
UPSALA
UNIVERSITET

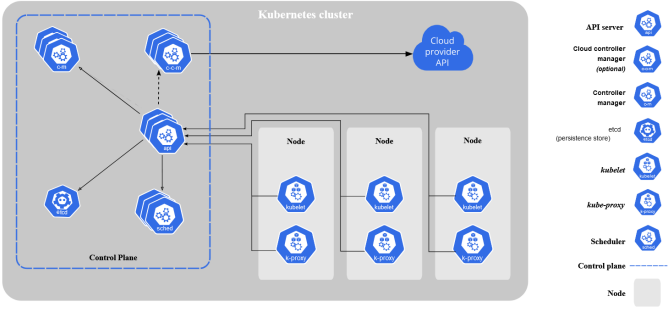
KUBERNETES SECURITY VULNERABITIES

A SUMMARY OF SECURITY EXPERIMENTS IN KUBERNETES

ALVARO REVUELTA

UPPSALA UNIVERSITET

K8S REFRESH



CLUSTER ARCHITECTURE

K8S REFRESH

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
spec:
  selector:
    matchLabels:
      app: nginx
  replicas: 2 # tells deployment to run 2 pods matching the template
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.14.2
        ports:
        - containerPort: 80
```

EXAMPLE OF A YAML FILE IN KUBERNETES

KUBERNETES PLAYGROUND

IF YOU DONT HAVE KUBERNETES INSTALLED, YOU CAN USE AN ONLINE PLAYGROUND

LINK TO KILLERCODA

WHY IS SECURITY IMPORTANT

- Kubernetes (K8s) was designed to be highly portable.
  1. Across clouds (Google, OpenStack, Amazon)
  2. The minimum requirements for a simple one node cluster are very low
- This means, by default, very few security mechanisms are implemented $\rightarrow$ it is the task for the administrator to do it
- Some security vulnerabities will be presented and how to mitigate them

EXPERIMENT 1: PODS AND CONTAINER PERMISSIONS

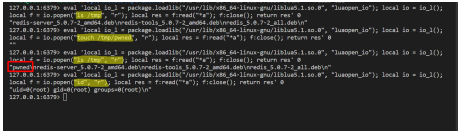
- By default, containers run as a root user.
- Malicious agents can exploit root access.
- Solution: Use security contexts to run as a non-privileged user and apply restrictions.

EXPERIMENT 1 - SOLUTION.

COMPUTER DEMO

EXPERIMENT 2: IMAGE VULNERABILITY

- Containers inherit libraries and binaries from base images.
- Image scanning can identify vulnerabilities.
- Example: Redis vulnerability CVE-2022-0543.

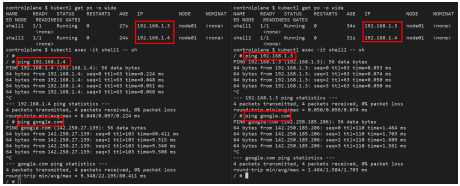


EXPERIMENT 2 - SOLUTION.

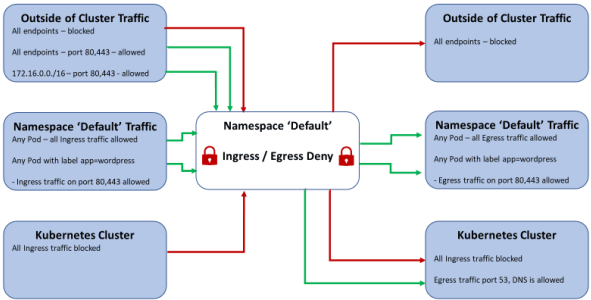
COMPUTER DEMO

EXPERIMENT 3: COMMUNICATION BETWEEN PODS

- By default, all resources can communicate with each other.
- Resource separation using namespaces and network policies.
- Limit traffic flow for better control.



EXPERIMENT 3



ANOTHER EXAMPLE OF NETWORK COMMUNICATION

UPPSALA UNIVERSITET

EXPERIMENT 3 - SOLUTION.

COMPUTER DEMO

EXPERIMENT 4: POD SERVICE ACCOUNT TOKENS

- Kubernetes automatically creates service accounts and tokens.
- Disable mounting tokens if not needed.
- Use Role-Based Access Control (RBAC) to restrict access.

```
[16]: ! mount | grep kubernetes
tmpfs on /run/secrets/kubernetes.io/serviceaccount type tmpfs (ro,relatime,size=12807532k)

[37]: ! cat /run/secrets/kubernetes.io/serviceaccount/token
```


eyJhbGciOiJSUzI1NiIsImtpZCI6IkhJRVBwZUpvQlVybWxQaXpXczc5QkpDOF9PZkVnUkRVT21iVmpZdGNfYlkifQ.eyJhdWQiOlsiaHR0cHM6Ly9r
dWJlcm5ldGVzLmRlZmF1bHQuc3ZjLmNsdXN0ZXIubG9jYWwiXSwiZXhwIjoxNzEzMDE5OTI3LCJpYXQiOjE2ODE0ODM5MjcsImlzcyI6Imh0dHBzOi8
va3ViZXJuZXRlcy5kZWZhdWx0LnN2Yy5jbHVzdGVyLmxvY2FsIiwia3ViZXJuZXRlcy5pbyI6eyJuYW1lc3BhY2UiOiJkZWZhdWx0IiwicG9kIjp7Im
5hbWUiOiJqdXAtNzhjNjg2NDk0ZC1mYmY0ciIsInVpZCI6IjJmMDkxMTdhLTQ2MWQtNDRmMy1hN2Q2LWRmZjhkYTk1ZmE4MCJ9LCJzZXJ2aWNlYWNjb
3VudCI6eyJuYW1lIjoiZGVmYXVsdCIsInVpZCI6IjM5MTMwNGE3LTk1MDYtNDQ0ZS05YzMwLWU2YzIzNjU0ODkyYiJ9LCJ3YXJuYWZ0ZXIiOjE2ODE0
ODc1MzR9LCJuYmYiOjE2ODE0ODM5MjcsInN1YiI6InN5c3RlbTpzZXJ2aWNlYWNjb3VudDpkZWZhdWx0OmRlZmF1bHQifQ.KePNd-EJBUHidDncHiJM
NQSIWHyS0qmZe-ttUCaGJv9_RhatoychnioZdFjWWd3FeRdKDAnnoF-jZ7Y7JY0_80GknFgnUeZ5omUCTFs-ryvJlXDY34pOj1lY5NJEM8hNS5tljt6
xyH5FHWjnWn9WXHDNTX9ADLf_FaOSHoDncVwxN7_tp-hocpoHmC_KlQm8Ojies_znYXYShKBUN73YGtyIDAXWWanE1_0zOdTJdtHKMiVmOMJ_v_3ivs
pcgF1v8AdVGrPp049BEIQS1sabR_GasKC3624Kwjmxug6h_UIgqA16ESIZwTXEyVf2tJbNgU8C2e4WbhbcPQnre4Dv-g


```
[38]: ! cat /run/secrets/kubernetes.io/serviceaccount/namespace
default
```

EXPERIMENT 4 - SOLUTION.

COMPUTER DEMO

EXPERIMENT 5: RESOURCE POLICIES

- Restrict resource usage with quotas and limits.
- Use LimitRange and ResourceQuotas for better control.
- Monitor and manage resource allocation.
- Several ways to implement

EXPERIMENT 5 - SOLUTION.

COMPUTER DEMO

TOOLS TO AUTOMATIZE FINDING THESE VULNERABITIES

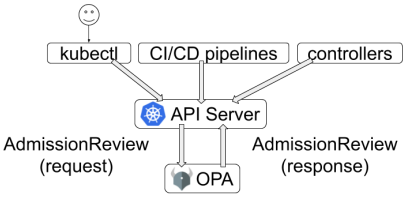
SYNTAX AND IMAGE SCANNERS

- Kube-linter → Checks the files tried to be deployed for misconfigurations.
- In experiment 2 we show how an image scanner works

UPPSALA UNIVERSITET

USE OPEN POLICIES

- Checks for these misconfigurations before deploying the files.



END

QUESTIONS

UPPSALA
UNIVERSITET