

Konfigurieren des CUCM für die IPsec-Verbindung zwischen Knoten

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurationsübersicht](#)

[IPsec-Verbindung überprüfen](#)

[IPsec-Zertifikate überprüfen](#)

[IPsec-Stammzertifikat vom Abonnenten herunterladen](#)

[IPsec-Stammzertifikat von Abonnent auf Herausgeber hochladen](#)

[Konfigurieren der IPsec-Richtlinie](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie eine IPsec-Verbindung zwischen den Cisco Unified Communications Manager (CUCM)-Knoten in einem Cluster hergestellt wird.

Anmerkung: Standardmäßig ist die IPsec-Verbindung zwischen den CUCM-Knoten deaktiviert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des CUCM verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der CUCM-Version 10.5(1).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um den CUCM zu konfigurieren und eine IPsec-Verbindung zwischen den Knoten in einem Cluster herzustellen.

Konfigurationsübersicht

Im Folgenden sind die einzelnen Schritte dieses Verfahrens aufgeführt, die in den folgenden Abschnitten im Einzelnen beschrieben werden:

1. Überprüfen der IPsec-Verbindung zwischen den Knoten
2. Überprüfen Sie die IPsec-Zertifikate.
3. Laden Sie die IPsec-Stammzertifikate vom Subscriber-Knoten herunter.
4. Laden Sie das IPsec-Stammzertifikat vom Subscriber-Knoten auf den Publisher-Knoten hoch.
5. Konfigurieren der IPsec-Richtlinie


IPsec-Verbindung überprüfen

Führen Sie die folgenden Schritte aus, um die IPsec-Verbindung zwischen den Knoten zu überprüfen:


1. Melden Sie sich bei der Seite "Betriebssystem-Administration" des CUCM-Servers an.
2. Navigieren Sie zu **Dienste > Ping**.
3. Geben Sie die IP-Adresse des Remote-Knotens an.
4. Aktivieren Sie das Kontrollkästchen **IPsec validieren**, und klicken Sie auf **Ping**.

Wenn keine IPsec-Verbindung besteht, werden ähnliche Ergebnisse angezeigt:

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-Zertifikate überprüfen

Führen Sie die folgenden Schritte aus, um die IPsec-Zertifikate zu überprüfen:

1. Melden Sie sich bei der Seite "Betriebssystemverwaltung" an.
2. Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**.
3. Suchen Sie nach den IPsec-Zertifikaten (melden Sie sich separat bei den Publisher- und Subscriber-Knoten an).

Anmerkung: Das Abonnentenknoten-IPsec-Zertifikat kann normalerweise nicht vom Verlegerknoten angezeigt werden. Sie können jedoch die IPsec-Zertifikate des Verlegerknotens auf allen Abonnentenknoten als IPsec-Trust-Zertifikat sehen.

Um die IPsec-Verbindung zu aktivieren, muss ein IPsec-Zertifikat von einem Knoten als **ipsec-trust**-Zertifikat auf dem anderen Knoten festgelegt sein:

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

IPsec-Stammzertifikat vom Abonnenten herunterladen

Führen Sie die folgenden Schritte aus, um das IPsec-Stammzertifikat vom Subscriber-Knoten herunterzuladen:

1. Melden Sie sich bei der Seite "Betriebssystemverwaltung" des Subscriber-Knotens an.
2. Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**.
3. Öffnen Sie das IPsec-Stammzertifikat, und laden Sie es im Format **.pem** herunter:

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
  [
```

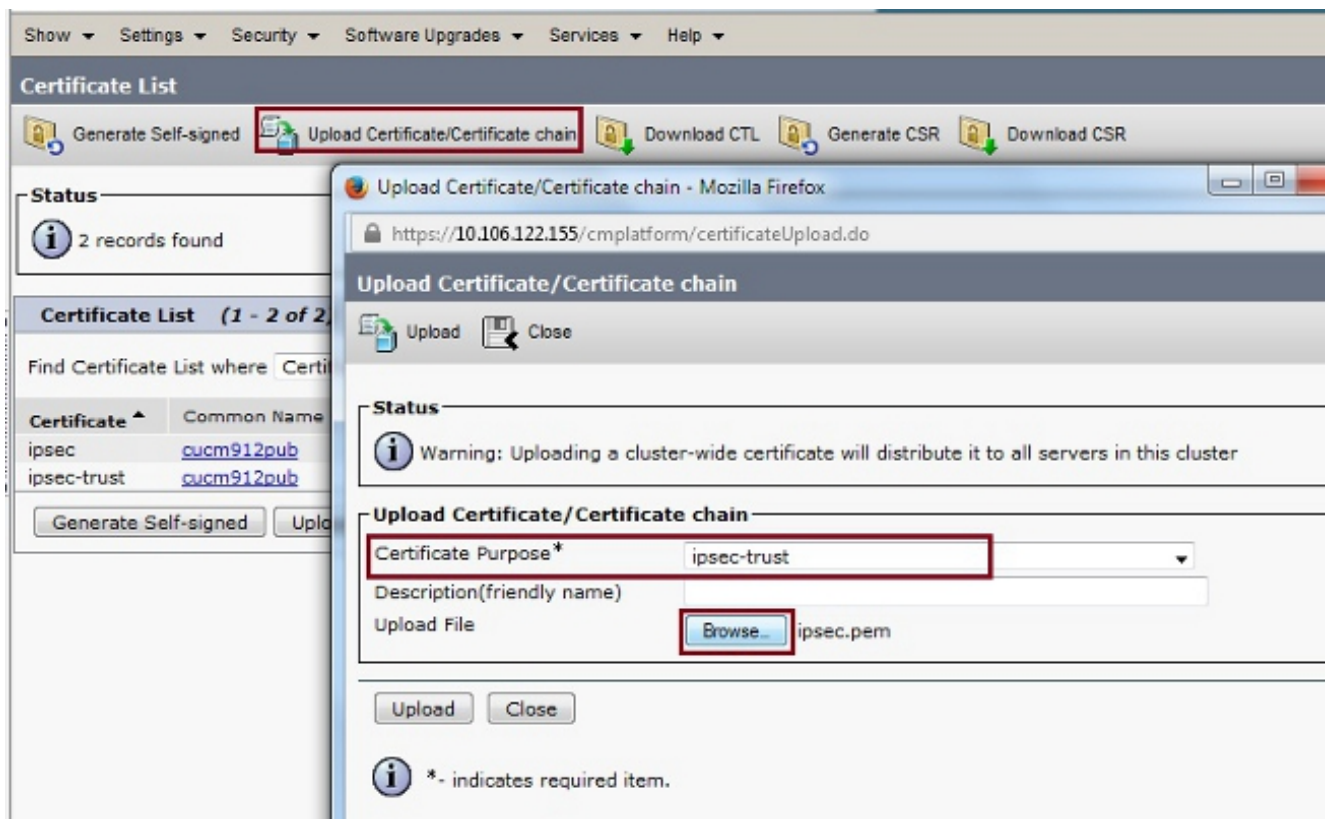
Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

IPsec-Stammzertifikat von Abonent auf Herausgeber hochladen

Führen Sie die folgenden Schritte aus, um das IPsec-Stammzertifikat vom Subscriber-Knoten auf den Publisher-Knoten hochzuladen:

1. Melden Sie sich auf der Seite "Betriebssystemverwaltung" des Verlegerknotens an.
2. Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**.
3. Klicken Sie auf **Zertifikat/Zertifikatskette hochladen**, und laden Sie das IPsec-Stammzertifikat des Abonnentenknotens als **ipsec-trust**-Zertifikat hoch:



4. Nachdem Sie das Zertifikat hochgeladen haben, überprüfen Sie, ob das IPsec-Stammzertifikat des Abonnentenknotens wie folgt angezeigt wird:

PUBLISHER

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	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Signed Certificate
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Anmerkung: Wenn Sie die IPsec-Verbindung zwischen mehreren Knoten in einem Cluster aktivieren müssen, müssen Sie auch die IPsec-Stammzertifikate für diese Knoten herunterladen und sie über dieselbe Prozedur auf den Publisher-Knoten hochladen.

Konfigurieren der IPsec-Richtlinie

Führen Sie die folgenden Schritte aus, um die IPsec-Richtlinie zu konfigurieren:

1. Melden Sie sich auf der Seite für die Betriebssystemverwaltung des Verlegers und der Subscriber-Knoten separat an.
2. Navigieren Sie zu **Sicherheit > IPSEC-Konfiguration**.
3. Verwenden Sie diese Informationen, um die IP-Adresse und die Zertifikatdetails zu konfigurieren:

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. The system is in non-FIPS Mode. The IPSEC Policy Details section is highlighted with a red box, showing the following configuration:

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

Below the IPSEC Policy Details, the Phase 1 DH Group and Phase 2 DH Group sections are visible, both with Phase One Life Time set to 3600 and Phase One DH set to Group 2. The IPSEC Policy Configuration section at the bottom has the Enable Policy checkbox selected. A Save button is at the bottom.

The screenshot shows the IPSEC Policy Configuration page for the SUBSCRIBER. The system is in non-FIPS Mode. The IPSEC Policy Details section is highlighted with a red box, showing the following configuration:

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

Below the IPSEC Policy Details, the Phase 1 DH Group and Phase 2 DH Group sections are visible, both with Phase One Life Time set to 3600 and Phase One DH set to Group 2. The IPSEC Policy Configuration section at the bottom has the Enable Policy checkbox selected. A Save button is at the bottom.

Überprüfung


Führen Sie die folgenden Schritte aus, um sicherzustellen, dass Ihre Konfiguration funktioniert und die IPsec-Verbindung zwischen den Knoten hergestellt ist:

1. Melden Sie sich bei der OS-Administration des CUCM-Servers an.
2. Navigieren Sie zu **Dienste > Ping**.
3. Geben Sie die IP-Adresse des Remote-Knotens an.
4. Aktivieren Sie das Kontrollkästchen **IPsec validieren**, und klicken Sie auf **Ping**.


Wenn die IPsec-Verbindung hergestellt wurde, wird eine Meldung wie diese angezeigt:

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

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Cisco Unified Communications Operating System Administration Guide, Version 8.6\(1\) - Einrichtung einer neuen IPsec-Richtlinie](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)