

CUCM と VCS 間のセキュア SIP トランクの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[VCS 証明書の取得](#)

[VCS 自己署名証明書の生成およびアップロード](#)

[CUCM サーバから VCS サーバへの自己署名証明書の追加](#)

[VCS サーバから CUCM サーバへの証明書のアップロード](#)

[SIP 接続](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

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あることが推奨されます。

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

使用するコンポーネント

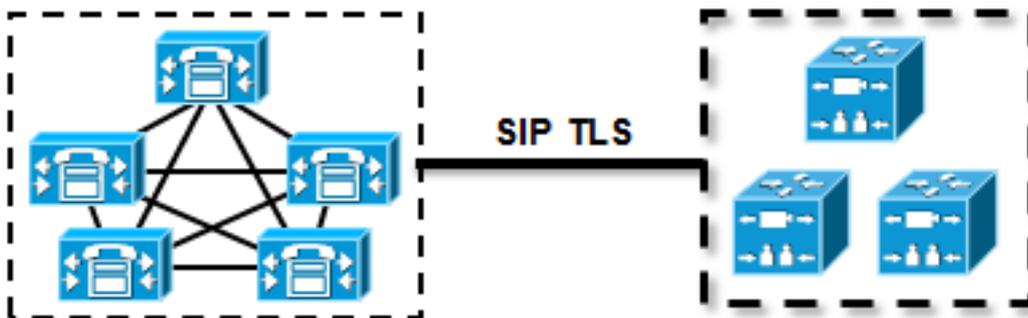
このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。この例では、Cisco VCS ソフトウェア バージョン X7.2.2 と CUCM バージョン 9.x を使用します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

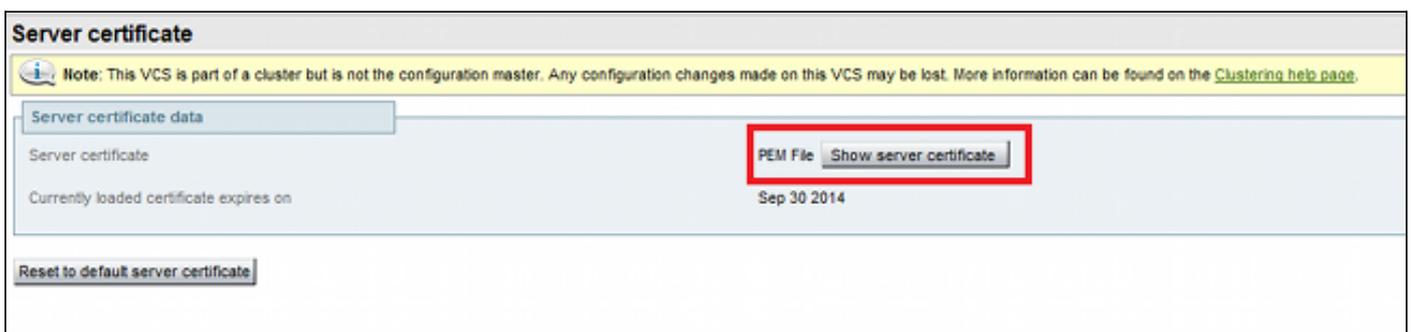
証明書が有効であることを確認してから、CUCM サーバと VCS サーバが互いの証明書を信頼するように両方のサーバに証明書を追加します。その後、SIP トランクを確立します。

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
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAzMTE1My1hNTE4LTAwNTA1
Njk5NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAzMTE1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY2l2Y28wHhcN
MTMwOTMwMDcxNzIwWWhcNMTQwOTMwMDcxNzIwWjCBMjFDMEEGA1UECgw6VGvtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAzMTE1My1hNTE4LTAwNTA1Njk5
NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAzMTE1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY2l2Y28wZ8wDQYJ
KozIhvcNAQEBCQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPiPl0I/
L21fyjyo05qv91zDCgy7PFZPpkDld/DNLIgpljjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsMVZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVL0gVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAKGA1UdEwQCMAAwJAYJYIZIAyB4QgENBBcWFVR1bXBv
cmFyeSBdZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqAJORhzQqRCHba+nEw
HwYDVR0jBBGwFoAUPhCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKozIhvcNAQEFBQAD
gYEAZklIMSfi49pljIYqYdOAIjOiashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiYODD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWP16CevopbJeliA=
```

-----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。

Certificate Information:

- ✔ **Common Name:** disco
- ✔ **Organization:** Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b
- ✔ **Organization Unit:** Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b
- ✔ **Valid From:** September 30, 2013
- ✔ **Valid To:** September 30, 2014
- ✔ **Issuer:** disco, Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b
- ✔ **Key Size:** 1024 bit
- ✔ **Serial Number:** 1 (0x1)

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。

Server certificate

Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the [Clustering help page](#).

Server certificate data

Server certificate PEM File

Currently loaded certificate expires on Sep 30 2014

Certificate signing request (CSR)

Certificate request There is no certificate signing request in progress

Upload new certificate

Select the server private key file "C:\privatekey.pem" ⓘ

Select the server certificate file "C:\vcs-cert.pem" ⓘ

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、[Security] > [Certificate Management] に移動し、自己署名CallManager.pem証明書を選択してダウンロードします。

Certificate Configuration

Regenerate Download Generate CSR Download CSR

Status

i Status: Ready

Certificate Settings

File Name CallManager.pem
 Certificate Name CallManager
 Certificate Type certs
 Certificate Group product-cm
 Description Self-signed certificate generated by system

Certificate File Data

```
[
  Version: V3
  Serial Number: 136322906787293084267780831508134358913
  Signature Algorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=Peg3, ST=Diegem, CN=MFC1Pub, OU=TAC, O=Cisco, C=BE
  Validity From: Wed Aug 01 12:28:35 CEST 2012
  To: Mon Jul 31 12:28:34 CEST 2017
  Subject Name: L=Peg3, ST=Diegem, CN=MFC1Pub, OU=TAC, O=Cisco, C=BE
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
  30818902818100e608e60cbd1a9984097e9c57479346363e535d002825be7445c00abfacd806acf0a2c1381cd1cc6ab06b4640
  b48dd54c883c3004e4db9f44e40f27bc2147de4a1a661b19dc077ca7ae8a0f8c4f608696d7cf7ba97273f6440ea1d8bc6973253
  e6cad651f33d19d91365f1c8d6257a93f8ef3ed1a28170d2088a848e7d7edc8110203010001
  Extensions: 3 present
  [
    Extension: KeyUsage (OID.2.5.29.15)
    Critical: false
    Usages: digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign,
  ]
  [
    Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
    Critical: false
    Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
  ]
]
```

Regenerate **Download** Generate CSR Download CSR

- 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。

Trusted CA certificate

i Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the [Clustering help page](#).

Upload

Select the file containing trusted CA certificates Choose... **i**

CA certificate PEM File **Show CA certificate**

Upload CA certificate Reset to default CA certificate

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。

- 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。

Upload Certificate/Certificate chain

Upload File Close

Status

i Status: Ready

Upload Certificate/Certificate chain

Certificate Name*

Description

Upload File

i *- indicates required item.

- 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。

Edit zone

Accept proxied registrations Deny ⓘ

Media encryption mode Auto ⓘ

Authentication

Authentication policy Treat as authenticated ⓘ

SIP authentication trust mode Off ⓘ

Location

Peer 1 address 10.48.36.203 ⓘ SIP, Active: 10.48.36.203:5061

Peer 2 address ⓘ

Peer 3 address ⓘ

Peer 4 address ⓘ

Peer 5 address ⓘ

Peer 6 address ⓘ

Advanced

Zone profile Cisco Unified Communications Manager ⓘ

Save Delete Cancel

Status

State	Active
Number of calls to this zone	0
Bandwidth used on this VCS	0 kbps
Total bandwidth used across this cluster	0 kbps
Search rules targeting this zone	0

トラブルシューティング

現在、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 管理者ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)