在CVP伺服器上為HTTPS Web訪問配置CA簽名證書

目錄

簡介

本檔案介紹如何在思科語音入口網站(CVP)營運管理入口網站(OAMP)伺服器上設定和驗證憑證授權單位(CA)簽署的憑證。

必要條件

已預配置基於Microsoft Windows的證書頒發機構伺服器。

需求

思科建議您瞭解PKI基礎設施。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

CVP版本11.0

Windows 2012 R2伺服器

Windows 2012 R2證書頒發機構

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

命令參考清單

```
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
```

製作備份

導航到資料夾c:\Cisco\CVP\conf\security並存檔所有檔案。如果OAMP Web訪問不起作用，請使用備份的檔案替換新建立的檔案。

產生CSR

檢查您的安全密碼。

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

導航到c:\Cisco\CVP\conf\security檔案夾。

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

> **附註**：本文使用Windows環境變數使Keytool命令更簡短，更易讀。在新增任何keytool命令之前，請確保已初始化變數。

1.建立臨時變數。

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

輸入命令以確保初始化變數。輸入正確的密碼。

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

列出憑證

列出金鑰庫中當前安裝的證書。

```
%kt% -list
```

提示：如果要最佳化清單，可以修改命令以僅顯示自簽名證書。

```
%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,
```

驗證自簽名OAMP認證資訊。

```
%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
```

刪除現有的OAMP證書

若要產生新的金鑰對，請移除已存在的憑證。

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

生成金鑰對

運行此命令可為具有選定金鑰大小的別名生成新的金鑰對。

```
%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]
```

驗證是否已產生金鑰對。

```
c:\Cisco\CVP\conf\security>dir | findstr oamp.key
05/27/2016  08:13 AM             1,724 oamp.key
```
確保輸入名字和姓氏作為OAMP伺服器。名稱必須可解析為IP地址。此名稱將出現在憑證的CN欄位中。

產生新的CSR

運行此命令可生成別名的證書請求並將其儲存到檔案（例如oamp.csr）。

```
%kt% -certreq -alias oamp_certificate -file oamp.csr
```
驗證是否成功產生CSR。

```
dir oamp.csr
08/25/2016 08:13 AM 1,136 oamp.csr
```
在CA上發出憑證

要獲取證書，您需要已配置證書頒發機構。

在瀏覽器中輸入給定的URL

http://<CA ip address>/certsrv

然後選擇Request certificate和Advanced certificate request。

```
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-----
```
將CSR的整個內容複製貼上到適當的功能表。選擇Web Server作為證書模板，然後選擇Base 64 encoded。然後按一下「Download certificate chain」。

您可以單獨匯出CA和Web伺服器生成的證書，也可以下載完整的證書鏈。在此示例中，使用全鏈選項。

匯入CA生成的證書

從檔案安裝證書。

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

要應用新證書，請重**新啟動全球資訊網發佈服**務和**思科**CVP OPSConsoleServer服務。

驗證

使用本節內容，確認您的組態是否正常運作。

最簡單的驗證方法是登入到CVP OAMP Web伺服器。您不應收到不受信任的證書警告消息。

另一種方法是檢查使用此指令的OAMP憑證。

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如果您需要驗證命令語法，請參閱CVP的配置和管理指南。

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

相關資訊

在思科語音作業系統(VOS)中通過CLI配置CA簽名的證書

獲取和上傳Windows Server自簽名或證書頒發機構(CA)的過程……

技術支援與文件 - Cisco Systems