Настройте Подписанный сертификат CA через CLI в голосовой операционной системе (VOS) Cisco

Содержание

Введение

Этот документ описывает действия настройки о том, как загрузить подписанный сертификат Центра сертификации (CA) третьей стороны на основанном сервере совместной работы голосовой операционной системы (VOS) любой Cisco при помощи интерфейса командной строки (CLI).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Основное понимание Инфраструктуры открытых ключей (PKI) и ее реализации на Cisco серверы VOS и Microsoft CA
- Инфраструктура DNS предварительно сконфигурирована

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Сервер VOS: версия 9.1.2 Cisco Unified Communications Manager (CUCM)
- CA: Windows 2012 Server
- Клиентский браузер: версия 47.0.1 Mozilla Firefox

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Во всей Cisco Унифицированный Comunications VOS продукты существует по крайней мере два учетных типа: приложение как (ccmadmin, ccmservice, cuadmin, cfadmin, cuic) и платформа VOS (cmplatform, drf, cli).

В некоторых определенных сценариях очень удобно управлять приложениями через веб-страницу и выполнить, платформа отнеслась действия через командную строку. Ниже вас может найти процедуру о том, как импортировать подписанный сертификат третьей стороны исключительно через CLI. В данном примере загружен сертификат Tomcat. Для CallManager или любого другого приложения это выглядит одинаково.

Генерируйте подписанный сертификат CA

Сводка команд

Список команд используется в статье.

```
show cert list own
show cert own tomcat

set csr gen CallManager
show csr list own
show csr own CallManager

show cert list trust
set cert import trust CallManager
set cert import own CallManager CallManager-trust/allevich-DC12-CA.pem
```

Проверьте корректную информацию о сертификате

Перечислите все загруженные надежные сертификаты.

```
admin:show cert list own tomcat/tomcat.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system CallManager/CallManager.pem:
Certificate Signed by allevich-DC12-CA CAPF/CAPF.pem: Self-signed certificate generated by
system TVS/TVS.pem: Self-signed certificate generated by system
```

Проверьте, кто выполнил сертификат для сервиса Tomcat.

```
admin:show cert own tomcat [ Version: V3 Serial Number: 85997832470554521102366324519859436690
```

```
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5) Issuer Name: L=Krakow, ST=Malopolskie,
CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL Validity From: Sun Jul 31 11:37:17 CEST 2016 To:
Fri Jul 30 11:37:16 CEST 2021 Subject Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local,
OU=TAC, O=Cisco, C=PL Key: RSA (1.2.840.113549.1.1.1) Key value: 3082010a0282010100a2
<output omited>
```

Это - подписанный сертификат, так как отправитель совпадает с предметом.

Генерируйте Запрос знака сертификата (CSR)

Генерируйте CSR.

```
admin:set csr gen tomcat Successfully Generated CSR for tomcat
```

Проверьте, что сертификат подписывается, requst генерировался успешно.

```
admin:show csr list own tomcat/tomcat.csr
```

Откройте его и скопируйте содержание к текстовому файлу. Сохраните его как **tac_tomcat.csr** файл.

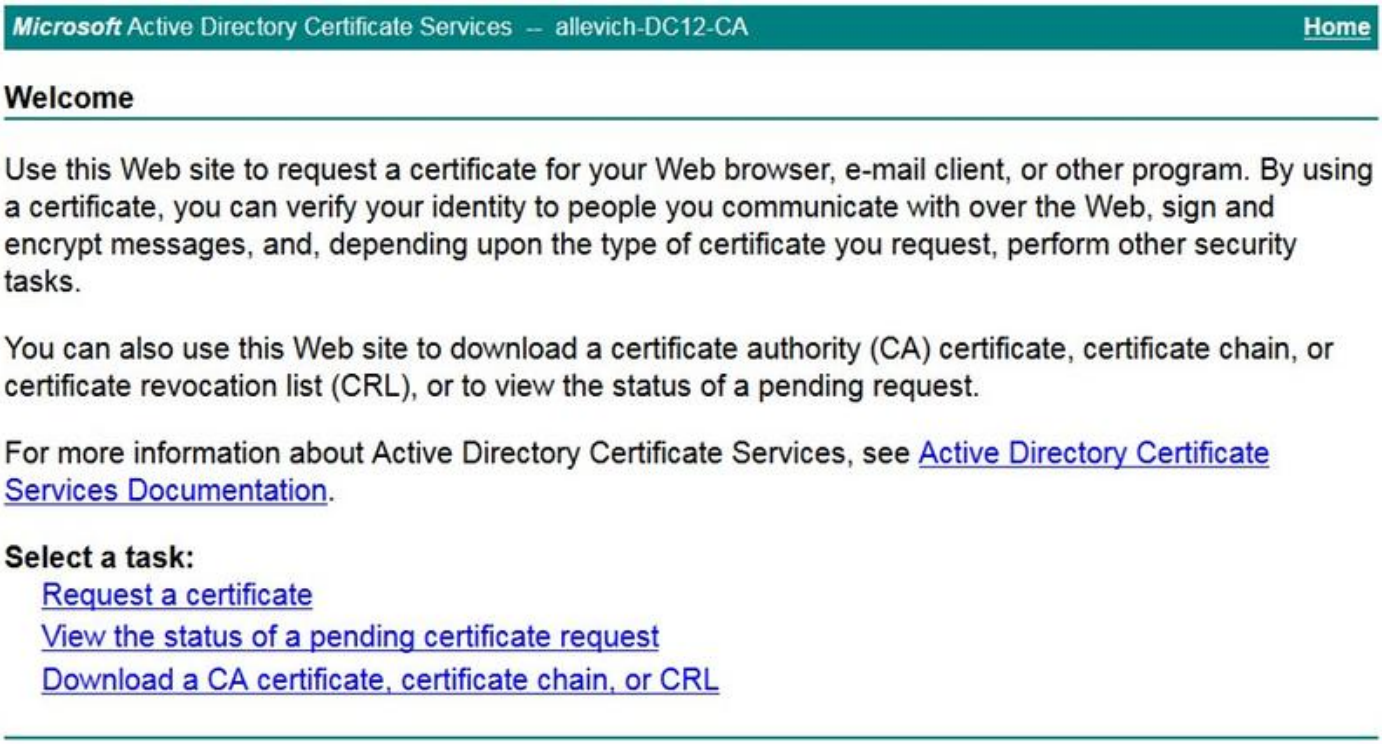
```
admin:show csr own tomcat -----BEGIN CERTIFICATE REQUEST-----
MIIDSjCCAjICAQAwgb0xCzAJBgNVBAYTAlBMMRQwEgYDVQQIEwtNYWxvcG9sc2tp
ZTEPMA0GA1UEBxMGS3Jha293MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFD
MR4wHAYDVQQDExV1Y20xLTEuYWxsZXZpY2gubG9jYWwxSTBHBgNVBAUTQDlhMWJk
NDA5M2VjOGYxNjljODhmNGUyZTYwZTYzM2RjNjlhZmFkNDY1YTgzMDhkNjRhNGU1
MzExOGQ0YjZkZjcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCVo5jh
lMqTUnYbHQUnYPt00PTflWbj7hi6PSYI7pVCbGUZBpIZ5PKwTD56OZ8SgpjYX5Pf
l9D09H2gtQJTMVv1Gm1eGdlJsbuABRKn6lWkO6b706MiGSgqel+41vnItjn3Y3kU
7h51nruJye3HpPQzvXXpOKJ/JeJc8InEvQcC/UQmFMKn0ulO0veFBHnG7TLDwDaQ
W1Al1rwrezN9Lwn2a/XZQR1P65sjmnkFFF2/FON4BmooeiiNJD0G+F4bKig1ymlR
84faF27plwHjcw8WAn2HwJT6O7TaE6EOJd0sgLU+HFAI3txKycS0NvLuMZYQH81s
/C74CIRWibEWT2qLAgMBAAGgRzBFBgkqhkiG9w0BCQ4xODA2MCcGA1UdJQQgMB4G
CCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwUwCwYDVR0PBAQDAgO4MA0GCSqG
SIb3DQEBBQUAA4IBAQBUu1FhKuyQ1X58A6+7KPkYsWtioS0PoycltuQsVo0aav82
PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPPhtt6asDuW30SqSx4eClfgmKH
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNoduPZ0/fo41QoJPwjE184U64WXB
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LId85NGHEiqyiWqwmt07pTkBc+
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMFsW2uYFj9pf/Wn4aDGuJoqdOH
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP -----END CERTIFICATE REQUEST-----
```

Генерируйте серверный сертификат Tomcat

Генерируйте сертификат для сервиса Tomcat на CA.

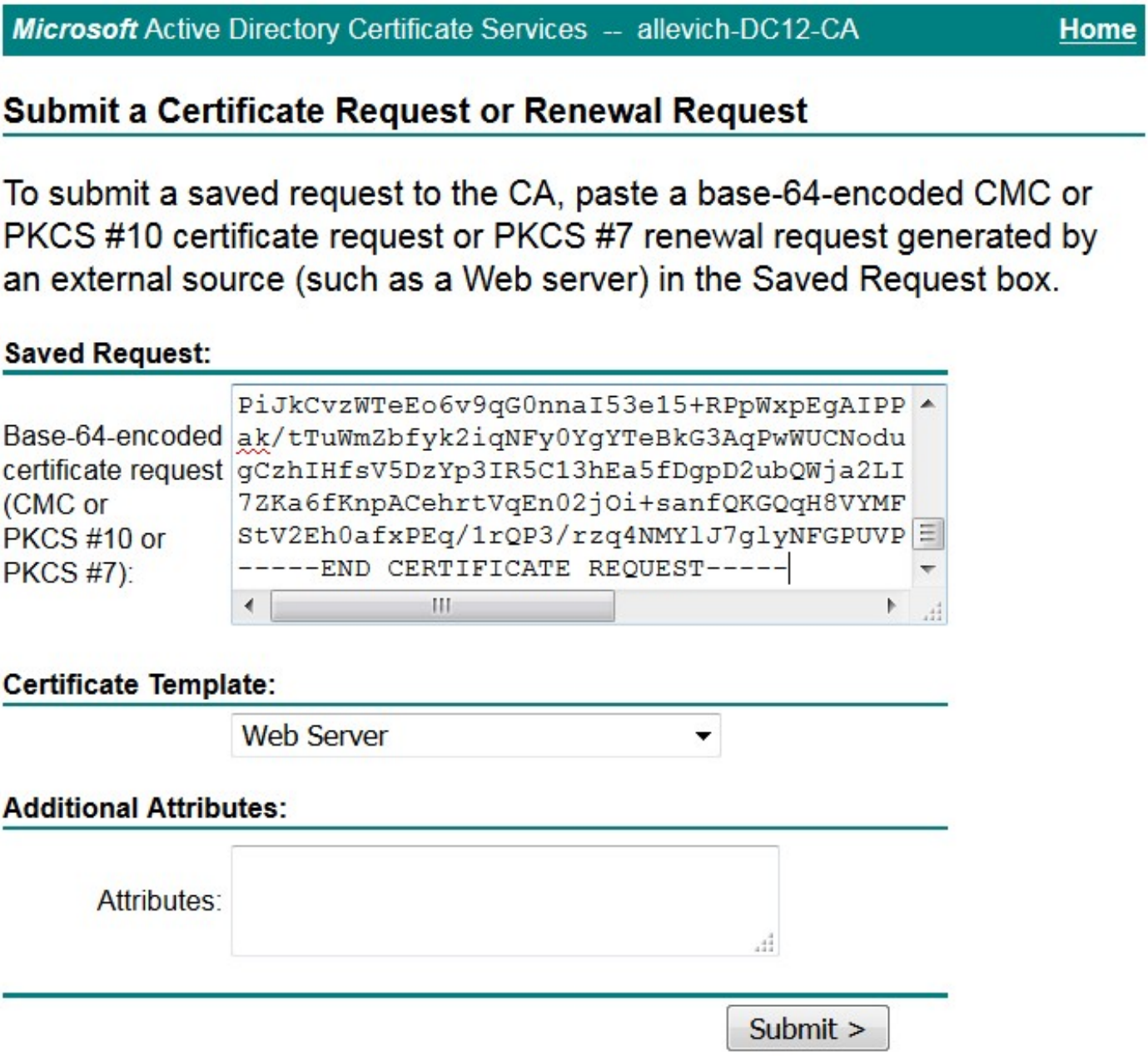
Откройте веб-страницу для Центра сертификации в браузере. Поместите корректные учетные данные в опознавательное приглашение.

http://dc12.allevich.local/certsrv/



Загрузите корневой сертификат CA. Выберите **Download a CA certificate, цепочку сертификатов или** меню **CRL**. В следующем меню выбирают надлежащий CA из списка. Способ кодирования должен быть **Ядром 64**. Загрузите сертификат ЦС и сохраните его к операционной системе с названием **ca.cer**.

Нажмите **Request a Certificate** и затем **Усовершенствованный Запрос сертификата**. **Шаблон сертификата** набора на Web-сервер и вставку содержание CSR от текстового файла **tac_tomcat.csr** как показано.



Совет: Если операция сделана в лабораторной работе (или Cisco, сервер VOS и CA находятся под тем же административным доменом) сэкономить копию времени и вставить CSR от буфера памяти.

Нажмите **Submit**. Выберите **закодированную** опцию **Base 64** и загрузите сертификат для сервиса Tomcat.

Примечание: Если генерация сертификата выполнена, оптом убеждаются для изменения названия сертификата к meaninful один.

Сертификат Tomcat импорта к Cisco сервер VOS

Сертификат CA импорта

Откройте сертификат CA, который был сохранен названием **ca.cer**. Это должно быть

импортированный сначала.

Скопируйте его содержание к буферу и введите следующую команду в CLI CUCM:

```
admin:set cert import trust tomcat Paste the Certificate and Hit Enter
```

Приглашение для вставки сертификата CA будет отображено. Вставьте его как показано ниже.

```
-----BEGIN CERTIFICATE-----
MIIDczCCAlugAwIBAgIQEZg1rT9fAL9B6HYkXMikITANBgkqhkiG9w0BAQUFADBM
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghhbGxldmlj
aDEZMBcGA1UEAxMQYWxsZXZpY2gtREMxMi1DQTAeFw0xNjA1MDExNzUxNTlaFw0y
MTA1MDExODAxNTlaMEwxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEYMBYGCgmSJomT
8ixkARkWCGFsbGV2aWNoMRkwFwYDVQQDExBhbGxldmljaC1EQzEyLUNBMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoL2ubJJOgyTX2X4zhmZs+fOZz7SF
O3GReUavF916UZ/CSP49EgHcuYw58846uxZw6bcjgwsaE+oMQD2EYHKZmQAALwxv
ERVfyc5kS6EM7oR6cwOnK5piZOUORzq/Y7teinF91wtOSJOR6ap8aEC3Bfr23SIN
bDJXMB5KYw68MtoebhiDYxExvY+XYREoqSFC4KeRrpTmuy7VfGPjv0clwmfm0/Ir
MzYtkAILcfvEVduz+KqZdehuwYWAIQBhvDszQGW5aUEXj+07GKRiIT9vaPOt6TBZ
g78IKQoXe6a8Uge/1+F9VlFvQiG3AeqkIvD/UHrZACfAySp8t+csGnr3vQIDAQAB
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUr1sv
r5HPbDhDGoSN5EeU7upV9iQwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBABfguqa6swmmXpStXdg0mPuqE9mnWQTPnWx91SSKyyY3+icHaUlXgW/9
WppSfMajzKOueWelzDOwsBk17CYEAiT6SGnak8/+Yz5NCY4fOowl7OvRz9jP1iOO
Zd9eowH6fgYw6+M5zsLvBB3SFGatKgUrpB9rExaWOtsZHCF5mrd13vl+BmpBxDCz
FuzSFfyxuMzOXkJPmH0LByBUw90h4s6wJgJHp9B0f6J5d9ES7PkzHuKVtIxvioHa
Uf1g9jqOqoe1UXQh+09uZKOi62gfkBcZiWkHaP0OmjOQCbSQcSLLMTJoRvLxZKNX
jzqAOylrPEYgvQFrkH1Yvo8fotXYw5A=
-----END CERTIFICATE-----
```

В случае, если трастовая загрузка сертификата успешна, эти выходные данные будут отображены.

```
Import of trust certificate is successful
```

Проверьте, что сертификат CA успешно импортирован как трастовый Tomcat.

```
admin:show cert list trust tomcat-trust/ucm1-1.pem: Trust Certificate tomcat-trust/allevich-win-CA.pem: w2008r2 139 <output omited for brevity>
```

Сертификат Tomcat импорта

Следующий шаг должен импортировать Tomcat CA подписанный сертификат. Операция выглядит одинаково как с трастовым tomcat свидетельством, просто команда является другой.

```
set cert import own tomcat tomcat-trust/allevich-DC12-CA.pem
```

Перезапустите службу

И наконец сервис Tomcat перезапуска.

```
utils service restart Cisco Tomcat
```

> **Внимание. :** Следует иметь в виду, что это разрушает использование подчиненных сервисов Web-сервера, как Функция Extension Mobility, Пропущенные вызовы, Корпоративный каталог и другие.

Проверка

Проверьте сертификат, который генерировался.

```
admin:show cert own tomcat [ Version: V3 Serial Number: 276529240473076562022540660071542142548731496 5 SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5) Issuer Name: CN=allevich-DC12-CA, DC=allevich, DC=local Validity From: Sun Jul 31 12:17:46 CEST 2016 To: Tue Jul 31 12:17:46 CEST 2018 Subject Name: CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL Key: RSA (1.2.840.113549.1.1.1) Key value: 3082010a028201010095a
```

Гарантируйте, что имя запрашивающей стороны принадлежит CA, который создал тот сертификат.

Вход в систему к веб-странице путем ввода FQDN сервера в браузере и никаком сертификате, предупреждающем, будет отображен.

Устранение неполадок

Цель этой статьи состоит в том, чтобы дать процедуру с синтаксисом команды о том, как загрузить сертификат через CLI, для не выделения логики Infrastucture с открытым ключом (PKI). Это не покрывает SAN сертификат, Подчиненный CA, 4096 длин ключа сертификата и много других сценариев.

В некоторых редких случаях при загрузке сертификата Web-сервера через CLI операция отказывает с сообщением об ошибках, "Неспособным считать сертификат CA". Обходной путь для этого должен установить сертификат с помощью веб-страницы.

Нестандартная конфигурация Центра сертификации может привести к проблеме с установкой сертификатов. Попытайтесь генерировать и установить сертификат от другого CA с основной конфигурацией по умолчанию.

Отступите план

В случае, если будет потребность генерировать подписанный сертификат, она может также быть сделана в CLI.

Введите команду ниже, и сертификат Tomcat будет восстановлен к самоподписанному.

```
admin:set cert regen tomcat WARNING: This operation will overwrite any CA signed certificate previously imported for tomcat Proceed with regeneration (yes|no)? yes Successfully Regenerated Certificate for tomcat. You must restart services related to tomcat for the regenerated certificates to become active.
```

Применять новый сервис Tomcat сертификата должно быть перезапущено.

```
admin:utils service restart Cisco Tomcat Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again Service Manager is running Cisco Tomcat[STOPPING] Cisco Tomcat[STOPPING] Commanded Out of Service Cisco Tomcat[NOTRUNNING] Service Manager is running Cisco Tomcat[STARTING] Cisco Tomcat[STARTING] Cisco Tomcat[STARTED]
```

Похожие статьи

Сертификат загрузки через веб-страницу

Процедура, чтобы получить и загрузить Windows Server Self-Signed или Центр сертификации (CA)...