

Configurar o CUCM para conexão IPsec entre nós

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Visão geral sobre a configuração](#)

[Verificar a conectividade IPsec](#)

[Verificar Certificados IPsec](#)

[Baixar Certificado Raiz IPsec do Assinante](#)

[Carregar Certificado Raiz IPsec do Assinante para o Publicador](#)

[Configurar Diretiva IPsec](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como estabelecer a conectividade IPsec entre os nós do Cisco Unified Communications Manager (CUCM) em um cluster.

Note: Por padrão, a conexão IPsec entre os nós CUCM está desabilitada.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do CUCM.

Componentes Utilizados

As informações neste documento são baseadas no CUCM Versão 10.5(1).

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

Use as informações descritas nesta seção para configurar o CUCM e estabelecer a conectividade IPsec entre os nós em um cluster.

Visão geral sobre a configuração

Estas são as etapas envolvidas neste procedimento, cada uma das quais é detalhada nas seções a seguir:

1. Verifique a conectividade IPsec entre os nós.
2. Verifique os certificados IPsec.
3. Baixe os certificados raiz IPsec do nó Assinante.
4. Carregue o certificado raiz IPsec do nó Assinante para o nó Publicador.
5. Configure a política IPsec.


Verificar a conectividade IPsec

Conclua estas etapas para verificar a conectividade IPsec entre os nós:


1. Faça login na página de administração do sistema operacional (SO) do servidor CUCM.
2. Navegue até **Serviços > Ping**.
3. Especifique o endereço IP do nó remoto.
4. Marque a caixa de seleção **Validate IPsec** e clique em **Ping**.

Se não houver conectividade IPsec, você verá resultados semelhantes a este:

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

Verificar Certificados IPsec

Conclua estas etapas para verificar os certificados IPsec:

1. Efetue login na página OS Administration.
2. Navegue até **Segurança > Gerenciamento de certificado**.
3. Procure os certificados IPsec (faça login nos nós Publicador e Assinante separadamente).

Note: O certificado IPsec do nó do assinante geralmente não pode ser exibido no nó do Publicador; no entanto, você pode ver os certificados IPsec do nó Publicador em todos os nós do Assinante como um certificado IPsec-Trust.

Para habilitar a conectividade IPsec, você deve ter um certificado IPsec de um nó definido como um certificado **ipsec-trust** no outro nó:

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 |

Note: A red box labeled "IPSEC Root certificates" has an arrow pointing to the "ipsec" row in the PUBLISHER table and the "ipsec" row in the SUBSCRIBER table.

Baixar Certificado Raiz IPsec do Assinante

Conclua estas etapas para baixar o certificado raiz IPsec do nó do Assinante:

1. Efetue login na página OS Administration do nó Subscriber.
2. Navegue até **Segurança > Gerenciamento de certificado**.
3. Abra o certificado raiz IPsec e baixe-o no 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 |

Note: A red box labeled "IPSEC Root certificates" has an arrow pointing to the "ipsec" row in the SUBSCRIBER table.

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
]
```

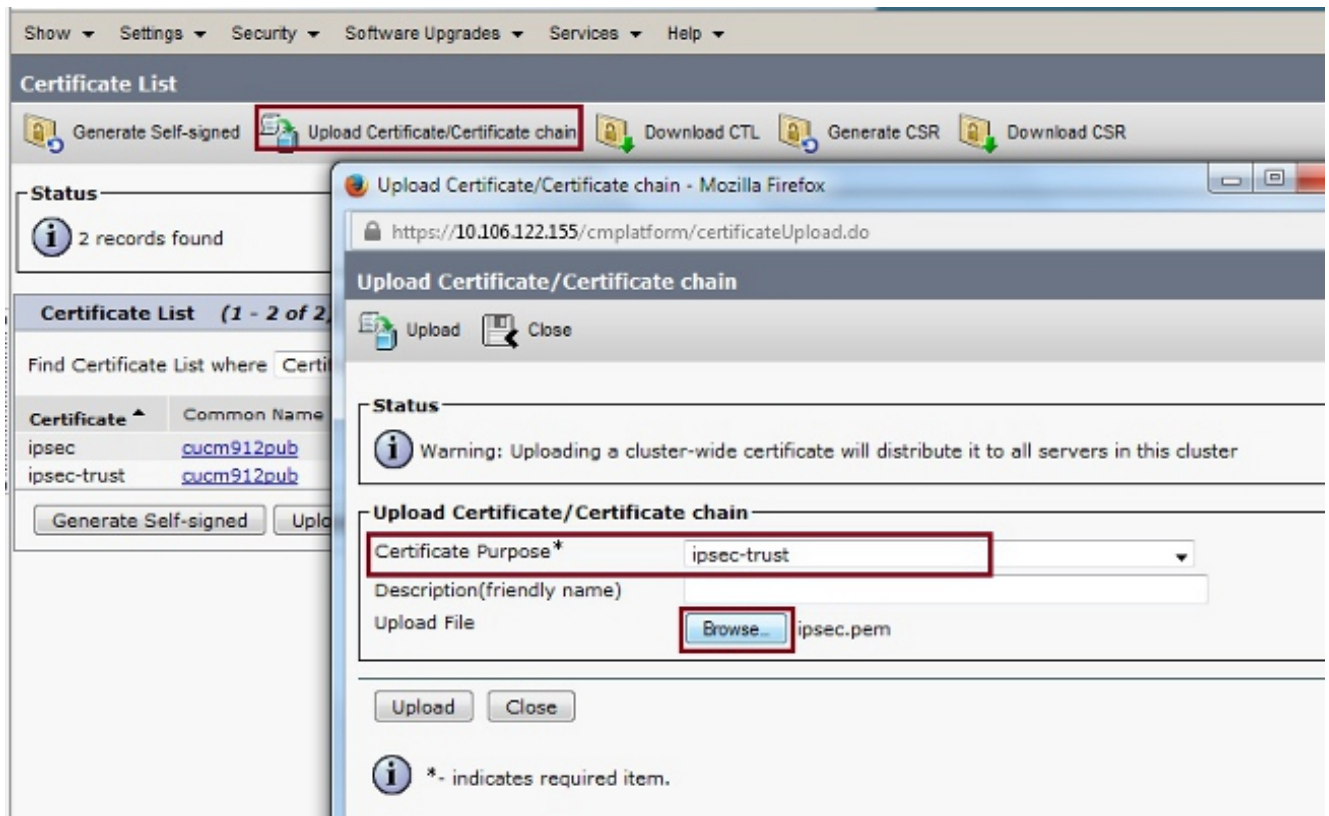
Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

Carregar Certificado Raiz IPsec do Assinante para o Publicador

Conclua estas etapas para carregar o certificado raiz IPsec do nó Assinante para o nó Publicador:

1. Efetue login na página OS Administration do nó Publisher.
2. Navegue até **Segurança > Gerenciamento de certificado**.
3. Clique em **Carregar certificado/cadeia de certificados** e carregue o certificado raiz IPsec do nó do assinante como um certificado **ipsec-trust**:



4. Após carregar o certificado, verifique se o certificado raiz IPsec do nó do assinante aparece conforme mostrado:

PUBLISHER

| Certificate List (1 - 3 of 3) | | | | | | | Rows per page |
|--|-------------|-------------|--------------|------------|------------|---|-------------------|
| Find Certificate List where: Certificate begins with ipsec | | | | | | | Find Clear Filter |
| Certificate | Common Name | Type | Distribution | Issued By | Expiration | Description | |
| ipsec | cuom912pub | Self-signed | cuom912pub | cuom912pub | 03/20/2019 | Self-signed certificate generated by system | |
| ipsec-trust | cuom10sub | Self-signed | cuom10sub | cuom10sub | 12/14/2019 | Signed Certificate | |
| ipsec-trust | cuom912pub | Self-signed | cuom912pub | cuom912pub | 03/20/2019 | Trust Certificate | |

Note: Se for necessário habilitar a conectividade IPsec entre vários nós em um cluster, você deverá baixar os certificados raiz IPsec para esses nós também e carregá-los no nó do Publicador por meio do mesmo procedimento.

Configurar Diretiva IPsec

Conclua estas etapas para configurar a política IPsec:

1. Efetue login na página OS Administration do Publisher e dos nós Subscriber separadamente.
2. Navegue até **Segurança > Configuração de IPSEC**.
3. Use estas informações para configurar o IP e os detalhes do 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), and ESP Algorithm (AES 128). The "Phase 1 DH Group" section has Phase One Life Time (3600) and Phase One DH (Group 2). The "Phase 2 DH Group" section has Phase Two Life Time (3600) and 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), and ESP Algorithm (AES 128). The "Phase 1 DH Group" section has Phase One Life Time (3600) and Phase One DH (Group 2). The "Phase 2 DH Group" section has Phase Two Life Time (3600) and Phase Two DH (Group 2). The "IPSEC Policy Configuration" section has the "Enable Policy" checkbox checked. A "Save" button is at the bottom.

Verificar


Conclua estas etapas para verificar se sua configuração funciona e se a conectividade IPsec entre os nós está estabelecida:

1. Faça login na Administração do SO do servidor CUCM.
2. Navegue até **Serviços > Ping**.
3. Especifique o endereço IP do nó remoto.
4. Marque a caixa de seleção **Validate IPsec** e clique em **Ping**.


Se a conectividade IPsec tiver sido estabelecida, você verá uma mensagem semelhante a esta:

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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Guia de Administração do Sistema Operacional Cisco Unified Communications, Versão 8.6\(1\) - Configuração de uma Nova Política IPsec](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)