

Configurar o certificado assinado de CA no server CVP para o acesso à Web HTTPS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Lista de referência de comandos](#)

[Faça um backup](#)

[Gerencia o CSR](#)

[Aliste os Certificados](#)

[Remova o certificado existente OAMP](#)

[Gerencia o par de chaves](#)

[Gerencia o CSR novo](#)

[Emita o certificado em CA](#)

[Importe o certificado gerado CA](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e verificar o certificado assinado do Certificate Authority (CA) no server portal do portal da administração e do Gerenciamento da operação da Voz de Cisco (CVP) (OAMP).

Pré-requisitos

Microsoft Windows baseou o server do Certificate Authority já preconfigured.

Requisitos

Cisco recomenda que você tem o conhecimento da infraestrutura PKI.

[Componentes Utilizados](#)

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

Versão 11.0 CVP

Server R2 de Windows 2012

Certificate Authority R2 de Windows 2012

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.

Configurar

Lista de referência de comandos

```
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
```

Faça um backup

Navegue ao dobrador `c:\Cisco\CVP\conf\security` e archive todos os arquivos. Se o acesso à Web OAMP não trabalha, substitua arquivos recém-criados com esses do backup.

Gerencia o CSR

Verifique sua senha de segurança.

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

Navegue ao dobrador de `c:\Cisco\CVP\conf\security`.

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

Nota: Neste artigo, a variável de ambiente Windows é usada para fazer comandos de Keytool muito mais curtos e mais legíveis. Antes que todo o comando do keytool esteja adicionado, assegure-se de que a variável esteja inicializada.

1. Crie uma variável provisória.

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

Incorpore o comando assegurar-se de que a variável esteja inicializada. Incorpore a senha correta.

```
echo %kt%
```

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

Aliste os Certificados

Aliste Certificados atualmente instalados no keystore.

```
%kt% -list
```

Dica: Se você quer refinar sua lista você pode alterar o comando indicar somente certificados auto-assinados.

```
%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,
```

Verify auto-assinou a informação de certificação OAMP.

```
%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
```

Remova o certificado existente OAMP

A fim gerar um par de chaves novo, remova o certificado que já existe.

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

Gerencia o par de chaves

Execute este comando gerar um par de chaves novo para o pseudônimo com tamanho chave selecionado.

```
%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]
```

Verifique que o par de chaves esteve gerado.

```
c:\Cisco\CVP\conf\security>dir | findstr oamp.key  
05/27/2016 08:13 AM 1,724 oamp.key
```

Assegure para dar entrada com o nome e sobrenome como seu server OAMP. O nome deve ser solucionável a um endereço IP de Um ou Mais Servidores Cisco ICM NT. Este nome aparecerá no campo do CN do certificado.

Gerencia o CSR novo

Execute este comando gerar o pedido do certificado para o pseudônimo e salvar o a um arquivo (por exemplo, oamp.csr).

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

Verifique que o CSR esteve gerado com sucesso.

```
dir oamp.csr
```

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

Emita o certificado em CA

Para obtê-lo ao certificado precisará um Certificate Authority já configurado.

Datilografe a URL dada em um navegador

endereço IP de Um ou Mais Servidores Cisco ICM NT >/certsrv de http:// <CA

Selecione então o **certificado do pedido** e **pedido do certificado avançado**.

```
more oamp.csr
```

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

```
MIIC/TCCAeUCAQAwgYcxIzAhBgkqhkiG9w0BCQEWFgFkbWluQGFSbGV2aWN0LmxvY2FsMQswCQYD  
VQQGEWJQTDEUMBIGAlUECBMLTWFsb3BvbHNraWUxZDZANBgNVBACTBktyYWtvdzEOMAwGA1UEChMF  
Q2l2Y28xDDAKBgNVBAStA1RBQzEOMAwGA1UEAxMFQ1ZQMTEWggEiMA0GCSqGSIb3DQEBAQUAA4IB  
DwAwggEKAoIBAQCvQEGmJpmzimqQA6zclmbWnkzAj3PvGKE9Qg0REfOnHpLq+ddx66o6OGr6TTb1  
BrqI8UeN1JdfuQj/m4HZvKsqRv1AWA5CtGRzjbOeNXPMCGotk00b9643M8DY0Q9LQ/+PxdzYGhie  
CxnHQURcAlSviphV4yxUVJ4QcLkzkbM9T8DSOJSJAI4gY+t03i0xxDTcXlaTQ1xkRYDba8JwzVHL  
TkVwtSRK2jqIzJuBPZwpXMZc8RDkffBurrVXhFb8ylvR/Q7cAzHPgpPLuK6KmwpOKv8CROWml3xA  
EgRd39szkZfbawRzddTqw8hM/2cLSoUKx0NMFY5dXzIszQFYlK5XAgMBAAGgMDAuBgkqhkiG9w0B  
CQ4xITAFMB0GA1UdDgQWBRe8u10Cd1HckIm9VjD3ZL/uXhgGzANBgkqhkiG9w0BAQsFAAOCAQEA  
c48VD1d/BJMaOXwz5riT1BCjxzLIMTNzv3W0K7ehtmYVTTaRCXLZ/sOX5ws807kwnOaZeIprzd  
lGvumS+dUgun/2QO0rp+B44gRvqp9KUTvv5C6YoBslm4H2xp9yaQpgzLBjuKRgl8yIzYnIvoVuPx  
racGSkyxKzxvrvxOX2qvxoVq71bf43Aps4+G85Cp3GWhIBQ+TtIKKxgZ/C64ThZgT9HtD9zbL3g0  
U8bPlF6JNjztzjmuGEdqsnf0fAjpPsfShQl0o4qIMBi7hBQusAwNBEB1xaAlYumD09+R/BK2KfMv  
Iy4CdsEfWlmjBb541TJEYzwOh7tpRZkjOqyVMQ==
```

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

A cópia e cola o índice inteiro do CSR ao menu apropriado. Selecione o **servidor de Web** como um molde de certificado e **Base64 codificaram**. Clique então o **certificate chain** da transferência.

Você pode exportar CA e o certificado gerado servidor de Web individualmente ou transferir uma corrente completa. Neste exemplo a opção da corrente completa é usada.

Certificado gerado CA da importação

Instale o certificado do arquivo.

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

Para aplicar o certificado novo reinicie serviços do **Serviço de Publicação na Web** e do **Cisco CVP OPSConsoleServer**.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A maneira a mais fácil de verificar é entrar ao servidor de Web CVP OAMP. Você não deve receber um mensagem de advertência não confiável do certificado.

Uma outra maneira é verificar o certificado OAMP usado com este comando.

```
%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 ....  
]  
]
```

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Se você precisa de verificar a sintaxe de comando refira a configuração e o Guia de Administração para o CVP.

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

Informações Relacionadas

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

[Procedimento para obter e transferir arquivos pela rede o - do auto de Windows Server assinado ou o Certificate Authority \(CA\)...](#)

Suporte Técnico e Documentação - Cisco Systems