**FluentBit Installation Guide and Setup**

*This documentation was done using Docker desktop installed, having kuberenetes for Docker enabled and using helm chart.*

First off we need to add the helm repo for FluentBit using   
“ helm repo add fluent https://fluent.github.io/helm-charts”

Next off we need to install it using “helm upgrade --install fluent-bit fluent/fluent-bit”

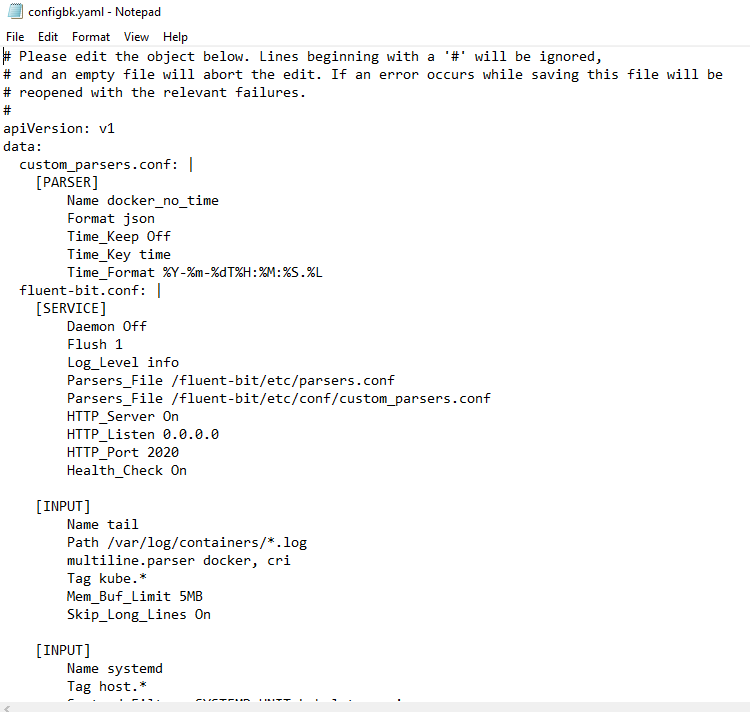
This way we should get it up and running, to confirm you can run “kubectl get pods”. You should see a pod running as follows:



Once you have your fluent-bit pod running you can then start your configurations. The configurations would be done in the configmap so we can run “kubectl get configmap” to confirm that it exists and take note of its name (in this case it is “fluent-bit”).

You can then run “kubectl edit configmap fluent-bit” to directly edit it with notepad.

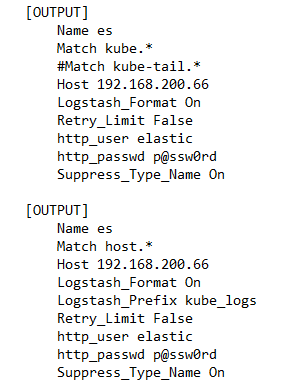
It should look something like this:



Most of our edits will be in the “fluent-bit.conf” section as this is our main configuration.

Sometimes the configmap wouldn’t look “pretty” so you can use something like [yaml-formatter](https://jsonformatter.org/yaml-formatter/4ecde8) to make it look pretty.

First off we need to check that everything is sending fine and there is connectivity, so what we would do is just edit the [OUTPUT] section to look something like this



Variables that needs to be changed according to your case:

1. es represents the specification of elastic search.
2. host would indicate your server (you may need to add a port field also).
3. http\_user and http\_passwd according to your credentials.

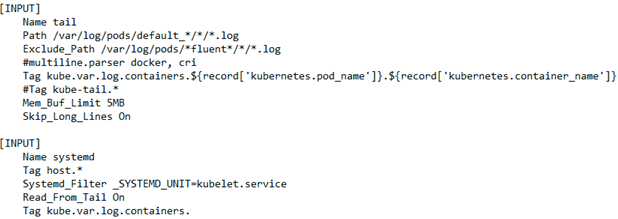
We can then save the configmap and confirm by seeing the edit applied as follows:



*You can always check the pod logs for debugging and troubleshooting using “kubectl logs <pod\_name>”*

*The fluent-bit service must be restarted to take into action the edited configmap, a simple way to do this is by deleting the already running pod, as a new one would be automatically created.*

Once that is done you must change the [INPUT] field to include logs form other pods, such as below



Note that we used tail, which is the most convenient and specified the path to be “/var/log/pods/default\_\*/\*/\*.log” this was for multiple reasons:

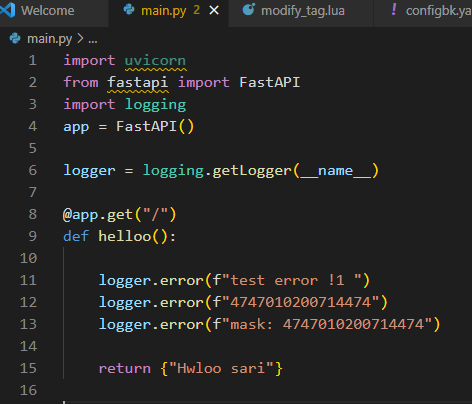
1. In our case this was the path that the logs were saved to, the path was found by running “kubectl inspect <container-ID>” and locating the logpath.
2. The (default) at the beginning of the path indicated the default namespace, so you could include a specific namespace or better see and check for your own custom pattern. (be aware of including all pods that may include system pods or pods related to kuberenetes that would result in overwhelming number of logs)
3. In this case we also **Excluded** any path that was related to FluentBit so that there would be no logs from FluentBit itself sent over. (you may include neuvector or any other paths you don’t want)

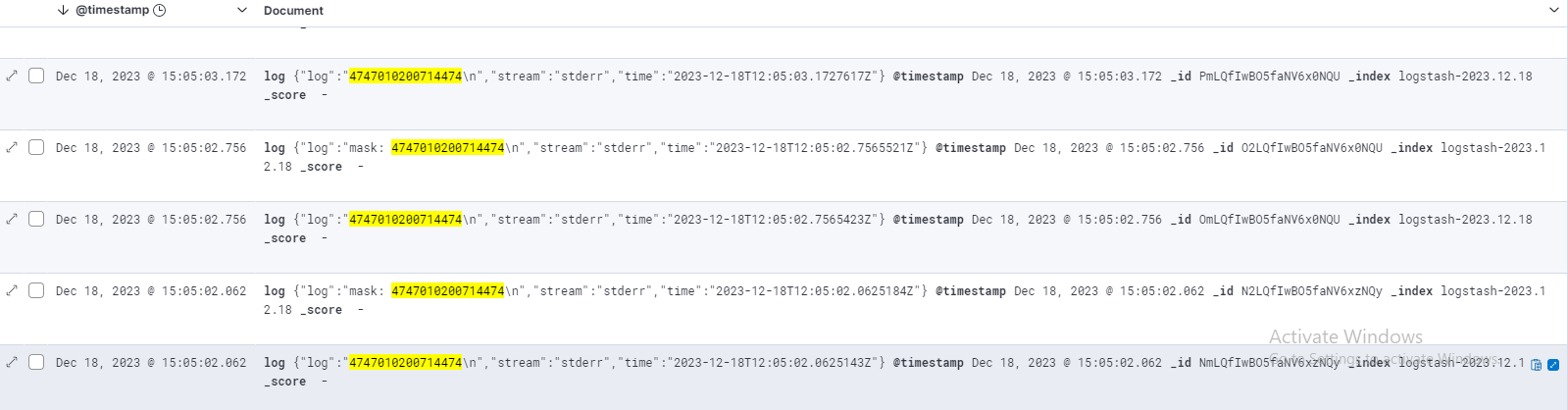
You can now test and see the generated logs by your other deployments. (after saving and applying)

After successfully verifying that logs are sent over and can be seen on elastic under Search > Content > Indices

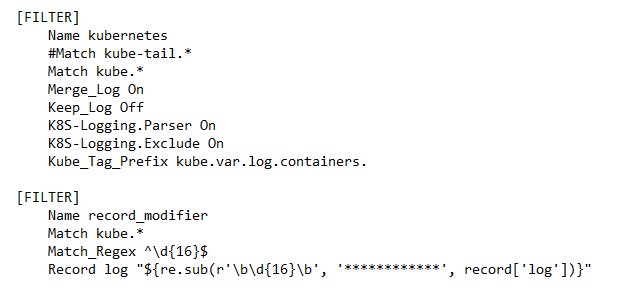
**Example case 2:**

In this case we generated and image that had the following code



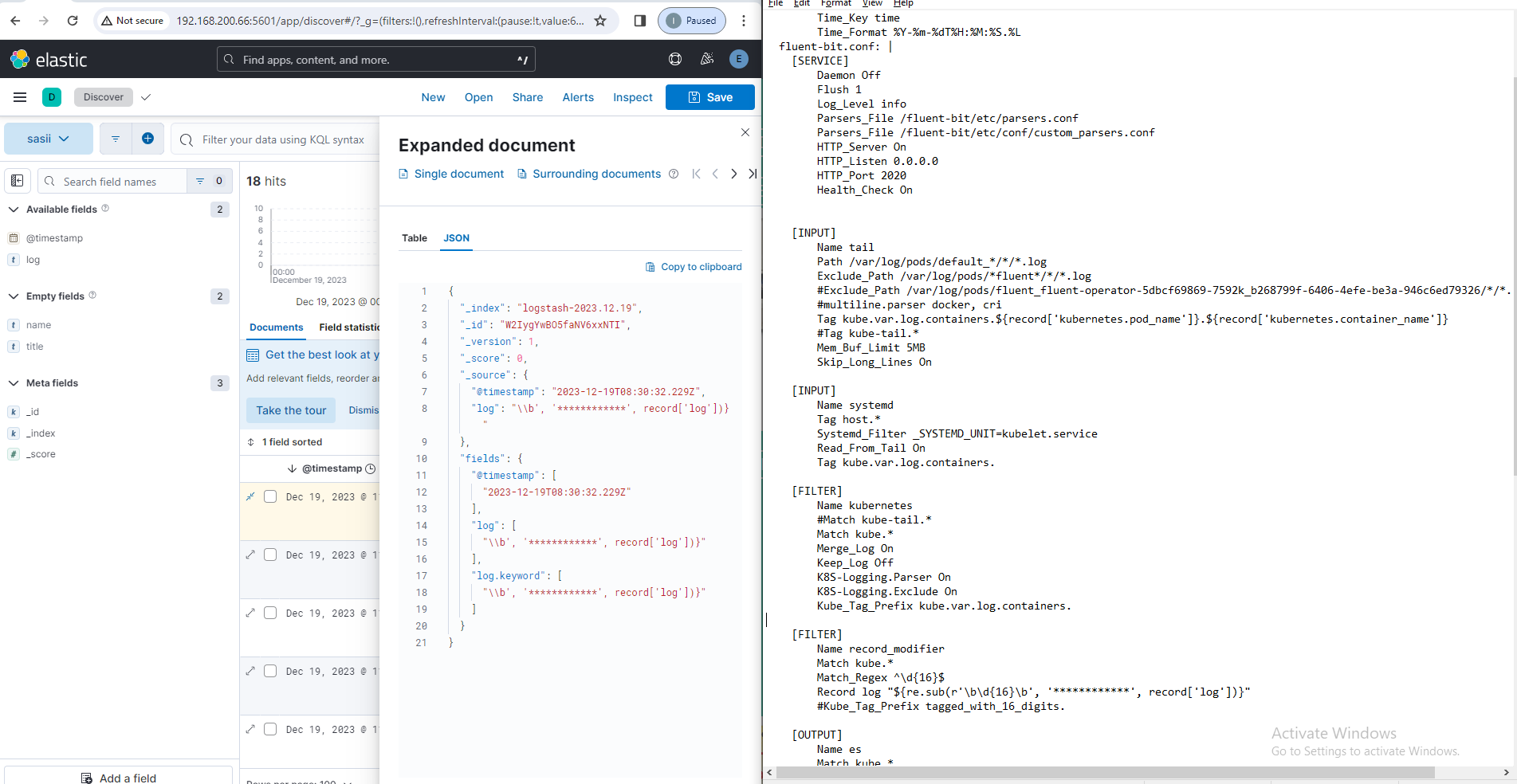
The purpose of this was to assume that the logs could contain PCI data that needs to be masked, so our application generated logs that had this card number and we can see it as below:

This is of course considered as a security gap and so this data needs to be masked, this could be done on the FluentBit configmap. The steps would include is to first identify the record containing this data and secondly replace it/mask it. This could be achieved as follows in the [FILTER] field:



What happens above is that as the logs are tagged they will go through a second filter, this filter will try to match the logs to a 16-digit number using the above regex and the record will be adjusted if it matches.

It is worth noting that as it is a regex match it needs to be adjusted to match your logs and you must find a pattern that suits your log format. In addition, it could be changed in the “Record log” variable depending on your need.

Now we can how this achieves the applied configurations and masking:

**Appendix:** Fluent-bit configmap:  
Deployment file and image:

apiVersion: v1

data:

custom\_parsers.conf: |

[PARSER]

Name docker\_no\_time

Format json

Time\_Keep Off

Time\_Key time

Time\_Format %Y-%m-%dT%H:%M:%S.%L

fluent-bit.conf: |

[SERVICE]

Daemon Off

Flush 1

Log\_Level info

Parsers\_File /fluent-bit/etc/parsers.conf

Parsers\_File /fluent-bit/etc/conf/custom\_parsers.conf

HTTP\_Server On

HTTP\_Listen 0.0.0.0

HTTP\_Port 2020

Health\_Check On

[INPUT]

Name tail

Path /var/log/pods/default\_\*/\*/\*.log

Exclude\_Path /var/log/pods/\*fluent\*/\*/\*.log

#multiline.parser docker, cri

Tag kube.var.log.containers.${record['kubernetes.pod\_name']}.${record['kubernetes.container\_name']}

#Tag kube-tail.\*

Mem\_Buf\_Limit 5MB

Skip\_Long\_Lines On

[INPUT]

Name systemd

Tag host.\*

Systemd\_Filter \_SYSTEMD\_UNIT=kubelet.service

Read\_From\_Tail On

Tag kube.var.log.containers.

[FILTER]

Name kubernetes

#Match kube-tail.\*

Match kube.\*

Merge\_Log On

Keep\_Log Off

K8S-Logging.Parser On

K8S-Logging.Exclude On

Kube\_Tag\_Prefix kube.var.log.containers.

[FILTER]

Name record\_modifier

Match kube.\*

Match\_Regex ^\d{16}$

Record log "${re.sub(r'\b\d{16}\b', '\*\*\*\*\*\*\*\*\*\*\*\*', record['log'])}"

[OUTPUT]

Name es

Match kube.\*

#Match kube-tail.\*

Host 192.168.200.66

Logstash\_Format On

Retry\_Limit False

http\_user elastic

http\_passwd p@ssw0rd

Suppress\_Type\_Name On

[OUTPUT]

Name es

Match host.\*

Host 192.168.200.66

Logstash\_Format On

Logstash\_Prefix kube\_logs

Retry\_Limit False

http\_user elastic

http\_passwd p@ssw0rd

Suppress\_Type\_Name On

kind: ConfigMap

metadata:

annotations:

meta.helm.sh/release-name: fluent-bit

meta.helm.sh/release-namespace: default

creationTimestamp: '2023-12-17T12:57:20Z'

labels:

app.kubernetes.io/instance: fluent-bit

app.kubernetes.io/managed-by: Helm

app.kubernetes.io/name: fluent-bit

app.kubernetes.io/version: 2.2.0

helm.sh/chart: fluent-bit-0.40.0

name: fluent-bit

namespace: default

resourceVersion: '215718'

uid: 892bb6fc-39e6-477b-a41e-6e54f1b9660a

---

apiVersion: apps/v1

kind: Deployment

metadata:

  labels:

    app: privapi

  name: privapi

spec:

  replicas: 1

  selector:

    matchLabels:

      app: privapi

  template:

    metadata:

      labels:

        app: privapi

    spec:

      containers:

      - image: mohammadradi/logging:v2

        name: priv-envapi

        securityContext:

          privileged: true

        ports:

        - containerPort: 55272

---

apiVersion: v1

kind: Service

metadata:

  name: privapi

  labels:

    app: privapi

spec:

  type: LoadBalancer

  selector:

    app: privapi

  ports:

    - protocol: TCP

      targetPort: 55272

      port: 8000