將此變通方法應用於受Field Notice FN74065影響的Cisco DNA Center

目錄

簡介

本檔案介紹使用過期的etcd憑證復原Cisco DNA Center安裝的程式。Cisco DNA Center在2.3.2.0版中引入了etcd的數位證書，以確保通過Kubernetes進行安全的資料通訊，包括節點內和集群內節點之間的資料通訊。這些證書的有效期為一年，並在到期前自動續訂。由幫助器容器處理更新後的證書，然後使其可用於ETCD容器。在受影響的Cisco DNA Center版本中，etcd容器無法動態識別並啟用這些更新的證書，並繼續指向過期的證書，直到etcd重新啟動。證書到期後，Cisco DNA Center將不可操作，本文檔提供了恢復受影響的Cisco DNA Center安裝的步驟。

狀況

受影響的版本：
2.3.2.x

2.3.3.x

2.3.5.3

2.3.7.0

固定版本：

2.3.3.7 HF4

2.3.5.3 HF5

2.3.5.4 2023年10月12日之後

2.3.5.4 HF3

2.3.7.3

症狀

當證書過期時，將觀察到一個或多個這些症狀。

1. Cisco DNA Center的GUI已關閉

2.大多數服務已關閉

3.在CLI中可看到這些錯誤

```
<#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
```

復原

恢復需要訪問根shell。在2.3.x.x中，預設情況下啟用受限制的shell。在2.3.5.x及更高版本中，訪問根shell需要同意令牌驗證。如果受影響的環境是2.3.5.3版，請與TAC一起恢復安裝。

步驟1：驗證問題

在CLI上，執行命令

```
etcdctl成員清單
```

如果問題是由證書過期引起的，則命令將失敗並返回錯誤。如果命令成功運行，則Cisco DNA Center不會受到此問題的影響。 以下是使用過期憑證的有效安裝的輸出範例。

```
etcdctl成員清單
客戶端： etcd群集不可用或配置錯誤；錯誤#0: x509：證書已過期或尚未生效：當前時間2023-10-20T20:50:14Z在2023-10-12T22:47:42Z之後
```

步驟2：驗證憑證

運行此命令以驗證證書到期日期。

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

出現提示時，請輸入密碼。在輸出中，驗證憑證是否已過期

```
磁懸浮的[sudo]密碼：
subject=CN = etcd-client
issuer=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6, O = Cisco Systems， OU = Cisco DNA Center
notBefore=10月8日00:59:37 2022 GMT
notAfter=10月7日00:59:37 2023 GMT
subject=CN = etcd-peer
issuer=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6, O = Cisco Systems， OU = Cisco DNA Center
notBefore=10月8日00:59:37 2022 GMT
notAfter=10月7日00:59:37 2023 GMT
```

第4步：重新啟動Docker

a.清除已退出的容器

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

根據已退出容器的數量，這可能需要幾分鐘的時間。

b.重新啟動Docker

```
sudo systemctl restart docker
```

此命令將重新啟動所有容器，並可能需要30至45分鐘才能完成。

第5步：驗證證書是否已續訂

從步驟2發出相同命令以驗證憑證是否已續訂。應該再續一年。

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

驗證GUI是否可訪問，以及訪問CLI是否沒有錯誤。

解決方案

此解決方法將使Cisco DNA Center保持正常運行狀態，最多一年。如現場通知FN74065中所述，有關永久修復，請將Cisco DNA Center安裝升級到固定版本。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。