Cisco VOS(Voice Operating System)의 CLI를 통해 CA 서명 인증서 구성

목차

소개

이 문서에서는 CLI(Command Line Interface)를 사용하여 Cisco VOS(Voice Operating System) 기반 협업 서버에서 서드파티 CA(Certificate Authority) 서명 인증서를 업로드하는 방법에 대한 컨피그레이션 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PKI(Public Key Infrastructure)에 대한 기본적인 이해 및 Cisco VOS 서버 및 Microsoft CA에 대한 구현
- DNS 인프라는 미리 구성되어 있음

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- VOS 서버:Cisco CUCM(Unified Communications Manager) 버전 9.1.2
- CA:Windows 2012 Server
- 클라이언트 브라우저:Mozilla Firefox 버전 47.0.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

모든 Cisco Unified Communications VOS 제품에는 최소 두 가지 자격 증명 유형이 있습니다 .(ccmadmin, cmservice, cuadmin, cfadmin, cuic) 및 VOS 플랫폼(cmplatform, drf, cli)과 같은 애플리케이션.

일부 특정 시나리오에서는 웹 페이지를 통해 애플리케이션을 관리하고 명령줄을 통해 플랫폼 관련 작업을 수행하는 것이 매우 편리합니다.아래에서는 CLI를 통해서만 3번째 서드파티 서명 인증서를 가져오는 방법에 대한 절차를 찾을 수 있습니다.이 예에서는 Tomcat 인증서가 업로드됩니다 .CallManager 또는 다른 응용 프로그램의 경우 동일하게 표시됩니다.

CA 서명 인증서 생성

명령 요약

문서에서 사용되는 명령 목록

```
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
```

올바른 인증서 정보 확인

업로드된 신뢰할 수 있는 인증서를 모두 나열합니다.

```
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
```

Tomcat 서비스에 대해 인증서를 발급한 사람을 확인합니다.

```
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>
```

발급자가 제목과 일치하므로 자체 서명 인증서입니다.

CSR(Certificate Sign Request) 생성

CSR 생성

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

인증서 서명 요청이 성공적으로 생성되었는지 확인합니다.

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

파일을 열고 내용을 텍스트 파일에 복사합니다.tac_tomcat.csr 파일로 저장합니다.

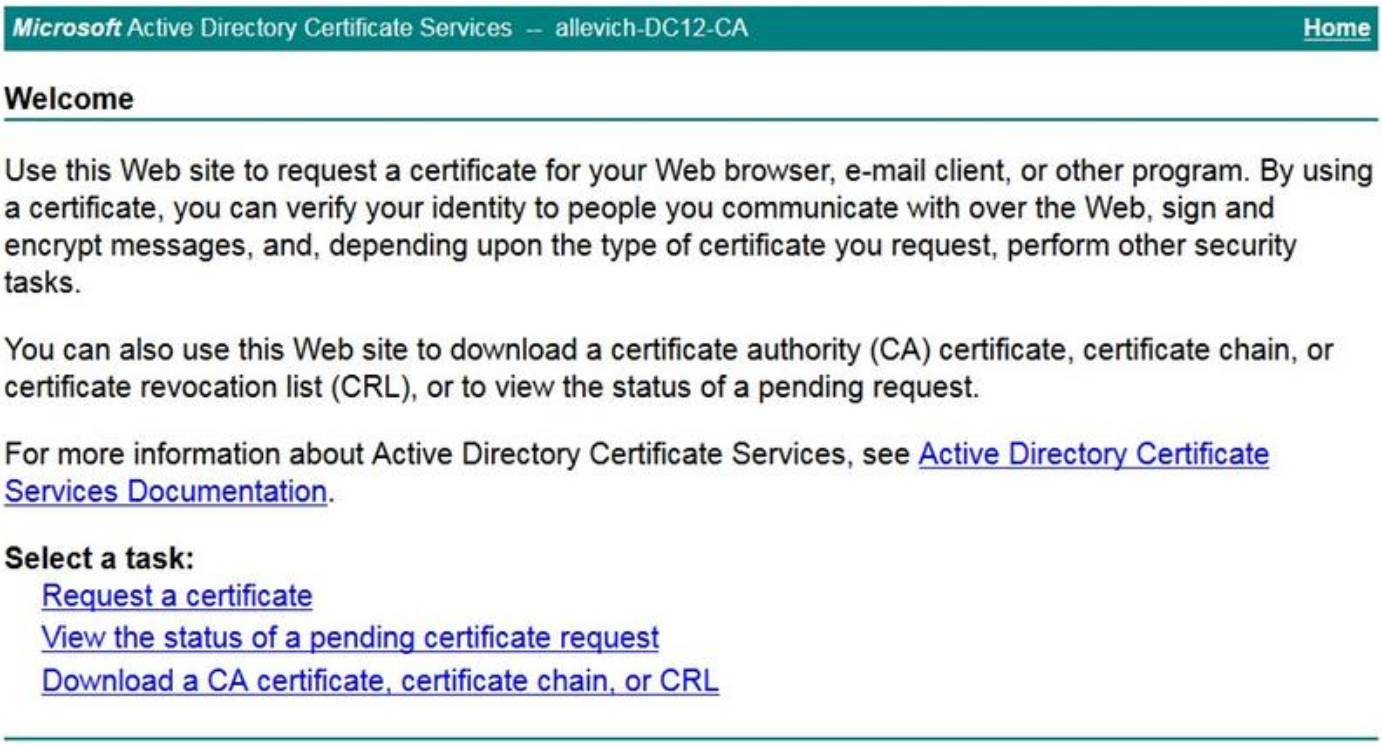
```
admin:show csr own tomcat

-----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-----
```

Tomcat 서버 인증서 생성

CA에서 Tomcat 서비스에 대한 인증서를 생성합니다.

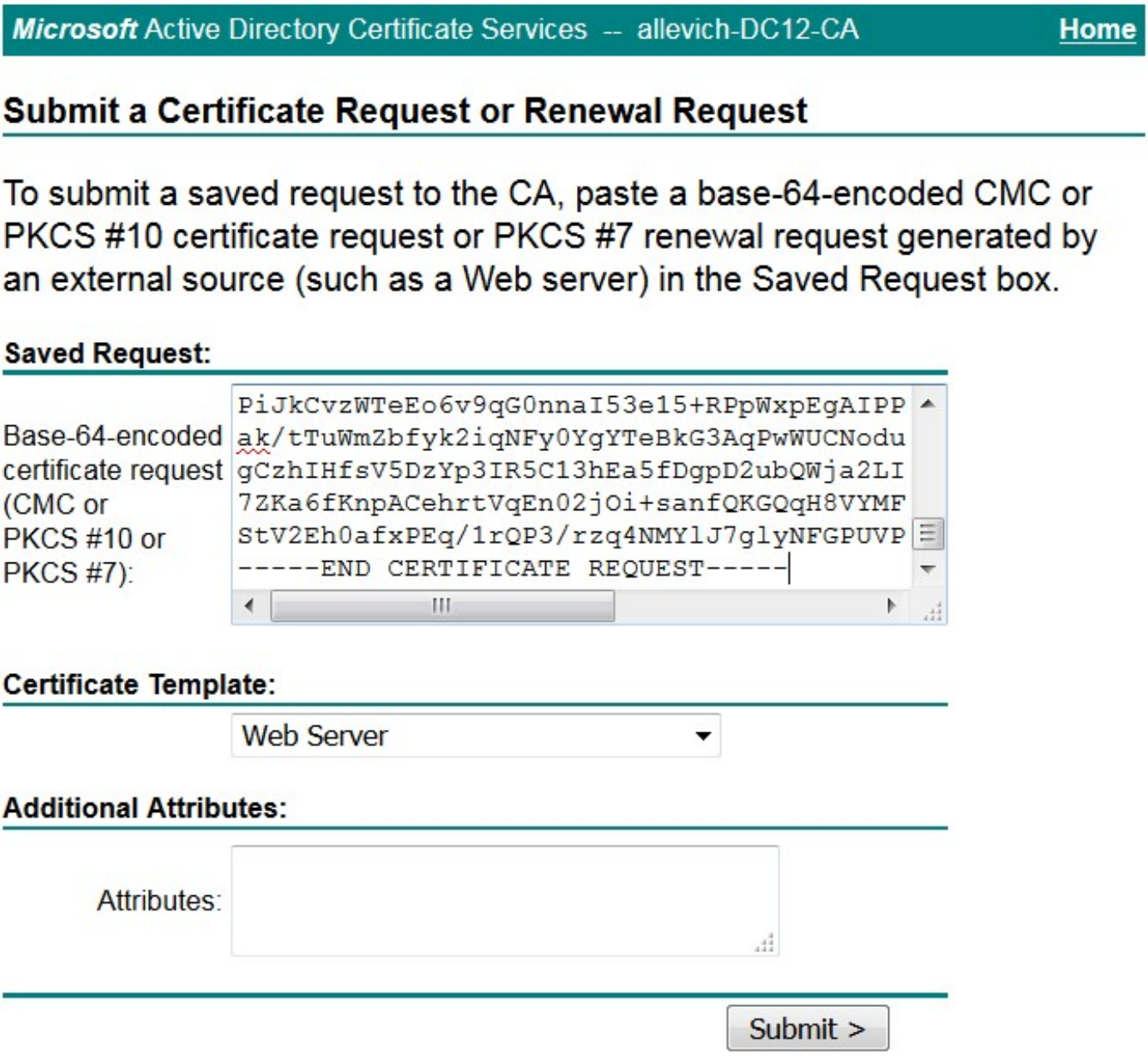
브라우저에서 인증 기관에 대한 웹 페이지를 엽니다.인증 프롬프트에 올바른 자격 증명을 입력합니다.

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



CA 루트 인증서를 다운로드합니다.Download **a CA certificate, certificate chain 또는 CRL** 메뉴**를** 선택합니다.다음 메뉴의 목록에서 적절한 CA를 선택합니다.인코딩 방법은 **Base 64**여야 합니다. CA 인증서를 다운로드하여 운영 체제에 ca**.cer**라는 이름으로 저장하십시오.

Request **a Certificate(인증서 요청)**와 Advanced Certificate Request(**고급 인증서 요청)를 차례로 누릅니다**.**인증서 템플릿**을 웹 서버로 설정하고 텍스트 파일 tac_tomcat**.csr**에서 CSR 내용**을** 다음과 같이 붙여넣습니다.



팁:Lab(또는 Cisco VOS 서버 및 CA가 동일한 관리 도메인 아래에 있음)에서 작업을 수행하여 시간 복사를 절약하고 메모리 버퍼에서 CSR을 붙여넣습니다.

제출을 **누릅니다**.Base **64 인코딩** 옵션을 선택하고 Tomcat 서비스에 대한 인증서를 다운로드합니다.

참고:인증서 생성을 대량으로 수행하는 경우 인증서의 이름을 의미 있는 이름으로 변경해야 합니다.

Cisco VOS 서버로 Tomcat 인증서 가져오기

CA 인증서 가져오기

이름이 ca.**cer**로 저장된 CA 인증서를 **엽니다**.먼저 가져와야 합니다.

해당 내용을 버퍼에 복사하고 CUCM CLI에 다음 명령을 입력합니다.

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

CA 인증서를 붙여넣으라는 프롬프트가 표시됩니다.아래에 표시된 대로 붙여넣습니다.

```
-----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-----
```

트러스트 인증서 업로드가 성공할 경우 이 출력이 표시됩니다.

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

CA 인증서를 Tomcat-trust 인증서로 성공적으로 가져왔는지 확인합니다.

```
admin:show cert list trust

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

Tomcat 인증서 가져오기

다음 단계는 Tomcat CA 서명 인증서를 가져오는 것입니다.이 작업은 tomcat-trust cert와 동일하게 표시되며 명령이 다릅니다.

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

서비스 다시 시작

마지막으로 Tomcat 서비스를 다시 시작합니다.

```
utils service restart Cisco Tomcat
```

> **주의:**익스텐션 모빌리티, 부재 중 전화, 회사 디렉터리 및 기타 같은 웹 서버 종속 서비스 운영을 중단한다는 점에 유의하십시오.

다음을 확인합니다.

생성된 인증서를 확인합니다.

```
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
```

발급자 이름이 해당 인증서를 생성한 CA에 속하는지 확인합니다.

브라우저에 서버의 FQDN을 입력하여 웹 페이지에 로그인하면 인증서 경고가 표시되지 않습니다.

문제 해결

이 문서의 목적은 PKI(Public Key Infrastructure)의 논리를 강조하지 않고 CLI를 통해 인증서를 업로드하는 방법에 대한 명령 구문을 제공하는 것입니다. SAN 인증서, 하위 CA, 4096 인증서 키 길이 및 기타 여러 시나리오에는 적용되지 않습니다.

CLI를 통해 웹 서버 인증서를 업로드할 때 "Unable to read CA certificate(CA 인증서를 읽을 수 없음)"라는 오류 메시지와 함께 작업이 실패하는 경우도 있습니다.이에 대한 해결 방법은 웹 페이지를 사용하여 인증서를 설치하는 것입니다.

비표준 인증 기관 컨피그레이션으로 인해 인증서 설치 문제가 발생할 수 있습니다.기본 기본 컨피그레이션을 사용하여 다른 CA에서 인증서를 생성하고 설치하려고 합니다.

백아웃 계획

자체 서명 인증서를 생성해야 하는 경우 CLI에서도 생성할 수 있습니다.

아래에 명령을 입력하면 자체 서명된 인증서로 Tomcat 인증서가 재생성됩니다.

```
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.
```

새 인증서를 적용하려면 Tomcat 서비스를 다시 시작해야 합니다.

```
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]
```

관련 문서

웹 페이지를 통해 인증서 업로드

Windows Server 자체 서명 또는 CA(Certificate Authority)를 가져오고 업로드하는 절차..