Генерируйте подписанный сертификат центра сертификации (CA) в сервере вызовов CVP для Transport Layer Security (TLS) SIP

Содержание

Введение

Этот документ описывает, как генерировать подписанный сертификат CA для сервера вызовов CVP и как проверить сертификат сервера вызовов CVP. От версии 11.6 CVP поддерживается связь TLS SIP.

Внесенный Менгзом Яном, специалистом службы технической поддержки Cisco.

Отредактированный Sahar Modares, специалистом службы технической поддержки Cisco.

Используемые компоненты

- Сервер вызовов 11.6 CVP

Порядок действий для настройки

Шаг 1. Найдите пароль для keystore.

Перейдите к **c : \Cisco\CVP\conf\security.properties** в сервере вызовов CVP для обнаружения этого пароля.

Этот файл содержит пароль для keystore, который требуется при работе keystore.

Шаг 2. Создайте временную переменную для предотвращения, входят, keystore пароль оценивают каждый раз.

Перейдите к **c:\Cisco\CVP\conf\security** и выполните эту команду:

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

Примечание: Storepass должен быть заменен вашим собственным keystore паролем.

Шаг 3. Демонтируйте certfiicate сервер существующего вызова.

Это происходит из-за ограничения размера ключа в сервере вызовов, который составляет 2048 битов.

Перейдите к **c:\Cisco\CVP\conf\security to find the existing certificate**. Выполните эту команду для удаления сертификата:

% %kt - - callserver_certificate

После удаления сертификата эта команда может использоваться для проверки всех сертификатов в сервере CVP:

% %kt -

И чтобы подтвердить, был ли сертификат сервера вызовов удален, выполните эту команду:

% %kt - | findstr callserver

Шаг 4. . Генерируйте пару ключей. Необходимо использовать пару ключей на 1024 бита.

Перейдите к **c:\Cisco\CVP\conf\security** и выполните эту команду:

% %kt -genkeypair - callserver_certificate -v - 1024-keyalg RSA

Когда вы выполняете эту команду, она запрашивает эту информацию:

Примечание: Необходимо использовать имя хоста сервера в качестве имени и фамилии.

```
   ?
[]: col115cvpcall02
  ?
[]: TAC
  ?
[] : Cisco
    ?
[]:
    ?
[]: NSW
      ?
[]: AU
CN=col115cvpcall02, OU=TAC, O=Cisco, L=Sydney, ST=NSW,  C=AU?
:
```

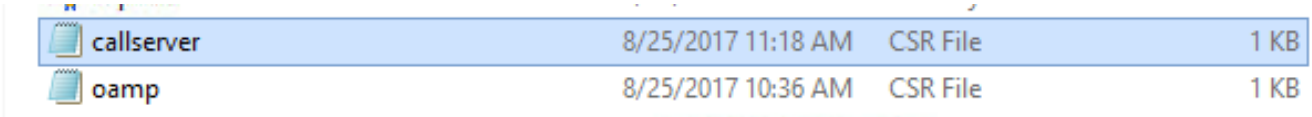
Шаг 5. . Генерируйте новый Запрос подписи сертификата (CSR).

Перейдите к **c:\Cisco\CVP\conf\security** и выполните эту команду:

% %kt -certreq - callserver_certificate - callserver.csr

Шаг 6. Подпишите CSR внутренним CA или независимым поставщиком C.

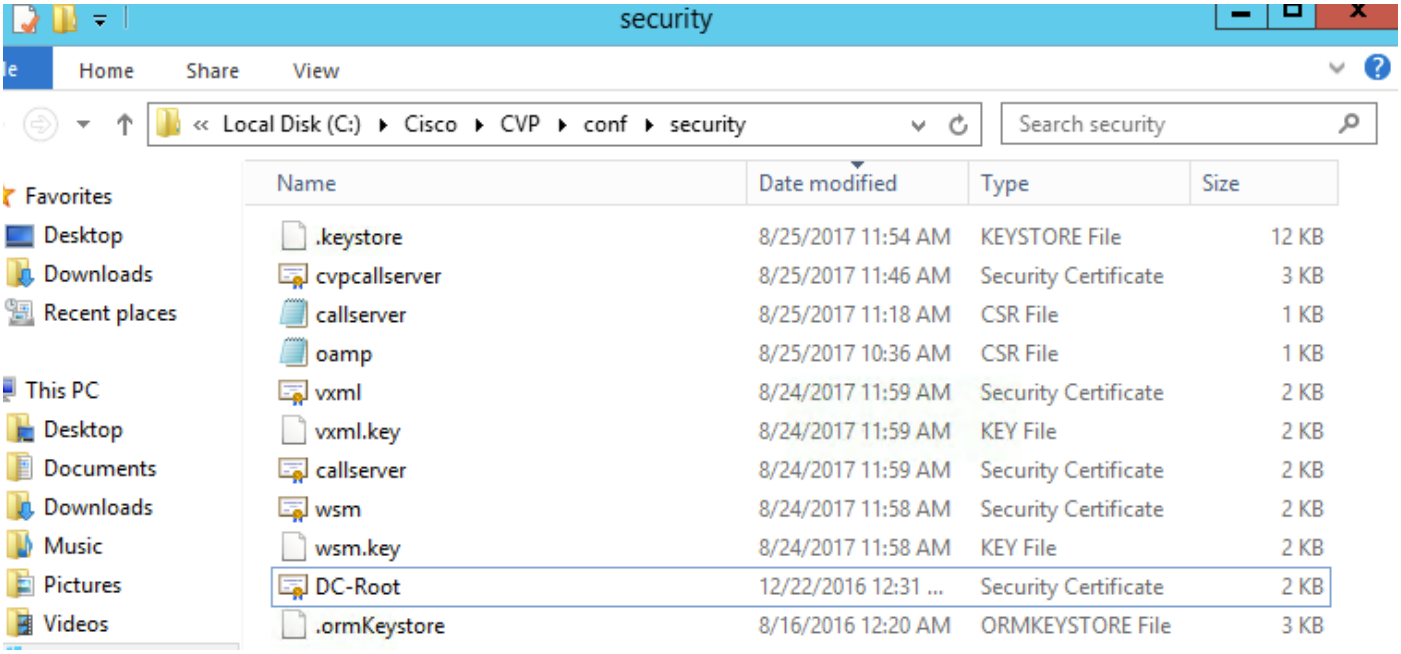
Перейдите к **c:\Cisco\CVP\conf\security** для обнаружения этого файла CSR:



Шаг 7. Установите узел CA.

Два сертификата скопированы к **c:\Cisco\CVP\conf\security**.

- CA
-



Выполните эту команду:

% %kt - импортирует-v-trustcacerts - root псевдонима - DC-Root.cer файла

В этой лабораторной работе свидетельство Узла CA является DC-Root.cer.

Шаг 8. Установите сертификат Сервера вызовов, который был подписан CA.

Перейдите к **c:\Cisco\CVP\conf\security**

Выполните эту команду:

% %kt - импортирует-v-trustcacerts - искажают callserver_certificate - файл cvpcallserver.cer
В этой лабораторной работе сертификат сервера вызовов является cvpcallserver.cer.

Шаг 9. Проверьте новый установленный сертификат

C:\Cisco\CVP\conf\security>
:

% %kt - -v - callserver_certificate name:callserver_certificate

> **Примечание:** Название псевдонима является неподвижным системным значением. Необходимо использовать callserver_certificate.

Пример:

Дата создания: 25 августа 2017

Тип элемента: PrivateKeyEntry

Длина цепочки сертификатов: 2

Сертификат [1]:

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

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

Серийный номер: 610000000e78c717ba3dd3dc2400000000000e

Допустимый от: пятница 25 августа 11:32:43 AEST 2017 до: суббота 25 августа 11:42:43 AEST 2018

Отпечатки пальца сертификата:

После завершения всех этих шагов CA был установлен подписанный сертификат для сервера вызовов. Когда TLS подключение для SIP установлен, этот сертификат используется.

Проверки

Эти две команды могут использоваться для распечатки всех сертификатов или только сертификатов сервера вызовов:

% %kt -

% %kt - | findstr callserver

Эта команда может использоваться для просмотра сведений о сертификате:

Название псевдонима: callserver_certificate

% %kt - -v - callserver_certificate
name:callserver_certificate

Ссылка:

Cisco Unified Customer Voice Portal, 11.6 (1)