GKE Security

Crafting Captivating Tales with Mighty Thor...

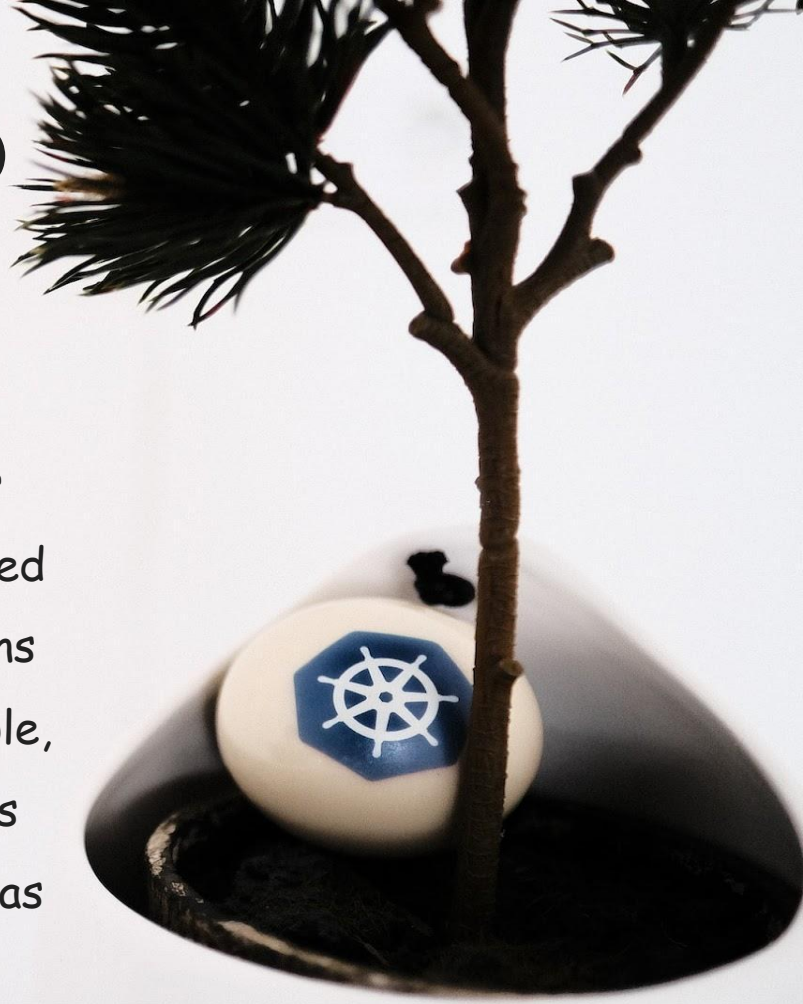
By:
Nitin S
Product Security, Salesforce

Contents

Activity first… (Find the ‘क’ thing)

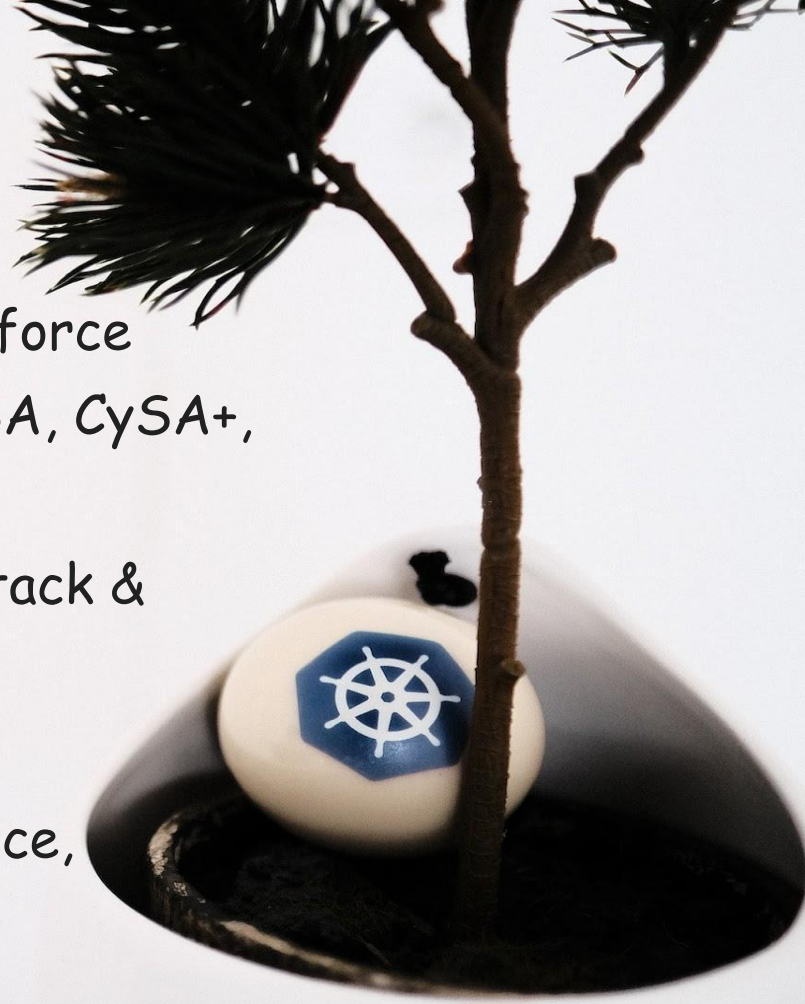
Why you need Kubernetes and what it can do ?

Containers are a good way to bundle and run your applications. In a production environment, you need to manage the containers that run the applications and ensure that there is no downtime. For example, if a container goes down, another container needs to start. Wouldn't it be easier if this behavior was handled by a system?

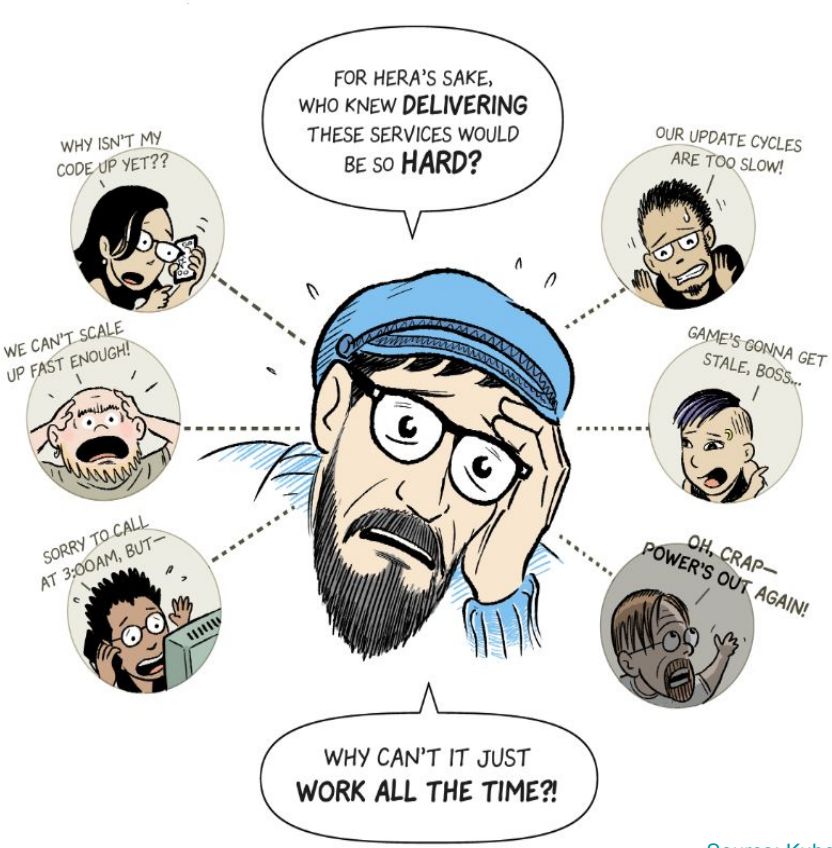


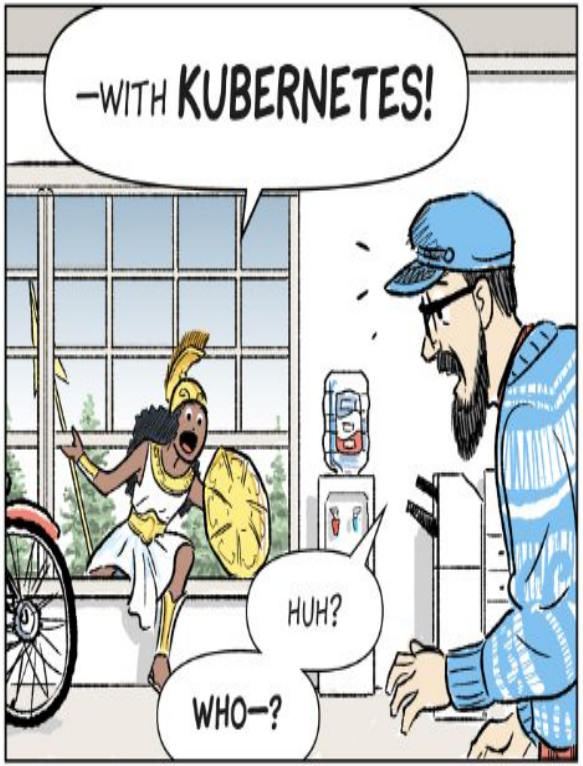
$ whoami

- Sr. Product Security Engineer, Salesforce
- 4x-AWS Certified, SANS GIAC GCSA, CySA+, Pentest+, etc.
- Author of "Securing Docker: The Attack & Defense Ways"
- Speaker at ACD South Asia 2021, NullCon Webinar, HexNode Conference, AWS Security Series, etc.



$ K8s Intro…





Source: Kubernetes Comic by Google

$ Mighty Thor 

Afraid of K8s!!!

SwiftOnSecurity
@SwiftOnSecurity

Subscribe

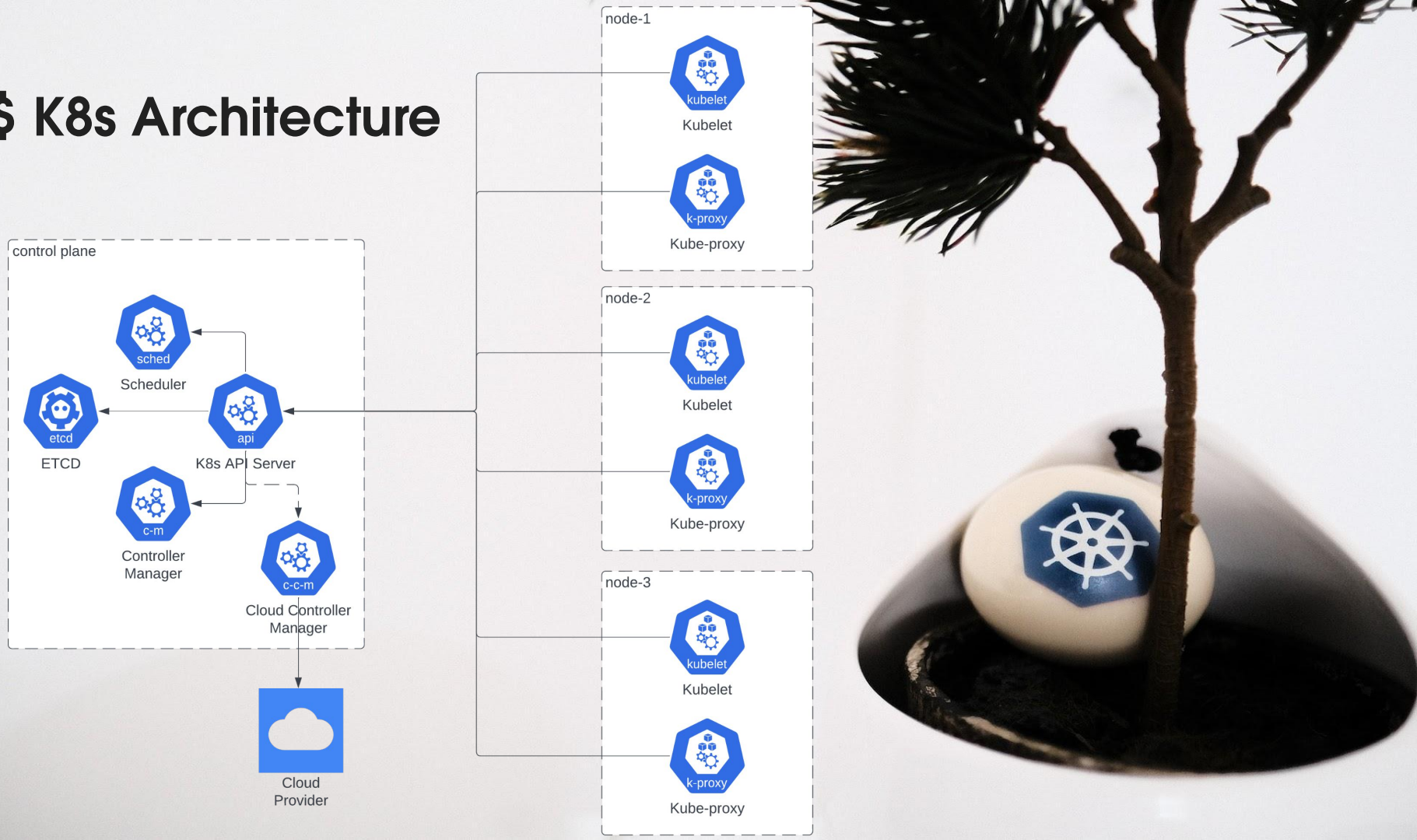
One time I tried to explain Kubernetes to someone.
Then we both didn't understand it.

9:10 PM · Aug 6, 2019

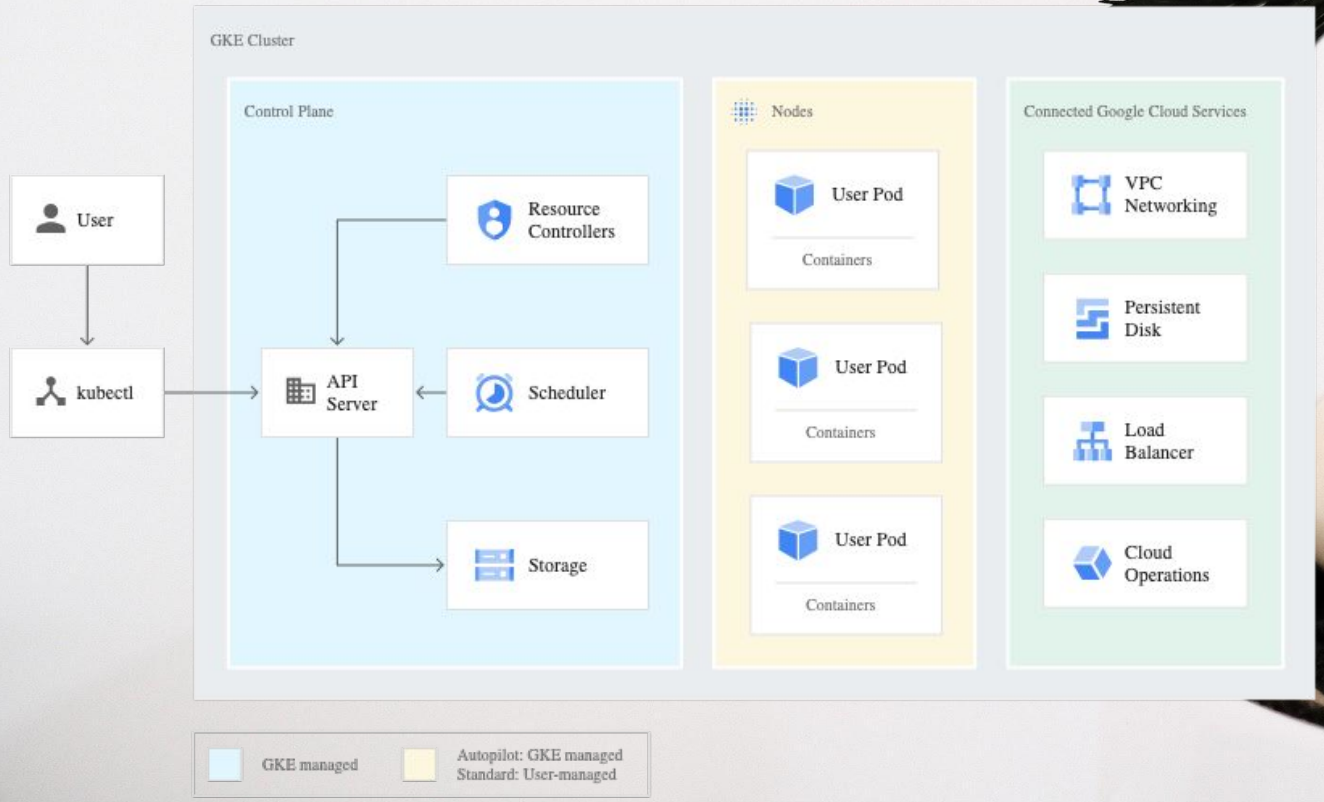
41 523 2.8K 43

Source: @SwiftOnSecurity at X Platform

$ K8s Architecture



$ GKE Architecture



Source: Official GKE Documentation

$ Shared Responsibility in GKE

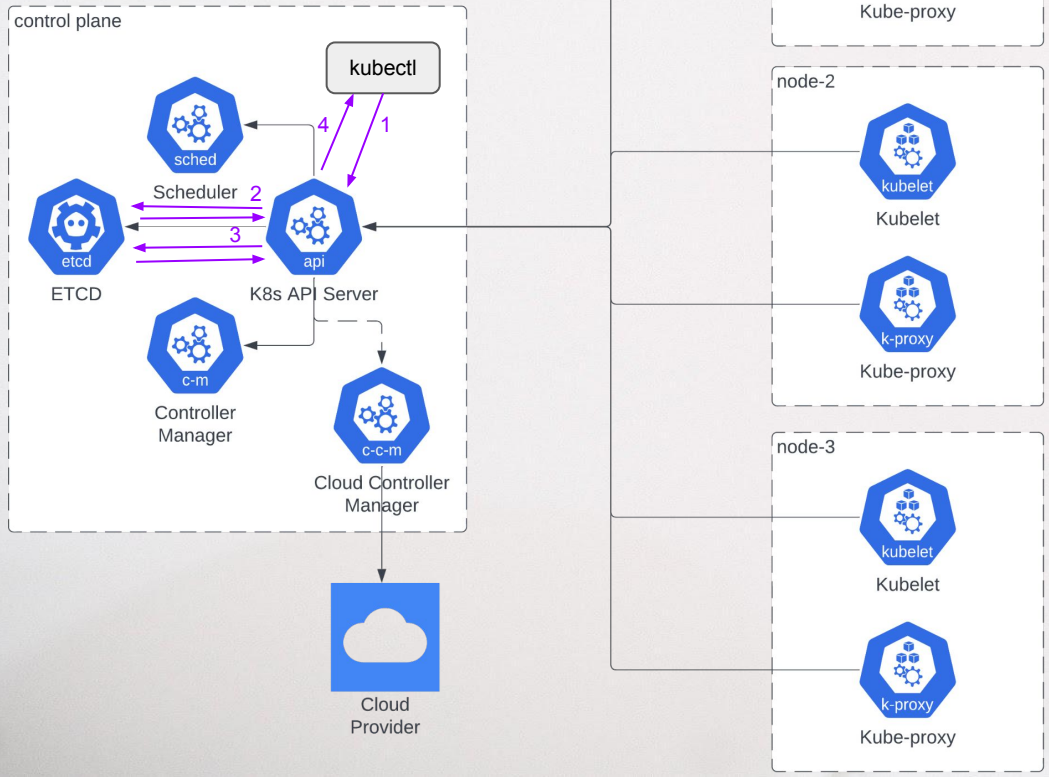
Google's Responsibility

- K8s Distro
- Node OS
- Control Plane
- Google Cloud Integrations

User's Responsibility

- Nodes
- Workloads

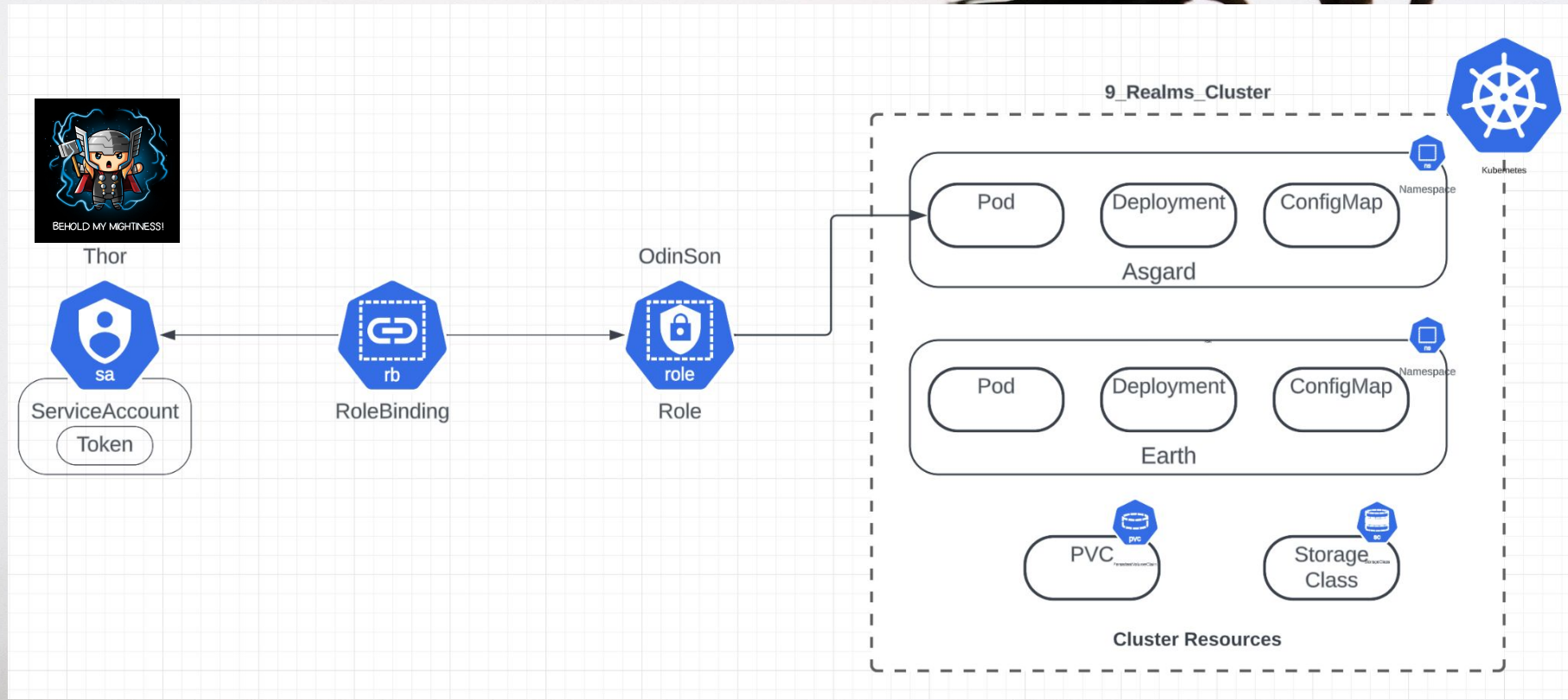
$ GKE RBAC Roles




```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: example-pod-reader
  namespace: my-namespace
rules:
- apiGroups: [“”]
  resources: [“pods”]
  verbs: [“get, watch, list”]
```

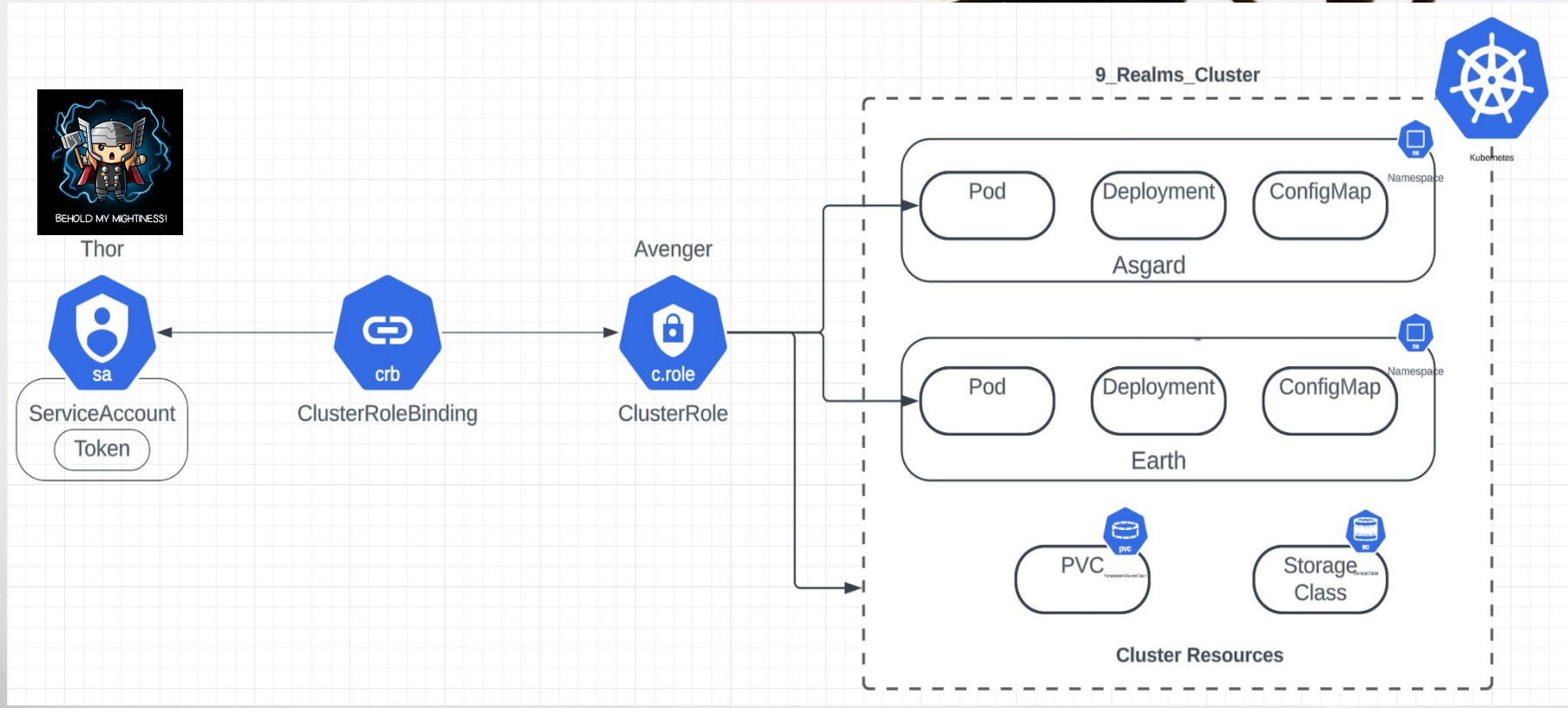
```
$ kubectl apply -f role.yaml
```

$ GKE RBAC Roles

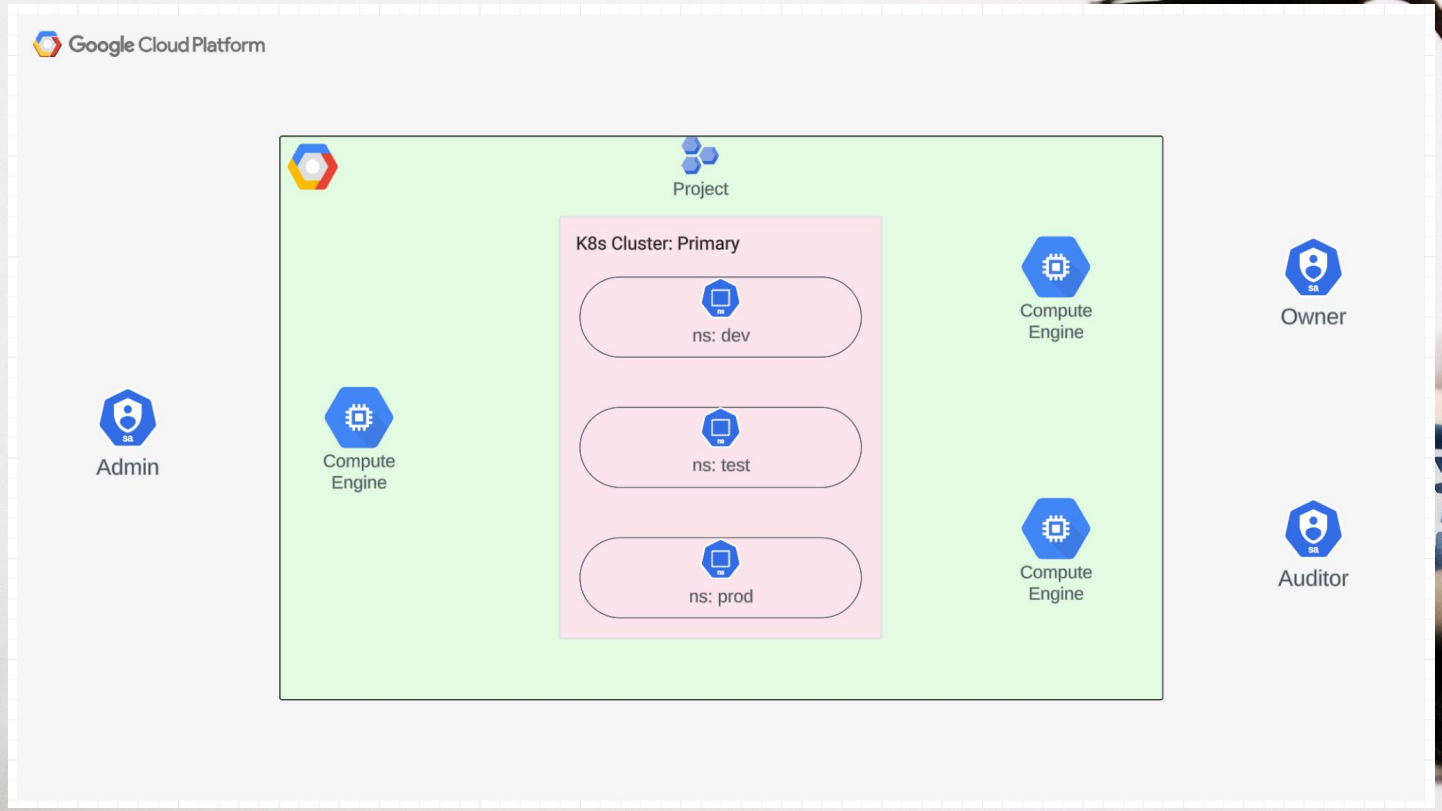


Thor, Just Says NO to HeimDall !!!

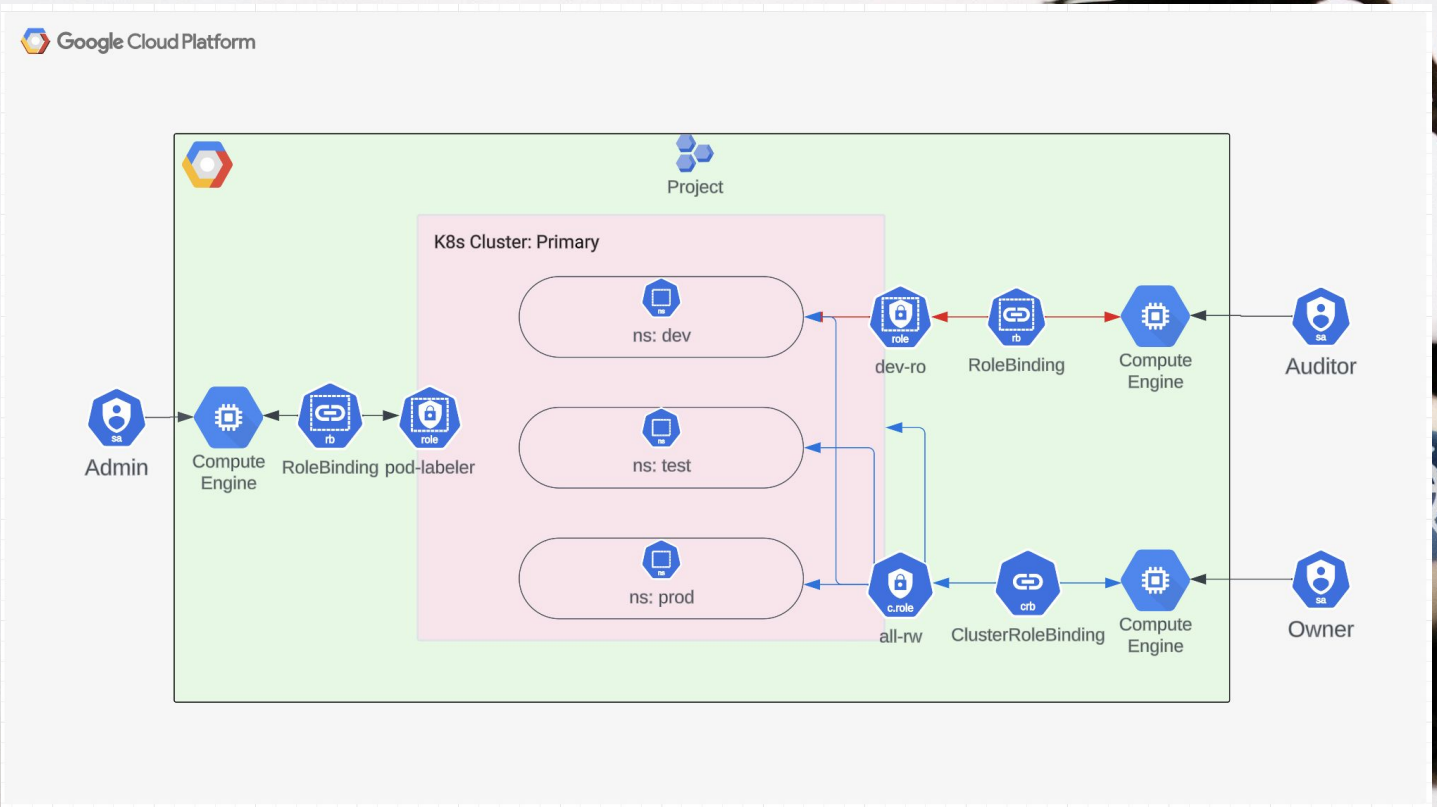
$ GKE RBAC ClusterRoles



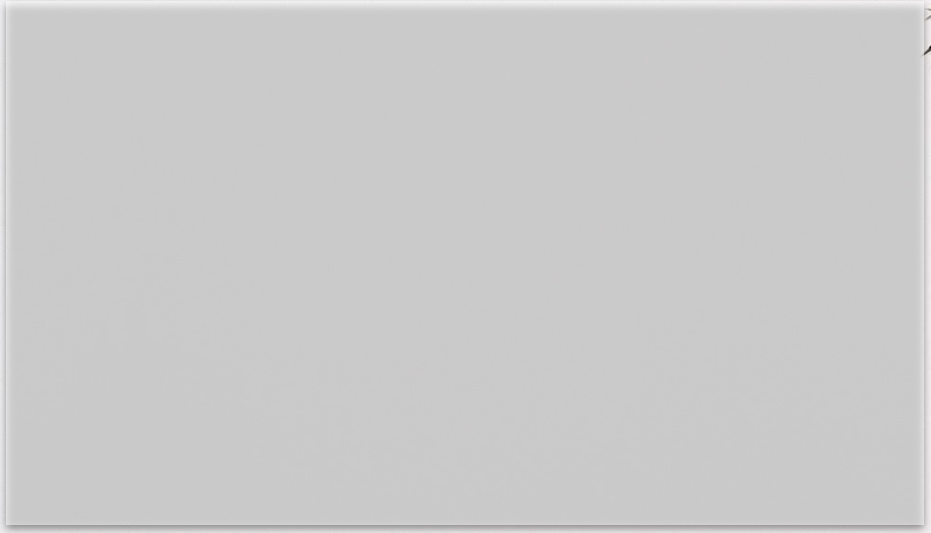
$ Before RBAC...


Google Cloud Platform
Project
K8s Cluster: Primary
ns: dev
ns: test
ns: prod
Admin
Compute Engine
Compute Engine
Compute Engine
Owner
Auditor

$ After RBAC...

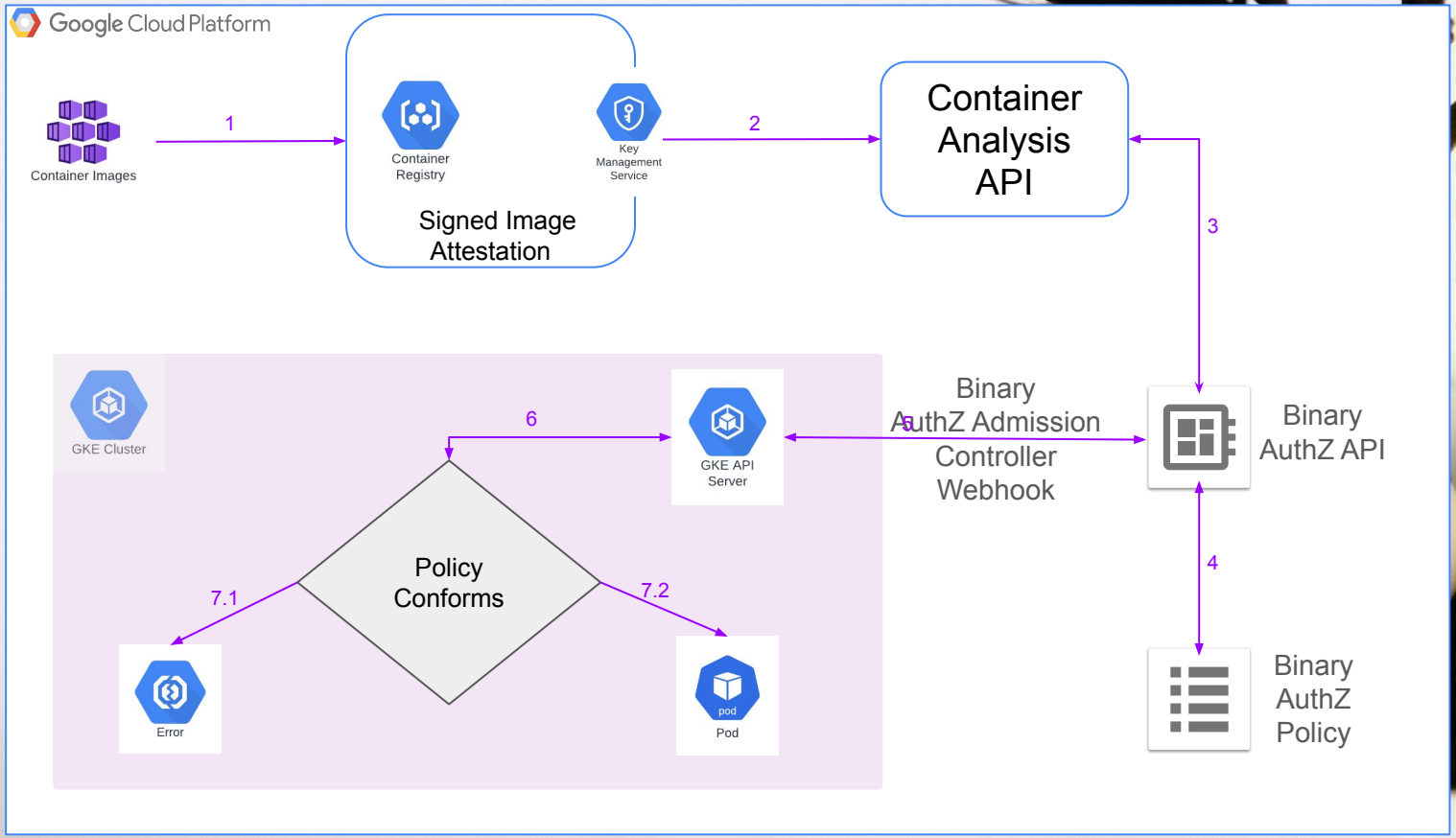

Google Cloud Platform
Project
K8s Cluster: Primary
ns: dev
ns: test
ns: prod
Admin
Compute Engine
RoleBinding
pod-labeler
dev-ro
RoleBinding
Compute Engine
Auditor
all-rw
ClusterRoleBinding
Compute Engine
Owner

$ Binary Authorization



- Supply Chain Security Feature
- Establish a preventative security posture by only running trusted code

$ Binary Authorization

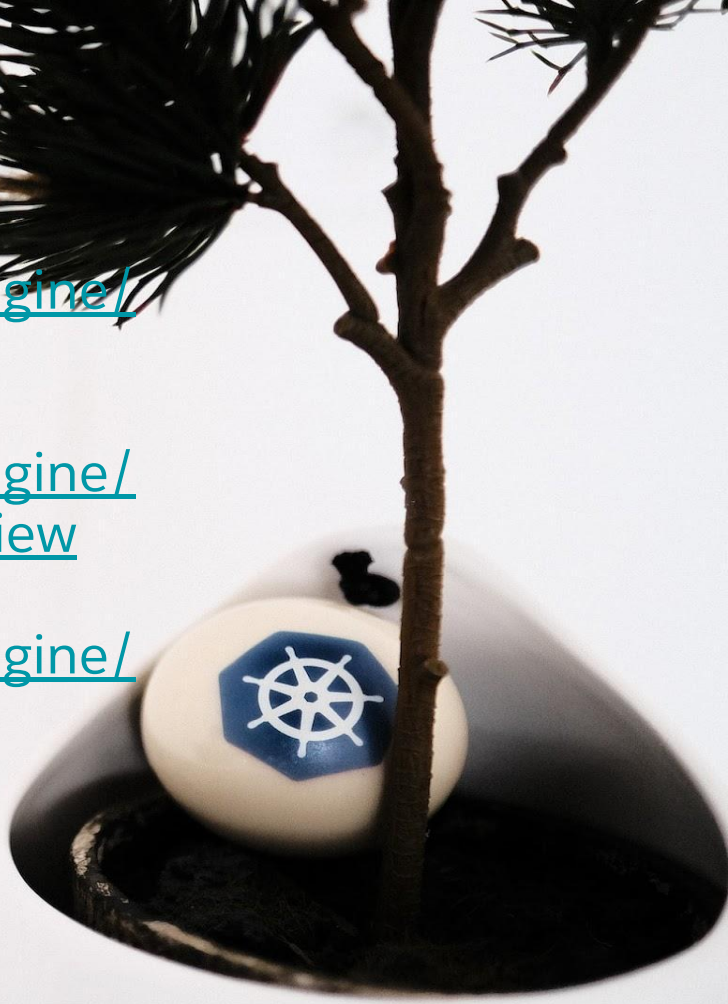


$ GKE Cluster Hardening

- Restrict Access to kubectl
- Use RBAC
- Use a N/W Policy
- Disable K8s Dashboard at all
- Disable Automatic Mounting of Service Account Token
- Use Binary Authorization for Pods and Ccontainer Images
- Use Pod Security Policies and other controls

References

- https://cloud.google.com/kubernetes-engine/docs/how-to/hardening-your-cluster
- https://cloud.google.com/kubernetes-engine/docs/concepts/kubernetes-engine-overview
- https://cloud.google.com/kubernetes-engine/docs/concepts/shared-responsibility



Thank You

Connect Over LinkedIn:

Ask Me on Quora: