HP Operations Orchestration

Versión de software: 10.20
Sistemas operativos Windows y Linux

Guía de protección

Fecha de publicación del documento: Noviembre de 2014
Fecha de lanzamiento del software: Noviembre de 2014

Avisos legales

Garantía

Las únicas garantías de los productos y servicios HP se exponen en el certificado de garantía que acompaña a dichos productos y servicios. El presente documento no debe interpretarse como una garantía adicional. HP no es responsable de omisiones, errores técnicos o de edición contenidos en el presente documento.

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

Leyenda de derechos limitados

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

Aviso de copyright

Avisos de marcas comerciales

Adobe™ es una marca comercial de Adobe Systems Incorporated.

Microsoft® y Windows® son marcas comerciales registradas 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.

Reconocimientos

Actualizaciones de la documentación

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

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

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

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

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

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

Soporte

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

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

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

- Buscar los documentos de la Base de conocimiento que le interesen
- Enviar y realizar un seguimiento de los casos de soporte y las solicitudes de mejora
- Descargar revisiones de software
- Gestionar contratos de soporte
- Buscar contactos de soporte de HP
- Consultar la información sobre los servicios disponibles
- Participar en debates con otros clientes de software
- Investigar sobre formación de software y registrarse para recibirla

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

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

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

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

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

Contenido

Protección de HP Operations Orchestration

Este documento describe cómo configurar la protección de seguridad para HP Operations Orchestration.

Para obtener más información sobre tareas administrativas, consulte la *Guía de administración de HP OO*.

Cláusula

Esta guía proporciona recomendaciones para salvaguardar la implementación de HP 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. Sin embargo, para proteger sus datos HP OO, es necesario proteger tanto HP OO como al entorno informático (por ejemplo, la infraestructura) en los que se ejecuta la aplicación.

Esta guía incluye recomendaciones que contribuyen a proteger HP 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.

Recomendaciones de seguridad sobre protección de sistemas

1. Instale la última versión de HP OO. Para obtener más información, consulte la *Guía de instalación de HP OO*.
2. (Opcional) Configuración de HP 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 HP OO para compatibilidad con FIPS 140-2 Nivel 1" en la página 22.
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 "Autenticación de certificado de servidor y cliente" en la página siguiente.
4. Proteger el servidor de HP OO Central eliminando el puerto HTTP y sustituyendo las contraseñas del almacén de claves y del almacén de confianza por contraseñas seguras. Consulte "Cambio o deshabilitación de puertos HTTP/HTTPS" en la página 14 y "Cambio de la contraseña del almacén de claves o del almacén de confianza" en la página 11.
5. Proteger HP OO Studio sustituyendo las contraseñas del almacén de claves y el almacén de confianza por contraseñas seguras. Consulte "Cambio de la contraseña del almacén de claves o del almacén de confianza" en la página 11.

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 14.
7. (Opcional) Configurar la versión del protocolo TLS. Consulte "Configuración del protocolo TLS" en la página 28.
8. Habilitar la autenticación en Central. Consulte "Habilitación de autenticación" en la *Guía del usuario de HP 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 HP 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: trabajadores" en *Guía del usuario de HP OO Central*.
11. En los entornos Windows y SQL server, configure HP OO para que funcione con autenticación Windows. Consulte "Configuración de HP OO para que funcione con autenticación Windows" en la *Guía de base de datos de HP 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 HP OO Central*.

Autenticación de certificado de servidor y 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.

HP OO usa la utilidad Keytool para gestionar claves criptográficas y certificados de confianza. Esta utilidad está incluida en la carpeta de instalación de HP OO, en **<installation dir>/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 HP OO Central incluyen dos archivos para la gestión de certificados:

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

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

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 **<installation dir>/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 del 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:** 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 <certificate_name> -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.

   ```
   c:\Program Files\Hewlett-Packard\oo-saml\central\var\security>keytool -list -keystore server.pfx -v -storetype PKCS12
   Enter keystore password:

   Keystore type: PKCS12
   Keystore provider: SunJSSE

   Your keystore contains 1 entry

   Alias name: le-775fb32c-269c-499b-bae8-fe7077479ec6
   Creation date: 24/04/2014
   Entry type: PrivateKeyEntry
   Certificate chain length: 2
   ```

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

   ```
   keytool -importkeystore -srckeystore <PKCS12 format certificate path> -destkeystore key.store -srcstoretype pkcs12 -deststoretype JKS -alias <cert alias> -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 de la contraseña del almacén de claves o del almacén de confianza" en la página 11.

   Se recomienda cambiar la contraseña predeterminada “changeit” en el almacén de claves generado automáticamente del servidor de Central. Consulte "Cambio de la contraseña del almacén de claves o del almacén de confianza" en la página 11.

8. 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 certificados

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

De forma predeterminada, HP 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 **<installation dir> ras/conf/ras-wrapper.conf** y establezca el valor `-Dssl.support-self-signed` 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 **<installation dir> ras/conf/ras-wrapper.conf** y establezca el valor `-Dssl.verifyHostName` en **true**. Ello verificará que el FQDN del certificado coincide con el FQDN de la solicitud.

   Por ejemplo:

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

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 <any_alias> -keystore client.truststore -file
   <certificate_name.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, HP 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. Establezca el valor `-Dssl.support-self-signed` en **false**. Esto habilita la entidad certificadora (CA) de certificados raíz de confianza.

   Por ejemplo:

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

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

   Por ejemplo:

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

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 <any_alias> -keystore client.truststore -file
   <certificate_name.cer> -storepass <changeit>
   ```

6. Ejecute OOSH.
7. Inicie Central.

Importación de un certificado raíz de CA en el almacén de confianza del depurador de estudio

Si está utilizando un certificado raíz personalizado para Studio, deberá importar la entidad certificadora (CA) de certificados raíz de confianza en el 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, HP 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 Studio y realice una copia de seguridad del archivo **client.truststore** original, ubicado en **<dir instalación>/studio/var/security/client.truststore**.
2. Edite el archivo **Studio.l4j.ini** en **<installation dir>/studio**.
3. Establezca el valor `-Dssl.support-self-signed` en **false**. Esto habilita la entidad certificadora (CA) de certificados raíz de confianza.

Por ejemplo:

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

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

   Por ejemplo:

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

5. Importe la autoridad de certificado raíz de confianza (CA) en el archivo de Studio **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 <any_alias> -keystore client.truststore -file
   <certificate_name.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 de la contraseña del almacén de claves o del 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 una contraseña, consulte "Cifrado de contraseñas" en la *Guía de administración de HP OO*.

   En OOSH, ejecute el siguiente comando:

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

   en 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.
4. Cambie también las contraseñas en el archivo **server.xml** que se encuentra en **<installation dir>/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"/>
   ```

   b. 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.
   c. Guarde el archivo.
5. Editar el archivo **central-wrapper.conf** que se encuentra en **<installation dir>central\conf\central-wrapper.conf** y cambiar:

   ```
   wrapper.java.additional.<x>=-Djavax.net.ssl.trustStorePassword=changeit
   ```

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 el parámetro `changeit` del almacén de confianza.
- **Para cambiar la contraseña del almacén de confianza de OOSH**: Edite el archivo **oosh.bat** y cambie el parámetro `changeit` del almacén de confianza.
- **Para cambiar la contraseña del almacén de confianza de Studio**: Edite el archivo **<installation dir>/studio/Studio.l4j.ini** y sustituya el parámetro `changeit` del almacén de confianza por la nueva contraseña en formato ofuscado.

  Para obtener más información sobre cómo ofuscar una contraseña, consulte la sección "Ofuscar las contraseñas" en la *Guía de administración de HP OO*.

Ocultación de las contraseñas del almacén de confianza y del almacén de claves de Studio

En HP 10.20 y posterior, las contraseñas del almacén de claves y el almacén de confianza se encuentran ocultas. Tras actualizar de 10.10 a 10.20, estas contraseñas solo se ocultarán si se dejan sin cambiar en el archivo **<install_dir>/studio/Studio.l4j.ini**. Toda otra contraseña que se haya cambiado en versiones anteriores no se ocultará automáticamente durante la actualización.

Si desea cambiar la contraseña del almacén de confianza, puede hacerlo en el archivo **Studio.l4j.ini** en formato oculto o en texto sin formato. Una vez que se hayan cambiado las contraseñas, tendrá que ocultarlas de forma manual para garantizar que no se muestren en texto sin formato en el Administrador de tareas del proceso de Studio:

1. Cierre Studio.
2. Localice el script **encrypt-password** en **<installation_folder>/central/bin**.
3. Oculte la contraseña personalizada emitiendo el siguiente comando:

   ```
   encrypt-password.bat --obfuscate <your password>
   ```

4. Cambie las contraseñas del archivo **<install_dir>/studio/Studio.l4j.ini** para los siguientes parámetros:

   ```
   -Djavax.net.ssl.keyStorePassword={OBFUSCATED}<obfuscated_password>
   -Djavax.net.ssl.trustStorePassword={OBFUSCATED}<obfuscated_password>
   ```

5. Cambie las contraseñas del almacén de claves y del almacén de confianza de estudio con ayuda de la utilidad keytool de la carpeta **<install_dir>/studio/var/security/**.

Nota: Si el certificado de cliente no está configurado para Studio Remote Debugger, el argumento de la ruta del almacén de claves se ignorará.

6. Inicie Studio.

¡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`.

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 HP 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 HP OO 10.x, repita estos pasos.

Cambio o deshabilitación de puertos HTTP/HTTPS

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 **puerto** 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 de un puerto

Por ejemplo, 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.

Para deshabilitar 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 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 <any_alias> -keystore client.truststore -file
   <certificate_name.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:\HP\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:/HP/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 "Autenticación de certificado de servidor y cliente" en la página 6.

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**: **<installation dir>/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 <any_alias> -keystore <path>/client.truststore -file
   <certificate_path> -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`.

   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
MTIwMTAwWjAiMCACAScXDTk5MDEwMTEyMDAwMFowDDAKBgNVHRUEAwoBAaAjMCEw
CgYDVR0UBAMCAQEwEwYDVR0jBAwwCoAIq5rr+cLnVI8wDQYJKoZIhvcNAQEFBQAD
gYEAC7lqZwejJRW7QvzH11/7cYcL3racgMxH3PSU/ufvyLk7ahR++RtHary/WeCv
RdyznLiIOA8ZBiguWtVPqsNysNn7WLofQIVa+/TD3T+lece4e1NwGQvj5Q+e2wRt
GXg+gCuTjTKUFfKRnWz7O7RyiJKKim0jtAF4RkCpLebNChY=
-----END X509 CRL-----
```


6. 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 HP 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 HP OO.

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 8.

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

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

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

```
wrapper.java.additional.<x>=-Djavax.net.ssl.keyStorePassword=changeit
```

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

4. Inicie el servidor de RAS.

Nota importante: 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 *HP OO Central User Guide*.

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 en el almacén de confianza del depurador de estudio" en la página 10.

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

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

```
-Djavax.net.ssl.keyStore="<installation
dir>/studio/var/security/certificate.p12"
```

```
-Djavax.net.ssl.keyStorePassword=changeit
```

```
-Djavax.net.ssl.keyStoreType=PKCS12
```

4. Inicie Studio.

Notas:

- En HP OO 10.20 y posterior, el parámetro `keyStorePassword` en **Studio.l4j.ini** está ofuscado de forma predeterminada si la contraseña se mantenía como valor predeterminado. Puede cambiar este parámetro y almacenarlo en texto no cifrado u ofuscado.
- 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 HP 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 HP 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 9.

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="<installation dir>/var/security/certificate.p12"
   -Djavax.net.ssl.keyStorePassword=changeit
   -Djavax.net.ssl.keyStoreType=PKCS12
   ```

4. Inicie OOSH.

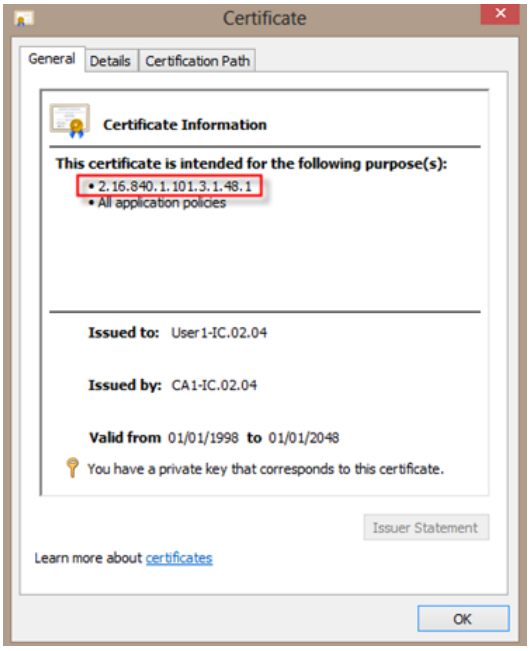
Nota: Para el certificado de cliente, debe definir un usuario, ya sea un usuario interno o un usuario LDAP. El nombre del usuario debe definirse en los atributos de certificado. El valor predeterminado es el atributo de CN. Consulte la sección Procesamiento de certificado principal para obtener más información.

Tenga en cuenta que incluso si HP 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 HP OO.

Procesamiento de directivas de certificado

HP 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.
- HP 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 HP OO, consulte la *HP 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 HP OO (LDAP o usuario interno).
- Para cambiar la expresión regular, cambie el elemento de configuración: `x509.subject.principal.regex`.

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

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

Esta sección explica cómo configurar HP 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.

Una vez configurado HP OO para ser compatible con FIPS 140-2, HP OO utiliza el siguiente algoritmo de seguridad:

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

HP OO usa el proveedor de seguridad: Software RSA BSAFE Crypto versión 6.1. Es el único proveedor de seguridad compatible con FIPS 140-2.

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

Requisitos previos

Nota: Si se realiza una actualización a partir de una instalación de HP OO 10.10 (y posterior) previamente configurada con FIPS, repita los pasos 4 y 5 siguientes y, a continuación, repita los pasos de la sección "Configuración de las Propiedades del archivo Java de seguridad" contenidos en "Configuración de HP OO para que sea compatible con FIPS 140-2" en la página 24.

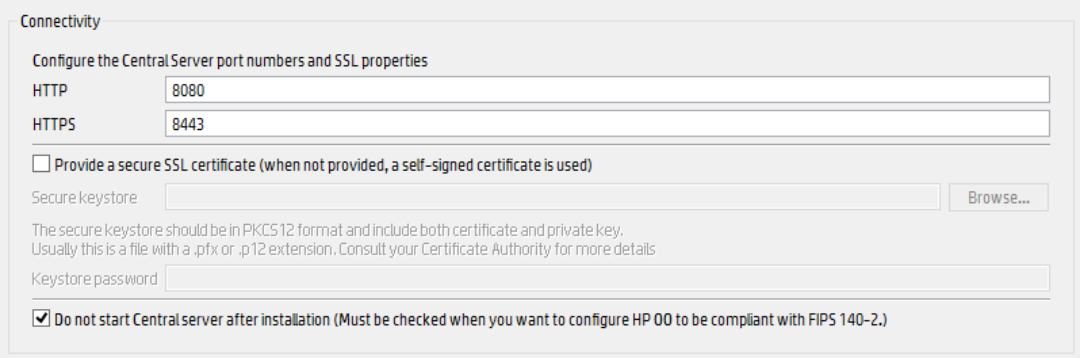
Antes de configurar HP OO para ser compatibles con FIPS 140-2, realice los pasos siguientes:

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

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

   No es posible configurar instalaciones de HP OO que se encuentren en uso (tanto las 9.x como las 10.x).
2. Compruebe que cuando se instaló HP 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 **Connectivity**, se ha seleccionado el cuadro de

verificación **Do not start Central server after installation**.



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**
   - **<oo_jre>\lib\security** (en donde **<oo_jre>** es el directorio en el que está instalado el JRE usado por HP OO. De forma predeterminada, es **<dir instalación>\java**)
4. Descargue e instale Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction Policy Files del siguiente sitio: http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html.

   Nota: Consulte el archivo **ReadMe.txt** del contenido descargado para obtener información sobre cómo implementar los archivos y actualizar el JRE usado por HP OO.
5. Instale los archivos de software RSA BSAFE Cripto. En el sistema donde está instalado HP OO, copie lo siguiente en **<oo_jre>\lib\ext** (en donde **<oo_jre>** es el directorio donde está instalado el JRE usado por HP OO. De forma predeterminada, es **<dir instalación>\java**).
   - **<dir instalación>\central\lib\cryptojce-6.1.jar**
   - **<dir instalación>\central\lib\cryptojcommon-6.1.jar**
   - **<dir instalación>\central\lib\jcmFIPS-6.1.jar**

Nota: Si se realiza una actualización a partir de una instalación de HP OO 10.10 (y posterior) previamente configurada con FIPS, repita los pasos 4 y 5 de la sección "Requisitos previos" anterior y, a continuación, repita los pasos de la sección "Configuración de las Propiedades del archivo Java de seguridad" contenidos en "Configuración de HP OO para que sea compatible con FIPS 140-2" en la página siguiente.

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

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

- Configurar las propiedades del archivo Java de seguridad
- Configuración del archivo encryption.properties y habilitación del modo FIPS
- Creación de un cifrado para HP OO compatible con FIPS
- Volver a cifrar la contraseña de la base de datos con el nuevo cifrado
- Iniciar HP 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 HP OO 10.10 sustituye completamente los archivos instalados de JRE. Por lo tanto, los pasos siguientes deben realizarse después de la actualización a 10.10.

Nota: Si se realiza una actualización a partir de una instalación de HP OO 10.10 (y posterior) previamente configurada con FIPS, repita los pasos 4 y 5 de la sección "Requisitos previos" en "Configuración de HP OO para compatibilidad con FIPS 140-2 Nivel 1" en la página 22 y, a continuación, repita los pasos contenidos aquí.

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 **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 **archivo java.security**.

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

Configuración del archivo encryption.properties y habilitación del modo FIPS

El archivo de propiedades de cifrado de HP 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 **<installation dir>\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 HP OO compatible con FIPS

Para crear o sustituir el archivo de almacenamiento de cifrado de HP 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 de la contraseña del almacén de claves o del almacén de confianza" en la página 11.

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

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 HP OO*, en "Cambio de la contraseña de la base de datos".

Iniciar HP OO

Inicie HP OO como se describe en la *Guía de instalación de HP OO*.

Sustitución del cifrado FIPS

HP OO, Central y RAS cumplen con el estándar para procesamiento de información federal 140-2 (FIPS 140-2) que define los requisitos técnicos para ser usado por Agencias Federales que especifiquen sistemas de seguridad criptográficos para la protección de datos confidenciales o valiosos.

Tras una nueva instalación de HP OO 10.10, tendrá la opción de 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

1. Vaya a **<Carpeta de instalación de Central>/var/security**.
2. Haga una copia de seguridad y elimine el archivo **encryption_repository**.
3. Vaya a **<Central installation folder>/bin**.
4. Ejecute el script **generate-keys**.

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

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 HP OO para compatibilidad con FIPS 140-2 Nivel 1" en la página 22.
2. Complete todos los pasos de "Configuración de las propiedades del archivo de seguridad Java" en "Configuración de HP OO para que sea compatible con FIPS 140-2" en la página 24.
3. Copie el archivo **encryption.properties** del archivo **<installation dir>\ras\var\security** a la carpeta **<installation dir>\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 HP OO para que sea compatible con FIPS 140-2" en la página 24.
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 HP OO para definir la versión de protocolo TSL compatible. De forma predeterminada, HP 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.


Java™
COMPATIBLE