

配置在CVP服务器的CA签名证书HTTPS Web访问的

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[命令参考参考目录](#)

[做一个备份](#)

[生成 CSR](#)

[列出证书](#)

[删除现有OAMP证书](#)

[生成密钥对](#)

[生成新的CSR](#)

[发行在CA的证书](#)

[导入CA生成的证书](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文描述如何配置和验证在思科语音门户(CVP)操作管理和门户(OAMP)服务器的Certificate Authority (CA)签名证书。

[先决条件](#)

Microsoft Windows已经预先配置基于认证机关服务器。

[要求](#)

思科建议您有PKI基础设施的知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

CVP版本11.0

Windows 2012 R2服务器

Windows 2012个R2认证机关

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

命令参考参考目录

```
more c:\Cisco\CVP\conf\security.properties
cd c:\Cisco\CVP\conf\security
```

```
%kt% -list
%kt% -list | findstr Priv
%kt% -list -v -alias oamp_certificate
```

```
%kt% -genkeypair -alias oamp_certificate -v -keysize 2048 -keyalg RSA
%kt% -import -v -trustcacerts -alias oamp_certificate -file oamp.p7b
```

做备份

导航到文件夹c:\Cisco\CVP\conf\security并且归档所有文件。如果OAMP Web访问不工作，请替换新建立的文件与那个从备份。

生成 CSR

检查您的安全密码。

```
more c:\Cisco\CVP\conf\security.properties
Security.keystorePW = fc]@2zfe*Ufe2J,.0uM$Ff
```

导航到c:\Cisco\CVP\conf\security文件夹。

```
cd c:\Cisco\CVP\conf\security
```

注意：在此条款，Windows环境变量用于使Keytool命令更短和更加可读。在所有keytool命令被添加前，请保证变量初始化。

1. 创建一个临时变量。

```
set kt=c:\Cisco\CVP\jre\bin\keytool.exe -storepass fc]@2zfe*Ufe2J,.0uM$Ff -storetype JCEKS -
keystore .keystore
```

输入命令保证变量初始化。输入正确密码。

```
echo %kt%
c:\Cisco\CVP\jre\bin\keytool.exe -storepass fc]@2zfe*Ufe2J,.0uM$Ff -storetype JCEKS -keystore
.keystore
```

列出证书

列出在keystore的当前安装的证书。

```
%kt% -list
```

提示：如果要完善您的列表您能修改命令显示仅自签名证书。

```
%kt% -list | findstr Priv
```

```
vxml_certificate, May 27, 2016, PrivateKeyEntry, oamp_certificate, May 27, 2016,  
PrivateKeyEntry, wsm_certificate, May 27, 2016, PrivateKeyEntry, callserver_certificate, May 27,  
2016, PrivateKeyEntry,
```

验证自己签署的OAMP认证信息。

```
%kt% -printcert -file oamp.crt
```

```
Owner: CN=CVP11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL Issuer: CN=CVP11, OU=TAC,  
O=Cisco, L=Krakow, ST=Malopolskie, C=PL Serial number: 3f44f086 Valid from: Fri May 27 08:13:38  
CEST 2016 until: Mon May 25 08:13:38 CEST 2026 Certificate fingerprints: MD5:  
58:F5:D3:18:46:FE:9A:8C:14:EA:73:0F:5F:12:E7:43 SHA1:  
51:7F:E7:FF:25:B6:B8:02:CD:18:84:E7:50:9E:F2:ED:B1:9E:78:40 Signature algorithm name:  
SHA1withRSA Version: 3
```

删除现有OAMP证书

为了生成一个新密钥对，请删除已经存在的证书。

```
%kt% -delete -alias oamp_certificate
```

生成密钥对

运行此命令生成别名的一个新密钥对与选定密钥大小。

```
%kt% -genkeypair -alias oamp_certificate -v -keysize 2048 -keyalg RSA
```

```
What is your first and last name?
```

```
[Unknown]: cvp11.allevich.local
```

```
What is the name of your organizational unit?
```

```
[Unknown]: TAC
```

```
What is the name of your organization?
```

```
[Unknown]: Cisco
```

```
What is the name of your City or Locality?
```

```
[Unknown]: Krakow
```

```
What is the name of your State or Province?
```

```
[Unknown]: Malopolskie
```

```
What is the two-letter country code for this unit?
```

```
[Unknown]: PL
```

```
Is CN=cvp11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL correct?
```

```
[no]: yes
```

```
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA)
```

```
with a validity of 90 days for: CN=cvp11, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL
```

```
(RETURN if same as keystore password):
```

```
[Storing .keystore]
```

验证密钥对生成。

```
c:\Cisco\CVP\conf\security>dir | findstr oamp.key
```

```
05/27/2016 08:13 AM 1,724 oamp.key
```

保证输入名和姓作为您的OAMP服务器。名称一定是可解决对IP地址。此名称在证书的CN字段将出现。

生成新的CSR

运行此命令生成别名的证书请求和保存它到文件(例如， oamp.csr)。

```
%kt% -certreq -alias oamp_certificate -file oamp.csr
```

验证CSR顺利地生成。

```
dir oamp.csr
```

```
08/25/2016 08:13 AM 1,136 oamp.csr
```

发行在CA的证书

要获得证书您将需要一认证机关已经已配置的。

键入在浏览器的给的URL

http:// <CA IP地址>/certsrv

然后Select请求证书和先进的证书请求。

```
more oamp.csr
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----
```

```
MIIC/TCCAeUCAQAwgYcxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGFSbGV2aWN0LmXvY2FsmQswCQYD
VQQGEWJQTDEUMBIGALUECBMLTWFSb3BvbHNraWUxDzANBgNVBACTBktyYWtvdzEOMAwGA1UEChMF
Q21zY28xDDAKBgNVBASATA1RBQzEOMAwGA1UEAxMFQ1ZQMTEwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAAoIBAQCvQEGmJpzmimQA6zclmbWnkzAj3PvGKe9Qg0REfOnHpLq+ddx66o6OGr6TTb1
BrqI8UeN1JDfuQj/m4HZvKsqRv1AWA5CtGRzjbOeNXPMCGotk00b9643M8DY0Q9LQ/+PxdzYGhie
CxnHQURcAIsViphV4yxUVJ4QcLkzkbM9T8DSoSJSJAI4gY+tO3i0xxDTcxlaTQ1xkRYDba8JwzVHL
TkVwtSRK2jqIzJuBPZwpXMZc8RDkffBurrVXhFb8ylvR/Q7cAzHPgpPLuK6KmwpOKv8CRoWml3xA
EgRd39szkZfbawRzddTqw8hM/2cLSouKx0NMFY5dXzIszQEYlK5XAgMBAAGgMDAuBgkqhkiG9w0B
CQ4xITAFMB0GA1UdDgQWBRe8ul0CdlHckIm9VjD3ZL/uXhgGzANBgkqhkiG9w0BAQsFAAOCAQEA
c48VDld/BJMAOXwxz5riT1BCjxzLIMTNzv3W00K7ehtmYVTTaRCXLZ/sOX5ws807kwnOaZeIpRzd
lGvumS+dUgun/2Q00rp+B44gRv9KUTvv5C6YoBslm4H2xp9yaQpgzLBJuKRgl8yIzYnIvoVuPx
racGSkyxKzxvrvxOX2qvxoVq71bf43Aps4+G85Cp3GWhIBQ+TtIKKxgZ/C64ThZgT9HtD9zbL3g0
U8bP1F6JNjztzjmuGEdqsnf0fAjpPsfShQ10o4qIMBi7hBQusAwNBEB1xaAlYumD09+R/BK2KfMv
Iy4CdsEfWlmjBb54lTJEYzwOh7tpRZkjOqyVMQ==
```

```
-----END NEW CERTIFICATE REQUEST-----
```

复制和插入CSR的整个内容对合适的菜单。选择**Web服务器**，认证模板和**Base64编码**。然后请单击**下载证书链**。

您能单个导出CA和Web服务器生成的证书或下载全双工一系列。在本例中使用全双工一系列选项。

导入CA生成的证书

安装证书从文件。

```
%kt% -import -v -trustcacerts -alias oamp_certificate -file oamp.p7b
```

要应用新证书请重新启动**Web发布服务**和**思科CVP OPSConsoleServer**服务。

验证

使用本部分可确认配置能否正常运行。

验证的简便的方法是登陆对**CVP OAMP Web服务器**。您不应该收到一个不信任证书警告消息。

另一个方式将检查OAMP证书与此命令一起使用。

```
%kt% -list -v -alias oamp_certificate
```

```
Alias name: oamp_certificate
```

```
Creation date: Oct 20, 2016
```

```
Entry type: PrivateKeyEntry
```

```
Certificate chain length: 2
```

```
Certificate[1]:
```

Owner: CN=cvp11.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL
Issuer: CN=pod1-POD1AD-CA, DC=pod1, DC=ccemea, DC=tac
Serial number: 130c0db6000000000017
Valid from: Thu Oct 20 12:48:08 CEST 2016 until: Sat Oct 20 12:48:08 CEST 2018
Certificate fingerprints:
MD5: BA:E8:FA:05:45:07:D0:3C:C8:81:1C:34:3D:21:AF:AC
SHA1: 30:04:F2:EE:37:22:9D:8D:27:8F:54:D2:BA:D4:0F:33:74:34:87:D8
Signature algorithm name: SHA1withRSA
Version: 3

Extensions:

#1: ObjectID: 1.3.6.1.4.1.311.20.2 Criticality=false
0000: 1E 12 00 57 00 65 00 62 00 53 00 65 00 72 00 76 ...W.e.b.S.e.r.v
0010: 00 65 00 72 .e.r

#2: ObjectID: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
[
accessMethod: caIssuers
accessLocation: URIName: ldap:///CN=pod1-POD1AD-CA,CN=AIA,
]
]

#3: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 9B 33 47 9E 76 DB F3 92 B2 F8 F9 86 3A 59 BA DE .3G.v.....:Y..
0010: C5 0B E5 E4
]
]

#4: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
[DistributionPoint:
[URIName: ldap:///CN=pod1-POD1AD-CA,CN=POD1AD,CN=CDP]
]]

#5: ObjectID: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
serverAuth
]

#6: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
DigitalSignature
Key_Encipherment
]

#7: ObjectID: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: CD FC 95 D1 60 44 9A 34 A9 EE 0E 3F C7 F5 5D 3C`D.4...?...<
0010: 46 DF 47 D9 F.G.
]
]

Certificate[2]:

Owner: CN=pod1-POD1AD-CA, DC=pod1, DC=ccemea, DC=tac
Issuer: CN=pod1-POD1AD-CA, DC=pod1, DC=ccemea, DC=tac
Serial number: 305dba13e0def8b474fefeb92f54acd
Valid from: Thu Sep 08 18:06:37 CEST 2016 until: Wed Sep 08 18:16:36 CEST 2021
Certificate fingerprints:

```
MD5: 50:04:5F:89:CA:7C:D6:71:82:10:C3:04:57:78:AB:AE
SHA1: A6:3B:07:29:AF:3A:07:73:9D:9B:4F:88:B5:A8:17:AC:0A:6D:C3:0D
Signature algorithm name: SHA1withRSA
Version: 3
```

Extensions:

```
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00 ...
```

```
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]
```

```
#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
DigitalSignature
Key_CertSign
Crl_Sign
]
```

```
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 9B 33 47 9E 76 DB F3 92 B2 F8 F9 86 3A 59 BA DE .3G.v.....:Y..
0010: C5 0B E5 E4 ....
]
]
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

如果需要验证命令语法参考配置和管理指南CVP的。

http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp8_5/configuration/guide/ConfigAdminGuide_8-5.pdf

相关信息

[通过在思科语音操作系统\(VOS\)的CLI配置CA签名证书](#)

[步骤获得并上载Windows服务器赛弗-签字的或Certificate Authority \(CA\)...](#)

技术支持和文档 - Cisco Systems