Configurazione del certificato firmato dalla CA tramite CLI in Cisco Voice Operating System (VOS)

Sommario

Introduzione

In questo documento viene descritta la procedura di configurazione per caricare un certificato firmato da un'Autorità di certificazione (CA) di terze parti su un server di collaborazione basato su VOS (Cisco Voice Operating System) tramite l'interfaccia della riga di comando (CLI).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di base dell'infrastruttura a chiave pubblica (PKI) e della relativa implementazione sui server Cisco VOS e Microsoft CA
- Infrastruttura DNS preconfigurata

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Server VOS: Cisco Unified Communications Manager (CUCM) versione 9.1.2
- CA Windows 2012 Server
- Browser client: Mozilla Firefox versione 47.0.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In tutti i prodotti VOS per comunicazioni unificate Cisco sono disponibili almeno due tipi di credenziali: applicazioni quali (ccmadmin, ccmservice, cuadmin, cfadmin, cuic) e piattaforma VOS (cmplatform, drf, cli).

In alcuni scenari specifici è molto conveniente gestire le applicazioni tramite la pagina Web ed eseguire le attività relative alla piattaforma tramite la riga di comando. Di seguito è riportata una procedura per importare certificati firmati da 3^{terze} parti esclusivamente tramite CLI. In questo esempio viene caricato il certificato Tomcat. Per CallManager o qualsiasi altra applicazione ha lo stesso aspetto.

Genera certificato firmato CA

Riepilogo comandi

Elenco dei comandi utilizzati nell'articolo.

```
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
```

Verifica informazioni sul certificato corrette

Elenca tutti i certificati protetti caricati.

```
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
```

Verifica chi ha rilasciato il certificato per il servizio Tomcat.

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 859978324705545211023663245198594366 90
  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>
```

Si tratta di un certificato autofirmato poiché l'autorità emittente corrisponde al soggetto.

Genera richiesta di firma del certificato (CSR)

Generare CSR.

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

Verificare che la richiesta di firma del certificato sia stata generata correttamente.

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

Aprire il file e copiarne il contenuto nel file di testo. Salvarlo come file **tac_tomcat.csr**.

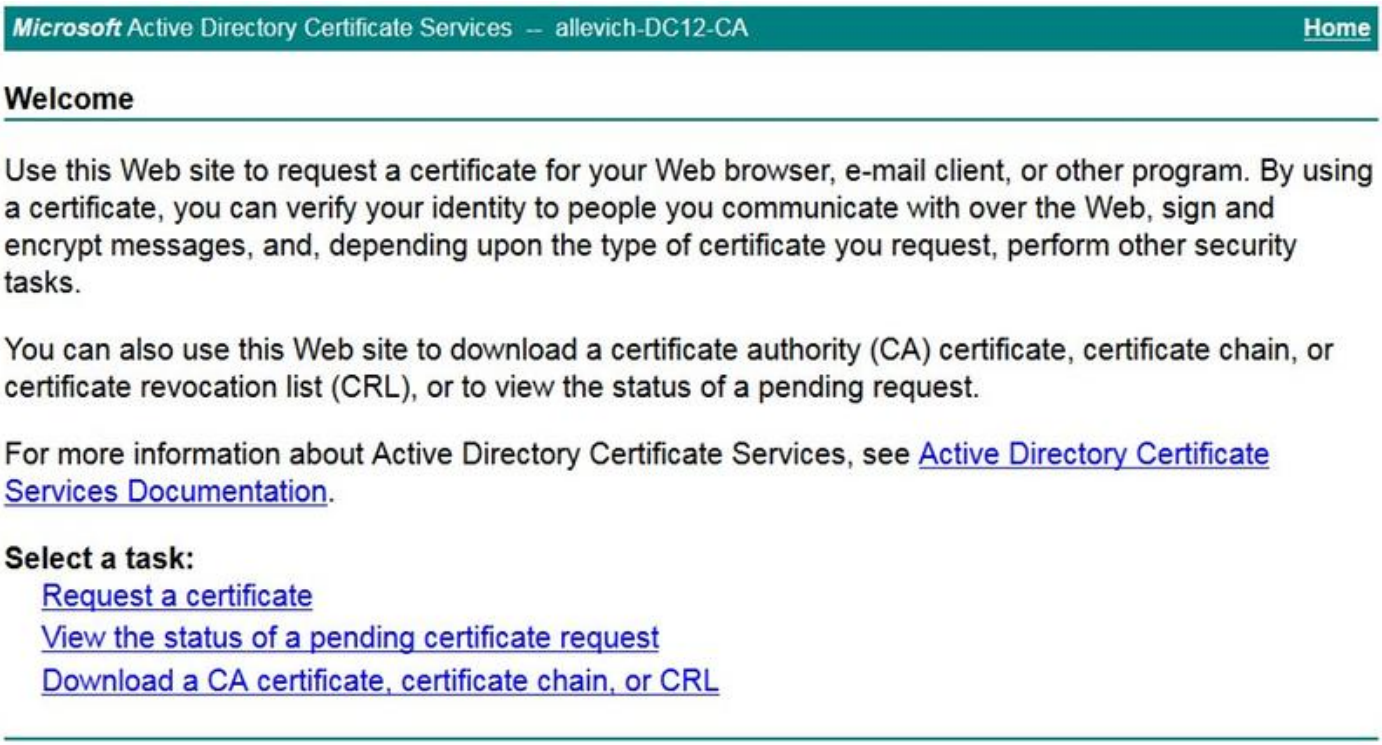
```
admin:show csr own tomcat

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

Genera certificato server Tomcat

Generare un certificato per il servizio Tomcat sulla CA.

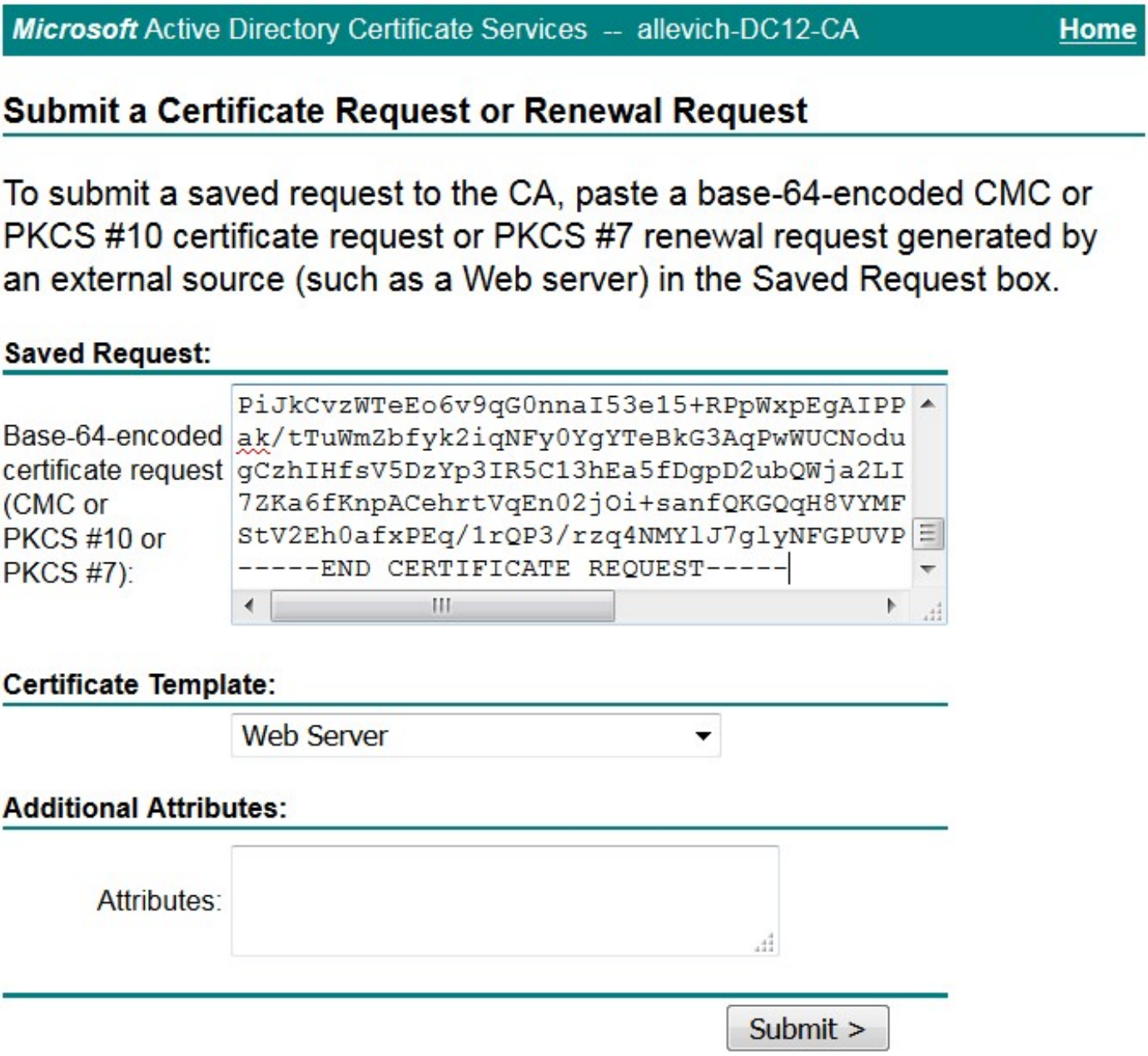
Aprire la pagina Web per l'Autorità di certificazione in un browser. Inserire le credenziali corrette nella richiesta di autenticazione.

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



Scaricare il certificato radice CA. Selezionare **Scarica certificato CA, catena di certificati o** menu **CRL**. Nel menu successivo scegliere la CA appropriata dall'elenco. Il metodo di codifica deve essere **Base 64**. Scaricare il certificato CA e salvarlo nel sistema operativo con il nome **ca.cer**.

Fare clic su **Richiedi certificato** e quindi su **Richiesta avanzata certificato**. Impostare **Modello di certificato** su server Web e incollare il contenuto CSR dal file di testo **tac_tomcat.csr** come mostrato.



> **Suggerimento**: Se l'operazione viene eseguita in laboratorio (o sul server Cisco VOS e la CA si trova nello stesso dominio amministrativo), è possibile risparmiare tempo copiando e incollando il CSR dal buffer di memoria.

Premere **Submit (Invia)**. Selezionare l'opzione **Base 64 Encoded** (Codificato base 64) e scaricare il certificato per il servizio Tomcat.

> **Nota:** Se la generazione del certificato viene eseguita in blocco, assicurarsi di modificare il nome del certificato in uno significativo.

Importa certificato Tomcat sul server Cisco VOS

Importa certificato CA

Aprire il certificato CA archiviato con il nome **ca.cer**. Deve prima essere importato.

Copiarne il contenuto nel buffer e digitare il comando seguente nella CLI di CUCM:

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

Verrà visualizzato un messaggio che richiede di incollare il certificato CA. Incollatelo come mostrato di seguito.

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

Se il caricamento di un certificato di attendibilità ha esito positivo, verrà visualizzato questo output.

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

Verificare che il certificato CA sia stato importato come Tomcat-trust-one.

```
admin:show cert list trust

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

Importa certificato Tomcat

Il passaggio successivo consiste nell'importare un certificato firmato da Tomcat CA. L'operazione ha lo stesso aspetto del certificato tomcat-trust, ma il comando è diverso.

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

Riavvia il servizio

Infine riavviare il servizio Tomcat.

```
utils service restart Cisco Tomcat
```

> **Attenzione:** Si tenga presente che interrompe il funzionamento dei servizi dipendenti dal server Web, come Extension Mobility, Missed Call, Corporate Directory e altri.

Verifica

Verificare il certificato generato.

```
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
```

Verificare che il nome dell'autorità di certificazione appartenga alla CA che ha costruito il certificato.

Accedere alla pagina Web digitando FQDN del server in un browser e non verrà visualizzato alcun avviso di certificato.

Risoluzione dei problemi

Lo scopo di questo articolo è quello di fornire una procedura con sintassi dei comandi su come caricare il certificato tramite la CLI, non di evidenziare la logica dell'infrastruttura a chiave pubblica (PKI). Non copre il certificato SAN, la CA subordinata, la lunghezza della chiave del certificato

4096 e molti altri scenari.

In alcuni rari casi, quando si carica un certificato server Web tramite la CLI, l'operazione non riesce e viene visualizzato il messaggio di errore "Unable to read CA certificate" (Impossibile leggere il certificato CA). Una soluzione a questo problema consiste nell'installare il certificato utilizzando la pagina Web.

Una configurazione non standard dell'Autorità di certificazione può causare il problema dell'installazione del certificato. Provare a generare e installare il certificato da un'altra CA con una configurazione predefinita di base.

Piano di backup

Nel caso in cui sia necessario generare un certificato autofirmato, è possibile farlo anche nella CLI.

Digitare il comando seguente e il certificato Tomcat verrà rigenerato in quello autofirmato.

```
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.
```

Per applicare un nuovo certificato, è necessario riavviare il servizio Tomcat.

```
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]
```

Articoli correlati

Carica certificato tramite pagina Web

Procedura per ottenere e caricare Windows Server autofirmato o CA (Certification Authority) ...