificados caducados y la importación de otros nuevos.

  Para obtener más información, consulte "Installation Enhancements - Updated Trusted Root Certificates" en *OO 10.20 Release Notes*.

- OO ofrece ahora la posibilidad de auditar eventos de modo que puede realizar el seguimiento de las infracciones de seguridad. La auditoría permite hacer seguimiento de acciones que han tenido lugar en Central, como por ejemplo inicios de sesión, desencadenamiento de flujos, creación de programaciones y edición de configuraciones.

  Actualmente, puede recuperar la traza de auditoría solo mediante las API. Para obtener más información, consulte la *Guía de API de OO*.

- OO admite ahora claves de cifrado que tengan 2048 bits (y más). Esto adapta nuestras claves de criptografía al estándar FIPS 186-4.

- Se ha añadido una nueva propiedad sslEnabledProtocols al archivo **server.xml** (que se encuentra en **<carpeta_instalación>/central/tomcat/conf/server.xml**):

  ```
  sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
  ```

  Esta propiedad garantiza que solo v1, TLS v1.1 y TLS v1.2 están permitidos, y que SSL 3.0 no lo está. Esto impide vulnerabilidades a ataques “POODLE” (Padding Oracle On Downgraded Legacy Encryption).

Documentos relacionados

Para obtener más información sobre seguridad y protección de OO, consulte los siguientes documentos:

- *OO Network Architecture White Paper*

Para obtener más información sobre OO, consulte los siguientes documentos:

- *Guía de conceptos de OO*
- *OO Administrator Guide*
- *Guía de arquitectura de OO*
- *Guía de bases de datos de OO*
- *Guía del usuario de Central de OO*
- *Guía de creación de Studio de OO*
- *OO Release Notes*
- *Guía de instalación, actualización y configuración de OO*
- *Requisitos del sistema de OO*
- *OO Studio Wizards User Guide*

Se pueden encontrar estos y otros documentos en HPE Live Network (https://hpln.hp.com/node/21/otherfiles#).

Información general de seguridad

Esta sección proporciona información general sobre los modelos y recomendaciones de seguridad para una implementación segura de HPE OO. Esto incluye cuestiones como autenticación, autorización, cifrado, etc. Si es necesario, hay referencias a otros documentos de HPE OO, que describen cómo completar tareas relativas a la seguridad.

Conceptos sobre seguridad

Glosario de HPE OO

Para obtener más información sobre los conceptos de HPEP OO, consulte la *Guía de conceptos de HPE OO*.

Permiso de rol

Un permiso es una autorización predefinida para llevar a cabo una tarea. HPE OO Central incluye una serie de permisos que se pueden asignar a roles.

Por ejemplo, con el permiso de **Programación** es posible ver y crear programaciones de ejecución.

Rol

Un rol es una recopilación de permisos.

Por ejemplo, al rol **Administrador de flujos** se le puede asignar el permiso **Ver programaciones** y **Gestionar programaciones**.

Usuario

Un usuario es un objeto asociado a una persona (o identidad de aplicación) que representa a la persona y define su autorización.

Los roles se asignan a los usuarios para definir las acciones que pueden llevar a cabo en Central. Por ejemplo, al usuario Joe Smith se le puede asignar el rol **Administrador de flujos**.

Se pueden configurar diversos tipos de usuarios:

- Los **usuarios LDAP** inician sesión en Central con su nombre de usuario y contraseña LDAP. Por ejemplo, utilizando el nombre de usuario y la contraseña de Active Directory.
- Los **usuarios internos** inician sesión en Central utilizando el nombre de usuario y la contraseña que se han configurado localmente en Central.
- **LWSSO** - HPE Lightweight Single Sign On (SSO) es un mecanismo en el que una única acción de autenticación de usuario y autorización puede permitir que un usuario acceda a todos los sistemas de HPE que admiten LWSSO. Por ejemplo, si los usuarios han iniciado sesión en otro cliente web de producto HPE con LWSSO habilitado, pueden entrar directamente en la aplicación HPE OO Central, omitiendo la pantalla de inicio de sesión de HPE OO Central.

Cuando un usuario interno y un usuario LDAP con el mismo rol inician sesión, no hay diferencias entre sus permisos.

Nota: Se recomienda utilizar usuarios LDAP en lugar de usuarios internos porque los usuarios LDAP son seguros según las directivas desplegadas por el proveedor LDAP.

Permiso Contenido

El permiso Contenido es el permiso para ver o ejecutar flujos individuales o flujos de una carpeta en particular.

Los usuarios a los que se les ha asignado un rol específico podrán acceder a los flujos según los permisos de contenido asignados a su rol.

Por ejemplo, los usuarios con el rol **Administrador** pueden tener derecho a ver y ejecutar todos los flujos del sistema, mientras que los usuarios con el rol **Usuario** pueden tener derecho a ejecutar determinados flujos y tener permiso para visualizar otros.

Conceptos comunes sobre seguridad

Seguridad del sistema

Los procesos y mecanismos mediante los cuales se protege a equipos basados en ordenador, información y servicios frente a accesos no deseados o no autorizados, cambios o daños.

Privilegio mínimo

Práctica que consiste en limitar el acceso al nivel mínimo que permite el funcionamiento normal. Es decir, consiste en conceder a una cuenta de usuario únicamente aquellos privilegios que sean esenciales para el trabajo del usuario en cuestión.

Autenticación

Proceso de identificación de un individuo, normalmente basado en un nombre de usuario y contraseña o en un certificado.

Autorización

Permiso para acceder a los objetos del sistema, basado en la identidad de un individuo.

Cifrado

Método para mejorar la seguridad de un mensaje o archivo mediante la codificación del contenido de modo que solo pueda ser leído por aquel que disponga de la clave de cifrado correcta para descodificarlo. Por ejemplo, el protocolo TLS cifra los datos de comunicación.

Contramedida

Método para minimizar el riesgo de una amenaza.

Defensa en profundidad

Capas protectoras para no depender únicamente de una sola medida de seguridad.

Riesgo

Un suceso potencialmente peligroso. Por ejemplo, un suceso que podría causar pérdidas económicas, dañar la imagen de la empresa, etc.

Amenaza

Activación de un suceso de riesgo que explota una vulnerabilidad.

Vulnerabilidad

Debilidad de un objetivo que podría ser explotado por una amenaza de seguridad.

Implementación y despliegue seguros

Configuración de seguridad predeterminada

En muchos casos, se recomienda modificar la configuración de seguridad predeterminada, que se proporciona lista para usar.

- **Autenticación**: de forma predeterminada, la autenticación no está habilitada en Central. Se recomienda habilitarla en cuanto se hayan configurado los usuarios. Para obtener información, consulte "Habilitación de la autenticación" en la *Guía del usuario de Central de HPE OO*.
- **Auditoría**: de forma predeterminada, la auditoría no está habilitada en Central. Se recomienda habilitarla. Para obtener información, consulte "Habilitación de la auditoría" en la *Guía del usuario de Central de HPE OO*.
- **Cifrado TLS**: de forma predeterminada, HPE OO admite tres protocolos TLS: 1.0, 1.1, 1.2. Se recomienda trabajar con la última versión. Para obtener más información, consulte "Configuración del protocolo TLS" en la página 66.
- **Certificado de servidor TLS**: de forma predeterminada, se solicita al usuario que proporcione un certificado de CA durante la instalación del servidor de OO.
- **Certificado de cliente**: de forma predeterminada, el certificado de cliente no está habilitado. Se recomienda trabajar con el certificado de cliente para autenticarse en Central. Para obtener más información, consulte "Configuración de la autenticación del certificado de cliente en Central" en la página 51.
- **Contraseñas del almacén de claves, del almacén de confianza y del certificado del servidor**: de forma predeterminada, se proporcionan contraseñas Java para el almacén de claves, el almacén de confianza y el certificado del servidor. Se recomienda reemplazarlos por contraseñas cifradas. Para obtener más información, consulte "Cambio y cifrado/ocultación de la contraseña del almacén de claves/almacén de confianza" en la página 44.
- **Cifrado RC4**: de forma predeterminada, el cifrado RC4 está habilitado. Se recomienda deshabilitar el cifrado RC4 en el nivel JRE. Para obtener más información, consulte "Supresión del cifrado RC4 de los cifrados admitidos por SSL" en la página 48.
- **Banner de seguridad**: de forma predeterminada, el banner de seguridad no está habilitado en Central. Se recomienda habilitarlo con un mensaje personalizado. Para obtener información, consulte "Configuración de un banner de seguridad" en la *Guía del usuario de Central de HPE OO*.

- **Autenticación Windows de la base de datos**: de forma predeterminada, la autenticación Windows no está habilitada en Central. Si trabaja con entornos Windows y SQL Server, se recomienda configurar HPE OO para que funcione con autenticación Windows. Consulte "Configuración de HPE OO para que funcione con autenticación Windows" en la *Guía de base de datos de HPE OO*.
- **Algoritmos predeterminados**: el archivo **encryption.properties** contiene los algoritmos predeterminados. Si desea cumplir con FIPS, consulte "Configuración de HPE OO para compatibilidad con FIPS 140-2 Nivel 1" en la página 59. Para ver más información sobre los valores predeterminados de FIPS 140-2 Nivel 1, consulte "Administración de cifrado" en "Cifrado" en la página 23.
- **Directiva de Java**: de forma predeterminada, el archivo **java.policy** no está protegido. Para obtener más información sobre cómo modificar el archivo **java.policy**, consulte "Cómo evitar que los flujos accedan al sistema de archivos local de Central/RAS" en la página 67.

Protección de seguridad de HPE OO

El capítulo Protección proporciona recomendaciones para salvaguardar el despliegue de HPE OO de riesgos o amenazas para la seguridad. Entre los motivos más importantes para proteger una aplicación se encuentra la protección de confidencialidad, integridad y disponibilidad de la información crítica de una organización.

Para proteger en su conjunto el sistema de HPE OO, es necesario proteger tanto HPE OO como el entorno informático (por ejemplo, la infraestructura y el sistema operativo) en los que se ejecuta la aplicación.

El capítulo Protección proporciona recomendaciones que contribuyen a proteger HPE OO a nivel de aplicación y excluye los métodos para la protección de la infraestructura en el entorno del cliente. El cliente es el único responsable de familiarizarse con su infraestructura/entorno y aplicar las directivas de protección correspondientes.

Seguridad física

HP Software recomienda que HPE OO esté protegido mediante controles de seguridad física definidos por su organización. Los componentes del servidor HPE OO se instalan en un entorno físico protegido, de acuerdo con los procedimientos recomendados. Por ejemplo, el servidor debe estar en una sala cerrada con control de acceso.

Directrices para una instalación segura

Sistemas operativos compatibles

Para obtener información sobre los tipos y versiones de sistemas operativos compatibles, consulte *Requisitos del sistema de HPE OO*.

Recomendaciones de protección para sistemas operativos

Póngase en contacto con el proveedor de su sistema operativo para conocer los procedimientos recomendados para proteger su sistema operativo.

Por ejemplo:

- Es necesario instalar parches
- Es necesario quitar o inhabilitar los servicios o el software innecesarios
- Es necesario asignar permisos mínimos a los usuarios
- Es necesario habilitar la auditoría

Protección de Tomcat

Cuando se instala HPE OO Central, Tomcat está parcialmente protegido de forma predeterminada. Si desea protección adicional, consulte las recomendaciones del capítulo Protección

Permisos de instalación

Los siguientes permisos son necesarios para instalar y ejecutar HPE OO:

Instalación de HPE OO	Windows/Linux: Todos los usuarios estándar que puedan ejecutar un proceso Java y que tengan permisos para crear carpetas y servicios
Ejecución de HPE OO	• Windows: El servicio Windows se ejecuta como usuario del sistema o como un usuario específico (el usuario debe tener acceso al directorio de instalación de HPE OO) • Linux: Todos los usuarios estándar que puedan ejecutar un proceso Java

Consulte también las recomendaciones del documento CIS Apache Tomcat 7.0.

Seguridad de red y comunicación

La *Guía de arquitectura de HPE OO* describe la topología básica de OO, la alta disponibilidad y la seguridad del equilibrador de carga.

El documento *HPE OO Network Architecture White Paper* describe la configuración de cortafuegos necesaria y sugiere dos soluciones alternativas que se pueden aplicar en los casos en que, a causa de restricciones de política, no se puede implementar la configuración de cortafuegos necesaria:

- Tunelización inversa SSH
- Proxy inverso

Seguridad de canal de comunicación

Protocolos y configuración admitidos

HPE OO admite el protocolo TLS.

Para obtener más información, consulte "Sustitución del certificado de servidor TLS de Central" en la página 38.

El administrador define los puertos de Central durante la instalación.

Seguridad de canal

HPE OO admite los siguientes canales seguros:

Canal (directo)	Protocolo seguro admitido
OOSH, explorador, depurador remoto de Studio o RAS → Central	Para un canal seguro, utilice la comunicación TLS para el cifrado y el certificado cliente de la autenticación.
Servidor de Central → LDAP	Para cifrar la comunicación entre Central y LDAP, utilice LDAP seguro con protocolo TLS.

Seguridad de RAS

En una topología con RAS inverso (que espera a que Central inicie la conexión), el siguiente mecanismo protege la seguridad del RAS:

- Si hay varios intentos de conexión consecutivos fallidos (porque se ha indicado un secreto compartido incorrecto), se producirá un retraso.

Para obtener más información sobre RAS inversos, consulte "Configuración de topología: Componentes y RAS" en la *Guía del usuario de Central de HPE OO*.

Seguridad de interfaz de administración

Acceso a la interfaz de administración

Existen varias formas de controlar el acceso a la interfaz de administración:

- Credenciales
- Certificación de cliente
- SAML

Cómo proteger la interfaz de administración: Recomendaciones

1. Se recomienda habilitar la autenticación en Central.

   Consulte "Habilitación de la autenticación" en la *Guía del usuario de HPE OO Central*

2. Se recomienda proteger la interfaz de administración con el protocolo TLS. Se debe configurar TLS entre el cliente y la interfaz de Central para el cifrado.

   Consulte "Trabajo con certificados de servidor y de cliente" en la página 37.

3. Se recomienda trabajar con usuarios LDAP, en lugar de con usuarios internos, por motivos de seguridad.

4. Se recomienda configurar la autenticación para acceder a Central a través de certificados cliente. Este método es más seguro que las contraseñas de usuario.

   Consulte "Trabajo con certificados de servidor y de cliente" en la página 37.

Gestión y autenticación de usuarios

Modelo de autenticación

Para permitir un arranque fácil del mecanismo de autenticación en HPE OO, el producto se inicia con la autenticación deshabilitada.

Se recomienda especialmente habilitar la autenticación justo después de la instalación.

Para obtener información sobre cómo habilitar la autenticación, consulte "Habilitación de la autenticación" en la *Guía del usuario de Central de HPE OO*.

Existen varias formas de autenticar el acceso a Central.

Elija el método de identificación de usuarios:

- Nombre del usuario y contraseña
- Certificación de cliente
- Token SAML
- Inicio de sesión único (HPE LWSSO)

Seleccione una de las dos formas de gestionar usuarios:

- Usuarios LDAP, guardados en un servidor LDAP como Active Directory (recomendado)
- Usuarios internos y contraseñas, guardados localmente en el servidor de Central (no recomendado)

Tipos de usuario

Distintos tipos de usuarios pueden tener permisos diferentes asignados a ellos. Por ejemplo, autor de flujo, administrador, administrador del sistema, etc.

Para ver más ejemplos de distintos tipos de usuario, que requieren permisos diferentes, consulte "Roles principales" en la *Guía de conceptos de OO*.

Administración y configuración de autenticación

Usuarios internos o LDAP

Puede configurar usuarios internos con contraseñas en la interfaz de usuario de Central o definir el usuario en el servidor LDAP y asignar grupos LDAP a roles de Central.

Nota: Se recomienda no utilizar usuarios internos sino una alternativa más segura como usuarios LDAP.

Para obtener información sobre cómo configurar usuarios internos, consulte "Configuración de seguridad: Usuarios internos" en la *Guía del usuario de Central de OO*.

Para obtener información sobre cómo asignar grupos LDAP a roles de Central, consulte "Configuración de seguridad: Autenticación LDAP" en la *Guía del usuario de Central de OO* y "LDAP Configuration" en *OO API Guide*.

SAML / Certificados de cliente / LW SSO

Para obtener información sobre cómo configurar Central para que funcione con SAML, consulte "Configuración de seguridad: SAML" en la *Guía del usuario de Central de OO*.

Para obtener información sobre cómo configurar Central para que funcione con certificados de cliente, consulte "Trabajo con certificados de servidor y de cliente" en la página 37.

Para obtener información sobre cómo configurar Central para que funcione con LW SSO, consulte "Configuración de seguridad: LWSSO" en la *Guía del usuario de Central de OO*, "Configuring LWSSO Settings" en *OO Administration Guide* y "LW SSO" en *OO API Guide*.

Autenticación de base de datos

OO admite cuatro bases de datos: Oracle, MS SQL, MySQL y Postgres.

Se recomienda utilizar una contraseña de base de datos compleja para autenticación de base de datos y una directiva de contraseñas complejas. Por ejemplo, el bloqueo después de un número determinado de intentos fallidos.

Al utilizar MS SQL, es posible trabajar con autenticación de base de datos o autenticación OS. Se recomienda trabajar con autenticación OS siempre que sea posible. Por ejemplo, es posible utilizar autenticación Windows para acceder a las bases de datos de Microsoft SQL Server.

- Para obtener información sobre cómo configurar la autenticación OS, consulte "Configuración de OO para que funcione con autenticación Windows" en la *Guía de bases de datos de HPE OO*.
- Consulte "Changing the Database Password" en *HPE OO Administration Guide*.
- Consulte los procedimientos recomendados por el proveedor de la base de datos (si los hay).

Autorización

Modelo de autorización

El acceso de usuario a los recursos de HPE OO se autoriza según el rol del usuario y los permisos configurados para el rol en cuestión.

Consulte:

- "Configuración de seguridad: roles" en la *Guía del usuario de HPE OO Central*
- "Asignación de permisos a una cuenta del sistema" en la *Guía del usuario de HPE OO Central*

Directrices para permisos mínimos

Se recomienda para:

- Seleccionar permisos adecuados para el rol.
- Utilizar permisos mínimos al crear nuevos roles.
- Conceder permisos mínimos y ampliar los permisos solo si es necesario para evitar una escalada de privilegios no deseada. Por ejemplo, empiece por permisos de visualizador y añada permisos adicionales de forma individual según convenga.

Configuración de autorizaciones

Central se instala con determinado roles predefinidos, que se pueden configurar y asignar a los usuarios. De forma predeterminada, los roles predefinidas tienen asignados los siguientes permisos:

Rol	Permisos predeterminados
Administrador	Todos
Usuario final	Ninguno
Todos los usuarios	Ninguno
Promotor	Todos los permisos de **Contenido**
Administrador del sistema	Todos los permisos de **Sistema**

Rol predeterminado

Es posible configurar uno de los roles con el atributo **Rol predeterminado**. Si lo hace, asegúrese de que este sea el rol con privilegios mínimos. Recuerde que, cuando se dan permisos a este rol, se ven afectados todos los usuarios LDAP, además de los que están explícitamente asociados con el rol.

Para obtener más información, consulte "Asignación de un rol para que sea el rol predeterminado" incluido en "Configuración de seguridad: roles" en la *Guía del usuario de HPE OO Central*.

Véase también:

- "Asignación de permisos a una cuenta del sistema" en la *Guía del usuario de HPE OO Central*
- "Configuración de permisos de contenido" en la *Guía del usuario de HPE OO Central*

Acceso a las áreas de trabajo en Studio

Al crear varias áreas de trabajo en Studio, se recomienda crear un área de trabajo en las carpetas en las que solo el usuario que las vaya a crear tenga permisos de lectura y escritura.

Las áreas de trabajo creadas en carpetas públicas pueden ser accesibles a todos los usuarios, lo que las predispone a la alteración y revelación de información confidencial.

Copia de seguridad

Para evitar la pérdida de datos, es sumamente recomendable realizar con frecuencia copias de seguridad en soportes seguros de los datos guardados en los servidores. Esto resulta de especial utilidad en situaciones de recuperación tras desastre y garantiza la continuidad empresarial.

Después de haber instalado OO, asegúrese de realizar una copia de seguridad de la carpeta **central\var\security** y del archivo **central\conf\database.properties**.

Ciertos datos del esquema de base de datos están cifrados y las claves para descifrarlos están almacenados localmente en el servidor de OO Central. Si se dañan o se eliminan estos archivos del sistema, el esquema quedará inutilizado porque no se podrán descifrar los datos.

Nota: Las claves están cifradas y, por lo tanto, es importante incluirlas en la copia de seguridad. Las claves están en la carpeta **security**.

Consulte:

- "Backing Up OO" en *HP OO Administration Guide*
- "Setting up Disaster Recovery" en *OO Administration Guide*
- "Copia de seguridad y recuperación de archivos de seguridad de Central" en la *Guía de instalación de OO*
- "Uso del Equilibrador de carga en despliegues OO" en la *Guía de arquitectura de OO*

Cifrado

Modelo de cifrado

HPE OO admite el cifrado y los algoritmos hash para proteger la información confidencial. El cifrado está diseñado para impedir la exposición y modificación de información confidencial, como contraseñas, definiciones, etc., en el sistema HPE OO.

Es importante utilizar algoritmos estándar conocidos, sin vulnerabilidades conocidas, para impedir el descifrado por parte de personas no autorizadas.

Nota: Por ejemplo, SSL no se utiliza debido a vulnerabilidades conocidas en el protocolo SSL.

Datos estáticos

Todas las contraseñas están protegidas mediante algoritmos conocidos y ninguna se deja como texto no cifrado.

Por ejemplo:

- Las contraseñas de las cuentas del sistema están cifradas.
- Las contraseñas de usuarios internos están con hash.
- Las contraseñas de bases de datos están cifradas.

Datos en tránsito

OO utiliza el protocolo Seguridad de la capa de transporte (Transport Layer Security, TLS) para cifrar los datos entre componentes (como Central y RAS).

Deshabilitación del puerto HTTP

Se recomienda deshabilitar el puerto HTTP, por motivos de seguridad, para que el único canal de comunicación esté en TLS y cifrado. Para obtener más información, consulte "Cambio de los puertos HTTP/HTTPS o deshabilitación del puerto HTTP" en la página 49.

Administración de cifrado

Procedimientos recomendados de cifrado

Para alcanzar altos niveles de seguridad y criptografía, se recomienda configurar OO para que sea conforme a los estándares federales de procesamiento de la información (Federal Information

Processing Standards, FIPS) 140-2. OO se puede configurar para que sea conforme a FIPS 140-2 Nivel 1.

Conjunto de configuración predeterminada

- Algoritmo de claves simétricas: AES con tamaño de clave 128
- Algoritmo hash: SHA1

Configuración avanzada

Después de configurar OO para su conformidad con FIPS 140-2, OO utiliza el siguiente algoritmo de seguridad:

- Algoritmo de claves simétricas: AES256
- Algoritmo hash: SHA256

Consulte "Configuración de HPE OO para que sea compatible con FIPS 140-2" en la página 62.

Certificados digitales

Un certificado digital es un "pasaporte" electrónico para una persona, servidor, estación, etc.

- Para utilizar el cifrado entre un explorador y el servidor de Central, debe instalar un certificado digital en el lado del servidor.
- Para utilizar el certificado de cliente a fin de autenticar el servidor de Central, debe instalar un certificado de cliente en el lado de cliente (por ejemplo, en el explorador, RAS, OOSH, Studio, etc.).

OO usa la utilidad Java Keytool para gestionar claves criptográficas y certificados de confianza. Esta utilidad está incluida en la carpeta de instalación de OO, en **<dir instalación>/java/bin/keytool**.

Ubicación de certificados

Las instalaciones de OO Central incluyen dos archivos para la gestión de certificados mediante Keytool:

- **<dir instalación>/central/var/security/client.truststore**: Contiene la lista de certificados de confianza
- **<dir instalación>/central/var/security/key.store**: Contiene el certificado privado de OO (incluida la clave privada)

Control de acceso al almacén de claves y al almacén de confianza

Se recomienda que el almacén de confianza y el almacén de claves se almacenen con permisos de lectura solo para el usuario que ejecuta el servicio de Central.

Reemplazo del certificado autofirmado de OO

Se recomienda reemplazar el certificado autofirmado de OO después de una nueva instalación de OO o si su certificado actual ha caducado.

Una parte del proceso de reemplazo del certificado genera un certificado de formato PKCS12, con la entidad de certificación (CA). Póngase en contacto con su CA para obtener información detallada específica sobre el proceso de certificación o consulte la directiva corporativa.

Para obtener más información, consulte "Sustitución del certificado de servidor TLS de Central" en la página 38.

Adición de firmas digitales a un paquete de contenido

Un paquete de contenido con una firma digital de una CA de confianza es una garantía de que el contenido es de confianza.

No es obligatorio añadir una firma digital.

- Los paquetes de contenido de OO listos para usar contienen una firma digital de Verisign.
- Se recomienda a los autores de OO añadir una firma digital a sus paquetes de contenido personalizados.
- Si se vulnera un paquete de contenido firmado, no se puede desplegar.
- Si la firma caduca, aparece una advertencia antes del despliegue y el usuario debe seleccionar una casilla en la que confirma que ignora la firma caducada.

Preste atención a los paquetes de contenido no firmados. Un paquete de contenido no firmado no es de confianza y puede incluir contenido malintencionado. Tenga en cuenta igualmente que un paquete de contenido no firmado es vulnerable y se puede quitar la firma.

Para obtener más información sobre la certificación digital de paquetes de contenido, consulte "Despliegue y gestión de paquetes de contenido" en la *Guía del usuario de Central de OO*.

Información confidencial en un paquete de contenido

Contraseñas de cuentas del sistema

No incluya contraseñas al crear un paquete de contenido. Las contraseñas se ocultarán dentro del paquete de contenido, lo que no es una opción segura.

El procedimiento recomendado de seguridad de OO es configurar las contraseñas de cuentas del sistema en Central. Para obtener más información, consulte "Configuración de cuentas del sistema para un paquete de contenido" en la *Guía del usuario de Central de OO*.

Auditoría y archivos de registro

Auditoría

La auditoría permite realizar un seguimiento de las acciones que tienen lugar en el servidor de Central, como inicios de sesión, activación de flujos, creación de programaciones, edición de configuraciones, etc. Los datos de auditoría permiten realizar un seguimiento de la actividad de los usuarios en el sistema de Central, rastreando quién llevó a cabo una acción determinada y cuándo. Por ejemplo, una auditoría mostraría que un usuario ejecutó un flujo, actualizó una configuración, eliminó una programación o falló una autenticación.

Los datos de auditoría se guardan en la base de datos. Para obtener más información, consulte "Auditing" en *HPE OO API Guide*.

Registros

Los registros permiten realizar un seguimiento de los errores, advertencias, mensajes informativos y mensajes de depuración.

Los registros se guardan en el servidor de archivos, en las ubicaciones siguientes:

- Central: **<instalación-oo>/central/var/logs**
- Studio: **<usuario>/.oo/logs**
- RAS: **<instalación-oo>/ras/var/logs**.

No se guarda información confidencial en los registros de auditoría ni en los archivos de registro

No se conserva información confidencial en los registros de auditoría ni en los archivos de registro en el sistema HPE OO.

Cómo obtener los registros de auditoría

Los registros de auditoría se pueden obtener a través de la API o mediante una consulta a la tabla OO_AUDIT. Para obtener más información, consulte "Auditing" en *HPE OO API Guide*.

Ejemplo de datos de auditoría:

```
[
{
“time”:1412312016740, “type”:”AuditConfigurationChange”,
“group”:”AuditManagement”, “subject”:” mydomain\myuser2”, “outcome”:”Success”,
“data”:”{"enabled":false}”
},
{
“time”:1412312016722, “type”:”InternalUserDelete”, “group”:”Authentication-
Authorization”, “subject”:”mydomain\myuser2”, “outcome”:”Success”, “data”:
{"usersNames":["admin"]}"
}
]
```

API e interfaces

API y modelo de interfaz

Es posible trabajar con las interfaces de programación de aplicaciones (API) públicas de HPE Operations Orchestration en lugar de hacerlo con la interfaz de usuario de HPE OO Central para realizar las mismas acciones. Algunas acciones solo se pueden llevar a cabo mediante las API, como la depuración y la auditoría. La API pública está basada en HTTP. Todas las API son RESTful y utilizan la notación de objetos JavaScript.

Funciones y administración de la API y configuración de seguridad de la interfaz

Es importante trabajar con las API de forma segura. Utilice los mecanismos de seguridad mencionados en esta guía (autenticación, cifrado, etc.) mientras trabaja con las API.

La interfaz de la API funciona en HTTP o HTTPS.

Nota: Cuando utilice nuestras API para visualizar HTML, es su responsabilidad protegerlas de ataques XSS.

Para obtener más información, consulte los siguientes capítulos en *HPE OO API Guide*:

- "LDAP Configuration"
- "Users"
- "LW SSO Configuration"
- "Authentication"
- "Roles"

Preguntas y respuestas sobre seguridad

¿Cómo puedo generar una solicitud de certificado que puede firmar una entidad de certificación (CA) externa?

Exporte la solicitud de certificado y envíela a una CA externa para su firma. Para ver instrucciones, consulte "Sustitución del certificado de servidor TLS de Central" en la página 38.

¿Qué puertos TCP/UDP utiliza HPE OO? ¿Cuál es la dirección, el usuario y el cifrado?

Al instalar HPE OO, tiene que configurar al menos un puerto disponible para el servidor de Central en los campos HTTP/HTTPS. Los valores proporcionados de forma predeterminada son 8080 y 8443 pero se pueden cambiar. Para obtener información sobre canales seguros entre Central y los demás componentes, consulte "Seguridad de red y comunicación" en la página 15

¿Dónde y cómo se almacenan las credenciales (cuentas de administración, usuarios de integración)?

Consulte "Gestión y autenticación de usuarios" en la página 18.

¿Cómo puedo configurar certificados SSL autofirmados para Central/RAS/Studio?

Durante la instalación de HPE OO, si no proporciona un certificado, se crea un certificado autofirmado de forma predeterminada. No obstante, no se recomienda utilizar certificados autofirmados por motivos de seguridad. HPE recomienda trabajar con un certificado de una CA raíz personalizada o de una CA conocida.

Para obtener información sobre cómo configurar certificados para HPE OO, consulte "Cifrado de la comunicación mediante certificado de servidor" en la página 38.

¿Cómo puedo habilitar o deshabilitar cualquier tipo de auditoría?

De forma predeterminada, la auditoría no está habilitada. Para obtener información detallada sobre cómo habilitarla, consulte "Habilitación de la auditoría" en la Guía del usuario de Central de HPE OO. Para obtener más información sobre la auditoría, consulte "Auditoría y archivos de registro" en la página 28.

¿Qué nivel de detalle aparece en los registros y cómo puedo cambiar el volumen de registro?

Los registros se pueden establecer en distintos niveles de granularidad. El nivel predeterminado es INFO pero es posible ajustarlo. Para obtener información detallada, consulte "Adjusting the Logging Levels" en *HPE OO Administration Guide*.

Para obtener más información sobre los archivos de registro, consulte "Auditoría y archivos de registro" en la página 28.

¿Cómo se cifra la información confidencial?

Consulte "Cifrado" en la página 23.

¿Está cifrada la comunicación entre Central y RAS?

Si usa HTTPS, está cifrada.

¿Está cifrada la comunicación entre HPE OO y otros componentes de integración (HPNA, CSA, AD, etc.)?

Esto depende de la integración que esté utilizando. Si usa HTTPS, está cifrada.

¿Cómo puedo restringir el acceso a la Biblioteca de flujos en función de los roles de usuario?

Consulte "Configuración de seguridad: roles" en la *Guía del usuario de Central de HPE OO*

¿Qué mecanismo de autenticación admite OO?

Los mecanismos de autenticación admitidos son LDAP, SAML y usuarios internos. HPE OO admite igualmente el certificado de cliente y LWSSO. Consulte "Gestión y autenticación de usuarios" en la página 18.

¿Es HPE OO conforme a FIPS 140-2?

Sí. Para obtener más información, consulte "Configuración de HPE OO para que sea compatible con FIPS 140-2" en la página 62.

¿Cuáles son los métodos de autenticación entre Central y RAS?

Contraseña de usuario o certificado de cliente.

¿Están cifradas o con hash todas las contraseñas?

Sí. Todas las contraseñas están protegidas mediante algoritmos conocidos y ninguna se deja como texto no cifrado.

¿Puedo limitar la dirección IP de usuario de Central?

No, esto no está admitido por ahora.

¿Cuenta HPE OO con certificado para criterios comunes?

Está en curso. Por ahora, estamos "en evaluación". Para obtener información detallada, consulte https://www.cse-cst.gc.ca/en/canadian-common-criteria-scheme/publication/list/evaluation-product.

Cuando uso OOSH, ¿puedo pasar información confidencial a Central?

Se recomienda usar un canal seguro al conectarse a Central. Consulte "Seguridad de red y comunicación" en la página 15.

Protección de Operations Orchestration

En esta sección se describe cómo configurar la protección de seguridad para Operations Orchestration.

Nota: Para obtener información sobre otras tareas administrativas, consulte la *Guía de instalación, actualización y configuración de OO*.

Recomendaciones de seguridad sobre protección de sistemas

1. Instale la última versión de HPE OO. Para obtener más información, consulte la *Guía de instalación, actualización y configuración de OO*.
2. (Opcional) Configuración de OO para compatibilidad con FIPS 140-2. Si opta por realizar este paso, deberá configurarla antes de iniciar el servidor de Central. Consulte "Configuración de HPE OO para compatibilidad con FIPS 140-2 Nivel 1" en la página 59.
3. Configurar el certificado de servidor de Central para cifrado TLS y certificado de cliente para una autenticación más robusta (mutua).

   Nota: Esto se puede hacer durante la instalación.

   Para el RAS, depurador y OOSH, ofrezca autenticación de certificados si es necesario (para el certificado de servidor) y use el certificado de cliente para autenticación con Central. Consulte "Trabajo con certificados de servidor y de cliente" en la página 37.

4. Proteger el servidor de HPE OO Central eliminando el puerto HTTP y sustituyendo las contraseñas del almacén de claves y del almacén de confianza por contraseñas seguras. Consulte "Cambio de los puertos HTTP/HTTPS o deshabilitación del puerto HTTP" en la página 49 y "Cambio y cifrado/ocultación de la contraseña del almacén de claves/almacén de confianza" en la página 44.
5. Proteja HPE OO Studio reemplazando las contraseñas del almacén de claves y del almacén de confianza por contraseñas complejas, y cifrando u ocultando las contraseñas en los archivos de configuración. Consulte "Cambio y cifrado/ocultación de la contraseña del almacén de claves/almacén de confianza" en la página 44.
6. Eliminar el cifrado RC4 de los cifrados compatibles con SSL Consulte "Supresión del cifrado RC4 de los cifrados admitidos por SSL" en la página 48.
7. (Opcional) Configurar la versión del protocolo TLS. Consulte "Configuración del protocolo TLS" en la página 66.
8. Habilitar la autenticación en Central. Consulte "Habilitación de autenticación" en la *Guía del usuario de OO Central*.

   Los usuarios internos no están protegidos, así que le aconsejamos que use LDAP seguro con una directiva de contraseñas robusta. Consulte "Configuración de seguridad: Autenticación LDAP" en la *Guía del usuario de OO Central*.
9. Proteger/brindar seguridad al sistema operativo y base de datos.
10. Añadir un banner de seguridad con un mensaje descriptivo. Por ejemplo, "Ha iniciado sesión en nuestro entorno de PRODUCCIÓN. No continúe a menos que esté familiarizado con la normativa de este sistema y haya recibido la formación adecuada". Consulte "Configuración de topología: componentes" en *Guía del usuario de OO Central*.
11. En los entornos Windows y SQL server, configure OO para que funcione con autenticación Windows. Consulte "Configuración de OO para que funcione con autenticación Windows" en la *Guía de base de datos de OO*.
12. Asegúrese de que la función de auditoría esté habilitada en Central. Para obtener más información, consulte "Habilitar auditoría" en la *Guía del usuario de OO Central*.

Configuración de seguridad predeterminada

En muchos casos, se recomienda modificar la configuración de seguridad predeterminada, que se proporciona lista para usar.

- **Autenticación**: de forma predeterminada, la autenticación no está habilitada en Central. Se recomienda habilitarla en cuanto se hayan configurado los usuarios. Para obtener información, consulte "Habilitación de la autenticación" en la *Guía del usuario de Central de HPE OO*.
- **Auditoría**: de forma predeterminada, la auditoría no está habilitada en Central. Se recomienda habilitarla. Para obtener información, consulte "Habilitación de la auditoría" en la *Guía del usuario de Central de HPE OO*.
- **Cifrado TLS**: de forma predeterminada, HPE OO admite tres protocolos TLS: 1.0, 1.1, 1.2. Se recomienda trabajar con la última versión. Para obtener más información, consulte "Configuración del protocolo TLS" en la página 66.
- **Certificado de servidor TLS**: de forma predeterminada, se solicita al usuario que proporcione un certificado de CA durante la instalación del servidor de OO.
- **Certificado de cliente**: de forma predeterminada, el certificado de cliente no está habilitado. Se recomienda trabajar con el certificado de cliente para autenticarse en Central. Para obtener más información, consulte "Configuración de la autenticación del certificado de cliente en Central" en la página 51.
- **Contraseñas del almacén de claves, del almacén de confianza y del certificado del servidor**: de forma predeterminada, se proporcionan contraseñas Java para el almacén de claves, el almacén de confianza y el certificado del servidor. Se recomienda reemplazarlos por contraseñas cifradas. Para obtener más información, consulte "Cambio y cifrado/ocultación de la contraseña del almacén de claves/almacén de confianza" en la página 44.
- **Cifrado RC4**: de forma predeterminada, el cifrado RC4 está habilitado. Se recomienda deshabilitar el cifrado RC4 en el nivel JRE. Para obtener más información, consulte "Supresión del cifrado RC4 de los cifrados admitidos por SSL" en la página 48.
- **Banner de seguridad**: de forma predeterminada, el banner de seguridad no está habilitado en Central. Se recomienda habilitarlo con un mensaje personalizado. Para obtener información, consulte "Configuración de un banner de seguridad" en la *Guía del usuario de Central de HPE OO*.
- **Autenticación Windows de la base de datos**: de forma predeterminada, la autenticación Windows no está habilitada en Central. Si trabaja con entornos Windows y SQL Server, se recomienda configurar HPE OO para que funcione con autenticación Windows. Consulte "Configuración de HPE OO para que funcione con autenticación Windows" en la *Guía de base de datos de HPE OO*.
- **Algoritmos predeterminados**: el archivo **encryption.properties** contiene los algoritmos predeterminados. Si desea cumplir con FIPS, consulte "Configuración de HPE OO para compatibilidad con FIPS 140-2 Nivel 1" en la página 59. Para ver más información sobre los valores

predeterminados de FIPS 140-2 Nivel 1, consulte "Administración de cifrado" en "Cifrado" en la página 23.

- **Directiva de Java**: de forma predeterminada, el archivo **java.policy** no está protegido. Para obtener más información sobre cómo modificar el archivo **java.policy**, consulte "Cómo evitar que los flujos accedan al sistema de archivos local de Central/RAS" en la página 67.

Trabajo con certificados de servidor y de cliente

Los certificados Transport Layer Security (TLS) vinculan digitalmente una clave criptográfica a los detalles de una organización, lo cual permite conexiones seguras y cifradas de un servidor web a un explorador.

HPE OO usa la utilidad Keytool para gestionar claves criptográficas y certificados de confianza. Esta utilidad está incluida en la carpeta de instalación de HPE OO, en **<dir instalación>/central/var/security/client.truststore>/java/bin/keytool**. Para obtener más información sobre la utilidad Keytool, consulte http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html.

Nota: Keytool es una utilidad de código fuente.

Las instalaciones de HPE OO Central incluyen dos archivos para la gestión de certificados:

- **<dir instalación>/central/var/security/client.truststore**: Contiene la lista de certificados de confianza.
- **<dir instalación>/central/var/security/key.store**: Contiene el certificado HPE OO (clave privada).

Recomendaciones:

- Se recomienda reemplazar el certificado autofirmado de HPE OO después de una nueva instalación de HPE OO o si su certificado actual ha caducado.
- Se recomienda almacenar el almacén de confianza y el almacén de claves con permisos de lectura solo para el usuario que ejecuta el servicio de Central.
- Se recomienda borrar la consola después de utilizar Keytool o usar la solicitud para entradas de contraseñas.

Cifrado de la comunicación mediante certificado de servidor

Sustitución del certificado de servidor TLS de Central

Puede usar un certificado firmado por una autoridad de certificados reconocida o un certificado de servidor personalizado de una autoridad de certificados local.

Sustituya los parámetros resaltados en <amarillo> para hacer coincidir la ubicación del archivo **key.store** y otra información en su equipo.

> **Nota:** El siguiente procedimiento usa la utilidad Keytool ubicada en **<dir instalación>/java/bin/keytool**.

1. Detenga Central y realice una copia de seguridad del archivo **key.store** original, ubicado en **<dir instalación>/central/var/security/key.store**.
2. Abra una línea de comandos en **<dir instalación>/central/var/security**.
3. Elimine el certificado de servidor existente del archivo **key.store** de Central mediante el siguiente comando:

   ```
   keytool -delete -alias tomcat -keystore key.store -storepass changeit
   ```

4. Si ya dispone de un certificado con extensión **.pfx** o **.p12**, pase al paso siguiente. De no ser así, debe exportar el certificado con clave privada en formato PKCS12 (.pfx,.p12). Por ejemplo, si el formato del certificado es PEM:

```
>openssl pkcs12 –export –in <cert.pem> -inkey <.key> -out <nombre de certificado>.p12 –name <nombre>
```

Si el formato del certificado es DER, añada el parámetro `–inform DER` después de pkcs12. Por ejemplo:

```
>openssl pkcs12 –inform DER –export –in <cert.pem> -inkey <.key> -out <nombre de certificado>.p12 –name <nombre>
```

> **Nota:**
>
> Para generar el certificado de formato PKCS12, debe utilizar la entidad de certificación (CA). Como este paso puede variar en función del proveedor y la directiva de CA, debe obtener de la CA una explicación detallada del proceso de generación de certificados.

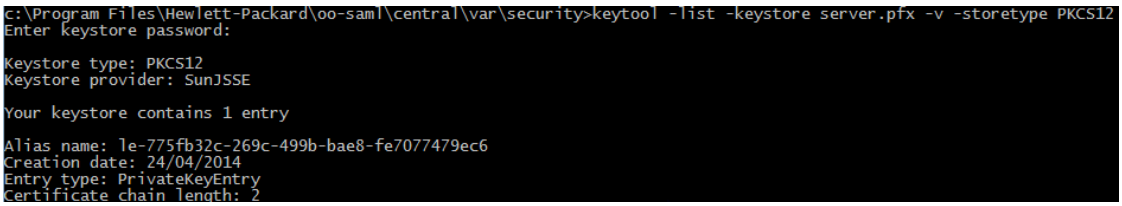
> **Nota:** Anote la contraseña proporcionada. La necesitará para la clave privada al introducir cuando tenga que introducir la frase de contraseña en el almacén de claves más adelante en este procedimiento.
>
> Asegúrese de elegir una contraseña segura.

5. Extraiga una lista de alias de los alias del certificado con ayuda del comando siguiente:

   ```
   keytool -list -keystore <nombre_certificado> -v -storetype PKCS12
   ```

   Se mostrarán los alias del certificado y deberán proporcionarse en el siguiente comando.

   En el ejemplo siguiente es la cuarta línea por abajo.

6. Importe el certificado de servidor en formato PKCS12 en el archivo de Central **key.store** mediante el siguiente comando:

   ```
   keytool -importkeystore -srckeystore <ruta de certificado de formato PKCS12> -destkeystore key.store -srcstoretype pkcs12 -deststoretype JKS -alias <alias certificado> -destalias tomcat
   ```

7. Si el certificado de servidor importado tiene una contraseña diferente de la del certificado de servidor original, se debe cambiar la contraseña keyPass. Siga las instrucciones descritas en

"Cambio y cifrado/ocultación de la contraseña del almacén de claves/almacén de confianza" en la página 44.

Se recomienda cambiar la contraseña predeterminada “changeit” en el almacén de claves generado automáticamente del servidor de Central. Consulte "Cambio y cifrado/ocultación de la contraseña del almacén de claves/almacén de confianza" en la página 44.

8. Inicie Central.

Importación de un certificado raíz de CA en el almacén de confianza de Central

Si está utilizando un certificado raíz personalizado para Central, deberá importar la entidad certificadora (CA) de certificados raíz de confianza en el archivo **client.truststore**. Si utiliza un CA raíz conocida (como Verisign), no es necesario que realice el siguiente procedimiento porque el certificado ya estará en el archivo **client.truststore**.

De forma predeterminada, HPE OO admite todos los certificados autofirmados. Sin embargo, en entornos de producción, se recomienda cambiar este valor predeterminado por un CA personalizado o un CA conocido por motivos de seguridad.

Sustituya los parámetros marcados en <amarillo>.

Nota: El siguiente procedimiento usa la utilidad Keytool ubicada en **<dir instalación>/java/bin/keytool**.

1. Detenga Central y realice una copia de seguridad del archivo **client.truststore** original, ubicado en **<dir instalación>/central/var/security/client.truststore**.
2. Importe la autoridad de certificado raíz de confianza (CA) al archivo de Central **client.truststore** si no se incluye aún en la lista de CA (de forma predeterminada, se incluyen todos los CA estándar):

   ```
   keytool -importcert -alias <cualquier_alias> -keystore <ruta a client.truststore> -file <nombre_certificado.cer> -storepass <changeit>
   ```

3. Inicie Central.

Importación de un Certificado raíz de CA a un almacén de confianza RAS

Después de instalar un RAS, si está utilizando un certificado raíz personalizado para Central y no ha proporcionado el certificado raíz durante la instalación de RAS, deberá importar la entidad certificadora (CA) de certificados raíz de confianza en el archivo **client.truststore** de RAS. Si utiliza una CA raíz

conocida, no es necesario que realice el siguiente procedimiento porque el certificado ya estará en el archivo **client.truststore**.

De forma predeterminada, HPE OO admite todos los certificados autofirmados. Sin embargo, en entornos de producción, se recomienda cambiar este valor predeterminado por un CA personalizado o un CA conocido por motivos de seguridad.

Sustituya los parámetros marcados en <amarillo>.

Nota: El siguiente procedimiento usa la utilidad Keytool ubicada en **<dir instalación>/java/bin/keytool**.

1. Detenga RAS y realice una copia de seguridad del archivo **client.truststore**, ubicado en **<dir instalación>/ras/var/security/client.truststore**.
2. Abra una línea de comandos en **<dir instalación>/ras/var/security**.
3. Abra el archivo **<dir instalación> ras/conf/ras-wrapper.conf** y asegúrese de que el valor `-Dssl.support-self-signed` esté establecido en **false**. Esto habilita la entidad certificadora (CA) de certificados raíz de confianza.

   Por ejemplo:

   ```
   wrapper.java.additional.<x>=-Dssl.support-self-signed=false
   ```

4. Abra el archivo **<dir instalación> ras/conf/ras-wrapper.conf** y asegúrese de que `-Dssl.verifyHostName` esté establecido en **false**. Ello verificará que el FQDN del certificado coincide con el FQDN de la solicitud.

   Por ejemplo:

   ```
   wrapper.java.additional.<x>=-Dssl.verifyHostName=true
   ```

   Nota: Esta propiedad está establecida en **true** de forma predeterminada.

5. Importe la autoridad de certificado raíz de confianza (CA) en el archivo RAS **client.truststore** si no se incluye aún en la lista de CA (de forma predeterminada se incluyen todos los CA más conocidos):

   ```
   keytool -importcert -alias <cualquier_alias> -keystore <ruta a
   client.truststore> -file <nombre_certificado.cer> -storepass <changeit>
   ```

6. Inicie RAS.

Importación de un certificado raíz de CA en el almacén de confianza de OOSH

Si está utilizando un certificado raíz personalizado para Central, deberá importar la entidad certificadora (CA) de certificados raíz de confianza en el archivo **client.truststore** de OOSH. Si utiliza un CA raíz conocida (como Verisign), no es necesario que realice el siguiente procedimiento porque el certificado ya estará en el archivo **client.truststore**.

De forma predeterminada, HPE OO admite todos los certificados autofirmados. Sin embargo, en entornos de producción, se recomienda cambiar este valor predeterminado por un CA personalizado o un CA conocido por motivos de seguridad.

Sustituya los parámetros marcados en <amarillo>.

Nota: El siguiente procedimiento usa la utilidad Keytool ubicada en **<dir instalación>/java/bin/keytool**.

1. Detenga Central y realice una copia de seguridad del archivo **client.truststore** original, ubicado en **<dir instalación>/central/var/security/client.truststore**.
2. Edite el archivo **oosh.bat** desde **<dir instalación>/central/bin**.
3. Asegúrese de que el valor `-Dssl.support-self-signed` se haya establecido en **false**. Esto habilita la entidad certificadora (CA) de certificados raíz de confianza.

   Por ejemplo:

   ```
   -Dssl.support-self-signed=false
   ```

4. Asegúrese de que `-Dssl.verifyHostName` esté establecido en **true**. Ello verificará que el FQDN del certificado coincide con el FQDN de la solicitud.

   Por ejemplo:

   ```
   -Dssl.verifyHostName=true
   ```

   Nota: Esta propiedad está establecida en **true** de forma predeterminada.

5. Importe la autoridad de certificado raíz de confianza (CA) al archivo de Central **client.truststore** si no se incluye aún en la lista de CA (de forma predeterminada, se incluyen todos los CA estándar):

   ```
   keytool -importcert -alias <cualquier_alias> -keystore <ruta a
   client.truststore> -file <nombre_certificado.cer> -storepass <changeit>
   ```

6. Ejecute OOSH.
7. Inicie Central.

Importación de un certificado raíz de CA al almacén de confianza de Studio

Si utiliza certificados personalizados en los servidores de Central, SVN o GIT, para que Studio pueda funcionar con ellos, deberá importar la entidad de certificación (CA) raíz de confianza al archivo **client.truststore** de Studio. Si utiliza un CA raíz conocida (como Verisign), no es necesario que realice el siguiente procedimiento porque el certificado ya estará en el archivo **client.truststore**.

De forma predeterminada, HPE OO admite todos los certificados autofirmados. Sin embargo, en entornos de producción, se recomienda cambiar este valor predeterminado por un CA personalizado o un CA conocido por motivos de seguridad.

Para crear una nueva carpeta **.oo**, Studio copia el archivo **client.truststore** de **<dir.instalación>/studio/var/security** a la carpeta **<usuario>/.oo**. Esta acción solo se debe realizar una vez, para garantizar que Studio pueda importar automáticamente los certificados (por ejemplo, para el depurador remoto de Studio). Studio utilizará este archivo como **client.truststore** si existe; en caso contrario, utilizará uno de la instalación de Studio (**<dir.instalación>/studio/var/security/client.truststore**).

Después de una actualización a 10.5x o posterior, la ubicación del almacén de confianza es la carpeta **<usuario>/.oo**.

Si desea importar manualmente un certificado, puede importar **.oo/client.truststore** o **client.truststore** en la carpeta de instalación de Studio.

Si utiliza varias áreas de trabajo, los cambios realizados en el archivo **client.trustore** que se encuentra en la carpeta **.oo** solo se aplicarán al área de trabajo específica. Para poder aplicar el cambio a todas las áreas de trabajo recién creadas, edite el archivo **client.trustore** que se encuentra en la carpeta de instalación de Studio.

Nota: El siguiente procedimiento usa la utilidad Keytool ubicada en **<dir instalación>/java/bin/keytool**.

1. Cierre Studio y realice una copia de seguridad del archivo **client.truststore** original, que se encuentra en **<usuario>/.oo**.

   Por ejemplo, **C:/Users/<nombre_usuario>/.oo**
2. Edite el archivo **Studio.l4j.ini** en **<dir instalación>/studio**.

3. Asegúrese de que el valor `-Dssl.support-self-signed` se haya establecido en **false**. Esto habilita la entidad certificadora (CA) de certificados raíz de confianza.

   Por ejemplo:

   ```
   -Dssl.support-self-signed=false
   ```

4. Asegúrese de que `-Dssl.verifyHostName` se haya establecido en **true**. Ello verificará que el FQDN del certificado coincide con el FQDN de la solicitud.

   Por ejemplo:

   ```
   -Dssl.verifyHostName=true
   ```

5. Importe la entidad de certificación raíz de confianza al archivo **client.truststore** de Studio si todavía no existe en la lista de CA (de forma predeterminada, se incluyen todos los CA reconocidos). Sustituya los parámetros resaltados en <amarillo>:

   ```
   keytool -importcert -alias <cualquier_alias> -keystore <ruta a
   client.truststore> -file <nombre_certificado.cer> -storepass <changeit>
   ```

6. Inicie Studio.

Para obtener más información, consulte "Depuración de un Central remoto con Studio" en la *Guía de creación de Studio*.

Cambio y cifrado/ocultación de la contraseña del almacén de claves/almacén de confianza

Cambio de las contraseñas del almacén de claves, el almacén de confianza y del certificado del servidor en la configuración de Central

1. Asegúrese de que Central esté ejecutándose.

   Nota: Antes de realizar este paso, asegúrese de que haya contraseñas cifradas. Para obtener más información sobre cómo cifrar contraseñas, consulte "Encrypting Passwords" en *HPE OO Administration Guide*.

   En OOSH, ejecute el siguiente comando:

   ```
   set-sys-config --key <keyName> --value <ecryptedPassword>
   ```

   donde `<keyName>` es uno de los valores de la tabla siguiente:

Elemento de configuración	Acción
`key.store.password`	Para establecer la contraseña utilizada para acceder al **key.store**. El valor predeterminado es `"changeit"`. Esto debe corresponderse con el valor de `keystorepass`, tal y como se indica en los pasos siguientes.
`key.store.private.key.alias.password`	Para establecer la contraseña utilizada para acceder al certificado de servidor (clave privada) desde **key.store**. El valor predeterminado es `"changeit"`. Esto debe corresponderse con el valor de `keyPass`, tal y como se indica en los pasos siguientes.

2. Detenga el servicio de Central.
3. Cambie las contraseñas del almacén de claves, el almacén de confianza y el certificado del servidor con ayuda de Keytool.

   Utilice el siguiente comando de la utilidad Keytool para cambiar la contraseña del almacén de claves:

   ```
   keytool -storepasswd -keystore <carpeta_
   instalación>/central/var/security/key.store
   ```

   Utilice el siguiente comando de la utilidad Keytool para cambiar la contraseña de entrada de clave privada certificada de servidor:

   ```
   keytool –keypasswd -alias tomcat -keystore <carpeta_
   instalación>/central/var/security/key.store
   ```

   Utilice el siguiente comando de la utilidad Keytool para cambiar la contraseña del almacén de confianza:

   ```
   keytool -storepasswd -keystore <carpeta_
   instalación>/central/var/security/client.truststore
   ```

4. Cambie también las contraseñas en el archivo **server.xml** que se encuentra en **<dir instalación>/central/tomcat/conf/server.xml**.

   a. Localice el conector de HTTPS. Por ejemplo:

   ```
   keyPass="changeit" keystoreFile="C:/Program Files/Hewlett-Packard/HP
   Operations Orchestration/central/var/security/key.store"
   keystorePass="changeit" keystoreType="JKS" maxThreads="200" port="8443"
   ```

```
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
secure="true" sslProtocol="TLSv1.2"
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" truststoreFile="C:/Program
Files/Hewlett-Packard/HP Operations
Orchestration/central/var/security/client.truststore"
truststorePass="changeit" truststoreType="JKS"/>
```

Cambie la contraseña correspondiente.

- `keyPass`: contraseña utilizada para acceder a la clave privada del certificado del servidor del archivo del almacén de claves especificado. El valor predeterminado es "`changeit`".
- `keystorePass`: contraseña utilizada para acceder al archivo del almacén de claves especificado. El valor predeterminado es el valor del atributo `keyPass`.

  Nota: Se recomienda no usar la misma contraseña de **keyPass**, y usar una contraseña segura.

- `Truststorepass`: contraseña para acceder al almacén de confianza (el cual incluye todos los CA de confianza). El valor predeterminado es el valor de la propiedad de sistema **javax.net.ssl.trustStorePassword**. Si dicha propiedad es nula, no se configurará ninguna contraseña para el almacén de confianza. Si se especifica una contraseña para el almacén de confianza no válida, se registrará una advertencia y se intentará acceder al almacén de confianza sin contraseña, omitiendo la validación del contenido del almacén de confianza.

b. Guarde el archivo.

5. Edite el archivo **central-wrapper.conf** ubicado en **<dir instalación> central\conf\central** y sustituya la contraseña del almacén de confianza por la nueva contraseña en formato cifrado u ocultado. Ejemplos:

   ```
   wrapper.java.additional.<x>=-Djavax.net.ssl.trustStorePassword={ENCRYPTED}
   <contraseña_cifrada>
   ```

   ```
   wrapper.java.additional.<x>=-Djavax.net.ssl.trustStorePassword={OBFUSCATED}
   <contraseña_ocultada>
   ```

   Para obtener más información sobre cómo cifrar u ocultar contraseñas, consulte "Cifrado y ocultación de contraseñas" en la página siguiente.

6. Inicie el servicio de Central.

Cambio de contraseñas RAS, OOSH, y del almacén de confianza de Studio

Nota: Debe cambiar las contraseñas del almacén de claves, el almacén de confianza y el certificado del servidor con ayuda de Keytool antes de realizar los pasos siguientes.

- **Para cambiar la contraseña del almacén de confianza independiente de RAS**: Edite el archivo **ras-wrapper.conf** y cambie la contraseña del almacén de confianza.
- **Para cambiar la contraseña del almacén de confianza de OOSH**: Edite el archivo **oosh.bat** y cambie la contraseña del almacén de confianza.
- **Para cambiar la contraseña del almacén de confianza de Studio**: Añada la propiedad **client.truststore.password** con la contraseña en formato oculto en el archivo **Studio.properties** de la carpeta **<user>/.oo**.

  ```
  client.truststore.password={OBFUSCATED}6L9+NqBjKYp5heuvMEzg0g==
  ```

  Si no se define esta propiedad, Studio recurrirá a la propiedad del sistema **javax.net.ssl.trustStorePassword** para la contraseña del almacén de confianza.

Para obtener más información sobre cómo ocultar contraseñas, consulte "Cifrado y ocultación de contraseñas" abajo.

Cifrado y ocultación de contraseñas

Puede cifrar u ocultar contraseñas utilizando el script `encrypt-password`, que encontrará en **<carpeta_instalación>/central/bin**.

Se recomienda utilizar el cifrado.

¡Importante! Después de utilizar el script `encrypt-password`, borre el historial de comandos.

Esto es así porque en un sistema operativo Linux el parámetro de contraseña se almacenará en texto no cifrado en **/$USER/.bash_history** y estará accesible por el comando `history`.

Cifrado de contraseñas

1. Localice el script `encrypt-password` en **<carpeta_instalación>/central/bin**.
2. Ejecute el script con la opción `-e -p <password>`, donde `password` es la contraseña que se desea cifrar.

Nota: Puede utilizar `-p` como indicador para cifrar la contraseña o bien `--password`.

La contraseña cifrada debe aparecer como sigue:

```
{ENCRYPTED}<some_chars>.
```

Ocultación de contraseñas

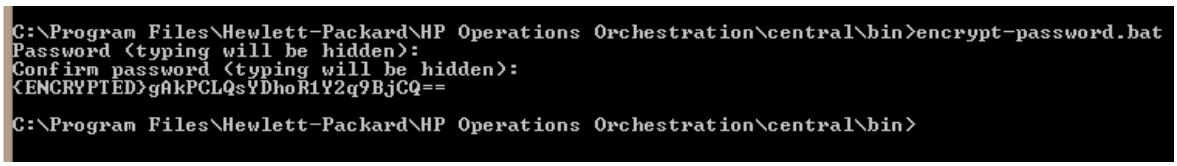
1. Localice el script `encrypt-password` en **<carpeta_instalación>/central/bin**.
2. Ejecute el script con la opción `-o <password>`, donde `password` es la contraseña que se desea ocultar.

   La contraseña ocultada debe aparecer como sigue:

```
{OBFUSCATED}<algunos_caracteres>.
```

Creación de una solicitud para la contraseña

Se recomienda ejecutar el script `encrypt-password` sin proporcionar el argumento `-p`. Por ejemplo:



Esta acción creará una solicitud para las entradas de contraseñas ocultas.

Supresión del cifrado RC4 de los cifrados admitidos por SSL

El host remoto admite el uso del cifrado RC4. Este cifrado no genera correctamente una secuencia pseudoaleatoria de bytes al introducir gran variedad de sesgos en la secuencia, disminuyendo así su aleatoriedad.

Si se cifra repetidamente texto sin formato (por ejemplo, cookies HTTP) y un atacante logra obtener muchos (digamos, unos diez millones) textos cifrados, podrá deducir el texto sin formato.

Deshabilite el cifrado RC4 en el nivel de JRE (empezando con Java 7):

1. Abra el archivo **$JRE_HOME/lib/security/java.security**.
2. Deshabilite el cifrado de RC4 eliminando los comentarios y cambiando los parámetros según el ejemplo siguiente:

```
jdk.certpath.disabledAlgorithms=RC4, MD2, RSA keySize < 1024
jdk.tls.disabledAlgorithms=RC4, MD5, DSA, RSA keySize < 1024
```

3. Reinicie el servidor de OO Central.

Para obtener más información, consulte http://stackoverflow.com/questions/18589761/restict-cipher-suites-on-jre-level.

Nota: Después de actualizar de una versión anterior de HPE OO 10.x, repita estos pasos.

Cambio de los puertos HTTP/HTTPS o deshabilitación del puerto HTTP

El archivo **server.xml** en **[OO_HOME]/central/tomcat/conf** contiene dos elementos llamados **<Connector>** en el elemento **<Service>**. Estos conectores definen o habilitan los puertos en los que escuchará el servidor.

Cada configuración de conector se define a través de sus atributos. El primer conector define un conector HTTP normal y el segundo un conector HTTPS.

De forma predeterminada, los conectores presentan el siguiente aspecto:

Conector de HTTP:

```
<Connector URIEncoding="UTF-8" compression="on" connectionTimeout="20000"
port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol"
redirectPort="8443"/>
```

Conector de HTTPS:

```
<Connector SSLEnabled="true" URIEncoding="UTF-8" clientAuth="false"
compression="on" keyAlias="tomcat" keyPass="changeit" keystoreFile="C:/Program
Files/Hewlett-Packard/HP Operations
Orchestration/central/var/security/key.store" keystorePass="changeit"
keystoreType="JKS" maxThreads="200" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
secure="true" sslProtocol="TLSv1.2" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
truststoreFile="C:/Program Files/Hewlett-Packard/HP Operations
Orchestration/central/var/security/client.truststore" truststorePass="changeit"
truststoreType="JKS"/>
```

De forma predeterminada, ambos están habilitados.

¡Importante! Si cambia o deshabilita uno de los puertos de Central en el archivo **server.xml**, también deberá actualizar el archivo **central-wrapper.conf** y hacer que todos los archivos **RAS-**

wrapper.conf apunten a la dirección URL de Central con el puerto actualizado. En caso contrario, fallarán todos los flujos cuando se ejecuten desde Central. Además, asegúrese de comprobar la configuración del equilibrador de carga.

Cambio de valores de puerto

Para cambiar los valores de uno de los puertos:

1. Edite el archivo **server.xml** que se encuentra en **<dir_ instalación>/central/tomcat/conf/server.xml**.
2. Localice el conector HTTP o HTTPS y ajuste el valor **port** en la línea.

   Nota: Si desea mantener activos tanto HTTP como HTTPS, pero quiere cambiar el puerto HTTPS, deberá cambiar el valor **redirectPort** del conector HTTP y el valor **port** del conector HTTPS.
3. Guarde el archivo.
4. Reinicie Central.

Deshabilitación del puerto HTTP

Es posible que desee deshabilitar el puerto HTTP, por motivos de seguridad, de modo que el único canal de comunicación esté en TLS y sea cifrado.

1. Edite el archivo **server.xml** que se encuentra en **<dir_ instalación>/central/tomcat/conf/server.xml**.
2. Localice el conector HTTP y elimine o comente la línea.
3. Importe la autoridad de certificado raíz de confianza (CA) al archivo de Central **client.truststore**, si no existe ya en la lista de CA:

   ```
   keytool -importcert -alias <cualquier_alias> -keystore <ruta a client.truststore> -file <nombre_certificado.cer> -storepass <changeit>
   ```

   Nota: Si utiliza una CA raíz conocida (como Verisign), no será necesario que realice el siguiente paso porque el certificado ya estará en el archivo **client.truststore**.
4. Guarde el archivo.
5. Reinicie Central.

Nota: Se puede asimismo deshabilitar el puerto HTTP durante la instalación.

Solución de problemas

Si el servidor no se inicia, abra el archivo **wrapper.log** y busque el error en `ProtocolHandler ["http-nio-8443"]`.

Puede suceder si Tomcat se está inicializando o se inicia el conector. Existen muchas variantes, pero el mensaje de error puede proporcionar información.

Todos los parámetros de conector HTTPS se encuentran en el archivo de configuración de Tomcat ubicado en **C:\HPE\oo\central\tomcat\conf\server.xml**.

Abra el archivo y desplácese hasta el final, hasta que vea el conector de HTTPS:

```
<Connector SSLEnabled="true" clientAuth="false" keyAlias="tomcat"
keystoreFile="C:/HPE/oo/central/var/security/keystore.p12" keystorePass="tomcat-
keystore-password" keystoreType="PKCS12" maxThreads="200" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
sslProtocol="TLSv1.2" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"/>
```

Averigüe si hay alguna coincidencia errónea en los parámetros comparándolos con los que introdujo en los pasos anteriores.

Autenticación de certificado de cliente (autenticación mutua)

La autenticación de certificado X.509 suele utilizarse para verificar la identidad de un servidor al usar TLS, sobre todo cuando se utiliza HTTPS desde un explorador. El explorador comprueba automáticamente que el certificado presentado por un servidor haya sido emitido por una autoridad certificadora de confianza y lo conserva.

También se puede usar TLS con autenticación mutua. El servidor solicita un certificado válido al cliente como parte del intercambio de señales TLS. El servidor autentica el cliente comprobando que el certificado esté firmado por una autoridad capacitada para ello. Si se ha proporcionado un certificado válido, se puede obtener a través de la API de servlet en una aplicación.

Configuración de la autenticación del certificado de cliente en Central

Antes de configurar la autenticación del certificado de cliente en Central, asegúrese de haber configurado el certificado de servidor TLS, tal como se describe en la sección "Trabajo con certificados de servidor y de cliente" en la página 37.

Establezca el atributo `clientAuth` en `true` si desea que la pila TLS solicite una cadena de certificados válida al cliente antes de aceptar una conexión. Establezca el atributo en `want` si desea que la pila TLS solicite un certificado de cliente, pero que no se produzca un error en caso de no existir. Un valor `false` (predeterminado) no solicitará una cadena de certificados a no ser que el cliente solicite un recurso protegido por una restricción de seguridad con autenticación CLIENT-CERT. (Para obtener más información, consulte la Referencia de configuración Apache Tomcat).

Establezca el archivo **Lista de revocación de certificados (CRL)**. Puede contener varias CRL. En la operación de algunos sistemas cifrados, normalmente infraestructuras de claves públicas (PKI), una lista de revocación de certificados (CRL) es una lista de certificados (o más específicamente, una lista de números de serie de certificados) que se han revocado y, por tanto, las entidades con dichos certificados (revocados) no deben considerarse fiables.

Nota: El siguiente procedimiento usa la utilidad Keytool ubicada en **<dir instalación>/java/bin/keytool**.

1. Detenga el servidor de Central.
2. Importe el certificado raíz adecuado (CA) en Central **client.truststore**: **<dir instalación>/central/var/security/client.truststore**, en caso de que no exista ya uno en la lista de CA (de forma predeterminada, la lista incluye todos los CA más conocidos). Por ejemplo:

   ```
   keytool -importcert -alias <cualquier_alias> -keystore <ruta>/client.truststore
   -file <ruta_certificado> -storepass <changeit>
   ```

3. Edite el archivo **server.xml** que se encuentra en **<dir_ instalación>/central/tomcat/conf/server.xml**.
4. Establezca el atributo `clientAuth` de la etiqueta `Connector` en `want` o en `true`. El valor predeterminado es `false`.

   Por ejemplo:

   ```
   <Connector SSLEnabled="true" URIEncoding="UTF-8" clientAuth="false"
   compression="on" keyAlias="tomcat" keyPass="changeit"
   keystoreFile="C:/Program Files/Hewlett-Packard/HP Operations
   Orchestration/central/var/security/key.store" keystorePass="changeit"
   keystoreType="JKS" maxThreads="200" port="8443"
   protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
   secure="true" server="OO" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
   sslProtocol="TLSv1.2" truststoreFile="C:/Program Files/Hewlett-Packard/HP
   Operations Orchestration/central/var/security/client.truststore"
   ```

```
truststorePass="changeit" truststoreType="JKS"/>
```

Nota: Le recomendamos que inicie el servidor al final de este procedimiento, pero tenga en cuenta que también es posible hacerlo en este instante.

5. (Opcional) Añada el atributo `crlFile` a fin de definir la lista de revocación de certificados para la validación de certificados TLS, por ejemplo:

   ```
   crlFile="<path>/crlname.<crl/pem>"
   ```

   El archivo puede tener la extensión `.crl` para una única lista de revocación de certificados o la extensión `.pem` (formato PEM CRL) para una o más listas. El formato PEM CRL utiliza las siguientes líneas de cabecera y pie de página:

   ```
   -----BEGIN X509 CRL-----
   -----END X509 CRL-----
   ```

   Ejemplo de la estructura de archivos `.pem` para un CRL (para más de uno, concatene otro bloque de CRL):

   ```
   -----BEGIN X509 CRL-----
   MIIBbzCB2QIBATANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzEYMBYGA1UE
   ChMPVS5TLiBHb3Zlcm5tZW50MQwwCgYDVQQLEwNEb0QxEDAOBgNVBAsTB1Rlc3Rp
   bmcxFTATBgNVBAMTDFRydXN0IEFuY2hvchcNOTkwMTAxMTIwMTAwWhcNNDgwMTAx
   MTIwMTAwWjAiMCACASScXDTk5MDEwMTEyMDAwMFowDDAKBgNVHRUEAwoBAaAjMCEw
   CgYDVR0UBAMCAQEwEwYDVR0jBAwwCoAIq5rr+cLnVI8wDQYJKoZIhvcNAQEFBQAD
   gYEAC7lqZwejJRW7QvzH11/7cYcL3racgMxH3PSU/ufvyLk7ahR++RtHary/WeCv
   RdyznLiIOA8ZBiguWtVPqsNysNn7WLofQIVa+/TD3T+lece4e1NwGQvj5Q+e2wRt
   GXg+gCuTjTKUFfKRnWz7O7RyiJKKim0jtAF4RkCpLebNChY=
   -----END X509 CRL-----
   ```

6. Editar el archivo **central-wrapper.conf** que se encuentra en **<dir instalación> central\conf\central** y cambiar:

   Quite la marca de comentario de las propiedades siguientes y establezca la ubicación del certificado cliente y la contraseña en un certificado cliente con un usuario administrador.

   ```
   #wrapper.java.additional.23=-Djavax.net.ssl.keyStore="%CENTRAL_
   HOME%/var/security/certificate.p12"

   #wrapper.java.additional.24.stripquotes=TRUE

   #wrapper.java.additional.25=-Djavax.net.ssl.keyStorePassword={OBFUSCATED}
   ZUoMreNLw6qIOyzX7g5YKw==

   #wrapper.java.additional.26=-Djavax.net.ssl.keyStoreType=PKCS12
   ```

Para obtener más información sobre cómo cifrar u ocultar contraseñas, consulte "Cifrado y ocultación de contraseñas" en la página 47.

7. Inicie el servidor de Central.

Nota: Debe definir un usuario para cada certificado de cliente, ya sea un usuario interno o un usuario LDAP. El nombre del usuario debe definirse en los atributos de certificado. El valor predeterminado es el atributo de CN. Consulte la sección Procesamiento de certificado principal para obtener más información.

Tenga en cuenta que incluso si HPE OO se ha configurado con múltiples configuraciones de LDAP, solo se puede autenticar al usuario utilizando los atributos de certificado cliente con el LDAP predeterminado.

Actualización de la configuración de un certificado de cliente en RAS

El certificado de cliente se configura durante la instalación del RAS. Sin embargo, si es necesario actualizar el certificado de cliente, puede hacerlo manualmente en el archivo **ras-wrapper.conf**.

Requisitos previos: Debe importar el certificado raíz de CA de Central en el almacén de confianza de RAS. Consulte "Importación de un Certificado raíz de CA a un almacén de confianza RAS" en la página 40.

Para actualizar la configuración del certificado de cliente en un RAS externo:

1. Detenga el servidor RAS.
2. Abra el archivo **ras-wrapper.conf** desde **<dir instalación>ras/conf/ras-wrapper.conf**.
3. Cambie lo siguiente según su certificado de cliente:

```
wrapper.java.additional.<x>=-Djavax.net.ssl.keyStore=<dir
instalación>/var/security/certificate.p12"
```

```
wrapper.java.additional.<x>=-Djavax.net.ssl.keyStorePassword={OBFUSCATED}
<contraseña_ocultada>
```

```
wrapper.java.additional.<x>=-Djavax.net.ssl.keyStoreType=PKCS12
```

4. Inicie el servidor RAS.

Notas importantes El certificado de cliente X.509 debe tener el nombre principal del RAS, el cual es el Id. de RAS (consulte Procesamiento de certificado principal).

Encontrará el Id.de RAS en la ficha **Topología** en Central. Consulte "Setting Up Topology – Workers" en *OO Central User Guide*.

En HPE OO 10.20 y versiones posteriores el parámetro `keyStorePassword` está oculto de forma predeterminada si la contraseña se mantiene como valor predeterminado. Puede cambiar este parámetro y almacenarlo en texto no cifrado u ocultado. Consulte "Cifrado y ocultación de contraseñas" en la página 47.

Configuración de un certificado de cliente en el depurador remoto de Studio

Requisitos previos: Debe importar el certificado raíz de CA de Central en el almacén de confianza del depurador de Studio. Consulte "Importación de un certificado raíz de CA al almacén de confianza de Studio" en la página 43.

Para configurar el certificado de cliente en el depurador remoto de Studio:

1. Cierre Studio.
2. Edite el archivo **Studio.l4j.ini** en **<dir instalación>/studio**.
3. Cambie lo siguiente según su certificado de cliente:

```
-Djavax.net.ssl.keyStore="<dir instalación>/studio/var/security/certificate.p12"
-Djavax.net.ssl.keyStorePassword={OBFUSCATED}<contraseña_ocultada>
-Djavax.net.ssl.keyStoreType=PKCS12
```

4. Inicie Studio.

Notas:

- En HPE OO 10.20 y versiones posteriores el parámetro `keyStorePassword` está oculto de forma predeterminada si la contraseña se mantiene como valor predeterminado. Puede cambiar este parámetro y almacenarlo en texto no cifrado u ocultado. Consulte "Cifrado y ocultación de contraseñas" en la página 47.
- Para el certificado de cliente, debe definir un usuario, ya sea un usuario interno o un usuario LDAP. El nombre del usuario debe definirse en los atributos de certificado. El valor predeterminado es el atributo de CN. Consulte la sección Procesamiento de certificado principal para obtener más información.
- Tenga en cuenta que incluso si HPE OO se ha configurado con múltiples configuraciones de LDAP, solo se puede autenticar al usuario utilizando los atributos de certificado cliente con el LDAP predeterminado. Central intentará primero autenticar al usuario con el LDAP

predeterminado y, si no es posible, intentará autenticarlo dentro del dominio interno de HPE OO.

Configuración de un certificado de cliente en OOSH

Requisitos previos: Debe importar el certificado raíz de CA de Central en el almacén de confianza de OOSH. Consulte "Importación de un certificado raíz de CA en el almacén de confianza de OOSH" en la página 42.

1. Detenga OOSH.
2. Edite el archivo **oosh.bat** desde **<dir instalación>/central/bin**.
3. Cambie lo siguiente según su certificado de cliente:

```
-Djavax.net.ssl.keyStore="<dir instalación>/var/security/certificate.p12"
-Djavax.net.ssl.keyStorePassword={OBFUSCATED}<contraseña_ocultada>
-Djavax.net.ssl.keyStoreType=PKCS12
```

4. Inicie OOSH.

Nota:

En HPE OO 10.20 y versiones posteriores el parámetro `keyStorePassword` está oculto de forma predeterminada si la contraseña se mantiene como valor predeterminado. Puede cambiar este parámetro y almacenarlo en texto no cifrado u ocultado. Consulte "Cifrado y ocultación de contraseñas" en la página 47.

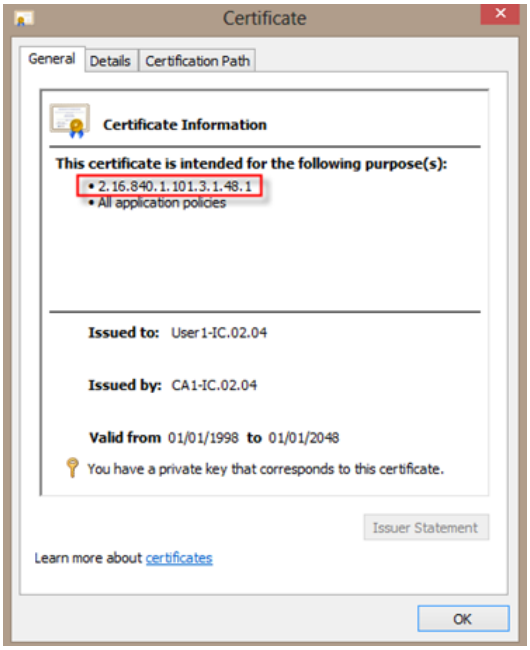
Para el certificado de cliente, debe definir un usuario, ya sea un usuario interno o un usuario LDAP. El nombre del usuario debe definirse en los atributos de certificado. El valor predeterminado es el atributo de CN. Consulte la sección Procesamiento de certificado principal para obtener más información.

Tenga en cuenta que incluso si HPE OO se ha configurado con múltiples configuraciones de LDAP, solo se puede autenticar al usuario utilizando los atributos de certificado cliente con el LDAP predeterminado. Central intentará primero autenticar al usuario con el LDAP predeterminado y, si no es posible, intentará autenticarlo dentro del dominio interno de HPE OO.

Procesamiento de directivas de certificado

HPE OO controla el procesamiento de las directivas de certificado para el certificado de punto final.

- Puede establecer la cadena de la finalidad en el certificado.
- HPE OO le permite añadir la cadena de directivas como un elemento de configuración y comprobar la cadena de directivas de cada certificado de punto final. Si no coincide, rechace el certificado.
- Habilite o deshabilite la verificación de directivas de certificado añadiendo el siguiente elemento de configuración: `x509.certificate.policy.enabled=true/false` (el valor predeterminado es `false`).
- Defina la lista de directivas añadiendo el siguiente elemento de configuración: `x509.certificate.policy.list=<comma_separated_list>` (el valor predeterminado es una lista vacía).



Para obtener más información acerca de cómo cambiar las propiedades del sistema de OO, consulte la *OO Shell Guide*.

Procesamiento de un principal de certificado

Puede definir cómo obtener el principal de un certificado usando una expresión regular que coincida con `Subject`. La expresión regular debe contener un único grupo. La expresión predeterminada `CN=(.?)` coincide con el campo de nombre común. Por ejemplo, `CN=Jimi Hendrix, OU=` asigna el nombre de usuario `Jimi Hendrix`.

- Las coincidencias distinguen entre mayúsculas y minúsculas.
- El principal del certificado es el nombre de usuario de HPE OO (LDAP o usuario interno).

- Para cambiar la expresión regular, cambie el elemento de configuración: `x509.subject.principal.regex`.

Habilitación de OO para que lea desde el campo Subject Alternative Name en un certificado

Puede habilitar OO para que lea desde el campo `Subject Alternative Name` en un certificado, mediante el elemento de configuración `x509.principal.lookup.field`.

Este elemento de configuración controla qué campo del certificado se usa para extraer el nombre de usuario.

Los valores posibles son los siguientes:

- `subjectDN`: representa el campo `Subject` del certificado, lo que significa que OO mantiene su comportamiento predeterminado e intenta extraer el nombre de usuario del campo **Subject**. Este es el valor predeterminado.
- `subjectAltNames.otherName.principalName`: representa `User Principal Name` (OID 1.3.6.1.4.1.311.20.2.3) incluido en la entrada `Other Name` de la extensión del certificado `Subject Alternative Names`. Para la autenticación con CAC, es posible que se necesite utilizar el valor del nombre principal de usuario, por lo que utilizará este valor.

Para obtener más información acerca de cómo cambiar los elementos de configuración de HPE OO, consulte *HPE OO Shell (OOSH) User Guide*.

Configuración de HPE OO para compatibilidad con FIPS 140-2 Nivel 1

Esta sección explica cómo configurar HPE Operations Orchestration para que sea compatible con el Estándar federal de procesamiento de información (FIPS) 140-2 Nivel 1.

FIPS 140-2 es un estándar sobre requisitos de seguridad para módulos criptográficos definidos por el Instituto Nacional de Normalización y Tecnología (NIST). Para ver la publicación de esta norma, vaya a: csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Después de configurar HPE OO para su conformidad con FIPS 140-2, HPE OO utiliza el siguiente algoritmo de seguridad:

- Algoritmo de claves simétricas: AES256
- Algoritmo hash: SHA256

HPE OO usa el proveedor de seguridad: Software RSA BSAFE Crypto versión 6.2.1. Es el único proveedor de seguridad compatible con FIPS 140-2.

Nota: Una vez configurado HPE OO para ser compatible con FIPS 140-2, no es posible volver a la configuración estándar sin reinstalar HPE OO.

Requisitos previos

Nota para actualizadores:

Si se realiza una actualización a partir de una instalación de HPE OO 10.10 (y posterior) previamente configurada con FIPS, consulte Pasos de requisitos previos para actualizadores.

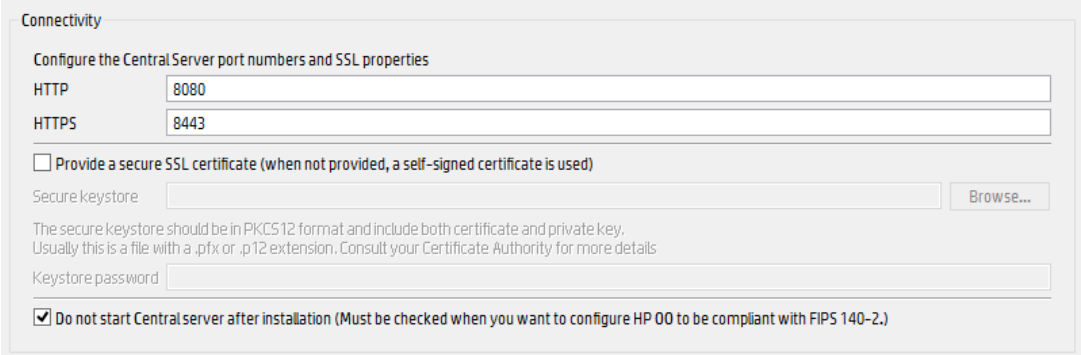
Antes de configurar HPE OO para ser compatibles con FIPS 140-2, realice los pasos siguientes:

Nota: Para ser compatible con FIPS140-2, es necesario desactivar LWSSO.

1. Compruebe que está configurando una nueva instalación de HPE OO versión 10.10 o posterior que sea compatible con FIPS 140-2 y que no se encuentre en uso.

   No es posible configurar instalaciones de HPE OO que se encuentren en uso (tanto las 9.x como las 10.x).

2. Compruebe que cuando se instaló HPE OO, se configuró para no iniciar el servidor de Central después de la instalación:
   - En una instalación silenciosa, el parámetro `should.start.central` se ha establecido en **no**.
   - En una instalación de asistente, en el paso **Conectividad**, se ha seleccionado el cuadro de verificación **No iniciar el servidor de Central después de la instalación**.



3. Realice una copia de seguridad de los siguientes directorios:
   - **<dir instalación>\central\tomcat\webapps\oo.war**
   - **<dir instalación>\central\tomcat\webapps\PAS.war**
   - **<dir instalación>\central\conf**
   - **<dir instalación>\java** (se debe realizar una copia de seguridad de toda la carpeta **java**)
4. Descargue **Server Oracle JRE 8** desde http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html y reemplace **OpenJDK (Zulu) JRE** con **Server Oracle JRE**.
   a. Borre todo lo que haya dentro de la carpeta **<dir instalación>\JAVA**.
   b. Extraiga el archivo descargado.
   c. Copie el contenido de la carpeta **JRE** en **<dir instalación>\JAVA**.
5. Descargue e instale Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction Policy Files del siguiente sitio:

   http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html

   Nota: Consulte el archivo **ReadMe.txt** del contenido descargado para obtener información sobre cómo desplegar los archivos y actualizar el JRE usado por HPE OO.
6. Instale los archivos de software RSA BSAFE Cripto. En el sistema donde está instalado HPE OO, copie lo siguiente en **<oo_jre>\lib\ext** (en donde **<oo_jre>** es el directorio donde está

instalado el JRE usado por HPE OO. De forma predeterminada, es **<dir instalación>\java**).

- **<dir instalación>\central\lib\cryptojce-6.2.1.jar**
- **<dir instalación>\central\lib\cryptojcommon-6.2.1.jar**
- **<dir instalación>\central\lib\jcmFIPS-6.2.1.jar**

Pasos de requisitos previos para actualizadores

1. Descargue Server Oracle JRE 8 y reemplace OpenJDK (Zulu) JRE por Server Oracle JRE.
   a. Borre todo lo que haya dentro de la carpeta **<dir actualización>\JAVA**.
   b. Extraiga el archivo descargado.
   c. Copie el contenido de la carpeta **JRE** en **<dir actualización>\JAVA**.

   http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html
2. Descargue e instale Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction Policy Files del siguiente sitio:

   http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

   Consulte el archivo **ReadMe.txt** del contenido descargado para obtener información sobre cómo desplegar los archivos y actualizar el JRE usado por HPE OO.
3. Instale los archivos de software RSA BSAFE Cripto. En el sistema en el que está instalado HPE OO, copie los archivos siguientes en **<oo_jre>\lib\ext**:

   (donde **<oo_jre>** es el directorio en el que está el JRE que el actualizador de HPE OO utiliza. De forma predeterminada, es **<dir actualización>\java**).

   - <dir instalación>\central\lib\cryptojce-6.2.1.jar
   - <dir instalación>\central\lib\cryptojcommon-6.2.1.jar
   - <dir instalación>\central\lib\jcmFIPS-6.2.1.jar

A continuación, siga los pasos de la sección "Configuración de las propiedades del archivo de seguridad Java" en "Configuración de HPE OO para que sea compatible con FIPS 140-2" en la página siguiente.

Configuración de HPE OO para que sea compatible con FIPS 140-2

La siguiente lista siguiente muestra los procedimientos que se deben realizar para configurar HPE OO para que sea compatible con FIPS 140-2:

1. Configurar las propiedades del archivo Java de seguridad.
2. Configuración del archivo encryption.properties y habilitación del modo FIPS.
3. Creación de un cifrado para HPE OO compatible con FIPS.
4. Volver a cifrar la contraseña de la base de datos con el nuevo cifrado.
5. Inicio de HPE OO.

Configurar las propiedades del archivo Java de seguridad

Edite el archivo de seguridad Java para añadir proveedores de seguridad adicionales y configurar las propiedades para que sean compatibles con FIPS 140-2.

Nota: La actualización a HPE OO 10.x sustituye completamente los archivos instalados de JRE. Por lo tanto, si está actualizando a 10.x, debe completar los pasos siguientes.

Nota: Si está actualizando desde una instalación de HPE OO 10.10 y versiones posteriores que estaban ya configuradas con FIPS, debe seguir la sección "Pasos de requisitos previos para actualizadores" en"Configuración de HPE OO para compatibilidad con FIPS 140-2 Nivel 1" en la página 59 y luego los pasos indicados aquí, donde **<oo_jre>** es el JRE incluido en la actualización (en la ubicación **<dir actualización>\JAVA**).

Asegúrese de realizar todos los cambios en la carpeta **java** dentro de la carpeta **upgrade** extraída.

Abra el archivo **<oo_jre>\lib\security\java.security** en un editor y realice los pasos siguientes:

1. Incremente el número de orden de preferencia `<nn>` en dos, en el formato **security.provider.<nn>=<provider_name>**, para todos los proveedores de la lista.

   Por ejemplo, cambie una entrada de proveedor de:

   ```
   security.provider.1=sun.security.provider.Sun
   ```

   a

   ```
   security.provider.3=sun.security.provider.Sun
   ```

2. Añada un nuevo proveedor predeterminado (RSA JCE). Añada el siguiente proveedor en la parte superior de la lista de proveedores:

   `security.provider.1=com.rsa.jsafe.provider.JsafeJCE`

3. Agregue el proveedor Extensión de sockets seguros de Java (JSSE) RSA BSAFE SSL-J.

   `security.provider.2=com.rsa.jsse.JsseProvider`

4. Copie y pegue la siguiente línea en el archivo **java.security** para asegurarse de utilizar **RSA BSAFE** en modo compatible con FIPS 140-2:

   `com.rsa.cryptoj.fips140initialmode=FIPS140_SSL_MODE`

   Puede pegar esta línea en el archivo **java.security**.

5. Puesto que el algoritmo ECDRBG128 de DRBG no es seguro (según NIST), debe establecer la propiedad de seguridad **com.rsa.crypto.default** en **HMACDRBG**, copiando la siguiente línea en el archivo **java.security**:

   `com.rsa.crypto.default.random=HMACDRBG`

   Puede pegar esta línea en el archivo **java.security**.

6. Guarde el archivo **java.security** y salga.

Configuración del archivo encryption.properties y habilitación del modo FIPS

El archivo de propiedades de cifrado de HPE OO se debe actualizar para que sea compatible con FIPS 140-2.

1. Haga copias de respaldo del archivo **encryption.properties** que se encuentra en **<dir instalación>\central\var\security**.
2. Abra el archivo **encryption.properties** en un editor de texto. Por ejemplo, edite el siguiente archivo:

   C:\Program Files\Hewlett-Packard\HP Operations Orchestration\central\var\security\encryption.properties.

3. Localice `keySize=128` y sustitúyalo con `keySize=256`.
4. Localice `secureHashAlgorithm=SHA1` y sustitúyalo con `secureHashAlgorithm=SHA256`.
5. Localice `FIPS140ModeEnabled=false` y sustitúyalo con `FIPS140ModeEnabled=true`.

   Nota: Si `FIPS140ModeEnabled=false` no existe, añada `FIPS140ModeEnabled=true` como

una línea nueva al final del archivo.

6. Guarde el archivo y ciérrelo.

Creación de un cifrado para OO compatible con FIPS

Para crear o sustituir el archivo de almacenamiento de cifrado de HPE OO a fin de que sea compatible con FIPS, consulte "Sustitución del cifrado FIPS" en la página siguiente.

Nota: AES tiene tres longitudes de clave aprobadas: 128/192/256 por publicación NIST SP800-131A.

Los siguientes algoritmos hash seguros son compatibles con FIPS: SHA1, SHA256, SHA384, SHA512.

Nota: Se recomienda cambiar las contraseñas del almacén de claves (y la entrada de clave privada) y el almacén de confianza. Consulte "Cambio y cifrado/ocultación de la contraseña del almacén de claves/almacén de confianza" en la página 44

Nota: Se recomienda eliminar todos los certificados raíz CA predeterminados que no estén en uso del almacén de confianza de OO. (El **client.truststore** se encuentra en **<instalación>/central/var/security**).

Nota: Si trabaja con el certificado de cliente, el certificado se debe generar con el proveedor JCE RSA conforme a FIPS y con los algoritmos hash seguros admitidos por FIPS, tal como se indica anteriormente.

Volver a cifrar la contraseña de la base de datos con el nuevo cifrado

Vuelva a cifrar la contraseña de la base de datos tal y como se describe en la *Guía de administración de HPE OO*, en "Cambio de la contraseña de la base de datos".

Inicio de HPE OO

Sustitución del cifrado FIPS

HPE OO Central y RAS cumplen la norma federal de proceso de la información 140-2 (FIPS 140-2), que define los requisitos técnicos que deben usar las agencias federales cuando especifican sistemas de seguridad basados en criptografía para la protección de datos confidenciales o valiosos.

Después de una nueva instalación de HPE OO, puede optar por cambiar la clave de cifrado FIPS.

Nota: Este procedimiento se aplica solo a instalaciones nuevas. No se puede realizar después de una actualización.

Cambio de la clave de cifrado FIPS en Central

Utilice el archivo **generate-keys.bat/sh** para sustituir la clave de cifrado FIPS en el repositorio de cifrado.

Nota: Este proceso realiza una copia de seguridad del archivo **encryption_repository** , así que es necesario que disponga de permisos de escritura.

1. Vaya a **<Carpeta de instalación de Central>/var/security**.
2. Realice una copia de seguridad del archivo **encryption_repository** y elimínelo de la carpeta **<Carpeta de instalación de Central>/var/security**.
3. Vaya a **<Central installation folder>/bin**.
4. Ejecute el script **generate-keys**.
5. Pulse la tecla **Y** para continuar.

   Se generará una clave maestra en **<Central installation folder>/var/security/encryption_repository**.

Nota: Si prefiere ejecutar el script **generate-keys** sin hacer una pausa para que el usuario escriba **Y** o **N**, utilice el indicador de modo silencioso **–s** al ejecutar el script.

Cambio de las propiedades de cifrado de RAS

Si la instalación de RAS se realiza en una ubicación nueva, debe completar todos los pasos siguientes.

Nota: Estos cambios solo son válidos si está trabajando en una nueva instalación de RAS después de haber cambiado las propiedades de cifrado de Central.

Para cambiar las propiedades de cifrado de RAS:

1. Complete todos los pasos de la sección "Requisitos previos" en "Configuración de HPE OO para compatibilidad con FIPS 140-2 Nivel 1" en la página 59.
2. Complete todos los pasos de "Configuración de las propiedades del archivo de seguridad Java" en "Configuración de HPE OO para que sea compatible con FIPS 140-2" en la página 62.
3. Copie el archivo **encryption.properties** del archivo **<dir instalación>\ras\var\security** a la carpeta **<dir instalación>\ras\bin**.
4. Utilizando un editor de texto, edite y cambie el archivo **encryption.properties** según convenga.

   Para obtener más información, consulte "Configuración del archivo encryption.properties y habilitación del modo FIPS" en "Configuración de HPE OO para que sea compatible con FIPS 140-2" en la página 62.
5. Guarde los cambios.
6. Abra el símbolo de la línea de comandos en la carpeta **<dir instalación>\ras\bin**.
7. Ejecute **oosh.bat**.
8. Ejecute el comando OOShell: `replace-encryption --file encryption.properties`

   Nota: Si ha copiado el archivo **encryption.properties** en otra carpeta, asegúrese de introducir la ubicación correspondiente en el comando OOShell.
9. Reinicie el servicio de RAS.

Configuración del protocolo TLS

Puede configurar HPE OO para definir la versión de protocolo TLS compatible. De forma predeterminada, HPE OO permite TLS v1, TLS v1.1 y TLS v1.2, pero esta lista se puede acotar.

Nota: SSLv3 y otras versiones de SSL no son compatibles.

1. Abra el archivo **<installation_folder>/central/tomcat/conf/server.xml**.
2. Localice el conector SSL (al final del archivo).

3. Edite el valor predeterminado de `sslEnabledProtocols`. Por ejemplo, cambie

   `sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"` por

   `sslEnabledProtocols="TLSv1.2"`

4. Reinicie el servidor.

Cómo evitar que los flujos accedan al sistema de archivos local de Central/RAS

Es necesario modificar la configuración del contenedor y los archivos java.policy de Central o RAS para evitar el acceso de los flujos al sistema de archivos local de Central o RAS, así como a recursos confidenciales.

Nota: Para explotar este escenario, un usuario necesitaría tener permisos de despliegue y de activación, además de autorización para los flujos o la potestad para autorizar flujos. Lo más probable es que los usuarios que disponen de dichos permisos sean usuarios de confianza.

Para protegerse de este escenario:

1. En el archivo de configuración del contenedor de Central o RAS (**<installation_ folder>/<ras/central>/conf/<central/ras>-wrapper.conf**), añada los parámetros `wrapper.java.additional.<nn>` de la siguiente manera:

   `wrapper.java.additional.<nn>=-Djava.security.manager`

   Sustituya <nn> por el número siguiente al último.

2. En el archivo **java.policy** (ubicado en **<installation_folder>/java/lib/security/java.policy**), añada lo siguiente. Esto permitirá el acceso a los recursos mínimos que necesita HPE OO e impedirá el acceso al sistema de archivos local de Central/RAS que contiene datos confidenciales.

```
grant codebase "file:${oo.home}/bin/-" {
                permission java.security.AllPermission;
};

grant codebase "file:${oo.home}/lib/-" {
                permission java.security.AllPermission;
};
```

```
grant codebase "file:${oo.home}/tomcat/-" {
                permission java.security.AllPermission;
};

grant codebase "file:${oo.home}/var/cache/-" {
                permission java.io.FilePermission "${oo.home}/var/logs",
"read, write";
};
```

Para permitir que el flujo acceda a los recursos del sistema de archivos local de Central/RAS, especifique lo siguiente en java.policy. Por ejemplo:

```
grant codebase "file:${oo.home}/var/cache/-" {
                permission java.io.FilePermission
"C:\\users\\cathy\\foo.bat", "read, write, execute, delete";
                permission java.io.FilePermission "C:\\users\\cathy\\-",
"read,write,execute,delete"; // Recursive Example
                permission java.io.FilePermission "C:\\users\\cathy\\*",
"read,write,execute,delete"; // Flat Example
                   .....
};
```

Hewlett Packard
Enterprise