Selbstsignierte Zertifikate in einer UCCE 12.6-Lösung austauschen

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Vorgehensweise CCE AW-Server und CCE Core-Anwendungsserver Abschnitt 1: Zertifikataustausch zwischen Router\Logger, PG und AW-Server Abschnitt 2: Zertifikataustausch zwischen NOS-Plattformanwendungen und AW-Server CVP OAMP-Server und CVP-Komponentenserver Abschnitt 1: Zertifikataustausch zwischen CVP OAMP-Server und Reporting-Server Abschnitt 2: Zertifikataustausch zwischen CVP OAMP-Server und CVP-Server und Reporting-Server Abschnitt 2: Zertifikataustausch zwischen CVP OAMP-Server- und VOS-Plattformanwendungen Abschnitt 3: Zertifikataustausch zwischen CVP-Server- und VOS-Plattformanwendungen CVP CallStudio-Webdienstintegration ZugehörigeInformationen

Einleitung

In diesem Dokument wird der Austausch selbstsignierter Zertifikate in der Unified Contact Center Enterprise (UCCE)-Lösung beschrieben.

Voraussetzungen

Anforderungen

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

- UCCE-Version 12.6(2)
- Customer Voice Portal (CVP) Version 12.6(2)
- Cisco Virtualized Voice Browser (VB)

Verwendete Komponenten

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

- UCCE 12.6(2)
- CVP 12.6(2)
- Cisco VVB 12,6 (2)
- 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 kennen.

Hintergrundinformationen

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

Um eine nahtlose sichere Kommunikation zwischen diesen Anwendungen in einer selbstsignierten Zertifikatumgebung zu erreichen, ist der Austausch von Zertifikaten zwischen den Servern ein Muss. Im nächsten Abschnitt werden die erforderlichen Schritte für den Austausch selbstsignierter Zertifikate zwischen den folgenden Komponenten detailliert beschrieben:

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

Hinweis: Dieses Dokument bezieht sich NUR auf CCE-Version 12.6. Links zu anderen Versionen finden Sie im Abschnitt mit verwandten Informationen.

Vorgehensweise

CCE AW-Server und CCE Core-Anwendungsserver

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

CCE AW-Server: Dieser Server benötigt ein Zertifikat von:

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

Hinweis: IIS- und Diagnose-Framework-Zertifikate werden benötigt.

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

Dasselbe gilt für andere AW-Server in der Lösung.

Router \ Protokollierungsserver: Dieser Server benötigt ein Zertifikat von:

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

Die erforderlichen Schritte für einen effektiven Austausch der selbstsignierten Zertifikate gegen 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, sind folgende Schritte erforderlich:

Schritt 1: Exportieren Sie IIS-Zertifikate von Router\Logger ,PG und allen AW-Servern. Schritt 2: Exportieren Sie DFP-Zertifikate (Diagnostic Framework Portal) von Router\Logger- und PG-Servern. Schritt 3: Importieren Sie IIS- und DEP. Zertifikate von Router\Logger. PG auf AW-Server

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

Vorsicht: Bevor Sie beginnen, müssen Sie den Schlüsselspeicher sichern und die Befehle vom Java-Home als Administrator ausführen.

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

Option 1: CLI-Befehl: echo %CCE_JAVA_HOME%



Option 2: Manuell über die erweiterte Systemeinstellung, wie im Bild dargestellt

Control Danel Marrie	and y system and second y y system	-	
Control Panel Home	System Properties ×		
💔 Device Manager	Computer Name Hardware Advanced Remote		
Remote settings	You must be looped on as an Administrator to make most of these changes	Environment Variables	
Advanced system settings	Performance		
	Visual effects, processor scheduling, memory usage, and vitual memory	User variables for Administrator	1
		Variable	Value
	Settings	Path	C:\Users\Administrator\AppData\Lo
	User Profiles	TEMP	C:\Users\Administrator\AppData\Lo
	Desktop settings related to your sign-in	IMP	C:\Users\Administrator\AppData\Lo
	Settings	*	
	Statup and Recovery		
	System startup, system failure, and debugging information		
	System startup, system failure, and debugging information Settings	System variables	
	System startup, system failure, and debugging information Settings	System variables Variable	Value
	System startup, system failure, and debugging information Settings Environment Variables	System variables Variable CCE_JAVA_HOME	Value C:\Program Files (x86)\OpenJDK\jre
	System startup, system failure, and debugging information Settings Environment Variables	System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_ProfilerC.	Value C:\Program Files (x86)\OpenJDK\jre- EnableV2Profiler
	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProfilerC. COMSPEC	Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe
	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jret EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.ApentProfiler
	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI	Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1
	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProtilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 ApoDynamics.AgentProfiler
	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AooDynamics.AgentProfiler
	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jret EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 ApoDynamics.AgentProfiler
	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 ApoDvnamics.AgentProfiler
	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProfAPI_ProfilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 AppDynamics.AgentProfiler
See also	System startup, system failure, and debugging information Settings Environment Variables OK Cancel Apply	System variables Variable CCE_JAVA_HOME COMPLUS_ProtAPI_ProtilerC. ComSpec COR_ENABLE_PROFILING COR_PROFILER CORECLR_ENABLE_PROFILI CORECLR_PROFILER	Value C:\Program Files (x86)\OpenJDK\jre EnableV2Profiler C:\Windows\system32\cmd.exe 1 AppDynamics.AgentProfiler 1 ApoDvnamics.AgentProfiler

(ii) Sichern Sie die Datei cacerts aus dem Ordner <ICM install directory>ssl\. 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 einem AW-Server von einem Browser zu den Servern (Roggers, PG, andere AW-Server) url: https://{servername}.

General	Details Certificatio	on Path		🔶 🐓 Certificate Export Wizard
Show:	<all></all>	~		Export File Format
Field	sion ial number nature algorithm nature hash algorithr uer id from id to niect	Value V3 0091088279797a0660 sha256RSA m sha256 UCCE-AW.ccwebex.com Tuesday, February 21, 2 Monday, February 16, 20 UCCE-AW.ccwebey.com	023 4 043 4	Certificates can be exported in a variety of Select the format you want to use: DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) Cryptographic Message Syntax Sta Include all certificates in the cert Personal Information Exchange - Ph
				Delete the private key if the ex Export all extended properties

(ii) Speichern Sie das Zertifikat in einem temporären Ordner. Beispiel: c:\temp\certs und geben Sie dem Zertifikat den Namen ICM{svr}[ab].cer.

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

Schritt 2: Exportieren Sie DFP-Zertifikate (Diagnostic Framework Portal) von Router\Logger und PG-Servern.

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



(ii) Speichern Sie das Zertifikat im Ordner Beispiel c:\temp\certs, und geben Sie dem Zertifikat den Namen dfp{svr}[ab].cer

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

Schritt 3: IIS- und DFP-Zertifikat von Rogger, PG auf AW-Server importieren.

Befehl zum Importieren der selbstsignierten IIS-Zertifikate in den AW-Server. Der Pfad zum Ausführen des Schlüssel-Tools: C:\Program Dateien (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin:

%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS Example:%CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore

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

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

%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp{svr}[ab].cer -alias {fqdn_of_server}_DFF Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\dfpAWA.cer -alias AWA_DFP -keystore

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

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

Schritt 4: IIS-Zertifikat von AW-Servern in Router\Logger importieren

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

Hinweis: Importieren Sie alle AW IIS-Serverzertifikate, die in die Roger A- und B-Seiten exportiert wurden.

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, sind folgende Schritte erforderlich:

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

Dieser Prozess gilt für VOS-Anwendungen wie:

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

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

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

(ii) Navigieren Sie zu **Security > Certificate Management**, und suchen Sie im Ordner tomcat-trust nach den Zertifikaten des primären Anwendungsservers.

dude Cisco Unified Operating System Ad	ministrat	tion		Casa Unified OS Administration • G
For Cace Unified Communications Solutions				admandratur About Lopio
Shou * Settings * Security * Software Upproces * Services * me		-		
Certificate List				
🔒 Generals Self-agence 🍙 Upload Carthonis Carthonis share 🔒 Gan	erate CSR			
turnest-trust Case ECC Rest, CA	Sal- speed	60	Com, ECC, And, CA	Coox_BCC_Aset_CA
towark trust (palanic Academic and Research Institutions RootCA)	spred	854	Melanic, Academic, and Jassanch, Institutions, RootCA, 201	Heleric, Audenic, and Jassarch, Institution
tomost-trust OCSTE VICENEY, Stubel Root, GB CA	Salf- signed	854	0157E_WISexley_Globel_Root_GB_CA	ODITE_WEBHAY_GIVEN_Root_68_CA
tomcat-bruit Amazon Root CA.4	Self- squed	ec.	Amazon_Root_CA_4	Amazon_Root_CA_4
tomost-trust <u>DST_Rest_CA_X3</u>	Salf- signed	854	DST_AwA_CA_X3	DDT_RHH_CA_X3
towat-load Additud External CA Real	Self-	854	AddTrust_External_CA_Root	AddTrust_External_CA_Root
tumcat-trust <u>pos.lock.com</u>	Dath- signed	834	og-bork.com	esp.bora.com
toreat-tool <u>Tricine Gelalizet Case 3</u>	Self- signed	834	1-felder_GolalHoot_Class_3	T-feleler_Gobalkoot_Cass_3
tomosh-trust <u>DisiCert Global Rout G2</u>	Self-	854	DigiCert_Global_Root_G2	DipCert_Global_Root_G2

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

-Certificate Settings-	
File Name	ccp.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly na	me) Trust Certificate
-Certificate File Data -	
[Version: V3 Serial Number: 5C35 SignatureAlgorithm: Issuer Name: L=BXB Validity From: Mon D To: Sat Dec 1 Subject Name: L=BXX Key: RSA (1.2.840.1) Key value: 3082010a0282010100 69f9980a1246814be9 88e0e816e64ad44c3 140216se5aca1f787 520da30a39b206d213	B3A89A8974719BB85B6A92CF710D SH4255withRSA (1.2.840.113549.1.1.11) , ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US ec 16 10:55:22 EST 2019 4 10:55:21 EST 2024 B, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 13549.1.1.1) lc1420ced76c23b9d60b01efbf331987ac5524639ba8af3f3430d2ca8766d199 a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992 9f03f62aadcbc08f591a960ef95eda7886b3e6e183a2fe8732352aee6abcfb722 9f03f62aadcbc08f591a960ef95eda7886b3e6e183a2fe8732352aee6abcfb722 9f03f62aadcbc08f591a960def95eda7886b3e6e183a2fe8732352aee6abcfb722 9f03f62aadcbc08f591a960def95eda7886b3e6e183a2fe8732352aee6abcfb722 014f387b0a11e2160e2d000236ba852962b9cb741723c447ace2a651b6f b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
Delete Download .	PEM File Download .DER File

Hinweis: Führen Sie die gleichen Schritte für den Abonnenten durch.

Schritt 2: VOS-Plattformanwendung in AW-Server importieren

Pfad zum Ausführen des Schlüssel-Tools: C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

Befehl zum Importieren der selbstsignierten Zertifikate:

%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.pem -alias {fqdn_of_VOS} -ke Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\CUICPub.pem -alias CUICPub -keystop

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

Hinweis: 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 Komponenten, in die selbstsignierte Zertifikate importiert werden müssen.

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

- Windows-Plattform: WSM-Zertifikat (Web Services Manager) des CVP-Servers und der Reporting-Server.
- VOS-Plattform: Cisco VB und Cloud Connect-Server.

(ii) CVP-Server: Dieser Server benötigt ein Zertifikat von

- Windows-Plattform: WSM-Zertifikat vom OAMP-Server.
- VOS-Plattform: Cloud Connect-Server und Cisco VB-Server für die sichere SIP- und HTTP-Kommunikation.

(iii) CVP-Reporting-Server: Für diesen Server ist ein Zertifikat von

• Windows-Plattform: WSM-Zertifikat vom OAMP-Server.

(iv) Cisco VVB-Server: Für diesen Server ist ein Zertifikat von

- Windows-Plattform: CVP Server VXML (Secure HTTP), CVP Server Call Server (Secure SIP)
- VOS-Plattform: Cloud Connect-Server

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

Abschnitt 1: Zertifikataustausch zwischen CVP OAMP-Server und CVP-Server und Reporting-Server Abschnitt 2: Zertifikataustausch zwischen CVP OAMP-Server- und VOS-Plattformanwendungen Abschnitt 3: Zertifikataustausch zwischen CVP-Server- und VOS-Plattformanwendungen

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

Server

Um diesen Austausch erfolgreich abzuschließen, sind folgende Schritte erforderlich:

Schritt 1: WSM-Zertifikat vom CVP-Server, Reporting- und OAMP-Server exportieren. Schritt 2: Importieren Sie WSM-Zertifikate vom CVP-Server und vom Reporting-Server in den OAMP-Server.

Schritt 3: CVP OAMP-Server-WSM-Zertifikat in CVP-Server und Reporting-Server importieren.

Vorsicht: Bevor Sie beginnen, müssen Sie dies tun:

1. Öffnen Sie ein Befehlsfenster als Administrator.

2. Für 12.6.2 rufen Sie zur Identifizierung des Keystore-Kennworts den Ordner %CVP_HOME%\bin auf, und führen Sie die Datei DecryptKeystoreUtil.bat aus.

3. Für 12.6.1 führen Sie den Befehl, um das Schlüsselspeicherkennwort zu identifizieren, mehr %CVP_HOME%\conf\security.properties aus.

4. Sie benötigen dieses Kennwort, wenn Sie die Befehle keytool ausführen.

5. Führen Sie im Verzeichnis %CVP_HOME%\conf\security\ den Befehl copy .keystore backup.keystore aus.

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 um den gewünschten Namen. Sie können sie in wsmX.crt umbenennen. Ersetzen Sie X durch den Hostnamen des Servers. 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 -al

(ii) Kopieren Sie das Zertifikat aus dem Pfad %CVP_HOME%\conf\security\wsm.crt von jedem Server, und benennen Sie es je nach Servertyp in 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 %CVP_HOME%\conf\security auf dem OAMP-Server.

ii) diese Zertifikate mit dem folgenden Befehl importieren:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -a

(iii) Neustart des Servers.

Schritt 3: CVP OAMP-Server-WSM-Zertifikat in CVP-Server und Reporting-Server importieren.

(i) Kopieren Sie das WSM-Zertifikat des OAMP-Servers (wsmoampX.crt) in das Verzeichnis

%CVP_HOME%\conf\security auf allen CVP-Servern und Reporting-Servern.

ii) Importieren Sie die Zertifikate mit dem folgenden Befehl:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -a

(iii) Starten Sie die Server neu.

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

Um diesen Austausch erfolgreich abzuschließen, sind folgende Schritte erforderlich:

Schritt 1: Exportieren des Anwendungszertifikats von der VOS-Plattform

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

Dieser Prozess gilt für VOS-Anwendungen wie:

- CUCM
- VVB
- Cloud Connect

Schritt 1: Exportieren des Anwendungszertifikats von der VOS-Plattform

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

(ii) Navigieren Sie zu **Security > Certificate Management**, und suchen Sie im Ordner tomcat-trust nach den Zertifikaten des primären Anwendungsservers.

Certificate L					
Conversion	Self-signed 🐴 Upical CellifularCellifule chain 🔣 Generali	COR			
-		signed			
tomost-trust	thants Riman, Red. CA - 62	Sall-	RSA	Banks, himany, Rook, GA, 1, 63	thanks_Primary_Root_CA60
tomost-trust	Subalivo	Salf- signed	90	GlobalSign	GistalSign
tomost-trust	EE Certification Centre Asst. CA	Self-	RSA	EE_Certification_Centre_Root_CA	EE_Certification_Centre_Root_CA
tomost-trust	State Size, Reef, CA	Sall-	854	GlobalSign_Root_CA	Gobe/Sign_Root_CA
tomost-trust	TRCA And, Certification, Authority	Self- signed	RSA	TWCA_Root_Certification_Authority	TeCs_Root_Certification_Authority
tomost-trust	Burrana Casa 3 Root CA	Self- signed	RSA	boypeen_Ceen_3_Acot_GA	Bogees_Cen_3_Root_CA
tomost-trust	Darfield Bencies Root Certificate Authority - 52	Self-	R.DA	Darfeld_Services_Root_Certificate_Authority62	Starfald_Services_Root_Certificate_Authority02
tomost-trust	YejSon, Case 3. Addic Arinary, Settleaton, Autority, 1	545	854	YerSign_Class_3_hblic_Primary_Cartification_Authority	Verdign_Class_3_Public_Primary_Certification_Authority_
tomiat-trust	rok178.boox.com	Saf-	854	million location	while how com
Tomost-Invest	Shame Cole: Carofication Authority	1et-	854	skang_Dobs_Certification_Authority	XRamp_Distel_Certification_Authority

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

Certificate Settings File Name Certificate Purpose Certificate Type	vvb125.bora.com.pem
File Name Certificate Purpose Certificate Type	vvb125.bora.com.pem
Certificate Purpose Certificate Type	
Certificate Type	tomcat-trust
	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate
SignatureAlgorithm: SHA2 Issuer Name: L=rtp, ST=r Validity From: Thu Dec 05 To: Tue Dec 03 06 Subject Name: L=rtp, ST	256withRSA (1.2.840.113549.1.1.11) nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US i06:51:10 PST 2019 i:51:09 PST 2024 =nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2,840,11354 Key value: 3082010a0282010100f16d 9fe42726c826e36113207d; 7096e81d65bdcd0cadbcbdd 9911b95c7 dbc90e27b9d1 c77de1da40e15f1c0ae40bc	9.1.1.1) 44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb 187db01780d0d7b1b38462c7df7fa9f17e87e0408077b556ffc2c00065 41df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c .d761b52fdb2aa7df0b2db78d2449cf529fc7561cf1b042345358f25009e 03dd815ceab5fc46a00daccd81013bd693614684c27e05de2004553004

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

(i) Kopieren Sie das VOS-Zertifikat in das Verzeichnis %CVP_HOME%\conf\security auf dem OAMP-Server.

ii) Importieren Sie die Zertifikate mit dem folgenden Befehl:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -al

(ii) Starten Sie den Server neu.

Abschnitt 3: Zertifikataustausch zwischen CVP-Server- und VOS-Plattformanwendungen

Dies ist ein optionaler Schritt zum Sichern der SIP-Kommunikation zwischen CVP und anderen Contact Center-Komponenten. Weitere Informationen finden Sie im CVP-Konfigurationsleitfaden: <u>CVP-Konfigurationsleitfaden - Sicherheit</u>.

CVP CallStudio-Webdienstintegration

Ausführliche Informationen zum Einrichten einer sicheren Kommunikation für Web Services-Element und Rest_Client-Element

siehe Benutzerhandbuch für Cisco Unified CVP VXML-Server und Cisco Unified Call Studio Release 12.6(2) - Web Service Integration [Cisco Unified Customer Voice Portal] - Cisco

Zugehörige Informationen

- CVP-Konfigurationsleitfaden: <u>CVP-Konfigurationsleitfaden Sicherheit</u>
- UCCE-Konfigurationsleitfaden: UCCE-Sicherheitsleitfaden
- PCCE-Administrationshandbuch: PCCE-Administrationshandbuch
- Selbstsignierte PCCE-Zertifikate 12.6: Austausch selbstsignierter PCCE-Zertifikate
- Selbstsignierte PCCE-Zertifikate 12.5: Selbstsigniertes PCCE-Zertifikat 12.5

- UCCE-selbstsigniertes Zertifikat 12.5: <u>UCCE-selbstsignierte Zertifikate 12.5</u>
 CCE CA Signed Certicates 12.5: <u>CCE CA Signed Certicates 12.5</u>
 <u>Technischer Support und Dokumentation für Cisco Systeme</u>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.