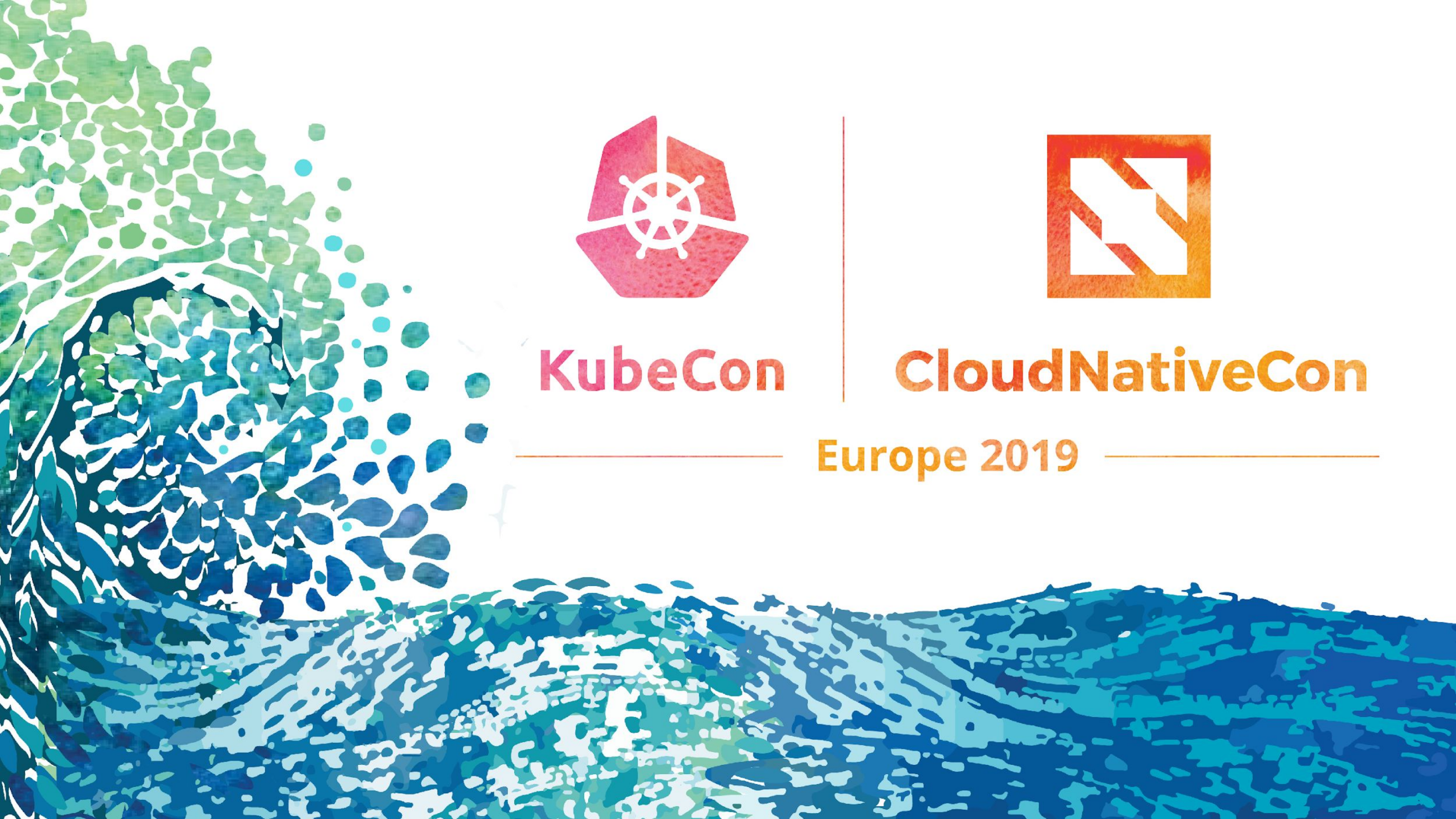


KubeCon | CloudNativeCon

Europe 2019

KubeCon | CloudNativeCon

Europe 2019

K8s Security and How to fix Clusters at Scale

Simon Pearce, SysEleven
Sebastian Scheele, Loodse

Why?

Service Provider

We Run Multiple Clusters

On OpenStack and AWS

Managed Clusters

24/7 Support

Service Level Agreement

K8s API Servers
Public

Motivation?

Managed Service

Security incidents

RunC
CVE-2019-5736

Attackers overwrite the RunC Binary and obtain host root access

Kubernetes CVE-2018-1002105

An API call to any aggregated API server endpoint can be escalated to perform any API request

The Challenge

Hundreds of Clusters

Multiple Clouds

Dealing with Security issues

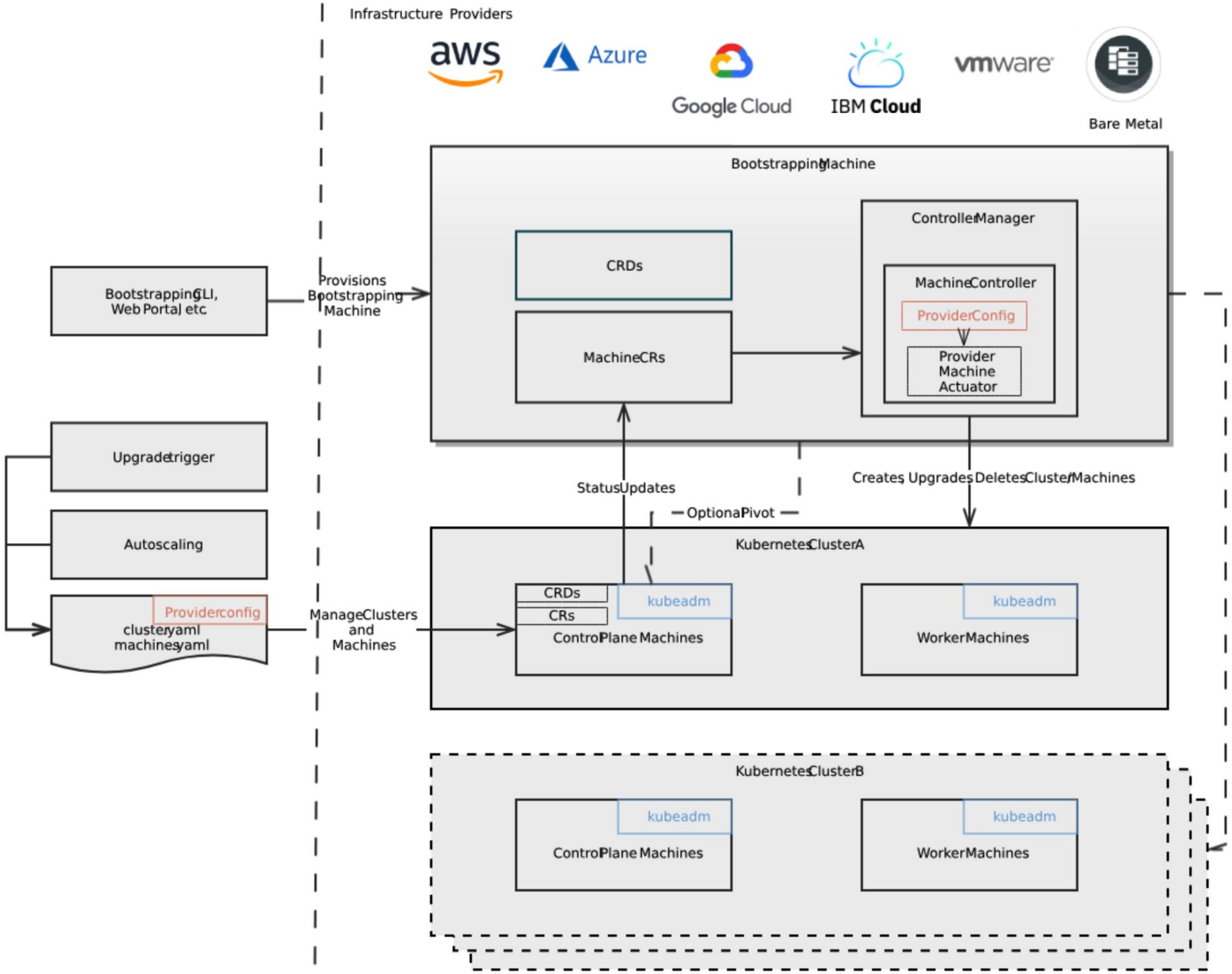
Upgrading Production Clusters

ASAP

How?

Build an Operator for Kubernetes

Use the Cluster API as building block


Infrastructure Providers
aws
Azure
Google Cloud
IBM Cloud
vmware
Bare Metal
Bootstrapping CLI, Web Portal, etc
Provisions Bootstrapping Machine
Bootstrapping Machine
CRDs
Machine CRs
Controller Manager
Machine Controller
ProviderConfig
Provider Machine Actuator
Upgrade trigger
Autoscaling
Providerconfig
cluster.yaml
machines.yaml
Manage Clusters and Machines
Status Updates
Optional Pivot
Creates, Upgrades, Deletes Cluster/Machines
Kubernetes Cluster A
CRDs
CRs
kubeadm
Control Plane Machines
kubeadm
Worker Machines
Kubernetes Cluster B
kubeadm
Control Plane Machines
kubeadm
Worker Machines

Cluster Creation

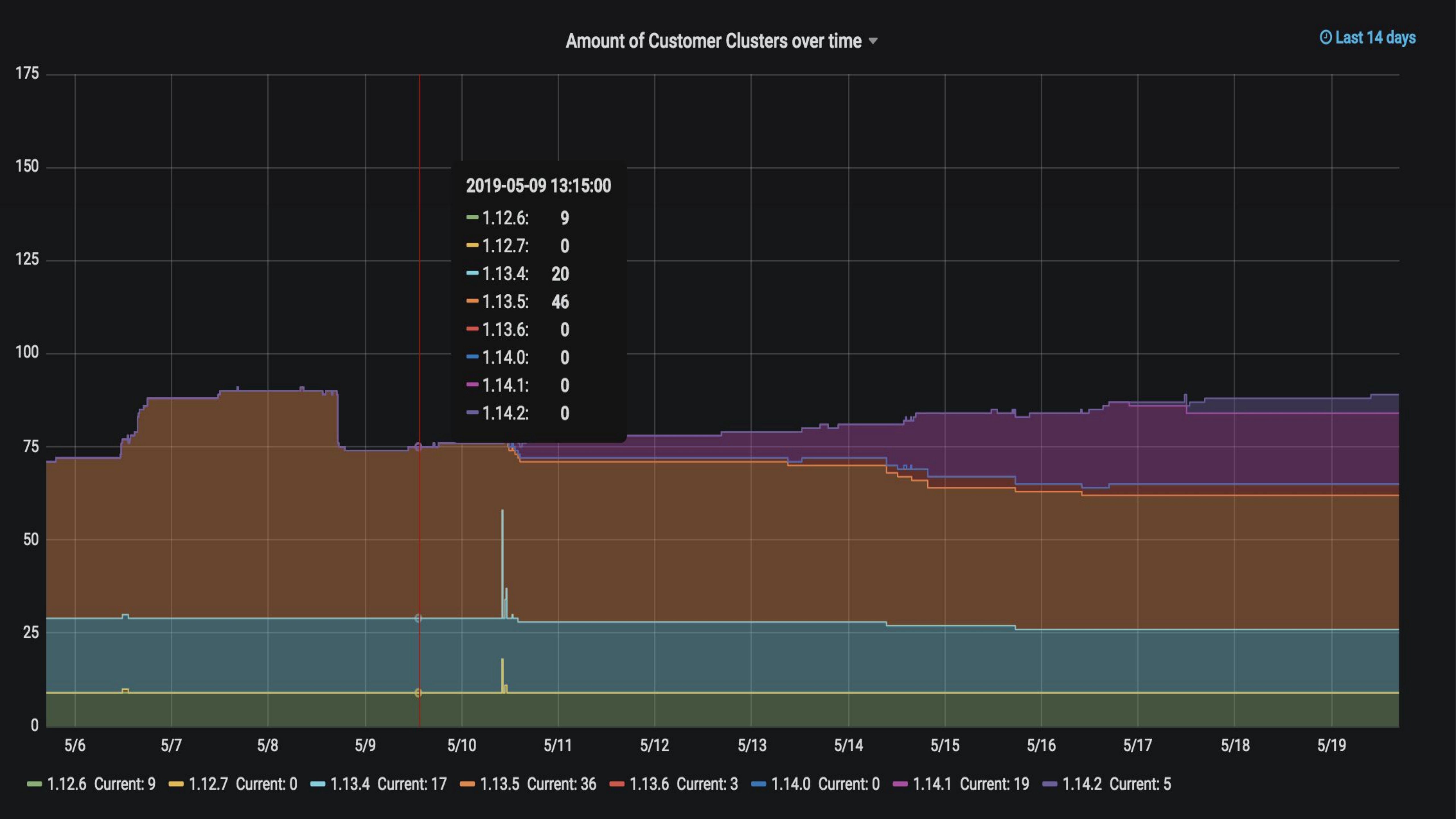
Cluster Configuration and Management

Machine Deployment Object

```
apiVersion: "cluster.k8s.io/v1alpha1"
kind: MachineDeployment
metadata:
  name: aws-machinedeployment
spec:
  paused: false
  replicas: 1
  strategy:
    type: RollingUpdate
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
  template:
    spec:
      providerSpec:
        value:
          cloudProvider: "aws"
       versions:
        kubelet: 1.13.1
```

Run Kubernetes in Kubernetes

Monitoring


Amount of Customer Clusters over time
Last 14 days
175
150
125
100
75
50
25
0
5/6
5/7
5/8
5/9
5/10
5/11
5/12
5/13
5/14
5/15
5/16
5/17
5/18
5/19
2019-05-09 13:15:00
1.12.6: 9
1.12.7: 0
1.13.4: 20
1.13.5: 46
1.13.6: 0
1.14.0: 0
1.14.1: 0
1.14.2: 0
1.12.6 Current: 9
1.12.7 Current: 0
1.13.4 Current: 17
1.13.5 Current: 36
1.13.6 Current: 3
1.14.0 Current: 0
1.14.1 Current: 19
1.14.2 Current: 5

Patch Cluster Object

Upgrade Process

What is effected?

How severe is the impact?

Change Advisory Board

Inform affected Customers

Patch all affected Clusters

Roll out new base image

Upgrade Machine Deployments

Rolling Upgrade

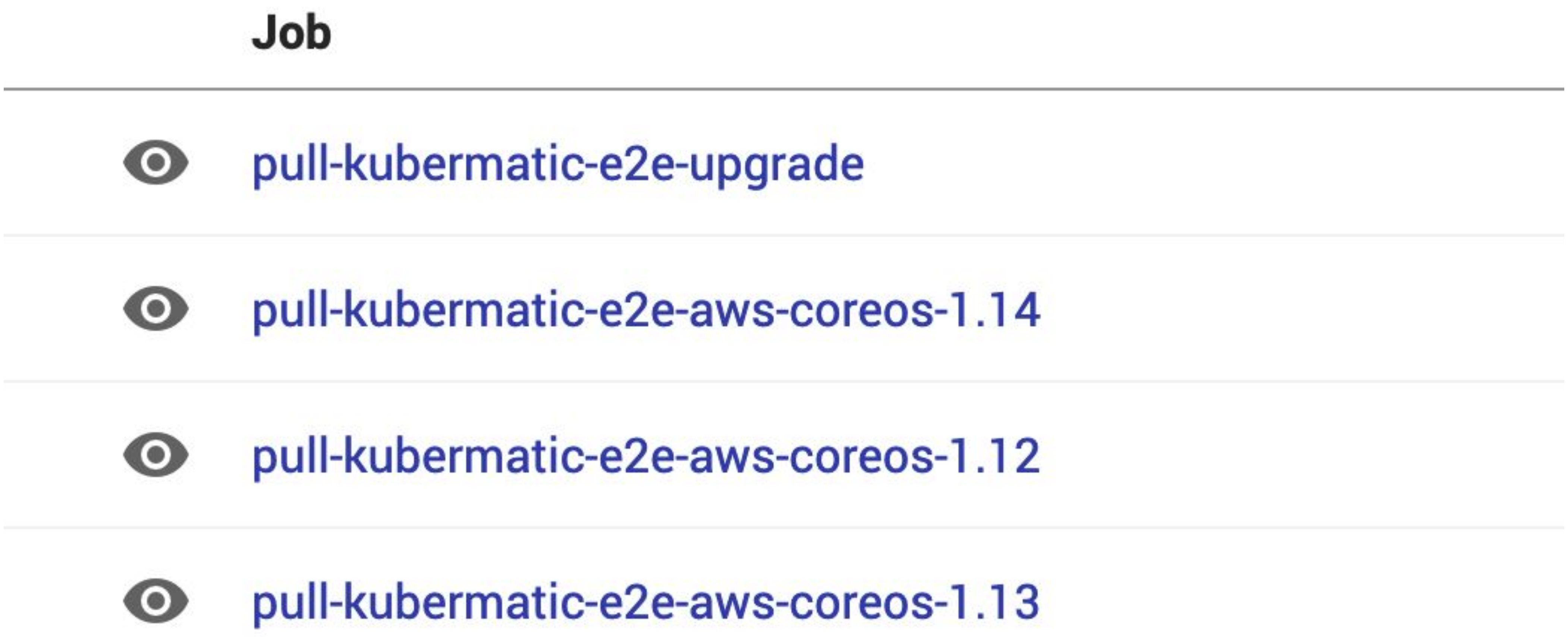
Upgrade Docker Daemon

Upgrade Kubelet

Best Practices

Automate all Upgrade Processes

E2E Tests on all Supported Clouds



Job
pull-kubermatic-e2e-upgrade
pull-kubermatic-e2e-aws-coreos-1.14
pull-kubermatic-e2e-aws-coreos-1.12
pull-kubermatic-e2e-aws-coreos-1.13

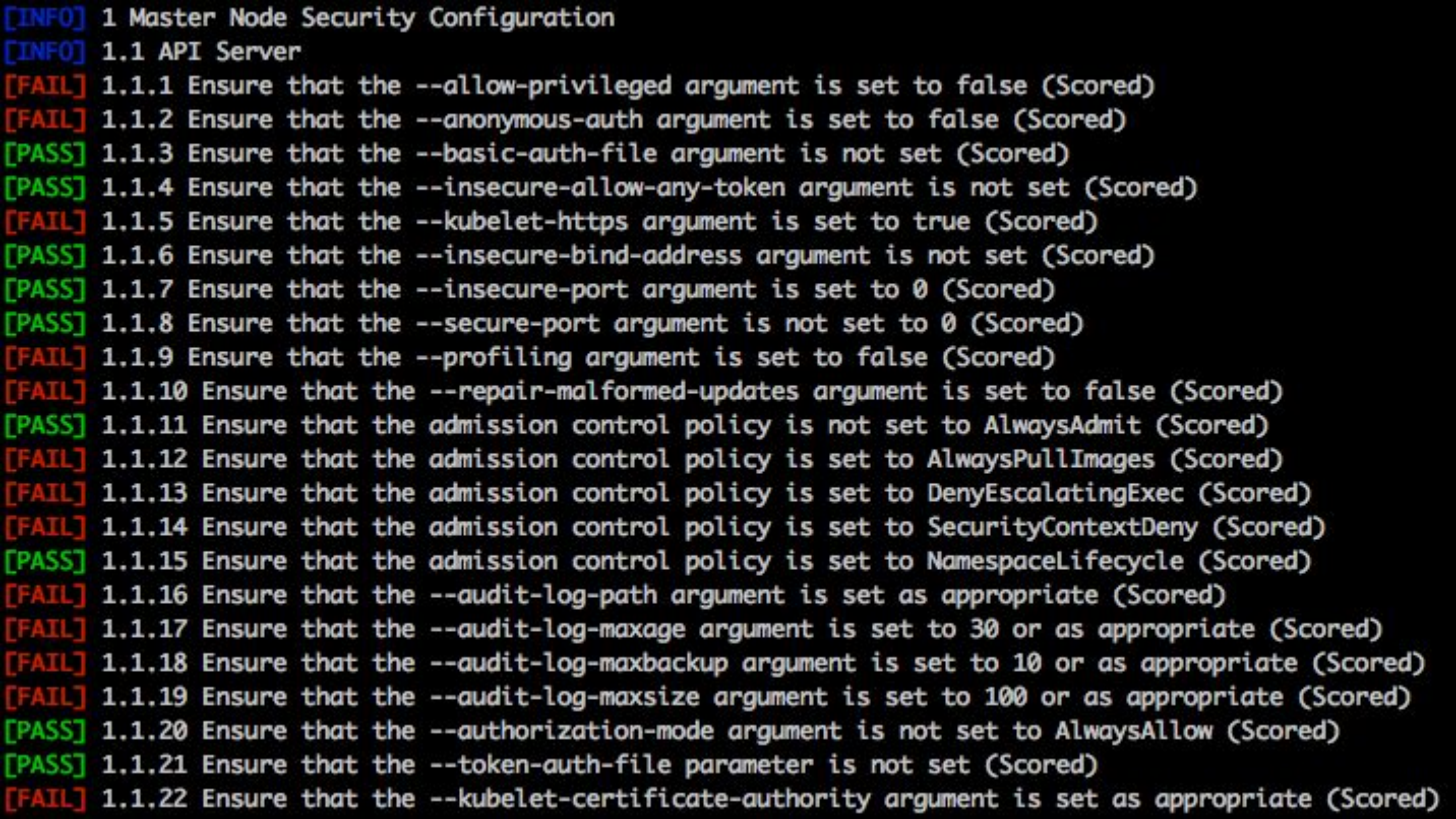
k8s Conformance Tests

Pod Security Policies

runAsUser

K8s Admission Controllers

Check CIS Benchmark



```
[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)
```

Kubernetes Security Announcements

https://kubernetes.io/docs/reference/issues-security/security/

Questions?

Thank you for listening