Kubernetes certificate management on the Flow Enterprise cluster

> **Note:** The commands in this article are available in Kubernetes version 1.19 and above. The format may change in future versions.

When installing Flow Enterprise Server, the underlying Kubernetes system generates Public Key Infrastructure (PKI) certificates for the internal use of the cluster. These certificates are used by components of the Kubernetes control plane and nodes to authenticate with each other.

Kubernetes manages these PKI certificates, but they are designed to expire after **one year**. Monitor the expiration dates of the cluster's PKI certificates and proactively update them once a year. If the certificates aren't updated, Flow will be unavailable and pods won't restart. Update certificates at any point before expiration.

Pluralsight provides utility scripts to manage the certificates. Make sure to download the latest `flow-enterprise-tools` package version 2.1.1.2 or higher to the primary node of the cluster and unzip it.

There are two new utilities included in the bin folder:

- `flow-cert-check` performs a check of all SSL certificates involved in the Kubernetes stack, except for the application url FQDN SSL certificate
- `flow-rotate-certs` allows you to rotate either selected or all certificates in the Kubernetes stack

On the primary node, check the current status of the certificates by running `sudo ./flow-cert-check`. A sample output is provided below:

```
[root@primary-node bin]$ sudo ./flow-cert-check

[INFO] Checking certificate status of all components..

[INFO] Checking cluster certificate expiration status ..

[check-expiration] Reading configuration from the cluster...

[check-expiration] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -oyaml'



CERTIFICATE            EXPIRES                RESIDUAL TIME CERTIFICATE AUTHORITY  EXTERNALLY MANAGED

admin.conf             Oct 26, 2022 22:47 UTC   355d                            no

apiserver              Oct 26, 2022 22:47 UTC   355d         ca                 no

apiserver-etcd-client    Oct 26, 2022 22:47 UTC   355d         etcd-ca            no
```

```
apiserver-kubelet-client Oct 26, 2022 22:47 UTC   355d          ca                  no

controller-manager.conf  Oct 26, 2022 22:47 UTC   355d                              no

etcd-healthcheck-client  Oct 26, 2022 22:47 UTC   355d          etcd-ca             no

etcd-peer                Oct 26, 2022 22:47 UTC   355d          etcd-ca             no

etcd-server              Oct 26, 2022 22:47 UTC   355d          etcd-ca             no

front-proxy-client       Oct 26, 2022 22:47 UTC   355d          front-proxy-ca      no

scheduler.conf           Oct 26, 2022 22:47 UTC   355d                              no



CERTIFICATE AUTHORITY   EXPIRES                  RESIDUAL TIME   EXTERNALLY MANAGED

ca                      Oct 24, 2031 22:47 UTC   9y              no

etcd-ca                 Oct 24, 2031 22:47 UTC   9y              no

front-proxy-ca          Oct 24, 2031 22:47 UTC   9y              no

[INFO] envoy proxy certificate validity dates:

notBefore=Oct 25 22:50:05 2021 GMT

notAfter=Oct 26 22:50:05 2022 GMT

[INFO] contour certificate validity dates:

notBefore=Oct 25 22:50:05 2021 GMT

notAfter=Oct 26 22:50:05 2022 GMT

[INFO] Replicated registry PKI cert validity dates:

notBefore=Oct 26 22:50:06 2021 GMT

notAfter=Oct 26 22:50:06 2022 GMT
```

If you need to rotate your certificates, use `flow-rotate-certs`. See the help text for this script with additional context by running it with the `-h` flag.

```
[root@primary-node bin]$ sudo ./flow-rotate-certs -h

This script rotates the Contour/Envoy proxy certs by recreating the certgen job

in the projectcontour namespace. The order of execution should be
```

```
    - rotate kubernetes api server cert with -k

    - rotate contour/envoy proxy certs with -c

    - rotate Replicated registry cert with -r

Flag -a|--all will accomplish the same steps in order.



Usage:      flow-rotate-certs [flags]



Available Flags:

    -a|--all          rotate all certs in the cluster

    -r|--registry     rotate embedded registry certs

    -c|--contour      rotate contour/envoy certs

    -k|--kube-api     rotate kubernetes api server certs

    -h|--help         print this help
```

Run this script with the `-a` flag to rotate all certs if desired.

> **Note**: If you choose to rotate the certificates individually, make sure you do them in the appropriate order as listed in the output from the `-h` flag.

```
[root@primary-node bin]$ sudo ./flow-rotate-certs -a

[INFO] Updating kubernetes api server certs..

[renew] Reading configuration from the cluster...

[renew] FYI: You can look at this config file with 'kubectl -n kube-system get cm kubeadm-config -oyaml'



certificate embedded in the kubeconfig file for the admin to use and for kubeadm itself renewed

certificate for serving the Kubernetes API renewed

certificate the apiserver uses to access etcd renewed
```

```
certificate for the API server to connect to kubelet renewed

certificate embedded in the kubeconfig file for the controller manager to use renewed

certificate for liveness probes to healthcheck etcd renewed

certificate for etcd nodes to communicate with each other renewed

certificate for serving etcd renewed

certificate for the front proxy client renewed

certificate embedded in the kubeconfig file for the scheduler manager to use renewed

[INFO] Updating Contour/Envoy Proxy certs ..

[INFO] Deleting previous certgen job from projectcontour namespace.

job.batch "contour-certgen-v1.14.1" deleted

[INFO] Applying new job definition.

job.batch/contour-certgen-v1.14.1 created

[INFO] Contour certificate rotate job submitted.

Waiting on jobs to complete = 0

[INFO] Here are the new contour/envoy proxy cert expiration dates.

[INFO] envoy proxy certificate validity dates:

notBefore=Oct 25 22:50:05 2021 GMT

notAfter=Oct 26 22:50:05 2022 GMT

[INFO] contour certificate validity dates:

notBefore=Oct 25 22:50:05 2021 GMT

notAfter=Oct 26 22:50:05 2022 GMT

/tmp/registry_pkiGbk /home/root/flow-enterprise-tools/bin

Generating a RSA private key

.........+++++

....+++++
```

```
writing new private key to 'registry.key'

-----

Signature ok

subject=CN = registry.kurl.svc.cluster.local

Getting CA Private Key

/home/root/flow-enterprise-tools/bin

[INFO] Registry PKI cert rotation completed.
```

Run `flow-cert-check` again to ensure all certificates have been renewed.

At this point, your certificates are updated. Refresh the Flow application URL on your browser to ensure the application is running as expected.

> **Note**: You do not need to restart any additional pods on the primary node for the renewed certificates to take effect. However, if you see any failures, please gather the events log using `kubectl get event` and contact support@pluralsight.com ().

back to top

If you need help, please email support@pluralsight.com () for 24/7 assistance.