Deep Network GmbH

Landsbergerstr. 302 | 80687 München | Deutschland +49 (0) 89 6151 5236 | www.deepnetwork.com

Effective AKS and Logging: 3-day Workshop

Effective Azure Kubernetes Service (AKS) and Logging workshop aims to give the knowledge of managing the logs inside an AKS cluster.

- On the first day, we will start with introducing the concepts and components in general and start getting our hands dirty with Elasticsearch and Kibana
- The second day will be about continuing the Elasticsearch topics and start getting knowledge about log collectors. In this day, we will have hands-on experience with Fluentbit/Fluentd
- For the last day, we will cover the leftover topics for Fluentbit/Fluentd from the earlier day and finish the day with end-to-end setup with putting all components together.

Pre- requisites

[Azure AKS introduction offering]

Program

Day-1

Introduction — 1h

How to see your logs in AKS — 1h

Where does AKS keeps the logs
What is Elasticsearch? Why it is suitable for storing logs?
What is log collectors (Fluentbit/Fluentd)? How they can fetch the logs from containers?
What is Kibana? How can you visualize your data?

Elasticsearch & Kibana - Up & Running — 6h

Deploying Elasticsearch as statefulset — 1h

Deploying Kibana as deployment

Lab-1: Set up an Elasticsearch Cluster — 2h

- Create a 3 node Elasticsearch Cluster
- Create a Kibana deployment
- Create an index
- Populate the index with some data
- Query the data from Kibana

Configuring Elasticsearch & Kibana — 1h

- The resource requirements
- Indices and shards

Lab-2: Configuring Elasticsearch Cluster — 2h

- Create a 3 node Elasticsearch Cluster
- Create indices with different primary and replica shard options and observe shard distribution across the nodes
- Populate indices with some data and observe log distribution across the shards

Deep Network GmbH

Landsbergerstr. 302 | 80687 München | Deutschland +49 (0) 89 6151 5236 | www.deepnetwork.com

Day-2

Elasticsearch & Kibana - Up & Running (con't) — 4.5h

Configuring Elasticsearch (con't) — 0.5h

- Mappings

Using Elasticsearch API — 0.5h

- Automated Configurations
- Monitoring

Lab-3: Mapping in Elasticsearch Indices — 2h

- Create a 3 node Elasticsearch Cluster
- Create couple of indices
- Use different mapping settings inside indices
- Populate indices with some data
- Observe insert latencies from Elasticsearch API
- Observe read latencies from Elasticsearch API

Managing Elasticsearch Indices with Curator — 0.5h

- Automated actions in indices

Lab-4: Using curator to automate actions in indices — 1h

- Create a 3 node Elasticsearch Cluster
- Index creation with curator jobs
- Index deletion with curator jobs

Fluentbit/Fluentd - Up & Running — 2.5h

Deploying Fluentbit/Fluentd as daemonset — 0.5h

Lab-5: Set up Fluentbit/Fluentd Daemonset — 2h

- Create a Fluentbit/Fluentd daemonset
- Configure it such that each Fluentbit/Fluentd pod collects and prints the logs of all pods inside the node
- Configure it such that each Fluentbit/Fluentd pod collects and prints the logs of specific pods inside the node

Deep Network GmbH

Landsbergerstr. 302 | 80687 München | Deutschland +49 (0) 89 6151 5236 | www.deepnetwork.com

Day-3

Fluentbit/Fluentd - Up & Running (Con't) — 6h

Processing logs — 1h

- Parsing
- Enriching

Lab-6: Processing Logs in Fluentbit/Fluentd — 2h

- Create a Fluentbit/Fluentd daemonset
- Parse the logs
- Enrich the logs
- Modify the logs

Forwarding logs to Elasticsearch — 0.5h

Monitoring Fluetndbit/Fluentd — 0.5h

Lab-7: The complete e2e setup — 2h

- Create a 3 node Elasticsearch Cluster & configure
- Create a Kibana deployment
- Create a Fluentbit/Fluentd daemonset & configure
- Forward logs from Fluentbit/Fluentd to Elasticsearch
- Query the logs from Kibana

QA Session — 1h