Gerar Certificado Assinado pela Autoridade de Certificação (CA) no Servidor de Chamadas CVP para Segurança de Camada de Transporte (TLS) SIP

Contents

Introduction

Este documento descreve como gerar um certificado assinado pela CA para o servidor de chamadas do Portal de Voz do Cliente (CVP) e como verificar o certificado do servidor de chamadas do CVP. A partir da versão 11.6 do CVP, a comunicação TLS do Session Initiation Protocol (SIP) é suportada.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CVP
- SIP

Componentes Utilizados

As informações neste documento são baseadas no CVP 11.6.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa1. Localizar senha para armazenamento de chaves.

Navegue até **c:\Cisco\CVP\conf\security.properties no servidor de chamadas CVP para encontrar esta senha.**

Este arquivo contém a senha do keystore, que é necessária ao operar o keystore.

Etapa 2. Crie uma variável temporária para evitar inserir o valor da senha do armazenamento de chaves sempre.

Navegue até **c:\Cisco\CVP\conf\security** e execute este comando:

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

> **Note**: O Storepass deve ser substituído pela sua própria senha do keystore.

Etapa 3. Remova o certificado do servidor de chamadas existente.

Navegue até **c:\Cisco\CVP\conf\security** para encontrar o certificado existente. Execute este comando para excluir o certificado:

%kt% -delete -alias callserver_certificate

Após a exclusão do certificado, esse comando pode ser usado para verificar todos os certificados no servidor CVP:

%kt% -list

Para confirmar se o certificado do servidor de chamadas foi excluído, execute este comando:

%kt% -list | findstr callserver

Etapa 4. Gere o par de chaves. Você deve usar um par de chaves de 2048 bits.

Navegue até **c:\Cisco\CVP\conf\security** e execute este comando:

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

Quando você executa este comando, ele solicita estas informações:

> **Note**: Você deve usar o nome de host do servidor como nome e sobrenome.

Qual é o seu nome e sobrenome?
[Desconhecido]: col115cvpcall02
Qual é o nome da sua unidade organizacional?
[Desconhecido]: TAC
Qual é o nome da sua empresa?
[Desconhecido]: Cisco
Qual é o nome da sua cidade ou localidade?
[Desconhecido]: Sydney
Qual é o nome do seu Estado ou Província?
[Desconhecido]: NSW
Qual é o código do país com duas letras para esta unidade?
[Desconhecido]: AU
CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW, C=AU correto?
[não]: sim

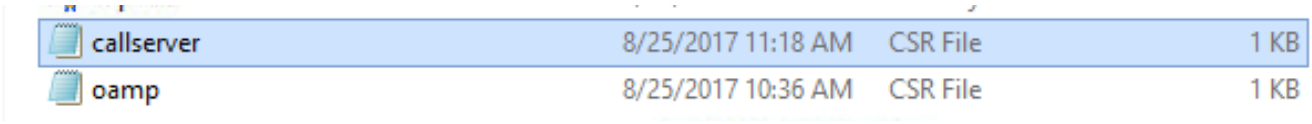
Etapa 5. Gere a nova solicitação de assinatura de certificado (CSR).

Navegue até **c:\Cisco\CVP\conf\security** e execute este comando:

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

Etapa 6. Assine o CSR por CA interna ou C de terceiros.

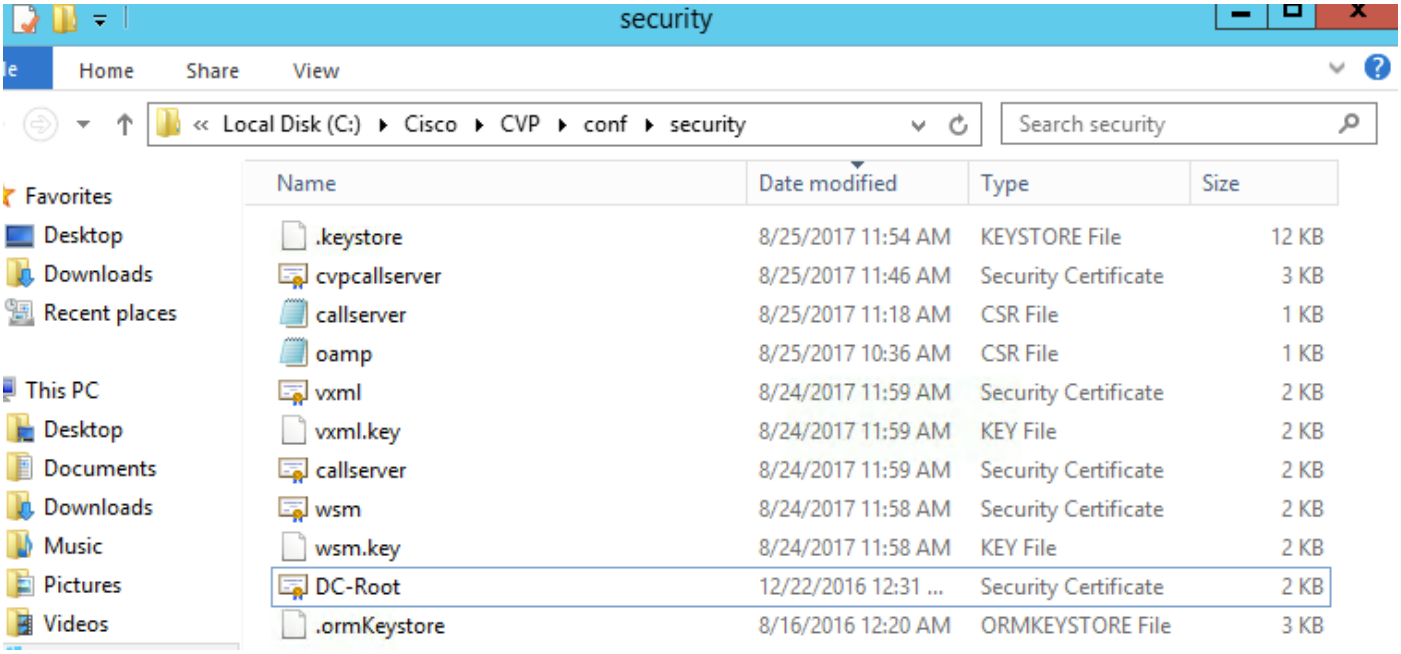
Navegue até **c:\Cisco\CVP\conf\security** para encontrar este arquivo CSR:



Etapa 7. Instale a CA raiz.

Dois certificados são copiados para **c:\Cisco\CVP\conf\security.**

- certificado CA raiz
- Certificado do servidor de chamadas assinado



Execute este comando:

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

Neste laboratório, o certificado da AC raiz é DC-Root.cer.

Etapa 8. Instalar certificado do servidor de chamadas assinado pela AC.

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

Execute este comando:

%kt% -import -v -trustcacerts -alias callserver_certificate -file cvpcallserver.cer
Neste laboratório, o certificado do servidor de chamadas é cvpcallserver.cer.

Etapa 9. Verificar o novo certificado instalado

Para verificar o novo certificado instalado, navegue para **C:\Cisco\CVP\conf\security>**
Execute este comando:

%kt% -list -v -alias callserver_certificate Nome do alias:callserver_certificate

> **Note**: O nome do alias é um valor fixo do sistema. Você deve usar callserver_certificate.

Exemplo:

Data de criação: 25 de agosto de 2017

Tipo de entrada: PrivateKeyEntry

Comprimento da cadeia de certificados: 2

Certificado[1]:

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

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

Número de série: 610000000e78c717ba3dd3dc24000000000000e

Válido de: Sex 25 de agosto 11:32:43 AEST 2017 até: Sáb 25 de agosto 11:42:43 AEST 2018

Impressões digitais do certificado:

Após concluir todas essas etapas, o certificado assinado pela CA para o servidor de chamadas foi instalado. Este certificado é usado quando a conexão TLS para SIP é estabelecida.

Verificar

Esses dois comandos podem ser usados para listar todos os certificados ou somente certificados do servidor de chamadas:

%kt% -list

%kt% -list | findstr callserver

Este comando pode ser usado para exibir detalhes do certificado:

Nome do alias: callserver_certificate

%kt% -list -v -alias callserver_certificate
Nome do alias:callserver_certificate

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

Guia de configuração do Cisco Unified Customer Voice Portal, versão 11.6(1)

Suporte Técnico e Documentação - Cisco Systems