

Syslog

This section explains how to set up and manage Syslog for your KumoScale application using the KumoScale Syslog custom resource file.

KumoScale software supports configuring a Syslog server to log KumoScale events. The KumoScale Provisioner service reads the Syslog configuration from the KumoScale storage nodes, collects event data from the connected application initiators, and sends these to the Syslog server. This page shows how to configure Syslog using custom resource files. For your orchestration environment, you may need to reference the relevant interface guide: [KumoScale REST API](#), [Cluster Manager CLI](#), [KumoScale Ansible](#), [KumoScale Kubernetes CSI Driver](#), or [KumoScale for OpenStack](#).

This page covers:

- [Configuring Syslog for KumoScale](#)
- [Creating a Syslog secret \(for TLS/SSL\)](#)
- [Syslog message format](#)

Configure Syslog for KumoScale

To configure a Syslog server to log KumoScale events, KumoScale software provides a **Syslog CRD**, a template of which is in **KumoScale_Operator/ks-config-operator/samples/kumoscale_v1_syslog_cr.yaml**. The table below shows the parameters supported in the Syslog CRD.

Syslog Parameter	Description	Optional/Required
url	The initiator url of the server in the format of: <protocol>://<ip/host>:<port>.	Required
useTls	Whether or not a secure connection should be used with TLS/SSL (the default is false).	Optional
certSecretName	The name of the secret that contains the certificate for this Syslog. See Syslog Secret for TLS/SSL for instructions on how to create a secret for the Syslog.	Required when UseTls=True

To configure and manage the Syslog, you will need to update the CRD with the appropriate values for your application. Use kubectl to create, modify, or delete a Syslog.

Create a Syslog with:

```
kubectl create -f <syslog-cr-file>
```

Update a Syslog with:

```
kubectl apply -f <syslog-cr-file>
```

Delete a Syslog with:

```
kubectl delete -f <syslog-cr-file>
```

For example, to configure Syslog to log KumoScale events for the initiator with url udp://172.##.###.##:10514 and without TLS/SSL:

- Make a copy of **kioxia.com_v1_syslog_cr.yaml** for editing, and save to a separate directory, for example **deploy/crds/myapp_syslog_cr.yaml**.
- Update and save **myapp_syslog_cr.yaml** with **name (syslog1)**, **url (udp://172.##.###.##:10514)** as shown below:

```
apiVersion: kumoscale.kioxia.com/v1
kind: Syslog
metadata:
  name: syslog1
spec:
  syslog:
    url: udp://172.##.###.##:10514
    useTls: false
```

- Create syslog1:

```
kubectl create -f myapp_syslog_cr.yaml
```

- Verify the Syslog service was created:

```
kubectl get syslog
```

- Once Syslog is configured for the storage cluster, you can also use

```
kubectl describe storagenodes
```

All storage nodes should report Syslog under the STATUS section.

A KumoScale software alarm is triggered if a Syslog server cannot be reached.

Syslog Secret for TLS/SSL

If the Syslog uses TLS/SSL you will need to create a Syslog secret from the Syslog certificate before you can create the Syslog. The secret should contain the syslog certificate base64 encoded. A secret CR file is included in **KumoScale_Operator/ks-config-operator/deploy/syslog-secret.yaml**.

1. Create a Syslog certificate secret **syslog-secret.yaml** from the certificate file with:

```
kubect1 create secret generic syslog-secret --from-file=cert=<path to certificate file>
```

2. Create the Syslog certificate:

```
kubect1 create -f syslog-secret.yaml
```

Note: If you need to update the secret - use **kubect1 replace** (not **apply**), otherwise sensitive data will be shown when using **kubect1 get secret -o yaml**

Syslog Message Format

Syslog Header

The header is configured according to the Syslog section in [Syslog Request for Comments \(RFC\) 5424](#):

Field	Description/Comments
PRI	A calculation regarding severity and priority. It is implemented according to the definition in the Syslog RFC, where Facility = 1 .
Host Name	The KumoScale ID
Application Name	“KumoScale”
Timestamp	The timestamp when the message sent

Syslog Body

Field	Description / Comments
The MSG	The Syslog message. For instance: <i>User Name executed command yyy’</i> for a command or <i>Event description</i> (for an event).
MSG Body	A map of pairs: <SD-ID, SD-PARAM> (SD=Structured Data) of the command ID, input, and output, or event ID and entity name (for an event).

Next: [Logging, Monitoring, and Alerting](#)
