

配置IPSec连接的CUCM节点之间

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[配置概述](#)

[验证IPSec连通性](#)

[检查IPsec证书](#)

[从订户下载IPsec根证明](#)

[从订户加载IPsec根证明到发布人](#)

[配置IPsec策略](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

本文描述如何设立Cisco Unified通信管理器(CUCM)节点之间的IPSec连通性在簇内。

Note:默认情况下，CUCM节点之间的IPSec连接是失效的。

Prerequisites

Requirements

Cisco建议您有CUCM知识。

Components Used

本文的信息根据CUCM版本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.

Configure

请使用在此部分在簇描述为了配置CUCM和设立节点之间的IPSec连通性的信息。

配置概述

这是在此程序涉及，其中每一在部分被选派跟随的步骤：

1. 验证节点之间的IPSec连通性。
2. 检查IPsec证书。
3. 从订户节点下载IPsec根证明。
4. 从订户节点加载IPsec根证明到发布人节点。
5. 配置IPsec策略。


验证IPSec连通性

完成这些步骤为了验证节点之间的IPSec连通性：


1. 记录到操作系统(OS) CUCM服务器的管理页面。
2. 连接对**Services> Ping**。
3. 指定远程节点IP地址。
4. 检查**验证IPsec**复选框并且点击**Ping**。

如果没有IPSec连通性，则您看到结果类似于此：

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

检查IPsec证书

完成这些步骤为了检查IPsec证书：

1. 记录到OS管理页面。
2. 连接对**安全 > Certificate Management**。
3. 搜索IPsec证书(日志到分开发布服务器和用户节点里)。

Note:订户节点IPsec认证从发布者节点通常不是看得见;然而，您能看到在所有的发布者节点IPsec证书订户节点作为IPsec信任认证。

为了enable (event) IPsec连通性，您必须有从作为在另一个节点的ipsec信任认证设置的一个节点的一个IPsec认证：

PUBLISHER

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	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" points to the "ipsec" certificate in both screenshots.

下载从订户的IPsec根证明

完成这些步骤为了从订户节点下载IPsec根证明：

1. 记录到OS订户节点的管理页面。
2. 连接对**安全**> **Certificate Management**。
3. 打开IPsec根证明并且下载它以.pem格式：

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" points to the "ipsec" certificate in this screenshot.

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
]
```

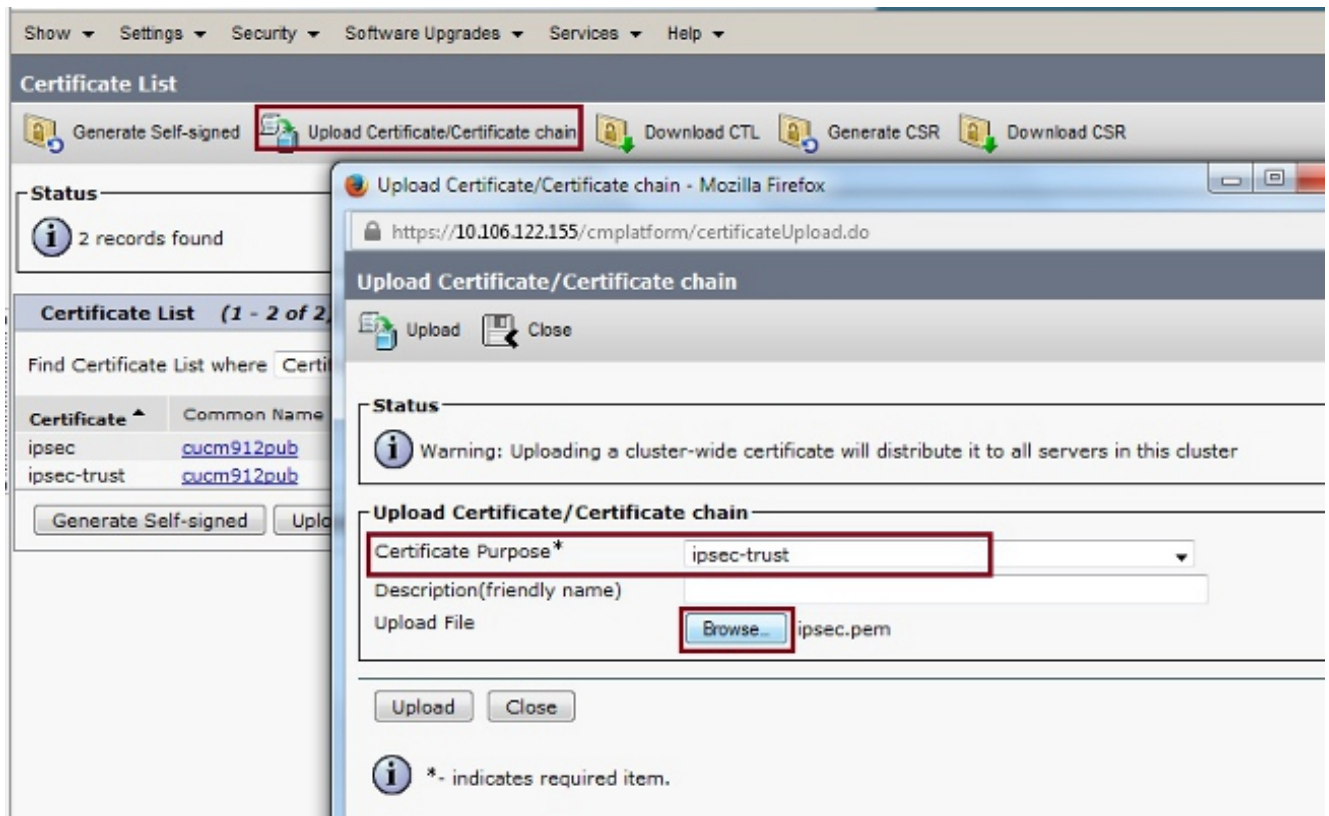
Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

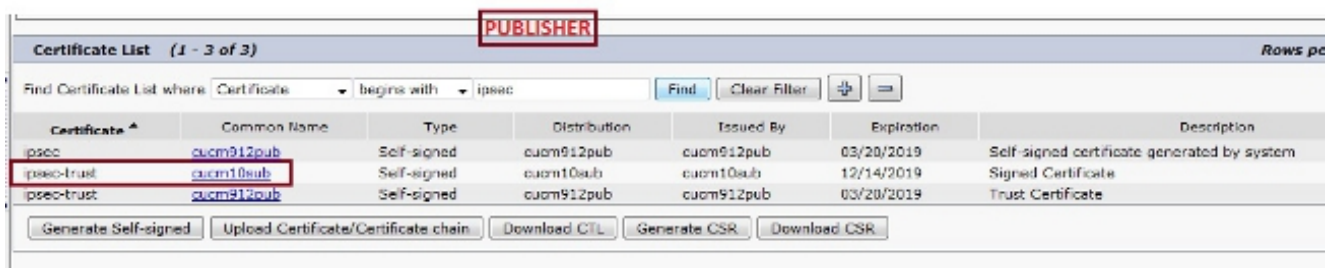
从订户加载IPsec根证明到发布人

完成这些步骤为了从订户节点加载IPsec根证明到发布人节点：

1. 记录到OS发布人节点的管理页面。
2. 连接对安全> Certificate Management。
3. 点击加载认证/证书链，并且加载订户节点IPsec根证明作为ipsec信任认证：



4. 在您加载认证后，请验证订户节点IPsec根证明出现如显示：



Note: 如果需要对enable (event)多个节点之间的IPSec连通性在簇，则您必须下载那些节点的IPsec根证明，并且加载他们到发布者节点通过同一个程序。

配置IPsec策略

完成这些步骤为了配置IPsec策略：

1. 分开记录到OS发布人和订户节点的管理页面。
2. 连接对安全> IPsec配置。
3. 请使用此信息为了配置IP和证书详细信息：

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 10.106.122.159
 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

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 cuom912pub.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

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

Verify


完成这些步骤为了验证您的配置工作，并且节点之间的IPSec连通性设立：

1. 记录到OS CUCM服务器的管理。
2. 连接对**Services> Ping**。
3. 指定远程节点IP地址。
4. 检查**验证IPsec**复选框并且点击**Ping**。


如果IPSec连通性设立了，则您看到消息类似于此：

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

目前没有针对此配置故障排除信息。

Related Information

- [Cisco Unified通信操作系统的管理指南，发布8.6\(1\) -请设置一个新的IPsec策略](#)
- [Technical Support & Documentation - Cisco Systems](#)