HP Operations Orchestration

Version du logiciel : 10.20
Systèmes d'exploitation Windows et Linux

Manuel de sécurisation

Date de publication du document : Novembre 2014
Date de lancement du logiciel : Novembre 2014

Mentions légales

Garantie

Les seules garanties applicables aux produits et services HP sont celles figurant dans les déclarations de garantie expresse accompagnant les dits produits et services. Aucun terme de ce document ne peut être interprété comme constituant une garantie supplémentaire. HP ne peut en aucun cas être tenu pour responsable des erreurs ou omissions techniques ou rédactionnelles du présent document.

Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.

Légende de restriction des droits

Logiciel confidentiel. Licence HP valide requise pour la détention, l'utilisation ou la copie. En accord avec les articles FAR 12.211 et 12.212, les logiciels informatiques, la documentation des logiciels et les informations techniques commerciales sont concédés au gouvernement américain sous licence commerciale standard du fournisseur.

Copyright

Marques

Adobe™ est une marque déposée de Adobe Systems Incorporated.

Microsoft® et Windows® sont des marques déposées de Microsoft Corporation aux États-Unis.

UNIX® est une marque déposée de The Open Group.

Ce produit inclut une interface de la bibliothèque de compression d'usage général 'zlib', Copyright © 1995 - 2002 Jean-loup Gailly et Mark Adler.

Remerciements

Mises à jour de la documentation

La page de titre du présent document contient les informations d'identifications suivantes :

- le numéro de version du logiciel ;
- la date de publication du document, qui change à chaque mise à jour de ce dernier ;
- la date de lancement du logiciel.

Pour obtenir les dernières mises à jour ou vérifier que vous disposez de l'édition la plus récente d'un document, accédez à la page : **http://h20230.www2.hp.com/selfsolve/manuals**

Pour accéder à ce site, vous devez créer un compte HP Passport et vous connecter comme tel. Pour obtenir un identifiant HP Passport, accédez à l'adresse : **http://h20229.www2.hp.com/passport-registration.html**

Vous pouvez également cliquer sur le lien **New users - please register** dans la page de connexion de HP Passport.

En vous abonnant au service d'assistance du produit approprié, vous recevrez en outre les dernières mises à jour ou les nouvelles éditions. Pour plus d'informations, contactez votre revendeur HP.

Assistance

Visitez le site d'assistance HP Software à l'adresse : **http://www.hp.com/go/hpsoftwaresupport**

Ce site fournit les informations de contact et les détails sur les offres de produits, de services et d'assistance HP Software.

L'assistance en ligne de HP Software propose des fonctions de résolution autonome. Le site constitue un moyen efficace d'accéder aux outils interactifs d'assistance technique nécessaires à la gestion de votre activité. En tant que client privilégié de l'assistance, vous pouvez depuis ce site :

- rechercher des documents de connaissances présentant un réel intérêt ;
- soumettre et suivre des demandes d'assistance et des demandes d'améliorations ;
- télécharger des correctifs logiciels ;
- gérer des contrats d'assistance ;
- rechercher des contacts de l'assistance HP ;
- consulter les informations sur les services disponibles ;
- participer à des discussions avec d'autres utilisateurs d'un même logiciel ;
- rechercher des cours de formation sur les logiciels et vous y inscrire.

Pour accéder à la plupart des offres d'assistance, vous devez vous enregistrer en tant qu'utilisateur disposant d'un compte HP Passport et vous identifier comme tel. De nombreuses offres nécessitent en outre un contrat d'assistance. Pour obtenir un identifiant HP Passport, accédez à l'adresse suivante :

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

Les informations relatives aux niveaux d'accès sont détaillées à l'adresse suivante :

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

HP Software Solutions Now accède au site Web du portail HPSW Solution and Integration. Ce site vous permet d'explorer les pages de HP Product Solutions qui comprendent une liste complète des intégrations entre produits HP, ainsi qu'une liste des processus ITIL. L'URL de ce site Web est **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Table des matières

Sécurisation de HP Operations Orchestration

Ce document décrit la configuration de la sécurité et la sécurisation de HP Operations Orchestration.

Pour plus d'informations sur les tâches d'administration, voir le manuel *HP OO Administration Guide*.

Limitation de responsabilité

Ce manuel a pour but de vous fournir des conseils pour protéger votre déploiement HP OO contre d'éventuels risques ou menaces pouvant compromettre la sécurité. La sécurisation d'une application vise principalement à protéger la confidentialité, l'intégrité et la disponibilité des données critiques d'une société. Toutefois, pour garantir la protection de vos données HP OO, vous devez sécuriser à la fois HP OO et l'environnement informatique (par exemple, l'infrastructure) dans lequel vous exécutez l'application.

Ce manuel décrit uniquement les opérations permettant de sécuriser HP OO au niveau de l'application et ne donne aucune information concernant la sécurisation de l'infrastructure au sein de l'environnement du client. Le client assume l'entière responsabilité de l'organisation et du fonctionnement de son infrastructure/environnent, ainsi que des stratégies à appliquer pour en garantir la sécurité.

Recommandations pour la sécurisation

1. Installez la version la plus récente de HP OO. Pour plus d'informations, voir le manuel *HP OO Installation Guide*.
2. (Facultatif) Configurez HP OO pour la mise en conformité avec la norme FIPS 140-2. Si vous optez pour cette solution, vous devez effectuer cette opération avant de démarrer le serveur Central. Voir " Configuration de HP OO pour la mise en conformité avec la norme FIPS 140-2 Niveau 1" , page 22.
3. Configurez le certificat du serveur Central pour le chiffrement TLS et le certificat du client pour l'authentification forte (mutuelle).

   Remarque : Vous pouvez effectuer cette opération pendant l'installation.

   Pour le RAS, le Débogage et OOSH, fournissez l'authentification du certificat si nécessaire (pour le certificat du serveur) et utilisez le certificat du client pour l'authentification sur le serveur Central. Voir "Authentification via certificat de serveur et de client" , page suivante.
4. Sécurisez le serveur HP OO Central en éliminant le port HTTP et en remplaçant les mots de passe KeyStore et TrustStore par des mots de passe forts (complexes). Voir "Modification ou désactivation des ports HTTP/HTTPS" , page 14 et "Modification du mot de passe KeyStore/TrustStore" , page 11.
5. Sécurisez HP OO Studio en remplaçant les mots de passe KeyStore et TrustStore par des mots de passe forts. Voir "Modification du mot de passe KeyStore/TrustStore" , page 11.
6. Supprimez l'algorithme de chiffrement RC4 des algorithmes pris en charge par SSL. Voir "Suppression de l'algorithme de chiffrement RC4 des algorithmes pris en charge par SSL" , page 14.

7. (Facultatif) Configurez la version du protocole TLS. Voir "Configuration du protocole TLS" , page 28.
8. Activez l'authentification dans Central. Voir « Activation de l'authentification » dans le *Manuel de l'utilisateur de HP OO Central*.

   Les utilisateurs internes ne sont pas sécurisés, vous devez donc utiliser un système LDAP sécurisé à l'aide de mots de passe forts. Voir « Configuration de la sécurité - Authentification LDAP » dans le *Manuel de l'utilisateur de HP OO Central*.
9. Sécurisez le système d'exploitation et la base de données.
10. Ajoutez une bannière de sécurité avec un message très explicite. Par exemple, « Vous essayez de vous connecter à notre environnement de PRODUCTION ! Ne poursuivez pas l'opération si vous ne connaissez pas les règles de gouvernance de ce système et si vous n'avez pas suivi la formation adéquate. » Voir « Configuration d'une bannière de sécurité » dans le *Manuel de l'utilisateur de HP OO Central*.
11. Dans l'environnement Windows et SQL Server, configurez HP OO de façon à utiliser l'authentification Windows. Voir « Configuration de HP OO pour fonctionner avec l'authentification Windows » dans le *manuel de base de données HP OO*.
12. Assurez-vous que l'audit est activé dans Central. Pour plus d'informations, voir « Activation de l'audit » dans le *Manuel de l'utilisateur de HP OO Central*.

Authentification via certificat de serveur et de client

Les certificats Transport Layer Security (TLS) associent numériquement une clé de chiffrement aux détails d'une organisation, ce qui permet d'établir des connexions sécurisées entre un serveur Web et un navigateur.

HP OO gère les clés de chiffrement et les certificats de confiance à l'aide de l'utilitaire Keytool. Cet utilitaire se trouve dans le dossier d'installation de HP OO, dans **<Répertoire d'installation>/java/bin/keytool**. Pour plus d'informations sur l'utilitaire Keytool, consultez http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html.

Remarque : Keytool est un utilitaire Open Source.

Les installations de HP OO Central contiennent deux fichiers pour la gestion des certificats :

- **<répertoire d'installation>/central/var/security/client.truststore** : contient la liste des certificats de confiance.
- **<répertoire d'installation>/central/var/security/key.store** : contient le certificat HP OO (clé privée).

Il est conseillé de remplacer le certificat HP OO auto-signé après une nouvelle installation de HP OO ou si votre certificat actuel a expiré.

Chiffrement de la communication avec un certificat de serveur

Remplacement du certificat de serveur TLS de Central

Vous pouvez utiliser un certificat signé par une autorité de certificat bien connue ou un certificat de serveur personnalisé d'une autorité de certificat locale.

Remplacez les paramètres qui sont mis en évidence en <jaune> pour adapter l'emplacement du fichier **key.store** et autres détails à votre ordinateur.

Remarque : La procédure suivante utilise l'utilitaire Keytool qui se trouve dans **<répertoire d'installation>/java/bin/keytool**.

1. Arrêtez Central et réalisez une sauvegarde du fichier **key.store** original qui se trouve dans **<répertoire d'installation>/central/var/security/key.store**.
2. Ouvrez une ligne de commande dans **<répertoire d'installation>/central/var/security**.
3. Supprimez le certificat de serveur existant dans le fichier **key.store** de Central à l'aide de la commande suivante :

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

4. Si vous possédez déjà un certifcat avec l'extension **.pfx** ou **.p12**, passez à l'étape suivante. Dans le cas contraire, il faudra exporter le certificat avec la clé privée au format PKCS12 (.pfx, .p12). Par exemple, si le certificat est au format PEM :

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

Si le certificat est au format DER, ajoutez le paramètre `–inform DER` après pkcs12. Par exemple :

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

Remarque : Prenez note du mot de passe que vous fournissez. Vous aurez besoin de ce mot de passe pour la clé privée lorsque vous devrez saisir la phrase secrète KeyStore plus loin dans cette procédure.

Veillez à choisir un mot de passe fort.

5. Affichez l'alias de l'alias du certificat dans la liste via la commande suivante :

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

   L'alias du certificat apparaît et vous devrez le spécifier dans la prochaine commande.

   Dans l'exemple ci-dessous, il s'agit de la quatrième ligne à partir du bas.

   ```
   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. Importez le certificat de serveur de format PKCS12 dans le fichier **key.store** de Central à l'aide de la commande suivante :

   ```
   keytool -importkeystore -srckeystore <chemin d'accès au certificat au format
   PKCS12> -destkeystore key.store -srcstoretype pkcs12 -deststoretype JKS -alias
   <alias du certificat> -destalias tomcat
   ```

7. Si le certificat de serveur importé a un mot de passe différent de celui du certificat de serveur original, il est important de modifier le mot de passe keyPass. Suivez les instructions fournies dans "Modification du mot de passe KeyStore/TrustStore" , page 11.

   Il est également recommandé de modifier le mot de passe par défaut « changeit » dans le KeyStore généré automatiquement dans le serveur Central. Voir "Modification du mot de passe KeyStore/TrustStore" , page 11.

8. Démarrez Central.

Importation d'une autorité de certificat racine dans un TrustStore de RAS

Après avoir installé un RAS, si vous utilisez un certifcat racine personnalisé pour Central et que vous n'aviez pas désigné ce certificat pendant l'installation du RAS, il faudra importer l'autorité de certificat racine de confiance dans le **client.truststore** du RAS. Si vous utilisez une autorité de certificat racine connue (telle que Verisign), il n'est pas nécessaire de réaliser la procédure suivante car le certificat se trouvera déjà dans le fichier **client.truststore**.

Par défaut, HP OO prend en charge tous les certificats auto-signés. Toutefois, dans un environnement de production, il est recommandé, pour des raisons de sécurité, de remplacer ce paramètre par défaut par une autorité de certificat personnalisée ou bien connue.

Remplacez les paramètres qui sont mis en évidence en <jaune>.

Remarque : La procédure suivante utilise l'utilitaire Keytool qui se trouve dans **<répertoire d'installation>/java/bin/keytool**.

1. Arrêtez RAS et réalisez une sauvegarde du fichier **client.truststore** original qui se trouve dans **<répertoire d'installation>/ras/var/security/client.truststore**.
2. Ouvrez une ligne de commande dans **<répertoire d'installation>/ras/var/security**.
3. Ouvrez le fichier **<répertoire d'installation> ras/conf/ras-wrapper.conf** et attribuez la valeur **false** à `-Dssl.support-self-signed`. Ceci active l'autorité de certificat racine de confiance.

   Par exemple :

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

4. Ouvrez le fichier **<répertoire d'installation> ras/conf/ras-wrapper.conf** et attribuez la valeur **true** à `-Dssl.verifyHostName`. Ceci vérifie que le FQDN du certificat correspond bien au FQDN de la demande.

   Par exemple :

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

5. Importez l'autorité de certificat de confiance racine dans le fichier **client.truststore** du RAS, s'il ne figure pas déjà dans la liste (par défaut, toutes les autorités de certificat connues se trouvent là) :

   ```
   keytool -importcert -alias <alias_quelconque> -keystore client.truststore -file <nom_certificat.cer> -storepass <changeit>
   ```

6. Démarrez RAS.

Importation d'une autorité de certificat racine dans le TrustStore de OOSH

Si vous utilisez un certificat racine personnalisé pour Central, il faudra importer l'autorité de certificat racine de confiance dans le **client.truststore** d'OOSH. Si vous utilisez une autorité de certificat racine connue (telle que Verisign), il n'est pas nécessaire de réaliser la procédure suivante car le certificat se trouvera déjà dans le fichier **client.truststore**.

Par défaut, HP OO prend en charge tous les certificats auto-signés. Toutefois, dans un environnement de production, il est recommandé, pour des raisons de sécurité, de remplacer ce paramètre par défaut par une autorité de certificat personnalisée ou bien connue.

Remplacez les paramètres qui sont mis en évidence en <jaune>.

Remarque : La procédure suivante utilise l'utilitaire Keytool qui se trouve dans **<répertoire d'installation>/java/bin/keytool**.

1. Arrêtez Central et réalisez une sauvegarde du fichier **client.truststore** original qui se trouve dans **<répertoire d'installation>/central/var/security/client.truststore**.
2. Modifiez le fichier **oosh.bat** dans **<répertoire d'installation>/central/bin**.
3. Attribuez la valeur **false** à `-Dssl.support-self-signed`. Ceci active l'autorité de certificat racine de confiance.

   Par exemple :

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

4. Attribuez la valeur **true** à `-Dssl.verifyHostName`. Ceci vérifie que le FQDN du certificat correspond bien au FQDN de la demande.

   Par exemple :

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

5. Importez l'autorité de certificat de confiance racine dans le fichier **client.truststore** de Central, s'il ne figure pas déjà dans la liste (par défaut, toutes les autorités de certificat connues se trouvent là) :

   ```
   keytool -importcert -alias <alias_quelconque> -keystore client.truststore -file <nom_certificat.cer> -storepass <changeit>
   ```

6. Exécutez OOSH.
7. Démarrez Central.

Importation d'une autorité de certificat racine dans le TrustStore du débogage de Studio

Une fois que Studio a été installé, si vous utilisez un certificat racine personnalisé pour Studio, il faudra importer l'autorité de certificat racine de confiance dans le **client.truststore** de Studio. Si vous utilisez une autorité de certificat racine connue (telle que Verisign), il n'est pas nécessaire de réaliser la procédure suivante car le certificat se trouvera déjà dans le fichier **client.truststore**.

Par défaut, HP OO prend en charge tous les certificats auto-signés. Toutefois, dans un environnement de production, il est recommandé, pour des raisons de sécurité, de remplacer ce paramètre par défaut par une autorité de certificat personnalisée ou bien connue.

Remplacez les paramètres qui sont mis en évidence en <jaune>.

Remarque : La procédure suivante utilise l'utilitaire Keytool qui se trouve dans **<répertoire d'installation>/java/bin/keytool**.

1. Quittez Studio et réalisez une sauvegarde du fichier **client.truststore** original qui se trouve dans **<répertoire d'installation>/studio/var/security/client.truststore**.
2. Modifiez le fichier **Studio.l4j.ini** dans **<rép_installation>/studio**.
3. Attribuez la valeur **false** à `-Dssl.support-self-signed`. Ceci active l'autorité de certificat racine de confiance.

   Par exemple :

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

4. Attribuez la valeur **true** à `-Dssl.verifyHostName`. Ceci vérifie que le FQDN du certificat correspond bien au FQDN de la demande.

   Par exemple :

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

5. Importez l'autorité de certificat de confiance racine dans le fichier **client.truststore** de Studio, s'il ne figure pas déjà dans la liste (par défaut, toutes les autorités de certificat connues se trouvent là) :

   ```
   keytool -importcert -alias <alias_quelconque> -keystore client.truststore -file <nom_certificat.cer> -storepass <changeit>
   ```

6. Démarrez Studio.

Pour plus d'informations, voir « Debugging a Remote Central with Studio » dans le manuel *Studio Authoring Guide*.

Modification du mot de passe KeyStore/TrustStore

Modification des mots de passe KeyStore, TrustStore et du certificat de serveur dans la configuration de Central

1. Assurez-vous que Central est en cours d'exécution.

   Remarque : Avant d'effectuer cette étape, vérifiez s'il y a des mots de passe chiffrés. Pour plus d'informations sur le chiffrement des mots de passe, voir "Encrypting Passwords" dans le manuel *HP OO Administration Guide*.

   À partir de OOSH, exécutez la commande suivante :

   ```
   set-sys-config --key <NomClé> --value <MotDePasseChiffré>
   ```

   en remplaçant `<NomClé>` par l'une des valeurs du tableau ci-dessous :

Élément de configuration	Action
key.store.password	Pour définir le mot de passe d'accès au **key.store**. La valeur par défaut est `"changeit"`. Il doit avoir la même valeur que `keystorePass`, décrit dans les étapes ci-dessous.
key.store.private.key.alias.password	Pour définir le mot de passe utilisé pour le certificat de serveur (clé privée) dans le **key.store**. La valeur par défaut est `"changeit"`.

	Il doit avoir la même valeur que `keyPass`, décrit dans les étapes ci-dessous.

2. Arrêtez le service Central.
3. Modifiez le mot de passe KeyStore, TrustStore et du certificat de serveur à l'aide de Keytool.
4. Modifiez également les mots de passe dans le fichier **server.xml** qui se trouve dans **<rép_installation>/central/tomcat/conf/server.xml**.
   a. Localisez le connecteur HTTPS Par exemple :

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

   b. Modifiez le mot de passe requis.
      - `keyPass` : mot de passe utilisé pour accéder à la clé privé du certificat de serveur depuis le fichier key.store indiqué. La valeur par défaut est "`changeit`".
      - `keystorePass` : le mot de passe pour accéder au fichier key.store indiqué. La valeur par défaut est la valeur de l'attribut `keyPass`.

        Remarque : Il est conseillé de ne pas utiliser le même mot de passe que pour **keyPass** et de choisir un mot de passe fort.

      - `truststorePass` : le mot de passe pour accéder au TrustStore (qui contient toutes les autorités de certificat de confiance). La valeur par défaut est la valeur de la propriété système **javax.net.ssl.trustStorePassword**. Si la valeur de cette propriété est null, aucun mot de passe TrustStore ne sera configuré. Si un mot de passe TrustStore non valide est proposé, un avertissement sera consigné et une tentative d'accès au TrustStore sans mot de passe sera réalisée, qui ignorera la validation du contenu du TrustStore.

   c. Enregistrez le fichier.
5. Modifiez le fichier **central-wrapper.conf** qui se trouve dans **<rép_installation> central\conf\central-wrapper.conf** de la façon suivante :

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

6. Lancez le service Central.

Modification des mots de passe RAS, OOSH et TrustStore Studio

Remarque : Vous devez modifier les mots de passe KeyStore, TrustStore et du certificat de serveur à l'aide de Keytool, avant d'effectuer les opérations suivantes.

- **Pour modifier le mot de passe du TrustStore RAS autonome** : Modifiez le fichier **ras-wrapper.conf** et modifiez le paramètre `changeit` du TrustStore.
- **Pour modifier le mot de passe du TrustStore OOSH** : Modifiez le fichier **oosh.bat** et modifiez le paramètre `changeit` du TrustStore.
- **Pour modifier le mot de passe du TrustStore Studio** : Modifiez le fichier **<rép_ installation>/studio/Studio.l4j.ini** et remplacez le paramètre `changeit` du TrustStore par le nouveau mot de passe en mode camouflé.

  Pour plus d'informations sur le camouflage des mots de passe, voir « How to Encrypt a Password » dans le manuel *HP OO Administration Guide*.

Camouflage des mots de passe KeyStore et TrustStore Studio

Dans HP 10.20 et les versions ultérieures, les mots de passe KeyStore et TrustStore de Studio sont camouflés. Après la mise à niveau de la version 10.10 à la version 10.20, ces mots de passe seront camouflés uniquement s'ils n'ont pas été modifiés dans le fichier **<rép_ installation>/studio/Studio.l4j.ini**. Tout mot de passe modifié dans les versions précédentes ne sera pas automatiquement camouflé pendant la mise à niveau.

Si vous souhaitez changer le mot de passe TrustStore ou KeyStore, vous pouvez le faire dans le fichier **Studio.l4j.ini** en mode camouflé ou texte lisible. Une fois que vous avez modifié les mots de passe, vous devez les camoufler manuellement, afin de garantir qu'ils n'apparaîtront pas en texte lisible dans le Gestionnaire de tâches pour le processus Studio :

1. Fermez Studio.
2. Repérez le script **encrypt-password** dans **<dossier_installation>/central/bin**.
3. Camouflez le mot de passe personnalisé à l'aide de la commande suivante :

   ```
   encrypt-password.bat --obfuscate <votre mot de passe>
   ```

4. Modifiez les mots de passe du fichier **<rép_installation>/studio/Studio.l4j.ini** pour les paramètres suivants :

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

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

5. Modifiez le mot de passe KeyStore et TrustStore Studio à l'aide de keytool dans le dossier **<rép_ installation>/studio/var/security/**.

   Remarque : Si le certificat du client n'est pas configuré pour le débogueur distant Studio, l'argument du chemin d'accès keyStore sera ignoré.

6. Démarrez Studio.

Important ! Après l'utilisation du script **encrypt-password**, effacez l'historique des commandes.

En effet, sous Linux, le paramètre du mot de passe est stocké en texte lisible sous **/$USER/.bash_history** et il est accessible à l'aide de la commande `history`.

Suppression de l'algorithme de chiffrement RC4 des algorithmes pris en charge par SSL

L'hôte distant prend en charge l'utilisation de l'algorithme de chiffrement RC4. Cet algorithme présente un défaut dans la création d'un flux d'octets pseudo-aléatoire qui entraîne l'insertion d'un large éventail de petits écarts dans le flux, ce qui réduit son caractère aléatoire.

Si du texte brut est chiffré à plusieurs reprises (par exemple, des cookies HTTP) et qu'un attaquant parvient à obtenir plusieurs (à savoir, des dizaines de millions) de textes de chiffrement, il pourrait arriver à découvrir le texte brut.

Désactiver l'algorithme de chiffrement RC4 au niveau du JRE (à partir de Java 7) :

1. Ouvrez le fichier **$JRE_HOME/lib/security/java.security**.
2. Désactivez l'algorithme de chiffrement RC4 en supprimant les commentaires et en modifiant les paramètres comme indiqué dans l'exemple ci-dessous :

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

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

3. Redémarrez le serveur HP OO Central.

Pour plus d'informations, consultez http://stackoverflow.com/questions/18589761/restict-cipher-suites-on-jre-level.

Remarque : Après la mise à niveau d'une version antérieure à HP OO 10.x, répétez ces étapes.

Modification ou désactivation des ports HTTP/HTTPS

Le fichier **server.xml** sous **[OO_HOME]/central/Tomcat/conf** contient deux éléments baptisés **<Connector>** sous l'élément **<Service>**. Ces connecteurs définissent ou activent les ports que le serveur écoute.

La configuration de chaque connecteur est définie via ses attributs. Le premier connecteur définit un connecteur HTTP régulier tandis que le deuxième définit un connecteur HTTPS.

Par défaut, les connecteurs ressemblent à ceci.

Connecteur HTTP :

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

Connecteur HTTPS :

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

Les deux sont activés par défaut.

Important ! Si vous modifiez ou désactivez l'un des ports de Central dans le fichier **server.xml**, vous devrez également mettre à jour le fichier **central-wrapper.conf** et chaque fichier **RAS-wrapper.conf** pour renvoyer à l'URL de Central avec le nouveau port. Dans le cas contraire, tous vos flux échoueront lorsque vous les exécuterez depuis Central. Assurez-vous également de bien vérifier les configurations du répartiteur de charge.

Modification des valeurs du port

Pour modifier les valeurs d'un des ports :

1. Modifiez le fichier **server.xml** qui se trouve dans **<rép_ installation>/central/tomcat/conf/server.xml**.
2. Localisez le connecteur HTTP ou HTTPS et modifiez la valeur **port** dans la ligne.

   Remarque : Si HTTP et HTTPS sont tous les deux actifs et que vous souhaitez modifier le port HTTPS, il faudra modifier la valeur **redirectPort** pour le connecteur HTTP et la valeur **port** pour le connecteur HTTPS.
3. Enregistrez le fichier.
4. Redémarrez Central.

Désactivation d'un port

Vous pouvez, par exemple, décider de désactiver le port HTTP pour des raisons de sécurité, afin que le seul canal de communication possible soit sur TLS et chiffré.

Pour désactiver un des ports :

1. Modifiez le fichier **server.xml** qui se trouve dans **<rép_ installation>/central/tomcat/conf/server.xml**.
2. Localisez le connecteur HTTP ou HTTPS et supprimez la ligne ou désactivez-la à l'aide d'un commentaire.
3. Importez l'autorité de certificat de confiance racine dans le fichier **client.truststore** de Central, s'il ne figure pas déjà dans la liste :

```
keytool -importcert -alias <alias_quelconque> -keystore client.truststore -file
<nom_certificat.cer> -storepass <changeit>
```

Remarque : Si vous utilisez une autorité de certificat racine connue (telle que Verisign), il n'est pas nécessaire de réaliser cette procédure car le certificat se trouvera déjà dans le fichier **client.truststore**.

4. Enregistrez le fichier.
5. Redémarrez Central.

Remarque : Il est également possible de désactiver le port HTTP pendant l'installation.

Dépannage

Si le serveur ne démarre pas, ouvrez le fichier **wrapper.log** et recherchez une erreur dans `ProtocolHandler ["http-nio-8443"]`.

Ceci peut se produire lorsque Tomcat s'initialise ou lance le connecteur. Il existe plusieurs versions, mais le message d'erreur peut fournir des informations.

Tous les paramètres du connecteur HTTPS se trouve dans le fichier de configuration Tomcat qui se trouve à l'emplacement **C:\HP\oo\central\tomcat\conf\server.xml**.

Ouvrez le fichier et parcourez-le jusqu'à ce que vous trouviez le connecteur HTTPS :

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

Vérifiez s'il y a des incohérences dans les paramètres en les comparant aux paramètres saisis lors des étapes antérieures.

Authentification par certificat client (authentification mutuelle)

L'authentification par certificat X.509 est la plus souvent utilisée pour vérifier l'identité d'un serveur avec le protocole TLS, généralement dans le cadre de l'utilisation du protocole HTTPS depuis un navigateur. Le navigateur vérifie automatiquement si le certificat présenté par un serveur a été émis par une des autorités de certification de confiance qui figure sur la liste que le serveur maintient.

Vous pouvez utiliser également TLS avec l'authentification mutuelle. Le serveur sollicite un certificat valide du client dans le cadre de la liaison TLS. Le serveur authentifie le client en confirmant que son certificat a été signé par une autorité acceptable. Si un certificat valide a été fourni, il peut être obtenu via l'API du servlet dans une application.

Configuration de l'authentification par certificat du client dans Central

Avant de configurer l'authentification par certificat de client dans Central, confirmez que vous avez configuré le certificat de serveur TLS, conformément à la description de la section "Authentification via certificat de serveur et de client" , page 6.

Donnez la valeur `true` à l'attribut `clientAuth` si vous souhaitez que la pile TLS demande au client une chaîne de certificat valide avant d'accepter une connexion. Attribuez la valeur `want` si vous souhaitez que la pile TLS demande un certificat au client, sans prévoir d'échec si aucun certificat n'est présenté. La valeur `false` (par défaut) ne requiert aucune chaîne de certificat sauf si le client sollicite une ressource protégée par une contrainte de sécurité qui utilise l'authentification CLIENT-CERT. (Pour plus d'informations, voir le manuel Apache Tomcat Configuration Reference).

Définissez le fichier **Liste de révocation des certificats (CRL)**. Il peut contenir plusieurs CRL. Dans certains systèmes de chiffrement, en général des infrastructures à clé publique (PKI), une liste de révocation des certificats désigne une liste de certificats (ou plus spécialement, une liste de numéros de série pour certificats) qui ont été révoqués et par conséquent, il ne faut plus faire confiance aux entités qui présentent ces certificats (révoqués).

Remarque : La procédure suivante utilise l'utilitaire Keytool qui se trouve dans **<répertoire d'installation>/java/bin/keytool**.

1. Arrêtez le serveur Central.
2. Importez le certificat racine (CA) approprié dans Central **client.truststore** : **<rép_ installation>/central/var/security/client.truststore**, s'il ne figure pas déjà dans la liste (par défaut, toutes les autorités de certificat connues se trouvent là). Par exemple :

   ```
   keytool -importcert -alias <alias_quelconque> -keystore
   <chemin>/client.truststore -file <chemin_certificat> -storepass <changeit>
   ```

3. Modifiez le fichier **server.xml** qui se trouve dans **<rép_ installation>/central/tomcat/conf/server.xml**.
4. Attribuez la valeur `want` ou `true` à l'attribut `clientAuth` dans la balise `Connector`. La valeur par défaut est `false`.

   Remarque : Il est recommandé de démarrer les serveur à la fin de cette procédure, mais vous pouvez le démarrer maintenant.

5. (Facultatif) Ajoutez l'attribut `crlFile` pour définir le fichier de liste de révocation de certificats pour la validation du certificat TLS, par exemple :

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

   Le fichier peut porter l'extension `.crl` pour une seule liste de révocation de certificats ou l'extension `.pem` (format PEM CRL) pour une ou plusieurs listes de révocation de certificats. Le format PEM CRL utilise l'en-tête et le pied de page suivant :

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

Exemple de structure de fichier `.pem` pour une liste de révocation de certificats (pour plusieurs listes, ajoutez un autre bloc 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. Démarrez le serveur Central.

Remarque : Pour chaque certificat de client, vous devez définir un utilisateur, soit interne, soit utilisateur LDAP. Le nom de l'utilisateur doit être défini dans les attributs du certificat. La valeur par défaut est l'attribut CN. Pour plus d'informations, voir Traitement du principal de certificat.

Sachez que même si HP OO est configuré avec plusieurs configurations LDAP, il est uniquement possible d'authentifier l'utilisateur à l'aide des attributs de certificat de client avec le LDAP par défaut. Central essaiera d'abord d'authentifier l'utilisateur avec le LDAP par défaut et, en cas d'échec, il tentera l'authentification au sein du domaine interne HP OO.

Mise à jour de la configuration d'un certificat de client dans RAS

Le certificat de client est configuré lors de l'installation du RAS. Toutefois, si vous devez actualiser le certificat, vous pouvez réaliser l'opération manuellement dans le fichier **ras-wrapper.conf**.

Prérequis : vous devez importer le certificat racine de l'autorité CA de Central dans le TrustStore de RAS. Voir "Importation d'une autorité de certificat racine dans un TrustStore de RAS" , page 8.

Pour actualiser la configuration du certificat de client dans un RAS externe :

1. Arrêtez le serveur RAS.
2. Ouvrez le fichier **ras-wrapper.conf** dans **<répertoire d'installation>ras/var/conf/ras-wrapper.conf**.
3. Modifiez la ligne suivante en fonction de votre certificat de client :

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

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

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

4. Démarrez le serveur RAS.

Remarques importantes ! Le certificat de client X.509 doit avoir le nom principal du RAS, qui est l'identifiant du RAS (voir Traitement d'un principal de certificat).

L'identifiant du RAS figure sous l'onglet **Topologie** dans Central. Voir la rubrique « Configuration de la topologie – Travailleurs » dans le *Manuel de l'utilisateur de HP OO Central*.

Configuration d'un certificat de client dans le débogueur à distance de Studio

Prérequis : vous devez importer le certificat racine de l'autorité CA de Central dans le TrustStore de Studio Debugger. Voir "Importation d'une autorité de certificat racine dans le TrustStore du débogage de Studio" , page 10.

Pour configurer le certificat de client dans le débogueur à distance de Studio.

1. Fermez Studio.
2. Modifiez le fichier **Studio.l4j.ini** dans **<rép_installation>/studio**.
3. Modifiez la ligne suivante en fonction de votre certificat de client :

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

-Djavax.net.ssl.keyStorePassword=changeit

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

4. Démarrez Studio.

Remarques :

- Dans HP OO 10.20 et versions ultérieures, le paramètre `keyStorePassword` dans **Studio.l4j.ini** est camouflé par défaut, si le mot de passe par défaut est conservé. Vous pouvez modifier ce paramètre et l'enregistrer en texte lisible ou camouflé.
- Pour le certificat de client, vous devez définir un utilisateur, soit interne, soit utilisateur LDAP. Le nom de l'utilisateur doit être défini dans les attributs du certificat. La valeur par défaut est l'attribut CN. Pour plus d'informations, voir Traitement du principal de certificat.
- Sachez que même si HP OO est configuré avec plusieurs configurations LDAP, il est uniquement possible d'authentifier l'utilisateur à l'aide des attributs de certificat de client avec le LDAP par défaut. Central essaiera d'abord d'authentifier l'utilisateur avec le LDAP par défaut et, en cas d'échec, il tentera l'authentification au sein du domaine interne HP OO.

Configuration d'un certificat de client dans OOSH

Prérequis : vous devez importer le certificat racine de l'autorité CA de Central dans le TrustStore de OOSH. Voir "Importation d'une autorité de certificat racine dans le TrustStore de OOSH" , page 9.

1. Arrêtez OOSH.
2. Modifiez le fichier **oosh.bat** dans **<répertoire d'installation>/central/bin**.

3. Modifiez la ligne suivante en fonction de votre certificat de client :

```
-Djavax.net.ssl.keyStore="<répertoire
d'installation>/var/security/certificate.p12"

-Djavax.net.ssl.keyStorePassword=changeit

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

4. Démarrez OOSH.

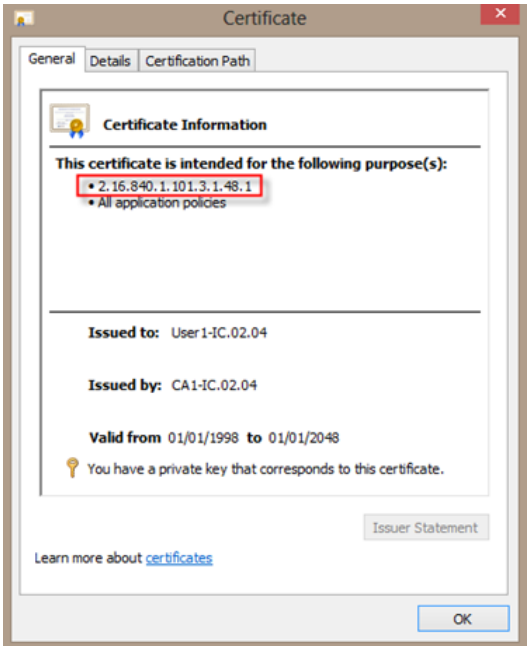
Remarque : Pour le certificat de client, vous devez définir un utilisateur, soit interne, soit utilisateur LDAP. Le nom de l'utilisateur doit être défini dans les attributs du certificat. La valeur par défaut est l'attribut CN. Pour plus d'informations, voir Traitement du principal de certificat.

Sachez que même si HP OO est configuré avec plusieurs configurations LDAP, il est uniquement possible d'authentifier l'utilisateur à l'aide des attributs de certificat de client avec le LDAP par défaut. Central essaiera d'abord d'authentifier l'utilisateur avec le LDAP par défaut et, en cas d'échec, il tentera l'authentification au sein du domaine interne HP OO.

Traitement des stratégies de certificat

HP OO gère le traitement des stratégies de certificat pour le certificat final.

- Vous pouvez définir la chaîne d'objectif dans le certificat.
- HP OO vous permet d'ajouter la ou les chaînes de stratégie en tant qu'élément de configuration et de vérifier chaque chaîne de stratégie pour chaque certificat final. En l'absence de correspondance, rejetez le certificat.
- Activez ou désactivez la vérification de la stratégie de certificat en ajoutant l'élément de configuration suivant : `x509.certificate.policy.enabled=true/false` (la valeur par défaut est `false`).
- Définissez la liste de stratégie en ajoutant l'élément de configuration suivant : `x509.certificate.policy.list=<liste_séparée_par_des_virgules>` (la valeur par défaut est une liste vide).



Pour plus d'informations sur la modification des propriétés système de HP OO, voir le manuel *HP OO Shell User Guide*.

Traitement d'un principal de certifcat

Vous pouvez définir la manière d'obtenir le principal d'un certificat à l'aide d'une équivalence d'expression régulière sur `Subject`. L'expression régulière doit compter un seul groupe. L'expression par défaut `CN=(.?)` établit l'équivalence avec le champ nom commun. Par exemple, `CN=Jimi Hendrix, OU=` affecte un nom d'utilisateur de `Jimi Hendrix`.

- Les équivalences sont sensibles à la casse.
- Le principal du certificat est le nom d'utilisateur dans HP OO (utilisateur LDAP ou interne).
- Pour changer l'expression régulière, changez l'élément de configuration : `x509.subject.principal.regex`.

Pour plus d'informations sur la modification des propriétés système de HP OO, voir le manuel *HP OO Shell User Guide*.

Configuration de HP OO pour la mise en conformité avec la norme FIPS 140-2 Niveau 1

Cette section explique comment configurer HP Operations Orchestration afin de garantir la conformité à la norme Federal Information Processing Standards (FIPS) 140-2 Niveau 1.

La norme FIPS 140-2 est une norme qui porte sur les exigences en matière de sécurité applicables aux modules de chiffrements définies par le National Institute of Standards Technology (NIST). Pour consultez la publication de cette norme, rendez-vous à : csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Après que vous avez configuré HP OO en vue de la conformité avec FIPS 140-2, HP OO utilise l'algorithme de sécurité suivant :

- Algorithme à clé symétrique : AES256
- Algorithme de hachage : SHA256

HP OO utilise le fournisseur de sécurité suivant : logiciel RSA BSAFE Crypto version 6.1.Il s'agit du seul fournisseur de sécurité pris en charge pour FIPS 140-2.

Remarque : Une fois que vous aurez configuré HP OO pour le rendre conforme à la norme FIPS 140-2, la seule manière de revenir à la configuration standard consiste à réinstaller HP OO.

Prérequis

Remarque : Si vous effectuez la mise à niveau à partir d'une installation de HP OO 10.10 (et ultérieure) déjà configurée avec FIPS, vous devez répéter les étapes 4 et 5 ci-dessous, puis répéter les étapes de la section « Configurer les propriétés du fichier de sécurité java » dans "Configuration de HP OO pour respecter la norme FIPS 140-2" , page 24.

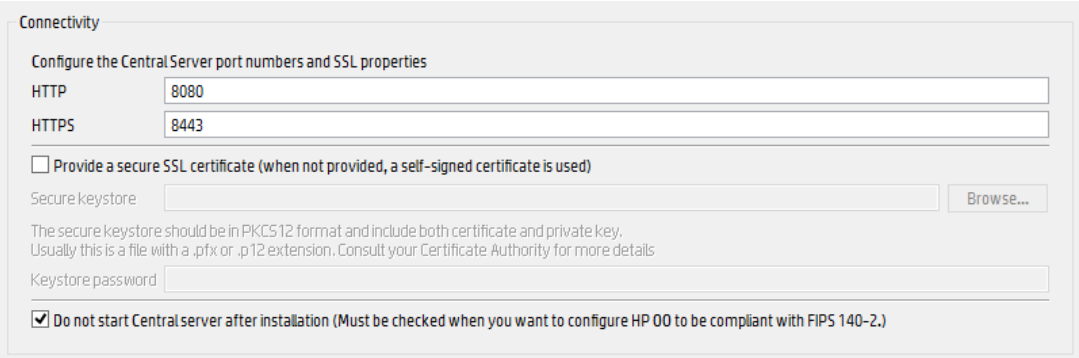
Avant de configurer HP OO pour le rendre conforme à la norme FIPS 140-2; réalisez les opérations suivantes :

Remarque : Pour la conformité FIPS 140-2, il faut désactiver LWSSO.

1. Pour respecter la norme FIPS 140-2, vérifiez que vous êtes en train de configurer une nouvelle installation de HP OO version 10.10 ou ultérieure, et que celle-ci n'est pas en cours d'utilisation.

   Vous ne pouvez pas configurer une installation de HP OO en cours d'utilisation (quelle que soit la version, 9.x ou 10.x).
2. Confirmez après l'installation de HP OO qu'il a été configuré pour ne pas démarrer le serveur Central après l'installation :

- Dans une installation silencieuse, la valeur **no** a été attribuée au paramètre `should.start.central`.
- Dans l'installation via un Assistant, à l'étape **Connectivité**, la case **Ne pas démarrer le serveur Central après l'installation** a été cochée.



3. Sauvegardez les répertoires suivants :
   - **<répertoire d'installation>\central\tomcat\webapps\oo.war**
   - **<répertoire d'installation>\central\tomcat\webapps\PAS.war**
   - **<répertoire d'installation>\central\conf**
   - **<oo_jre>\lib\security** (où **<oo_jre>** est le répertoire dans lequel le JRE utilisé par HP OO est installé. Par défaut, il s'agit de **<rép_installation>\java**)
4. Téléchargez et installez les fichiers Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction Policy depuis le site suivant : http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html.

   Remarque : Voir le fichier **ReadMe.txt** du contenu téléchargé pour savoir comment déployer les fichiers et mettre le JRE utilisé par HP OO à jour.
5. Installez les fichiers du logiciel RSA BSAFE Crypto. Sur le système où HP OO est installé, copiez les éléments suivants dans **<oo_jre>\lib\ext** (où **<oo_jre>** est le répertoire dans lequel le JRE utilisé par HP OO est installé. Par défaut, il s'agit de **<rép_installation\java**).
   - **<répertoire d'installation>\central\lib\cryptojce-6.1.jar**
   - **<répertoire d'installation>\central\lib\cryptojcommon-6.1.jar**
   - **<répertoire d'installation>\central\lib\jcmFIPS-6.1.jar**

Remarque : Si vous effectuez la mise à niveau à partir d'une installation de HP OO 10.10 (et ultérieure) déjà configurée avec FIPS, vous devez répéter les étapes 4 et 5 de la section « Prérequis » ci-dessus, puis répéter les étapes de la section « Configurer les propriétés du fichier de sécurité java » dans "Configuration de HP OO pour respecter la norme FIPS 140-2" , page suivante.

Configuration de HP OO pour respecter la norme FIPS 140-2

La liste suivante décrit les procédures à exécuter pour mettre HP OO en conformité avec la norme FIPS 140-2 :

- Configurer les propriétés du fichier de sécurité java
- Configurer le fichier encryption.properties et activer le mode FIPS
- Créer un chiffrement HP OO conforme avec la norme FIPS
- Re-chiffrer le mot de passe de la base de données avec le nouveau chiffrement
- Démarrer HP OO.

Configurer les propriétés du fichier de sécurité java

Modifiez le fichier de sécurité Java pour le JRE afin d'ajouter des fournisseurs de sécurité complémentaires et configurez les propriétés pour garantir la conformité à la norme FIPS 140-2.

Remarque : La mise à niveau à HP OO 10.10 remplace complètement les fichiers JRE installés. Par conséquent, les étapes suivantes doivent être réalisées après la mise à niveau à 10.10.

Remarque : Si vous effectuez la mise à niveau à partir d'une installation de HP OO 10.10 (et ultérieure) déjà configurée avec FIPS, vous devez répéter les étapes 4 et 5 de la section « Prérequis » dans " Configuration de HP OO pour la mise en conformité avec la norme FIPS 140-2 Niveau 1" , page 22, puis répéter les étapes ci-dessous.

Ouvrez le fichier **<oo_jre>\lib\security\java.security** dans un éditeur et réalisez les étapes suivantes :

1. Pour chaque fournisseur indiqué, au format **security.provider.<nn>=<nom_du_fournisseur>**, augmentez le numéro d'ordre de préférence `<nn>` de 2.

   Par exemple, modifiez une entrée de fournisseur de :

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

   en

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

2. Ajoutez un nouveau fournisseur par défaut (RSA JCE) Ajoutez le fournisseur suivant en haut de la liste des fournisseurs :

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

3. Ajoutez le fournisseur Java Secure Sockets Extension (JSSE) de RSA BSAFE SSL-J.

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

4. Copiez et collez la ligne suivante dans le fichier **java.security** pour confirmer que **RSA BSAFE** est utilisé dans un mode conforme à FIPS 140-2 :

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

Vous pouvez copier cette ligne n'importe où dans le fichier **java.security**.

5. Étant donné que l'algorithme par défaut ECDRBG128 de DRGB n'est pas sûr (selon NIST), définissez la propriété de sécurité **com.rsa.crypto.default** sur **HMACDRBG**, en copiant la ligne suivante dans le fichier **java.security** :

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

   Vous pouvez copier cette ligne n'importe où dans le fichier **java.security**.
6. Enregistrez et fermez le fichier **java.security**.

Configurer le fichier encryption.properties et activer le mode FIPS

Le fichier de propriétés de chiffrement de HP OO doit être mis à jour afin d'être conforme à la norme FIPS 140-2.

1. Sauvegardez le fichier **encryption.properties**, situé dans **<répertoire_installation>\central\var\security**.
2. Ouvrez le fichier **encryption.properties** dans un éditeur de texte. Par exemple, modifiez le fichier suivant :

   C:\Program Files\Hewlett-Packard\HP Operations Orchestration\central\var\security\encryption.properties.
3. Localisez `keySize=128` et remplacez-le par `keySize=256`.
4. Localisez `secureHashAlgorithm=SHA1` et remplacez-le par `secureHashAlgorithm=SHA256`.
5. Localisez `FIPS140ModeEnabled=false` et remplacez-le par `FIPS140ModeEnabled=true`.

   Remarque : Si `FIPS140ModeEnabled=false` n'existe pas, ajoutez `FIPS140ModeEnabled=true` en tant que nouvelle ligne à la fin du fichier.
6. Enregistrez et fermez le fichier.

Créer un chiffrement HP OO conforme avec la norme FIPS

Pour créer ou remplacer le fichier de stockage de chiffrement de HP OO afin de le rendre conforme à FIPS, voir "Remplacement du chiffrement FIPS" , page suivante.

Remarque : AES possède trois longueurs de clé approuvés : 128/192/256 selon la publication NIST SP800-131A

Les algorithmes de hachage sécurisés suivants sont pris en charge dans la norme FIPS : SHA1, SHA256, SHA384, SHA512.

Remarque : Il est recommandé de modifier les mots de passe du keystore (ainsi que sa clé privée) et du truststore. Voir "Modification du mot de passe KeyStore/TrustStore" , page 11.

Remarque : Il est recommandé de supprimer du truststore HP OO tous les certificats racine par défaut de l'autorité CA qui ne sont pas utilisés. (Le fichier **client.truststore** est situé dans **<rép_installation>/central/var/security**.)

Re-chiffrer le mot de passe de la base de données avec le nouveau chiffrement

Re-chiffrez le mot de passe de la base de données en suivant les instructions du manuel *HP OO Administration Guide*, dans la section « Changing the Database Password ».

Démarrer HP OO.

Démarrez HP OO comme décrit dans le manuel *HP OO 10.10 Installation Guide*.

Remplacement du chiffrement FIPS

HP OO, Central et RAS adhèrent à la norme Federal Information Processing Standard 140-2 (FIPS 140-2) qui définit les exigences techniques que les organismes fédéraux doivent respecter lorsqu'ils mettent en place des systèmes de sécurité à chiffrement pour la protection des données sensibles ou de valeur.

Après une installation directe de HP OO 10.10, vous avez la possibilité de modifier la clé de chiffrement FIPS.

Remarque : Cette procédure concerne uniquement les nouvelles installations. Elle ne peut être exécutée après une mise à jour.

Modification de la clé de chiffrement FIPS sur Central

1. Accédez au dossier **<rép_installation_Central>/var/security**.
2. Réalisez une sauvegarde du fichier **encryption_repository** et supprimez-le.
3. Accédez au dossier **<rép_installation_Central>/bin/**.
4. Exécutez le script **generate-keys**.

   Accédez au dossier **<rép_installation_Central>/var/security/encryption_repository**.

Modification des propriétés de chiffrement de RAS

Si l'installation du RAS se trouve dans un nouvel emplacement, il faudra réaliser toutes les étapes ci-dessous.

Remarque : Ces modifications sont uniquement valides si vous travaillez sur une nouvelle installation RAS après que vous avez modifié les propriétés de chiffrement de Central.

Pour modifier les propriétés de chiffrement du RAS :

1. Réalisez toutes les étapes décrites dans la section « Prérequis » de " Configuration de HP OO pour la mise en conformité avec la norme FIPS 140-2 Niveau 1" , page 22.
2. Réalisez toutes les étapes décrites dans la section « Configurer les propriétés du fichier de sécurité java » de "Configuration de HP OO pour respecter la norme FIPS 140-2" , page 24.
3. Copiez le fichier actuel **encryption.properties** depuis **<rép_installation>\ras\var\security** vers le dossier **<rép_installation>\ras\bin**
4. À l'aide d'un éditeur de texte, modifiez le contenu du fichier **encryption.properties** en fonction des besoins.

   Pour plus d'informations, voir « Configurer le fichier encryption.properties et activer le mode FIPS » dans "Configuration de HP OO pour respecter la norme FIPS 140-2" , page 24.
5. Enregistrez les modifications.
6. Ouvrez une invite de ligne de commande dans le dossier **<rép_installation>\ras\bin**.
7. Exécutez **oosh.bat**.
8. Exécutez la commande OOShell : `replace-encryption --file encryption.properties`

   Remarque : Si vous aviez copié le fichier **encryption.properties** dans un autre dossier, confirmez que vous avez saisi l'emplacement correct dans la commande OOShell.
9. Redémarrez le service RAS.

Configuration du protocole TLS

Vous pouvez configurer HP OO pour définir la version du protocole TSL prise en charge. Par défaut, HP OO reconnaît TLS v1, TLS v1.1 et TLS v1.2, mais vous pouvez limiter davantage.

Remarque : SSLv3 et les autres versions de SSL ne sont pas prises en charge.

1. Ouvrez le fichier **<rép_installation>/central/tomcat/conf/server.xml**.
2. Repérez le connecteur SSL (à la fin du fichier).
3. Modifiez la valeur par défaut de `sslEnabledProtocols`. Par exemple, vous pouvez remplacer `sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"` par `sslEnabledProtocols="TLSv1.2"`
4. Redémarrez le serveur.


Java™
COMPATIBLE