Configure el certificado firmado CA vía el CLI en el sistema operativo de la Voz de Cisco (VOS)

Contenido

Introducción

Este documento describe los pasos para la configuración en cómo cargar por teletratamiento el certificado firmado del Certificate Authority (CA) de las de otras compañías en cualquier servidor basado de la Colaboración del sistema operativo de la Voz de Cisco (VOS) usando el comando line interface(cli).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica del Public Key Infrastructure (PKI) y de su puesta en práctica en los servidores de Cisco VOS y Microsoft CA
- Se preconfigura la infraestructura DNS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor VOS: Versión 9.1.2 del encargado de las Comunicaciones unificadas de Cisco (CUCM)
- CA: Servidor de Windows 2012
- Buscador del cliente: Versión 47.0.1 de Mozilla Firefox

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

En todo el Cisco los Productos unificados de Comunications VOS allí son por lo menos dos tipos de las credenciales: la aplicación tiene gusto (ccmadmin, ccmservice, cuadmin, cfadmin, cuic) y plataforma VOS (cmplatform, drf, cli).

En algunos decorados específicos es muy conveniente manejar las aplicaciones vía la página web y realizar las actividades relacionadas plataforma vía la línea de comando. Debajo de usted puede encontrar un procedimiento en cómo importar el certificado firmado de las de otras compañías solamente vía el CLI. En este Tomcat del ejemplo se carga por teletratamiento el certificado. Para CallManager o cualquier otra aplicación mira lo mismo.

Genere el certificado firmado CA

Comandos summary

Una lista de los comandos usados en el artículo.

```
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
```

Controle la información correcta del certificado

Enumere todos los certificados confiables cargados por teletratamiento.

```
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
```

Controle quién publicó el certificado para el servicio de 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>
```

Esto es un certificado autofirmado puesto que el emisor hace juego el tema.

Genere la petición de la muestra del certificado (el CSR)

Genere el CSR.

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

Verifique que el requst de la muestra del certificado fuera generado con éxito.

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

Ábralo y copie el contenido al archivo de texto. Sálvelo como fichero tac_tomcat.csr.

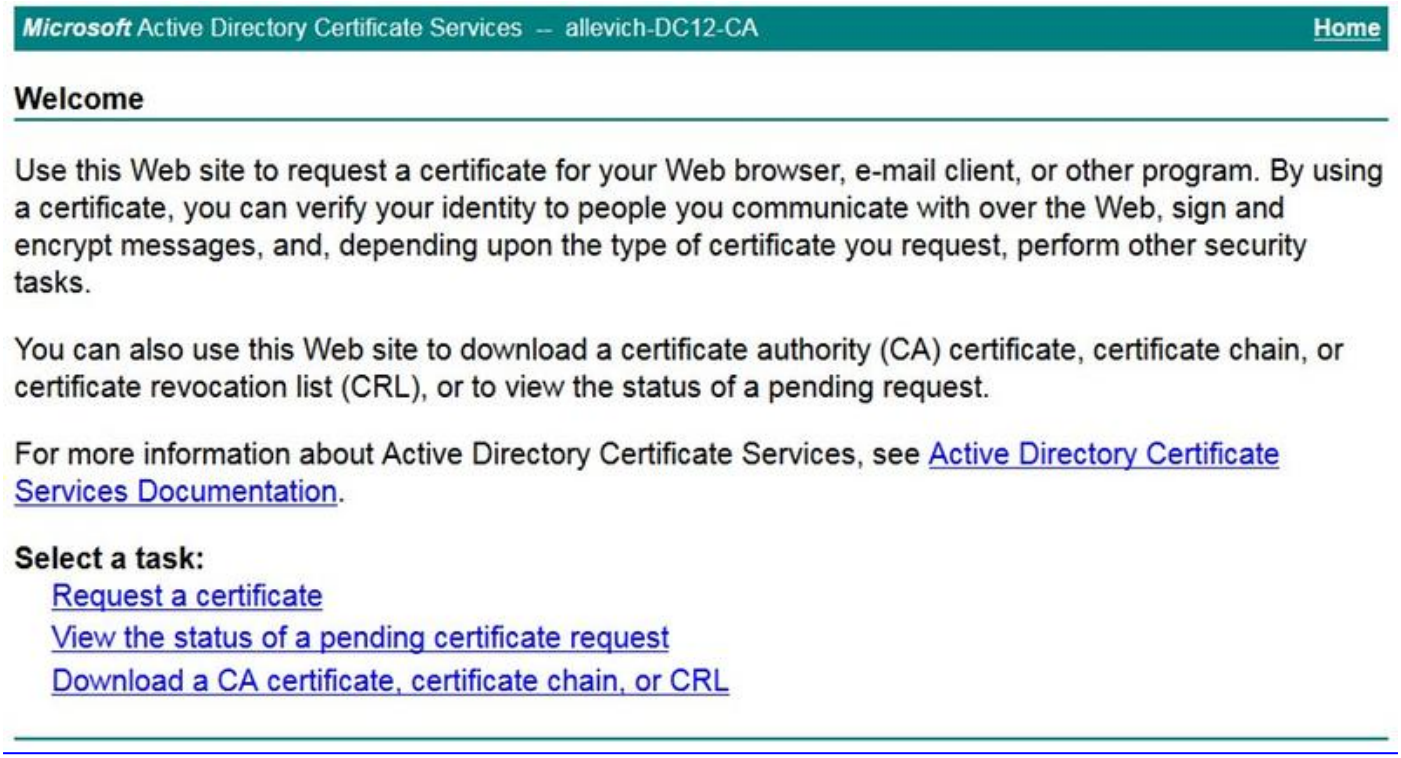
```
admin:show csr own tomcat

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

Genere el certificado de servidor de Tomcat

Genere un certificado para el servicio de Tomcat en el CA.

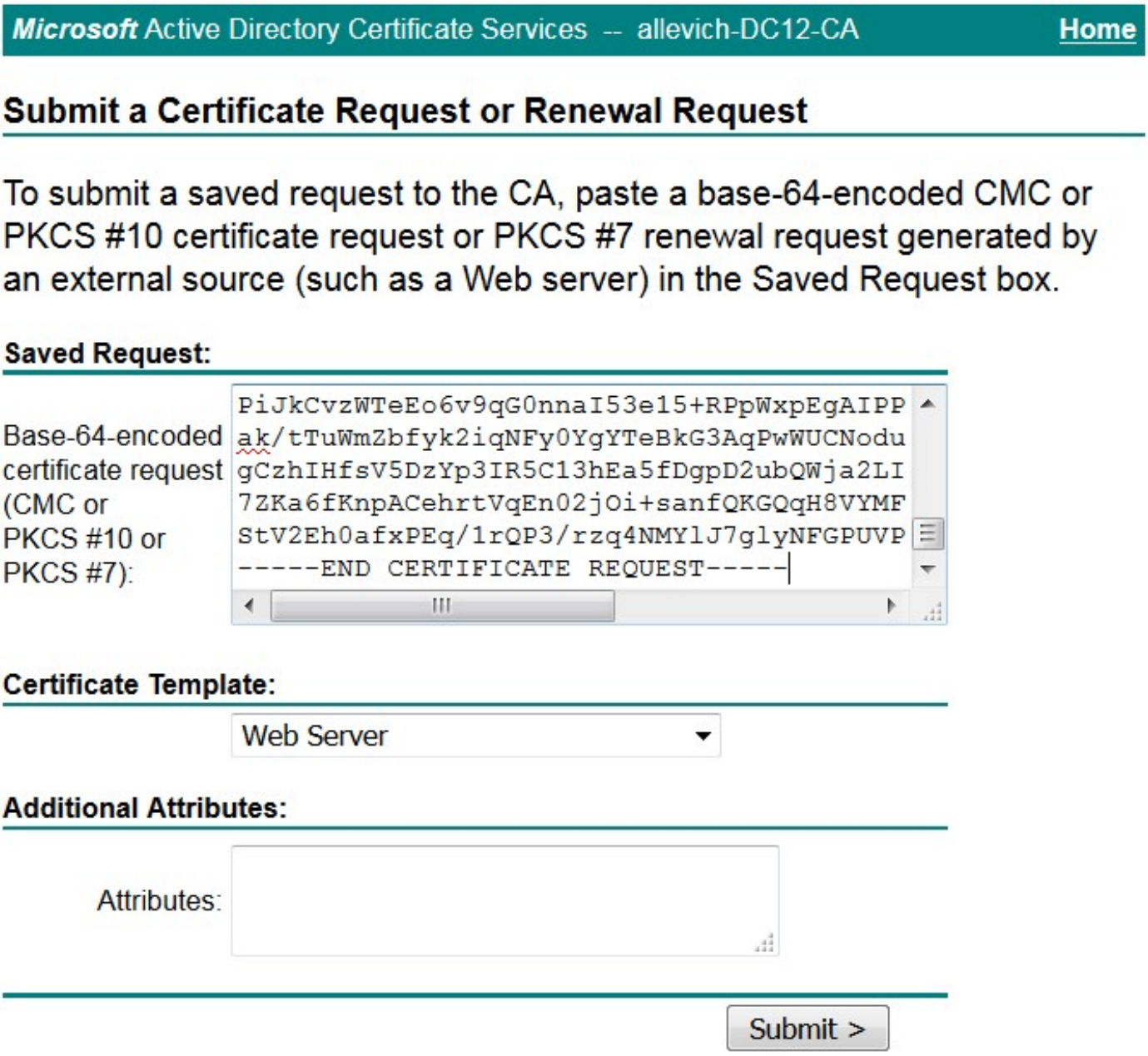
Abra la página web para la autoridad de certificación en un navegador. Ponga las credenciales correctas en el mensaje de la autenticación.

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



Descargue el certificado raíz CA. Seleccione la **transferencia directa un certificado CA, una Cadena de certificados, o un** menú **CRL**. En el menú siguiente elija el CA apropiado de la lista. El método de codificación debe ser **base 64**. Descargue el certificado CA y sálvelo al sistema operativo con el nombre **ca.cer**.

Presione la **petición un certificado** y una **solicitud de certificado** entonces **avanzada**. Fije el **Certificate Template plantilla de certificado al** servidor Web y pegue el contenido CSR del archivo de texto **tac_tomcat.csr como se muestra**.



> Consejo: Si la operación se hace en el laboratorio (o el servidor de Cisco VOS y el CA está bajo mismo Administrative Domain) para salvar la copia del tiempo y para pegar el CSR de memoria intermedia.

La prensa **somete**. Seleccione la opción **codificada base 64** y descargue el certificado para el servicio de Tomcat.

> **Note**: Si la generación del certificado se realiza en el bulto asegure para cambiar un nombre del certificado meaninful.

Importe el certificado de Tomcat al servidor de Cisco VOS

Importe el certificado CA

Abra el certificado CA que fue salvado con un nombre **ca.cer**. Debe ser importado primero.

Copie su contenido al almacenador intermediario y pulse el comando siguiente en el CUCM CLI:

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

El mensaje para pegar el certificado CA será visualizado. Pegúelo como se muestra abajo.

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

En caso de que una carga por teletratamiento del certificado de confianza sea acertada esta salida será visualizada.

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

Verifique que el certificado CA esté importado con éxito como Tomcat-confianza una.

```
admin:show cert list trust

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

Importe el certificado de Tomcat

El siguiente paso es importar el certificado firmado de Tomcat CA. La operación mira lo mismo que con el CERT de la Tomcat-confianza, apenas el comando es diferente.

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

Reiniciar el servicio

Y recomience pasado el servicio de Tomcat.

```
utils service restart Cisco Tomcat
```

> Precaución: Tenga en cuenta que interrumpe la operación de los servicios dependientes del servidor Web, como la movilidad de la extensión, las llamadas faltadas, Corporate Directory (Directorio corporativo) y el otros.

Verificación

Verifique el certificado que fue generado.

```
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
```

Asegúrese de que el nombre del emisor pertenezca al CA que construyó ese certificado.

Ábrase una sesión a la página web por el FQDN que pulsa del servidor en un navegador y no se visualizará ninguna advertencia del certificado.

Troubleshooting

La meta de este artículo es dar un procedimiento con la sintaxis de ordenes en cómo cargar por teletratamiento el certificado vía el CLI, para no destacar la lógica de la clave pública Infrastucture (PKI). No cubre el certificado SAN, el CA subordinado, la longitud de clave de 4096 certificados y muchos otros decorados.

En algunos casos pocos probables al cargar por teletratamiento un certificado del servidor Web vía el CLI la operación falla con un mensaje de error “incapaz de leer el certificado CA”. Una solución alternativa para ésa es instalar el certificado usando la página web.

Una configuración no estándar de la autoridad de certificación puede llevar al problema con la instalación del certificado. Intente generar y instalar el certificado de otro CA con una configuración de valor por defecto básica.

Se retira el plan

En caso de que haya una necesidad de generar un certificado autofirmado puede también ser hecho en el CLI.

Pulse el comando abajo y el certificado de Tomcat será regenerado uno mismo-firmado.

```
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.
```

Para aplicar un nuevo servicio de Tomcat del certificado debe ser recomenzada.

```
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]
```

Artículos relacionados

Certificado de la carga por teletratamiento vía la página web

Procedimiento para obtener y para cargar por teletratamiento el - del uno mismo del Servidor Windows firmado o el Certificate Authority (CA)…