Configurar o certificado assinado de CA através do CLI no sistema operacional da Voz de Cisco (VOS)

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Gerencia o certificado assinado de CA](#)
[Comandos summary](#)
[Verifique a informação correta do certificado](#)
[Gerencia o pedido do sinal do certificado (o CSR)](#)
[Gerencia o certificado de servidor de Tomcat](#)
[Importe o certificado de Tomcat ao server de Cisco VOS](#)
[Importe o certificado de CA](#)
[Importe o certificado de Tomcat](#)
[Reinicie o serviço](#)
[Verificar](#)
[Troubleshooting](#)
[Suporte para fora o plano](#)
[Artigos relacionados](#)

Introdução

Este original descreve etapas de configuração em como transferir arquivos pela rede o certificado assinado do Certificate Authority (CA) da 3ª parte em todo o Collaboration Server baseado do sistema operacional da Voz de Cisco (VOS) usando o comando line interface(cli).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica do Public Key Infrastructure (PKI) e sua aplicação em server de Cisco VOS e em Microsoft CA
- A infraestrutura DNS preconfigured

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Server VOS: Versão 9.1.2 do gerente das comunicações unificadas de Cisco (CUCM)
- CA: Server de Windows 2012
- Navegador cliente: Versão 47.0.1 de Mozilla Firefox

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Em todo o Cisco o Produtos unificado de Comunications VOS lá é pelo menos dois tipos das credenciais: o aplicativo gosta (ccmadmin, ccmservice, cuadmin, cfadmin, cuic) e plataforma VOS (cmplatform, drf, CLI).

Em algumas encenações específicas é muito conveniente controlar aplicativos através do página da web e executar atividades relativas plataforma através da linha de comando. Abaixo de você pode encontrar um procedimento em como importar unicamente o certificado assinado da 3ª parte através do CLI. Neste Tomcat do exemplo o certificado é transferido arquivos pela rede. Para o CallManager ou o todo o outro aplicativo olha o mesmos.

Gerencia o certificado assinado de CA

Comandos summary

Uma lista dos comandos usados no artigo.

```
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
```

Verifique a informação correta do certificado

Aliste todos os certificados confiáveis transferidos arquivos pela rede.

```
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
```

Verifique quem emitiu o certificado para o serviço 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>
```

Este é um certificado auto-assinado desde que o expedidor combina o assunto.

Gerencia o pedido do sinal do certificado (o CSR)

Gerencia o CSR.

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

Verifique que o requst do sinal do certificado esteve gerado com sucesso.

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

Abra-o e copie-o o índice ao arquivo de texto. Salvar o como **arquivo tac_tomcat.csr**.

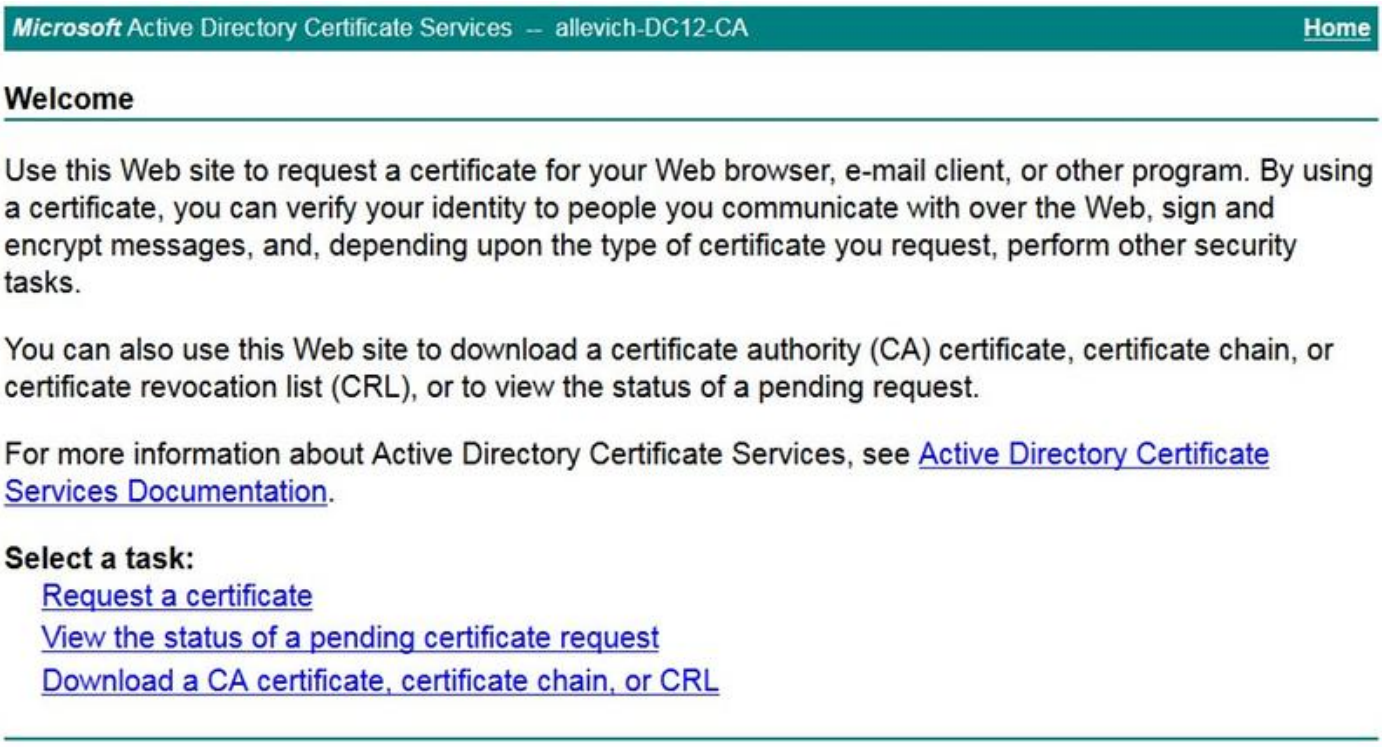
```
admin:show csr own tomcat

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

Gerencia o certificado de servidor de Tomcat

Gerencia um certificado para o serviço de Tomcat em CA.

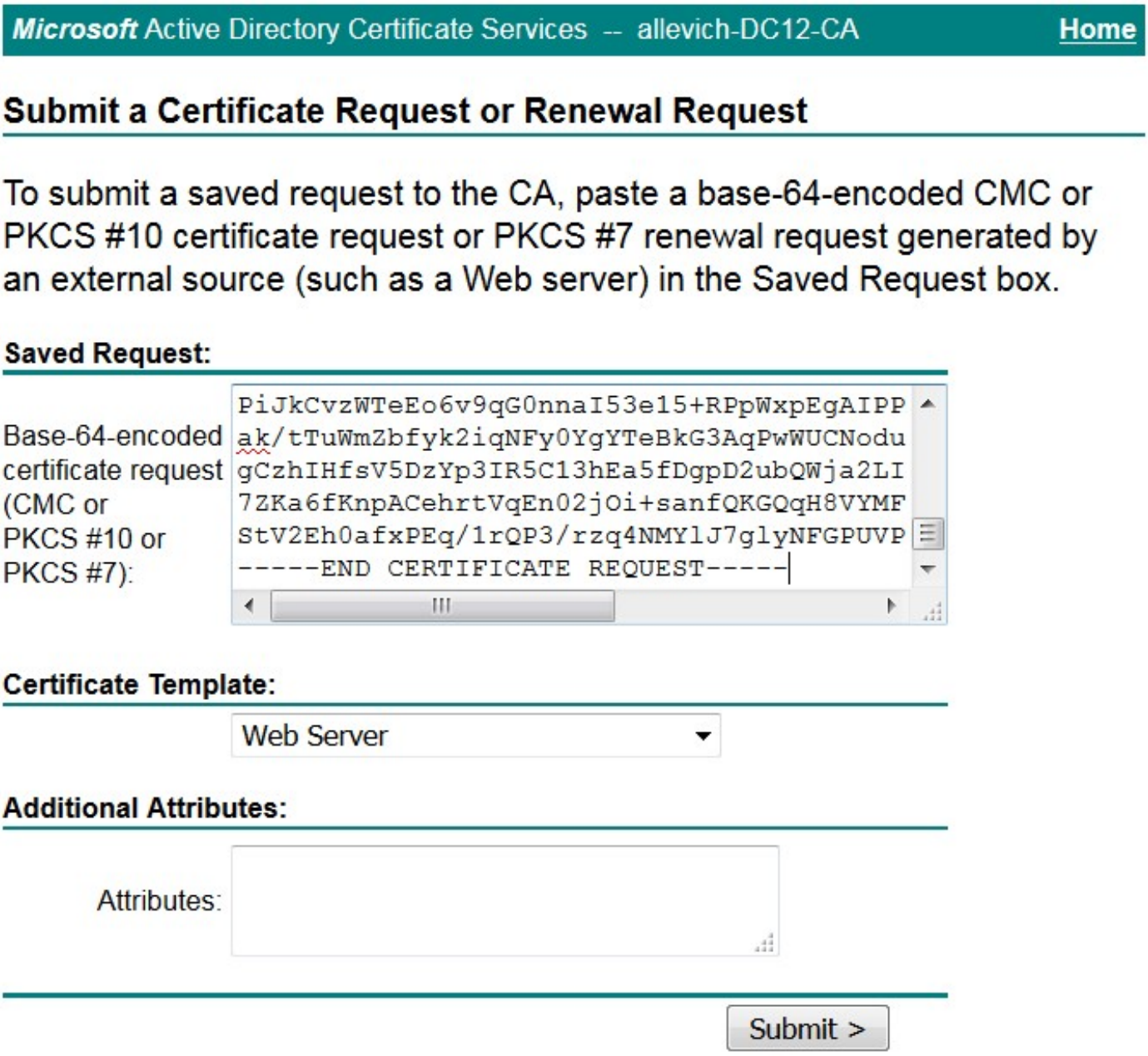
Abra o página da web para o Certificate Authority em um navegador. Põe as credenciais corretas na alerta da autenticação.

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



Transfira o certificado de raiz de CA. Selecione a **transferência um certificado de CA, um certificate chain, ou um** menu **CRL**. No menu seguinte escolha CA apropriado da lista. O método de codificação deve ser **Base64**. Transfira o certificado de CA e salvar o ao sistema operacional com nome **ca.cer**.

Pressione o **pedido um certificado** e um **pedido do certificado** então **avançado**. Ajuste o **molde de certificado ao** servidor de Web e cole o índice CSR do arquivo de texto **tac_tomcat.csr como mostrado**.



> Dica: Se a operação é feita no laboratório (ou o server de Cisco VOS e CA estão sob o mesmo campo administrativo) para salvar a cópia do tempo e para colar o CSR do buffer de memória.

A imprensa **submete-se**. Selecione a opção **codificada Base64** e transfira o certificado para o serviço de Tomcat.

> **Note**: Se a geração do certificado é executada no volume assegure para mudar um nome do certificado a um meaninful.

Importe o certificado de Tomcat ao server de Cisco VOS

Importe o certificado de CA

Abra o certificado de CA que foi armazenado com um nome **ca.cer**. Deve ser importado

primeiramente.

Copie seu índice ao buffer e datilografe o comando seguinte no CUCM CLI:

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

A alerta para colar o certificado de CA será indicada. Cole-a como mostrado abaixo.

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

Caso que uma transferência de arquivo pela rede do certificado de confiança é bem sucedida esta saída estará indicada.

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

Verifique que o certificado de CA está importado com sucesso como a Tomcat-confiança uma.

```
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 o certificado de Tomcat

A próxima etapa é importar o certificado assinado de Tomcat CA. A operação olha o mesmos que

com CERT da Tomcat-confiança, apenas o comando é diferente.

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

Reinicie o serviço

E ultimamente serviço de Tomcat do reinício.

```
utils service restart Cisco Tomcat
```

> Cuidado: Mantenha na mente que interrompe o funcionamento de serviços dependentes do servidor de Web, como a mobilidade de extensão, atendimentos faltados, diretório corporativo e o outro.

Verificar

Verifique o certificado que foi gerado.

```
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
```

Assegure-se de que o nome de emissor pertença a CA que construiu esse certificado.

Entre ao página da web datilografando o FQDN do server em um navegador e nenhum aviso do certificado será indicado.

Troubleshooting

O objetivo deste artigo é dar um procedimento com sintaxe de comando em como transferir arquivos pela rede o certificado através do CLI, para não destacar a lógica da chave pública Infrastucture (PKI). Não cobre o certificado SAN, CA subordinado, um comprimento chave de 4096 certificados e umas muitas outras encenações.

Em alguns casos raros ao transferir arquivos pela rede um certificado do servidor de Web através do CLI a operação falha com um Mensagem de Erro “incapaz de ler o certificado de CA”. Uma ação alternativa para aquela é instalar o certificado usando o página da web.

Uma configuração não padrão do Certificate Authority pode conduzir ao problema com instalação certificada. Tente gerar e instalar o certificado de um outro CA com uma configuração padrão básica.

Suporte para fora o plano

Caso que haverá uma necessidade de gerar um certificado auto-assinado pode igualmente ser feito no CLI.

Datilografe o comando abaixo e o certificado de Tomcat será regenerado ao auto-assinado.

```
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 um serviço novo de Tomcat do certificado deve ser reiniciada.

```
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]
```

Artigos relacionados

Certificado da transferência de arquivo pela rede através do página da web

Procedimento para obter e transferir arquivos pela rede o - do auto de Windows Server assinado ou o Certificate Authority (CA)…