Anwendung des Workaround auf Cisco DNA Center Affected by Field Notice FN74065

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Wiederherstellung einer Cisco DNA Center-Installation mit einem abgelaufenen Zertifikat usw. beschrieben. Cisco DNA Center hat in Version 2.3.2.0 digitale Zertifikate für etc. eingeführt, um eine sichere Datenkommunikation über Kubernetes sicherzustellen, sowohl innerhalb eines Knotens als auch zwischen Knoten in einem Cluster. Diese Zertifikate sind ein Jahr gültig und werden vor ihrem Ablauf automatisch verlängert. Die erneuerten Zertifikate werden von einem Hilfscontainer verarbeitet und dann dem etc.-Container zur Verfügung gestellt. Bei betroffenen Cisco DNA Center-Releases erkennt und aktiviert der Container "etc" diese erneuerten Zertifikate nicht dynamisch und verweist weiterhin auf die abgelaufenen Zertifikate, bis "etc" neu gestartet wird. Nach Ablauf des Zertifikats ist Cisco DNA Center nicht mehr funktionsfähig. Dieses Dokument enthält die erforderlichen Schritte zur Wiederherstellung der betroffenen Cisco DNA Center-Installation.

Bedingungen

Betroffene Versionen:
2.3.2.x

2.3.3.x

2.3.5.3

2.3.7.0

Feste Versionen:

2.3.3.7 HF4

2.3.5.3 HF5

2.3.5.4 nach dem 12. Oktober 2023

2.3.5.4 HF3

2.3.7.3

Symptome

Wenn das Zertifikat abläuft, werden eines oder mehrere dieser Symptome beobachtet.

1. Die Benutzeroberfläche des Cisco DNA Center ist ausgefallen.

2. Die meisten Dienste sind ausgefallen

3. Diese Fehler werden in der CLI angezeigt.

```
<#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
```

Wiederherstellung

Die Wiederherstellung benötigt Zugriff auf die Root-Shell. In 2.3.x.x war eingeschränkte Shell standardmäßig aktiviert. In Version 2.3.5.x und höher ist eine Überprüfung des Zustimmungstokens erforderlich, um auf die Root-Shell zuzugreifen. Wenn die betroffene Umgebung Version 2.3.5.3 ist, arbeiten Sie mit dem TAC zusammen, um die Installation wiederherzustellen.

Schritt 1: Überprüfen des Problems

Führen Sie in der CLI den Befehl

```
Liste der Mitglieder von etcCTL
```

Wenn das Problem auf den Ablauf des Zertifikats zurückzuführen ist, schlägt der Befehl fehl und gibt einen Fehler zurück. Wenn der Befehl erfolgreich ausgeführt wird, ist Cisco DNA Center von diesem Problem nicht betroffen. Dies ist ein Beispiel für die Ausgabe einer durchgeführten Installation mit abgelaufenem Zertifikat.

```
Liste der Mitglieder von etcCTL
client: etc cluster is not available or misconfigured; error #0: x509: zertifikat abgelaufen oder noch nicht gültig: aktuelle zeit 2023-10-20T20:50:14Z is after 2023-10-12T22:47:42Z
```

Schritt 2: Überprüfen des Zertifikats

Führen Sie diesen Befehl aus, um das Ablaufdatum des Zertifikats zu überprüfen.

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

Geben Sie auf Aufforderung das Sudo-Kennwort ein. Überprüfen Sie in der Ausgabe, ob das Zertifikat abgelaufen ist.

```
[sudo] Passwort für maglev:
subject=CN = ecd-Client
emitter=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6, O = Cisco Systems, OU = Cisco DNA Center
notBefore=Okt 8 00:59:37 2022 GMT
notAfter=Okt 7 00:59:37 2023 GMT
subject=CN = ec-Peer
emitter=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6, O = Cisco Systems, OU = Cisco DNA Center
notBefore=Okt 8 00:59:37 2022 GMT
notAfter=Okt 7 00:59:37 2023 GMT
```

Schritt 4: Docker neu starten

a. Löschen Sie die ausgetretenen Container.

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

Je nach Anzahl der ausgefahrenen Container kann dies einige Minuten dauern.

b. Docker neu starten

```
sudo systemctl restart docker
```

Dieser Befehl startet alle Container neu und kann 30 bis 45 Minuten in Anspruch nehmen.

Schritt 5: Überprüfen, ob das Zertifikat erneuert wurde

Führen Sie den gleichen Befehl aus Schritt 2 aus, um zu überprüfen, ob das Zertifikat erneuert wurde. Sie hätte um ein Jahr verlängert werden müssen.

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

Stellen Sie sicher, dass auf die GUI zugegriffen werden kann und der Zugriff auf die CLI fehlerfrei erfolgt.

Lösung

Diese Problemumgehung sorgt dafür, dass das Cisco DNA Center maximal ein Jahr lang betriebsbereit ist. Aktualisieren Sie die Cisco DNA Center-Installation auf eine feste Version, um einen dauerhaften Fehler zu beheben, wie in der Problemhinweis-Nr. FN74065 erwähnt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.