

Configuración de CUCM para la conexión IPsec entre nodos

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Información general sobre configuración](#)

[Verificar conectividad IPsec](#)

[Comprobar certificados IPsec](#)

[Descargar certificado raíz IPsec del suscriptor](#)

[Cargar certificado raíz IPsec del suscriptor al editor](#)

[Configurar directiva IPsec](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo establecer la conectividad IPsec entre los nodos de Cisco Unified Communications Manager (CUCM) dentro de un clúster.

Nota: De forma predeterminada, la conexión IPsec entre los nodos de CUCM está deshabilitada.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de CUCM.

Componentes Utilizados

La información de este documento se basa en la versión 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.

Configurar

Utilice la información que se describe en esta sección para configurar CUCM y establecer la conectividad IPsec entre los nodos de un clúster.

Información general sobre configuración

Estos son los pasos que se incluyen en este procedimiento, cada uno de los cuales se detalla en las siguientes secciones:

1. Verifique la conectividad IPsec entre los nodos.
2. Compruebe los certificados IPsec.
3. Descargue los certificados raíz IPsec del nodo de suscriptor.
4. Cargue el certificado raíz IPsec desde el nodo Suscriptor al nodo Editor.
5. Configure la directiva IPsec.

Verificar conectividad IPsec

Complete estos pasos para verificar la conectividad IPsec entre los nodos:

1. Inicie sesión en la página de administración del sistema operativo (SO) del servidor de CUCM.
2. Vaya a **Servicios > Ping**.
3. Especifique la dirección IP del nodo remoto.
4. Marque la casilla de verificación **Validar IPsec** y haga clic en **Ping**.

Si no hay conectividad IPsec, verá resultados similares a los siguientes:

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

Comprobar certificados IPsec

Complete estos pasos para verificar los certificados IPsec:

1. Inicie sesión en la página Administración del sistema operativo.
2. Vaya a **Seguridad > Administración de certificados**.
3. Busque los certificados IPsec (inicie sesión en los nodos Editor y Suscriptor por separado).

Nota: El certificado IPsec del nodo de suscriptor no suele verse desde el nodo de editor; sin embargo, puede ver los certificados IPsec del nodo de editor en todos los nodos de suscriptor como un certificado de confianza IPsec.

Para habilitar la conectividad IPsec, debe tener un certificado IPsec de un nodo establecido como un certificado **ipsec-trust** en el otro nodo:

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

Descargar certificado raíz IPsec del suscriptor

Complete estos pasos para descargar el certificado raíz IPsec del nodo de suscriptor:

1. Inicie sesión en la página Administración del sistema operativo del nodo Suscriptor.
2. Vaya a **Seguridad > Administración de certificados**.
3. Abra el certificado raíz IPsec y descárguelo en el formato **.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
]
```

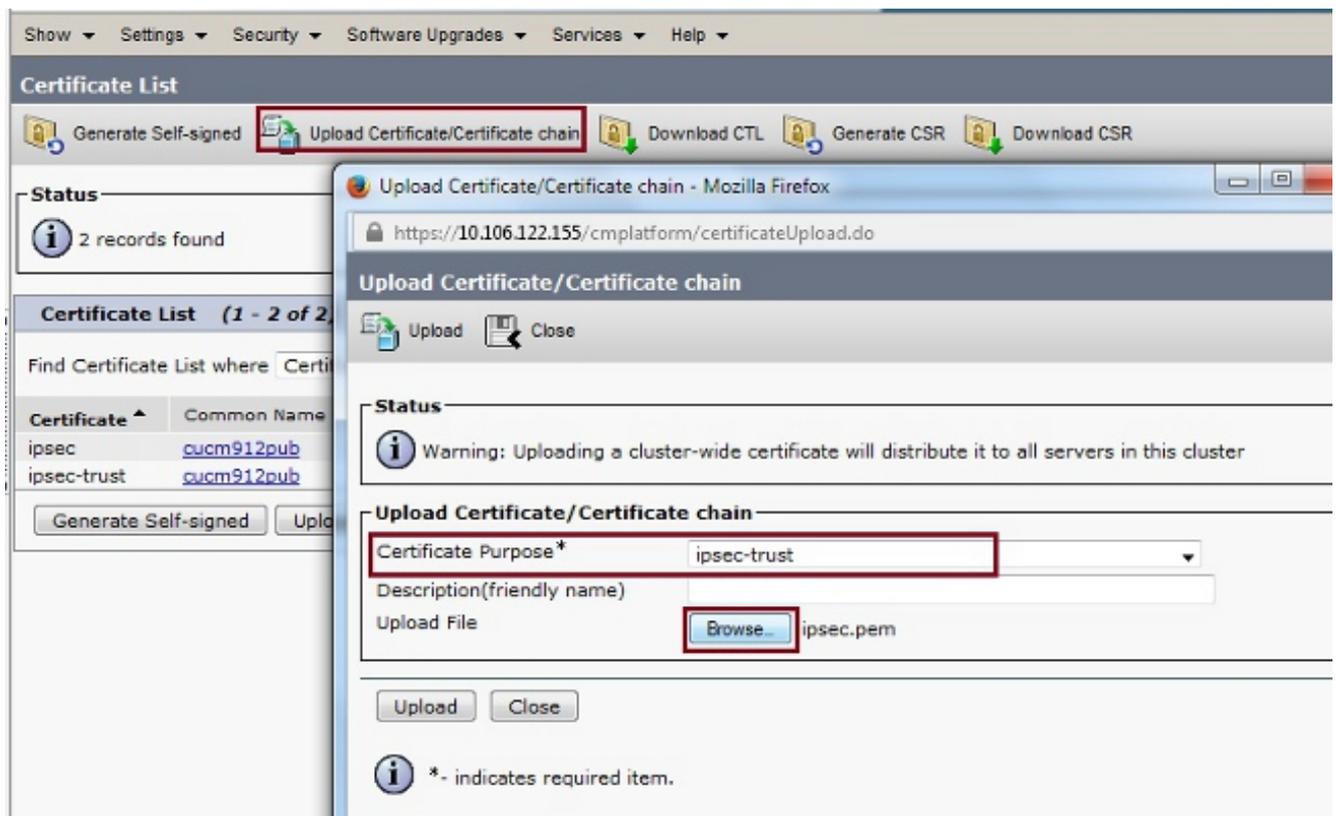
Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

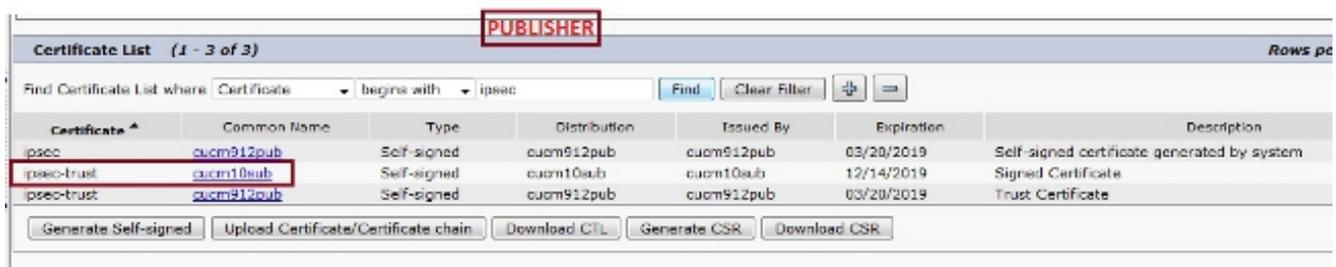
Cargar certificado raíz IPsec del suscriptor al editor

Complete estos pasos para cargar el certificado raíz IPsec desde el nodo Suscriptor al nodo Editor:

1. Inicie sesión en la página Administración del sistema operativo del nodo Editor.
2. Vaya a **Seguridad > Administración de certificados**.
3. Haga clic en **Cargar certificado/cadena de certificado**, y cargue el certificado raíz IPsec del nodo de suscriptor como un certificado **ipsec-trust**:



4. Después de cargar el certificado, verifique que el certificado raíz IPsec del nodo de suscriptor aparezca como se muestra:



Nota: Si necesita habilitar la conectividad IPsec entre varios nodos de un clúster, también debe descargar los certificados raíz IPsec para esos nodos y cargarlos en el nodo de editor mediante el mismo procedimiento.

Configurar directiva IPsec

Complete estos pasos para configurar la política IPsec:

1. Inicie sesión en la página Administración del sistema operativo de los nodos Editor y Suscriptor por separado.
2. Vaya a **Security > IPSEC Configuration**.
3. Utilice esta información para configurar la IP y los detalles del certificado:

PUBLISHER : 10.106.122.155 & cucm912pub.pem

SUBSCRIBER: 10.106.122.15 & cucm10sub.pem

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Show Settings Security Software Upgrades Services Help

IPSEC Policy Configuration **PUBLISHER**

Save

The system is in non-FIPS Mode

IPSEC Policy Details

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

Phase 1 DH Group

Phase One Life Time* 3600

Phase One DH* Group 2

Phase 2 DH Group

Phase Two Life Time* 3600

Phase Two DH* Group 2

IPSEC Policy Configuration

Enable Policy

Save

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Show Settings Security Software Upgrades Services Help

IPSEC Policy Configuration **SUBSCRIBER**

Save

The system is in non-FIPS Mode

IPSEC Policy Details

Policy Group Name* ToPublisher

Policy Name* ToPublisher

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

Phase 1 DH Group

Phase One Life Time* 3600

Phase One DH* Group 2

Phase 2 DH Group

Phase Two Life Time* 3600

Phase Two DH* Group 2

IPSEC Policy Configuration

Enable Policy

Save

Verificación

Complete estos pasos para verificar que su configuración funcione y que la conectividad IPsec entre los nodos esté establecida:

1. Inicie sesión en la Administración del sistema operativo del servidor de CUCM.
2. Vaya a **Servicios > Ping**.
3. Especifique la dirección IP del nodo remoto.
4. Marque la casilla de verificación **Validar IPsec** y haga clic en **Ping**.

Si se ha establecido la conectividad IPsec, aparecerá un mensaje similar a este:

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

Troubleshoot

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

Información Relacionada

- [Guía de administración del sistema operativo de Comunicaciones Unificadas de Cisco, versión 8.6\(1\) - Configuración de una nueva directiva IPsec](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)