Applying the workaround to Cisco DNA Center Affected by Field Notice FN74065

Contents

Introduction

This document describes the procedure to recover a Cisco DNA Center installation with an expired etcd certificate. Cisco DNA Center introduced digital certificates for etcd in release 2.3.2.0 to ensure secure data communication over Kubernetes, both within a node and between nodes in a cluster. These certificates are valid for one year and are automatically renewed before they expire. The renewed certificates are processed by a helper container and then made available to the etcd container. In affected Cisco DNA Center releases, the etcd container does not recognize and activate those renewed certificates dynamically and continues to point to the expired certificates until etcd is restarted. Once the certificate expires Cisco DNA Center becomes inoperable, and this document provides steps to recover the affected Cisco DNA Center installation.

Conditions

Affected versions:
2.3.2.x

2.3.3.x

2.3.5.3

2.3.7.0

Fixed versions:

2.3.3.7 HF4

2.3.5.3 HF5

2.3.5.4 after October 12th 2023

2.3.5.4 HF3

2.3.7.3

Symptoms

When the certificate expires, one or more of these symptoms will be observed.

1. Cisco DNA Center's GUI is down

2. Most of the services are down

3. These errors are seen in the CLI

```
<#root>

WARNING:urllib3.connectionpool:Retrying (Retry(total=0, connect=None, read=None, redirect=None, status=

SSL: CERTIFICATE_VERIFY_FAILED

] certificate verify failed (_ssl.c:727)'),)': /v2/keys/maglev/config/node-x.x.x.x?sorted=true&recursiv
```

Recovery

The recovery needs access to the root shell. In 2.3.x.x, restricted shell was enabled by default. In 2.3.5.x and above, consent token validation is required to access the root shell. If the affected environment is on release 2.3.5.3, please work with the TAC to recover the installation.

Step 1: Verify the problem

From the CLI, run the command

```
etcdctl member list
```

If the issue is due to certificate expiration, the command will fail and return an error. If the command runs successfully, then Cisco DNA Center is not affected by this issue. This is an example of the output from an effected installation with an expired certificate.

```
etcdctl member list
client: etcd cluster is unavailable or misconfigured; error #0: x509: certificate has expired or is not yet
valid: current time 2023-10-20T20:50:14Z is after 2023-10-12T22:47:42Z
```

Step 2: Verify the certificate

Run this command to verify the certificate expiration date.

```
for certs in $(ls /etc/maglev/.pki/ | grep etcd | grep -v -e key -e .cnf); do sudo openssl x509 -noout -subject -
issuer -dates -in /etc/maglev/.pki/$certs;done
```

Please enter the sudo password when prompted. In the output verify if the certificate has expired

```
[sudo] password for maglev:
subject=CN = etcd-client
issuer=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6, O = Cisco Systems, OU = Cisco DNA Center
notBefore=Oct 8 00:59:37 2022 GMT
notAfter=Oct 7 00:59:37 2023 GMT
subject=CN = etcd-peer
issuer=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6, O = Cisco Systems, OU = Cisco DNA Center
notBefore=Oct 8 00:59:37 2022 GMT
notAfter=Oct 7 00:59:37 2023 GMT
```

Step 4: Restart Docker

a. Clear the exited containers

```
docker rm -v $(docker ps -q -f status=exited)
```

Depending upon the number of exited containers, this can take a few minutes.

b. Restart Docker

```
sudo systemctl restart docker
```

This command restarts all the containers and could take 30 to 45 minutes to complete.

Step 5: Verify the certificate has renewed

Issue the same command from Step 2 to verify that the certificate has renewed. It should have renewed for a year.

```
for certs in $(ls /etc/maglev/.pki/ | grep etcd | grep -v -e key -e .cnf); do sudo openssl x509 -noout -subject -issuer -dates -in /etc/maglev/.pki/$certs;done
```

Verify that the GUI is accessible and accessing the CLI has no errors.

Solution

This workaround will keep Cisco DNA Center up and running for a maximum of one year. For a permanent fix, please upgrade the Cisco DNA Center installation to a fixed release as mentioned in Field Notice FN74065.