Hewlett Packard Enterprise

Operations Orchestration

Version du logiciel : 10.60
Systèmes d'exploitation Windows et Linux

Manuel de sécurité et sécurisation

Date de publication du document : Mai 2016

Date de lancement du logiciel : Mai 2016

Mentions légales

Garantie

Les seules garanties applicables aux produits et services Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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.

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

Ce site nécessite un HP Passport et une connexion. Pour obtenir un ID de HP Passport, cliquez sur **S'inscrire** dans le site HP Software Support ou cliquez sur **Créer un compte** sur la page de connexion 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 commercial HPE.

Table des matières

Introduction

Bienvenue dans le Manuel de sécurité et sécurisation de HPE OO.

Ce manuel est conçu pour faciliter le travail du personnel informatique qui doit déployer et gérer les instances de HPE Operations Orchestration (HPE OO) ide manière sécurisée. Notre objectif est d'aider ce personnel à prendre les décisions correctes concernant les capacités et les fonctionnalités fournies par HPE OO pour faire face aux exigences de sécurité des entreprises modernes.

Les exigences de sécurité de l'entreprise sont en constante évolution et ce manuel peut être considéré comme la meilleure réponse de HPE à ces strictes exigences. Dans le cas d'exigences de sécurité supplémentaires non traitées par ce manuel, vous êtes priés d'ouvrir une fiche d'assistance auprès de l'équipe d'assistance HPE pour les en informer de manière à inclure la rubrique dans les éditions futures.

Vue d'ensemble du système technique

HPE OO est une application à l'échelle de l'entreprise basée sur la technologie J2EE (Java 2 Enterprise Edition). La technologie J2EE propose une approche basée sur des composants pour la conception, développement, assemblage et déploiement des applications d'entreprise.

Mises à jour de la sécurité

De la version OO 10.20 à la version 10.50, les mises à jour de sécurité suivantes ont été effectuées :

- Si la case **Activer la capture des utilisateurs identifiés** est cochée dans Central, HPE OO capture temporairement (de manière sécurisée) les informations d'identification de l'utilisateur connecté lorsque ce dernier exécute des flux dans Remote Debugger. Un message avertit que les informations d'identification peuvent être capturées.
- Dans HPE OO 10.5x, la valeur ne comporte aucun rôle par défaut. De cette manière, l'administrateur peut mieux contrôler l'autorisation de l'utilisateur, car les utilisateurs obtiennent les rôles qui leurs sont explicitement affectés ou qui le sont à leur groupe LDAP.
- Lorsque HPE OO comporte plusieurs configurations LDAP, l'administrateur peut marquer l'une d'elles en tant que valeur par défaut de sorte que les utilisateurs y appartenant n'aient pas à sélectionner un domaine à la connexion.
- HPE OO 10.5x sécurise les données sensibles (par exemple, les mots de passe) au cours de l'exécution. Si une variable est marquée comme sensible dans Studio, elle sera récupérée chiffrée pour l'utilisation dans les scriptlets.

De HPE OO 10.10 à 10.20 les mises à jour de la sécurité suivantes ont été effectuées :

- Il est désormais possible d'octroyer les autorisations aux comptes système dans HPE OO. L'administrateur a ainsi la possibilité de déterminer les utilisateurs qui peuvent consulter les divers comptes système et exécuter les flux qui les utilisent. Cette fonction est idéale pour les clients ayant plusieurs organisations, car elle permet de masquer certains comptes système pour certains utilisateurs.

  Pour plus d'informations, voir « Content Management Enhancements - Apply Permissions to Multiple Roles » dans le document *OO 10.20 Release Notes*.

- Il est désormais possible d'appliquer des autorisations à plusieurs rôles dans la boîte de dialogue Modifier les autorisations. Dans la versions précédentes, vous pouviez sélectionner un rôle à la fois.

  Pour plus d'informations, voir « Content Management Enhancements - Permissions for System Accounts » dans le document *OO 10.20 Release Notes*.

- Lorsque vous mettez à niveau une installation OO d'une version 10.x antérieure, le TrustStore SSL est mis à jour pour intégrer les certificats racine de confiance actualisés, tels qu'ils ont été publiés par Oracle. Les certificats expirés sont supprimés et les nouveaux sont importés à leur place.

  Pour plus d'informations, voir « Installation Enhancements - Updated Trusted Root Certificates » dans le document *OO 10.20 Release Notes*.

- OO propose désormais une fonction d'audit pour les événements, ce qui vous permet d'effectuer le suivi des violations de la sécurité. L'audit garde la trace des actions réalisées dans Central, notamment les connexions, les déclenchements de flux, la création de planifications, la modification de configurations, etc.

  Actuellement, vous pouvez récupérer le journal d'audit uniquement via API. Pour plus d'informations, voir le manuel *OO API Guide*.

- OO prend désormais en charge les clés de chiffrement ayant une longueur de 2 048 bits (et plus). Ceci aligne les clés de chiffrement à la norme FIPS 186-4.

- Une nouvelle propriété sslEnabledProtocols a été ajoutée au fichier **server.xml** (situé dans **<rép_installation>/central/tomcat/conf/server.xml**) :

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

  Cette propriété vérifie que seuls les protocoles TLS v1, TLS v1.1 et TLS v1.2 sont autorisés et que SSL 3.0 ne l'est pas. Ceci permet d'empêcher la vulnérabilité à la faille POODLE (Padding Oracle On Downgraded Legacy Encryption).

Documents connexes

Pour plus d'informations sur la sécurisation de OO, voir les documents suivants :

- *OO Network Architecture White Paper*

Pour plus d'informations sur OO, voir les documents suivants :

- *Manuel Concepts de OO*
- *Manuel Administrateur de OO*
- *Manuel Architecture de OO*
- *Manuel Base de données OO*
- *Manuel de l'utilisateur de OO Central*
- *Manuel de OO Studio Authoring*
- *Notes de version OO*
- *Manuel d'installation, mise à niveau et configuration de OO*
- *Configuration requise OO*
- *Manuel de l'utilisateur de OO Studio Wizards*

Vous trouverez ces documents et d'autres ressources utiles sur HPE Live Network (https://hpln.hp.com/node/21/otherfiles#).

Sécurité - Aperçu

Cette section fournit un aperçu des modèles de sécurité et des recommandations pour une mise en œuvre sécurisée de HPE OO. Les rubriques concernent l'authentification, l'autorisation, le chiffrement, etc. Vous trouverez également des références à d'autres documents HPE OO qui décrivent les tâches relatives à la sécurité.

Sécurité - Concepts

Glossaire HPE OO

Pour plus d'informations sur les concepts de HPE OO, voir le manuel *Concepts de HPE OO*.

Autorisation de rôle

Une autorisation est une capacité prédéfinie pour réaliser une tâche. HPE Central est livré avec un ensemble d'autorisations qui peuvent être affectées à des rôles.

Par exemple, l'autorisation **Planifier** permet à son détenteur de voir et de créer des planifications d'exécution de flux.

Rôle

Un rôle est une collection d'autorisations.

Par exemple, le rôle **Administrateur de flux** peut être autorisé à **Afficher les planifications** et **Gérer les planifications**.

Utilisateur

Un utilisateur est un objet associé à une personne (ou identité d'application) pour représenter cette personne et définir ses autorisations.

Les rôles sont affectés aux utilisateurs afin de déterminer les actions qu'ils sont autorisés à réaliser dans Central. Par exemple, le rôle **Administrateur de flux** peut être affecté à l'utilisateur Pierre Durand.

Plusieurs types d'utilisateurs différents peuvent être configurés :

- Les **utilisateurs LDAP** se connectent à Central à l'aide de leur nom d'utilisateur et de leur mot de passe LDAP. Par exemple en utilisant leur nom d'utilisateur et mot de passe Active Directory.
- Les **utilisateurs internes** se connectent à Central à l'aide du nom d'utilisateur et du mot de passe définis en local dans Central.
- **LWSSO** - HPE Lightweight Single Sign On (SSO) est un mécanisme qui permet à une seule action d'authentification et d'autorisation de l'utilisateur d'accéder à tous les systèmes HPE qui prennent an charge LWSSO. Par exemple, si un utilisateur ouvre une session dans un autre client Web d'un produit HPE pour lequel l'authentification LWSSO a été activée, comme le client Web SM ou BSM, cet utilisateur pourra accéder à l'application HPE OO Central directement sans passer par l'écran d'ouverture de session de HPE OO Central.

Quand un utilisateur interne et un utilisateur LDAP possédant le même rôle sont connectés, il n'existe aucune différence entre leurs autorisations.

Remarque : Il est recommandé d'utiliser des utilisateurs LDAP plutôt que des utilisateurs internes, car les utilisateurs LDAP sont sécurisés selon des stratégies mise en œuvre par le fournisseur LDAP.

Autorisation du contenu

L'autorisation du contenu est une autorisation qui permet de consulter ou d'exécuter des flux individuels ou des flux dans un dossier en particulier.

Les utilisateurs qui ont reçu un rôle en particulier pourront accéder aux flux en fonction des autorisations du contenu associées à leur rôle.

Par exemple, les utilisateurs possédant le rôle **Administrateur** peuvent être autorisés à afficher et à exécuter tous les flux du système, tandis que ceux qui possèdent le rôle **Utilisateur** pourront exécuter certains flux et consulter les autres.

Sécurité - Concepts communs

Sécurité du système

Processus et mécanismes à travers lesquels les équipements informatiques, les données et les services sont protégés des accès, modifications ou dommages non intentionnels ni autorisés.

Privilège de base

Méthode qui consiste à limiter l'accès au niveau minimum nécessaire pour permettre le fonctionnement normal. Cela revient à octroyer au compte utilisateur uniquement les privilèges essentiels au travail de cet utilisateur.

Authentification

Processus d'identification d'un individu, normalement basé au nom d'utilisateur et mot de passe, ou certificat.

Autorisation

Permission d'accéder aux objets système selon l'identité de l'individu.

Chiffrement

Méthode pour améliorer la sécurité d'un message ou fichier en brouillant le contenu de sorte qu'ils puissent être lus uniquement par les personnes possédant la clé de chiffrement pour le décoder. Par exemple, le protocole TLS chiffre les données de communication.

Contre-mesure

Moyen d'atténuer le risque d'une menace.

Défense en profondeur

Méthode qui consiste à mettre en œuvre plusieurs couches de protection pour ne pas devoir se fier à une seule mesure de sécurité.

Risque

Événement probable pouvant causer un dommage. Par exemple, perte financière, dommage à l'image de la société, etc.

Menace

Déclenchement d'un événement de risque qui exploite une faille.

Vulnérabilité

Faiblesse d'une cible pouvant être potentiellement exploitée par une menace de sécurité.

Mise en œuvre et déploiement sécurisés

Paramètres de sécurité par défaut

Dans plusieurs cas, il est recommandé de modifier les paramètres de sécurité prêts à l'emploi fournis par défaut.

- **Authentification** - par défaut, l'authentification n'est pas activée dans Central. Il est recommandé de l'activer au plus tôt une fois les utilisateurs configurés. Pour plus d'informations, voir « Activation de l'authentification » dans le *Manuel de l'utilisateur de HPE OO Central*.
- **Audit** - par défaut, l'audit n'est pas activé dans Central. Il est recommandé de l'activer. Pour plus d'informations, voir « Activation de l'audit » dans le *Manuel de l'utilisateur de HPE OO Central*.
- **Chiffrement TLS** - Par défaut, HPE OO prend en charge 3 protocoles TLS : 1.0, 1.1, 1.2. Il est recommandé de travailler avec la version plus récente. Pour plus d'informations, voir « Configuration du protocole TLS », page 66.
- **Certificat de serveur TLS** : par défaut, l'utilisateur doit fournir un certificat d'autorité de certification au cours de l'installation du serveur OO.
- **Certificat client** - par défaut, le certificat client n'est pas activé. Il est recommandé de travailler avec un certificat client pour l'authentification à Central. Pour plus d'informations, voir « Configuration de l'authentification par certificat du client dans Central », page 51.
- **KeyStore, TrustStore et certificat de serveur** - par défaut, les mots de passe Java sont fournis pour le magasin de clé, magasin d'approbation et certificat de serveur. Il est recommandé de remplacer ces mots de passe chiffrés. Pour plus d'informations, voir « Modification et chiffrement/camouflage du mot de passe du keystore/truststore », page 44
- **Chiffrement RC4** - par défaut, le chiffrement RC4 est activé. Il est recommandé de désactiver le chiffrement RC4 au niveau JRE. Pour plus d'informations, voir « Suppression de l'algorithme de chiffrement RC4 des algorithmes pris en charge par SSL », page 48.
- **Bannière de sécurité** - par défaut, la bannière de sécurité n'est pas activée dans Central. Il est recommandé de l'activer avec un message personnalisé. Pour plus d'informations, voir « Configuration d'une bannière de sécurité » dans le *Manuel de l'utilisateur de HPE OO Central*.
- **Authentification Windows de la base de données** - par défaut, l'authentification Windows n'est pas activée dans Central. Si vous travaillez dans l'environnement Windows et SQL Server, configurez HPE OO de façon à utiliser l'authentification Windows. Voir « Configuration de HPE OO pour fonctionner avec l'authentification Windows » dans le *Manuel de base de données HPE OO*.

- **Algorithmes par défaut** - le fichier **encryption.properties** contient les algorithmes par défaut. Pour respecter la norme FIPS, voir « Configuration de HPE OO pour la mise en conformité avec la norme FIPS 140-2 Niveau 1 », page 59. Pour plus d'informations sur les valeurs par défaut de FIPS 140-2 niveau 1, voir « Encryption Administration » dans « Chiffrement », page 23.
- **Stratégie Java** - par défaut, le fichier **java.policy** n'est pas sécurisé. Pour plus d'informations sur la modification du fichier **java.policy**, voir « Interdire aux flux l'accès au système de fichiers local de Central/RAS », page 67.

Sécurisation de HPE OO

Le chapitre Sécurisation a pour but de vous fournir des conseils pour protéger votre déploiement HPE 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.

Pour garantir la protection totale de votre système HPE OO, vous devez sécuriser à la fois HPE OO et l'environnement informatique (par exemple, l'infrastructure) dans lequel vous exécutez l'application.

Le chapitre Sécurisation fournit les opérations permettant de sécuriser HPE 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.

Sécurité physique

HP Software recommande que HPE OO soit protégé par des contrôles de sécurité physique définis par votre organisation. Les composants du serveur HPE OO sont installés dans un environnement physiquement sécurisé selon les pratiques conseillées. Par exemple, le serveur doit se trouver dans une pièce fermée dont l'accès est contrôlé.

Consignes d'installation sécurisée

Systèmes d'exploitation pris en charge

Pour plus d'informations sur les types et les versions de systèmes d'exploitation pris en charge, voir le manuel *HPE OO*.

Recommandations de sécurisation du système d'exploitation

Contactez le fournisseur du système d'exploitation pour connaître les pratiques conseillées pour sécuriser le système d'exploitation.

Par exemple :

- Les correctifs à installer
- Les services et logiciels à désinstaller ou désactiver
- Les autorisations minimales à affecter aux utilisateurs
- Activation de l'audit

Sécurisation de Tomcat

Lorsque vous installez HPE OO Central, Tomcat est partiellement sécurisé par défaut. Si vous recherchez une sécurisation supplémentaire, voir les recommandations du chapitre Sécurisation.

Autorisations d'installation

Les autorisations suivantes sont requises pour installer et exécuter HPE OO :

Installation de HPE OO	Windows/Linux : Tout utilisateur en mesure d'exécuter un processus Java et qui est autorisé à créer des dossiers et des services
Exécution de HPE OO	• Windows : Le service Windows est exécuté sous le compte de l'utilisateur système ou d'un utilisateur spécifique (l'utilisateur doit pouvoir accéder au répertoire d'installation de HPE OO) • Linux : Tout utilisateur standard en mesure d'exécuter un processus Java

Voir également les recommandations du document CIS Apache Tomcat 7.0.

Sécurité du réseau et des communications

Le *Manuel d'architecture de HPE OO* décrit les principes de sécurité OO concernant la topologie, la haute disponibilité et le répartiteur de charge.

Le document *HPE OO Network Architecture White Paper* décrit la configuration requise du pare-feu et propose deux solutions pour les cas où, à cause de restrictions de la stratégie, la configuration requise du pare-feu ne peut pas être mise en œuvre :

- Tunnel SSH inverse
- Proxy inverse

Sécurité du canal de communication

Protocoles pris en charge et configuration

HPE OO prend en charge le protocole TLS.

Pour plus d'informations, voir « Remplacement du certificat de serveur TLS de Central », page 38.

Les ports Central sont définis par l'administrateur au cours de l'installation.

Sécurité du canal

HPE OO prend en charge les canaux sécurisés suivants :

Canal (redirigé)	Protocole sécurisé pris en charge
OOSH, navigateur, Studio Remote Debugger ou RAS → Central	Pour un canal sécurisé, utilisez la communication TLS pour le chiffrement et le certificat client pour l'authentification.
Central → serveur LDAP	Pour chiffrer la communication entre Central et LDAP, utilisez Secure LDAP, via le protocole TLS.

Sécurité des serveurs RAS

Dans une topologie de serveur RAS inverse (qui attend que le serveur Central établisse la connexion), le mécanisme suivant assure la sécurité du RAS :

- Si plusieurs tentatives de connexion consécutives échouent (à cause d'une erreur de saisie de la clé secrète partagée), un certain délai va s'écouler.

Pour plus d'informations sur les serveurs RAS inverses, voir « Configuration de la topologie - Travailleurs et serveurs RAS » dans le *Manuel de l'utilisateur de HPE OO Central*.

Sécurité de l'interface d'administration

Accès à l'interface d'administration

Plusieurs moyens sont disponibles pour contrôler l'accès à l'interface d'administration :

- Informations d'identification
- Certificat client
- SAML

Sécurisation de l'interface d'administration - Recommandations

1. Il est recommandé d'activer l'authentification dans Central.

   Voir « Activation de l'authentification » dans le *Manuel de l'utilisateur de HPE OO Central*.

2. Il est recommandé de sécuriser l'interface d'administration avec le protocole TLS. Vous devez configurer TLS entre le client et l'interface Central pour le chiffrement.

   Voir « Fonctionnement des certificats serveur et client », page 37.

3. Il est recommandé de travailler avec des utilisateurs LDAP au lieu des utilisateurs internes, car c'est plus sûr.

4. Il est recommandé de configurer l'authentification pour accéder à Central via les certificats client. C'est plus sûr des mots de passe utilisateur.

   Voir « Fonctionnement des certificats serveur et client », page 37.

Gestion et authentification de l'utilisateur

Modèle d'authentification

Pour faciliter l'amorçage du mécanisme d'authentification dans HPE OO, celle-ci est désactivée au premier démarrage.

Il est vivement recommandé d'activer l'authentification immédiatement après l'installation.

Pour plus d'informations, voir « Activation de l'authentification » dans le *Manuel de l'utilisateur de HPE OO Central*.

Plusieurs méthodes sont disponibles pour authentifier l'accès à Central.

Choisissez la méthode d'identification des utilisateurs :

- Nom d'utilisateur et mot de passe
- Certificat client
- Jeton SAML
- LWSSO (authentification unique) HPE

Choisissez la méthode de gestion des utilisateurs :

- Utilisateurs LDAP enregistrés sur serveur LDAP comme Active Directory (recommandée)
- Utilisateurs et mots de passe internes enregistrés en local sur serveur Central (non recommandée)

Types d'utilisateurs

L'autorisation affectée à l'utilisateur varie selon le type d'utilisateur. Par exemple, auteur de flux, administrateur, administrateur système, etc.

Pour plus d'exemples sur les différents types d'utilisateurs, exigeant différentes autorisations, voir « Personnages principaux » dans le manuel *Concepts de OO*.

Administration et configuration de l'authentification

Utilisateurs internes ou LDAP

Vous pouvez configurer les utilisateurs internes avec des mots de passe dans l'interface de Central ou définir l'utilisateur dans le serveur LDAP et mapper les groupes LDAP sur les rôles de Central.

Remarque : Nous déconseillons d'utiliser les utilisateurs internes. Utilisez plutôt une solution plus sécurisée comme les utilisateurs LDAP.

Pour plus d'informations sur la configuration d'utilisateurs internes, voir « Configuration de la sécurité - Utilisateurs internes » dans le *Manuel de l'utilisateur de OO Central*.

Pour plus d'informations sur le mappage des groupes LDAP sur les rôles de Central, voir « Configuration de la sécurité - Authentification LDAP » dans le Manuel de l'utilisateur de *OO Central* et « LDAP Configuration » dans le manuel *OO API Guide*.

SAML / Certificats client / LWSSO

Pour plus d'informations sur la configuration de Central pour opérer avec SAML, voir « Configuration de la sécurité - SAML » dans le *Manuel de l'utilisateur de OO Central*.

Pour plus d'informations sur la configuration de Central pour opérer avec les certificats client, voir « Fonctionnement des certificats serveur et client », page 37.

Pour plus d'informations sur la configuration de Central pour opérer avec l'authentification unique LWSSO, voir « Configuration de la sécurité - LWSSO » dans le *Manuel de l'utilisateur de OO Central*, « Configuring LWSSO » dans le manuel *OO Administration Guide* et « LW SSO » dans le manuel *OO API Guide*.

Authentification de la base de données

OO prend en charge quatre bases de données : Oracle, MS SQL, MySQL et Postgres.

Il est recommandé d'utiliser un mot de passe fort pour l'authentification de la base de données et une forte stratégie de mot de passe. Par exemple, le verrouillage après un certain nombre de tentatives échouées.

Avec MS SQL, vous pouvez choisir entre l'authentification de la base de données ou l'authentification du SE. Nous recommandons de'opérer avec l'authentification du SE, si possible. Par exemple, vous pouvez utiliser l'authentification Windows au moment d'accéder aux bases de données Microsoft SQL Server.

- Pour plus d'informations sur la configuration de l'authentification du SE, voir « Configuration de OO pour fonctionner avec l'authentification Windows » dans le *Manuel de la base de données HPE OO*.
- Voir « Changing the Database Password » dans le manuel *HPE OO System Administration Guide*.
- Voir les pratiques recommandées par le fournisseur de la base de données (si disponibles).

Autorisation

Modèle d'autorisation

L'accès utilisateur aux ressources HPE OO est autorisé selon le rôle de l'utilisateur et les autorisations configurées pour ce rôle.

Voir :

- « Configuration de la sécurité - Rôles » dans le *Manuel de l'utilisateur de HPE OO Central*
- « Affectation d'autorisations à un compte système » dans le *Manuel de l'utilisateur de HPE OO Central*.

Consignes d'autorisations minimales

Il est recommandé de :

- Sélectionner les autorisations appropriées pour le rôle
- Utiliser des autorisations minimales lorsque vous créez des rôles.
- Octroyer des autorisations minimales et les étendre uniquement selon les exigences pour éviter une hausse non souhaitée des privilèges. Par exemple, commencer par les autorisations Affichage et y ajouter les autorisations nécessaires au cas par cas.

Configuration de l'autorisation

Central est installé avec de nombreux rôles prêts à l'emploi que vous pouvez configurer et affecter aux utilisateurs. Par défaut, les rôles prêts à l'emploi disposent des autorisations suivantes :

Rôle	Autorisations par défaut
Administrator	Toutes
End_user	Aucune
Everybody	Aucune
Promoter	Toutes les autorisations relatives au **contenu**
System_admin	Toutes les autorisations relatives au **système**

Rôle par défaut

Il est possible de configurer l'un des rôles avec l'attribut **Rôle par défaut**. Le cas échéant, vérifiez que ce rôle comporte les plus bas privilèges. Sachez que lorsque vous attribuez des autorisations à ce rôle, ceci affecte tous les utilisateurs LDAP en plus de ceux explicitement associés à ce rôle.

Pour plus d'informations, voir « Affection d'un rôle en tant que rôle par défaut » dans le *Manuel de l'utilisateur de HPE OO Central*.

Voir également :

- « Affectation d'autorisations à un compte système » dans le *Manuel de l'utilisateur de HPE OO Central*.
- « Définition des autorisations pour le contenu » dans le *Manuel de l'utilisateur de HPE OO Central*

Accéder aux Espaces de travail dans Studio

Lorsque vous créez plusieurs espaces de travail dans Studio, nous vous recommandons d'en créer un dans les dossiers dans lesquels seul l'auteur est autorisé à lire et à écrire.

Les espaces de travail créés dans des dossiers publics sont accessibles à tous les utilisateurs, ce qui risque de compromettre des données sensibles ou même de les divulguer.

Sauvegarde

Dans le but d'éviter toute perte de données, il est vivement recommandé de sauvegarder périodiquement vos données du serveur sur des médias sécurisés. Ceci est également utile pour les récupérations d'urgence et la continuité de l'activité de l'entreprise.

Après avoir installé OO, effectuez une sauvegarde du dossier **central\var\security** et du fichier **central\conf\database.properties**.

Certaines données du schéma de base de données sont chiffrées et les clés de déchiffrement sont stockées en local sur le serveur OO Central. Si ces fichiers système sont endommagés ou supprimés, le schéma devient inutile car vous n'aurez plus aucun moyen pour déchiffrer les données.

Remarque : Étant donné que les clés sont chiffrées, il est important de les inclure dans la sauvegarde. Les clés sont situées dans le dossier **security**.

Voir :

- « Backing Up OO » dans le manuel *OO Administration Guide*
- « Setting up Disaster Recovery » dans le manuel *OO Administration Guide*
- « Backing Up and Recovering the Central Security Files » dans le *Manuel d'installation de OO*
- « Using a Load Balancer in HP OO Deployment » dans le manuel *OO Architecture Guide*

Chiffrement

Modèle de chiffrement

Pour protéger les données sensibles, HPE OO prend en charge le chiffrement et les algorithmes de hachage. Le chiffrement est conçu pour empêcher l'exposition et la modification des données sensibles, telles que les mots de passe, les définitions, etc. dans le système HPE OO.

Afin d'empêcher le déchiffrement par des personnes non autorisées, il est important d'utiliser des algorithmes standard connus sans failles découvertes.

Remarque : Par exemple, SSL n'est pas utilisé à cause des failles connues dans le protocole SSL.

Données statiques

Tous les mots de passe stockés sont protégés au moyen d'algorithmes connus et aucun n'est laissé en clair.

Par exemple :

- Les mots de passe du compte système sont chiffrés.
- Les mots de passe de l'utilisateur interne sont hachés.
- Les mots de passe de la base de données sont chiffrés.

Données en transit

OO utilise le protocole TLS (Transport Layer Security) pour chiffrer les données entre les composants (tels que les serveurs Central et RAS).

Désactivation du port HTTP

Il est recommandé de désactiver le port HTTP pour des raisons de sécurité, afin que le seul canal de communication possible soit sur TLS et chiffré. Pour plus d'informations, voir « Modification des ports HTTP/HTTPS ou désactivation du port HTTP », page 48.

Administration du chiffrement

Pratiques conseillées pour le chiffrement

Afin d'atteindre des niveaux supérieurs de sécurité et de chiffrement, il est recommandé de configurer OO pour le rendre conforme à la norme FIPS (Federal Information Processing Standards) 140-2. OO peut être configuré pour respecter le niveau 1 de la norme FIPS 140-2.

Jeu de configurations par défaut

- Algorithme à clé symétrique : AES avec taille de clé 128
- Algorithme de hachage : SHA1

Paramètres avancés

Après avoir configuré OO pour sa conformité avec FIPS 140-2, OO utilise l'algorithme de sécurité suivant :

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

Voir « Configuration de HPE OO pour respecter la norme FIPS 140-2 », page 62.

Certificats numériques

Un certificat numérique est un passeport électronique pour une personne, serveur, gare, etc

- Pour utiliser le chiffrement entre un navigateur et le serveur Central, vous devez installer un certificat numérique côté serveur.
- Pour utiliser le certificat client pour authentifier le serveur Central, vous devez installer un certificat client côté client (par exemple, sur le navigateur, RAS, OOSH, Studio, etc.).

OO gère les clés de chiffrement et les certificats de confiance à l'aide de l'utilitaire Keytool Java. Cet utilitaire se trouve dans le dossier d'installation de OO, dans **<rép_installation>/java/bin/keytool**.

Emplacement du certificat

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

- **<rép_installation>/central/var/security/client.truststore** : contient la liste des certificats de confiance.
- **<rép_installation>/central/var/security/key.store** : Contient le certificat OO privé (y compris la clé privée)

Contrôle de l'accès au KeyStore et TrustStore

Il est conseillé d'octroyer les autorisations de lecture pour TrustStore et KeyStore uniquement à l'utilisateur qui exécute le service Central.

Remplacement du certificat OO auto-signé

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

Une partie du processus de remplacement du certificat consiste à générer un ceritificat au format PKCS12 en utilisant une autorité de certification. Pour plus d'informations sur le processus du certificat, contactez votre autorité de certification ou faites référence à la stratégie de votre entreprise.

Pour plus d'informations, voir « Remplacement du certificat de serveur TLS de Central », page 38.

Ajout de signatures numériques à un pack de contenu

Si le pack de contenu comporte une signature numérique d'une autorité de certification approuvée, cela signifie qu'il est possible de faire confiance au contenu.

L'ajout d'une signature numérique n'est pas obligatoire.

- Les packs de contenu OO prêts à l'emploi contiennent une signature numérique de l'autorité Verisign.
- Il est recommandé que les auteurs de packs de contenu personnalisés dans OO leur ajoutent une signature numérique.
- Les packs de contenu violés ne peuvent plus être déployés.
- Si la signature est expirée, un avertissement s'affiche avant le déploiement, et l'utilisateur doit sélectionner une case pour accepter la signature expirée.

Faites attention aux packs de contenu non signés. Ne faites pas confiance à un pack de contenu non signé car il pourrait inclure du contenu dangereux. Sachez également qu'un pack de contenu non signé peut avoir été violé et sa signature supprimée.

Pour plus d'informations sur la certification numérique des packs de contenu, voir « Déploiement et gestion des packs de contenu » dans le Manuel de l'utilisateur de *OO Central*.

Informations sensibles dans un pack de contenu

Mots de passe du compte système

N'incluez pas de mots de passe lorsque vous créez un pack de contenu. Les mots de passe seront camouflés au sein du pack de contenu, ce qui n'est pas une option fiable.

La pratique conseillée pour la sécurité de OO consiste à configurer les mots de passe du compte système dans Central. Pour plus d'informations, voir « Configuration de comptes système pour un pack de contenu » dans le Manuel de l'utilisateur de *OO Central*.

Audit et fichiers journaux

Audit

L'audit garde la trace des actions réalisées sur le serveur Central, notamment les connexions, les déclenchements de flux, la création de planifications, la modification de configurations, etc. Les données d'audit permettent de garder la trace de l'activité de l'utilisateur sur le système Central, en enregistrant pour chaque action le quand, qui et quoi. Par exemple, l'audit montre qu'un utilisateur a exécuté un flux, mis à jour une configuration, supprimé une planification ou échoué une authentification.

Les données d'audit sont enregistrées dans la base de données. Pour plus d'informations, voir « Auditing » dans le manuel *HPE OO API Guide*.

Journaux

Les journaux permettent de garder la trace des erreurs, avertissements, informations et messages de débogage.

Les journaux sont enregistrés dans le serveur de fichiers dans les emplacements suivants :

- Central - **<installation-oo>/central/var/logs**
- Studio - **<utitlisateur>/.oo/logs**
- RAS - **<installation-oo>/ras/var/logs**.

Aucune donnée sensible n'est conservée dans les enregistrements d'audit ni dans les fichiers journaux

Le système HPE OO ne conserve aucune donnée sensible dans les enregistrements d'audit ou dans les fichiers journaux.

Obtention des enregistrements d'audit

Vous pouvez obtenir les enregistrements d'audit via API ou via une requête sur la table OO_AUDIT. Pour plus d'informations, voir « Auditing » dans le manuel *HPE OO API Guide*.

Exemple de données d'audit :

```
[
{
```

```
“time”:1412312016740, “type”:”AuditConfigurationChange”,
“group”:”AuditManagement”, “subject”:” mondomaine\monutilisateur2”,
“outcome”:”Success”, “data”:”{"enabled":false}”

},

{

“time”:1412312016722, “type”:”InternalUserDelete”, “group”:”Authentication-
Authorization”, “subject”:”mondomaine\monutilisateur2”, “outcome”:”Success”,
“data”:{"usersNames":["admin"]}"

}

]
```

API et interfaces

API et modèle d'interface

Pour effectuer les memes actions, vous pouvez opérer avec les interfaces de programmation d'applications (API) publiques de HPE Operations Orchestration au lieu d'utiliser l'interface utilisateur de HPE OO Central. Certaines actions peuvent etre effectuées uniquement via les API, telles que purge et audit. L'API publique est basée sur HTTP. Toutes les API sont RESTful et utilisent le format JSON.

Fonctionnalités et administration de la configuration de sécurité de l'API et de l'interface

Il est important de travailler en toute sécurité avec les API. Pour ce faire, utilisez les mesures de sécurité décrites dans ce manuel (authentification, chiffrement, etc.).

L'interface API est compatible avec HTTP ou HTTPS.

Remarque : Lorsque vous utilisez nos API pour afficher du HTML, vous prenez la responsabilité de les protéger contre les attaques XSS.

Pour plus d'informations, voir les chapitres suivants dans le manuel *HPE OO API Guide* :

- « LDAP Configuration »
- « Users »
- « LW SSO Configuration »
- « Authentication »
- « Roles »

Securité - Questions et réponses

Comment puis-je générer une demande de certificat qui peut être signée par une autorité de certification externe ?

Exportez la demande de certificat et envoyez-la à l'autorité de certification externe pour la signature. Pour plus d'informations, voir « Remplacement du certificat de serveur TLS de Central », page 38.

Quels ports TCP/UDP sont utilisés par HPE OO ? Quelle est la direction, l'utilisateur, le chiffrement ?

Lorsque vous installez HPE OO, vous devez configurer au moins un port disponible pour le serveur Central dans les champs HTTP/HTTPS. Les valeurs par défaut fournies sont 8080 et 8443, mais vous pouvez les modifier. Pour plus d'informations sur les canaux sécurisés entre Central et les autres composants, voir « Sécurité du réseau et des communications », page 15

Où et comment sont stockées les informations d'identification (comptes administrateur, utilisateurs d'intégration) ?

Voir « Gestion et authentification de l'utilisateur », page 18.

Comment configurer les certificats SSL auto-signés pour Central/RAS/Studio ?

Si au cours de l'installation de HPE OO vous ne fournissez pas de certificat, un certificat auto-signé est créé par défaut. Toutefois, pour des raisons de sécurité, il est déconseillé d'utiliser des certificats auto-signés. HPE recommande de travailler avec un certificat d'un autorité de certification racine personnalisée ou d'une autorité de certification approuvée.

Pour plus d'informations sur la configuration de certificats pour HPE OO, voir « Chiffrement de la communication avec un certificat de serveur », page 37.

Comment activer ou désactiver les différents types d'audit ?

Par défaut l'audit n'est pas activée. Pour plus d'informations, voir « Activation de l'audit » dans le Manuel de l'utilisateur de HPE OO Central. Pour plus d'informations sur l'audit, voir « Audit et fichiers journaux », page 28.

Quel est le niveau des détails dans les journaux et comment modifier le volume journalisé ?

Vous pouvez définir différents niveaux de granularité des journaux. Le niveau par défaut est INFO, mais vous pouvez le modifier. Pour plus d'informations, voir « Adjusting the Logging Levels » dans le manuel *HPE OO System Administration Guide*.

Pour plus d'informations sur les fichiers journaux, voir « Audit et fichiers journaux », page 28.

Comment sont chiffrées les informations sensibles ?

Voir « Chiffrement », page 23.

La communication entre Central et RAS est-elle chiffrée ?

Elle l'est si vous utilisez HTTPS.

La communication entre HPE OO et les autres composants d'intégration (HPNA, CSA, AD, etc) est-elle chiffrée ?

Cela dépend de l'intégration que vous utilisez. Elle l'est si vous utilisez HTTPS.

Comment restreindre l'accès à la Bibliothèque des flux selon les rôles utilisateur ?

Voir « Configuration de la sécurité - Rôles » dans le *Manuel de l'utilisateur de HPE OO Central*.

Quel est le mécanisme d'authentification pris en charge par OO ?

Les mécanismes d'authentification pris en charge sont LDAP, SAML les utilisateurs internes. HPE OO prend également en charge les certificats client et LWSSO. Voir « Gestion et authentification de l'utilisateur », page 18.

HPE OO est-il conforme à la norme FIPS 140-2 ?

Oui. Pour plus d'informations, voir « Configuration de HPE OO pour respecter la norme FIPS 140-2 », page 62.

Quels sont les méthodes d'authentification entre Central et RAS ?

Mot de passe utilisateur ou certificat client.

Les mots de passe stockés sont-ils tous chiffrés ou sécurisés par hachage ?

Oui. Tous les mots de passe stockés sont protégés au moyen d'algorithmes connus et aucun n'est laissé en clair.

Puis-je limiter l'adresse IP de l'utilisateur Central ?

Non, ceci n'est pas pris en charge pour l'instant.

HPE OO est-il certifié pour les critères communs ?

C'est en cours. Nous sommes actuellement dans la phase d'évaluation. Pour plus d'informations, voir https://www.cse-cst.gc.ca/en/canadian-common-criteria-scheme/publication/list/evaluation-product.

Lorsque j'utilise OOSH, puis-je transférer des données sensibles vers Central ?

Nos recommandations prévoit d'utiliser un canal sécurisé lorsque vous vous connectez à Central. Voir « Sécurité du réseau et des communications », page 15.

Renforcer la sécurité pour Operations Orchestration

Cette section explique comment renforcer la configuration de la sécurisation de Operations Orchestration.

Remarque : Pour plus d'informations sur les tâches administratives, voir le *Manuel d'installation, mise à jour et configuration de OO*.

Recommandations pour la sécurisation

1. Installez la version la plus récente de HPE OO. Pour plus d'informations, voir le *Manuel d'installation, mise à niveau et configuration de OO*.
2. (Facultatif) Configurez 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 HPE OO pour la mise en conformité avec la norme FIPS 140-2 Niveau 1 », page 59.
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 « Fonctionnement des certificats serveur et client », page 37.

4. Sécurisez le serveur HPE 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 des ports HTTP/HTTPS ou désactivation du port HTTP », page 48 et « Modification et chiffrement/camouflage du mot de passe du keystore/truststore », page 44.
5. Sécurisez HPE OO Studio en remplaçant les mots de passe KeyStore et TrustStore par des mots de passe renforcés, et chiffrez ou masquez les mots de passe dans les fichiers de configuration. Voir « Modification et chiffrement/camouflage du mot de passe du keystore/truststore », page 44.
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 48.
7. (Facultatif) Configurez la version du protocole TLS. Voir « Configuration du protocole TLS », page 66.
8. Activez l'authentification dans Central. Voir « Activation de l'authentification » dans le *Manuel de l'utilisateur de 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 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 OO Central*.
11. Dans l'environnement Windows et SQL Server, configurez OO de façon à utiliser l'authentification Windows. Voir « Configuration de OO pour fonctionner avec l'authentification Windows » dans le *manuel de base de données 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 OO Central*.

Paramètres de sécurité par défaut

Dans plusieurs cas, il est recommandé de modifier les paramètres de sécurité prêts à l'emploi fournis par défaut.

- **Authentification** - par défaut, l'authentification n'est pas activée dans Central. Il est recommandé de l'activer au plus tôt une fois les utilisateurs configurés. Pour plus d'informations, voir « Activation de l'authentification » dans le *Manuel de l'utilisateur de HPE OO Central*.
- **Audit** - par défaut, l'audit n'est pas activé dans Central. Il est recommandé de l'activer. Pour plus d'informations, voir « Activation de l'audit » dans le *Manuel de l'utilisateur de HPE OO Central*.
- **Chiffrement TLS** - Par défaut, HPE OO prend en charge 3 protocoles TLS : 1.0, 1.1, 1.2. Il est recommandé de travailler avec la version plus récente. Pour plus d'informations, voir « Configuration du protocole TLS », page 66.
- **Certificat de serveur TLS** : par défaut, l'utilisateur doit fournir un certificat d'autorité de certification au cours de l'installation du serveur OO.
- **Certificat client** - par défaut, le certificat client n'est pas activé. Il est recommandé de travailler avec un certificat client pour l'authentification à Central. Pour plus d'informations, voir « Configuration de l'authentification par certificat du client dans Central », page 51.
- **KeyStore, TrustStore et certificat de serveur** - par défaut, les mots de passe Java sont fournis pour le magasin de clé, magasin d'approbation et certificat de serveur. Il est recommandé de remplacer ces mots de passe chiffrés. Pour plus d'informations, voir « Modification et chiffrement/camouflage du mot de passe du keystore/truststore », page 44
- **Chiffrement RC4** - par défaut, le chiffrement RC4 est activé. Il est recommandé de désactiver le chiffrement RC4 au niveau JRE. Pour plus d'informations, voir « Suppression de l'algorithme de chiffrement RC4 des algorithmes pris en charge par SSL », page 48.
- **Bannière de sécurité** - par défaut, la bannière de sécurité n'est pas activée dans Central. Il est recommandé de l'activer avec un message personnalisé. Pour plus d'informations, voir « Configuration d'une bannière de sécurité » dans le *Manuel de l'utilisateur de HPE OO Central*.
- **Authentification Windows de la base de données** - par défaut, l'authentification Windows n'est pas activée dans Central. Si vous travaillez dans l'environnement Windows et SQL Server, configurez HPE OO de façon à utiliser l'authentification Windows. Voir « Configuration de HPE OO pour fonctionner avec l'authentification Windows » dans le *Manuel de base de données HPE OO*.
- **Algorithmes par défaut** - le fichier **encryption.properties** contient les algorithmes par défaut. Pour respecter la norme FIPS, voir « Configuration de HPE OO pour la mise en conformité avec la

norme FIPS 140-2 Niveau 1 », page 59. Pour plus d'informations sur les valeurs par défaut de FIPS 140-2 niveau 1, voir « Encryption Administration » dans « Chiffrement », page 23.

- **Stratégie Java** - par défaut, le fichier **java.policy** n'est pas sécurisé. Pour plus d'informations sur la modification du fichier **java.policy**, voir « Interdire aux flux l'accès au système de fichiers local de Central/RAS », page 67.

Fonctionnement des certificats serveur et 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.

HPE 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 HPE OO, dans **<rép_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 HPE OO Central contiennent deux fichiers pour la gestion des certificats :

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

Recommendations :

- Il est conseillé de remplacer le certificat HPE OO auto-signé après une nouvelle installation de HPE OO ou si votre certificat actuel a expiré.
- Il est conseillé d'octroyer les autorisations de lecture pour TrustStore et KeyStore uniquement à l'utilisateur qui exécute le service Central.
- Il est conseillé d'effacer la console après utilisation de la commande Keytool ou d'utiliser l'invite pour les entrées de mot de passe.

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 :

Pour générer le certificat au format PKCS12, vous devez utiliser une autorité de certification. Vu que cette étape varie selon l'autorité de certification, consultez le fournisseur pour les détails du processus de génération du certificat.

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.

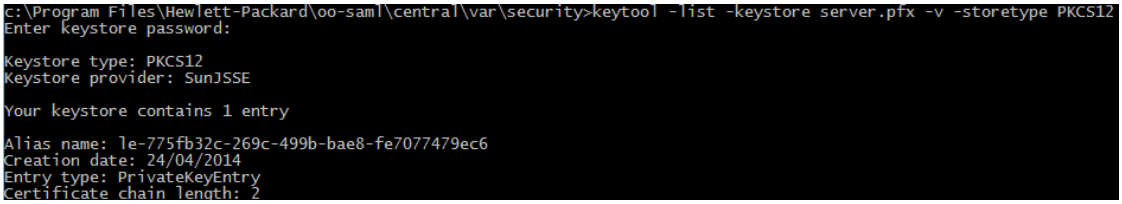
Veillez à choisir un mot de passe fort.

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.

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 et chiffrement/camouflage du mot de passe du keystore/truststore », page 44.

   Il est également recommandé de modifier le mot de passe par défaut « changeit » dans le KeyStore généré automatiquement dans le serveur Central. Voir « Modification et chiffrement/camouflage du mot de passe du keystore/truststore », page 44.

8. Démarrez Central.

Importation d'un certificat racine d'une autorité de certificat dans le TrustStore Central

Si vous utilisez un certificat racine personnalisé pour Central, il faudra importer l'autorité de certificat racine de confiance dans le **client.truststore**. 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, HPE 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. 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 <tout_alias> -keystore <chemin de client.truststore>
   -file <nom_certificat.cer> -storepass <changezmoi>
   ```

3. 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, HPE 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 **<rép_installation>/ras/var/security/client.truststore**.
2. Ouvrez une ligne de commande dans **<répertoire d'installation>/ras/var/security**.
3. Ouvrez le fichier **<rép_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 **<rép_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
   ```

   Remarque : La valeur par défaut de cette propriété est **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 <tout_alias> -keystore <chemin de client.truststore>
   -file <nom_certificat.cer> -storepass <changezmoi>
   ```

6. Démarrez le serveur 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, HPE 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. Vérifiez que la valeur `-Dssl.support-self-signed` est définie sur **false**. Ceci active l'autorité de certificat racine de confiance.

   Par exemple :

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

4. Vérifiez que la valeur `-Dssl.verifyHostName` est définie sur **true**. Ceci vérifie que le FQDN du certificat correspond bien au FQDN de la demande.

   Par exemple :

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

   Remarque : La valeur par défaut de cette propriété est **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 <tout_alias> -keystore <chemin de client.truststore>
   -file <nom_certificat.cer> -storepass <changezmoi>
   ```

6. Exécutez OOSH.
7. Démarrez Central.

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

Si vous utilisez des certificats personnalisés dans les serveurs Central, SVN ou GIT, vous devrez importer l'autorité de certificat racine de confiance (CA) dans le fichier **client.truststore** de Studio pour que ce dernier fonctionne avec ces certificats. 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, HPE 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.

Pour un dossier **.oo** nouveau, Studio copie le fichier **client.truststore** de **<rép_ installation>/studio/var/security** vers le dossier **<utilisateur>/.oo**. Cette action a lieu une seule fois afin de s'assurer que Studio puisse automatiquement importer les certificats (par exemple, pour Studio Remote Debugger). Studio utilise ce fichier en tant que **client.truststore** s'il existe ; autrement il utilise celui de l'installation de Studio (**<rép_installation>/studio/var/security/client.truststore**).

Après une mise à niveau vers 10.5x ou une version ultérieure, l'emplacement du Truststore devient le dossier **<utilisateur>/.oo**.

Si vous souhaitez importer manuellement un certificat, vous pouvez l'importer dans le fichier **.oo/client.truststore** ou dans le fichier **client.truststore** du dossier d'installation de Studio.

Si vous utilisez plusieurs espaces de travail, les modifications apportées au fichier **client.trustore** dans le dossier **.oo** s'appliqueront uniquement à cet espace de travail. Pour appliquer vos modifications à tous les nouveaux espaces de travail créés, modifiez le fichier **client.trustore** dans le dossier d'installation de Studio.

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

1. Fermez Studio et sauvegardez le fichier **client.truststore** d'origine, stocké dans **<utilisateur>/.oo**

   Par exemple, **C:/Users/<nomutilisateur>/.oo**

2. Modifiez le fichier **Studio.l4j.ini** dans **<rép_installation>/studio**.

3. Vérifiez que la valeur `-Dssl.support-self-signed` est définie sur **false**. Ceci active l'autorité de certificat racine de confiance.

   Par exemple :

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

4. Vérifiez que la valeur `-Dssl.support-self-verifyHostName` est définie sur **true**. 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). Remplacez les paramètres qui sont mis en surbrillance <jaune>.

   ```
   keytool -importcert -alias <tout_alias> -keystore <chemin de client.truststore>
   ```

```
-file <nom_certificat.cer> -storepass <changezmoi>
```

6. Démarrez Studio.

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

Modification et chiffrement/camouflage du mot de passe du 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 « Chiffrement des mots de passe » dans le *Manuel d'administration de HPE OO*.

   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.

   Utilisez la commande keytool suivante pour modifier le mot de passe KeyStore :

   ```
   keytool -storepasswd -keystore <rép_
   installation>/central/var/security/key.store
   ```

   Utilisez la commande keytool suivante pour modifier le mot de passe de l'entrée de clé privée du certificat du serveur :

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

   Utilisez la commande keytool suivante pour modifier le mot de passe TrustStore :

   ```
   keytool -storepasswd -keystore <rép_
   installation>/central/var/security/client.truststore
   ```

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"/>
   ```

   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.

b. Enregistrez le fichier.

5. Modifiez le fichier **central-wrapper.conf** situé sous **<rép_installation> central\conf\central** et remplacez le mot de passe TrustStore avec le nouveau mot de passe au format chiffré ou camouflé. Exemples :

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

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

   Pour plus d'informations sur le chiffrement ou le camouflage des mots de passe, voir « Chiffrement et camouflage des mots de passe », page suivante.

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 changez le mot de passe du TrustStore.
- **Pour modifier le mot de passe du TrustStore OOSH** : Modifiez le fichier **oosh.bat** et changez le mot de passe du TrustStore.
- **Pour modifier le mot de passe du TrustStore Studio** : Ajoutez la propriété **client.truststore.password** avec le mot de passe camouflé au fichier **Studio.properties** dans le dossier **<utilisateur>/.oo**.

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

  Si cette propriété n'est pas définie, Studio à la propriété système **javax.net.ssl.trustStorePassword** pour le mot TrustStore.

Pour plus d'informations sur le camouflage des mots de passe, voir « Chiffrement et camouflage des mots de passe », page suivante.

Chiffrement et camouflage des mots de passe

Vous pouvez chiffrer ou camoufler un mot de passe en utilisant le script `encrypt-password` situé sous **<dossier_installation>/central/bin**.

Il est conseillé d'appliquer le chiffrement.

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`.

Chiffrement des mots de passe

1. Repérez le script `encrypt-password` dans **<dossier_installation>/central/bin**.
2. Exécutez le script avec l'option `-e -p <mot de passe>` où `mot de passe` est le mot de passe que vous souhaitez chiffrer.

   Remarque : Vous pouvez utiliser l'indicateur `-p` pour chiffrer le mot de passe ou `--password`.

   Le mot de passe chiffré doit ressembler à ceci :

   ```
   {ENCRYPTED}<quelques_caractères>.
   ```

Camouflage des mots de passe

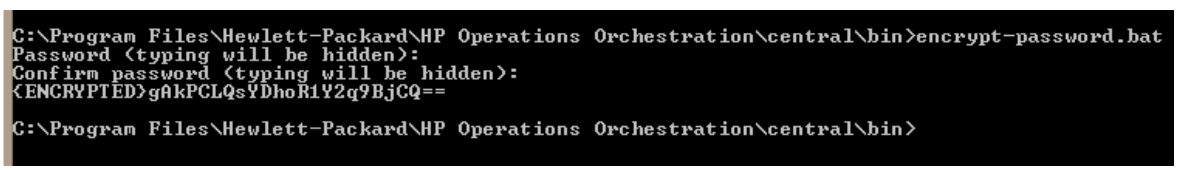
1. Repérez le script `encrypt-password` dans **<dossier_installation>/central/bin**.
2. Exécutez le script avec l'option `-o <mot de passe>` où `mot de passe` est le mot de passe que vous souhaitez camoufler.

   Le mot de passe camouflé doit ressembler à ceci :

   ```
   {OBFUSCATED}<quelques_caractères>.
   ```

Création d'une invite pour le mot de passe

Il est conseillé d'exéctuer le script `encrypt-password` sans fournir l'argument `-p`. Par exemple :



Ceci permet de créer une invite pour les entrées de mots de passe masqués.

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 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 HPE OO 10.x, répétez ces étapes.

Modification des ports HTTP/HTTPS ou désactivation du port HTTP

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 du port HTTP

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

1. Modifiez le fichier **server.xml** qui se trouve dans **<rép_ installation>/central/tomcat/conf/server.xml**.
2. Localisez le connecteur HTTP 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 <tout_alias> -keystore <chemin de client.truststore>
   -file <nom_certificat.cer> -storepass <changezmoi>
   ```

   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 trouvent dans le fichier de configuration Tomcat, à l'emplacement **C:\HPE\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:/HPE/oo/central/var/security/keystore.p12" keystorePass="tomcat-
keystore-password" keystoreType="PKCS12" maxThreads="200" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
sslProtocol="TLSv1.2" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"/>
```

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 « Fonctionnement des certificats serveur et client », page 37.

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`.

   Par exemple :

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

   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="<chemin>/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. Modifiez le fichier **central-wrapper.conf** qui se trouve dans **<rép_installation>central\conf\central**.

   Annulez la mise en commentaire des propriétés suivantes et définissez l'emplacement et le mot de passe du certificat client sur un certificat client avec un utilisateur administrateur.

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

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

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

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

   Pour plus d'informations sur le chiffrement ou le camouflage des mots de passe, voir « Chiffrement et camouflage des mots de passe », page 47.

7. 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 HPE OO est configuré avec plusieurs configurations LDAP, il est uniquement possible d'authentifier l'utilisateur à l'aide des attributs de certificat client avec le LDAP par défaut.

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 40.

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={OBFUSCATED}
   <obfuscated_password>
   ```

   ```
   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 OO Central*.

Dans HPE OO 10.20 et versions ultérieures, le paramètre `keyStorePassword` 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. Voir « Chiffrement et camouflage des mots de passe », page 47.

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 de Studio », page 42.

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={OBFUSCATED}<mot-de-passe_camouflé>

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

4. Démarrez Studio.

Remarques :

- Dans HPE OO 10.20 et versions ultérieures, le paramètre `keyStorePassword` 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. Voir « Chiffrement et camouflage des mots de passe », page 47.
- 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 HPE OO est configuré avec plusieurs configurations LDAP, il est uniquement possible d'authentifier l'utilisateur à l'aide des attributs de certificat client avec le LDAP par défaut. Central tentera d'abord d'authentifier l'utilisateur avec le LDAP par défaut. En cas d'échec il tentera d'authentifier dans le cadre du domaine HPE OO interne.

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 41.

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={OBFUSCATED}<mot-de-passe_camouflé>

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

4. Démarrez OOSH.

Remarque :

Dans HPE OO 10.20 et versions ultérieures, le paramètre `keyStorePassword` 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. Voir « Chiffrement et camouflage des mots de passe », page 47.

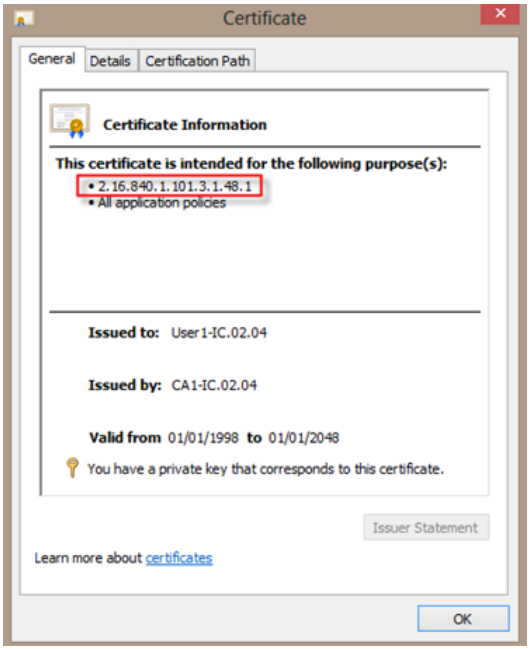
Pour le certificat de client, vous devez définir un utilisateur, soit interne, soit utilisateur LDAP. Le nom de l'utilisateur doit être défini dans les attributs du certificat. La valeur par défaut est l'attribut CN. Pour plus d'informations, voir Traitement du principal de certificat.

Sachez que même si HPE OO est configuré avec plusieurs configurations LDAP, il est uniquement possible d'authentifier l'utilisateur à l'aide des attributs de certificat client avec le LDAP par défaut. Central tentera d'abord d'authentifier l'utilisateur avec le LDAP par défaut. En cas d'échec il tentera d'authentifier dans le cadre du domaine HPE OO interne.

Traitement des stratégies de certificat

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

- Vous pouvez définir la chaîne d'objectif dans le certificat.
- HPE 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 du système 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 HPE OO (utilisateur LDAP ou interne).
- Pour changer l'expression régulière, changez l'élément de configuration : `x509.subject.principal.regex`.

Autoriser OO à lire le champ du nom alternatif du sujet dans un certificat

Vous pouvez autoriser OO à lire le contenu du champ `Nom alternatif du sujet` dans un certificat à l'aide de l'élément de configuration `x509.principal.lookup.field`.

Cet élément de configuration contrôle quel champ du certificat est utilisé pour extraire le nom d'utilisateur.

Les valeurs possibles sont :

- `subjectDN` : représente le champ `Subject` du certificat, qui signifie que OO ne change pas son comportement par défaut et tente de récupérer le nom d'utilisateur dans ce champ **Subject**. Il s'agit de la valeur par défaut.
- `subjectAltNames.otherName.principalName` : représente le `Nom principal de l'utilisateur` (OID 1.3.6.1.4.1.311.20.2.3) stocké dans l'entrée `Other Name` de l'extension de certificat `Subject Alternative Names`. Pour l'Authentification CAC, vous devrez peut-être utiliser la valeur du Nom principal de l'utilisateur.

Pour plus d'informations sur la modification des éléments de configuration de HPE OO, voir le manuel *HPE OO Shell (OOSH) User Guide*.

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

Cette section explique comment configurer HPE 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 sur : csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

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

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

HPE OO utilise le fournisseur de sécurité suivant : Logiciel RSA BSAFE Crypto, version 6.2.1. Il s'agit du seul fournisseur de sécurité pris en charge pour FIPS 140-2.

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

Prérequis

Remarques pour la mise à niveau :

Si vous effectuez la mise à niveau à partir d'une installation de HPE OO 10.10 (et ultérieure) déjà configurée avec FIPS, voir Prérequis pour la mise à niveau.

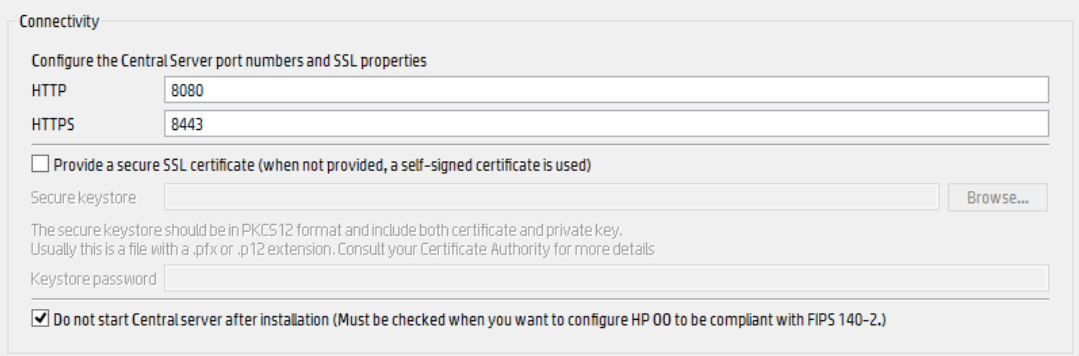
Avant de configurer HPE OO pour le rendre conforme à la norme FIPS 140-2; réalisez les opérations suivantes :

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 HPE 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 HPE OO en cours d'utilisation (quelle que soit la version, 9.x ou 10.x).

2. Confirmez après l'installation de HPE 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**
   - **<rép_installation>\java** (tout le dossier **java** doit être sauvegardé)
4. Téléchargez **Server Oracle JRE 8** à partir de http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html, et remplacez **OpenJDK (Zulu) JRE** avec **Server Oracle JRE**.
   a. Supprimez le contenu du dossier **<rép_installation>\JAVA**.
   b. Décompressez l'archive téléchargée.
   c. Copiez le contenu du dossier **JRE** dans **<rép_installation>\JAVA**.
5. 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/server-jre8-downloads-2133154.html

Remarque : Pour plus d'informations sur le déploiement des fichiers et la mise à niveau de JRE par HPE OO, consultez le fichier **ReadMe.txt** présent dans le contenu téléchargé.

6. Installez les fichiers du logiciel RSA BSAFE Crypto. Sur le système sur lequel HPE OO est installé, copiez les éléments suivants dans **<oo_jre>\lib\ext** (où **<oo_jre>** est le répertoire dans lequel est installé le JRE utilisé par HPE OO. Par défaut, il s'agit de **<rép_installation\java**).
   - **<rép_installation>\central\lib\cryptojce-6.2.1.jar**
   - **<rép_installation>\central\lib\cryptojcommon-6.2.1.jar**
   - **<rép_installation>\central\lib\jcmFIPS-6.2.1.jar**

Étapes prérequises pour la mise à niveau

1. Téléchargez Server Oracle JRE 8 et remplacez OpenJDK (Zulu) JRE avec Server Oracle JRE.
   a. Supprimez le contenu du dossier **<rép_mise-à-niveau>\JAVA**.
   b. Décompressez l'archive téléchargée.
   c. Copiez le contenu du dossier **JRE** dans **<rép_mise-à-niveau>\JAVA**.

   http://www.oracle.com/technetwork/java/javase/downloads/server-jre8-downloads-2133154.html
2. 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/jce8-download-2133166.html

   Pour plus d'informations sur le déploiement des fichiers et la mise à niveau de JRE par HPE OO, consultez le fichier **ReadMe.txt** présent dans le contenu téléchargé.
3. Installez les fichiers du logiciel RSA BSAFE Crypto. Sur le système sur lequel HPE OO est installé, copiez les fichiers suivants dans **<oo_jre>\lib\ext** :

   (où **<oo_jre>** est le répertoire dans lequel est installé le JRE utilisé par la mise à jour de HPE OO. Par défaut, il s'agit de **<rép_upgrade\java**).
   - <rép_installation>\central\lib\cryptojce-6.2.1.jar
   - <rép_installation>\central\lib\cryptojcommon-6.2.1.jar
   - <rép_installation>\central\lib\jcmFIPS-6.2.1.jar

Ensuite, réalisez toutes les étapes décrites dans la section « Configurer les propriétés du fichier de sécurité java » de « Configuration de HPE OO pour respecter la norme FIPS 140-2 », page suivante.

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

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

1. Configurer les propriétés du fichier de sécurité java.
2. Configurer le fichier encryption.properties et activer le mode FIPS.
3. Créer un chiffrement HPE OO conforme avec la norme FIPS.
4. Re-chiffrer le mot de passe de la base de données avec le nouveau chiffrement.
5. Démarrer HPE 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 vers HPE OO 10.x remplace intégralement les fichiers JRE installés. Par conséquent, si vous effectuez la mise à niveau vers la version 10.x, vous devez compléter les étapes suivantes.

Remarque : Si vous effectuez la mise à niveau à partir d'une installation de HPE OO 10.10 ou ultérieure déjà configurée avec FIPS, vous devez appliquer les instructions de la section « Étapes prérequises pour la mise à niveau » dans « Configuration de HPE OO pour la mise en conformité avec la norme FIPS 140-2 Niveau 1 », page 59, puis respecter les étapes ci-dessous, où **<oo_jre>** est le JRE inclus dans la mise à niveau (situé sous **<rép_upgrade>\JAVA**)

Veillez à effectuer toutes les modifications dans le dossier **java** qui se trouve dans le dossier **upgrade** décompressé.

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 HPE 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 OO conforme avec la norme FIPS

Pour créer ou remplacer le fichier de stockage de chiffrement de HPE 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 et chiffrement/camouflage du mot de passe du keystore/truststore », page 44

Remarque : Il est recommandé de supprimer du Truststore 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**.)

Remarque : Si vous travaillez avec le certificat client, le certificat doit être généré par le fournisseur RSA JSE conforme à FIPS et inclure les algorithmes de hachage sécurisés pris en charge dans FIPS, comme indiqué ci-dessous.

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 *HPE OO Administration Guide*, dans la section « Changing the Database Password ».

Démarrez HPE OO

Remplacement du chiffrement FIPS

HPE 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 nouvelle installation de HPE OO, 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

Utilisez le fichier **generate-keys.bat/sh** pour remplacer la clé de chiffrement FIPS dans le référentiel de chiffrement.

Remarque : Ce processus inclut la sauvegarde du fichier **encryption_repository** ; vous devez donc disposer de l'autorisation d'écriture.

1. Accédez au dossier **<rép_installation_Central>/var/security**.
2. Sauvegardez le fichier **encryption.properties** et supprimer-le du dossier **<rép_installation Central>/var/security**.
3. Accédez au dossier **<rép_installation_Central>/bin/**.
4. Exécutez le script **generate-keys**.
5. Appuyez sur la touche **Y** pour continuer.

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

Remarque : Si vous préférez exécuter le script **generate-keys** sans l'invite utilisateur pour taper **Y** ou **N**, utilisez l'indicateur de mode silencieux **–s** lorsque vous exécutez le script.

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 HPE OO pour la mise en conformité avec la norme FIPS 140-2 Niveau 1 », page 59.
2. Réalisez toutes les étapes décrites dans la section « Configurer les propriétés du fichier de sécurité java » de « Configuration de HPE OO pour respecter la norme FIPS 140-2 », page 62.
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 HPE OO pour respecter la norme FIPS 140-2 », page 62.
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 HPE OO pour définir la version du protocole TSL prise en charge. Par défaut, HPE 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.

Interdire aux flux l'accès au système de fichiers local de Central/RAS

Vous devez modifier les fichiers wrapper de configuration et java.policy de Central ou RAS, dans le but d'interdire aux flux l'accès au système de fichiers local de Central ou RAS, et par conséquent interdire l'accès aux ressources sensibles.

Remarque : Pour réaliser ce scénario, l'utilisateur doit disposer des autorisations pour le déploiement et le déclenchement, outre à celles relatives aux flux attribués et à l'attribution de flux. Les utilisateurs avec de telles autorisations sont normalement des utilisateurs fiables.

Pour protéger ce scénario :

1. Dans le fichier wrapper de configuration de Central ou RAS (**<dossier_ installation>/<ras/central>/conf/<central/ras>-wrapper.conf**), ajoutez le paramètre `wrapper.java.additional.<nn>` comme suit :

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

   Remplacez <nn> avec le nombre après le dernier nombre.
2. Dans le fichier **java.policy** (situé sous **<dossier_installation>/java/lib/security/java.policy**), ajoutez les éléments suivants. Ceci permet l'accès aux ressources minimum requises par HPE OO et empêche l'accès au système de fichiers local de Central/RAS qui contient les données sensibles.

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

```
};

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

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

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

Pour permettre au flux d'accéder aux ressources dans le système de fichiers local de Central/RAS, vous devez indiquer ces éléments dans le fichier java.policy. Par exemple :

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

Hewlett Packard
Enterprise