CUCM と VCS 間のセキュア SIP トランクの設定例

目次

概要

このドキュメントでは、Cisco Unified Communications Manager（CUCM）と Cisco TelePresence Video Communication Server（VCS）との間にセキュアな Session Initiation Protocol（SIP）接続をセットアップする方法を説明します。

CUCM と VCS は密接に統合されます。 ビデオ エンドポイントは CUCM または VCS のどちらにでも登録できるため、この 2 台のデバイスの間に SIP トランクが存在する必要があります。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Unified Communications Manager
- Cisco TelePresence Video Communication Server
- 証明書

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。 この例では、Cisco VCS ソフトウェア バージョン X7.2.2 と CUCM バージョン 9.x を使用します。

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

証明書が有効であることを確認してから、CUCM サーバと VCS サーバが互いの証明書を信頼するように両方のサーバに証明書を追加します。その後、SIP トランクを確立します。

ネットワーク図

VCS 証明書の取得

デフォルトでは、すべての VCS システムに仮証明書が付属しています。 管理ページで、[Maintenance] > [Certificate management] > [Server certificate] に移動します。 [Show server certificate] をクリックします。新しいウィンドウが開き、証明書の raw データが表示されます。

証明書の raw データの例は次のとおりです。

```
-----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-----
```

証明書をデコードし、ローカル PC での OpenSSL またはオンライン証明書デコーダ（SSL Shopper など）を使用して証明書のデータを表示できます。

VCS 自己署名証明書の生成およびアップロード

すべての VCS サーバの証明書には同じ共通名が使用されているため、新しい証明書をサーバ上に配置する必要があります。 自己署名証明書を使用することも、認証局（CA）から署名を受けた証明書を使用することもできます。 この手順について詳しくは、『Cisco VCS を使用した Cisco TelePresence 証明書の作成および使用 展開ガイド』を参照してください。

以下の手順で、VCS 自体を使用して自己署名証明書を生成し、その証明書をアップロードする方法を説明します。

1. root として VCS にログインし、OpenSSL を起動して、秘密キーを生成します。

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

2. 生成した秘密キーを使用して証明書署名要求（CSR）を生成します。

```
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. 自己署名証明書を生成します。

```
~ # 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. 証明書が使用可能になったことを確認します。

```
~ # 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. WinSCP で証明書をダウンロードし、Web ページに証明書をアップロードして VCS が使用

できるようにします。 秘密キーと生成された証明書の両方が必要です。

6. すべての VCSV サーバについて、以上の手順を繰り返します。

CUCM サーバから VCS サーバへの自己署名証明書の追加

VCS が証明書を信頼するように、CUCM サーバから証明書を追加します。 この例では、CUCM の標準的な自己署名証明書を使用します。 CUCM はインストール時に自己署名証明書を生成するため、VCS で行ったように証明書を生成する必要はありません。

以下の手順で、CUCM サーバから VCS サーバに自己署名証明書を追加する方法を説明します。

1. CUCM から CallManager.pem 証明書をダウンロードします。 [OS Administration] ページにログインして [Security] > [CertificateManagement] に移動し、自己署名証明書 CallManager.pem を選択してダウンロードします。

2. この証明書を信頼された CA 証明書として VCS に追加します。それにはまず、VCS で [Maintenance] > [Certificate management] > [Trusted CA certificate] に移動し、[Show CA certificate] を選択します。

   新しいウィンドウが開き、現在信頼されているすべての証明書が表示されます。

3. 現在信頼されているすべての証明書をテキスト ファイルにコピーします。 テキスト エディタで CallManager.pem ファイルを開き、ファイルの内容をコピーします。コピーした内容を、現在信頼されている証明書をコピーしたテキスト ファイルの末尾に追加します。

```
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-----
```

   CUCM クラスタに複数のサーバがある場合、それらすべてのサーバをここに追加します。

4. ファイルを CATrust.pem という名前で保存し、[Upload CA certificate] をクリックしてこのファイルを VCS にアップロードします。

   これで、VCS は CUCM が提示する証明書を信頼するようになります。

5. すべての VCSV サーバについて、以上の手順を繰り返します。

VCS サーバから CUCM サーバへの証明書のアップロード

CUCM は VCS によって提示された証明書を信頼する必要があります。

以下の手順で、生成した VCS 証明書を CallManager-Trust 証明書として CUCM にアップロードする方法を説明します。

1. [OS Administration] ページで、[Security] > [Certificate Management] に移動し、証明書の名前を入力してその場所を参照し、[Upload File] をクリックします。

2. すべての VCS サーバから証明書をアップロードします。 このステップは、VCS と通信するすべての CUCM サーバで行う必要があります。 これは通常、CallManager サービスを実行しているすべてのノードです。

SIP 接続

証明書が検証されて両方のシステムが互いを信頼するようになったら、VCS 上にネイバー ゾーンを設定し、CUCM 上に SIP トランクを設定します。 この手順について詳しくは、『Cisco VCS（SIP トランク）を使用した Cisco TelePresence Cisco Unified Communications Manager 展開ガイド』を参照してください。

確認

VCS 上のネイバー ゾーンで SIP 接続がアクティブであることを確認します。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco VCS（SIP トランク）を使用した Cisco TelePresence Cisco Unified Communications Manager 展開ガイド

- Cisco TelePresence Video Communication Server 管理者ガイド
- Cisco VCS を使用した Cisco TelePresence 証明書の作成および使用 展開ガイド
- Cisco Unified Communications オペレーティング システム管理ガイド
- Cisco Unified Communications Manager 管理ガイド
- テクニカル サポートとドキュメント – Cisco Systems