

Dépannage de l'impossibilité de se connecter au certificat X509 du serveur expiré

Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

Introduction

Ce document décrit les étapes à suivre pour résoudre `Unable to connect to the server: x509: certificate has expired or is not valid` ERREUR .

Problème

Connexions à l'infrastructure de microservices d'abonné de noyau de cloud Ultra (SMI) Kubectl jeter l'erreur.

La communication du noeud du plan de contrôle Kubernetes se fait par tunnel SSL. Le tunnel SSL repose généralement sur un ensemble d'autorités de certification tierces de confiance pour établir l'authenticité des certificats.

Lorsque le certificat a expiré, la communication du noeud du plan de contrôle s'arrête.

Pour vérifier l'expiration des certificats : `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}' | xargs
gs -n2 sh -c 'echo container $0 namespace $1;kubectl -n $1 get secret $0 -o
jsonpath="{.data.tls\.crt}" | base64 -d | openssl
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
-----
```

Solution

1. Vérifiez que le fichier apiserver.crt affiche la date de fin correcte.

```
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. Vérifiez la date de fin dans 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. Vérifiez l'état du conteneur 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 eba1ae204a2 "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. Redémarrez les conteneurs docker de kube-apiserver et kube-scheduler sur les trois noeuds du plan de contrôle.

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

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

5. Vérifiez que le fichier apiserver.crt affiche la date de fin correcte.

```
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. Vérifiez que la date de fin est mise à jour dans SSL et qu'elle est correcte.

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

```
openssl x509 -inform pem -noout -text
```

7. Vérifiez que le cluster est sain

Pour plus d'informations sur les opérations, reportez-vous aux [guides Cisco Ultra Cloud Core - Subscriber Microservices Infrastructure](#).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.