Asegure el trunk del SORBO entre el ejemplo de configuración CUCM y VCS

Contenido

Introducción

Este documento describe cómo configurar una conexión segura del Session Initiation Protocol (SIP) entre el administrador de las Comunicaciones unificadas de Cisco (CUCM) y el servidor del comunicación mediante video del Cisco TelePresence (VCS).

Los CUCM y los VCS se integran de cerca. Porque los punto final de video se pueden registrar en el CUCM o el VCS, los trunks del SORBO deben existir entre los dispositivos.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de las Comunicaciones unificadas de Cisco
- Servidor del comunicación mediante video del Cisco TelePresence
- Certificados

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Asegúrese de que los Certificados son válido, agregue los Certificados a los servidores CUCM y VCS de modo que confíen en los Certificados de cada uno, después establecen el trunk del SORBO.

Diagrama de la red

Obtenga el certificado VCS

Por abandono, todos los sistemas VCS vienen con el certificado temporal. En la página de administración, navegue al Certificate Management (Administración de certificados) > al **certificado de servidor del mantenimiento**. Haga clic el **certificado de la show server**, y una nueva ventana se abre con los datos sin procesar del certificado:

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

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

Usted puede decodificar el certificado y ver los datos del certificado con el uso del OpenSSL en su PC local o el uso de un decodificador en línea del certificado tal como comprador SSL:

Genere y cargue el certificado autofirmado VCS

Porque cada servidor VCS tiene un certificado con el mismo Common Name, usted necesita poner los nuevos Certificados en el servidor. Usted puede elegir utilizar los certificados autofirmados o los Certificados firmados por el Certificate Authority (CA). Vea la creación y el uso del certificado del Cisco TelePresence con el Guía de despliegue de Cisco VCS para los detalles de este procedimiento.

Este procedimiento describe cómo utilizar el VCS sí mismo para generar un certificado autofirmado, después carga ese certificado:

1. Inicie sesión como raíz al VCS, comience el 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 un pedido 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 están disponibles ahora:

```
~ # 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 carguelos en la página web así que el VCS puede utilizar los Certificados; usted necesita la clave privada y el certificado generado:

6. Relance este procedimiento para todos los servidores VCS.

Agregue el certificado autofirmado del servidor CUCM al servidor VCS

Agregue los Certificados de los servidores CUCM de modo que el VCS los confíe en. En este ejemplo, usted está utilizando los certificados autofirmados estándar de CUCM; CUCM genera los certificados autofirmados durante la instalación así que usted no necesita crear ésos como usted hizo en el VCS.

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

1. Descargue el certificado CallManager.pem del CUCM. El registro en la página de administración OS, navega a la Seguridad **> a** CertificateManagement**, después** selecciona y descarga el certificado uno mismo-firmado CallManager.pem:

2. Agregue este certificado como certificado de CA de confianza en el VCS.On el VCS, navegue al Certificate Management (Administración de certificados) del **mantenimiento > confiaba en el certificado de CA**, y seleccionan el **certificado de CA de la demostración**:

   Una nueva ventana se abre con todos los Certificados que se confíen en actualmente.

3. Copie todos los actualmente certificados confiables a un archivo de texto. Abra el archivo CallManager.pem en un editor de textos, copie su contenido, y agregue ese contenido a la parte inferior del mismo archivo de texto después actualmente de los certificados confiables:

   ```
   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-----
   ```
   Si usted tiene los servidores múltiples en el CUCM agrupan, agregan todos aquí.

4. Salve el archivo como CATrust.pem, y haga clic el **certificado de** UploadCA **para** cargar el archivo de nuevo al VCS:

El VCS ahora confiará en los Certificados ofrecidos por CUCM.

5. Relance este procedimiento para todos los servidores VCS.

Cargue el certificado del servidor VCS al servidor CUCM

El CUCM necesita confiar en los Certificados ofrecidos por el VCS.

Este procedimiento describe cómo cargar el certificado VCS que usted generó en el CUCM como certificado de la CallManager-confianza:

1. En la página de administración OS, navegue al Certificate Management (Administración de certificados) de la **Seguridad**, ingrese el nombre del certificado, hojee a su ubicación, y haga clic el **archivo de la carga**:

2. Cargue el certificado de todos los servidores VCS. Haga esto en cada servidor CUCM que comunique con el VCS; éste es típicamente todos los Nodos que están dirigiendo el servicio de CallManager.

Conexión del SORBO

Una vez que se validan los Certificados y ambos sistemas se confían en, configure la zona vecina en VCS y el trunk del SORBO en CUCM. Vea al administrador de las Comunicaciones unificadas de Cisco del Cisco TelePresence con el Guía de despliegue de Cisco VCS (trunk del SORBO) para los detalles de este procedimiento.

Verificación

Confirme que la conexión del SORBO es activa en la zona vecina en VCS:

Troubleshooting

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

Información Relacionada

- Administrador de las Comunicaciones unificadas de Cisco del Cisco TelePresence con el Guía de despliegue de Cisco VCS (trunk del SORBO)
- Guía de Administrador del servidor del comunicación mediante video del Cisco TelePresence
- Creación y uso del certificado del Cisco TelePresence con el Guía de despliegue de Cisco

VCS

- Guía de administración del sistema operativo de las Comunicaciones unificadas de Cisco
- Guía del control del administrador de las Comunicaciones unificadas de Cisco
- Soporte Técnico y Documentación - Cisco Systems