Risoluzione dei problemi relativi alla mancata connessione al certificato X509 del server scaduto

Sommario

Introduzione

In questo documento vengono descritte le procedure per **Unable to connect to the server: x509: certificate has expired or is not yet valid** errore.

Problema

Le connessioni a Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) Kubectl generano l'errore.

La comunicazione del nodo del control plane Kubernetes avviene attraverso il tunnel SSL. Per stabilire l'autenticità dei certificati, il tunnel SSL in genere si basa su un insieme di autorità di certificazione di terze parti attendibili.

Quando il certificato è scaduto, la comunicazione del nodo del control plane si interrompe.

Per verificare la scadenza dei certificati: **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
----------------------
```

Soluzione

1. Verificare che apiserver.crt visualizzi la data di fine corretta.

```
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. Controllare la data di fine 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. Controllare lo stato del contenitore docker.

```
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. Riavviare i contenitori docker di kube-apiserver e kube-scheduler su tutti e tre i nodi del control plane.

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

5. Confermare che apiserver.crt mostri la data di fine corretta.

```
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. Verificare che la data di fine sia aggiornata in SSL e che la data di fine sia corretta.

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

7. Verificare che il cluster sia integro

Per ulteriori informazioni sulle operazioni, consultare le guide all'infrastruttura Cisco Ultra Cloud Core - Subscriber Microservices.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).