Field NoticeFN74065の影響を受けるCisco DNA Centerへの回避策の適用

内容

はじめに

このドキュメントでは、期限切れのetcd証明書を使用してCisco DNA Centerのインストールを回復する手順について説明します。Cisco DNA Centerは、ノード内およびクラスタ内のノード間の両方でKubernetesを介した安全なデータ通信を保証するために、リリース2.3.2.0でetcdのデジタル証明書を導入しました。これらの証明書は1年間有効で、有効期限が切れる前に自動的に更新されます。更新された証明書はヘルパーコンテナによって処理され、etcdコンテナで使用可能になります。該当するCisco DNA Centerリリースでは、etcdコンテナは更新された証明書を動的に認識してアクティブ化せず、etcdが再起動されるまで期限切れの証明書を指し示し続けます。証明書の期限が切れると、Cisco DNA Centerが動作不能になります。このドキュメントでは、該当するCisco DNA Centerのインストールを回復する手順について説明します。

条件

該当バージョン
2.3.2.x（2018年12月）

2.3.3.x（2015年9月）

2.3.5.3

2.3.7.0

修正バージョン：

2.3.3.7 HF4

2.3.5.3 HF5

2023年10月12日以降2.3.5.4

2.3.5.4 HF3

2.3.7.3

症状

証明書の期限が切れると、次の症状が1つ以上発生します。

1. Cisco DNA CenterのGUIがダウンしている

2.ほとんどのサービスがダウンしている

3. CLIに次のエラーが表示される

```
<#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
```

リカバリ

リカバリには、ルートシェルへのアクセスが必要です。2.3.x.xでは、制限付きシェルはデフォルトで有効になっています。2.3.5.x以降では、同意トークンの検証は、ルートシェルにアクセスするために必要です。該当する環境がリリース2.3.5.3である場合は、TACと協力してインストールを回復してください。

手順1：問題を確認します。

CLIから、次のコマンドを実行します。

```
etcdctlメンバリスト
```

証明書の期限切れが原因で問題が発生した場合、コマンドは失敗し、エラーが返されます。コマンドが正常に実行された場合、Cisco DNA Centerはこの問題の影響を受けません。 次に、期限切れの証明書を含む該当するインストールからの出力例を示します。

```
etcdctlメンバリスト
クライアント： etcdクラスタが使用できないか、または正しく構成されていません。エラー#0:
x509：証明書の有効期限が切れているか、まだ有効ではありません：現在時刻2023-10-
20T20:50:14Z is after 2023-10-12T22:47:42Z
```

手順2：証明書を確認します。

証明書の有効期限を確認するには、次のコマンドを実行します。

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

プロンプトが表示されたら、sudoパスワードを入力してください。出力で、証明書が期限切れかどうかを確認します

```
[sudo] maglevのパスワード：
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
```

ステップ4:Dockerを再起動します。

a.終了したコンテナをクリアします

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

終了したコンテナの数によっては、数分かかる場合があります。

b. Dockerを再起動します

```
sudo systemctl restart docker
```

このコマンドはすべてのコンテナを再起動します。完了するまで30 ~ 45分かかることがあります。

ステップ5：証明書が更新されたことを確認します。

手順2と同じコマンドを発行して、証明書が更新されたことを確認します。一年間も更新すべきだったのに。

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

GUIにアクセスでき、CLIへのアクセスにエラーがないことを確認します。

解決方法

この回避策により、Cisco DNA Centerは最大1年間稼働し続けます。永続的な修正については、Field NoticeFN74065で説明されているように、Cisco DNA Centerのインストールを修正済みリリースにアップグレードしてください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。