Exchange des certificats auto-signés dans une solution UCCE

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Fond **Procédure** Serveurs CCE AW et serveurs d'applications CCE Core Section 1 : Échange de certificats entre Router\Logger, PG et AW Server. Section 2 : Échange de certificats entre les applications de la plate-forme VOS et le serveur AW. Serveur OAMP CVP et serveurs de composants CVP Section 1 : Échange de certificats entre CVP OAMP Server et CVP Server et Reporting Servers. Section 2 : Échange de certificats entre le serveur OAMP CVP et les applications de la plateforme VOS. Section 3 : Échange de certificats entre le serveur CVP et les serveurs CVB. **CVP CallStudio WEBService Integration** Informations connexes

Introduction

Ce document décrit comment échanger des certificats auto-signés dans la solution Unified Contact Center Enterprise (UCCE).

Contribué par Anuj Bhatia, Robert Rogier et Ramiro Amaya, ingénieurs du TAC Cisco

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)
- Navigateur vocal virtualisé Cisco (VVB)

Components Used

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

• UCCE 12.5(1)

- CVP 12.5(1)
- Cisco VVB 12.5
- Console d'exploitation CVP (OAMP)
- CVP New OAMP (NOAMP)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

Dans la solution UCCE, la configuration de nouvelles fonctionnalités qui impliquent des applications de base telles que Roggers, Peripheral Gateways (PG), Admin Workstations (AW), Finesse, Cisco Unified Intelligent Center (CUIC), etc est effectuée via la page d'administration de Contact Center Enterprise (CCE). Pour les applications de réponse vocale interactive (IVR) telles que CVP, Cisco VVB et les passerelles, NOAMP contrôle la configuration des nouvelles fonctionnalités. À partir de CCE 12.5(1) en raison de la sécurité-management-conformité (SRC), toute la communication à l'administrateur CCE et à NOAMP est strictement effectuée via le protocole HTTP sécurisé.

Pour assurer une communication transparente et sécurisée entre ces applications dans un environnement de certificats auto-signé, l'échange de ces certificats entre les serveurs devient une nécessité. La section suivante explique en détail les étapes nécessaires pour échanger un certificat auto-signé entre :

- Serveurs CCE AW et serveurs d'applications CCE Core
- Serveur OAMP CVP et serveurs de composants CVP

Procédure

Serveurs CCE AW et serveurs d'applications CCE Core

Il s'agit des composants à partir desquels les certificats auto-signés sont exportés et des composants dans lesquels les certificats auto-signés doivent être importés.

Serveurs CCE AW : Ce serveur requiert un certificat de :

• Plate-forme Windows : Router and Logger(Rogger){A/B}, Peripheral Gateway (PG){A/B}, tous les serveurs AW/ADS et Email and Chat (ECE).

Note: Les certificats IIS et de cadre de diagnostic sont nécessaires.

• Plate-forme VOS : Cisco Unified Call Manager (CUCM), Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect et d'autres serveurs applicables faisant partie de la base de données d'inventaire.

Il en va de même pour les autres serveurs AW de la solution.

Routeur \ Serveur de journalisation : Ce serveur requiert un certificat de :

• Plate-forme Windows : Certificat IIS de tous les serveurs AW.

Les étapes nécessaires pour échanger efficacement les certificats autosignés pour CCE sont divisées dans ces sections.

Section 1 : Échange de certificats entre Router\Logger, PG et AW Server. Section 2 : Échange de certificats entre l'application de plate-forme VOS et le serveur AW.

Section 1 : Échange de certificats entre Router\Logger, PG et AW Server.

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter les certificats IIS à partir de Router\Logger, PG et tous les serveurs AW. Étape 2. Exporter les certificats DFP (Diagnostic Framework Portico) des serveurs Router\Logger et PG.

Étape 3. Importez des certificats IIS et DFP à partir de Router\Logger, PG vers des serveurs AW. Étape 4. Importez le certificat IIS vers Router\Logger à partir des serveurs AW.

Attention : Avant de commencer, vous devez sauvegarder le keystore et exécuter les commandes à partir de la maison java en tant qu'administrateur.

(i) Connaître le chemin d'accès de la maison java pour s'assurer que l'outil de clé java est hébergé. Il y a deux façons de trouver le chemin de la maison java.

Option 1 : Commande CLI : **écho %JAVA_HOME%**



Option 2 : Manuellement via le paramètre système avancé, comme illustré dans l'image



Note: Sur UCCE 12.5, le chemin par défaut est C:\Program Files

(x86)\Java\jre1.8.0_221\bin. Cependant, si vous avez utilisé le programme d'installation 12.5(1a) ou si 12.5 ES55 est installé (OpenJDK ES obligatoire), utilisez CCE_JAVA_HOME au lieu de JAVA_HOME puisque le chemin du data store a changé avec OpenJDK. Plus d'informations sur la migration OpenJDK dans CCE et CVP dans ces documents : <u>Installer et</u> <u>migrer vers OpenJDK dans CCE 2.5(1)</u> et <u>installer et migrer vers OpenJDK dans CVP</u> <u>12.5(1)</u>.

(ii) Sauvegarder le fichier cacerts à partir du dossier C:\Program Fichiers (x86)\Java\jre1.8.0_221\lib\security. Vous pouvez le copier vers un autre emplacement.

(iii) Ouvrez une fenêtre de commande en tant qu'administrateur pour exécuter les commandes.

Étape 1. Exporter les certificats IIS à partir de Router\Logger, PG et tous les serveurs AW.

(i) Sur le serveur AW à partir d'un navigateur, accédez à l'URL des serveurs (Roggers, PG, autres serveurs AW) : https://{servername}.

CCE via Chrome Browser

| ← → C ▲ Not secure aw125a | .bora.com | | |
|--|--------------|---|--|
| ← → C ▲ Not secure aw125a Certificate General Details Certification Path Show: <all></all> Field Value Version V3 Serial number Signature algorithm sha256RSA Signature algorithm sha256 Signature algorithm sha256 Signature hash algorithm wa125a.bora. Valid from Monday, Seption Valid to Sunday, Seption | Lbora.com | Certificate Export Wizard Export File Format Certificates can be exported in a variety of file formats. Select the format you want to use: DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78) Include all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful | |
| Edit Properties | Copy to File | Export all extended properties Enable certificate privacy Microsoft Serialized Certificate Store (.SST) | |

(ii)Enregistrez le certificat dans un dossier temporaire, par exemple c:\temp\certs et nommez le certificat en ICM{svr}[ab].cer.

Remarque : sélectionnez l'option Base-64 encoded X.509 (.CER).

Étape 2. Exporter les certificats DFP (Diagnostic Framework Portico) des serveurs Router\Logger et PG.

(i) Sur le serveur AW, ouvrez un navigateur et accédez aux serveurs (Router, Logger ou Roggers, PG) URL DFP : https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion.

Portico via Chrome Browser



(ii) Enregistrez le certificat dans l'exemple de dossier c:\temp\certs et nommez le certificat en dfp{svr}[ab].cer

Note: Sélectionnez l'option Base-64 encoded X.509 (.CER).

Étape 3. Importez les certificats IIS et DFP de Rogger, PG vers les serveurs AW.

Commande pour importer les certificats auto-signés IIS dans le serveur AW. Chemin d'accès à l'outil Clé : Fichiers C:\Program (x86)\Java\jre1.8.0_221\bin :

keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer

Note: Importez tous les certificats de serveur exportés vers tous les serveurs AW.

Commande d'importation des certificats DFP autosignés dans les serveurs AW :

keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import storepass changeit -alias {fqdn_of_server}_DFP -file c:\temp\certs\ dfp{svr}[ab].cer Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" import -storepass changeit -alias myrgra.domain.com_DFP -file c:\temp\certs\dfprgra.cer

Note: Importez tous les certificats de serveur exportés vers tous les serveurs AW.

Redémarrez le service Apache Tomcat sur les serveurs AW.

Étape 4. Importez le certificat IIS vers Router\Logger à partir des serveurs AW.

Commande pour importer les certificats auto-signés IIS dans les serveurs Rogger :

keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer

Note: Importez tous les certificats de serveur IIS AW exportés sur les côtés Rogger A et B.

Redémarrez le service Apache Tomcat sur les serveurs Rogger.

Section 2 : Échange de certificats entre les applications de la plate-forme VOS et le serveur AW.

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS. Étape 2. Importer des certificats d'application de plate-forme VOS vers le serveur AW.

Ce processus s'applique à toutes les applications VOS telles que :

- CUCM
- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS.

(i) Accédez à la page Cisco Unified Communications Operating System Administration : https://FQDN:8443/cmplatform.

(ii) Accédez à **Security > Certificate Management** et recherchez les certificats du serveur principal de l'application dans le dossier tomcat-trust.

| Cisco Unified Operating System Admin For Case Volted Communications Solutions | istrat | ion | | Revigition Class Unified ISS Administration • Sk administration About Lagon |
|--|--------|------|--|--|
| Drov + Settings + Security + Schwarzuppietes + Secure + Help + | | | | |
| Gertificate List | | | | |
| 💦 Generale Set report 🐴 Spinal Carthoda Carthoda ataw 🛞 Generale | C94 | | | |
| torresh lovel Case ECC Real Ch | Sel- | 80 | Care, BCC, Real, CA | Core_BCC_Real_CA |
| toward-boat Indiana Audience and Research Institutions ResEA 2011 | Sel- | 854 | Inferic/caleric_int/leases/Unitation_RetGi_201 | 1 Nelevic, Andersic, and Jaseard South An |
| tomati trust (2572 W25eley Shite) Bost 58 CA | Self- | 854 | 015TE_WISerier_Ghitei_Rook_GB_CA | 00570_WtSekin_Gistel_Root_00_CA |
| tomost-trust Amazon Root Ck. 4 | Sel- | ec. | Amazon, Root, CA, A | Amazon, Root, CA, 4 |
| tomonithust <u>007 April 04 X0</u> | Self- | 854 | 057_Aux_C4_X3 | DST_Root_CA_K3 |
| tomat-trust <u>AMTrust Educat CA April</u> | Self- | 854 | AddTrast_Doenal_CA_Root | AddTrust_Doternal_CA_Root |
| tonanthat <u>option.on</u> | Set- | 83.4 | op.ton.an | copiliera.com |
| Koncast Road - Effective Delastical Case 3 | bail- | 124 | P Tabilac_DobaRost_Class_3 | Final ColeRed Case 3 |
| tonation Decet Order Aut 52 | Set- | 83.0 | DipCw1_Dobal_Root_02 | Digitizet_States_Root_S2 |

(iii) Sélectionnez le certificat et cliquez sur télécharger le fichier .PEM pour l'enregistrer dans un dossier temporaire sur le serveur AW.

| File Name | con hora com nem | | | | | |
|---|---|--|--|--|--|--|
| Cartificate Durnors | tomest-trust | | | | | |
| Certificate Purpose concertrusc | | | | | | |
| Certificate Type trust-certs | | | | | | |
| Certificate Group | product-cpi | | | | | |
| Description(friend | ly name) Trust Certificate | | | | | |
| | | | | | | |
| Certificate File D | ata | | | | | |
| | | | | | | |
| Version V2 | | | | | | |
| Version: V3 | | | | | | |
| The second se | CC3CR3A90A9074710RR9EREA03CE710D | | | | | |
| Serial Number: : | 5C35B3A89A8974719BB85B6A92CF710D | | | | | |
| SignatureAlgorit | 5C35B3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) BXB, ST=ma, CN=cco, bcca.com, QU=BXB,TAC, Q=TAC, C=US | | | | | |
| SignatureAlgorit Issuer Name: L= Validity From: M | 5C35B3A89A89747199B85B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) •BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 | | | | | |
| Serial Number: SignatureAlgorit Issuer Name: Le Validity From: M To: Sat D | 5C35B3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) #BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 | | | | | |
| Senal Number: 3 SignatureAlgorit Issuer Name: L- Validity From: M To: Sat (Subject Name: U | SC35B3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) #BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 _=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US | | | | | |
| Senai Number: 1 SignatureAlgorit Issuer Name: L Validity From: M To: Sat (Subject Name: I Key: RSA (1.2.8 | SC35B3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) | | | | | |
| Senai Number: 1 SignatureAlgorit Issuer Name: L Validity From: M To: Sat (Subject Name: I Key: RSA (1.2.8 Key value: | SC35B3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) #BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 _=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) | | | | | |
| Senai Number: 3 SignatureAlgorit Issuer Name: L- Validity From: M To: Sat (Subject Name: I Key: RSA (1.2.8 Key value: 3082010a028201 | SC35B3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 .=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) 0100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 | | | | | |
| Senai Number: 3 SignatureAlgorit Issuer Name: L Validity From: M To: Sat (Subject Name: I Key: RSA (1.2.8 Key value: 3082010a028201 69f9980a1246814 | SC35B3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:21 EST 2019 Dec 14 10:55:21 EST 2024 .=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) 0100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 Hbe9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 | | | | | |
| Senai Number: 3 SignatureAlgorit Issuer Name: Le Validity From: M To: Sat (Subject Name: I Key: RSA (1.2.8 Key value: 3082010a028201 69f9980a1246814 88e0e816e64ad4 | SC35B3A89A8974719BB85B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:21 EST 2019 Dec 14 10:55:21 EST 2024 .=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) 0100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 Hbe9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 | | | | | |
| Serial Number: 3 SignatureAlgorit Issuer Name: Le Validity From: M To: Sat (Subject Name: L Key: RSA (1.2.8 Key value: 3082010a028201 69f9980a1246814 88e0e816e64ad4 f140216a5e5aca1 | SC35B3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) •BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 .=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) 0100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 ibe9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f | | | | | |
| Senai Number: 3 SignatureAlgorit Issuer Name: Le Validity From: M To: Sat (Subject Name: L Key: RSA (1.2.8 Key value: 3082010a028201 69f9980a1246814 88e0e816e64ad4 f140216a5e5aca1 520da30a39b206 | SC3SB3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) •BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 .=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) 0100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 ibe9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a | | | | | |
| Senai Number: 3 SignatureAlgorit Issuer Name: Le Validity From: M To: Sat (Subject Name: L Key: RSA (1.2.8 Key value: 3082010a028201 69f9980a1246814 88e0e816e64ad4 f140216a5e5aca1 520da30a39b206 | SC3SB3A89A8974719B885B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) •BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 .=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) 0100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 ibe9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a | | | | | |
| Senai Number: 3 SignatureAlgorit Issuer Name: Le Validity From: M To: Sat (Subject Name: L Key: RSA (1.2.8 Key value: 3082010a028201 699980a1246814 88e0e816e64ad4 f140216a5e5aca1 520da30a39b206 | SC3SB3A89A8974719BB85B6A92CF710D hm: SHA256withRSA (1.2.840.113549.1.1.11) BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US on Dec 16 10:55:22 EST 2019 Dec 14 10:55:21 EST 2024 .=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 40.113549.1.1.1) 0100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 Hbe9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a | | | | | |

Note: Effectuez les mêmes étapes pour l'abonné.

Étape 2. Importer l'application de plate-forme VOS vers le serveur AW.

Chemin d'accès à l'outil Clé : C:\Program Fichiers (x86)\Java\jre1.8.0_221\bin

Commande d'importation des certificats auto-signés :

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -
storepass changeit -alias {fqdn_of_vos} -file c:\temp\certs\vosapplicationX.pem
```

Redémarrez le service Apache Tomcat sur les serveurs AW.

Note: Effectuez la même tâche sur d'autres serveurs AW.

Serveur OAMP CVP et serveurs de composants CVP

Il s'agit des composants à partir desquels les certificats auto-signés sont exportés et des composants dans lesquels les certificats auto-signés doivent être importés.

i) Serveur OAMP CVP : Ce serveur requiert un certificat de

- Plate-forme Windows : Certificat Web Services Manager (WSM) provenant des serveurs CVP Server et Reporting.
- Plate-forme VOS : Intégration de Cisco VVB pour Customer Virtual Agent (CVA), serveur Cloud Connect pour intégration de Webex Experience Management (WXM).
- ii) Serveurs CVP : Ce serveur requiert un certificat de

- Plate-forme Windows : Certificat WSM du serveur OAMP.
- Plate-forme VOS : Serveur Cloud Connect pour l'intégration WXM, serveur Cisco VVB pour les communications SIP et HTTP sécurisées.
- iii) Serveurs de rapports CVP : Ce serveur requiert un certificat de
 - Plate-forme Windows : Certificat WSM du serveur OAMP.

(iv) Serveurs Cisco VVB : ce serveur nécessite un certificat de

Plate-forme Windows : Serveur CVP VXML (HTTP sécurisé), serveur d'appels CVP (SIP sécurisé)

Les étapes nécessaires pour échanger efficacement les certificats auto-signés dans l'environnement CVP sont expliquées dans ces trois sections.

Section 1 : Échange de certificats entre CVP OAMP Server et CVP Server et Reporting Servers. Section 2 : Échange de certificats entre le serveur OAMP CVP et les applications de la plateforme VOS.

Section 3 : Échange de certificats entre le serveur CVP et les serveurs VVB.

Section 1 : Échange de certificats entre CVP OAMP Server et CVP Server et Reporting Servers.

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter le certificat WSM à partir du serveur CVP, du serveur de rapports et du serveur OAMP.

Étape 2. Importez des certificats WSM à partir du serveur CVP et du serveur de rapports dans le serveur OAMP.

Étape 3. Importez le certificat WSM du serveur OAMP CVP dans les serveurs CVP Server et Reporting.

Attention : Avant de commencer, procédez comme suit :

1. Obtenez le mot de passe de la banque de clés. Exécutez la commande : plus %CVP_HOME%\conf\security.properties

2. Copiez le dossier %CVP_HOME%\conf\security dans un autre dossier.

3. Ouvrez une fenêtre de commande en tant qu'administrateur pour exécuter les commandes.

Étape 1. Exporter le certificat WSM à partir du serveur CVP, du serveur de rapports et du serveur OAMP.

(i) Exportez le certificat WSM de chaque serveur CVP vers un emplacement temporaire et renommez le certificat avec le nom souhaité. Vous pouvez le renommer wsmX.crt. Remplacez X par un numéro ou une lettre unique. Par exemple, wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

Commande d'exportation des certificats auto-signés :

(ii) Copiez le certificat à partir du chemin C:\Cisco\CVP\conf\security\wsm.crt à partir de chaque serveur et renommez-le wsmX.crt en fonction du type de serveur.

Étape 2. Importez des certificats WSM à partir du serveur CVP et du serveur de rapports dans le serveur OAMP.

(i) Copiez chaque certificat WSM du serveur CVP et du serveur Reporting (wsmX.crt) dans le répertoire C:\Cisco\CVP\conf\security du serveur OAMP.

(ii) Importez ces certificats avec la commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmcsX.crt
```

(iii) Redémarrer le serveur.

Étape 3. Importez le certificat WSM du serveur OAMP CVP dans les serveurs CVP Server et Reporting.

(i) Copiez le certificat WSM du serveur OAMP (wsmoampX.crt) dans le répertoire C:\Cisco\CVP\conf\security sur tous les serveurs CVP et Reporting.

(ii) Importez les certificats avec la commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmoampX.crt
```

(iii) Redémarrer les serveurs.

Section 2 : Échange de certificats entre le serveur OAMP CVP et les applications de la plateforme VOS.

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter le certificat d'application à partir de la plate-forme VOS.

Étape 2. Importez le certificat d'application VOS dans le serveur OAMP.

Étape 1. Exporter le certificat d'application à partir de la plate-forme VOS.

(i) Accédez à la page Cisco Unified Communications Operating System Administration : <u>https://FQDN:8443/cmplatform</u>.

(ii) Accédez à **Security > Certificate Management** et recherchez les certificats du serveur principal de l'application dans le dossier tomcat-trust.

| Certificate L | M | | | | |
|-----------------|--|--------|-----|---|---|
| Connector | Bell agreed 🖓 Epited California California daan 👔 Calemate | CRM | | | |
| | | signed | | | |
| formation and | Wants Primery Red. CL - 22 | mpred | *** | Banks, Privacy, Red., 64, - , 63 | thanks_Primary_Real_CitCit |
| tomosh trust | GitteSot | Self- | 90 | GobySon | GoldSign |
| SHOPFINE. | III Cardination Carbo Root Ch | Saf- | 834 | HE_Detification_Dentre_Root_DA | BE_Cartification_Cantre_Root_CA |
| termosit-trust | Gistelline April CA | Self. | 854 | Gibbe Sign_Root_CA | Gob#Sgs_Root_Ck |
| SHOPFIE | THEN NOT CAREFULATION Authority | Safe. | 854 | TwCA_Root_Carlification_Authority | TWCA, Root, Cartification, Authority |
| formula in well | Burness Circs 3 Acet Ci. | Extr. | 854 | Buyyona, Cleve, 3, Juni, Cl. | Bargeres_Cleve_3_Revi_Cli |
| tomost-trust | Staffeld Services Root Catillooks Authority - 62 | Sall- | 854 | Starfield, Services, Root, Certificate, Authority, -, ED | Stafeld, Service, Asth, Cetholox, Authority, -, 52 |
| Small Fruit | Verbie: Case 3 Male Privary Celification Authority - | Bell- | 434 | Willigh, Class, J., Addis, Primary, Certification, Authority, 1 | Verilige_Dass_3_Public_Primary_Detrification_Authority_ |
| towood-trust | vitul5.bea.com | Self. | 854 | mattin burn com | with 125, how.com |
| School Full | stars total factoria suffare | 147 | 104 | reary_state_conten_waterby | XRang_Stiller_CellStortur_Authority |

(iii) Sélectionnez le certificat et cliquez sur télécharger le fichier .PEM pour l'enregistrer dans un dossier temporaire sur le serveur OAMP.

| - Status | | | | | | | |
|--|--|---|--|--|--|--|--|
| (i) Statu | is: Ready | | | | | | |
| - Certificat | e Settings | | | | | | |
| File Name | | vvb125.bora.com.pem | | | | | |
| Certificate | Purpose | tomcat-trust | | | | | |
| Certificate | Certificate Type trust-certs | | | | | | |
| Certificate | Certificate Group product-cpi | | | | | | |
| Descriptio | n(friendly name) | Trust Certificate | | | | | |
| Version: Serial N Signatur Issuer N Validity To Subject Key RS Key va 3082010a 9fe42726 7096e810 | V3 umber: 68FE55F reAlgorithm: SHI lame: L=rtp, ST From: Thu Dec (0 Name: L=rtp, S' A (1.2.840.1135 lue: s0282010100f16 c826e36113207 165bdcd0cadbcb | 6F863110B44D835B825D84D3 256withR5A (1.2.840.113549.1.1.11) nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US 06:51:10 PST 2019 :S1:09 PST 2024 =nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US 9.1.1.1) 44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb 187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065 d1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c | | | | | |
| a911095cr/dbc9c9e2/09010/61052rdb288/dr0b2db78d2449cr529fcr/561cf1b042345358f25009e c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00daccd81013bd693614684c27e05de2004553004 | | | | | | | |
| Delete | Download .PEM | File Download .DER File | | | | | |

Étape 2. Importez le certificat d'application VOS dans le serveur OAMP.

(i) Copiez le certificat C VVB dans le répertoire C:\Cisco\CVP\conf\security sur le serveur OAMP.

(ii) Importez les certificats avec la commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -alias {fqdn_of_vos} -file c:\cisco\cvp\conf\security\vvb.pem
```

(ii) Redémarrer le serveur.

Section 3 : Échange de certificats entre le serveur CVP et les serveurs CVB.

Cette étape est facultative pour sécuriser la communication SIP et HTTP entre les serveurs CVB et CVP. Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter le certificat d'application CVB à partir de la plate-forme VOS.

Étape 2. Importez le certificat d'application vos dans les serveurs CVP.

Étape 3 : Exporter le certificat callserver et vxml des serveurs CVP.

Étape 4 : Importer le certificat callserver et vxml dans les serveurs CVB.

Étape 1. Exporter le certificat d'application à partir de la plate-forme vos.

(i) Suivez les mêmes étapes que celles indiquées à l'étape 1 de la section 2 pour les serveurs CVB.

Étape 2. Importer le certificat d'application VOS dans le serveur CVP.

(i) Suivez les mêmes étapes que celles indiquées à l'étape 2 de la section 2 sur tous les serveurs CVP.

Étape 3 : Exporter les certificats callserver et vxml des serveurs CVP

(i) Exportez le serveur d'appels et le certificat vxml de chaque serveur CVP vers un emplacement temporaire et renommez le certificat avec le nom souhaité. Vous pouvez le renommer callserverX.crt \ vxmlX.crt Replace X avec un numéro ou une lettre unique.

Commande d'exportation des certificats auto-signés :

```
Callserver certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\.keystore -export -alias callserver_certificate -file
%CVP_HOME%\conf\security\callserverX.crt
Vxml certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\.keystore -export -alias vxml_certificate -file
%CVP_HOME%\conf\security\vxmlX.crt
```

(ii) Copiez le certificat à partir du chemin C:\Cisco\CVP\conf\security\wsm.crt depuis chaque serveur et renommez-le callserverX.crt \ vxmlX.crt en fonction du type de certificat.

Étape 4 : Importer le certificat callserver et vxml dans les serveurs CVB.

(i) Accédez à la page Cisco Unified Communications Operating System Administration : <u>https://FQDN:8443/cmplatform</u>.

(ii) Naviguez jusqu'à Security > Certificate Management et sélectionnez option upload Certificate/Certificate chain.



(iii) Dans la chaîne de certificat/certificat de téléchargement, sélectionnez le champ d'objet du certificat tomcat-trust et téléchargez les certificats exportés comme indiqué à l'étape 3.

| Upload Certificate/Certificate chain | | | | | | |
|---|----------------------------|--|--|--|--|--|
| Deload 🖳 Close | | | | | | |
| -Status Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster -Upload Certificate/Certificate chain | | | | | | |
| Certificate Purpose* | tomcat-trust | | | | | |
| Description(friendly name) | | | | | | |
| Upload File | Choose File No file chosen | | | | | |
| | | | | | | |
| Upload Close | | | | | | |

(iv) Redémarrer le serveur.

CVP CallStudio WEBService Integration

Pour plus d'informations sur la façon d'établir une communication sécurisée pour l'élément Web Services et l'élément Rest_Client

reportez-vous au <u>Guide de l'utilisateur pour Cisco Unified CVP VXML Server et Cisco Unified Call</u> <u>Studio version 12.5(1) - Web Service Integration [Cisco Unified Customer Voice Portal] - Cisco</u>

Informations connexes

- Guide de configuration du CVP : Guide de configuration CVP Sécurité
- Guide de configuration UCCE : <u>Guide de configuration UCCE Sécurité</u>
- Guide d'administration de PCCE : <u>Guide d'administration PCE Sécurité</u>
- Certificats UCCE auto-signés : certificats autosignés Exchange UCCE
- Certificats auto-signés PCCE : <u>Certificats autosignés Exchange PCCE</u>
- Installer et migrer vers OpenJDK dans CCE 12.5(1) : Migration CCE OpenJDK
- Installer et migrer vers OpenJDK dans CVP 12.5(1) : <u>Migration CVP OpenJDK</u>

Support et documentation techniques - Cisco Systems