Mandiant

UPDATE THE ACTOR TEST INTERFACE TO USE A SIGNED CERTIFICATE

You can update the Actor test interface to use a certificate signed by a Certificate Authority (CA). This update helps a proxy, load balancer, or web application firewall (WAF) trust the certificate and allow the traffic to pass through for testing.

- When upgrading Network Actor software, the `https-server-cert.pem` and `https-server-key.pem` files get overwritten.
- As a best practice, back up the `https-server-cert.pem` and `https-server-key.pem` files before making any changes to the Network Actor software.

1. SSH to the Network Actor and switch to the root user:

```
sudo bash
```

2. Navigate to the folder that contains the test interface certificate:

```
cd /opt/apps/verodin/node/node/tmp/certs
```

3. Generate a Certificate Signing Request (CSR) with a private key:

```
openssl req -new -newkey rsa:2048 -nodes -keyout https-server-key.pem -out server.csr
```

You're prompted for the CN value, which is generally the FQDN. For example, `testint.example.com`.

FQDNs must comply with RFC 1123, a standard that defines the requirements for FQDNs on the internet. This standard specifies that FQDNs can only contain the following:

- Letters (A-Z, a-z)
- Digits (0-9)
- Hyphens (-)

Underscores are not permitted.

For more information, see **RFC 1123: Requirements for Internet Hosts (https://www.rfc-editor.org/rfc/rfc1123.html)**.

4. Optional: Check the SSL file `SERVER_KEY_FILENAME.pem` and verify consistency:

```
openssl rsa -in SERVER_KEY_FILENAME.pem -check
```

An `RSA key ok` result appears, followed by the output of the key.

5. Check the CSR, verify the CSR, and and print the data that was entered when generating the CSR:

```
openssl req -text -noout -verify -in server.csr
```

- A `verify OK` result appears, followed by the Certificate Request details.
- The CA signs the CSR file (`server.csr`) with a generated signed certificate.

6. Use the CSR to request a certificate from your CA.
7. After you receive the certificate from the CA, copy the signed certificate to Network Actor folder:

```
cp SERVER_CERT_FILENAME.pem /opt/apps/verodin/node/node/tmp/certs
```

8. Rename the signed certificate to `https-server-cert.pem`.
9. Optional: Verify that the certificate and key have matching MD5 has values.

```
openssl x509 -noout -modulus -in https-server-cert.pem | openssl md5
```

```
openssl rsa -noout -modulus -in https-server-key.pem | openssl md5
```

After these commands are run, two identical MD5 hash values appear.

10. Restart Network Actor Services:

```
vrestart
```

11. After generating your signed certificates, export the private key:

```
openssl pkcs12 -export -out server.p12 -inkey https-server-key.pem -in https-server-cert.pem -certfile <CARoot>.pem
```