Wazuh Setup on Kubernetes

Pre-requisites

- A Kubernetes cluster already deployed.
- The kubernetes cluster should have a non-default Storage Provisioner configured for Wazuh storages.
- The kubernetes cluster should have load balancer service installed for Wazuh services.

Resource Requirement

To deploy Wazuh on Kubernetes, the cluster should have at least the following resources available:

- 2 CPU units
- 3 Gi of memory
- 2 Gi of storage

Deployment

I. NFS Deployment:

- On Kubernetes Worker Node:

```
✔ apt install nfs-kernel-server
✔ mkdir -p /srv/nfs/wazuh-data  # create the nfs directory
✔ chmod 777 /srv/nfs/wazuh-data
✔ nano /etc/exports
  /srv/nfs/wazuh-data *(rw,sync,no_subtree_check,no_root_squash)
✔ exportfs -a
✔ systemctl restart nfs-kernel
```

- On Kubernetes Master Node:

- Install helm:

```
✔ 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
```

- Configure the NFS:

✔ helm repo add nfs-subdir-external-provisioner https://kubernetes-sigs.github.io/nfs-subdir-external-provisioner/

✔ helm install nfs-subdir-external-provisioner nfs-subdir-external-provisioner/nfs-subdir-external-provisioner --set nfs.server=<worker-ip-add> --set nfs.path=/srv/nfs/wazuh-data

II. LoadBalancer Deployment:

The manifest will deploy MetalLB to the cluster, in **metallb-system** namespace. The components are:

- The ***metallb-system/controller*** *deployment*. A cluster-wide controller that handles IP assignments.
- The **metallb-system/speaker** which is a *daemonset*. That is the component to make the services reachable.
- The ***service accounts*** for the controller and speaker, along with the *RBAC permissions* that the components require.

✔ kubectl apply -f https://raw.githubusercontent.com/metallb/metallb/v0.13.7/config/manifests/metallb-native.yaml

Verify the deployment

✔ kubectl get all --namespace metallb-system

The installation manifest does not include a configuration file. MetalLB’s components although will start, they will remain idle until we provide the required configuration as an IpAddressPool, a new Kind introduced in this version and replaced the old way of provisioning address pool configuration with ConfigMap.

Let’s name it metallb-config.yaml

```
apiVersion: metallb.io/v1beta1
kind: IPAddressPool
metadata:
  name: default-pool
  namespace: metallb-system
spec:
  addresses:
  - 192.168.1.240-192.168.1.250
```

deploy these manifests:

✔ kubectl apply -f metallb-config.yaml

III. Wazuh Deployment:

1. Clone this repository to deploy the necessary services and pods.

```
✔ git clone https://github.com/wazuh/wazuh-kubernetes.git -b v4.9.2 --depth=1

✔ cd wazuh-kubernetes
```

2. Setup SSL certificates

- Can generate self-signed certificates for the Wazuh indexer cluster using the script at `wazuh/certs/indexer_cluster/generate_certs.sh` or provide your own.

```
✔ bash wazuh-kubernetes/wazuh/certs/indexer_cluster/generate_certs.sh
```

- Can generate self-signed certificates for the Wazuh dashboard cluster using the script at `wazuh/certs/dashboard_http/generate_certs.sh` or provide your own.

```
✔ bash wazuh-kubernetes/wazuh/certs/dashboard_http/generate_certs.sh
```

3.Change the storage provisioner for deployer with configured provisioner in the cluster.

```
✔ kubectl get sc
```

After that, edit file wazuh-kubernetes/envs/local-env/storage-class.yaml

```
✔ nano wazuh-kubernetes/envs/local-env/storage-class.yaml
```

4. (optional) Change the dashboard service configuration. Deploying the dashboard on Nodeport.

```
nano wazuh-kubernetes/wazuh/indexer_stack/wazuh-dashboard/dashboard-svc.yaml
```

```
apiVersion: v1
kind: Service
metadata:
  name: dashboard
  namespace: wazuh
  labels:
    app: wazuh-dashboard
    # dns: route53
  annotations:
    # domainName: 'changeme'
    # service.beta.kubernetes.io/aws-load-balancer-ssl-cert: 'changeme'
    #service.beta.kubernetes.io/aws-load-balancer-ssl-ports: '443'
    #service.beta.kubernetes.io/aws-load-balancer-backend-protocol: https
spec:
  type: NodePort
```

```
selector:
  app: wazuh-dashboard
ports:
  - name: dashboard
    port: 443
    targetPort: 5601
    nodePort: 30001
```

5. Also change the storage and cpu configuration of the pod from the yaml files listed on the path as follows:

```
✔ nano wazuh-kubernetes/wazuh/wazuh_managers/wazuh-master-sts.yaml
✔ nano wazuh-kubernetes/wazuh/wazuh_managers/wazuh-worker-sts.yaml
✔ nano wazuh-kubernetes/wazuh/indexer_stack/wazuh-indexer/cluster/indexer-sts.yaml
```

6. After that, apply the Wazuh kubernetes deployment kustomization for local kubernetes environment.

```
✔  kubectl apply -k wazuh-kubernetes/envs/local-env
```

7. Verifying the deployment

Namespace

```
✔ kubectl get namespaces | grep wazuh
```

Services

```
✔  kubectl get services -n wazuh
```

Deployments

```
✔  kubectl get deployments -n wazuh
```

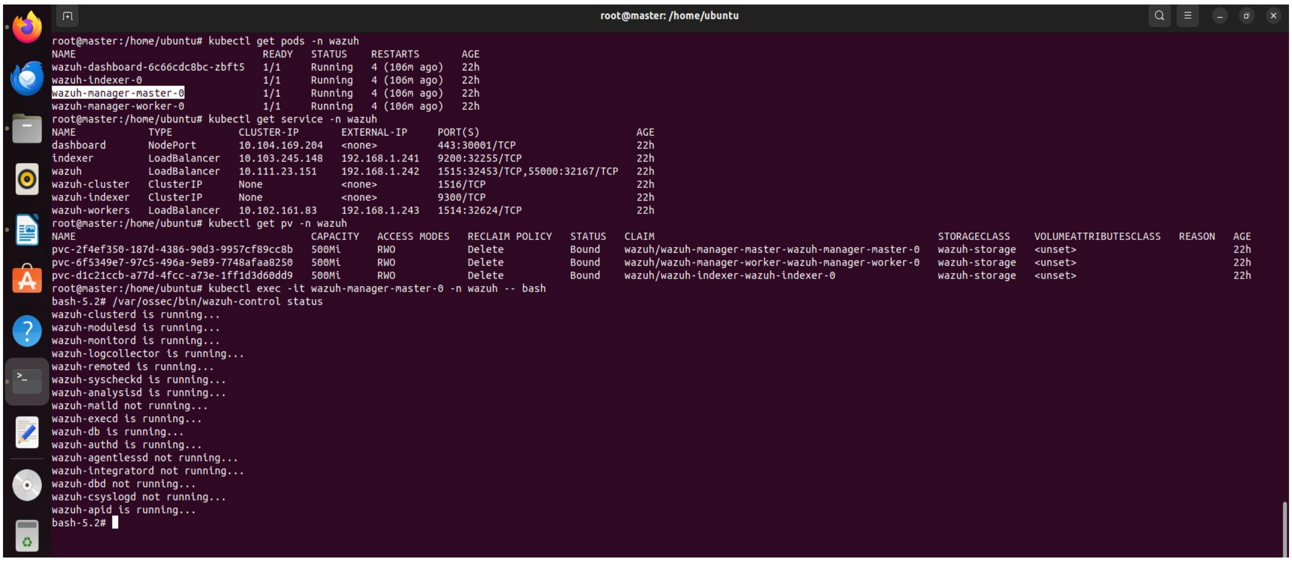
Statefulset

```
✔  kubectl get statefulsets -n wazuh
```

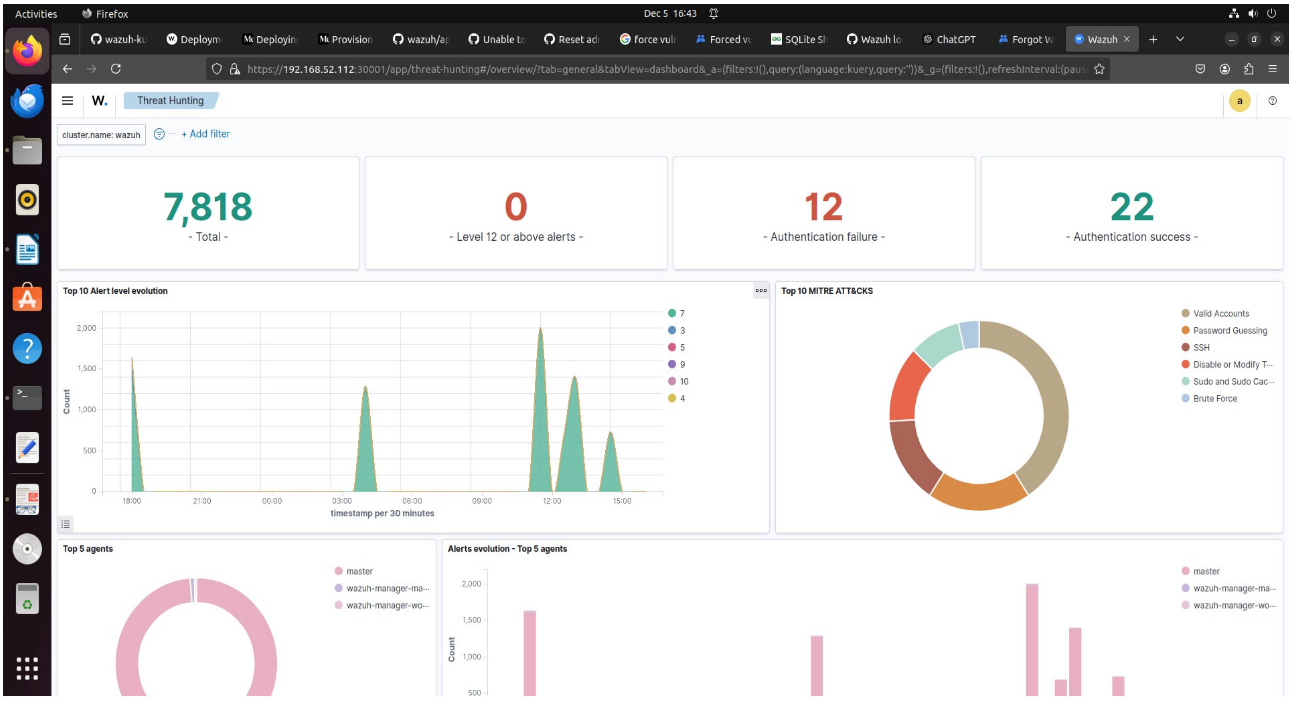
Pods

```
✔  kubectl get pods -n wazuh
```

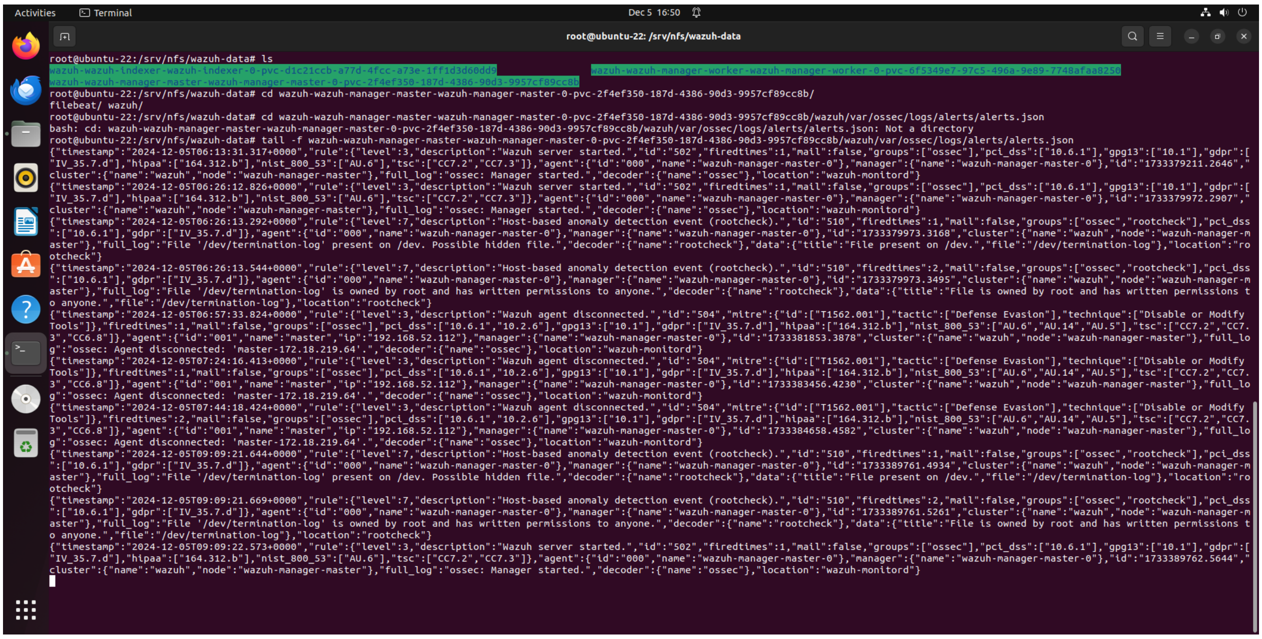
1. Verifying the deployment.



```
root@master:/home/ubuntu# kubectl get pods -n wazuh
NAME                              READY   STATUS    RESTARTS       AGE
wazuh-dashboard-6c66cdc8bc-zbft5   1/1     Running   4 (106m ago)   22h
wazuh-indexer-0                    1/1     Running   4 (106m ago)   22h
wazuh-manager-master-0             1/1     Running   4 (106m ago)   22h
wazuh-manager-worker-0             1/1     Running   4 (106m ago)   22h
root@master:/home/ubuntu# kubectl get service -n wazuh
NAME             TYPE           CLUSTER-IP       EXTERNAL-IP     PORT(S)                          AGE
dashboard        NodePort       10.104.169.204   <none>          443:30001/TCP                    22h
indexer          LoadBalancer   10.103.245.148   192.168.1.241   9200:32255/TCP                   22h
wazuh            LoadBalancer   10.111.23.151    192.168.1.242   1515:32453/TCP,55000:32167/TCP   22h
wazuh-cluster    ClusterIP      None             <none>          1516/TCP                         22h
wazuh-indexer    ClusterIP      None             <none>          9300/TCP                         22h
wazuh-workers    LoadBalancer   10.102.161.83    192.168.1.243   1514:32624/TCP                   22h
root@master:/home/ubuntu# kubectl get pv -n wazuh
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                                              STORAGECLASS    VOLUMEATTRIBUTESCLASS   REASON   AGE
pvc-2f4ef350-187d-4386-90d3-9957cf89cc8b   500Mi      RWO            Delete           Bound    wazuh/wazuh-manager-master-wazuh-manager-master-0   wazuh-storage   <unset>                          22h
pvc-6f5349e7-97c5-496a-9e89-7748afaa8250   500Mi      RWO            Delete           Bound    wazuh/wazuh-manager-worker-wazuh-manager-worker-0   wazuh-storage   <unset>                          22h
pvc-d1c21ccb-a77d-4fcc-a73e-1ff1d3d60dd9   500Mi      RWO            Delete           Bound    wazuh/wazuh-indexer-wazuh-indexer-0                 wazuh-storage   <unset>                          22h
root@master:/home/ubuntu# kubectl exec -it wazuh-manager-master-0 -n wazuh -- bash
bash-5.2# /var/ossec/bin/wazuh-control status
wazuh-clusterd is running...
wazuh-modulesd is running...
wazuh-monitord is running...
wazuh-logcollector is running...
wazuh-remoted is running...
wazuh-syscheckd is running...
wazuh-analysisd is running...
wazuh-maild not running...
wazuh-execd is running...
wazuh-db is running...
wazuh-authd is running...
wazuh-agentlessd not running...
wazuh-integratord not running...
wazuh-dbd not running...
wazuh-csyslogd not running...
wazuh-apid is running...
bash-5.2#
```



2. Can check the alerts through NFS storage mounted on worker node.



```
root@ubuntu-22:/srv/nfs/wazuh-data# ls
wazuh-wazuh-indexer-wazuh-indexer-0-pvc-d1c21ccb-a77d-4fcc-a73e-1ff1d3d60dd9            wazuh-wazuh-manager-worker-wazuh-manager-worker-0-pvc-6f5349e7-97c5-496a-9e89-7748afaa8250
wazuh-wazuh-manager-master-wazuh-manager-master-0-pvc-2f4ef350-187d-4386-90d3-9957cf89cc8b
root@ubuntu-22:/srv/nfs/wazuh-data# cd wazuh-wazuh-manager-master-wazuh-manager-master-0-pvc-2f4ef350-187d-4386-90d3-9957cf89cc8b/
filebeat/ wazuh/
root@ubuntu-22:/srv/nfs/wazuh-data# cd wazuh-wazuh-manager-master-wazuh-manager-master-0-pvc-2f4ef350-187d-4386-90d3-9957cf89cc8b/wazuh/var/ossec/logs/alerts/alerts.json
bash: cd: wazuh-wazuh-manager-master-wazuh-manager-master-0-pvc-2f4ef350-187d-4386-90d3-9957cf89cc8b/wazuh/var/ossec/logs/alerts/alerts.json: Not a directory
root@ubuntu-22:/srv/nfs/wazuh-data# tail -f wazuh-wazuh-manager-master-wazuh-manager-master-0-pvc-2f4ef350-187d-4386-90d3-9957cf89cc8b/wazuh/var/ossec/logs/alerts/alerts.json
{"timestamp":"2024-12-05T06:13:31.317+0000","rule":{"level":3,"description":"Wazuh server started.","id":"502","firedtimes":1,"mail":false,"groups":["ossec"],"pci_dss":["10.6.1"],"gpg13":["10.1"],"gdpr":[
"IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC7.2","CC7.3"]},"agent":{"id":"000","name":"wazuh-manager-master-0"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733379211.2646","
cluster":{"name":"wazuh","node":"wazuh-manager-master"},"full_log":"ossec: Manager started.","decoder":{"name":"ossec"},"location":"wazuh-monitord"}
{"timestamp":"2024-12-05T06:26:12.826+0000","rule":{"level":3,"description":"Wazuh server started.","id":"502","firedtimes":1,"mail":false,"groups":["ossec"],"pci_dss":["10.6.1"],"gpg13":["10.1"],"gdpr":[
"IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC7.2","CC7.3"]},"agent":{"id":"000","name":"wazuh-manager-master-0"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733379972.2907","
cluster":{"name":"wazuh","node":"wazuh-manager-master"},"full_log":"ossec: Manager started.","decoder":{"name":"ossec"},"location":"wazuh-monitord"}
{"timestamp":"2024-12-05T06:26:13.292+0000","rule":{"level":7,"description":"Host-based anomaly detection event (rootcheck).","id":"510","firedtimes":1,"mail":false,"groups":["ossec","rootcheck"],"pci_dss
":["10.6.1"],"gdpr":["IV_35.7.d"]},"agent":{"id":"000","name":"wazuh-manager-master-0"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733379973.3168","cluster":{"name":"wazuh","node":"wazuh-manager-m
aster"},"full_log":"File '/dev/termination-log' present on /dev. Possible hidden file.","decoder":{"name":"rootcheck"},"data":{"title":"File present on /dev.","file":"/dev/termination-log"},"location":"ro
otcheck"}
{"timestamp":"2024-12-05T06:26:13.544+0000","rule":{"level":7,"description":"Host-based anomaly detection event (rootcheck).","id":"510","firedtimes":2,"mail":false,"groups":["ossec","rootcheck"],"pci_dss
":["10.6.1"],"gdpr":["IV_35.7.d"]},"agent":{"id":"000","name":"wazuh-manager-master-0"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733379973.3495","cluster":{"name":"wazuh","node":"wazuh-manager-m
aster"},"full_log":"File '/dev/termination-log' is owned by root and has written permissions to anyone.","decoder":{"name":"rootcheck"},"data":{"title":"File is owned by root and has written permissions t
o anyone.","file":"/dev/termination-log"},"location":"rootcheck"}
{"timestamp":"2024-12-05T06:57:33.824+0000","rule":{"level":3,"description":"Wazuh agent disconnected.","id":"504","mitre":{"id":["T1562.001"],"tactic":["Defense Evasion"],"technique":["Disable or Modify
Tools"]},"firedtimes":1,"mail":false,"groups":["ossec"],"pci_dss":["10.6.1","10.2.6"],"gpg13":["10.1"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6","AU.14","AU.5"],"tsc":["CC7.2","CC7.
3","CC6.8"]},"agent":{"id":"001","name":"master","ip":"192.168.52.112"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733381853.3878","cluster":{"name":"wazuh","node":"wazuh-manager-master"},"full_lo
g":"ossec: Agent disconnected: 'master-172.18.219.64'.","decoder":{"name":"ossec"},"location":"wazuh-monitord"}
{"timestamp":"2024-12-05T07:24:16.413+0000","rule":{"level":3,"description":"Wazuh agent disconnected.","id":"504","mitre":{"id":["T1562.001"],"tactic":["Defense Evasion"],"technique":["Disable or Modify
Tools"]},"firedtimes":1,"mail":false,"groups":["ossec"],"pci_dss":["10.6.1","10.2.6"],"gpg13":["10.1"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6","AU.14","AU.5"],"tsc":["CC7.2","CC7.
3","CC6.8"]},"agent":{"id":"001","name":"master","ip":"192.168.52.112"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733383456.4230","cluster":{"name":"wazuh","node":"wazuh-manager-master"},"full_lo
g":"ossec: Agent disconnected: 'master-172.18.219.64'.","decoder":{"name":"ossec"},"location":"wazuh-monitord"}
{"timestamp":"2024-12-05T07:44:18.424+0000","rule":{"level":3,"description":"Wazuh agent disconnected.","id":"504","mitre":{"id":["T1562.001"],"tactic":["Defense Evasion"],"technique":["Disable or Modify
Tools"]},"firedtimes":2,"mail":false,"groups":["ossec"],"pci_dss":["10.6.1","10.2.6"],"gpg13":["10.1"],"gdpr":["IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6","AU.14","AU.5"],"tsc":["CC7.2","CC7.
3","CC6.8"]},"agent":{"id":"001","name":"master","ip":"192.168.52.112"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733384658.4582","cluster":{"name":"wazuh","node":"wazuh-manager-master"},"full_lo
g":"ossec: Agent disconnected: 'master-172.18.219.64'.","decoder":{"name":"ossec"},"location":"wazuh-monitord"}
{"timestamp":"2024-12-05T09:09:21.644+0000","rule":{"level":7,"description":"Host-based anomaly detection event (rootcheck).","id":"510","firedtimes":1,"mail":false,"groups":["ossec","rootcheck"],"pci_dss
":["10.6.1"],"gdpr":["IV_35.7.d"]},"agent":{"id":"000","name":"wazuh-manager-master-0"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733389761.4934","cluster":{"name":"wazuh","node":"wazuh-manager-m
aster"},"full_log":"File '/dev/termination-log' present on /dev. Possible hidden file.","decoder":{"name":"rootcheck"},"data":{"title":"File present on /dev.","file":"/dev/termination-log"},"location":"ro
otcheck"}
{"timestamp":"2024-12-05T09:09:21.669+0000","rule":{"level":7,"description":"Host-based anomaly detection event (rootcheck).","id":"510","firedtimes":2,"mail":false,"groups":["ossec","rootcheck"],"pci_dss
":["10.6.1"],"gdpr":["IV_35.7.d"]},"agent":{"id":"000","name":"wazuh-manager-master-0"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733389761.5261","cluster":{"name":"wazuh","node":"wazuh-manager-m
aster"},"full_log":"File '/dev/termination-log' is owned by root and has written permissions to anyone.","decoder":{"name":"rootcheck"},"data":{"title":"File is owned by root and has written permissions t
o anyone.","file":"/dev/termination-log"},"location":"rootcheck"}
{"timestamp":"2024-12-05T09:09:22.573+0000","rule":{"level":3,"description":"Wazuh server started.","id":"502","firedtimes":1,"mail":false,"groups":["ossec"],"pci_dss":["10.6.1"],"gpg13":["10.1"],"gdpr":[
"IV_35.7.d"],"hipaa":["164.312.b"],"nist_800_53":["AU.6"],"tsc":["CC7.2","CC7.3"]},"agent":{"id":"000","name":"wazuh-manager-master-0"},"manager":{"name":"wazuh-manager-master-0"},"id":"1733389762.5644","
cluster":{"name":"wazuh","node":"wazuh-manager-master"},"full_log":"ossec: Manager started.","decoder":{"name":"ossec"},"location":"wazuh-monitord"}
```

References

- https://akyriako.medium.com/load-balancing-with-metallb-in-bare-metal-kubernetes-271aab751fb8
- https://documentation.wazuh.com/current/deployment-options/deploying-with-kubernetes/kubernetes-deployment.html
- https://github.com/wazuh/wazuh-kubernetes/tree/master