aws

COMMUNITY DAY

AOTEAROA

aws

COMMUNITY DAY

AOTEAROA

EKS Pod Admission Control: KMS + Cosign + Kyverno

Dinesh Sharma | 06/09/2023

WHAT, WHY & HOW

- WHAT does securing container supply chain security means?
- WHY is securing the container supply chain important?
- HOW to secure the container supply chain?

WHAT does container supply chain security means?

“Securing container supply chain refers to the set of practices and technologies that are used to ensure the security of container images as it moves through the software supply chain, from development to production.”

aws COMMUNITY DAY AOTEAROA

WHY is securing the container supply chain important?

“We need container supply chain security to ensure that the container images we use to build and run our applications are secure and haven't been tampered with”

aws COMMUNITY DAY AOTEAROA

HOW can we secure the container supply chain?

- Container vulnerability scanning (both OS and Application)
- Signing container images
- Pod admission control

aws

COMMUNITY DAY

AOTEAROA

Signing container images

Cosign

Cosign is an open-source project that enables users to sign and verify container images.

KMS

Cosign can be integrated with KMS to sign the container image

Pod admission control

Pod admission control refers to a process which ensures that only authorized and signed containers can run inside a K8 cluster.

In layman terms, It's like a bouncer at a club who checks everyone's ID to make sure they're old enough to enter and don't have anything dangerous on them

How to implement pod admission control ?

Kyverno

Kyverno is a Kubernetes-native policy engine that enables you to define, validate, and enforce policies for your Kubernetes workloads.

Kyverno policies

Policy to verify image and namespace
Policy to verify if the images are from allowed registries

Demo

aws

COMMUNITY DAY

AOTEAROA

Thanks