

Configure el CUCM para conexión IPSec en medio los Nodos

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Información general sobre configuración](#)

[Verifique conectividad IPSec](#)

[Marque los Certificados del IPSec](#)

[Descargue el certificado raíz del IPSec del suscriptor](#)

[Cargue el certificado raíz del IPSec del suscriptor a Publisher](#)

[Configure la directiva del IPSec](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo establecer conectividad IPSec entre los Nodos del administrador de las Comunicaciones unificadas de Cisco (CUCM) dentro de un cluster.

Nota: Por abandono, conexión IPSec en medio los Nodos CUCM se inhabilitan.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del CUCM.

Componentes Utilizados

La información en este documento se basa en la versión 10.5(1) 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

Utilice la información que se describe en esta sección para configurar el CUCM y establecerlo conectividad IPsec entre los Nodos en un cluster.

Información general sobre configuración

Aquí están los pasos que están implicados en este procedimiento, que se detalla en las secciones que siguen:

1. Verifique conectividad IPsec en medio los Nodos.
2. Marque los Certificados del IPsec.
3. Descargue los certificados raíz del IPsec del nodo del suscriptor.
4. Cargue el certificado raíz del IPsec del nodo del suscriptor al nodo de Publisher.
5. Configure la directiva del IPsec.


Verifique conectividad IPsec

Complete estos pasos para verificar conectividad IPsec en medio los Nodos:


1. Registre en el operating system (OS) la página de administración del servidor CUCM.
2. Navegue a los **servicios > al ping**.
3. Especifique la dirección IP del nodo remoto.
4. Marque la casilla de verificación del **IPsec del validar** y haga clic el **ping**.

Si hay ningún conectividad IPsec, después usted ve los resultados similares a esto:

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

Certificados del IPSec del control

Complete estos pasos para marcar los Certificados del IPSec:

1. Registro en la página de administración OS.
2. Navegue al **Certificate Management (Administración de certificados) de la Seguridad**.
3. Busque para los Certificados del IPSec (registro en los Nodos del editor y suscriptor por separado).

Nota: El certificado del IPSec del nodo del suscriptor no es generalmente viewable del nodo de Publisher; sin embargo, usted puede ver los Certificados del IPSec del nodo de Publisher en todos los Nodos del suscriptor como certificado de la IPSec-confianza.

Para habilitar conectividad IPSec, usted debe tener un certificado del IPSec a partir de un nodo fijado como certificado de la IPSec-confianza 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

Certificado raíz del IPsec de la descarga del suscriptor

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

1. Registro en la página de administración OS del nodo del suscriptor.
2. Navegue al **Certificate Management (Administración de certificados)** de la Seguridad.
3. Abra el certificado raíz del IPsec y descarguelo en el formato del **.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
]
```

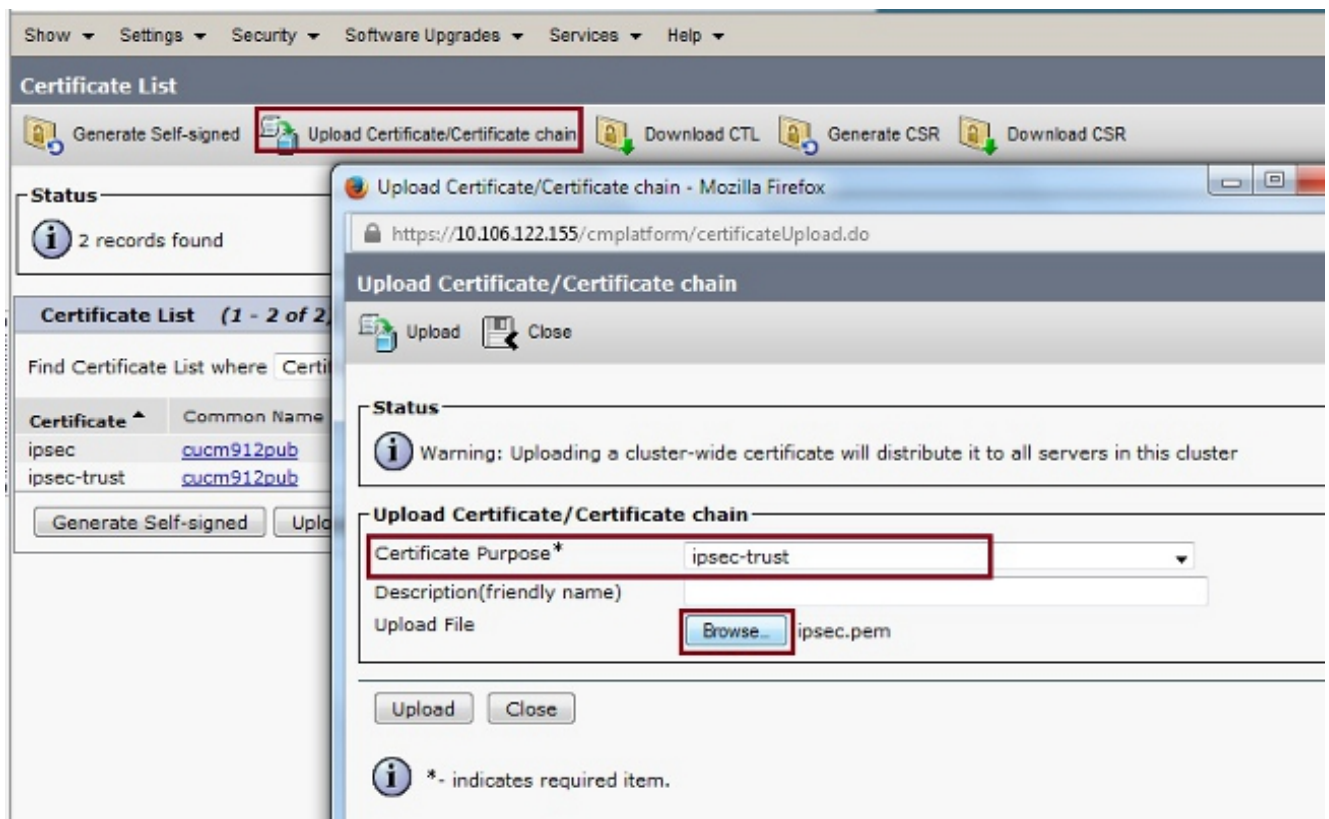
Regenerate Generate CSR Download .PEM File Download .DER File

Close

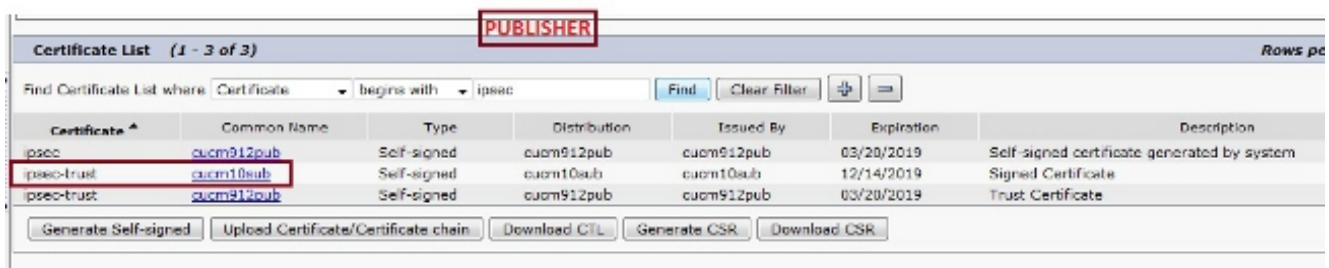
Cargue el certificado raíz del IPsec del suscriptor a Publisher

Complete estos pasos para cargar el certificado raíz del IPsec del nodo del suscriptor al nodo de Publisher:

1. Registro en la página de administración OS del nodo de Publisher.
2. Navegue al **Certificate Management (Administración de certificados)** de la Seguridad.
3. Haga clic el **certificado/la Cadena de certificados de la carga**, y cargue el certificado raíz del IPsec del nodo del suscriptor como certificado de la IPsec-**confianza**:



- Después de que usted cargue el certificado, verifique que aparezca el certificado raíz del IPsec del nodo del suscriptor como se muestra:



Nota: Si le requieren habilitar conectividad IPsec entre los nodos múltiples en un cluster, después usted debe descargar los certificados raíz del IPsec para esos Nodos también, y los carga al nodo de Publisher vía el mismo procedimiento.

Directiva del IPsec de la configuración

Complete estos pasos para configurar la directiva del IPsec:

- Registro en la página de administración OS de Publisher y de los Nodos del suscriptor por separado.
- Navegue a la **Seguridad > a la configuración IPsec**.
- Utilice esta información para configurar el IP y a los detalles del certificado:

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*	10.106.122.159
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 has:

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

The "Phase 2 DH Group" section has:

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*	ToPublisher
Authentication Method*	Certificate
Preshared Key	
Peer Type*	Different
Certificate Name*	cucm912pub.pem
Destination Address*	10.106.122.155
Destination Port*	ANY
Source Address*	10.106.122.159
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 has:

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

The "Phase 2 DH Group" section has:

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.

Verificación


Complete estos pasos para verificar que sus trabajos de la configuración y que conectividad IPsec en medio los Nodos están establecidos:

1. Registro en la administración OS del servidor CUCM.
2. Navegue a los **servicios > al ping**.
3. Especifique la dirección IP del nodo remoto.
4. Marque la casilla de verificación del **IPSec del validar** y haga clic el **ping**.


Si conectividad IPsec se ha establecido, después usted ve un mensaje similar a esto:

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

Troubleshooting

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

Información Relacionada

- [La guía de administración del sistema operativo de las Comunicaciones unificadas de Cisco, libera 8.6\(1\) – configure una nueva directiva del IPsec](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)