HP Universal CMDB et Configuration Manager

Version du logiciel : 10.10

Manuel de sécurisation renforcée

Date de publication du document : Novembre 2013

Date de lancement du logiciel : Novembre 2013

Mentions légales

Garantie

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

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

Légende de restriction des droits

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

Copyright

Marques

Adobe® est une marque déposée de Adobe Systems Incorporated.

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

UNIX® est une marque déposée de The Open Group.

Crédits

Ce produit inclut un logiciel développé par Apache Software Foundation (http://www.apache.org/).

Ce produit inclut un logiciel développé par OpenSSL Project destiné à être utilisé dans le kit de ressources OpenSSL (http://www.openssl.org/)

Ce produit inclut un logiciel de chiffrement développé par Eric Young (eay@cryptsoft.com)

Ce produit inclut un logiciel développé par Tim Hudson (tjh@cryptsoft.com)

Mises à jour de la documentation

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

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

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

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

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

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

Assistance

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

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

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

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

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

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

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

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

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

Table des matières

Chapitre 1 : Introduction à la sécurisation renforcée

Contenu de ce chapitre :

Sécurisation renforcée - Présentation

Cette section présente le concept d'une application sécurisée HP Universal CMDB et décrit la planification et l'architecture requises pour implémenter la sécurité. Il est vivement recommandé de lire cette section avant de passer à l'étude de la sécurisation renforcée dans les sections suivantes.

HP Universal CMDB a été conçu pour faire partie d'une architecture sécurisée et peut, par conséquent, affronter et traiter les menaces de sécurité auxquelles il peut être exposé.

Les directives relatives à la sécurisation renforcée traitent de la configuration requise pour améliorer (renforcer) la sécurité de HP Universal CMDB.

Les informations relatives à la sécurisation renforcée sont destinées principalement aux administrateurs de HP Universal CMDB. Ceux-ci doivent se familiariser avec les paramètres et recommandations de sécurisation renforcée avant de commencer les procédures de sécurisation renforcée.

Il est vivement recommandé d'utiliser un proxy inverse avec HP Universal CMDB pour bénéficier d'une architecture sécurisée. Pour plus d'informations sur la configuration d'un proxy inverse en vue de l'utiliser avec HP Universal CMDB, voir " Utilisation d'un proxy inverse " , page 37.

Si vous devez utiliser une architecture sécurisée différente de celle décrite dans ce manuel avec HP Universal CMDB, contactez l'Assistance HP Software pour déterminer l'architecture la mieux appropriée à vos besoins.

Pour plus d'informations sur Data Flow Probe, voir " Sécurisation renforcée de Data Flow Probe " , page 70.

Remarque :

- Les procédures de sécurisation renforcée partent du principe que vous n'implémentez que les instructions fournies dans ces chapitres et que vous n'exécutez pas d'autres étapes de sécurisation renforcée décrites ailleurs.
- Lorsque les procédures de sécurisation renforcée s'appliquent à une architecture distribuée spécifique, cela ne signifie pas que cette architecture soit la meilleure pour répondre aux besoins de votre entreprise.
- Les procédures décrites dans les chapitres suivants doivent être exécutées sur des ordinateurs dédiés à HP Universal CMDB. L'utilisation de ces ordinateurs à d'autres fins que celles de HP Universal CMDB peut produire des résultats inattendus.
- Les informations de sécurisation renforcée fournies dans cette section ne doivent pas être considérées comme une aide à l'évaluation des risques de sécurité de vos systèmes informatisés.

Préparation à la sécurisation renforcée

- Évaluez le risque/l'état de sécurité de l'ensemble de votre réseau, et utilisez les conclusions pour déterminer la meilleure intégration de HP Universal CMDB dans votre réseau.
- Analysez l'infrastructure technique de HP Universal CMDB et les fonctions de sécurité de HP Universal CMDB.
- Étudiez toutes les directives relatives à la sécurisation renforcée.
- Vérifiez que HP Universal CMDB est entièrement opérationnel avant de passer aux procédures de sécurisation renforcée.
- Suivez les procédures de sécurisation renforcée dans l'ordre chronologie de chaque chapitre. Par exemple, si vous décidez de configurer le serveur HP Universal CMDB pour prendre en charge SSL, consultez le chapitre " Activation de la communication SSL (Secure Sockets Layer) " , page 18 et suivez les instructions dans l'ordre chronologique.
- HP Universal CMDB ne prend pas en charge l'authentification de base avec des mots de passe vides. N'utilisez pas de mot de passe pour définir les paramètres de connexion d'authentification de base.

Astuce : Imprimez les procédures de sécurisation renforcée et cochez-les lorsque vous les avez implémentées.

Déploiement de UCMDB dans une architecture sécurisée

Plusieurs mesures sont recommandées pour déployer vos serveurs HP Universal CMDB en toute sécurité.

- **Architecture DMZ utilisant un pare-feu**

  L'architecture sécurisée décrite dans ce manuel est une architecture DMZ type qui utilise un périphérique comme pare-feu. Le concept de base d'une telle architecture consiste à créer une séparation complète et à éviter un accès direct entre les clients HP Universal CMDB et le serveur HP Universal CMDB.

- **Navigateur sécurisé**

  Dans un environnement Windows, Internet Explorer et Firefox doivent être configurés pour gérer de façon sécurisée les scripts, les applets et les cookies Java.

- **Protocole de communication SSL**

  Ce protocole sécurise la connexion entre le client et le serveur. Les URL qui requièrent une connexion SSL utilisent une version sécurisée (HTTPS) du protocole HTTP. Pour plus d'informations, voir " Activation de la communication SSL (Secure Sockets Layer) " , page 18.

- **Architecture de proxy inverse**

  L'une des solutions les plus sécurisées et recommandées suggère le déploiement de HP Universal CMDB à l'aide d'un proxy inverse. HP Universal CMDB prend entièrement en charge l'architecture de proxy inverse sécurisée. Pour plus d'informations, voir " Utilisation d'un proxy inverse " , page 37.

Accès au système

Sécurisation renforcée de l'accès à Java JMX

Remarque : La procédure décrite ci-après s'applique également à la console JMX de Data Flow Probe.

Pour limiter l'accès au port JMX RMI à l'entrée des informations d'identification, procédez comme suit :

1. Dans le fichier **wrapper.conf** du serveur (qui se trouve sous **C:\hp\UCMDB\UCMDBServer\bin**), entrez la ligne suivante :

   wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true

Ce paramétrage force JMX à demander une authentification.

- **Pour la console JMX de Data Flow Probe**, procédez comme suit :

  Dans les fichiers **WrapperGateway.conf** et **WrapperManager.conf** situés sous **C:\hp\UCMDB\DataFlowProbe\bin**, entrez la ligne suivante :

  wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true

2. Remplacez le nom de fichier **jmxremote.password.template** (situé sous **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) par **jmxremote.password**.

   Remarque : Pour le JMX de Data Flow Probe, ce fichier se trouve sous **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.

3. Dans le fichier **jmxremote.password**, ajoutez les mots de passe des rôles **monitorRole** et **controlRole**.

   Exemple :

   monitorRole QED

   controlRole R&D

   attribue le mot de passe **QED** à **monitorRole** et le mot de passe **R&D** à **controlRole**.

   Remarque : Assurez-vous que seul le propriétaire dispose des droits en lecture et écriture sur le fichier **jmxremote.password**, car ce fichier contient les mots de passe en texte clair. Le propriétaire du fichier doit être le même utilisateur que celui sous lequel le serveur UCMDB est exécuté.

4. Dans le fichier **jmxremote.access** (situé dans **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**), attribuez les droits d'accès à **monitorRole** et **controlRole**.

   Exemple :

   monitorRole readonly

   controlRole readwrite

   accorde un accès en lecture seule à **monitorRole** et un accès en lecture/écriture à **controlRole**.

   Remarque : Pour la console JMX de Data Flow Probe, ce fichier se trouve sous

C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management.

5. Protégez les fichiers comme suit :

   - **Pour Windows seulement :** exécutez les commandes suivantes à partir de la ligne de commande pour protéger les fichiers :

     cacls jmxremote.password /P <nom_utilisateur>:F

     cacls jmxremote.access /P <nom_utilisateur>:R

     où **<nom_utilisateur>** est le propriétaire du fichier qui apparaît dans les propriétés des deux fichiers. Ouvrez les propriétés de ces fichiers, assurez-vous de leur pertinence et qu'elles comportent un seul propriétaire.

   - **Pour les systèmes d'exploitation Solaris et Linux :** définissez les autorisations pour le fichier de mots passe en exécutant la commande suivante :

     chmod 600 jmxremote.password

6. **Pour les mises à niveau de Service Pack, les migrations de serveur et la récupération en cas d'urgence :** modifiez la propriété du fichier **jmxremote.access** (situé dans **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) en l'attribuant à l'utilisateur du système d'exploitation qui exécute l'installation liée à la mise à niveau ou la migration.

Remarque :

- Pour la console JMX de Data Flow Probe, ce fichier se trouve sous **C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**.
- Avant de désinstaller le produit, modifiez les autorisations pour le fichier **<dossier d'installation de UMCDB>\bin\jre\lib\management\jmxremote.password** afin que vous puissiez le modifier sous le nom d'utilisateur à l'aide duquel vous êtes connecté.

Modification du mot de passe ou du nom d'utilisateur système de la console JMX

La console JMX utilise des utilisateurs système, c'est-à-dire des utilisateurs interclients dans un environnement multiclient. Vous pouvez vous connecter à la console JMX avec n'importe quel nom d'utilisateur. Le nom d'utilisateur et le mot de passe par défaut sont **sysadmin/sysadmin**.

Vous modifiez le mot de passe par le biais de la console JMX ou à l'aide de l'outil Gestion du serveur.

Pour changer le mot de passe ou le nom d'utilisateur système via la console JMX :

1. Lancez un navigateur Web et entrez l'adresse suivante : **http://localhost.<nom_ domaine>:8080/jmx-console**.
2. Entrez les informations d'identification pour l'authentification de la console JMX.
3. Recherchez **UCMDB:service=Authorization Services** et cliquez sur le lien pour accéder à la page Operations.
4. Recherchez l'opération **resetPassword**.
   - Dans le champ **userName**, entrez **sysadmin**.
   - Dans le champ **password**, entrez un nouveau mot de passe.
5. Cliquez sur **Invoke** pour enregistrer vos modifications.

Pour changer le mot de passe ou le nom d'utilisateur système à l'aide de l'outil Gestion du serveur :

1. **Pour Windows :** exécutez le fichier suivant : **C:\hp\UCMDB\UCMDBServer\tools\server_ management.bat.**

   Pour Linux : exécutez le fichier **server_management.sh** qui se trouve dans le dossier suivant : **/opt/hp/UCMDB/UCMDBServer/tools/**.
2. Connectez-vous à l'outil à l'aide des informations d'identification **sysadmin/sysadmin**.
3. Cliquez sur le lien Utilisateurs.
4. Sélectionnez l'utilisateur système et cliquez sur **Modifier le mot de passe de l´utilisateur connecté**.
5. Entrez l'ancien et le nouveau mot de passe et cliquez sur **OK**.

Modification de l'utilisateur du service du serveur HP Universal CMDB

Sur une plate-forme Windows, le service HP Universal CMDB qui exécute tous les services et processus de HP Universal CMDB est installé lorsque vous exécutez l'utilitaire de configuration de base de données et de serveur. Par défaut, ce service est exécuté sous l'utilisateur du système local. Cependant, vous pourriez avoir besoin d'affecter un utilisateur différent pour exécuter le service (par exemple, si vous utilisez l'authentification NTLM).

L'utilisateur que vous affectez pour effectuer le service doit disposer des autorisations suivantes :

- Autorisations de base de données suffisantes (définies par l'administrateur de base de données)
- Autorisations réseau suffisantes

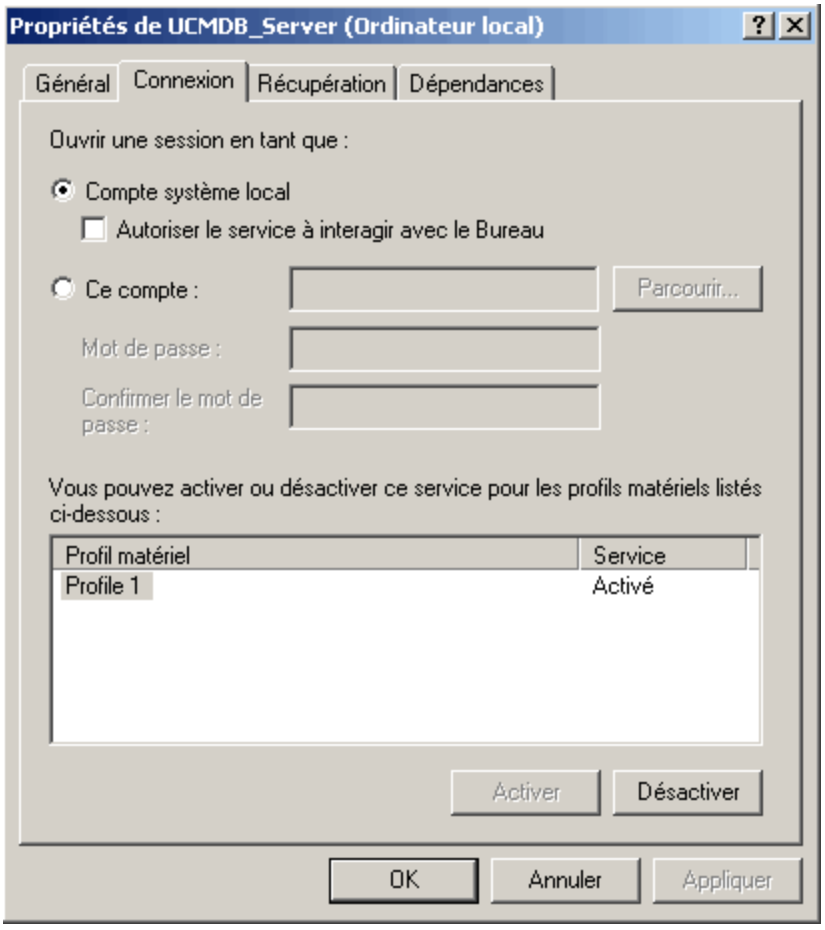
- Autorisations d'administrateur sur le serveur local

Pour modifier l'utilisateur du service :

1. Désactivez HP Universal CMDB via le menu Démarrer (**Démarrer > Tous les programmes > HP UCMDB > Arrêter le serveur HP Universal CMDB**) ou en arrêtant le service du serveur HP Universal CMDB. Pour plus d'informations, voir la section décrivant le démarrage et l'arrêt du service du serveur HP UCMDB dans le *Manuel d'administration HP Universal CMDB*

2. Dans la fenêtre **Services** de Windows, double-cliquez sur **UCMDB_Server**. La boîte de dialogue **Propriétés Serveur_UCMDB (ordinateur local)** apparaît.

3. Cliquez sur l'onglet Ouvrir une session.



4. Sélectionnez **Ce compte** et recherchez un autre utilisateur dans la liste des utilisateurs valides de l'ordinateur.

5. Entrez puis confirmez le mot de passe Windows de l'utilisateur sélectionné.

6. Cliquez sur **Appliquer** pour enregistrer vos paramètres et sur **OK** pour fermer la boîte de dialogue.

7. Activez HP Universal CMDB via le menu Démarrer (**Démarrer > Tous les programmes > HP UCMDB > Démarrer le serveur HP Universal CMDB**) ou en démarrant le service du serveur HP Universal CMDB. Pour plus d'informations, voir la section décrivant le démarrage et l'arrêt du service du serveur HP UCMDB dans le *Manuel d'administration HP Universal CMDB*

Chiffrer le mot de passe de base de données pour Configuration Manager

Le mot de passe de base de données de Configuration Manager est stocké dans le fichier **<*répertoire_installation_Configuration_Manager*>\conf\database.properties**. Si vous souhaitez chiffrer le mot de passe, notre algorithme de chiffrement par défaut est compatible avec les normes FIPS 140-2.

Le chiffrement est réalisé à l´aide d´une clé, qui permet de chiffrer le mot de passe. La clé est ensuite chiffrée à l´aide d´une autre clé, appelée clé principale. Les deux clés sont chiffrées à l´aide du même algorithme. Pour plus d´informations sur les paramètres utilisés dans la procédure de chiffrement, voir " Paramètres du chiffrement du mot de passe de la base de données Configuration Manager " , page suivante

Attention : Si vous modifiez l´algorithme de chiffrement, tous les mots de passe préalablement chiffrés ne sont plus utilisables.

Pour modifier le chiffrement de votre mot de passe de base de données :

1. Ouvrez le fichier **<*répertoire_installation_Configuration_Manager*>\conf\database.properties** et modifiez les champs suivants :

   - **engineName.** Entrez le nom de l´algorithme de chiffrement.
   - **keySize.** Entrez la taille de la clé principale de l´algorithme sélectionné.

2. Exécutez le script **generate-keys.bat**, qui crée le fichier **<*répertoire_installation_Configuration_Manager*>\security\encrypt_repository** et génère la clé de chiffrement.

3. Exécutez l´utilitaire **bin\encrypt-password.bat** pour chiffrer le mot de passe. Définissez l´indicateur **-h** pour afficher les options disponibles.

4. Copiez le résultat de l´utilitaire de chiffrement de mot de passe et insérez le chiffrement obtenu dans le fichier **conf\database.properties**.

Paramètres du chiffrement du mot de passe de la base de données Configuration Manager

Le tableau ci-dessous contient les paramètres inclus dans le fichier **encryption.properties** utilisé pour le chiffrement de mot de passe de base de données CM. Pour plus d'informations sur le chiffrement du mot de passe de base de données, voir " Chiffrer le mot de passe de base de données pour Configuration Manager " , page précédente.

Paramètre	Description
cryptoSource	Indiquer l´infrastructure d´implémentation de l´algorithme de chiffrement. Les options sont les suivantes : • **lw.** Uses Bouncy Castle lightweight implementation (Option par défaut) • **jce.** Java Cryptography Enhancement (infrastructure de chiffrement Java standard)
storageType	Indiquer le type de stockage de clé. Actuellement, seul le **fichier binaire** est pris en charge.
binaryFileStorageName	Indiquer l´emplacement du fichier dans lequel la clé principale est stockée.
cipherType	Type de chiffrement. Actuellement, seul **symmetricBlockCipher** est pris en charge.
engineName	Nom de l´algorithme de chiffrement. Les options suivantes sont disponibles : • **AES.** American Encryption Standard. Ce chiffrement est compatible FIPS 140-2. (Option par défaut) • **Blowfish** • **DES** • **3DES.** (Compatible FIPS 140-2) • **Null**. Aucun chiffrement

Paramètre	Description
keySize	Taille de la clé principale. Elle est déterminée par l´algorithme : • **AES.** 128, 192 ou 256 (Option par défaut 256) • **Blowfish** 0-400 • **DES** 56 • **3DES.** 156
encodingMode	Codage ASCII des résultats du chiffrement binaire. Les options suivantes sont disponibles : • **Base64** (Option par défaut) • **Base64Url** • **Hex**
algorithmModeName	Mode de l´algorithme. Actuellement, seul **CBC** est pris en charge.
algorithmPaddingName	Algorithme de remplissage utilisé. Les options suivantes sont disponibles : • **PKCS7Padding** (Option par défaut) • **PKCS5Padding**
jceProviderName	Nom de l´algorithme de chiffrement JCE. **Remarque :** Ne s´applique que si crytpSource est jce. Pour lw, engineName est utilisé.

Chapitre 2 : Activation de la communication SSL (Secure Sockets Layer)

Contenu de ce chapitre :

Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé - UCMDB

Ces sections expliquent comment configurer HP Universal CMDB pour prendre en charge la communication via le canal SSL (Secure Sockets Layer).

1. **Conditions préalables**

   a. Avant de passer à la procédure suivante, supprimez l'ancien fichier **server.keystore** sous **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

   b. Placez le magasin de clés HP Universal CMDB (type JKS) dans le dossier **C:\hp\UCMDB\UCMDBServer\conf\security**.

2. **Générer un magasin de clés de serveur**

   a. Créez un magasin de clés (type JKS) à l'aide d'un certificat auto-signé et d'une clé privée correspondante :

      - À partir de **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, exécutez la commande suivante :

        ```
        keytool -genkey -alias hpcert -keystore
        C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
        ```

        La boîte de dialogue de la console s'affiche.

      - Entrez le mot de passe du magasin de clés (keystore). Si le mot de passe a changé, exécutez l'opération JMX **changeKeystorePassword** dans **UCMDB:service=Security Services**. Si le mot de passe n'a pas changé, utilisez le mot de passe par défaut **hppass**.

      - Répondez à la question, **Quels sont vos nom et prénom ?** Entrez le nom du serveur Web HP Universal CMDB. Entrez les autres paramètres inhérents à votre entreprise.

      - Entrez le mot de passe de la clé. Il DOIT être identique à celui du magasin de clés.

        Un magasin de clés JKS est créé sous le nom **server.keystore** avec un certificat de serveur appelé **hpcert**.

   b. Exportez le certificat auto-signé dans un fichier :

      À partir de **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**, exécutez la commande suivante :

      ```
      keytool -export -alias hpcert -keystore
      C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <votre
      mot de passe> -file hpcert
      ```

3. **Placer le certificat dans le magasin de données d'approbations du client**

   Après la génération du fichier **server.keystore** et l'exportation du certificat du serveur, pour chaque client devant communiquer avec HP Universal CMDB par le biais de SSL à l'aide de ce certificat auto-signé, placez celui-ci dans les magasins d'approbations du client.

   > **Remarque : server.keystore** ne peut contenir qu'un seul certificat de serveur.

4. **Désactiver le port HTTP 8080**

   Pour plus d'informations, voir " Activer ou désactiver les ports HTTP/HTTPS " , page 30.

Remarque : Vérifiez que la communication HTTPS fonctionne avant de fermer le port HTTP.

5. **Redémarrer le serveur**

6. **Afficher HP Universal CMDB**

   Pour vérifier que le serveur UCMDB est sécurisé, entrez l'URL suivante dans le navigateur Web : **https://<nom ou adresse IP du serveur UCMDB>:8443/ucmdb-ui**.

Activer SSL sur l'ordinateur serveur à l'aide d´un certificat auto-signé - Configuration Manager

Cette section explique comment configurer Configuration Manager pour prendre en charge l'authentification et le chiffrement à l'aide du canal SSL (Secure Sockets Layer).

Configuration Manager utilise Tomcat 7.0.19 comme serveur d´applications.

1. **Conditions préalables** (ne s'applique pas dans le cas d'une première installation)

   Avant de démarrer la procédure suivante, supprimez, le cas échéant, l'ancien fichier **tomcat.keystore** du dossier ***<répertoire_installation_Configuration_Manager>*\java\windows\x86_64\lib\security** ou ***<répertoire_installation_Configuration_Manager>*\java\linux\x86_64\lib\security** (selon l'environnement).

2. **Générer un magasin de clés de serveur**

   Créez un magasin de clés (type JKS) à l'aide d'un certificat auto-signé et d'une clé privée correspondante :

   - À partir du fichier ***<répertoire_installation_Configuration_Manager>*\java\windows\x86_64\bin** ou ***<répertoire_installation_Configuration_Manager>*\java\linux\x86_64\bin**, exécutez la commande suivante :

     ```
     keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\
     security\tomcat.keystore
     ```

     La boîte de dialogue de la console s'affiche.

   - Entrez le mot de passe du magasin de clés (keystore). S´il a été modifié, changez-le manuellement dans le fichier.

   - Répondez à la question, **Quels sont vos nom et prénom ?** Entrez le nom du serveur Web de Configuration Manager. Entrez les autres paramètres inhérents à votre entreprise.

   - Entrez le mot de passe de la clé. Il DOIT être identique à celui du magasin de clés.

Un keystore JKS est créé sous le nom **tomcat.keystore** avec un certificat de serveur appelé **hpcert**.

3. **Placer le certificat dans le magasin de données de confiance du client**

   Ajoutez le certificat aux magasins approuvés du client dans Internet Explorer sur votre ordinateur (**Outils >Options Internet > Contenu >Certificats**). Sinon, vous serez invité à le faire lors de la première utilisation de Configuration Manager.

   Limitation : **tomcat.keystore** ne peut contenir qu´un seul certificat de serveur.

4. **Modifier le fichier server.xml**

   Ouvrez le fichier **server.xml** qui se trouve dans le dossier **<*répertoire_installation_Configuration_Manager*>\servers\server-0\conf**. Localisez la section commençant par

   ```
   Connector port="8143"
   ```

   qui apparaît sous forme de commentaires. Activez le script en supprimant le caractère de commentaire et ajoutez les attributs suivants au connecteur HTTPS :

   ```
   keystoreFile="<emplacement du fichier tomcat.keystore>"
   keystorePass="<mot de passe>"
   ```

   (voir l'étape 2)

   Excluez la ligne suivante par un commentaire :

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   ```

   Remarque : Vous ne devez pas bloquer le port de connexion HTTP. Si vous voulez bloquer la communication HTTP, vous pouvez utiliser un pare-feu à cet effet.

5. **Redémarrer le serveur**

   Redémarrez le serveur Configuration Manager.

6. **Vérifier la sécurité du serveur**

   Pour vérifier que le serveur Configuration Manager est sécurisé, entrez l´URL suivante dans le navigateur Web : **https://<nom ou adresse IP du serveur Configuration Manager>:8143/cnc**.

7. Dans Configuration Manger, sélectionnez **Paramètres>Gestion d'applications> Paramètres de messagerie**, puis modifiez le protocole et le port dans l'**URL complète de Configuration Manager** selon les valeurs indiquées ci-dessus.

8. Dans UCMDB, sélectionnez **Gestionnaire des paramètres d'infrastructure>Paramètres**

généraux, puis modifiez le protocole et le port dans l'**URL de Configuration Manager** selon les valeurs indiquées ci-dessus.

Astuce : Si vous n´arrivez pas à vous connecter, utilisez un autre navigateur ou passez à une version plus récente du navigateur.

Activer SSL sur l'ordinateur serveur à l'aide d'un certificat d'une autorité de certification - UCMDB

Pour utiliser un certificat émis pour une autorité de certification, le magasin de clés (keystore) doit être au format Java. L´exemple suivant explique comment formater le magasin de clés pour un ordinateur Windows.

1. **Conditions préalables**

   Avant de passer à la procédure suivante, supprimez l'ancien fichier **server.keystore** sous **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore**.

2. **Générer un magasin de clés de serveur**

   a. Générez un certificat signé par une autorité de certification et installez-le sous Windows.

   b. Exportez le certificat dans un fichier ***.pfx** (y compris les clés privées) à l´aide de Microsoft Management Console (**mmc.exe**).

      Entrez une chaîne comme mot de passe pour le fichier **pfx**. (Ce mot de passe vous est demandé lors de la conversion du type de keystore en un keystore JAVA.) Le fichier **.pfx** contient un certificat public et une clé privée et il est protégé par un mot de passe.

   c. Copiez le fichier **.pfx** que vous avez créé dans le dossier suivant : **C:\hp\UCMDB\UCMDBServer\conf\security**.

   d. Ouvrez l'invite de commande et remplacez le répertoire par **C:\hp\UCMDB\UCMDBServer\bin\jre\bin.**

      Remplacez le type de keystore **PKCS12** par un keystore **JAVA** en exécutant la commande suivante :

      ```
      keytool -importkeystore -srckeystore c:\hp\UCMDB\UCMDBServer\conf\securit
      y\<nom du fichier pfx> -srcstoretype PKCS12 -destkeystore server.keystore
      ```

      Le mot de passe du keystore source (**.pfx**) vous est demandé. Il s'agit du mot de passe que vous avez fourni lors de la création du fichier **pfx** à l'étape b.)

   e. Entrez le mot de passe keystore de destination. Ce mot de passe doit être le même que celui défini précédemment dans la méthode JMX **changeKeystorePassword**, sous

Security Services. Si le mot de passe n'a pas changé, utilisez le mot de passe par défaut **hppass**.

> **Remarque :** Le mot de passe du keystore source doit être identique à celui du keystore de destination.

f. Une fois le certificat généré, désactivez le port HTTP 8080. Pour plus d'informations, voir " Activer ou désactiver les ports HTTP/HTTPS " , page 30.

g. Si vous avez utilisé un mot de passe différent de **hppass** ou le mot de passe du fichier **.pfx**, exécutez la méthode JMX **changeKeystorePassword** et vérifiez que la clé comporte le même mot de passe.

> **Remarque :** Vérifiez que la communication HTTPS fonctionne avant de fermer le port HTTP.

3. **Redémarrer le serveur**

4. **Vérifier la sécurité du serveur**

   Pour vérifier que le serveur UCMDB est sécurisé, entrez l'URL suivante dans le navigateur Web : **https://<nom ou adresse IP du serveur UCMDB>:8443/ucmdb-ui**.

> **Attention : server.keystore** ne peut contenir qu'un seul certificat de serveur.

Activer SSL sur l'ordinateur serveur à l'aide d'un certificat d'une autorité de certification - Configuration Manager

Dans le cas de Configuration Manager, pour utiliser un certificat émis par une autorité de certification, le magasin de clés (keystore) doit être au format Java. L´exemple suivant explique comment formater le magasin de clés pour un ordinateur Windows.

1. **Conditions préalables**

   Avant de démarrer la procédure suivante, supprimez, le cas échéant, l'ancien fichier **tomcat.keystore** du dossier ***<répertoire_installation_Configuration_Manager>*\java\windows\x86_64\lib\security** ou ***<répertoire d'installation de Configuration Manager>*\java\linux\x86_64\lib\security** (selon l'environnement).

2. **Générer un magasin de clés de serveur**

a. Générez un certificat signé par une autorité de certification et installez-le sous Windows.

b. Exportez le certificat dans un fichier ***.pfx** (y compris les clés privées) à l´aide de Microsoft Management Console (**mmc.exe**).

Entrez une chaîne comme mot de passe pour le fichier **pfx**. (Ce mot de passe vous est demandé lors de la conversion du type de keystore en un keystore JAVA.)
Le fichier **.pfx** contient un certificat public et une clé privée et il est protégé par un mot de passe.

Copiez le fichier **.pfx** que vous avez créé dans le dossier suivant : ***<répertoire_installation_Configuration_Manage>*\java\lib\security**.

c. Ouvrez l'invite de commande et remplacez ce répertoire par ***<répertoire_installation_Configuration_Manager>*\java\bin**.

Remplacez le type de keystore **PKCS12** par un keystore **JAVA** en exécutant la commande suivante :

```
keytool -importkeystore -srckeystore <répertoire_installation_Configuration_Manager>\conf\security\<nom du fichier pfx> -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

Le mot de passe du keystore source (**.pfx**) vous est demandé. Il s´agit du mot de passe que vous avez fourni lors de la création du fichier pfx à l´étape b.

3. **Modifier le fichier server.xml**

Ouvrez le fichier **server.xml** qui se trouve dans le dossier ***<répertoire_installation_Configuration_Manager>*\servers\server-0\conf**. Localisez la section commençant par

```
Connector port="8143"
```

qui apparaît sous forme de commentaires. Activez le script en supprimant le caractère de commentaire et ajoutez les deux lignes suivantes :

```
keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />
```

Excluez la ligne suivante par un commentaire :

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
```

Remarque : Vous ne devez pas bloquer le port de connexion HTTP. Si vous voulez bloquer la communication HTTP, vous pouvez utiliser un pare-feu à cet effet.

4. **Redémarrer le serveur**

Redémarrez le serveur Configuration Manager.

5. **Vérifier la sécurité du serveur**

   Pour vérifier que le serveur Configuration Manager est sécurisé, entrez l´URL suivante dans le navigateur Web : **https://<nom ou adresse IP du serveur Configuration Manager>:8143/cnc**.

6. Dans Configuration Manger, sélectionnez **Paramètres>Gestion d'applications> Paramètres de messagerie**, puis modifiez le protocole et le port dans l'**URL complète de Configuration Manager** selon les valeurs indiquées ci-dessus.

7. Dans UCMDB, sélectionnez **Gestionnaire des paramètres d'infrastructure>Paramètres généraux**, puis modifiez le protocole et le port dans l'**URL de Configuration Manager** selon les valeurs indiquées ci-dessus.

Limitation : **tomcat.keystore** ne peut contenir qu´un seul certificat de serveur.

Activer SSL sur les ordinateurs client - UCMDB

Si le certificat utilisé par le serveur Web de HP Universal CMDB est émis par une autorité de certification bien connue, il est fort probable que votre serveur Web valide le certificat sans action supplémentaire.

Si l'autorité de certification n'est pas approuvée par le navigateur Web, vous devez importer le chemin d'approbation complet du certificat ou importer le certificat utilisé explicitement par HP Universal CMDB dans le magasin d'approbations du navigateur.

L'exemple ci-après explique comment importer le certificat **hpcert** auto-signé dans le magasin d'approbations de Windows afin qu'il puisse être utilisé par Internet Explorer.

Pour importer un certificat dans le magasin d'approbations de Windows :

1. Recherchez le certificat **hpcert** et renommez-le **hpcert.cer**.

   Dans l'Explorateur Windows, l'icône indique que le fichier est un certificat de sécurité.

2. Double-cliquez sur **hpcert.cer** pour ouvrir la boîte de dialogue Certificat Internet Explorer.

3. Suivez les instructions permettant d'activer l'approbation en installant le certificat avec l'Assistant Importation de certificat.

Remarque : Pour importer le certificat émis par le serveur UCMDB dans le navigateur Web, vous pouvez également vous connecter à UCMDB et installer le certificat lorsque l'avertissement signalant un certificat non approuvé s'affiche.

Activer SSL à l´aide d´un certificat client - Configuration Manager

Si le certificat utilisé par le serveur Web de Configuration Manager est émis par une autorité de certification bien connue, il est fort probable que votre serveur Web valide le certificat sans action supplémentaire.

Si l´autorité de certification n´est pas approuvée par le magasin d´approbations du serveur, importez le certificat CA dans ce magasin.

L´exemple suivant démontre comment importer le certificat auto-signé **hpcert** dans le magasin d´approbations du serveur (cacerts).

Pour importer un certificat dans le magasin d´approbations du serveur :

1. Sur l´ordinateur client, localisez et renommez le certificat **hpcert** en **hpcert.cer**.
2. Copiez **hpcert.cer** dans le dossier ***<répertoire_installation_Configuration_Manager>*\java\windows\x86_64bin** de l'ordinateur serveur.
3. Sur l´ordinateur serveur, importez le certificat d´autorité de certification dans le magasin d´approbations (cacerts) à l´aide de l´utilitaire keytool avec la commande suivante :

   ```
   <répertoire_installation_Configuration_Manager>\java\bin\keytool.exe -import
   -alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
   ```

4. Modifiez comme suit le fichier **server.xml** (stocké dans le dossier ***<répertoire_installation_Configuration_Manager>*\servers\server-0\conf**) :
   a. Effectuez les modifications décrites dans " Modifier le fichier server.xml " , page 24.
   b. Après avoir apporté ces modifications, ajoutez les attributs suivants au connecteur HTTPS :

      ```
      truststoreFile="../../java/lib/security/cacerts"
      truststorePass="changeit" />
      ```

   c. Définissez `clientAuth="true"`.
5. Vérifiez la sécurité du serveur comme indiqué dans " Vérifier la sécurité du serveur " , page précédente.

Activer SSL sur le SDK client

Vous pouvez utiliser le transport HTTPS entre les SDK client et serveur :

1. Sur l'ordinateur client, dans le produit qui incorpore le SDK client, recherchez le paramètre de transport et vérifiez qu'il est configuré sur HTTPS, et non HTTP.

2. Téléchargez le certificat public auto-signé ou de l'autorité de certification dans l'ordinateur client, puis importez-le dans le magasin d'approbations **cacerts** du JRE qui va se connecter au serveur.

   Utilisez la commande suivante :

   ```
   Keytool -import -alias <nom de l'autorité de certification> -trustcacerts -f
   ile <chemin du certificat public de serveur> -keystore <chemin du magasin d'
   approbations cacerts du JRE client (par ex., x:\program files\java\jre\lib\s
   ecurity\cacerts)>
   ```

Activer l'authentification mutuelle de certificat pour le SDK

Ce mode utilise SSL et active l'authentification du serveur par UCMDB et l'authentification du client par le client UCMDB-API. Le serveur et le client UCMDB-API envoient leurs certificats à l'autre entité pour authentification.

Remarque : La méthode d'activation de SSL décrite ci-après sur le SDK avec l'authentification mutuelle est recommandée, car elle constitue le mode de communication le plus sécurisé.

1. Renforcez la sécurisation du connecteur du client UCMDB-API dans UCMDB :

   a. Accédez à la console JMX de UCMDB. Lancez un navigateur Web et entrez l'adresse suivante : **http://<nom ou adresse IP de l'ordinateur UCMDB>:8080/jmx-console**. Si nécessaire, connectez-vous avec un nom d'utilisateur et un mot de passe (par défaut, sysadmin/sysadmin).

   b. Recherchez **UCMDB:service=Ports Management Services** et cliquez sur le lien pour accéder à la page Operations.

   c. Recherchez l'opération **PortsDetails** et cliquez sur **Invoke**. Notez le numéro de port de l'authentification client de la connexion HTTPS. Sa valeur par défaut est 8444, et il doit être activé.

   d. Revenez à la page Operations.

   e. Pour mapper le connecteur ucmdb-api sur le mode d'authentification mutuelle, appelez la méthode **mapComponentToConnectors** avec les paramètres suivants :

      - **componentName** : ucmdb-api
      - **isHTTPSWithClientAuth** : true
      - Tous les autres indicateurs : false

Le message suivant apparaît :

Operation succeeded. Component ucmdb-api is now mapped to: HTTPS_CLIENT_AUTH ports.

f. Revenez à la page Operations.

2. Vérifiez que le JRE qui exécute le client UCMDB-API comporte un magasin de clés contenant un certificat client.

3. Exportez le certificat du client UCMDB-API à partir de son magasin de clés.

4. Importez le certificat du client UCMDB-API dans le magasin d'approbations du serveur UCMDB.

   a. À partir de l'ordinateur d'UCMDB, copiez le fichier du certificat du client UCMDB-API dans le répertoire UCMDB suivant :

   C:\HP\UCMDB\UCMDBServer\conf\security

   b. Exécutez la commande suivante :

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
   C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <exported
   du client UCMDB-api exporté> - alias ucmdb-api
   ```

   c. Entrez le mot de passe truststore du serveur UCMDB (**hppass** par défaut).

   d. Lorsque le message **Trust this certificate?** apparaît, appuyez sur **y** puis sur **Entrée**.

   e. Vérifiez que le résultat **Certificate** a été ajouté au magasin de clés.

5. Exportez le certificat du serveur UCMDB à partir de son magasin de clés (keystore) serveur.

   a. À partir de l'ordinateur UCMDB, exécutez la commande suivante :

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert
   -keystore
   C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore
   -file C:\HP\UCMDB\conf\security\server.cert
   ```

   b. Entrez le mot de passe du magasin d'approbations du serveur UCMDB (**hppass** par défaut).

   c. Vérifiez que le certificat est créé dans le répertoire

   C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

6. Importez le certificat UCMDB exporté dans le JRE du magasin d'approbations du client UCMDB-API.

7. Redémarrez le serveur UCMDB et le client UCMDB-API.

8. Pour vous connecter à partir du client UCMDB-API au serveur UCMDB-API, utilisez le code suivant :

```
UcmdbServiceProvider provider = UcmdbServiceFactory.getServiceProvider
("https", <SOME_HOST_NAME>, <HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER
(default:8444>));
UcmdbService ucmdbService = provider.connect(provider.createCertificateCrede
ntials(<TheClientKeystore.
Exemple :: "c:\\client.keystore">, <KeystorePassword>), provider.createClien
tContext(<ClientIdentification>));
```

Configurer la prise en charge CAC sur UCMDB

(missing or bad snippet)
Pour plus d'informations sur l'authentification LW-SSO, voir " Activation de la connexion à HP Universal CMDB via LW-SSO " , page 97.

Modifier le mot de passe du magasin de clés du serveur

Après l'installation du serveur, le port HTTPS est ouvert et le magasin est sécurisé avec un mot de passe faible (**hppass** par défaut). Si vous prévoyez d'utiliser uniquement SSL, vous devez changer ce mot de passe.

La procédure ci-après explique comment modifier uniquement le mot de passe **server.keystore**. Cependant, vous devrez exécuter la même procédure pour modifier le mot de passe **server.truststore**.

Remarque : Exécutez chaque étape de cette procédure.

1. Démarrez le serveur UCMDB.

2. Changez le mot de passe dans la console JMX :

   a. Lancez le navigateur Web, puis entrez comme suit l'adresse du serveur : **http://<nom d'hôte ou adresse IP du serveur UCMDB>:8080/jmx-console**.

      Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

   b. Sous UCMDB, cliquez sur **UCMDB:service=Security Services** pour ouvrir la page Operations.

c. Recherchez et exécutez l'opération **changeKeystorePassword**.

Ce champ ne doit pas être vide et doit comprendre au moins six caractères. Le mot de passe a été modifié uniquement dans la base de données.

3. Arrêtez le serveur UCMDB.

4. Exécutez les commandes.

À partir de **C:\hp\UCMDB\UCMBServer\bin\jre\bin**, exécutez les commandes suivantes :

a. Changez le mot de passe store :

keytool -storepasswd -new <nouveau_mot_passe_keystore> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <mot_passe_keystore_actuel>

b. La commande ci-après affiche la clé interne du keystore. Le premier paramètre correspond à l'alias. Enregistrez ce paramètre pour la commande suivante :

keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

c. Changez le mot de passe key (si le mot de passe store n'est pas vide) :

keytool -keypasswd -alias <alias> -keypass <mot_passe_actuel> -new <nouveau_mot_passe> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

d. Entrez le nouveau mot de passe.

5. Démarrez le serveur UCMDB.

6. Répétez la procédure pour le mot de passe truststore du serveur.

Activer ou désactiver les ports HTTP/HTTPS

Vous pouvez activer ou désactiver les ports HTTP et HTTPS à partir de l'interface utilisateur ou de la console JMX.

Pour activer ou désactiver les ports HTTP/HTTPS à partir de l'interface utilisateur :

1. Connectez-vous à HP Universal CMDB.

2. Sélectionnez **Administration > Gestionnaire des paramètres d'infrastructure**.

3. Entrez **http** ou **https** dans la zone **Filtrer** (par nom) pour afficher les paramètres HTTP.

- **Activer les connexions HTTP(S)**. **True** : le port est activé. **False** : le port est désactivé.

4. Redémarrez le serveur pour appliquer la modification.

> **Attention :** Le port HTTPS est ouvert par défaut. Sa fermeture empêche le fonctionnement de **Server_Management.bat**.

Pour activer ou désactiver les ports HTTP/HTTPS à partir de la console JMX :

1. Lancez un navigateur Web et entrez l'adresse suivante : http://localhost.<nom_ domaine>:8080/jmx-console.
2. Entrez les informations d'identification pour l'authentification de la console JMX. Les informations d'identification par défaut sont les suivantes :
   - Nom de connexion = **sysadmin**
   - Mot de passe = **sysadmin**
3. Recherchez **UCMDB:service=Ports Management Services** et cliquez sur le lien pour accéder à la page Operations.
4. Pour activer ou désactiver le port HTTP, recherchez l'opération **HTTPSetEnable** et définissez la valeur.
   - **True :** le port est activé.
   - **False :** le port est désactivé.
5. Pour activer ou désactiver le port HTTPS, recherchez l'opération **HTTPSSetEnable** et définissez la valeur.
   - **True :** le port est activé.
   - **False :** le port est désactivé.
6. Pour activer ou désactiver le port HTTPS avec l'authentification du client, recherchez l'opération **HTTPSClientAuthSetEnable** et définissez la valeur.
   - **True :** le port est activé.
   - **False :** le port est désactivé.

Mapper les composants Web UCMDB sur les ports

Vous pouvez configurer le mappage de chaque composant UCMDB sur les ports disponibles à partir de la console JMX.

Pour afficher la configuration des composants en cours :

1. Lancez un navigateur Web et entrez l'adresse suivante : **http://localhost.<nom_ domaine>:8080/jmx-console**.
2. Entrez les informations d'identification pour l'authentification de la console JMX. Les informations d'identification par défaut sont les suivantes :

   Nom de connexion = **sysadmin**

   Mot de passe = **sysadmin**
3. Recherchez **UCMDB:service=Ports Management Services** et cliquez sur le lien pour accéder à la page Operations.
4. Recherchez la méthode **ComponentsConfigurations** et cliquez sur **Invoke**.
5. Pour chaque composant, les ports valides et les ports mappés en cours s'affichent.

Pour mapper les composants :

1. Recherchez **UCMDB:service=Ports Management Services** et cliquez sur le lien pour accéder à la page Operations.
2. Recherchez la méthode **mapComponentToConnectors**.
3. Entrez un nom de composant dans le champ Value. Sélectionnez **True** ou **False** pour chacun des ports correspondant à votre sélection. Cliquez sur **Invoke**. Le composant sélectionné est mappé sur les ports sélectionnés. Vous pouvez rechercher les noms de composant en appelant la méthode **serverComponentsNames**.
4. Répétez la procédure pour chaque composant concerné.

Remarque :

- Chaque composant doit être mappé sur au moins un port. Si un composant n'est mappé sur aucun port, il est mappé par défaut sur le port HTTP.
- Si vous mappez un composant sur le port HTTPS avec et sans authentification du client, seule l'option authentification du client est mappée (dans ce cas, l'autre option est redondante).
- Si vous définissez **isHTTPSWithClientAuth** avec la valeur **True** pour le composant interface utilisateur de UCMDB, vous devez également définir la valeur **True** pour le composant racine (root).

Vous pouvez également modifier la valeur attribuée à chacun des ports.

Pour définir les valeurs des ports :

1. Recherchez **UCMDB:service=Ports Management Services** et cliquez sur le lien pour accéder à la page Operations.

2. Pour définir une valeur pour le port HTTP, recherchez la méthode **HTTPSetPort** et entrez une valeur dans le champ **Value**. Cliquez sur **Invoke**.

3. Pour définir une valeur pour le port HTTPS, recherchez la méthode **HTTPSSetPort** et entrez une valeur dans le champ **Value**. Cliquez sur **Invoke**.

4. Pour définir une valeur pour le port HTTPS avec authentification du client, recherchez la méthode **HTTPSClientAuthSetPort** et entrez une valeur dans le champ **Value**. Cliquez sur **Invoke**.

Configurer Configuration Manager pour l'utiliser avec UCMDB à l'aide de SSL

Vous pouvez configurer Configuration Manager pour fonctionner avec UCMDB en utilisant SSL (Secure Sockets Layer). Le connecteur SSL sur le port 8443 est activé par défaut dans UCMDB.

1. Allez dans **<répertoire d'installation UCMDB>\bin\jre\bin** et exécutez la commande suivante :

   ```
   keytool -export -alias hpcert -keystore <répertoire_serveur_UCMDB>
   \conf\security\server.keystore -storepass hppass -file <fichiercertificat>
   ```

2. Copiez le fichier de certificat dans un emplacement temporaire sur l'ordinateur qui héberge Configuration Manager.

3. Effectuez la nouvelle installation ou reconfigurez une installation existante de Configuration Manager. Pour plus d'informations, voir les sections correspondantes dans le *Manuel de déploiement HP Universal CMDB*.

   Dans l'écran de configuration UCMDB, définissez le protocole sur HTTPS et choisissez le fichier de certificat que vous avez copié à l'étape 2.

4. Copiez **hpcert.cer** dans le dossier ***<répertoire_installation_Configuration_Manager>*\java\windows\x86_64\bin** de l'ordinateur serveur.

5. Sur l'ordinateur serveur, importez le certificat d'autorité de certification dans le magasin d'approbations (cacerts) à l'aide de l'utilitaire keytool avec la commande suivante :

   ```
   <répertoire_installation_Configuration_Manager>\java\bin\keytool.exe -import
   -alias hp -file hpcert.cer -keystore <répertoire_installation_Configuration_
   Manager>\java\windows\x86_64\lib\security\cacerts
   ```

6. Copiez **hpcert.cer** dans le dossier **<*répertoire_installation_Configuration_Manager*>\java\windows\x86_64\lib\security** de l'ordinateur serveur.

7. Créez un magasin de clés (type JKS) à l'aide d'un certificat auto-signé et d'une clé privée correspondante. **À partir du dossier <*répertoire_installation_Configuration_Manager*>\java\windows\x86_64\bin**, exécutez la commande suivante :

   ```
   keytool –genkey –alias tomcat –keyalg RSA –keystore <répertoire_installation_
   Configuration_Manager>\java\windows\x86_64\lib\security\tomcat.keystore
   ```

   a. Entrez un mot de passe de magasin de clés.

   b. Répondez à la question `Quels sont vos nom et prénom ?`, entrez le nom du serveur Web de Configuration Manager et les autres paramètres en fonction de votre organisation.

   c. Entrez le mot de passe de clé. Il DOIT être identique à celui du magasin de clés. Un magasin de clés JKS est créé sous le nom **tomcat.keystore** avec un certificat de serveur appelé **hpcert**.

8. Modifiez le fichier **server.xml** comme suit :

   a. Ouvrez le fichier server.xml qui se trouve dans le dossier **<*répertoire_installation_Configuration_Manager*>\servers\server-0\conf**. Localisez la section commençant par

      ```
      Connector port="8143"
      ```

      qui apparaît sous forme de commentaire. Activez le script en supprimant le caractère de commentaire et ajoutez les lignes suivantes :

      ```
      keystoreFile="<répertoire_installation_Configuration_Manager>\java\window
      s\x86_64\lib\security\tomcat.keystore"
      keystorePass="password"
      truststoreFile="<répertoire_installation_Configuration_Manager>\java\wind
      ows\x86_64\lib\security\cacerts"
      truststorePass="changeit" />
      ```

   b. Mettez en commentaire la ligne suivante :

      ```
      <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEn
      gine="on" />
      ```

9. Redémarrez le serveur.

Pour configurer Configuration Manager pour fonctionner avec d´autres produits (tels que les processus d´équilibrage) en utilisant SSL, importez le certificat de sécurité du produit dans le magasin d´approbations Configuration Manager (magasin d´approbations par défaut) en exécutant la commande suivante :

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias> -keystore
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file <certificatefile>
```

Autoriser l'utilisation de l'adaptateur KPI UCMDB avec SSL

Vous pouvez configurer l'envoi des informations de l'adaptateur KPI UCMDB par SSL (Secure Sockets Layer).

1. Exportez le certificat Configuration Manager :

   ```
   <ACCUEIL_JAVA_CM>\bin\keytool -export -alias tomcat -keystore
   <ACCUEIL_JAVA_CM>\lib\security\tomcat.keystore -storepass
   <mot de passe du keystore> -file <nom du fichier de certificat>
   ```

2. Importez le certificat que vous avez exporté de Configuration Manager vers le magasin d'approbations UCMDB comme suit :

   ```
   <répertoire du serveur UCMDB>\bin\jre\bin keytool -import -trustcacerts
   -alias tomcat -keystore <répertoire du serveur UCMDB>\bin\jre\lib
   \security\cacerts -storepass changeit -file <fichiercertificat>
   ```

3. Importez le certificat que vous avez exporté de Configuration Manager vers le magasin d'approbations UCMDB comme suit :

   a. À partir de l'invite de commande, exécutez la commande suivante :

      ```
      <répertoire de DataFlowProbe>\bin\jre\bin\keytool.exe -import -v -keystor
      e
      <répertorie de DataFlowProbe>\conf\security\hpprobeTrustStore.jks -file
      <certificatefile> -alias tomcat
      ```

   b. Entrez le mot de passe du magasin de clés : logomania

   c. Lorsque le message **Trust this certificate?** apparaît, appuyez sur **y** puis sur **Entrée**.

      Le message suivant apparaît :

      Certificate was added to keystore.

      Pour plus d'informations sur le renforcement de Data Flow Probe, voir " Sécurisation renforcée de Data Flow Probe " , page 70.

4. Redémarrez UCMDB, Data Flow Probe et Configuration Manager.

Configuration du support SSL pour UCMDB Browser

Remarque : Les instructions fournies ici s'appliquent à UCMDB Browser version 1.95. Si vous utilisez une version postérieure suite à une mise à niveau de UCMDB Browser effectuée

séparément du reste de la suite de produits UCMDB, voir la section relative à la configuration du support SSL dans le manuel *HP Universal CMDB Browser Installation and Configuration Guide* de cette version.

Pour installer et configurer le support SSL sur Tomcat :

1. Créez un fichier keystore destiné au stockage de la clé privée et du certificat auto-signé du serveur en exécutant l'une des commandes suivantes :

   - Pour Windows : **%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
   - Pour Unix : **$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

   Dans les deux cas, utilisez la valeur de mot de passe **changeit** (pour tous les autres champs de la boîte de dialogue de la console, vous pouvez choisir n'importe quelle valeur).

2. Supprimez les commentaires de l'entrée **SSL HTTP/1.1 Connector** dans **$CATALINA_BASE/conf/server.xml**, où **$CATALINA_BASE** désigne le répertoire d'installation de Tomcat.

   Remarque : Pour une description complète de la procédure de configuration de **server.xml** afin d'utiliser SSL, voir le site officiel d'Apache Tomcat. http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

3. Redémarrez le serveur Tomcat.

Pour utiliser le protocole HTTPS afin d'établir la connexion avec le serveur UCMDB :

1. Dans **ucmdb_browser_config.xml**, affectez la valeur **https** à la balise**<protocol>** et attribuez la valeur de port HTTPS (par défaut, 8443) du serveur UCMDB à la balise **<port>.**

2. Téléchargez le certificat public du serveur UCMDB sur l'ordinateur UCMDB Browser (si vous utilisez SSL sur le serveur UCMDB, l'administrateur UCMDB peut vous fournir le certificat), puis importez-le dans le magasin d'approbations **cacerts** du JRE qui va se connecter au serveur. Pour ce faire, exécutez la commande suivante :

   "%JAVA_HOME%\bin\keytool" -import -alias ucmdb -trustcacerts -file <fichier de certificat de serveur UCMDB> -keystore "%JAVA_HOME%\jre\lib\security\cacerts"

   où **<fichier de certificat de serveur UCMDB>** est le chemin d'accès complet au fichier du certificat public du serveur UCMDB.

3. Redémarrez le serveur Tomcat.

Chapitre 3 : Utilisation d'un proxy inverse

Cette section décrit les ramifications de sécurité d'un proxy inverse et contient des instructions sur l'utilisation de celui-ci avec HP Universal CMDB et Configuration Manager. Seuls les aspects de la sécurité d'un proxy inverse sont abordés ; les autres aspects tels que la mise en cache et la répartition de la charge ne sont pas traités.

Contenu de ce chapitre :

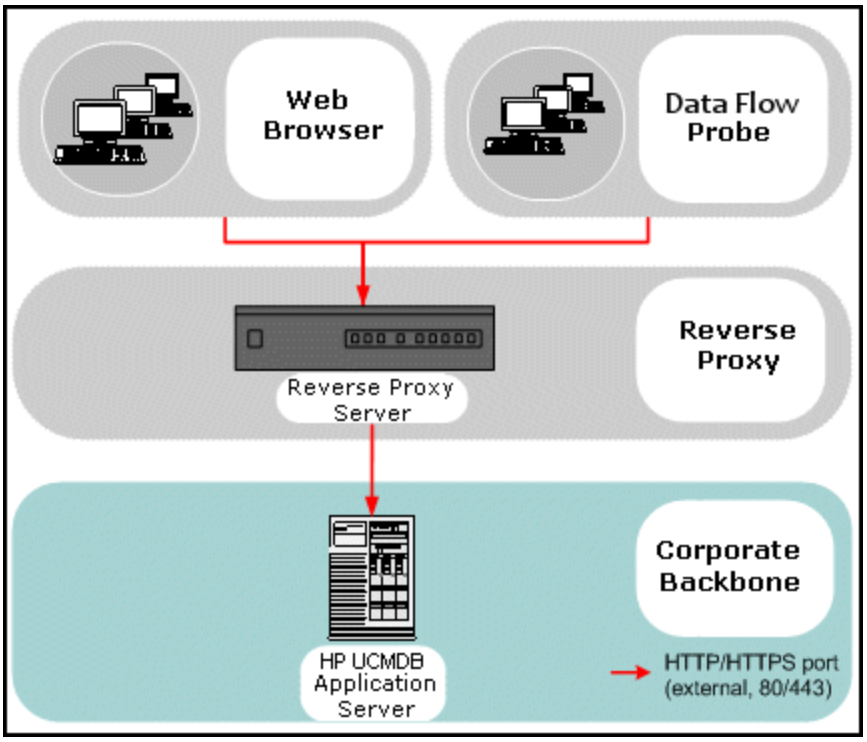
Proxy inverse - Présentation

Un proxy inverse est un serveur intermédiaire qui est placé entre l'ordinateur client et les serveurs Web. Pour l'ordinateur client, le proxy inverse est considéré comme un serveur Web standard qui prend en charge les demandes de protocole HTTP de l'ordinateur client.

L'ordinateur client envoie des demandes ordinaires de contenu Web en utilisant le nom du proxy inverse au lieu de celui d'un serveur Web. Le proxy inverse envoie la demande à un des serveurs Web. Bien que la réponse soit renvoyée à l'ordinateur client par le proxy inverse, pour l'ordinateur client, elle apparaît comme si elle avait été envoyée par le serveur Web.

Il est possible de disposer de plusieurs proxys inverses, avec des URL différentes, représentant la même instance UCMDB/CM. Un serveur proxy inverse unique peut également servir à accéder à plusieurs serveurs UCMDB/CM. Pour ce faire, il s'agit de définir différents contextes racine pour chaque serveur UCMDB/CM.

HP Universal CMDB et Configuration Manager prennent en charge un proxy inverse dans une architecture DMZ. Le proxy inverse est un médiateur HTTP entre Data Flow Probe, le client Web et le serveur HP Universal CMDB/CM.



Remarque :

- Les différents types de proxy inverse requièrent des syntaxes de configuration différentes. Reportez-vous à l'exemple de configuration d'un proxy inverse Apache 2.0.x à la section " Exemple : configuration d'Apache 2.0.x " , page 40.
- Il est uniquement nécessaire de configurer le paramètre URL frontale lors de la création d'un lien direct à un rapport à l'aide du planificateur.

Aspects de la sécurité d'un serveur proxy inverse

Un serveur proxy inverse fonctionne comme un hôte bastion. Le proxy est configuré pour être le seul ordinateur accessible directement par les clients externes, ce qui obscurcit le reste du réseau interne. L'utilisation d'un proxy inverse permet au serveur d'applications d'être placé dans un ordinateur à part du réseau interne.

Cette section décrit l'utilisation d'une DMZ et d'un proxy inverse dans un environnement de topologie dos à dos.

L'utilisation d'un proxy inverse dans un tel environnement présente les principaux avantages suivants en terme de sécurité :

- La conversion du protocole DMZ est inutile. Les protocoles entrant et sortant sont identiques (seul l'en-tête est modifié).

- Seul l'accès HTTP au proxy inverse est autorisé ; les pare-feux d'inspection des paquets avec état peuvent ainsi mieux protéger la communication.
- Un ensemble statique restreint de demandes redirigées peut être défini sur le proxy inverse.
- La plupart des fonctions de sécurité du serveur Web sont disponibles sur le proxy inverse (méthodes d'authentification, chiffrement, etc.).
- Le proxy inverse filtre les adresses IP des serveurs réels ainsi que l'architecture du réseau interne.
- Le seul client accessible du serveur Web est le proxy inverse.
- Cette configuration prend en charge les pare-feux NAT (contrairement aux autres solutions).
- Le proxy inverse requiert un nombre minimal de ports ouverts dans le pare-feu.
- Le proxy inverse offre de bonnes performances comparativement aux autres solutions de bastion.

Configurer un proxy inverse

Cette section explique comment configurer un proxy inverse. Aucune configuration n'est nécessaire dans UCMDB, comme dans la version 10.01. Côté proxy inverse, modifiez le fichier de configuration conformément à la documentation fournie avec le proxy inverse. Reportez-vous à l'exemple décrit à la section " Exemple : configuration d'Apache 2.0.x " , page suivante.

Pour les travaux planifiés qui ont été créés avant la version 10.01 de UCMDB, vous devez également définir la configuration dans UCMDB en procédant comme suit :

Configurer un proxy inverse à l'aide des paramètres d'infrastructure

La procédure ci-après explique comment accéder aux paramètres d'infrastructure pour configurer un proxy inverse. La configuration est uniquement nécessaire lors de la création d'un lien direct à un rapport à l'aide du planificateur.

Pour configurer un proxy inverse :

1. Sélectionnez la catégorie **Administration > Gestionnaire des paramètres d'infrastructure > Paramètres généraux**.
2. Modifiez le paramètre **URL frontale**. Entrez, par exemple, l'adresse **https://my_proxy_server:443/**.

Remarque : Une fois cette modification effectuée, vous ne pouvez plus accéder au serveur HP Universal CMDB directement par un client. Pour modifier la configuration du proxy inverse, utilisez la console JMX sur l'ordinateur serveur. Pour plus d'informations, voir « Configurer un proxy inverse à l'aide de la console JMX » ci-dessous.

Configurer un proxy inverse à l'aide de la console JMX

Vous pouvez modifier la configuration du proxy inverse à l'aide de la console JMX sur l'ordinateur du serveur HP Universal CMDB. Cette configuration n'est nécessaire que lors de la création d'un lien direct à un rapport à l'aide du planificateur.

Pour modifier une configuration de proxy inverse :

1. Sur l'ordinateur du serveur HP Universal CMDB, lancez le navigateur Web et entrez l'adresse suivante :

   http://<nom ou adresse IP de l'ordinateur>.<nom_domaine>:8080/jmx-console

   où **<nom ou adresse IP de l'ordinateur>** est l'ordinateur sur lequel HP Universal CMDB est installé. Si vous y êtes invité, entrez un nom d'utilisateur et un mot de passe pour vous connecter.

2. Cliquez sur le lien **UCMDB-UI > UCMDB-UI:name=UI Server frontend settings**.

   Dans le champ **setUseFrontendURLBySettings**, entrez l'URL du serveur proxy, par exemple `https://my_proxy_server:443/`.

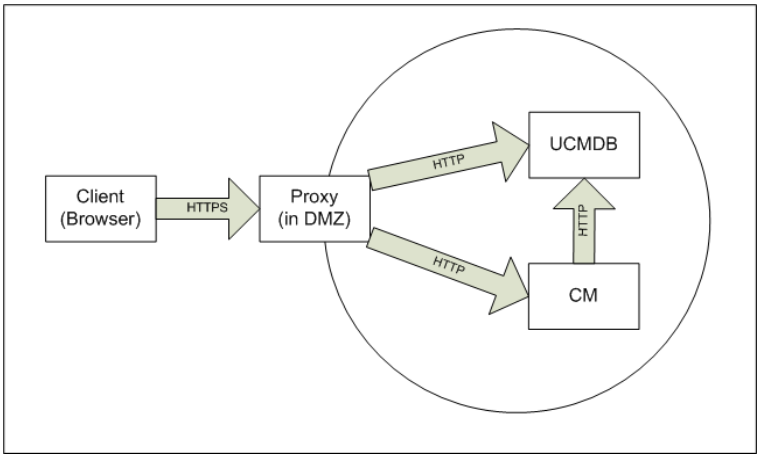
3. Cliquez sur **Invoke**.

4. Pour afficher la valeur de ce paramètre, utilisez la méthode **showFrontendURLInSettings**.

Exemple : configuration d'Apache 2.0.x

Cette section décrit un exemple de fichier de configuration qui prend en charge l'utilisation d'un proxy inverse Apache 2.0.x dans le cas où les sondes des flux de données et les utilisateurs de l'application se connectent à HP Universal CMDB.

Le diagramme suivant illustre la procédure de configuration d'un proxy inverse pour Configuration Manager et la base UCMDB.



Remarque :

- Dans cet exemple, le nom et le port DNS de l'ordinateur HP Universal CMDB est UCMDB_server.
- Dans cet exemple, le nom et le port DNS de HP Configuration Manger est UCMDB_CM_server.
- Seuls les utilisateurs maîtrisant l'administration Apache doivent effectuer cette modification.

1. Ouvrez le fichier **<répertoire racine de l'ordinateur Apache>\Webserver\conf\httpd.conf**.
2. Activez les modules suivants :
   - **LoadModule proxy_module modules/mod_proxy.so**
   - **LoadModule proxy_http_module modules/mod_proxy_http.so**
3. Ajoutez les lignes suivantes au fichier **httpd.conf** :

```
ProxyRequests off
<Proxy *>
     Order deny,allow
     Deny from all
     Allow from all
</Proxy>

ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
```

```
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
```

4. Enregistrez vos modifications.

Connecter Data Flow Probe par un proxy inverse ou un répartiteur de charge à l'aide de l'authentification mutuelle

Exécutez la procédure ci-après pour connecter Data Flow Probe via un proxy inverse ou un répartiteur de charge à l'aide le l'authentification mutuelle. Cette procédure s'applique à la configuration suivante :

- authentification SSL mutuelle entre la sonde et un proxy inverse ou un répartiteur de charge, reposant sur un certificat client fourni par la sonde et demandé par le proxy inverse ou le répartiteur de charge ;
- connexion SSL standard entre le proxy inverse ou le répartiteur de charge et le serveur UCMDB.

Remarque : Les instructions ci-après utilisent le magasin de clés **cKeyStoreFile** pour la sonde. Il s'agit d'un magasin de clés client prédéfini qui fait partie de l'installation de Data Flow Probe et contient des certificats auto-signés. Pour plus d'informations, voir " Magasins de clés et d'approbations par défaut de Data Flow Probe " , page 86.

Il est recommandé de créer un magasin de clés unique contenant une clé privée nouvellement générée. Pour plus d'informations, voir " Créer un magasin de clés pour Data Flow Probe " , page 85.

Obtenir un certificat auprès d'une autorité de certification

Obtenez le certificat racine auprès de l'autorité de certification et importez-le aux emplacements suivants :

- magasin d'approbations de Data Flow Probe
- cacerts JVM de Data Flow Probe

- magasin d'approbations du serveur UCMDB
- magasin d'approbations du proxy inverse.

1. Importez le certificat racine de l'autorité de certification dans le magasin d'approbations de Data Flow Probe.

   a. Placez le certificat racine de l'autorité de certification dans le répertoire suivant : <répertoire d'installation de Data Flow Probe >\conf\security\<nom du fichier de certificat>.

   b. Importez le certificat racine de l'autorité de certification dans le magasin d'approbations de Data Flow Probe en exécutant le script suivant :

   ```
   <répertoire d'installation de Data Flow Probe>\bin\jre\bin\keytool.exe -i
   mport -trustcacerts -alias <VotreAlias> -file C:\hp\UCMDB\DataFlowProbe\c
   onf\security\<nom de fichier du certificat> -keystore <répertoire d'insta
   llation de Data Flow Probe>\conf\security\hpprobeTrustStore.jks
   ```

   Le mot de passe par défaut est : **logomania**.

2. Importez le certificat racine de l'autorité de certification dans le cacerts JVM de Data Flow Probe en exécutant le script suivant :

   ```
   <répertoire d'installation de Data Flow Probe>\bin\jre\bin\keytool.exe -impo
   rt -trustcacerts -alias <VotreAlias> -file <répertoire d'installation de Data
   Flow Probe>\conf\security\<nom du fichier de certificat> -keystore <répertoi
   re d'installation de Data Flow Probe>\bin\jre\lib\security\cacerts
   ```

   Le mot de passe par défaut est : **changeit**.

3. Importez le certificat racine de l'autorité de certification dans le magasin d'approbations UCMDB.

   a. Placez le certificat racine de l'autorité de certification dans le répertoire suivant : <répertoire d'installation UCMDB>\conf\security\<nom du fichier de certificat>.

   b. Importez le certificat racine de l'autorité de certification dans le magasin d'approbations UCMDB en exécutant le script suivant :

   ```
   <répertoire d'installation UCMDB>\bin\jre\bin\keytool.exe -import -trustc
   acerts -alias <VotreAlias> -file <répertoire d'installation UCMDB>\conf\s
   ecurity\<nom du fichier de certificat> -keystore <répertoire d'installati
   on UCMDB>\conf\security\sever.truststore
   ```

   Le mot de passe par défaut est : **hppass**.

4. Importez le certificat racine de l'autorité de certification dans le magasin d'approbations du proxy inverse. Cette étape dépend du fournisseur.

Convertir le certificat en magasin de clés Java

Obtenez le certificat client (et la clé privée) de Data Flow Probe auprès de l'autorité de certification

au format PFX/PKCS12. Convertissez-le ensuite en magasin de clés Java en exécutant le script suivant :

```
<répertoire d'installation de Data Flow Probe>\bin\jre\bin\keytool.exe -importke
ystore -srckeystore <chemin complet du magasin de clés PFX> -destkeystore <chemi
n complet du magasin de clés de la nouvelle destination> -srcstoretype PKCS12
```

Les mots de passe du magasin de clés source et cible vous seront demandés.

Pour le mot de passe du magasin de clés source, utilisez le même mot de passe que celui utilisé lors de l'exportation du magasin de clés PFX.

Le mot de passe par défaut du magasin de clés cible pour Data Flow Probe est : **logomania**.

Remarque : Si le mot de passe que vous avez entré pour le magasin de clés cible diffère de celui par défaut du magasin de clés de Data Flow Probe (logomania), vous devez fournir le nouveau mot de passe au format chiffré dans le fichier **<répertoire d'installation de la sonde>\conf\ssl.properties** (javax.net.ssl.keyStorePassword). Pour plus d'informations, voir " Chiffrer les mots de passe des magasins de clés et d'approbations de la sonde " , page 86.

Placez le nouveau magasin de clés dans le répertoire suivant : **<répertoire d'installation de Data Flow Probe>\conf\security**.

Attention : Ne remplacez pas le fichier **hpprobeKeyStore.jks**.

Modifier le fichier des propriétés SSL pour utiliser le magasin de clés nouvellement créé

Attribuez la valeur **javax.net.ssl.keyStore** au magasin de clés qui contient le certificat client dans le fichier **<répertoire d'installation de Data Flow Probe>\conf\ssl.properties**.

Si le mot de passe qui est associé au magasin de clés diffère du mot de passe par défaut du magasin de Data Flow Probe (logomania), actualisez **javax.net.ssl.keyStorePassword** après l'avoir chiffré. Pour plus d'informations sur le chiffrement du mot de passe, voir " Chiffrer les mots de passe des magasins de clés et d'approbations de la sonde " , page 86.

Vérifier la configuration de Data Flow Probe

Modifiez le fichier **<répertoire d'installation de Data Flow Probe>\conf\DataFlowProbe.properties** comme suit :

```
appilog.agent.probe.protocol = HTTPS

serverName = <adresse du serveur proxy inverse>

serverPortHttps = <port HTTPS utilisé par le proxy inverse comme port d'écoute p
our rediriger les demandes vers la base UCMDB>
```

Configurer UCMDB pour une utilisation du protocole SSL

Pour plus d'informations, voir " Activation de la communication SSL (Secure Sockets Layer) " , page 18.

Si le certificat du serveur UCMDB est créé par la même autorité de certification qui a généré le reste des certificats dans la procédure, le proxy inverse ou le répartiteur de charge approuve le certificat UCMDB.

Configurer la prise en charge de CAC pour UCMDB par un proxy inverse

Cette section explique comment configurer la prise en charge de Common Access Card (CAC) sur UCMDB à l'aide d'un proxy inverse.

1. Pour accéder à la console JMX, lancez votre navigateur Web et entrez l'adresse du serveur, comme suit : http://<nom d'hôte ou adresse IP du serveur UCMDB>:8080/jmx-console.

   Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

2. Sous UCMDB, cliquez sur **UCMDB:service=Ports Management Services** pour ouvrir la page Operations.

   - (Facultatif) Cliquez sur **ComponentsConfigurations**. Procédez comme suit :
     - Pour **HTTPSetPort**, définissez la valeur **8080** et cliquez sur **Invoke**.
     - Cliquez sur **Back to MBean**.
   - Cliquez sur **mapComponentToConnectors**. Procédez comme suit :
     - Dans le service mapComponentToConnectors, définissez la valeur **ucmdb-ui** pour **componentName**.
     - Pour **isHTTP** uniquement, définissez la valeur **true** et cliquez sur **Invoke**.
     - Cliquez sur **Back to MBean**.
     - Dans le service mapComponentToConnectors, définissez la valeur **root** pour **componentName**.
     - Pour **isHTTP** uniquement, définissez la valeur **true** et cliquez sur **Invoke**.

3. Sous UCMDB, cliquez sur **UCMDB:service=Security Services** pour ouvrir la page Operations.

   - Pour **loginWithCAC**, définissez la valeur **true** et cliquez sur **Invoke**.
   - Cliquez sur **Back to MBean**.
   - Pour **withReverseProxy**, définissez la valeur **true** et cliquez sur **Invoke**.

Ce paramètre indique au serveur UCMDB d'extraire de l'en-tête UCMDB_SSL_CLIENT_CERT le nom d'utilisateur à utiliser dans UCMDB et le certificat à utiliser pour l'authentification.

- Cliquez sur **Back to MBean**.
- (Facultatif) Pour **onlyCACCerts**, définissez la valeur **true** et cliquez sur **Invoke**.

  Définissez la valeur **true** pour cette opération de façon à accepter uniquement les certificats provenant d'un périphérique CAC physique.

4. Redémarrez le serveur UCMDB.

Exemple : Configuration d'Apache 2.4.4

Cette section décrit un exemple de fichier de configuration pour Apache 2.4.4 (dans le fichier **<répertoire racine de l'ordinateur Apache>\Webserver\conf\httpd.conf** :

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
ServerName Apache_Server_Name:80
Include conf/extra/httpd-ssl.conf
```

Cette section décrit un exemple de fichier de configuration pour Apache 2.4.4 avec SSL (dans le fichier **<répertoire racine de l'ordinateur Apache>\Webserver\conf\extra\httpd-ssl.conf** :

```
Listen 8443<VirtualHost _default_:8443>
ServerName Apache_Server_Name:8443
SSLCACertificateFile "c:/Apache24/conf/ssl.crt"
SSLCARevocationFile "c:/Apache24/conf/ssl.crl"
#SSLCARevocationCheck chain|leaf|none
SSLCARevocationCheck leaf
RequestHeader set UCMDB_SSL_CLIENT_CERT %{SSL_CLIENT_CERT}e


ProxyRequests off
<Proxy *>
     Order deny,allow
     Deny from all
     Allow from all
</Proxy>

ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
```

```
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
SSLVerifyClient require
SSLVerifyDepth  10
SSLOptions+ExportCertData
```

Chapitre 4 : Gestion des informations d'identification des flux de données

Contenu de ce chapitre :

Gestion des informations d'identification des flux de données - Présentation

Pour effectuer une intégration d'exécution ou de découverte, vous devez configurer les informations d'identification permettant d'accéder au système distant. Ces informations sont configurées dans la fenêtre Configuration de Data Flow Probe et enregistrées dans le serveur UCMDB. Pour plus d'informations, voir la section relative à la configuration de Data Flow Probe dans le *Manuel de gestion des flux de données HP Universal CMDB*.

Le stockage des informations d'identification est géré par le composant Confidential Manager. Pour plus d'informations, voir " Confidential Manager " , page 105.

Data Flow Probe peut accéder aux informations d'identification à l'aide du client Confidential Manager. Ce client réside dans Data Flow Probe et communique avec le serveur Confidential Manager qui se trouve sur le serveur UCMDB. La communication enter le client et le serveur Confidential Manager est chiffrée, et le client Confidential Manager requiert une authentification lors d'une connexion avec le serveur Confidential Manager.

L'authentification du client Confidential Manager sur le serveur Confidential Manager repose sur un composant LW-SSO. Avant de se connecter au serveur Confidential Manager, le client Confidential Manager envoie d'abord un cookie LW-SSO. Le serveur Confidential Manager vérifie le cookie et si celui-ci est valide, la communication est établie avec le client Confidential Manager. Pour plus d'informations sur LW-SSO, voir " Configurer les paramètres LW-SSO " , page 53.

La communication entre le client et le serveur Confidential Manager est chiffrée. Pour plus d'informations sur la mise à jour de la configuration du chiffrement, voir " Configurer le chiffrement de la communication Confidential Manager " , page 54.

Attention : L'authentification Confidential Manager utilise l'heure universelle définie sur l'ordinateur (UTC). Pour garantir le succès de l'authentification, veillez à ce que l'heure universelle définie sur Data Flow Probe et du serveur UCMDB soit la même. Le serveur et la sonde peuvent appartenir à des fuseaux horaires différents, puisque l'heure UTC est indépendante du fuseau horaire ou de l'heure d'été.

Le client Confidential Manager conserve un cache local des informations d'identification. Il est configuré pour télécharger toutes les informations d'identification du serveur Confidential Manager qu'il stocke dans un cache. Les modifications des informations d'identification sont synchronisées automatiquement et en permanence à partir du serveur Confidential Manager. Le cache peut être du type système de fichiers ou cache mémoire, selon les paramètres préconfigurés. En outre, le cache

est chiffré et n'est pas accessible en externe. Pour plus d'informations sur la mise à jour des paramètres du cache, voir " Configurer le mode cache du client Confidential Manager dans la sonde " , page 58. Pour plus d'informations sur la mise à jour du chiffrement du cache, voir " Configurer les paramètres de chiffrement du cache du client Confidential Manager dans la sonde " , page 59.

Pour plus d'informations sur la résolution des problèmes, voir " Changer le niveau des messages des fichiers journaux du client Confidential Manager " , page 62.

Vous pouvez copier les informations d'identification d'un serveur UCMDB à l'autre. Pour plus d'informations, voir " Exporter et importer les informations de plage réseau et d'identification au format chiffré " , page 60.

Remarque : Le fichier **DomainScopeDocument** (DSD) qui a été utilisé pour le stockage des informations d'identification dans la sonde (UCMDB version 9.01 ou antérieure) ne contient plus d'informations d'identification sensibles. Ce fichier contient à présent une liste de sondes et des informations de plage réseau. Il contient également la liste des informations d'identification pour chaque domaine, où chaque entrée comprend uniquement l'ID des informations d'identification et une plage réseau (définie pour cette entrée).

Contenu de cette section :

Principes de base de sécurité

Notez le principe de sécurité suivant :

Vous avez sécurisé la console JMX du serveur et de la sonde UCMDB pour permettre aux seuls administrateurs système d'accéder au système UCMDB, de préférence via l'accès localhost seulement.

Exécution de Data Flow Probe en mode autonome

Lorsque les processus Probe Gateway (passerelle) et Probe Manager (gestionnaire) d'une sonde sont exécutés séparément, le composant du client Confidential Manager devient partie intégrante du processus de gestionnaire. Les informations d'identification sont mises en mémoire cache et utilisées uniquement par le gestionnaire. Pour accéder au serveur Confidential Manager sur le système UCMDB, la demande du client Confidential Manager est gérée par le processus de passerelle, avant d'être transmise au système UCMDB à partir de la passerelle.

Cette configuration est automatique lorsque la sonde est configurée en mode autonome.

Mise à jour permanente du cache des informations d'identification

Lors de sa première connexion avec le serveur Confidential Manager, le client Confidential Manager télécharge toutes les informations d'identification pertinentes (configurées dans le domaine de la sonde). Après la première communication réussie, le client Confidential Manager conserve une synchronisation constante avec le serveur Confidential Manager. Une synchronisation différentielle est effectuée à une minute d'intervalle, au cours de laquelle seules les différences entre le serveur Confidential Manager et le client Confidential Manager sont synchronisées. Si les informations d'identification sont modifiées côté serveur UCMDB (ajout de nouvelles informations ou mise à jour ou suppression des informations existantes), le client Confidential Manager reçoit immédiatement une notification de la part du serveur UCMDB et effectue une synchronisation supplémentaire.

Synchronisation de toutes les sondes avec les modifications de configuration

Pour que la communication soit performante, le client Confidential Manager doit être mis à jour avec la configuration de l'authentification du serveur Confidential Manager (chaîne d'initialisation LW-SSO) et la configuration du chiffrement (de la communication Confidential Manager). Par exemple, lorsque la chaîne d'initialisation est modifiée sur le serveur, la sonde doit connaître la nouvelle chaîne afin de l'authentifier.

Le serveur UCMDB surveille en permanence les modifications apportées à la configuration du chiffrement de la communication Confidential Manager et à la configuration de l'authentification Confidential Manager. Il effectue un contrôle toutes les 15 secondes et, en cas de modification, envoie la configuration mise à jour aux sondes. La configuration est transmise aux sondes sous une forme chiffrée, et elle stockée côté sonde dans un emplacement sécurisé. Le chiffrement de la configuration à envoyer est effectué à l'aide d'une clé de chiffrement symétrique. Par défaut, le serveur UCMDB et Data Flow Probe sont installés avec la même clé de chiffrement symétrique par défaut. Pour une sécurité optimale, il est vivement recommandé de modifier cette clé avant d'ajouter les informations d'identification au système. Pour plus d'informations, voir " Générer ou mettre à jour la clé de chiffrement " , page 63.

Remarque : En raison de l'intervalle de surveillance de 15 secondes, il est possible que le client Confidential Manager côté sonde ne puisse pas être mis à jour avec la dernière configuration pendant 15 secondes.

Si vous choisissez de désactiver la synchronisation automatique de la configuration de l'authentification et de la communication Confidential Manager entre le serveur UCMDB et Data Flow Probe, chaque fois que vous mettrez à jour la configuration de l'authentification et de la communication Confidential Manager côté serveur UCMDB, vous devrez également mettre à jour toutes les sondes avec la nouvelle configuration. Pour plus d'informations, voir " Désactiver la synchronisation automatique des paramètres de chiffrement et d'authentification du client Confidential Manager entre le serveur UCMDB et les sondes " , page 55.

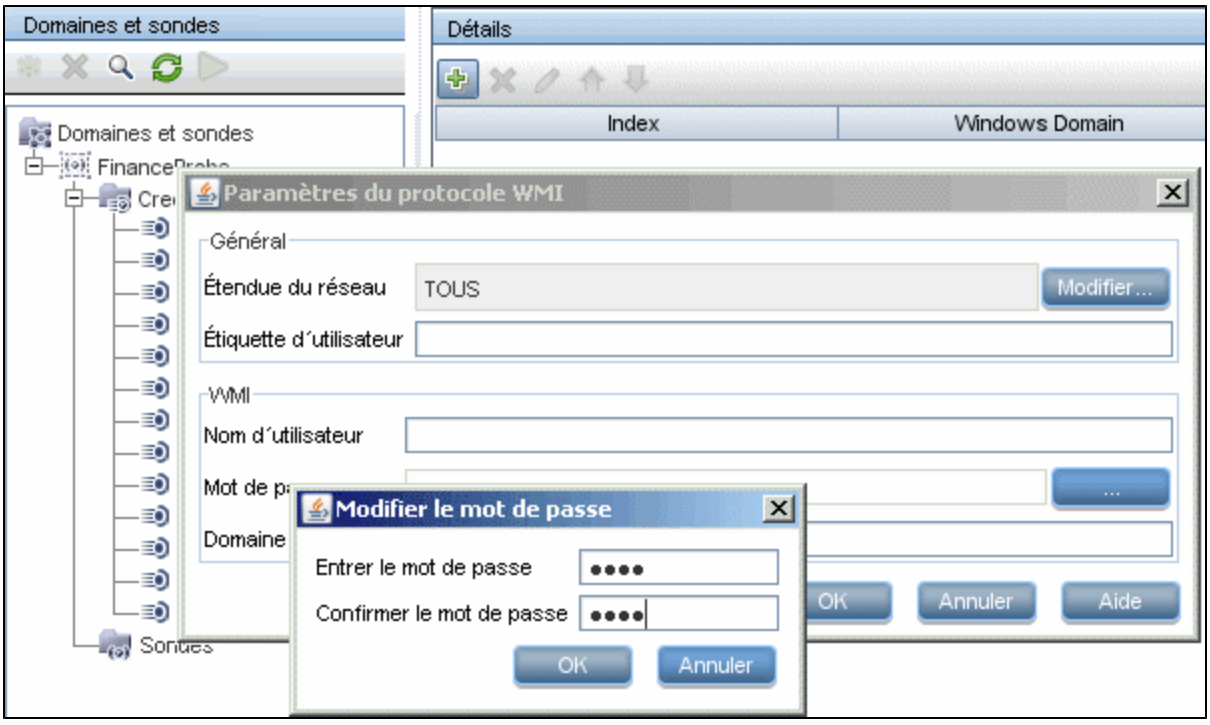
Stockage sécurisé dans la sonde

Toutes les informations sensibles (telles que la configuration de l'authentification et de la communication Confidential Manager et la clé de chiffrement) sont stockées dans un emplacement sécurisé de la sonde, à savoir dans le fichier **secured_storage.bin** qui se trouve dans **C:\hp\UCMDB\DataFlowProbe\conf\security**. Cet emplacement sécurisé est chiffré à l'aide de DPAPI reposant sur le mot de passe utilisateur Windows et le processus de chiffrement. DPAPI est une méthode standard permettant de protéger les données confidentielles telles que des certificats ou des clés privées sur les systèmes Windows. La sonde doit toujours être exécutée sous le même utilisateur Windows, afin qu'elle puisse à tout moment lire les informations stockées dans l'emplacement sécurisé en cas de modification du mot de passe.

Affichage des informations d'identification

Remarque : Cette section traite de l'affichage des informations d'identification lorsque le sens des données va de CMDB à HP Universal CMDB

Les mots de passe ne sont pas envoyés à l'application depuis la base de données CMDB. Autrement dit, HP Universal CMDB affiche des astérisques (*) dans le champ du mot de passe, quel que soit le contenu :



Mise à jour des informations d'identification

Remarque : Cette section traite de la mise à jour des informations d'identification lorsque le sens des données va de HP Universal CMDB à CMDB.

- Dans cette direction, la communication n'est pas chiffrée. Vous devez donc vous connecter au serveur UCMDB via une connexion https\SSL ou vous assurer que vous vous connectez à un réseau approuvé.

  Bien que la communication ne soit pas chiffrée, les mots de passe ne sont pas transmis en clair au réseau. Comme ils sont chiffrés à l'aide d'une clé par défaut, il est fortement recommandé d'utiliser une connexion SSL pour optimiser la fiabilité au cours du transit.

- Vous pouvez utiliser des caractères spéciaux et étendus pour les mots de passe.

Configurer les paramètres de chiffrement et d'authentification du client Confidential Manager

Cette tâche décrit la configuration des paramètres de chiffrement et d'authentification du client Confidential Manager sur le serveur UCMDB. Il couvre étapes suivantes :

- " Configurer les paramètres LW-SSO " , ci-dessous
- " Configurer le chiffrement de la communication Confidential Manager " , page suivante

Configurer les paramètres LW-SSO

Cette procédure explique comment modifier la chaîne d'initialisation LW-SSO sur le serveur UCMDB. La modification est envoyée automatiquement aux sondes (sous forme de chaîne chiffrée), à moins que le serveur UCMDB soit configuré de façon à ne pas la recevoir automatiquement. Pour plus d'informations, voir " Désactiver la synchronisation automatique des paramètres de chiffrement et d'authentification du client Confidential Manager entre le serveur UCMDB et les sondes " , page 55.

1. Sur le serveur UCMDB, lancez le navigateur Web et entrez l'adresse **http://localhost:8080/jmx-console**.
2. Cliquez sur **UCMDB-UI:name=LW-SSO Configuration** pour ouvrir la page JMX MBEAN View.
3. Recherchez la méthode **setInitString**.
4. Saisissez la nouvelle chaîne d'initialisation LW-SSO.
5. Cliquez sur Invoke.

Configurer le chiffrement de la communication Confidential Manager

Cette procédure explique comment modifier les paramètres de chiffrement de la communication Confidential Manager sur le serveur UCMDB. Ces paramètres définissent le chiffrement de la communication entre le client Confidential Manager et le serveur Confidential Manager. La modification est envoyée automatiquement aux sondes (sous forme de chaîne chiffrée), à moins que le serveur UCMDB soit configuré de façon à ne pas la recevoir automatiquement. Pour plus d'informations, voir " Désactiver la synchronisation automatique des paramètres de chiffrement et d'authentification du client Confidential Manager entre le serveur UCMDB et les sondes " , page suivante.

1. Sur le serveur UCMDB, lancez le navigateur Web et entrez l'adresse **http://localhost:8080/jmx-console.**
2. Cliquez sur **UCMDB:service=Security Services** pour ouvrir la page JMX MBEAN View.
3. Cliquez sur la méthode **CMGetConfiguration**.
4. Cliquez sur **Invoke**.

   Le XML de la configuration Confidential Manager en cours apparaît.
5. Copiez le contenu du XML affiché.
6. Revenez à la page **Security Services** JMX MBean View.
7. Cliquez sur la méthode **CMSetConfiguration**.
8. Collez le XML copié dans le champ **Value**.
9. Mettez à jour les paramètres appropriés liés au transport et cliquez sur **Invoke**.

   Exemple :

```
<transport>
      <encryptTransportMode>true</encryptTransportMode>
      <CMEncryptionDecryption>
            <encryptDecryptInitString>radiohead</encryptDecryptInitStrin
            g>
            <cryptoSource>lw</cryptoSource>
            <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
            <cipherType>symmetricBlockCipher</cipherType>
```

```
            <engineName>AES</engineName>
            <algorithmModeName>CBC</algorithmModeName>
            <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
            <keySize>256</keySize>
            <pbeCount>20</pbeCount>
            <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
            <encodingMode>Base64Url</encodingMode>
            <useMacWithCrypto>false</useMacWithCrypto>
            <macType>hmac</macType>
            <macKeySize>256</macKeySize>
            <macHashName>SHA256</macHashName>
      </CMEncryptionDecryption>
</transport>
```

Pour plus d'informations sur les valeurs qui peuvent être mises à jour, voir " Paramètres de chiffrement Confidential Manager " , page 67.

Configurer manuellement les paramètres de chiffrement et d'authentification du client Confidential Manager dans la sonde

Cette tâche comprend les étapes suivantes :

- " Désactiver la synchronisation automatique des paramètres de chiffrement et d'authentification du client Confidential Manager entre le serveur UCMDB et les sondes " , ci-dessous
- " Configurer les paramètres de chiffrement et d'authentification du client Confidential Manager dans la sonde " , page suivante
- " Configurer le chiffrement de la communication Confidential Manager dans la sonde " , page 57

Désactiver la synchronisation automatique des paramètres de chiffrement et d'authentification du client Confidential Manager entre le serveur UCMDB et les sondes

Par défaut, le serveur UCMDB est configuré pour envoyer automatiquement les paramètres Confidential Manager/LW-SSO à toutes les sondes. Ces informations sont envoyées sous forme de chaîne chiffrée aux sondes qui les déchiffrent lorsqu'elles les récupèrent. Vous pouvez configurer le serveur UCMDB de sorte qu'il n'envoie pas automatiquement les fichiers de configuration Confidential Manager/LW-SSO à toutes les sondes. Dans ce cas, il vous incombe de mettre à jour manuellement toutes les sondes avec les nouveaux paramètres Confidential Manager/LW-SSO.

Pour désactiver la synchronisation automatique des paramètres Confidential Manager/LW-SSO :

1. Dans UCMDB, cliquez sur **Administration > Gestionnaire des paramètres d'infrastructure> Paramètres généraux**.
2. Sélectionnez **Activer la synchronisation automatique de la configuration CM/LW-SSO et de la chaîne d'initialisation des sondes.**
3. Cliquez sur le champ **Valeur** et remplacez la valeur **True** par **False**.
4. Cliquez sur le bouton **Save**.
5. Redémarrez le serveur UCMDB .

Configurer les paramètres de chiffrement et d'authentification du client Confidential Manager dans la sonde

Cette procédure s'applique si le serveur UCMDB a été configuré pour ne pas envoyer automatiquement aux sondes les paramètres et la configuration LW-SSO/Confidential Manager. Pour plus d'informations, voir " Désactiver la synchronisation automatique des paramètres de chiffrement et d'authentification du client Confidential Manager entre le serveur UCMDB et les sondes " , page précédente.

1. À partir de l'ordinateur de la sonde, lancez le navigateur Web et entrez l'adresse : **http://localhost:1977**.

   Remarque : Si les processus Probe Manager (gestionnaire) et Probe Gateway (passerelle) de la sonde sont exécutés séparément, l'adresse doit être entrée comme suit sur l'ordinateur qui exécute le gestionnaire : **http://localhost:1978**.

2. Cliquez sur **type=CMClient** pour ouvrir la page JMX MBEAN View.
3. Recherchez la méthode **setLWSSOInitString** et saisissez la même chaîne d'initialisation que celle utilisée pour la configuration LW-SSO d'UCMDB.
4. Cliquez sur le bouton **setLWSSOInitString**.

Configurer le chiffrement de la communication Confidential Manager dans la sonde

Cette procédure s'applique si le serveur UCMDB a été configuré pour ne pas envoyer automatiquement aux sondes les paramètres et la configuration LW-SSO/Confidential Manager. Pour plus d'informations, voir " Désactiver la synchronisation automatique des paramètres de chiffrement et d'authentification du client Confidential Manager entre le serveur UCMDB et les sondes " , page 55.

1. À partir de l'ordinateur de la sonde, lancez le navigateur Web et entrez l'adresse : **http://localhost:1977**.

   Remarque : Si les processus Probe Manager (gestionnaire) et Probe Gateway (passerelle) de la sonde sont exécutés séparément, l'adresse doit être entrée comme suit sur l'ordinateur qui exécute le gestionnaire : **http://localhost:1978**.

2. Cliquez sur **type=CMClient** pour ouvrir la page JMX MBEAN View.
3. Mettez à jour les paramètres ci-après liés au transport.

   Remarque : Vous devez mettre à jour les mêmes paramètres que ceux actualisés sur le serveur UCMDB. Pour ce faire, certaines méthodes peuvent nécessiter la mise à jour de plusieurs paramètres dans la sonde. Pour afficher la configuration en cours de la sonde, cliquez sur **displayTransportConfiguration** dans la page JMX MBEAN View. Pour plus d'informations, voir " Configurer le chiffrement de la communication Confidential Manager " , page 54. Pour plus d'informations sur les valeurs pouvant être mises à jour, voir " Paramètres de chiffrement Confidential Manager " , page 67.

   a. **setTransportInitString** modifie le paramètre **encryptDecryptInitString**.

   b. **setTransportEncryptionAlgorithm** modifie les paramètres Confidential Manager de la sonde en fonction des correspondances suivantes :

      - **Engine name** se rapporte à l'entrée <engineName>
      - **Key size** se rapporte à l'entrée <keySize>
      - **Algorithm padding name** se rapporte à l'entrée <algorithmPaddingName>

- **PBE count** se rapporte à l'entrée <pbeCount>
- **PBE digest algorithm** se rapporte à l'entrée <pbeDigestAlgorithm>

c. **setTransportEncryptionLibrary** modifie les paramètres Confidential Manager de la sonde en fonction des correspondances suivantes :

- **Encryption Library name** se rapporte à l'entrée <cryptoSource>
- **Support previous lightweight cryptography versions** se rapporte à l'entrée <lwJCEPBECompatibilityMode>

d. **setTransportMacDetails** modifie les paramètres Confidential Manager de la sonde en fonction des correspondances suivantes :

- **Use MAC with cryptography** se rapporte à l'entrée <useMacWithCrypto>
- **MAC key size** se rapporte à l'entrée <macKeySize>

4. Cliquez sur le bouton **reloadTransportConfiguration** pour que les modifications soient prises en compte dans la sonde.

Pour plus d'informations sur les différents paramètres et leurs valeurs possibles, voir " Paramètres de chiffrement Confidential Manager " , page 67.

Configurer le cache du client Confidential Manager

Cette tâche comprend les étapes suivantes :

- " Configurer le mode cache du client Confidential Manager dans la sonde " , ci-dessous
- " Configurer les paramètres de chiffrement du cache du client Confidential Manager dans la sonde " , page suivante

Configurer le mode cache du client Confidential Manager dans la sonde

Le client Confidential Manager stocke les informations d'identification dans le cache et les met à jour lorsqu'elles sont modifiées sur le serveur. Le cache peut être stocké dans le système de fichiers ou en mémoire.

- **Lorsqu'il est stocké dans le système de fichiers**, les informations d'identification sont toujours disponibles même si la sonde ne parvient pas à se connecter au serveur en cas de redémarrage.
- **Lorsqu'il est stocké en mémoire**, son contenu est effacé et toutes les informations sont à nouveau extraites à partir du serveur en cas de redémarrage de la sonde. Si le serveur n'est pas

disponible, il est impossible d'exécuter une découverte ou une intégration car la sonde n'inclut aucune information d'identification.

Pour modifier ce paramètre :

1. Ouvrez le fichier **DataFlowProbe.properties** dans un éditeur de texte. Ce fichier se trouve dans le dossier **c:\hp\UCMDB\DataFlowProbe\conf**.
2. Recherchez l'attribut suivant :
com.hp.ucmdb.discovery.common.security.storeCMData=true
   - Pour stocker les informations dans le système de fichiers, conservez la valeur par défaut (**true**).
   - Pour les stocker en mémoire, entrez **false**.
3. Enregistrez le fichier **DataFlowProbe.properties** :
4. Redémarrez la sonde.

Configurer les paramètres de chiffrement du cache du client Confidential Manager dans la sonde

Cette procédure explique comment modifier les paramètres de chiffrement dans le fichier cache du système de fichiers du client Confidential Manager. Notez que la modification des paramètres de chiffrement du cache du système de fichiers du client Confidential Manager implique la création d'un fichier cache dans le système de fichiers. Ce processus requiert le redémarrage de la sonde et une synchronisation complète avec le serveur UCMDB.

1. À partir de l'ordinateur de la sonde, lancez le navigateur Web et entrez l'adresse : **http://localhost:1977**.

   Remarque : Si les processus Probe Manager (gestionnaire) et Probe Gateway (passerelle) de la sonde sont exécutés séparément, l'adresse doit être entrée comme suit sur l'ordinateur qui exécute le gestionnaire : **http://localhost:1978**.

2. Cliquez sur **type=CMClient** pour ouvrir la page JMX MBEAN View.
3. Mettez à jour les paramètres ci-après relatifs au cache.

   Remarque : Certaines méthodes peuvent nécessiter la mise à jour de plusieurs paramètres dans la sonde. Pour afficher la configuration en cours de la sonde, cliquez sur **displayCacheConfiguration** dans la page JMX MBEAN View.

a. **setCacheInitString** modifie le paramètre <encryptDecryptInitString> du cache du système de fichiers.

b. **setCacheEncryptionAlgorithm** modifie les paramètres du cache du système de fichiers en fonction des correspondances suivantes :

   - **Engine name** se rapporte à l'entrée <engineName>
   - **Key size** se rapporte à l'entrée <keySize>
   - **Algorithm padding name** se rapporte à l'entrée <algorithmPaddingName>
   - **PBE count** se rapporte à l'entrée <pbeCount>
   - **PBE digest algorithm** se rapporte à l'entrée <pbeDigestAlgorithm>

c. **setCacheEncryptionLibrary** modifie les paramètres du cache du système de fichiers en fonction des correspondances suivantes :

   - **Encryption Library name** se rapporte à l'entrée <cryptoSource>
   - **Support previous lightweight cryptography versions** se rapporte à l'entrée <lwJCEPBECompatibilityMode>

d. **setCacheMacDetails** modifie les paramètres du cache du système de fichier en fonction des correspondances suivantes :

   - **Use MAC with cryptography** se rapporte à l'entrée <useMacWithCrypto>
   - **MAC key size** se rapporte à l'entrée <macKeySize>

4. Cliquez sur le bouton **reloadCacheConfiguration** pour que les modifications soient prises en compte dans la sonde. Cette action entraîne le redémarrage de la sonde.

> **Remarque :** Vérifiez qu'aucun travail n'est en cours d'exécution dans la sonde.

Pour plus d'informations sur les différents paramètres et leurs valeurs possibles, voir " Paramètres de chiffrement Confidential Manager " , page 67.

Exporter et importer les informations de plage réseau et d'identification au format chiffré

Vous pouvez exporter et importer des informations de plage réseau et d'identification au format chiffré afin de pouvoir copier les informations d'identification d'un serveur UCMDB à l'autre. Par exemple, vous pouvez effectuer cette opération lors d'une récupération suite à un blocage du système ou lors d'une mise à niveau.

- **Pour exporter des informations d'identification,** vous devez entrer un mot de passe (de votre choix). Les informations sont chiffrées avec ce mot de passe.
- **Pour importer les informations d'identification,** vous devez utiliser le mot de passe qui a été défini lors de l'exportation du fichier DSD (domainScopeDocument).

Remarque : Le document d'informations d'identification exporté contient également les informations de plage réseau définies dans le système à partir duquel le document a été exporté. les informations de plage réseau sont importées avec le document des informations d'identification.

Pour exporter les informations d'identification du serveur UCMDB :

1. Sur le serveur UCMDB, lancez le navigateur Web et entrez l'adresse **http://localhost:8080/jmx-console**. Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.
2. Cliquez sur **UCMDB:service=DiscoveryManager** pour ouvrir la page JMX MBEAN View.
3. Recherchez l'opération **exportCredentialsAndRangesInformation**. Procédez comme suit :
   - Entrez votre ID client (la valeur par défaut est 1).
   - Entrez le nom du fichier exporté.
   - Entrez votre mot de passe.
   - Définissez **isEncrypted=True** pour chiffrer le fichier exporté avec le mot de passe fourni ou **isEncrypted=False** pour ne pas chiffrer le fichier exporté (dans ce cas, les mots de passe et autres informations sensibles ne seront pas exportés).
4. Cliquez sur **Invoke** pour exporter le fichier.

   Dès que le processus d'exportation a abouti, le fichier est enregistré à l'emplacement suivant : **c:\hp\UCMDB\UCMDBServer\conf\discovery\<rép_client>**.

Pour importer les informations d'identification du serveur UCMDB :

1. Sur le serveur UCMDB, lancez le navigateur Web et entrez l'adresse **http://localhost:8080/jmx-console**.

   Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

2. Cliquez sur **UCMDB:service=DiscoveryManager** pour ouvrir la page JMX MBEAN View.

3. Recherchez l'opération **importCredentialsAndRangesInformation**.

4. Entrez votre ID client (la valeur par défaut est 1).

5. Entrez le nom du fichier à importer. Ce fichier doit être placé dans **c:\hp\UCMDB\UCMDBServer\conf\discovery\<rép_client>**.

6. Entrez le mot de passe. Ce dernier doit être identique à celui qui a été utilisé lors de l'exportation du fichier.

7. Cliquez sur **Invoke** pour importer les informations d'identification.

Changer le niveau des messages des fichiers journaux du client Confidential Manager

Les deux fichiers journaux suivants disponibles dans la sonde contiennent des informations relatives à la communication Confidential Manager entre le serveur et le client Confidential Manager :

- " Fichier journal du client Confidential Manager " , ci-dessous
- " Fichier journal LW-SSO " , ci-dessous

Fichier journal du client Confidential Manager

Le fichier **security.cm.log** se trouve dans le dossier **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Ce journal contient des messages d'information échangés entre le serveur et le client Confidential Manager. Par défaut, le niveau de journal INFO est défini pour ces messages.

Pour définir le niveau de journal DEBUG :

1. Dans le serveur du Gestionnaire des sondes des flux de données, accédez au répertoire **c:\hp\UCMDB\DataFlowProbe\conf\log**.

2. Ouvrez le fichier **security.properties** dans un éditeur de texte.

3. Remplacez la ligne :

   ```
   loglevel.cm=INFO
   ```

par :

```
loglevel.cm=DEBUG
```

4. Enregistrez le fichier.

Fichier journal LW-SSO

Le fichier **security.lwsso.log** se trouve dans le dossier **c:\hp\UCMDB\DataFlowProbe\runtime\log**.

Ce journal contient des messages d'information relatives à LW-SSO. Par défaut, le niveau de journal INFO est défini pour ces messages.

Pour définir le niveau de journal DEBUG :

1. Dans le serveur du Gestionnaire des sondes des flux de données, accédez au répertoire **c:\hp\UCMDB\DataFlowProbe\conf\log**.
2. Ouvrez le fichier security.properties dans un éditeur de texte.
3. Remplacez la ligne :

   ```
   loglevel.lwsso=INFO
   ```

   par :

   ```
   loglevel.lwsso=DEBUG
   ```

4. Enregistrez le fichier.

Générer ou mettre à jour la clé de chiffrement

Vous pouvez générer ou mettre à jour une clé de chiffrement pour chiffrer ou déchiffrer les configurations de l'authentification et de la communication Confidential Manager échangées entre le serveur UCMDB et Data Flow Probe. Dans chaque cas (création ou mise à jour), le serveur UCMDB crée une clé de chiffrement sur la base des paramètres que vous fournissez (par exemple, longueur de clé, cycles PBE supplémentaires, fournisseur JCE) et la distribue aux sondes.

L'exécution de la méthode **generateEncryptionKey** génère une nouvelle clé de chiffrement. Cette clé est stockée uniquement dans un emplacement sécurisé, et son nom et ses informations ne sont pas connus. Si vous réinstallez une instance de Data Flow Probe existante ou que vous connectez une nouvelle sonde au serveur UCMDB, cette nouvelle clé générée n'est pas reconnue par la nouvelle sonde. Dans ce cas, il est préférable d'utiliser la méthode **changeEncryptionKey** pour modifier les clés de chiffrement. Ainsi, lorsque vous réinstallerez une sonde existante ou en installerez une nouvelle, vous pourrez importer la clé existante (dont vous connaissez le nom et l'emplacement) en exécutant la méthode **importEncryptionKey** dans la console JMX de la sonde.

Remarque :

- La méthode de création de clé (**generateEncryptionKey**) est différente de la méthode de mise à jour de clé (**changeEncryptionKey**), car **generateEncryptionKey** crée une nouvelle clé de chiffrement aléatoire alors que **changeEncryptionKey** importe une clé de chiffrement dont vous fournissez le nom.
- Un système ne peut contenir qu'une seule clé de chiffrement, quel que soit le nombre de sondes installées.

Cette tâche comprend les étapes suivantes :

- " Générer une nouvelle clé de chiffrement " , page suivante
- " Mettre à jour une clé de chiffrement sur un serveur UCMDB " , page 65
- " Mettre à jour une clé de chiffrement dans une sonde " , page 66
- " Modifier manuellement la clé de chiffrement lorsque le gestionnaire et la passerelle de la sonde sont installés sur des ordinateurs distincts " , page 67
- " Définir plusieurs fournisseurs JCE " , page 67

Générer une nouvelle clé de chiffrement

Vous pouvez générer une nouvelle clé pour le chiffrement ou le déchiffrement sur le serveur UCMDB et Data Flow Probe. Le serveur UCMDB remplace l'ancienne clé par la nouvelle et distribue celle-ci aux sondes.

Pour générer une nouvelle clé de chiffrement via la console JMX :

1. Sur le serveur UCMDB, lancez le navigateur Web et entrez l'adresse **http://localhost:8080/jmx-console**.

   Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

2. Cliquez sur **UCMDB:service=DiscoveryManager** pour ouvrir la page JMX MBEAN View.

3. Recherchez l'opération generateEncryptionKey.

   a. Dans le champ du paramètre **customerId**, entrez 1 (valeur par défaut).

   b. Pour **keySize**, indiquez la longueur de la clé de chiffrement. Valeurs autorisées : 128, 192 et 256.

   c. Pour **usePBE**, spécifiez **True** ou **False** :

      - **True :** utiliser des cycles de hachage PBE supplémentaires.
      - **False :** ne pas utiliser de cycles de hachage PBE supplémentaires.

d. Pour **jceVendor**, vous pouvez choisir d'utiliser un fournisseur JCE autre que celui par défaut. Si ce champ est vide, le fournisseur par défaut est utilisé.

e. Pour **autoUpdateProbe**, spécifiez **True** ou **False** :

- **True :** le serveur distribue automatiquement la nouvelle clé aux sondes.
- **False :** la nouvelle clé doit être placée manuellement dans les sondes.

f. Pour **exportEncryptionKey**, spécifiez **True** ou **False**.

- **True :** outre la création du nouveau mot de passe et son stockage dans un emplacement sécurisé, le serveur exporte le nouveau mot de passe vers le système de fichiers (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**). Cette option permet de mettre à jour les sondes manuellement avec le nouveau mot de passe.
- **False :** le nouveau mot de passe n'est pas exporté vers le système de fichiers. Pour mettre à jour les sondes manuellement, attribuez au paramètre **autoUpdateProbe** la valeur False, et au paramètre **exportEncryptionKey** la valeur True.

> **Remarque :** Vérifiez que la sonde est en service et connectée au serveur. Si la sonde s'arrête, la clé ne pourra pas atteindre la sonde. Si vous modifiez la clé avant l'arrêt de la sonde, la clé est à nouveau envoyée à la sonde dès le redémarrage de celle-ci. Cependant, si vous avez modifié plusieurs fois la clé avant l'arrêt de la sonde, vous devez modifier la clé manuellement par le biais de la console JMX (sélectionnez **False** pour **exportEncryptionKey**).

4. Cliquez sur **Invoke** pour générer la clé de chiffrement.

Mettre à jour une clé de chiffrement sur un serveur UCMDB

Utilisez la méthode **changeEncryptionKey** pour importer votre propre clé de chiffrement dans le serveur UCMDB et la distribuer à toutes les sondes.

Pour mettre à jour une clé de chiffrement par le biais de la console JMX :

1. Sur le serveur UCMDB, lancez le navigateur Web et entrez l'adresse **http://localhost:8080/jmx-console.**

   Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

2. Cliquez sur **UCMDB:service=DiscoveryManager** pour ouvrir la page JMX MBEAN View.

3. Recherchez l'opération **changeEncryptionKey**.

a. Dans le champ du paramètre **customerId**, entrez **1** (valeur par défaut).

b. Pour **newKeyFileName**, entrez le nom de la nouvelle clé.

c. Pour **keySizeInBits**, indiquez la longueur de la clé de chiffrement. Valeurs autorisées : 128, 192 et 256.

d. Pour **usePBE**, spécifiez **True** ou **False** :

- **True :** utilisez des cycles de hachage PBE supplémentaires.
- **False :** n'utilisez pas de cycles de hachage PBE supplémentaires.

e. Pour **jceVendor**, vous pouvez choisir d'utiliser un fournisseur JCE autre que celui par défaut. Si ce champ est vide, le fournisseur par défaut est utilisé.

f. Pour **autoUpdateProbe**, spécifiez **True** ou **False** :

- **True :** le serveur distribue automatiquement la nouvelle clé aux sondes.
- **False :** la nouvelle clé doit être distribuée manuellement par le biais de la console JMX de la sonde.

> **Remarque :** Vérifiez que la sonde est en service et connectée au serveur. Si la sonde s'arrête, la clé ne pourra pas atteindre la sonde. Si vous modifiez la clé avant l'arrêt de la sonde, la clé est à nouveau envoyée à la sonde dès le redémarrage de celle-ci. Cependant, si vous avez modifié plusieurs fois la clé avant l'arrêt de la sonde, vous devez modifier la clé manuellement par le biais de la console JMX (sélectionnez **False** pour **autoUpdateProbe**).

4. Cliquez sur **Invoke** pour générer et mettre à jour la clé de chiffrement.

Mettre à jour une clé de chiffrement dans une sonde

Si vous choisissez de ne pas distribuer automatiquement la clé de chiffrement à toutes les sondes à partir du serveur UCMDB (en raison de problèmes de sécurité), vous devez télécharger la nouvelle clé de chiffrement vers toutes les sondes et exécuter la méthode **importEncryptionKey** sur la sonde :

1. Placez la clé de chiffrement dans le répertoire **C:\hp\UCMDB\DataFlowProbe\conf\security**.

2. À partir de l'ordinateur de la sonde, lancez le navigateur Web et entrez l'adresse : **http://localhost:1977**.

   Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

> **Remarque :** Si les processus Probe Manager (gestionnaire) et Probe Gateway (passerelle) de la sonde sont exécutés séparément, l'adresse doit être entrée comme suit sur l'ordinateur qui exécute le gestionnaire : **http://localhost:1978**.

3. Dans le domaine de la sonde, cliquez sur **type=SecurityManagerService**.
4. Recherchez la méthode **importEncryptionKey**.
5. Entrez le nom du fichier de clé de chiffrement qui réside dans **C:\hp\UCMDB\DataFlowProbe\conf\security**. Ce fichier contient la clé à importer.
6. Cliquez sur le bouton **importEncryptionKey**.
7. Effectuez un redémarrage de la sonde.

Modifier manuellement la clé de chiffrement lorsque le gestionnaire et la passerelle de la sonde sont installés sur des ordinateurs distincts

1. À partir de l'ordinateur du gestionnaire, démarrez le service Probe Manager (**Démarrer > Programmes > HP UCMDB > Probe Manager**).
2. Importez la clé du serveur à l'aide de JMX Probe Manager. Pour plus d'informations, voir " Générer une nouvelle clé de chiffrement " , page 64.
3. Une fois la clé de chiffrement importée, redémarrez les services Probe Manager et Probe Gateway.

Définir plusieurs fournisseurs JCE

Lorsque vous générez une clé de chiffrement via la console JMX, vous pouvez définir plusieurs fournisseurs JCE à l'aide des méthodes **changeEncryptionKey** et **generateEncryptionKey**.

Pour changer le fournisseur JCE par défaut :

1. Enregistrez les fichiers jar du fournisseur JCE dans **$JRE_HOME/lib/ext**.
2. Copiez les fichiers jar dans le dossier $JRE_HOME :
   - Pour le serveur UCMDB : $JRE_HOME réside dans **c:\hp\UCMDB\UCMDBServer\bin\jre**
   - Pour Data Flow Probe : $JRE_HOME réside dans **c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. Ajoutez la classe du fournisseur à la fin de la liste des fournisseurs dans le fichier **$JRE_HOME\lib\security\java.security**.

4. Mettez à jour les fichiers **local_policy.jar** et **US_export_policy.jar** pour inclure les politiques JCE illimitées. Vous pouvez télécharger ces fichiers jar à partir du site Web de Sun.

5. Redémarrez le serveur UCMDB et Data Flow Probe.

6. Recherchez le champ du fournisseur JCE pour la méthode **changeEncryptionKey** ou **generateEncryptionKey** et ajoutez le nom du fournisseur JCE.

Paramètres de chiffrement Confidential Manager

Ce tableau répertorie les paramètres de chiffrement qui peuvent être modifiés à l'aide des différentes méthodes JMX. Ces paramètres s'appliquent au chiffrement des communications entre le client et le serveur Confidential Manager, ainsi qu'au chiffrement du cache du client Confidential Manager.

Nom du paramètre Confidential Manager	Nom du paramètre Confidential Manager de la sonde	Description du paramètre	Valeurs possibles	Valeur par défaut
cryptoSource	Encryption Library name	Ce paramètre définit la bibliothèque de chiffrement à utiliser.	lw, jce, windowsDPAPI, lwJCECompatible	lw
lwJCEPBE Compatibilité Mode	Support previous lightweight cryptography versions	Ce paramètre définit si le chiffrement léger précédent est pris en charge ou non.	true, false	true
engineName	Engine name	Nom du mécanisme de chiffrement	AES, DES, 3DES, Blowfish	AES
keySize	Key size	Longueur de la clé de chiffrement en octets	Pour AES : 128, 192 ou 256 ; Pour DES : 64 ; Pour 3DES : 192 ; Pour Blowfish : toute valeur comprise entre 32 et 448	256
algorithm Remplissage Nom	Algorithm padding name	Normes de remplissage	PKCS7Padding, PKCS5Padding	PKCS7Padding

Nom du paramètre Confidential Manager	Nom du paramètre Confidential Manager de la sonde	Description du paramètre	Valeurs possibles	Valeur par défaut
pbeCount	PBE count	Nombre de hachages à exécuter pour créer la clé à partir du mot de passe (chaîne d'initialisation)	Tout nombre positif	20
pbeDigest Algorithme	PBE digest algorithm	Type de hachage	SHA1, SHA256, MD5	SHA1
useMacWith Crypto	Use MAC with cryptography	Indique si l'algorithme MAC doit être utilisé avec le chiffrement	true, false	false
macKeySize	MAC key size	Dépend de l'algorithme MAC	256	256

Résolution des problèmes et limitations

Si vous changez le nom de domaine par défaut sur le serveur UCMDB, vous devez d'abord vérifier que Data Flow Probe n'est pas en cours d'exécution. Après avoir appliqué le nom de domaine par défaut, vous devez exécuter le script **DataFlowProbe\tools\clearProbeData.bat** côté Data Flow Probe.

Remarque : L'exécution du script clearProbeData.bat déclenche un cycle de découverte côté sonde lorsque celle-ci est opérationnelle.

Chapitre 5 : Sécurisation renforcée de Data Flow Probe

Contenu de ce chapitre :

Modifier le mot de passe chiffré de base de données PostgreSQL

Cette section explique comment modifier le mot de passe chiffré pour l'utilisateur de la base de données PostgreSQL.

1. Créer la forme chiffrée d'un mot de passe (AES, clé de 192 octets)

   a. Accédez à la console JMX de Data Flow Probe. Lancez un navigateur Web et entrez l'adresse suivante : **http://<nom ou adresse IP de l'ordinateur de Data Flow Probe>:1977**. Si vous exécutez Data Flow Probe localement, entrez **http://localhost:1977**.

Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

Remarque : Si vous n'avez pas créé d'utilisateur, connectez-vous à l'aide du nom d'utilisateur par défaut sysadmin et du mot de passe sysadmin.

b. Recherchez le service **Type=MainProbe** et cliquez sur le lien pour ouvrir la page Operations.

c. Recherchez l'opération **getEncryptedDBPassword**.

d. Dans le champ **DB Password**, entrez le mot de passe à crypter.

e. Appelez l'opération en cliquant sur le bouton **getEncryptedDBPassword**.

Vous obtenez une chaîne de mot de passe chiffrée, telle que la suivante :

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61
,61
```

2. Arrêter Data Flow Probe

Démarrer > Tous les programmes > HP UCMDB > Arrêter Data Flow Probe

3. Exécuter le script set_dbuser_password.cmd

Ce script se trouve dans le dossier **C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd**

Exécutez le script **set_dbuser_password.cmd** avec le nouveau mot de passe comme premier argument et le mot de passe du compte racine PostgreSQL comme deuxième argument.

Exemple :

set_dbuser_password <mon_mot_de_passe><mot_de_passe_racine>.

Le mot de passe doit être saisi dans sa forme non chiffrée (en clair).

4. Mettre à jour le mot de passe dans les fichiers de configuration de Data Flow Probe

a. Le mot de passe doit résider chiffré dans les fichiers de configuration. Pour récupérer la forme chiffrée du mot de passe, utilisez la méthode JMX **getEncryptedDBPassword**, comme indiqué à l'étape 1.

b. Ajoutez le mot de passe chiffré aux propriétés suivantes dans le fichier **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** :

- **appilog.agent.probe.jdbc.pwd**

  Exemple :

  ```
  appilog.agent.probe.jdbc.user = mamprobe
  appilog.agent.probe.jdbc.pwd =
  66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,
  61,61
  ```

- **appilog.agent.local.jdbc.pwd**
- **appilog.agent.normalization.jdbc.pwd**

5. Démarrer Data Flow Probe

   Démarrer > Tous les programmes > HP UCMDB > Démarrer Data Flow Probe

Script clearProbeData : utilisation

Pour recréer l'utilisateur de la base de données sans modifier son mot de passe actuel, exécutez le script **clearProbeData.bat** pour Windows ou le script **clearProbeData.sh** pour Linux.

Après avoir exécuté le script :

- Recherchez les erreurs éventuelles dans le fichier **C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log** pour, **/opt/hp/UCMDB/DataFlowProbe/runtime/log/probe_setup.log** pour Linux.
- Supprimez le fichier car il contient le mot de passe de base de données.

Remarque : Vous ne devez exécuter ce script que si vous y avez été invité par l'assistance HP Software .

Définir le mot de passe chiffré de la console JMX

Cette section explique comment chiffrer le mot de passe de l'utilisateur JMX. Le mot de passe chiffré est stocké dans le fichier DataFlowProbe.properties. Les utilisateurs doivent se connecter pour accéder à la console JMX.

1. ### Créer la forme chiffrée d'un mot de passe (AES, clé de 192 octets)

   a. Accédez à la console JMX de Data Flow Probe. Lancez un navigateur Web et entrez l'adresse suivante : **http://<nom ou adresse IP de l'ordinateur de Data Flow Probe>:1977**. Si vous exécutez Data Flow Probe localement, entrez **http://localhost:1977**.

   Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

> **Remarque :** Si vous n'avez pas créé d'utilisateur, connectez-vous à l'aide du nom d'utilisateur par défaut sysadmin et du mot de passe sysadmin.

b. Recherchez le service **Type=MainProbe** et cliquez sur le lien pour ouvrir la page Operations.

c. Recherchez l'opération **getEncryptedKeyPassword**.

d. Dans le champ **Key Password**, entrez le mot de passe à chiffrer.

e. Appelez l'opération en cliquant sur le bouton **getEncryptedKeyPassword**.

Vous obtenez une chaîne de mot de passe chiffrée, telle que la suivante :

```
85,-9,-61,11,105,-93,-81,118
```

2. Arrêter Data Flow Probe

Démarrer > Tous les programmes > HP UCMDB > Arrêter Data Flow Probe

3. Ajouter le mot de passe chiffré

Ajoutez le mot de passe chiffré à la propriété suivante dans le fichier **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** :

appilog.agent.Probe.JMX.BasicAuth.Pwd

Exemple :

```
appilog.agent.Probe.JMX.BasicAuth.User=sysadmin
appilog.agent.Probe.JMX.BasicAuth.Pwd=12,-35,-37,82,-2,20,57,-40,38,80,-111,-99,-64,-5,35,-122
```

> **Remarque :** Pour désactiver l'authentification, laissez ces champs vides. Les utilisateurs pourront ainsi accéder à la page principale de la console JMX de Data Flow Probe sans avoir à entrer d'authentification.

4. Démarrer Data Flow Probe

Démarrer > Tous les programmes > HP UCMDB > Démarrer Data Flow Probe

Testez le résultat dans un navigateur Web.

Définir le mot de passe de UpLoadScanFile

Cette section explique comment définir le mot de passe de **UpLoadScanFile** utilisé lors de l'enregistrement du balayage hors site. Le mot de passe chiffré est stocké dans le fichier **DataFlowProbe.properties**. Les utilisateurs doivent se connecter pour accéder à la console JMX.

1. **Créer la forme chiffrée d'un mot de passe (AES, clé de 192 octets)**

   a. Accédez à la console JMX de Data Flow Probe. Lancez un navigateur Web et entrez l'adresse suivante : **http://<nom ou adresse IP de l'ordinateur de Data Flow Probe>:1977**. Si vous exécutez Data Flow Probe localement, entrez **http://localhost:1977**.

   Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

   > **Remarque :** Si vous n'avez pas créé d'utilisateur, connectez-vous à l'aide du nom d'utilisateur par défaut sysadmin et du mot de passe sysadmin.

   b. Recherchez le service **Type=MainProbe** et cliquez sur le lien pour ouvrir la page Operations.

   c. Recherchez l'opération **getEncryptedKeyPassword**.

   d. Dans le champ **Key Password**, entrez le mot de passe à chiffrer.

   e. Appelez l'opération en cliquant sur le bouton **getEncryptedKeyPassword**.

   Vous obtenez une chaîne de mot de passe chiffrée, telle que la suivante :

   ```
   85,-9,-61,11,105,-93,-81,118
   ```

2. **Arrêter Data Flow Probe**

   Démarrer > Tous les programmes > HP UCMDB > Arrêter Data Flow Probe

3. **Ajouter le mot de passe chiffré**

   Ajoutez le mot de passe chiffré à la propriété suivante dans le fichier **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** :

   com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd

   Exemple :

   ```
   com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile
   com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,77,-
   108,14,127,4,-89,101,-33,-31,116,53
   ```

4. **Démarrer Data Flow Probe**

   Démarrer > Tous les programmes > HP UCMDB > Démarrer Data Flow Probe

   Testez le résultat dans un navigateur Web.

Accès distant au serveur PostgreSQL

Cette section explique comment autoriser/restreindre l'accès au compte PostgreSQL de Data Flow Probe à partir d'ordinateurs distants.

Remarque :

- Par défaut, l'accès est restreint.
- Vous ne pouvez pas accéder au compte racine PostgreSQL à partir d'ordinateurs distants.

Pour autoriser l'accès à PostgreSQL :

- Exécutez le script suivant dans une fenêtre d'invite de commandes :

  C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\enable_remote_user_access.cmd

Pour restreindre l'accès à PostgreSQL :

- Exécutez le script suivant dans une fenêtre d'invite de commandes :

  C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd

Activation de SSL entre le serveur UCMDB et Data Flow Probe

Vous pouvez configurer l'authentification pour la sonde et le serveur UCMDB à l'aide de certificats. Le certificat de chaque composant est envoyé et authentifié avant l'établissement de la connexion.

Remarque : La méthode d'activation de SSL sur Data Flow Probe décrite ci-après étant la plus sécurisée, elle constitue, par conséquent, le mode de communication recommandé. Elle remplace la procédure d'authentification de base.

Contenu de cette section :

Présentation

UCMDB prend en charge les modes de communication suivants entre le serveur UCMDB et Data Flow Probe :

- **Authentification du serveur.** Ce mode utilise SSL, et la sonde authentifie le certificat du serveur UCMDB. Pour plus d'informations, voir " Activer SSL avec l'authentification (à sens unique) du serveur " , ci-dessous.
- **Authentification mutuelle.** Ce mode utilise SSL et active l'authentification du serveur par la sonde et l'authentification du client par le serveur. Pour plus d'informations, voir " Activer l'authentification mutuelle (bidirectionnelle) de certificat " , page 79.
- **HTTP standard.** Pas de communication SSL. Il s'agit du mode par défaut. Le composant Data Flow Probe ne requiert aucun certificat. Il communique avec le serveur par le biais du protocole HTTP standard.

Remarque : L'utilisation du protocole SSL empêche le module de découverte de faire appel aux chaînes de certificats. Par conséquent, si vous utilisez des chaînes de certificats, il convient de générer un certificat auto-signé afin que Data Flow Probe puisse communiquer avec le serveur UCMDB.

Magasins de clés et d'approbations

Le serveur UCMDB et Data Flow Probe utilisent des magasins de clés et d'approbations.

- **Magasin de clés.** Fichier contenant des entrées de clé (un certificat et une clé privée correspondante).
- **Magasin d'approbations.** Fichier contenant des certificats qui permettent de vérifier un hôte distant (par exemple, lors de l'authentification du serveur, le magasin d'approbations de Data Flow Probe doit inclure le certificat du serveur UCMDB).

Limite de l'authentification mutuelle

Le magasin de clés de Data Flow Probe (défini dans le fichier **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**) doit contenir une (1) seule entrée clé.

Activer SSL avec l'authentification (à sens unique) du serveur

Ce mode utilise SSL, tandis que la sonde authentifie le certificat du serveur.

Contenu de cette tâche :

- " Conditions préalables " , ci-dessous
- " Configuration du serveur UCMDB " , ci-dessous
- " Configuration de Data Flow Probe " , page suivante
- " Redémarrer les ordinateurs " , page 79

Conditions préalables

1. Vérifiez que le module UCMDB et la sonde sont actifs.

   Remarque : Si la sonde est installée en mode autonome, ces instructions se rapportent à la passerelle (composant Probe Gateway).

2. Si la base UCMDB ou la sonde ne sont pas installées dans les dossiers par défaut, notez l'emplacement correspondant et modifiez les commandes en conséquence.

Configuration du serveur UCMDB

1. **Exportez le certificat UCMDB.**

   a. À partir de l'invite de commande, exécutez la commande suivante :

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <alias du keystore> -keystore <chemin du fichier keystore> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   où :

   - **alias du keystore** est le nom attribué au magasin de clés.
   - **chemin du fichier keystore** est le chemin d'accès complet au fichier du magasin de clés.

   Par exemple, pour accéder au magasin de clés server.keystore prédéfini, exécutez la commande suivante :

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. Entrez le mot de passe du magasin de clés (keystore). Par exemple, le mot de passe prédéfini est **hppass**.

   c. Vérifiez que le certificat a été créé dans le répertoire suivant : **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Renforcez la sécurisation du connecteur de la sonde dans UCMDB.**

   a. Accédez à la console JMX de UCMDB. Dans votre navigateur Web, entrez l'URL suivante : **http://<nom ou adresse IP de l'ordinateur UCMDB>:8080/jmx-console**. Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

   b. Sélectionnez le service : **Ports Management Services**.

   c. Appelez la méthode **PortsDetails** et notez le numéro de port pour HTTPS. (Valeur par défaut : 8443) Vérifiez que la valeur de la colonne **Is Enabled** est **True**.

   d. Revenez à **Ports Management Services**.

   e. Pour mapper le connecteur de la sonde au mode d'authentification du serveur, appelez la méthode **mapComponentToConnectors** avec les paramètres suivants :

      - **componentName** : mam-collectors
      - **isHTTPS** : true
      - **Tous les autres indicateurs** : false

      Le message suivant apparaît :

      Operation succeeded. Component mam-collectors is now mapped to: HTTPS ports.

   f. Revenez à **Ports Management Services**.

   g. Pour mapper le connecteur Confidential Manager sur le mode d'authentification du serveur, appelez la méthode **mapComponentToConnectors** avec les paramètres suivants :

      - **componentName** : cm
      - **isHTTPS** : true
      - **Tous les autres indicateurs** : false

      Le message suivant apparaît :

      Operation succeeded. Component cm is now mapped to: HTTPS ports.

3. **Copiez le certificat UCMDB sur chaque ordinateur sonde.**

   Copiez le fichier de certificat **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** de l'ordinateur du serveur UCMDB dans le dossier suivant de chaque ordinateur sonde : **C:\HP\UCMDB\DataFlowProbe\conf\security**

Configuration de Data Flow Probe

Remarque : Vous devez configurer chaque ordinateur sonde.

1. **Importez le fichier server.cert que vous avez créé lors de la procédure** " Exportez le certificat UCMDB. " , page 77**, dans le magasin d'approbations de la sonde.**

   a. À partir de l'invite de commande, exécutez la commande suivante :

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:
   \HP\UCMDB\DataFlowProbe\conf\security\hpprobeTrustStore.jks -file C:\HP\U
   CMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
   ```

   b. Entrez le mot de passe du magasin de clés : logomania

   c. Lorsque le message **Trust this certificate?** apparaît, appuyez sur **y** puis sur **Entrée**.

   Le message suivant apparaît :

   Certificate was added to keystore.

2. **Ouvrez le fichier DataFlowProbe.properties sous : C:\HP\UCMDB\DataFlowProbe\conf**

   a. Mettez à jour la propriété **appilog.agent.probe.protocol** en entrant **HTTPS**.

   b. Mettez à jour la propriété **serverPortHttps** en entrant le numéro de port approprié. (Utilisez le numéro de port issu de l'étape 2c " Configuration du serveur UCMDB " , page 77.)

Redémarrer les ordinateurs

Redémarrez le serveur UCMDB et les ordinateurs sonde.

Activer l'authentification mutuelle (bidirectionnelle) de certificat

Ce mode utilise SSL et active l'authentification du serveur par la sonde et l'authentification du client par le serveur. Le serveur et la sonde envoient leurs certificats à l'autre entité pour authentification.

Contenu de cette tâche :

Conditions préalables

1. Vérifiez que UCMDB et Data Flow Probe sont actifs.

   Remarque : Si la sonde est installée en mode autonome, ces instructions se rapportent à la passerelle (composant Probe Gateway).

2. Si UCMDB ou Data Flow Probe ne sont pas installés dans les dossiers par défaut, notez l'emplacement correspondant et modifiez les commandes en conséquence.

Configuration initiale du serveur UCMDB

1. **Exportez le certificat UCMDB.**

   a. À partir de l'invite de commande, exécutez la commande suivante :

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <alias du keystore> -keystore <chemin du fichier keystore> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   où :

   - **alias du keystore** est le nom attribué au magasin de clés.
   - **chemin du fichier keystore** est le chemin d'accès complet au fichier du magasin de clés.

   Par exemple, pour accéder au magasin de clés server.keystore prédéfini, exécutez la commande suivante :

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. Entrez le mot de passe du magasin de clés (keystore). Par exemple, le mot de passe prédéfini est **hppass**.

   c. Vérifiez que le certificat a été créé dans le répertoire suivant : **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **Renforcez la sécurisation du connecteur de Data Flow Probe dans UCMDB.**

   a. Accédez à la console JMX d'UCMDB. Dans votre navigateur Web, entrez l'URL suivante : **http://<nom ou adresse IP de l'ordinateur UCMDB>:8080/jmx-console**. Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

   b. Sélectionnez le service : **Ports Management Services**.

c. Appelez la méthode **PortsDetails** et notez le numéro de port pour HTTPS avec l'authentification client. (Valeur par défaut : 8444) Vérifiez que la valeur de la colonne **Is Enabled** est **True**.

d. Revenez à **Ports Management Services**.

e. Pour mapper le connecteur de Data Flow Probe sur le mode d'authentification mutuelle, appelez la méthode **mapComponentToConnectors** avec les paramètres suivants :

- **componentName** : mam-collectors
- **isHTTPSWithClientAuth** : true
- **Tous les autres indicateurs** : false

Le message suivant apparaît :

Operation succeeded. Component mam-collectors is now mapped to: HTTPS_ CLIENT_AUTH ports.

f. Revenez à **Ports Management Services**.

g. Pour mapper le connecteur Confidential Manager au mode d'authentification mutuelle, appelez la méthode **mapComponentToConnectors** avec les paramètres suivants :

- **componentName** : cm
- **isHTTPSWithClientAuth** : true
- **Tous les autres indicateurs** : false

Le message suivant apparaît :

Operation succeeded. Component cm is now mapped to: HTTPS_CLIENT_AUTH ports.

3. **Copiez le certificat UCMDB sur chaque ordinateur sonde.**

Copiez le fichier de certificat **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** de l'ordinateur du serveur UCMDB dans le dossier suivant de chaque ordinateur de Data Flow Probe : **C:\HP\UCMDB\DataFlowProbe\conf\security**

Configuration de Data Flow Probe

Remarque : Vous devez configurer chaque ordinateur de Data Flow Probe.

1. **Importez le fichier server.cert que vous avez créé lors de la procédure** " Exportez le certificat UCMDB. " , page 80**, dans le magasin d'approbations de la sonde.**

   a. À partir de l'invite de commande, exécutez la commande suivante :

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:
   \HP\UCMDB\DataFlowProbe\conf\security\hpprobeTrustStore.jks -file C:\HP\U
   CMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
   ```

   b. Entrez le mot de passe du magasin de clés : logomania

   c. Lorsque le message **Trust this certificate?** apparaît, appuyez sur **y** puis sur **Entrée**.

   Le message suivant apparaît :

   Certificate was added to keystore.

2. **Créez un fichier client.keystore**

   a. À partir de l'invite de commande, exécutez la commande suivante :

   ```
   c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool –genkey –alias <NomSonde> -keya
   lg RSA –sigalg SHA256withRSA –keysize 2048 –keystore c:\HP\UCMDB\DataFlow
   Probe\conf\security\client.keystore
   ```

   où **NomSonde** est l'alias unique de Data Flow Probe.

   > **Remarque :** Pour s'assurer de l'unicité de l'alias, utilisez l'identificateur qui a été attribué à la sonde au moment de sa définition.

   b. Entrez le mot de passe du magasin de clés comprenant au moins six caractères et notez-le.

   c. Confirmez le mot de passe.

   d. Appuyez sur **Entrée** en réponse à chacune des questions suivantes :

   What is your first and last name? [Unknown]:

   What is the name of your organizational unit?[Unknown]:

   What is the name of your organization?[Unknown]:

   What is the name of your City or Locality?[Unknown]:

   What is the name of your State or Province?[Unknown]:

   What is the two-letter country code for this unit?[Unknown]:

e. Tapez **yes** en réponse à la question **Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?**

f. Appuyez sur **Entrée** en réponse à la question suivante :

Enter key password for <clé de sonde> (RETURN if same as keystore password):

g. Vérifiez que le fichier a été créé dans le dossier suivant et que sa taille est supérieure à 0 : **C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

3. **Exportez le nouveau certificat client.**

a. À partir de l'invite de commande, exécutez la commande suivante :

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias <NomSond
e> -keystore C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -fil
e C:\hp\UCMDB\DataFlowProbe\conf\security\<NomSonde>.cert
```

b. Lorsque vous y êtes invité, entrez le mot de passe du magasin de clés. (Il s'agit du mot de passe noté à l'étape 2b plus haut.)

Le message suivant apparaît :

Certificate stored in file <C:\hp\UCMDB\DataFlowProbe\conf\security\<NomSonde>.cert>

4. **Ouvrez le fichier DataFlowProbe.properties sous : C:\HP\UCMDB\DataFlowProbe\conf**

a. Mettez à jour la propriété **appilog.agent.probe.protocol** en entrant **HTTPS**.

b. Mettez à jour la propriété **serverPortHttps** en entrant le numéro de port approprié. (Utilisez le numéro de port issu de l'étape 2c " Configuration initiale du serveur UCMDB " , page 80.)

5. **Ouvrez le fichier ssl.properties sous : C:\HP\UCMDB\DataFlowProbe\conf\security**

a. Mettez à jour la propriété **javax.net.ssl.keyStore** sur **client.keystore**.

b. Chiffrez le mot de passe noté à l'étape 2b plus haut.

i. Démarrez Data Flow Probe (ou vérifiez que ce composant est déjà actif).

ii. Accédez au JMX de la sonde : allez à : **http://<nom d'hôte_sonde>:1977**

Par exemple, si vous exécutez la sonde en local, rendez-vous sur : **http://localhost:1977**.

iii. Sélectionnez le lien **type=MainProbe**.

iv. Recherchez l'opération **getEncryptedKeyPassword** en faisant défiler la liste vers le bas.

v. Entrez le mot de passe dans le champ **Key Password**.

vi. Sélectionnez le bouton **EnregetEncryptedKeyPassword**.

c. Copiez et collez les mot de passe chiffré afin de mettre à jour la propriété **javax.net.ssl.keyStorePassword**.

> **Remarque :** Les chiffres sont séparés par une virgule. Par exemple : -20,50,34,-40,-50.)

6. **Copiez le certificat de la sonde sur chaque ordinateur UCMDB.**

Copiez le fichier **C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert** depuis l'ordinateur de Data Flow Probe vers l'ordinateur UCMDB sous **C:\HP\UCMDB\UCMDBServer\conf\security\<NomSonde>.cert**.

Configuration du serveur UCMDB

1. **Ajoutez chaque certificat de sonde au magasin d'approbations d'UCMDB.**

> **Remarque :** Vous devez effectuer les opérations suivantes pour chaque certificat de sonde.

a. À partir de l'invite de commande, exécutez la commande suivante :

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore C:\hp
\UCMDB\UCMDBServer\conf\security\server.truststore -file C:\hp\UCMDB\UCMDB
Server\conf\security\<NomSonde>.cert -alias <NomSonde>
```

b. Entrez le mot de passe du magasin de clés. Par exemple, le mot de passe prédéfini est **hppass**.

c. Lorsque le message **Trust this certificate?** apparaît, appuyez sur **y** puis sur **Entrée**.

Le message suivant apparaît :

Certificate was added to keystore.

Redémarrer les ordinateurs

Redémarrez le serveur UCMDB et les ordinateurs sonde.

Contrôler l'emplacement du fichier domainScopeDocument

Le système de fichiers de la sonde contient (par défaut) la clé de chiffrement et le fichier **domainScopeDocument**. À chaque démarrage, la sonde extrait le fichier **domainScopeDocument** du serveur et le stocke dans son système de fichiers. Pour empêcher les utilisateurs non autorisés d'accéder à ces informations d'identification, vous pouvez configurer la sonde de façon à conserver le fichier **domainScopeDocument** dans la mémoire de la sonde, et non dans son système de fichiers.

Pour contrôler l'emplacement du fichier domainScopeDocument :

1. Ouvrez **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** et remplacez la ligne :

   ```
   appilog.collectors.storeDomainScopeDocument=true
   ```

   par :

   ```
   appilog.collectors.storeDomainScopeDocument=false
   ```

   Les dossiers serverData des composants Probe Gateway (passerelle) et Probe Manager (gestionnaire) ne contiennent plus le fichier **domainScopeDocument**.

   Pour plus d'informations sur l'utilisation du fichier **domainScopeDocument** afin de renforcer la sécurisation de la Gestion des flux de données (GFD), voir " Gestion des informations d'identification des flux de données " , page 48.

2. Redémarrez la sonde.

Créer un magasin de clés pour Data Flow Probe

1. À partir de l'ordinateur de la sonde, exécutez la commande suivante :

   ```
   c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool –genkey –alias <NomSonde> -keyalg
   RSA –sigalg SHA256withRSA –keysize 2048 –keystore c:\HP\UCMDB\DataFlowProbe\
   conf\security\client.keystore
   ```

2. Entrez un mot de passe pour le nouveau magasin de clés.

3. Entrez vos informations lorsque vous y êtes invité.

4. Lorsque le message **Is CN=… C=… Correct?** apparaît, entrez **yes** et appuyez sur **Entrée**.

5. Appuyez à nouveau sur **Entrée** pour accepter le mot de passe du magasin de clés comme mot de passe principal.

6. Vérifiez que **client.keystore** a été créé dans le répertoire **C:\HP\UCMDB\DataFlowProbe\conf\security**.

Chiffrer les mots de passe des magasins de clés et d'approbations de la sonde

Les mots de passe des magasins de clés et d'approbations sont enregistrés chiffrés sous **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**. Cette procédure explique comment chiffrer le mot de passe.

1. Démarrez Data Flow Probe (ou vérifiez qu'elle est toujours active).
2. Accédez à la console JMX de Data Flow Probe. Lancez un navigateur Web et entrez l'adresse suivante : http://<nom ou adresse IP de l'ordinateur de Data Flow Probe>:1977. Si vous exécutez Data Flow Probe localement, entrez http://localhost:1977.

   Remarque : Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe. Si vous n'avez pas créé d'utilisateur, connectez-vous à l'aide du nom d'utilisateur par défaut sysadmin et du mot de passe par défaut sysadmin.
3. Recherchez le service **Type=MainProbe** et cliquez sur le lien pour ouvrir la page Operations.
4. Recherchez l'opération **getEncryptedKeyPassword**.
5. Entrez votre mot de passe de magasin de clés ou d'approbations dans le champ **Key Password** et appelez l'opération en cliquant sur **getEncryptedKeyPassword**.
6. Vous obtenez une chaîne de mot de passe chiffrée, telle que la suivante :

   ```
   66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
   ```
7. Copiez et collez le mot de passe chiffré dans la ligne relative au magasin de clés ou d'approbations dans le fichier suivant : **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties.**

Magasins de clés et d'approbations par défaut de Data Flow Probe

Contenu de cette section :

Serveur UCMDB

Les fichiers se trouvent dans le répertoire **C:\HP\UCMDB\UCMDBServer\conf\security.**

Entité	Nom du fichier/Terme	Mot de passe/Terme	Alias
Magasin de clés du serveur	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
Magasin d'approbations du serveur	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	hpcert (entrée approuvée par défaut)
Magasin de clés du client	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow Probe

Les fichiers se trouvent dans le répertoire **C:\HP\UCMDB\DataFlowProbe\conf\security.**

Entité	Nom du fichier/Terme	Mot de passe/Terme	Alias
Magasin de clés de la sonde	hpprobeKeyStore.jks (pKeyStoreFile)	logomania (pKeyStorePass)	hpprobe
Data Flow Probe utilise par défaut le magasin de clés **cKeyStoreFile** lors de la procédure d'authentification mutuelle. Il s'agit d'un magasin de clés client qui fait partie de l'installation d'UCMDB.			
Magasin d'approbations de la sonde	hpprobeTrustStore.jks (pTrustStoreFile)	logomania (pTrustStorePass)	hpprobe (entrée approuvée par défaut)
cKeyStorePass est le mot de passe par défaut de **cKeyStoreFile**.			

Chapitre 6 : Authentification de signature unique (Lightweight Single Sign-On, LW-SSO) – Références générales

Contenu de ce chapitre :

Authentification LW-SSO - Présentation

LW-SSO est une méthode de contrôle d'accès qui permet à un utilisateur d'établir une seule connexion aux ressources de plusieurs systèmes logiciels sans avoir à se reconnecter par la suite. Les applications figurant dans le groupe configuré de systèmes logiciels tiennent compte de cette authentification. Il n'est donc pas nécessaire de procéder à une autre authentification lorsque vous passez d'une application à une autre.

Les informations de cette section s'applique à LW-SSO versions 2.2 et 2.3.

- **Délai d'expiration du jeton LW-SSO**

  La valeur du délai d'expiration du jeton LW-SSO détermine la validité de la session de l'application. Par conséquent, la valeur de son délai d'expiration doit être au moins identique à celle de la session de l'application.

- **Configuration recommandée pour le délai d'expiration du jeton LW-SSO**

  Chaque application qui utilise LW-SSO doit configurer le délai d'expiration du jeton. La valeur recommandée est 60 minutes. Pour une application ne requérant pas un haut niveau de sécurité, il est possible de configurer une valeur de 300 minutes.

- **Heure GMT**

  Toutes les applications impliquées dans une intégration LW-SSO doivent utiliser la même heure GMT avec une différence maximum de 15 minutes.

- **Fonctionnalité multidomaine**

La fonctionnalité multidomaine implique que toutes les applications qui participent à l'intégration LW-SSO configurent les paramètres trustedHosts (ou les paramètres **protectedDomains**) s'ils sont requis pour s'intégrer dans des applications de différents domaines DNS. De plus, ils doivent également ajouter le domaine approprié dans l'élément **lwsso** de la configuration.

- **Obtenir un SecurityToken pour la fonctionnalité URL**

  Pour recevoir des informations envoyées sous la forme d'un **SecurityToken pour URL** en provenance d'autres applications, l'application hôte doit configurer le domaine approprié dans l'élément **lwsso** de la configuration.

Configuration système LW-SSO

Application	Version	Commentaires
Java	1.5 et versions ultérieures	
API HTTP Servlets	2.1 et versions ultérieures	
Internet Explorer	6.0 et versions ultérieures	Le navigateur doit activer le cookie de session HTTP et la fonction de redirection HTTP 302
Firefox	2.0 et versions ultérieures	Le navigateur doit activer le cookie de session HTTP et la fonction de redirection HTTP 302
Authentifications JBoss	JBoss 4.0.3 JBoss 4.3.0	
Authentifications Tomcat	Tomcat 5.0.28 autonome Tomcat 5.5.20 autonome	
Authentifications Acegi	Acegi 0.9.0 Acegi 1.0.4	
Moteurs de services Web	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

Avertissements de sécurité LW-SSO

Cette section présente les avertissements de sécurité relatifs à la configuration LW-SSO :

- **Paramètre confidentiel InitString dans LW-SSO.**LW-SSO utilise une méthode de chiffrement symétrique (Symmetric Encryption) pour valider et créer un jeton LW-SSO. Le paramètre **initString** de la configuration sert à l'initialisation de la clé secrète. Une application crée un jeton et chaque application partageant le même paramètre initString valide le jeton.

  Attention :

  - Il n'est pas possible d'utiliser LW-SSO sans définir le paramètre **initString**.
  - Le paramètre **initString** contient des informations confidentielles et doit être traité comme tel en termes de publication, de transport et de persistance.
  - Le paramètre **initString** doit être partagé uniquement entre des applications mutuellement intégrées à l'aide de LW-SSO.
  - Le paramètre **initString** doit contenir au minimum 12 caractères.

- **Activer LW-SSO uniquement en cas de besoin.**LW-SSO doit être désactivé sauf spécification contraire.

- **Niveau de sécurité d'authentification.** L'application qui utilise l'infrastructure d'authentification la plus faible et émet un jeton LW-SSO devant être approuvé par d'autres applications intégrées détermine le niveau de sécurité d'authentification de toutes les applications.

  Seules les applications qui utilisent des infrastructures d'authentification fortes et sécurisées émettent un jeton LW-SSO.

- **Implications du chiffrement symétrique.**LW-SSO utilise le chiffrement symétrique pour émettre et valider des jetons LW-SSO. Par conséquent, toute application qui utilise LW-SSO peut émettre un jeton devant être approuvé par toutes les autres applications qui partagent le même paramètre initString. Ce risque potentiel est pertinent lorsqu'une application qui partage un paramètre initString, réside ou est accessible depuis un emplacement non fiable.

- **Mappage des utilisateurs (synchronisation).**L'infrastructure LW-SSO n'assure pas le mappage des utilisateurs entre les applications intégrées. Par conséquent, l'application intégrée doit contrôler le mappage des utilisateurs. Nous vous recommandons de partager le même registre utilisateur (comme LDAP/AD) entre toutes les applications intégrées.

  L'échec du mappage des utilisateurs peut provoquer des violations de sécurité et un comportement négatif des applications. Par exemple, le même nom d'utilisateur peut être attribué à différents utilisateurs réels dans les différentes applications.

  De plus, lorsqu'un utilisateur se connecte à une application (AppA) et accède ensuite à une seconde application (AppB) qui utilise l'authentification de conteneur ou d'application, l'échec du mappage de l'utilisateur peut forcer l'utilisateur à se connecter manuellement à AppB et à entrer un nom d'utilisateur. Si l'utilisateur entre un autre nom que celui utilisé pour la connexion à AppA,

le comportement suivant peut se produire : si l'utilisateur accède ensuite à une troisième application (AppC) à partir d'AppA ou d'AppB, il y accède en utilisant les noms d'utilisateur spécifiés pour la connexion à AppA ou AppB respectivement.

- **Gestionnaire des identités**. Utilisé pour l'authentification, toutes les ressources non protégées du Gestionnaire des identités doivent être configurées à l'aide du paramètre **nonsecureURLs** du fichier de configuration LW-SSO.
- **Mode démonstration de LW-SSO.**
  - Ce mode ne doit être utilisé qu'à des fins de démonstration.
  - Il ne doit être utilisé que dans des réseaux non sécurisés.
  - Il ne doit pas être utilisé en production. Toute combinaison du mode démonstration avec le mode production ne doit pas être utilisée.

Résolution des problèmes et limitations

Cette section décrit les problèmes et les limitations connus lors de l'utilisation de l'authentification LW-SSO.

Problèmes connus

Cette section décrit les problèmes connus en matière d'authentification LW-SSO.

- **Contexte de la sécurité.**Le contexte de la sécurité LW-SSO ne prend en charge qu'une valeur d'attribut par nom d'attribut.

  Par conséquent, lorsque le jeton SAML2 envoie plusieurs valeurs pour le même nom d'attribut, une seule valeur est acceptée par l'infrastructure LW-SSO.

  De même, si le jeton IdM est configuré pour envoyer plusieurs valeurs pour le même nom d'attribut, une seule valeur est acceptée par l'infrastructure LW-SSO.

- **Fonctionnalité de déconnexion multidomaine dans Internet Explorer 7.** La fonctionnalité de déconnexion multidomaine peut échouer dans les conditions suivantes :
  - Le navigateur utilisé est Internet Explorer 7 et l'application appelle plus de trois verbes de redirection HTTP 302 consécutifs dans la procédure de déconnexion.

  Dans ce cas, Internet Explorer 7 risque de ne pas interpréter correctement la réponse de redirection HTTP 302 et afficher une page d'erreur **Internet Explorer ne peut pas afficher la page Web**.

  Pour contourner le problème, il est recommandé, si possible, de réduire le nombre de commandes de redirection de l'application dans la séquence de déconnexion.

Limitations

Notez les limitations suivantes lors de l'authentification LW-SSO :

- **Accès client à l'application.**

  Si un domaine est défini dans la configuration LW-SSO :

  - Les clients de l'application doivent accéder à l'application à l'aide d'un nom de domaine complet (FQDN) dans l'URL de connexion, par exemple, http://monserveur.**domaineentreprise**.com/AppWeb.
  - LW-SSO ne peut pas prendre en charge les URL contenant une adresse IP, par exemple, http://192.168.12.13/WebApp.
  - LW-SSO ne peut pas prendre en charge les URL ne contenant pas de domaine, http://monserveur/AppWeb.

  Si un domaine n'est pas défini dans la configuration LW-SSO : Le client peut accéder à l'application sans nom complet de domaine dans l'URL de connexion. Dans ce cas, un cookie de session LW-SSO est créé spécifiquement pour un seul ordinateur sans informations de domaine. Par conséquent, le cookie n'est pas délégué par le navigateur à un autre navigateur, et ne transmet pas aux autres ordinateurs situés dans le même domaine DNS. Cela signifie que LW-SSO ne fonctionne pas dans le même domaine.

- **Intégration de l'infrastructure LW-SSO.**Les applications peuvent influencer et utiliser les fonctionnalités LW-SSO uniquement si elles sont pré-intégrées dans l'infrastructure LW-SSO.

- **Prise en charge multidomaine.**

  - La fonctionnalité multidomaine repose sur un référent HTTP. Par conséquent, LW-SSO prend en charge les liens d'une application vers une autre et non pas la saisie d'une URL dans une fenêtre de navigateur, sauf si les applications partagent le même domaine.
  - Le premier lien croisé de domaine qui utilise **HTTP POST** n'est pas pris en charge.

    La fonctionnalité multidomaine ne prend pas en charge la première demande **HTTP POST** d'une seconde application (seule la demande **HTTP GET** est prise en charge). Par exemple, si votre application comporte un lien HTTP vers une seconde application, une demande **HTTP GET** est prise en charge, mais une demande **HTTP FORM** ne l'est pas. Toutes les demandes émises après la première peuvent être **HTTP POST** ou **HTTP GET.**
  - Taille du jeton LW-SSO :

    Le volume des informations que LW-SSO peut transférer d'une application d'un domaine vers une autre application d'un autre domaine est limité à 15 Groupes/Rôles/Attributs (notez que chaque élément peut contenir en moyenne 15 caractères).

- Liaison d'une page protégée (HTTPS) à une page non protégée (HTTP) dans une configuration multidomaine :

  La fonctionnalité multidomaine ne fonctionne pas pour la liaison d'une page protégée (HTTPS) à une page non protégée (HTTP). Il s'agit d'une limitation du navigateur où l'en-tête du référent n'est pas envoyé lors de la liaison à partir d'une ressource protégée à une ressource non protégée. Pour un exemple, voir : `http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP`

- Comportement des cookies tiers dans Internet Explorer :

  Microsoft Internet Explorer 6 contient un module qui prend en charge le "projet Platform for Privacy Preferences (P3P)", ce qui signifie que les cookies provenant d'un domaine tiers sont bloqués par défaut dans la zone de sécurité Internet. Les cookies de session sont également considérés comme des cookies tiers par IE et sont, par conséquent, bloqués, ce qui provoque l'arrêt de LW-SSO. Pour plus d'informations, voir . `http://support.microsoft.com/kb/323752/fr-fr`.

  Pour résoudre ce problème, ajoutez l'application lancée (ou un sous-ensemble de domaines DNS comme *.mondomaine.com) à l'intranet ou à la zone de confiance de votre ordinateur (dans Microsoft Internet Explorer, sélectionnez **Menu > Outils > Options Internet > Sécurité > Intranet local > Sites > Avancé**). Les cookies seront ainsi acceptés.

  Attention : Le cookie de session LW-SSO est le seul utilisé par l'application tierce bloquée.

- **Jeton SAML2**

  - La fonctionnalité de déconnexion n'est pas prise en charge lorsque le jeton SAML2 est utilisé.

    Par conséquent, si le jeton SAML2 est utilisé pour accéder à une seconde application, un utilisateur qui se déconnecte de la première application ne l'est pas de la seconde.

  - **Le délai d'expiration du jeton SAML2 n'est pas reflété dans la gestion de session de l'application.**

    Par conséquent, si le jeton SAML2 est utilisé pour accéder à une seconde application, la gestion de chaque session de l'application est traitée de manière indépendante.

- **Domaine JAAS.**Le domaine JAAS de Tomcat n'est pas pris en charge.

- **Utilisation d'espaces dans les répertoires Tomcat.**L'utilisation d'espaces dans les répertoires Tomcat n'est pas prise en charge.

  Il n'est pas possible d'utiliser LW-SSO lorsqu'un chemin d'installation Tomcat (dossiers) inclut des espaces (par exemple, Program Files) et que le fichier de configuration LW-SSO est situé dans le dossier Tomcat **common\classes**.

- **Configuration du processus d'équilibrage de la charge.**Un répartiteur de charge déployé avec LW-SSO doit être configuré pour utiliser des sessions permanentes.
- **Mode démonstration.** Dans ce mode, LW-SSO prend en charge les liens d'une application vers une autre, mais pas la saisie d'une URL dans une fenêtre de navigateur en raison de l'absence d'un en-tête de référent HTTP dans ce cas.

Chapitre 7 : Authentification de la connexion HP Universal CMDB

Contenu de ce chapitre :

Configuration d'une méthode d'authentification

Vous pouvez utiliser les méthodes d'authentification suivantes :

- **Au niveau du service HP Universal CMDB interne.**
- **Via le protocole LDAP (Lightweight Directory Access Protocol).** Vous pouvez utiliser un serveur LDAP externe dédié pour stocker les informations d'authentification, au lieu d'utiliser le service HP Universal CMDB interne. Le serveur LDAP doit résider sur le même sous-réseau que celui de tous les serveurs HP Universal CMDB.

  Pour plus d'informations sur LDAP, voir la section relative au mappage LDAP dans le *Manuel d'administration HP Universal CMDB*.

  La méthode d'authentification par défaut utilise le service HP Universal CMDB interne. Si vous utilisez la méthode par défaut, vous n'avez aucune modification à effectuer dans le système.

  Ces options s'appliquent aux connexions établies via les services Web ou l'interface utilisateur.

- **Via LW-SSO.** HP Universal CMDB est configuré avec l'authentification LW-SSO. LW-SSO permet de vous connecter à HP Universal CMDB et d'accéder automatiquement aux autres applications configurées qui sont exécutées dans le même domaine, sans avoir besoin de vous connecter à ces applications.

  Lorsque la prise en charge de l'authentification LW-SSO est activée (elle est désactivée par défaut), vérifiez que l'authentification LW-SSO est également activée pour les autres applications de l'environnement SSO (Single Sign-On) et que celles-ci utilisent le même paramètre initString.

Activation de la connexion à HP Universal CMDB via LW-SSO

Pour activer LW-SSO pour HP Universal CMDB, procédez de l'une des façons suivantes :

1. Accédez à la console JMX en entrant l'adresse suivante dans votre navigateur Web : **http://<nom_serveur>:8080/jmx-console**, où **<nom_serveur>** est le nom de l'ordinateur sur lequel HP Universal CMDB est installé.
2. Sous **UCMDB-UI**, cliquez sur **name=LW-SSO Configuration** pour ouvrir la page Operations.
3. Définissez la chaîne d'initialisation à l'aide de la méthode **setInitString**.
4. Définissez le nom de domaine de l'ordinateur sur lequel UCMDB est installé à l'aide de la méthode **setDomain**.
5. Appelez la méthode **setEnabledForUI** en attribuant la valeur **True** au paramètre.
6. **Facultatif**. Pour utiliser la fonctionnalité multidomaine, sélectionnez la méthode **addTrustedDomains**, entrez les valeurs de domaine et cliquez sur **Invoke**.
7. **Facultatif.** Pour utiliser un proxy inverse, sélectionnez la méthode **updateReverseProxy**, attribuez la valeur **True** au paramètre **Is reverse proxy enabled**, entrez une URL pour le paramètre **Reverse proxy full server URL**, puis cliquez sur Invoke. Pour accéder à UCMDB directement et à l'aide d'un proxy inverse, définissez la configuration supplémentaire suivante : sélectionnez la méthode **setReverseProxyIPs**, entrez l'adresse IP au paramètre Reverse proxy ip/s, puis cliquez sur **Invoke.**
8. **Facultatif**. Pour accéder à UCMDB à l'aide d'un point d'authentification externe, sélectionnez la méthode **setValidationPointHandlerEnable**, attribuez la valeur **True** au paramètre **Is validation point handler enabled**, entrez l'URL du point d'authentification dans le paramètre **Authentication point server**, puis cliquez sur **Invoke.**
9. Pour afficher la configuration LW-SSO telle qu'elle a été enregistrée dans le mécanisme des paramètres, sélectionnez la méthode **retrieveConfigurationFromSettings**.
10. Pour afficher la configuration LW-SSO réelle chargée, appelez la méthode **retrieveConfiguration**.

Remarque : Vous ne pouvez pas activer LW-SOO à partir de l'interface utilisateur.

Définition d'une connexion sécurisée avec le protocole SSL (Secure Sockets Layer)

Comme le processus de connexion implique la transmission des informations confidentielles entre HP Universal CMDB et le serveur LDAP, vous pouvez appliquer un certain niveau de sécurité au contenu. Pour ce faire, vous activez la communication SSL sur le serveur LDAP et vous configurez HP Universal CMDB de façon à l'utiliser avec SSL.

HP Universal CMDB prend en charge le protocole SSL qui utilise un certificat émis par une autorité de certification (CA) approuvée.

La plupart des serveurs LDAP, notamment Active Directory, peuvent exposer un port sécurisé pour une connexion SSL. Si vous utilisez Active Directory avec une autorité de certification privée, vous devez ajouter celle-ci aux autres autorités de certification dans le JRE.

Pour plus d'informations sur la configuration de la plate-forme HP Universal CMDB afin qu'elle prenne en charge la communication avec SSL, voir " Activation de la communication SSL (Secure Sockets Layer) " , page 18.

Pour ajouter une autorité de certification aux autorités de certification approuvées afin d'exposer un port sécurisé pour une connexion SSL :

1. Exportez un formulaire de certificat de votre autorité de certification dans la machine virtuelle Java (JVM) utilisée par HP Universal CMDB en procédant comme suit :

   a. À partir de l'ordinateur du serveur UCMDB, accédez au dossier **UCMDBServer\bin\JRE\bin**.

   b. Exécutez la commande suivante :

   ```
   Keytool -import -file <votre fichier de certificat> -keystore C:\hp\UCMDB
   \UCMDBServer\bin\JRE\lib\security\cacerts
   ```

   Par exemple :

   ```
   Keytool -import -file c:\ca2ss_ie.cer -keystore C:\hp\UCMDB\UCMDBServer\b
   in\JRE\lib\security\cacerts
   ```

2. Sélectionnez la catégorie **Administration > Gestionnaire des paramètres d'infrastructure > LDAP - Général**.

   Remarque : Il est également possible de configurer ces paramètres à l'aide de la console JMX. Pour plus d'informations, voir " Activation et définition de la méthode d'authentification LDAP à l'aide de la console JMX " , page 101.

3. Recherchez le paramètre **URL du serveur LDAP** et entrez une valeur dans le format suivant :

   ```
   ldaps://<hôteLDAP>[:<port>]/[<baseDN>][??étendue]
   ```

Par exemple :

```
ldaps://my.ldap.server:389/ou=People,o=myOrg.com??sub
```

Notez le **s** dans **ldaps**.

4. Cliquez sur **Enregistrer** pour enregistrer la nouvelle valeur ou sur le bouton **Restaurer les valeurs par défaut** pour remplacer l'entrée par la valeur par défaut (URL vide).

Utilisation de la console JMX pour tester les connexions LDAP

Cette section décrit une méthode permettant de tester la configuration de l'authentification LDAP à l'aide de la console JMX.

1. Lancez votre navigateur Web et entrez l'adresse suivante : **http://<nom_serveur>:8080/jmx-console**, où **<nom_serveur>** est le nom de l'ordinateur sur lequel HP Universal CMDB est installé.

   Si vous y êtes invité, entrez un nom d'utilisateur et un mot de passe pour vous connecter.

2. Sous **UCMDB**, cliquez sur **UCMDB:service=LDAP services** pour ouvrir la page JMX MBEAN View.

3. Recherchez **testLDAPConnection.**

4. Dans la zone **Value** du paramètre **customer id**, entrez l'ID du client.

5. Cliquez sur **Invoke.**

   La page JMX MBEAN Operation Result indique si la connexion LDAP a été établie. Si tel est le cas, la page indique également les groupes racine LDAP.

Activation et définition de la méthode d'authentification LDAP

Vous pouvez activer et définir la méthode d'authentification LDAP pour un système HP Universal CMDB.

Remarque :

- Vous pouvez également configurer les paramètres d'authentification LDAP à l'aide de la console JMX. Pour plus d'informations, voir " Activation et définition de la méthode d'authentification LDAP à l'aide de la console JMX " , page 101.

- Pour la description d'un exemple de paramètres d'authentification LDAP, voir " Paramètres d'authentification LDAP - Exemple " , page 102.

Pour activer et définir la méthode d'authentification LDAP dans l'interface utilisateur de UCMDB :

1. Sélectionnez la catégorie **Administration > Gestionnaire des paramètres d'infrastructure > LDAP - Général**.
2. Sélectionnez **URL du serveur LDAP** et entrez la valeur de cette URL dans le format suivant :

   ```
   ldap://<hôteLDAP>[:<port>]/[<baseDN>][??étendue]
   ```

   Par exemple :

   ```
   ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
   ```

3. Sélectionnez la catégorie **Définition de groupe LDAP**, puis entrez le nom unique du groupe général pour le paramètre **DN de base des groupes**.
4. Recherchez le paramètre **DN de base des groupes racine** et entrez le nom unique du groupe racine.
5. Sélectionnez la catégorie **LDAP - Général**, recherchez le paramètre **Activer la synchronisation des autorisations** et vérifiez que sa valeur est **True.**
6. Sélectionnez la catégorie **Authentification générale LDAP**, recherchez le paramètre **Mot de passe de l'utilisateur autorisé à effectuer des recherches** et entrez le mot de passe.
7. Sélectionnez la catégorie **Options LDAP pour les classes et les attributs**, recherchez **Objet de classe groupe**, puis renseignez le nom de classe d'objet (**group** pour Microsoft Active Directory et **groupOfUniqueNames** pour Oracle Directory Server).
8. Accédez à **Attribut Membres du groupe** et renseignez le nom de l'attribut (**member** pour Microsoft Active Directory et **uniqueMember** pour Oracle Directory Server).
9. Accédez à **Classe d'objet utilisateurs** et renseignez le nom de la classe d'objet (**user** pour Microsoft Active Directory et **inetOrgPerson** pour Oracle Directory Server).
10. Accédez à **Attribut UUID** et spécifiez l'attribut d'identification unique d'un utilisateur dans le serveur d'annuaire. Veillez à ce que l'attribut sélectionné soit unique dans le serveur d'annuaire. Par exemple, lors de l'utilisation de SunOne/Oracle Directory Server, l'attribut UID n'est pas unique. Dans ce cas, il convient d'utiliser soit l'attribut d'adresse e-mail, soit le nom unique. En effet, l'utilisation d'un attribut non unique comme attribut d'identification unique dans la base UCMDB risque d'altérer le fonctionnement lors de la connexion.

11. Enregistrez les nouvelles valeurs. Pour remplacer une entrée par la valeur par défaut, cliquez sur le bouton **Restaurer les valeurs par défaut**.

12. Si le paramètre d'infrastructure **Respect de la casse activé lors de l'authentification LDAP** sous **LDAP - Général** a la valeur **Vrai**, l'authentification respecte la casse.

    Attention : Lorsque la valeur du paramètre d'infrastructure est modifiée, il incombe à l'administrateur UCMDB de supprimer manuellement tous les utilisateurs externes.

13. Mappez les groupes d'utilisateurs LDAP aux groupes d'utilisateurs UCMDB. Pour plus d'informations, voir " Authentification de la connexion HP Universal CMDB " , page 96.

14. Pour définir un ensemble par défaut d'autorisations dans un groupe LDAP dépourvu de mappage de groupes, sélectionnez la catégorie **LDAP - Général**, accédez à **Groupe d'utilisateurs affecté automatiquement**, puis entrez le nom du groupe.

15. **Important :** Si vous configurez LDAP dans un environnement haute disponibilité, vous devez redémarrer le cluster afin que vos modifications soient prises en compte.

Remarque : Chaque utilisateur LDAP est enregistré avec un prénom, un nom et une adresse e-mail dans le référentiel local. Si la valeur d'un de ces paramètres stockés dans le serveur LDAP est différente de celle enregistrée dans le référentiel local, la valeur du serveur LDAP remplace la valeur locale à chaque connexion.

Activation et définition de la méthode d'authentification LDAP à l'aide de la console JMX

Cette tâche explique comment configurer les paramètres d'authentification LDAP à l'aide de la console JMX.

Remarque :

- Dans un environnement haute disponibilité, veillez à vous connecter à la console JMX du serveur rédacteur.
- Vous pouvez également configurer les paramètres d'authentification LDAP dans UCMDB. Pour plus d'informations, voir " Activation et définition de la méthode d'authentification LDAP " , page 99.
- Pour la description d'un exemple de paramètres d'authentification LDAP, voir " Paramètres d'authentification LDAP - Exemple " , page suivante.

Pour configurer les paramètres d'authentification LDAP :

1. Lancez votre navigateur Web et entrez l'adresse suivante : **http://<nom_serveur>:8080/jmx-console**, où **<nom_serveur>** est le nom de l'ordinateur sur lequel HP Universal CMDB est installé.

   Si vous y êtes invité, entrez un nom d'utilisateur et un mot de passe pour vous connecter.

2. Sous **UCMDB**, cliquez sur **UCMDB:service=LDAP services** pour ouvrir la page JMX MBEAN View.

3. Pour afficher les paramètres d'authentification LDAP en cours, recherchez la méthode **getLDAPSettings**. Cliquez sur **Invoke**. Un tableau contenant tous les paramètres LDAP et leurs valeurs apparaît.

4. Pour modifier les valeurs des paramètres d'authentification LDAP, recherchez la méthode **configureLDAP**. Entrez les valeurs des paramètres à modifier et cliquez sur **Invoke**. La page JMX MBEAN Operation Result indique si les paramètres d'authentification LDAP ont été mis à jour.

   Remarque : Si vous n'entrez aucune valeur pour un paramètre, sa valeur en cours est conservée.

5. Après avoir configuré les paramètres LDAP, vous pouvez vérifier les informations d'identification LDAP :

   a. Recherchez la méthode **verifyLDAPCredentials**.

   b. Entrez l'ID du client, le nom d'utilisateur et le mot de passe.

   c. Cliquez sur **Invoke**.

      La page JMX MBEAN Operation Result indique si l'utilisateur a réussi l'authentification LDAP.

6. **Important :** Si vous configurez LDAP dans un environnement haute disponibilité, vous devez redémarrer le cluster afin que vos modifications soient prises en compte.

Remarque : Chaque utilisateur LDAP est enregistré avec un prénom, un nom et une adresse e-mail dans le référentiel local. Si la valeur d'un de ces paramètres stockés dans le serveur LDAP est différente de celle enregistrée dans le référentiel local, la valeur du serveur LDAP remplace la valeur locale à chaque connexion.

Paramètres d'authentification LDAP - Exemple

Le tableau suivant contient un exemple de définition de valeurs pour l'authentification LDAP :

Paramètre	Valeur
Classe d'objet utilisateurs	user
Respect de la casse activé lors de l´authentification LDAP	false
Attribut Membres du groupe	member
Résolution de nom distingué (DN)	true
Filtre de recherche de groupes racine	(objectCategory=group)
Chaîne de connexion LDAP	ldap://myldap.example.com:389/OU=Users,OU=Dept,OU=US,DC=example,DC=com??sub
Utilisateur de recherche LDAP	CN=John Doe,OU=Users,OU=Dept,OU=US,DC=example,DC=com
Objet de classe groupe	group
Utiliser l'algorithme ascendant pour trouver les groupes parents depuis le serveur LDAP.	true
Attribut UUID	sAMAccountName
Attribut Nom du groupe	cn
Filtre de base de groupe	(objectclass=group)
Filtre utilisateurs	(&(sAMAccountName=*)(objectclass=user))
Nombre de tentatives de recherche	3
Attribut Nom affiché du groupe	cn
Portée de la recherche de groupes racine	sub
Attribut Nom affiché de l'utilisateur	cn
Portée de la recherche de groupe	sub
Activer l'authentification LDAP	false
Activer la synchronisation LDAP	true
Groupe racine	OU=Users,OU=Security Groups,DC=example,DC=com
Base du groupe	OU=AMRND,OU=Security Groups,DC=example,DC=com

Paramètre	Valeur
Groupe par défaut	AdminsGroup
Attribut Description du groupe	description

Récupération de la configuration LW-SSO en cours dans un environnement distribué

Lorsque le module UCMDB est incorporé dans un environnement distribué, par exemple dans un déploiement BSM, procédez comme suit pour récupérer la configuration LW-SSO en cours sur l'ordinateur de traitement.

Pour récupérer la configuration LW-SSO en cours :

1. Lancez un navigateur Web et entrez l'adresse suivante : `http://localhost.<nom_domaine>:8080/jmx-console.`

   Si vous y êtes invité, entrez un nom d'utilisateur et un mot de passe.

2. Recherchez **UCMDB:service=Security Services** et cliquez sur le lien pour accéder à la page Operations.

3. Recherchez l'opération **retrieveLWSSOConfiguration**.

4. Cliquez sur **Invoke** pour récupérer la configuration.

Chapitre 8 : Confidential Manager

Contenu de ce chapitre :

Confidential Manager - Présentation

L'infrastructure Confidential Manager (CM) résout le problème de gestion et de distribution des données sensibles pour HP Universal CMDB et les autres produits HP Software.

Confidential Manager se compose de deux composants : le client et le serveur. Ces deux composants sont chargés de transférer les données de façon sécurisée.

- Le client Confidential Manager est une bibliothèque utilisée par les applications pour accéder aux données sensibles.
- Le serveur Confidential Manager reçoit les demandes des clients Confidential Manager ou de clients tiers et exécute les tâches demandées. De plus, il est chargé d'enregistrer les données de façon sécurisée.

Confidential Manager chiffre les informations d'identification au cours de leur transport, dans le cache du client, à l'état de persistance et en mémoire. Confidential Manager utilise le chiffrement symétrique pour transporter les informations d'identification entre le client et le serveur Confidential Manager à l'aide d'un secret partagé. Confidential Manager utilise divers secrets pour le chiffrement du cache, des données persistantes et du transport en fonction de la configuration.

Pour plus d'informations sur la gestion du chiffrement des informations d'identification dans Data Flow Probe, voir " Gestion des informations d'identification des flux de données " , page 48.

Considérations sur la sécurité

- Vous pouvez utiliser les tailles de clé suivantes pour l'algorithme de sécurité : 128, 192 et 256 bits. L'algorithme est exécuté plus rapidement avec la clé la plus petite mais il est moins sécurisant. La taille de 128 bits assure une sécurité suffisante dans la plupart des cas.
- Pour améliorer la sécurité du système, attribuez au paramètre MAC **useMacWithCrypto** la valeur **true.** Pour plus d'informations, voir " Propriétés de chiffrement " , page 108.
- Pour tirer parti des fournisseurs de sécurité renforcée, vous pouvez utiliser le mode JCE.

Configurer le serveur HP Universal CMDB

Lorsque vous utilisez HP Universal CMDB, vous devez configurer le secret et les crypto-propriétés du chiffrement à l'aide des méthodes JMX suivantes :

1. À partir de l'ordinateur du serveur HP Universal CMDB, lancez le navigateur Web et entrez comme suit l'adresse du serveur : **http://<nom d'hôte ou adresse IP du serveur UCMDB>:8080/jmx-console.**

   Vous devrez peut-être vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe.

2. Sous UCMDB, cliquez sur **UCMDB:service=Security Services** pour ouvrir la page Operations.

3. Pour récupérer la configuration en cours, recherchez l'opération **CMGetConfiguration**.

   Cliquez sur **Invoke** pour afficher le fichier XML de configuration du serveur Confidential Manager.

4. Pour modifier la configuration, copiez le XML que vous avez appelé à l'étape précédente dans un éditeur de texte. Effectuez vos modifications en fonction du tableau de la section " Propriétés de chiffrement " , page 108.

   Recherchez l'opération **CMSetConfiguration**. Copiez la configuration mise à jour dans la zone **Value** et cliquez sur **Invoke.** La nouvelle configuration est écrite dans le serveur UCMDB.

5. Pour ajouter des utilisateurs à CM à des fins d'autorisation et de réplication, recherchez l'opération **CMAddUser**. Ce processus est également utile dans le processus de réplication. Dans une réplication, le serveur esclave doit communiquer avec le serveur maître à l'aide d'un utilisateur privilégié.

   - **username**. Nom d'utilisateur.
   - **customer.** La valeur par défaut est ALL_CUSTOMERS.
   - **resource.** Nom de ressource. La valeur par défaut est ROOT_FOLDER.
   - **permission.** Valeurs disponibles : ALL_PERMISSIONS, CREATE, READ, UPDATE et DELETE. La valeur par défaut est ALL_PERMISSIONS.

   Cliquez sur **Invoke**.

6. Si nécessaire, redémarrez HP Universal CMDB.

   Dans la plupart des cas, il inutile de redémarrer le serveur. Néanmoins, la modification de l'une des ressources suivantes peut nécessiter le redémarrage du serveur :

- Type de stockage
- Nom de table de base de données ou noms de colonne
- Initiateur de la connexion à la base de données
- Propriétés de connexion à la base de données (URL, utilisateur, mot de passe, nom de classe de pilote)
- Type de base de données

Remarque :

- Il est important que le serveur UCMDB et ses clients possèdent les mêmes crypto-propriétés de transport. Si ces propriétés ont été modifiées sur le serveur UCMDB, vous devez les modifier sur tous les clients. (Cela ne s'applique pas au composant Data Flow Probe, car il est exécuté dans le même processus que le serveur UCMDB. La crypto-configuration du transport est donc inutile dans ce cas.)
- La réplication de Confidential Manager n'est pas configurée par défaut, mais il est possible de la configurer, si nécessaire.
- Si la réplication de Confidential Manager est activée et que la propriété **initString** du transport ou toute autre crypto-propriété maître est modifiée, toutes les propriétés esclaves doivent également l'être.

Définitions

Crypto-propriétés de stockage. Configuration définissant la conservation et le chiffrement des données par le serveur (base de données ou fichier, crypto-propriétés à utiliser pour chiffrer et déchiffrer les données, etc.), le stockage sécurisé des informations d'identification, ainsi que le mode de traitement du chiffrement selon la configuration utilisée.

Crypto-propriétés de transport. La configuration du transport définit le chiffrement du transport entre le serveur et les clients, la configuration utilisée, le transfert sécurisé des informations d'identification, ainsi que le mode de traitement du chiffrement selon la configuration utilisée. Vous devez utiliser les mêmes crypto-propriétés pour le chiffrement et le déchiffrement du transport et pour le serveur et le client.

Réplications crypto-propriétés de réplication. Les données sécurisées conservées par Confidential Manager sont répliquées de façon sécurisée entre les serveurs. Ces propriétés définissent le mode de transfert des données entre le serveur esclave et le serveur maître.

Remarque :

- La configuration du serveur Confidential Manager est conservée dans la table de base de données **CM_CONFIGURATION.**

- Le fichier de configuration par défaut du serveur Confidential Manager se trouve dans app-infra.jar sous le nom **defaultCMServerConfig.xml.**

Propriétés de chiffrement

Le tableau ci-après répertorie les propriétés de chiffrement. Pour plus d'informations sur l'utilisation de ces paramètres, voir " Configurer le serveur HP Universal CMDB " , page 106.

Paramètre	Description	Valeur recommandée
encryptTransportMode	Chiffre les données transportées : true, false	true
encryptDecrypt InitString	Mot de passe du chiffrement	8 caractères minimum
cryptoSource	Bibliothèque d'implémentation de chiffrement à utiliser : • lw • jce • windowsDPAPI • lwJCECompatible	lw
lwJCEPBE CompatibilityMode	Prend en charge les versions précédentes de chiffrement léger : • true • false	true
cipherType	Type de chiffrement utilisé par Confidential Manager. Confidential Manager prend en charge une seule valeur : **symmetricBlockCipher**	symmetricBlockCipher

Paramètre	Description	Valeur recommandée
engineName	• AES • Blowfish • DES • 3DES • Null (pas de chiffrement)	AES
algorithmModeName	Mode d'algorithme de chiffrement de bloc : • CBC	CBC
algorithmPaddingName	Normes de remplissage : • PKCS7Padding • PKCS5Padding	PKCS7Padding
keySize	Dépend de l'algorithme (valeur prise en charge par **engineName**)	256
pbeCount	Nombre de hachages à exécuter pour créer la clé à partir de **encryptDecryptInitString** Tout nombre positif.	1000
pbeDigestAlgorithm	Type de hachage : • SHA1 • SHA256 • MD5	SHA256
encodingMode	Représentation ASCII de l'objet chiffré : • Base64 • Base64Url	Base64Url
useMacWithCrypto	Définit si MAC est utilisé avec le chiffrement : • true • false	false

Paramètre	Description	Valeur recommandée
macType	Type de MAC (Message Authentication Code) : • hmac	hmac
macKeySize SHA256	Dépend de l'algorithme MAC	256
macHashName	Algorithme MAC de hachage : • SHA256	SHA256

Chapitre 9 : Sécurisation renforcée haute disponibilité

Contenu de ce chapitre :

Authentification de cluster

Pour activer l'authentification de cluster :

1. Dans UCMDB, sélectionnez **Administration > Gestionnaire des paramètres d'infrastructure**.

2. Recherchez le paramètre **Enable joining High Availability cluster authentication** et attribuez-lui la valeur **true**.

3. Spécifiez un magasin de clés d'authentification de serveur (certificat °+ clés publique et privée) au format JKS. Ce magasin de clés sera placé sur tous les serveurs et utilisé pour l'authentification lors de la connexion à un cluster haute disponibilité.

   Placez le magasin de clés à l'emplacement suivant : **<dossier d'installation de UCMDB>\conf\security** et nommez-le **cluster.authentication.keystore.**

   > **Remarque :** UCMDB est livré avec ce magasin de clés préconfiguré, prêt à l'emploi. Il est identique pour toutes les nouvelles installations de UCMDB et donc, non sécurisé. Si vous souhaitez authentifier des demandes de jointure en toute sécurité, supprimez ce fichier et créez-en un autre.

4. Générez un magasin de clés d'authentification de cluster en procédant comme suit :

   a. À partir de C:\hp\UCMDB\UCMDBServer\bin\jre\bin, exécutez la commande suivante :

   ```
   keytool -genkey -alias hpcert –keystore <dossier d'installation de UCMDB>
   \conf\security\cluster.authentication.keystore -keyalg RSA
   ```

   La boîte de dialogue de la console s'ouvre pour vous demander d'entrer un nouveau mot de passe de magasin de clés.

   b. Le mot de passe par défaut est **hppass**. Si vous voulez utiliser un autre mot de passe,

mettez à jour le serveur en exécutant la méthode JMX suivante : **UCMDB:service=High Availability Services: changeClusterAuthenticationKeystorePassword**

c. Dans la boîte de dialogue de la console, répondez à la question **What is your first and last name?** en entrant le nom du cluster.

d. Entrez les autres paramètres en fonction des informations de votre organisation.

e. Entrez un mot de passe pour la clé. Il doit être identique à celui du magasin de clés.

Le magasin de clé JKS est créé sous **<dossier d'installation de UCMDB>\conf\security\cluster.authentication.keystore**

5. Remplacez l'ancien magasin **<dossier d'installation de UCMDB>\conf\security\cluster.authentication.keystore** sur tous les serveurs du cluster par le nouveau magasin de clés.

6. Redémarrez tous les serveurs du cluster.

Chiffrement des messages de cluster

Utilisez le chiffrement de message de cluster pour chiffrer tous les messages du cluster.

Pour activer le chiffrement de message de cluster :

1. Dans UCMDB, sélectionnez **Administration > Gestionnaire des paramètres d'infrastructure**.

2. Recherchez le paramètre **Enable joining High Availability cluster communication encryption** et attribuez-lui la valeur **true**.

3. Spécifiez une clé secrète pour le chiffrement symétrique sur tous les serveurs. La clé doit être placée dans un magasin de clés du type JCEKS à l'emplacement **<dossier d'installation de UCMDB>\conf\security\cluster.encryption.keystore**.

Remarque : UCMDB est livré avec ce magasin de clés préconfiguré, prêt à l'emploi. Il est identique pour toutes les nouvelles installations de UCMDB et donc, non sécurisé. Si vous souhaitez chiffrer les messages de cluster en toute sécurité, supprimez ce fichier et créez-en un autre en procédant comme suit :

4. À partir de **<dossier d'installation de UCMDB>\bin\jre\bin**, exécutez la commande suivante :

Keytool –genseckey –alias hpcert –keystore <dossier d'installation de UCMDB>\conf\security\cluster.encryption.keystore –storetype JCEKS

5. Vous êtes invité à entrer le mot de passe du nouveau magasin de clés. Le mot de passe par

défaut est « hpass ». Si vous voulez utiliser un autre mot de passe, mettez à jour le serveur en exécutant la méthode JMX suivante :

UCMDB:service=High Availability Services: changeClusterEncryptionKeystorePassword

6. Remplacez l'ancien magasin **<dossier d'installation de UCMDB>\conf\security\cluster.encryption.keystore** sur tous les serveurs du cluster par ce nouveau magasin de clés.

7. Redémarrez les serveurs.

Résolution des problèmes

Chaque fois que le serveur démarre, il envoie un message de test au cluster pour vérifier qu'il est connecté correctement au cluster. Si la connexion présente un problème, ce message échoue et le serveur est arrêté pour éviter de bloquer l'ensemble du cluster.

Voici certains exemples de configuration de chiffrement de cluster incorrecte :

- Le chiffrement est désactivé sur un nœud alors qu'un autre nœud l'a activé.
- Fichier cluster.encryption.keystore incorrect ou manquant
- Clé incorrecte ou manquante dans le magasin de clés.

Si le serveur est bloqué en raison d'un problème de configuration, les messages d'erreur suivants s'affichent :

```
2012-09-11 17:48:23,584 [Thread-14] FATAL - #### Server failed to connect proper
ly to the cluster and its service is stopped! Please fix the problem and start i
t again ####
```

```
2012-09-11 17:48:23,586 [Thread-14] FATAL -       Potential problems can be: wro
ng security configuration (wrong or missing cluster.encryption.keystore, wrong k
ey, disabled encryption in a cluster with enabled encryption)
```

Changement de clé dans key.bin

Dans un environnement haute disponibilité comportant plusieurs serveurs, modifiez comme suit la **clé** dans le fichier **key.bin** :

1. Accédez à l'ordinateur rédacteur (writer) dans JMX. Vous pouvez choisir n'importe quel ordinateur dans le cluster et cliquer sur le lien **writer** en haut de chaque page page.

2. Dans la section UCMDB de la console, cliquez sur **UCMDB:service=Discovery Manager**.

3. Pour changer la clé, procédez de l'une des façons suivantes :

- Cliquez sur **changeEncryptionKey** (cette action importe la clé de chiffrement existante)
- Cliquez sur **generateEncryptionKey** (cette action génère une clé de chiffrement aléatoire)

4. Sur l'ordinateur rédacteur, accédez au système de fichiers et recherchez **key.bin** sous **C:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**

5. Copiez le fichier **key.bin** depuis son emplacement sur l'ordinateur rédacteur vers chacun des ordinateurs du cluster dans le dossier **C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_1**, puis renommez le fichier de destination (par exemple, **key_new.bin**).

6. Pour chacun des autres serveurs (lecteurs), procédez comme suit :

   a. Convertissez le lecteur en rédacteur (à partir de JMX haute disponibilité) et attendez que la conversion soit terminée.

   b. Connectez-vous au JMX du rédacteur en cours et cliquez sur **UCMDB:service=Discovery Manager**.

   c. Cliquez et appelez **changeEncryptionKey**, utilisez les mêmes détails que vous avez entrés à l'étape 3 (pour **newKeyFileName**, utilisez le nouveau nom que vous avez affecté à l'étape 5).

   d. Vérifiez que vous obtenez le message suivant : **Key was created successfully**.

Vos commentaires sont toujours les bienvenus.

Pour soumettre vos commentaires relatifs à ce document, vous pouvez contacter l'équipe de documentation par e-mail. Si un client de messagerie est configuré sur ce système, cliquez sur le lien ci-dessus pour accéder à une fenêtre contenant le libellé suivant sur la ligne Objet :

Commentaires sur Manuel de sécurisation renforcée (Universal CMDB et Configuration Manager 10.10)

Il vous suffit ensuite d'ajouter vos commentaires et de cliquer sur Envoyer.

Si aucun client de messagerie n'est disponible, copiez le libellé ci-dessus dans une fenêtre d'un client de messagerie Web et envoyez votre message de commentaires à SW-Doc@hp.com.