Amazon Elasticsearch Service Workshop

Christian Mueller
AWS Senior Solutions Architect

aws certified Machine Learning Specialty
aws certified Big Data Specialty
aws certified Solutions Architect Associate
aws certified Solutions Architect Professional
aws certified Security Specialty
aws certified SysOps Administrator Associate
aws certified Cloud Practitioner
aws certified DevOps Engineer Professional
aws certified Advanced Networking Specialty
aws certified Developer Associate
aws certified Alexa Skill Builder Specialty

Agenda for the week

Monday

Personal Introduction

Goal for this workshop

Workshop architecture

Current usage of Splunk

Introduction into core AWS services for this workshop

Tuesday

Lab-1: Set-up of Amazon Elasticsearch cluster

Lab-1 execution

Lab-2: Provision Amazon EKS cluster with Fluentd

Lab-2 execution

Wednesday

Lab-3: Automated backup & retention

Lab-3 execution

Lab-4: Ad-hoc queries on old data

Lab-4 execution

Lab-5: Governance

Lab-5 execution

Thursday

Deep dive into Amazon Elasticsearch Service

Roadmap

Cost calculation of the proposed architecture with the assumed load

”Ask us anything about the architecture & services we proposed”

Friday

Adapting the MVP to your needs

or

Addressing missing features in this MVP

General feedback

Conclusion & next steps

Agenda for Monday

Introduction

Personal Introduction

What's your job role?

What AWS experience do you have?

Anything in particular you are looking for?

Goal

What is your desired outcome for this week?

What is your desired outcome for this PoC?

How do you measure it?

Architecture

Walk through to workshop architecture at high level.

Discuss the main focus for each lab?

Get first feedback whether something important is missing.

Splunk

How do you use Splunk today [in the context of this PoC]?

Which features of Splunk you are using?

Services

Elasticsearch Service

CloudFormation / SAM

Step Functions

Lambda

API Gateway

CloudWatch

[EKS]

Agenda for Tuesday

Lab-1

Introduction into the architecture

Ways to share common configurations (endpoints, …)

Using CloudFormation to provisioning an ES cluster

Access the cluster with the CLI and Kibana

Lab-1

Implement Lab-1 in your account(s)

Lab-2

Introduction into the architecture

Using CloudFormation to provisioning an Amazon EKS cluster with Fluentd to ingest sample [log] data

Lab-2

Implement Lab-2 in your account(s)

Agenda for Wednesday

Lab-3

Introduction into the architecture

How to create manual index snapshots?

How to delete outdated indexes?

Automate the process with Step Functions & Lambda

Lab-3

Implement Lab-3 in your account(s)

Lab-4

Introduction into the architecture

How to restore index snapshots?

Automate the process of creating a new Amazon ES cluster and restore index snapshots with Step Functions & Lambda

Lab-4

Implement Lab-4 in your account(s)

Lab-5

Introduction into the architecture

How to automate monitoring / operations for the ES cluster?

How to terminate the on-demand ES cluster automatically?

Automate these operations with Step Functions and Lambda

Lab-5

Implement Lab-5 in your account(s)

Agenda for Thursday

ES deep dive

Deep dive into Amazon ES

Roadmap

Outlook what’s coming in the near future.

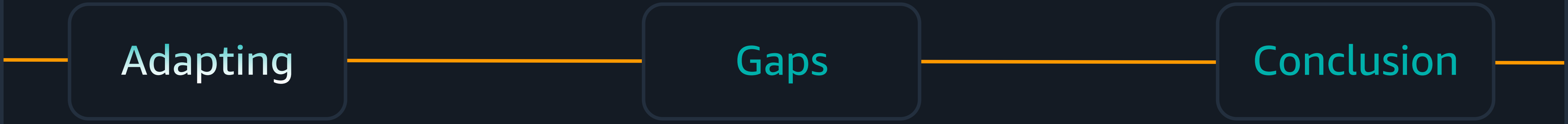
Cost

Calculate the cost for this architecture

Ask anything

Ask us anything about the AWS/Amazon services we are using in this architecture.

Agenda for Friday



Adapting

General feedback to the workshop

How can we improve the workshop / MVP so that it would be more useful for you?

Gaps

Addressing missing features in Amazon ES

Addressing missing features in this MVP

Conclusion

Conclusion

Next steps

Thank you!

Christian Mueller

AWS Sr. Solutions Architect

cmr@amazon.de