Flow Enterprise monitoring tools

Tags: Flow Enterprise Server

As part of the KOTS package, Flow comes with Prometheus alertmanager and Grafana pre-installed. It also comes configured with basic alerts.

> **Note:** To use these services you must have Flow version 2020.3.1-4 or newer and kotsadm 1.19.6 or higher version. Use the most updated version of `flow-enterprise-tools` to configure these services. If you have `flow-enterprise-tools` version 2.1.1.1 or previous, you must use a `flow-support-tools` version before 1.0.3.3 to configure these services.

> **Important:** Securing the monitoring components requires that the TLK certificates used for Flow are signed by a **valid public certificate authority**, like Sectigo, Verisign, Digicert, Entrust, etc. Internal certificate authorities will not work with this configuration. If your certificates are signed by an internal certificate authority, the standard dashboard will not display the stock graphs on the Flow admin console due to certificate trust issues. However, this does not limit the underlying functionality of Grafana or Prometheus.

By default, Prometheus and Grafana are enabled on non-TLS ports. But there is an installation tool in the `flow-enterprise-tools` package to secure those services to use the existing TLS certificates you used to configure your Flow URL. Enable this if you want to monitor alerts from the Kubernetes system.

Prometheus and Grafana support Flow running directly on an internal server as well as running behind a supported load balancer.

In this article

Configuring access

Install Flow as directed. The default installation creates Prometheus and Grafana services in the **monitoring** namespaces. Access the service using http protocol if desired.

In the example below, `http://<ipaddress of node>:30902` provides access to the Grafana portal.

> **Note:** Access will not be secured at this point. Secure access to Prometheus and Grafana using the steps provided below.

```
user@primary-node:~/flow-enterprise-tools$ kubectl -n monitoring get svc

NAME                TYPE       CLUSTER-IP    EXTERNAL-IP PORT(S)                AGE

alertmanager-operated    ClusterIP   None        <none>     9093/TCP,9094/TCP,9094/UDP 36h

grafana             NodePort    10.96.1.224   <none>     80:30902/TCP            36h

grafana-internal       ClusterIP   None        <none>     3000/TCP              36h

kube-state-metrics      ClusterIP   10.96.0.72    <none>     8080/TCP              36h

prometheus-adapter      ClusterIP   10.96.0.103   <none>     443/TCP               36h

prometheus-alertmanager  NodePort    10.96.1.198   <none>     9093:30903/TCP          36h

prometheus-k8s         NodePort    10.96.1.216   <none>     9090:30900/TCP          36h

prometheus-node-exporter ClusterIP   10.96.3.233   <none>     9100/TCP              36h

prometheus-operated     ClusterIP   None        <none>     9090/TCP              36h

prometheus-operator     ClusterIP   10.96.3.74    <none>     8080/TCP              36h

prometheus-pushgateway   ClusterIP   10.96.3.10    <none>     9091/TCP              36h
```

The default admin identification and password for Grafana is printed in the console when you install Flow. It is also available in the `flow-install-stable.log` file for reference and at the end of running the script noted below.

To secure access to both Prometheus and Grafana via TLS:

1. Download the latest version of `flow-enterprise-tools` on the primary node of the cluster. Contact Pluralsight Support for the download link. The file name is of the format `flow-enterprise-tools-stable-X.X.X.X.tar.gz`
2. Extract the `flow-enterprise-tools` package
3. Change directory to the `bin` directory and run `./flow-secure-monitoring-services.sh -H "fully-qualified-host-name"`

> **Note:** The fully qualified host name must be the Flow application URL used during the Flow installation. If you installed Flow behind a load balancer, this hostname would be the load balancer fully qualified domain name (FQDN).

4. The output should look like below:

```
user@primary-node:~/flow-enterprise-tools/bin$ ./flow-secure-monitoring-services -H
flow.mydomain.com
[INFO] Securing monitoring endpoints ..
[INFO] Setting external URL for Prometheus
prometheus.monitoring.coreos.com/k8s replaced
[INFO] Setting external URL for grafana
NAME      DATA   AGE
grafana   1      36h
configmap/grafana replaced
[INFO] Searching for pods...
[INFO] Found 1 pods
[INFO] Deleting pod grafana-7658d88cf-bnh9s
pod "grafana-7658d88cf-bnh9s" deleted
[INFO] Deleting non-TLS services for Grafana, Prometheus and AlertManager
service "grafana" deleted
service "prometheus-k8s" deleted
[INFO] Grafana login user id is : admin
[INFO] Grafana login password is : A4pKQiGMh
[INFO] SUCCESS
```

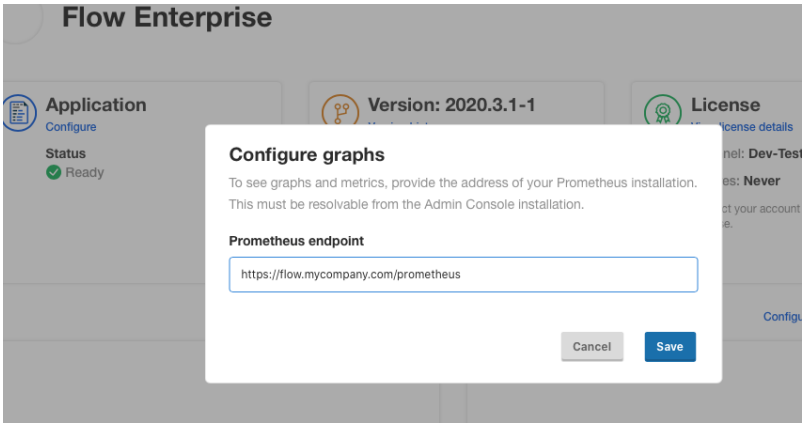
5. The services should look like the following in the **monitoring** namespace. The non-TLS services, with the type NodePort are removed.

```
user@primary-node:~/flow-enterprise-tools/bin$ kubectl -n monitoring get svc
NAME                    TYPE        CLUSTER-IP     EXTERNAL-IP   PORT(S)                  AGE
alertmanager-operated   ClusterIP   None           <none>        9093/TCP,9094/TCP,9094/UDP   36h
grafana-internal        ClusterIP   None           <none>        3000/TCP                 36h
kube-state-metrics      ClusterIP   10.96.0.72     <none>        8080/TCP                 36h
prometheus-adapter      ClusterIP   10.96.0.103    <none>        443/TCP                  36h
prometheus-alertmanager NodePort    10.96.1.198    <none>        9093:30903/TCP           36h
prometheus-node-exporter ClusterIP  10.96.3.233    <none>        9100/TCP                 36h
prometheus-operated     ClusterIP   None           <none>        9090/TCP                 36h
prometheus-operator     ClusterIP   10.96.3.74     <none>        8080/TCP                 36h
prometheus-pushgateway  ClusterIP   10.96.3.10     <none>        9091/TCP                 36h
```

6. Log in to the Flow admin console, usually located at `https://<flow app url>:8800`

7. Click **Configure Prometheus Address**

8. Enter the URL `https://<flow app url>/prometheus` in the Prometheus Endpoint box. Click **Save**.



Access Prometheus at `https://<flow app url>/prometheus`.

Access the Prometheus alertmanager at `https://<flow app url>/alertmanager`.

Access Grafana at `https://<flow app url>/grafana`.

back to top

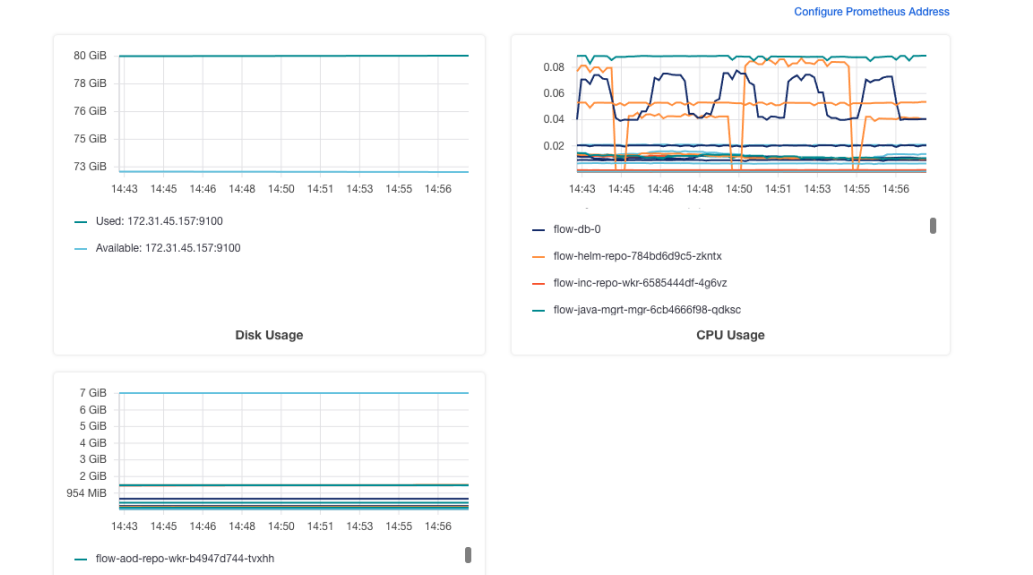
What do I do when upgrading Flow?

When you update Flow via the Flow admin console, the non-TLS services will return to in-service state. As part of the upgrade process, rerun the configuration steps above after every patch update and major version upgrade.

back to top

Troubleshooting

If the stock graphs are not displaying on the admin console at port 8800, it's most likely a certificate trust issue. When graphs are working, they should look something like the below screenshot.



`Kotsadm-pod` will display the following error message when using the `kubectl logs -f kotsadm-<unique identifier>` command if you're experiencing a certificate trust issue. Use the errors in the log output to verify you've loaded the certificates correctly.

```
{"level":"error","ts":1604508300.2007086,"msg":"failed to prometheus query range: failed to do req: Get \"https://                    /prometheus/api/v1/query_range?end=1604508300&query=sum%28rate%28container_cpu_usage_seconds_total%7Bnamespace%3D%22default%22%2Ccontainer%21%3D%22POD%22%2Cpod%21%3D%22%22%7D%5B5m%5D%29%29+by+%28pod%29&start=1604507400&step=11\": x509: certificate signed by unknown authority"}
```

If you need help, please contact Pluralsight Support.