# CUCM和VCS之間的安全SIP中繼配置示例

# 目錄

 簡介

 必要條件

 需求

 採用元件

 設定

 網路圖表

 獲取VCS證書

 生成和上傳VCS自簽名證書

 將自簽名證書從CUCM伺服器新增到VCS伺服器

 將證書從VCS伺服器上傳到CUCM伺服器

 SIP連線

 驗證

 疑難排解

 相關資訊

# 簡介

本文說明如何在Cisco Unified Communications Manager(CUCM)和Cisco TelePresence Video Communication Server(VCS)之間建立安全會話發起協定(SIP)連線。

CUCM和VCS緊密整合。由於影片終端可以在CUCM或VCS上註冊,因此裝置之間必須存在SIP中 繼。

# 必要條件

### 需求

思科建議您瞭解以下主題:

- 思科整合通訊管理員
- Cisco TelePresence視訊通訊伺服器
- 憑證

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。此示例使用Cisco VCS軟體版本X7.2.2和CUCM版本

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

確保證書有效,將證書新增到CUCM和VCS伺服器,以便它們信任彼此的證書,然後建立SIP中繼 。

### 網路圖表



### 獲取VCS證書

預設情況下,所有VCS系統都附帶臨時證書。在管理頁面上,導航到Maintenance > Certificate management > Server certificate。按一下「Show server certificate」,便會開啟一個新視窗,其中 包含憑證的原始資料:

Server certificate					
Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the Clustering help page.					
Server certificate data					
Server certificate	PEM File Show server certificate				
Currently loaded certificate expires on	Sep 30 2014				
Reset to default server certificate					

#### 以下是原始憑證資料範例:

#### ----BEGIN CERTIFICATE-----

MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmjFDMEEGA1UECgw6VGVt cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1 Njk5NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw LTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wHhcN MTMwOTMwMDcxNzIwWhcNMTQwOTMwMDcxNzIwWjCBmjFDMEEGA1UECgw6VGVtcG9y YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5 NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5 YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wgZ8wDQYJ KoZIhvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPipL0I/ L21fyyjoO5qv9lzDCgy7PFZPxkD1d/DNLIgp1jjUqdfFV+64r80kESwB0+4DFlut tWZLQ1uKzzdsmvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVl0gVFCEV4c7ZvAV4S E8m9YNY9AgMBAAGjczBxMAkGA1UdEwQCMAAwJAYJYIZIAYb4QgENBBcWFVRlbXBv cmFyeSBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqAjORhzQqRCHba+nEw HwYDVR0jBBgwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD gYEAZklIMSfi49p1jIYqYdOAIjOiashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7 1Zc3zT16WL6hsj+90GASI/TGthQ2n7yUWP16CevopbJe1iA= -----END CERTIFICATE-----

您可以解碼證書,並檢視證書資料,方法是在本地PC上使用OpenSSL,或使用線上證書解碼器(例 如<u>SSL Shopper)</u>:

Certificate Information: Common Name: disco Organization: Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b Organization Unit: Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b Valid From: September 30, 2013 Valid To: September 30, 2014 Issuer: disco, Temporary Certificate 587745f0-29a0-11e3-a518-005056995b4b Key Size: 1024 bit Serial Number: 1 (0x1)

### 生成和上傳VCS自簽名證書

由於每個VCS伺服器都有一個具有相同公用名稱的證書,因此需要將新證書放在伺服器上。您可以 選擇使用自簽名的憑證或由憑證授權單位(CA)簽名的憑證。 有關此過程的詳細資訊,請參閱<u>Cisco</u> <u>TelePresence Certificate Creation and Use with Cisco VCS Deployment Guide</u>。

以下過程介紹了如何使用VCS本身生成自簽名證書,然後上傳該證書:

1. 以root使用者身份登入到VCS,啟動OpenSSL並生成私鑰:

2. 使用此私鑰可產生憑證簽署請求(CSR):

OpenSSL> req -new -key privatekey.pem -out certcsr.pem You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.

```
Country Name (2 letter code) [AU]:BE

State or Province Name (full name) [Some-State]:Vlaams-Brabant

Locality Name (eg, city) []:Diegem

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco

Organizational Unit Name (eg, section) []:TAC

Common Name (e.g. server FQDN or YOUR name) []:radius.anatomy.com

Email Address []:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:
```

#### OpenSSL> exit 3. 生成自簽名證書:

~ # openssl x509 -req -days 360 -in certcsr.pem -signkey privatekey.pem -out vcscert.pem
Signature ok
subject=/C=BE/ST=Vlaams-Brabant/L=Diegem/O=Cisco/OU=TAC/CN=radius.anatomy.com
Getting Private key
~ #

4. 確認證書現在可用:

~ # ls -ltr \*.pem

-rw-r--r-- 1 root root 891 Nov 1 09:23 privatekey.pem
-rw-r--r-- 1 root root 664 Nov 1 09:26 certcsr.pem
-rw-r--r-- 1 root root 879 Nov 1 09:40 vcscert.pem

5. 使用<u>WinSCP</u>下載憑證,並將其上傳到網頁上,以便VCS可以使用憑證;您需要私鑰和產生的 憑證:

Server certificate						
Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the Clustering help page.						
Server certificate data						
Server certificate	PEM File Show server certificate					
Currently loaded certificate expires on	Sep 30 2014					
Reset to default server certificate						
Certificate signing request (CSR)						
Certificate request	There is no certificate signing request in progress					
Generate CSR						
Upload new certificate						
Select the server private key file	"C1privatekey.pem" Choose ()					
Select the server certificate file	"C:tvcscert.pem" (i)					
Upload server certificate data						

6. 對所有VCS伺服器重複此過程。

### 將自簽名證書從CUCM伺服器新增到VCS伺服器

新增來自CUCM伺服器的證書,以便VCS信任它們。在本示例中,您使用的是來自CUCM的標準自 簽名證書;CUCM會在安裝期間生成自簽名證書,因此您無需像在VCS上那樣建立這些證書。

以下過程介紹了如何從CUCM伺服器向VCS伺服器新增自簽名證書:

1. 從CUCM下載CallManager.pem證書。登入到「作業系統管理」頁面,導航到**安全 > 證書管理** ,然後選擇並下載自簽名的CallManager.pem證書:

Certificate Configuration
Regenerate Download Generate CSR Download CSR
- Status
i Status: Ready
- Certificate Settings
File Name CallManager.pem
Certificate Name CallManager
Certificate Type certs
Certificate Group product-cm
Description Self-signed certificate generated by system
- Cartificata Filo Data
Version: V3 Serial Number: 136322906787293084267780831508134358913
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=Peg3, ST=Diegem, CN=MFCl1Pub, OU=TAC, O=Cisco, C=BE
Validity From: Wed Aug 01 12:28:35 CEST 2012
Subject Name: L=Peg3, ST=Diegem, CN=MFCl1Pub, OU=TAC, O=Cisco, C=BE
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100e608e60cbd1a9984097e9c57479346363e535d002825be7445c00abtacd806act0a2c1381c01cc6ab06b4640 h48dd54c883c3004e4dh9f44e40f27bc2147de4a1a661b19dc077ca7ae8a0f8c4f608696d7cf7ba97273f6440ea1d8bc6973253
e6cad651f33d19d91365f1c8d6257a93f8ef3ed1a28170d2088a848e7d7edc8110203010001
Extensions: 3 present
Extension: Keyllsage (OID 2 5 29 15)
Critical: false
Usages: digitalSignature, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign,
Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
Critical: false
Usage olds: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
Regenerate Download Generate CSR Download CSR

2. 將此證書新增為VCS上的受信任CA證書。在VCS上,導航到Maintenance > Certificate management > Trusted CA certificate,然後選擇Show CA certificate:

Trusted CA certificate					
Level Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the Clustering help page					
Upload					
Select the file containing trusted CA certificates	Choose				
CA certificate	PEM File Show CA certificate				
Upload CA certificate Reset to default CA certificate					

此時會開啟一個新視窗,顯示當前信任的所有證書。

3. 將所有當前受信任的證書複製到文本檔案中。在文本編輯器中開啟CallManager.pem檔案,複 製其內容,並將該內容新增到當前受信任證書之後的同一文本檔案的底部:

CallManagerPub
=================
BEGIN CERTIFICATE
MIICmDCCAgGgAwIBAgIQZo7WOmjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
${\tt MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ21zY28xDDAKBgNVBAsTA1RBQzERMA8G}$
$\verb A1UEAxMITUZDbDFQdWIxDzANBgNVBAgTBkRpZWdlbTENMAsGA1UEBxMEUGVnMzAe   \\$
${\tt Fw0xMjA4MDExMD14MzVaFw0xNzA3MzExMD14MzRaMF4xCzAJBgNVBAYTAkJFMQ4w}$
DAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMREwDwYDVQQDEwhNRkNsMVB1YjEP
${\tt MA0GA1UECBMGRG11Z2VtMQ0wCwYDVQQHEwRQZWczMIGfMA0GCSqGS1b3DQEBAQUA}$
A4GNADCBiQKBgQDmCOYMvRqZhAl+nFdHk0Y2PlNdACglvnRFwAq/rNgGrPCiwTgc
$0 \verb"cxqsGtGQLSN1UyIPDAE5NufR0QPJ7whR95KGmYbGdwHfKeuig+MT2CGltfPe6ly"$
c/ZEDqHYvGlzJT5srWUfM9GdkTZfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
$\verb"o1cwVTALBgNVHQ8EBAMCArwwJwYDVR01BCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC"$
BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX606BAnLCalbKEn6YV7BpkQwDQYJKoZI
hvc NAQEFBQADgYEAkEGDdRdMOtX4ClhEatQE3ptT6L6RRAyP8oDd3dIGEOYWhA2H
Aqrw77loieva297AwgcKbPxnd5lZ/aBJxvmF8TIiOSkjy+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRr1IRzAJDeygLIq+wc=
END CERTIFICATE

如果CUCM集群中有多個伺服器,請在此處新增所有伺服器。

4. 將檔案另存為CATrust.pem,然後按一下Upload CA certificate,以便將檔案上傳回VCS:

Note: This VCS is part of a cluster but is not the configuration master. Any configuration changes made on this VCS may be lost. More information can be found on the Clustering help page.						
"CACATrust.pem" (i)						
PEM File Show CA certificate						

VCS現在將信任CUCM提供的證書。

5. 對所有VCS伺服器重複此過程。

### 將證書從VCS伺服器上傳到CUCM伺服器

CUCM需要信任VCS提供的證書。

以下過程介紹了如何上傳在CUCM上生成的VCS證書作為CallManager-Trust證書:

 在OS管理頁面上,導航到安全 > 證書管理,輸入證書名稱,瀏覽到其位置,然後點選上傳檔 案:

Upload Certificate/Certificate chain
Upload File Close
Status
I Status: Ready
Upload Certificate/Certificate chain
Certificate CallManager-trust
Description
Upload File "C:\vcscert.pem" Choose
- Upload File Close
indicates required item.

2. 從所有VCS伺服器上傳證書。在與VCS通訊的每個CUCM伺服器上執行此操作;這通常是運行 CallManager服務的所有節點。

### SIP連線

驗證證書且兩個系統相互信任後,在VCS上配置鄰居區域並在CUCM上配置SIP中繼。有關此過程 的詳細資訊,請參閱<u>Cisco TelePresence Cisco Unified Communications Manager with Cisco</u> <u>VCS(SIP中繼)部署指南</u>。

# 驗證

確認SIP連線在VCS上的鄰居區域中處於活動狀態:

Edit zone Accept proxied registrations Media encryption mode		Deny V (j) Auto V (j)			
Authentication Authentication policy SIP authentication trust mode		Treat as authenticated 💌 👔	Treat as authenticated  () Off  ()		
Location Peer 1 address Peer 2 address Peer 3 address Peer 4 address Peer 5 address Peer 6 address Peer 6 address		10.48.36.203		SIP: Active: 10.48.36.203:5061	
Advanced Zone profie Save Delete Cancel		Cisco Unified Communications Manager	•		
Status State	Active				
Number of calls to this zone Bandwidth used on this VCS Total bandwidth used across this cluster Search rules targeting this zone	0 0 kbps 0 kbps 0				

# 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

- <u>Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS(SIP中繼)部</u> <u>署指南</u>
- 思科網真會議視訊通訊伺服器管理員指南
- Cisco TelePresence證書建立和使用與Cisco VCS部署指南
- <u>思科統一通訊作業系統管理指南</u>
- Cisco Unified Communications Manager管理指南
- 技術支援與文件 Cisco Systems