



Automatic certificate renewal cron job for Flow Enterprise Server

Tags: **Flow on-prem**

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.

Read more about [Kubernetes certificate management on the Flow Enterprise Server cluster](#).

Kubernetes certificates expire every year and need to be regularly renewed. These renewals sometimes surprise system maintainers. To avoid surprises and keep certificates renewed, follow these steps to create a cron job to renew the certificates regularly.

In this article

[Install the tools package](#)

[Create the cron job](#)

[Test the cron job](#)

Install the tools package

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. Make sure you don't already have a `flow-enterprise-tools` folder, then extract the package using `tar -xvf flow-enterprise-tools-<channel>[-airgap]-<version>.tar.gz`. If you already have a `flow-enterprise-tools` folder, either rename the folder or extract the package elsewhere.

Install `flow-enterprise-tools` on the primary node by running `cd flow-enterprise-tools sudo ./install-enterprise-tools.sh`. Then follow the prompts to set the path location and installation location.

[back to top](#)

Create the cron job

Next, create a `flow-rotate-certs` file.

```
cd /etc/cron.d/ vim flow-rotate-certs
```

Paste the following template into the `flow-rotate-certs` file to automatically renew the certificates every 90 days.

```
# rotate Kubernetes certificates every 90 days
# certificates expire after one year but renewing every 90 days makes it easier to validate the certificates
regularly

0 5 */90 * * root KUBECONFIG=/etc/kubernetes/admin.conf /opt/flow-enterprise-tools/bin/flow-rotate-certs -a
>> /var/log/flow-rotate-certs.log 2>&1
```

Note: While certificates only need to be renewed once a year, renewing them every 90 days makes it easier to ensure the certificates are regularly updated. If you'd prefer to use a different time interval, change the day value from 90 to whatever your preferred day interval is.

[back to top](#)

Test the cron job

To make sure this cron job is working, test the cron job by changing the interval, then tailing the log file to make sure the certificates are updating. To tail the log file use `tail -f /var/log/flow-rotate-certs.log`.

A good test is to have the job run every six seconds to make sure the certificates are updating correctly. To run this test, add the following line to the `/etc/cron.d/flow-rotate-certs` file. Once you've verified it's working correctly, remove this line so the job doesn't keep running every six seconds.

```
*/10 * * * * root KUBECONFIG=/etc/kubernetes/admin.conf /opt/flow-enterprise-tools/bin/flow-rotate-certs -a >>
/var/log/flow-rotate-certs.log 2>&1
```

Important: Remove this test line once you've verified the job is working correctly.

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