Solução de problemas de login do Expressway MRA e problema de chamada B2B devido ao vencimento do certificado CA Sectigo em 30 de maio

Contents

Introduction

Este documento descreve as soluções para o problema de login MRA (Mobile Remote Access) e chamada B2B (Business-to-Business) devido ao vencimento do certificado CA Sectigo em 30 de maio.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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.

Problema

O pacote de certificado CA Sectigo expirou em 30 de maio, o que causou interrupções na implantação do Expressway/VCS. Você pode enfrentar interrupções de chamada de MRA e B2B devido a falhas de certificado/negociação TLS. A maioria desses problemas são originalmente causados pela expiração do certificado Sectigo. O mesmo foi documentado na assessoria divulgada pelo link Sectigo

Sintomas

A expiração do certificado levará aos seguintes sintomas

- Login no MRA, Chamadas B2B não funcionando
- Clustering down
- Zona de passagem (com falhas de TLS)

- CA Sectigo utilizada para assinar o certificado VCS/Expressway

Trechos de registro de referência

```
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"
```

Solução

Etapa 1. Você precisa baixar o certificado dos links a seguir e substituí-lo por certificados Sectigo
Trust expirados em todos os nós de peer.

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

https://censys.io/certificates/e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c
3d4cbd2/pem

> **Note**: Enquanto escreve o documento acima, os links são redirecionados de acordo com a
> orientação da Sectigo.

Etapa 2. Carregado o certificado baixado no Expressway navegando para **Manutenção >
Segurança > Certificado CA
confiável**

Status System Configuration Users Maintenance

Overview

System mode

Mobile and Remote Access .... Selecte...
Selected modes .... Return...

System information

System name
Up time .... 12 day
Software version .... X12.5.
IPv4 address 10.106
Options .... 1 Rich

Resource usage (last updated: 16:31:54 IST)

Registered calls
Current video
Current audio (SIP) 0
Peak video 0
Peak audio (SIP) 0

Maintenance menu:

- Upgrade
- Logging
- Option keys
- Tools
- Security
- Backup and restore
- Diagnostics
- Maintenance mode
- Language
- Serviceability
- Restart options

Security submenu:

- Trusted CA certificate
- Server certificate
- CRL management
- Client certificate testing
- Certificate-based authentication configuration
- Secure traversal test
- Ciphers
- SSH configuration

Trusted CA certificate

You are here: Maintenance ▸ Security ▸ Trusted CA certificate

Type	Issuer	Subject	Expiration date	Validity ▲	View
Certificate	O=Temporary CA 51fea799-f577-49f7-8cc4-c0a76a0b83d8, OU=Temporary CA 51fea799-f577-49f7-8cc4-c0a76a0b83d8, CN=Temporary CA 51fea799-f577-49f7-8cc4-c0a76a0b83d8	Matches Issuer	May 17 2025	Valid	View (decoded)
Certificate	CN=TP-WINTP-CA	Matches Issuer	Feb 02 2024	Valid	View (decoded)
Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	O=Internet2, CN=InCommon RSA Server CA	Oct 06 2024	Valid	View (decoded)
Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	Matches Issuer	Jan 19 2038	Valid	View (decoded)

Show all (decoded) Show all (PEM file) Delete Select all Unselect all

Upload

Select the file containing trusted CA certificates   Browse... rootaddrsa.cer   ⓘ

Append CA certificate Reset to default CA certificate

Status System Configuration Users Maintenance   ? Help ⊶ Logout

Trusted CA certificate

You are here: Maintenance ▸ Security ▸ Trusted CA certificate

Type	Issuer	Subject	Expiration date	Validity ▲	View
Certificate	O=Temporary CA 51fea799-f577-49f7-8cc4-c0a76a0b83d8, OU=Temporary CA 51fea799-f577-49f7-8cc4-c0a76a0b83d8, CN=Temporary CA 51fea799-f577-49f7-8cc4-c0a76a0b83d8	Matches Issuer	May 17 2025	Valid	View (decoded)
Certificate	CN=TP-WINTP-CA	Matches Issuer	Feb 02 2024	Valid	View (decoded)
Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	O=Internet2, CN=InCommon RSA Server CA	Oct 06 2024	Valid	View (decoded)
Certificate	O=The USERTRUST Network, CN=USERTrust RSA Certification Authority	Matches Issuer	Jan 19 2038	Valid	View (decoded)

Show all (decoded) Show all (PEM file) Delete Select all Unselect all

---

Etapa 3. Exclua o certificado CA Sectigo/AddTurst expirado no arquivo confiável de certificados Expressways navegando para **Manutenção > Segurança > Certificado CA confiável.**

Etapa 4. Reinicie o Expressway navegando até **Manutenção > Opções de reinicialização > Reiniciar**

Informações Relacionadas

[Solução de problemas de vídeo no Expressway Sectigo Certificate Expiration](#)