Applicazione della soluzione al Cisco DNA Center interessato dall'avviso sui prodotti FN74065

Sommario

Introduzione

Questo documento descrive la procedura per recuperare un'installazione di Cisco DNA Center con un certificato etcd scaduto. Cisco DNA Center ha introdotto i certificati digitali per l'etcd nella release 2.3.2.0 per garantire una comunicazione sicura dei dati su Kubernetes, sia all'interno di un nodo che tra i nodi di un cluster. Questi certificati sono validi per un anno e vengono rinnovati automaticamente prima della scadenza. I certificati rinnovati vengono elaborati da un contenitore helper e quindi resi disponibili per il contenitore etcd. Nelle versioni interessate di Cisco DNA Center, il contenitore etcd non riconosce e non attiva dinamicamente i certificati rinnovati e continua a puntare ai certificati scaduti fino al riavvio di etcd. Dopo la scadenza del certificato, Cisco DNA Center non è più utilizzabile e in questo documento viene descritto come ripristinare l'installazione di Cisco DNA Center interessata.

Condizioni

Versioni interessate:
2.3.2.x

2.3.3.x

2.3.5.3

2.3.7.0

Versioni fisse:

2.3.3.7 HF4

2.3.5.3 HF5

2.3.5.4 dopo il 12 ottobre 2023

2.3.5.4 HF3

2.3.7.3

Sintomi

Alla scadenza del certificato, uno o più di questi sintomi saranno osservati.

1. L'interfaccia utente di Cisco DNA Center è inattiva

2. La maggior parte dei servizi è inattiva

3. Questi errori sono visualizzati nella 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
```

Ripristino

Per il ripristino è necessario accedere alla shell radice. Nella versione 2.3.x.x, la shell con restrizioni è stata abilitata per impostazione predefinita. Nella versione 2.3.5.x e successive, per accedere alla shell radice è necessaria la convalida del token di consenso. Se l'ambiente interessato è nella release 2.3.5.3, collaborare con il TAC per ripristinare l'installazione.

Passaggio 1: Verificare il problema

Dalla CLI, eseguire il comando

```
elenco membri etcdctl
```

Se il problema è dovuto alla scadenza del certificato, il comando avrà esito negativo e restituirà un errore. Se il comando viene eseguito correttamente, Cisco DNA Center non è interessato dal problema. Questo è un esempio dell'output di un'installazione eseguita con un certificato scaduto.

```
elenco membri etcdctl
client: il cluster etcd non è disponibile o non è configurato correttamente; errore n. 0: x509: il certificato è scaduto o non è ancora valido: l'ora corrente 2023-10-20T20:50:14Z è successiva a 2023-10-12T22:47:42Z
```

Passaggio 2: Verificare il certificato

Eseguire questo comando per verificare la data di scadenza del certificato.

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

Quando richiesto, immettere la password sudo. Nell'output verificare se il certificato è scaduto

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

Passaggio 4: Riavviare Docker

a. Svuotare i contenitori usciti

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

A seconda del numero di contenitori usciti, questa operazione può richiedere alcuni minuti.

b. Riavvia Docker

```
sudo systemctl restart docker
```

Questo comando riavvia tutti i contenitori e potrebbe richiedere da 30 a 45 minuti.

Passaggio 5: Verificare che il certificato sia stato rinnovato

Eseguire lo stesso comando dal passaggio 2 per verificare che il certificato sia stato rinnovato. Avrebbe dovuto rinnovarsi per un anno.

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

Verificare che la GUI sia accessibile e che l'accesso alla CLI non contenga errori.

Soluzione

Questa soluzione permetterà a Cisco DNA Center di restare operativo per un massimo di un anno. Per una correzione permanente, aggiornare l'installazione di Cisco DNA Center a una versione fissa, come indicato nella notifica sul campo FN74065.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).