CA-ondertekend certificaat in CVP-gespreksserver voor SIP-transportlaag (TLS) genereren

Inhoud

Inleiding

In dit document wordt beschreven hoe een CA-ondertekend certificaat voor de Call Server van Customer Voice Portal (CVP) moet worden gegenereerd en hoe het certificaat van de Call Server van het CVP moet worden geverifieerd. Van CVP versie 11.6 wordt de communicatie van Session Initiation Protocol (SIP) ondersteund.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CVP
- SIP

Gebruikte componenten

De informatie in dit document is gebaseerd op CVP 11.6.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Stap 1. Vind het wachtwoord voor het toetsenbord.

Navigeer naar **c:\Cisco\CVP\conf\security.properties in CVP call server om dit wachtwoord te vinden.**

Dit bestand bevat het wachtwoord voor het toetsenbord dat bij het gebruik van het toetsenbord vereist is.

Stap 2. Maak een tijdelijke variabele om te voorkomen dat telkens de waarde van het sleutelopslagwachtwoord wordt ingevoerd.

Navigeren naar **c:\Cisco\CVP\conf\security** en voer deze opdracht uit:

set kt=c:\Cisco\CVP\jre\bin\keytool.exe -storepass 592 (!aT@Hbt){[c)b7n6 {Mj6J[0P4C~X2?4!zv~5(@2*12DM97) -storetype JCEKS -keystore .keystore

> Opmerking: **De** opslag moet worden vervangen door uw eigen toetsenbord wachtwoord.

Stap 3. Verwijder het bestaande certificaat van de callserver.

Navigeer naar **c:\Cisco\CVP\conf\security** om het bestaande certificaat te vinden. Start deze opdracht om het certificaat te verwijderen:

%kt% -Delete -alias callserver_certificaat

Na het schrappen van het certificaat kan deze opdracht worden gebruikt om alle certificaten in de CVP-server te controleren:

%kt%-lijst

En om te bevestigen of het Call Server certificaat werd verwijderd, voert u deze opdracht uit:

%kt%-lijst | findstr-callserver

Stap 4. Generate the key pair. U moet 2048 bits paar gebruiken.

Navigeren naar **c:\Cisco\CVP\conf\security** en voer deze opdracht uit:

%kt% -genkeypair -alias callserver_certificaat -v-keysize 2048-keyalg RSA

Wanneer u deze opdracht uitvoert, vraagt deze informatie:

> Opmerking: U moet de hostname van de server als voornaam en achternaam gebruiken.

Wat is je voor- en achternaam?
[Onbekend]: col115cv02
Wat is de naam van uw organisatie?
[Onbekend]: TAC
Hoe heet je organisatie?
[Onbekend]: Cisco
Wat is de naam van je stad of omgeving?
[Onbekend]: Sydney
Wat is de naam van uw land of provincie?
[Onbekend]: NSW
Wat is de landcode van twee letters voor deze eenheid?
[Onbekend]: AU
Is CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU correct?
[neen]: ja

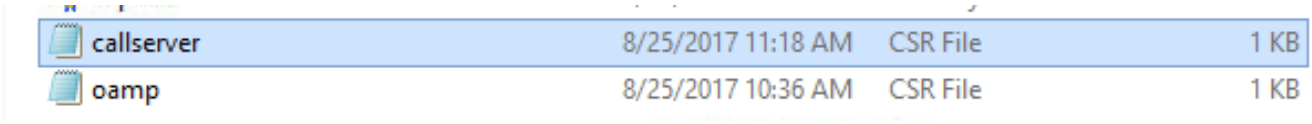
Stap 5. Generate de nieuwe certificaataanvraag (CSR).

Navigeren naar **c:\Cisco\CVP\conf\security** en voer deze opdracht uit:

%kt% -certreq -alias callserver_certificaat -file callserver.csr

Stap 6. Teken de CSR door interne CA of derde C.

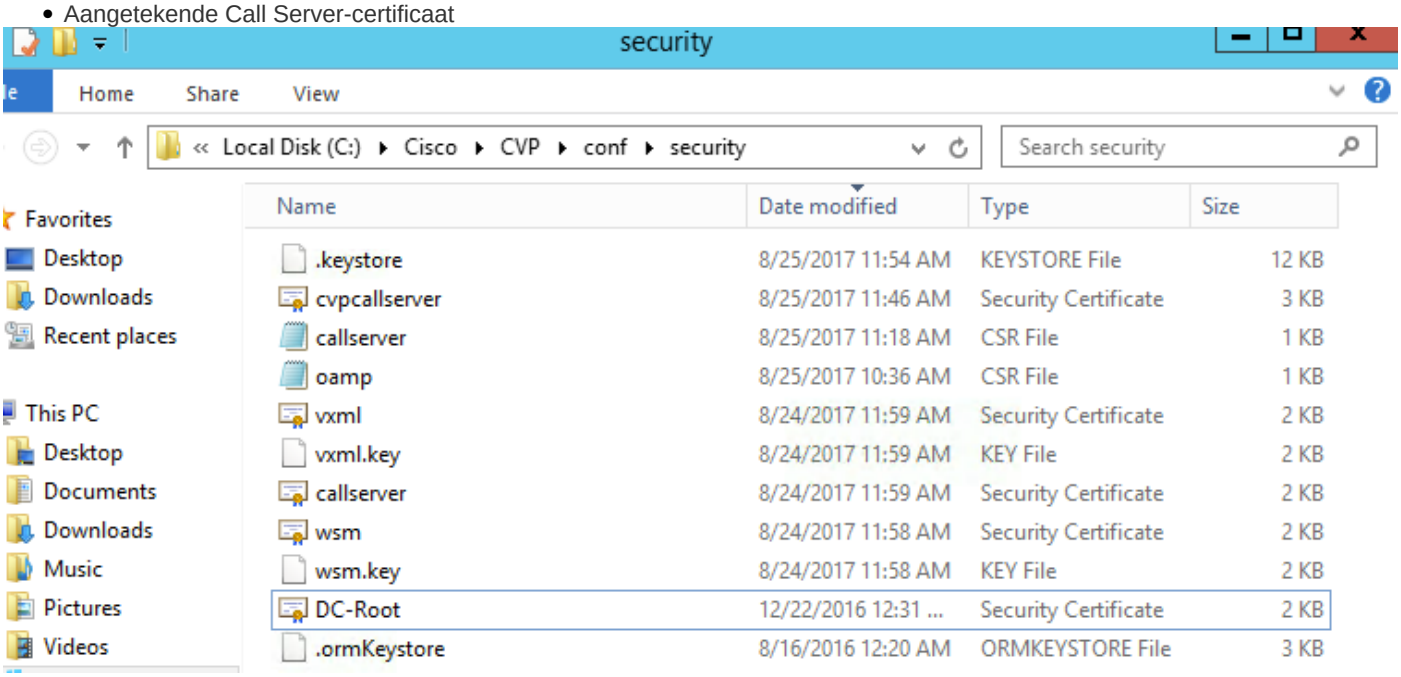
Navigeren naar **c:\Cisco\CVP\conf\security** om dit CSR-bestand te vinden:



Stap 7. Installeer de Root CA.

Twee certificaten worden gekopieerd naar **c:\Cisco\CVP\conf\security.**

- Root CA-certificaat
- Aangetekende Call Server-certificaat



Start deze opdracht:

%kt% -import -v-trustcacerts -alias root-file DC-Root.cer

In dit lab is de Root CA cert DC-Root.cer.

Stap 8. Installeer het Call Server-certificaat dat door CA is ondertekend.

Navigeren naar **c:\Cisco\CVP\conf\security**

Start deze opdracht:

%kt% -import -v -trustcacerts -alias callserver_certificaat -file cvpcallserver.cer
In dit laboratorium, is het certificaat van de vraagserver cvpcallserver.cer.

Stap 9. Controleer het nieuwe geïnstalleerde certificaat

Kijk op **C:\Cisco\CVP\conf\security** om het nieuwe geïnstalleerde certificaat te controleren
Start deze opdracht:

%kt% -list -v -alias callserver_certificaat Alias naam:callserver_certificaat

> Opmerking: Aliasnaam is een vaste systeemwaarde. Je moet callserver_certificaat gebruiken.

Voorbeeld:

Creatiedatum: 25 aug. 2017

Type binnenkomst: PrivateKeyEntry

Lengte certificaatketen: 2

Certificaat[1]:

Eigenaar: CN=col115cv02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU

Afgever: CN=col115-COL115-CA, DC=col115, DC=org, DC=au

Serienummer: 610000000e78c717ba3dd3dc24000000000000e

Geldig vanaf: 25 februari 2017, 11:32:43 AEST, tot: Sat aug 25:11:42:43 AEST 2018

Certificaatvingerafdrukken:

Na voltooiing van al deze stappen, werd CA ondertekend certificaat voor Call Server geïnstalleerd. Dit certificaat wordt gebruikt wanneer een TLS-verbinding voor SIP is ingesteld.

Verifiëren

Deze twee opdrachten kunnen worden gebruikt om een lijst op te stellen van alle certificaten of alleen de Call Server certificaten:

%kt%-lijst

%kt%-lijst | findstr-callserver

Deze opdracht kan worden gebruikt om certificeringsgegevens weer te geven:

Naam alias: callserver_certificaat

%kt% -list -v -alias callserver_certificaat
Aliennaam:callserver_certificaat

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

Configuratiehandleiding voor Cisco Unified Customer Voice Portal, release 11.6(1)

Technische ondersteuning en documentatie – Cisco Systems