De tijdelijke oplossing toepassen op Cisco DNA Center beïnvloed door meldingen uit het veld FN74065

Inhoud

Inleiding

Dit document beschrijft de procedure om een installatie van Cisco DNA Center met een verlopen etcd-certificaat te herstellen. Cisco DNA Center heeft digitale certificaten voor etcd geïntroduceerd in release 2.3.2.0 om beveiligde datacommunicatie via Kubernetes te garanderen, zowel binnen een knooppunt als tussen knooppunten in een cluster. Deze certificaten zijn één jaar geldig en worden automatisch verlengd voordat ze verlopen. De vernieuwde certificaten worden door een helpercontainer verwerkt en vervolgens ter beschikking gesteld van de etcd-container. Bij releases van het Cisco DNA Center herkent en activeert de etcd-container die vernieuwde certificaten niet dynamisch en blijft hij doorverwijzen naar de verlopen certificaten totdat etcd is herstart. Wanneer het certificaat verloopt, wordt Cisco DNA Center inoperabel en dit document bevat stappen om de getroffen installatie van Cisco DNA Center te herstellen.

Voorwaarden

Betrokken versies:
2.3.2.x.

2.3.3.x.

2.3.5.3

2.3.7.0

Vaste versies:

2.3.3.7. HF4

2.3.5.3 HF5

2.3.5.4 na 12 oktober 2023

2.3.5.4 HF3

2.3.7.3

Symptomen

Wanneer het certificaat vervalt, zullen één of meerdere van deze symptomen worden waargenomen.

1. De GUI van Cisco DNA Center is niet beschikbaar

2. De meeste diensten zijn niet beschikbaar

3. Deze fouten worden in het 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
```

Terugwinning

Het herstel heeft toegang tot de wortelschelp nodig. In 2.3.x.x werd gelimiteerde shell standaard ingeschakeld. In 2.3.5.x en hoger, toestemming token validatie is vereist om toegang te krijgen tot de wortel shell. Als de getroffen omgeving op release 2.3.5.3 staat, werk dan samen met de TAC om de installatie te herstellen.

Stap 1: Controleer het probleem

Voer de opdracht uit vanuit de CLI

```
etcdctl lidlijst
```

Als de kwestie aan certificaatafloop toe te schrijven is, zal het bevel ontbreken en zal een fout terugkeren. Als de opdracht succesvol wordt uitgevoerd, is dit niet van invloed op Cisco DNA Center. Dit is een voorbeeld van de output van een uitgevoerde installatie met een verlopen certificaat.

```
etcdctl lidlijst
client: etcd-cluster is niet beschikbaar of verkeerd geconfigureerd; fout #0: x509: certificaat is verlopen of nog niet geldig: huidige tijd 2023-10-20T20:50:14Z is na 2023-10-12T22:47:42Z
```

Stap 2: Controleer het certificaat

Voer deze opdracht uit om de verloopdatum van het certificaat te controleren.

```
voor certs in $(ls /etc/maglev/.pki/ | grep etcd | grep -v -e key -e .cnf); do sudo openssl x509 -no -subject -issuer -dates -in /etc/maglev/.pki/$certs;gedaan
```

Voer het wachtwoord voor het wachtwoord in zodra dit wordt gevraagd. Controleer in het uitvoerdocument of het certificaat is verlopen

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

Stap 4: Docker opnieuw starten

a. Verwijder de gebruikte containers

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

Afhankelijk van het aantal afgesloten containers, kan dit een paar minuten duren.

b. Docker opnieuw starten

```
sudo systemctl
```

Deze opdracht herstart alle containers en kan 30 tot 45 minuten duren om te voltooien.

Stap 5: Controleer of het certificaat is verlengd

Voer dezelfde opdracht uit vanuit Stap 2 om te verifiëren dat het certificaat is vernieuwd. Het had met een jaar moeten worden verlengd.

```
voor certs in $(ls /etc/maglev/.pki/ | grep etcd | grep -v -e key -e .cnf); do sudo openssl x509 -no -subject -issuer -dates -in /etc/maglev/.pki/$certs;gedaan
```

Controleer dat de GUI toegankelijk is en dat het benaderen van de CLI geen fouten bevat.

Oplossing

Deze tijdelijke oplossing houdt Cisco DNA Center maximaal één jaar draaiend. Voor een permanente oplossing dient u de installatie van Cisco DNA Center te upgraden naar een vaste release zoals vermeld in melding uit het veld FN74065.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.