# Wazuh



---

# Server

## About

- All of Wazuh on the server-side runs as a stateful set because node names need to be static for clustering.

### References

- Wazuh on GitHub
- Wazuh on Docker Hub
- Wazuh Kibana Plugin
- Wazuh automatically generates SSL certs. I've also verified this when observing logs, and connecting to it through Kibana.
- Port List
- Clustering Info

- Wazuh's tools

### Special Things the Chart Does

1. Username/Password is used by **Kibana** to authenticate to the **Wazuh** API server is injected by the `helm` chart @ `/var/ossec/api/configuration-template/auth/user`. Couldn't inject on the path in the docs because it contained symlinks.

2. Overwrites `filebeat.yml` to point it to `fluentd`.

## Useful Commands

### List Cluster Members

```
/var/ossec/bin/cluster_control -l
```

### Run Configuration File Test

```
/var/ossec/bin/ossec-analysisd -d -t
```

### Restart all OSSEC Processes

```
/var/ossec/bin/ossec-control restart
```

### See status of all processes related to Wazuh

This also seems to clean up processes, not just report status.

```
/var/ossec/bin/ossec-control status
```

### Test Security Alerts

- https://documentation.wazuh.com/current/user-manual/ruleset/testing.html

```
/var/ossec/bin/ossec-logtest
```

```
Mar  8 22:39:13 ip-10-0-0-10 sshd[2742]: Accepted publickey for root from 73.189.13
```

# Prerequisites

## Set Basic Auth for Kibana Plugin -> Wazuh API Communication

```
htpasswd -n -b chipper
```

These values go in `./server/k8s/helm/wazuh/files/auth.txt`. The chart reads from this file and mounts it in the container.

# Install / Upgrade / Delete

## Install

```
helm --debug install --namespace client --name wazuh './server/k8s/helm/wazuh'
```

### Post-Installation

**Kibana** uses a plugin to interact with **Wazuh**'s API. In the app, set these values:

`username` = `chipper`

`password` =

`url` = `https://wazuh-cluster.client.svc.cluster.local`

`port` = `55000`

This configuration is saved in Elasticsearch, so even if Kibana is reset (including volumes), nothing should change in terms of config.

If you encounter an error about `api.log` doesn't exist, run:

```
touch /var/ossec/data/logs/api.log && chown ossec:ossec /var/ossec/data/logs/api.log
```

### Upgrade

```
helm --debug upgrade --namespace client wazuh './server/k8s/helm/wazuh'
```

### Delete (DANGER)

```
helm del --purge wazuh
```

## Troubleshooting

- Error *Elasticsearch Template Missing*. The Fix.