Exemple de configuration de liaison SIP sécurisée entre CUCM et VCS

Table des matières

Introduction

Ce document décrit comment configurer une connexion SIP (Session Initiation Protocol) sécurisée entre Cisco Unified Communications Manager (CUCM) et le serveur Cisco TelePresence Video Communication Server (VCS).

Le CUCM et le VCS sont étroitement intégrés. Étant donné que les terminaux vidéo peuvent être enregistrés sur CUCM ou VCS, des liaisons SIP doivent exister entre les périphériques.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solutions 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 le logiciel Cisco VCS version X7.2.2 et CUCM version 9.x.

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.

Configurer

Assurez-vous que les certificats sont valides, ajoutez les certificats aux serveurs CUCM et VCS afin qu'ils se fassent mutuellement confiance, puis établissez la ligne principale SIP.

Diagramme du réseau

Obtenir un certificat VCS

Par défaut, tous les systèmes VCS sont fournis avec un certificat temporaire. Sur la page admin, accédez à Maintenance > Certificate management > Server certificate. Cliquez sur Show server certificate, et une nouvelle fenêtre s'ouvre avec les données brutes du certificat :

Voici un exemple des données brutes du 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
gYEAZklIMSfi49p1jIYqYdOAIjOiashYVfqGUUMFr4V1hokM9OByGGTbx8jx6Y/S
p1SyT4ilU5uiYODD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+9OGAsI/TGthQ2n7yUWPl6CevopbJe1iA=
-----END CERTIFICATE-----
```

Vous pouvez décoder le certificat et voir les données du certificat en utilisant OpenSSL sur votre PC local ou en utilisant un décodeur de certificat en ligne tel que SSL Shopper :

Générer et télécharger un certificat autosigné VCS

Étant donné que chaque serveur VCS possède un certificat portant le même nom commun, vous devez placer de nouveaux certificats sur le serveur. Vous pouvez choisir d'utiliser des certificats

auto-signés ou des certificats signés par l'autorité de certification (AC). Pour plus d'informations sur cette procédure, reportez-vous au Guide de déploiement de création et d'utilisation de certificats Cisco TelePresence avec Cisco VCS.

Cette procédure décrit comment utiliser le VCS lui-même pour générer un certificat auto-signé, puis télécharger ce certificat :

1. Connectez-vous en tant qu'utilisateur racine au serveur VCS, démarrez 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. Utilisez 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. Vérifiez 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 afin que le VCS puisse utiliser les certificats ; vous avez besoin de la clé privée et du certificat généré :

6. Répétez cette procédure pour tous les serveurs VCS.

Ajouter un certificat auto-signé du serveur CUCM au serveur VCS

Ajoutez les certificats des serveurs CUCM afin que le VCS les approuve. Dans cet exemple, vous utilisez les certificats auto-signés standard de CUCM ; CUCM génère des certificats auto-signés au cours de l'installation de sorte que vous n'avez pas besoin de les créer comme vous l'avez fait sur le VCS.

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

1. Téléchargez le certificat CallManager.pem depuis CUCM. Connectez-vous à la page OS Administration, accédez à Security > Certificate Management, puis sélectionnez et téléchargez le certificat auto-signé CallManager.pem :

2. Ajoutez ce certificat en tant que certificat CA approuvé sur le VCS.Sur le VCS, accédez à Maintenance > Certificate management > Trusted CA certificate, et sélectionnez Show CA certificate :

   Une nouvelle fenêtre s'ouvre avec tous les certificats qui sont actuellement approuvés.

3. Copiez tous les certificats actuellement approuvés dans 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 approuvés :

```
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 serveurs dans le cluster CUCM, ajoutez-les tous ici.

4. Enregistrez le fichier sous le nom CATrust.pem, et cliquez sur Upload CA certificate afin de télécharger le fichier à nouveau sur le VCS :

Le VCS fait désormais confiance aux certificats offerts par CUCM.

5. Répétez cette procédure pour tous les serveurs VCS.

Télécharger le certificat du serveur VCS vers le serveur CUCM

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

Cette procédure décrit comment télécharger le certificat VCS que vous avez généré sur le CUCM en tant que certificat CallManager-Trust :

1. Sur la page OS Administration, accédez à Security > Certificate Management, entrez le nom du certificat, accédez à son emplacement, puis cliquez sur Upload File:

2. Téléchargez le certificat depuis tous les serveurs VCS. Effectuez cette opération sur chaque serveur CUCM qui communiquera avec le VCS ; il s'agit généralement de tous les noeuds qui exécutent le service CallManager.

Connexion SIP

Une fois que les certificats sont validés et que les deux systèmes se font confiance, configurez la zone voisine sur VCS et la ligne principale SIP sur CUCM. Pour plus d'informations sur cette procédure, reportez-vous au Guide de déploiement de Cisco TelePresence Cisco Unified

Communications Manager avec Cisco VCS (ligne principale SIP).

Vérifier

Vérifiez que la connexion SIP est active dans la zone voisine sur VCS :

Dépannage

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

Informations connexes

- Guide de déploiement de Cisco TelePresence Cisco Unified Communications Manager avec Cisco VCS (ligne principale SIP)
- Guide de l'administrateur du serveur de communication vidéo Cisco TelePresence
- Guide de déploiement de Cisco TelePresence Certificate Creation and Use With Cisco VCS
- Guide d'administration du système d'exploitation Cisco Unified Communications
- Guide d'administration de Cisco Unified Communications Manager
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.