HTTPS Web アクセスのための CVP サーバの設定 CA 署名入り認証

目次

概要

この資料に Cisco 音声門脈（CVP）オペレーション管理および管理ポータル（OAMP）サーバの認証局（CA） 署名入り認証を設定し確認する方法を記述されています。

前提条件

Microsoft Windows は認証権限サーバを既に前もって構成されています基づかせていました。

要件

Cisco は PKI インフラストラクチャのナレッジがあることを推奨します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

CVP バージョン 11.0

Windows 2012 R2 サーバ

Windows 2012 R2 認証局（CA）

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

コマンドレファレンス リスト

```
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
```

バックアップを作成して下さい

フォルダ c:\Cisco\CVP\conf\security にナビゲートし、すべてのファイルをアーカイブして下さい。 OAMP Web アクセスがはたらかない場合、バックアップからの物と新しく作成されたファイルを置き換えて下さい。

CSR の生成

セキュリティパスワードを確認して下さい。

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

c:\Cisco\CVP\conf\security フォルダにナビゲートして下さい。

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

> **注:** この技術情報では Keytool コマンドを大いにより短くおよびより読解可能にさせるのに、ウィンドウ環境変数が使用されています。 どの keytool コマンドでも追加される前に、変数が初期化されるようにして下さい。

1. テンポラリ変数を作成して下さい。

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

変数が初期化されるようにするためにコマンドを入力して下さい。 正しいパスワードを入力して下さい。

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

証明書をリストして下さい

keystore の現在インストール済み証明書をリストして下さい。

```
%kt% -list
```

> **ヒント**： リストを精製したいと思えば自己署名証明書だけ表示するためにコマンドを修正できます。

```
%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,
```

自己署名 OAMP 認証情報を確認して下さい。

```
%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
```

既存の OAMP 証明書を取除いて下さい

New 鍵ペアを作成するために、証明書を取除きま既に存在 します。

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

Generate 鍵ペア

指定キー サイズのエイリアスのための New 鍵ペアを作成するためにこのコマンドを実行して下さい。

```
%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]
```

キーのペアが作成されたことを確認して下さい。

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

OAMP サーバとして姓最初に入るために確認すれば。 名前は IP アドレスに解決可能である必要があります。 この名前は証明書の CN フィールドに現われます。

生成する新しい CSR

エイリアスのための Certificate 要求を生成し、ファイルに保存するためにこのコマンドを実行して下さい（たとえば、oamp.csr）。

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

CSR が正常に生成されたことを確認して下さい。

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

CA の証明書を発行して下さい

証明書に得ることは既に設定された認証局（CA）必要とします。

ブラウザのある特定の URL を入力して下さい

http:// <CA IP アドレス >/certsrv

それから SELECT 要求 **証明書**および**高度 Certificate 要求**。

```
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-----
```

適切なメニューに CSR の全体の内容をコピー アンド ペーストして下さい。 **符号化される**証明書のテンプレートおよび **Base 64** として『Web Server』 を選択 して下さい。 それから**証明書 チェーンを**『Download』 をクリック して下さい。

CA および Webサーバによって生成される証明書をそれぞれエクスポートするか、または完全なチェーンをダウンロードできます。 この例で完全なチェーン オプションは使用されます。

インポート CA によって生成される証明書

ファイルから証明書をインストールして下さい。

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

新しい証明書を加えるために**ワールドワイドウェブパブリッシングサービス**および Cisco CVP OPSConsoleServer サービスを再開して下さい。

確認

このセクションでは、設定が正常に機能していることを確認します。

確認する最も簡単な方法は CVP OAMP Webサーバへログインすることです。 信頼できない証明書 警告メッセージを得ないで下さい。

もう一つの方法はこのコマンドで使用される OAMP 証明書をチェックすることです。

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

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

コマンド構文を確認する必要があったら CVP のための設定および管理 ガイドを参照して下さい。

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

関連情報

オペレーティング システム Cisco 音声の CLI による設定 CA 署名入り認証（VOS）

得るべきプロシージャおよび署名する Upload ウィンドウ サーバ 自己-または認証局（CA）…

テクニカルサポートとドキュメント - Cisco Systems