Communication JMX sécurisée entre les composants CVP OAMP et CVP avec authentification mutuelle

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Générer des certificats CSR pour WSM

Générer un certificat client signé par l'autorité de certification pour WSM

Générer un certificat client CA-Signed pour OAMP (à effectuer sur OAMP)

Informations connexes

Introduction

Ce document décrit comment sécuriser la communication Java Management Extensions (JMX) entre Customer Voice Portal (CVP) Operation and Management Console (OAMP) et CVP Server et CVP Reporting Server dans la solution Cisco Unified Contact Center Enterprise (UCCE) via des certificats signés par l'autorité de certification (CA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCCE version 12.5(1)
- Customer Voice Portal (CVP) version 12.5 (1)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- UCCE 12.5(1)
- CVP 12.5(1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

OAMP communique avec CVP Call Server, CVP VXML Server et CVP Reporting Server via le protocole JMX. La communication sécurisée entre OAMP et ces composants CVP empêche les failles de sécurité JMX. Cette communication sécurisée est facultative, elle n'est pas requise pour le fonctionnement normal entre OAMP et les composants CVP.

Vous pouvez sécuriser les communications JMX en :

- Générez la demande de signature de certificat (CSR) pour le Gestionnaire de services Web (WSM) dans le serveur CVP et le serveur de rapports CVP.
- Générez un certificat client CSR pour WSM dans CVP Server et CVP Reporting Server.
- Générer un certificat client CSR pour OAMP (à effectuer sur OAMP).
- Signer les certificats par une autorité de certification.
- Importez les certificats signés CA, racine et intermédiaire dans CVP Server, CVP Reporting Server et OAMP.
- [Facultatif] Connexion sécurisée à OAMP via JConsole.
- CLI du système sécurisé.

Générer des certificats CSR pour WSM

Étape 1. Connectez-vous au serveur CVP ou Reporting. Récupérez le mot de passe keystore à partir du fichier security.properties.

Remarque : À l'invite de commandes, entrez autres %CVP_HOME%\conf\security.properties. Security.keystorePW = <Retourne le mot de passe keystore> Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 2. Accédez à %CVP_HOME%\conf\security et supprimez le certificat WSM. Utilisez cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate.

Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 3. Répétez l'étape 2 pour les certificats de serveur d'appels (callserver_certificate) et de serveur VXML (vxml_certificate) sur le serveur CVP et le certificat de serveur d'appels (callserver_certificate) sur le serveur Reporting.

Étape 4 : génération d’un certificat signé par une autorité de certification pour le service WSM Utilisez cette commande :

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore

%CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_certificate -v -keysize 2048 -keyalg RSA.

1. Entrez les détails à l'invite et tapez Yes pour confirmer.
2. Entrez le mot de passe keystore lorsque vous y êtes invité.

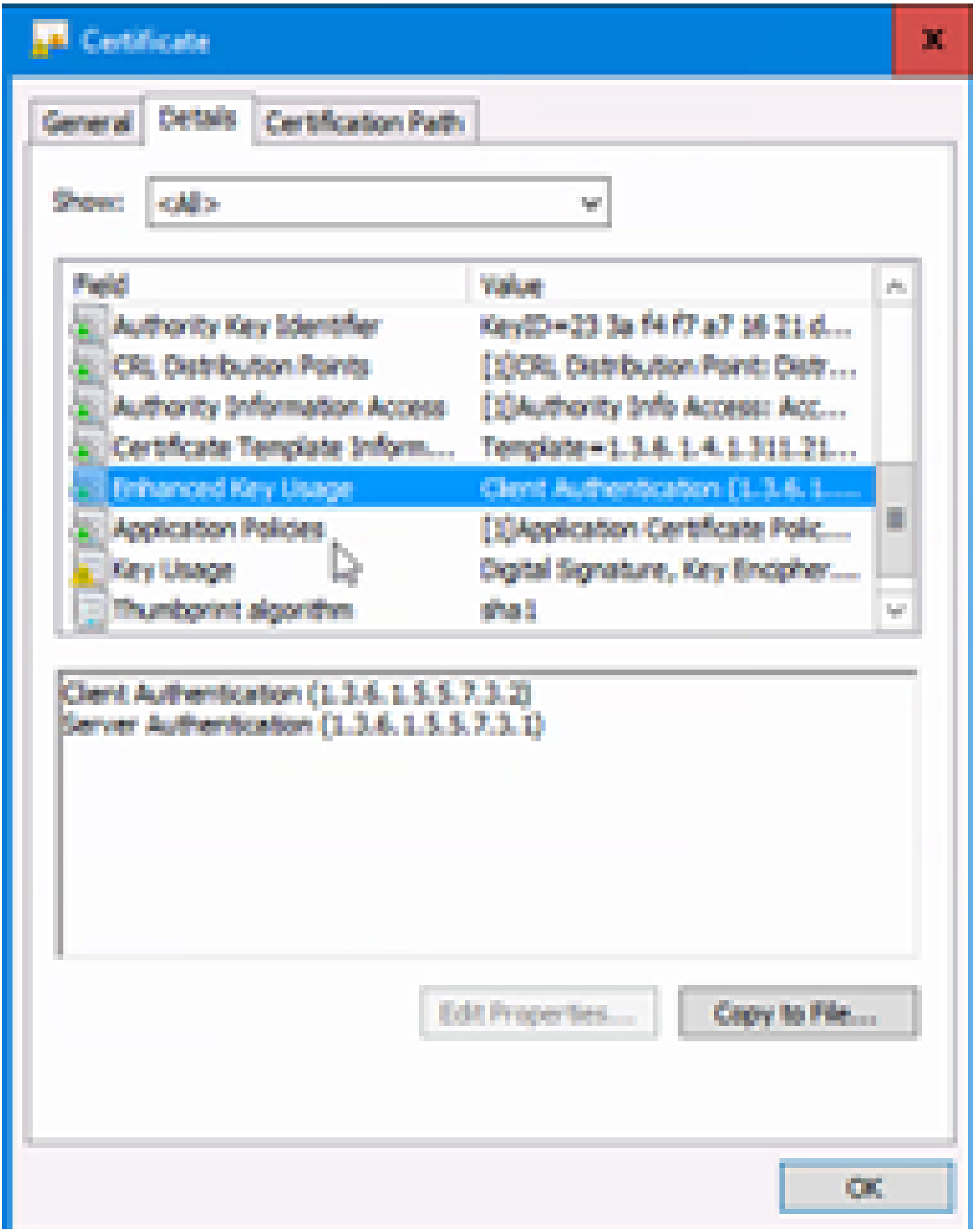
Remarque : Notez le nom CN pour référence ultérieure.

Étape 5 : génération de la demande de certificat pour l’alias Exécutez cette commande et enregistrez-la dans un fichier. Par exemple, wsm.csr.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.csr.

1. Entrez le mot de passe du keystore lorsque vous y êtes invité.

Étape 6. Obtenez le certificat signé par une autorité de certification. Suivez la procédure pour créer un certificat signé par une autorité de certification avec l'autorité de certification et assurez-vous d'utiliser un modèle d'authentification de certificat client-serveur lorsque l'autorité de certification génère le certificat signé.



Étape 7 : téléchargement du certificat signé, du certificat racine et du certificat intermédiaire de l'autorité de certification

Étape 8. Copiez le certificat WSM racine, intermédiaire et signé par l'autorité de certification dans

%CVP_HOME%\conf\security\.

Étape 9. Importez le certificat racine avec cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cer>.

1. Entrez le mot de passe keystore lorsque vous y êtes invité.
2. À l'invite Trust this certificate, tapez Yes.

Étape 10. Importez le certificat intermédiaire avec cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermédiaire -file %CVP_HOME%\conf\security\<nom_fichier_intermédiaire_cer>.

1. Entrez le mot de passe keystore lorsque vous y êtes invité.
2. À l'invite Trust this certificate, tapez Yes.

Étape 11. Importez le certificat WSM signé par l'autorité de certification à l'aide de cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias wsm_certificate -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>.

1. Entrez le mot de passe du keystore lorsque vous y êtes invité.

Étape 12. Répétez les étapes 4 à 11 (il n'est pas nécessaire d'importer deux fois les certificats racine et intermédiaire) pour les certificats de serveur d'appels et de serveur VXML sur le serveur CVP et le certificat de serveur d'appels sur le serveur Reporting.

Étape 13 - Configurez le WSM dans CVP Server et CVP Reporting Server.

1. Accédez à c:\cisco\cvp\conf\jmx_wsm.conf.

Ajoutez ou mettez à jour le fichier comme indiqué et enregistrez-le :

```
javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2099
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 3000
javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword=< keystore_password >
javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.trustStorePassword=< keystore_password >
javax.net.ssl.trustStoreType=JCEKS
```

2. Exécutez la commande regedit.

```
Append this to the file at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2
```

```
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
Djavax.net.ssl.trustStorePassword=
```

```
Djavax.net.ssl.trustStoreType=JCEKS
```

Étape 14. Configuration de JMX de CVP Callserver dans CVP Server et Reporting Server

1. Accédez à c:\cisco\cvp\conf\jmx_callserver.conf.

Mettez à jour le fichier comme indiqué et enregistrez-le :

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2098
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 2097
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword =
```

```
javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.trustStorePassword=< keystore_password >
javax.net.ssl.trustStoreType=JCEKS
```

Étape 15. Configuration de JMX du serveur VXML dans le serveur CVP

1. Accédez à c:\cisco\cvp\conf\jmx_vxml.conf.

Modifiez le fichier comme indiqué et enregistrez-le :

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword =
```

2. Exécutez la commande regedit.

- ```
  Append theese to the file at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Pr
  ```

  ```
  Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
  Djavax.net.ssl.trustStorePassword=
  ```

  ```
  Djavax.net.ssl.trustStoreType=JCEKS
  ```

3. Redémarrez le service WSM, le serveur d'appels et les services VXML Server sur le serveur CVP et le service WSM et le service Call Server sur Reporting Server.

Remarque : Lorsque la communication sécurisée est activée avec JMX, elle force le keystore à être %CVP_HOME%\conf\security\.keystore, au lieu de %CVP_HOME%\jre\lib\security\cacerts.
Par conséquent, les certificats de %CVP_HOME%\jre\lib\security\cacerts doivent être importés dans %CVP_HOME%\conf\security\.keystore.

Générer un certificat client signé par l'autorité de certification pour WSM

Étape 1. Connectez-vous au serveur CVP ou Reporting. Récupérez le mot de passe keystore à partir du fichier security.properties.

Remarque : À l'invite de commandes, entrez autres %CVP_HOME%\conf\security.properties. Security.keystorePW = <Retourne le mot de passe

---
  ```

keystore> Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 2. Accédez à %CVP_HOME%\conf\security et générez un certificat signé par l'autorité de certification pour l'authentification du client avec callserver avec cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN du certificat WSM CVP Server ou Reporting Server> -v -keysize 2048 -keyalg RSA

1. Entrez les détails à l'invite et tapez Oui pour confirmer.
2. Entrez le mot de passe du keystore lorsque vous y êtes invité.

Remarque : L'alias est identique au CN utilisé pour générer le certificat du serveur WSM.

Étape 3. Générez la demande de certificat pour l'alias à l'aide de cette commande et enregistrez-la dans un fichier (par exemple, jmx_client.csr).

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN du certificat WSM CVP Server ou Reporting Server> -fichier %CVP_HOME%\conf\security\jmx_client.csr

1. Entrez le mot de passe du keystore lorsque vous y êtes invité.
2. Vérifiez que le CSR a été généré correctement avec cette commande : dir jmx_client.csr.

Étape 4. Signature du certificat client JMX sur une autorité de certification

Remarque : Suivez la procédure pour créer un certificat signé par une autorité de certification avec l'autorité de certification. Téléchargez le certificat client JMX signé par l'autorité de certification (les certificats racine et intermédiaire ne sont pas requis car ils ont été téléchargés et importés précédemment).

1. Entrez le mot de passe du keystore lorsque vous y êtes invité.
2. À l'invite Trust this certificate, tapez Yes.

Étape 5. Copiez le certificat du client JMX signé par l'autorité de certification dans %CVP_HOME%\conf\security\.

Étape 6. Importez le certificat client JMX signé par l'autorité de certification à l'aide de cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN du certificat WSM CVP Server ou Reporting Server> -file %CVP_HOME%\conf\security\<nom du certificat client JMX signé par l'autorité de certification>

1. Entrez le mot de passe du keystore lorsque vous y êtes invité.

Étape 7. Redémarrez Cisco CVP Call Server, VXML Server et les services WSM.

Étape 8. Répétez la même procédure pour Reporting Server, si elle est implémentée.

Générer un certificat client CA-Signed pour OAMP (à effectuer sur OAMP)

Étape 1 : connexion au serveur OAMP Récupérez le mot de passe keystore à partir du fichier security.properties.

Remarque : À l'invite de commandes, entrez more %CVP_HOME%\conf\security.properties. Security.keystorePW = <Retourne le mot de passe keystore> Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 2. Accédez à %CVP_HOME%\conf\security et générez un certificat signé par une autorité de certification pour l'authentification client avec le serveur CVP ou le WSM CVP Reporting Server. Utilisez cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN du certificat WSM du serveur CVP ou du serveur de rapports CVP> -v -keysize 2048 -keyalg RSA.

1. Entrez les détails à l'invite et tapez Oui pour confirmer.
2. Entrez le mot de passe du keystore lorsque vous y êtes invité.

Étape 3. Générez la demande de certificat pour l'alias à l'aide de cette commande et enregistrez-la dans un fichier (par exemple, jmx.csr).

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN du certificat WSM du serveur CVP ou du serveur de rapports CVP> -file %CVP_HOME%\conf\security\jmx.csr.

1. Entrez le mot de passe du keystore lorsque vous y êtes invité.

Étape 4. Signature du certificat sur une autorité de certification

---

Remarque : Suivez la procédure pour créer un certificat signé par une autorité de certification à l'aide de cette dernière. Téléchargez le certificat et le certificat racine de l'autorité de certification.

Étape 5. Copiez le certificat racine et le certificat client JMX signé par l'autorité de certification dans %CVP_HOME%\conf\security\.

Étape 6. Importez le certificat racine de l’autorité de certification. Utilisez cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore

%CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>.

1. Entrez le mot de passe du keystore lorsque vous y êtes invité.
2. À l'invite Trust this certificate, tapez Yes.

Étape 7. Importez le certificat client JMX signé par l'autorité de certification du serveur CVP et du serveur de rapports CVP. Utilisez cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <certificat WSM du serveur CVP ou du serveur de rapports CVP> -file %CVP_HOME%\conf\security\<nom_fichier_de_votre_certificat_signé_de_CA>.

1. Entrez le mot de passe du keystore lorsque vous y êtes invité.

Étape 8 : redémarrage du service OAMP

Étape 9. Connectez-vous à OAMP pour activer la communication sécurisée entre OAMP et Call Server, VXML Server ou Reporting Server. Accédez à Device Management > Call Server. Cochez la case Enable secure communication with the Ops console. Enregistrez et déployez Call Server et VXML Server.

Étape 10. Exécutez la commande regedit.

Accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java.

Ajoutez-le au fichier et enregistrez-le.

```
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
Djavax.net.ssl.trustStorePassword=



Djavax.net.ssl.trustStoreType=JCEKS
```

Remarque : Une fois les ports sécurisés pour JMX, vous ne pouvez accéder à JConsole qu'après avoir effectué les étapes définies pour JConsole répertoriées dans les documents Oracle.

Étape 1. Redémarrez le service OAMP.

Informations connexes

- Guide de configuration sécurisée CVP
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.