Dépannage du problème de connexion MRA Expressway et d'appel B2B en raison de l'expiration du certificat CA Sectigo le 30 mai

Contenu

Introduction

Ce document décrit les solutions pour le problème de connexion MRA (Mobile Remote Access) et d'appel B2B (Business-to-Business) dû à l'expiration du certificat CA Sectigo le 30 mai.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problème

Le package de certificats CA Sectigo a expiré le 30 mai, ce qui a provoqué des pannes pour le déploiement d'Expressway/VCS. Vous pouvez rencontrer des pannes de connexion MRA et d'appel B2B en raison d'échecs de négociation de certificat/TLS. La majorité de ces problèmes sont à l'origine de l'expiration du certificat Sectigo. La même chose a été documentée sur l'avis publié par le lien Sectigo
https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000rgSZ

Symptômes

L'expiration du certificat entraînera les symptômes suivants :

- Connexion MRA, appels B2B inactifs
- Mise en grappe vers le bas
- Zone de traversée (avec échecs TLS)

- Sectigo CA utilisé pour signer le certificat VCS/Expressway

Extraits du journal de référence

```
2020-05-31T00:02:55.897-04:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP"
Src-ip="10.106.102.215" Src-port="11239" Dst-ip="10.106.102.222" Dst-port="5061" Detail="No SSL
error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2020-05-31
04:02:55,897"

2020-05-31T00:02:55.897-04:00 expe tvcs: UTCTime="2020-05-31 04:02:55,896"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method="::TTSSLErrorOutput" Thread="0x7f8dafea0700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="5" bServer="true"
localAddress="['IPv4''TCP''10.106.102.222:5061']"
remoteAddress="['IPv4''TCP''10.106.102.215:11239']"

2020-05-31T00:02:55.897-04:00 expe tvcs: UTCTime="2020-05-31 04:02:55,897" Module="network.tcp"
Level="DEBUG": Src-ip="10.106.102.215" Src-port="11239" Dst-ip="10.106.102.222" Dst-port="5061"
Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Solution

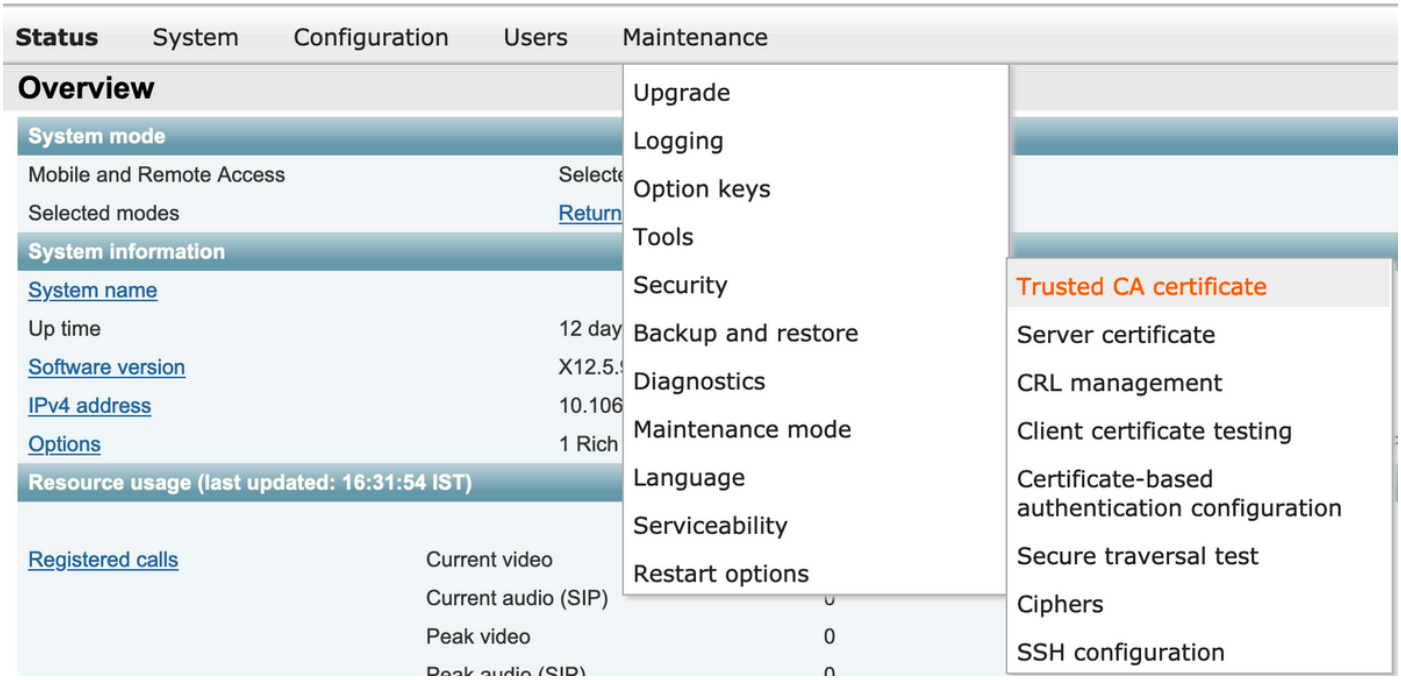
Étape 1. Vous devez télécharger le certificat à partir des liens suivants et le remplacer par des certificats Sectigo Trust expirés sur tous les noeuds homologues.

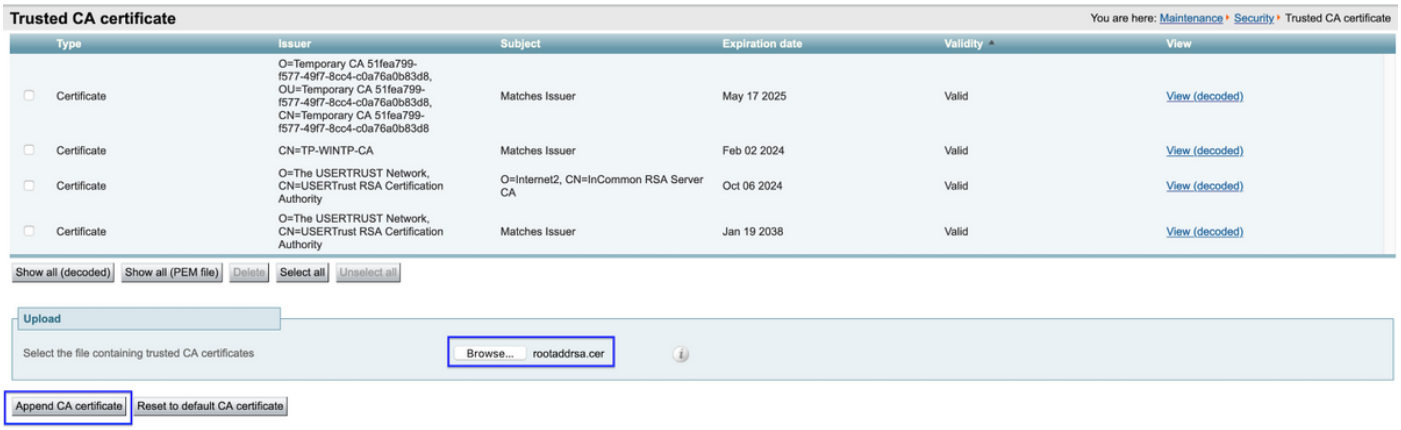
https://censys.io/certificates/52f0e1c4e58ec629291b60317f074671b85d7ea80d5b07273463534b32b40234/pem

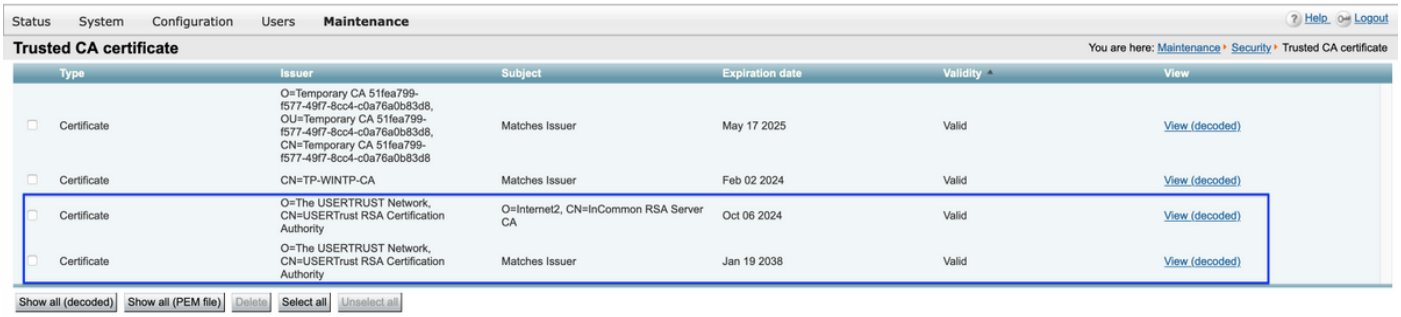
https://censys.io/certificates/e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2/pem

> **Note**: Lors de la rédaction du document ci-dessus liens où redirigé par avis Sectigo.

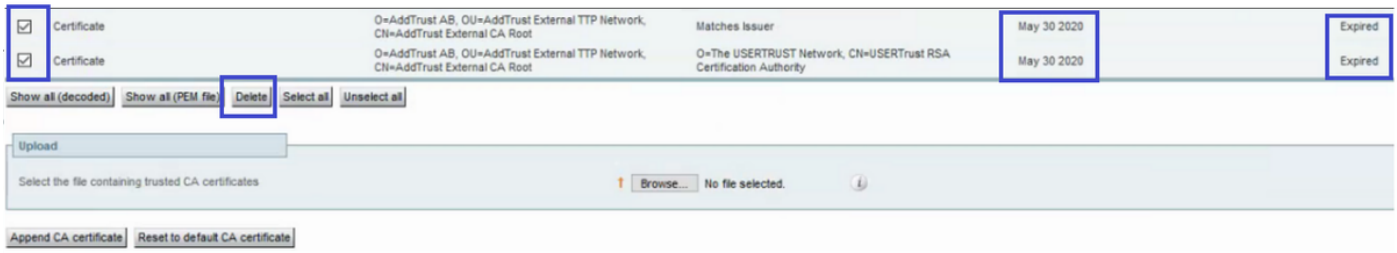
Étape 2. Téléchargé le certificat téléchargé sur Expressway en accédant à **Maintenance > Security > Trusted CA Certificate**



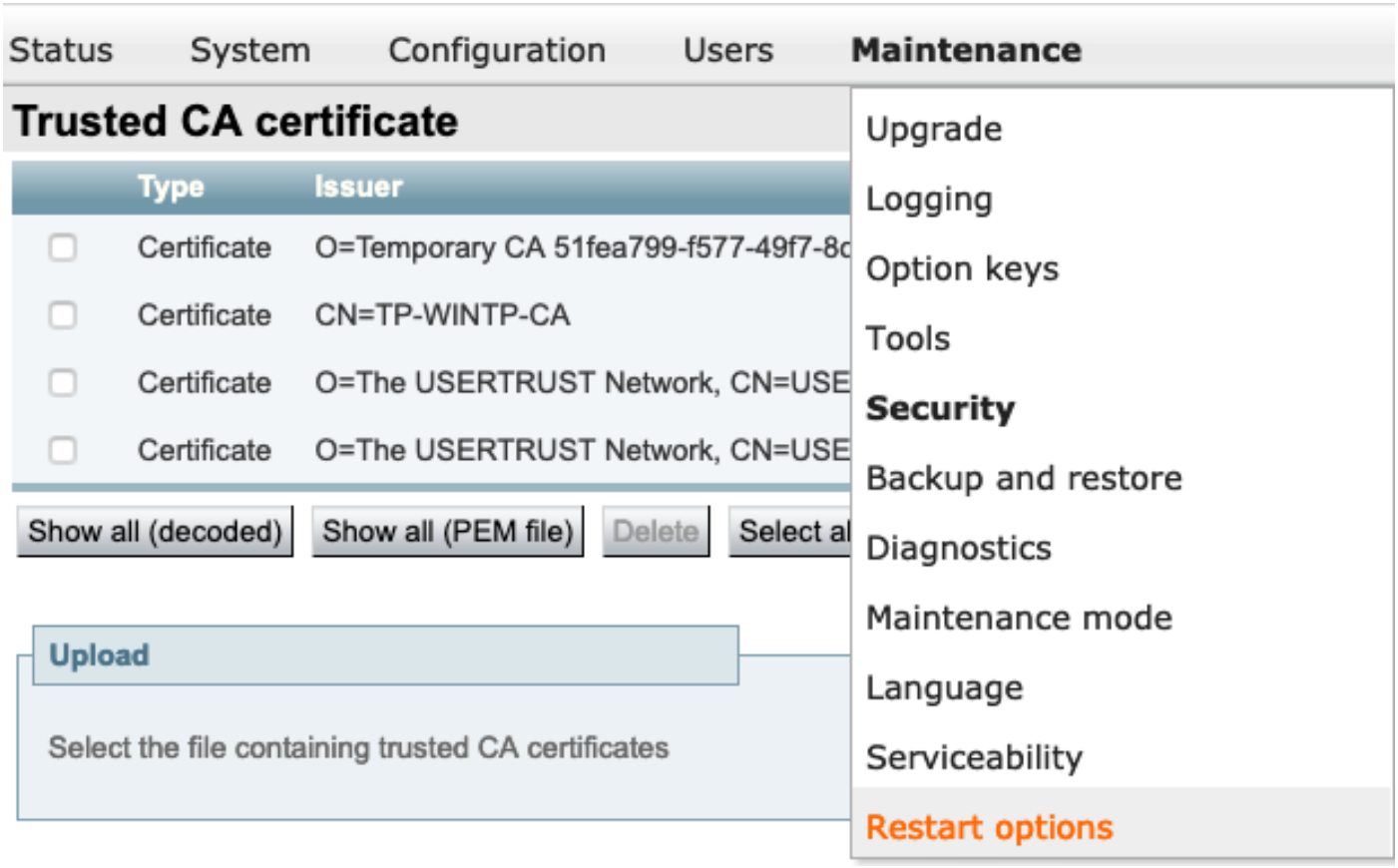


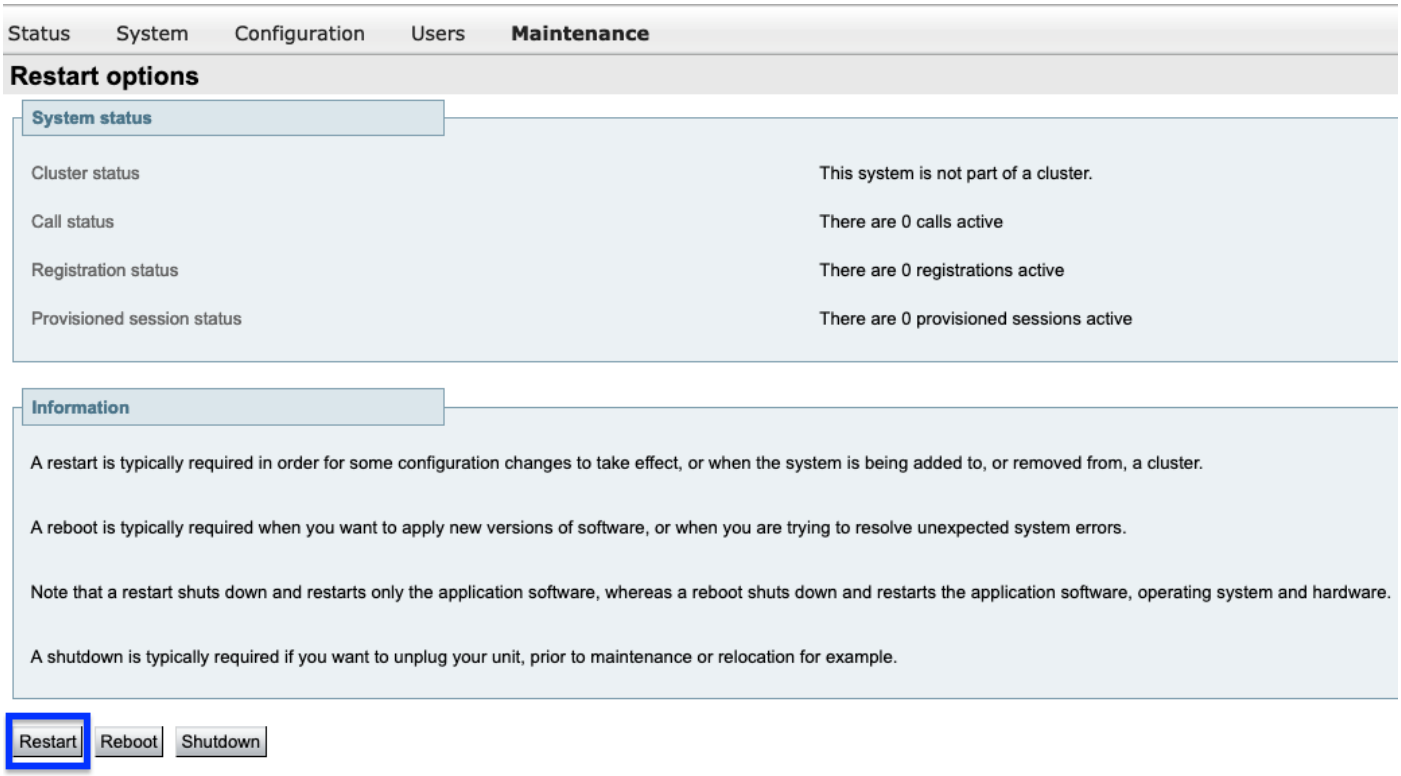


Étape 3. Supprimez le certificat CA Sectigo/AddTurst expiré sur le magasin d'approbation de certificat Expressways en accédant à **Maintenance > Security > Trusted CA Certificate.**



Étape 4. Redémarrez Expressway en accédant à **Maintenance > Restart Options > Restart**





Informations connexes

[Dépannage de la vidéo sur Expressway Sectigo Certificate Expiry]