

Ejemplo de configuración de enlace troncal SIP seguro entre CUCM y VCS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Obtener certificado de VCS](#)

[Generar y cargar certificado autofirmado de VCS](#)

[Agregar certificado autofirmado del servidor CUCM al servidor VCS](#)

[Cargar certificado del servidor VCS al servidor CUCM](#)

[Conexión SIP](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar una conexión segura de protocolo de inicio de sesión (SIP) entre Cisco Unified Communications Manager (CUCM) y Cisco TelePresence Video Communication Server (VCS).

CUCM y VCS están estrechamente integrados. Como los terminales de vídeo se pueden registrar en CUCM o VCS, deben existir enlaces troncales SIP entre los dispositivos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager
- Cisco TelePresence Video Communication Server
- Certificados

Componentes Utilizados

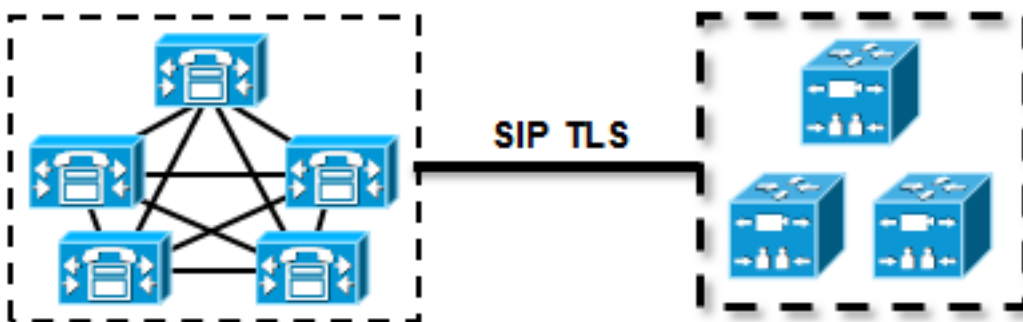
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. Este ejemplo utiliza la versión X7.2.2 del software Cisco VCS y la versión 9.x de CUCM.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Asegúrese de que los certificados son válidos, agregue los certificados a los servidores CUCM y VCS para que confíen en los certificados de los demás y, a continuación, establezca el troncal SIP.

Diagrama de la red



Obtener certificado de VCS

De forma predeterminada, todos los sistemas VCS incluyen un certificado temporal. En la página de administración, navegue hasta **Mantenimiento > Administración de certificados > Certificado de servidor**. Haga clic en **Show server certificate**, y se abrirá una nueva ventana con los datos sin procesar del certificado:

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 **Show server certificate**

Currently loaded certificate expires on Sep 30 2014

[Reset to default server certificate](#)

Este es un ejemplo de los datos del certificado sin procesar:

```

-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBMjFDMEEGA1UECgw6VGvt
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTF1My1hNTE4LTAwNTA1
Njk5NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAtMTF1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY21zY28wHhcN
MTMwOTMwMDcxNzIwWhcNMTQwOTMwMDcxNzIwWjCBMjFDMEEGA1UECgw6VGvtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTF1My1hNTE4LTAwNTA1Njk5
NWl0YjFDMEEGA1UECww6VGvtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAtMTF1My1hNTE4LTAwNTA1Njk5NWl0YjEOMAwGA1UEAwwFY21zY28wZ8wDQYJ
KoZiHvcNAQEbbQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPiPL0I/
L21fyjyo05qv91zDCgy7PFZPxD1d/DNLIgpljjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzZdsMvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVL0gVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAKGA1UdEwQCMAAwJAYJYIZIAyB4QgENBBcWFVR1bXBv
cmFyeSBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqA jORhzQqRCHba+nEw
HwYDVR0jBBGwFoAUPhCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49pljIYqYdOAIjOiaShYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWP16CevopbJeliA=
-----END CERTIFICATE-----

```

Puede decodificar el certificado y ver los datos del certificado mediante el uso de OpenSSL en su equipo local o el uso de un decodificador de certificados en línea como [SSL Shopper](#) :

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)

Generar y cargar certificado autofirmado de VCS

Dado que cada servidor VCS tiene un certificado con el mismo nombre común, debe colocar certificados nuevos en el servidor. Puede optar por utilizar certificados autofirmados o certificados firmados por la Autoridad de certificación (CA). Consulte la [Guía de creación y uso de certificados de Cisco TelePresence con Cisco VCS Deployment Guide](#) para obtener detalles sobre este procedimiento.

Este procedimiento describe cómo utilizar el propio VCS para generar un certificado autofirmado y, a continuación, cargarlo:

1. Inicie sesión como root en el VCS, inicie OpenSSL y genere una clave privada:

```

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

```

2. Utilice esta clave privada para generar una solicitud de firma de certificado (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. Genere el certificado autofirmado:

```
~ # 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. Confirme que los certificados ya están disponibles:

```
~ # 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. Descargue los certificados con [WinSCP](#) y cárguelos en la página web para que el VCS pueda utilizar los certificados; necesita la clave privada y el certificado generado:

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 [Show server certificate](#)

Currently loaded certificate expires on Sep 30 2014

[Reset to default server certificate](#)

Certificate signing request (CSR)

Certificate request There is no certificate signing request in progress

[Generate CSR](#)

Upload new certificate

Select the server private key file "C:\privatekey.pem" [Choose...](#) ⓘ

Select the server certificate file "C:\vcs-cert.pem" [Choose...](#) ⓘ

[Upload server certificate data](#)

6. Repita este procedimiento para todos los servidores VCS.

Agregar certificado autofirmado del servidor CUCM al servidor VCS

Agregue los certificados de los servidores de CUCM para que VCS confíe en ellos. En este ejemplo, está utilizando los certificados autofirmados estándar de CUCM; CUCM genera certificados autofirmados durante la instalación, por lo que no es necesario crearlos tal y como hizo en el VCS.

Este procedimiento describe cómo agregar un certificado autofirmado del servidor de CUCM al servidor VCS:

1. Descargue el certificado CallManager.pem de CUCM. Inicie sesión en la página Administración del sistema operativo, navegue hasta **Seguridad > Administración de certificados**, luego seleccione y descargue el certificado autofirmado CallManager.pem:

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

2. Agregue este certificado como certificado de CA de confianza en el VCS. En el VCS, navegue hasta **Mantenimiento > Administración de certificados > Certificado de CA de confianza** y seleccione **Mostrar certificado de CA**:

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

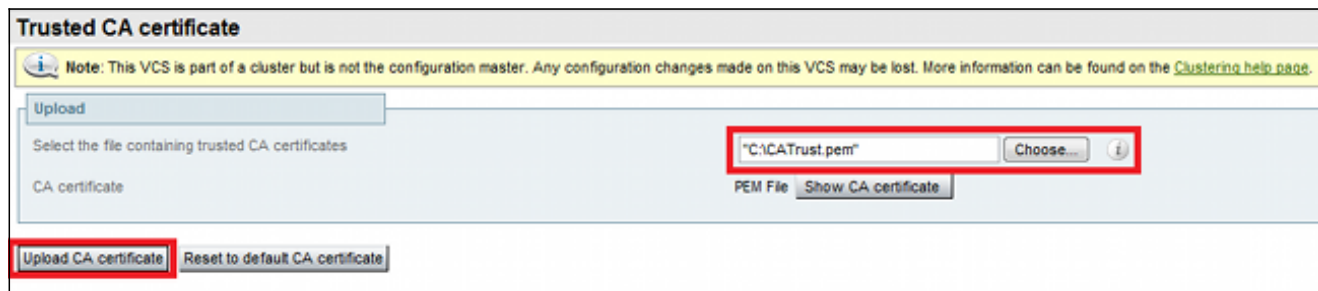
Se abre una nueva ventana con todos los certificados actualmente fiables.

3. Copie todos los certificados actualmente fiables en un archivo de texto. Abra el archivo CallManager.pem en un editor de texto, copie su contenido y agréguelo al final del mismo archivo de texto después de los certificados actualmente confiables:

```
CallManagerPub
=====
-----BEGIN CERTIFICATE-----
MIICmDCCAgGgAwIBAgIQZo7W0mjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ2l2Y28xDDAKBgNVBAsTA1RBQzERMA8G
A1UEAxMITUZDbDFQdWlxdzANBgNVBAGTBkRzZWRlbTENMAAsGA1UEBxMEUGVnMzAe
Fw0xMjA4MDExMDI0MzVaFw0xNzA3MzExMDI0MzRaMF4xMzA5BgNVBAYTAkFJbG91
DAYDVQQKEwVudXNjbzEMMAoGA1UECjMDVEFDMREwDwYDVQDEwNHNRkNsMVB1YjEP
MA0GA1UECjBGRG1lZ2VtMQ0wCwYDVQQLHwZmIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDmCOYmVrQzHAl+nFdHk0Y2PlNdACglvnRFwAq/rNgGrPCiwTgc
0cxqsGtGQLSN1UyIPDAE5NufROQPJ7whR95KGMybGdwHfKeuig+MT2CGlTfPe6ly
c/ZEDqHYvGlzJT5srWUFm9GdkTZfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
o1cwVTALBgNVHQ8EBAMCARwwJwYDVR0lBCAwHgYIKwYBBQUHAWEGCCsGAQUFBwMC
BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX6O6BAnLCalbKE6YV7BpkQwDQYJKoZI
hvcNAQEFBQADgYEAkEGDdRdMOtX4ClhEatQE3ptT6L6RRAyP8oDd3dIGEYOWhA2H
Aqrw77loieva297AwgcKbPxnd5Lz/aBJxvmF8TIIOSkfy+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRr1IRzAJDeygLIq+wc=
-----END CERTIFICATE-----
```

Si tiene varios servidores en el clúster de CUCM, agréguelos todos aquí.

4. Guarde el archivo como **CATrust.pem** y haga clic en **Cargar certificado de CA** para cargar el archivo nuevamente en el VCS:



VCS confiará ahora en los certificados ofrecidos por CUCM.

5. Repita este procedimiento para todos los servidores VCS.

Cargar certificado del servidor VCS al servidor CUCM

CUCM debe confiar en los certificados que ofrece VCS.

Este procedimiento describe cómo cargar el certificado VCS que generó en CUCM como un certificado CallManager-Trust:

1. En la página Administración del sistema operativo, navegue hasta **Seguridad > Administración de certificados**, ingrese el nombre del certificado, navegue hasta su ubicación y haga clic en **Cargar archivo**:

Upload Certificate/Certificate chain

Upload File Close

Status

i Status: Ready

Upload Certificate/Certificate chain

Certificate Name*

Description

Upload File

i *- indicates required item.

2. Cargue el certificado de todos los servidores VCS. Haga esto en cada servidor CUCM que se comuniquen con el VCS; generalmente se trata de todos los nodos que ejecutan el servicio CallManager.

Conexión SIP

Una vez que se validen los certificados y ambos sistemas confíen entre sí, configure la zona vecina en VCS y el troncal SIP en CUCM. Consulte la [Guía de implementación de Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS \(SIP Trunk\)](#) para obtener detalles sobre este procedimiento.

Verificación

Confirme que la conexión SIP está activa en la zona vecina en VCS:

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 ⓘ 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 ⓘ

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

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Cisco TelePresence Guía de implementación de Cisco Unified Communications Manager con Cisco VCS \(SIP Trunk\)](#)
- [Guía del administrador de Cisco TelePresence Video Communication Server](#)
- [Guía de implementación de creación y uso de certificados de Cisco TelePresence con Cisco VCS](#)
- [Guía de administración del sistema operativo Cisco Unified Communications](#)
- [Guía de administración de Cisco Unified Communications Manager](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)