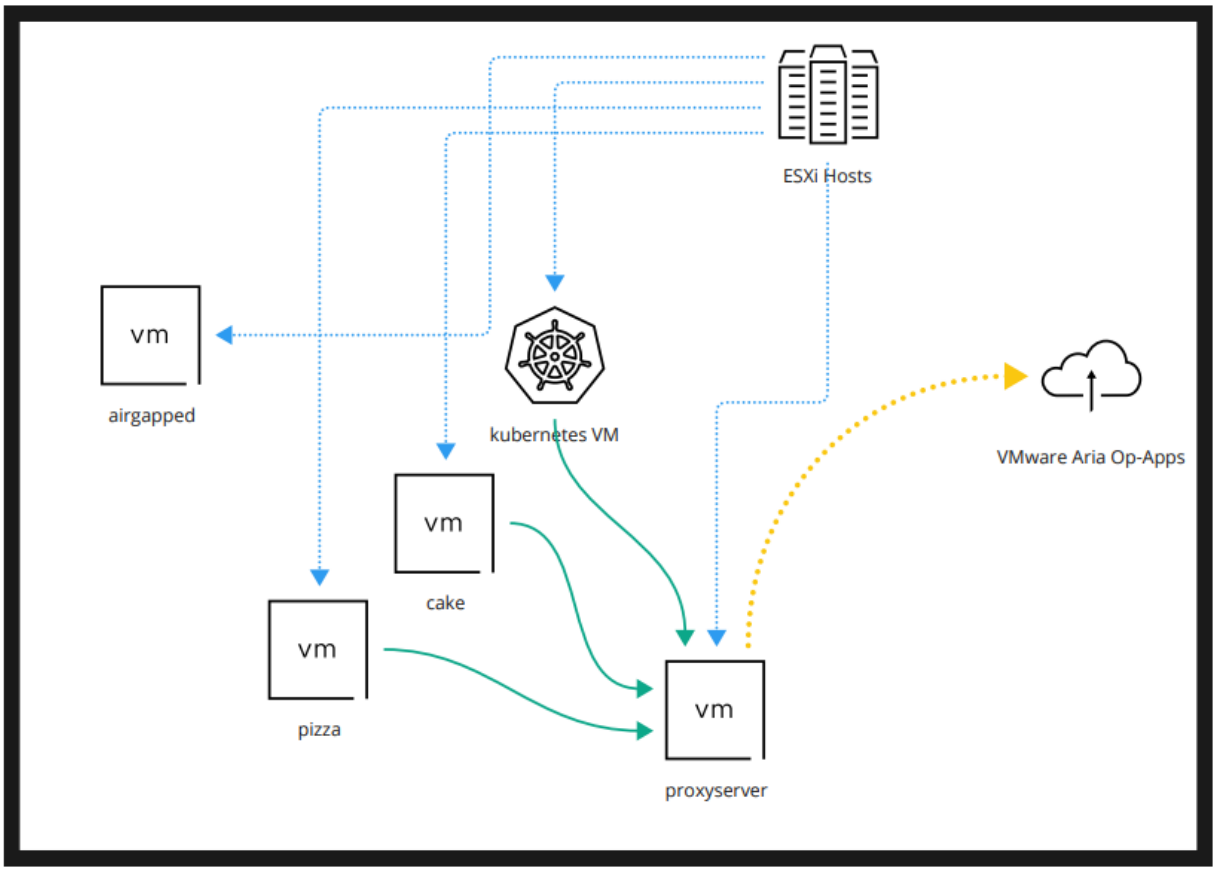
Introduction Scenario

You have been assigned to set up Fluentd on a Linux Virtual Machines (VMs) and Logs in a Kubernetes Cluster. You must configure Fluentd and deploy Kubernetes Integration with Logs and ensure that it sends logs to our Logging Platform in vmware.wavefront.com cluster.

Environment:



Instructions:

- When you are asked to create a chart using Logs browser, this is enclosed in brackets with the number, e.g: [2], please record these links as at the end Part 1 you will be asked to share those, there are 5 links expected to be shared.
- In each VM you can run command <hint> to get some help.
- You can achieve tasks in multiple ways, just try to make things work.
- Issues are not related to underlying infrastructure this is focus on configuration of Fluentd, Linux, Wavefront Proxy and Kubernetes integration.
- If you have any issues/questions does not hesitate to reach out to #aoa-hyperlogs-hol channel.

Part 1 | Fluentd (td-agent)

Tasks:

You will be provided with some Linux VMs that has been pre-installed with Fluentd. Your task is to configure Fluentd to send logs to Aria Op-Apps.

To complete Part 1, you will need to perform the following steps:

- 1. Find a way to send Logs without the need to install anything just using curl commands to the WF Proxy running on <proxyserver> VM you can use <cake> VM and make sure these are reaching SaaS side, also set a new proxy name, equal to <hol-yourname>
  WARNING: If this task is not done you cannot perform next tasks.
  a. [1] Create a Logs chart querying this log, using **Logs Browser** and save the shorten link.
- 2. Check if Fluentd is installed on the <cake> VM and is running correctly.
- 3. Make sure in VM <cake> Fluentd is monitoring /var/log/syslog and sending logs correctly, logs must be tagged like this.
  a. Source, must be equal to <yourname-source>
  b. Application <cake>
  c. Add tag: key=hol and value=yourname
  d. [2] Find logs with message < I love dummy Logs huh> using Logs browser] and save the shorten link.
- 4. VM <airgapped> is a VM which does not have direct connection to the <proxyserver> VM, find a way to send a dummy log from this VM to the <proxyserver> using Fluentd.
  a. [3] Find log sent using Logs browser and save the shorten link.

```
curl -X POST \
     -H "Content-Type: application/json" \
     -d '{
          "message": "This is a message from airgapped VM",
          "source": "'"$HOSTNAME"'",
          "application": "SIEM",
          "hol": "yourName"
     }' \
     http://localhost:8888/
```

- 5. Send nginx access logs located on /var/log/ngnix from <airgapped> VM, you can produce more logs accessing/refreshing Web Page located on Lab Chrome bookmarks.
    a. Bonus point: Make the Logs look prettier with a <filter> directive.
    b. [4] Save a shortened URL of the nginx access logs.
- 6. Pizza VM is messy, final output must be,
    a. Only logs from auth.log and postgres should flow, both to the wf proxy and also write to /fluentd/logs.
    b. All Logs must be tagged, with *application=pizza* and input=pattern used respectively.
    c. [5] Find logs sent, using Logs browser and save the shorten link, including both inputs.
- 7. Write all inbound logs sent to the Wavefront Proxy to a local file.
- 8. Share all shortened links gather so far to Slack channel: #aoa-hyperlogs-hol

Part 2 | Kubernetes:

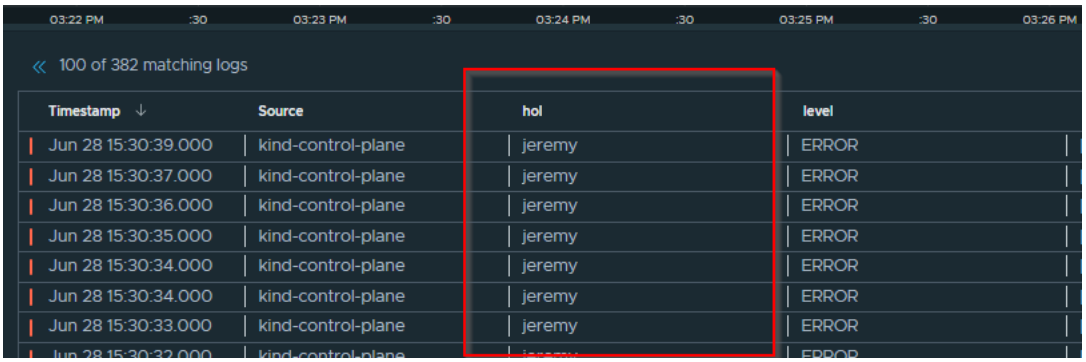
Scenario:

Aria Op-Apps integration was deployed in the local Kubernetes cluster and Development team calls you mentioning they are not seeing Logs, figure out what is happening, Logs and Metrics should be flowing.

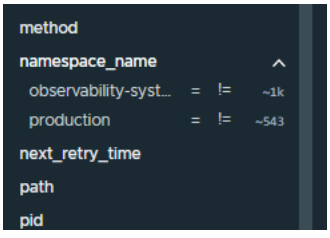
To complete Part 2, you will need to perform the following steps:

Tasks:

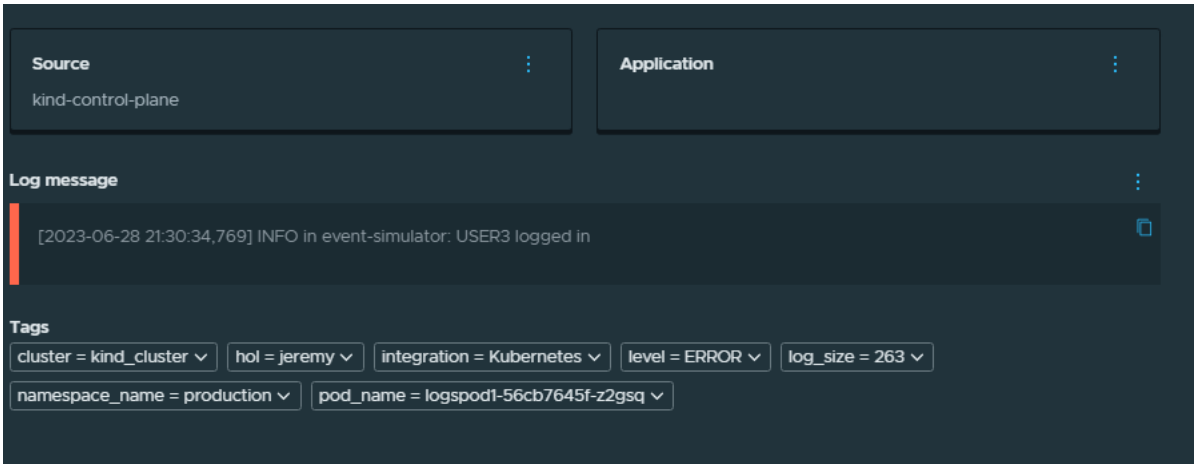
1. Make sure currently integration is supported, take necessary actions.
2. Once issue is resolved, you must deploy the new integration using yaml located on /home/ubuntu/operator/wavefront.yaml due security policies, make sure metrics and logs are flowing. (Use your personal token if needed).
3. All Logs must have the following tag “hol=yourname”



4. Deny all logs from unwanted namespaces we must only see logs for these namespaces: [production, observability-system, default]



5. No Logs should contain following tags [container_id, container_name, pod_id]



6. [Optional] What image are the Logs collectors pods using?

Part 3 | Verification [Optional]

1. Using <**Hyperlogs Performance Dashboard**> in Mon and <**Operations for Applications Service and Proxy Data**> dashboards analyze how the metrics changed since the Lab started.
2. Play/Catch a vRLIC backend request: https://sunnylabs.zendesk.com/knowledge/articles/8123680312212/en-us?brand_id=59190