

노드 간 IPsec 연결을 위한 CUCM 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[구성 개요](#)

[IPsec 연결 확인](#)

[IPsec 인증서 확인](#)

[가입자에서 IPsec 루트 인증서 다운로드](#)

[구독자에서 게시자로 IPsec 루트 인증서 업로드](#)

[IPsec 정책 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 클러스터 내의 CUCM(Cisco Unified Communications Manager) 노드 간에 IPsec 연결을 설정하는 방법에 대해 설명합니다.

참고: 기본적으로 CUCM 노드 간의 IPsec 연결은 비활성화되어 있습니다.

사전 요구 사항

요구 사항

CUCM에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 CUCM 버전 10.5(1)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든

명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

CUCM을 구성하고 클러스터의 노드 간에 IPsec 연결을 설정하려면 이 섹션에 설명된 정보를 사용하십시오.

구성 개요

이 절차와 관련된 단계는 다음과 같습니다. 각 단계는 다음 섹션에 자세히 설명되어 있습니다.

1. 노드 간의 IPsec 연결을 확인합니다.
2. IPsec 인증서를 확인합니다.
3. 가입자 노드에서 IPsec 루트 인증서를 다운로드합니다.
4. 가입자 노드에서 게시자 노드로 IPsec 루트 인증서를 업로드합니다.
5. IPsec 정책을 구성합니다.

IPsec 연결 확인

노드 간의 IPsec 연결을 확인하려면 다음 단계를 완료하십시오.

1. CUCM 서버의 OS(운영 체제) 관리 페이지에 로그인합니다.
 2. **Services(서비스) > Ping**으로 이동합니다.
 3. 원격 노드 IP 주소를 지정합니다.
 4. **Validate IPsec(IPsec 검증)** 확인란을 선택하고 **Ping**을 클릭합니다.
- IPsec 연결이 없는 경우 다음과 유사한 결과가 표시됩니다.

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
            
```

IPsec 인증서 확인

IPsec 인증서를 확인하려면 다음 단계를 완료하십시오.

1. OS 관리 페이지에 로그인합니다.
2. Security(보안) > Certificate Management(인증서 관리)로 이동합니다.
3. IPsec 인증서를 검색합니다(게시자 노드와 가입자 노드에 별도로 로그인합니다).

참고: 가입자 노드 IPsec 인증서는 일반적으로 게시자 노드에서 볼 수 없습니다. 그러나 모든 가입자 노드의 게시자 노드 IPsec 인증서를 IPsec-Trust 인증서로 볼 수 있습니다.

IPsec 연결을 활성화하려면 한 노드의 IPsec 인증서가 다른 노드의 ipsec 신뢰 인증서로 설정되어 있어야 합니다.

PUBLISHER

Certificate List (1 - 2 of 2) Rows p

Find Certificate List where Certificate begins with ipsec Find Clear Filter

| 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 |

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR Download CSR

IPSEC Root certificates

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec Find Clear Filter

| 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 |

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

가입자에서 IPsec 루트 인증서 다운로드

가입자 노드에서 IPsec 루트 인증서를 다운로드하려면 다음 단계를 완료합니다.

1. 가입자 노드의 OS 관리 페이지에 로그인합니다.
2. Security(보안) > Certificate Management(인증서 관리)로 이동합니다.
3. IPsec 루트 인증서를 열고 .pem 형식으로 다운로드합니다.

IPSEC Root certificates

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec Find Clear Filter

| 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 |

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

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
]
```

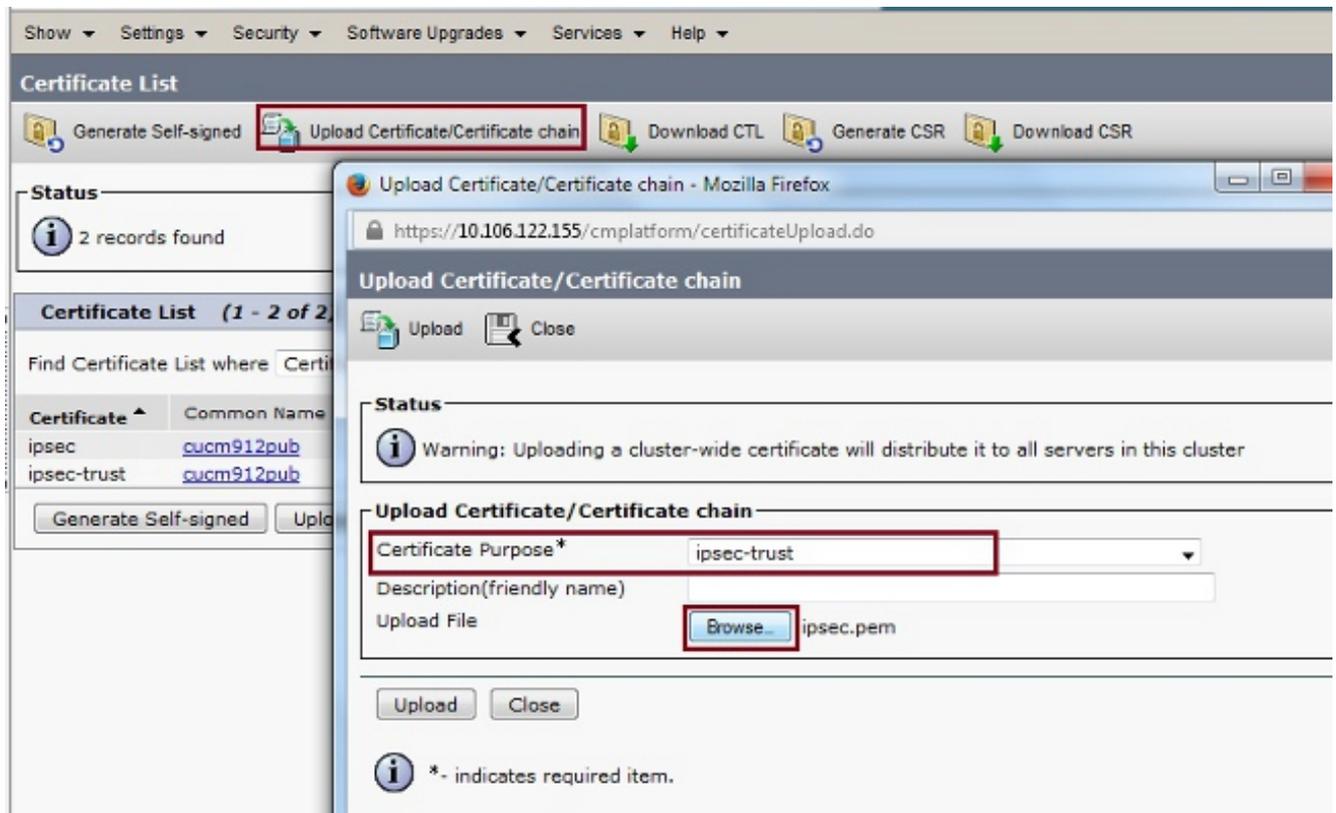
Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

구독자에서 게시자로 IPsec 루트 인증서 업로드

가입자 노드에서 게시자 노드로 IPsec 루트 인증서를 업로드하려면 다음 단계를 완료합니다.

1. 게시자 노드의 OS 관리 페이지에 로그인합니다.
2. Security(보안) > Certificate Management(인증서 관리)로 이동합니다.
3. Upload Certificate/Certificate chain(인증서/인증서 체인 업로드)을 클릭하고 가입자 노드 IPsec 루트 인증서를 ipsec-trust 인증서로 업로드합니다.



4. 인증서를 업로드한 후 다음과 같이 가입자 노드 IPsec 루트 인증서가 나타나는지 확인합니다.



참고: 클러스터의 여러 노드 간에 IPsec 연결을 활성화해야 하는 경우 해당 노드에 대한 IPsec 루트 인증서도 다운로드하고 동일한 절차를 통해 게시자 노드에 업로드해야 합니다.

IPsec 정책 구성

IPsec 정책을 구성하려면 다음 단계를 완료하십시오.

1. 게시자 및 가입자 노드의 OS 관리 페이지에 별도로 로그인합니다.
2. Security(보안) > IPSEC Configuration(IPSEC 컨피그레이션)으로 이동합니다.
3. IP 및 인증서 세부사항을 구성하려면 다음 정보를 사용하십시오.

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

다음을 확인합니다.

컨피그레이션이 작동하고 노드 간의 IPsec 연결이 설정되었는지 확인하려면 다음 단계를 완료하십시오.

1. CUCM 서버의 OS 관리에 로그인합니다.
2. Services(서비스) > Ping으로 이동합니다.
3. 원격 노드 IP 주소를 지정합니다.

4. Validate IPsec(IPsec 검증) 확인란을 선택하고 Ping을 클릭합니다.

IPsec 연결이 설정된 경우 다음과 유사한 메시지가 표시됩니다.

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

Ping

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- [Cisco Unified Communications 운영 체제 관리 설명서, 릴리스 8.6\(1\) - 새 IPsec 정책 설정](#)
- [기술 지원 및 문서 - Cisco Systems](#)