Aplicando a solução alternativa ao Cisco DNA Center afetado pelo aviso de campo FN74065

Contents

Introdução

Este documento descreve o procedimento para recuperar uma instalação do Cisco DNA Center com um certificado etcd expirado. O Cisco DNA Center introduziu certificados digitais para etcd na versão 2.3.2.0 para garantir a comunicação segura de dados através do Kubernetes, tanto dentro de um nó quanto entre nós em um cluster. Esses certificados são válidos por um ano e são renovados automaticamente antes de expirarem. Os certificados renovados são processados por um contêiner auxiliar e disponibilizados para o contêiner etcd. Nas versões afetadas do Cisco DNA Center, o contêiner etcd não reconhece e ativa esses certificados renovados dinamicamente e continua a apontar para os certificados expirados até que o etcd seja reiniciado. Quando o certificado expira, o Cisco DNA Center torna-se inoperante e este documento fornece etapas para recuperar a instalação afetada do Cisco DNA Center.

Condições

Versões Afetadas:
2.3.2.x

2.3.3.x

2.3.5.3

2.3.7.0

Versões fixas:

2.3.3.7 HF4

2.3.5.3 HF5

2.3.5.4 após 12 de outubro de 2023

2.3.5.4 HF3

2.3.7.3

Sintomas

Quando o certificado expirar, um ou mais desses sintomas serão observados.

1. A GUI do Cisco DNA Center está inoperante

2. A maioria dos serviços está inoperante

3. Estes erros são vistos na 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
```

Recuperação

A recuperação precisa de acesso ao shell raiz. No 2.3.x.x, o shell restrito foi ativado por padrão. No 2.3.5.x e acima, a validação do token de consentimento é necessária para acessar o shell raiz. Se o ambiente afetado estiver na versão 2.3.5.3, trabalhe com o TAC para recuperar a instalação.

Etapa 1: Verifique o problema

Na CLI, execute o comando

```
lista de membros etcdctl
```

Se o problema ocorrer devido à expiração do certificado, o comando falhará e retornará um erro. Se o comando for executado com êxito, o Cisco DNA Center não será afetado por esse problema. Este é um exemplo da saída de uma instalação afetada com um certificado expirado.

```
lista de membros etcdctl
cliente: cluster etcd indisponível ou configurado incorretamente; #0 de erro: x509: o certificado expirou ou ainda não é válido: tempo atual 2023-10-20T20:50:14Z é posterior a 2023-10-12T22:47:42Z
```

Etapa 2: Verifique o certificado

Execute este comando para verificar a data de expiração do certificado.

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

Insira a senha sudo quando solicitado. Na saída, verifique se o certificado expirou

```
[sudo] senha para maglev:
subject=CN = etcd-client
```

```
emitente=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6, O = Cisco Systems, OU = Cisco DNA Center
notBefore=Out 8 00:59:37 2022 GMT
notAfter=00:59:37 de outubro de 2023 GMT
subject=CN = etcd-peer
emitente=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6, O = Cisco Systems, OU = Cisco DNA Center
notBefore=Out 8 00:59:37 2022 GMT
notAfter=00:59:37 de outubro de 2023 GMT
```

Etapa 4: Reinicie o Docker

a. Limpe os contêineres saídos

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

Dependendo do número de contêineres de saída, isso pode levar alguns minutos.

b. Reinicie o Docker

```
sudo systemctl restart docker
```

Esse comando reinicia todos os contêineres e pode levar de 30 a 45 minutos para ser concluído.

Etapa 5: Verifique se o certificado foi renovado

Emita o mesmo comando da Etapa 2 para verificar se o certificado foi renovado. Deveria ter sido renovado por um ano.

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

Verifique se a GUI está acessível e se o acesso à CLI não apresenta erros.

Solução

Essa solução alternativa manterá o Cisco DNA Center funcionando por no máximo um ano. Para uma correção permanente, atualize a instalação do Cisco DNA Center para uma versão fixa, conforme mencionado na Nota de campo FN74065.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.