排除无法连接到服务器X509证书过期的故障

目录

简介

本文档介绍解决 **Unable to connect to the server: x509: certificate has expired or is not yet valid** 错误.

问题

与Ultra Cloud Core Subscriber Microservices Infrastructure(SMI)Kubectl的连接会引发错误。

Kubernetes控制平面节点通信通过SSL隧道进行。SSL隧道通常依赖于一组受信任的第三方证书颁发机构来建立证书的真实性。

证书过期后，控制平面节点通信停止。

要检查证书到期，请执行以下操作： **kubectl get secrets --all-namespaces | grep 'kubernetes.io/tls' | awk '{print $2, $1}' | xargs -n2 sh -c 'echo container $0 namespace $1;kubectl -n $1 get secret $0 -o jsonpath="{.data.tls\.crt}" | base64 -d | openssl x509 -noout -enddate; echo ----------'**

```
cloud-user@k8-rcdn-primary-1:~$ kubectl get secrets --all-namespaces | grep 'kubernetes.io/tls'
| awk '{print $2, $1}' | xar
gs -n2 sh -c 'echo container $0 namespace $1;kubectl -n $1 get secret $0 -o
jsonpath="{.data.tls\.crt}" | base64 -d | open
ssl x509 -noout -enddate; echo ----------'
container cert-cli-cee-k8-rcdn-ops-center-ingress namespace cee-k8-rcdn
notAfter=May 1 16:54:39 2023 GMT
----------
container cert-docs-cee-k8-rcdn-product-documentation-ingress namespace cee-k8-rcdn
notAfter=May 1 16:56:04 2023 GMT
----------
container cert-grafana-ingress namespace cee-k8-rcdn
notAfter=May 1 16:56:06 2023 GMT
----------
container cert-restconf-cee-k8-rcdn-ops-center-ingress namespace cee-k8-rcdn
notAfter=May 1 16:54:40 2023 GMT
----------
container cert-show-tac-cee-k8-rcdn-ops-center-ingress namespace cee-k8-rcdn
notAfter=May 1 16:54:40 2023 GMT
----------
container cert-show-tac-cee-k8-rcdn-smi-show-tac-ingress namespace cee-k8-rcdn
notAfter=May 1 16:56:07 2023 GMT
----------
container cert-cli-smf-rcdn-ops-center-ingress namespace smf-rcdn
notAfter=May 1 16:54:56 2023 GMT
----------
```

```
container cert-restconf-smf-rcdn-ops-center-ingress namespace smf-rcdn
notAfter=May 1 16:54:57 2023 GMT
----------------------
container cert-show-tac-smf-rcdn-ops-center-ingress namespace smf-rcdn
notAfter=May 1 16:54:57 2023 GMT
----------------------
container cert-cli-smf-rcdn1-ops-center-ingress namespace smf-rcdn1
notAfter=May 1 16:55:07 2023 GMT
----------------------
container cert-restconf-smf-rcdn1-ops-center-ingress namespace smf-rcdn1
notAfter=May 1 16:55:08 2023 GMT
----------------------
container cert-show-tac-smf-rcdn1-ops-center-ingress namespace smf-rcdn1
notAfter=May 1 16:55:08 2023 GMT
----------------------
container cert-cli-smf-rcdn2-ops-center-ingress namespace smf-rcdn2
notAfter=May 3 18:11:26 2023 GMT
----------------------
container cert-restconf-smf-rcdn2-ops-center-ingress namespace smf-rcdn2
notAfter=May 3 18:11:28 2023 GMT
----------------------
container cert-show-tac-smf-rcdn2-ops-center-ingress namespace smf-rcdn2
notAfter=May 3 18:11:27 2023 GMT
----------------------
container cert-cli-smf-rcdn3-ops-center-ingress namespace smf-rcdn3
notAfter=May 3 18:11:41 2023 GMT
----------------------
container cert-restconf-smf-rcdn3-ops-center-ingress namespace smf-rcdn3
notAfter=May 3 18:11:43 2023 GMT
----------------------
container cert-show-tac-smf-rcdn3-ops-center-ingress namespace smf-rcdn3
notAfter=May 3 18:11:42 2023 GMT
----------------------
```

解决方案

1.验证apiserver.crt是否显示正确的结束日期。

```
ubuntu@labnode-cnat-cnat-core-primary1:~$ cd /data/kubernetes/pki
ubuntu@labnode-cnat-cnat-core-primary1:/data/kubernetes/pki$ sudo su
root@labnode-cnat-cnat-core-primary1:/data/kubernetes/pki# sudo cat
/data/kubernetes/pki/apiserver.crt | openssl x509 -enddate -noout
notAfter=Feb 17 08:22:04 2022 GMT
```

2.检查SSL中的结束日期。

```
ubuntu@labnode-cnat-cnat-core-primary1:~$ echo | openssl s_client -showcerts -servername
gnupg.org -connect localhost:6443 2>/dev/null | openssl x509 -inform pem -noout -text
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 44335566778899aabba (0xabcdef0123456789)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN = kubernetes
Validity
Not Before: Mar 17 11:59:23 2020 GMT
Not After : Mar 19 10:37:35 2021 GMT
```

3.检查docker容器状态。

```
root@labnode-cnat-cnat-core-primary1:/data/kubernetes/pki# docker ps -f "name=k8s_kube-
apiserver"
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
f988867819ed c2c9a0406787 "kube-apiserver --ad…" 12 months ago Up 12 months k8s_kube-
apiserver_kube-apiserver-labnode-cnat-cnat-core-primary1_kube-
system_00112233445566778899aabbccddeeff_0
root@labnode-cnat-cnat-core-primary1:/data/kubernetes/pki#
root@labnode-cnat-cnat-core-primary1:/data/kubernetes/pki# docker ps -f "name=k8s_kube-
controller"
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
929a8f1ef716 6e4bffa46d70 "kube-controller-man…" 3 days ago Up 3 days k8s_kube-controller-
manager_kube-controller-manager-labnode-cnat-cnat-core-primary1_kube-
system_112233445566778899aabbccddeeff00_2
root@labnode-cnat-cnat-core-primary1:/data/kubernetes/pki# docker ps -f "name=k8s_kube-
scheduler"
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
32783a2c3a71 ebac1ae204a2 "kube-scheduler --au…" 12 months ago Up 12 months k8s_kube-
scheduler_kube-scheduler-labnode-cnat-cnat-core-primary1_kube-
system_2233445566778899aabbccddeeff0011_1
root@labnode-cnat-cnat-core-primary1:/data/kubernetes/pki#
```

4.在所有三个控制平面节点上重新启动kube-apiserver和kube-scheduler的docker容器。

```
docker ps -f "name=k8s_kube-apiserver" -q | xargs docker restart
docker ps -f "name=k8s_kube-scheduler" -q | xargs docker restart
```

5.确认apiserver.crt显示正确的结束日期。

```
root@labnode-cnat-cnat-core-primary1:/data/kubernetes/pki# sudo cat
/data/kubernetes/pki/apiserver.crt | openssl x509 -enddate -noout
notAfter=Feb 17 08:22:04 2022 GMT
```

6.验证在SSL中更新了结束日期并且其结束日期正确。

```
echo | openssl s_client -showcerts -servername gnupg.org -connect localhost:6443 2>/dev/null |
openssl x509 -inform pem -noout -text
```

7.验证群集是否正常

有关操作的详细信息，请参阅思科超云核心 — 用户微服务基础设施指南。

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）。