Aplicación de la solución alternativa a Cisco DNA Center Affected by Field Notice FN74065

Contenido

Introducción

Este documento describe el procedimiento para recuperar una instalación de Cisco DNA Center con un certificado etcd caducado. Cisco DNA Center introdujo certificados digitales para etcd en la versión 2.3.2.0 para garantizar la comunicación segura de datos a través de Kubernetes, tanto dentro de un nodo como entre nodos en un clúster. Estos certificados son válidos durante un año y se renuevan automáticamente antes de que caduquen. Los certificados renovados son procesados por un contenedor auxiliar y, a continuación, se ponen a disposición del contenedor etcd. En las versiones afectadas de Cisco DNA Center, el contenedor etcd no reconoce y activa dinámicamente esos certificados renovados y continúa señalando a los certificados caducados hasta que se reinicie etcd. Una vez que caduca el certificado, Cisco DNA Center deja de funcionar y este documento proporciona los pasos para recuperar la instalación de Cisco DNA Center afectada.

Condiciones

Versiones Afectadas:
2.3.2.x.

2.3.3.x.

2.3.5.3

2.3.7.0

Versiones fijas:

2.3.3.7 HF4

2.3.5.3 HF5

2.3.5.4 después del 12 de octubre de 2023

2.3.5.4 HF3

2.3.7.3

Síntomas

Cuando caduque el certificado, se observará uno o más de estos síntomas.

1. La GUI del Cisco DNA Center está inactiva

2. La mayoría de los servicios están inactivos

3. Estos errores se observan en la 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
```

Recuperación

La recuperación necesita acceso al shell raíz. En 2.3.x.x, el shell restringido estaba habilitado de forma predeterminada. En 2.3.5.x y superiores, se requiere validación de token de consentimiento para acceder al shell raíz. Si el entorno afectado se encuentra en la versión 2.3.5.3, trabaje con el TAC para recuperar la instalación.

Paso 1: Verifique el problema

Desde la CLI, ejecute el comando

```
lista de miembros de etcdctl
```

Si el problema se debe a la expiración del certificado, el comando no funcionará y devolverá un error. Si el comando se ejecuta correctamente, el Centro de ADN de Cisco no se verá afectado por este problema. Este es un ejemplo del resultado de una instalación realizada con un certificado caducado.

```
lista de miembros de etcdctl
cliente: el clúster etcd no está disponible o está mal configurado; error #0: x509: el certificado ha caducado o todavía no es válido: la hora actual 2023-10-20T20:50:14Z es posterior a 2023-10-12T22:47:42Z
```

Paso 2: Verificar el certificado

Ejecute este comando para verificar la fecha de vencimiento del certificado.

```
para certificados 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
```

Introduzca la contraseña de sudo cuando se le solicite. En el resultado, compruebe si el certificado ha caducado

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

Paso 4: Reinicio de Docker

a. Borrar los contenedores salientes

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

Dependiendo del número de contenedores salientes, esto puede tardar unos minutos.

b. Reiniciar Docker

```
sudo systemctl restart docker
```

Este comando reinicia todos los contenedores y podría tardar de 30 a 45 minutos en completarse.

Paso 5: compruebe que el certificado se ha renovado

Ejecute el mismo comando desde el paso 2 para verificar que el certificado se ha renovado. Debería haber sido renovado por un año.

```
para certificados 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
```

Verifique que la GUI esté accesible y que el acceso a la CLI no tenga errores.

Solución

Esta solución alternativa mantendrá Cisco DNA Center en funcionamiento durante un máximo de un año. Para obtener una solución permanente, actualice la instalación de Cisco DNA Center a una versión fija como se menciona en el aviso práctico FN74065.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).