HP Operations Orchestration

Para Windows y Linux:

Versión de software: 10.10

Guía de configuración y protección del sistema

Fecha de publicación del documento: Mayo de 2014

Fecha de lanzamiento del software: Mayo 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.

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

AMD y el símbolo de flecha de AMD son marcas comerciales de Advanced Micro Devices, Inc.

Google™ y Google Maps™ son marcas comerciales de Google Inc.

Intel®, Itanium®, Pentium® e Intel® Xeon® son marcas comerciales de Intel Corporation en Estados Unidos y en otros países.

Java es una marca comercial registrada de Oracle o sus afiliados.

Microsoft®, Windows®, Windows NT®, Windows® XP y Windows Vista® son marcas comerciales registradas estadounidenses de Microsoft Corporation.

Oracle es una marca comercial registrada de Oracle Corporation y/o sus empresas afiliadas.

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

Actualizaciones de la documentación

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

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

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

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

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

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

Soporte

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

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

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

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

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

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

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

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

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

Contenido

Configuración y protección del sistema

Este documento describe cómo configurar y proteger HP Operations Orchestration.

Autenticación de certificado de servidor y cliente

Los certificados Secure Socket Layer (SSL)/Transport Layer Security (TLS) vinculan digitalmente una clave criptográfica a los detalles de una organización, lo cual permite conexiones seguras 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.

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 de HP OO.

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

Autenticación del certificado de servidor

Sustitución del certificado de servidor SSL/TLS de Central

Puede usar un certificado firmado por una empresa reconocida o un certificado de servidor personalizado.

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.key> -out <certificate name>.p12 –name <name>
   ```

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

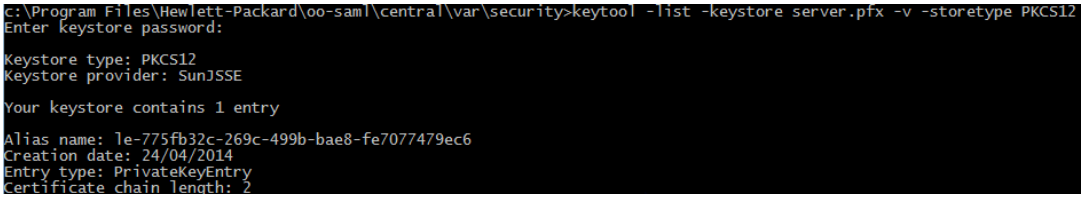
   ```
   >openssl pkcs12 –inform DER –export –in <cert.pem> -inkey <.key> -out <certificate name>.p12 –name <name>
   ```

   Nota: Anote la contraseña proporcionada. La necesitará para la clave privada al introducir más adelante la frase de contraseña en el procedimiento.

5. Extraiga los alias de los alias de certificados usando el comando siguiente:

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

   El alias se mostrará en la pantalla. En el ejemplo siguiente es la cuarta línea por abajo.



6. Importe el certificado de servidor en formato PKCS12 en el archivo **key.store**:

   keytool -importkeystore -srckeystore <PKCS12 format certificate path> -destkeystore key.store -srcstoretype pkcs12 -deststoretype JKS -alias <cert alias> -destalias tomcat

7. 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.

Sustitución del certificado de servidor SSL/TLS de Central con un certificado autofirmado

Puede generar un certificado autofirmado mediante la utilidad keytool.

Nota: Tras actualizar a HP OO 10.10:

- Si el nuevo Central está instalado en el mismo equipo que la instalación anterior, puede utilizar el certificado autofirmado existente.
- Si los nuevos Central están instalados en diferentes equipos, tendrá que generar un nuevo certificado autofirmado para cada uno de ellos incluso si disponía de un certificado para las versiones anteriores.

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

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

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. Genere un certificado autofirmado:

   ```
   keytool -genkey -alias tomcat -keyalg RSA -keypass <changeit >-keystore
   <path/for/new/Keystore> -storepass <changeit>-storetype pkcs12 -dname
   "CN=<CENTRAL_FQDN>, OU=<ORGANIZATION_UNIT>, O=<ORGANIZATION>, L=<LOCALITY>,
   C=<COUNTRY>"
   ```

   Nota: Si no introduce una ruta para generar el nuevo almacén de claves, se creará en la carpeta donde se haya introducido el comando, por ejemplo **<installation dir>/central/var/security**.

5. Importe el certificado autofirmado al archivo **key.store** de Central:

   ```
   keytool -v -importkeystore -srckeystore <new/path/created/Keystore> -
   srcstoretype PKCS12 -srcstorepass <changeit> -destkeystore key.store -
   deststoretype JKS -deststorepass <changeit>
   ```

6. Inicie Central.

Importación de 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 está utilizando un certificado raíz firmado estándar, no es necesario que realice el siguiente procedimiento porque el certificado ya está 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 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 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 **<dir instalación> ras/conf/ras-wrapper.conf** y establezca el valor `-Dssl.verifyHostName` en **true**. Verificará el nombre de host.

   Por ejemplo:

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

5. Importe la entidad certificadora (CA) de certificados raíz de confianza en el archivo **client.truststore** de RAS:

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

6. Inicie RAS.

Importación de un certificado 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 está utilizando un certificado raíz firmado estándar, no es necesario que realice el siguiente procedimiento porque el certificado ya está 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 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**. Verificará el nombre de host.

   Por ejemplo:

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

5. Importe la entidad certificadora (CA) de certificados raíz de confianza en el archivo **client.truststore** de Central:

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

6. Ejecute OOSH.

Importación de un certificado en el almacén de confianza del depurador de Studio

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

está utilizando un certificado raíz firmado estándar, no es necesario que realice el siguiente procedimiento porque el certificado ya está 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 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**. Verificará el nombre de host.

   Por ejemplo:

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

5. Importe la entidad certificadora (CA) de certificados raíz de confianza en el archivo **client.truststore** de Studio:

   ```
   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

- **Para cambiar la contraseña de Central**:

  a. Edite el archivo **server.xml** que se encuentra en **<dir_ instalación>/central/tomcat/conf/server.xml**.

b. 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" truststoreFile="C:/Program
Files/Hewlett-Packard/HP Operations
Orchestration/central/var/security/client.truststore"
truststorePass="changeit" truststoreType="JKS"/>
```

c. Cambie la contraseña correspondiente.

- `keyPass`: la contraseña utilizada para acceder al certificado de servidor desde el archivo del almacén de claves especificado. El valor predeterminado es "`changeit`".
- `keystorePass`: la contraseña utilizada para acceder al archivo del almacén de claves especificado. El valor predeterminado es el valor del atributo `keyPass`.
- `truststorePass`: la contraseña para acceder al almacén 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 una vez al almacén de confianza sin contraseña, omitiendo la validación del contenido del almacén de confianza.

d. Guarde el archivo.

e. Abra el archivo **central-wrapper.conf**, ubicado en **central/conf** y cambie:

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

f. Reinicie Central.

- **Para cambiar la contraseña del almacén de confianza 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 cambie el parámetro `changeit` de este almacén de confianza.

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. Edite la propiedad **jdk.tls.disabledAlgorithms** para deshabilitar el cifrado RC4.

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

Cambio o cierre 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" truststoreFile="C:/Program Files/Hewlett-
Packard/HP Operations Orchestration/central/var/security/client.truststore"
truststorePass="changeit" truststoreType="JKS"/>
```

De forma predeterminada, ambos están habilitados.

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 **redirectPort** para el conector HTTP.

3. Guarde el archivo.
4. Reinicie Central.

Deshabilitación de un puerto

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. Guarde el archivo.
4. Reinicie Central.

Autenticación de certificado de cliente (autenticación mutua)

La autenticación de certificado X.509 suele utilizarse para verificar la identidad de un servidor al usar SSL/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 puede usar SSL/TLS con la autenticación mutua. El servidor solicita un certificado válido al cliente como parte del intercambio de señales SSL/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 SSL/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 SSL solicite una cadena de certificados válidos al cliente antes de aceptar una conexión. Establezca el atributo en `want` si desea que la pila SSL solicite un certificado de cliente, pero que no se produzca un error en caso de no presentarse. 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 servicio de Central.
2. Importe el certificado raíz adecuado (CA) en Central **client.truststore**: **<dir instalación>/central/var/security/client.truststore**, 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. Añada el atributo `crlFile` a fin de definir la lista de revocación de certificados para la validación de certificados SSL/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 almacén de confianza RAS" en la página 9.

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 **<dir instalación>ras/var/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, que 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 en el almacén de confianza del depurador de Studio" 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.

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.

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 en el almacén de confianza de OOSH" en la página 10.

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.

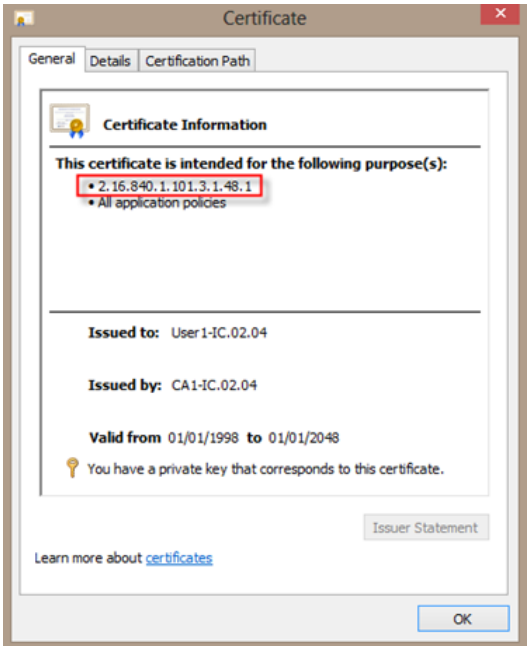
Tenga en cuenta que incluso si HP OO se ha configurado con múltiples configuraciones de LDAP, solo se puede autenticar al usuario utilizando los atributos de certificado cliente con el LDAP predeterminado. Central intentará primero autenticar al usuario con el LDAP predeterminado y, si no es posible,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



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`.

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"/>
```

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

Estándar federal de procesamiento de información (FIPS)

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

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

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: AES
- Algoritmo hash: SHA1

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 23.

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

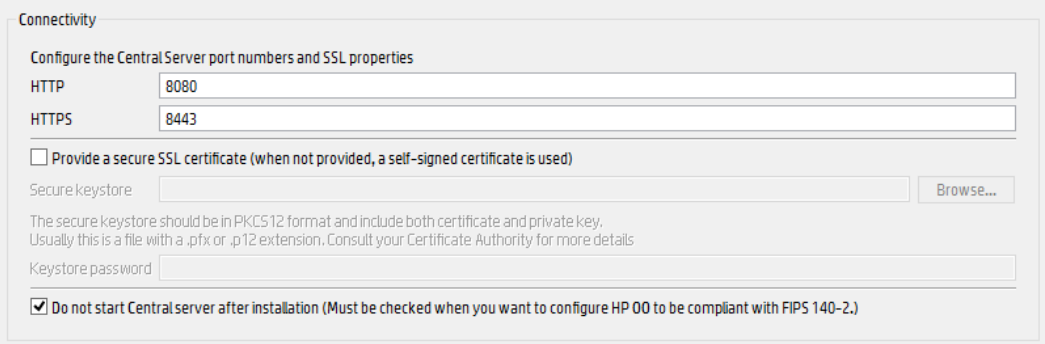
Nota: Para ser compatible con FIPS140-2, es necesario desactivar LWSSO.

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 si son 9.x como 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 **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**
   - **<oo_jre>\lib\security** (donde **<oo_jre>** es el directorio en el que está instalado el JRE usado por HP OO. De forma predeterminada, es **<installation dir>\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** (donde **<oo_jre>** es el directorio donde está instalado el JRE usado por HP OO. De forma predeterminada, es **<installation dir\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" abajo.

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:

- Configure 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
- Sustitución de la contraseña de la base de datos
- Inicio de HP OO

Configuración de 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 "Estándar federal de procesamiento de información (FIPS)" en la página 21 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 en dos, para todos los proveedores incluidos en la enumeración, en el formato **security.provider.<nn>=<provider_name>**, el número de orden de preferencia `<nn>`.

   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" abajo.

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 del almacén de confianza de HP OO. (el almacén de confianza del cliente se encuentra en <installation>/central/var/security.)

Sustitución de la contraseña de la base de datos

Sustituya la contraseña de la base de datos tal como se describe en "Cambio de la contraseña de la base de datos" en la página 30.

Inicio de 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 el algoritmo de cifrado FIPS.

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

Cambio del algoritmo 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 "Estándar federal de procesamiento de información (FIPS)" en la página 21.
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 23.
3. Copie el archivo **encryption.properties** de la carpeta `<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 HP OO para que sea compatible con FIPS 140-2" en la página 23.
5. Guarde los cambios.
6. Obra 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 de los parámetros de LWSSO

Al instalar HP OO 10.10, si decide actualizar la configuración LWSSO en HP OO 9.x, se migrará dicha configuración LWSSO, si bien LWSSO se deshabilitará en HP OO 10.10 incluso si se encontraba habilitado anteriormente en HP OO 9.x.

Al habilitar LWSSO posteriormente, es posible que reciba advertencias en determinados casos. Para borrar las advertencias del registro, siga los pasos que se enuncian a continuación para ajustar la propiedad de URL de gestión con ayuda del nombre de dominio completo.

- Si Central y RAS se encuentran instalados en un mismo equipo y la configuración de LWSSO está habilitada, la propiedad URL de gestión debe establecerse utilizando el nombre de dominio completo.

  a. Detenga el proceso del RAS.

  b. En el archivo **ras/conf/ras-wrapper.conf**, cambie

     ```
     wrapper.java.additional.<x>=-Dmgmt.url=<protocol>://localhost:<port>/oo
     ```

     a

     ```
     wrapper.java.additional.<x>=-
     Dmgmt.url=<protocol>://<FullyQualifiedDomainName>:<port>/oo
     ```

  c. Inicie el proceso del RAS.

- Si el RAS se encuentra instalado en un equipo distinto del de Central y la configuración LWSSO está habilitada, debe especificar la URL de gestión de Central con el nombre de dominio completo durante la instalación del RAS, en lugar de con la dirección IP.

- Si conecta otra aplicación a Central mediante LWSSO, debe especificar la URL de gestión de Central con el nombre de dominio completo.

  a. Detenga el proceso de Central.

  b. En el archivo **central/conf/central-wrapper.conf**, cambie

     ```
     wrapper.java.additional.<x>=-Dmgmt.url=<protocol>://localhost:<port>/oo
     ```

     a

```
wrapper.java.additional.<x>=-
Dmgmt.url=<protocol>://<FullyQualifiedDomainName>:<port>/oo
```

c. Inicie el proceso de Central.

Configuración de la directiva XSS

HP OO tiene protección de XSS con AntiSamy. La directiva de protección predeterminada es "antisamy", la cual permite la mayoría de elementos HTML y puede ser útil cuando los usuarios envían páginas HTML completas.

Esta directiva es configurable en una de las directivas compatibles por AntiSamy. Para obtener más información, consulte

https://www.owasp.org/index.php/Category:OWASP_AntiSamy_Project#Stage_2_-_Choosing_a_base_policy_file

La directiva es configurable mediante una propiedad de configuración del sistema llamada `xss.policy`. Entre los valores posibles se incluye: antisamy (predeterminado), antisamy-slashdot, antisamy-myspace, antisamy-ebay, antisamy-anythinggoes, antisamy-tinymc.

Para comprobar si la directiva esté configurada, vaya a **https://host/oo/reports/sysinfo** y busque el parámetro `xss.policy` en la sección **configuración del sistema**.

La forma más sencilla de cambiar la directiva Slashdot predeterminada es mediante la utilidad shell de HP Operations Orchestration.

1. Haga doble clic en el archivo por lotes `oosh.bat` para iniciar la utilidad OOSH.
2. En la línea de comandos, escriba, por ejemplo:

```
ssc --url https://host/oo --key  xss.policy --value antisamy-anythinggoes
```

Para obtener más información sobre la utilidad Shell de HP Operations Orchestration, consulte *HP Operations Orchestration Shell User Guide*.

Configuración de la localización

Configuración de la configuración regional del sistema en Central-wrapper.conf

Si el sistema HP OO está localizado, deberá establecer las siguientes propiedades para que reflejen la configuración regional del sistema, en el archivo **central-wrapper.conf**:

```
set.LANG=

set.LC_ALL=

set.LANGUAGE=
```

```
wrapper.java.additional.<x>=-Duser.language=
wrapper.java.additional.<x>=-Duser.country=
```

Por ejemplo, para Japonés: `set.LANG=ja_JP` y `set.LC_ALL=ja_JP`

Configuración del sistema

Cambio de la contraseña de la base de datos

1. Si Central se está ejecutando, detenga el servicio de Central.
2. Ejecute el script encrypt-password con la opción -e -p <contraseña>, donde contraseña es la contraseña de la base de datos.
3. Copie el resultado, debe aparecer como sigue:

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

4. Vaya a la carpeta **<Carpeta de instalación de Central>/conf** y abra el archivo **database.properties**.
5. Cambie el valor `db.password` con el valor que se ha copiado.

Cambio de la IP de la base de datos

Esta sección es importante cuando es necesario configurar HP OO para que funcione con otra instancia de base de datos. Todos los parámetros de base de datos, como las credenciales de base de datos, nombre de esquema, tablas, etc., deben ser idénticos.

1. Edite el archivo **\HP Operations Orchestration\\conf central\database.properties.**
2. Busque el parámetro `jdbc.url`. Por ejemplo:

   ```
   jdbc.url=jdbc\:jtds\:sqlserver\://16.60.185.109\:1433/schemaName;sendStringP
   arametersAsUnicode\=true
   ```

3. Cambie la dirección IP\FQDN del servidor de base de datos.
4. Guarde el archivo.
5. Reinicie Central.

Ajuste de los niveles de registro

Es posible ajustar la granularidad de la información que se proporciona en el registro, por separado para registros normales, implementación y ejecución.

Las opciones de granularidad son las siguientes:

- `INFO`: Información de registro predeterminada
- `DEBUG`: Más información de registro

- `ERROR/WARNING`: Menos información de registro

Para ajustar la granularidad en el registro:

1. Abra el archivo **log4j.properties** (en **/<oo-installation>/central/conf/log4j.properties**).
2. Sustituya `INFO` con `DEBUG` o `ERROR/WARNING` en la siguiente ubicación en el archivo **log4j.properties**.

   Por ejemplo:

```
log.level=INFO
execution.log.level=DEBUG
deployment.log.level=DEBUG
```

Ajuste del tiempo de trabajos Quartz

En el sistema HP OO, se ejecutan periódicamente trabajos Quartz para el mantenimiento del sistema.

Cada trabajo se ejecuta durante un tiempo y se repite a intervalos. A continuación, se muestran ejemplos de desencadenadores de trabajos:

Nombre del desencadenador	Intervalo de repetición actual	Qué sucede
onRolling:OO_EXECUTION_STATES_Trigger	4,5 minutos	Listado de tabla de estados para la depuración
queueCleanerTrigger	1 minuto	Depuración de las tablas de cola
queueRecoveryTrigger	2 minutos	Comprueba si el sistema necesita recuperación
recoveryVersionTrigger	0,5 minutos	Contador de version que debe utilizarse para la recuperación
splitJoinTrigger	1 segundo	Une las divisiones finalizadas
onRolling:OO_EXECUTION_EVENTS_Trigger **Nota:** Este desencadenador ha quedado obsoleto.	12 horas	Listado de tabla de eventos para la depuración

Si desea ajustar el tiempo de estos trabajos para mejorar el rendimiento, realice las siguientes acciones:

Nota: Todo ajuste que se realice al tiempo puede afectar al sistema notablemente. Consulte con su representante de servicio HP antes de realizar cambios a estos desencadenadores.

1. Vaya a la página Jminix con la dirección URL: **{OO_HOST}:{OO_PORT}/oo/jminix/**

   Nota: Necesita permiso **Gestionar configuración del sistema** para ir a **jminix**.

2. Abra la ficha OO. En **MBeans** hay una operación llamada **jobTriggersMBean**.

3. Utilice esta operación e introduzca los valores en la ficha de la derecha y use el nombre del desencadenador que desea cambiar. Utilice exactamente el mismo nombre que la tabla, con el nuevo valor del intervalo de repetición.

Se cambiarán los tiempos de desencadenamiento del trabajo.

Nota: El mecanismo de persistencia de eventos ha quedado obsoleto (consulte **onRolling:OO_EXECUTION_EVENTS_Trigger**). Puede configurar este trabajo si usa el Depurador remoto o si activa el indicador **events.persistency**. Consulte "Activación del mecanismo de registro de eventos" en la página siguiente.

Cambio de la dirección URL de Central/equilibrador de carga en el RAS

Se recomienda configurar la dirección URL de Central/equilibrador de carga mediante el instalador, pero si necesita para realizar cambios en la dirección URL una vez instalado el RAS, puede editar el archivo **ras-wrapper.conf**.

Por ejemplo, sería necesario si hubiera instalado un RAS contra Central/equilibrador de carga y el FQDN de Central/equilibrador de carga hubiese cambiado. Debería cambiar la dirección URL de Central/equilibrador de carga a nivel del RAS para que pudiera volver a comunicarse con Central/equilibrador de carga.

1. Detenga el RAS.

2. Abra el archivo **ras-wrapper.conf**, que se encuentra en **<carpeta de instalación>\ras\conf**.

3. Edite la dirección URL en la siguiente línea:

   ```
   wrapper.java.additional.<x>=-Dmgmt.url=http://localhost:8080/oo
   ```

4. Reinicie el RAS.

Activación del mecanismo de registro de eventos

El mecanismo de registro de eventos ha quedado obsoleto en HP OO 10.10 y se eliminará en una próxima versión.

HP OO se ha implementado sin el mecanismo de registro de eventos. No obstante, si desea utilizar este mecanismo, puede activar el indicador **events.persistency**. Tenga en cuenta que para escenarios de agrupaciones en clúster y para mejorar el rendimiento, se recomienda dejar el indicador desactivado.

Para activar este indicador:

1. Detenga el proceso y actualice el archivo **wrapper.conf** en cada nodo (Central/RAS) de su sistema.

   En Central, vaya a **<installation_path>\central\conf\central-wrapper.conf**

   En RAS, vaya a **<installation_path>\ras\conf\ras-wrapper.conf**

2. En el archivo **wrapper.conf**, busque el parámetro **-Devents.persistency** y cambie el valor a **true**.

3. Reinicie el proceso.


Java™
COMPATIBLE