Fluentbit to Azure Analytics

- Overview
- Pre Requisits
 - Install Brew (Mac)
 Install Helm
- Install H
 Create Test Pod
 - Create our Deployment
 - Deploy it
 - Deploy it
 Delete it
 - Test SSH connection
 - Check Logging
- Install Fluentbit
- Generate Some Logs
- View Logs in Azure Sentinel
 - Example Queries
- References

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/vi
kina: Deployment
metadata:
labelar
spec.
aslastar:
templata:
metadata:
labels:
app: ubuntu
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
                        READY STATUS
                                          RESTARTS
NAME
                                                    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

••• • 🔹 📫 Patel, Kasi 🗙 🖬 (10	unread 🗙 👋 Fluentbit :: 🗙 🍞 Kubernete	x 🚼 Azure Mori X 🏏 Kubernetici X 🔿 helm-chari X 🔺 Azur	Ser 🗴 💲 Syslog Tur 🗙 🦽 docke	r - H X 🛞 rastashee; X 🔿 GitHub - :	🗆 🗙 🦛 Kubernet: 🗙 🏭 ssh - SSH 🗙 🗍	🖶 Helm Insi 🗙 🍃 The Missir 🗴 😒 Export Kul 🗙 🕻	GitHub - 1 × O nokla-cyti × + O
← → C ☆ @ portal.azure.co	m/#blade/Microsoft_Azure_Security_Insight	s/MainMenuBlade/7/id/%2Fsubscriptions%2F06d9b186+61de+4089-9	3c2-0dc2036bedfa%2Fresourcegroup	os%2Fjohn%2Fproviders%2Fmicrosoft.se	curityinsightsarg%2Fsentinel%2Fjohn		🖈 📓 🙂 🗯 🕘 🗄
🖻 Personal 🛅 Games 🛅 D&O 🗎	vaccine 🔠 Work 🛕 John - Google Drive 🤞	💺 Wiki,imehan.com 📫 Spotting and solvi 🛅 poc 💥 R&D Cyberdon	e 🎯 Kubeflow Central 🔀 Kubeflo	w "Malicio 📴 Shuffle 🛞 TheHive - Log	ain 📔 Source: Request B 🚹 Brewery Stuff -	Ja 🛸 Mounting Scamp 🥝 Capital City Acryl 🥣 Fit	eerglass & Gelc 🚯 🗄 Reading List
😑 Microsoft Azure 🕑 Upgrad	5e		vices, and docs (G+/)			E 🗣 🐓	🐵 ? 🖉 john.mehan®nokia.com 🧟
Home > Azure Sentinel							
P Azure Sentinel Log	IS 🖈 …						×
P Search (Cmd+/) ≤	🧬 New Query 1* 🛛 🗧 🕂					♡ Feedbac	k 😰 Queries 🕞 Query explorer 🍥 🛄 🗠
General	🧬 john	Time range : Last 24 hours	hare \lor + New alert rule \lor \mapsto E	xport 🗸 🔗 Pin to dashboard 🛛 🚟 For	mat query		_
Overview 0	Tables Queries ··· 《	1 fluentbit_CL 2 where kubernetes labels app s contains "ubuntu"					
🧬 Logs	D Search :	3 4					
News & guides	Filter E Group by: Solution V	5					
Threat management	Collapse all	· ·					
Maddents	Favorites						۸
Hunting	You can add favorites by clicking	Results Chart 🔲 Columns 🗸 🕅 Add bookmark 🛛	Display time (UTC+00:00) 🗸 🛛 🖲	Group columns			
Notebooks	on the % icon	Completed. Showing results from the last 24 hours.					© 00:00.4 [10 records ₩
Entity behavior	E SecurityAlert	☐ TimeGenerated [UTC]	mData 🛛 🖓 kubernetes_labels_app	_s 🗸 kubernetes_labels_pod_template,	_hash_s ⊽ time_t (UTC)	² _timestamp_d ⊽ log_s	∑ stream_s ⊃ i
O Threat intelligence (Preview)	 E SecurityIncident 	> _ 2021-07-14, 4:49:56.691 p.m.	ubuntu	ddc759bb8	2021-07-14, 4:49:56.019 p.m.	1,626,281,396.019 Failed password for root from 192	168.65.6 port 61696 ssh2 stderr (
Configuration	LogManagement	> _ 2021-07-14, 4:49:45.731 p.m.	ubuntu	ddc759bb8	2021-07-14, 4:49:45.392 p.m.	1,626,281,385.392 Invalid user john from 192.168.65.	6 port 61546 stderr I
Data connectors	Heartbeat	 2021-07-14, 4:49:47.860 p.m. 	ubuntu	ddc759bb8	2021-07-14, 4:49:46.928 p.m.	1,626,281,386.929 Could not get shadow information	for NOUSER stderr i
📥 Analytics	E Derf	> _ 2021-07-14, 4:49:47.860 p.m.	ubuntu	ddc759bb8	2021-07-14, 4:49:46.954 p.m.	1,626,281,386.955 Failed password for invalid user jo	hn from 192.168.65.6 port stderr I
🖸 Watchlist	► E Synlog	> _ 2021-07-14, 4:49:48.788 p.m.	ubuntu	ddc759bb8	2021-07-14, 4:49:48.004 p.m.	1,626,281,388.005 Failed password for invalid user jo	hn from 192.168.65.6 port stderr I
S Automation	► III Usage	> _ 2021-07-14, 4:49:49.947 p.m.	ubuntu	ddc759bb8	2021-07-14, 4:49:49.014 p.m.	1,626,281,389.015 Failed password for invalid user jo	hn from 192.168.65.6 port stderr (
Solutions (Preview)	 Custom Logs 	> _ 2021-07-14, 4:49:49.947 p.m.	ubuntu	ddc759bb8	2021-07-14, 4:49:49.017 p.m.	1,626,281,389.017 Connection closed by invalid user	john 192.168.65.6 port 61 stderr (
Community	ContainerNodeinventory_CL	2021-07-14, 4:49:57,744 p.m.	ubuntu	ddc759bb8	2021-07-14, 4:49:56.931 p.m.	1,626,281,396.932 Failed password for root from 192	168.65.6 port 61696 ssh2 stderr
Settings	E fluentbit_CL	2021-07-14, 4:49:58:698 p.m.	ubuntu	000759008	2021-07-14, 4:49:57.797 p.m.	1626,28 (397.797 Palled password for root from 192	100.000 port 01090 senz stolerr
	H KubeEvents_CL	· · · · · · · · · · · · · · · · · · ·	usunu	646708660	2021-07-14, 4148-07-000 p.m.	Connection Connection Connection	ing user four 192.100.00.00
	E KubePodInventory_CL						
					\square		
				III II Page 1 of 1	▶ ▶I 50 ▼ items per page		1 - 10 of 10 items
-							

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