

Configurer CUCM pour la connexion IPsec entre les noeuds

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Présentation de la configuration](#)

[Vérifier la connectivité IPsec](#)

[Vérifier les certificats IPsec](#)

[Télécharger le certificat racine IPsec depuis l'abonné](#)

[Télécharger le certificat racine IPsec de l'abonné vers l'éditeur](#)

[Configurer la stratégie IPsec](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment établir la connectivité IPsec entre les noeuds Cisco Unified Communications Manager (CUCM) dans un cluster.

Note: Par défaut, la connexion IPsec entre les noeuds CUCM est désactivée.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître le CUCM.

Components Used

Les informations contenues dans ce document sont basées sur la version 10.5(1) 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.

Configuration

Utilisez les informations décrites dans cette section afin de configurer le CUCM et d'établir la connectivité IPsec entre les noeuds dans un cluster.

Présentation de la configuration

Voici les étapes de cette procédure, chacune d'entre elles étant détaillée dans les sections suivantes :

1. Vérifiez la connectivité IPsec entre les noeuds.
2. Vérifiez les certificats IPsec.
3. Téléchargez les certificats racine IPsec à partir du noeud Abonné.
4. Téléchargez le certificat racine IPsec du noeud Abonné vers le noeud Éditeur.
5. Configurez la stratégie IPsec.

Vérifier la connectivité IPsec

Complétez ces étapes afin de vérifier la connectivité IPsec entre les noeuds :

1. Connectez-vous à la page Operating System (OS) Administration du serveur CUCM.
2. Accédez à **Services > Ping**.
3. Spécifiez l'adresse IP du noeud distant.
4. Cochez la case **Valider IPsec** et cliquez sur **Ping**.

S'il n'y a pas de connectivité IPsec, alors vous voyez des résultats similaires à ceci :

Ping Configuration

 Ping

Status

 Status: Ready

Ping Settings

Hostname or IP Address*

Ping Interval*

Packet Size*

Ping Iterations

Validate IPsec

Ping Results

IPsec connection failed..
Reasons :
a)No IPsec Policy on 10.106.110.8
b)Invalid Certificates IPsec connection failed..
Reasons :
a)No IPsec Policy on 10.106.110.8
b)Invalid Certificates

Vérifier les certificats IPsec

Complétez ces étapes afin de vérifier les certificats IPsec :

1. Connectez-vous à la page OS Administration.
2. Accédez à **Security > Certificate Management**.
3. Recherchez les certificats IPsec (connectez-vous séparément aux noeuds Éditeur et Abonné).

Note: Le certificat IPsec du noeud Abonné n'est généralement pas visible à partir du noeud Éditeur ; cependant, vous pouvez voir les certificats IPsec du noeud Éditeur sur tous les noeuds Abonné en tant que certificat IPsec-Trust.

Pour activer la connectivité IPsec, vous devez avoir un certificat IPsec d'un noeud défini comme un certificat **ipsec-trust** sur l'autre noeud :

PUBLISHER

Certificate List (1 - 2 of 2) Rows p

Find Certificate List where Certificate begins with ipsec

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Télécharger le certificat racine IPsec depuis l'abonné

Complétez ces étapes afin de télécharger le certificat racine IPsec à partir du noeud Abonné :

1. Connectez-vous à la page Administration du système d'exploitation du noeud Abonné.
2. Accédez à **Security > Certificate Management**.
3. Ouvrez le certificat racine IPsec et téléchargez-le au format **.pem** :

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Certificate Details for cucm10sub, ipsec

Regenerate Generate CSR Download .PEM File Download .DER File

Status

Status: Ready

Certificate Settings

File Name	ipsec.pem
Certificate Purpose	ipsec
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
Version: V3
Serial Number: 6B71952138766EF415EFE831AEB5F943
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=blr, ST=karnataka, CN=cucm10sub, OU=cucm, O=cisco, C=IN
Validity From: Mon Dec 15 23:26:27 IST 2014
To: Sat Dec 14 23:26:26 IST 2019
Subject Name: L=blr, ST=karnataka, CN=cucm10sub, OU=cucm, O=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100a376b6ad7825abe3069a421538c851a32d815321de77791985f99f2f9a
4b695016352b98cc72b26461cc629d0d2b35fc774d20fa13ae6c476164b7ccca82eb73034
7b6ad7e5069d732468f501ba53a018f9bbe422f6c76a4e4023fbad9bcf2f7d122cbe681375
feb7adb41068344a97a4f9b224180c6f8b223f75194ec7d987b0203010001
Extensions: 3 present
]
```

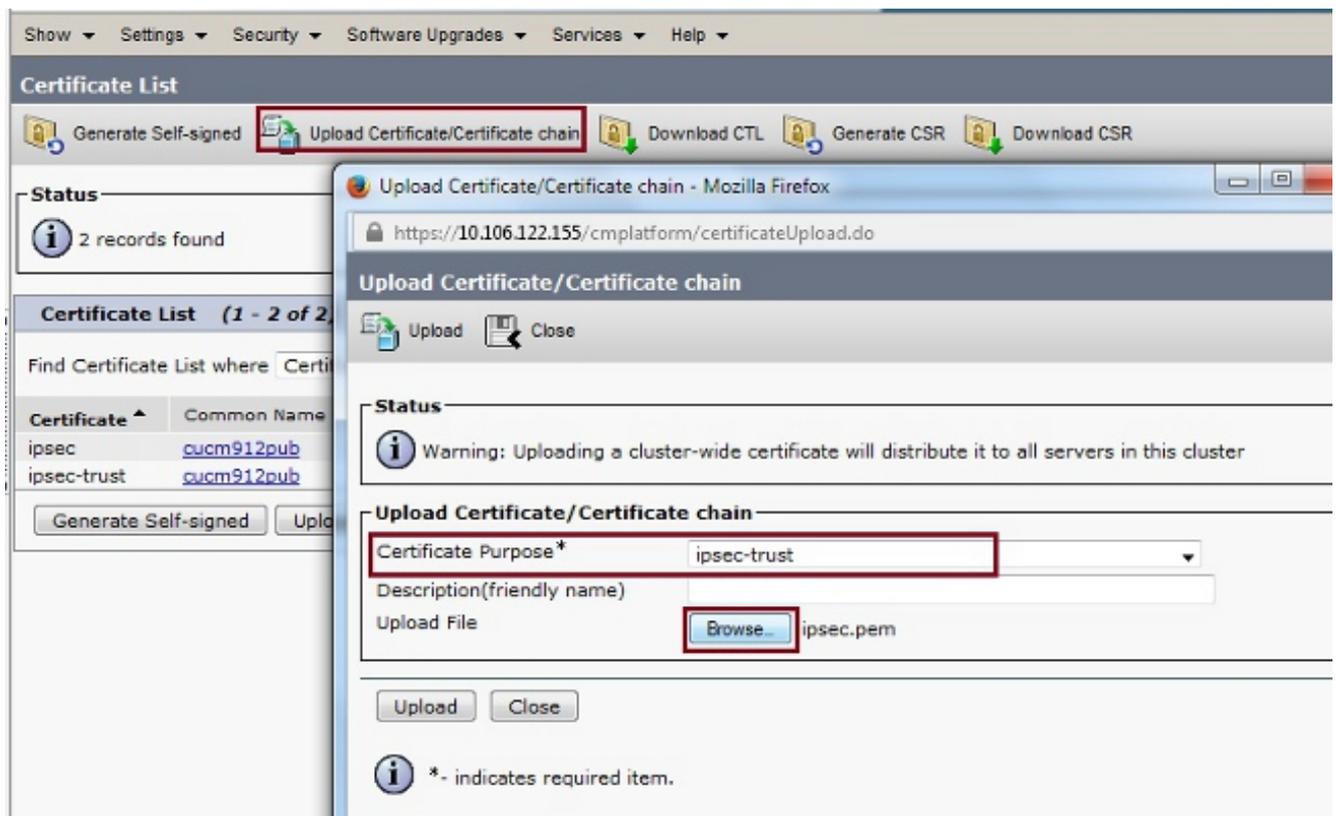
Regenerate Generate CSR Download .PEM File Download .DER File

Close

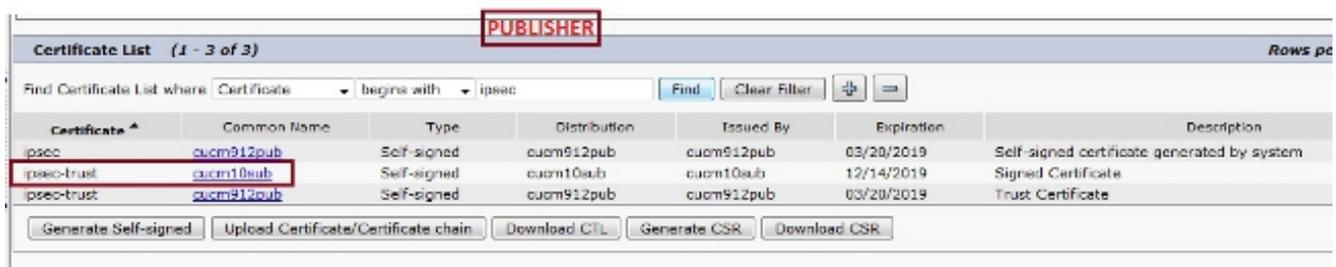
Télécharger le certificat racine IPsec de l'abonné vers l'éditeur

Complétez ces étapes afin de télécharger le certificat racine IPsec du noeud Abonné au noeud Éditeur :

1. Connectez-vous à la page OS Administration du noeud Publisher.
2. Accédez à **Security > Certificate Management**.
3. Cliquez sur **Upload Certificate/Certificate chain**, et téléchargez le certificat racine IPsec du noeud Abonné en tant que certificat **ipsec-trust** :



4. Après avoir téléchargé le certificat, vérifiez que le certificat racine IPsec du noeud Abonné apparaît comme suit :



Note: Si vous devez activer la connectivité IPsec entre plusieurs noeuds dans un cluster, vous devez télécharger les certificats racines IPsec pour ces noeuds également, puis les télécharger vers le noeud Éditeur via la même procédure.

Configurer la stratégie IPsec

Complétez ces étapes afin de configurer la stratégie IPsec :

1. Connectez-vous séparément à la page OS Administration des noeuds Publisher et Subscriber.
2. Accédez à **Security > IPSEC Configuration**.
3. Utilisez ces informations afin de configurer l'IP et les détails du certificat :

PUBLISHER : 10.106.122.155 & cucm912pub.pem

SUBSCRIBER: 10.106.122.15 & cucm10sub.pem

The screenshot shows the IPSEC Policy Configuration page for the PUBLISHER node. The page is titled "IPSEC Policy Configuration" and includes a "Save" button. A message states "The system is in non-FIPS Mode". The "IPSEC Policy Details" section contains the following fields:

Policy Group Name*	ToSubscriber
Policy Name*	ToSub
Authentication Method*	Certificate
Preshared Key	
Peer Type*	Different
Certificate Name*	cucm10sub.pem
Destination Address*	10.106.122.155
Destination Port*	ANY
Source Address*	10.106.122.155
Source Port*	ANY
Mode*	Transport
Remote Port*	500
Protocol*	TCP
Encryption Algorithm*	3DES
Hash Algorithm*	SHA1
ESP Algorithm*	AES 128

The "Phase 1 DH Group" section contains:

Phase One Life Time*	3600
Phase One DH*	Group 2

The "Phase 2 DH Group" section contains:

Phase Two Life Time*	3600
Phase Two DH*	Group 2

The "IPSEC Policy Configuration" section has the "Enable Policy" checkbox checked. A "Save" button is at the bottom.

The screenshot shows the IPSEC Policy Configuration page for the SUBSCRIBER node. The page is titled "IPSEC Policy Configuration" and includes a "Save" button. A message states "The system is in non-FIPS Mode". The "IPSEC Policy Details" section contains the following fields:

Policy Group Name*	ToPublisher
Policy Name*	ToPub
Authentication Method*	Certificate
Preshared Key	
Peer Type*	Different
Certificate Name*	cucm912pub.pem
Destination Address*	10.106.122.155
Destination Port*	ANY
Source Address*	10.106.122.155
Source Port*	ANY
Mode*	Transport
Remote Port*	500
Protocol*	TCP
Encryption Algorithm*	3DES
Hash Algorithm*	SHA1
ESP Algorithm*	AES 128

The "Phase 1 DH Group" section contains:

Phase One Life Time*	3600
Phase One DH*	Group 2

The "Phase 2 DH Group" section contains:

Phase Two Life Time*	3600
Phase Two DH*	Group 2

The "IPSEC Policy Configuration" section has the "Enable Policy" checkbox checked. A "Save" button is at the bottom.

Vérification

Complétez ces étapes afin de vérifier que votre configuration fonctionne et que la connectivité IPsec entre les noeuds est établie :

1. Connectez-vous à l'administration du système d'exploitation du serveur CUCM.
2. Accédez à **Services > Ping**.
3. Spécifiez l'adresse IP du noeud distant.
4. Cochez la case **Valider IPsec** et cliquez sur **Ping**.

Si la connectivité IPsec a été établie, un message semblable à celui-ci s'affiche :

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Ping Configuration

 Ping

Status

 Status: Ready

Ping Settings

Hostname or IP Address*

Ping Interval*

Packet Size*

Ping Iterations

Validate IPsec

Ping Results

Successfully validated IPsec connection to 10.106.122.159
Successfully validated IPsec connection to 10.106.122.159

Dépannage

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

Informations connexes

- [Guide d'administration du système d'exploitation Cisco Unified Communications, version 8.6\(1\) - Configuration d'une nouvelle stratégie IPsec](#)
- [Support et documentation techniques - Cisco Systems](#)