Being a regulated entity in AWS

LUNAR

Talents in Tech

113

(563 overall)

21

Squads

16#

Largest bank in DK

Founded in

2015

+650K

Users

123K new in 2022

3

Hubs

CPH+AAR+STO

100+

Daily deploys

400+

Microservices

Agenda

Access federation and management

Infrastructure and security as code

Relevant regulation and next steps

LUNAR

Access federation and management

LUNAR

Why and how?

Access federation

- Carry the context of your identity provider into AWS and audit logs
- Centralised and easy access management
- Automatically comply with your password and MFA policies
- Use the AWS IAM Identity Center

AWS SSB: ACCT.02, ACCT.05, ACCT.06

Pro tip

Go to documentation for AWS CLI SSO integration

Access federation

- Use the AWS CLI tool (https://github.com/aws/aws-cli) which supports SSO login for AWS IAM Identity Center:

```
aws sso login
```

See the QR code for a how to do this!

Why and how?

Access management

- Design IAM roles to enable least privilege access control
- Developers will have less risk of making mistakes that might affect the business
- Less access rights = less ways to mess up

AWS SSB: ACCT.04, WKLD.01

Pro tip

Go to documentation for AWS IAM Access Analyzer policy generation

Access management

- Day 1: Managed policies
- Day 2: Write your own policies

- Use the IAM Access Analyzer to generate least-privilege policies! (see QR code)

Infrastructure and security as code

LUNAR®

Why and how?

Infrastructure as Code (IaC)

- Limit Click-Ops and migrate to IaC!
- Use Terraform or AWS CloudFormation to define the resources
- IaC enables proper change management for your infrastructure

Pro tip

Go to the Atlantis Github repository

Infrastructure as Code (IaC)

- Use automation tools for deployment, don't allow developer machines for deployment!
- Free automation for Terraform: Atlantis (see QR code)

Why and how?

Go to the community created Terraform modules

Security as Code (SaC)

- Implement your security best practises as code
- Make it easy to do the right things!
- Create or use pre-defined modules for Terraform or CloudFormation
- Community created ones are also available (see QR code)

AWS SSB: WKLD.15

Relevant regulation and next steps

LUNAR®

Why and what?

Relevant regulation

- Financial entities: The Digital Operational Resilience Act (DORA)
- A lot of others: NIS 2
- Certifications etc: PCI DSS, ISO27001, SOC1&2

All of these different regulations and certifications have requirements regarding access management, the use of least privilege and proper and secure change management.

Why and what?

Go to the AWS Well-Architected framework

Next steps

- Start with the AWS Startup Security Baseline
- Move on to the AWS Well-Architected framework

The AWS Well-Architected Framework describes key concepts, design principles, and architectural best practices for designing and running workloads in the cloud.

Go to the link in the QR code to get started!