HP Operations Orchestration

Für Windows und Linux

Softwareversion: 10.10

Systemkonfigurations- und Optimierungshandbuch

Datum der Dokumentveröffentlichung: Mai 2014

Datum des Software-Release: Mai 2014

Rechtliche Hinweise

Garantie

Die Garantiebedingungen für Produkte und Services von HP sind in der Garantieerklärung festgelegt, die diesen Produkten und Services beiliegt. Keine der folgenden Aussagen kann als zusätzliche Garantie interpretiert werden. HP haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.

Eingeschränkte Rechte

Vertrauliche Computersoftware. Gültige Lizenz von HP für den Besitz, Gebrauch oder die Anfertigung von Kopien erforderlich. Entspricht FAR 12.211 und 12.212. Kommerzielle Computersoftware, Computersoftwaredokumentation und technische Daten für kommerzielle Komponenten werden an die US-Regierung per Standardlizenz lizenziert.

Copyright-Hinweis

Markenhinweise

Adobe™ ist eine Marke von Adobe Systems Incorporated.

Dieses Produkt enthält eine Schnittstelle der freien Programmbibliothek zum Komprimieren, 'zlib', geschützt durch Copyright © 1995-2002 Jean-loup Gailly und Mark Adler.

AMD und das AMD-Pfeilsymbol sind Marken von Advanced Micro Devices, Inc.

Google™ und Google Maps™ sind Marken von Google Inc.

Intel®, Itanium®, Pentium® und Intel® Xeon® sind Marken der Intel Corporation in den USA und anderen Ländern.

Java ist eine eingetragene Marke von Oracle und/oder ihrer Tochtergesellschaften.

Microsoft®, Windows®, Windows NT®, Windows® XP und Windows Vista® sind in den USA eingetragene Marken der Microsoft Corporation.

Oracle ist eine eingetragene Marke von Oracle Corporation und/oder ihrer Tochtergesellschaften.

UNIX® ist eine eingetragene Marke von The Open Group.

Aktualisierte Dokumentation

Auf der Titelseite dieses Dokuments befinden sich die folgenden identifizierenden Informationen:

- Software-Versionsnummer, die Auskunft über die Version der Software gibt.
- Datum der Dokumentveröffentlichung, das bei jeder Änderung des Dokuments ebenfalls aktualisiert wird.
- Datum des Software-Release, das angibt, wann diese Version der Software veröffentlicht wurde.

Unter der unten angegebenen Internetadresse können Sie überprüfen, ob neue Updates verfügbar sind, und sicherstellen, dass Sie mit der neuesten Version eines Dokuments arbeiten: **http://h20230.www2.hp.com/selfsolve/manuals**

Für die Anmeldung an dieser Website benötigen Sie einen HP Passport. Hier können Sie sich für eine HP Passport-ID registrieren: **http://h20229.www2.hp.com/passport-registration.html**

Alternativ können Sie auf den Link **New user registration** (Neuen Benutzer registrieren) auf der HP Passport-Anmeldeseite klicken.

Wenn Sie sich beim Support-Service eines bestimmten Produkts registrieren, erhalten Sie ebenfalls aktualisierte Softwareversionen und überarbeitete Ausgaben der zugehörigen Dokumente. Weitere Informationen erhalten Sie bei Ihrem HP-Kundenbetreuer.

Support

Besuchen Sie die HP Software Support Online-Website von HP unter: **http://www.hp.com/go/hpsoftwaresupport**

Auf dieser Website finden Sie Kontaktinformationen und Details zu Produkten, Services und Support-Leistungen von HP Software.

Der Online-Support von HP Software bietet Kunden mit Hilfe interaktiver technischer Support-Werkzeuge die Möglichkeit, ihre Probleme intern zu lösen. Als Valued Support Customer können Sie die Support-Website für folgende Aufgaben nutzen:

- Suchen nach interessanten Wissensdokumenten
- Absenden und Verfolgen von Support-Fällen und Erweiterungsanforderungen
- Herunterladen von Software-Patches
- Verwalten von Support-Verträgen
- Nachschlagen von HP-Support-Kontakten
- Einsehen von Informationen über verfügbare Services
- Führen von Diskussionen mit anderen Softwarekunden
- Suchen und Registrieren für Softwareschulungen

Für die meisten Support-Bereiche müssen Sie sich als Benutzer mit einem HP Passport registrieren und anmelden. In vielen Fällen ist zudem ein Support-Vertrag erforderlich. Hier können Sie sich für eine HP Passport-ID registrieren:

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

Weitere Informationen zu Zugriffsebenen finden Sie unter:

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

HP Software Solutions Now greift auf die Website von HPSW Solution and Integration Portal zu. Auf dieser Website finden Sie HP-Produktlösungen für Ihre Unternehmensanforderungen, einschließlich einer Liste aller Integrationsmöglichkeiten zwischen HP-Produkten sowie eine Aufstellung der ITIL-Prozesse. Der URL dieser Website lautet **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Inhalt

Systemkonfiguration und Optimierung

Dieses Dokument beschreibt die Konfiguration und Optimierung von HP Operations Orchestration.

Server- und Clientauthentifizierung über Zertifikate

SSL/TLS-Zertifikate (Secure Socket Layer/Transport Layer Security) binden einen kryptografischen Schlüssel digital an die Details einer Organisation und ermöglichen so sichere Verbindungen zwischen einem Webserver und einem Browser.

HP OO verwendet das Dienstprogramm Keytool zur Verwaltung kryptografischer Schlüssel und vertrauenswürdiger Zertifikate. Dieses Dienstprogramm ist im Installationsordner von HP OO enthalten; Sie finden es unter **<Installationsverzeichnis>/java/bin/keytool**. Weitere Informationen zum Dienstprogramm Keytool finden Sie unter http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html.

Installationen von HP OO Central enthalten zwei Dateien für die Verwaltung von Zertifikaten:

- **<Installationsverzeichnis>/central/var/security/client.truststore**: Enthält die Liste der vertrauenswürdigen Zertifikate.
- **<Installationsverzeichnis>/central/var/security/key.store**: Enthält das HP OO-Zertifikat.

Es wird empfohlen, das HP OO-Zertifikat im Anschluss an eine Neuinstallation von HP OO oder nach abgelaufener Gültigkeitsdauer Ihres aktuellen Zertifikats zu ersetzen.

Authentifizierung mit Serverzertifikat

Ersetzen des Central-SSL/TLS-Serverzertifikats

Sie können ein von einem bekannten Unternehmen signiertes Zertifikat oder ein benutzerdefiniertes Serverzertifikat verwenden.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter, um sie auf den Speicherort der Datei **key.store** und andere Details auf Ihrem Computer abzustimmen.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie Central und sichern Sie die **key.store**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/central/var/security** befindet.
2. Öffnen Sie eine Befehlszeile im Ordner **<Installationsverzeichnis>/central/var/security**.
3. Löschen Sie das vorhandene Serverzertifikat aus der Datei **key.store**, indem Sie den

folgenden Befehl eingeben:

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

4. Wenn Sie bereits ein Zertifikat mit der Erweiterung **.pfx** oder **.p12** besitzen, fahren Sie mit dem nächsten Schritt fort. Sollte dies nicht der Fall sein, müssen Sie das Zertifikat mit dem privaten Schlüssel in das PKCS12-Format (.pfx, .p12) exportieren. Beispiel: Das Zertifikat liegt im Format PEM vor:

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

   Wenn das Zertifikat im Format DER vorliegt, fügen Sie den Parameter `-inform DER` hinter pkcs12 an. Beispiel:

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

   Hinweis: Notieren Sie sich das Kennwort, das Sie angeben. Sie benötigen dieses Kennwort für den privaten Schlüssel bei der späteren Eingabe der Passphrase für den Schlüsselspeicher.

5. Extrahieren Sie mit dem folgenden Befehl den Alias für den Alias Ihres Zertifikats:

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

   Der Alias wird angezeigt. Im folgenden Beispiel ist dies die vierte Zeile von unten.

   ```
   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. Importieren Sie das Serverzertifikat im PKCS12-Format in die Central-Datei **key.store**:

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

7. Es wird empfohlen, das Standardkennwort “changeit” im automatisch generierten Keystore des Central-Servers zu ändern. Weitere Informationen finden Sie unter "Ändern des Kennworts für den Schlüsselspeicher/Vertrauensspeicher" auf Seite 11.

8. Starten Sie Central.

Ersetzen des Central-SSL/TLS-Serverzertifikats mit einem selbstsignierten Zertifikat

Sie können ein selbstsigniertes Zertifikat mit dem Dienstprogramm Keytool erstellen.

Hinweis: Nach dem Upgrade auf HP OO 10.10:

- Wenn eine neue Central-Version auf demselben Computer installiert wird wie die vorherige Installation, können Sie das vorhandene selbstsignierte Zertifikat verwenden.
- Wenn neue Central-Versionen auf anderen Computern installiert werden, müssen Sie für jede Installation ein neues selbstsigniertes Zertifikat generieren, auch wenn Sie für die vorherige Version ein Zertifikat hatten.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter, um sie auf den Speicherort der Datei **key.store** und andere Details auf Ihrem Computer abzustimmen.

1. Beenden Sie Central und sichern Sie die **key.store**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/central/var/security** befindet.
2. Öffnen Sie eine Befehlszeile im Ordner **<Installationsverzeichnis>/central/var/security**.
3. Löschen Sie das vorhandene Serverzertifikat aus der Datei **key.store**, indem Sie den folgenden Befehl eingeben:

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

4. Erzeugen Sie ein selbstsigniertes Zertifikat:

   ```
   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>"
   ```

   Hinweis: Wenn Sie keinen Pfad für die Generierung des neuen Schlüsselspeichers angeben, wird er in dem Ordner erstellt, in dem Sie den Befehl eingegeben haben, z. B. **<Installationsverzeichnis>/central/var/security**.

5. Importieren Sie das selbstsignierte Serverzertifikat in die Central-Datei **key.store**:

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

6. Starten Sie Central.

Importieren eines Zertifikats in einen RAS-Vertrauensspeicher

Wenn Sie ein benutzerdefiniertes Stammzertifikat für Central verwenden und dieses Stammzertifikat bei der RAS-Installation nicht angegeben haben, müssen Sie nach der Installation eines RAS die vertrauenswürdige Stammzertifizierungsstelle (CA) in die RAS-Datei **client.truststore** importieren. Wenn Sie ein signiertes Standardstammzertifikat verwenden, müssen Sie das folgende Verfahren nicht durchführen, weil das Zertifikat bereits in der Datei **client.truststore** angegeben ist.

Standardmäßig unterstützt HP OO alle selbstsignierten Zertifikate. Allerdings ist es in einer Produktionsumgebung ratsam, diese Standardeinstellung aus Sicherheitsgründen zu ändern.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie RAS und sichern Sie die **client.truststore**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/ras/var/security** befindet.
2. Öffnen Sie eine Befehlszeile im Ordner **<Installationsverzeichnis>/ras/var/security**.
3. Öffnen Sie die Datei **<Installationsverzeichnis>ras/conf/ras-wrapper.conf** und legen Sie für `-Dssl.support-self-signed`den Wert **false** fest. Dies aktiviert die vertrauenswürdige Zertifizierungsstelle (CA).

   Beispiel:

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

4. Öffnen Sie die Datei **<Installationsverzeichnis>ras/conf/ras-wrapper.conf** und legen Sie für `-Dssl.verifyHostName`den Wert **true** fest. Hiermit wird der Hostname überprüft.

   Beispiel:

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

5. Importieren Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die RAS-Datei **client.truststore**:

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

6. Starten Sie RAS.

Importieren eines Zertifikats in den OOSH-Vertrauensspeicher

Wenn Sie ein benutzerdefiniertes Stammzertifikat für Central verwenden, müssen Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die OOSH-Datei **client.truststore** importieren. Wenn Sie ein signiertes Standardstammzertifikat verwenden, müssen Sie das folgende Verfahren nicht durchführen, weil das Zertifikat bereits in der Datei **client.truststore** angegeben ist.

Standardmäßig unterstützt HP OO alle selbstsignierten Zertifikate. Allerdings ist es in einer Produktionsumgebung ratsam, diese Standardeinstellung aus Sicherheitsgründen zu ändern.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie Central und sichern Sie die **client.truststore**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/central/var/security** befindet.
2. Bearbeiten Sie die Datei **oosh.bat** im Ordner **<Installationsverzeichnis>/central/bin**.
3. Legen Sie für `-Dssl.support-self-signed` den Wert **false** fest. Dies aktiviert die vertrauenswürdige Zertifizierungsstelle (CA).

   Beispiel:

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

4. Legen Sie für `-Dssl.verifyHostName` den Wert **true** fest. Hiermit wird der Hostname überprüft.

   Beispiel:

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

5. Importieren Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die Central-Datei **client.truststore**:

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

6. Führen Sie OOSH aus.

Importieren eines Zertifikats in den Studio Debugger-Vertrauensspeicher

Wenn Sie ein benutzerdefiniertes Stammzertifikat für Studio verwenden, müssen Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) nach der Installation von Studio in die Studio-

Datei **client.truststore** importieren. Wenn Sie ein signiertes Standardstammzertifikat verwenden, müssen Sie das folgende Verfahren nicht durchführen, weil das Zertifikat bereits in der Datei **client.truststore** angegeben ist.

Standardmäßig unterstützt HP OO alle selbstsignierten Zertifikate. Allerdings ist es in einer Produktionsumgebung ratsam, diese Standardeinstellung aus Sicherheitsgründen zu ändern.

Ersetzen Sie die in <Gelb> hervorgehobenen Parameter.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie Studio und sichern Sie die **client.truststore**-Originaldatei, die sich im Ordner **<Installationsverzeichnis>/studio/var/security** befindet.
2. Bearbeiten Sie die Datei **Studio.l4j.ini** im Ordner **<Installationsverzeichnis>/studio**.
3. Legen Sie für `-Dssl.support-self-signed` den Wert **false** fest. Dies aktiviert die vertrauenswürdige Zertifizierungsstelle (CA).

   Beispiel:

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

4. Legen Sie für `-Dssl.verifyHostName` den Wert **true** fest. Hiermit wird der Hostname überprüft.

   Beispiel:

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

5. Importieren Sie die vertrauenswürdige Stammzertifizierungsstelle (CA) in die Studio-Datei **client.truststore**:

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

6. Starten Sie Studio.

Weitere Informationen finden Sie unter "Debuggen einer Remote-Instanz von Central mit Studio" im *Studio-Erstellungshandbuch*.

Ändern des Kennworts für den Schlüsselspeicher/Vertrauensspeicher

- **So ändern Sie das Kennwort für Central**:

  a. Bearbeiten Sie die Datei **server.xml**, die sich im Ordner **<Installationsverzeichnis>/central/tomcat/conf** befindet.

b. Suchen Sie den HTTPS-Connector. Beispiel:

```
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. Ändern Sie das erforderliche Kennwort.

- `keyPass` – Das Kennwort für den Zugriff auf das Serverzertifikat aus der angegebenen Schlüsselspeicherdatei. Der Standardwert ist "`changeit`".
- `keystorePass` – Das Kennwort für den Zugriff auf die angegebene Schlüsselspeicherdatei. Der Standardwert ist der Wert des Attributs `keyPass`.
- `truststorePass` – Das Kennwort für den Zugriff auf den Vertrauensspeicher. Der Standardwert ist der Wert der Systemeigenschaft **javax.net.ssl.trustStorePassword**. Wenn diese Eigenschaft null ist, wird kein Vertrauensspeicherkennwort konfiguriert. Wird ein ungültiges Vertrauensspeicherkennwort angegeben, wird eine Warnung protokolliert und ein Versuch unternommen, ohne Kennwort auf den Vertrauensspeicher zuzugreifen; dabei wird die Überprüfung des Vertrauensspeicherinhalts übersprungen.

d. Speichern Sie die Datei.

e. Öffnen Sie die Datei **central-wrapper.conf** unter **central/conf** und ändern Sie die Zeile:

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

f. Starten Sie Central erneut.

- **So ändern Sie das Kennwort für den RAS-Vertrauensspeicher**: Bearbeiten Sie die Datei **ras-wrapper.conf** und ändern Sie den Parameter `changeit` des Vertrauensspeichers.
- **So ändern Sie das Kennwort für den OOSH-Vertrauensspeicher**: Bearbeiten Sie die Datei **oosh.bat** und ändern Sie den Parameter `changeit` des Vertrauensspeichers.
- **So ändern Sie das Kennwort für den Studio-Vertrauensspeicher**: Bearbeiten Sie die Datei **<Installationsverzeichnis>/studio/Studio.l4j.ini** und ändern Sie den Parameter `changeit` des Vertrauensspeichers.

Entfernen der RC4-Verschlüsselung aus den unterstützten SSL-Verschlüsselungsverfahren

Der Remotehost unterstützt die Verwendung der RC4-Verschlüsselung. Diese Verschlüsselung ist bei der Generierung eines pseudozufälligen Bytestroms fehlerhaft, sodass eine Vielzahl kleiner

Verzerrungen in den Strom gelangt und die Zufälligkeit der Daten reduziert.

Wenn einfacher Text wiederholt verschlüsselt wird (Beispiel: HTTP-Cookies) und ein Angreifer imstande ist, viele (im zweistelligen Millionenbereich) verschlüsselte Texte in die Hände zu bekommen, kann er den Text möglicherweise entschlüsseln.

Deaktivieren Sie die RC4-Verschlüsselung auf der JRE-Ebene (beginnend mit Java 7):

1. Öffnen Sie die Datei **$JRE_HOME/lib/security/java.security**.
2. Bearbeiten Sie die Eigenschaft **jdk.tls.disabledAlgorithms**, um die RC4-Verschlüsselung zu deaktivieren.

Weitere Informationen finden Sie unter http://stackoverflow.com/questions/18589761/restict-cipher-suites-on-jre-level.

Ändern oder Schließen des HTTP/HTTPS-Ports

Die Datei **server.xml** im Verzeichnis **[OO_HOME]\central\Tomcat\conf** enthält zwei **<Connector >**-Elemente unter dem Element **<Service>**. Diese Connector definieren oder aktivieren die Ports, die der Server überwacht.

Jede Connector-Konfiguration wird anhand von zugehörigen Attributen definiert. Der erste Connector definiert einen Standard-HTTP- und der zweite Connector einen HTTPS-Connector.

Standardmäßig sehen diese Connectoren wie folgt aus:

HTTP-Connector:

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

HTTPS-Connector:

```
<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"/>
```

Standardmäßig sind beide Connectoren aktiviert.

Ändern der Portwerte

So ändern Sie die Werte eines Ports:

1. Bearbeiten Sie die Datei **server.xml**, die sich im Ordner **<Installationsverzeichnis>/central/tomcat/conf** befindet.
2. Suchen Sie die Zeile mit dem HTTP- oder HTTPS-Connector und ändern Sie den Wert für **Port**.

   Hinweis: Wenn Sie sowohl HTTP und HTTPS aktiv halten und den HTTPS-Port ändern möchten, müssen Sie den **redirectPort** für den HTTP-Connector ändern.

3. Speichern Sie die Datei.
4. Starten Sie Central erneut.

Deaktivieren eines Ports

So deaktivieren Sie einen der Ports:

1. Bearbeiten Sie die Datei **server.xml**, die sich im Ordner **<Installationsverzeichnis>/central/tomcat/conf** befindet.
2. Suchen Sie den HTTP- oder HTTPS-Connector und löschen Sie die Zeile oder kommentieren Sie sie aus.
3. Speichern Sie die Datei.
4. Starten Sie Central erneut.

Clientzertifikatauthentifizierung (Gegenseitige Authentifizierung)

Die X. 509-Zertifikat-Authentifizierung wird am häufigsten beim Überprüfen der Identität eines Servers bei Verwendung von SSL/TLS genutzt; meist sind dies HTTPS-Verbindungen eines Browsers. Der Browser überprüft automatisch, ob das von einem Server vorgelegte Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgegeben wurde, die sich in einer von ihm verwalteten Liste befindet.

Sie können SSL/TLS aber auch für eine gegenseitige Authentifizierung verwenden. Der Server fordert als Teil des SSL/TLS-Handshake ein gültiges Zertifikat vom Client an. Der Server authentifiziert den Client, indem er prüft, ob das Zertifikat von einer vertrauenswürdigen Authentifizierungsstelle signiert wurde. Wenn ein gültiges Zertifikat bereitgestellt wurde, können Sie es über die Servlet-API in einer Anwendung abrufen.

Konfigurieren der Clientzertifikatauthentifizierung in Central

Stellen Sie vor dem Konfigurieren der Clientzertifikatauthentifizierung in Central sicher, dass Sie das SSL/TLS-Serverzertifikat wie in "Server- und Clientauthentifizierung über Zertifikate" auf Seite

6 beschrieben konfiguriert haben.

Legen Sie für das Attribut `clientAuth` den Wert `true` fest, wenn der SSL-Stack eine gültige Zertifikatskette vom Client anfordern soll, bevor eine Verbindung akzeptiert wird. Geben Sie `want` an, um festzulegen, dass der SSL-Stack ein Clientzertifikat anfordert, aber nicht fehlschlägt, wenn kein Zertifikat vorgelegt wird. Wird `false` (Standard) angegeben, ist keine Zertifikatskette erforderlich, es sei denn der Client fordert eine Ressource an, die durch eine Sicherheitseinschränkung geschützt ist, die auf einer Clientzertifikatauthentifizierung beruht. (Weitere Informationen finden Sie in der Apache Tomcat Configuration Reference.)

Geben Sie die Datei mit der **Zertifikatsperrliste (CRL)** an. Die Datei kann mehrere CRLs enthalten. Bei einigen kryptografischen Systemen, in der Regel Public-Key-Infrastrukturen (PKIs), werden in einer Zertifikatsperrliste Zertifikate (genauer gesagt Seriennummern von Zertifikaten) erfasst, die widerrufen wurden. Entitäten, die solche (widerrufene) Zertifikate vorlegen, sollten als nicht mehr vertrauenswürdig betrachtet werden.

Hinweis: Bei dem folgenden Verfahren wird das Dienstprogramm Keytool verwendet, das sich im Ordner **<Installationsverzeichnis>/java/bin/keytool** befindet.

1. Beenden Sie den Central-Server.
2. Importieren Sie das zugehörige Stammzertifikat (CA) in Central **client.truststore**: **<Installationsverzeichnis>/central/var/security/client.truststore**. Beispiel:

   ```
   keytool -importcert -alias <any_alias> -keystore <path>/client.truststore -
   file <certificate_path> -storepass <changeit>
   ```

3. Bearbeiten Sie die Datei **server.xml**, die sich im Ordner **<Installationsverzeichnis>/central/tomcat/conf** befindet.
4. Legen Sie für das Attribut `clientAuth` im Tag `Connector` den Wert `want` oder `true` fest. Die Standardeinstellung ist `false`.

   Hinweis: An diesem Punkt kann der Server gestartet werden. Es wird aber empfohlen, den Server erst am Ende dieser Prozedur zu starten.

5. Fügen Sie das Attribut `crlFile` hinzu, um die Datei mit den Zertifikatsperrlisten für die SSL/TLS-Zertifikatprüfung zu definieren. Beispiel:

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

   Die Datei kann die Erweiterung `.crl` für eine einzelne Zertifikatsperrliste oder `.pem` (PEM CRL-Format) für eine oder mehrere Zertifikatsperrlisten aufweisen. Das PEM-CRL-Format verwendet die folgenden Kopf- und Fußzeilen:

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

Beispiel für die `.pem`-Dateistruktur mit einer CRL (mehrere CRLs werden mit weiteren CRL-Blöcken verkettet):

```
-----BEGIN X509 CRL-----
MIIBbzCB2QIBATANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzEYMBYGA1UE
ChMPVS5TLiBHb3Zlcm5tZW50MQwwCgYDVQQLEwNEb0QxEDAOBgNVBAsTB1Rlc3Rp
bmcxFTATBgNVBAMTDFRydXN0IEFuY2hvchcNOTkwMTAxMTIwMTAwWhcNNDgwMTAx
MTIwMTAwWjAiMCACAScXDTk5MDEwMTEyMDAwMFowDDAKBgNVHRUEAwoBAaAjMCEw
CgYDVR0UBAMCAQEwEwYDVR0jBAwwCoAIq5rr+cLnVI8wDQYJKoZIhvcNAQEFBQAD
gYEAC7lqZwejJRW7QvzH11/7cYcL3racgMxH3PSU/ufvyLk7ahR++RtHary/WeCv
RdyznLiIOA8ZBiguWtVPqsNysNn7WLofQIVa+/TD3T+lece4e1NwGQvj5Q+e2wRt
GXg+gCuTjTKUFfKRnWz7O7RyiJKKim0jtAF4RkCpLebNChY=
-----END X509 CRL-----
```

6. Starten Sie den Central-Server.

Hinweis: Für jedes Clientzertifikat müssen Sie entweder einen internen Benutzer oder einen LDAP-Benutzer definieren. Der Name des Benutzers sollte in den Zertifikatattributen definiert sein. Der Standardwert ist der Wert des CN-Attributs. Weitere Informationen finden Sie im Abschnitt Verarbeiten eines Zertifikatprinzipals.

Beachten Sie Folgendes: Auch wenn Sie in HP OO mehrere LDAP-Konfigurationen eingerichtet haben, kann ein Benutzer nur mit den Clientzertifikatattributen aus dem Standard-LDAP authentifiziert werden. Central versucht zuerst, den Benutzer mit dem Standard-LDAP zu authentifizieren, und unternimmt, wenn dies fehlschlägt, einen weiteren Authentifizierungsversuch in der internen HP OO-Domäne.

Aktualisieren der Konfiguration eines Clientzertifikats in RAS

Das Clientzertifikat wird bei der Installation des RAS konfiguriert. Wenn Sie das Clientzertifikat jedoch aktualisieren müssen, können Sie die Datei **ras-wrapper.conf** manuell bearbeiten.

Voraussetzung: Sie müssen das CA-Stammzertifikat von Central in den RAS-Truststore importieren. Weitere Informationen finden Sie unter "Importieren eines Zertifikats in einen RAS-Vertrauensspeicher" auf Seite 9.

So aktualisieren Sie die Konfiguration des Clientzertifikats in einem externen RAS:

1. Beenden Sie den RAS-Server.
2. Öffnen Sie die Datei **ras-wrapper.conf** im Ordner **<Installationsverzeichnis>/ras/var/conf**.
3. Ändern Sie die folgenden Angaben gemäß Ihrem Clientzertifikat:

```
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. Starten Sie den RAS-Server.

Wichtiger Hinweis! Das X. 509-Clientzertifikat muss den Prinzipalnamen des RAS, die RAS-ID, enthalten (siehe Verarbeiten eines Zertifikatprinzipals).

Sie finden die RAS-ID auf der Registerkarte **Topologie** in Central. Weitere Informationen finden Sie unter "Einrichten der Topologie – Worker" im *HP OO Central-Benutzerhandbuch*.

Konfigurieren eines ClientZertifikats in Studio Remote Debugger

Voraussetzung: Sie müssen das CA-Stammzertifikat von Central in den Studio Debugger-Truststore importieren. Weitere Informationen finden Sie unter "Importieren eines Zertifikats in den Studio Debugger-Vertrauensspeicher" auf Seite 10.

So konfigurieren Sie das Clientzertifikat in Studio Remote Debugger:

1. Schließen Sie Studio.
2. Bearbeiten Sie die Datei **Studio.l4j.ini** im Ordner **<Installationsverzeichnis>/studio**.
3. Ändern Sie die folgenden Angaben gemäß Ihrem Clientzertifikat:

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

-Djavax.net.ssl.keyStorePassword=changeit

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

4. Starten Sie Studio.

Hinweis: Für jedes Clientzertifikat müssen Sie entweder einen internen Benutzer oder einen LDAP-Benutzer definieren. Der Name des Benutzers sollte in den Zertifikatattributen definiert sein. Der Standardwert ist der Wert des CN-Attributs. Weitere Informationen finden Sie im Abschnitt Verarbeiten eines Zertifikatprinzipals.

Beachten Sie Folgendes: Auch wenn Sie in HP OO mehrere LDAP-Konfigurationen eingerichtet haben, kann ein Benutzer nur mit den Clientzertifikatattributen aus dem Standard-LDAP authentifiziert werden. Central versucht zuerst, den Benutzer mit dem Standard-LDAP zu authentifizieren, und unternimmt, wenn dies fehlschlägt, einen weiteren Authentifizierungsversuch in der internen HP OO-Domäne.

Konfigurieren eines Clientzertifikats in OOSH

Voraussetzung: Sie müssen das CA-Stammzertifikat von Central in den OOSH-Truststore importieren. Weitere Informationen finden Sie unter "Importieren eines Zertifikats in den OOSH-Vertrauensspeicher" auf Seite 10.

1. Beenden Sie OOSH.
2. Bearbeiten Sie die Datei **oosh.bat** im Ordner **<Installationsverzeichnis>/central/bin**.
3. Ändern Sie die folgenden Angaben gemäß Ihrem Clientzertifikat:

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

4. Starten Sie OOSH.

Hinweis: Für jedes Clientzertifikat müssen Sie entweder einen internen Benutzer oder einen LDAP-Benutzer definieren. Der Name des Benutzers sollte in den Zertifikatattributen definiert sein. Der Standardwert ist der Wert des CN-Attributs. Weitere Informationen finden Sie im Abschnitt Verarbeiten eines Zertifikatprinzipals.

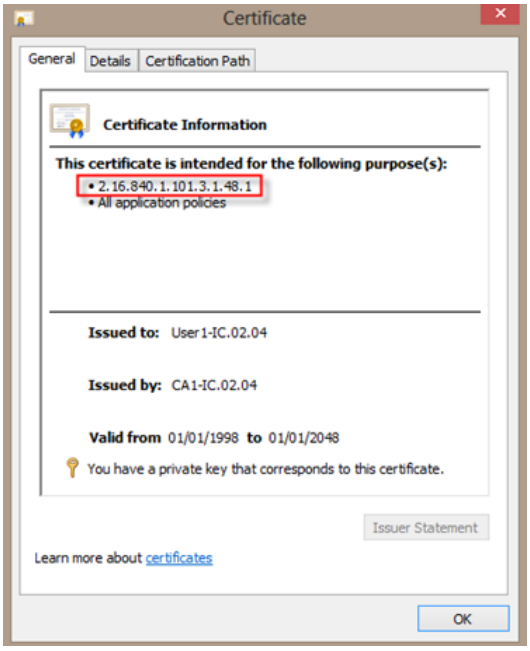
Beachten Sie Folgendes: Auch wenn Sie in HP OO mehrere LDAP-Konfigurationen eingerichtet haben, kann ein Benutzer nur mit den Clientzertifikatattributen aus dem Standard-LDAP authentifiziert werden. Central versucht zuerst, den Benutzer mit dem Standard-LDAP zu authentifizieren, und unternimmt, wenn dies fehlschlägt, einen weiteren Authentifizierungsversuch in der internen HP OO-Domäne.

Verarbeiten der Zertifikatrichtlinien

HP OO obliegt die Verarbeitung von Zertifikatrichtlinien für das Endpunktzertifikat.

- Sie können die Zweckzeichenfolge im Zertifikat festlegen.
- In HP OO können Sie die Richtlinienzeichenfolge(n) als Konfigurationselement hinzufügen und die Richtlinienzeichenfolge eines jeden Endpunktzertifikats überprüfen. Wenn es nicht übereinstimmt, wird das Zertifikat abgelehnt.
- Aktivieren oder deaktivieren Sie die Überprüfung der Zertifikatrichtlinien, indem Sie das folgende Konfigurationselement hinzufügen: `x509.certificate.policy.enabled=true/false` (Standardeinstellung ist `false`).
- Definieren Sie die Richtlinienliste, indem Sie das folgende Konfigurationselement hinzufügen: `x509.certificate.policy.list=<comma_separated_list>` (Standardeinstellung ist eine

leere Liste).



Verarbeiten eines Zertifikatprinzipals

Sie können definieren, wie der Prinzipal aus einem Zertifikat abgerufen wird, indem Sie einen regulären Ausdruck als Vergleichskriterium für `Subject` angeben. Der reguläre Ausdruck sollte eine einzelne Gruppe enthalten. Der Standardausdruck `CN=(.?)` zieht für den Vergleich das Feld "Allgemeiner Name" (Common Name, CN) heran. Beispiel: `CN=Jimi Hendrix, OU=` weist den Benutzernamen `Jimi Hendrix` zu.

- Groß- und Kleinschreibung wird ignoriert.
- Der Prinzipal des Zertifikats ist der Benutzername in HP OO (LDAP- oder interner Benutzer).
- Um den regulären Ausdruck zu ändern, ändern Sie das Konfigurationselement `x509.subject.principal.regex`.

Fehlerbehebung

Wenn der Server nicht startet, öffnen Sie die Datei **wrapper.log** und suchen nach einem Fehler in `ProtocolHandler ["http-nio-8443"]`.

Dieser Fehler kann beim Initialisieren von Tomcat oder beim Starten des Connectors auftreten. Er tritt in vielen Variationen auf, aber die Fehlermeldung enthält weitere Informationen.

Alle HTTPS-Connector-Parameter sind in der Tomcat-Konfigurationsdatei angegeben, die sich unter **C:\HP\oo\central\tomcat\conf\Server.xml** befindet.

Öffnen Sie die Datei und scrollen Sie nach unten, bis Sie den HTTPS-Connector sehen:

```
<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"/>
```

Prüfen Sie, ob eine Nichtübereinstimmung bei den Parametern vorliegt, indem Sie sie mit den in den vorherigen Schritten eingegebenen Parametern vergleichen.

Federal Information Processing Standard (FIPS)

Konfigurieren der FIPS 140-2-Konformität in HP OO

In diesem Abschnitt wird erläutert, wie Sie HP Operations Orchestration konfigurieren, um Übereinstimmung mit den Federal Information Processing Standards (FIPS) 140-2 zu erzielen.

FIPS 140-2 ist ein Standard, der Sicherheitsanforderungen für kryptografische Module definiert und von der US-Behörde National Institute of Standards Technology (NIST) festgelegt wurde. Der Standard wurde veröffentlicht unter: csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Nachdem Sie die HP OO-Konfiguration an den FIPS 140-2-Standard angepasst haben, verwendet HP OO die folgenden Sicherheitsalgorithmen:

- Symmetrischer Schlüsselalgorithmus: AES
- Hash-Algorithmus: SHA1

HP OO verwendet den Sicherheitsanbieter RSA BSAFE Crypto Software Version 6.1. Dies ist der einzige unterstützte Sicherheitsanbieter für FIPS 140-2.

Hinweis: Nachdem Sie die HP OO-Konfiguration an den FIPS 140-2-Standard angepasst haben, können Sie die Standardkonfiguration nur durch eine Neuinstallation von HP OO wiederherstellen.

Voraussetzungen

Hinweis: Beim Upgrade einer Installation von HP OO 10.10 (und höher), die bereits mit FIPS konfiguriert wurde, müssen Sie die Schritte 4 und 5 im folgenden Abschnitt wiederholen und dann die Schritte im Abschnitt "Konfigurieren der Eigenschaften in der Java-Sicherheitsdatei" in "Konfigurieren der FIPS 140-2-Konformität von HP OO" auf Seite 23 wiederholen.

Führen Sie vor der FIPS 140-2-konformen HP OO-Konfiguration die folgenden Schritte aus:

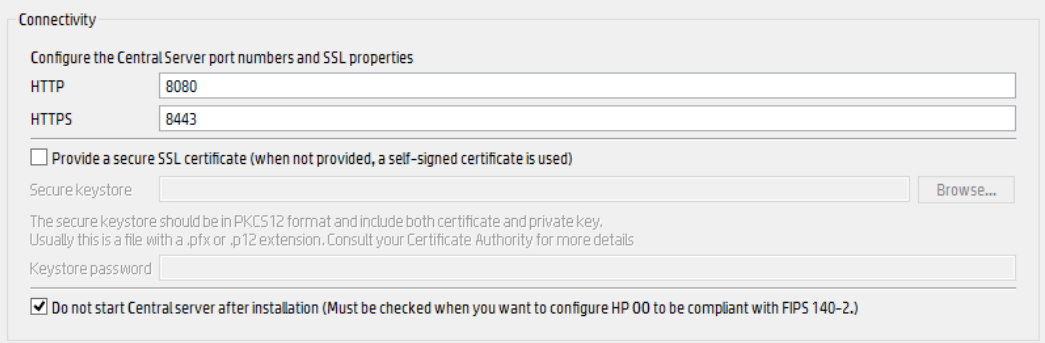
Hinweis: Um den FIPS140-2-Standard zu erfüllen, müssen Sie LWSSO ausschalten.

1. Vergewissern Sie sich, dass Sie eine neue Installation von HP OO Version 10.10 oder höher für FIPS 140-2 konfigurieren, die gerade nicht verwendet wird.

   Eine Installation von HP OO, die gerade verwendet wird (ob Version 9.x oder 10.x), kann nicht konfiguriert werden.

2. Vergewissern Sie sich, dass HP OO bei der Installation so konfiguriert wurde, dass der Central Server nach der Installation nicht gestartet wird:

- Bei einer Installation im Hintergrund wurde der Parameter `should.start.central` auf **no** gesetzt.
- In einer mit dem Assistenten durchgeführten Installation wurde beim Schritt **Verbindung** das Kontrollkästchen **Central Server nach der Installation nicht starten** aktiviert.



3. Sichern Sie die folgenden Verzeichnisse:
   - **<Installationsverzeichnis>\central\tomcat\webapps\oo.war**
   - **<Installationsverzeichnis>\central\tomcat\webapps\PAS.war**
   - **<Installationsverzeichnis>\central\conf**
   - **<oo_jre>\lib\security** (**<oo_jre>** ist das Verzeichnis, in dem die von HP OO verwendete JRE installiert ist. Standardmäßig ist dies das Verzeichnis **<Installationsverzeichnis>\java**)
4. Laden Sie die Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction Policy Files von der folgenden Website herunter und installieren Sie sie: http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html.

   Hinweis: Informationen, wie Sie die Dateien verteilen und die von HP OO verwendete JRE aktualisieren, finden Sie in der Datei **ReadMe.txt**, die zu den heruntergeladenen Dateien gehört.
5. Installieren Sie die RSA BSAFE Crypto-Dateien. Kopieren Sie auf dem System, auf dem HP OO installiert ist, die folgenden Dateien in den Ordner **<oo_jre>\lib\ext**(**<oo_jre>** steht für das Verzeichnis, in dem die von HP OO verwendete JRE installiert ist. Standardmäßig ist dies der Ordner **<Installationsverzeichnis>\java**).
   - **<Installationsverzeichnis>\central\lib\cryptojce-6.1.jar**
   - **<Installationsverzeichnis>\central\lib\cryptojcommon-6.1.jar**
   - **<Installationsverzeichnis>\central\lib\jcmFIPS-6.1.jar**

Hinweis: Beim Upgrade einer Installation von HP OO 10.10 (und höher), die bereits mit FIPS konfiguriert wurde, müssen Sie die Schritte 4 und 5 im obigen Abschnitt "Voraussetzungen" wiederholen und dann die Schritte im Abschnitt "Konfigurieren der Eigenschaften in der Java-Sicherheitsdatei" in "Konfigurieren der FIPS 140-2-Konformität von HP OO" unten wiederholen.

Konfigurieren der FIPS 140-2-Konformität von HP OO

Die folgende Liste enthält die Prozeduren, die Sie durchführen müssen, um HP OO in Übereinstimmung mit FIPS 140-2 zu konfigurieren:

- Konfigurieren der Eigenschaften in der Java-Sicherheitsdatei
- Konfigurieren der Datei "encryption.properties" und Aktivieren des FIPS-Modus
- Erstellen einer FIPS-kompatiblen HP OO-Verschlüsselung
- Ersetzen des Datenbankkennworts
- Starten von HP OO

Konfigurieren der Eigenschaften in der Java-Sicherheitsdatei

Bearbeiten Sie die Java-Security-Datei für JRE, um zusätzliche Sicherheitsanbieter hinzuzufügen, und konfigurieren Sie die Eigenschaften für die FIPS 140-2-Konformität.

Hinweis: Das Upgrade auf HP OO 10.10 ersetzt alle installierten JRE-Dateien. Deshalb müssen Sie nach dem Upgrade auf 10.10 die folgenden Schritte durchführen:

Hinweis: Beim Upgrade einer Installation von HP OO 10.10 (und höher), die bereits mit FIPS konfiguriert wurde, müssen Sie die Schritte 4 und 5 im Abschnitt "Voraussetzungen" in " Federal Information Processing Standard (FIPS)" auf Seite 21 wiederholen und dann die Schritte im vorliegenden Abschnitt wiederholen.

Öffnen Sie die Datei **< oo_jre>\lib\security\java.security** in einem Editor und führen Sie die folgenden Schritte aus:

1. Erhöhen Sie bei jedem im Format **security.provider.<nn>=<provider_name>** gelisteten Anbieter die Reihenfolgennummer `<nn>` um zwei.

   Ändern Sie beispielsweise den Anbietereintrag:

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

   in

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

2. Fügen Sie einen neuen Standardanbieter hinzu (RSA JCE). Fügen Sie den folgenden Anbieter am Anfang der Anbieterliste ein:

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

3. Fügen Sie RSA BSAFE als neuen SSL-J Java Secure Sockets Extension (JSSE) Provider hinzu.

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

4. Kopieren und fügen Sie die folgende Zeile in die Datei **java.security** ein, um sicherzustellen, dass **RSA BSAFE** im FIPS 140-2-konformen Modus verwendet wird:

   ```
   com.rsa.cryptoj.fips140initialmode=FIPS140_SSL_MODE
   ```

   Sie können diese Zeile an beliebiger Stelle in der Datei **java.security** einfügen.

5. Da der Standard-DRBG-Algorithmus ECDRBG128 (gemäß NIST) nicht sicher ist, legen Sie für die security-Eigenschaft **com.rsa.crypto.default** den Wert **HMACDRBG** fest, indem Sie die folgende Zeile in die Datei **java.security** kopieren:

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

   Sie können diese Zeile an beliebiger Stelle in der Datei **java.security** einfügen.

6. Speichern und schließen Sie die Datei **java.security**.

Konfigurieren der Datei "encryption.properties" und Aktivieren des FIPS-Modus

Die HP OO-Datei **encryption.properties** muss aktualisiert werden, um FIPS 140-2-konform zu sein.

1. Sichern Sie die Datei **encryption.properties**, die sich in **<Installationsverzeichnis>\central\var\security** befindet.

2. Öffnen Sie die Datei **encryption.properties** in einem Texteditor. Bearbeiten Sie beispielsweise die folgende Datei:

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

3. Suchen Sie nach `keySize=128` und ersetzen Sie diese Angabe durch `keySize=256`.

4. Suchen Sie nach `secureHashAlgorithm=SHA1` und ersetzen Sie diese Angabe durch `secureHashAlgorithm=SHA256`.

5. Suchen Sie nach `FIPS140ModeEnabled=false` und ersetzen Sie diese Angabe durch `FIPS140ModeEnabled=true`.

   Hinweis: Wenn `FIPS140ModeEnabled=false` nicht vorhanden ist, fügen Sie `FIPS140ModeEnabled=true` als neue Zeile am Ende der Datei hinzu.

6. Speichern und schließen Sie die Datei.

Erstellen einer FIPS-kompatiblen HP OO-Verschlüsselung

Informationen dazu, wie Sie eine HP OO-Verschlüsselungsspeicherdatei erstellen oder ersetzen, sodass sie FIPS-konform ist, finden Sie unter "Ersetzen der FIPS-Verschlüsselung" unten.

Hinweis: Für AES sind drei Schlüssellängen zulässig: 128/192/256 laut NIST SP800-131A.

Diese Secure-Hash-Algorithmen werden in FIPS unterstützt: SHA1, SHA256, SHA384, SHA512.

Hinweis: Es wird empfohlen, die Kennwörter für den Keystore (und den Eintrag mit dem privaten Schlüssel) und den Truststore zu ändern. Weitere Informationen finden Sie unter "Ändern des Kennworts für den Schlüsselspeicher/Vertrauensspeicher" auf Seite 11.

Hinweis: Es wird empfohlen, alle Standard-CA-Stammzertifikate im HP OO-Truststore zu löschen. (Die Datei Client.truststore befindet sich unter <Installation>/central/var/security.)

Ersetzen des Datenbankkennworts

Ersetzen Sie das Datenbankkennwort wie unter "Ändern des Datenbankkennworts" auf Seite 30 beschrieben.

Starten von HP OO

Starten Sie HP OO gemäß Beschreibung im *HP OO-Installationshandbuch*.

Ersetzen der FIPS-Verschlüsselung

HP OO, Central und RAS entsprechen dem FIPS-Standard 140-2 (Federal Information Processing Standard), der die technischen Anforderungen definiert, die von US-Bundesbehörden einzuhalten sind, wenn diese Organisationen kryptografische Sicherheitssysteme zum Schutz vertraulicher oder wertvoller Daten spezifizieren.

Nach einer Neuinstallation von HP OO 10.10 haben Sie die Möglichkeit, den FIPS-Verschlüsselungsalgorithmus zu ändern.

Hinweis: Dieses Verfahren ist nur bei Neuinstallationen möglich. Sie können es nicht nach Upgradeinstallationen anwenden.

Ändern des FIPS Verschlüsselungsalgorithmus in Central

1. Wechseln Sie zu **<Central-Installationsordner>/var/security**.
2. Sichern und löschen Sie die Datei **encryption_repository**.
3. Wechseln Sie zu **<Central-Installationsordner>/bin**.
4. Führen Sie das Skript **generate-keys** aus.

   Ein neuer Masterschlüssel wird in **<Central-Installationsordner>/var/security/encryption_repository** generiert.

Ändern der RAS-Verschlüsselungseigenschaften

Wenn Sie die RAS-Installation an einem neuen Standort durchgeführt haben, müssen Sie alle folgenden Schritte ausführen.

Hinweis: Diese Änderungen sind nur gültig, wenn Sie eine neue RAS-Installation bearbeiten, nachdem Sie die Central-Verschlüsselungseigenschaften geändert haben.

So ändern Sie die RAS-Verschlüsselungseigenschaften:

1. Führen Sie alle Schritte im Abschnitt "Voraussetzungen" in " Federal Information Processing Standard (FIPS)" auf Seite 21 aus.
2. Führen Sie alle Schritte im Abschnitt "Konfigurieren der Eigenschaften in der Java Security-Datei" in "Konfigurieren der FIPS 140-2-Konformität von HP OO" auf Seite 23 aus.
3. Kopieren Sie die aktuelle **encryption.properties**-Datei aus dem Ordner `<Installationsverzeichnis>\ras\var\security` in den Ordner `<Installationsverzeichnis>\ras\bin`.
4. Bearbeiten und ändern Sie die Datei **encryption.properties** in einem Texteditor nach Bedarf.

   Weitere Informationen finden Sie unter "Konfigurieren der Datei encryption.properties und Aktivieren des FIPS-Modus" in "Konfigurieren der FIPS 140-2-Konformität von HP OO" auf Seite 23.
5. Speichern Sie die Änderungen.
6. Öffnen Sie eine Befehlszeile im Ordner `<Installationsverzeichnis>\ras\bin`.
7. Führen Sie die Datei **oosh.bat** aus.

8. Führen Sie den OOShell-Befehl aus: `replace-encryption --file encryption.properties`

   Hinweis: Wenn Sie die Datei **encryption.properties** in einen anderen Ordner kopiert haben, müssen Sie den richtigen Speicherort im OOShell-Befehl angeben.

9. Starten Sie den RAS-Dienst wieder.

Konfigurieren der LWSSO-Einstellungen

Wenn Sie bei der Installation von HP OO 10.10 die Auswahl treffen, die LWSSO-Einstellungen aus HP OO 9.x zu aktualisieren, werden diese LWSSO-Einstellungen migriert, aber LWSSO wird in HP OO 10.10 deaktiviert, auch wenn es in HP OO 9.x aktiviert war.

Wenn Sie LWSSO nachträglich aktivieren, erhalten Sie unter Umständen Warnungen bei bestimmten Szenarien. Um die Warnungen aus dem Protokoll zu löschen, legen Sie als Wert der Management-URL-Eigenschaft den vollständig qualifizierten Domänennamen fest.

- Wenn Central und RAS auf dem gleichen Computer installiert und die LWSSO-Einstellungen aktiviert sind, müssen Sie für die Management-URL-Eigenschaft den vollständig qualifizierten Domänennamen angeben.

  a. Beenden Sie den RAS-Prozess.

  b. Ändern Sie die Datei **ras/conf/raswrapper.conf** wie folgt:

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

  in

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

  c. Starten Sie den RAS-Prozess.

- Wenn RAS auf einem anderen Computer als Central installiert ist und die LWSSO-Einstellungen aktiviert sind, müssen Sie bei der RAS-Installation die Management-URL von Central mit dem vollqualifizierten Domänennamen (FQDN) anstelle der IP-Adresse angeben.

- Bei Verbindung einer anderen Anwendung mit Central über LWSSO müssen Sie die Management-URL von Central mit dem vollqualifizierten Domänennamen (FQDN) angeben.

  a. Beenden Sie den Central-Prozess.

  b. Ändern Sie die Datei **central/conf/central-wrapper.conf** wie folgt:

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

  in

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

c. Starten Sie den Central-Prozess.

Konfigurieren der XSS-Richtlinie

HP OO verfügt über XSS-Schutz mit AntiSamy. Die Standardsicherheitsrichtlinie ist "antisamy". Sie lässt die meisten HTML-Elemente zu und kann nützlich sein, wenn Benutzer ganze HTML-Seiten übergeben.

Diese Richtlinie kann an eine der von AntiSamy unterstützten Richtlinien angepasst werden. Weitere Informationen finden Sie unter

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

Die Richtlinie ist über eine Systemkonfigurationseigenschaft namens `xss.policy` konfigurierbar. Mögliche Werte sind: antisamy (Standardeinstellung), antisamy-slashdot, antisamy-myspace, antisamy-ebay, antisamy-anythinggoes, antisamy-tinymc.

Um zu prüfen, welche Richtlinie konfiguriert ist, wechseln Sie zu **https://host/oo/reports/sysinfo** und suchen nach dem Parameter `xss.policy` im Abschnitt **Systemkonfiguration**.

Am einfachsten ändern Sie die Slashdot-Richtlinie mit dem Dienstprogramm HP Operations Orchestration Shell.

1. Doppelklicken Sie auf die Batchdatei `oosh.bat`, um das OOSH-Dienstprogramm zu starten.
2. Geben Sie in der Befehlszeile den Befehl (Beispiel) ein:

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

Weitere Informationen zum Dienstprogramm HP Operations Orchestration Shell finden Sie im HP *Operations Orchestration Shell User Guide*.

Konfigurieren der Lokalisierung

Einstellen des Systemgebietsschemas in Central-wrapper.conf

Wenn Sie ein lokalisiertes HP OO-System einsetzen, müssen Sie die folgenden Eigenschaften in der Datei **Central-wrapper.conf** an das Gebietsschema des Systems anpassen:

```
set.LANG=

set.LC_ALL=

set.LANGUAGE=
```

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

Als Beispiel wird hier die japanische Version angegeben: `set.LANG=ja_JP` und `set.LC_ALL=ja_JP`

Konfigurieren des Systems

Ändern des Datenbankkennworts

1. Wenn Central gerade ausgeführt wird, dann beenden Sie den Central-Dienst.
2. Führen Sie das encrypt-password-Skript mit der Option -e -p <Kennwort> aus, wobei das Kennwort das Kennwort der Datenbank ist.
3. Kopieren Sie das Ergebnis; es sollte wie folgt aussehen:

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

4. Öffnen Sie den Ordner **<Central-Installationsordner>/conf** und öffnen Sie die Datei **database.properties**.
5. Ändern Sie den Wert von `db.password` in den Wert, den Sie kopiert haben.

Ändern der Datenbank-IP

Dieser Abschnitt ist relevant, wenn Sie HP OO für die Arbeit mit einer anderen Datenbankinstanz konfigurieren möchten. Alle Datenbankparameter wie Datenbank-Anmeldeinformationen, Schemaname, Tabellen usw. sollten identisch sein.

1. Bearbeiten Sie die Datei **\HP Operations Orchestration\central\conf\database.properties**.
2. Suchen Sie den Parameter `jdbc.url`. Beispiel:

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

3. Ändern Sie die IP-Adresse und den FQDN des Datenbankservers.
4. Speichern Sie die Datei.
5. Starten Sie Central erneut.

Anpassen der Protokollierungsebenen

Es ist möglich, die Granularität der im Protokoll erfassten Informationen einzeln für reguläre Anmeldung, Bereitstellung und Ausführung anzupassen.

Die Granularitätsoptionen umfassen:

- `INFO` – Standardprotokollierungsinformationen
- `DEBUG` – Mehr Protokollierungsinformationen

- `FEHLER/WARNUNG` – Weniger Protokollierungsinformationen

So passen Sie die Granularität der Protokollierung an:

1. Öffnen Sie die Datei **log4j.properties** (unter **<OO-Installationsverzeichnis>/central/conf**).
2. Ersetzen Sie `INFO` durch `DEBUG` oder `FEHLER/WARNUNG` an der folgenden Position in der Datei **log4j.properties**.

   Beispiel:

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

Anpassen des Timings von Quartz-Jobs

Im HP OO-System werden im Rahmen der Systemwartung in regelmäßigen Abständen Quartz-Jobs ausgeführt.

Jeder Job wird in der festgelegten Dauer ausgeführt und in den festgelegten Intervallen wiederholt. Im Folgenden finden Sie einige Beispiele für Job-Trigger:

Triggername	Aktuelles Wiederholungsintervall	Ereignis
onRolling:OO_EXECUTION_STATES_Trigger	4,5 Minuten	Rollieren der Statustabelle zum Löschen
queueCleanerTrigger	1 Minute	Löschen der Warteschlangentabellen
queueRecoveryTrigger	2 Minuten	Prüft, ob eine Systemwiederherstellung erforderlich ist
recoveryVersionTrigger	0,5 Minuten	Versionszähler für die Wiederherstellung
splitJoinTrigger	1 Sekunde	Verbindet abgeschlossene Teile
onRolling:OO_EXECUTION_EVENTS_Trigger **Hinweis:** Dieser Trigger wird nicht mehr unterstützt.	12 Stunden	Rollieren der Ereignistabelle zum Löschen

Wenn Sie das Timing dieser Jobs verändern möchten, um die Leistung zu verbessern, führen Sie die folgenden Schritte aus:

Hinweis: Jede Änderung der Zeitangaben kann sich nachhaltig auf das System auswirken. Wenden Sie sich an den zuständigen HP-Kundendienstmitarbeiter, bevor Sie Änderungen an diesen Triggern vornehmen.

1. Rufen Sie die Jminix-Seite über die folgende URL auf: **{OO_HOST}:{OO_PORT}/oo/jminix/**

   Hinweis: Sie müssen die Berechtigung **Systemeinstellungen verwalten** besitzen, um die Seite **jminix** aufrufen zu können.

2. Öffnen Sie die Registerkarte **OO**. Unter **MBeans** finden Sie eine Operation mit dem Namen **jobTriggersMBean**.

3. Verwenden Sie diese Operation und geben Sie die Werte auf der rechten Registerkarte ein. Verwenden Sie dabei den Namen des Triggers, den Sie ändern möchten. Verwenden Sie exakt denselben Namen wie die Tabelle mit einem neuen Wert für das Wiederholungsintervall.

Damit werden die Startzeiten des Jobs geändert.

Hinweis: Der Mechanismus für die Persistenz der Ereignisse wird nicht mehr unterstützt (siehe **onRolling:OO_EXECUTION_EVENTS_Trigger**). Sie können diesen Job konfigurieren, wenn Sie den Remote Debugger verwenden oder wenn Sie das Flag **events.persistency** aktiviert haben. Weitere Informationen finden Sie unter "Aktivieren des Ereignisprotokollierungsmechanismus" auf der nächsten Seite.

Ändern der URL eines Central/Load Balancers auf dem RAS

Es wird empfohlen, die URL eines Central/Load Balancers über das Installationsprogramm zu konfigurieren. Wenn Sie aber Änderungen an der URL vornehmen müssen, nachdem der RAS bereits installiert wurde, können Sie die Datei **ras-wrapper.conf** bearbeiten.

Dies wäre beispielsweise dann erforderlich, wenn Sie einen RAS für einen Central/Load Balancer installiert haben und der vollqualifizierte Domänenname des Central/Load Balancers geändert würde. In diesem Fall müssen Sie die auf dem RAS gespeicherte URL des Central/Load Balancers ändern, damit der RAS wieder mit dem Central/Load Balancer kommunizieren kann.

1. Beenden Sie den RAS.

2. Öffnen Sie die Datei **ras-wrapper.conf**, die sich im Ordner **<Installationsordner>\ras\conf** befindet.

3. Bearbeiten Sie die URL in der folgenden Zeile:

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

4. Starten Sie den RAS erneut.

Aktivieren des Ereignisprotokollierungsmechanismus

Der Ereignisprotokollierungsmechanismus wird in HP OO 10.10 nicht mehr unterstützt und wird in einer der zukünftigen Versionen entfernt.

HP OO wird ohne den Ereignisprotokollierungsmechanismus bereitgestellt. Wenn Sie den Mechanismus aber verwenden möchten, können Sie das Flag **events.persistency** aktivieren. Es wird allerdings empfohlen, das Flag nicht zu aktivieren, wenn Sie mit Clusterszenarien arbeiten oder die Leistung steigern möchten.

So aktivieren Sie das Flag:

1. Halten Sie den Prozess an und aktualisieren Sie die Datei **wrapper.conf** auf jedem Knoten (Central/RAS) in Ihrem System.

   Wechseln Sie in Central zu **<Installationspfad>\central\conf\central-wrapper.conf**.

   Wechseln Sie im RAS zu **<Installationspfad>\ras\conf\ras-wrapper.conf**.

2. Suchen Sie in der Datei **wrapper.conf** nach dem Parameter **-Devents.persistency** und ändern Sie den Parameterwert in **true**.

3. Starten Sie den Prozess erneut.


Java™
COMPATIBLE