ノード間の IPSec 用 CUCM の設定

内容

<u>概要</u> <u>前提条件</u> <u>要件</u> 使用するコンポーネント 設定 設定の概要 IPSec接続の確認 IPsec証明書の確認 サブスクライバからのIPsecルート証明書のダウンロード サブスクライバからパブリッシャへのIPsecルート証明書のアップロード IPSecポリシーの設定 確認 トラブルシュート 関連情報

概要

このドキュメントでは、クラスタ内のCisco Unified Communications Manager(CUCM)ノード間で IPSec接続を確立する方法について説明します。

注:デフォルトでは、CUCMノード間のIPsec接続は無効になっています。

前提条件

要件

CUCMに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、CUCMバージョン10.5(1)に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

設定

このセクションで説明されている情報を使用して、CUCMを設定し、クラスタ内のノード間で IPSec接続を確立します。

設定の概要

次に、この手順に含まれる手順を示します。各手順については、以降のセクションで詳しく説明 します。

- 1. ノード間のIPSec接続を確認します。
- 2. IPSec証明書を確認します。
- 3. サブスクライバノードからIPsecルート証明書をダウンロードします。
- 4. サブスクライバノードからパブリッシャノードにIPsecルート証明書をアップロードします。
- 5. IPsecポリシーを設定します。

IPSec接続の確認

- ノード間のIPSec接続を確認するには、次の手順を実行します。
 - 1. CUCMサーバの[Operating System (OS) Administration]ページにログインします。
 - 2. [Services] > [Ping] に移動します。
 - 3. リモートノードのIPアドレスを指定します。

4. [Validate IPsec] チェックボックスをオンにして、[Ping] をクリックします。 IPSec接続がない場合は、次のような結果が表示されます。

Ping Configuration					
Ping					
- Status					
G Status Boady					
Jacus: Ready					
Ping Settings					
Hostname or IP Address*	10.106.110.8				
Ping Interval*	1.0				
Packet Size* 56					
Ping Iterations					
Validate IPSec					
Ping Results					
IPSec connection failed					
Reasons :	10 105 110 8				
b)Invalid Certificates IPSec connection failed					
Reasons : a)No IPSec Policy on	10 105 110 8				
b)Invalid Certificates	,				

IPsec証明書の確認

IPSec証明書を確認するには、次の手順を実行します。

- 1. [OS Administration]ページにログインします。
- 2. [Security] > [Certificate Management] に移動します。
- 3. IPsec証明書を検索します(パブリッシャノードとサブスクライバノードに別々にログイン します)。

注:通常、サブスクライバノードのIPsec証明書はパブリッシャノードからは表示できません。ただし、パブリッシャノードのIPsec証明書は、すべてのサブスクライバノードでIPsec-Trust証明書として表示されます。

IPSec接続を有効にするには、一方のノードのIPSec証明書を他方のノードの**ipsec-trust**証明書として設定する必要があります。

		PUE	BLISHER			
Certificate List	(1 - 2 of 2)					Rows p
Find Certificate List w	here Certificate 👻	begins with 🛛 🛨 ips	ec	Find Clear Filter	4 =	
Certificate *	Common Name	Туре	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
Certificate List	(1 - 2 of 2)	SUB	SCRIBER			Rows
Find Certificate List	where Certificate	begins with 🐳 ip	1880	Find Clear Filter	÷ =	
Certificate *	Common Name	Туре	Distribution	Issued By	Expiration	Description
ipsec	cucm10sub	Self-signed	cuem10sub	cucm10sub	12/14/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	oucm912pub	cucm912pub	03/20/2019	Trust Certificate
Generate Self-sig	ned Upload Certificate	e/Certificate chain	Generate CSR			

サブスクライバからのIPsecルート証明書のダウンロード

サブスクライバノードからIPsecルート証明書をダウンロードするには、次の手順を実行します。

- 1. サブスクライバノードの[OS Administration]ページにログインします。
- 2. [Security] > [Certificate Management] に移動します。
- 3. IPSecルート証明書を開き、.pem形式でダウンロードします。

IPSE	C ROOT CERTIFICATES	SUR	SCRIPER			
Certificate List	(1 - 2 of 2)	506	SCRIDER			Roy
Find Certificate List	where Certificate -	begins with 👻 ip	98C	Find Clear Filter	÷ =	
Certificate	Common Name	Тура	Distribution	Essued By	Expiration	Description
psec	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Self-signed certificate generated by system
	oucro912pulp	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Certificate Details for Regenerate 💽 Ge	cucm10sub, ipsec
Status Status: Ready	
Certificate Settings-	
File Name Certificate Purpose Certificate Type Certificate Group	ipsec.pem ipsec certs product-cpi
Certificate File Data	
Version: V3 Serial Number: 6B71 SignatureAlgorithm: Issuer Name: L=blr, Validity From: Mon D To: Sat Dec 1 Subject Name: L=blr Key: RSA (1.2.840.1 Key value:	952138766EF415EFE831AEB5F943 SHA1withRSA (1.2.840.113549.1.1.5) ST=karnataka, CN=cucm10sub, OU=cucm, O=cisco, C=IN ec 15 23:26:27 IST 2014 14 23:26:26 IST 2019 , ST=karnataka, CN=cucm10sub, OU=cucm, O=cisco, C=IN 13549.1.1.1)
30818902818100a376 4b695016352b98cc72b 7b6ad7e5069d732468 feb7adb41068344a97a Extensions: 3 presen	b6ad/825abe3069a421538c851a32d815321de/7/91985f99f2f9a 26461cc629d0d2b35fc774d20fa13ae6c476164b7ccca82eb73034 f501ba53a018f9bbe422f6c76a4e4023fbad9bcf2f7d122cbe681375 a4f9b224180c6f8b223f75194ec7d987b0203010001 t
Regenerate Gen	erate CSR Download .PEM File Download .DER File
Close	

サブスクライバからパブリッシャへのIPsecルート証明書のアップロード

サブスクライバノードからパブリッシャノードにIPsecルート証明書をアップロードするには、次 の手順を実行します。

- 1. パブリッシャノードの[OS Administration]ページにログインします。
- 2. [Security] > [Certificate Management] に移動します。
- 3. [Upload Certificate/Certificate chain] をクリックし、サブスクライバノードIPsecルート証明 書をipsec-trust証明書としてアップロードします。

Show - Settings - Security -	Software Upgrades 👻 Services 👻 Help 👻
Certificate List	
Generate Self-signed	pad 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 The Close
Find Certificate List where Certi	
Certificate Common Name ipsec <u>cucm912pub</u> ipsec-trust <u>cucm912pub</u>	Status Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster
Generate Self-signed Uplo	Upload Certificate/Certificate chain
	Certificate Purpose* ipsec-trust
	Upload File Browse_ ipsec.pem
	Upload Close
	i *- indicates required item.

4. 証明書をアップロードした後、サブスクライバノードIPsecルート証明書が次のように表示 されることを確認します。

ind Certificate List	where Certificate -	begins with 🛛 🛨 ip	986	Find Clear Filter	4 =	
Certificate *	Common Name	Туре	Distribution	Issued By	Expiration	Description
sec	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Self-signed certificate generated by system
sec-trust	cucm10sub	Self-signed	cucrn10sub	cucm10sub	12/14/2019	Signed Certificate
osec-trust	cucm912pub	Self-signed	cuom912pub	cucm912pub	03/20/2019	Trust Certificate

注:クラスタ内の複数のノード間でIPsec接続を有効にする必要がある場合は、これらのノードのIPsecルート証明書もダウンロードし、同じ手順でパブリッシャノードにアップロードする必要があります。

IPSecポリシーの設定

IPSecポリシーを設定するには、次の手順を実行します。

- 1. パブリッシャとサブスクライバノードのOS Administrationページに個別にログインします。
- 2. [Security] > [IPSEC Configuration] に移動します。
- 3. IPと証明書の詳細を設定するには、次の情報を使用します。

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

* * * * *	*	*	*	*	*
-----------	---	---	---	---	---

SEC Policy Configur			and a second of function of the second of th	
	ation PUBLISHER	IPSEC Policy Configu	aration SUBSCRIBER	
Save		Bave		
he system is in non-	FIPS Mode	The system is in nor	n-FIPS Node	_
PSEC Policy Details-		IPSEC Policy Details		
olicy Group Name [®]	ToSubscriber	Policy Group Name*	ToPublisher	
olicy Name*	TaSub	Policy Name*	ToPublisher	
uthentication Hethod*	* Certificate	Authentication Method	* Certificate v	
rechared Key		Preshared Key		
eer Type*	Different	Pasar Types	Different	1
Certificate Name*	cucm10sub.pem	Certificate Name*	cuam912pub.pem	
Sestination Address *	10.106.122.159	Destination Accress*	10.105.122.155	٦.
Sestination Port*	ANY	Destination Fort*	ANY	
Source Address*	10,106,122,155	Source Address*	10.105.122.159	-
Source Port*	ANY	Source Port ⁴	ANY	-
lode*	Transport	Mode*	Transport	
tempte Port*	500	Remote Part ^a	500	
* loool	TOP	Protocol*	TCP .	
noryption Algorithm*	3DES	Encryption Algorithm*	3DE5 v	1
lash Algorithm*	SHA1	Hash Algorithm*	SHA1 -	1
SP Algorithm*	A65 128	ESP Algorithm *	AES 128	
hase 1 DH Group-		-Phase 1 DH Group-		
have One Life Time* 3	600	Phase One Life Time ⁴	3600	
hase One DH 4	Sroup 2	Phase One DH*	Group 2	
hase 2 DH Group-		Phase 2 DH Group		
hase Two Life Time* 3	600	Phase Two Life Time [®]	3600	
hase Two DH *	Group 2	Phase Two DH*	Group 2 •	
PSEC Policy Configur	ation	IPSEC Policy Configu Enable Policy	uration	

確認

次の手順を実行して、設定が機能していること、およびノード間のIPSec接続が確立されている ことを確認します。

- 1. CUCMサーバのOS Administrationにログインします。
- 2. [Services] > [Ping] に移動します。
- 3. リモートノードのIPアドレスを指定します。

4. [Validate IPsec] チェックボックスをオンにして、[Ping] をクリックします。 IPSec接続が確立されると、次のようなメッセージが表示されます。

Show - Settings - Secu	rity ▼ Software Upgrades ▼ Services ▼ Help ▼
Ping Configuration	
Ping 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	

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ^Cisco Unified Communications Operating System Administration Guide, Release 8.6(1) <u>Set Up a New IPsec Policy</u>
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>