Sécurisez le joncteur réseau de SIP exemple entre CUCM et de VCS configuration

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Configurez](#)
[Diagramme du réseau](#)
[Obtenez le certificat de VCS](#)
[Générez et téléchargez le certificat Auto-signé par VCS](#)
[Ajoutez le certificat Auto-signé du serveur CUCM au serveur de VCS](#)
[Certificat de téléchargement de serveur de VCS au serveur CUCM](#)
[Connexion de SIP](#)
[Vérifiez](#)
[Dépannez](#)
[Informations connexes](#)

Introduction

Ce document décrit comment installer une connexion sécurisée de Protocole SIP (Session Initiation Protocol) entre Cisco Unified Communications Manager (CUCM) et le serveur de communication vidéo Cisco TelePresence (VCS).

Les CUCM et le VCS sont étroitement intégrés. Puisque des points finaux visuels peuvent être enregistrés sur le CUCM ou le VCS, les joncteurs réseau de SIP doivent exister entre les périphériques.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Communications Manager
- Serveur de communication vidéo Cisco TelePresence
- Certificats

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques. Cet exemple utilise la version de logiciel X7.2.2 de VCS de Cisco et la version 9.x CUCM.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Assurez-vous que les Certificats sont valides, ajoutez les Certificats aux serveurs CUCM et de VCS de sorte qu'ils fassent confiance aux Certificats de chacun, puis établissent le joncteur réseau de SIP.

Diagramme du réseau

Obtenez le certificat de VCS

Par défaut, tous les systèmes de VCS été livré avec le certificat provisoire. À la page d'admin, naviguez vers la **Gestion de maintenance** > de **certificat** > le **certificat de serveur**. Cliquez sur le **certificat de serveur d'exposition**, et une nouvelle fenêtre s'ouvre avec les données brutes du certificat :

C'est un exemple des données brutes de certificat :

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

Vous pouvez décoder le certificat et voir les données de certificat par l'utilisation d'OpenSSL sur votre ordinateur local ou l'utilisation d'un décodeur en ligne de certificat tel que le client SSL :

Générez et téléchargez le certificat Auto-signé par VCS

Puisque chaque serveur de VCS a un certificat avec le même nom commun, vous devez mettre de nouveaux Certificats sur le serveur. Vous pouvez choisir d'utiliser les Certificats auto-signés ou les Certificats signés par l'Autorité de certification (CA). Voyez la création et l'utilisation de certificat de TelePresence Cisco avec le guide de déploiement de VCS de Cisco pour des détails de cette procédure.

Cette procédure décrit comment employer le VCS elle-même pour générer un certificat auto-signé, puis télécharge ce certificat :

1. Ouvrez une session comme racine au VCS, commencez OpenSSL, et générez une clé privée :

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

2. Employez cette clé privée afin de générer une demande de signature de certificat (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. Générez le certificat auto-signé :

```
~ # 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. Confirmez que les Certificats sont maintenant 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. Téléchargez les Certificats avec WinSCP, et téléchargez-les sur la page Web ainsi le VCS peut utiliser les Certificats ; vous avez besoin de la clé privée et du certificat généré :

6. Répétez cette procédure pour tous les serveurs de VCS.

Ajoutez le certificat Auto-signé du serveur CUCM au serveur de VCS

Ajoutez les Certificats des serveurs CUCM de sorte que le VCS leur fasse confiance. Dans cet exemple, vous utilisez la norme les Certificats auto-signés de CUCM ; CUCM génère les Certificats auto-signés pendant l'installation ainsi vous n'avez pas besoin de créer ceux comme vous avez fait sur le VCS.

Cette procédure décrit comment ajouter un certificat auto-signé du serveur CUCM au serveur de VCS :

1. Téléchargez le certificat CallManager.pem du CUCM. Connectez-vous dans la page de gestion de SYSTÈME D'EXPLOITATION, naviguez vers la Sécurité **> le** CertificateManagement**, puis** sélectionnez et téléchargez le certificat auto-signé CallManager.pem :

2. Ajoutez ce certificat comme certificat de CA de confiance sur le VCS.On le VCS, naviguez vers la **Gestion de maintenance** > de **certificat > a fait confiance au certificat de CA**, et sélectionne le **certificat de CA d'exposition** :

   Une nouvelle fenêtre s'ouvre avec tous les Certificats qui sont actuellement faits confiance.

3. Copiez tous les Certificats actuellement de confiance sur un fichier texte. Ouvrez le fichier CallManager.pem dans un éditeur de texte, copiez son contenu, et ajoutez ce contenu au bas du même fichier texte après les Certificats actuellement de confiance :

```
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 vous avez plusieurs les serveurs dans le CUCM groupent, ajoutent tous ici.

4. Sauvegardez le fichier comme CATrust.pem, et cliquez sur le **certificat d'**UploadCA **afin de** télécharger le fichier de nouveau au VCS :

   Le VCS fera confiance maintenant aux Certificats offerts par CUCM.

5. Répétez cette procédure pour tous les serveurs de VCS.

Certificat de téléchargement de serveur de VCS au serveur CUCM

Le CUCM doit faire confiance aux Certificats offerts par le VCS.

Cette procédure décrit comment télécharger le certificat de VCS que vous avez généré sur le CUCM comme certificat de CallManager-confiance :

1. Àla page de gestion de SYSTÈME D'EXPLOITATION, naviguez vers la **Gestion de Sécurité > de certificat**, écrivez le nom de certificat, parcourez à son emplacement, et cliquez sur Upload le **fichier** :

2. Téléchargez le certificat de tous les serveurs de VCS. Faites ceci sur chaque serveur CUCM qui communiquera avec le VCS ; c'est typiquement tous les Noeuds qui exécutent le service de CallManager.

Connexion de SIP

Une fois que des Certificats sont validés et les deux systèmes se font confiance, configurez la zone voisine sur le VCS et le joncteur réseau de SIP sur CUCM. Voyez la TelePresence Cisco Cisco Unified Communications Manager avec le guide de déploiement de VCS de Cisco (joncteur réseau de SIP) pour des détails de cette procédure.

Vérifiez

Confirmez que la connexion de SIP est en activité dans la zone voisine sur le VCS :

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- TelePresence Cisco Cisco Unified Communications Manager avec le guide de déploiement de VCS de Cisco (joncteur réseau de SIP)
- Guide de l'administrateur de serveur de communication vidéo Cisco TelePresence
- Création et utilisation de certificat de TelePresence Cisco avec le guide de déploiement de VCS de Cisco
- Guide d'administration de système d'exploitation de Cisco Unified Communications
- Guide d'administration de Cisco Unified Communications Manager
- Support et documentation techniques - Cisco Systems