Genere el certificado firmado del Certificate Authority (CA) en el servidor de la llamada del CVP para el SORBO Transport Layer Security (TLS)

Contenido

Introducción

Este documento describe cómo generar el certificado firmado de CA para el servidor de la llamada del CVP y cómo verificar el certificado de servidor de la llamada del CVP. De la versión 11.6 del CVP, se soporta la comunicación de TLS del SORBO.

Contribuido por Mingze Yan, ingeniero de Cisco TAC.

Editado por Sahar Modares, ingeniero de Cisco TAC.

Componentes Utilizados

- Servidor 11.6 de la llamada del CVP

Pasos de configuración

Step1. Contraseña del hallazgo para el keystore.

Navegue a **c:\Cisco\CVP\conf\security.properties en el servidor de la llamada del CVP para encontrar esta contraseña.**

Este archivo contiene la contraseña para el keystore, se requiere que al actuar el keystore.

Step2. Cree una variable temporal para evitar ingresan el valor de contraseña del keystore cada vez.

Navegue a **c:\Cisco\CVP\conf\security** y funcione con este comando:

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

> **Note**: **Storepass** se debe substituir por su propia contraseña del keystore.

Step3. Quite el certfiicate del servidor de la llamada existente.

Esto es debido a la limitación del keysize en el servidor de la llamada que es 2048 bits.

Navegue a **c:\Cisco\CVP\conf\security** para encontrar el certificado existente. Funcione con este comando de borrar el certificado:

el %kt% - cancelación - alias callserver_certificate

Después de la cancelacíon del certificado, este comando se puede utilizar para verificar todos los Certificados en el servidor del CVP:

el %kt% - lista

Y para confirmar si el certificado de servidor de la llamada fue borrado, funcione con este comando:

el %kt% - lista | callserver del findstr

Paso 4. Genere el par clave. Usted debe utilizar el par clave de 1024 bits.

Navegue a **c:\Cisco\CVP\conf\security** y funcione con este comando:

los %kt% - genkeypair - alias callserver_certificate - v - keysize 1024 - el keyalg RSA

Cuando usted funciona con este comando, pide esta información:

> **Note:** Usted debe utilizar el nombre de host del servidor como el primer nombre y último nombre.

¿Cuál es su nombre y apellido?
[Unknown]: col115cvpcall02
¿Cuál es el nombre de su unidad organizativa?
[Unknown]: TAC
¿Cuál es el nombre de su organización?
[Unknown]: Cisco
¿Cuál es el nombre de su ciudad o lugar?
[Unknown]: Sydney
¿Cuál es el nombre de su estado o provincia?
[Unknown]: NSW
¿Cuál es el código del país de la dos-carta para esta unidad?
[Unknown]: AU
¿Está CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU correcto?
[no]: sí

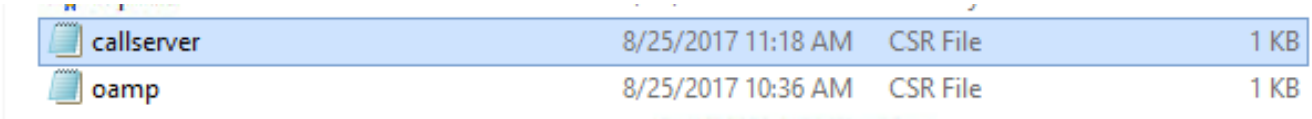
Step5. Genere el nuevo pedido de firma de certificado (CSR).

Navegue a **c:\Cisco\CVP\conf\security** y funcione con este comando:

el %kt% - certreq - alias callserver_certificate - clasifíe callserver.csr

Step6. Firme el CSR por CA interno o el C de tercera persona.

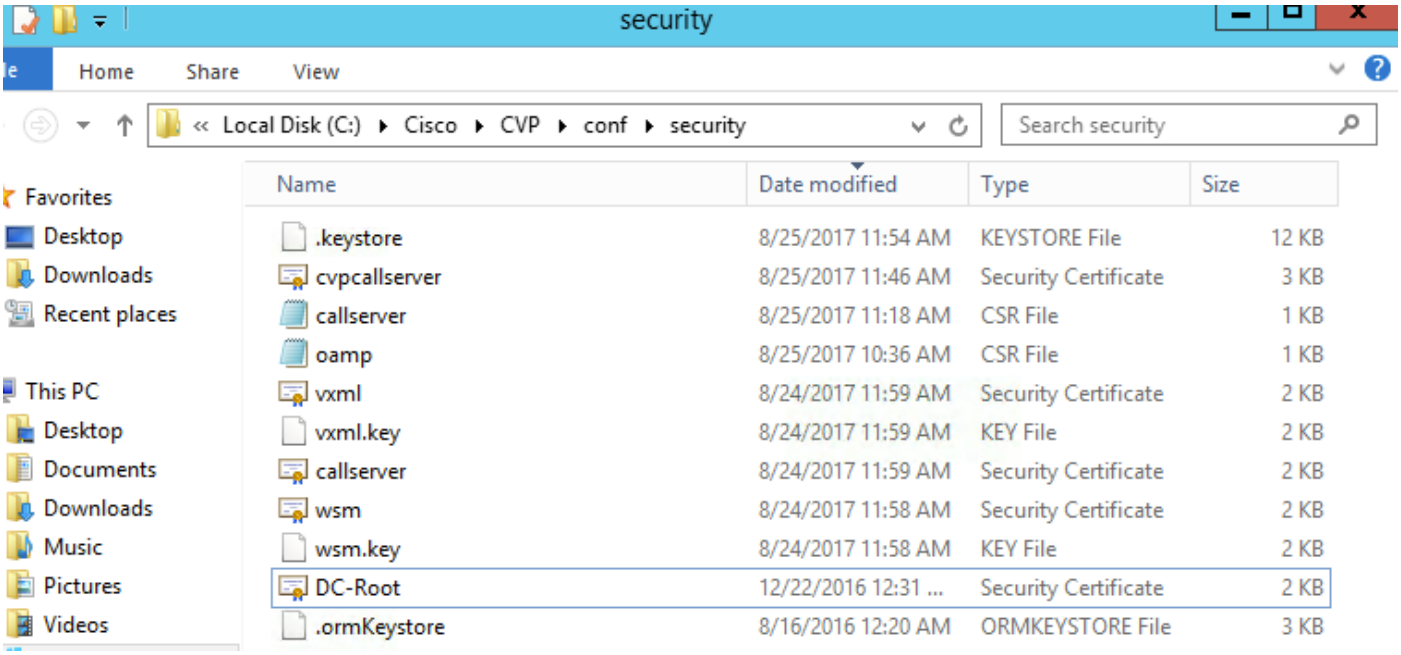
Navegue a **c:\Cisco\CVP\conf\security** para encontrar este archivo CSR:



Step7. Instale raíz CA.

Dos Certificados se copian a **c:\Cisco\CVP\conf\security.**

- Certificado raíz CA
- Certificado de servidor firmado de la llamada



Funcione con este comando:

el %kt% - importación - v - los trustcacerts - alias raíz - clasifíe DC-Root.cer

En este laboratorio, raíz CA el CERT es DC-Root.cer.

Paso 8. Instale el certificado de servidor de la llamada que fue firmado por CA.

Navegue a **c:\Cisco\CVP\conf\security**

Funcione con este comando:

el %kt% - importación - v - los trustcacerts - alias callserver_certificate - clasifíe cvpcallserver.cer
En este laboratorio, el certificado de servidor de la llamada es cvpcallserver.cer.

Paso 9. Verifique el nuevo certificado instalado

Para verificar el nuevo certificado instalado, navegue a **C:\Cisco\CVP\conf\security >**
Funcione con este comando:

el %kt% - lista - v - alias nombre de alias del callserver_certificate: callserver_certificate

> **Note**: El nombre de alias es un valor fijo del sistema. Usted debe utilizar el callserver_certificate.

Ejemplo:

Fecha de creación: De agosto el 25 de 2017

Tipo de entrada: PrivateKeyEntry

Longitud de Cadena de certificados: 2

Certificate[1]:

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

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

Número de serie: 610000000e78c717ba3dd3dc2400000000000e

Válido de: Fri 25 de agosto 11:32:43 AEST 2017 hasta: Sat 25 de agosto 11:42:43 AEST 2018

Huellas dactilares del certificado:

Tras completar todos estos pasos, el certificado firmado de CA para el servidor de la llamada fue instalado. Se utiliza este certificado cuando la conexión TLS para el SORBO se establece.

Verificaciones

Estos dos comandos se pueden utilizar para enumerar todos los Certificados o solamente certificados de servidor de la llamada:

el %kt% - lista

el %kt% - lista | callserver del findstr

Este comando se puede utilizar para ver a los detalles del certificado:

Nombre de alias: callserver_certificate

el %kt% - lista - v - alias callserver_certificate
Nombre de alias: callserver_certificate

Referencia:

Guía de configuración para el Cisco Unified Customer Voice Portal, versión 11.6(1)