解決方法並恢復cBR-8上過期的製造商證書

目錄

簡介

本文描述防止、解決和恢復電纜數據機(CM)拒絕(pk)服務對cBR-8電纜數據機終端系統(CMTS)產生的製造商證書(Manu Cert)到期影響的選項。

問題

CM在cBR-8上停滯在reject(pk)狀態的原因有很多，其中一個原因是手動證書過期。Manu Cert用於CM和CMTS之間的身份驗證。在本文檔中，Manu Cert是DOCSIS 3.0安全規範CM-SP-SECv3.0所說的CableLabs Mfg CA證書或製造商CA證書。Expire表示cBR-8系統日期/時間超過Manu Cert有效性結束日期/時間。

在Manu Cert過期後嘗試向cBR-8註冊的CM被CMTS標籤為reject(pk)，並且不在服務中。已在cBR-8中註冊且在Manu Cert到期時處於服務狀態的CM可以保持服務狀態，直到CM下次嘗試註冊為止，這可以在單個CM離線事件、cBR-8電纜線卡重新啟動、cBR-8重新載入或其他事件觸發CM註冊後發生。此時CM身份驗證失敗，cBR-8將其標籤為reject(pk)，並且不在服務中。

本文檔中的資訊將對cBR-8產品公告中的電纜數據機和過期製造商證書中發佈的內容進行擴展和重新格式化。

> **附註**：思科錯誤ID CSCvv21785;在某些版本的Cisco IOS XE中，此錯誤會導致cBR-8重新載入後受信任手動憑證驗證失敗。在某些情況下，Manu Cert存在，但不再處於受信任狀態。在這種情況下，可通過本文檔中描述的步驟將Manu Cert信任狀態更改為可信。如果show cable privacy manufacturer-cert-list命令的輸出中沒有Manu Cert，則可以手動重新新增Manu Cert，也可以使用AuthInfo執行本文檔中介紹的步驟。

Manu證書資訊

可從遠端裝置通過cBR-8 CLI命令或簡單網路管理協定(SNMP)命令檢視手動證書資訊。cBR-8 CLI還支援SNMP set、get和get-bulk命令。這些命令和資訊用於本文檔中介紹的解決方案。

手動證書資訊欄位和屬性

- 索引：為cBR-8資料庫/MIB中的每個Manu Cert分配的唯一整數
- 主題： 使用者名稱與它在X509憑證中編碼的完全相同
  cn:公用名ou:組織單位o:組織l:地區s:StateOrProvinceName思:國家/地區名稱
- 頒發者：證書頒發機構
- 串列：以十六進位制八位位元組字串表示的證書序列號
- 狀態:證書的信任狀態
  可信不可信鏈接根
- 來源：憑證如何到達CMTS
  snmp配置檔案外部資料庫其他authentInfocompiledInfoCode
- 狀態/行狀態：證書狀態
  active（作用中）notInService未就緒createAndGo建立並等待銷毀

- 證書：X509 DER編碼的證書頒發機構證書
- 有效日期：定義相對於CMTS系統日期和時間的manu證書有效期的起始日期和終止日期
  開始日期：Manu證書生效的日期和時間結束日期：Manu證書不再有效的日期和時間
- 證書：X509 DER編碼的證書頒發機構證書
- 指紋：CA憑證的SHA-1雜湊

cBR-8 CLI命令

使用這些cBR-8 CLI命令可以檢視手動證書資訊。

- 在cBR-8 CLI exec模式或線路卡CLI exec模式下：CBR8-1#**show cable privacy manufacturer-cert-list**
- 在cBR-8線路卡CLI執行模式下：Slot-6-0#**show crypto pki certificates**

這些Cisco IOS® XE SNMP命令從cBR-8 CLI用於獲取和設定SNMP OID。

- snmp get
- snmp get-bulk
- snmp set

以下cBR-8電纜介面配置命令用於本文檔的解決方案部分中所述的解決方法和恢復。

- cable privacy retain-failed-certificates
- cable privacy skip-validity-period

DOCSIS-BPI-PLUS-MIB OID

Manu Cert資訊在docsBpi2CmtsCACertEntry OID分支1.3.6.1.2.1.10.127.6.1.2.5.2.1中定義，如SNMP對象導航器中所述。

相關SNMP OID

```
docsBpi2CmtsCACertSubject 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
docsBpi2CmtsCACertIssuer 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
docsBpi2CmtsCACertSerialNumber 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
docsBpi2CmtsCACertSource 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
docsBpi2CmtsCACertStatus 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
docsBpi2CmtsCACert 1.3.6.1.2.1.10.127.6.1.2.5.2.1.8
```

在命令示例中，省略號(...)表示為便於閱讀，省略了某些資訊。

解決方案

CM韌體更新是最好的長期解決方案。本文檔中介紹的變通方法允許具有過期的Manu證書的CM在cBR-8上註冊並保持聯機，但僅建議短期使用這些變通方法。如果CM韌體更新不可行，則從安全和運營的角度來看，CM更換策略是一個很好的長期解決方案。此處描述的解決方案可解決不同的條件或情形，並可以單獨使用，有些還可相互結合使用；

- 更新CM韌體
- 將已知手動證書設定為「可信」
- 已知手動證書到期後恢復CM服務
- 在cBR-8上安裝未知的過期手動證書並標籤為受信任
- 使用cBR-8 CLI命令允許身份驗證資訊新增過期的CM證書和手動證書

> **附註**：如果刪除BPI，則會禁用加密和身份驗證，從而最大程度地降低了作為解決方案的可行性。

更新CM韌體

在許多情況下，CM製造商會提供CM韌體更新，以延長Manu證書的有效結束日期。此解決方案是最佳選擇，當在Manu Cert過期之前執行時，可防止相關服務影響。CM載入新韌體，並用新的手動證書和CM證書重新註冊。新證書可以正確進行身份驗證，並且CM可以成功向cBR-8註冊。新的手動證書和CM證書可以建立一個新的證書鏈，使其返回到已在cBR-8中安裝的已知根證書。

將已知手動證書設定為「可信」

當CM韌體更新因CM製造商停業而無法使用時，不再支援CM模型等，在有效結束日期之前，可以在cBR-8中主動將已知、近期具有有效結束日期的Manu Certs標籤為可信。cBR-8 CLI命令和SNMP用於識別個人證書資訊（如序列號和信任狀態），而SNMP用於在cBR-8中將個人證書信任狀態設定為受信任，從而允許關聯的CM註冊並保持服務。

當前服務中和聯機CM的已知手動證書通常由cBR-8通過DOCSIS基線隱私介面(BPI)協定從CM獲取。從CM傳送到cBR-8的AuthInfo消息包含手動證書。每個唯一的Manu Cert儲存在cBR-8記憶體中，其資訊可通過cBR-8 CLI命令和SNMP檢視。

當Manu Cert標籤為可信任時，它會執行兩個重要操作。首先，它允許cBR-8 BPI軟體忽略過期有效日期。其次，在cBR-8 NVRAM中將Manu Cert儲存為可信證書。這在cBR-8重新載入中保留了Manu Cert狀態，並且無需在cBR-8重新載入時重複此過程。

CLI和SNMP命令示例演示如何識別手動證書索引、序列號和信任狀態；然後使用該資訊將信任狀態更改為可信。示例重點介紹具有索引4和序列號437498F09A7DCBC1FA7AA101FE976E40的Manu證書。

從cBR-8 CLI檢視手動證書資訊

在本示例中，使用cBR-8 CLI命令**show cable privacy manufacturer-cert-list**。

```
CBR8-1#show cable privacy manufacturer-cert-list

Cable Manufacturer Certificates:

Index: 4
Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Motorola Corporation Cable Modem Root Certificate Authority,ou=ASG,ou=DOCSIS,l=San
Diego,st=California,o=Motorola Corporation,c=US
State: Chained
Source: Auth Info
RowStatus: Active
Serial:      437498F09A7DCBC1FA7AA101FE976E40
Thumbprint:  FA07609998FDCAFA8F80D87F1ACFC70E6C52C80F
Fingerprint: 0EABDBD19D8898CA9C720545913AB93B

Index: 5
Issuer: cn=CableLabs Root Certification Authority,ou=Root CA01,o=CableLabs,c=US
Subject: cn=CableLabs Device Certification Authority,ou=Device CA01,o=CableLabs,c=US
State: Chained
Source: Auth Info
RowStatus: Active
Serial:      701F760559283586AC9B0E2666562F0E
Thumbprint:  E85319D1E66A8B5B2BF7E5A7C1EF654E58C78D23
Fingerprint: 15C18A9D6584D40E88D50D2FF4936982
```

從cBR-8 CLI使用SNMP檢視手動證書資訊

在本示例中，使用cBR-8 CLI命令snmp get-bulk。證書索引4和5是儲存在CMTS記憶體中的手動證書。索引1、2和3是根證書。此處不考慮根證書，因為它們的到期日期要長得多。

```
docsBpi2CmtsCACertSubject
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
SNMP Response: reqid 1752673, errstat 0, erridx 0
```

```
docsBpi2CmtsCACertSubject.1 = Data Over Cable Service Interface Specifications
docsBpi2CmtsCACertSubject.2 = tComLabs - Euro-DOCSIS
docsBpi2CmtsCACertSubject.3 = CableLabs
docsBpi2CmtsCACertSubject.4 = Motorola
docsBpi2CmtsCACertSubject.5 = CableLabs

docsBpi2CmtsCACertIssuer
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
SNMP Response: reqid 1752746, errstat 0, erridx 0
docsBpi2CmtsCACertIssuer.1 = DOCSIS Cable Modem Root Certificate Authority
docsBpi2CmtsCACertIssuer.2 = Euro-DOCSIS Cable Modem Root CA
docsBpi2CmtsCACertIssuer.3 = CableLabs Root Certification Authority
docsBpi2CmtsCACertIssuer.4 = DOCSIS Cable Modem Root Certificate Authority
docsBpi2CmtsCACertIssuer.5 = CableLabs Root Certification Authority

CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
SNMP Response: reqid 2300780, errstat 0, erridx 0
docsBpi2CmtsCACertSerialNumber.1 =
58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C 19
docsBpi2CmtsCACertSerialNumber.2 =
63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1 2C
docsBpi2CmtsCACertSerialNumber.3 =
62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7 61
docsBpi2CmtsCACertSerialNumber.4 =
43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40
docsBpi2CmtsCACertSerialNumber.5 =
70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F 0E

docsBpi2CmtsCACertTrust
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
SNMP Response: reqid 1752778, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.1 = 4
docsBpi2CmtsCACertTrust.2 = 4
docsBpi2CmtsCACertTrust.3 = 4
docsBpi2CmtsCACertTrust.4 = 3    (3 = chained)
docsBpi2CmtsCACertTrust.5 = 3

docsBpi2CmtsCACertSource
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
SNMP Response: reqid 1752791, errstat 0, erridx 0
docsBpi2CmtsCACertSource.1 = 4
docsBpi2CmtsCACertSource.2 = 4
docsBpi2CmtsCACertSource.3 = 4
docsBpi2CmtsCACertSource.4 = 5   (5 = authentInfo)
docsBpi2CmtsCACertSource.5 = 5

docsBpi2CmtsCACertStatus
CBR8-1#snmp get-bulk v2c 10.122.151.12 vrf Mgmt-intf Cisco123 non-repeaters 0 max-repetitions 5
oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
SNMP Response: reqid 1752804, errstat 0, erridx 0
docsBpi2CmtsCACertStatus.1 = 1
docsBpi2CmtsCACertStatus.2 = 1
docsBpi2CmtsCACertStatus.3 = 1
docsBpi2CmtsCACertStatus.4 = 1   (1 = active)
docsBpi2CmtsCACertStatus.5 = 1
```

從遠端裝置使用SNMP檢視手動證書資訊

本文檔中的遠端裝置SNMP示例使用來自遠端Ubuntu Linux伺服器的SNMP命令。具體的SNMP命令

和格式取決於用於執行SNMP命令的裝置和作業系統。

```
docsBpi2CmtsCACertSubject
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.1 = STRING: "Data Over Cable Service Interface
Specifications"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.2 = STRING: "tComLabs - Euro-DOCSIS"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.3 = STRING: "CableLabs"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.4 = STRING: "Motorola Corporation"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.5 = STRING: "CableLabs"

docsBpi2CmtsCACertIssuer
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.1 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.2 = STRING: "Euro-DOCSIS Cable Modem Root CA"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.3 = STRING: "CableLabs Root Certification Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.4 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.5 = STRING: "CableLabs Root Certification Authority"

docsBpi2CmtsCACertSerialNumber
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.1 = Hex-STRING: 58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C
19
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.2 = Hex-STRING: 63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1
2C
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.3 = Hex-STRING: 62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7
61
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E
40
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.5 = Hex-STRING: 70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F
0E

docsBpi2CmtsCACertTrust
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.1 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.2 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.3 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 3   (3 = chained)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.5 = INTEGER: 3

docsBpi2CmtsCACertSource
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.1 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.2 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.3 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4 = INTEGER: 5   (5 = authentInfo)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.5 = INTEGER: 5

docsBpi2CmtsCACertStatus
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.1 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.2 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.3 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.4 = INTEGER: 1   (1 = active)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.5 = INTEGER: 1
```

在CLI中確定Manu證書有效結束日期

使用cBR-8線路卡CLI命令**show crypto pki certificates**確定手動證書有效結束日期。此命令輸出不包括手動證書索引。證書序列號可用於將從此命令獲知的手動證書資訊與從SNMP獲知的手動證書資訊相關聯。

```
CBR8-1#request platform software console attach

request platform software console attach 6/0
#
# Connecting to the CLC console on 6/0.
# Enter Control-C to exit the console connection.
#
Slot-6-0>enable
Slot-6-0#show crypto pki certificates

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 701F760559283586AC9B0E2666562F0E   Certificate Usage:
Signature
 Issuer:
    cn=CableLabs Root Certification Authority
    ou=Root CA01
    o=CableLabs
    c=US
  Subject:
    cn=CableLabs Device Certification Authority
    ou=Device CA01
    o=CableLabs
    c=US
 Validity Date:
    start date: 00:00:00 GMT Oct 28 2014
    end   date: 23:59:59 GMT Oct 27 2049
 Associated Trustpoints: e85319d1e66a8b5b2bf7e5a7c1ef654e58c78d23

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 437498F09A7DCBC1FA7AA101FE976E40
 Certificate Usage: Signature
 Issuer:
   cn=DOCSIS Cable Modem Root Certificate Authority
   ou=Cable Modems
   o=Data Over Cable Service Interface Specifications
    c=US
  Subject:
   cn=Motorola Corporation Cable Modem Root Certificate Authority
   ou=ASG
   ou=DOCSIS
   l=San Diego
   st=California
   o=Motorola Corporation
   c=US
  Validity Date:
     start date: 00:00:00 GMT Jul 11 2001
     end   date: 23:59:59 GMT Jul 10 2021
 Associated Trustpoints: fa07609998fdcafa8f80d87f1acfc70e6c52c80f

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 629748CAC0A60DCBD0FFA89140D8D761
 Certificate Usage: Signature
 Issuer:
   cn=CableLabs Root Certification Authority
   ou=Root CA01
   o=CableLabs
   c=US
  Subject:
   cn=CableLabs Root Certification Authority
```

```
   ou=Root CA01
   o=CableLabs
   c=US
  Validity Date:
    start date: 00:00:00 GMT Oct 28 2014
    end   date: 23:59:59 GMT Oct 27 2064
  Associated Trustpoints: DOCSIS-D31-TRUSTPOINT

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 634B5963790E810F3B5445B3714CF12C
 Certificate Usage: Signature
 Issuer:
    cn=Euro-DOCSIS Cable Modem Root CA
    ou=Cable Modems
    o=tComLabs - Euro-DOCSIS
    c=BE   Subject:
    cn=Euro-DOCSIS Cable Modem Root CA
    ou=Cable Modems
    o=tComLabs - Euro-DOCSIS
    c=BE
  Validity Date:
   start date: 00:00:00 GMT Sep 21 2001
   end   date: 23:59:59 GMT Sep 20 2031
  Associated Trustpoints: DOCSIS-EU-TRUSTPOINT

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 5853648728A44DC0335F0CDB33849C19
  Certificate Usage: Signature
 Issuer:
    cn=DOCSIS Cable Modem Root Certificate Authority
    ou=Cable Modems
    o=Data Over Cable Service Interface Specifications
    c=US
  Subject:
     cn=DOCSIS Cable Modem Root Certificate Authority
     ou=Cable Modems
     o=Data Over Cable Service Interface Specifications
     c=US
   Validity Date:
     start date: 00:00:00 GMT Feb 1 2001
     end   date: 23:59:59 GMT Jan 31 2031
  Associated Trustpoints: DOCSIS-US-TRUSTPOINT
```

將Manu Cert Trust State設定為Trusted

示例顯示Manu Cert的信任狀態從鏈結更改為可信，其索引= 4，序列號= 437498f09a7dcbc1fa7aa101fe976e40

OID:docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5值：

1:可信
2:不可信
3:鏈接
4:根

此示例顯示用於更改信任狀態的cBR-8 CLI snmp-set命令

```
CBR8-1#snmp set v2c 192.168.1.1 vrf Mgmt-intf private oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
```

```
integer 1
SNMP Response: reqid 2305483, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.4 = 1 (1 = trusted)
```

此示例顯示遠端裝置使用SNMP更改信任狀態

```
jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 i 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

使用cBR-8 CLI或SNMP確認手動證書更改

- 信任值已從鏈結更改為受信任
- 來源值已變更為SNMP，這表示憑證上次由SNMP管理，而不是從BPI通訊協定AuthInfo訊息管理

此示例顯示用於確認更改的cBR-8 CLI命令

```
CBR8-1#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:
...
Index: 4
Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Motorola Corporation Cable Modem Root Certificate Authority,ou=ASG,ou=DOCSIS,l=San
Diego,st=California,o=Motorola Corporation,c=US
State: Trusted
Source: SNMP
RowStatus: Active
Serial:      437498F09A7DCBC1FA7AA101FE976E40
Thumbprint:  DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
Fingerprint: D41D8CD98F00B204E9800998ECF8427E
...
```

此示例顯示遠端裝置使用SNMP確認更改

```
jdoe@server1:~$ snmpget -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)

jdoe@server1:~$ snmpget -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4 = INTEGER: 1 (1 = snmp)
```

已知手動證書到期後恢復CM服務

先前已知的Manu證書是cBR-8資料庫中已經存在的證書，通常由來自以前CM註冊的AuthInfo消息生成。如果Manu證書未標籤為受信任和過期，則使用過期的Manu證書並離線的CM將無法重新註冊並標籤為拒絕(pk)。 本節介紹如何從該條件中恢復，以及如何允許具有過期的Manu證書的CM註冊和保持服務。

當CM無法聯機並且由於過期的Manu Certs而被標籤為reject(pk)時，將生成一條系統日誌消息，該消息包含CM MAC地址和過期的Manu Cert序列號。

從cBR-8日誌消息中識別過期的Manu證書序列號

```
CLC 6/0: Jan 11 17:36:07.094: %CBR-3-MANUFACTURE_CA_CM_CERTIFICATE_FORMAT_ERROR:
<133>CMTS[DOCSIS]: CM MAC Addr <1234.5678.9ABC> on Interface Cable6/0/0 U1 : Manu Cert S/N
```

```
437498F09A7DCBC1FA7AA101FE976E40 has Expired
```

識別過期的Manu證書的索引，並將Manu證書信任狀態設定為Trusted

此示例顯示cBR-8 CLI SNMP命令，這些命令用於從日誌消息中標識Manu Cert序列號索引，然後使用該索引將Manu Cert信任狀態設定為trusted。

```
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
SNMP Response: reqid 2351849, errstat 0, erridx 0
docsBpi2CmtsCACertSerialNumber.1 =
58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C 19
docsBpi2CmtsCACertSerialNumber.2 =
63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1 2C
docsBpi2CmtsCACertSerialNumber.3 =
62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7 61
docsBpi2CmtsCACertSerialNumber.4 =
43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40
docsBpi2CmtsCACertSerialNumber.5 =
70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F 0E

CBR8-1#snmp set v2c 192.168.1.1 vrf Mgmt-intf private oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
integer 1
SNMP Response: reqid 2353143, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.4 = 1 (1 = trusted)
```

此示例顯示遠端裝置使用SNMP命令從日誌消息中識別手動證書序列號的索引，然後使用該索引將手動證書信任狀態設定為可信。

```
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4 | grep
"43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E
40

jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 i 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

在cBR-8上安裝未知的過期手動證書並標籤為受信任

當cBR-8不知道已過期的Manu證書時，在到期前無法對其進行管理（標籤為受信任），也無法恢復。當以前未知且未在cBR-8上註冊的CM嘗試向未知且過期的Manu證書註冊時，會發生這種情況。Manu Cert必須通過SNMP從遠端裝置新增到cBR-8，或使用**cable privacy retain-failed-certificates** cBR-8電纜介面配置來允許AuthInfo新增過期的手動證書。cBR-8 CLI SNMP命令無法用於新增證書，因為證書資料中的字元數超過CLI接受的最大字元數。 如果新增了自簽名證書，則必須在cBR-8電纜介面下配置**cable privacy accept-self-signed-certificate** 命令，然後cBR-8才能接受證書。

使用SNMP向cBR-8新增到期手動證書

使用這些docsBpi2CmtsCACertTable OID值將手動證書新增為新表條目。可以使用[如何解碼數據機停滯狀態診斷的DOCSIS證書中的CA證書轉儲步驟獲知由docsBpi2CmtsCACert OID定義的手動證書的十六進位制值。]

```
docsBpi2CmtsCACertStatus 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7 (Set to 4 to create the row entry)
```

```
docsBpi2CmtsCACert 1.3.6.1.2.1.10.127.6.1.2.5.2.1.8 (The hexadecimal data, as an X509Certificate
value, for the actual X.509 certificate)
docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (Set to 1 to set the Manu Cert Trust
state to trusted)
```

為新增的Manu證書使用唯一的索引號。使用**show cable privacy manufacturer-cert-list**命令可以檢查cBR-8上已存在的Manu Certs的索引。

```
CBR8-2#show cable privacy manufacturer-cert-list | i Index
Index: 4
Index: 5
Index: 6
Index: 7
```

本節中的示例對新增到cBR-8資料庫的Manu Cert使用索引值11。

> **提示：**始終先設定CertStatus屬性，然後再設定實際證書資料。否則，CMTS會假定憑證已鏈結，並立即嘗試與製造商和根憑證驗證憑證。

某些作業系統無法接受指定證書的十六進位制資料字串輸入所需的輸入行。因此，可以使用圖形SNMP管理器來設定這些屬性。對於許多證書，如果更方便，可以使用指令碼檔案。

此示例顯示一個遠端裝置使用SNMP向cBR-8新增手動證書證書。大多數證書資料被提交以供可讀性使用，如示例(...)所示。

```
jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7.11 i 4
1.3.6.1.2.1.10.127.6.1.2.5.2.1.8.11 x "0x3082...38BD" 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.11 i 1
```

允許使用cBR-8 CLI命令通過AuthInfo新增過期的手動證書

Manu Cert通常通過從CM傳送到cBR-8的BPI協定AuthInfo消息進入cBR-8資料庫。在AuthInfo消息中收到的每個唯一且有效的手動證書都會新增到資料庫中。如果Manu證書對於CMTS（不在資料庫中）未知且有效期已過期，則AuthInfo會被拒絕，並且Manu證書不會新增到cBR-8資料庫中。當cBR-8電纜介面配置下存在**cable privacy retain-failed-certificates**變通配置時，AuthInfo交換器可將過期的手動證書新增到CMTS。這允許將過期的手動證書新增到cBR-8資料庫中，作為不可信證書。要使用過期的Manu證書，必須使用SNMP將其標籤為可信。將過期的手動證書新增到cBR-8並標籤為trusted時，建議刪除**cable privacy retain-failed-certificates**配置，以便其他（可能有害的）手動證書不會進入系統。

```
CBR8-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#int Cable6/0/0
CBR8-1(config-if)#cable privacy retain-failed-certificates
CBR8-1(config-if)#end
```

使用cBR-8 CLI命令允許身份驗證資訊新增過期的CM證書和手動證書

當在每個相關纜線介面下設定了**cable privacy retain-failed-certificates**和**cable privacy skip-validity-period**指令時，AuthInfo交換器可將過期的CM憑證新增到CMTS。這會導致cBR-8忽略在CM BPI AuthInfo消息中傳送的所有CM和Manu Certs的過期有效日期檢查。在將過期的CM和Manu Certs新增到cBR-8並標籤為trusted時，建議刪除所述的配置，這樣，附加的、可能不需要的證書就不會進入系統。

```
CBR8-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#interface Cable6/0/0
CBR8-1(config-if)#cable privacy retain-failed-certificates
CBR8-1(config-if)#cable privacy skip-validity-period
CBR8-1(config-if)#end
CBR8-1#copy run start
```

其他資訊

MAC域/電纜介面配置注意事項

cable privacy retain-failed-certificates和**cable privacy skip-validity-period**配置命令在MAC域/電纜介面級別使用，不受限制。retain-failed-certificates命令可以將任何失敗的證書新增到cBR-8資料庫中，而skip-validity-period命令可以跳過所有Manu和CM證書的有效日期檢查。

SNMP封包大小注意事項

如果Cert OctetString大於SNMP資料包大小，則Cert資料的SNMP get可以返回空值。使用大型證書時，可以使用cBR-8 SNMP配置；

```
CBR8-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#snmp-server packetsize 3000
CBR8-1(config)#end
CBR8-1#copy run start
```

手動證書調試

使用**debug cable privacy ca-cert**和**debug cable mac-address <CM mac-address>**命令支援cBR-8上的Manu Cert debug。有關其他調試資訊，請參閱支援文章如何解碼數據機停滯狀態診斷的DOCSIS證書。其中包括用於獲取手動證書的十六進位制值的CA證書轉儲步驟。

相關支援檔案

- 適用於Cisco CMTS路由器的DOCSIS 1.1提供有關cBR-8支援和配置DOCSIS基線隱私介面(BPI+)的其他資訊。
- Cisco CMTS Cable Command Reference提供有關本文檔中引用的cBR-8 CLI命令的資訊。
- 在uBR10K上解決和恢復過期的製造商證書提供的資訊與uBR10K CMTS的本文檔類似。
- 技術支援與文件 - Cisco Systems