將Expressway核心的根/中間證書上傳到CUCM

目録 箇介 背景資訊 超態 步驟 1.獲取簽署Expressway C伺服器證書的根證書和中間證書 步驟 2.上傳CUCM上的根證書和中間證書(如果適用) 步驟 3.在CUCM上重新啟動必要的服務 相關資訊

簡介

本文檔介紹如何將已簽名Expressway-C證書的CA的根證書和中間證書上傳到CUCM發佈伺服器。

背景資訊

由於X14.0.2中Expressway上的流量伺服器服務的改進,即使伺服器(CUCM)處於非安全模式,只要 伺服器(CUCM)請求在8443以外的埠(例如,6971,6972)上運行的服務,Expressway-C就會傳送 其客戶端證書。由於進行了此更改,因此需要將Expressway-C證書簽名證書頒發機構(CA)同時作為 tomcat-trust和callmanager-trust增加到CUCM中。

在Expressway升級到X14.0.2或更高版本後,無法上傳CUCM上的Expressway-C簽名CA導致 MRA登入失敗。

要使CUCM信任Expressway-C傳送的證書,tomcat-trust和callmanager-trust必須包含根CA以及參 與簽署Expressway-C證書的任何中間CA。

組態

步驟 1.獲取簽署Expressway C伺服器證書的根證書和中間證書

當您最初從簽署該伺服器證書的CA收到伺服器證書時,您還擁有該伺服器證書的根證書和中間證書 ,並將它們儲存在安全位置。如果您仍然擁有這些檔案或可以從您的CA再次下載這些檔案,則可以 轉到第2步,在該步中可以找到有關如何將它們上傳到CUCM的說明。

如果不再擁有這些檔案,您可以從Expressway-C Web介面下載它們。這有點複雜,因此強烈建議 您聯絡您的CA,儘可能從他們下載信任庫。

在Expressway-C上,導航到維護>安全>伺服器證書,然後按一下「伺服器證書」旁邊的顯示(解碼)按鈕。這將打開一個包含Expressway-C伺服器證書內容的新窗口/頁籤。您可以在此處查詢「 頒發者」欄位:

<#root>

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
55:00:00:02:21:bb:2d:41:60:55:d7:b2:27:00:01:00:00:02:21
Signature Algorithm: sha256WithRSAEncryption
Issuer: O=DigiCert Inc, CN=DigiCert Global CA-1
Validity
Not Before: Dec 8 10:36:57 2021 GMT
Not After : Dec 8 10:36:57 2023 GMT
Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab
Subject Public Key Info:
...
```

在本示例中,Expressway-C伺服器證書由DigiCert Inc.組織頒發,其通用名稱為DigiCert Global CA-1。

現在,導航到維護>安全>受信任CA證書,在清單中檢視您是否有證書在「主題」欄位中具有完全相 同的值。在本示例中,這是Subject欄位中的O=DigiCert Inc, CN=DigiCert Global CA-1。如果找到 匹配項,則表示這是中繼CA。您需要此檔案,並且需要繼續查詢,直到找到根CA。

如果您找不到相符專案,請在「簽發者」欄位中搜尋具有此值的憑證,且其主旨與簽發者相符。如 果您找到相符專案,則表示這是根CA檔案,是我們唯一需要的檔案。

Туре	Issuer	Subject
Certificate	CN=vngtp-ACTIVE-DIR-CA	Matches Issuer
Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
Certificate	O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root	Matches Issuer
Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	Matches Issuer
Certificate	O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority	Matches Issuer
Certificate	O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2	Matches Issuer
Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer
Certificate	O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc For authorized use only, CN=thawte Primary Root CA	Matches Issuer
Certificate	O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5	Matches Issuer
Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert Global CA-1

Show all (decoded) Show all (PEM file) Delete Select all Unselect all

Expressway信任儲存

在本例中,在找到證書後,您注意到Subject欄位與Issuer欄位不匹配。這表示這是中繼CA憑證。除 了根憑證之外,您還需要此憑證。如果主題表明與頒發者匹配,則您會知道這是根證書頒發機構 ,也是您需要信任的唯一證書。

如果您有中間憑證,您必須繼續執行,直到我們找到根憑證為止。為此,請檢視您的中間證書的 Issuer欄位。然後在Subject欄位中查詢具有相同值的證書。在我們的示例中,這是O=DigiCert Inc, OU=<u>www.digicert.com</u>, CN=DigiCert Global Root CA -您將在Subject欄位中查詢具有此值 的證書。如果找不到相符的憑證,請在主旨為相符簽發者的[簽發者]欄位中尋找此值。

在本示例中,您可以看到我們的Expressway C伺服器證書由中間CA O=DigiCert Inc.簽署 , CN=DigiCert Global CA-1由根CA O=DigiCert Inc.簽署。OU=<u>www.digicert.com</u>, CN=DigiCert Global Root CA。由於您已經找到根CA,因此您的工作已經完成。但是,如果您找到另一個中間 CA,則需要繼續此過程,直到您辨識出每個中間CA和根CA。

要下載根證書檔案和中間證書檔案,請按一下清單下的Show all (PEM file)按鈕。這會以PEM格式 顯示所有根和中間證書。向下滾動,直到找到符合其中一個中間憑證或根憑證的憑證。在本示例中 ,您首先找到的是O=DigiCert Inc, CN=DigiCert Global Root CA -您需要將此證書複製到一個檔案 並將其儲存在本地。

Epn3o0WC4zxe9Z2etiefC7IpJ50CBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz ksLi4xaNmjICq44Y3ekQEe5+NauQrz4w1HrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS R9I4LtD+gdwyah617jzV/0eBHRnDJELqYzmp -----END CERTIFICATE-----

O=DigiCert Inc, CN=DigiCert Global Root CA

----BEGIN CERTIFICATE-----

. . .

MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUN1cnQgSW5jMRkwFwYDVQQLExB3 d3cuZG1naWN1cnQuY29tMSAwHqYDVQQDExdEaWdpQ2VydCBHbG9iYWwqUm9vdCBD QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTA1VT MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j b20xIDAeBgNVBAMTFORpZ21DZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG 9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLegKTTo1egUKKPC3eQyaK17hL011sB CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97 nh6Vfe63SKMI2taveqw5BmV/S10fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt 43C/dxC//AH2hdmoRBBYMq11GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P T19sd16gSzeRntwi5m30FBgOasv+zbMUZBfHWymeMr/y7vrTC0LUg7dBMtoM10/4 gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR TLtm8KPiGxvD17I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvD17I90VUw DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg 060/nVsJ8dW041P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dW0IrWcBAI+0tKIJF PnlUkiaY4IBIqDfv8NZ5YBberOqOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXc1VzDAGySj4dzp30d8tbQk CAUw7C29C79Fv1C5qfPrmAESrciIxpq0X40KPMbp1ZWVbd4= ----END CERTIFICATE-----

O=The Go Daddy Group, Inc. ----BEGIN CERTIFICATE----MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh MB8GA1UEChMYVGh1IEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE ...

對於每個根和最終的中間證書,複製所有以(包括)-----BEGIN CERTIFICATE-----開頭(包括)-----END CERTIFICATE-----結尾的內容。將每個檔案放在不同的文字檔案中,並在底部加上1個額外 的空白行(在-----END CERTIFICATE-----行之後)。以.pem副檔名儲存這些檔案:root.pem、 intermediate1.pem、intermediate2.pem、...每個根/中間憑證都需要一個單獨的檔案。在上一個範

----BEGIN CERTIFICATE-----

MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUN1cnQgSW5jMRkwFwYDVQQLExB3 d3cuZG1naWN1cnQuY29tMSAwHqYDVQQDExdEaWdpQ2VydCBHbG9iYWwqUm9vdCBD MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j b20xIDAeBgNVBAMTF0RpZ21DZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG 9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaK17hL011sB CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97 nh6Vfe63SKMI2taveqw5BmV/S10fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt 43C/dxC//AH2hdmoRBBYMq11GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P T19sd16gSzeRntwi5m30FBgOasv+zbMUZBfHWymeMr/y7vrTC0LUg7dBMtoM10/4 gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR TLtm8KPiGxvD17I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvD17I90VUw DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg 060/nVsJ8dW041P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dW0IrWcBAI+0tKIJF PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV01s YSEY1QSteDws0oBrp+uvFRTp2InBuThs4pFsiv9kuXc1VzDAGySj4dzp30d8tbQk CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=

----END CERTIFICATE----



注意:底部必須有一個空行。

步驟 2.上傳CUCM上的根證書和中間證書(如果適用)

- 登入您的CUCM發佈伺服器的Cisco Unified OS Administration頁面。
- 導航到安全>證書管理。
- 按一下Upload Certificate/Certificate chain按鈕。
- 在新視窗中,開始從步驟1上傳根憑證。上傳至tomcat-trust。

Upload Certificate/Certificate chain				
Upload The Close				
_ Status				
i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster				
Upload Certificate/Certificate chain				
Certificate Purpose*	tomcat-trust ~			
Description(friendly name)	DigiCert root CA Certificate			
Upload File	Browse root.pem			
Upload Close				
(i) *- indicates required item.				

- 按一下Upload按鈕,然後必須看到Success: Certificate Uploaded。忽略要求您立即重新啟動Tomcat的消息。
- 現在使用CallManager-trust上傳相同的根檔案以用於證書目的。
- 對Expressway-C上使用的所有中間證書重複上述步驟(上傳到tomcat-trust和CallManagertrust)。

步驟 3.在CUCM上重新啟動必要的服務

需要在CUCM集群中的每個CUCM節點上重新啟動這些服務:

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

可以從CUCM的Cisco Unified Serviceability頁面重新啟動Cisco CallManager和Cisco TFTP:

- 登入到CUCM發佈伺服器的Cisco Unified Serviceability頁面。
- 導航到工具>控制中心-功能服務。
- 選擇您的Publisher作為伺服器。
- 選擇Cisco CallManager服務,然後按一下Restart按鈕。
- 重新啟動Cisco CallManager服務後,選擇Cisco TFTP service,然後按一下Restart按鈕。

Cisco Tomcat只能從CLI重新啟動:

- 打開與CUCM發佈伺服器的命令列連線。
- 使用命令utils service restart Cisco Tomcat。

相關資訊

技術支援與檔案- Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。