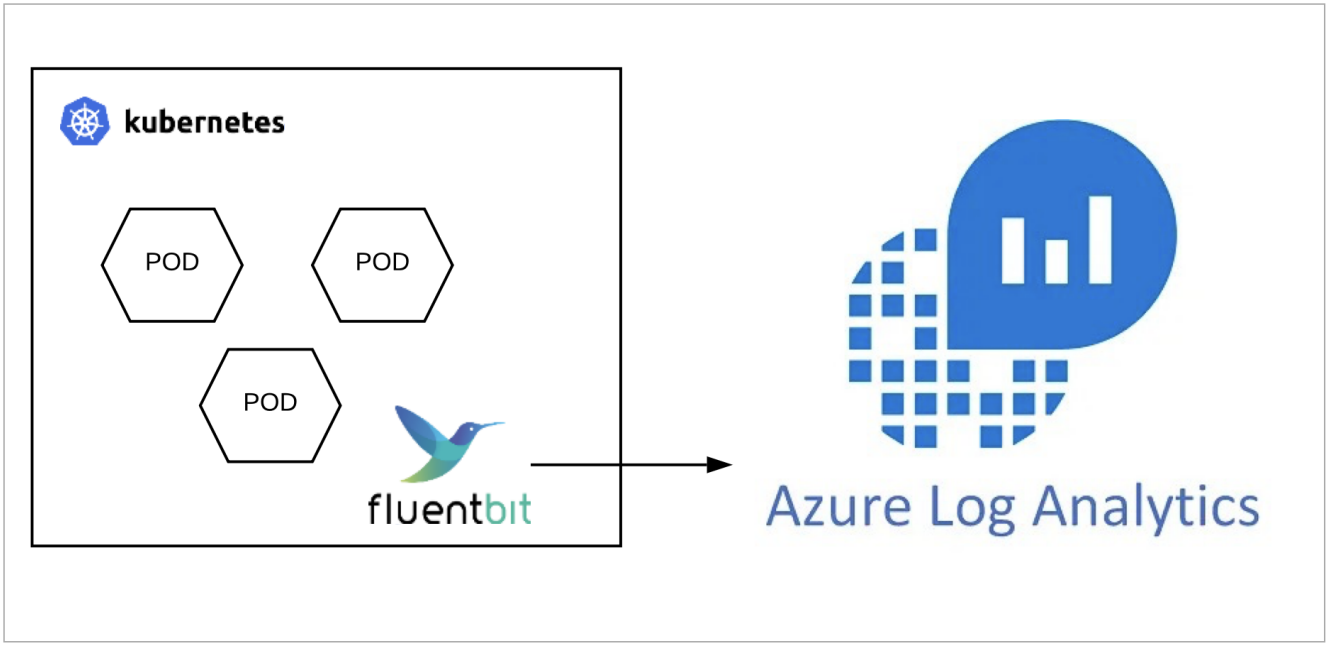
Fluentbit to Azure Analytics

Overview



Pre Requisits

Install Brew (Mac)

See https://brew.sh/

Install Helm

See https://helm.sh/docs/intro/install/

On Mac:

```
$ brew install helm
```

Create Test Pod

In order to properly test our logging solution, we will first add a ubuntu deployment to our Kubernetes cluster.

Create our Deployment

Create a yaml file to define our test ubuntu deployment. In this example we have sshd echoing to stdout (-e argument) in order to see the logs in Kubernetes.

```
$ vi ubuntu.yaml
```

ubuntu.yaml

```
apiVersion: v1
kind: Service
metadata:
  name: ubuntu
  labels:
    app: ubuntu
spec:
  type: NodePort
  ports:
    - port: 22
      targetPort: 22
      nodePort: 30022
  selector:
    app: ubuntu
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: ubuntu
  labels:
    app: ubuntu
spec:
  replicas: 1
  selector:
    matchLabels:
      app: ubuntu
  template:
    metadata:
      labels:
        app: ubuntu
    spec:
      containers:
        - name: ubuntu
          image: rastasheep/ubuntu-sshd:18.04
          command: [ "/usr/sbin/sshd","-D","-e" ]
```

Deploy it

```
$ kubectl apply -f ubuntu.yaml
```

Delete it

Want to start over, you can by deleting your previously applied yaml file.

```
$ kubectl delete -f ubuntu.yaml
```

Test SSH connection

Login to the pod using SSH (default password is root)

```
$ ssh -p 30022 root@localhost
```

Check Logging

```
$ kubectl get pods
NAME                      READY   STATUS    RESTARTS   AGE
ubuntu-ddc759bb8-5blsd   1/1     Running   0          2m14s

$ kubectl logs -f ubuntu-ddc759bb8-5blsd
Accepted password for root from 192.168.65.6 port 57022 ssh2
Received disconnect from 192.168.65.6 port 57022:11: disconnected by user
Disconnected from user root 192.168.65.6 port 57022
Failed password for root from 192.168.65.6 port 57088 ssh2
Failed password for root from 192.168.65.6 port 57088 ssh2
Failed password for root from 192.168.65.6 port 57088 ssh2
```

Install Fluentbit

```
$ mkdir tmp
$ cd tmp
$ git clone https://github.com/fluent/helm-charts.git
$ cd helm-charts/charts/fluent-bit/
$ vi values.yaml
```

Add the output config for azure. We can comment out the other OUTPUTS since we won't be using them.

```
...
    [OUTPUT]
        Name azure
                Match *
        Customer_ID XXX
        Shared_Key XXXX
```

Install

```
$ helm install fluent-bit .
```

Verify that it has been installed

```
$ kubectl get pods
```

Output:

```
NAME                     READY   STATUS    RESTARTS   AGE
fluent-bit-d7hr2         1/1     Running   0          38s
```

Check fluent-bit logs for errors

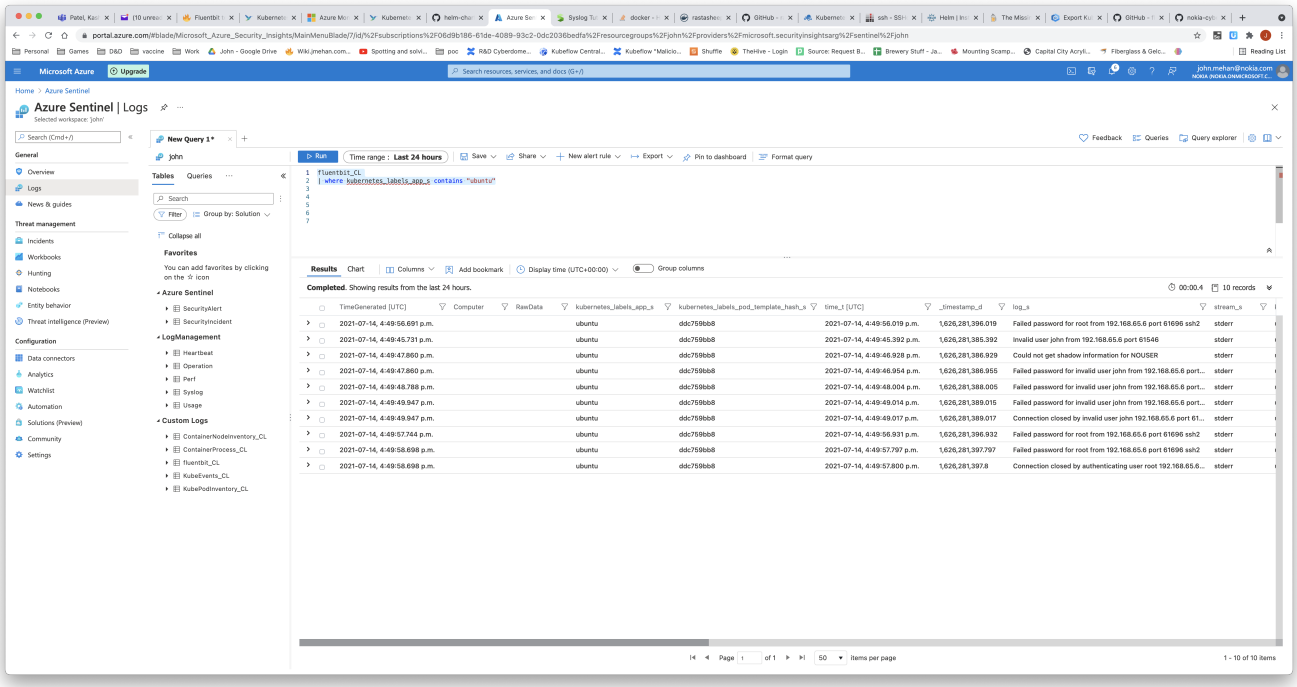
```
kubectl logs -f fluent-bit-d7hr2
```

Generate Some Logs

Using our test pod, we will generate some failed login attempts

```
$ ssh root@localhost -p 30022
root@localhost's password:
Permission denied, please try again.
root@localhost's password:
Permission denied, please try again.
root@localhost's password:
root@localhost: Permission denied (publickey,password).
```

View Logs in Azure Sentinel



Example Queries

```
fluentbit_CL


fluentbit_CL
| where kubernetes_labels_app_s contains "ubuntu"

fluentbit_CL
| where kubernetes_labels_app_s contains "ubuntu"
| where log_s contains "Failed password"
```

References

Reference	URL
Fluent bit	https://docs.fluentbit.io/manual/
Fluentbit Kubernetes Logging	https://docs.fluentbit.io/manual/installation/kubernetes
Azure Log Analytics	https://docs.fluentbit.io/manual/pipeline/outputs/azure
Azure Monitor overview	https://docs.microsoft.com/en-us/azure/azure-monitor/overview