Solution et récupération des certificats de fabricant expirés sur uBR10K

Table des matières

- Introduction
- Problème
  - Informations sur le certificat Manu
    - Champs et attributs des informations de certification Manu
    - Commandes CLI uBR10K
    - OID DOCSIS-BPI-PLUS-MIB
- Solution
  - Mettre à jour le microprogramme CM
  - Définir un certificat Manu connu sur Approuvé
    - Afficher les nombreuses informations de certification de l'interface de ligne de commande uBR10K
    - Afficher les informations de certification du manuel avec SNMP à partir d'un périphérique distant
    - Définissez l'état d'approbation de certificat Manu connu expiré sur Approuvé avec SNMP
    - Confirmez que le certificat Manu a été modifié avec l'interface de ligne de commande uBR10K ou avec SNMP
  - Récupérer le service CM après expiration d'un certificat Manu connu
    - Identifier le numéro de série connu expiré du certificat Manu
    - Identifiez l'index du certificat Manu connu arrivé à expiration et définissez l'état d'approbation du certificat Manu sur Approuvé
  - Installez un certificat Manu expiré inconnu sur l'uBR10K et marquez-le comme approuvé
    - Ajout d'un certificat Manu inconnu expiré à l'uBR10K avec SNMP
    - Ajouter un certificat Manu expiré lors de l'enregistrement CM dans l'interface de ligne de commande
  - Autoriser l'ajout de certificats CM et Manu expirés par AuthInfo avec une commande CLI uBR10K
  - Additional Information
    - Considérations relatives à la configuration du domaine MAC/de l'interface câble
    - Considération de la taille des paquets SNMP
    - Débogage du certificat Manu
    - Documentation d'assistance associée

Introduction

Ce document décrit les options permettant d'empêcher, de contourner et de récupérer les impacts du service de rejet (pk) du modem câble (CM) sur le CMTS (Cable Modem Termination System) uBR10K résultant de l'expiration du certificat du fabricant (Manu Cert).

Problème

Il existe différentes causes pour qu'un CM soit bloqué dans l'état de rejet (pk) sur l'uBR10K. 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 appelle le certificat CA de fabrication CableLabs ou le certificat CA de fabricant. Expire signifie que la date/heure système du uBR10K dépasse la date/heure de fin de validité du certificat Manu.

Un CM qui tente de s'enregistrer auprès de l'uBR10K après l'expiration de la certification Manu est marqué comme reject(pk) par le CMTS et n'est pas en service. Un CM déjà enregistré avec l'uBR10K et en service à l'expiration du certificat Manu peut rester en service jusqu'à la prochaine tentative d'enregistrement du CM, ce qui peut se produire après un seul événement de modem hors ligne, un redémarrage de la carte de ligne câblée uBR10K, un rechargement de l'uBR10K ou d'autres événements qui déclenchent l'enregistrement du modem. À ce moment, le CM échoue l'authentification, est marqué comme rejeté (pk) par l'uBR10K et n'est pas en service.

DOCSIS 1.1 pour les routeurs Cisco CMTS fournit des informations supplémentaires sur la prise en charge et la configuration d'uBR10K de l'interface DOCSIS BPI+ (Baseline Privacy Interface).

Informations sur le certificat Manu

Les informations relatives à la certification Manu peuvent être consultées via les commandes CLI uBR10K ou le protocole SNMP (Simple Network Management Protocol). 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 uBR10K

- Objet : Le nom du sujet exactement tel qu'il est codé dans le certificat X509
    - nc : NomCommun
    - ou : UnitéOrganisationnelle
    - o : Organisation
    - l : Localité
    - s : NomÉtatOuProvince
    - c : NomPays
- Émetteur : L'autorité de certification
- Série : Numéro de série du certificat représenté dans une chaîne d’octets hexadécimale
- Province: État de confiance du certificat
    - de confiance
    - non fiable
    - en chaîne
    - racine
- Source : Comment le certificat a atteint le CMTS
    - snmp
    - fichierConfiguration
    - base de données externe
    - other (autre)

    - authentInfo
    - codeInfoCompilé
- État/ÉtatLigne : État du certificat
    - actif
    - non en service
    - non prêt
    - CréerEtAtteindre
    - createandWait
    - détruire
- Cert : Le certificat de l'autorité de certification codé 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 valide
    - date de fin : Date et heure auxquelles le certificat Manu n'est plus valide
- Cert : Le certificat de l'autorité de certification codé DER X509
- Empreinte numérique : Hachage SHA-1 d'un certificat CA

Commandes CLI uBR10K

Le résultat de cette commande inclut des informations sur la certification Manu. L'index de certificat Manu ne peut être obtenu que par SNMP

- À partir du mode d'exécution CLI uBR10K ou du mode d'exécution CLI Linecard : uBR10K#show cable privacy fabricant-cert-list
- En mode d'exécution CLI de la carte de ligne uBR10K : Slot-6-0#show crypto pki certificates

Ces commandes de configuration d'interface de câble sont utilisées pour les solutions de contournement et la récupération

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

OID DOCSIS-BPI-PLUS-MIB

Les informations de certification de manuel 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.

Remarque : Dans le logiciel uBR10k, la RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB a été implémentée avec la branche/le chemin de MIB OID incorrect. La plate-forme uBR10k n'est plus commercialisée et n'est plus prise en charge. Il n'y a donc pas de solution à ce problème. Au lieu du chemin MIB/branche 1.3.6.1.2.10.127.6 attendu, le chemin MIB/branche 1.3.6.1.2.1.9999 doit être utilisé pour les interactions SNMP avec les MIB/OID BPI2 sur l'uBR10k.
ID de bogue Cisco associé CSCum28486

Il s'agit des équivalents de chemin d'accès complet de l'OID MIB BPI2 pour les informations de certification Manu sur l'uBR10k comme indiqué dans le bogue Cisco ID 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
```

Les exemples de commandes de ce document utilisent des points de suspension (...) pour indiquer que certaines informations ont été omises pour des raisons de lisibilité.

Solution

La mise à jour du microprogramme CM est la meilleure solution à long terme. Les solutions de contournement qui permettent aux CM possédant des certificats Manu expirés de s'enregistrer et de rester en ligne avec l'uBR10K sont décrites dans ce document, mais ces solutions de contournement ne sont recommandées que pour une utilisation à court terme. Si la mise à jour du microprogramme 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 concernent différentes conditions ou scénarios et peuvent être utilisées individuellement ou, pour certaines, en combinaison les unes avec les autres ;

- Mettre à jour le microprogramme CM
- Définir un certificat Manu connu sur Approuvé
- Récupérer le service CM après expiration d'un certificat Manu connu
- Installez un certificat Manu expiré inconnu sur l'uBR10k et marquez-le comme approuvé
- Autoriser l'ajout de certificats CM et Manu expirés par AuthInfo avec une commande CLI uBR10K

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

Mettre à jour le microprogramme CM

Dans de nombreux cas, les fabricants de produits CM fournissent des mises à jour de microprogramme 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 empêche les impacts de service associés. Les CM chargent le nouveau micrologiciel et se réenregistrent avec les nouveaux certificats Manu et CM. Les nouveaux certificats peuvent s'authentifier

correctement et les CM peuvent s'enregistrer avec succès auprès de l'uBR10K. Les nouveaux certificats Manu Cert et CM Cert peuvent recréer une nouvelle chaîne de certificats à partir du certificat racine connu déjà installé dans l'uBR10K.

Définir un certificat Manu connu sur Approuvé

Lorsqu'une mise à jour du micrologiciel CM n'est pas disponible en raison d'une cessation d'activité d'un fabricant CM, de l'absence de prise en charge d'un modèle CM, etc., les certificats Manu déjà connus sur l'uBR10k avec des dates de fin de validité dans un avenir proche peuvent être marqués de manière proactive comme approuvés dans l'uBR10k avant l'expiration. Le numéro de série, la date de fin de validité et l'état du certificat Manu sont disponibles avec les commandes CLI uBR10K. Le numéro de série, l'état de confiance et l'index du certificat Manu sont disponibles avec SNMP.

Les certifications Manu connues pour les modems actuellement en service et en ligne sont généralement acquises par l'uBR10K à partir d'un CM via le protocole DOCSIS Baseline Privacy Interface (BPI). Le message AUTH-INFO envoyé par le CM à l'uBR10K contient le certificat Manu. Chaque certificat Manu unique est stocké dans la mémoire uBR10K et ses informations peuvent être consultées avec les commandes CLI uBR10K et SNMP.

Lorsque le certificat Manu est marqué comme fiable, cela fait deux choses importantes. Tout d'abord, il permet au logiciel BPI uBR10K d'ignorer la date de validité expirée. Ensuite, il stocke le certificat Manu comme étant de confiance dans la mémoire NVRAM uBR10K. Cela permet de conserver l'état de certification Manu sur un rechargement uBR10K et d'éviter de répéter cette procédure en cas de rechargement uBR10K

Les exemples de commandes CLI et SNMP montrent comment identifier un index de certificat Manu, un numéro de série, un état de confiance ; utilisez ensuite ces informations pour passer de l'état d'approbation à approuvé. Les exemples portent sur un certificat Manu portant l'index 5 et le numéro de série 45529C2654797E1623C6E723180A9E9C.

Afficher les nombreuses informations de certification de l'interface de ligne de commande uBR10K

Dans cet exemple, les commandes CLI uBR10K show crypto pki certificates et show cable privacy constructeur-cert-list sont utilisées pour afficher les informations de certification Manu connues.

<#root>

```
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 Inte
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris Interac
State: Chained  <-- Cert Trust State is Chained


Source: Auth Info    <-- CertSource is Auth Info


RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C  <-- Serial Number


Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

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

OID SNMP uBR10K pertinents :

```
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
```

Dans cet exemple, la commande snmpwalk est utilisée pour afficher des informations dans la

table de certification du manuel uBR10k. Le numéro de série connu du certificat Manu peut être mis en corrélation avec l'index du certificat Manu, qui peut être utilisé pour définir l'état de confiance. Les commandes et formats SNMP spécifiques dépendent du périphérique et du système d'exploitation utilisés pour exécuter la commande/requête SNMP.

<#root>

```
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 <-- S


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)
```

Définissez l'état d'approbation de certificat Manu connu expiré sur Approuvé avec SNMP

Valeurs pour OID : docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (l'OID sur uBR10k est 1.3.6.1.2.1.999.1.2.5.2.1.5)

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

L'exemple montre l'état d'approbation qui est passé de l'état enchaîné à l'état approuvé pour le certificat Manu avec l'index = 5 et le numéro de série = 45529C2654797E1623C6E723180A9E9C.

<#root>

```
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
```

Confirmez que le certificat Manu a été modifié avec l'interface de ligne de commande uBR10K ou avec SNMP

- La valeur d'approbation est passée de « enchaîné » à « Approuvé »
- La valeur source a changé en « SNMP », ce qui indique que le certificat a été géré en dernier par SNMP et non à partir du message BPI Protocol AuthInfo

<#root>

```
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 <-- S

...
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 Inte
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris Interac
State: Trusted

Source: SNMP

RowStatus: Active
```

Serial: 45529C2654797E1623C6E723180A9E9C

Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

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

Un certificat Manu précédemment connu est un certificat déjà présent dans la base de données uBR10K, généralement à la suite de messages AuthInfo d'un enregistrement CM précédent. Si un certificat Manu n'est pas marqué comme étant approuvé et que le certificat expire, tous les CM qui utilisent le certificat Manu expiré peuvent ensuite passer hors ligne et tenter de s'enregistrer, mais le uBR10K les marque comme étant rejetés (pk) et ils ne sont pas en service. Cette section décrit comment récupérer de cette condition et permettre aux CM avec des certificats Manu expirés de s'enregistrer et de rester en service.

Identifier le numéro de série connu expiré du certificat Manu

Vous pouvez vérifier les informations de certificat Manu pour un CM coincé dans reject(pk) à l'aide de la commande CLI uBR10K show cable modem <CM MAC Address>privacy.

<#root>

```
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
```

Identifiez l'index du certificat Manu connu arrivé à expiration et définissez l'état d'approbation du certificat Manu sur Approuvé

Utilisez les mêmes commandes CLI et SNMP uBR10K que celles décrites dans la section précédente pour identifier l'index du certificat Manu en fonction du numéro de série du certificat Manu. Utilisez le numéro d'index expiré du certificat Manu pour définir l'état d'approbation du certificat Manu sur Approuvé avec SNMP.

<#root>

```
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)
```

Installez un certificat Manu expiré inconnu sur l'uBR10K et marquez-le comme approuvé

Dans le cas où un certificat Manu expiré n'est pas connu de l'uBR10K, de sorte qu'il ne peut pas être géré (marqué comme approuvé) avant l'expiration et ne peut pas être récupéré, le certificat Manu doit être ajouté à l'uBR10K et marqué comme approuvé. Cette condition se produit lorsqu'un CM qui est précédemment inconnu et non enregistré sur un uBR10K tente de s'enregistrer avec un certificat Manu inconnu et expiré.

Le certificat Manu peut être ajouté à l'uBR10K par le jeu SNMP ou par la configuration des certificats de rétention d'échec de confidentialité des câbles.

Ajout d'un certificat Manu inconnu expiré à l'uBR10K avec SNMP

Afin d'ajouter un certificat de fabricant, ajoutez une entrée à la table docsBpi2CmtsCACertTable.

Spécifiez ces attributs pour chaque entrée.

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.999.1.2.5.2.1.7 (défini sur 4 pour créer l'entrée de ligne)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.999.1.2.5.2.1.8 (Données hexadécimales, sous la forme d'une valeur de certificat X509, pour le certificat X.509 réel)
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.999.1.2.5.2.1.5 (défini sur 1 pour définir l'état Manu Cert Trust sur Approuvé)

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

La commande SNMP et les résultats dans l'exemple ajoutent un certificat ASCII DER Encoded ASN.1 X.509 à la base de données uBR10K avec les paramètres suivants :

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

Utilisez un numéro d'index unique pour le certificat Manu ajouté. Lorsqu'un certificat Manu expiré est ajouté, l'état n'est pas approuvé, sauf s'il est défini manuellement sur approuvé. Si un certificat auto-signé est ajouté, la commande cable privacy accept-self-signed-certificate doit être configurée sous la configuration de l'interface de câble uBR10K avant que l'uBR10K puisse accepter le certificat.

Dans cet exemple, une partie du contenu du certificat est omise pour des raisons de lisibilité, indiqué par des points (...).

```
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.
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 3
...
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 e
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)
```

Ajouter un certificat Manu expiré lors de l'enregistrement CM dans l'interface de ligne de

commande

Un certificat Manu entre généralement dans la base de données uBR10K par le message BPI Protocol AuthInfo envoyé à l'uBR10K par le CM. Chaque certificat Manu unique et valide reçu dans un message AuthInfo est ajouté à la base de données. Si le certificat Manu n'est pas connu du CMTS (pas dans la base de données) et que les dates de validité ont expiré, AuthInfo est rejeté et le certificat Manu n'est pas ajouté à la base de données uBR10K. Un certificat Manu non valide peut être ajouté à l'uBR10K par AuthInfo lorsque la configuration de contournement de rétention des certificats défaillants de confidentialité des câbles est présente sous la configuration d'interface de câble uBR10K. Cela permet d'ajouter le certificat Manu expiré à la base de données uBR10K comme non fiable. Pour pouvoir utiliser le certificat Manu expiré, vous devez utiliser SNMP pour le marquer comme étant approuvé.

<#root>

```
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
```

Lorsque le certificat Manu expiré est ajouté à l'uBR10K et marqué comme approuvé, la suppression de la configuration cable privacy keep-failed-certificates est recommandée pour empêcher l'ajout d'autres certificats Manu expirés inconnus sur l'uBR10K.

Autoriser l'ajout de certificats CM et Manu expirés par AuthInfo avec une commande CLI uBR10K

Dans certains cas, le certificat CM expire. Pour cette situation, en plus de la configuration cable privacy keep-failed-certificates, une autre configuration est nécessaire sur l'uBR10K. Sous chaque domaine MAC uBR10K (interface câble) approprié, ajoutez la configuration cable privacy skip-valid-period et enregistrez la configuration. Ceci amène l'uBR10K à ignorer les vérifications de période de validité expirées pour TOUS les certificats CM et Manu envoyés dans le message CM BPI AuthInfo.

<#root>

```
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
```

Additional Information

Considérations relatives à la configuration du domaine MAC/de l'interface câble

Les commandes de configuration cable privacy keep-failed-certificates et cable privacy skip-valid-period sont utilisées au niveau du domaine MAC / interface câble et ne sont pas restrictives. La commande keep-failed-certificates peut ajouter n'importe quel certificat défaillant à la base de données uBR10K et la commande skip-valid-period peut ignorer les vérifications de date de validité sur tous les certificats Manu et CM.

Considération de la taille des paquets SNMP

Une configuration SNMP uBR10K supplémentaire peut être nécessaire lorsque des certificats de grande taille sont utilisés. SNMP Get of Cert data peut être NULL si cert OctetString est supérieur à la taille du paquet SNMP. Exemple ;

<#root>

```
uBR10K#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
uBR10K(config)#
```

snmp-server packetsize 3000

```
uBR10K(config)#end
```

Débogage du certificat Manu

Le débogage du certificat Manu sur l'uBR10K est pris en charge par 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.

Documentation d'assistance associée

- Modems câble et certificats de fabricant arrivant à expiration sur le bulletin produit cBR-8 - Cisco
- Routeurs haut débit universels de la gamme Cisco uBR10000
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.