将此解决方法应用于受Field Notice FN影响的Cisco DNA Center74065

目录

简介

本文档介绍使用过期的etcd证书恢复Cisco DNA Center安装的过程。Cisco DNA Center在2.3.2.0版中引入了etcd的数字证书，以确保在节点内部和集群节点之间通过Kubernetes进行安全数据通信。这些证书的有效期为一年，并在到期前自动续订。由帮助器容器处理更新后的证书，然后使其可用于ETCD容器。在受影响的Cisco DNA Center版本中，etcd容器无法动态识别并激活这些更新的证书，并继续指向已过期的证书，直到etcd重新启动。证书到期后，Cisco DNA Center将无法运行，本文档提供了恢复受影响的Cisco DNA Center安装的步骤。

条件

受影响的版本:
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日之后

2.3.5.4 HF3

2.3.7.3

症状

证书到期时，将观察到一个或多个这些症状。

1.思科DNA中心的GUI已关闭

2.大多数服务已关闭

3.在CLI中可看到这些错误

```
<#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
```

恢复

恢复需要访问根外壳。在2.3.x.x中，默认情况下启用受限制的shell。在2.3.5.x及更高版本中，访问根外壳需要同意令牌验证。如果受影响的环境是2.3.5.3版，请与TAC一起恢复安装。

第1步：检验问题

从CLI运行命令

```
etcdctl member list
```

如果问题是由证书过期引起的，则命令将失败并返回错误。如果命令运行成功，则Cisco DNA Center不会受到此问题的影响。 这是使用过期证书的有效安装的输出示例。

```
etcdctl member list
客户端：etcd群集不可用或配置错误；错误#0:x509：证书已过期或尚未生效：当前时间2023-10-20T20:50:14Z在2023-10-12T22:47:42Z之后
```

第2步：验证证书

运行此命令以验证证书到期日期。

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

出现提示时，请输入密码。在输出中，验证证书是否已过期

```
磁悬浮的[sudo]密码：
subject=CN = etcd-client
issuer=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6,O =思科系统，OU =思科DNA中心
notBefore=Oct 8 00:59:37 2022 GMT
notAfter=Oct 7 00:59:37 2023 GMT
subject=CN = etcd-peer
issuer=CN = d0be82b3-0b50-e7bd-6bcd-b817c249f1c6,O =思科系统，OU =思科DNA中心
notBefore=Oct 8 00:59:37 2022 GMT
notAfter=Oct 7 00:59:37 2023 GMT
```

第4步：重新启动Docker

a.清除已退出的容器

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

根据已退出容器的数量，这可能需要几分钟的时间。

b.重新启动Docker

```
sudo systemctl restart docker
```

此命令会重新启动所有容器，并且可能需要30至45分钟才能完成。

第5步：验证证书已续订

从第2步发出相同命令以验证证书已续订。应该再续一年

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

验证GUI可访问并且访问CLI没有错误。

解决方案

此解决方法将使Cisco DNA Center保持运行状态并最多一年。如需永久修复，请将Cisco DNA Center安装升级到固定版本，如现场通知FN74065中所述。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。