

Configurar o certificado assinado 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 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 nos server de Cisco VOS e no 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 Communications 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 CallManager ou todo o outro aplicativo olha o mesmos.

Gerencia o certificado assinado 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
```


Gerencia o certificado de servidor de Tomcat

Gerencia um certificado para o serviço de Tomcat no CA.

Abra o página da web para o Certificate Authority em um navegador. Põe as credenciais corretas no alerta da autenticação.

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

Microsoft Active Directory Certificate Services – allevich-DC12-CA

[Home](#)

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Transfira o certificado de raiz CA. Selecione a **transferência um certificado de CA, um certificate chain, ou um** menu **CRL**. No menu seguinte escolha o CA apropriado da lista. O método de codificação deve ser a **base 64**. 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 **avanzado**. Ajuste o **molde de certificado** ao servidor de Web e cole o índice CSR do arquivo de texto **tac_tomcat.csr** como **mostrado**.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPP
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNodu
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LI
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMF
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

Dica: Se a operação é feita no laboratório (ou o server de Cisco VOS e o 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 **64 baixos a** opção **codificada** e transfira o certificado para o serviço de Tomcat.

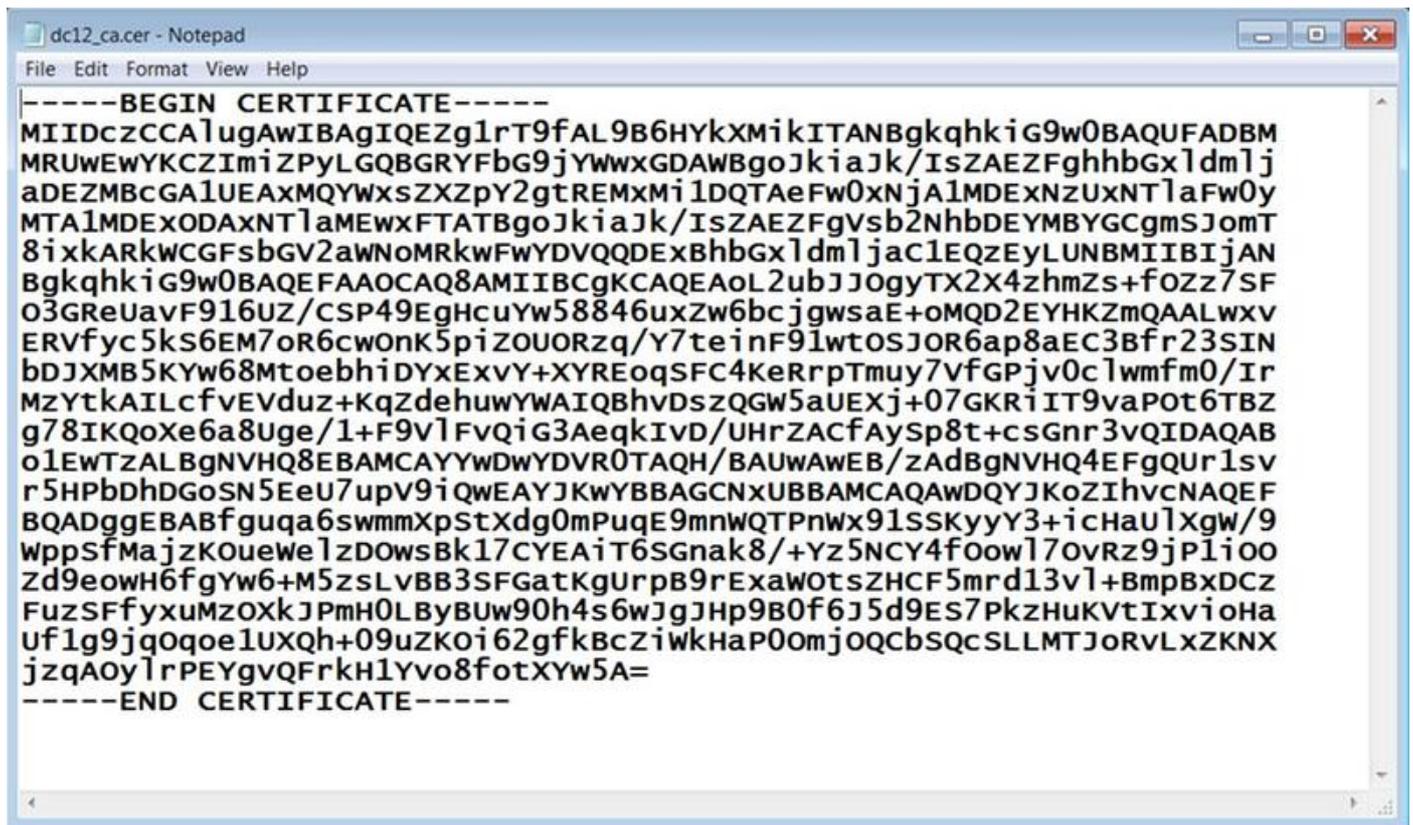
Nota: Se a geração do certificado é executada no volume assegure para mudar um nome do certificado a um meaningful.

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

O alerta para colar o certificado de CA será indicado. Cole-o 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/ucml-1.pem: Trust Certificate  
tomcat-trust/allevich-win-CA.pem: w2008r2 139  
<output omitted 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 da extensão, atendimentos faltados, diretório corporativo e o outro.

Verificar

Verifique o certificado que foi gerado.

```
admin:show cert own tomcat
```

```
[
  Version: V3
  Serial Number: 2765292404730765620225406600715421425487314965
  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 ao 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 Infrastructure (PKI). Não cobre o certificado SAN, o CA subordinado, o comprimento chave de 4096 certificados e as 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 \(CA\)...](#)