配置CUCM以實現節點之間的IPsec連線

目錄

簡介

本文檔介紹如何在集群內的Cisco Unified Communications Manager(CUCM)節點之間建立IPsec連線。

附註:預設情況下,CUCM節點之間的IPsec連線處於禁用狀態。

必要條件

需求

思科建議您瞭解CUCM。

採用元件

本檔案中的資訊是根據CUCM版本10.5(1)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

使用本節中介紹的資訊配置CUCM並在集群中的節點之間建立IPsec連線。

組態概觀

以下是此過程中涉及的步驟,以下各節詳述了每個步驟:

1. 檢驗節點之間的IPsec連線。

2. 檢查IPsec證書。

- 3. 從訂閱伺服器節點下載IPsec根證書。
- 4. 將IPsec根證書從訂閱伺服器節點上傳到發佈伺服器節點。

5. 配置IPsec策略。

檢驗IPsec連線

完成以下步驟,驗證節點之間的IPsec連線:

- 1. 登入到CUCM伺服器的作業系統(OS)管理頁面。
- 2. 導覽至Services > Ping。
- 3. 指定遠端節點IP地址。

4. 選中Validate IPsec覈取方塊並按一下Ping。 如果沒有IPsec連線,則會看到類似以下的結果:

| Ping Configuration | | |
|---|---|----|
| Ping | | |
| Status Status: Ready | | |
| Ping Settings | | |
| Hostname or IP Address* | 10.106.110.8 | |
| Ping Interval* | 1.0 | |
| Packet Size* | 56 | |
| Ping Iterations | 1 | |
| Validate IPSec | | |
| Ping Results | | |
| IPSec connection failed Reasons : a)No IPSec Policy on b)Invalid Certificates Reasons : a)No IPSec Policy on b)Invalid Certificates | 10.106.110.8 IPSec connection failed 10.106.110.8 | 44 |

檢查IPsec證書

完成以下步驟即可檢查IPsec憑證:

- 1. 登入到「作業系統管理」頁。
- 2. 導覽至Security > Certificate Management。

3. 搜尋IPsec證書(分別登入到發佈伺服器和訂閱伺服器節點)。

附註:通常無法從發佈伺服器節點檢視訂閱伺服器節點IPsec證書;但是,可以將所有訂閱伺 服器節點上的發佈伺服器節點IPsec證書視為IPsec-Trust證書。

要啟用IPsec連線,必須將來自一個節點的IPsec證書設定為另一個節點上的ipsec-trust證書:

| | | PUB | LISHER | | | |
|---------------------------|-----------------------|----------------------|--------------|-------------------|------------|---|
| Certificate List (1 | - 2 of 2) | | | | | Rows p |
| Find Certificate List whe | ere Certificate 👻 | begins with 🛛 🛨 ipse | ec (| Find Clear Filter | 4 = | |
| 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 | cuom912pub | 03/20/2019 | Trust Certificate |
| Certificate List (| 1 - 2 of 2) | SUB | SCRIBER | | | Rows |
| Find Certificate List wi | here Certificate + | begins with 👻 ip | 880 | Find Clear Filter | ÷ = | |
| Certificate * | Common Name | Туре | 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 | oucm912pub | cucm912pub | 03/20/2019 | Trust Certificate |
| Generate Self-signe | ed Upload Certificate | /Certificate chain | Generate CSR | | | |

從訂閱伺服器下載IPsec根證書

完成以下步驟,以便從訂閱伺服器節點下載IPsec根證書:

- 1. 登入到訂閱伺服器節點的OS管理頁。
- 2. 導覽至Security > Certificate Management。
- 3. 開啟IPsec根證書並以.pem格式下載:

| IPSE | C Root certificates | | | | | |
|-----------------------|---------------------|-------------------|--------------|-------------------|------------|---|
| Certificate List | (1 - 2 of 2) | SUB | SCRIBER | | | Row |
| Find Certificate List | where Certificate - | begins with 👻 ips | 960 | Find Clear Filter | 4 = | |
| 1 | Common Name | Туре | Distribution | Essued By | Expiration | Description |
| Certificate | | | | | | |
| / Certificate * | cucm10sub | Self-signed | cucm10sub | cucm10sub | 12/14/2019 | Self-signed certificate generated by system |

| 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 fab7adb41068344a97a4f9b234180ef8b232f75194ae7d987b0203010001 |
| Extensions: 3 present |
| Regenerate Generate CSR Download .PEM File Download .DER File |
| Close |

將IPsec根證書從訂閱伺服器上載到發佈伺服器

完成以下步驟,將IPsec根證書從訂閱伺服器節點上傳到發佈伺服器節點:

- 1. 登入到發佈伺服器節點的「作業系統管理」頁。
- 2. 導覽至Security > Certificate Management。
- 3. 點選**Upload Certificate/Certificate chain**,然後上傳使用者節點IPsec根證書作為**ipsec-trust**證 書:

| Show - Settings - Security - | Software Upgrades 👻 Services 👻 Help 👻 | |
|-----------------------------------|---|--|
| Certificate List | | |
| Generate Self-signed | load Certificate/Certificate chain 🔋 Download CTL 🧃 Generate CSR 🔋 Download CSR | |
| Status | Upload Certificate/Certificate chain - Mozilla Firefox | |
| i 2 records found | https://10.106.122.155/cmplatform/certificateUpload.do | |
| | Upload Certificate/Certificate chain | |
| Certificate List (1 - 2 of 2, | 🔤 Upload 🖳 Close | |
| Find Certificate List where Certi | | |
| Certificate Common Name | Status Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster | |
| Concrete Self-signed Uple | _ Upload Certificate/Certificate chain | |
| Generate Sen-signed Opio | Certificate Purpose* ipsec-trust 🗸 | |
| | Description(friendly name) Upload File Browse_ ipsec.pem | |
| | Upload Close | |
| | (i) *- indicates required item. | |

4. 上傳憑證後,確認訂閱者節點IPsec根憑證是否按以下方式顯示:

| Certificate List (| (1 - 3 of 3) | | | | | Rows |
|-------------------------|--------------------|--------------------|--------------|-------------------|------------|---|
| Find Certificate List w | here Certificate + | begins with 🛛 🛨 ip | 98C | Find Clear Filter | 4 = | |
| Certificate * | Common Name | Туре | Distribution | Issued By | Expiration | Description |
| psec | 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 |
| insec-trust | cucm912pub | Self-signed | cucm912pub | cuam912pub | 03/20/2019 | Trust Certificate |

附註:如果需要啟用群集中多個節點之間的IPsec連線,則必須同時下載這些節點的IPsec根證 書,並通過相同過程將其上傳到Publisher節點。

配置IPsec策略

完成以下步驟以配置IPsec策略:

- 1. 分別登入到發佈伺服器和訂閱伺服器節點的「作業系統管理」頁。
- 2. 導航到Security > IPSEC Configuration。
- 3. 使用以下資訊設定IP和憑證詳細資訊:
 - * * * * *

PUBLISHER : 10.106.122.155 & cucm912pub.pem SUBSCRIBER: 10.106.122.15 & cucm10sub.pem

| Solve * Setting * Security * Settioner libration * Services * Help * IDEC Policy Configuration RUDITISETER ************************************ | cisco U For Cisco U | Inified Operating System Adr Unified Communications Solutions | ninistratio | cisco For Cisco U | Unified Operating System Adminis Unified Communications Solutions | stration |
|--|--------------------------------|--|-------------|----------------------------------|--|----------|
| PDSCL Policy Configuration PUBLISHER Image: Sore IPSCL Policy Configuration SUBSCRIBES Image: Sore Image: Sore Image: Sore Image: Sore Image: Sore Image: Sore Image: Sore Image: Sore Image: Sore Image: Sore | Show + Satings + Sa | curty • Software Upgrades • Services • Het | p 🛩 | Show + Settings + Se | county 💌 Software Upgrades 👻 Services 💌 Help 💌 | |
| The system is in non-FTPS Mode IPSEC Policy Details Policy Mane ¹ Tos.b Authentication Nethod* Cotinate Very Mane ¹ Cotinate Cotinate Cotinate Cotinate Very Mane ¹ Cotinate Phase Cotinate Phase Cotinate | IPSEC Policy Configur | ation PUBLISHER | | IPSEC Policy Configur | ration SUBSCRIBER | |
| The system is in non-FIPS Mode IPSEC Policy Details Policy Graup Name [®] ToSubscriper Pathenciabio Nethod Continuote Preshered Key Pare Type [®] Confinence unit Different unit Different Confination Mathed [®] Confinition Mathed [®] control Different control Different Confination Mathed [®] Confination Mathed [®] Confination Mathed [®] Preshered Key Descination Port [®] Mary Descination Port [®] Unins.122.159 Douce Address [®] Ini.Ini.122.159 Source Address [®] Ini.Ini.122.159 Source Address [®] Ini.Ini.122.159 Source Address [®] Arry Rodia Port [®] Mary Descination Port [®] Arry Descination Port [®] Arry | Save | | | Bave | | |
| IPSCC Policy Details Policy Group Name* ToSub Authentication Rehod* Certificate Method* Certificate Method* Certificate Name* Preshared Key Partice Rehod* Certificate Name* Source Port* AnY Source Port* Source Port* Note* Transport Name* Noteof* TCP Encryption Algorithm* Source Port* Assorthm* Source Port* Nater Name* Phase 1 DH Group | The system is in non- | FIPS Mode | | The system is in non- | -F1PS Node | |
| Policy Group Name* ToSubscriber Policy Name* ToSubscriber Policy Name* ToSubscriber Auchentization Method* Contribute Prechared Key | IPSEC Policy Details | | | IPSEC Policy Details | | |
| Policy Name* ToSub Authentication Method* Cortificate Prechared Key Perform Prechared Key Perform Destribution Mathod* Cortificate • Prechared Key Paul- Destribution Mathod* Cortificate • Cortificate Name* cucm10sub.pem • Destribution Mathod* Cucm10sub.pem • Destribution Mathod* Iointo.122.155 • Destribution Port* Axry Source Address* 10.106.122.159 Destribution Address* Iointo.122.159 • Destribution Address* 10.106.122.159 Destribution Address* Iointo.122.159 • Destribution Address* 10.106.122.159 Source Address* Iointo.122.159 • Destribution Address* 10.106.122.159 Source Address* Transport • Part Part Part Source Address* Transport • Part | Policy Group Name [®] | ToSubscriber | | Policy Group Name* | ToPublisher | |
| Authentication Nethod* Cortificate Prechared Key Parer Typa* Ciffication Kames* Curtification Kames* Curtification Kames* Curtification Kames* Curtification Kames* Curtification Kames* Construction Address* 10.106.122.135 Destination Port* Auv Source Port* Avy Source Port* Auv Node* Transport Remota Port* 500 Protocol* TCP Encrybion Algorithm* Solication Fort* Autor Nation* Source Port* Auv Node* Transport Nation* Source Port* Phase One Life Time* Source Port* Phase Cort Ibit Time* Source Port* Phase Cort Ibit Time* Source Port* Phase Too Life Time* Source Port* Phase Too Life Time* Source Port* Phase Too Life Time* <td>Policy Name*</td> <td>TeSub</td> <td></td> <td>Policy Name*</td> <td>ToPublisher</td> <td></td> | Policy Name* | TeSub | | Policy Name* | ToPublisher | |
| Preshared Key | Authentication Method* | Certificate | | Authentication Method* | Certificate 👻 | |
| Peer Type* Different Curtification Address* Curtification Address* In 106.122.105 Destination Address* In 106.122.105 Destination Address* In 106.122.130 Destination Address* In 106.122.130 Destination Address* In 106.122.130 Destination Accress* In 106.120.120.120 Protocol* The Accretion Accress* Destination Accress* In 106.120.120.120.120 Phase 1 Def Group Phase 1 Def Group | Preshared Key | | | Preshared Key | | |
| Contification Name* cuccm10sub.pem Contribution Port* Num Destination Address* 10.106.122.155 Destination Address* 10.106.122.155 Source Address* 10.106.122.153 Source Address* 10.106.122.153 Source Address* 10.106.122.153 Source Address* 10.106.122.159 Destination Fort* Anv Mode* Transport Remute Part* 500 Protocol* TCP Protocol* TCP Protocol* TCP Encryption Algorithm* SDES Abgorithm* SHA1 ENA Algorithm* SHA2 Phase 1 | Peer Type* | Different | - | Peter Types* | Different - | |
| Destination Port [®] 10.106.122.159 Destination Port [®] ANY Source Address [®] 10.106.122.153 Source Port [®] ANY Source Port [®] Transport Remate Port [®] 500 Protocol [®] TCP Encryption Algorithm [®] SHA1 Source Port [®] SHA1 Sthat Sthat Sthat Sthat </td <td>Certificate Name*</td> <td>cucm10sub.pem</td> <td></td> <td>Certificate Name³</td> <td>cucm912pub.pem</td> <td></td> | Certificate Name* | cucm10sub.pem | | Certificate Name ³ | cucm912pub.pem | |
| Destination Port* ANY Source Address* 10.106.122.135 Source Address* 10.106.122.139 Source Port* ANY Node* Transport Remote Port* ANY Node* Transport Remote Port* Source Address* 10.106.122.139 Source Address* Source Port* ANY Node* Transport Remote Port* Source Ref* Aux Transport Protocol* TCP Encryption Algorithm* SHA1 etsh Algorithm* SHA2 < | Destination Address* | 10.106.122.159 | | Desbnation Address" | 10.105.122.155 | |
| Source Address* 10.100.122.133 Source Fort* ANY Node* Transport Remain Part* 500 Protocol* TCP Protocol* TCP Protocol* TCP Encryption Algorithm* SHA1 ESP Algorithm* SHA1 Phase 1 DH Group Phase 0 ne Life Time* Phase 0 ne Life Time* 9600 Phase 1 DH Group Phase 1 DH Group 2 Phase 1 DH Group Phase 1 DH Group 2 Phase 1 DH Group Phase 1 DH Group 2 | Destination Port* | ANY | | Destination Port* | ANY | |
| Source Port* ANY Mode* Transport Remate Port* 500 Protocol* TCP Encrybion Algorithm* SHA1 Source Port* ARS 128 Phase 1 DH Group Phase Cross Port* Phase Cross Port* Phase Cross Port* ARS 128 Phase Cross Port* Phase Cr | Source Address* | 10.106.122.155 | | Source Address* | 10.105.122.159 | |
| Mode* Transport Ramatia Port* 500 Protocol* TCP Encrybion Algorithm* 3DES Hish Algorithm* SHA1 * Hish Algorithm* AES 128 | Source Port* | ANY | | Source Port* | ANY | |
| Remote Part ⁴ 500 Protocol ⁴ TCP Encryption Algorithm ⁴ 3DES Encryption Algorithm ⁴ 5HA1 Encryption Algorithm ⁴ 5HA1 ENC STAR * Phase 1 DH Group Phase One Life Time ⁴ S600 Phase One DH ⁴ Group 2 Phase Two Life Time ⁴ S600 Phase Two DH ⁴ Croup 2 Croup 2 Croup 2 Croup 2 Construction Croup 2 <pcroup 2<="" p=""> Croup 2<td>Mode*</td><td>Transport</td><td>-</td><td>Node*</td><td>Transport -</td><td></td></pcroup> | Mode* | Transport | - | Node* | Transport - | |
| Protocol* TCP Encryption Algorithm* SDES SHA1 AES 128 Phase 1 DH Group Phase One Life Time* S600 Phase One Life Time* S600 Phase One Life Time* S600 Phase Two DH* Group 2 Croup 2 Croup 2 Croup 2 Comparison Croup 2 Comparison Croup 2 Croup 2 Comparison Croup 2 Comparison Croup 2 Comparison < | Remote Port * | 500 | | Remote Part ^a | 500 | |
| Encryption Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES Hash Algorithm* 3DES | Protocol * | TCP | | Protocol* | TCP . |] |
| Hash Algorithm* SHA1 ARS 128 Phase 1 DH Group Phase One DH * Se00 Phase One DH * Group 2 Phase Two DH * Group 2 Phase Tw | Encryption Algorithm* | 3069 | | Encryption Algorithm* | 3DES 🗸 | |
| ESP Algorithm* AES 128 Phase 1 DH Group Phase One DH* Phase One DH* Group 2 Phase Two DH* Group 2 Phase Two DH* Group 2 Phase Two DH* Group 2 Phase Two DH* Group 2 Phase Two DH* Group 2 Phase Two DH* Group 2 Phase Two DH* Group 2 IPSEC Policy Configuration IPSEC Policy Configuration IPSEC Policy Configuration IPSEC Policy Configuration | Hash Algorithm* | SHA1 | • | Hash Algorithm* | SHA1 - | |
| Phase 1 DH Group Phase One Life Time* 3600 Phase One DH* Group 2 • Phase Two DH & Group 2 • | ESP Algorithm* | AES 128 | • | ESP Algorithm * | AES 128 - | |
| Phase One Life Time* 3600 Phase One Dif* Group 2 Phase Two Dife Time* 3600 Time* 3600 3600 3600 3600 3600 3600 3600 3600 3600 3600 3600 | Phase 1 DH Group- | | | -Phase 1 DH Group- | | _ |
| Phase One DH* Group 2 Phase One DH* Group 2 Phase Two DH Group Phase Two DH Group 2 Phase Two DH* Group 2 Phase Phase Policy Phase Phase Polic | Phase One Life Time* 3 | 1600 | | Phase One Life Time ⁴ | 3600 | |
| Phase 2 DH Group Phase Two Life Time* 3600 Phase Two DH* Group 2 Ph | Phase One DH 6 | Group 2 | - | Phase One DH* | Group 2 - | |
| Phase Two Life Time* 3600 Phase Two DH* Croup 2 | Phase 2 DH Group- | | | -Phase 2 DH Group- | | |
| Phase Two DH * Group 2 IPSEC Policy Configuration IPSEC Policy | Phase Two Life Time* 3 | 1600 | | Phase Two Life Time # | 3600 | 1 |
| IPSEC Policy Configuration IPSEC Policy Configuration Image: Second Se | Phase Two DH * | Group 2 | • | Phase Two DH* | Group 2 + | |
| Enable Policy | IPSEC Policy Configur | ation | | IPSEC Policy Configu | ration | |
| | Enable Policy | | | Enable Policy | | |
| | | | | | | |
| Save | Save | | | Save | | |

驗證

完成以下步驟,驗證您的配置是否有效,以及節點之間是否建立了IPsec連線:

1. 登入到CUCM伺服器的作業系統管理。

2. 導覽至Services > Ping。

3. 指定遠端節點IP地址。

4. 選中Validate IPsec覈取方塊,然後按一下Ping。 如果已建立IPsec連線,則您會看到類似以下的訊息:

| Show - Settings - Secu | rity - Software Upgrades - Services - Help - | | | | |
|--|--|--|--|--|--|
| Ping Configuration | | | | | |
| Ping | | | | | |
| Status | | | | | |
| i Status: Ready | | | | | |
| Ping Settings | | | | | |
| Hostname or IP Address* | 10.106.122.159 | | | | |
| Ping Interval* | 1.0 | | | | |
| Packet Size* | 56 | | | | |
| Ping Iterations | 1 * | | | | |
| Validate IPSec | | | | | |
| - Ping Results | | | | | |
| Successfully validated IPS connection to 10.106.122. | ec connection to 10.106.122.159Successfully validated IPSec 159 | | | | |
| | | | | | |
| | | | | | |
| Ping | | | | | |

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 思科統一通訊作業系統管理指南8.6(1)版 設定新的IPsec策略
- 技術支援與文件 Cisco Systems