Troubleshooting Expressway MRA Login and B2B Calling Issue due to Sectigo CA Certificate Expiry on 30th May

Contents

Introduction

Prerequisites

Requirements

Components Used

Problem

Symptoms

Reference Log Snippets

Solution

Related Information

Troubleshooting Video on Expressway Sectigo Certificate Expiry

Introduction

This document describes the solutions for MRA (Mobile Remote Access) Login and B2B (Business-to-Business) Calling issue due to Sectigo CA Certificate Expiry on 30th May.

Prerequisites

Requirements

There are no specific requirements for this 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.

Problem

The Sectigo CA certificate package expired on 30th May which causing outages for Expressway/VCS deployment. You may experience MRA Login and B2B Calling outages due to certificate/TLS Negotiation failures. The majority of these issues are root caused to the expiration of the Sectigo certificate. Same has been documented on the advisory released by Sectigo link https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N0000000rgSZ

Symptoms

Certificate expiry will to lead to following symptoms

- MRA Login, B2B Calls not working
- Clustering down
- Traversal Zone (with TLS failures)
- Sectigo CA used to sign VCS/Expressway certificate

Reference Log Snippets

```
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

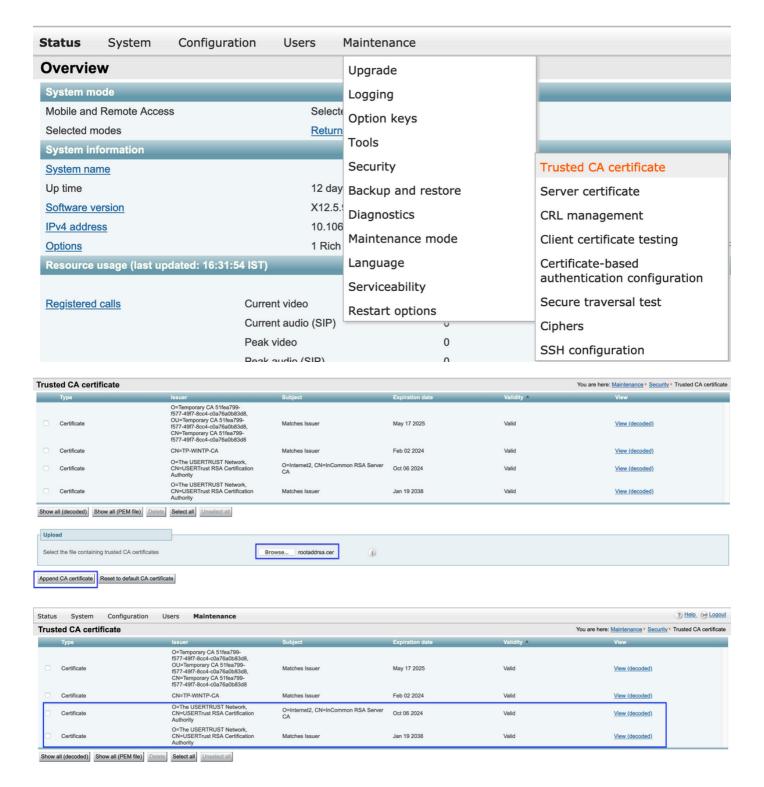
Step 1. You need to download certificate from the following links and replace them with expired Sectigo Trust certificates on all the peer nodes.

https://censys.io/certificates/52f0e1c4e58ec629291b60317f074671b85d7ea80d5b07273463534b3 2b40234/pem

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

Note: While writing the document above links where redirected per Sectigo advisory.

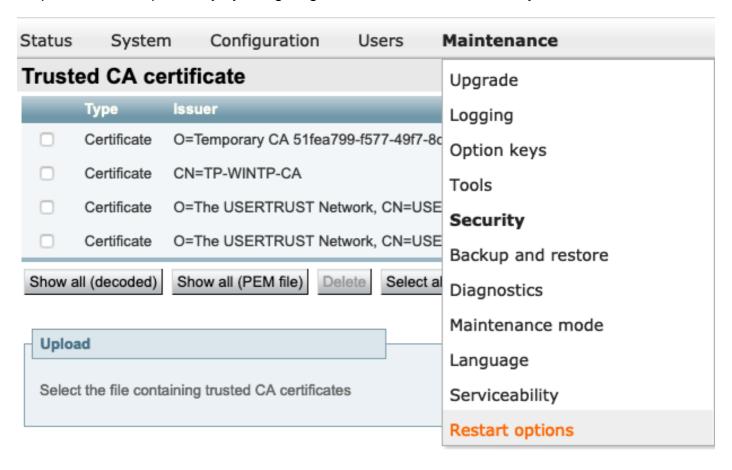
Step 2. Uploaded the downloaded certificate on Expressway by navigating to **Maintenance > Security > Trusted CA Certificate**

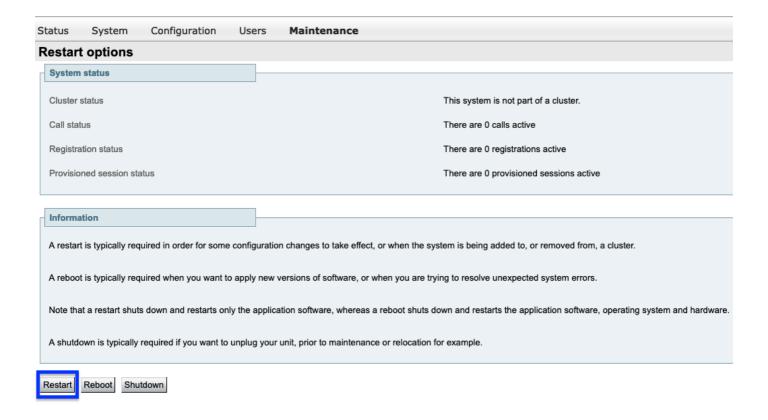


Step 3. Delete the expired Sectigo/AddTurst CA certificate on Expressways certificate trust store by navigating to **Maintenance > Security > Trusted CA Certificate.**



Step 4. Restart Expressway by navigating to **Maintenance > Restart Options > Restart**





Related Information

Troubleshooting Video on Expressway Sectigo Certificate Expiry