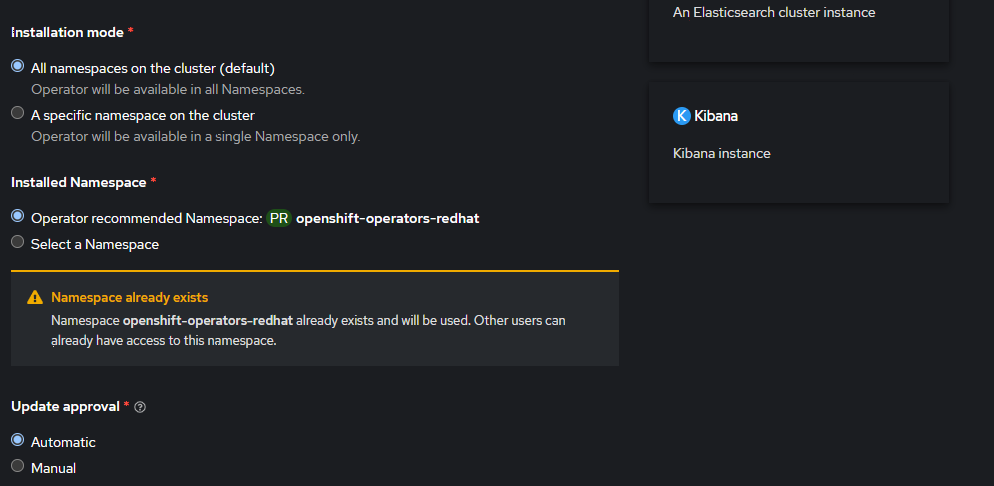
EFK SETUP USING OPERATORS IN OPENSHIFT :

--- GO TO ADMINSTRATOR >> OPERATORHUB :

* INSTALL BELOW OPERATPRS :

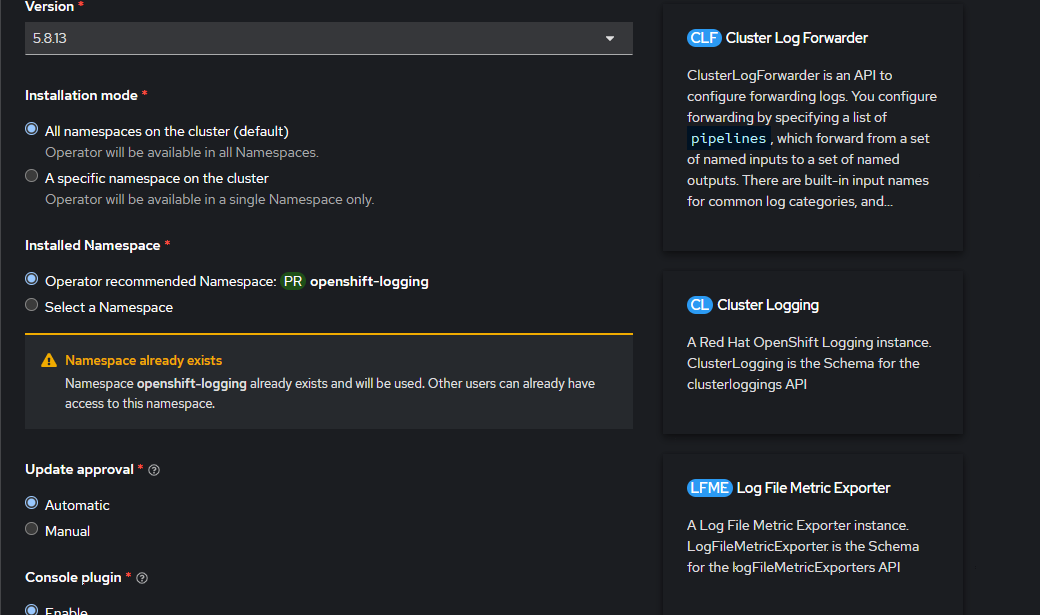
OpenShift Elasticsearch Operator

VERSION : 5.8

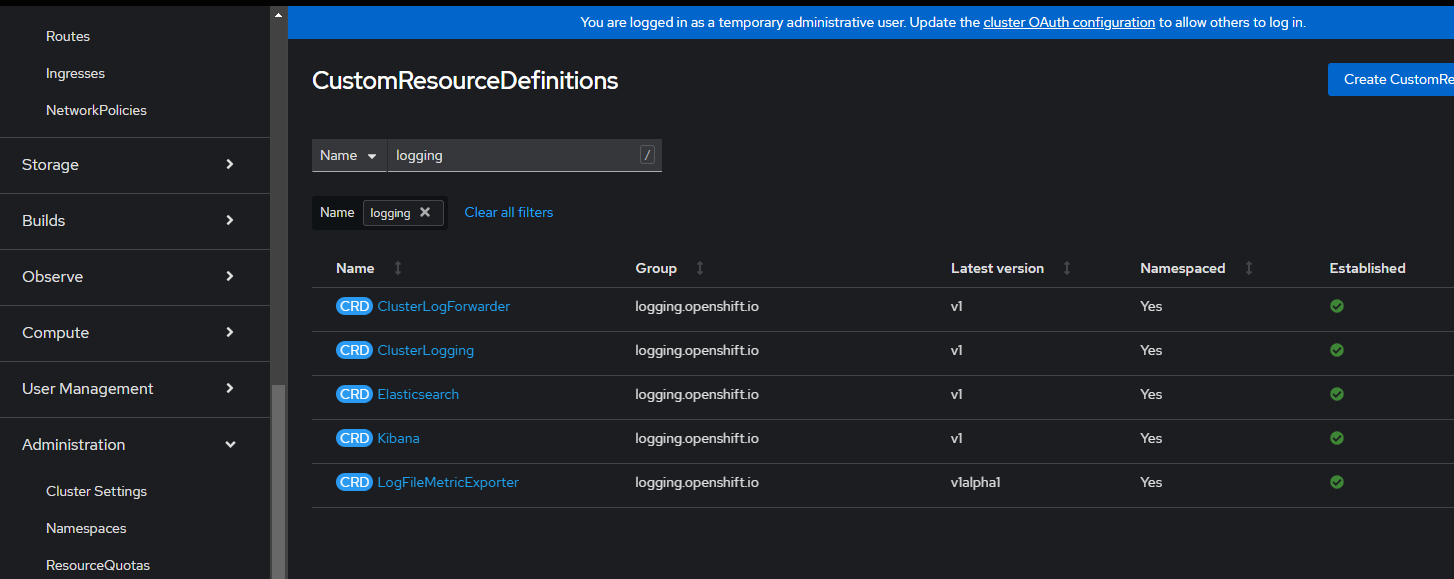


* Click install ..

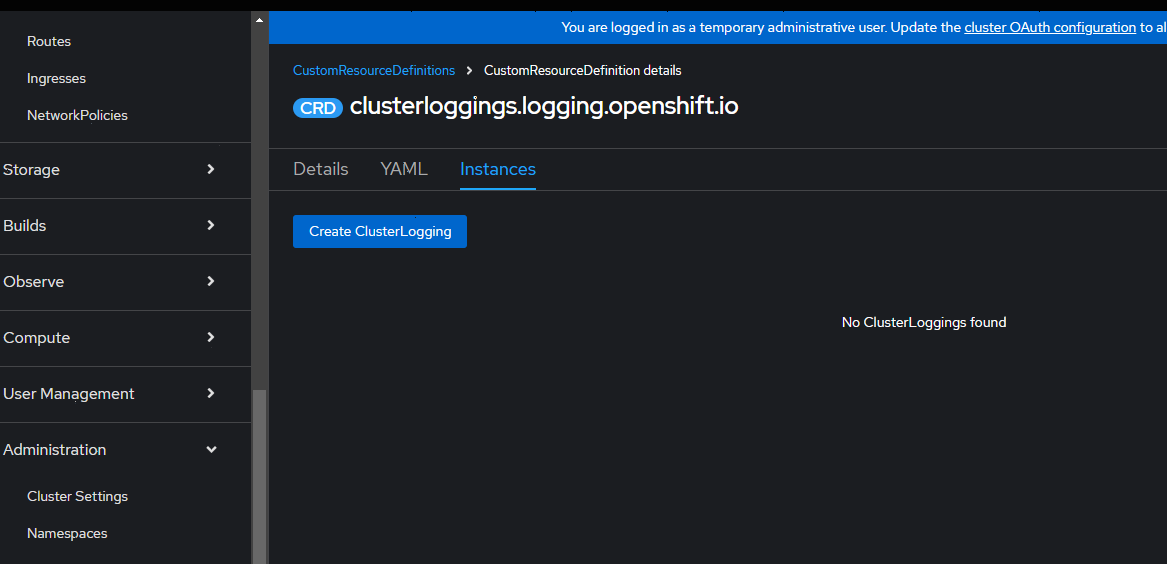
--- Search for Red Hat OpenShift Logging operator , version : 5.8 : install that too



* NOW go to Administrator >> Administration >> Customresource defn >> and search for clusterlogging crd :



* Go to instances >> create cluster logging instance :



* Create a clusterlogging instance by updating the yaml as below :

apiVersion: "logging.openshift.io/v1"

kind: "ClusterLogging"

metadata:

name: "instance"

namespace: "openshift-logging"

spec:

managementState: "Managed"

logStore:

type: "elasticsearch"

retentionPolicy:

application:

maxAge: 1d

infra:

maxAge: 3d

audit: # Changed from "aud" to "audit"

maxAge: 3d

elasticsearch:

nodeCount: 3

storage:

storageClassName: gp3-csi

size: "20G"

resources:

requests:

memory: "4Gi" # Memory request

limits:

memory: "8Gi" # Optional limit for better resource management

redundancyPolicy: "SingleRedundancy"

visualization:

type: "kibana"

kibana:

replicas: 1

resources:

requests:

memory: "256Mi" # Correct placement

limits:

memory: "256Mi" # Correct placement

proxy:

resources:

requests:

memory: "256Mi" # Ensure correct indentation

limits:

memory: "256Mi" # Ensure correct indentation

curation:

type: "curator"

curator:

schedule: "30 3 \* \* \*" # Ensure proper cron schedule syntax

collection:

logs:

type: "fluentd"

fluentd: {}

* Create instance , than go to workloads >> check pods in openshift-logging namespace and openshift-redhat-operator namespace
* Now go to routes >> kibana >> serve the url :

