Générez le certificat signé d'Autorité de certification (CA) dans le serveur d'appel CVP pour le Transport Layer Security de SIP (le TLS)

Contenu

Introduction

Ce document décrit comment générer le certificat signé CA pour le serveur d'appel CVP et comment vérifier le certificat de serveur d'appel CVP. De la version 11.6 CVP, la transmission de TLS de SIP est prise en charge.

Contribué par Mingze Yan, ingénieur TAC Cisco.

Édité par Sahar Modares, ingénieur TAC Cisco.

Composants utilisés

- Serveur 11.6 d'appel CVP

Configuration Steps

Step1. Mot de passe de découverte pour le keystore.

Naviguez vers **c:\Cisco\CVP\conf\security.properties dans le serveur d'appel CVP afin de trouver ce mot de passe.**

Ce fichier contient le mot de passe pour le keystore, qui est exigé en actionnant le keystore.

Step2. Créez une variable temporaire pour éviter écrivent la valeur du mot de passe de keystore chaque fois.

Naviguez vers **c:\Cisco\CVP\conf\security** et exécutez cette commande :

placez le kt= c:\Cisco\CVP\jre\bin\keytool.exe - les storepass 592(!aT@Hbt{[c)b7n6{Mj6J[0P4C~X2?4!zv~5(@2*12Dm97 - le storetype JCEKS - le keystore .keystore

> **Note**: **Storepass** doit être remplacé par votre propre mot de passe de keystore.

Step3. Enlevez le certfiicate existant de serveur d'appel.

C'est dû à la limite du keysize dans le serveur d'appel qui est 2048 bits.

Naviguez vers **c:\Cisco\CVP\conf\security** pour trouver le certificat existant. Exécutez cette commande de supprimer le certificat :

%kt% - effacement - alias callserver_certificate

Après la suppression du certificat, cette commande peut être utilisée afin de vérifier tous les Certificats dans le serveur CVP :

%kt% - liste

Et afin de confirmer si le certificat de serveur d'appel était supprimé, exécutez cette commande :

%kt% - liste | callserver de findstr

Étape 4. Générez la paire de clés. Vous devez utiliser la paire de clés de 1024 bits.

Naviguez vers **c:\Cisco\CVP\conf\security** et exécutez cette commande :

%kt% - genkeypair - alias callserver_certificate - v - keysize 1024 - le keyalg RSA

Quand vous exécutez cette commande, elle demande ces informations :

> **Note**: Vous devez utiliser l'adresse Internet du serveur en tant que le prénom et nom de famille.

Quel est votre premier et nom de famille ?
[Inconnu] : col115cvpcall02
Quel est le nom de votre unité organisationnelle ?
[Inconnu] : TAC
Quel est le nom de votre organisation ?
[Inconnu] : Cisco
Quel est le nom de votre ville ou localité ?
[Inconnu] : Sydney
Quel est le nom de votre état ou province ?
[Inconnu] : NSW
Quel est code de pays à deux lettres pour cette unité ?
[Inconnu] : AU
CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU est-il correct ?
[non] : oui

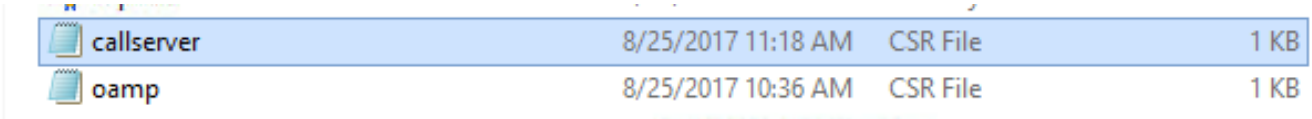
Step5. Générez la nouvelle demande de signature de certificat (CSR).

Naviguez vers **c:\Cisco\CVP\conf\security** et exécutez cette commande :

%kt% - certreq - alias callserver_certificate - classez callserver.csr

Step6. Signez le CSR par CA interne ou tiers C.

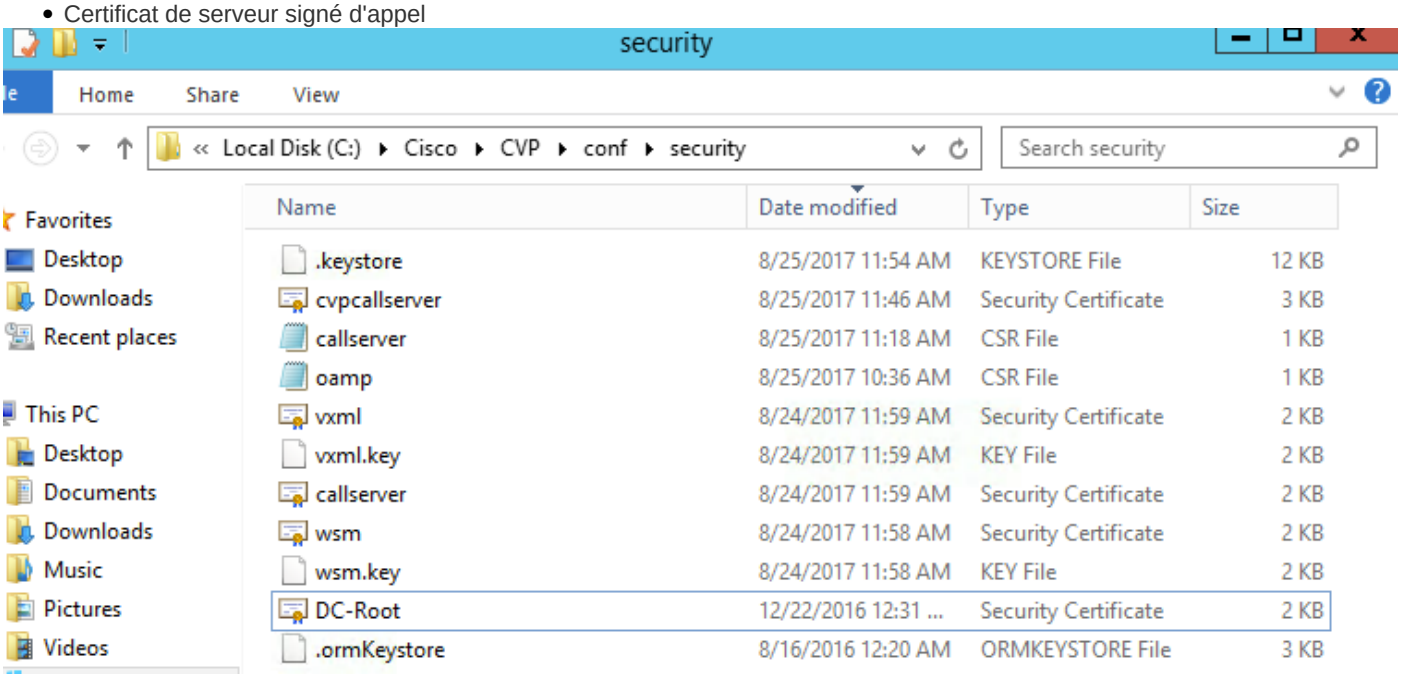
Naviguez vers **c:\Cisco\CVP\conf\security** afin de trouver ce fichier CSR :



Step7. Installez la racine CA.

Deux Certificats sont copiés sur **c:\Cisco\CVP\conf\security.**

- Certificat de CA de racine
- Certificat de serveur signé d'appel



Exécutez cette commande :

%kt% - importation - v - des trustcacerts - alias racine - classez DC-Root.cer

Dans ce laboratoire, le CERT de la racine CA est DC-Root.cer.

Étape 8. Installez le certificat de serveur d'appel qui a été signé par CA.

Naviguez vers **c:\Cisco\CVP\conf\security**

Exécutez cette commande :

%kt% - importation - v - des trustcacerts - alias callserver_certificate - classez cvpcallserver.cer
Dans ce laboratoire, le certificat de serveur d'appel est cvpcallserver.cer.

Étape 9. Vérifiez le nouveau certificat installé

Afin de vérifier le nouveau certificat installé, naviguez vers **C:\Cisco\CVP\conf\security >**
Exécutez cette commande :

%kt% - liste - v - alias pseudonyme de callserver_certificate : callserver_certificate

> **Note**: Le pseudonyme est une valeur à système stable. Vous devez utiliser le callserver_certificate.

Exemple :

Date de création : Août 25, 2017

Type d'entrée : PrivateKeyEntry

Portée de certificat : 2

Certificate[1] :

Propriétaire : CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU

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

Numéro de série : 610000000e78c717ba3dd3dc2400000000000e

Valide de : Fri 25 août 11:32:43 AEST 2017 jusqu'à : SAT 25 août 11:42:43 AEST 2018

Empreintes digital de certificat :

Àla fin de toutes ces étapes, le certificat signé CA pour le serveur d'appel a été installé. Ce certificat est utilisé quand la connexion de TLS pour le SIP est établie.

Vérifications

Ces deux commandes peuvent être utilisées pour répertorier tous les Certificats ou seulement Certificats de serveur d'appel :

%kt% - liste

%kt% - liste | callserver de findstr

Cette commande peut être utilisée pour visualiser des détails de certificat :

Pseudonyme : callserver_certificate

%kt% - liste - v - alias callserver_certificate
Pseudonyme : callserver_certificate

Référence :

Guide de configuration pour le Portail Cisco Unified Customer Voice, version 11.6(1)