在CUCM和VCS配置示例之间的安全SIP中继

目录

简介

本文描述如何设置Cisco Unified Communications Manager (CUCM)和思科网真视频通信服务器(VCS)之间的一安全会话初始化协议(SIP)连接。

CUCM和VCS严密集成。由于视频端点在CUCM或VCS可以注册， SIP中继必须存在设备之间。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager
- 思科网真视频通信服务器
- 证书

使用的组件

本文档不限于特定的软件和硬件版本。此示例使用Cisco VCS软件版本X7.2.2和CUCM版本9.x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

保证证书有效，请添加证书到CUCM和VCS服务器，以便他们委托彼此的证书，然后建立SIP中继。

网络图

获取VCS证书

默认情况下，所有VCS系统附有临时证书。在管理员页面上，请导航对**维护>** Certificate Management >Server**证书**。点击**Show server证书**，并且新窗口打开与证书的原始数据：

这是原始身份验证数据的示例：

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmjFDMEEGA1UECgw6VGVt
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1
Njk5NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wHhcN
MTMwOTMwMDcxNzIwWhcNMTQwOTMwMDcxNzIwWjCBmjFDMEEGA1UECgw6VGVtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5
NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPipL0I/
L21fyyjoO5qv9lzDCgy7PFZPxkD1d/DNLIgp1jjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsmvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVlOgVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAkGA1UdEwQCMAAwJAYJYIZIAYb4QgENBBcWFVRlbXBv
cmFyeSBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqAjORhzQqRCHba+nEw
HwYDVR0jBBgwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49p1jIYqYdOAIjOiashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJe1iA=
-----END CERTIFICATE-----
```

您能解码证书和通过使用在您的本地PC的Openssl或使用一个联机证书编码器看到身份验证数据例如SSL顾客：

生成并且上传VCS自签名证书

由于每个VCS服务器有与同一公用名称的一证书，您在服务器上需要把新建的证书放。您能选择使用Certificate Authority (CA)或证书签字的自签名证书。请参阅思科网真证书创建和使用用Cisco VCS部署指南关于此步骤详细信息。

此步骤描述如何使用VCS生成自签名证书，然后上传该证书：

1. 登陆作为根对VCS，开始Openssl，并且生成专用密钥：

```
~ # openssl
OpenSSL> genrsa -out privatekey.pem 1024
Generating RSA private key, 1024 bit long modulus
.................................++++++
.............++++++
e is 65537 (0x10001)
```

2. 请使用此专用密钥为了生成证书签名请求(CSR) ：

```
OpenSSL> req -new -key privatekey.pem -out certcsr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BE
State or Province Name (full name) [Some-State]:Vlaams-Brabant
Locality Name (eg, city) []:Diegem
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:radius.anatomy.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL> exit
```

3. 生成自签名证书：

```
~ # openssl x509 -req -days 360 -in certcsr.pem -signkey privatekey.pem -out vcscert.pem
Signature ok
subject=/C=BE/ST=Vlaams-Brabant/L=Diegem/O=Cisco/OU=TAC/CN=radius.anatomy.com
Getting Private key
~ #
```

4. 确认证书当前是可用的：

```
~ # ls -ltr *.pem
-rw-r--r-- 1 root root 891 Nov 1 09:23 privatekey.pem
-rw-r--r-- 1 root root 664 Nov 1 09:26 certcsr.pem
-rw-r--r-- 1 root root 879 Nov 1 09:40 vcscert.pem
```

5. 下载与WinSCP的证书，并且上传他们在网页，因此VCS能使用证书;您需要专用密钥和生成的证书：

6. 重复所有VCS服务器的此步骤。

从CUCM服务器添加自签名证书到VCS服务器

从CUCM服务器添加证书，以便VCS将委托他们。在本例中，您使用从CUCM的标准的自签名证书;CUCM在安装时生成自签名证书，因此您不需要创建那些，您在VCS执行。

此步骤描述如何添加从CUCM服务器的一自签名证书到VCS服务器：

1. 下载从CUCM的CallManager.pem证书。登录OS管理页面，导航对安全> CertificateManagement，然后选择和下载自已签署的CallManager.pem证书：

2. 添加此证书作为在VCS.On的一个委托CA证书VCS，导航对**维护>** Certificate Management **>委托CA证书**，并且选择**显示CA证书**：

   新窗口打开与当前委托的所有证书。

3. 当前复制所有信任证书到文本文件。打开在文本编辑的CallManager.pem文件，复制其内容，并且当前添加该内容到同一个文本文件的底部在信任证书以后：

   ```
   CallManagerPub
   ======================
   -----BEGIN CERTIFICATE-----
   MIICmDCCAgGgAwIBAgIQZo7WOmjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
   MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ2lzY28xDDAKBgNVBAsTA1RBQzERMA8G
   A1UEAxMITUZDbDFQdWIxDzANBgNVBAgTBkRpZWdlbTENMAsGA1UEBxMEUGVnMzAe
   Fw0xMjA4MDExMDI4MzVaFw0xNzA3MzExMDI4MzRaMF4xCzAJBgNVBAYTAkJFMQ4w
   DAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMREwDwYDVQQDEwhNRkNsMVB1YjEP
   MA0GA1UECBMGRGllZ2VtMQ0wCwYDVQQHEwRQZWczMIGfMA0GCSqGSIb3DQEBAQUA
   A4GNADCBiQKBgQDmCOYMvRqZhAl+nFdHk0Y2PlNdACglvnRFwAq/rNgGrPCiwTgc
   0cxqsGtGQLSN1UyIPDAE5NufROQPJ7whR95KGmYbGdwHfKeuig+MT2CGltfPe6ly
   c/ZEDqHYvGlzJT5srWUfM9GdkTZfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
   o1cwVTALBgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC
   BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX6O6BAnLCalbKEn6YV7BpkQwDQYJKoZI
   hvcNAQEFBQADgYEAkEGDdRdMOtX4ClhEatQE3ptT6L6RRAyP8oDd3dIGEOYWhA2H
   Aqrw77loieva297AwgcKbPxnd5lZ/aBJxvmF8TIiOSkjy+dJW0asZWfei9STxVGn
   NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRrlIRzAJDeygLIq+wc=
   -----END CERTIFICATE-----
   ```
   如果有在CUCM的多个服务器集群，添加所有此处。

4. 保存文件作为CATrust.pem，并且点击UploadCA**证书为了**上传文件回到VCS ：

   VCS当前将委托CUCM提供的证书。

5. 重复所有VCS服务器的此步骤。

上传证书从VCS服务器到CUCM服务器

CUCM需要委托VCS提供的证书。

此步骤描述如何上传您在CUCM生成作为CallManager托拉斯证书的VCS证书：

1. 在OS管理页面，请导航对**安全>** Certificate Management，输入验证名称，浏览到其位置，并

且点击**上传文件**：

2. 上传从所有VCS服务器的证书。执行此在与VCS将联络的每个CUCM服务器;这典型地是管理CallManager服务的所有节点。

SIP连接

一旦证书验证，并且两个系统互相委托，请配置VCS的邻接区域和在CUCM的SIP中继。请参阅思科网真Cisco Unified Communications Manager用Cisco VCS (SIP中继)部署指南关于此步骤详细信息。

验证

确认SIP连接是活跃的在VCS的邻接区域：

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科网真Cisco Unified Communications Manager用Cisco VCS (SIP中继)部署指南
- 思科网真视频通信服务器管理员指南
- 思科网真证书创建和使用用Cisco VCS部署指南
- Cisco Unified通信操作系统管理指南
- Cisco Unified Communications Manager管理指南
- 技术支持和文档 - Cisco Systems