Application de la solution de contournement au centre Cisco DNA affecté par la note de service FN74065

Table des matières

Introduction

Ce document décrit la procédure de récupération d'une installation Cisco DNA Center avec un certificat etcd expiré. Cisco DNA Center a introduit les certificats numériques pour l'ETC dans la version 2.3.2.0 afin de garantir une communication sécurisée des données via Kubernetes, à la fois au sein d'un noeud et entre les noeuds d'un cluster. Ces certificats sont valides pendant un an et sont automatiquement renouvelés avant leur expiration. Les certificats renouvelés sont traités par un conteneur auxiliaire, puis mis à la disposition du conteneur ETC. Dans les versions affectées de Cisco DNA Center, le conteneur etcd ne reconnaît pas et n'active pas ces certificats renouvelés de manière dynamique et continue à pointer vers les certificats expirés jusqu'à ce que etcd soit redémarré. Une fois que le certificat expire, Cisco DNA Center devient inutilisable et ce document fournit des étapes pour récupérer l'installation de Cisco DNA Center affectée.

Conditions

Versions concernées :
2.3.2.x

2.3.3.x

Commutateurs 2.3.5.3

Commutateurs 2.3.7.0

Versions fixes :

2.3.3.7 HF4

2.3.5.3 HF5

2.3.5.4 après le 12 octobre 2023

2.3.5.4 HF3

Commutateurs 2.3.7.3

Symptômes

À l'expiration du certificat, un ou plusieurs de ces symptômes seront observés.

1. L'interface utilisateur graphique de Cisco DNA Center est désactivée

2. La plupart des services sont hors service

3. Ces erreurs sont visibles dans l'interface de ligne de commande

```
<#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
```

Récupération

La restauration doit avoir accès à l'interpréteur de commandes racine. Dans 2.3.x.x, le shell restreint était activé par défaut. Dans les versions 2.3.5.x et ultérieures, la validation du jeton de consentement est requise pour accéder à l'interpréteur de commandes racine. Si l'environnement affecté se trouve dans la version 2.3.5.3, contactez le TAC pour récupérer l'installation.

Étape 1 : Vérifiez le problème

À partir de l'interface de ligne de commande, exécutez la commande

```
liste des membres etcdctl
```

Si le problème est dû à l'expiration du certificat, la commande échoue et renvoie une erreur. Si la commande s'exécute correctement, Cisco DNA Center n'est pas affecté par ce problème. Ceci est un exemple de la sortie d'une installation effectuée avec un certificat expiré.

```
liste des membres etcdctl
client : le cluster etcd est indisponible ou mal configuré ; erreur #0 : x509 : le certificat a expiré ou n'est pas encore valide : heure actuelle 2023-10-20T20:50:14Z est postérieure à 2023-10-12T22:47:42Z
```

Étape 2 : Vérifiez le certificat

Exécutez cette commande pour vérifier la date d'expiration du certificat.

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

Entrez le mot de passe sudo lorsque vous y êtes invité. Dans le résultat, vérifiez si le certificat a expiré

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

Étape 4 : Redémarrez Docker

a. Videz les conteneurs sortants

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

Selon le nombre de conteneurs sortis, cette opération peut prendre quelques minutes.

b. Redémarrer Docker

```
sudo systemctl restart docker
```

Cette commande redémarre tous les conteneurs et peut prendre de 30 à 45 minutes.

Étape 5 : Vérifiez que le certificat a été renouvelé

Exécutez la même commande à l'étape 2 pour vérifier que le certificat a été renouvelé. Elle aurait dû être renouvelée pour un an.

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

Vérifiez que l'interface utilisateur graphique est accessible et que l'accès à la CLI ne comporte aucune erreur.

Solution

Cette solution de contournement permettra à Cisco DNA Center de rester opérationnel pendant un an maximum. Pour obtenir un correctif permanent, veuillez mettre à niveau l'installation de Cisco DNA Center vers une version fixe, comme indiqué dans la note de service FN74065.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.