

通过在操作系统Cisco的语音的CLI配置CA签名的证书(VOS)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[生成CA签名的证书](#)

[Summary命令](#)

[检查正确的证书信息](#)

[生成认证符号请求\(CSR\)](#)

[生成Tomcat服务器证明](#)

[导入Tomcat认证Cisco VOS服务器](#)

[导入CA证书](#)

[导入Tomcat认证](#)

[重新启动服务](#)

[Verify](#)

[Troubleshoot](#)

[取消计划](#)

[相关条款](#)

Introduction

本文描述关于怎样的配置步骤加载在所有Cisco语音操作系统的(VOS)通过使用命令行界面(CLI)，基于Collaboration Server的第三方Certificate Authority (CA)签名的证书。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 公共密钥基础设施(PKI)基本的了解和其在Cisco VOS服务器和Microsoft CA的实施
- 预先配置DNS基础设施

Components Used

本文档中的信息基于以下软件和硬件版本：

- VOS服务器 : Cisco Unified通信管理器(CUCM)版本9.1.2
- CA : Windows 2012服务器
- 客户端浏览器 : Mozilla Firefox版本47.0.1

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

背景信息

在所有Cisco Unified Communications VOS产品中有至少两种证件类型 : 应用程序喜欢(ccmadmin、ccmservice、cuadmin , cfadmin , cuic)和VOS平台(cmplatform、drf , cli)。

在一些特定方案中通过网页管理应用程序和通过line命令执行平台涉及的活动是非常方便的。在您之下可以查找关于怎样的一个程序通过CLI独自地导入第三方签名的证书。在此示例Tomcat认证被加载。对于呼叫管理器或其他应用程序它查找同样。

生成CA签名的证书

Summary命令

用于条款的命令列表。

```
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
```

检查正确的证书信息

列出所有被加载的信任证书。

```
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
```

检查谁发行了Tomcat服务的认证。

```
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 omitted>
```

因为发布者匹配主题，这是自签证书。

生成认证符号请求(CSR)

生成CSR。

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

验证认证符号request顺利地生成了。

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

打开它并且复制内容到文本文件。保存它，**tac_tomcat.csr**文件。

```
admin:show csr own tomcat
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDSjCCAjICAQAwb0xCzAJBgNVBAYTAlBMMRQwEgYDVQQIEwtNYWxvcG9sc2tp
ZTEPMA0GA1UEBxMGS3Jha293MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFD
MR4wHAYDVQQQDExv1Y20xLTEuYWxsZXZpY2gubG9jYVwxSTBHBGNVBAUTQDlhMWJk
NDA5M2VjOGYxNj1jODhmNGUyZTYwZTYzM2RjNj1hZmFkNDY1YTgzMDhkNjRhNGU1
MzExOGQ0YjZkZjcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvo5jh
lMqTUnYbHQUnYpt00PTflWbj7hi6PSYI7pVCbGUZBpIZ5PKwTD56OZ8SgpjYX5Pf
l9D09H2gtQJTMVv1GmleGdlJsbuABRKn6lWkO6b706MiGSgqe1+41vnItjn3Y3kU
7h51nrUjye3HpPQzvXXpOKJ/JeJc8InEvQcC/UQmFMKn0ul00veFBHnG7TLDwDaQ
W1A1lrwrezN9Lwn2a/XZQR1P65sjmnkFFF2/FON4BmooeiinJD0G+F4bKiglymlR
84faF27plwHjcw8Wan2HwJT607TaE6EOJd0sgLU+HFAl3txKycS0NvLuMZYQH81s
/C74CIRWibEWT2qLAGMBAAGRzBFBGkqhkiG9w0BCQ4xODA2MCcGA1UdJQgqMB4G
CCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAWUwCwYDVR0PBAQDAgO4MA0GCSqG
SIb3DQEBBQUAA4IBAQBUn1FhKuyQ1X58A6+7KPkYsWtioS0PoycltuQsVo0aav82
PiJkCvzWTeEo6v9qG0nnaI53e15+RppWxpEgAIPPhtt6asDuW30SqSx4eClfgmKH
ak/tTuWmZbfyk2iqNFy0YgYTEbK3AqPwWUCNoduPZ0/fo4lQoJPwje184U64WXB
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LId85NGHEiqyiWqwm07pTkBc+
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMFsW2uYFj9pf/Wn4aDGuJoqdOH
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----
```

生成Tomcat服务器证明

生成Tomcat服务的一个认证在CA。

打开认证机关的网页在浏览器。放置正确的证件在认证提示。

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

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](#)

下载CA根证明。选择**下载CA证书、证书链或者CRL**菜单。在Next菜单从列表请选择适当的CA。编码方法应该是Base64。下载CA证书并且保存它对操作系统与命名ca.cer。

按**请求认证**然后**提前的证书请求**。设置**认证模板**为Web服务器并且粘贴CSR内容从文本文件tac_tomcat.csr如显示。

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 >

提示：如果操作在实验室里完成(或Cisco VOS服务器和CA在)节省时间的同样管理域下复制和插入从存储器缓冲区的CSR。

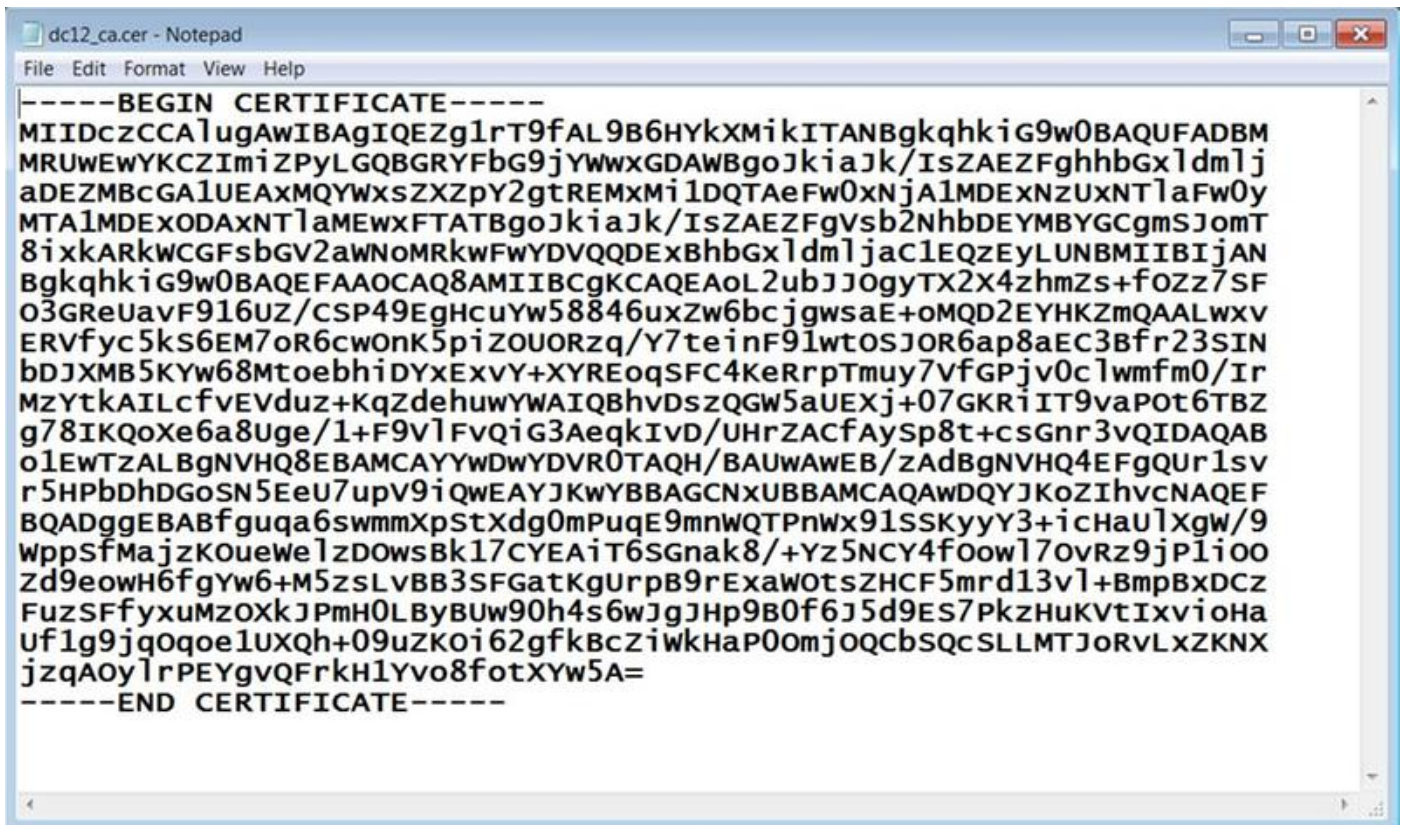
出版社**提交**。选择**Base64编码**的选项并且下载Tomcat服务的认证。

Note:如果认证生成进行散装请保证更改认证的名字到一meaningful一个。

导入Tomcat认证Cisco VOS服务器

导入CA证书

打开存储与命名**ca.cer**的CA证书。必须首先导入它。



复制其内容到缓冲区并且键入以下in命令CUCM CLI :

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

粘帖CA证书的提示将显示。粘帖它如下所示。

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

万一信任认证加载是成功的此输出将显示。

```
admin:set cert import trust tomcat
```

Paste the Certificate and Hit Enter

验证CA证书成功导入作为Tomcat信任一。

```
admin:show cert list trust
```

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

导入Tomcat认证

下一步是导入Tomcat CA签名的证书。操作查找同样与Tomcat信任cert，命令不同的。

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

重新启动服务

并且请最后重新启动Tomcat服务。

```
utils service restart Cisco Tomcat
```

警告：记住它打乱Web服务器从属的服务的操作，类似扩展移动性、未接电话，公共目录和其他。

Verify

验证生成的认证。

```
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=ucml-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
```

保证发证者名字属于修建该认证的CA。

登陆对网页通过键入服务器的FQDN在浏览器的，并且认证警告不会显示。

Troubleshoot

此条款的目标是产生与命令句法的一个程序关于怎样通过CLI加载认证，不突出显示逻辑公共密钥Infrastructure (PKI)。它不包括SAN认证、辅助CA、4096个认证密钥长度和许多其他方案。

少许罕见的情况，当加载Web服务器认证通过CLI操作失效与无法的错误信息“读CA证书”时。那的一个解决方法是安装认证使用网页。

一种非标准的认证机关配置可能导致认证安装的问题。设法从与一个基本的默认配置的另一个CA生成和安装认证。

取消计划

万一将有需要生成自签证书在CLI可能也执行。

键入下面命令，并且Tomcat认证将被重新生成到自己签署的一个。

```
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.
必须重新启动要运用新证书Tomcat服务。

```
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]
```

相关条款

[加载认证通过网页](#)

[程序获得并上载Windows服务器自己-签字的或Certificate Authority \(CA\)...](#)