Soluzione e recupero dei certificati scaduti del produttore su cBR-8

Sommario

Introduzione

In questo documento vengono descritte le opzioni per prevenire, risolvere e ripristinare il problema del servizio di rifiuto del modem via cavo (CM) sul sistema di terminazione del modem via cavo cBR-8 (CMTS) in seguito alla scadenza del certificato del produttore (Manu Cert).

Problema

Esistono diverse cause per cui un CM si blocca nello stato di rifiuto (pk) in cBR-8. Una causa è la scadenza del certificato Manu. Il Manu Cert viene utilizzato per l'autenticazione tra un CM e CMTS. In questo documento, un certificato Manu è ciò che la specifica di sicurezza DOCSIS 3.0 CM-SP-SECv3.0 definisce certificato CA Mfg di CableLabs o certificato CA del produttore. Scadenza indica che la data/ora di sistema cBR-8 supera la data/ora di fine della validità del Manu Cert.

Un CM che tenta di eseguire la registrazione con cBR-8 dopo la scadenza del Manu Cert viene contrassegnato come rifiuto (pk) dal CMTS e non è in servizio. Un CM già registrato con cBR-8 e in servizio alla scadenza del Manu Cert può rimanere in servizio fino al successivo tentativo di registrazione da parte del CM, che può verificarsi dopo un singolo evento CM offline, il riavvio della scheda cablata cBR-8, il ricaricamento cBR-8 o altri eventi che attivano la registrazione del CM. In quel momento il CM non riesce l'autenticazione, viene contrassegnato come rifiuto (pk) da cBR-8 e non è in servizio.

Le informazioni di questo documento ampliano e riformattano il contenuto pubblicato nei modem cablati e nei certificati dei produttori in scadenza nel bollettino sui prodotti cBR-8.

> **Nota:** ID bug Cisco CSCv21785; In alcune versioni di Cisco IOS XE, questo bug impedisce la convalida di un Manu Cert attendibile dopo un ricaricamento cBR-8. In alcuni casi il Manu Cert è presente ma non è più nello stato di fiducia. In tal caso, lo stato di attendibilità del certificato Manu può essere modificato in attendibile seguendo la procedura descritta in questo documento. Se il Manu Cert non è presente nell'output del comando show cable privacy Manufacturer-cert-list, il Manu Cert può essere aggiunto di nuovo manualmente o tramite AuthInfo con la procedura descritta in questo documento.

Informazioni sul certificato Manu

Èpossibile visualizzare le informazioni relative al certificato manuale tramite i comandi CLI cBR-8 o i comandi SNMP (Simple Network Management Protocol) da un dispositivo remoto. La CLI cBR-8 supporta anche i comandi set, get e get-bulk del protocollo SNMP. Questi comandi e queste informazioni vengono utilizzati dalle soluzioni descritte più avanti nel documento.

Gestisci campi informazioni certificato e attributi

- Indice: Numero intero univoco assegnato a ogni Manu Cert nel database cBR-8/MIB
- Oggetto: Nome del soggetto esattamente come è codificato nel certificato X509 cn: NomeComuneUo: Unità organizzativao: Organizzazionel. Localitàs: NomeProvinciac: NomePaese
- Emittente: Autorità di certificazione
- Seriale: Numero di serie del certificato rappresentato in una stringa di ottetti esadecimali
- State: Stato di attendibilità del certificato attendibilenon attendibileconcatenatoradice
- Fonte: Modalità con cui il certificato ha raggiunto il CMTS snmpFileConfigurazionedatabase esternoOther (Altro)InformazioniAutenticazionecompiledInfoCode
- Status/RowStatus: Stato certificato activenotInServiziononProntocreaVaiACcreateand Waitdistruggere

- Certificato: Il certificato dell'autorità di certificazione codificato DER X509
- Data di validità: Le date di inizio e di fine che definiscono il periodo di validità del certificato Manu relativo alla data e all'ora del sistema CMTS
  data di inizio: Data e ora di inizio validità del certificato manudata di fine: Data e ora in cui il certificato manu non è più valido
- Certificato: Il certificato dell'autorità di certificazione codificato DER X509
- Identificazione personale: Hash SHA-1 di un certificato CA

Comandi CLI cBR-8

Èpossibile visualizzare le informazioni relative al certificato manuale con questi comandi CLI di cBR-8.

- Da modalità di esecuzione CLI cBR-8 o modalità di esecuzione CLI Linecard: CBR8-1**#show cable privacy Manufacturer-cert-list**
- Da cBR-8 Linecard CLI in modalità di esecuzione: Slot-6-0**#show crypto pki certificates**

Questi comandi Cisco IOS® XE SNMP vengono utilizzati dalla CLI di cBR-8 per ottenere e impostare gli OID SNMP.

- snmp get
- snmp get-bulk
- set snmp

I comandi di configurazione dell'interfaccia del cavo cBR-8 vengono utilizzati per soluzioni alternative e il ripristino descritti nella sezione Soluzione di questo documento.

- protezione della privacy dei cavi - conservazione dei certificati non riusciti
- privacy cavo skip-valid-period

OID DOCSIS-BPI-PLUS-MIB

Le informazioni sul certificato di autenticazione sono definite nel branch OID docsBpi2CmtsCACertEntry 1.3.6.1.2.1.10.127.6.1.2.5.2.1, descritto in SNMP Object Navigator.

OID SNMP rilevanti

```
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
```

Negli esempi di comandi, i puntini di sospensione (...) indicano che alcune informazioni sono state omesse per motivi di leggibilità.

Soluzione

L'aggiornamento del firmware CM è la migliore soluzione a lungo termine. Le soluzioni descritte in

questo documento consentono ai CM con certificati Manu scaduti di registrarsi e rimanere online con il cBR-8, ma sono consigliate solo per un utilizzo a breve termine. Se l'aggiornamento del firmware di un CM non è un'opzione, una strategia di sostituzione del CM è una buona soluzione a lungo termine dal punto di vista della sicurezza e delle operazioni. Le soluzioni qui descritte si riferiscono a condizioni o scenari diversi e possono essere utilizzate singolarmente o, in alcuni casi, in combinazione tra loro;

- Aggiorna firmware CM
- Impostare un certificato utente noto come attendibile
- Ripristina servizio CM dopo la scadenza di un certificato Manu noto
- Installare un certificato Manu scaduto sconosciuto in cBR-8 e contrassegnare come attendibile
- Consentire l'aggiunta di certificati CM e di certificati manuali scaduti da parte di AuthInfo con un comando CLI cBR-8

Nota: Se BPI viene rimosso, la crittografia e l'autenticazione verranno disabilitate, riducendo al minimo la possibilità di utilizzo di tale funzionalità come soluzione alternativa.

Aggiorna firmware CM

In molti casi, i produttori di CM forniscono aggiornamenti del firmware CM che estendono la data di fine validità del Manu Cert. Questa soluzione è la migliore e, se eseguita prima della scadenza di un Manu Cert, impedisce l'impatto dei servizi correlati. I CM caricano il nuovo firmware e registrano nuovamente i nuovi certificati Manu e i certificati CM. I nuovi certificati possono essere autenticati in modo corretto e i certificati di certificazione possono essere registrati con cBR-8. I nuovi certificati di autenticazione e certificati di certificazione possono creare una nuova catena di certificati per il certificato radice noto già installato in cBR-8.

Impostare un certificato utente noto come attendibile

Quando un aggiornamento del firmware di CM non è disponibile a causa di un produttore CM che ha cessato l'attività, nessun ulteriore supporto per un modello CM, e così via, i certificati Manu già noti sul cBR-8 con date di fine validità nel prossimo futuro possono essere contrassegnati come attendibili in cBR-8 prima della data di fine validità. I comandi CLI cBR-8 e il protocollo SNMP vengono utilizzati per identificare le informazioni del certificato di autenticazione, ad esempio il numero di serie e lo stato di attendibilità, mentre il protocollo SNMP viene utilizzato per impostare lo stato di attendibilità del certificato di autenticazione su attendibile in cBR-8, che consente ai CM associati di registrarsi e rimanere in servizio.

I certificati manuali noti per i CM attualmente in servizio e online vengono in genere appresi da cBR-8 da un CM tramite il protocollo BPI (DOCSIS Baseline Privacy Interface). Il messaggio AuthInfo inviato da CM a cBR-8 contiene il certificato Manu. Ciascun Manu Cert univoco è memorizzato nella memoria cBR-8 e le relative informazioni possono essere visualizzate dai comandi CLI cBR-8 e da SNMP.

Quando il Manu Cert è contrassegnato come attendibile, ciò fa due cose importanti. Innanzitutto, consente al software cBR-8 BPI di ignorare la data di validità scaduta. In secondo luogo, il Manu Cert viene archiviato come attendibile nella NVRAM cBR-8. In questo modo lo stato del certificato Manu viene mantenuto durante un ricaricamento cBR-8 ed elimina la necessità di ripetere questa procedura in caso di ricaricamento cBR-8.

Gli esempi di comandi CLI e SNMP mostrano come identificare un indice Manu Cert, un numero di serie e uno stato di trust; utilizzare quindi tali informazioni per impostare lo stato di attendibilità su attendibile. Gli esempi si concentrano sul certificato manu con indice 4 e numero di serie 437498F09A7DCBC1FA7AA101FE976E40.

Visualizzazione delle informazioni sui certificati manuali dalla CLI di cBR-8

Nell'esempio viene utilizzato il comando **show cable privacy Manufacturer-cert-list di** cBR-8 CLI.

```
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
```

Visualizzazione delle informazioni sul certificato di autenticità tramite SNMP dalla CLI di cBR-8

Nell'esempio viene usato il comando snmp get-bulk di cBR-8 CLI. Gli indici di certificato 4 e 5 sono i certificati manu memorizzati nella memoria CMTS. Gli indici 1, 2 e 3 sono certificati radice. I certificati radice non rappresentano un problema in quanto le date di scadenza sono molto più lunghe.

```
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
```

Visualizzazione delle informazioni sul certificato di autenticazione con SNMP da un dispositivo remoto

Gli esempi di protocollo SNMP del dispositivo remoto riportati in questo documento utilizzano i comandi SNMP di un server Ubuntu Linux remoto. I comandi e i formati SNMP specifici dipendono dal dispositivo e dal sistema operativo utilizzati per eseguire i comandi SNMP.

```
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
```

Identificare la data di fine validità del certificato Manu nella CLI

Utilizzare il comando **show crypto pki certificates del** cBR-8 linecard CLI per identificare la data di fine validità del certificato manu. L'output di questo comando non include l'indice del certificato del manu. Il numero di serie del certificato può essere utilizzato per mettere in correlazione le informazioni sul certificato manu apprese da questo comando con le informazioni sul certificato manu apprese da SNMP.

```
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
```

Impostare lo stato del trust tra certificati di autenticazione su Attendibile

Gli esempi mostrano che lo stato di trust è passato da concatenato a attendibile per il certificato Manu con indice = 4 e numero di serie = 437498f09a7dcbc1fa7aa101fe976e40

OID valori docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5:

1: attendibile
2: non attendibile
3: concatenato
4: radice

Nell'esempio viene mostrato il comando cBR-8 CLI snmp-set utilizzato per modificare lo stato di attendibilità

```
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)
```

Nell'esempio viene mostrato come utilizzare il protocollo SNMP per modificare lo stato di attendibilità di un dispositivo remoto

```
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)
```

Confermare le modifiche apportate al certificato tramite la CLI di cBR-8 o SNMP

- Valore di trust modificato da concatenato a attendibile
- Il valore di origine è stato modificato in SNMP, che indica che l'ultimo certificato è stato gestito da SNMP e non dal messaggio AuthInfo del protocollo BPI

Nell'esempio viene mostrato il comando cBR-8 CLI utilizzato per confermare le modifiche

```
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
...
```

Nell'esempio viene mostrato come utilizzare il protocollo SNMP su un dispositivo remoto per confermare le modifiche

```
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)
```

Ripristina servizio CM dopo la scadenza di un certificato Manu noto

Un certificato Manu precedentemente noto è un certificato già presente nel database cBR-8, in genere come risultato dei messaggi AuthInfo della precedente registrazione CM. Se un certificato Manu non è contrassegnato come attendibile e scade, qualsiasi produttore a contratto che utilizza il certificato Manu scaduto e passa alla modalità non in linea non potrà registrarsi nuovamente e verrà contrassegnato come rifiuto (pk). In questa sezione viene descritto come ripristinare questa condizione e consentire ai CM con certificati Manu scaduti di registrarsi e rimanere in servizio.

Quando i CM non sono in linea e vengono contrassegnati come rifiutati (pk) a causa di certificati Manu scaduti, viene generato un messaggio syslog contenente l'indirizzo MAC del CM e il numero di serie del certificato Manu scaduto.

Identificare il numero di serie del certificato manu scaduto dal messaggio di registro cBR-8

```
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
```

Identificare l'indice per il certificato manu scaduto e impostare lo stato di attendibilità del certificato manu su Attendibile

In questo esempio vengono illustrati i comandi SNMP della CLI cBR-8 utilizzati per identificare l'indice per il numero di serie del certificato Manu dal messaggio di log, che viene quindi utilizzato per impostare lo stato di attendibilità del certificato Manu su 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)
```

In questo esempio viene illustrato come un dispositivo remoto utilizzi i comandi SNMP per identificare l'indice del numero di serie del certificato Manu dal messaggio di log, che viene quindi utilizzato per impostare lo stato di attendibilità del certificato Manu su trusted.

```
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)
```

Installare un certificato Manu scaduto sconosciuto in cBR-8 e contrassegnare come attendibile

Quando un certificato Manu scaduto non è noto a cBR-8, non può essere gestito (contrassegnato come attendibile) prima della scadenza e non può essere recuperato. Questo si verifica quando un CM precedentemente sconosciuto e non registrato su un cBR-8 tenta di eseguire la registrazione con un Manu Cert sconosciuto e scaduto. Il Manu Cert deve essere aggiunto a cBR-8 da SNMP da un dispositivo remoto o utilizzare la configurazione dell'interfaccia dei cavi **cable privacy retention-failed-certificates** cBR-8 per consentire a AuthInfo di aggiungere un Manu Cert scaduto. Impossibile utilizzare i comandi SNMP della CLI cBR-8 per aggiungere un certificato. Il numero di caratteri nei dati del certificato supera il numero massimo di caratteri accettato dalla CLI. Se viene aggiunto un certificato autofirmato, il comando **cable privacy accept-self-signed-certificate** deve essere configurato nell'interfaccia del cavo cBR-8 prima che il cBR-8 possa accettare il certificato.

Aggiungere un certificato manu scaduto a cBR-8 con SNMP

Utilizzare i valori OID docsBpi2CmtsCACertTable seguenti per aggiungere il certificato manu come nuova voce di tabella. Il valore esadecimale del Manu Cert definito dall'OID docsBpi2CmtsCACert può essere appreso eseguendo i passaggi di dettaglio dei certificati CA descritti nell'articolo di supporto Come decodificare il certificato DOCSIS per la diagnosi dello stato di blocco del modem.

```
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)
```

Utilizzare un numero di indice univoco per il certificato manu aggiunto. Gli indici dei certificati manu già presenti sulla cBR-8 possono essere controllati con il comando **show cable privacy Manufacturer-cert-list**.

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

Gli esempi in questa sezione utilizzano il valore di indice 11 per il Manu Cert aggiunto al database cBR-8.

> **Suggerimento**: Impostare sempre gli attributi CertStatus prima dei dati effettivi del certificato. In caso contrario, il CMTS presuppone che il certificato sia concatenato e tenta immediatamente di verificarlo con i produttori e i certificati radice.

Alcuni sistemi operativi non sono in grado di accettare righe di input della lunghezza necessaria per immettere la stringa di dati esadecimale che specifica un certificato. Per questo motivo, è possibile utilizzare un manager SNMP grafico per impostare questi attributi. Per diversi certificati, è possibile utilizzare un file di script, se lo si desidera.

Nell'esempio viene mostrato come un dispositivo remoto utilizzi il protocollo SNMP per aggiungere un certificato Manu Cert a cBR-8. La maggior parte dei dati del certificato vengono omessi per essere letti, indicati da ellissi (...).

```
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
```

Consentire l'aggiunta di un certificato manu scaduto da AuthInfo con un comando cBR-8 CLI

In genere, un certificato di autenticazione accede al database cBR-8 tramite il messaggio AuthInfo del protocollo BPI inviato al cBR-8 da CM. Ogni certificato Manu univoco e valido ricevuto in un messaggio AuthInfo viene aggiunto al database. Se il Manu Cert è sconosciuto al CMTS (non nel database) e ha date di validità scadute, AuthInfo viene rifiutato e il Manu Cert non viene aggiunto al database cBR-8. Un certificato manu scaduto può essere aggiunto al CMTS dallo scambio AuthInfo quando è presente la configurazione della soluzione alternativa dei **certificati di conservazione della privacy dei cavi** in cBR-8. Ciò consente di aggiungere il certificato Manu scaduto al database cBR-8 come non attendibile. Per utilizzare il certificato manu scaduto, è

necessario utilizzare il protocollo SNMP per contrassegnarlo come attendibile. Quando il certificato manu scaduto viene aggiunto al cBR-8 e contrassegnato come attendibile, si consiglia di rimuovere la configurazione dei **certificati di conservazione della privacy dei cavi in** modo che i certificati manu aggiuntivi, potenzialmente indesiderati, non entrino nel sistema.

```
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
```

Consentire l'aggiunta di certificati CM e di certificati manuali scaduti da parte di AuthInfo con un comando CLI cBR-8

Un certificato CM scaduto può essere aggiunto al CMTS dallo scambio AuthInfo quando sotto ogni interfaccia del cavo sono configurati i comandi **cable privacy retention-failed-certificates** e **cable privacy skip-valid-period**. In questo modo, cBR-8 ignora i controlli delle date di validità scadute per TUTTI i certificati CM e Manu inviati nel messaggio AuthInfo BPI CM. Quando i certificati CM e Manu scaduti vengono aggiunti a cBR-8 e contrassegnati come attendibili, è consigliabile rimuovere la configurazione descritta in modo da evitare l'accesso al sistema da parte dei certificati aggiuntivi, potenzialmente indesiderati.

```
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
```

Ulteriori informazioni

Considerazioni sulla configurazione dell'interfaccia cavo/dominio MAC

I comandi **cable privacy retention-failed-certificates** e **cable privacy skip-valid-period** configuration vengono utilizzati a livello di dominio MAC/interfaccia cavi e non sono restrittivi. Il comando keep-failed-certificates può aggiungere qualsiasi certificato non riuscito al database cBR-8 e il comando skip-invalid-period può ignorare i controlli della data di validità su tutti i certificati Manu e CM.

Considerazioni sulle dimensioni del pacchetto SNMP

Un'istruzione SNMP get per i dati Cert può restituire un valore NULL se Cert OctetString è più grande delle dimensioni del pacchetto SNMP. È possibile utilizzare una configurazione SNMP cBR-8 quando si utilizzano certificati di grandi dimensioni.

```
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
```

Debug del certificato del manu

Manu Cert debug su cBR-8 è supportato con i comandi **debug cable privacy ca-cert** e **debug cable mac-address <CM mac-address>**. Per ulteriori informazioni sul debug, consultare l'articolo di supporto Decode DOCSIS Certificate for Modem Stuck State Diagnosis. Sono inclusi i passaggi di dump del certificato CA utilizzati per conoscere il valore esadecimale di un certificato Manu.

Documentazione di supporto correlata

- DOCSIS 1.1 per i router Cisco CMTS fornisce informazioni aggiuntive sul supporto cBR-8 e sulla configurazione dell'interfaccia BPI+ (DOCSIS Baseline Privacy Interface).
- La guida di riferimento ai comandi di Cisco CMTS Cable fornisce informazioni sui comandi CLI di cBR-8 menzionati in questo documento.
- Lavorare e recuperare i certificati scaduti del produttore su uBR10K fornisce informazioni simili a quelle fornite in questo documento per i CMTS uBR10K.
- Documentazione e supporto tecnico – Cisco Systems