Soluzione e recupero dei certificati scaduti del produttore su uBR10K

Sommario

[Introduzione](#)
[Problema](#)
[Informazioni sul certificato Manu](#)
[Gestisci campi informazioni certificato e attributi](#)
[Comandi CLI uBR10K](#)
[OID DOCSIS-BPI-PLUS-MIB](#)
[Soluzione](#)
[Aggiorna firmware CM](#)
[Impostare un certificato utente noto come attendibile](#)
[Visualizzare le informazioni sui molti certificati dalla CLI uBR10K](#)
[Visualizzazione delle informazioni sul certificato di autenticazione con SNMP da un dispositivo remoto](#)
[Impostare lo stato di attendibilità del certificato di autenticazione noto scaduto su Attendibile con SNMP](#)
[Confermare la modifica del certificato manu con la CLI uBR10K o con SNMP](#)
[Ripristina servizio CM dopo la scadenza di un certificato Manu noto](#)
[Identificare il numero di serie del certificato manu noto scaduto](#)
[Identificare l'indice per il certificato Manu noto scaduto e impostare lo stato di attendibilità del certificato Manu su Attendibile](#)
[Installare un certificato manu scaduto sconosciuto su uBR10K e contrassegnare come attendibile](#)
[Aggiunta di un certificato manu sconosciuto scaduto all'uBR10K con SNMP](#)
[Aggiunta di un certificato manu scaduto durante la registrazione di CM nella CLI](#)
[Consenti l'aggiunta di certificati CM e di certificati manuali scaduti da parte di AuthInfo con un comando CLI uBR10K](#)
[Ulteriori informazioni](#)
[Considerazioni sulla configurazione dell'interfaccia cavo/dominio MAC](#)
[Considerazioni sulle dimensioni del pacchetto SNMP](#)
[Debug del certificato del manu](#)
[Documentazione di supporto correlata](#)

Introduzione

In questo documento vengono descritte le opzioni per prevenire, risolvere e ripristinare il problema del servizio di rifiuto del modem via cavo (CCM) (pk) che influisce sul sistema di terminazione del modem via cavo uBR10K (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) sull'uBR10K. 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 uBR10K supera la data/ora di fine della validità del Manu Cert.

Un CM che tenta di eseguire la registrazione con uBR10K dopo la scadenza del Manu Cert viene contrassegnato come rifiuto (pk) dal CMTS e non è in servizio. Una scheda di gestione già registrata con uBR10K e in servizio alla scadenza del certificato manu può rimanere in servizio fino al successivo tentativo di registrazione da parte della scheda di gestione, che può verificarsi dopo un singolo evento offline del modem, il riavvio della scheda di rete cablata uBR10K, il ricaricamento uBR10K o altri eventi che attivano la registrazione del modem. A quel punto il CM non riesce l'autenticazione, viene contrassegnato come rifiuto (pk) dall'uBR10K e non è in servizio.

Lo standard DOCSIS 1.1 per i router Cisco CMTS fornisce informazioni aggiuntive sul supporto uBR10K e sulla configurazione dell'interfaccia BPI+ (DOCSIS Baseline Privacy Interface).

Informazioni sul certificato Manu

Èpossibile visualizzare le informazioni relative al certificato manuale tramite i comandi CLI uBR10K o il protocollo SNMP (Simple Network Management Protocol). Questi comandi e queste informazioni vengono utilizzati dalle soluzioni descritte più avanti nel documento.

Gestisci campi informazioni certificato e attributi

- Indice: Un numero intero univoco assegnato a ciascun Manu Cert nel database uBR10K/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
  activenotInServiziononProntocreaVaiACcreaeattenderedistruggere
- 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 uBR10K

L'output di questo comando include alcune informazioni relative al certificato manu. L'indice del certificato di autenticazione può essere ottenuto solo da SNMP

- Dalla modalità di esecuzione CLI uBR10K o dalla modalità di esecuzione CLI Linecard: uBR10K**#show cable privacy Manufacturer-cert-list**
- Dalla modalità di esecuzione uBR10K Linecard CLI: Slot-6-0**#show crypto pki certificates**

Questi comandi di configurazione dell'interfaccia dei cavi sono utilizzati per risolvere i problemi e ripristinare il sistema

- uBR10K(config-if)#cable privacy hold-failed-certificates
- uBR10K(config-if)#cable privacy skip-valid-period

OID DOCSIS-BPI-PLUS-MIB

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

> **Nota:** Nel software uBR10k, la RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB è stata implementata con la diramazione/il percorso MIB OID errato. Poiché la piattaforma uBR10k non è più in vendita e ha superato la data di fine supporto del software, non è possibile risolvere il problema. Anziché il percorso/ramo MIB previsto 1.3.6.1.2.10.127.6, **il percorso/ramo MIB 1.3.6.1.2.1.9999 deve essere utilizzato per le interazioni SNMP con i MIB/OID BPI2 sull'uBR10k.**
> ID bug Cisco correlato CSCum28486

Di seguito vengono riportati gli equivalenti di percorso completo MIB OID BPI2 per le informazioni sul certificato manu sull'uBR10k come indicato nell'ID bug Cisco CSCum28486:

```
docsBpi2CmtsCACertTable = 1.3.6.1.2.1.9999.1.2.5.2
docsBpi2CmtsCACertEntry = 1.3.6.1.2.1.9999.1.2.5.2.1
docsBpi2CmtsCACertIndex = 1.3.6.1.2.1.9999.1.2.5.2.1.1
docsBpi2CmtsCACertSubject = 1.3.6.1.2.1.9999.1.2.5.2.1.2
docsBpi2CmtsCACertIssuer = 1.3.6.1.2.1.9999.1.2.5.2.1.3
docsBpi2CmtsCACertSerialNumber = 1.3.6.1.2.1.9999.1.2.5.2.1.4
docsBpi2CmtsCACertTrust = 1.3.6.1.2.1.9999.1.2.5.2.1.5
docsBpi2CmtsCACertSource = 1.3.6.1.2.1.9999.1.2.5.2.1.6
docsBpi2CmtsCACertStatus = 1.3.6.1.2.1.9999.1.2.5.2.1.7
docsBpi2CmtsCACert = 1.3.6.1.2.1.9999.1.2.5.2.1.8
```

Gli esempi di comandi riportati in questo documento utilizzano i puntini di sospensione (...) per indicare che alcune informazioni sono state omesse ai fini della leggibilità.

Soluzione

L'aggiornamento del firmware CM è la migliore soluzione a lungo termine. Le soluzioni che consentono ai CM con certificati Manu scaduti di registrarsi e rimanere online con l'uBR10K sono descritte in questo documento, 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 sull'uBR10k e contrassegnarlo come attendibile
- Consenti l'aggiunta di certificati CM e di certificati manuali scaduti da parte di AuthInfo con un comando CLI uBR10K

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 correttamente e i CM possono registrarsi con l'uBR10K. Il nuovo certificato di autenticazione e il nuovo certificato di autenticazione possono creare una nuova catena di certificati per il certificato radice noto già installato nell'uBR10K.

Impostare un certificato utente noto come attendibile

Quando un aggiornamento del firmware CM non è disponibile a causa di un produttore CM cessato l'attività, nessun ulteriore supporto per un modello CM, ecc, i certificati manu già noti sull'uBR10k con date di fine validità nel prossimo futuro possono essere contrassegnati come attendibili nell'uBR10k prima della scadenza. Il numero di serie, la data di fine validità e lo stato del certificato del manu sono disponibili con i comandi CLI uBR10K. Il numero di serie, lo stato di attendibilità e l'indice del certificato del manu si trovano con SNMP.

I certificati manuali noti per i modem attualmente in servizio e online vengono in genere appresi dall'uBR10K da un CM tramite il protocollo BPI (DOCSIS Baseline Privacy Interface). Il messaggio AUTH-INFO inviato dal CM all'uBR10K contiene il Manu Cert. Ogni singolo Manu Cert è memorizzato nella memoria uBR10K e le sue informazioni possono essere visualizzate con i comandi CLI uBR10K e SNMP.

Quando il Manu Cert è contrassegnato come attendibile, ciò fa due cose importanti. Innanzitutto, consente al software BPI uBR10K di ignorare la data di validità scaduta. In secondo luogo, il Manu Cert viene archiviato come attendibile nella NVRAM dell'uBR10K. In questo modo lo stato del certificato manu viene mantenuto durante un ricaricamento uBR10K ed elimina la necessità di ripetere questa procedura in caso di ricaricamento uBR10K

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 riferiscono a un Manu Cert con indice 5 e numero di serie 45529C2654797E1623C6E723180A9E9C.

Visualizzare le informazioni sui molti certificati dalla CLI uBR10K

In questo esempio, i comandi uBR10K CLI **show crypto pki certificates** e **show cable privacy**

Manufacturer-cert-list sono utilizzati per visualizzare le informazioni note sul certificato manu.

```
UBR10K-01#telnet 127.0.0.81
Trying 127.0.0.81 ... Open

clc_8_1>en
clc_8_1#show crypto pki certificates
CA Certificate
 Status: Available
  Certificate Serial Number: 45529C2654797E1623C6E723180A9E9C
 Certificate Usage: Not Set
 Issuer:
   cn=DOCSIS Cable Modem Root Certificate Authority
   ou=Cable Modems
   o=Data Over Cable Service Interface Specifications
   c=US
 Subject:
   cn=Arris Cable Modem Root Certificate Authority
   ou=Suwanee\
    Georgia
   ou=DOCSIS
   o=Arris Interactive\
    L.L.C.
   c=US
 Validity Date:
   start date: 20:00:00 EDT Sep 11 2001
    end   date: 19:59:59 EDT Sep 11 2021
 Associated Trustpoints: 0edbf2a98b45436b6e4b464797c08a32f2a2cd66
clc_8_1#exit

[Connection to 127.0.0.81 closed by foreign host]

uBR10K-01#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:

Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris
Interactive\, L.L.C.,c=US
State: Chained  <-- Cert Trust State is Chained
Source: Auth Info    <-- CertSource is Auth Info
RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C  <-- Serial Number
Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

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

OID SNMP uBR10K rilevanti:

```
docsBpi2CmtsCACertTable = 1.3.6.1.2.1.9999.1.2.5.2.1
docsBpi2CmtsCACertSubject = 1.3.6.1.2.1.9999.1.2.5.2.1.2
docsBpi2CmtsCACertIssuer = 1.3.6.1.2.1.9999.1.2.5.2.1.3
docsBpi2CmtsCACertSerialNumber = 1.3.6.1.2.1.9999.1.2.5.2.1.4
docsBpi2CmtsCACertTrust = 1.3.6.1.2.1.9999.1.2.5.2.1.5
docsBpi2CmtsCACertSource = 1.3.6.1.2.1.9999.1.2.5.2.1.6
```

In questo esempio, il comando snmpwalk viene utilizzato per visualizzare le informazioni nella tabella dei certificati di alimentazione uBR10k. Il numero di serie del certificato di autenticazione conosciuto può essere correlato all'indice del certificato di autenticazione, che può essere

utilizzato per impostare lo stato di attendibilità. I comandi e i formati SNMP specifici dipendono dal dispositivo e dal sistema operativo utilizzati per eseguire il comando/la richiesta SNMP.

```
Workstation-1$snmpwalk -v 2c -c snmpstring1 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.1 = STRING: "Data Over Cable Service Interface
Specifications"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.2 = STRING: "tComLabs - Euro-DOCSIS"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.3 = STRING: "Scientific-Atlanta\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.4 = STRING: "CableLabs\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.5 = STRING: "Arris Interactive\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.1 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.2 = STRING: "Euro-DOCSIS Cable Modem Root CA"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.3 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.4 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.5 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.1 = Hex-STRING: 58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C
19
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.2 = Hex-STRING: 63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1
2C
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.3 = Hex-STRING: 57 BF 2D F6 0E 9F FB EC F8 E6 97 09 DE 34 BC
26
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.4 = Hex-STRING: 26 B0 F6 BD 1D 85 E8 E8 E8 C1 BD DF 17 51 ED
8C
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.5 = Hex-STRING: 45 52 9C 26 54 79 7E 16 23 C6 E7 23 18 0A 9E
9C <-- Serial Number
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.1 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.2 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.3 = INTEGER: 3
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.4 = INTEGER: 3
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.5 = INTEGER: 3 <-- Trust State (3 = Chained)
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.1 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.2 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.3 = INTEGER: 5
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.4 = INTEGER: 5
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.5 = INTEGER: 5 <-- Source authentInfo (5)
```

Impostare lo stato di attendibilità del certificato di autenticazione noto scaduto su Attendibile con SNMP

Valori per OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (OID su uBR10k è 1.3.6.1.2.1.9999.1.2.5.2.1.5)

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

Nell'esempio viene mostrato come lo stato di trust sia stato modificato da concatenato a attendibile per il certificato Manu con indice = 5 e numero di serie = 45529C2654797E1623C6E723180A9E9C.

```
Workstation-1$ snmpset -v 2c -c snmpstring1 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1.5.5 i 1
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.5 = INTEGER: 1
```

Confermare la modifica del certificato manu con la CLI uBR10K o con SNMP

- Il valore di trust è stato 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

```
Workstation-1$ snmpwalk -v 2c -c snmpstring1 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.5 = STRING: "Arris Interactive\\"
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.5 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.5 = Hex-STRING: 45 52 9C 26 54 79 7E 16 23 C6 E7 23 18 0A 9E
9C <-- Serial Number
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.5 = INTEGER: 1 <-- Trust State (3 = trusted)
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.5 = INTEGER: 1 <-- Source (1 = SNMP)
```

```
uBR10K-01#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:

Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris
Interactive\, L.L.C.,c=US
State: Trusted
Source: SNMP
RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C
Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

Ripristina servizio CM dopo la scadenza di un certificato Manu noto

Un certificato Manu precedentemente noto è un certificato già presente nel database uBR10K, in genere come risultato dei messaggi AuthInfo della precedente registrazione CM. Se un certificato Manu non è contrassegnato come attendibile e il certificato scade, tutti i CM che utilizzano il certificato Manu scaduto possono successivamente passare offline e tentare di registrarsi, ma l'uBR10K li contrassegna come rifiuto (pk) e non sono in servizio. In questa sezione viene descritto come ripristinare questa condizione e consentire ai CM con certificati Manu scaduti di registrarsi e rimanere in servizio.

Identificare il numero di serie del certificato manu noto scaduto

Le informazioni Manu Cert per un CM bloccato in rifiuto (pk) possono essere controllate con il comando **show cable modem <indirizzo MAC CM> della** CLI uBR10K.

```
show cable modem 1234.5678.9abc privacy verbose

MAC Address : 1234.5678.9abc
Primary SID : 4640
BPI Mode : BPI+++
BPI State : reject(kek)
Security Capabilities :
BPI Version : BPI+++
Encryption : DES-56
EAE : Unsupported
Latest Key Sequence : 1
...
```

```
Expired Certificate : 1
Certificate Not Activated: 0
Certificate in Hotlist : 0
Public Key Mismatch : 0
Invalid MAC : 0
Invalid CM Certificate : 0
CA Certificate Details :
Certificate Serial : 45529C2654797E1623C6E723180A9E9C
Certificate Self-Signed : False
Certificate State : Chained
CM Certificate Details :
CM Certificate Serial : 008D23BE727997B9D9F9D69FA54CF8A25A
CM Certificate State : Chained,CA Cert Expired
KEK Reject Code : Permanent Authorization Failure
KEK Reject Reason : CM Certificate Expired
KEK Invalid Code : None
KEK Invalid Reason : No Information
```

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

Utilizzare gli stessi comandi uBR10K CLI e SNMP descritti nella sezione precedente per identificare l'indice del Manu Cert basato sul numero di serie del Manu Cert. Utilizzare il numero di indice del certificato Manu scaduto per impostare lo stato di attendibilità del certificato Manu su trusted con SNMP.

```
jdoe@server1[983]-->./snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1.4
...
1.3.6.1.2.1.9999.1.2.5.2.1.4.5 = Hex-STRING: 45 52 9C 26 54 79 7E 16 23 C6 E7 23 18 0A 9E 9C
...

jdoe@server1[983]-->./setany -v2c 192.168.1.1 private 1.3.6.1.2.1.9999.1.2.5.2.1.5.5 -i 1
docsBpi2CmtsCACertTrust.5 = trusted(1)
```

Installare un certificato manu scaduto sconosciuto su uBR10K e contrassegnare come attendibile

Se un certificato Manu scaduto non è noto all'uBR10K, pertanto non può essere gestito (contrassegnato come attendibile) prima della scadenza e non può essere recuperato, il certificato deve essere aggiunto all'uBR10K e contrassegnato come attendibile. Questa condizione si verifica quando un CM precedentemente sconosciuto e non registrato in un uBR10K tenta di eseguire la registrazione con un Manu Cert sconosciuto e scaduto.

Il Manu Cert può essere aggiunto all'uBR10K tramite SNMP Set o la configurazione dei certificati di mantenimento della privacy dei cavi.

Aggiunta di un certificato manu sconosciuto scaduto all'uBR10K con SNMP

Per aggiungere un certificato del produttore, aggiungere una voce alla tabella docsBpi2CmtsCACertTable. Specificare questi attributi per ogni voce.

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.999.1.2.5.2.1.7 (impostato su 4 per creare la voce di riga)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.999.1.2.5.2.1.8 (dati esadecimali, come valore del certificato X509, per il certificato X.509 effettivo)

- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.999.1.2.5.2.1.5 (impostato su 1 per impostare lo stato del trust tra certificati di autenticazione su trusted)

La maggior parte dei sistemi operativi non accetta righe di input della lunghezza necessaria per immettere la stringa esadecimale che specifica un certificato. Per questo motivo, si consiglia di utilizzare un programma di gestione grafico SNMP per impostare questi attributi. Per diversi certificati, è possibile utilizzare un file di script, se lo si desidera.

Il comando SNMP e i risultati riportati nell'esempio aggiungono un certificato ASA X.509 codificato DER ASCII al database uBR10K con i seguenti parametri:

```
Index = 11
Status = createAndGo (4)
Trust state =  trusted (1)
```

Utilizzare un numero di indice univoco per il certificato manu aggiunto. Quando viene aggiunto un certificato Manu scaduto, lo stato non è attendibile a meno che non sia impostato manualmente su attendibile. Se viene aggiunto un certificato autofirmato, il comando **cable privacy accept-self-signed-certificate** deve essere configurato nella configurazione dell'interfaccia del cavo uBR10K prima che uBR10K possa accettare il certificato.

In questo esempio, parte del contenuto del certificato viene omesso per motivi di leggibilità, indicati da puntini di sospensione (...).

```
jdoe@server1[983]-->./setany -v2c 192.168.1.1 private 1.3.6.1.2.1.9999.1.2.5.2.1.7.11 -i 4
1.3.6.1.2.1.9999.1.2.5.2.1.8.11 - o "30 82 04 00 30 82 02 e8 a0 03 02 01
02 02 10 43 74 98 f0 9a 7d cb c1 fa 7a a1 01 fe 97 6e 40 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05
05 00 30 81 97 31 0b 30 09 06 03 55 04 06 13 02 55 53
...
d8 26 21 f1 41 eb c4 87 90 65 2d 23 38 08 31 9c 74 16 30 05 18 d2 89 5e 9b 21 13 e3 e9 6a f9 3b
59 5e e2 05 0e 89 e5 9d 2a 40 c2 9b 4f 21 1f 1b b7 2c
13 19 3d 56 ab 4b 09 a9 1e 62 5c ee c0 d2 ba 2d" 1.3.6.1.2.1.9999.1.2.5.2.1.5.11 -i 1
docsBpi2CmtsCACertStatus.11 = createAndGo(4)
docsBpi2CmtsCACert.11 =
30 82  04 00   30 82  02 e8    a0 03  02 01   02 02  10 43
74 98  f0 9a   7d cb  c1 fa    7a a1  01 fe   97 6e  40 30
...
f9 3b  59 5e   e2 05  0e 89    e5 9d  2a 40   c2 9b  4f 21
1f 1b  b7 2c   13 19  3d 56    ab 4b  09 a9   1e 62  5c ee
c0 d2  ba 2d
docsBpi2CmtsCACertTrust.11 = trusted(1)
```

Aggiunta di un certificato manu scaduto durante la registrazione di CM nella CLI

Un certificato di autenticazione entra in genere nel database uBR10K tramite il messaggio AuthInfo del protocollo BPI inviato al uBR10K 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 uBR10K. Un certificato manu non valido può essere aggiunto all'uBR10K tramite AuthInfo quando la configurazione della soluzione alternativa dei **certificati di conservazione della privacy dei cavi** è presente nella configurazione dell'interfaccia del cavo uBR10K. Ciò consente di aggiungere il certificato manu scaduto al database uBR10K come non attendibile. Per utilizzare il certificato manu scaduto, è necessario utilizzare il protocollo SNMP per contrassegnarlo come attendibile.

```
uBR10K#config t
Enter configuration commands, one per line.  End with CNTL/Z.
uBR10K(config)#int Cable6/0/0
uBR10K(config-if)#cable privacy retain-failed-certificates
uBR10K(config-if)#end
```

Quando il certificato manu scaduto viene aggiunto all'uBR10K e contrassegnato come attendibile, si consiglia di rimuovere la configurazione dei **certificati di conservazione non riuscita per la privacy dei cavi** per evitare di aggiungere altri certificati manu scaduti sconosciuti all'uBR10K.

Consenti l'aggiunta di certificati CM e di certificati manuali scaduti da parte di AuthInfo con un comando CLI uBR10K

In alcuni casi, il certificato CM scade. In questo caso, oltre alla configurazione **dei certificati di conservazione della privacy dei cavi**, è necessaria un'altra configurazione sull'uBR10K. In ciascun dominio MAC uBR10K (Cable Interface) rilevante, aggiungere la configurazione **cable privacy skip-valid-period** e salvare la configurazione. In questo modo uBR10K ignora i controlli del periodo di validità scaduto per TUTTI i certificati CM e Manu inviati nel messaggio CM BPI AuthInfo.

```
uBR10K#config t
Enter configuration commands, one per line.  End with CNTL/Z.
uBR10K(config)#interface Cable6/0/0
uBR10K(config-if)#cable privacy skip-validity-period
uBR10K(config-if)#end
uBR10K#copy run start
```

Ulteriori informazioni

Considerazioni sulla configurazione dell'interfaccia cavo/dominio MAC

I comandi per la configurazione della privacy dei cavi retention-failed-certificates e cable privacy skip-valid-period 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 uBR10K 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

Quando si utilizzano certificati di grandi dimensioni, può essere necessaria una configurazione SNMP uBR10K aggiuntiva. Il valore di SNMP Get dei dati Cert può essere NULL se il valore di cert OctetString è maggiore delle dimensioni del pacchetto SNMP. Ad esempio;

```
uBR10K#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
uBR10K(config)#snmp-server packetsize 3000
uBR10K(config)#end
```

Debug del certificato del manu

Manu Cert debug su uBR10K us 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.

Documentazione di supporto correlata

- Modem cablati e certificati del produttore in scadenza su cBR-8 Product Bulletin - Cisco
- Cisco serie uBR1000 Universal Broadband Router
- Documentazione e supporto tecnico – Cisco Systems