Standard Operating Procedure

*Sumo Logic Integration*

## PURPOSE

The purpose of this standard operating procedure (SOP) is to provide a detailed step-by-step procedure to integrate Sumo Logic.

## PROCEDURE

1. Request will come to push pods logs of service, projects, projects prefix (i.e. blue in this scenario) to Sumo Logic.
2. Log in as system:admin:

login --username=system:admin

1. Go into project named logging:

oc get projects

cd project logging

1. Check ds and pvc:

os get ds

oc get pvc

there is one file for nginx and one file for pciapp

1. Go to the relevant project:

oc project <project name>

1. home/svc-vxby-ose/OpenShift/artifacts/logging/<project name> (change *vxby* based on location)

Red Hat has created scripts to create DaemonSets for logging project which creates Fluentd pods on region=primary label nodes.

1. Copy the following scripts:

cp -fr sumologic-presentationapp-install.sh sumologic-blue-install.sh

cp -fr sumologic-presentationapp-template.yaml sumologic-blue-template.yaml

cp -fr sumologic-presentationapp-uninstall.sh sumologic-blue-uninstall.sh

1. Change file owner and change the user:

chown -R svc-vxby-ose:svc-vxby-ose \* (change *vxby* based on location)

su – svc-vxby-ose

1. Need to create secrets accordingly for each of collector source. Secrets are created with collector-URL as key value as endpoint URL collected from Sumo Logic.

These secrets are opaque secrets and passed env variables to pods and thus enable pods of particular DaemonSets to send logs to particular collector URL.

Edit sumologic-blue-install.sh

*Look for “oc create secret generic sumologic”*

*:%s/presentationapp/blue/g*

This will take blue path from the ansible host

Make this change for sumologic-blue-template.yaml

fluentd\_sumologic\_<project name>

sumologic\_include\_<project name>\_…

1. Edit /etc/ansible/hosts

Add

sumologic\_include\_path=/mnt/log/containers/blue-\*\_<project name>\_\*.log

1. Double check sumologic-blue-install.sh for blue path

Modified 4 lines.

Include EXECUTE\_NAMESPACE\_REGEX by uncommenting it.

1. After modifying Red Hat scripts accordingly, need to run Red Hat scripts and it will trigger Fluentd pods on each of the nodes to collect logs.

sh sumologic-blue-install.sh

check for “success”.

1. oc get ds

verify that the new DaemonSet

fluentd-sumologic-blue

is there and region=primary

1. oc get pods

oc describe pods

oc project <project name>

oc get dc

oc get pods

oc get routes

oc scale dc/blue ---replicas=0

oc get pods

oc scale dc/blue --replicas =2

oc get pods

oc project logging

oc get pods

oc rsh flentd-sumologic-blue-<name>

cd /mnt/log/containers

ls -la

verify blue pods.

cat <name of the blue log>.log

To see the logs, which would post to Sumo Logic.

Check *var/lib/docker*

1. Test and verify Sumo Logic logs in dashboard.

## VALIDATION

Follow the validation steps in “Procedure”.

**Document Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Effective Date | Reviewed by | Approved by |
| 1.0 | 10/1/2018 | KyungIn Kim | Yashi Kumar |
|  |  |  |  |

Document Modification History & Revision Log

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Date Modified | Revised by | Role | Section Affected | Reference | Remarks |
| 1.0 |  |  |  |  |  |  |
| 1.1 |  |  |  |  |  |  |