Certificado firmado de CA de la configuración en el servidor del CVP para el Acceso Web HTTPS

Contenido

Introducción

Este documento describe cómo configurar y verificar el certificado firmado del Certificate Authority (CA) en el servidor porta del portal de la administración y de la Administración de la operación de la Voz de Cisco (CVP) (OAMP).

Prerrequisitos

Microsoft Windows basó el servidor del Certificate Authority se preconfigura ya.

Requisitos

Cisco recomienda que usted tiene conocimiento de la infraestructura PKI.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Versión 11.0 del CVP

Servidor del r2 de Windows 2012

Certificate Authority del r2 de Windows 2012

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Lista de referencia 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
```

Haga un respaldo

Navegue a la carpeta **c:\Cisco\CVP\conf\security** y archive todos los archivos. Si el Acceso Web OAMP no trabaja, substituya los archivos creados recientemente por los que está del respaldo.

Genere el CSR

Marque su contraseña de seguridad.

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

Navegue a la carpeta de **c:\Cisco\CVP\conf\security**.

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

> **Note**: En este artículo, la variable del entorno Windows se utiliza para hacer los comandos de Keytool mucho más cortos y más legibles. Antes de que se agregue cualquier comando del keytool, asegúrese de que la variable esté inicializada.

1. Cree una variable temporal.

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

Ingrese el comando de asegurarse de que la variable está inicializada. Ingrese la contraseña correcta.

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

Enumere los Certificados

Enumere los Certificados actualmente instalados en el keystore.

```
%kt% -list
```

> Consejo: Si usted quiere refinar su lista usted puede modificar el comando de visualizar solamente los certificados autofirmados.

```
%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 uno mismo-firmó la información de certificación 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
```

Quite el certificado existente OAMP

Para generar un nuevo par clave, quite el certificado que existe ya.

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

Genere el par clave

Funcione con este comando de generar un nuevo par clave para el alias con el tamaño de clave seleccionado.

```
%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 el par clave fuera generado.

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

Asegure para ingresar el nombre y apellido como su servidor OAMP. El nombre debe ser resolvable a una dirección IP. Este nombre aparecerá en el campo CN del certificado.

Genere el nuevo CSR

Funcione con este comando de generar el pedido de certificado para el alias y de salvarlo a un archivo (por ejemplo, oamp.csr).

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

Verifique que el CSR fuera generado con éxito.

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

Publique el certificado en CA

Para conseguirle al certificado necesitará un Certificate Authority configurado ya.

Teclee el URL dado en un navegador

IP Address >/certsrv de http:// <CA

Entonces seleccione el **certificado de la petición** y el **pedido de certificado avanzado**.

```
more oamp.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC/TCCAeUCAQAwgYcxIzAhBgkqhkiG9w0BCQEWFGFkbWluQGFsbGV2aWNoLmxvY2FsMQswCQYD
VQQGEwJQTDEUMBIGA1UECBMLTWFsb3BvbHNraWUxDzANBgNVBAcTBktyYWtvdzEOMAwGA1UEChMF
Q2lzY28xDDAKBgNVBAsTA1RBQzEOMAwGA1UEAxMFQ1ZQMTEwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCvQEGmJPmzimqQA6zc1mbWnkzAj3PvGKe9Qg0REfOnHpLq+ddx66o6OGr6TTb1
BrqI8UeN1JDfuQj/m4HZvKsqRv1AWA5CtGRzjbOeNXPMCGOtkO0b9643M8DY0Q9LQ/+PxdzYGhie
CxnhQURcAIsViphV4yxUVJ4QcLkzkbM9T8DSoJSJAI4gY+tO3i0xxDTcxlaTQ1xkRYDba8JwzVHL
TkVwtSRK2jqIzJuBPZwpXMZc8RDkffBurrVXhFb8ylvR/Q7cAzHPgpPLuK6KmwpOKv8CRoWml3xA
EgRd39szkZfbawRzddTqw8hM/2cLSoUKx0NMFY5dXzIszQEYlK5XAgMBAAGgMDAuBgkqhkiG9w0B
CQ4xITAfMB0GA1UdDgQWBBRe8ul0CdlHckIm9VjD3ZL/uXhgGzANBgkqhkiG9w0BAQsFAAOCAQEA
c48VD1d/BJMaOXwxz5riT1BCjxzLIMTNzv3W00K7ehtmYVTTaRCXLZ/sOX5ws807kwnOaZeIpRzd
lGvumS+dUgun/2QO0rp+B44gRvgp9KUTvv5C6YoBslm4H2xp9yaQpgzLBJuKRgl8yIzYnIvoVuPx
racGSkyxKzxvrvxOX2qvxoVq71bf43Aps4+G85Cp3GWhIBQ+TtIKKxgZ/C64ThZgT9HtD9zbL3g0
U8bPlF6JNjztzjmuGEdqsNf0fAjpPsfShQl0o4qIMBi7hBQusAwNBEB1xaAlYumD09+R/BK2KfMv
Iy4CdsEfWlmjBb54lTJEYzwOh7tpRZkjOqyVMQ==
-----END NEW CERTIFICATE REQUEST-----
```

La copia y pega el contenido entero del CSR al menú apropiado. Seleccione al **servidor Web** como un Certificate Template plantilla de certificado y un **base 64 codificaron**. Entonces haga clic

la **Cadena de certificados de la descarga**.

Usted puede exportar CA y el certificado generado servidor Web individualmente o descargar un encadenamiento lleno. En este ejemplo se utiliza la opción del encadenamiento lleno.

Certificado generado CA de la importación

Instale el certificado del archivo.

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

Para aplicar el nuevo certificado recomience los servicios de **OPSConsoleServer del CVP del servicio editorial de Internet** y de **Cisco**.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La manera más fácil de verificar es iniciar sesión al servidor Web del CVP OAMP. Usted no debe conseguir un mensaje de advertencia untrusted del certificado.

Otra manera es marcar el certificado OAMP usado con 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 sección brinda información que puede utilizar para la solución de problemas en su configuración.

Si usted necesita verificar la sintaxis de los comandos refiera a la configuración y a la guía de administración para el 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

Información Relacionada

Certificado firmado de CA de la configuración vía el CLI en el sistema operativo de la Voz de Cisco (VOS)

Procedimiento para obtener y para cargar el - del uno mismo del Servidor Windows firmado o el Certificate Authority (CA)…

Soporte Técnico y Documentación - Cisco Systems