Solution et récupération des certificats de fabricant expirés sur cBR-8

Contenu

Introduction

Ce document décrit les options permettant d'empêcher, de contourner et de récupérer les impacts du service de rejet de modem câble (CM) sur le système CMTS (Cable Modem Termination System) cBR-8 résultant de l'expiration du certificat de fabricant (Manu Cert).

Problème

Il y a différentes causes pour qu'un CM soit coincé dans l'état de rejet (pk) sur le cBR-8. L'une des causes est l'expiration du certificat Manu. Le certificat Manu est utilisé pour l'authentification entre un CM et un CMTS. Dans ce document, un certificat Manu est ce que la spécification de sécurité DOCSIS 3.0 CM-SP-SECv3.0 désigne comme certificat d'autorité de certification Mfg CableLabs ou certificat d'autorité de certification Fabricant. Expire signifie que la date/heure système cBR-8 dépasse la date/heure de fin de validité du certificat Manu.

Un CM qui tente de s'enregistrer auprès du cBR-8 après l'expiration du certificat Manu est marqué comme rejeté (pk) par le CMTS et n'est pas en service. Un CM déjà enregistré avec le cBR-8 et en service à l'expiration du certificat Manu peut rester en service jusqu'à la prochaine tentative d'enregistrement du CM, qui peut se produire après un événement hors ligne CM unique, le redémarrage de la carte de ligne câblée cBR-8, le rechargement cBR-8 ou tout autre événement déclenche l'enregistrement du CM. À ce moment-là, le CM échoue à l'authentification, est marqué rejet(pk) par le cBR-8 et n'est pas en service.

Les informations contenues dans ce document sont développées et reformater le contenu publié dans le Bulletin des produits sur les modems câble et les certificats de fabricant arrivant à expiration dans cBR-8.

> **Note**: ID de bogue Cisco CSCvv21785 ; Dans certaines versions de Cisco IOS XE, ce bogue provoque l'échec de validation d'un certificat Manu approuvé après un rechargement cBR-8. Dans certains cas, le Cert Manu est présent mais n'est plus dans l'état de confiance. Dans ce cas, l'état d'approbation Cert Manu peut être modifié pour être approuvé avec les étapes décrites dans ce document. Si le certificat Manu n'est pas présent dans la sortie de la commande show cable privacy maker-cert-list, le certificat Manu peut être réajouté manuellement ou par AuthInfo avec les étapes décrites dans ce document.

Informations sur le certificat Manu

Les informations de certificat Manu peuvent être affichées via des commandes CLI cBR-8 ou des commandes SNMP (Simple Network Management Protocol) à partir d'un périphérique distant. L'interface de ligne de commande cBR-8 prend également en charge les commandes SNMP set, get et get-vrac. Ces commandes et informations sont utilisées par les solutions décrites dans ce document.

Champs et attributs des informations de certification Manu

- Index : Entier unique attribué à chaque certificat Manu dans la base de données/MIB cBR-8
- Objet : Nom du sujet tel qu'il est codé dans le certificat X509
  cn : NomCommunou : Unité d'organisationo : Organisationl : Localités :
  NomProvinceOuÉtatc : NomPays
- Émetteur : L'autorité de certification
- Série : Numéro de série de certificat représenté dans une chaîne d'octet hexadécimale
- Province: Statut d'approbation du certificat
  fiablenon fiableen chaîneracine
- Source : Comment le certificat a atteint le CMTS
  snmp fichierConfigurationexternalDatabaseother (autre)authentInfocompiléInfoCode
- Status/RowStatus : État du certificat
  actifnonEnServicenon prêtcreateAndGocréer et attendredétruire

- Cert : Le certificat d'autorité de certification encodé en DER X509
- Date de validité : Les dates de début et de fin qui définissent la période de validité du certificat Manu par rapport à la date et à l'heure système CMTS
  date de début : Date et heure auxquelles le certificat Manu devient validedate de fin : Date et heure auxquelles le certificat Manu n'est plus valide
- Cert : Le certificat d'autorité de certification encodé en DER X509
- Empreinte numérique : Hachage SHA-1 d'un certificat CA

Commandes CLI cBR-8

Les informations Manu Cert peuvent être affichées à l'aide de ces commandes CLI cBR-8.

- Àpartir du mode d'exécution CLI cBR-8 ou du mode d'exécution CLI de la carte de ligne : CBR8-1**#show cable privacy maker-cert-list**
- En mode d'exécution CLI de la carte de ligne cBR-8 : Slot-6-0**#show crypto pki certificate**

Ces commandes SNMP Cisco IOS® XE sont utilisées à partir de l'interface de ligne de commande cBR-8 pour obtenir et définir des OID SNMP.

- snmp get
- snmp get-vrac
- les opérations SNMP SET

Ces commandes de configuration d'interface de câble cBR-8 sont utilisées pour les contournements et la récupération décrits dans la section Solution de ce document.

- cable privacy keep-fail-certificate
- cable privacy skip-validité-periode

OID DOCSIS-BPI-PLUS-MIB

Les informations de certificat manu sont définies dans la branche OID docsBpi2CmtsCACertEntry 1.3.6.1.2.1.10.127.6.1.2.5.2.1, décrite dans le Navigateur d'objets SNMP.

OID SNMP pertinents

```
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
```

Dans les exemples de commandes, l'ellipse (...) indique que certaines informations ont été omises pour être lisibles.

Solution

La mise à jour du micrologiciel CM est la meilleure solution à long terme. Les solutions décrites dans ce document permettent aux modems modems titulaires de certificats Manu expirés de

s'enregistrer et de rester en ligne avec le cBR-8, mais ces solutions ne sont recommandées que pour une utilisation à court terme. Si une mise à jour du micrologiciel CM n'est pas une option, une stratégie de remplacement CM est une bonne solution à long terme du point de vue de la sécurité et des opérations. Les solutions décrites ici traitent de conditions ou de scénarios différents et peuvent être utilisées individuellement ou, dans certains cas, en association ;

- Mettre à jour le micrologiciel CM
- Définir un certificat Manu connu sur Trusted
- Récupérer le service CM après l'expiration d'un certificat Manu connu
- Installer un certificat Manu périmé inconnu sur le cBR-8 et Mark Trusted
- Autoriser l'ajout par AuthInfo de certificats CM expirés et de certificats manu avec une commande CLI cBR-8

  Note: Si le BPI est supprimé, cela désactive le chiffrement et l'authentification, ce qui réduit la viabilité de cette solution de contournement.

Mettre à jour le micrologiciel CM

Dans de nombreux cas, les fabricants de CM fournissent des mises à jour du micrologiciel de CM qui prolongent la date de fin de validité du certificat Manu. Cette solution est la meilleure option et, lorsqu'elle est exécutée avant l'expiration d'un certificat Manu, elle prévient les impacts de services associés. Les CM chargent le nouveau micrologiciel et se réinscrivent avec les nouveaux certificats Manu et CM. Les nouveaux certificats peuvent s'authentifier correctement et les CM peuvent s'enregistrer avec succès auprès du cBR-8. Le nouveau certificat Manu et le nouveau certificat CM peuvent créer une nouvelle chaîne de certificats vers le certificat racine connu déjà installé dans le cBR-8.

Définir un certificat Manu connu sur Trusted

Lorsqu'une mise à jour du micrologiciel CM n'est pas disponible en raison d'une interruption de l'activité d'un fabricant CM, qu'aucun autre support pour un modèle CM, etc., les certificats Manu déjà connus sur le cBR-8 avec des dates de fin de validité dans un avenir proche peuvent être marqués de manière proactive comme approuvés dans le cBR-8 avant la date de fin de validité. Les commandes CLI cBR-8 et SNMP sont utilisées pour identifier les informations de certificat Manu telles que le numéro de série et l'état d'approbation, et SNMP est utilisé pour définir l'état d'approbation de certificat Manu sur approuvé dans le cBR-8, ce qui permet aux CM associés de s'enregistrer et de rester en service.

Les certificats Manu connus pour les CM actuellement en service et en ligne sont généralement appris par le cBR-8 à partir d'un CM via le protocole BPI (Baseline Privacy Interface) DOCSIS. Le message AuthInfo envoyé par le CM au cBR-8 contient le certificat Manu. Chaque certificat Manu unique est stocké dans la mémoire cBR-8 et ses informations peuvent être affichées par les commandes CLI cBR-8 et SNMP.

Lorsque le certificat Manu est marqué comme étant fiable, cela fait deux choses importantes. Tout d'abord, il permet au logiciel BPI cBR-8 d'ignorer la date de validité expirée. Deuxièmement, il stocke le certificat Manu comme approuvé dans la mémoire NVRAM cBR-8. Cela préserve l'état de Cert Manu sur un rechargement cBR-8 et élimine la nécessité de répéter cette procédure en cas de rechargement cBR-8.

Les exemples de commandes CLI et SNMP montrent comment identifier un index de certificat

Manu, un numéro de série et un état d'approbation ; ensuite, utilisez ces informations pour modifier l'état d'approbation en approuvé. Les exemples portent sur le certificat Manu avec index 4 et numéro de série 437498F09A7DCBC1FA7AA101FE976E40.

Afficher les informations de certification Manu à partir de l'interface de ligne de commande cBR-8

Dans cet exemple, la commande CLI cBR-8 **show cable privacy maker-cert-list** est utilisée.

```
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
```

Afficher les informations de certification Manu avec SNMP à partir de l'interface de ligne de commande cBR-8

Dans cet exemple, la commande CLI cBR-8 snmp get-vrac est utilisée. Les indices de certification 4 et 5 sont les certificats Manu stockés dans la mémoire CMTS. Les indices 1, 2 et 3 sont des certificats racine. Les certificats racines ne sont pas concernés ici car leurs dates d'expiration sont beaucoup plus longues.

```
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
```

Afficher les informations de certification Manu avec SNMP à partir d'un périphérique distant

Les exemples SNMP de périphérique distant dans ce document utilisent des commandes SNMP provenant d'un serveur Ubuntu Linux distant. Les commandes et formats SNMP spécifiques dépendent du périphérique et du système d'exploitation utilisés pour exécuter les commandes 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
```

Identifier la date de fin de validité du certificat Manu dans l'interface de ligne de commande

Utilisez la commande CLI cBR-8 linecard **show crypto pki certificate** pour identifier la date de fin de validité du certificat Manu. Cette sortie de commande n'inclut pas l'index de certificat Manu. Le numéro de série du certificat peut être utilisé pour corréler les informations de certificat Manu apprises à partir de cette commande avec les informations de certificat Manu apprises à partir du protocole 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
```

Définir l'état d'approbation du certificat Manu sur Fiable

Les exemples montrent que l'état d'approbation est passé de chaîné à approuvé pour le certificat Manu avec Index = 4 et Numéro de série = 437498f09a7dcbc1fa7aa101fe976e40

OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 valeurs :

1: fiable
2: non fiable
3: en chaîne
4: racine

Cet exemple montre la commande snmp-set de l'interface de ligne de commande cBR-8 utilisée pour modifier l'état d'approbation

```
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)
```

Cet exemple montre comment un périphérique distant utilise SNMP pour modifier l'état d'approbation

```
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)
```

Confirmer les modifications de certificat Manu avec l'interface de ligne de commande cBR-8 ou avec SNMP

- La valeur d'approbation est passée de chaîne à confiance
- La valeur source est passée à SNMP, ce qui indique que le certificat a été géré pour la dernière fois par SNMP et non à partir du message AuthInfo du protocole BPI.

Cet exemple montre la commande CLI cBR-8 utilisée pour confirmer les modifications

```
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
...
```

Cet exemple montre comment un périphérique distant utilise SNMP pour confirmer les modifications

```
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)
```

Récupérer le service CM après l'expiration d'un certificat Manu connu

Un certificat Manu précédemment connu est un certificat déjà présent dans la base de données cBR-8, généralement à la suite de messages AuthInfo provenant d'un enregistrement CM précédent. Si un certificat Manu n'est pas marqué comme approuvé et expire, tout CM qui utilise le certificat Manu expiré et qui se déconnecte ne peut pas se réenregistrer et est marqué comme rejeté(pk). Cette section décrit comment se rétablir de cette condition et permettre aux CM ayant des certificats Manu expirés de s'enregistrer et de rester en service.

Lorsque les CM ne parviennent pas à se connecter et sont marqués comme rejetés (pk) en raison de certificats manu expirés, un message syslog est généré et contient l'adresse MAC CM et le numéro de série du certificat manu expiré.

Identifier le numéro de série du certificat Manu expiré à partir du message du journal 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
```

Identifiez l'index du certificat Manu expiré et définissez l'état de confiance du certificat Manu sur Fisted

Cet exemple montre les commandes SNMP de l'interface de ligne de commande cBR-8 utilisées pour identifier l'index du numéro de série du certificat Manu à partir du message journal, qui est ensuite utilisé pour définir l'état d'approbation du certificat Manu sur approuvé.

```
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)
```

Cet exemple montre qu'un périphérique distant utilise des commandes SNMP pour identifier l'index du numéro de série du certificat Manu à partir du message de journal, qui est ensuite utilisé pour définir l'état d'approbation du certificat Manu sur approuvé.

```
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)
```

Installer un certificat Manu périmé inconnu sur le cBR-8 et Mark Trusted

Lorsqu'un certificat Manu expiré n'est pas connu du cBR-8, il ne peut pas être géré (marqué comme approuvé) avant expiration et ne peut pas être récupéré. Cela se produit lorsqu'un CM qui est précédemment inconnu et qui n'est pas enregistré sur un cBR-8 tente de s'enregistrer avec un certificat Manu inconnu et expiré. Le certificat Manu doit être ajouté au cBR-8 par SNMP à partir d'un périphérique distant ou utiliser la configuration d'interface **de câble** cBR-8 de **rétention des certificats de confidentialité des câbles** pour permettre l'ajout d'un certificat Manu expiré par AuthInfo. Les commandes SNMP de l'interface de ligne de commande cBR-8 ne peuvent pas être utilisées pour ajouter un certificat, car le nombre de caractères dans les données du certificat dépasse le nombre maximal de caractères acceptés par l'interface de ligne de commande. Si un certificat auto-signé est ajouté, la commande **cable privacy accept-self-signed-certificate** doit être configurée sous l'interface de câble cBR-8 avant que le cBR-8 puisse accepter le certificat.

Ajouter un certificat Manu expiré au cBR-8 avec SNMP

Utilisez ces valeurs OID docsBpi2CmtsCACertTable pour ajouter le certificat Manu comme nouvelle entrée de table. La valeur hexadécimale du certificat Manu défini par l'OID docsBpi2CmtsCACert peut être apprise avec les étapes de vidage du certificat CA décrites dans l'article de support Comment décoder le certificat DOCSIS pour le diagnostic d'état de blocage du 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)
```

Utilisez un numéro d'index unique pour le certificat Manu ajouté. Les indices des certificats Manu déjà présents sur le cBR-8 peuvent être vérifiés à l'aide de la commande **show cable privacy maker-cert-list**.

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

Les exemples de cette section utilisent une valeur d'index de 11 pour le certificat Manu ajouté à la base de données cBR-8.

> **Astuce** : Définissez toujours les attributs CertStatus avant les données de certificat réelles. Sinon, le CMTS suppose que le certificat est chaîné et tente immédiatement de le vérifier auprès des fabricants et des certificats racine.

Certains systèmes d'exploitation ne peuvent pas accepter les lignes d'entrée aussi longues que nécessaire pour entrer la chaîne de données hexadécimale qui spécifie un certificat. Pour cette raison, un gestionnaire SNMP graphique peut être utilisé pour définir ces attributs. Pour un certain nombre de certificats, un fichier de script peut être utilisé, si cela est plus pratique.

Cet exemple montre comment un périphérique distant utilise SNMP pour ajouter un certificat Manu au cBR-8. La plupart des données de certificat sont omises pour lisibilité, indiquées par des lettres (...).

```
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
```

Autoriser l'ajout d'un certificat Manu expiré par AuthInfo avec une commande CLI cBR-8

En règle générale, un certificat Manu entre dans la base de données cBR-8 par le message AuthInfo du protocole BPI envoyé à cBR-8 à partir du CM. Chaque certificat Manu unique et valide reçu dans un message AuthInfo est ajouté à la base de données. Si le certificat Manu est inconnu du CMTS (non dans la base de données) et a expiré, AuthInfo est rejeté et le certificat Manu n'est pas ajouté à la base de données cBR-8. Un certificat Manu expiré peut être ajouté au CMTS par l'échange AuthInfo lorsque la configuration de contournement des certificats **de rétention de la confidentialité des câbles** est présente dans la configuration d'interface de câble cBR-8. Cela

permet d'ajouter le certificat Manu expiré à la base de données cBR-8 comme non approuvé. Pour utiliser le certificat Manu expiré, SNMP doit être utilisé pour le marquer comme fiable. Lorsque le certificat Manu expiré est ajouté au cBR-8 et marqué comme approuvé, la suppression de la configuration **cable privacy keep-fail-certificate** est recommandée de sorte que les certificats Manu supplémentaires, potentiellement indésirables, ne pénètrent pas dans le système.

```
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
```

Autoriser l'ajout par AuthInfo de certificats CM expirés et de certificats manu avec une commande CLI cBR-8

Un certificat CM expiré peut être ajouté au CMTS par l'échange AuthInfo lorsque les commandes **cable privacy keep-fail-certificate** et **cable privacy skip-validité-période** sont configurées sous chaque interface de câble appropriée. Cela fait que cBR-8 ignore les vérifications de date de validité expirées pour TOUS les certificats CM et manu envoyés dans le message AuthInfo BPI CM. Lorsque les certificats CM et Manu expirés sont ajoutés au cBR-8 et marqués comme approuvés, la suppression de la configuration décrite est recommandée de sorte que les certificats supplémentaires, potentiellement indésirables, n'entrent pas dans le système.

```
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

Examen de la configuration des interfaces de domaine/câble MAC

Les commandes de configuration **cable privacy keep-fail-certificate** et **cable privacy skip-validité-période** sont utilisées au niveau du domaine MAC / interface de câble et ne sont pas restrictives. La commande keep-fail-certificate peut ajouter n'importe quel certificat défaillant à la base de données cBR-8 et la commande skip-validité-période peut ignorer les vérifications de date de validité sur tous les certificats Manu et CM.

Prise en compte de la taille des paquets SNMP

Une requête SNMP get for Cert data peut renvoyer une valeur NULL si Cert OctetString est supérieur à la taille de paquet SNMP. Une configuration SNMP cBR-8 peut être utilisée lorsque des certificats de grande taille sont utilisés ;

```
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
```

Débogage du certificat Manu

Manu Cert debug sur cBR-8 est pris en charge avec les commandes **debug cable privacy ca-cert** et **debug cable mac-address <CM mac-address>**. Des informations de débogage supplémentaires sont expliquées dans l'article de support How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis. Cela inclut les étapes de vidage de certificat CA utilisées pour apprendre la valeur hexadécimale d'un certificat Manu.

Documentation d'assistance associée

- DOCSIS 1.1 pour les routeurs CMTS Cisco fournit des informations supplémentaires sur la prise en charge et la configuration de l'interface de confidentialité de ligne de base (BPI+) DOCSIS.
- Cisco CMTS Cable Command Reference fournit des informations sur les commandes CLI cBR-8 référencées dans ce document.
- Work Around and Recover Expired Manufacturer Certificates on uBR10K fournit des informations similaires à celles de ce document pour le CMTS uBR10K.
- Support et documentation techniques - Cisco Systems