WALLSEC

Kubernetes for Beginners

#UnFUCK24 Workshop

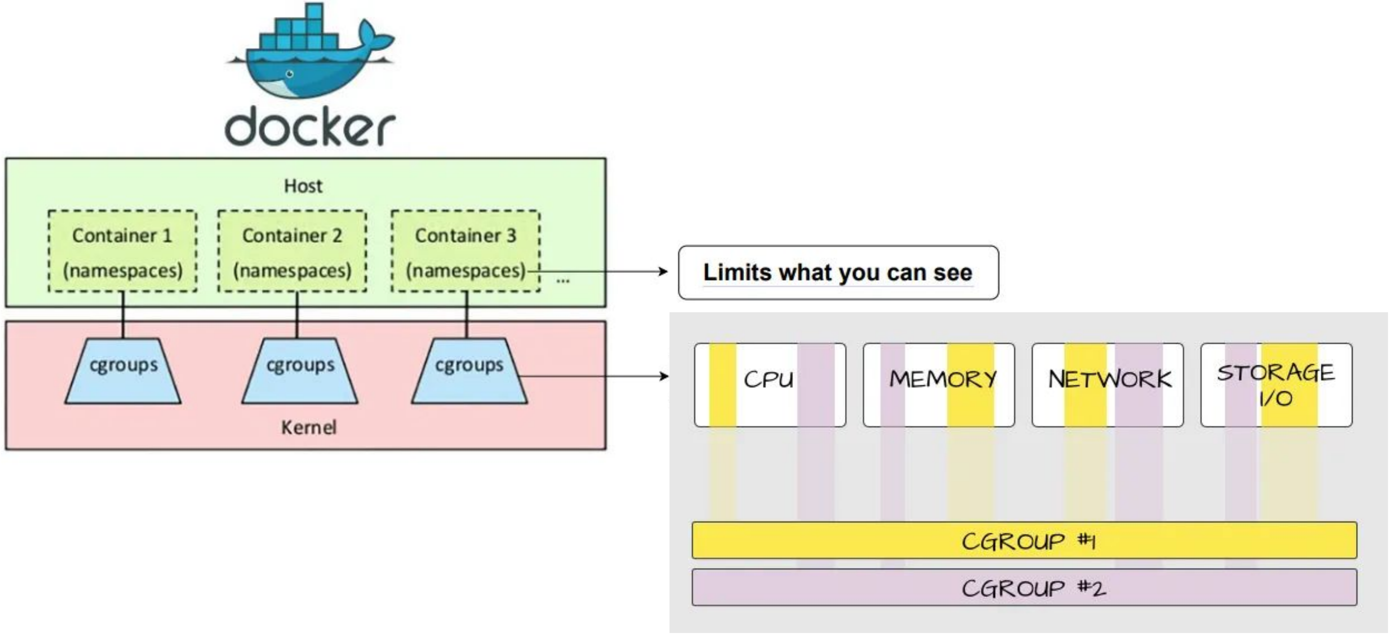
Date: 27.04.2024

Agenda

- Docker
    - Linux Namespaces
    - Container build process
- Kubernetes
    - Overview of architecture / components
    - Run a web application on Kubernetes
    - Security aspects / Hacking Mutillidae
- Optional Topics:
    - Volumes (in detail)
    - RBAC

Containers - Defined by Linux Namespaces

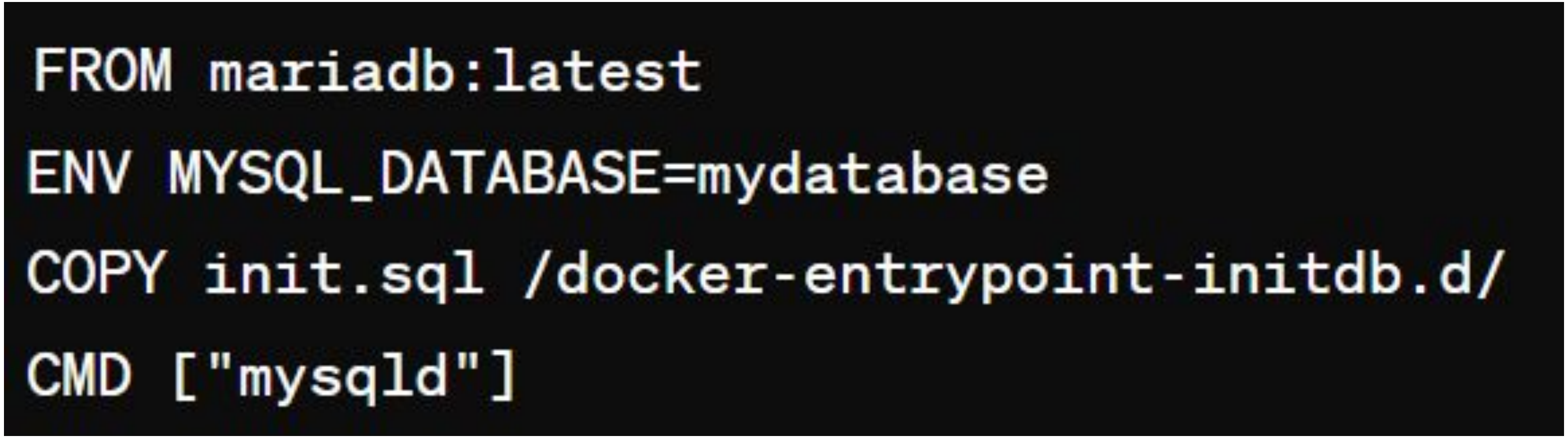
- Built on Linux Kernel features
- Encapsulated environments for applications and dependencies



Source: https://medium.com/@mrdevsecops/

Container Build Process - Docker File

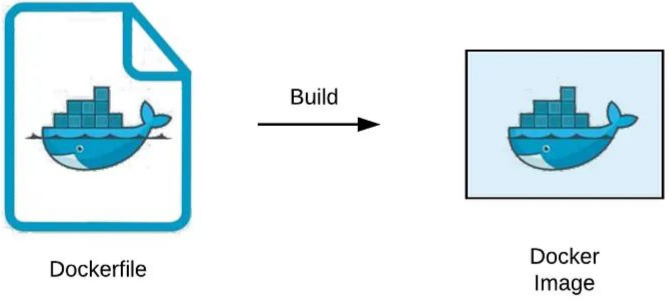
- Specifies the instructions needed to build a Docker Image



```
FROM mariadb:latest
ENV MYSQL_DATABASE=mydatabase
COPY init.sql /docker-entrypoint-initdb.d/
CMD ["mysqld"]
```

Container Build Process - Docker Image

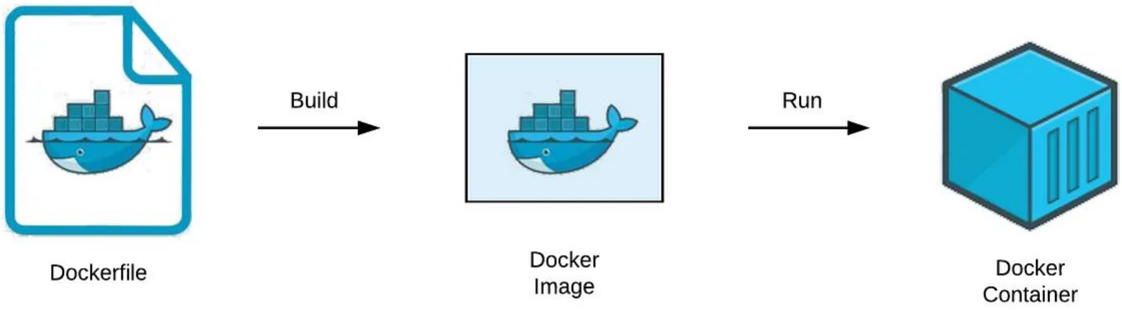
- Contains the application (code, dependencies)
- Serves as a template for generating Docker Containers
- Example: https://hub.docker.com/layers/webpwnized/mutillidae/database/images/



Source: https://medium.com/

Container Build Process - Docker Container

- Minimalistic toolset
- Storage modifications only during runtime
- Data persistence through mounted volumes



Source: https://medium.com/

Docker Setup in Ubuntu

Source: https://grigorkh.medium.com/

Intro To Kubernetes

- What is Kubernetes?
  - Container orchestration tool for managing containerized applications

- Why is it needed?
  - Evolution of software development
  - Monoliths → Microservices → Containers → Hundreds of Containers
- Features
  - High Availability
  - Scalability
  - Recovery

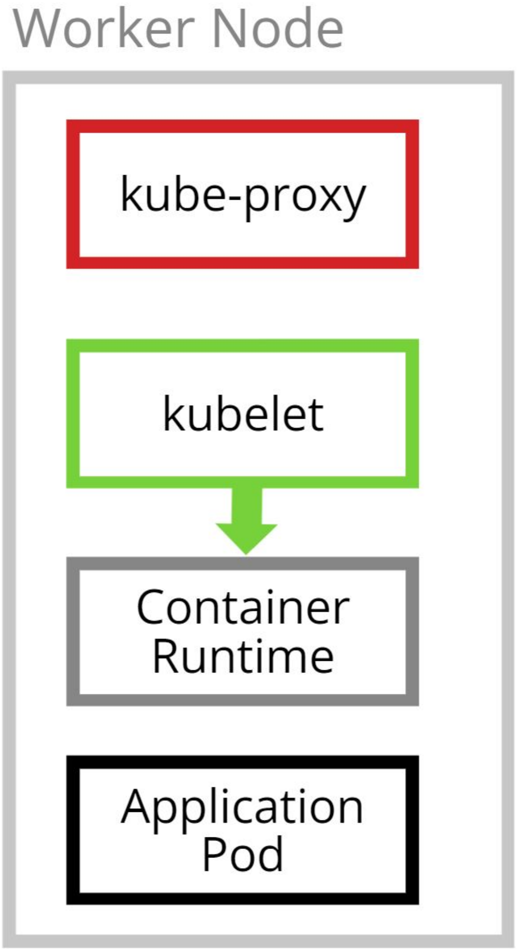
Source: https://github.com/kubernetes/

Kubernetes Cluster

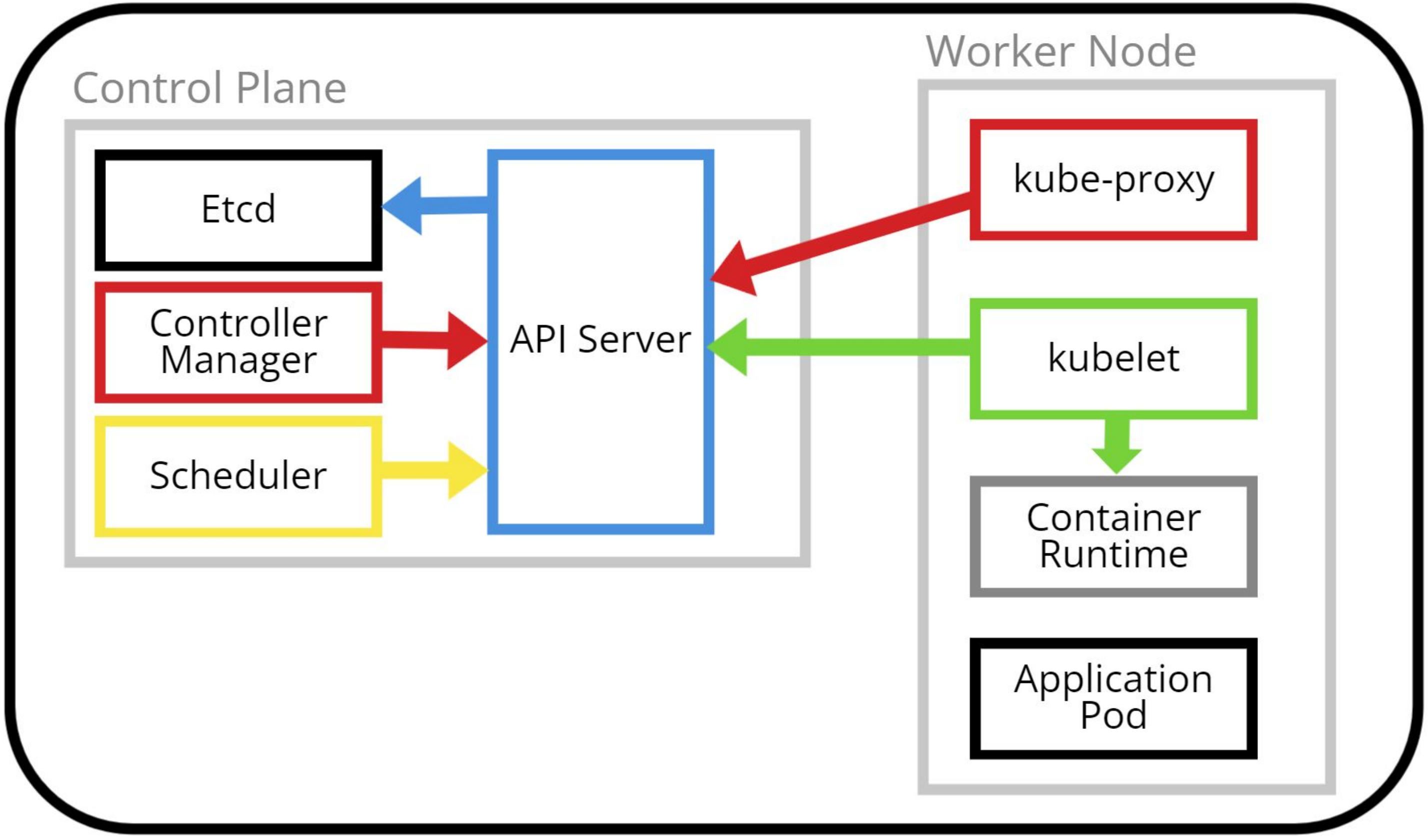
- Biggest organizational unit
- Consists of multiple Nodes working together
  - Worker Nodes
  - Master Nodes

Worker Nodes

- Virtual or physical machine
- Managed by the Control Plane
- Create Docker Container
- Provide the runtime
- Runs applications (Pods)

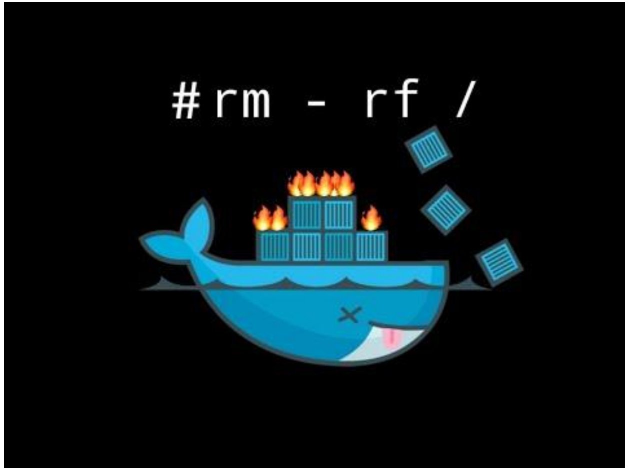


Kubernetes Cluster Architecture



Kubernetes Data Persistence

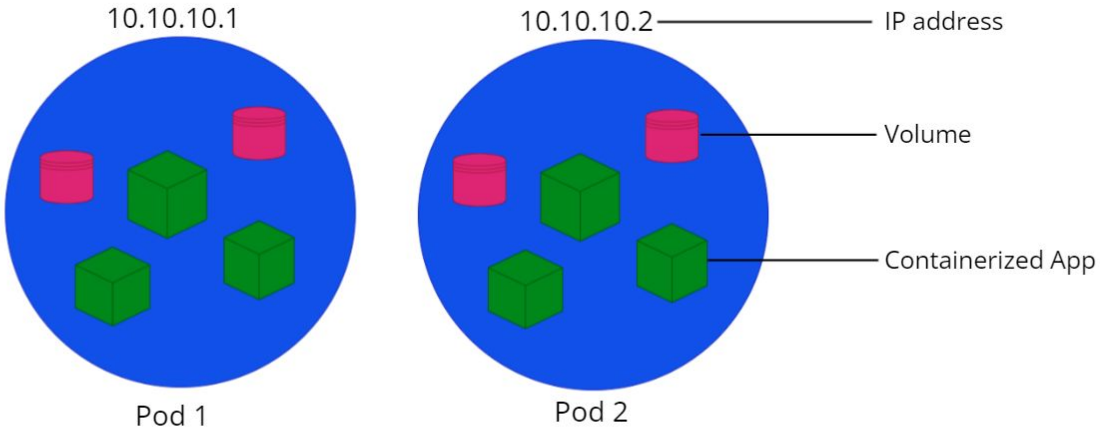
- No K8S-style (elegant) solution for persistence
- Local volumes / network shares



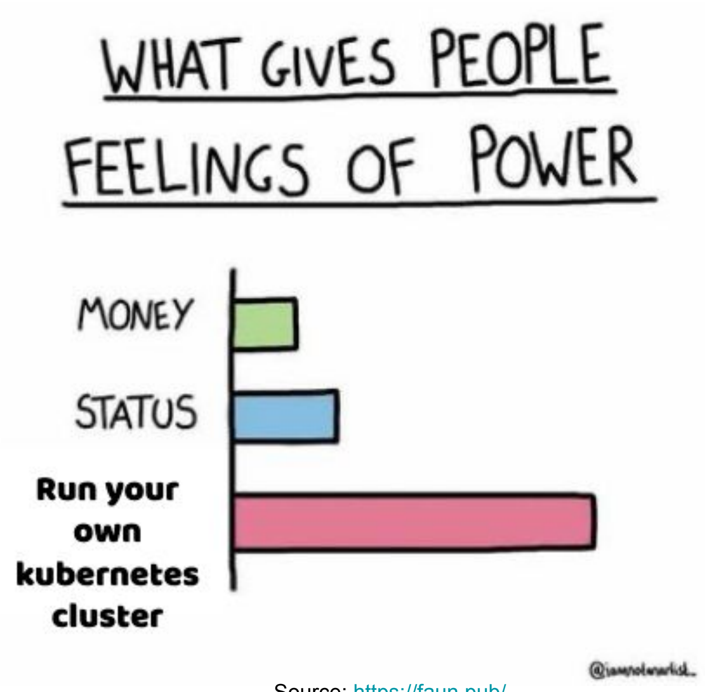
Source: https://www.youtube.com/@DAPHindiGaming/

Kubernetes Pods

- Smallest deployable unit
- Group of one or more containers
- Storage extension with Volumes



Create your own Cluster with Minikube


WHAT GIVES PEOPLE FEELINGS OF POWER
MONEY
STATUS
Run your own kubernetes cluster
@iamnotanartist_

Source: https://faun.pub/

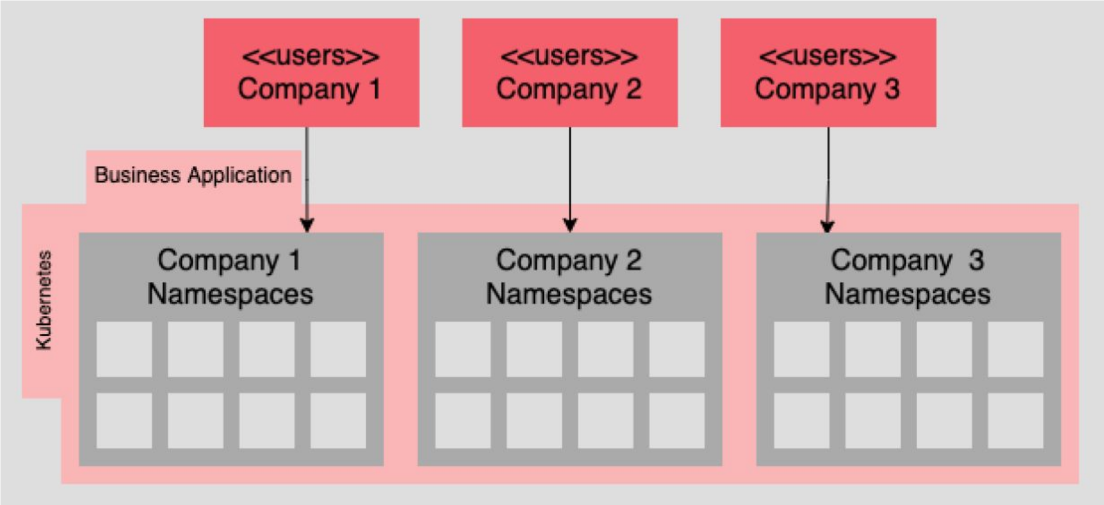
Minikube

- Lightweight Kubernetes implementation
- Simulates a Kubernetes environment
- Runs locally on a single Node

Source:https://github.com/kubernetes/minikube/

Kubernetes Namespaces

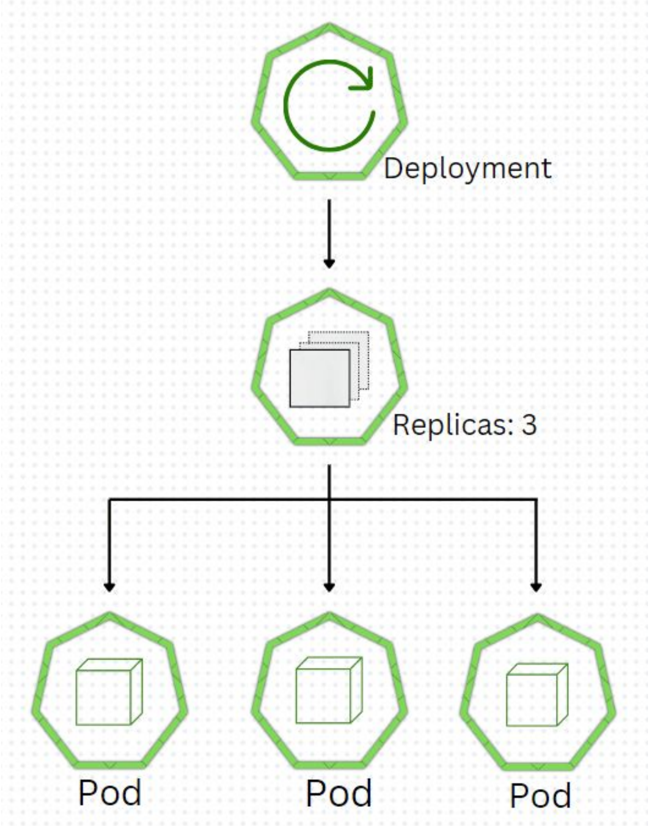
- Not Linux namespaces
- Resource isolation
- Resource allocation
- Resource sharing
- Component organization
- Access control policies



Source: https://www.redhat.com/

Deployment

- Deploying stateless applications
- Manages lifecycle of Pods
- Rollbacks and updates
- Self-Healing capabilities
- E.g. weather service



Source: https://media.geeksforgeeks.org/

Let’s deploy Mutillidae II

- Vulnerable Web-application
- Web Security Training
- Over 40 Challenges

Source: https://i1.wp.com/

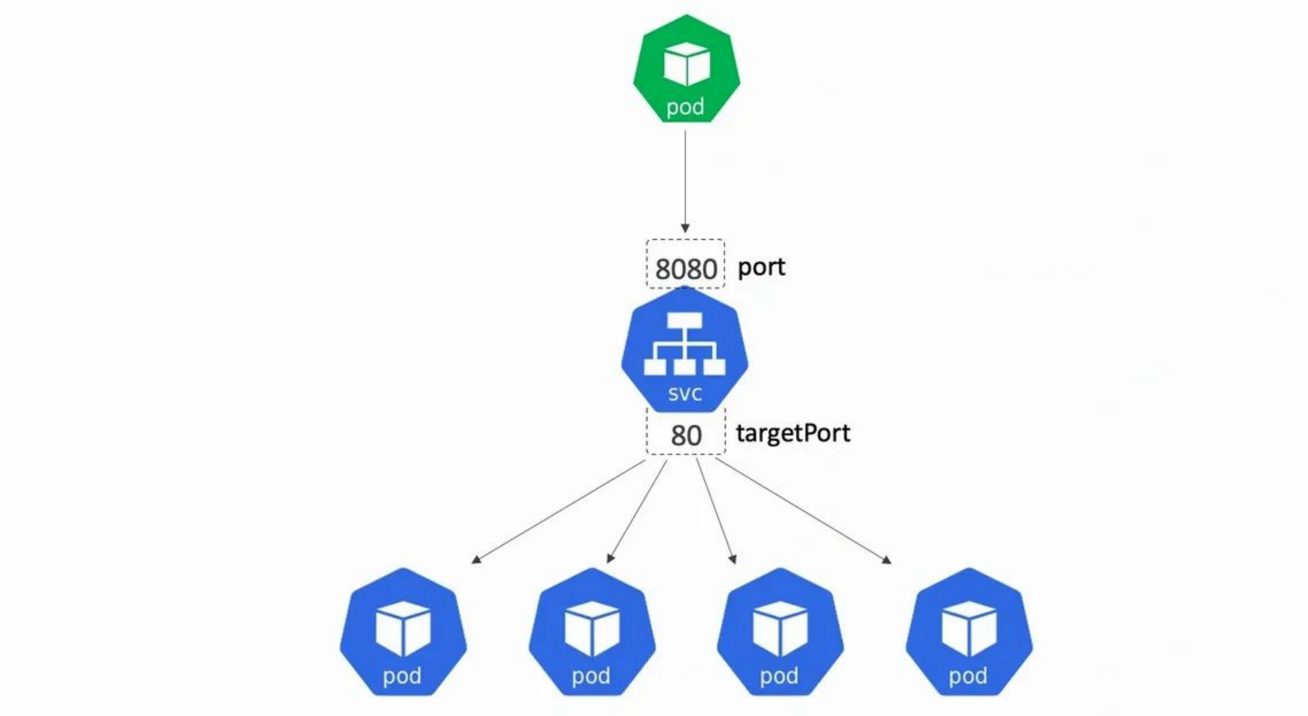
Kubectl

- Command Line Interface (CLI)
- Performs CRUD operations on Kubernetes resources
- Management of the Kubernetes Cluster

Source: https://camo.githubusercontent.com/

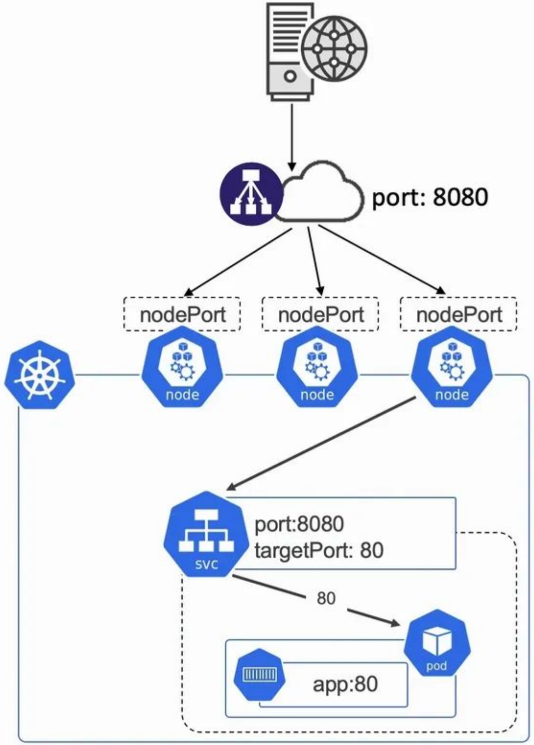
Services

- Abstraction of Pods
- Permanent IP address
- Load Balancing
- Service types:
    - ClusterIP (default)
    - NodePort
    - LoadBalancer
    - ExternalName



Source: https://nigelpoulton.com/

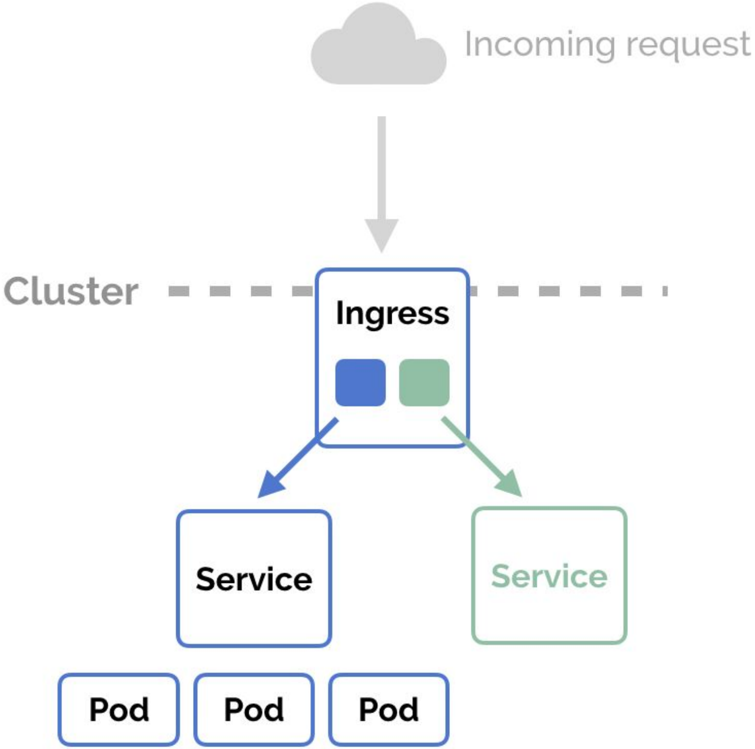
Exposing the Web-Application



Source:https://i0.wp.com/

Ingress

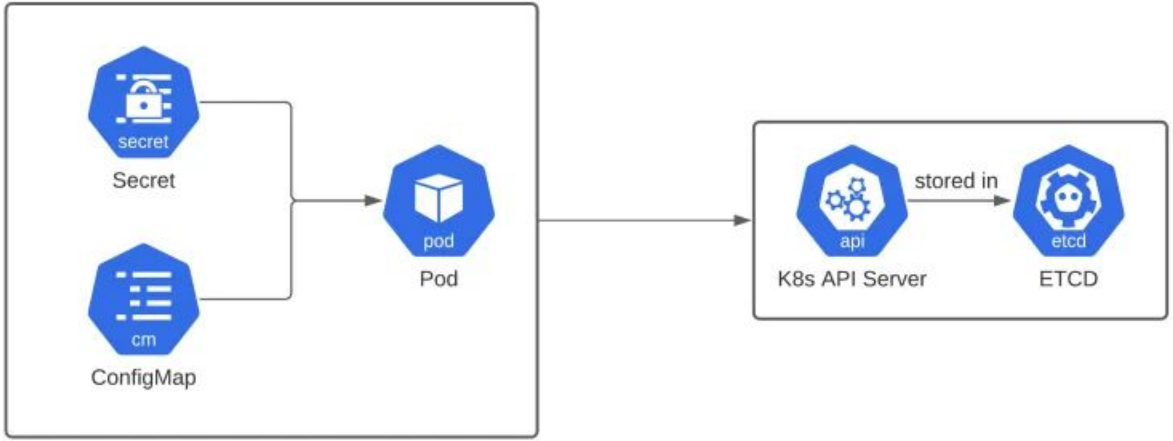
- Single entry-point
- Nginx-based reverse proxy
- Load balancing
- SSL/TLS-Termination



Source: https://matthewpalmer.net/

Kubernetes ConfigMap and Secret

- ConfigMap
  - External configuration data (e.g. URLs)
- Secret
  - Sensitive information (e.g. credentials)



Source: https://in4it.io/

Persistent Volume

- Independent lifecycle
- Node or network volumes
- Mounted on Pods
- Access modes

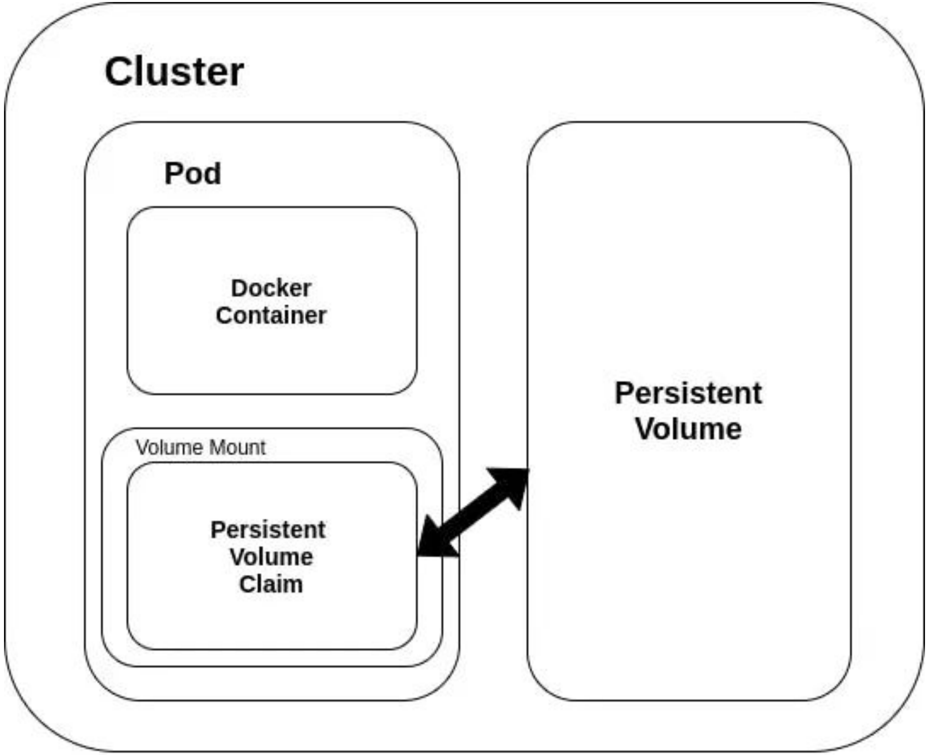
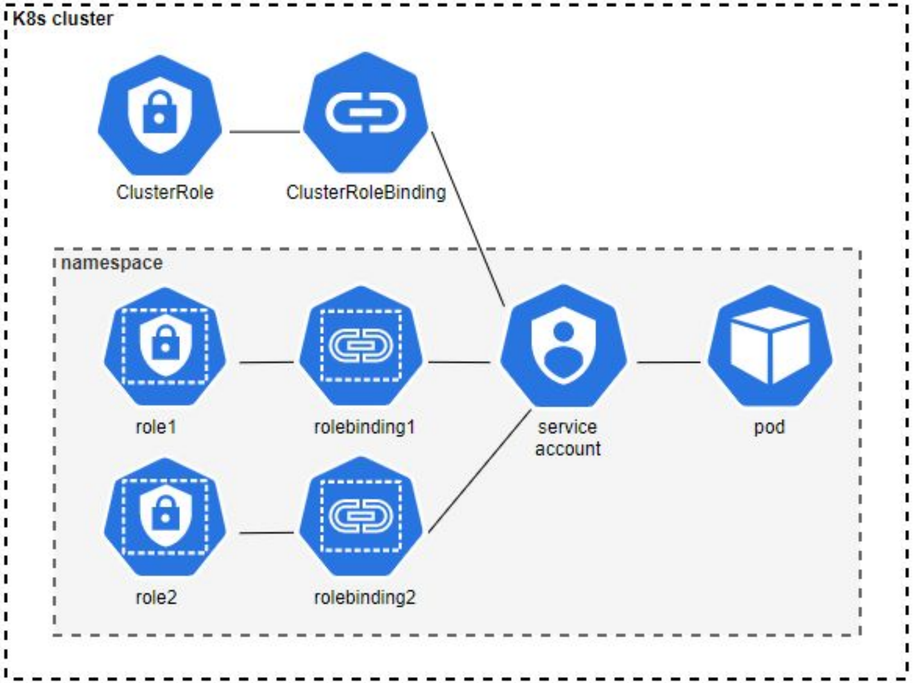


Figure 1-B

Source: https://www.kreyman.de/

Role Based Access Control (RBAC)

- Create a Service Account
- Define a Role with permissions
  - ClusterRole
  - Role
- Bind role(s) to the ServiceAccount
  - ClusterRoleBinding
  - RoleBinding



Source: https://engineering.dynatrace.com/

Optimize your Cluster

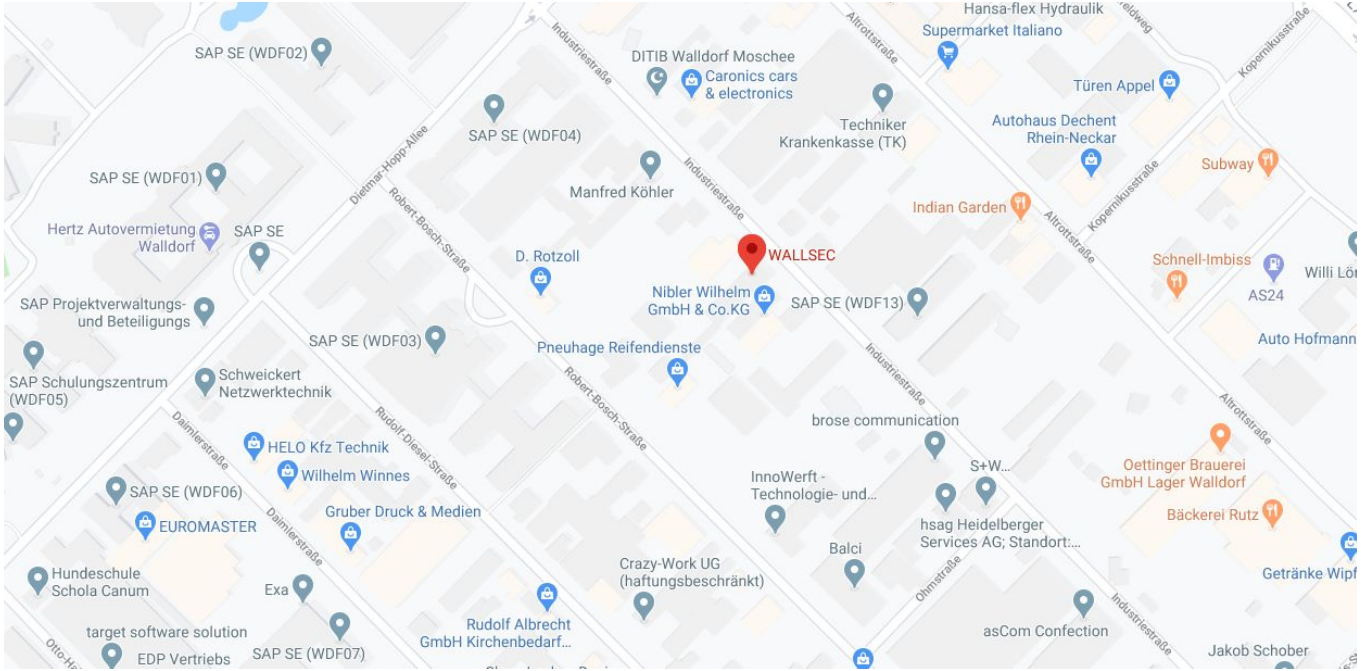
- Replace the Persistent Volume with a Projected Volume
- Define Network Policies and Pod Security Policies
- Service Accounts for each Service running in the Cluster

RUNNING KUBERNETES IN PRODUCTION THEY SAID
EVERGREEN
IT WILL BE EASY THEY SAID
imgflip.com

Source: https://dev.to/

Contact

WALLSEC GmbH
Industriestrasse 44
69190 - Walldorf
Germany
Tel: +49 6227 6550040
Fax: +49 6227 6550081
Email: contact@wallsec.de



WALLSEC GmbH. All Rights Reserved.

The materials provided here by WALLSEC GmbH is for informational purposes only and WALLSEC GmbH shall not be liable for errors with respect to those materials. The information in this document is not a commitment or a legal obligation to provide the service or deliver a product.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of WALLSEC GmbH. The information contained herein may be changed without prior notice.