LFN Mentorship Project Presentation

August 2020

Log Analysis and Alerting

› **Introduction**
  › **Name**: Adarsh Yadav
  › **Location**: Delhi, India
  › **University**: University Of Delhi
  › **Mentor(s)**: Sridhar K. N. Rao
  › **LFN Project:** OPNFV - VSPERF

Log Analysis and Alerting

Project Description:

› Help user to understand the test behaviour and analyze the performance results from logs generated by VSperf

› Alert Management solution to send alerts.

Tools:

› Elasticsearch, Fluentd, Kibana, Elastalert, Kubernetes, Ansible, Jupyter-Notebook

Log Analysis and Alerting

Project Objectives:

› Deployment of K8s cluster

› Deploy EFK Stack

› Achieve high availability

› Configure Fluentd

› Alert Configuration

Log Analysis and Alerting

› **Project Deliverables:**

  › Client-Side Ansible Playbooks for BM
    › Deploy and Configure agents
  › Server-Side Ansible playbooks for BM
    › Deploy K8S Cluster
    › Deploy and configure EFK
    › Alerting Configuration
  › Jupyter Notebooks
    › Analysis of Logs
  › Visualization and alert management in OPNFV airship.

Log Analysis and Alerting

› **Project Execution & Accomplishments**:

› Client-Side Ansible Playbooks
   › Deploy and Configure agents
› Server-Side Ansible playbooks
   › Deploy K8S Cluster
   › Deploy and configure EFK
   › Alerting Configuration
› Jupyter Notebooks
   › Analysis of Logs

LF NETWORKING

Log Analysis and Alerting

Log Analysis and Alerting

Log Analysis and Alerting

› **Deliverables that were not completed.**

  › We had planned to take our work on monitoring and logging to OPNFV-Airship.

  › Unfortunately the OPNFV-Airship deployments were not stable and the LMA components of the Airship constantly crashed.

  › OPNFV-Airship team could not fix the issues.

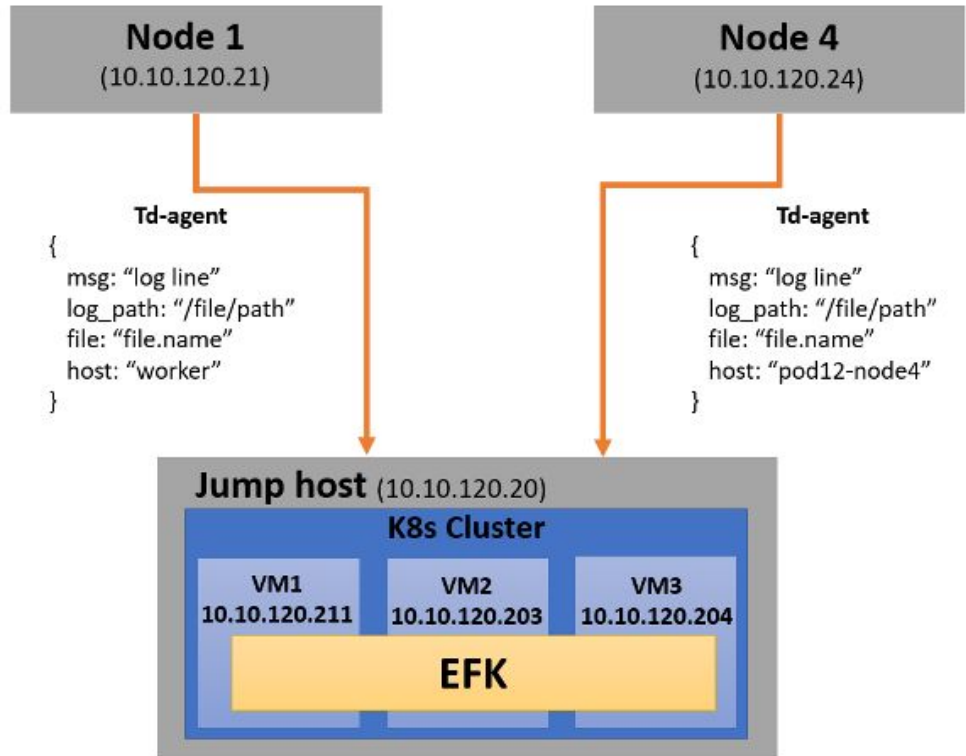# Log Analysis and Alerting

› **Recommendations for future work**:

› CLA - Closed Loop Automation
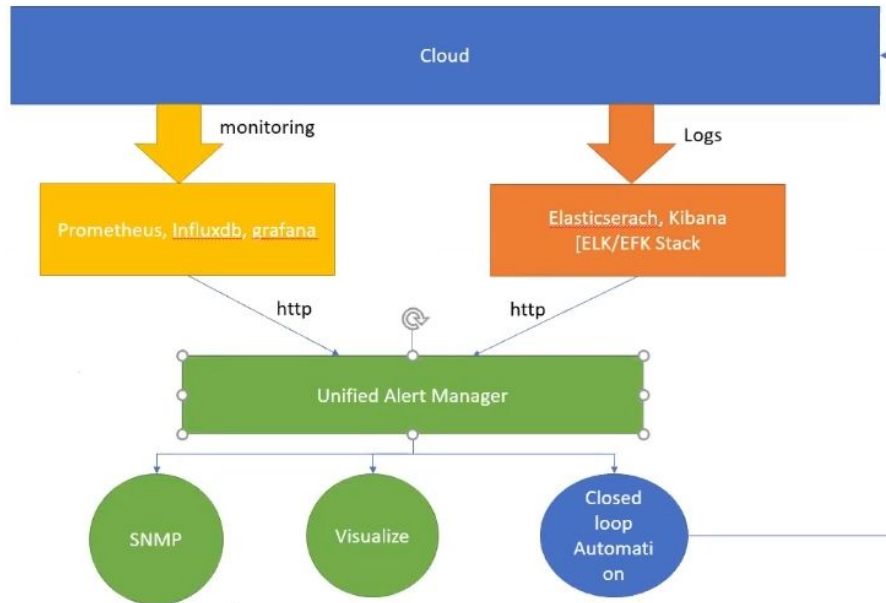
Log Analysis and Alerting

› **Project Output or Results:**

Log Analysis and Alerting

› **Project Output or Results:**

```
[root@vm1 ~]# kubectl get pods -n logging
NAME                              READY   STATUS    RESTARTS   AGE
elastalert-64ddfc8d4c-4mh52       1/1     Running   0          3d17h
fluentd-7b5cc69df5-pw2jp          1/1     Running   0          3d17h
fluentd-7b5cc69df5-tq6vj          1/1     Running   0          3d17h
logging-es-vm1-data-0             1/1     Running   0          3d17h
logging-es-vm1-master-0           1/1     Running   0          3d17h
logging-es-vm2-data-0             1/1     Running   0          3d17h
logging-es-vm2-master-0           1/1     Running   0          3d17h
logging-es-vm3-data-0             1/1     Running   0          3d17h
logging-es-vm3-master-0           1/1     Running   0          3d17h
logging-kb-85bb9d6d68-4cvqc       1/1     Running   0          3d17h
nginx-685456d445-4sbzp            1/1     Running   0          3d17h
nginx-685456d445-xzxn4            1/1     Running   0          3d17h
```
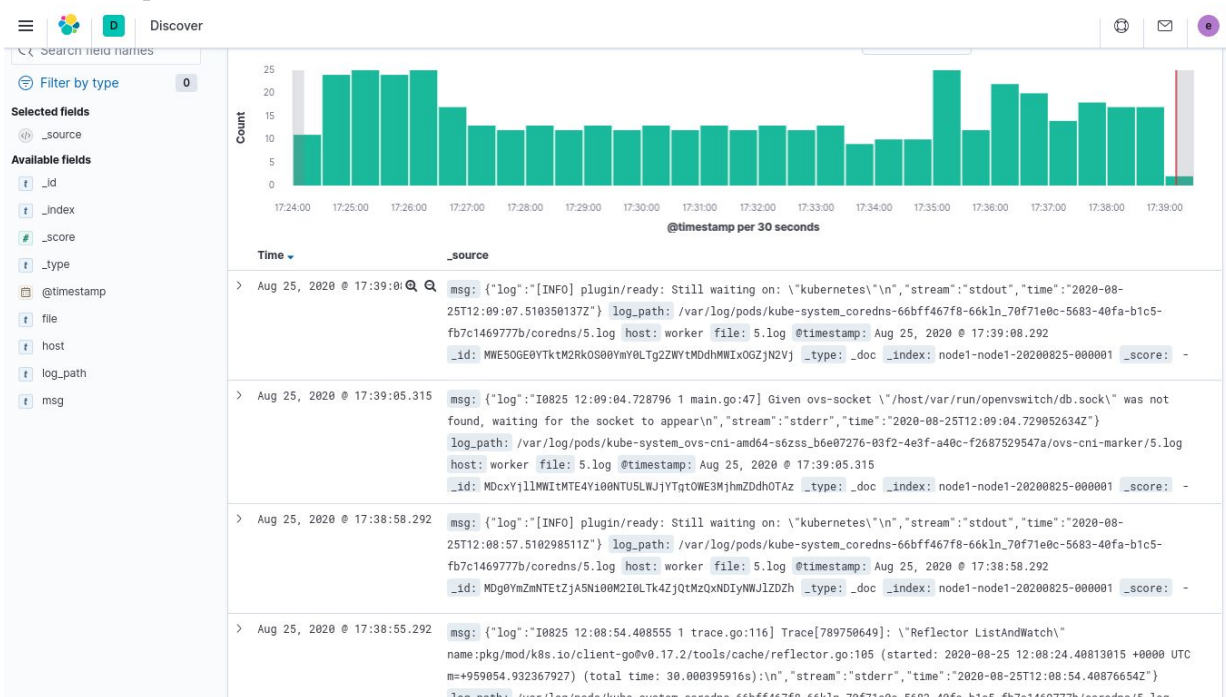
Log Analysis and Alerting

› **Project Output or Results:**

  › Alert

```
{"type": "pattern-match", "label": "failed", "index": "node1-20200810", "log": "2
020-08-10 14:57:49,059 : Failed to run test", "log_path": "/tmp/results_2020-08-1
0_14-53-57/vsperf-overall_2020-06-11_06-53-57.log", "reason": "Failed to run test
", "num_hits": 2, "num_matches": 2}
```
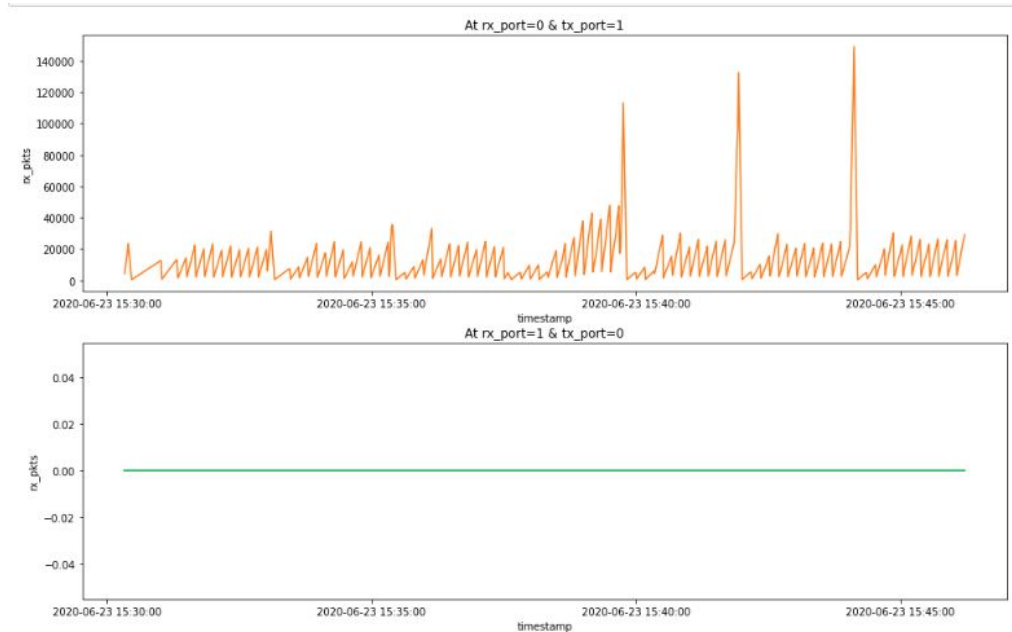
THE **LINUX** FOUNDATION

LFNETWORKING

Log Analysis and Alerting

› **Project Output or Results:** Elasticsearch

Log Analysis and Alerting

› **Project Output or Results:** Jupyter Notebook

Log Analysis and Alerting

› **Project Output or Results:**

  › Time Analysis from logs

```
Setup duration:    0.671 s
Iteration duration:  35.239 s
Traffic duration:  666.741 s
Test duration:   667.842 s
Report duration:   0.015 s
```

THE **LINUX** FOUNDATION

LFNETWORKING

Log Analysis and Alerting

› **Insights Gained:**

  › Develops technical skills

  › Meet with other people that can inspire you and help you.

  › Exposure to real world software development scenarios

THANK YOU!

THE **LINUX** FOUNDATION

LF NETWORKING