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

Contenu

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.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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 vulnérabilités de sécurité JMX. Cette communication sécurisée est facultative, elle n'est pas requise pour le fonctionnement régulier entre OAMP et les composants CVP.

Vous pouvez sécuriser les communications JMX en :

- Générez la demande de signature de certificat (CSR) pour Web Service Manager (WSM) dans CVP Server et CVP Reporting Server.
- Générer un certificat client CSR pour WSM dans CVP Server et CVP Reporting Server.
- Générer un certificat client CSR pour OAMP (à faire 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 JConsole à OAMP.
- CLI du système sécurisé.

Générer des certificats CSR pour WSM

Étape 1. Connectez-vous au serveur CVP ou au serveur de rapports. Récupérez le mot de passe de la banque de clés à partir du fichier **security.properties**.

> **Note**: À l'invite de commandes, entrez plus de %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 and delete the WSM certificate. 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 de la banque de clés lorsque vous y êtes invité.

Étape 3. Répétez l'étape 2 pour les certificats Call Server et VXML Server sur le serveur CVP et le certificat Call Server sur le serveur Reporting Server.

Étape 4. Générer un certificat signé par l'autorité de certification pour le serveur 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 **Oui** pour confirmer.
2. Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.

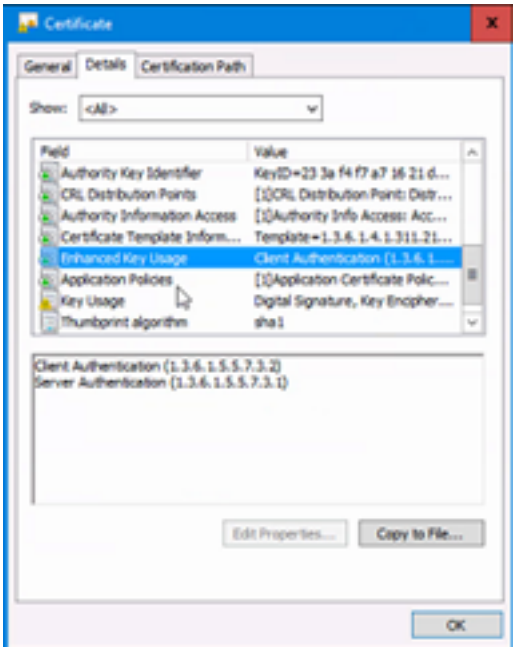
   Note: Notez le nom CN pour référence future.

Étape 5. Générez 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 de la banque de clés 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 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. Téléchargez le certificat signé, le certificat racine et le certificat intermédiaire de l'autorité de certification.

Étape 8. Copiez le certificat WSM signé par la racine, l'intermédiaire et 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 de la banque de clés lorsque vous y êtes invité.
2. Àl'invite Approuver ce certificat, tapez **Oui**.

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 -fichier %CVP_HOME%\conf\security\<filename_of_intermédiaire_cer>.

1. Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.

2. À l'invite Approuver ce certificat, tapez **Oui**.

Étape 11. Importez le certificat WSM signé par l'autorité de certification avec 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 de la banque de clés lorsque vous y êtes invité.

Étape 12. Répétez les étapes 4 à 11 (les certificats racine et intermédiaire n'ont pas besoin d'être importés deux fois), pour les certificats Call Server et VXML Server sur le certificat CVP Server et Call Server sur le serveur de rapports.

Étape 13 - Configurez WSM dans CVP.

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

Étape 14. Configurez 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 =
```

Étape 15. Configurez JMX de VXMLServer sur CVP Server.

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\Procrun 2.0\VXMLServer\Parameters\Java:
  Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
  Djavax.net.ssl.trustStorePassword=
  ```

3. Redémarrez les services WSM, Call Server et VXML Server sur le serveur CVP et WSM Service et Call Server sur Reporting Server.

> **Remarque :** Lorsque la communication sécurisée est activée avec JMX, elle force le magasin de clés 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 CA pour WSM

Étape 1. Connectez-vous au serveur CVP ou au serveur de rapports. Récupérez le mot de passe de la banque de clés à partir du fichier **security.properties**.

> **Note**: À l'invite de commandes, entrez plus de %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 and generate a CA-signed certificate for client authentication with callserver with this command.

%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 Reporting> -v -keysize 2048 -keyalg RSA

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

> **Note**: L'alias sera le même que le CN utilisé pour générer le certificat du serveur WSM.

Étape 3. Générez la demande de certificat pour l'alias avec 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 certificat WSM du serveur CVP ou du serveur Reporting> -file %CVP_HOME%\conf\security\jmx_client.csr

1. Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.
2. Vérifiez que le CSR a été généré avec succès avec sa commande : **dir jmx_client.csr**

Étape 4. Signez le certificat client JMX sur une autorité de certification.
  ```

Note: 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 puisqu'ils ont été téléchargés et importés précédemment).

1. Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.
2. À l'invite Approuver ce certificat, tapez Oui.

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

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

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN du certificat WSM du serveur CVP ou du serveur Reporting> -fichier %CVP_HOME%\conf\security\<nom du fichier du certificat client JMX signé CA>

1. Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.

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

Étape 8. Répétez la même procédure pour Reporting Server, si implémenté.

Générer un certificat client signé CA pour OAMP (à faire sur OAMP)

Étape 1. Connectez-vous au serveur OAMP. Récupérez le mot de passe de la banque de clés à partir du fichier **security.properties**.

Note: 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 la sécurité **%CVP_HOME%\conf** et générez un certificat signé CA pour l'authentification client avec le serveur CVP WSM. Utilisez cette commande.

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

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

Étape 3. Générez la demande de certificat pour l'alias avec 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> -fichier %CVP_HOME%\conf\security\jmx.csr.

1. Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.

Étape 4. Signez le certificat sur une CA.

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

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

Étape 6. Importer 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 de la banque de clés lorsque vous y êtes invité.
2. À l'invite Approuver ce certificat, tapez Oui.

Étape 7. Importez le certificat client JMX signé CA de CVP. Utilisez cette commande.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN du certificat WSM du serveur d'appels> -fichier %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>.

1. Entrez le mot de passe de la banque de clés lorsque vous y êtes invité.

Étape 8. Redémarrez le service OAMP.

Étape 9. Connectez-vous à OAMP. pour activer la communication sécurisée entre OAMP et Call Server ou VXML Server. Accédez à **Device Management > Call Server**. Cochez la case Activer la communication sécurisée avec la console Ops. 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=
```

> **Remarque** : une fois les ports sécurisés pour JMX, JConsole n'est accessible qu'après avoir effectué les étapes définies pour JConsole répertoriées dans les documents Oracle.

Informations connexes

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