Fehlerbehebung kann keine Verbindung mit dem X509-Serverzertifikat herstellen abgelaufen

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Lösung des **Unable to connect to the server: x509: certificate has expired or is not yet valid** fehler.

Problem

Verbindungen zu Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) Kubectl lösen den Fehler aus.

Unable to connect to the server: x509: certificate has expired or is not yet valid

Die Kommunikation auf der Kontrollebene erfolgt über SSL-Tunnel. Der SSL-Tunnel stützt sich in der Regel auf eine Reihe von vertrauenswürdigen Zertifizierungsstellen von Drittanbietern, um die Authentizität von Zertifikaten festzustellen.

Wenn das Zertifikat abgelaufen ist, wird die Kommunikation des Steuerungsebenenknotens beendet.

So überprüfen Sie den Ablauf von Zertifikaten: **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
----------------------
```

Lösung

1. Vergewissern Sie sich, dass auf apiserver.crt das richtige Enddatum angezeigt wird.

```
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. Überprüfen Sie das Enddatum in SSL.

```
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. Überprüfen Sie den Docker-Containerstatus.

```
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. Starten Sie die Docker-Container von kube-apiserver und kube-Scheduler auf allen drei Knoten der Kontrollebene neu.

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

5. Bestätigen Sie, dass apiserver.crt das richtige Enddatum anzeigt.

```
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. Vergewissern Sie sich, dass das Enddatum in SSL aktualisiert wurde und das korrekte Enddatum aufweist.

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

7. Überprüfen Sie, ob der Cluster fehlerfrei ist.

Einzelheiten zu den Abläufen finden Sie in den Leitfäden für die Cisco Ultra Cloud Core-Subscriber Microservices-Infrastruktur.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.