Tauschen Sie selbstsignierte Zertifikate in einer UCCE-Lösung aus.

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrund Vorgehensweise CCE AW-Server und CCE Core-Anwendungsserver Abschnitt 1: Zertifikataustausch zwischen Router\Logger, PG und AW-Server. Abschnitt 2: Zertifikataustausch zwischen VOS-Plattformanwendungen und AW-Server. **CVP-OAMP-Server und CVP-Komponentenserver** Abschnitt 1: Zertifikataustausch zwischen CVP OAMP-Server und CVP-Server und Reporting-Servern. Abschnitt 2: Zertifikataustausch zwischen CVP OAMP-Server und VOS-Plattformanwendungen. Abschnitt 3: Zertifikataustausch zwischen CVP-Server und CVVB-Servern. **CVP CallStudio-WEBService-Integration** Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt den Austausch selbstsignierter Zertifikate in der Unified Contact Center Enterprise (UCCE)-Lösung.

Unterstützt von Anuj Bhatia, Robert Rogier und Ramiro Amaya, Cisco TAC Engineers

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- UCCE-Version 12.5(1)
- Customer Voice Portal (CVP) Version 12.5 (1)
- Cisco Virtualized Voice Browser (VVB)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

• UCCE 12.5(1)

- CVP 12.5(1)
- Cisco VVB 12,5
- CVP Operations Console (OAMP)
- CVP New OAMP (NOAMP)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrund

Bei der UCCE-Lösung erfolgt die Konfiguration neuer Funktionen, die Kernanwendungen umfassen, wie z. B. Roggers (PG), Admin Workstations (AW), Finesse, Cisco Unified Intelligent Center (CUIC) usw., über die Administratorseite von Contact Center Enterprise (CCE). Für Interactive Voice Response (IVR)-Anwendungen wie CVP, Cisco VVB und Gateways steuert NOAMP die Konfiguration neuer Funktionen. Aus CCE 12.5(1) erfolgt aufgrund von Security-Management-Compliance (SRC) die gesamte Kommunikation mit CCE admin und NOAMP ausschließlich über ein sicheres HTTP-Protokoll.

Um eine nahtlose sichere Kommunikation zwischen diesen Anwendungen in einer selbstsignierten Zertifikatsumgebung zu erreichen, wird der Austausch dieser Zertifikate zwischen den Servern zum Muss. Im nächsten Abschnitt werden die Schritte für den Austausch eines selbstsignierten Zertifikats zwischen den folgenden Elementen ausführlich erläutert:

- CCE AW-Server und CCE Core-Anwendungsserver
- CVP OAMP-Server- und CVP-Komponenten-Server

Vorgehensweise

CCE AW-Server und CCE Core-Anwendungsserver

Dies sind die Komponenten, aus denen selbstsignierte Zertifikate exportiert werden, und die Komponenten, in die selbstsignierte Zertifikate importiert werden müssen.

CCE AW-Server: Für diesen Server ist ein Zertifikat von erforderlich:

• Windows-Plattform: Router and Logger(Rogger){A/B}, Peripheral Gateway (PG){A/B}, alle AW/ADS- und E-Mail- und Chat-Server (ECE).

Anmerkung: IIS- und Diagnostic-Framework-Zertifikate werden benötigt.

 VOS-Plattform: Cisco Unified Call Manager (CUCM), Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect und andere relevante Server, die Teil der Bestandsdatenbank sind.

Gleiches gilt für andere AW-Server in der Lösung.

Router \ Logger-Server: Für diesen Server ist ein Zertifikat von erforderlich:

• Windows-Plattform: Alle AW-Server IIS-Zertifikate.

Die Schritte für den effektiven Austausch der selbstsignierten Zertifikate für CCE sind in diese Abschnitte unterteilt.

Abschnitt 1: Zertifikataustausch zwischen Router\Logger, PG und AW-Server. Abschnitt 2: Zertifikataustausch zwischen VOS-Plattformanwendung und AW-Server.

Abschnitt 1: Zertifikataustausch zwischen Router\Logger, PG und AW-Server.

Um diesen Austausch erfolgreich abzuschließen, müssen folgende Schritte ausgeführt werden:

Schritt 1: Exportieren Sie IIS-Zertifikate von Router\Logger,PG und allen AW-Servern. Schritt 2: Exportieren von DFP-Zertifikaten (Diagnostic Framework Portico) von Router\Loggerund PG-Servern.

Schritt 3: Importieren Sie IIS- und DFP-Zertifikate von Router\Logger, PG auf AW-Server. Schritt 4: Importieren Sie das IIS-Zertifikat von den AW-Servern in Router\Logger.

Vorsicht: Bevor Sie beginnen, müssen Sie den Keystore sichern und die Befehle von der Java-Startseite aus als Administrator ausführen.

(i) Kennen Sie den Java-Home-Pfad, um sicherzustellen, wo das Java-Schlüsselprogramm gehostet wird. Es gibt mehrere Möglichkeiten, den Java-Heim-Pfad zu finden.

Option 1: CLI-Befehl: echo %JAVA_HOME%



Option 2: Manuell über die Systemeinstellung "Erweitert", wie im Bild gezeigt



Anmerkung: Auf UCCE 12.5 lautet der Standardpfad C:\Program Dateien (x86)\Java\jre1.8.0_221\bin. Wenn Sie jedoch den 12.5(1a) Installer verwendet haben oder 12.5 ES55 installiert haben (obligatorisches OpenJDK ES), dann verwenden Sie CCE_JAVA_HOME anstelle von JAVA_HOME, da sich der Datenspeicherpfad mit OpenJDK geändert hat. Weitere Informationen zur OpenJDK-Migration in CCE und CVP finden Sie in diesen Dokumenten: Installation und Migration zu OpenJDK in CCE 2.5(1) und Installation und Migration zu OpenJDK in CVP 12.5(1).

(ii) Sichern Sie die Aktwaredatei aus dem Ordner C:\Program Dateien (x86)\Java\jre1.8.0_221\lib\security. Sie können es an einen anderen Speicherort kopieren.

(iii) Öffnen Sie ein Befehlsfenster als Administrator, um die Befehle auszuführen.

Schritt 1: Exportieren Sie IIS-Zertifikate von Router\Logger, PG und allen AW-Servern.

(i) Navigieren Sie auf dem AW-Server von einem Browser zu den Servern (Roggers , PG , andere AW-Server) url: https://{servername}.

CCE via Chrome Browser

←	\rightarrow G	A Not see	ture aw125a.bora	.com				
Cene Shoi	rtificate ral Details w: <all> eld Version Serial numbi Signature hi Signature hi Suprature hi Suprature</all>	Certification Pa er Igorithm ash algorithm	th Value V3 00 a9 ab b9 bc 76 4b sha256RSA sha256 aw 125a.bora.com Monday, September Sunday, September aw 125a.bora.com	x 76 8f	d d def	÷	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) DER encoded X.509 (.CER) DER 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 Export all extended properties 	
			Edit Properties	Copy to File			Microsoft Serialized Certificate Store (.SST)	

(ii) Speichern Sie das Zertifikat in einem temporären Ordner, z. B. c:\temp\certs, und nennen Sie das Zertifikat als ICM{svr}[ab].cer.

Hinweis: Wählen Sie die Option Base-64-codierte X.509 (.CER) aus.

Schritt 2: Exportieren von DFP-Zertifikaten (Diagnostic Framework Portico) von Router\Loggerund PG-Servern.

(i) Öffnen Sie auf dem AW-Server einen Browser, und navigieren Sie zu den Servern (Router, Logger oder Roggers, PGs) DFP url: https://{servername}:7890/icmdp/rest/DiagnosticPortal/GetProductVersion.

Portico via Chrome Browser



(ii) Speichern Sie das Zertifikat im Ordner "Beispiel c:\temp\certs" und nennen Sie das Zertifikat als dfp{svr}[ab].cer.

Anmerkung: Wählen Sie die Option Base-64-codiertes X.509 (.CER) aus.

Schritt 3: Importieren Sie IIS- und DFP-Zertifikate von Rogger, PG auf AW-Server.

Befehl zum Importieren der selbstsignierten IIS-Zertifikate in den AW-Server. Der Pfad zum Ausführen des Key-Tools: C:\Program Dateien (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

Anmerkung: Importieren Sie alle in alle AW-Server exportierten Serverzertifikate.

Befehl zum Importieren der selbstsignierten DFP-Zertifikate in AW-Server:

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

Anmerkung: Importieren Sie alle in alle AW-Server exportierten Serverzertifikate.

Starten Sie den Apache Tomcat-Dienst auf den AW-Servern neu.

Schritt 4: Importieren Sie das IIS-Zertifikat von den AW-Servern in Router\Logger.

Befehl zum Importieren der selbstsignierten IIS-Zertifikate in Rogger-Server:

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

Anmerkung: Importieren Sie alle AW IIS-Serverzertifikate, die in Rogger-A- und -B-Seiten exportiert werden.

Starten Sie den Apache Tomcat-Dienst auf den Rogger-Servern neu.

Abschnitt 2: Zertifikataustausch zwischen VOS-Plattformanwendungen und AW-Server.

Um diesen Austausch erfolgreich abzuschließen, müssen folgende Schritte ausgeführt werden:

Schritt 1: Exportieren von Zertifikaten für den Anwendungsserver der VOS-Plattform Schritt 2: Importieren von VOS-Plattform-Anwendungszertifikaten in einen AW-Server.

Dieser Prozess gilt für alle VOS-Anwendungen, z. B.:

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

Schritt 1: Exportieren von Zertifikaten für den Anwendungsserver der VOS-Plattform

(i) Navigieren Sie zur Seite "Cisco Unified Communications Operating System Administration" (Verwaltung des Cisco Unified Communications-Betriebssystems): <u>https://FQDN:8443/cmplatform</u>

(ii) Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**, und suchen Sie die primären Serverzertifikate der Anwendung im Ordner tomcat-trust.

click, Cisco Unified Operating System Admin For Case Wolfed Communications Industry	istrat	ion		Analyzation Class Unified 05 Administration • Class administration About Logic	
Draw + Settings + Security + Schwarz Lagrantes + Services + Help +					
Cretificate List					
💫 lanana belapat 🐴 spise (withole Cellule can 🖳 lanana					
torest-trust Case 202 Rest CA	Sel-	80	Care, #CC, Red, CA	Core, NCC_Root_CA	
toreshipset. Indiana Academic and Research Institutions Root54, 2011	Sel-	854	relevalues, and lasers, Instatution, Inst52,202	Referic, Audenic, and Jasen M. Jost Mark	
tomost-trust (1572 Villetier, State) Book GB CA	Self-	854	01571E_WCSeriev_Ghibel_Rook_GB_CA	01578_WSeries_Gistel_Root_08_C4	
tomost-trust Amazon Root CA. 4	Sel-	ec.	Amazon_Root_CA_4	Amazon, Root, CA, 4	
tomosi trust <u>257 Fast CK X2</u>	Sel-	854	057_Awt_C4_x3	051_Roid_CA_X3	
tomonithat <u>Addhuit Donnal CA Ros</u>	Self-	854	AddTsat_Enternal_CA_Root	AddTruit_Diterral_Ck_Rolt	
tenantus <u>colocium</u>	Self-	83.4	man and an	cop.bore.com	
tancat trust <u>Effecting Strategict Case 3</u>	ball.	83.4	Ffeidec_StateRost_Cauc_3	Preside Content of Case 3	
torical-built <u>DeCet Ostal Rolt 62</u>	Self-	63.0	DipCet_Dobs_Rost_02	DigiCelt_States_Root_52	

(iii) Wählen Sie das Zertifikat aus, und klicken Sie auf .PEM-Datei herunterladen, um es in einem temporären Ordner auf dem AW-Server zu speichern.

Ella Manaa	are here even even
rile Name	ccp.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly na	ame) Trust Certificate
Certificate File Data	
1	
Version: V3	
Coniel Humbers CON	
Serial Number: 5C3	5B3A89A8974719B885B6A92CF710D
SignatureAlgorithm:	5B3A89A8974719B885B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11)
Senai Number: SC3: SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon f	5B3A89A8974719B885B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
Senal Number: SC3: SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon (To: Sat Dec	5B3A89A8974719B885B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 0ec 16 10:55:21 EST 2019
Serial Number: 5C3 SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon (To: Sat Dec Subject Name: L=B)	5B3A89A8974719B885B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 14 10:55:21 EST 2024 (B, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
Serial Number: SC3 SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon (To: Sat Dec Subject Name: L=B) Key: RSA (1.2.840.1	SB3A89A8974719BB85B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 14 10:55:21 EST 2024 (B, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US (13549.1.1.1)
Serial Number: SC3 SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon (To: Sat Dec Subject Name: L=B) Key: RSA (1.2.840.1 Key value:	SB3A89A8974719BB85B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 14 10:55:21 EST 2024 (B, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 13549.1.1.1)
Serial Number: SC3 SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon (To: Sat Dec Subject Name: L=B) Key: RSA (1.2.840.1 Key value: 3082010a028201010	SB3A89A8974719BB85B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 14 10:55:21 EST 2024 (B, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US (13549.1.1.1) Dc1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199
Serial Number: SC3: SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon (To: Sat Dec Subject Name: L=B) Key: RSA (1.2.840.1 Key value: 3082010a028201010 69f9980a1246814bes	SB3A89A8974719BB85B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 14 10:55:21 EST 2024 (8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 13549.1.1.1) Dc1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 133c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 133c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992
Seral Number: 5C3 SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon (To: Sat Dec Subject Name: L=B) Key: RSA (1.2.840.1 Key value: 3082010a028201010 69f9980a1246814be5 88e0e816e64ad44c3 f140216a5e5aca1f28	SB3A89A8974719BB85B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 14 10:55:21 EST 2024 (8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 113549.1.1.1) Dc1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 133c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 19f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 1914f382b0a11e2160e2d0002368ba852962bb9c7a1723c447aceb2a651b6f
Senal Number: 5C3: SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon U To: Sat Dec Subject Name: L=BX Key: RSA (1.2.840.1 Key value: 3082010a028201010 69f9980a1246814be9 88e0e816e64ad44c3 f140216a5e5aca1f78 520da30a39b206d21	SB3A89A8974719BB85B6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 14 10:55:21 EST 2024 (B, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 113549.1.1.1) 0c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 va3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 19f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 19f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722 19f04f887b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f 3b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
Seral Number: SC3 SignatureAlgorithm: Issuer Name: L=BXI Validity From: Mon (To: Sat Dec Subject Name: L=B) Key: RSA (1.2.840.1 Key value: 3082010a028201010 69f9980a1246814be5 88e0e816e64ad444c3 f140216a5e5aca1f78 520da30a39b206d21;	SB3A89A8974719B88SB6A92CF710D SHA256withRSA (1.2.840.113549.1.1.11) 8, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US Dec 16 10:55:22 EST 2019 14 10:55:21 EST 2024 (B, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 13549.1.1.1) 0c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 la3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 19f03f62aadcbc08f591a960ef95eda7ba6b3e6e183a2fe8732252aee6abcfb722 7b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f 3b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a

Anmerkung: Führen Sie die gleichen Schritte für den Abonnenten aus.

Schritt 2: Importieren der VOS-Plattformanwendung in den AW-Server

Pfad zum Ausführen des Key-Tools: C:\Program Dateien (x86)\Java\jre1.8.0_221\bin

Befehl zum Importieren der selbstsignierten Zertifikate:

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

Starten Sie den Apache Tomcat-Dienst auf den AW-Servern neu.

Anmerkung: Führen Sie die gleiche Aufgabe auf anderen AW-Servern aus.

CVP-OAMP-Server und CVP-Komponentenserver

Dies sind die Komponenten, aus denen selbstsignierte Zertifikate exportiert werden, und die Komponenten, in die selbstsignierte Zertifikate importiert werden müssen.

(i) CVP OAMP-Server: Dieser Server benötigt ein Zertifikat von

- Windows-Plattform: Web Services Manager (WSM)-Zertifikat von CVP-Server und Reporting-Servern.
- VOS-Plattform: Integration von Cisco VB für Customer Virtual Agent (CVA), Cloud Connect-Server für die Integration von WebEx Experience Management (WXM).
- (ii) CVP-Server: Dieser Server benötigt ein Zertifikat von

- Windows-Plattform: WSM-Zertifikat vom OAMP-Server.
- VOS-Plattform: Cloud Connect-Server für die WXM-Integration, Cisco VVB-Server für sichere SIP- und HTTP-Kommunikation.
- (iii) CVP-Reporting-Server: Dieser Server benötigt ein Zertifikat von
 - Windows-Plattform: WSM-Zertifikat vom OAMP-Server.

(iv) Cisco VVB-Server: Dieser Server benötigt ein Zertifikat von

• Windows-Plattform: CVP-Server VXML (sicheres HTTP), CVP-Server-Callserver (sicheres SIP)

Die Schritte, die für den effektiven Austausch der selbstsignierten Zertifikate in der CVP-Umgebung erforderlich sind, werden in diesen drei Abschnitten erläutert.

Abschnitt 1: Zertifikataustausch zwischen CVP OAMP-Server und CVP-Server und Reporting-Servern.

Abschnitt 2: Zertifikataustausch zwischen CVP OAMP-Server und VOS-Plattformanwendungen. Abschnitt 3: Zertifikataustausch zwischen CVP-Server und VVB-Servern.

Abschnitt 1: Zertifikataustausch zwischen CVP OAMP-Server und CVP-Server und Reporting-Servern.

Um diesen Austausch erfolgreich abzuschließen, müssen folgende Schritte ausgeführt werden:

Schritt 1: WSM-Zertifikat vom CVP-Server, Reporting und OAMP-Server exportieren.

Schritt 2: Importieren von WSM-Zertifikaten vom CVP-Server und Reporting-Server in den OAMP-Server

Schritt 3: Importieren des CVP OAMP-Server-WSM-Zertifikats in CVP-Server und Reporting-Server.

Vorsicht: Bevor Sie beginnen, müssen Sie Folgendes tun:

1. Rufen Sie das Keystore-Kennwort ab. Führen Sie den Befehl aus: mehr

- %CVP_HOME%\conf\security.properties
- 2. Kopieren Sie den Ordner %CVP_HOME%\conf\security in einen anderen Ordner.
- 3. Öffnen Sie ein Befehlsfenster als Administrator, um die Befehle auszuführen.

Schritt 1: WSM-Zertifikat vom CVP-Server, Reporting und OAMP-Server exportieren.

(i) Exportieren Sie das WSM-Zertifikat von jedem CVP-Server an einen temporären Speicherort, und benennen Sie das Zertifikat mit einem gewünschten Namen um. Sie können es als wsmX.crt umbenennen. Ersetzen Sie X durch eine eindeutige Nummer oder einen Buchstaben. Beispiel: wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

Befehl zum Exportieren der selbstsignierten Zertifikate:

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

(ii) Kopieren Sie das Zertifikat aus dem Pfad C:\Cisco\CVP\conf\security\wsm.crt von jedem Server und benennen Sie es je nach Servertyp als wsmX.crt um.

Schritt 2: Importieren von WSM-Zertifikaten vom CVP-Server und Reporting-Server in den OAMP-Server

(i) Kopieren Sie alle CVP-Server- und Reporting-Server-WSM-Zertifikate (wsmX.crt) in das Verzeichnis C:\Cisco\CVP\conf\security auf dem OAMP-Server.

(ii) Importieren Sie diese Zertifikate mit folgendem Befehl:

%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) Starten Sie den Server neu.

Schritt 3: Importieren des CVP OAMP-Server-WSM-Zertifikats in CVP-Server und Reporting-Server.

(i) Kopieren Sie das OAMP-Server-WSM-Zertifikat (wsmoampX.crt) in das Verzeichnis C:\Cisco\CVP\conf\security auf allen CVP-Servern und Reporting-Servern.

ii) Importieren Sie die Zertifikate mit dem Befehl:

```
%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) Starten Sie die Server neu.

Abschnitt 2: Zertifikataustausch zwischen CVP OAMP-Server und VOS-Plattformanwendungen.

Um diesen Austausch erfolgreich abzuschließen, müssen folgende Schritte ausgeführt werden:

Schritt 1: Exportieren des Anwendungszertifikats von der VOS-Plattform

Schritt 2: Importieren des VOS-Anwendungszertifikats in den OAMP-Server

Schritt 1: Exportieren des Anwendungszertifikats von der VOS-Plattform

(i) Navigieren Sie zur Seite "Cisco Unified Communications Operating System Administration" (Verwaltung des Cisco Unified Communications-Betriebssystems): <u>https://FQDN:8443/cmplatform</u>

(ii) Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**, und suchen Sie die primären Serverzertifikate der Anwendung im Ordner tomcat-trust.

section the						
Connete	Bell agreed 🐴 Epiteal Certificate Certificate state. 📳 Generate	CRM				
		signed				
Invested in well	Wards Trimery Test, CL - 22	mpred	***	Banks, Privacy, Red., 64, - , 63	theole_Primary_Bool_COCO	
tomost-trust	GlobalStot	Self-	90	GobySon	GobelSign	
SINCE FUE	III Definition Derive Real DA	Saf-	834	HE_Detification_Dentre_Root_DA	HI_CARTRONICA_CARTRO_ROAT_CA	
termosil thrush	GinterStore Apart, CA	Self.	854	Gibbe Sign_Root_CA	Gold/Spt_Root_Ck	
SHOPFINE	TWON NEW CARSFLEROW Authority	Safe.	REA	TwC4_Root_Cardification_Authority	TWO, Red, Genillation, Authority	
formula in well	Bornes, Cros. 3, Rol. Cl.	Extr.	854	Buyyona, Cleve, 3, Juni, Cl.	Bayees_Cless_3_Rest_E3	
tomost-trust	Staffeld Services Root Catillopia Authority - 62	Sall-	854	Starfield, Services, Root, CettRoote, Authority, -, ED	Stafield, Services, Rost, Certificate, Authority, -, 92	
Second trust	Verifier Class 2 Public Primary Certification Authority -	Bel-	434	Verilian Class 3, Adds, Primary, Cellification, Autority, -	Verifiqe, Dass, 3, Public, Primary, Dertification, Authority,	
tomost-trust	with 15 bern com	Salt.	RSA	mattill born com	with 125 how.com	
School Your.	many today destruction sufficiency	147	104	reary_state_conten_waterby	XRang_State_Carthonics_Authority	

(iii) Wählen Sie das Zertifikat aus, und klicken Sie auf .PEM-Datei herunterladen, um es in einem temporären Ordner auf dem OAMP-Server zu speichern.

Status —				-			
i Status: Ready							
Certificat	e Settings—			_			
File Name vvb125.bora.com.pem							
Certificate Purpose tomcat-trust							
Certificate Type trust-certs							
Certificate Group product-cpi							
Description(friendly name) Trust Certificate							
Signatur Issuer N Validity To Subject Key: RS Key va 30820100 9fe42726 7096e810	reAlgorithm: 5 lame: L=rtp, 5 From: Thu Dec 0 Name: L=rtp, A (1.2.840.11 lue: 0282010100f c826e361132 l65bdcd0cadb	HA256wit ST=nc, CN c 05 06:5 3 06:51:0 . ST=nc, C 3549.1.1. f16d44864 07d187db cbdd1df1c	thRSA (1.2.840.113549.1.1.11) wvvb125.bora.com, OU=lab, O=bora, C=US 1:10 PST 2019 9 PST 2024 N=vvb125.bora.com, OU=lab, O=bora, C=US 1) lbefb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb 01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065 d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c				
a911b95c c77de1da	17dbc9c9e270 40e15f1c0ae4	9d1d7610 40bc03dd8	b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e 815ceab5fc46a00daccd81013bd693614684c27e05de2004553004	1			
Delete	Download .	EM File	Download .DER File				

Schritt 2: Importieren des VOS-Anwendungszertifikats in den OAMP-Server

(i) Kopieren Sie das C VVB-Zertifikat in das Verzeichnis C:\Cisco\CVP\conf\security auf dem OAMP-Server.

ii) Importieren Sie die Zertifikate mit dem Befehl:

%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) Starten Sie den Server neu.

Abschnitt 3: Zertifikataustausch zwischen CVP-Server und CVVB-Servern.

Dies ist ein optionaler Schritt zum Sichern der SIP- und HTTP-Kommunikation zwischen den CVVB- und CVP-Servern. Um diesen Austausch erfolgreich abzuschließen, müssen folgende Schritte ausgeführt werden:

- Schritt 1: Exportieren Sie das CVVB-Anwendungszertifikat von der VOS-Plattform.
- Schritt 2: Importieren Sie das vos-Anwendungszertifikat in die CVP-Server.
- Schritt 3: Exportieren des Anrufservers und des VXML-Zertifikats von den CVP-Servern.
- Schritt 4: Importieren von Anrufserver- und VXML-Zertifikaten in CVVB-Server.

Schritt 1: Exportieren Sie das Anwendungszertifikat von der vos-Plattform.

(i) Befolgen Sie für CVVB-Server die gleichen Heftklammern wie in Abschnitt 2 Schritt 1 angegeben.

Schritt 2: Importieren des VOS-Anwendungszertifikats in den CVP-Server

(i) Befolgen Sie auf allen CVP-Servern die gleichen Schritte wie in Schritt 2 von Abschnitt 2 beschrieben.

Schritt 3: Anrufserver und VXML-Zertifikat von CVP-Servern exportieren

(i) Exportieren von Anrufservern und VXML-Zertifikaten von jedem CVP-Server an einen temporären Speicherort und Umbenennen des Zertifikats mit einem gewünschten Namen. Sie können es als callserverX.crt \ vxmlX.crt Replace X durch eine eindeutige Zahl oder einen Buchstaben umbenennen.

Befehl zum Exportieren der selbstsignierten Zertifikate:

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) Kopieren Sie das Zertifikat aus dem Pfad C:\Cisco\CVP\conf\security\wsm.crt von jedem Server und benennen Sie es basierend auf dem Zertifikatstyp als callserverX.crt \ vxmlX.crt um.

Schritt 4: Importieren von Anrufserver- und VXML-Zertifikaten in CVVB-Server.

(i) Navigieren Sie zur Seite "Cisco Unified Communications Operating System Administration" (Verwaltung des Cisco Unified Communications-Betriebssystems): <u>https://FQDN:8443/cmplatform</u>

(ii) Navigieren Sie zu Sicherheit > Zertifikatsverwaltung, und wählen Sie die Option Zertifikat/Zertifikatskette hochladen aus.



(iii) Wählen Sie auf dem Upload-Zertifikat/der Zertifikatskette "tomcat trust" im Zertifikatszweckfeld

aus, und laden Sie die exportierten Zertifikate gemäß Schritt 3 hoch.

Jpload Certificate/Certificate chain								
Dpload 🖳 Close								
Status								
Warning: Uploading a	Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster							
- Unload Certificate/Certi	ficate chain-							
opidad Certificate/Certi								
Certificate Purpose*	Certificate Purpose tomcat-trust							
Description(friendly name)								
Upload File Choose File No file chosen								
Usland Mars								
Upicad Close								

(iv) Starten Sie den Server neu.

CVP CallStudio-WEBService-Integration

Ausführliche Informationen zum Herstellen einer sicheren Kommunikation für Webdienstelement und REST_Client-Element

Weitere Informationen finden Sie im <u>Benutzerhandbuch für Cisco Unified CVP VXML Server und</u> <u>Cisco Unified Call Studio Release 12.5(1) - Web Service Integration [Cisco Unified Customer</u> <u>Voice Portal] - Cisco</u>

Zugehörige Informationen

- CVP-Konfigurationsleitfaden: CVP-Konfigurationsleitfaden Sicherheit
- UCCE-Konfigurationsleitfaden: UCCE-Konfigurationsleitfaden Sicherheit
- PCCE-Administrationsleitfaden: PCE-Administratorhandbuch Sicherheit
- Selbstsignierte UCCE-Zertifikate: Tauschen Sie selbstsignierte UCCE-Zertifikate aus.
- Selbstsignierte PCCE-Zertifikate: <u>Tauschen Sie selbstsignierte PCCE-Zertifikate aus.</u>
- Installation und Migration zu OpenJDK in CCE 12.5(1): <u>CCE OpenJDK-Migration</u>
- Installation und Migration zu OpenJDK in CVP 12.5(1): <u>CVP OpenJDK Migration</u>

Technischer Support und Dokumentation für Cisco Systeme