Solução alternativa e recuperação de certificados de fabricante expirados no cBR-8

Contents

Introduction

Este documento descreve as opções para impedir, contornar e recuperar os impactos do serviço Cable Modem Termination System (CMTS) do CM (Cable Modem Termination System) (Cable Modem Termination System) do cBR-8 resultantes da expiração do Certificado do Fabricante (Certificado Manu).

Problema

Há diferentes causas para um CM ficar preso no estado reject(pk) no cBR-8. Uma causa é o vencimento do certificado Manu. O certificado Manu é usado para autenticação entre um CM e CMTS. Neste documento, um certificado Manu é o que a Especificação de Segurança DOCSIS 3.0 CM-SP-SECv3.0 se refere como certificado CA Mfg do CableLabs ou certificado CA do fabricante. Expirar significa que a data/hora do sistema cBR-8 excede a data/hora de término da validade do certificado Manu.

Um CM que tenta se registrar no cBR-8 após o certificado Manu expirar está marcado como reject(pk) pelo CMTS e não está em serviço. Um CM já registrado no cBR-8 e em serviço quando o certificado Manu expira pode permanecer em serviço até a próxima vez que o CM tentar registrar-se, o que pode ocorrer após um único evento CM offline, reinicialização do cartão de linha a cabo cBR-8, recarregamento do cBR-8 ou outro evento disparar o registro de CM. Nesse momento, o CM falhou na autenticação, está marcado como reject(pk) pelo cBR-8 e não está em serviço.

As informações neste documento são expandidas e reformam o conteúdo publicado no Cable Modems and Expiring Manufaturer Certificates no cBR-8 Product Bulletin.

> **Note**: ID de bug da Cisco CSCvv21785; Em algumas versões do Cisco IOS XE, esse bug faz com que um certificado Manu confiável falhe na validação após uma recarga do cBR-8. Em alguns casos, o certificado Manu está presente, mas já não está no estado de confiança. Nesse caso, o estado confiável do certificado Manu pode ser alterado para confiável com as etapas descritas neste documento. Se o certificado Manu não estiver presente na saída do comando show cable privacy manufaturer-cert-list, o certificado Manu pode ser adicionado novamente manualmente ou por AuthInfo com as etapas descritas neste documento.

Manu Cert Information

As informações do certificado Manu podem ser visualizadas por meio de comandos CLI cBR-8 ou comandos SNMP (Simple Network Management Protocol) de um dispositivo remoto. A CLI cBR-8 também suporta comandos set, get e get-bulk SNMP. Esses comandos e informações são usados pelas soluções descritas neste documento.

Campos e atributos das informações do certificado Manu

- Índice: Um inteiro exclusivo atribuído a cada certificado Manu no banco de dados/MIB cBR-8
- Assunto: O nome do requerente tal como está codificado no certificado X509 cn: CommonNameou: Unidade organizacionalo: OrganizaçãoI: Localidades: EstadoOuNomeDaProvínciac : Nome do país
- Emissor: Autoridade de certificação
- Série: Número de série do certificado representado em uma string de octeto hexadecimal
- Estado: O status de Confiança do certificado confiávelnão confiávelem cadeiaroot
- Fonte: Como o certificado atingiu o CMTS snmp:arquivo de configuraçãoexternalDatabaseoutrosauthentInfocompiladoInfoCode
- Status/Status da linha: Status do certificado

ativonãoEmServiçonãoProntocriarEgocriar e aguardardestruir

- Cert: O certificado de autoridade de certificação codificado X509 DER
- Data de validade: As datas de início e término que definem o período de validade do certificado Manu relativo à data e hora do sistema CMTS
  data de início: A data e a hora em que o certificado Manu se torna válidodata de término: A data e a hora em que o certificado Manu já não é válido
- Cert: O certificado de autoridade de certificação codificado X509 DER
- Impressão digital: O hash SHA-1 de um certificado CA

Comandos CLI cBR-8

As informações do certificado Manu podem ser visualizadas com esses comandos CLI cBR-8.

- A partir do modo exec CLI do cBR-8 ou do modo exec CLI do Linecard: CBR8-1**#show cable privacy manufaturer-cert-list**
- Do modo exec CLI da placa de linha cBR-8: Slot-6-0**#show crypto pki certificate**

Esses comandos SNMP do Cisco IOS® XE são usados na CLI do cBR-8 para obter e definir OIDs SNMP.

- snmp get
- snmp get-bulk
- snmp set

Esses comandos de configuração de interface de cabo cBR-8 são usados para soluções alternativas e recuperação descritas na seção Solução deste documento.

- cable privacy rett-failed-certificate
- cable privacy skip-valid-period

OIDs DOCSIS-BPI-PLUS-MIB

As informações do certificado Manu são definidas na ramificação 1.3.6.1.2.1.10.127.6.1.2.5.2.1 do OID docsBpi2CmtsCACertEntry, descrita no SNMP Object Navigator.

OIDs SNMP relevantes

```
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
```

Em exemplos de comandos, elipse (...) indica que algumas informações foram omitidas para leitura.

Solução

A atualização do firmware CM é a melhor solução a longo prazo. As soluções alternativas descritas neste documento permitem que CMs com certificados Manu expirados se registrem e permaneçam online com o cBR-8, mas essas soluções alternativas são recomendadas somente para uso a curto prazo. Se uma atualização de firmware de CM não for uma opção, uma estratégia de substituição de CM é uma boa solução de longo prazo do ponto de vista da segurança e das operações. As soluções aqui descritas abordam diferentes condições ou cenários e podem ser utilizadas individualmente ou em combinação entre si;

- Atualizar firmware CM
- Defina um certificado manu conhecido como confiável
- Recupere o serviço CM depois que um certificado Manu conhecido expirar
- Instalar um certificado Manu Expired desconhecido no cBR-8 e Marcar como confiável
- Permitir certificados CM expirados e certificados Manu a serem adicionados por AuthInfo com um comando CLI cBR-8

Note: Se o BPI for removido, isso desabilitará a criptografia e a autenticação, o que minimizará a viabilidade disso como uma solução alternativa.

Atualizar firmware CM

Em muitos casos, os fabricantes de CM fornecem atualizações de firmware CM que estendem a data final de validade do certificado Manu. Essa solução é a melhor opção e, quando executada antes da expiração do certificado Manu, evita os impactos relacionados ao serviço. Os CMs carregam o novo firmware e registram-se novamente com os novos certificados Manu e CM. Os novos certificados podem ser autenticados corretamente e os CMs podem se registrar com êxito no cBR-8. O novo certificado Manu e o certificado CM podem criar uma nova cadeia de certificados de volta ao certificado raiz conhecido já instalado no cBR-8.

Defina um certificado manu conhecido como confiável

Quando uma atualização de firmware CM não está disponível devido ao fato de um fabricante de CM ter deixado de funcionar, não há suporte adicional para um modelo CM, e assim por diante, os certificados Manu já conhecidos no cBR-8 com datas finais de validade no futuro próximo podem ser marcados proativamente como confiáveis no cBR-8 antes da data final de validade. Os comandos CLI cBR-8 e o SNMP são usados para identificar informações de certificado Manu, como número de série e estado confiável, e o SNMP é usado para definir o estado confiável do certificado Manu como confiável no cBR-8, o que permite que CMs associados se registrem e permaneçam em serviço.

Os certificados Manu conhecidos para CMs em serviço e on-line são normalmente aprendidos pelo cBR-8 de um CM através do protocolo DOCSIS Baseline Privacy Interface (BPI). A mensagem AuthInfo enviada do CM para o cBR-8 contém o certificado Manu. Cada certificado Manu exclusivo é armazenado na memória cBR-8 e suas informações podem ser visualizadas por comandos CLI cBR-8 e SNMP.

Quando o certificado Manu é marcado como confiável, isso faz duas coisas importantes. Primeiro, permite que o software BPI cBR-8 ignore a data de validade expirada. Segundo, armazena o certificado Manu como confiável na NVRAM cBR-8. Isso preserva o estado do certificado Manu em uma recarga do cBR-8 e elimina a necessidade de repetir esse procedimento no caso de uma recarga do cBR-8.

Os exemplos de comandos CLI e SNMP demonstram como identificar um índice de certificado Manu, um número de série e um estado de confiança; em seguida, use essas informações para alterar o estado confiável para confiável. Os exemplos se concentram no certificado Manu com índice 4 e número de série 437498F09A7DCBC1FA7AA101FE976E40.

Exibir informações de certificado Manu da CLI cBR-8

Neste exemplo, é usado o comando cBR-8 CLI **show cable privacy manufaturer-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
```

Veja as informações de certificado Manu com SNMP da CLI cBR-8

Neste exemplo, o comando cBR-8 CLI snmp get-bulk é usado. Cert Indices 4 e 5 são os Manu Certs armazenados na memória CMTS. Os índices 1, 2 e 3 são certificados raiz. Os certificados raiz não são a preocupação aqui, pois suas datas de expiração são muito mais longas.

```
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
```

Exibir informações de certificado manu com SNMP de um dispositivo remoto

Os exemplos de dispositivos remotos SNMP neste documento usam comandos SNMP de um servidor Linux Ubuntu remoto. Os comandos e formatos específicos do SNMP dependem do dispositivo e do sistema operacional usados para executar os comandos 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
```

Identifique a data de término da validade do certificado Manu na CLI

Use o comando CLI da placa de linha cBR-8 **show crypto pki certificate** para identificar a data de término da validade do certificado Manu. Esta saída de comando não inclui o Manu Cert Index. O Número de série do certificado pode ser usado para correlacionar as informações do certificado Manu aprendidas desse comando com as informações do certificado Manu obtidas do 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
```

Defina o estado de confiança do certificado Manu como confiável

Os exemplos mostram que o estado de confiança mudou de encadeado para confiável para o certificado Manu com índice = 4 e número de série = 437498f09a7dcbc1fa7aa101fe976e40

OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 valores:

1: confiável
2: não confiável
3: em cadeia
4: root

Este exemplo mostra o comando cBR-8 CLI snmp-set usado para alterar o estado de confiança

```
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)
```

Este exemplo mostra um dispositivo remoto que usa SNMP para alterar o estado de confiança

```
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)
```

Confirme as alterações do certificado Manu com o CLI cBR-8 ou com SNMP

- O valor de confiança mudou de encadeado para confiável
- O valor de origem foi alterado para SNMP, que indica que o certificado foi gerenciado pela última vez pelo SNMP e não pela Mensagem AuthInfo do Protocolo BPI

Este exemplo mostra o comando cBR-8 CLI usado para confirmar as alterações

```
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
...
```

Este exemplo mostra um dispositivo remoto que usa SNMP para confirmar as alterações

```
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)
```

Recupere o serviço CM depois que um certificado Manu conhecido expirar

Um certificado Manu conhecido anteriormente já está presente no banco de dados cBR-8, normalmente como resultado de mensagens AuthInfo de registro CM anterior. Se um certificado Manu não estiver marcado como fidedigno e expirar, qualquer CM que utilize o certificado Manu expirado e fique offline não poderá registrar novamente e está marcado como reject(pk). Esta seção descreve como se recuperar dessa condição e permite que CMs com certificados Manu expirados se registrem e permaneçam em serviço.

Quando os CMs não ficam on-line e são marcados como reject(pk) como resultado de certificados Manu expirados, uma mensagem de syslog é gerada e contém o endereço MAC CM e o número de série do certificado Manu expirado.

Identificar o número de série do certificado Manu expirado a partir da mensagem de 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
```

Identifique o índice do certificado Manu expirado e defina o estado de confiança do certificado

Manu como confiável

Este exemplo mostra os comandos SNMP CLI cBR-8 usados para identificar o índice para o número de série do certificado Manu da mensagem de log, que é então usado para definir o estado confiável do certificado Manu como confiável.

```
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)
```

Este exemplo mostra que um dispositivo remoto usa comandos SNMP para identificar o índice do número de série do certificado Manu da mensagem de registro, que é então usado para definir o estado confiável do certificado Manu como confiável.

```
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)
```

Instalar um certificado Manu Expired desconhecido no cBR-8 e Marcar como confiável

Quando um certificado Manu expirado não é conhecido pelo cBR-8, ele não pode ser gerenciado (marcado como confiável) antes da expiração e não pode ser recuperado. Isso acontece quando um CM anteriormente desconhecido e não registrado em um cBR-8 tenta se registrar com um certificado Manu desconhecido e expirado. O certificado Manu deve ser adicionado ao cBR-8 por SNMP a partir de um dispositivo remoto ou usar a configuração da interface de cabo **cable privacy retfail-certificate** cBR-8 para permitir que um certificado Manu expirado seja adicionado por AuthInfo. Os comandos SNMP da CLI do cBR-8 não podem ser usados para adicionar um certificado porque o número de caracteres nos dados do certificado excede o máximo de caracteres aceitos pela CLI. Se um certificado autoassinado for adicionado, o comando **cable privacy accept-self-signed-certificate** deverá ser configurado na interface de cabo cBR-8 antes que o cBR-8 possa aceitar o certificado.

Adicione um certificado Manu expirado ao cBR-8 com SNMP

Use estes valores OID docsBpi2CmtsCACertTable para adicionar o certificado Manu como uma nova entrada de tabela. O valor hexadecimal do certificado Manu definido pelo OID docsBpi2CmtsCACert pode ser aprendido com as etapas de despejo do certificado CA descritas no artigo de suporte Como decodificar o certificado DOCSIS para o diagnóstico de estado de pilha de 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)
```

Use um número de índice exclusivo para o certificado Manu adicionado. Os índices dos certificados Manu já presentes no cBR-8 podem ser verificados com o comando **show cable privacy manufaturer-cert-list**.

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

Os exemplos nesta seção usam um valor de índice de 11 para o certificado Manu adicionado ao banco de dados cBR-8.

> **Tip**: Sempre defina os atributos de CertStatus antes dos dados de certificado reais. Caso contrário, o CMTS assume que o certificado está encadeado e tenta verificá-lo imediatamente com os fabricantes e os certificados raiz.

Alguns sistemas operacionais não podem aceitar linhas de entrada que sejam o tempo necessário para inserir a sequência de dados hexadecimal que especifica um certificado. Por esse motivo, um gerenciador de SNMP gráfico pode ser usado para definir esses atributos. Para vários certificados, um arquivo de script pode ser usado, se mais conveniente.

Este exemplo mostra um dispositivo remoto que usa SNMP para adicionar um certificado de certificado Manu ao cBR-8. A maioria dos dados do certificado é omitida para leitura, indicada por elipses (...).

```
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
```

Permitir que um certificado Manu expirado seja adicionado por AuthInfo com um comando CLI cBR-8

Um certificado Manu normalmente insere o banco de dados cBR-8 pela mensagem BPI Protocol AuthInfo enviada ao cBR-8 do CM. Cada certificado Manu exclusivo e válido recebido em uma mensagem AuthInfo é adicionado ao banco de dados. Se o certificado Manu for desconhecido do CMTS (não no banco de dados) e tiver expirado as datas de validade, AuthInfo será rejeitado e o certificado Manu não será adicionado ao banco de dados cBR-8. Um certificado Manu expirado pode ser adicionado ao CMTS pela troca AuthInfo quando a configuração alternativa **dos certificados retardados do cabo** estiver presente na configuração da interface de cabo cBR-8. Isso permite a adição do certificado Manu expirado ao banco de dados cBR-8 como não confiável. Para usar o certificado Manu expirado, o SNMP deve ser usado para marcá-lo como confiável.

Quando o certificado Manu expirado é adicionado ao cBR-8 e marcado como confiável, a remoção da configuração **de certificados retardados de privacidade do cabo** é recomendada para que certificados Manu adicionais, potencialmente indesejados, não entrem no 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
```

Permitir certificados CM expirados e certificados Manu a serem adicionados por AuthInfo com um comando CLI cBR-8

Um certificado CM expirado pode ser adicionado ao CMTS pela troca AuthInfo quando ambos os comandos **cable privacy retfail-certificate** e **cable privacy skip-valid-period** são configurados em cada interface de cabo relevante. Isso faz com que o cBR-8 ignore as verificações da data de validade expirada para TODOS os certificados CM e Manu enviados na mensagem CM BPI AuthInfo. Quando os certificados CM e Manu expirados são adicionados ao cBR-8 e marcados como confiáveis, a remoção da configuração descrita é recomendada para que os certificados adicionais, potencialmente indesejados, não entrem no sistema.

```
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
```

Additional Information

Consideração de configuração de interface de cabo/domínio MAC

Os comandos de configuração **cable privacy retfail-certificate** e **cable privacy skip-valid-period** são usados no nível de domínio MAC / interface de cabo e não são restritivos. O comando reter certificados com falha pode adicionar qualquer certificado com falha ao banco de dados cBR-8 e o comando skip-valid-period pode ignorar as verificações de data de validade em todos os certificados Manu e CM.

Consideração do tamanho do pacote SNMP

Um SNMP get para dados de Cert pode retornar um valor NULL se o Cert OctetString for maior que o tamanho do pacote SNMP. Uma configuração de SNMP cBR-8 pode ser usada quando certificados de grande porte são usados;

```
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
```

Depuração de certificado Manu

O debug do certificado Manu no cBR-8 é suportado com os comandos **debug cable privacy ca-cert** e **debug cable mac-address <CM mac-address>**. Informações adicionais de depuração são explicadas no artigo de suporte Como decodificar o certificado DOCSIS para o diagnóstico de estado de pilha de modem. Isso inclui as etapas de despejo de certificado CA usadas para aprender o valor hexadecimal de um certificado Manu.

Documentação de suporte relacionada

- O DOCSIS 1.1 para os Cisco CMTS Routers fornece informações adicionais sobre o suporte cBR-8 e a configuração da DOCSIS Baseline Privacy Interface (BPI+).
- A Referência de Comandos de Cabo do Cisco CMTS fornece informações sobre os comandos CLI do cBR-8 referenciados neste documento.
- Trabalhe em conjunto e Recupere certificados de fabricantes expirados em uBR10K fornece informações semelhantes a este documento para o uBR10K CMTS.
- Suporte Técnico e Documentação - Cisco Systems