Настройте подписанный сертификат CA на сервере CVP для веба - доступа HTTPS

Содержание

Введение

Этот документ описывает, как настроить и проверить подписанный сертификат Центра сертификации (CA) на Портале Администрирования и управления Операции Речевого портала Cisco (CVP) (OAMP) сервер.

Предварительные условия

Microsoft Windows базировался, сервер Центра сертификации уже предварительно сконфигурирован.

Требования

Cisco рекомендует ознакомиться с инфраструктурой PKI.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Версия 11.0 CVP

Windows 2012 R2 Server

Windows 2012 R2 Certificate Authority

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Список Справочника по командам

```
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
```

Сделайте резервную копию

Перейдите к папке **c:\Cisco\CVP\conf\security and archive all the files**. Если веб - доступ OAMP не работает, замена недавно созданные файлы с теми от резервной копии.

Генерируйте CSR

Проверьте свой надежный пароль.

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

Перейдите к папке **c:\Cisco\CVP\conf\security**.

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

> **Примечание:** В этой статье переменная Среды WINDOWS используется для создания команд Keytool намного короче и более читаемый. Прежде чем любая keytool команда добавлена, гарантируйте, что инициализируется переменная.

1. Создайте временную переменную.

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

Введите команду, чтобы гарантировать, что инициализируется переменная.
Введите правильный пароль.

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

Перечислите сертификаты

Список в настоящее время устанавливал сертификаты в keystore.

```
%kt% -list
```

> **Совет:** Если вы хотите совершенствовать свой список, можно модифицировать команду для отображения только подписанных сертификатов.

```
%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,
```

Проверьте самоподписанную информацию о сертификате 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
```

Удалите существующий сертификат OAMP

Для генерации новой пары ключей удалите сертификат, который уже существует.

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

Генерируйте пару ключей

Выполните эту команду для генерации новой пары ключей для псевдонима с выбранным размером ключа.

```
%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]
```

Проверьте, что генерировалась пара ключей.

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

Убедитесь для ввода имени и фамилиени как Сервера OAMP. Название должно быть разрешимым к IP-адресу. Это название появится в поле CN сертификата.

Генерируйте новый CSR

Выполните эту команду, чтобы генерировать запрос сертификата для псевдонима и сохранить его в файл (например, oamp.csr).

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

Проверьте, что CSR генерировался успешно.

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

Выполните сертификат на CA

Для получения сертификата, вам будет нужен Центр сертификации, уже настроенный.

Введите данный URL в браузере

http://<CA IP-адрес>/certsrv

Затем выберите **сертификат Request** и **Усовершенствованный запрос сертификата**.

```
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-----
```

Скопируйте и вставьте все содержание CSR к соответствующему меню. Выберите **Web Server** как шаблон сертификата и **Ядро 64 закодированных**. Затем нажмите **цепочку сертификатов Download**.

Можно экспортировать CA, и Web-сервер генерировал сертификат индивидуально, или загрузите полную цепочку. В данном примере используется полная цепочечная опция.

Импорт CA генерируемый сертификат

Установите сертификат от файла.

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

Для применения нового сертификата перезапускают **Сервис веб-публикации** и **сервисы Cisco CVP OPSConsoleServer**.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Самый легкий способ проверить состоит в том, чтобы войти к CVP Web-сервер OAMP. Вы не должны получать недоверяемое предупреждающее сообщение сертификата.

Иначе должен проверить сертификат OAMP, используемый с этой командой.

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

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Если необходимо проверить, что синтаксис команды обращается к Конфигурации и Руководству по администрированию для 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/ConfigAdmin Guide_8-5.pdf

Дополнительные сведения

Настройте Подписанный сертификат CA через CLI в голосовой операционной системе (VOS) Cisco

Процедура, чтобы получить и загрузить Windows Server Self-Signed или Центр сертификации (CA)...

Cisco Systems – техническая поддержка и документация