

Configurare CUCM per la connessione IPSec tra i nodi

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Panoramica della configurazione](#)

[Verifica connettività IPsec](#)

[Verifica certificati IPsec](#)

[Scarica certificato radice IPsec dal Sottoscrittore](#)

[Carica certificato radice IPsec dal Sottoscrittore al server di pubblicazione](#)

[Configura criterio IPsec](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come stabilire la connettività IPsec tra i nodi Cisco Unified Communications Manager (CUCM) all'interno di un cluster.

Nota: Per impostazione predefinita, la connessione IPsec tra i nodi CUCM è disabilitata.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di CUCM.

Componenti usati

Le informazioni fornite in questo documento si basano sulla versione 10.5(1) di CUCM.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Utilizzare le informazioni descritte in questa sezione per configurare CUCM e stabilire la connettività IPsec tra i nodi di un cluster.

Panoramica della configurazione

Di seguito sono riportati i passaggi della procedura, descritti in dettaglio nelle sezioni seguenti:

1. Verificare la connettività IPsec tra i nodi.
2. Controllare i certificati IPsec.
3. Scaricare i certificati radice IPsec dal nodo del Sottoscrittore.
4. Caricare il certificato radice IPsec dal nodo Sottoscrittore al nodo Server di pubblicazione.
5. Configurare il criterio IPsec.


Verifica connettività IPsec

Per verificare la connettività IPsec tra i nodi, completare i seguenti passaggi:


1. Accedere alla pagina Amministrazione del sistema operativo del server CUCM.
2. Selezionare **Servizi > Ping**.
3. Specificare l'indirizzo IP del nodo remoto.
4. Selezionare la casella di controllo **Convalida IPsec** e fare clic su **Ping**.

Se non è disponibile una connettività IPsec, i risultati saranno simili a quelli riportati di seguito:

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

Verifica certificati IPSec

Per controllare i certificati IPSec, completare la procedura seguente:

1. Accedere alla pagina Amministrazione del sistema operativo.
2. Passare a **Protezione > Gestione certificati**.
3. Cercare i certificati IPSec (accedere separatamente ai nodi del server di pubblicazione e del Sottoscrittore).

Nota: Il certificato IPSec del nodo del Sottoscrittore non è in genere visualizzabile dal nodo del server di pubblicazione. è tuttavia possibile visualizzare i certificati IPSec del nodo del server di pubblicazione in tutti i nodi del Sottoscrittore come certificato di attendibilità IPSec.

Per abilitare la connettività IPSec, è necessario disporre di un certificato IPSec di un nodo impostato come certificato **di trust IPSec** dell'altro 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

Scarica certificato radice IPsec dal Sottoscrittore

Completare questa procedura per scaricare il certificato radice IPsec dal nodo del Sottoscrittore:

1. Accedere alla pagina Amministrazione del sistema operativo del nodo Sottoscrittore.
2. Passare a **Protezione > Gestione certificati**.
3. Aprire il certificato radice IPsec e scaricarlo nel 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
]
```

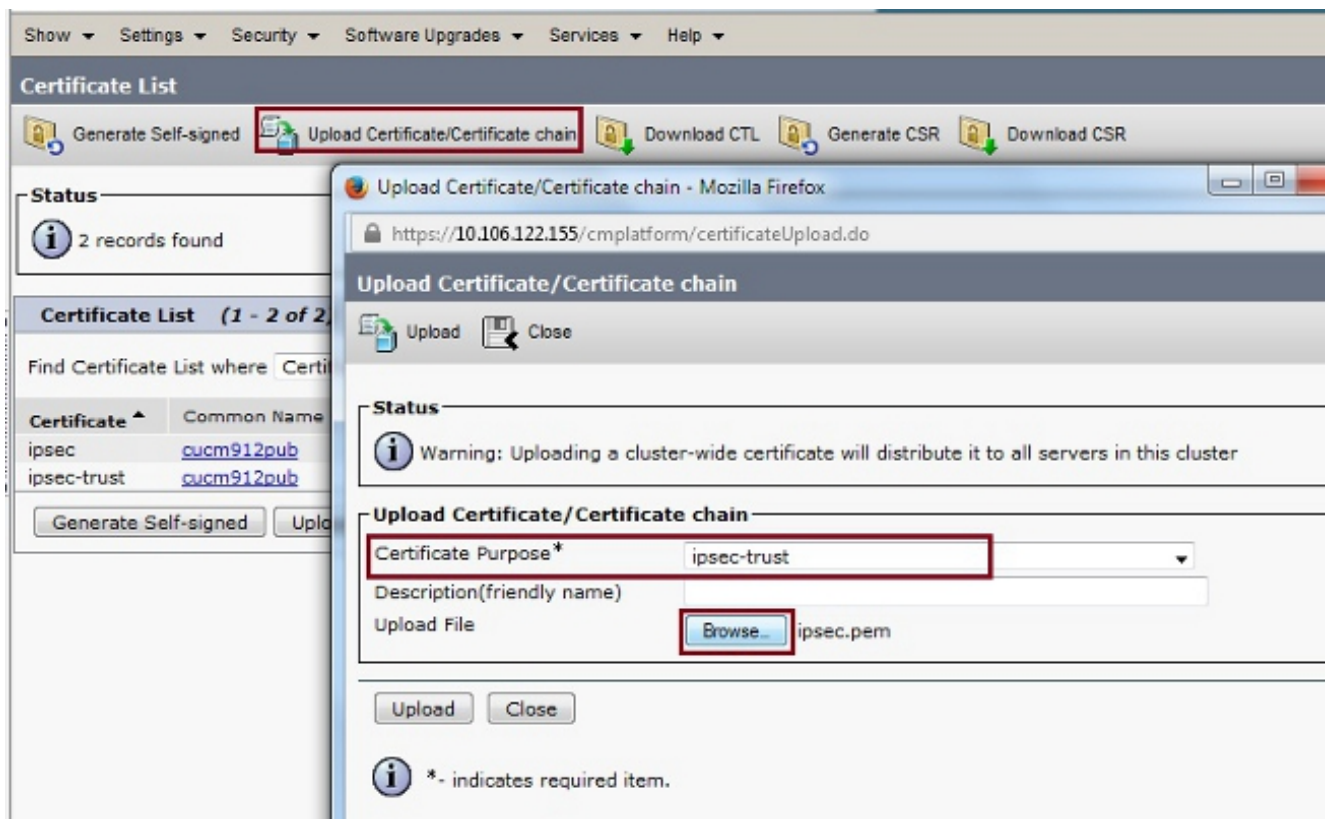
Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

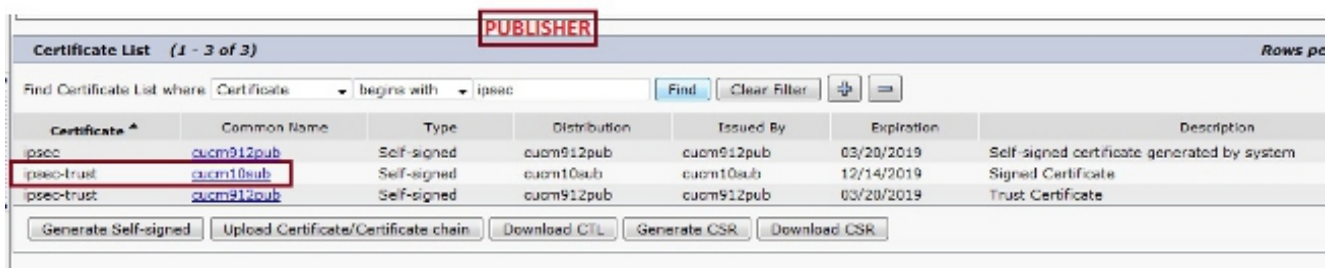
Carica certificato radice IPsec dal Sottoscrittore al server di pubblicazione

Per caricare il certificato radice IPsec dal nodo Sottoscrittore al nodo Server di pubblicazione, completare la procedura seguente:

1. Accedere alla pagina Amministrazione del sistema operativo del nodo Publisher.
2. Passare a **Protezione > Gestione certificati**.
3. Fare clic su **Upload Certificate/Certificate chain** e caricare il certificato radice IPsec del nodo del Sottoscrittore come certificato **di attendibilità IPsec**:



4. Dopo aver caricato il certificato, verificare che il certificato radice IPsec del nodo del Sottoscrittore venga visualizzato come illustrato di seguito:



Nota: Se è necessario abilitare la connettività IPsec tra più nodi in un cluster, è necessario scaricare anche i certificati radice IPsec per tali nodi e caricarli nel nodo di Publisher mediante la stessa procedura.

Configura criterio IPsec

Per configurare il criterio IPsec, completare la procedura seguente:

1. Accedere alla pagina Amministrazione del sistema operativo del server di pubblicazione e ai nodi del Sottoscrittore separatamente.
2. Selezionare **Protezione > Configurazione IPSEC**.
3. Utilizzare queste informazioni per configurare i dettagli dell'IP e del certificato:

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 system is in non-FIPS mode. The configuration details are as follows:

Field	Value
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

The screenshot shows the 'IPSEC Policy Configuration' page for the 'SUBSCRIBER' node. The system is in non-FIPS mode. The configuration details are as follows:

Field	Value
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

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

Verifica


Completare questa procedura per verificare che la configurazione funzioni e che sia stabilita la connettività IPsec tra i nodi:

1. Accedere all'amministrazione del sistema operativo del server CUCM.
2. Selezionare **Servizi > Ping**.
3. Specificare l'indirizzo IP del nodo remoto.
4. Selezionare la casella di controllo **Convalida IPsec** e fare clic su **Ping**.


Se è stata stabilita la connettività IPsec, verrà visualizzato un messaggio simile al seguente:

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

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- [Guida all'amministrazione del sistema operativo Cisco Unified Communications, versione 8.6\(1\) - Impostazione di un nuovo criterio IPsec](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)