Use below URL for LAB:

<https://medium.com/@chris_linguine/how-to-monitor-distributed-logs-in-kubernetes-with-the-efk-stack-1218a565ce0c>

To deploy EFK Stack as per above article, please configure following prior to deploying the the yamls.

1. Give the security Groups allow all permissions.
2. Deploy the AWS File System.
3. Deploy EFS provisioner as Elasticsearch needs persistent volume.
4. Check the EFS is proper mounted to the EFS Provisioner. Timeout error in you don't give proper security groups for nodes and efs file system.
5. Deploy Elasticsearch First
6. Deploy Kibana
7. Deploy FluentD
8. Deploy a new deployment using sreeharshav/rollingupdate:v5

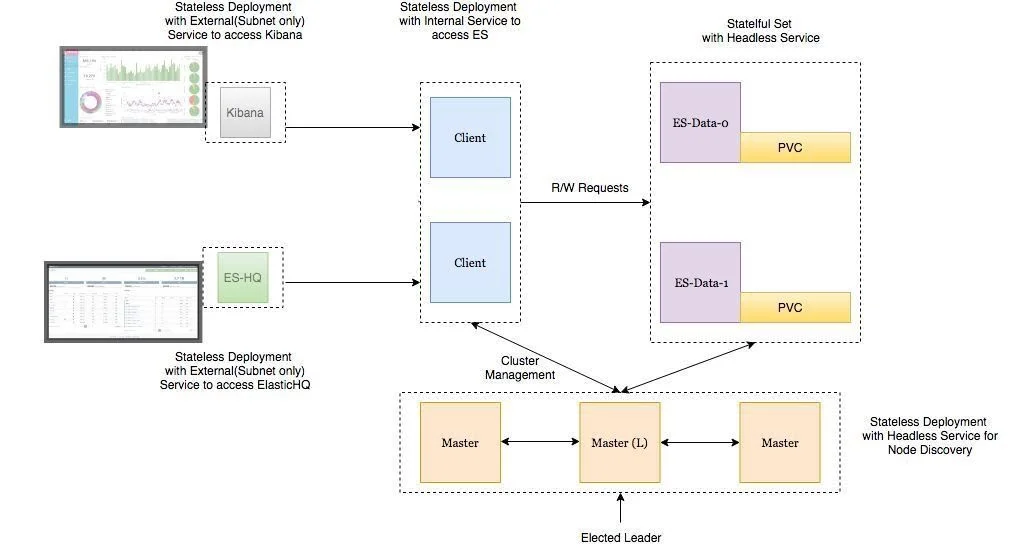
kubectl create deploy testing001 --image=sreeharshav/rollingupdate:v5 --replicas 2

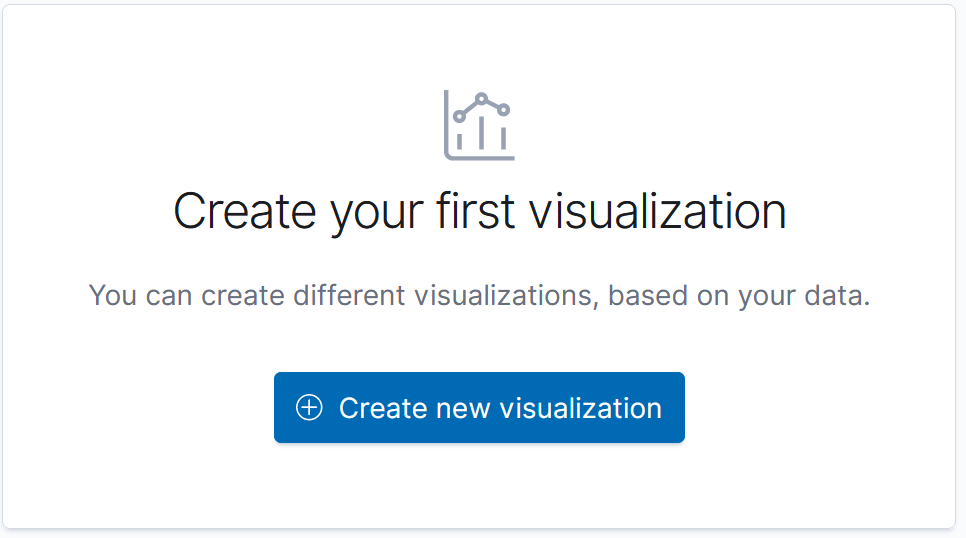
1. Run a curl to the deployment to generate logs and login to kibana . You need to expose kubana on the nodeport.
2. Enter logstash-\* in the field for the index pattern.

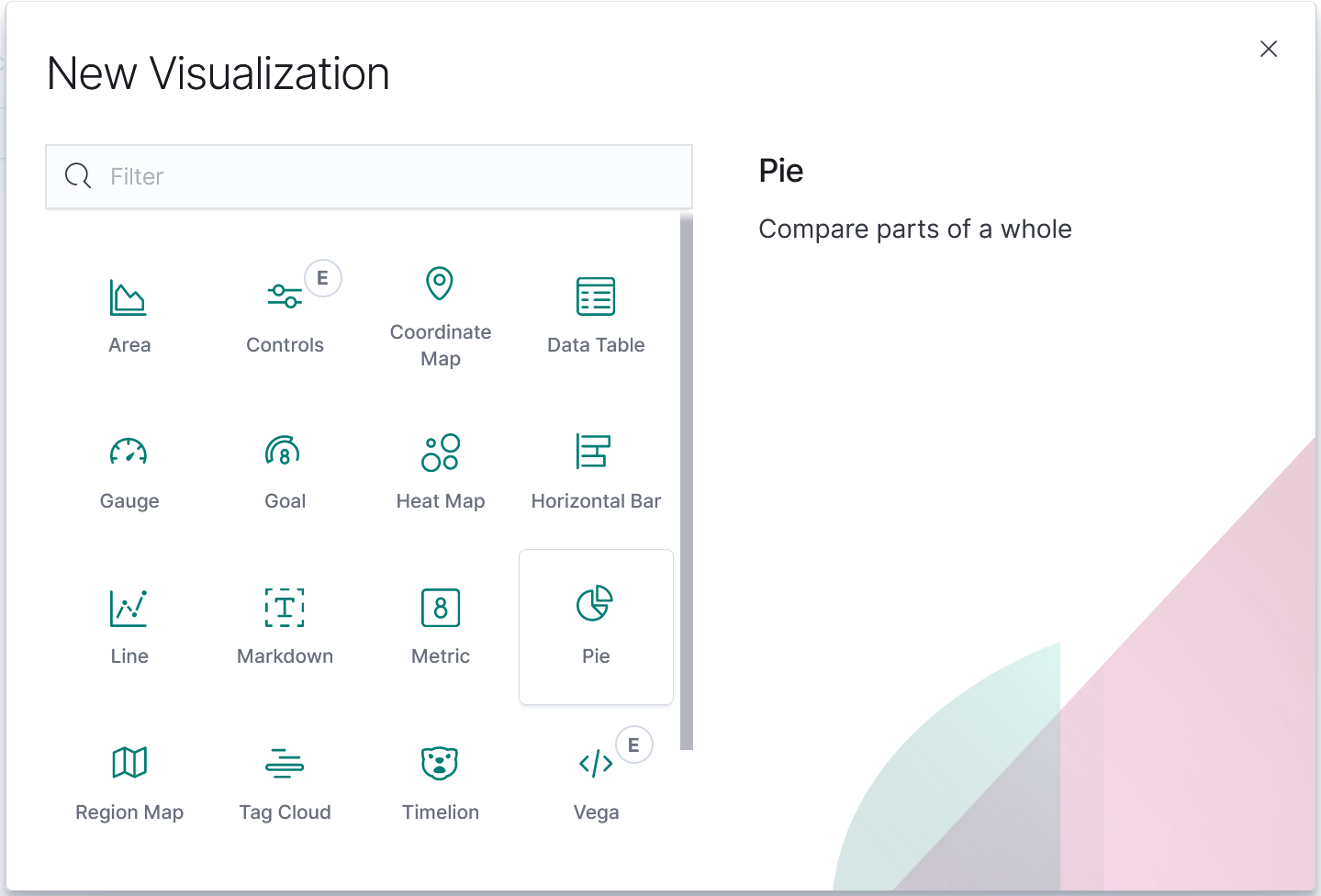
kubernetes.pod\_name : testdeploy01-554db8cfb8-ffqh7

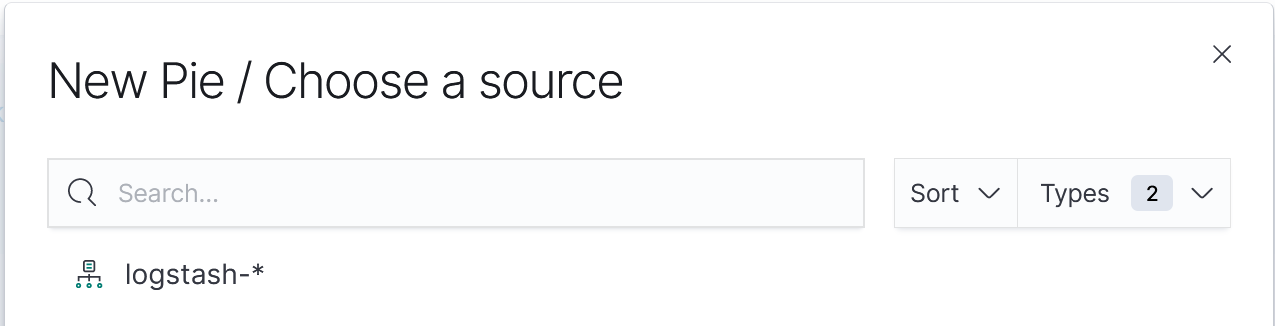
Creating KIBANA Visualizations:

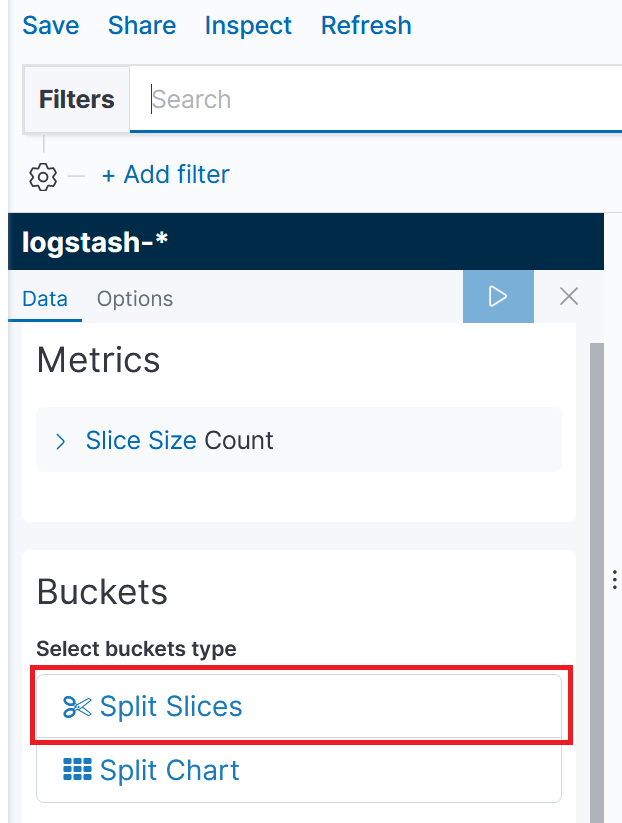
<https://sysdig.com/blog/kubernetes-security-logging-fluentd-falco/>



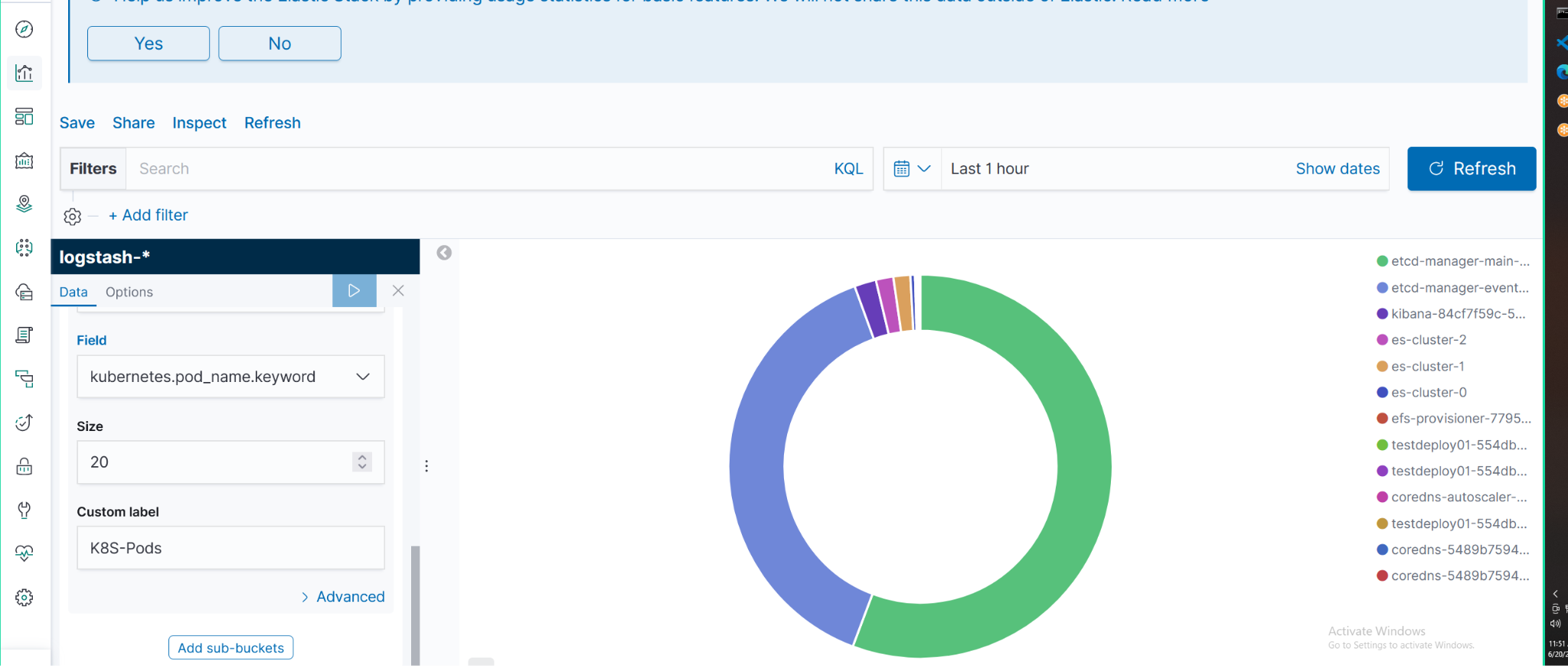


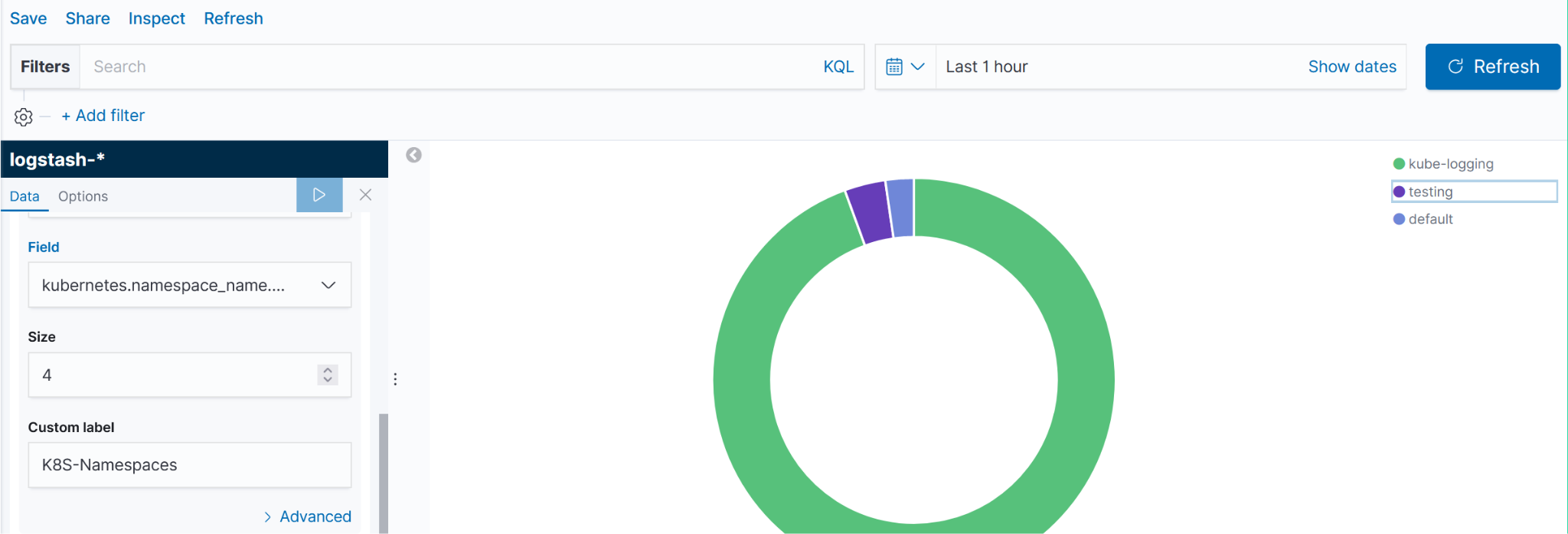






1. Number of hits based on the POD name



1. Deployed a new namespace and deployed a new app with opened the traffic with nodeport.
2. 

Testing 403/304 Error:

Remove index.html in all pods and access the website for generating the errors.

