

# Solução de problemas Não foi possível conectar ao servidor Certificado X509 expirado

## Contents

[Introduction](#)

[Problema](#)

[Solução](#)

## Introduction

Este documento descreve as etapas para resolver o `Unable to connect to the server: x509: certificate has expired or is not valid` ERRO.

## Problema

As conexões com o Kubectl do Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) geram o erro.

A comunicação do nó do plano de controle Kubernetes acontece através do túnel SSL. O túnel SSL normalmente depende de um conjunto de autoridades de certificação de terceiros confiáveis para estabelecer a autenticidade dos certificados.

Quando o certificado expira, a comunicação do nó do plano de controle para.

Para verificar a expiração de certificados: `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
-----
```

## Solução

### 1. Verifique se apiserver.crt mostra a data final correta.

```
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. Verifique a data final em 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: 44335566778899aabbba (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. Verifique o estado do contêiner do 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. Reinicie os contêineres docker do kube-apiserver e do kube-scheduler nos três nós do plano de controle.

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

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

### 5. Confirme se apiserver.crt mostra a data final correta.

```
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. Verifique se a data final está atualizada em SSL e se ela tem a data final correta.

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

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

### 7. Verifique se o cluster está íntegro

Consulte os [guias Cisco Ultra Cloud Core - Subscriber Microservices Infrastructure](#) para obter detalhes sobre as operações.

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.