Filebeat + ELK Stack Tutorial With Kubernetes

`ArtifactHub Official`

```
# Kibana Helm Chart
https://artifacthub.io/packages/helm/elastic/kibana

# Logstash Helm Chart
https://artifacthub.io/packages/helm/elastic/logstash

# Filebeat Helm Chart
https://artifacthub.io/packages/helm/elastic/filebeat

# Elasticsearch Helm Chart
https://artifacthub.io/packages/helm/elastic/elasticsearch
```

`Installing Helm (Ubuntu)`

```
https://helm.sh/docs/intro/install/
```

Members of the Helm community have contributed a **Helm package** for Apt. This package is generally up to date.

```
curl https://baltocdn.com/helm/signing.asc | gpg --dearmor | sudo tee
/usr/share/keyrings/helm.gpg > /dev/null
sudo apt-get install apt-transport-https --yes
echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/helm.gpg]
https://baltocdn.com/helm/stable/debian/ all main" | sudo tee
/etc/apt/sources.list.d/helm-stable-debian.list
sudo apt-get update
sudo apt-get install helm
```

- [ ] Create a customized directory for storing data based on project requirements, so here we create a new directory and give it permission, as the following path:

  ```
  $ mkdir /tmp/share/elasticsearch/data/nodes
  $ chown -R 1000:1000 /usr/share/elasticsearch/data/nodes
  ```

- [ ] Before installing Elastic-search, you need to create an available PV and PVC and then bind them.
- [ ] Finally, change the mountPath directory in the contents of the statefullset file to the previously created path for storing data.

  ```
  volumeMounts:
  - mountPath: "/tmp/share/elasticsearch/data/nodes"
  ```

`elasticsearch-pv.yaml`

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: elastic-master-pv-0
  labels:
    app: elasticsearch-master
spec:
  storageClassName: k8s-kibana-logs
  capacity:
    storage: 30Gi
  accessModes:
    - ReadWriteOnce
  volumeMode: Filesystem
  persistentVolumeReclaimPolicy: Retain
  claimRef:
    namespace: default
    name: elasticsearch-master-elasticsearch-master-0
  hostPath:
    path: "/tmp/share/elasticsearch/data/nodes"
  nodeAffinity:
    required:
      nodeSelectorTerms:
      - matchExpressions:
        - key: kubernetes.io/hostname
          operator: In
          values:
          - k8s-node1.lab.example.com
---
apiVersion: v1
kind: PersistentVolume
metadata:
  name: elastic-master-pv-1
  labels:
    app: elasticsearch-master
spec:
  storageClassName: k8s-kibana-logs
  capacity:
    storage: 30Gi
  accessModes:
    - ReadWriteOnce
  volumeMode: Filesystem
  persistentVolumeReclaimPolicy: Retain
  claimRef:
    namespace: default
    name: elasticsearch-master-elasticsearch-master-1
  hostPath:
    path: "/tmp/share/elasticsearch/data/nodes"
  nodeAffinity:
    required:
      nodeSelectorTerms:
      - matchExpressions:
        - key: kubernetes.io/hostname
          operator: In
          values:
          - k8s-node2.lab.example.com
---
apiVersion: v1
```

```
kind: PersistentVolume
metadata:
  name: elastic-master-pv-2
  labels:
    app: elasticsearch-master
spec:
  storageClassName: k8s-kibana-logs
  capacity:
    storage: 30Gi
  accessModes:
    - ReadWriteOnce
  volumeMode: Filesystem
  persistentVolumeReclaimPolicy: Retain
  claimRef:
    namespace: default
    name: elasticsearch-master-elasticsearch-master-2
  hostPath:
    path: "/tmp/share/elasticsearch/data/nodes"
  nodeAffinity:
    required:
      nodeSelectorTerms:
      - matchExpressions:
        - key: kubernetes.io/hostname
          operator: In
          values:
          - k8s-node1.lab.example.com
```

elasticsearch-pvc.yaml

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  labels:
    app: elasticsearch-master
  name: elasticsearch-master-elasticsearch-master-0
  namespace: default
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 30Gi
  volumeMode: Filesystem
status:
  accessModes:
  - ReadWriteOnce
  capacity:
    storage: 30Gi
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  labels:
    app: elasticsearch-master
  name: elasticsearch-master-elasticsearch-master-1
  namespace: default
```

```
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 30Gi
  volumeMode: Filesystem
status:
  accessModes:
  - ReadWriteOnce
  capacity:
    storage: 30Gi
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  labels:
    app: elasticsearch-master
  name: elasticsearch-master-elasticsearch-master-0
  namespace: default
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 30Gi
  volumeMode: Filesystem
status:
  accessModes:
  - ReadWriteOnce
  capacity:
    storage: 30Gi
```

`elasticsearch-master.yaml`

```
kubectl edit statefulsets.apps elasticsearch-master
apiVersion: apps/v1
kind: StatefulSet
metadata:
  ...
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
        volumeMounts:
        - mountPath: "/tmp/share/elasticsearch/data/nodes"
          name: elasticsearch-master
      dnsPolicy: ClusterFirst
    ...
```

```
$ helm install elasticsearch elasticsearch
$ helm install filebeat filebeat
$ helm install logstash logstash
$ helm install kibana kibana
```

- [ ] Changes the LoadBalancer of the type of the Kibana content to `NodePort`

```
$ kubectl edit svc kibana-kibana
...
type: NodePort
...
```

- [ ] Open your browser and enter Kibana URL: https://:, like the following:

```
http://192.168.126.100:31533
```