Kubernetes Deep Dive

Nigel Poulton

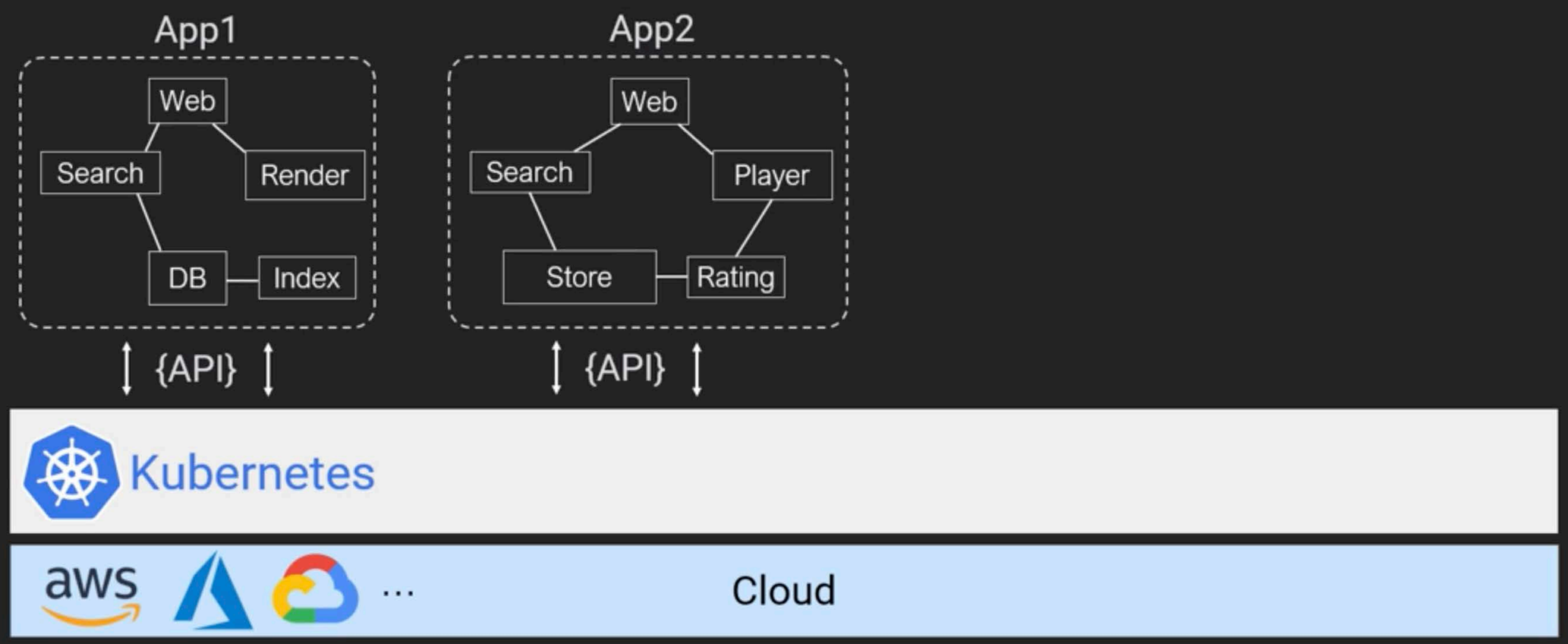
A CLOUD GURU

Why Kubernetes

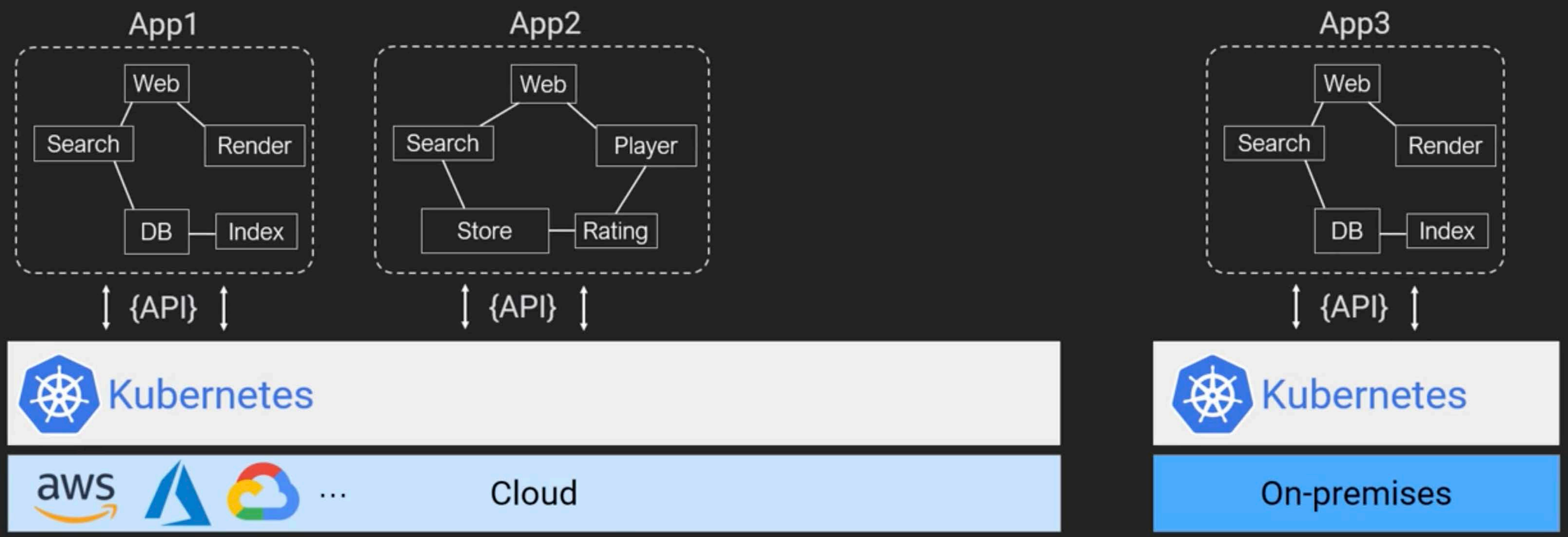
kubernetes

Becoming the de facto cloud-native standard...

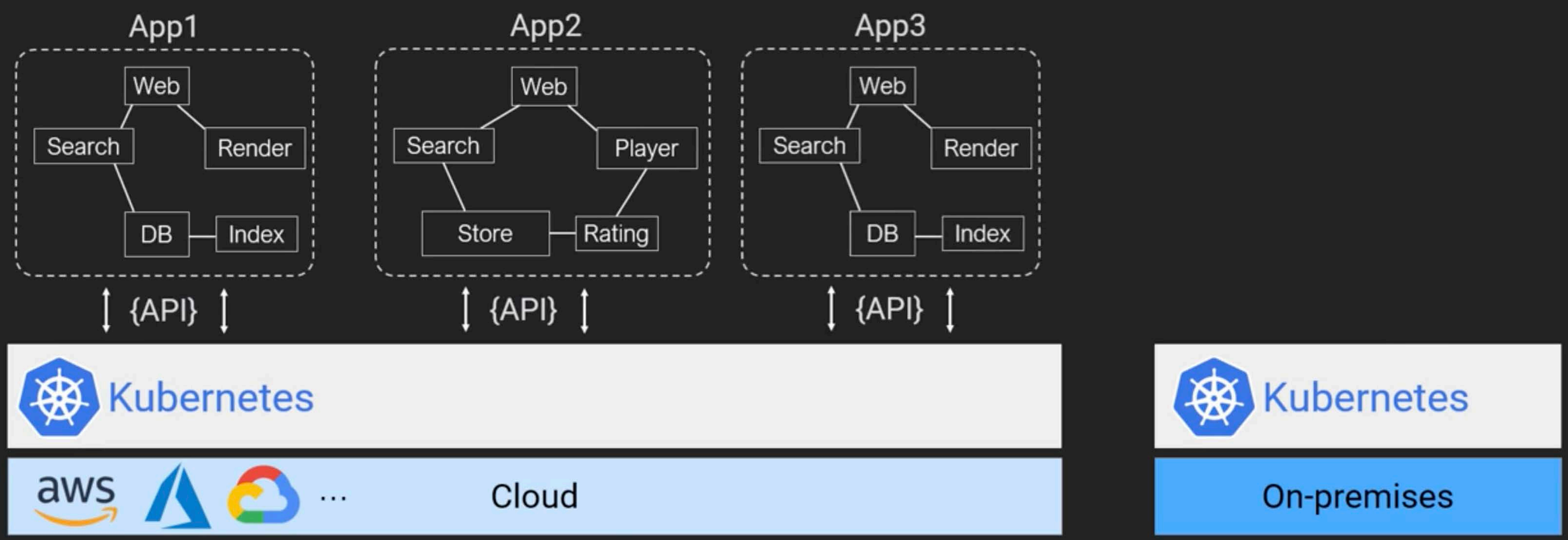
Why Kubernetes



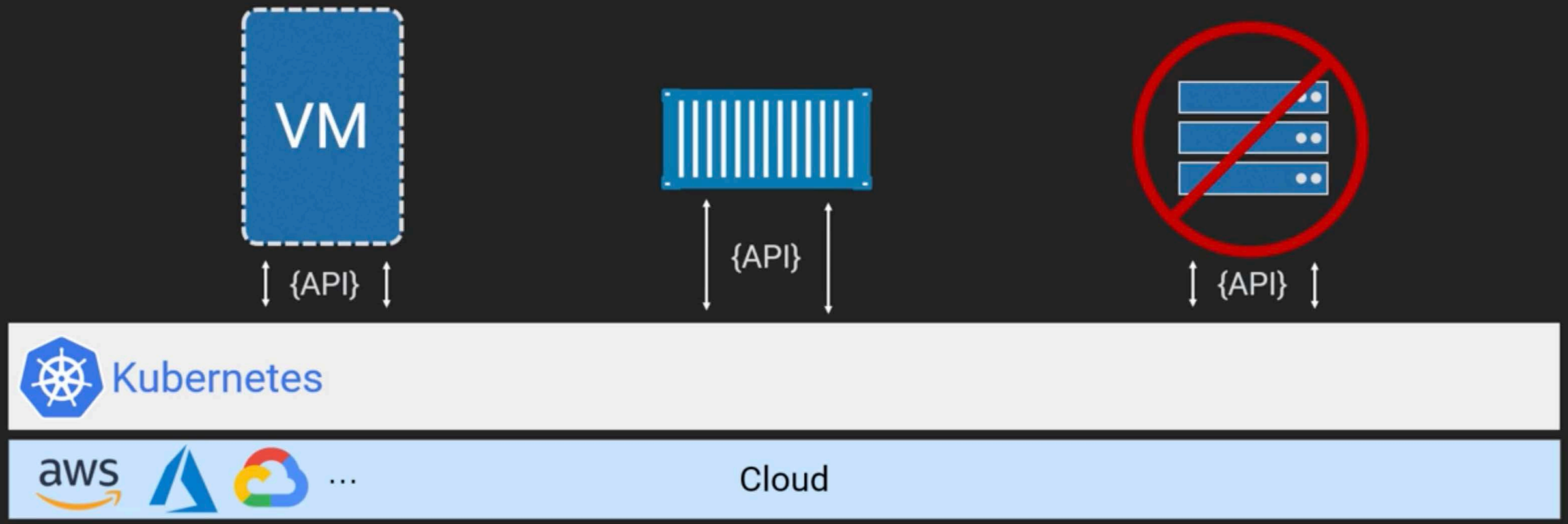
Why Kubernetes



Why Kubernetes

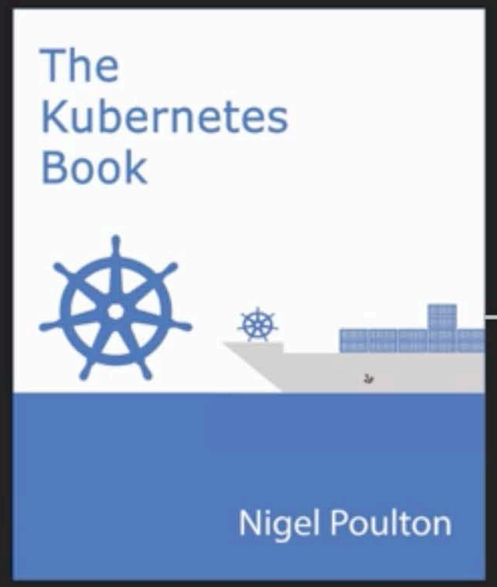


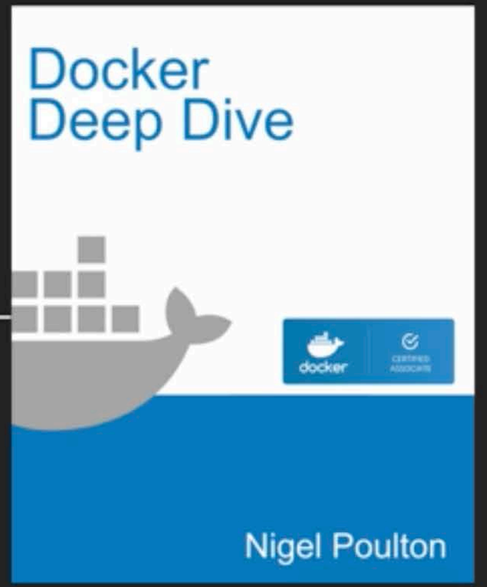
Why Kubernetes



About Me

A CLOUD GURU

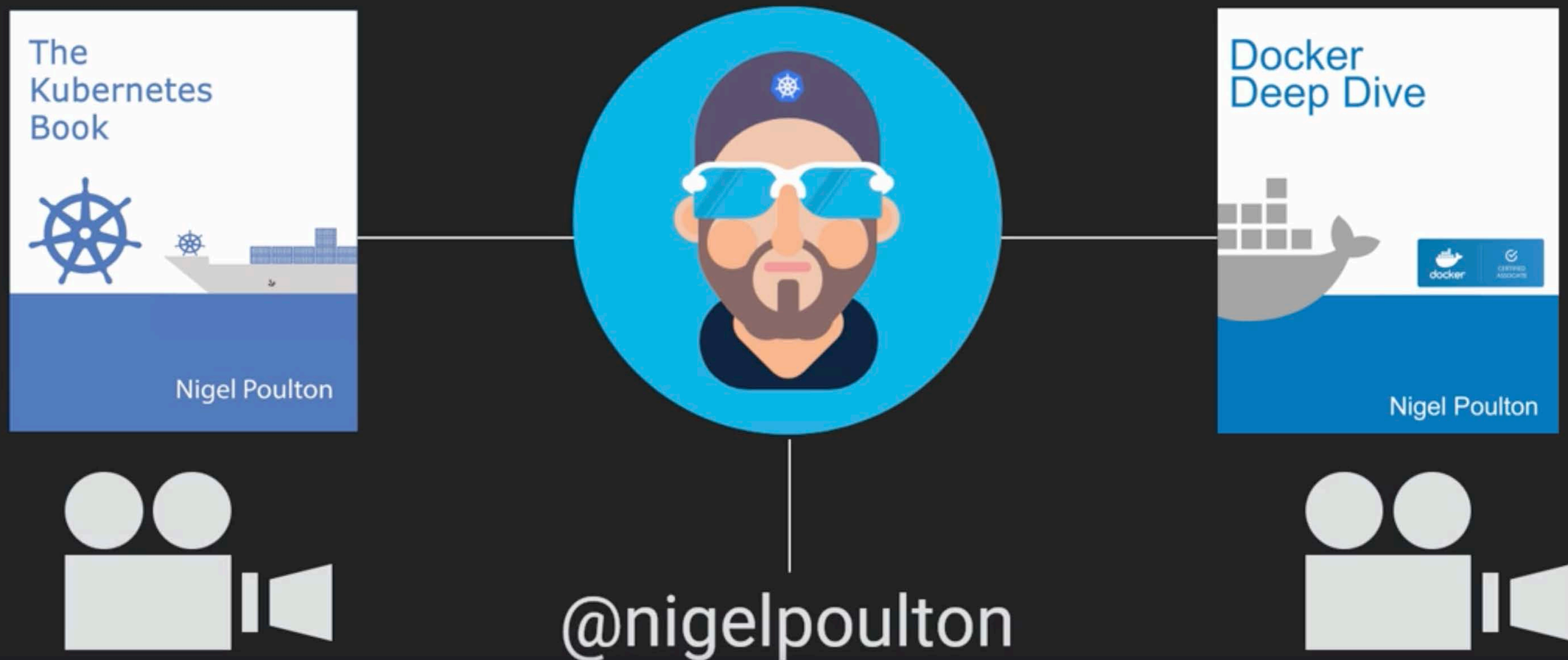




Kubernetes Deep Dive

About Me

A CLOUD GURU



15 15 04:22 / 06:45

A CLOUD GURU

How Deep?

Individual parts ✗

K8s platform ✓

K8s is shorthand for **Kubernetes**.
The **8** represents the 8 letters between the **K** and the **s.**

Developing FAST!

Schedule

A CLOUD GURU

Lesson Plan

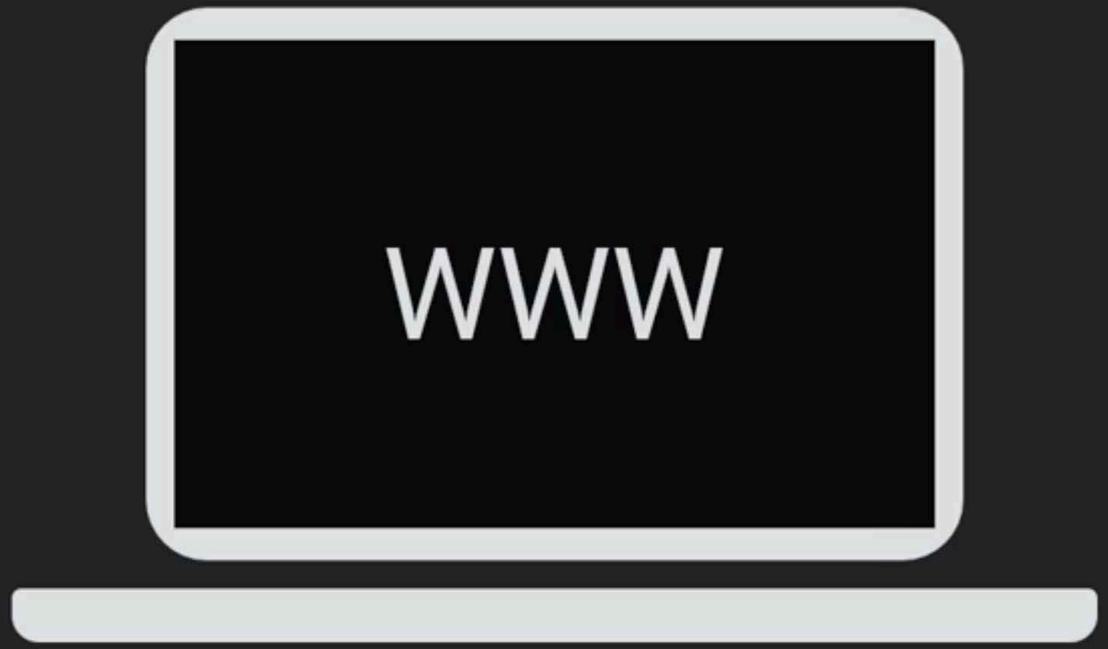
- Kubernetes Big Picture
- Kubernetes App Architecture
- Kubernetes Networking
- Kubernetes Storage
- From Code to Kubernetes
- Kubernetes Deployments
- Scaling Kubernetes Apps
- RBAC and Admission Control
- Other Kubernetes Stuff
- What Next

*<u>**SORRY**</u> about the bullet-points!! 🙄

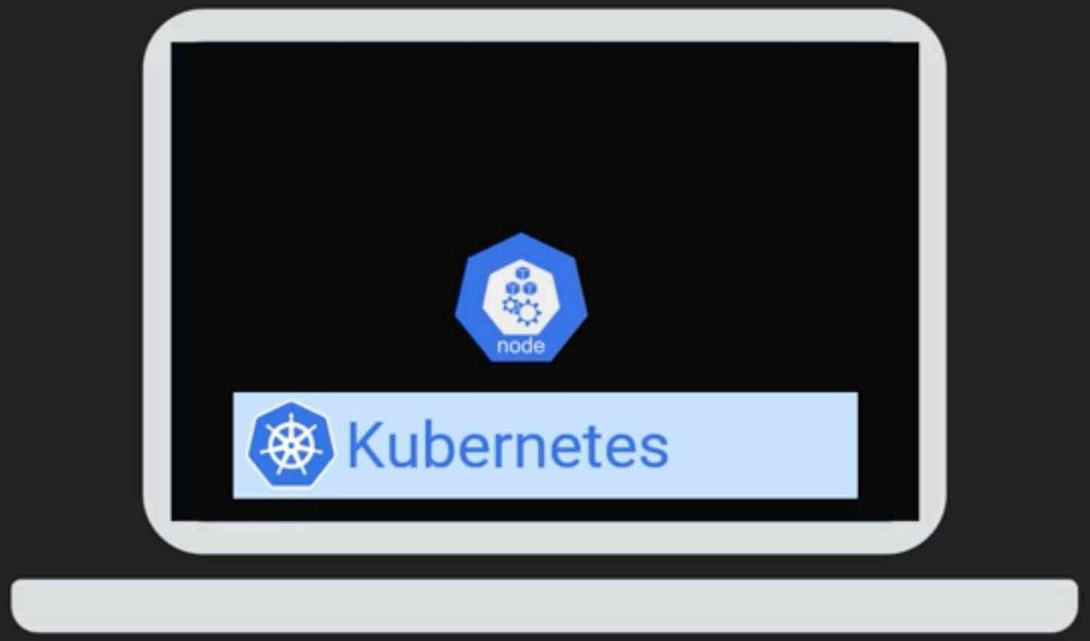
Course Prereqs

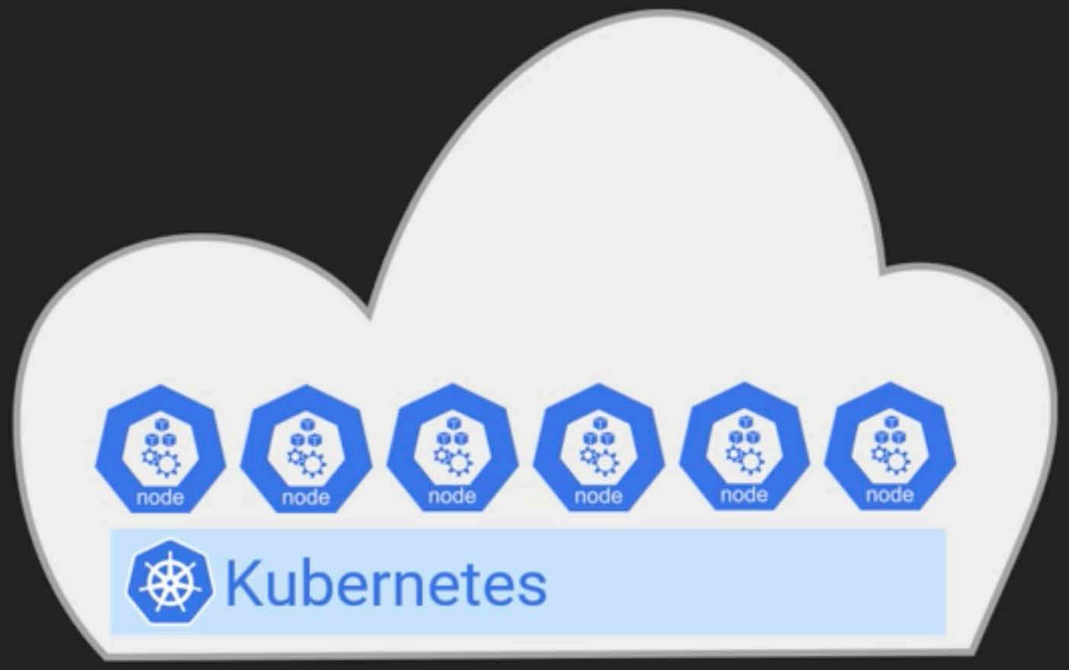
A CLOUD GURU

The Course



The Course



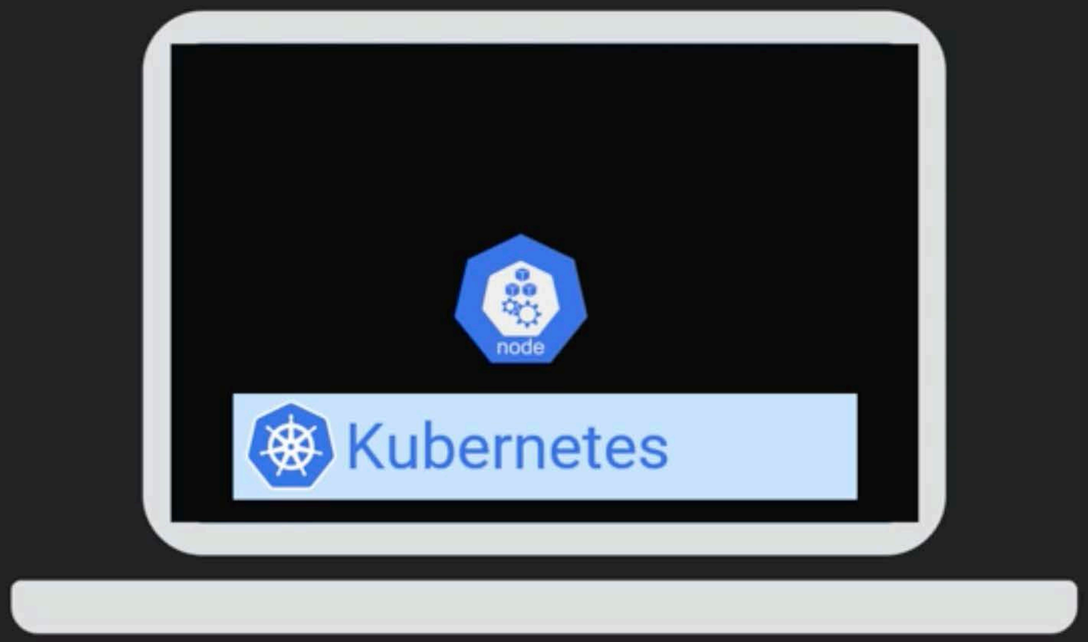


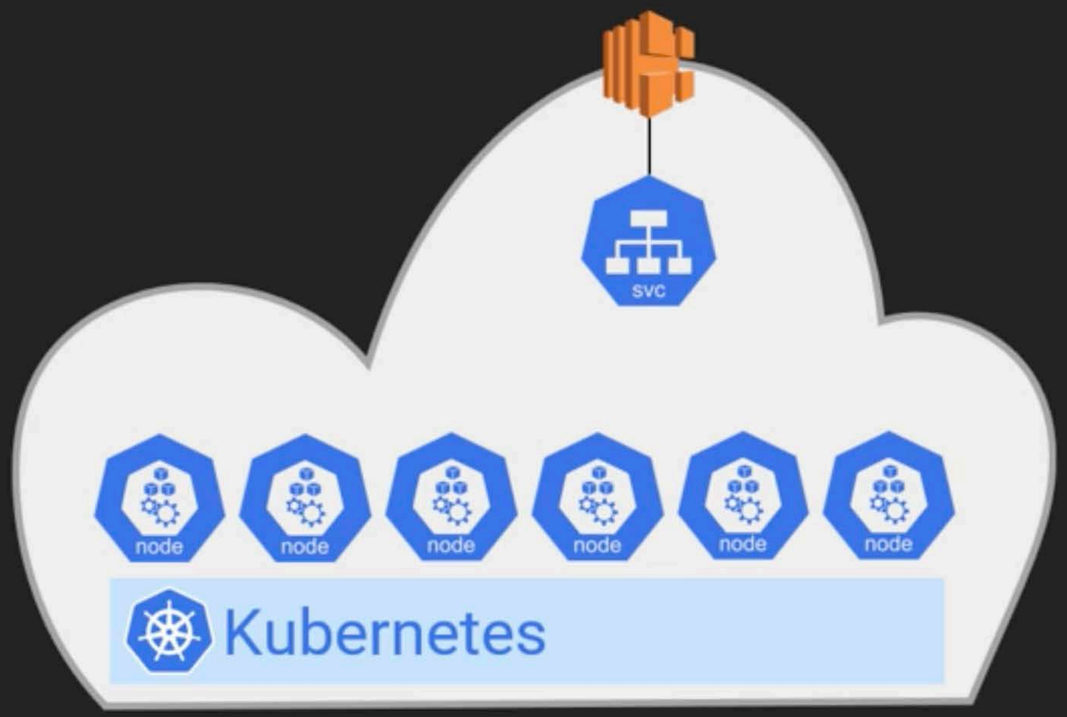
Kubernetes icons from: https://github.com/octo-technology/kubernetes-icons

Kubernetes Deep Dive

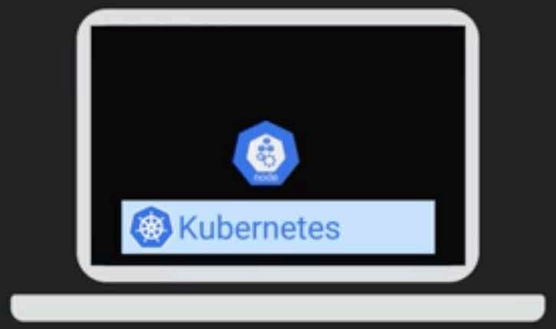
The Course

A CLOUD GURU

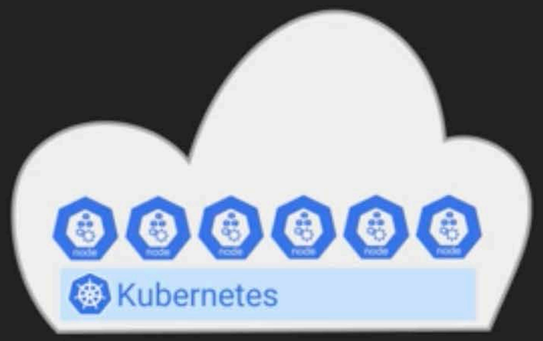




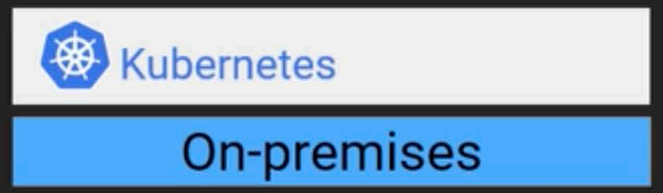
Installations...



- Minikube
- Docker for Desktop



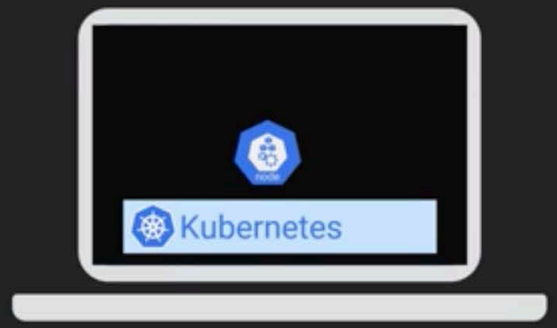
- AKS (hosted)
- EKS (hosted)
- GKE (hosted)
- Kops



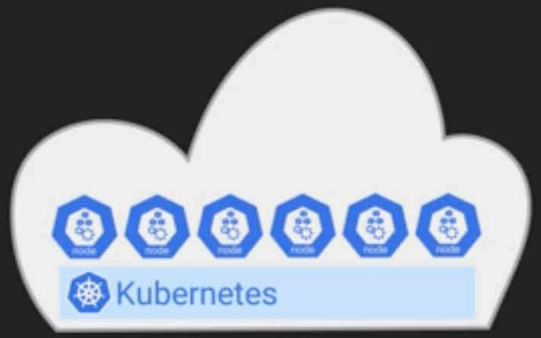
Cloud options may incur costs!

Installations...

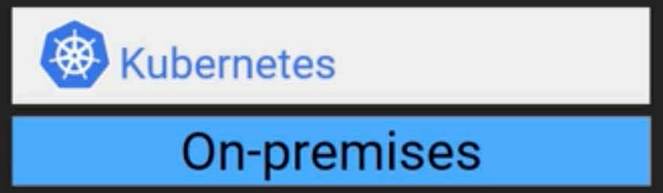
A CLOUD GURU



- Minikube
- Docker for Desktop



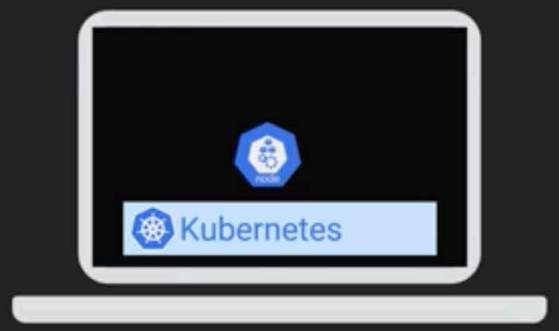
- AKS (hosted)
- EKS (hosted)
- GKE (hosted)
- Kops



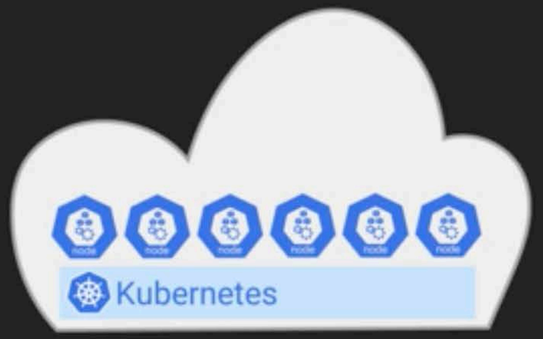
- Kubeadm

* Play with Kubernetes (PWK)
http://play-with-k8s.com

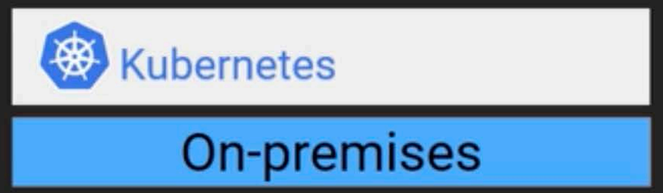
Installations...



- Minikube
- Docker for Desktop



- AKS (hosted)
- EKS (hosted)
- GKE (hosted)
- Kops



- Kubeadm

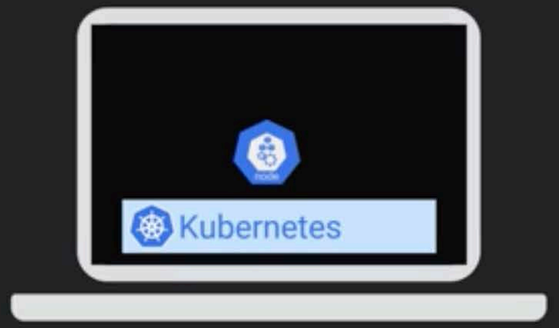
Ease/speed of installation

- Fairly easy
- Really easy
- Really really easy

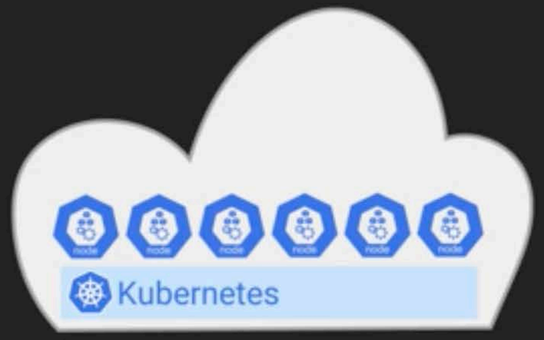
* Play with Kubernetes (PWK)
http://play-with-k8s.com

Installations...

A CLOUD GURU



- Minikube
- Docker for Desktop

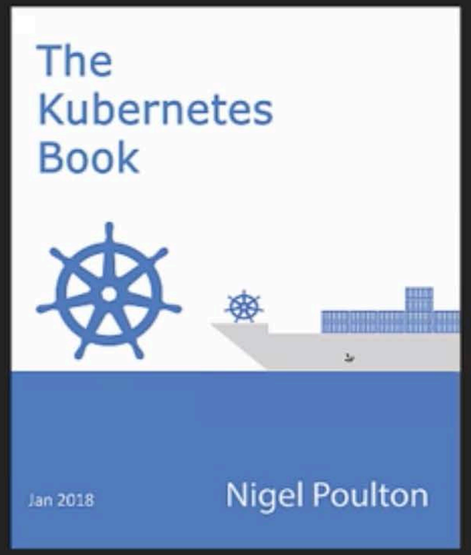


- AKS (hosted)
- EKS (hosted)
- GKE (hosted)
- Kops

Kubernetes

On-premises

- Kubeadm



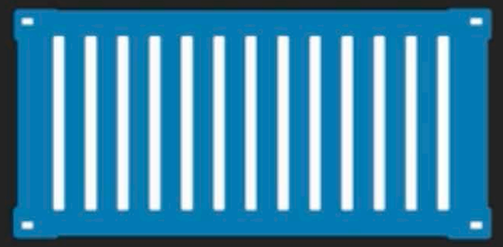
Ease/speed of installation

- Fairly easy
- Really easy
- Really really easy

* Play with Kubernetes (PWK)
http://play-with-k8s.com

Prereqs

Understanding of the **cloud** and **containers** is beneficial



Kubernetes Big Picture

A CLOUD GURU

Lesson Plan

A CLOUD GURU

- Kubernetes Primer
- Kubernetes API
- Kubernetes Objects
- Getting a Quick Kubernetes Cluster

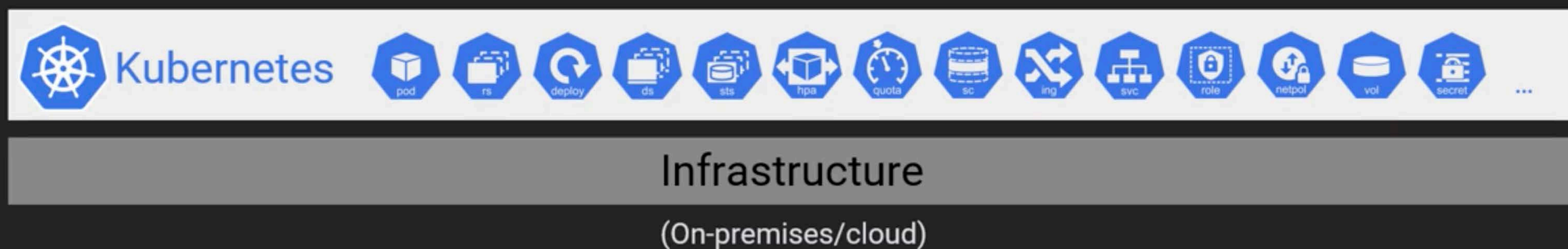
15 15 01:00 / 01:03

Kubernetes Primer

A CLOUD GURU

Big Picture

A CLOUD GURU

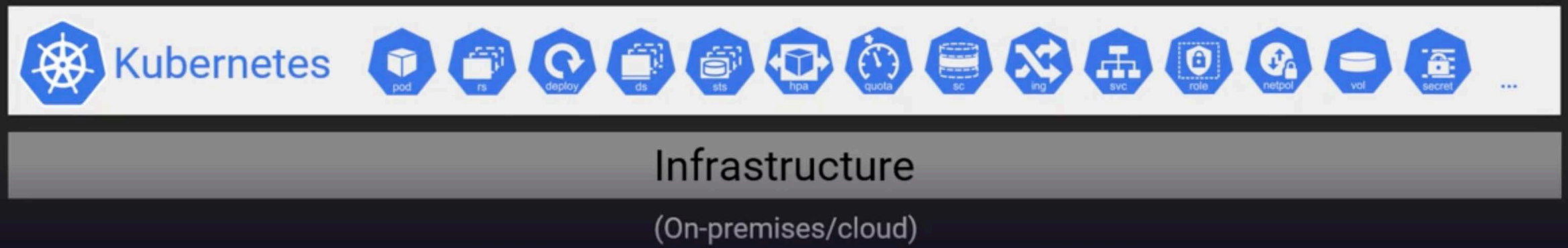


15 15 00:38 / 05:14

Big Picture

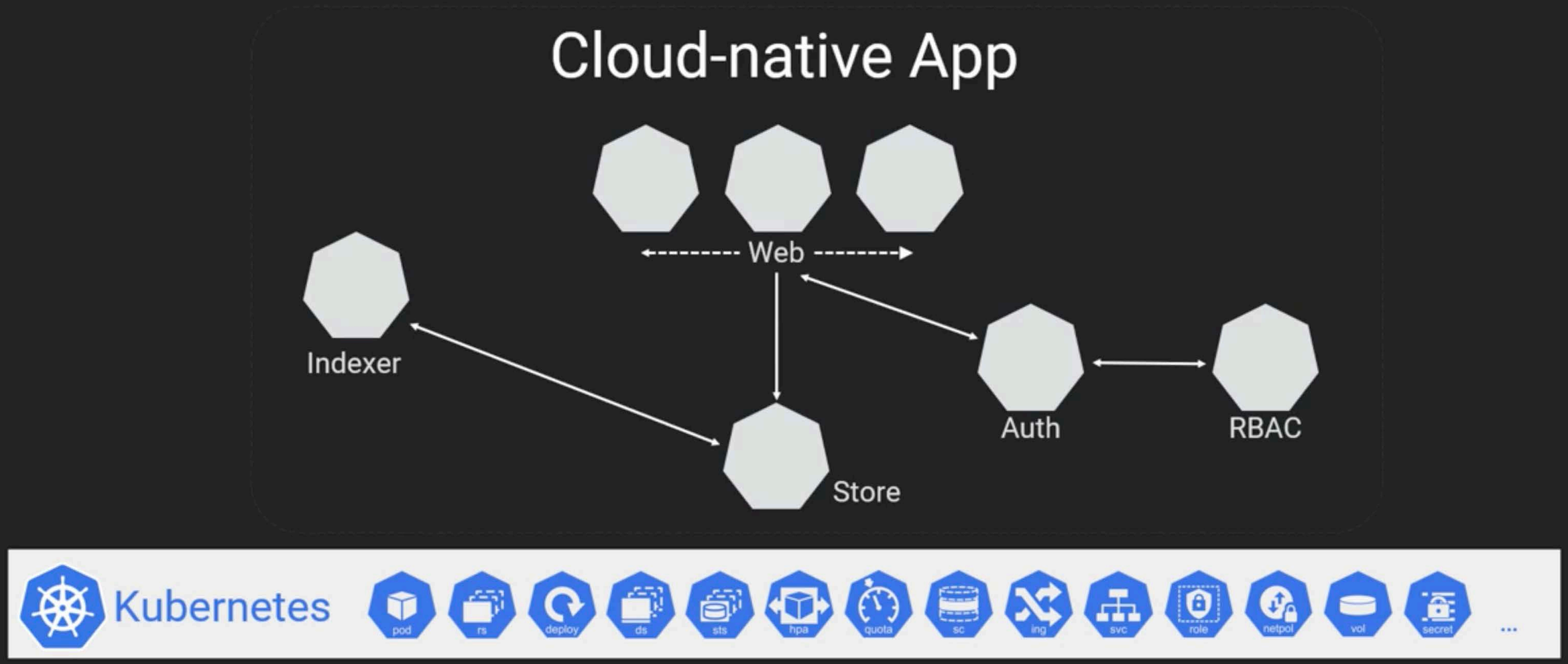
A CLOUD GURU

Cloud-native App



15 15 00:44 / 05:14

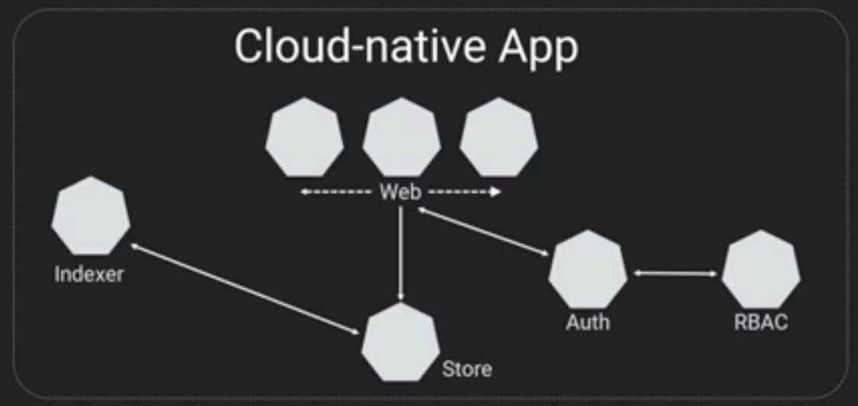
Big Picture

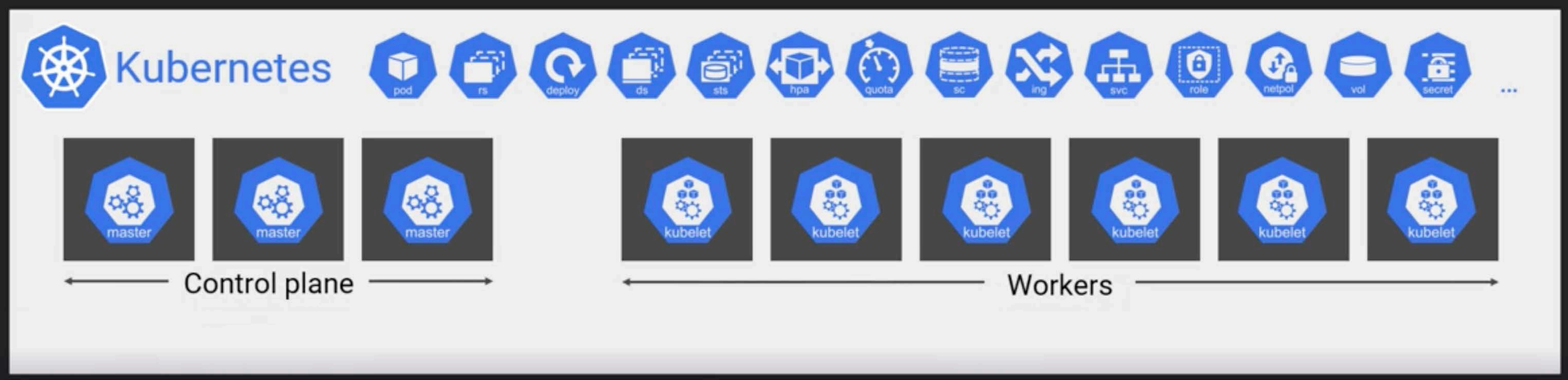


15 15 00:54 / 05:14

Big Picture

A CLOUD GURU



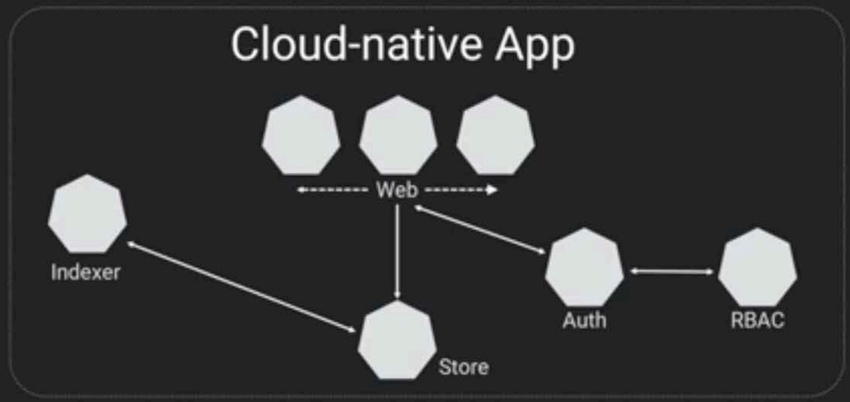


Infrastructure (On-premises/cloud)

15 15 01:51 / 05:14

Big Picture

A CLOUD GURU



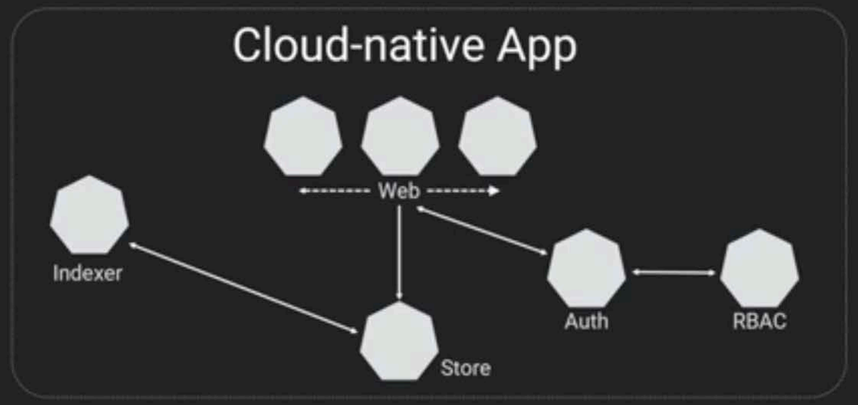
Infrastructure (On-premises/cloud)

15 15 02:08 / 05:14

Big Picture

A CLOUD GURU

Stateful

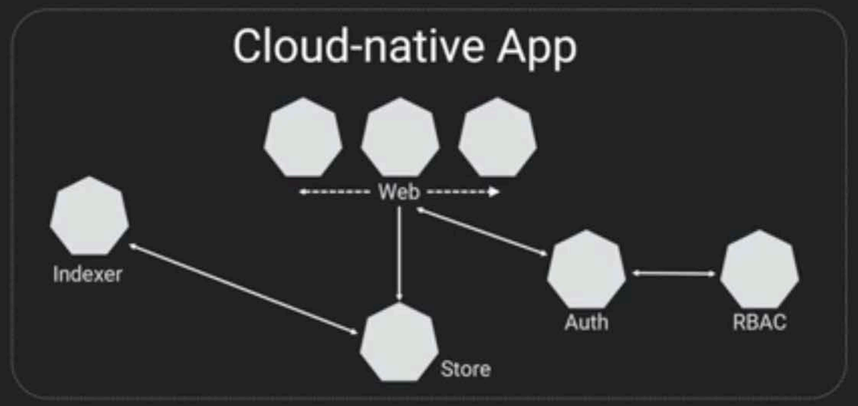


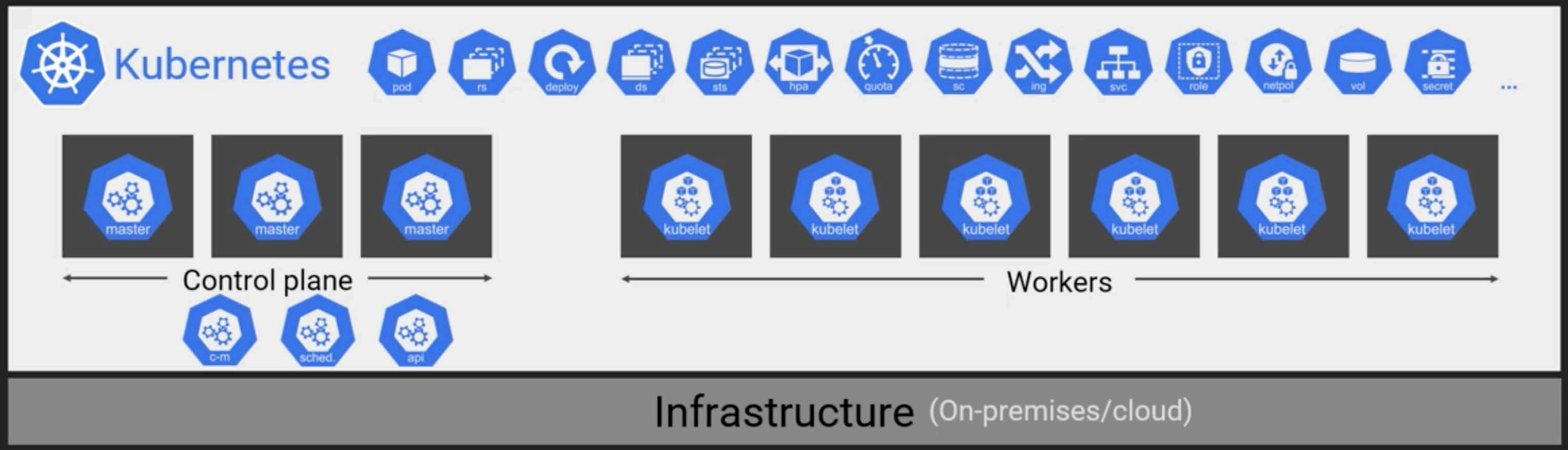
Infrastructure (On-premises/cloud)

15 15 02:39 / 05:14

Big Picture

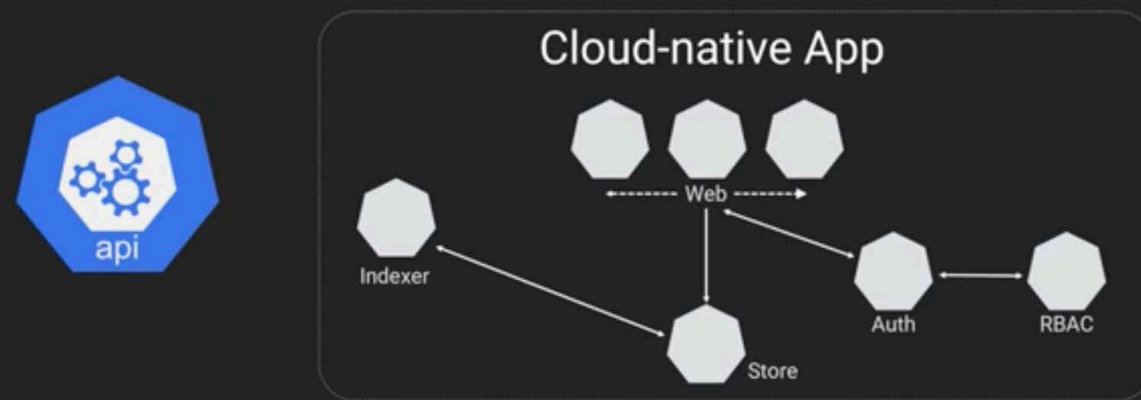
etcd
Stateful
Beware at scale

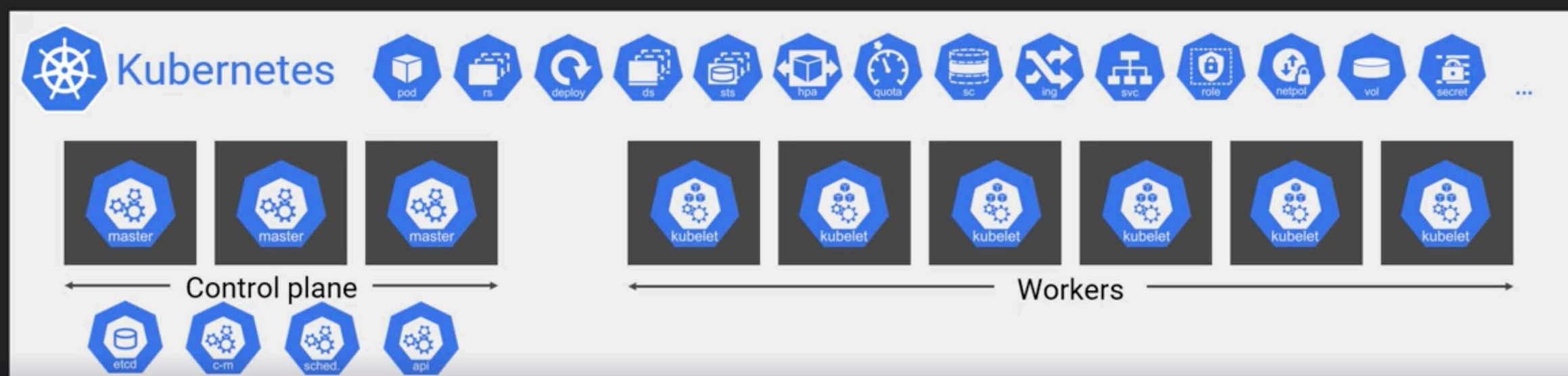

Cloud-native App
Web
Indexer
Auth
RBAC
Store


Kubernetes
pod
rs
deploy
ds
sts
hpa
quota
sc
ing
svc
role
netpol
vol
secret
...
master
master
master
kubelet
kubelet
kubelet
kubelet
kubelet
kubelet
Control plane
Workers
c-m
sched.
api
Infrastructure (On-premises/cloud)

Big Picture

A CLOUD GURU



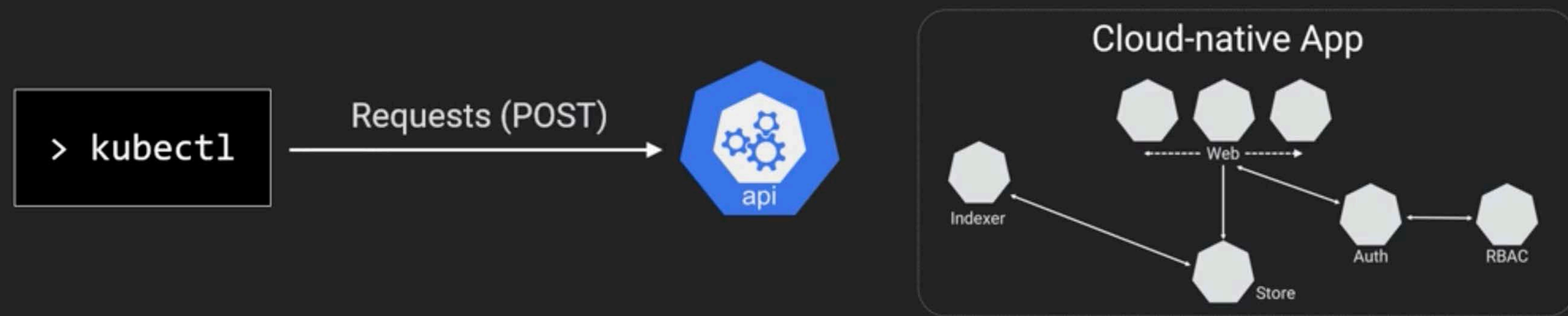


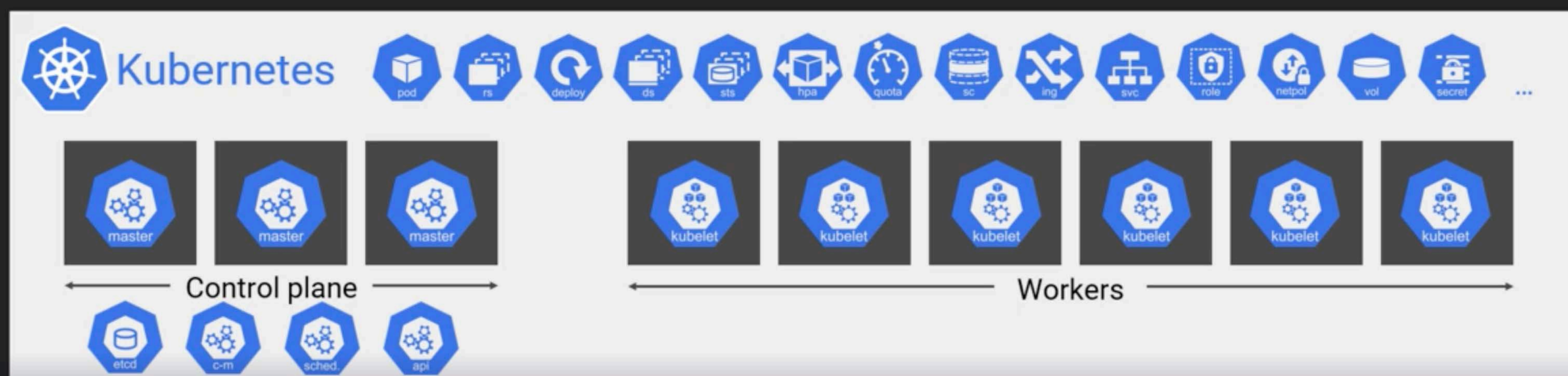
Infrastructure (On-premises/cloud)

15 15 03:42 / 05:14

Big Picture

A CLOUD GURU



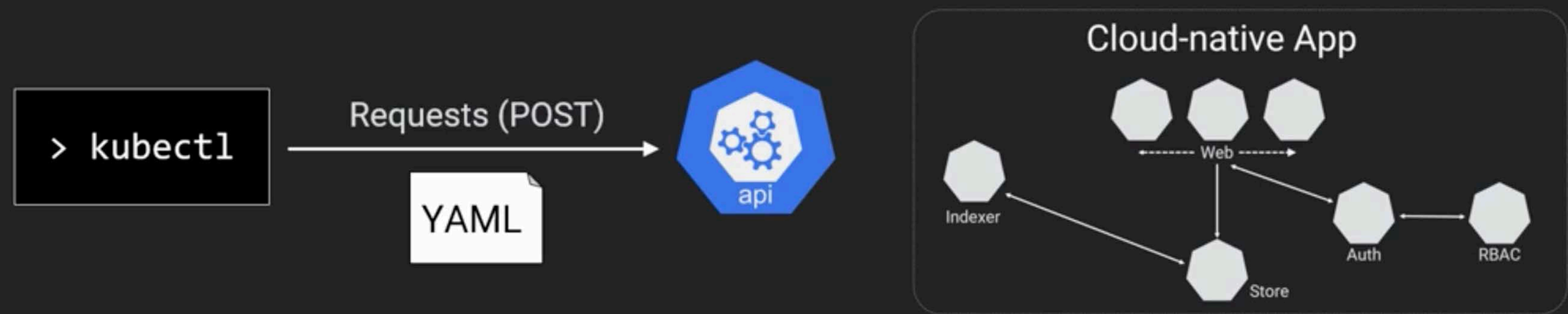


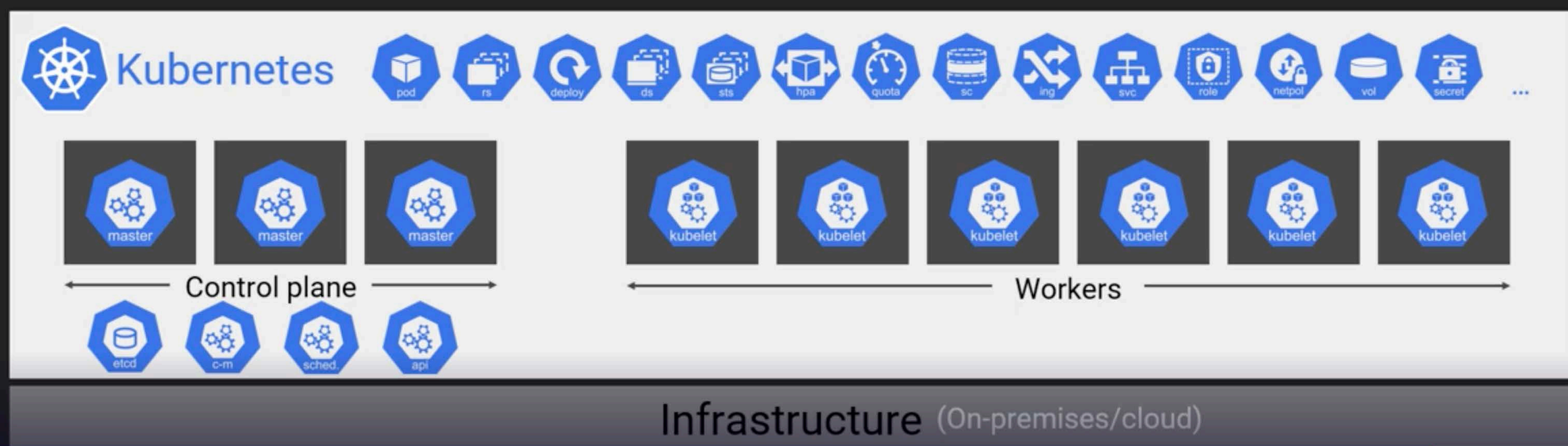
Infrastructure (On-premises/cloud)

15 15 04:05 / 05:14

Big Picture

A CLOUD GURU





15 15 04:36 / 05:14

The Kubernetes API

A CLOUD GURU

The Kubernetes API

A CLOUD GURU

The Kubernetes API

A CLOUD GURU

REST

CRUD

- Create
- Read
- Update
- Delete

GET POST PATCH UPDATE PUT DELETE

15 15 01:09 / 06:41

The Kubernetes API

A CLOUD GURU

```
> kubectl
```

POST

A CLOUD GURU

Declarative Configuration

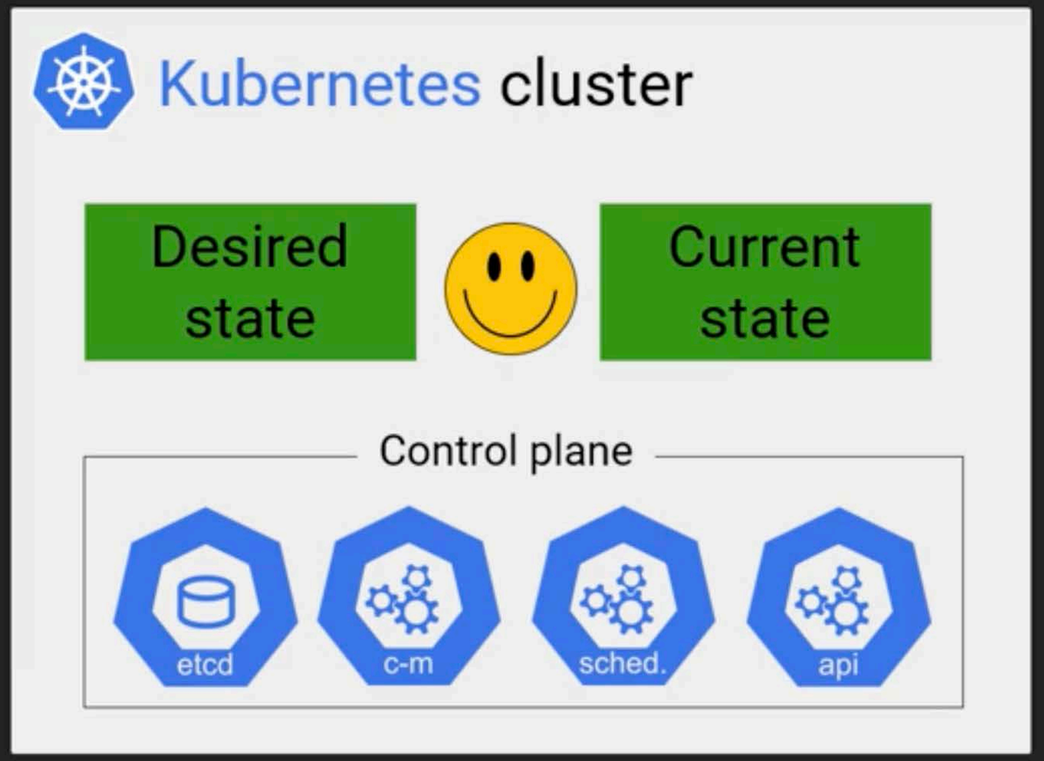
The Kubernetes API

A CLOUD GURU

```
> kubecti
```

YAML

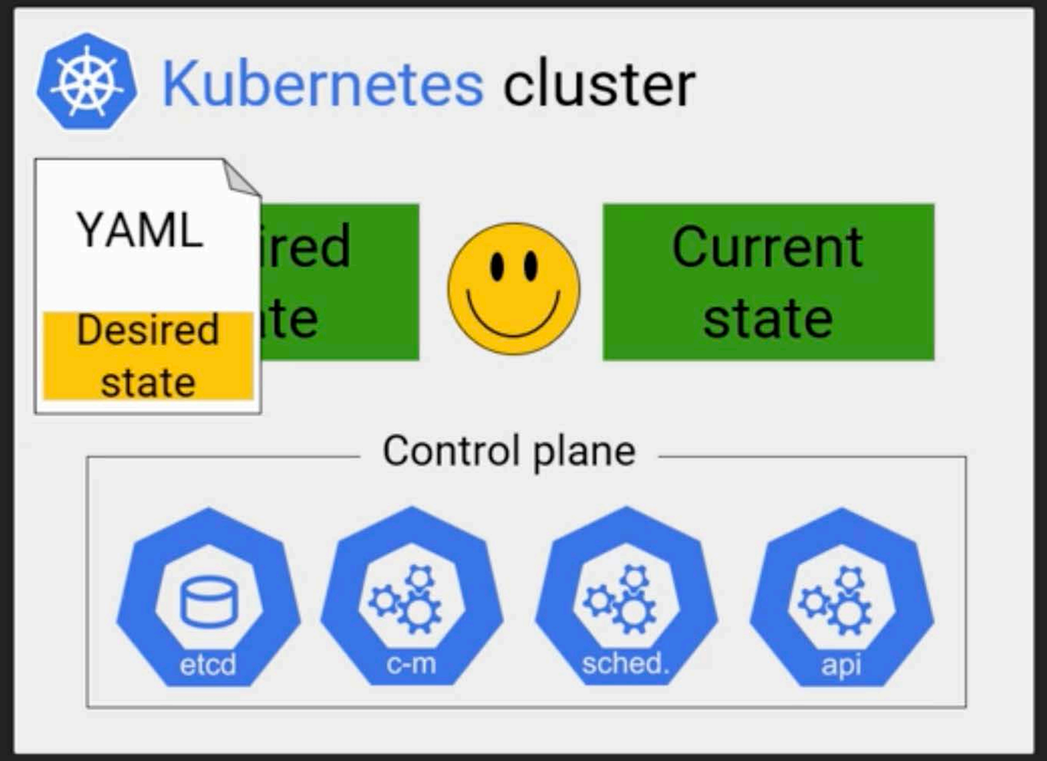
Desired state



The Kubernetes API

A CLOUD GURU

```
> kubectl
```

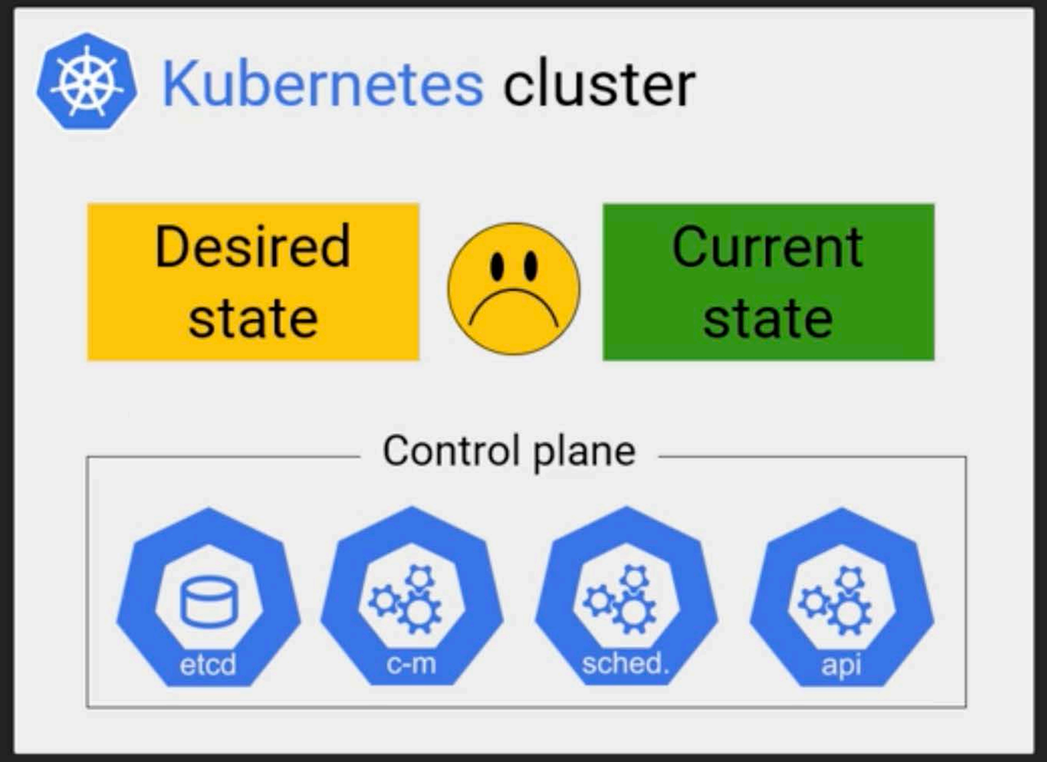


15 15 02:14 / 06:41

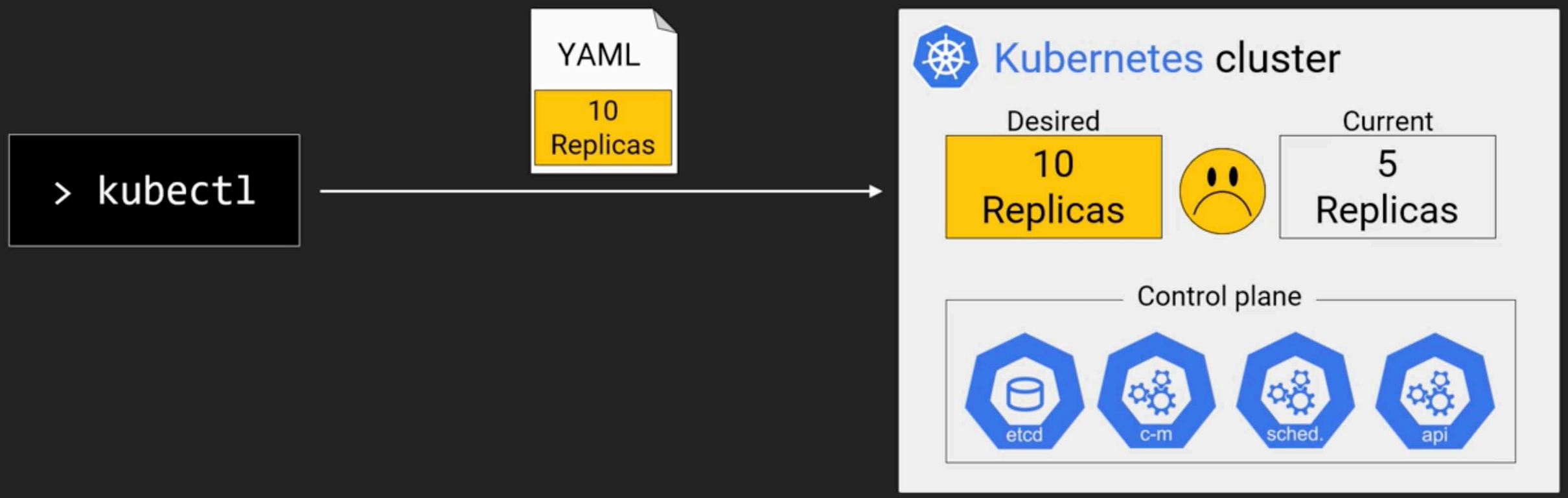
The Kubernetes API

A CLOUD GURU

```
> kubectl
```



The Kubernetes API



The Kubernetes API

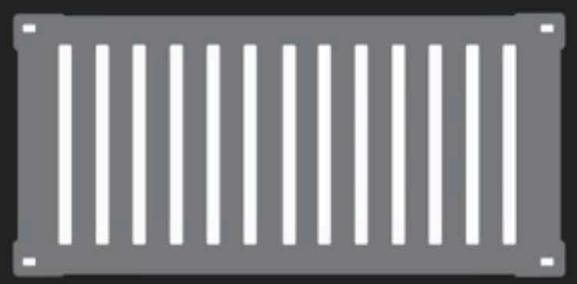
The **core API group** is often referred to with empty quotes - ""

Kubernetes Objects

A CLOUD GURU

Kubernetes Objects

A CLOUD GURU



15 15 00:24 / 02:45

Kubernetes Objects

A CLOUD GURU

Contains one or more containers

Atomic unit of scheduling

Object on the cluster

Defined in the **v1** API group

15 15 00:58 / 02:45

Kubernetes Objects

A CLOUD GURU

Object on the cluster

Defined in the **apps/v1** API group

Scaling

Rolling updates

15 15 01:26 / 02:45

Kubernetes Objects

A CLOUD GURU

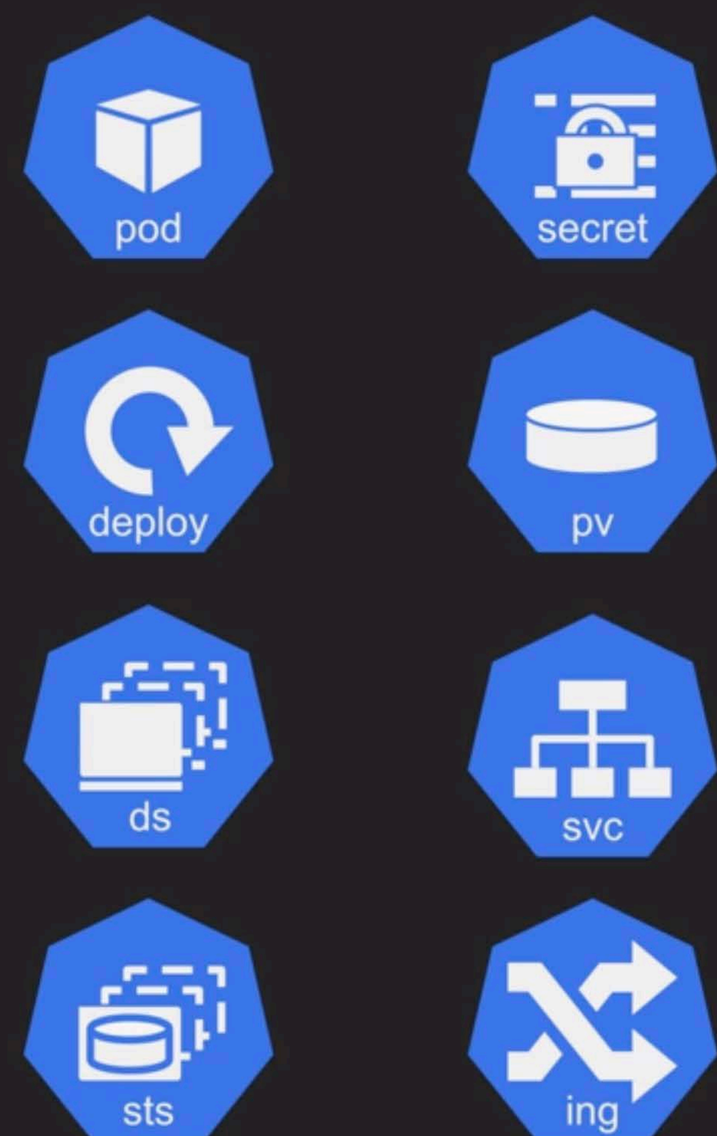
Wrap one or more containers

Scalability and application releases

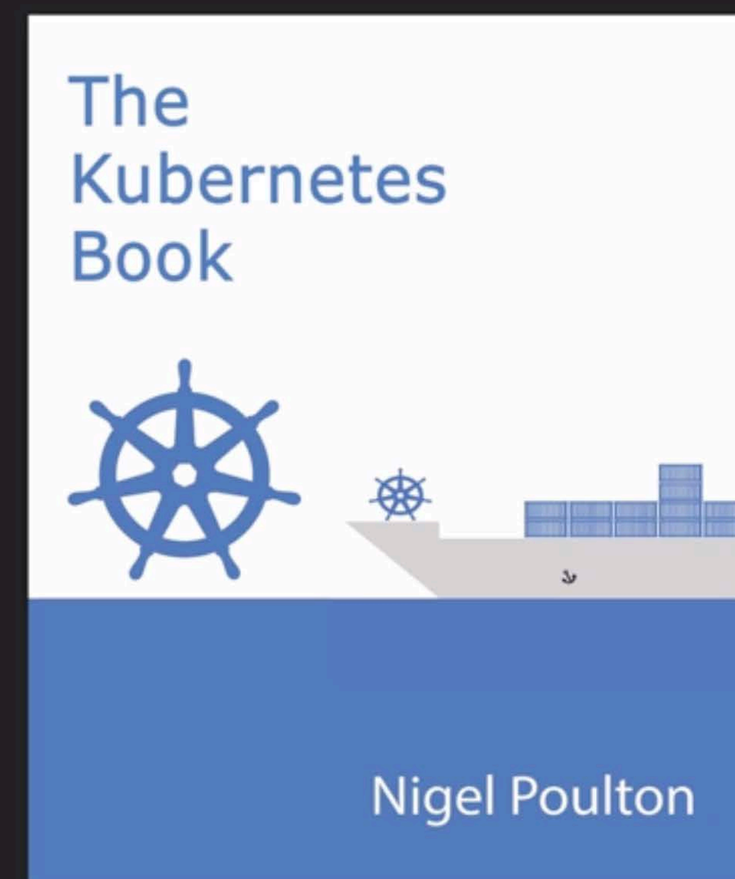
One Pod per node

Stateful app components

Kubernetes Objects



...



Spin-up a quick Kubernetes cluster

A CLOUD GURU

Contribute

https://play-with-k8s.com

Play with Kubernetes

A simple, interactive a to learn Kubernetes

github

docker

Login

Contribute

https://play-with-k8s.com

Play with Kubernetes

A simple, interactive a to learn Kubernetes

github

docker

Login

Contribute

https://play-with-k8s.com

Play with Kubernetes

A simple, interactive and fun playground to learn Kubernetes

Start

15 15 00:36 / 02:59

03:59:57

CLOSE SESSION

Instances

+ ADD NEW INSTANCE

Add instances to your playground.

Sessions and all their instances are deleted after 03:59:57 hours.

03:59:49

CLOSE SESSION

Instances

+ ADD NEW INSTANCE

192.168.0.8
node1

be7qj7qo_be7qj92o2l8g00d4gtkg

IP
192.168.0.8

Memory

CPU

URL
ip172-18-0-41-be7qj7qo2l8g00d4gtk0.direct.labs.play-with-k8

DELETE

```
You can bootstrap a cluster as follows:

1. Initializes cluster master node:

 kubeadm init --apiserver-advertise-address $(hostname -i)


 2. Initialize cluster networking:

 kubectl apply -n kube-system -f \
    "https://cloud.weave.works/k8s/net?k8s-version=$(kubectl version | base64 |
tr -d '\n')"


 3. (Optional) Create an nginx deployment:

 kubectl apply -f https://raw.githubusercontent.com/kubernetes/website/master/co
ntent/cn/docs/user-guide/nginx-app.yaml


                         The PWK team.


[node1 ~]$
```

Product Support Company Partners Contact Us

www.docker.com

docker

Why Docker? Products Solutions Customers Resources

Get Started

Build, Manage and Secure Your Apps Anywhere. Your Way.

The Dev to Ops Choice for Container Platforms

Learn More

15 15 00:59 / 02:59

Product Support Company Partners Contact Us

www.docker.com

docker

Why Docker? Products Solutions Customers Resources

Get Started

Docker Enterprise
Enterprise-grade Container Platform

Docker Desktop
Complete Dev Environment

Docker Engine
Industry-standard Container Engine

Docker Hub
Largest Container Content Library

Build, Manag e Your Apps Anywh .

The Dev to Ops Choice for

Learn More

https://www.docker.com/products/docker-desktop

Product Support Company Partners Contact Us

www.docker.com

docker

Why Docker? Products Solutions Customers Resources

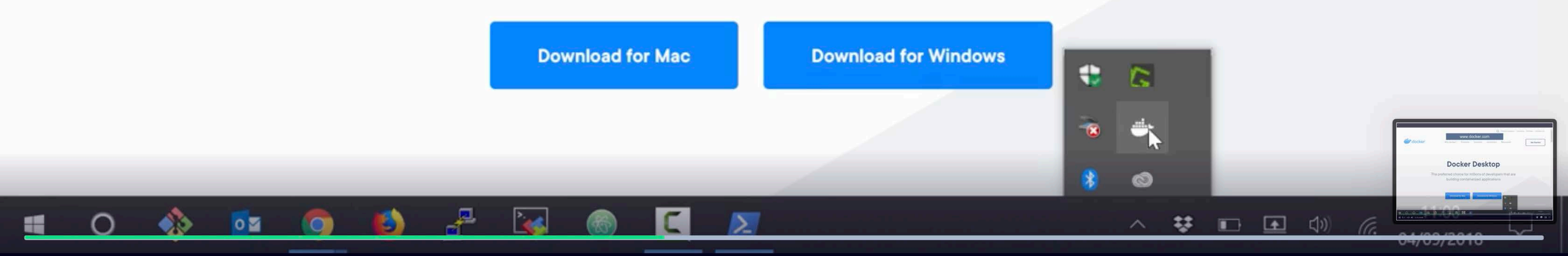
Get Started

Docker Desktop

The preferred choice for millions of developers that are building containerized applications

Download for Mac

Download for Windows



15 15 01:15 / 02:59

Product Support Company Partners Contact Us

www.docker.com

docker

Why Docker? Products Solutions Customers Resources

Get Started

Docker Desktop

The preferred choice for million ... re
building containerized ...

Download for Mac

Do

- About Docker
- Discover Docker Enterprise Edition
- Settings
- Check for Updates
- Diagnose and Feedback...
- Switch to Windows containers...
- Docker Store
- Documentation
- Kitematic
- nigelpoulton
- Repositories
- Kubernetes
- Restart...
- Quit Docker

11:00
04/09/2018

Contact Us

Started

Settings

General

Shared Drives

Advanced

Network

Proxies

Daemon

Kubernetes

Reset

Kubernetes

Configure and manage the kubernetes cluster

☑ Enable Kubernetes

Starts a Kubernetes single-node cluster when starting Docker.

Default orchestrator for `docker stack` commands (changes ~/.docker/config.json):

○ Kubernetes ◉ Swarm

☐ Show system containers (advanced)

Show kubernetes internal containers when using Docker commands.

Apply

● Docker is running

● Kubernetes is running

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\k8s> kubectl get nodes
NAME                 STATUS    ROLES     AGE       VERSION
docker-for-desktop   Ready     master    27d       v1.10.3
PS C:\k8s>
```

15 15 01:28 / 02:59

Google Cloud Platform acg1 cloud.google.com

DASHBOARD ACTIVITY CUSTOMIZE

Project info

Project name
acg1

Project ID
acg1-206211

Project number
292661174106

Go to project settings

Resources

This project has no resources

Trace

No trace data from the past 7 days

APIs

Requests (requests/sec)

api/request_count:consumed_api:REDUCE_SUM(acg1-206211)
: 0.033

Go to APIs overview

Google Cloud Platform status

All services normal

Go to Cloud status dashboard

Billing

Estimated charges GBP £0.38
For the billing period Sep 1 – 4, 2018

View detailed charges

Error Reporting

No sign of any errors. Have you set up Error Reporting?

Learn how to set up Error Reporting

Google Cloud Platform acg1 cloud.google.com

Home

Marketplace

Billing

APIs & Services

Support

IAM & admin

Getting started

Security

COMPUTE

App Engine

Compute Engine

Kubernetes Engine

Clusters

Workloads

Services

Applications

Configuration

Storage

CUSTOMIZE

API APIs

Requests (requests/sec)

0.035

0.034

0.033

0.032

0.031

10:15 10:30 10:45 11 AM

i/request_count:consumed_api:REDUCE_SUM(acg1-
6211)
.033

Go to APIs overview

Google Cloud Platform status

All services normal

Go to Cloud status dashboard

Billing

Estimated charges GBP £0.38

For the billing period Sep 1 – 4, 2018

View detailed charges

Error Reporting

No sign of any errors. Have you set up Error Reporting?

Learn how to set up Error Reporting

https://console.cloud.google.com/kubernetes/list?project=acg1-2...

Google Cloud Platform acg1 cloud.google.com

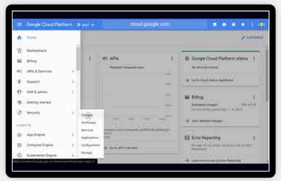
Clusters

Kubernetes Engine

Kubernetes clusters

Containers package an application so it can be easily deployed to run in its own isolated environment. Containers are managed in clusters that automate VM creation and maintenance. Learn more

Create cluster | Deploy container | Take the quickstart



https://console.cloud.google.com/kubernetes/add?project=acg1-...

Google Cloud Platform acg1 cloud.google.com

Create a Kubernetes cluster

Name

cluster-1

Location type

- (•) Zonal
- ( ) Regional

Zone

europe-west2-b

Master version

1.10.6-gke.2

Node pools

default-pool

Number of nodes

3

Machine type

Customize to select cores, memory and GPUs

1 vCPU 3.75 GB memory Customize

Advanced edit

Google Cloud Platform acg1 cloud.google.com

Create a Kubernetes cluster

1.10.6-gke.2

Node pools

default-pool

Number of nodes

3

Machine type

Customize to select cores, memory and GPUs

1 vCPU 3.75 GB memory Customize

Advanced edit

+ Add node pool

Advanced options

You will be billed for the 3 nodes (VM instances) in your cluster. Learn more

Create Cancel

Equivalent REST or command line

Google Cloud Platform acg1

Kuberne...usters

CREATE CLUSTER DEPLOY REFRESH SHOW INFO PANEL

A Kubernetes cluster is a managed group of uniform VM instances for running Kubernetes. Learn more

Filter by label or name

Name	Location	Cluster size	Total cores	Total memory	Notifications	Labels	
cluster-1	europe-west2-b	3	3 vCPUs	11.25 GB			Connect

15 15 02:20 / 02:59

Connect to the cluster

You can connect to your cluster via command-line or using a dashboard.

Command-line access

Configure kubectl command line access by running the following command:

```
$ gcloud container clusters get-credentials cluster-1 --zone europe-west2-b --project acg1-206211
```

Copied

Run in Cloud Shell

Cloud Console dashboard

You can view the workloads running in your cluster in the Cloud Console Workloads dashboard.

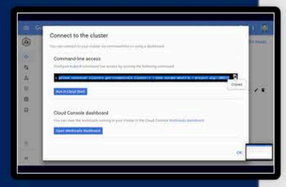
Open Workloads dashboard

OK

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\k8s> kubectl get nodes
NAME                 STATUS    ROLES     AGE       VERSION
docker-for-desktop   Ready     master    27d       v1.10.3
PS C:\k8s>
PS C:\k8s>
PS C:\k8s> gcloud container clusters get-credentials cluster-1 --zone europe-west2
-b --project acg1-206211
```



App Architecture

A CLOUD GURU

Lesson Plan

A CLOUD GURU

- Kubernetes App Theory
- Sample Kubernetes App
- Recap

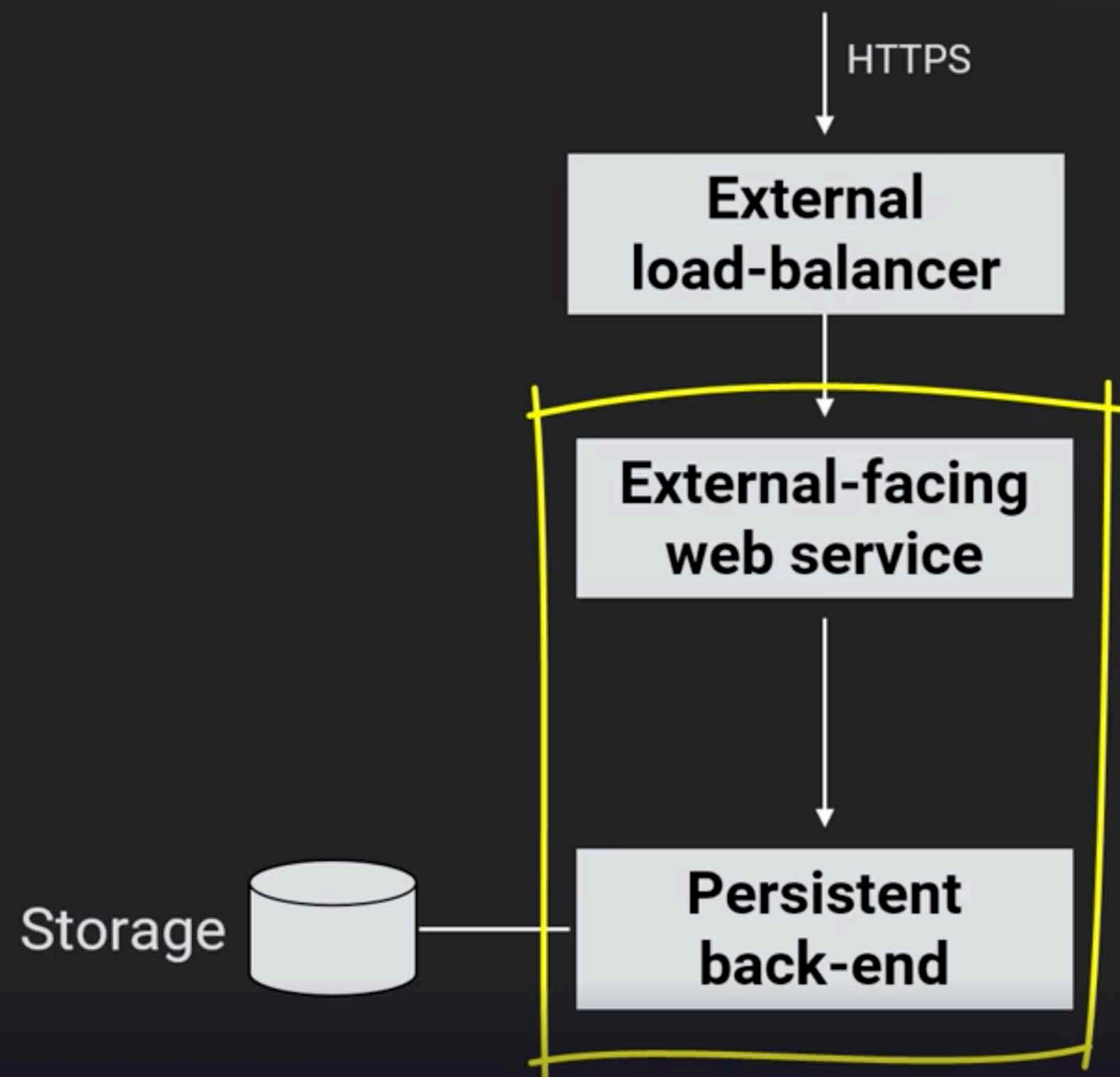
Kubernetes App Theory

A CLOUD GURU

App Architecture

Kubernetes App Theory

A CLOUD GURU

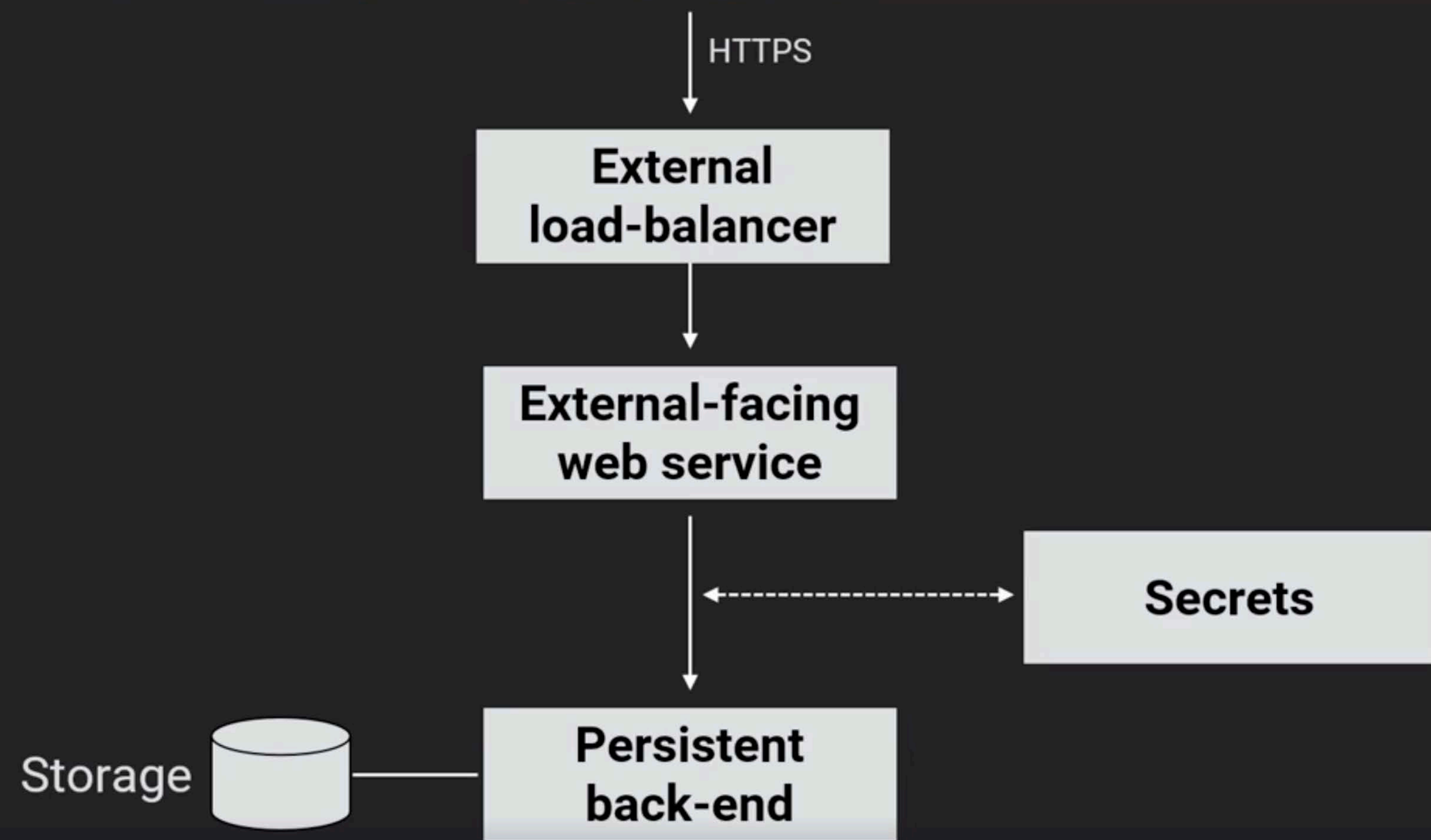


15 15 00:36 / 05:05

App Architecture

Kubernetes App Theory

A CLOUD GURU

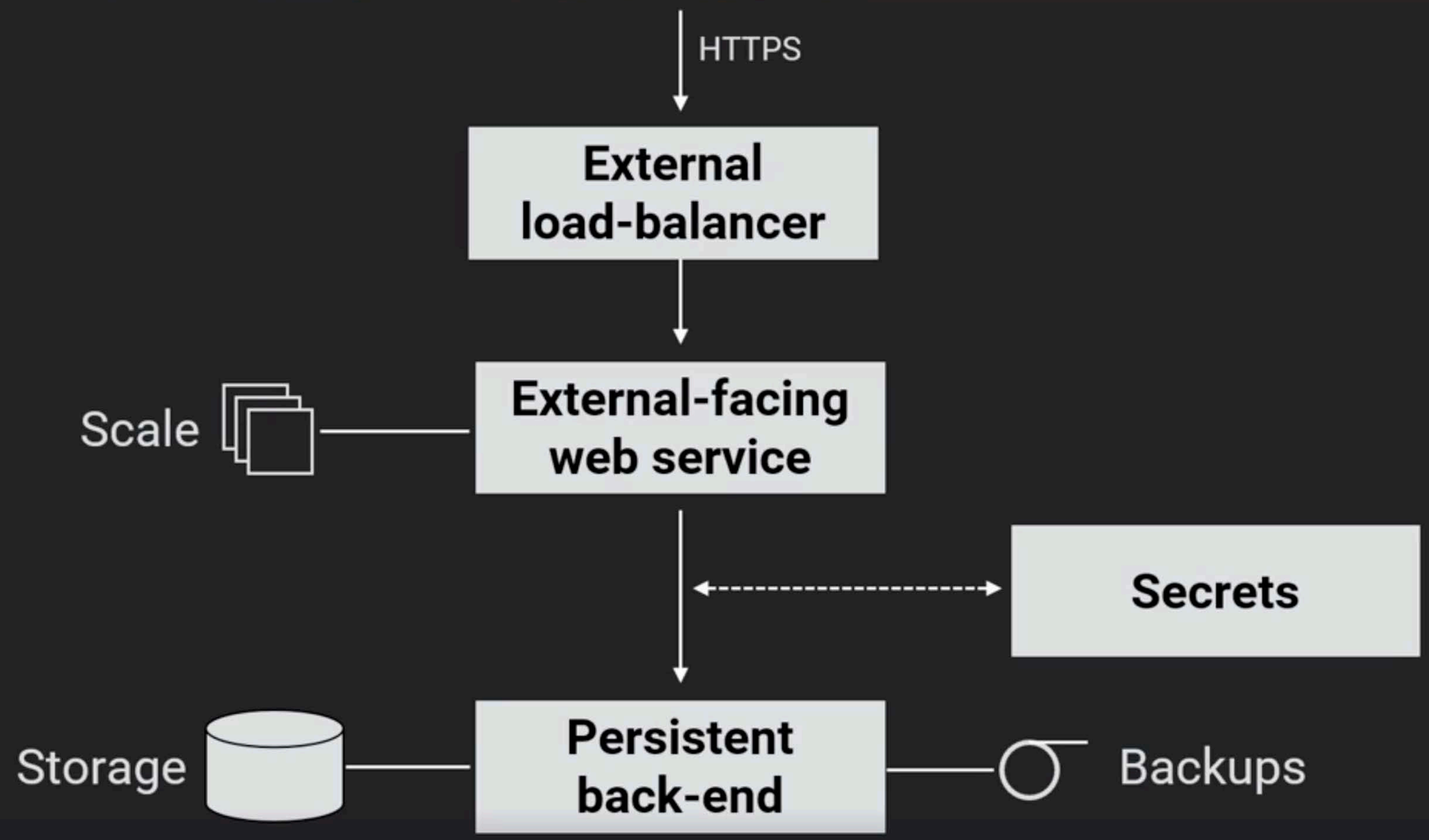


15 15 00:40 / 05:05

App Architecture

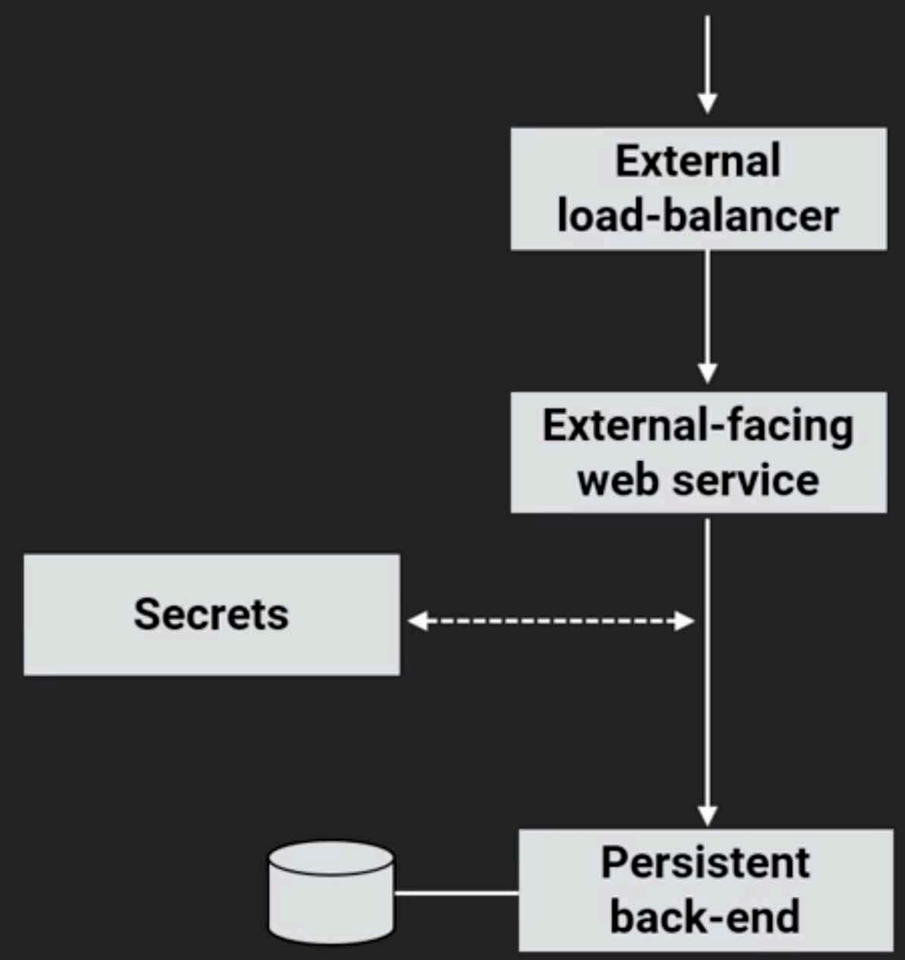
Kubernetes App Theory

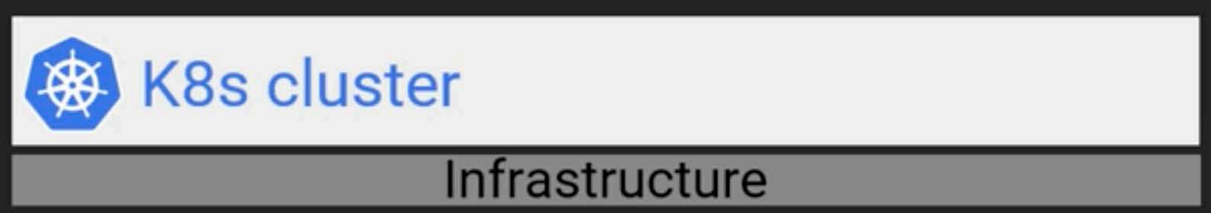
A CLOUD GURU



15 15 00:55 / 05:05

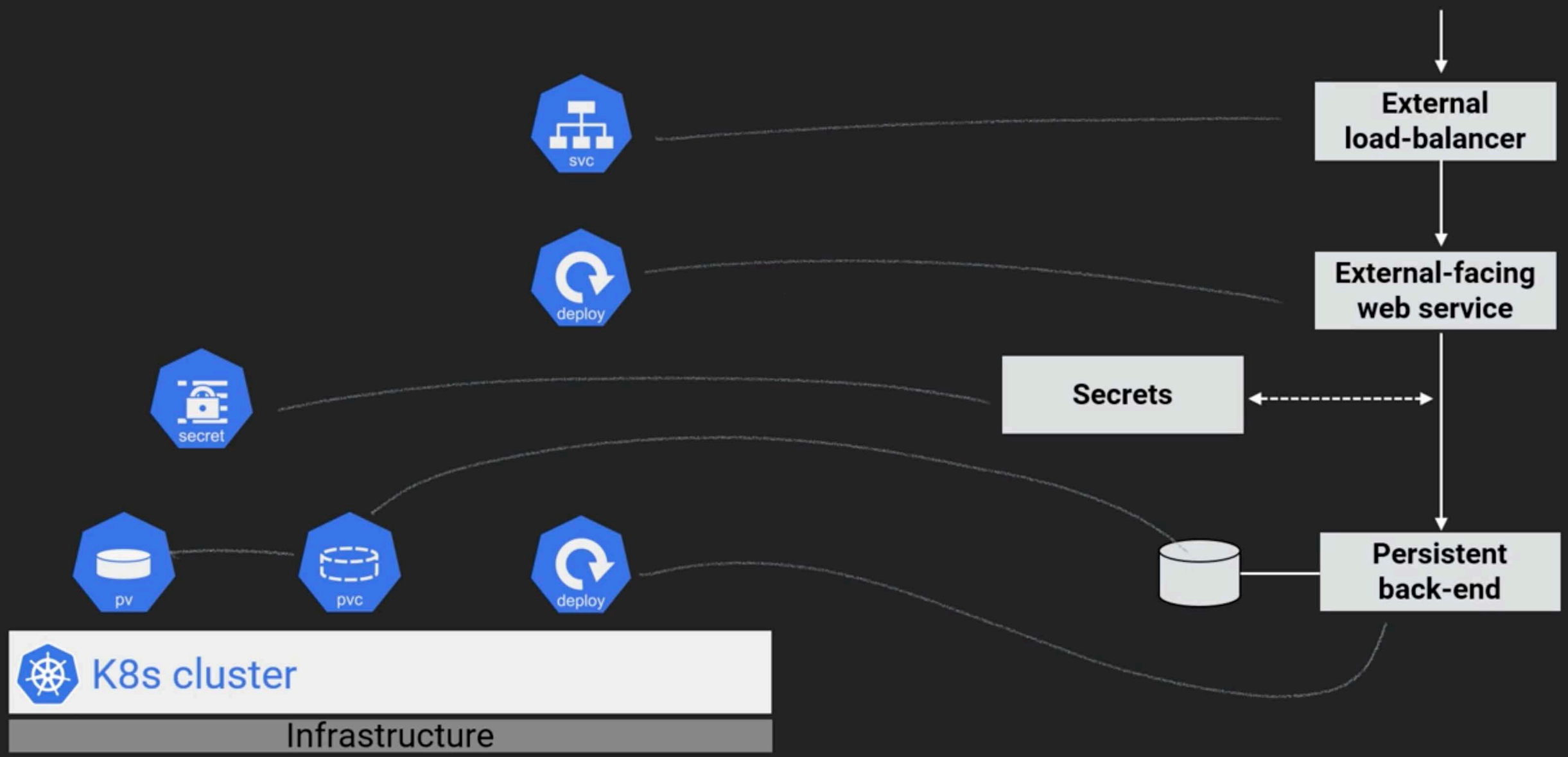
Kubernetes App Theory





App Architecture

Kubernetes App Theory



Kubernetes Sample App

A CLOUD GURU

Search or jump to... / Pull requests Issues Marketplace Explore

nigelpoulton / k8s-sample-apps
forked from kubernetes/examples

Code | Pull requests 0 | Projects 0 | Wiki | Insights | Settings

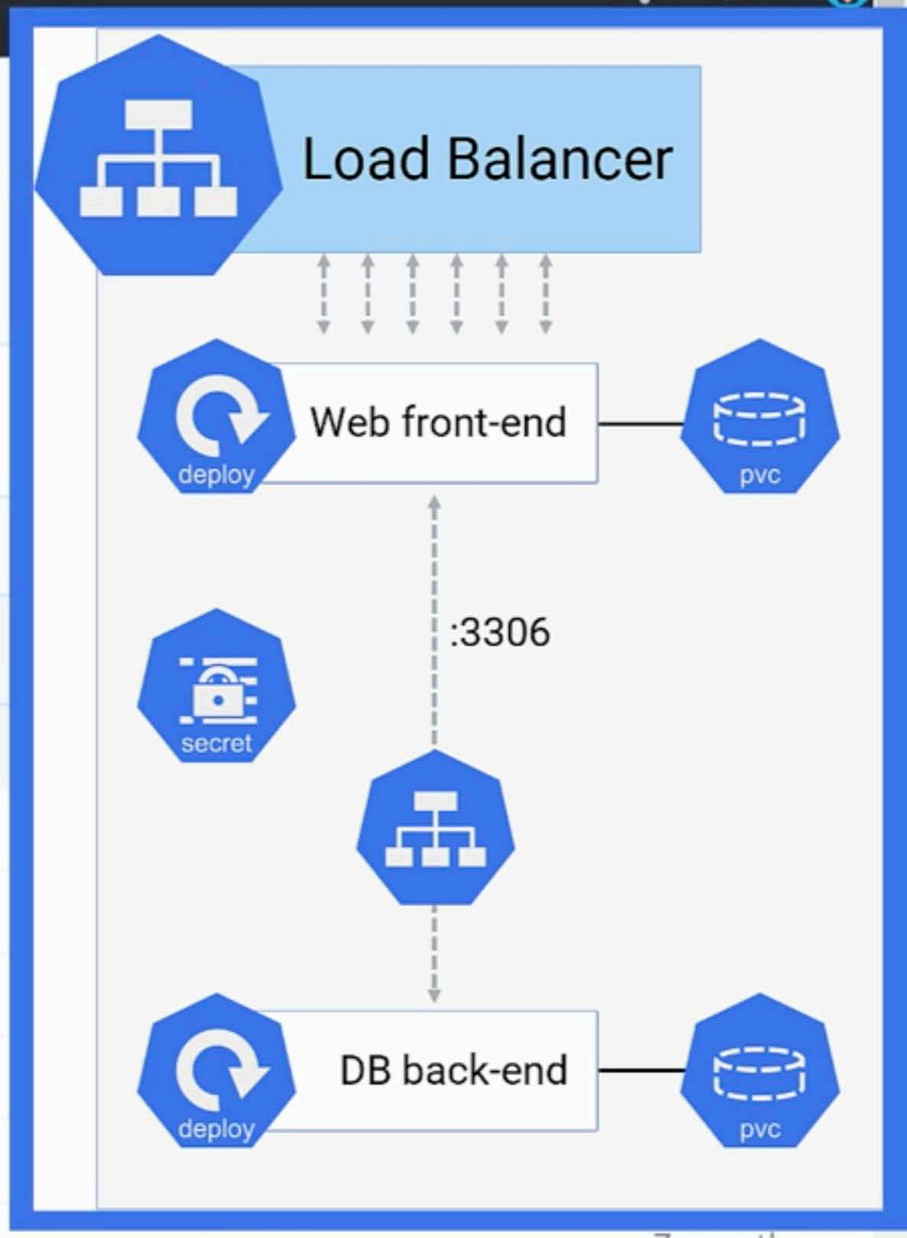
Branch: master | k8s-sample-apps / mysql-wordpress-pd /

This branch is 28 commits behind kubernetes:master.

jheyduk and ahmetb add missing comment (#195)

..

OWNERS	Move maintained examples to root, update README	
README.md	Redirect tutorials to the docs site (#85)	
WordPress.png	Move maintained examples to root, update README	
gce-volumes.yaml	Move maintained examples to root, update README	
local-volumes.yaml	Move maintained examples to root, update README	
mysql-deployment.yaml	add missing comment (#195)	7 months ago



11:22
06/09/2018

Code | Pull requests 0 | Projects 0 | Wiki | Insights | Settings

Branch: master

k8s-sample-apps / mysql-wordpress-pd /

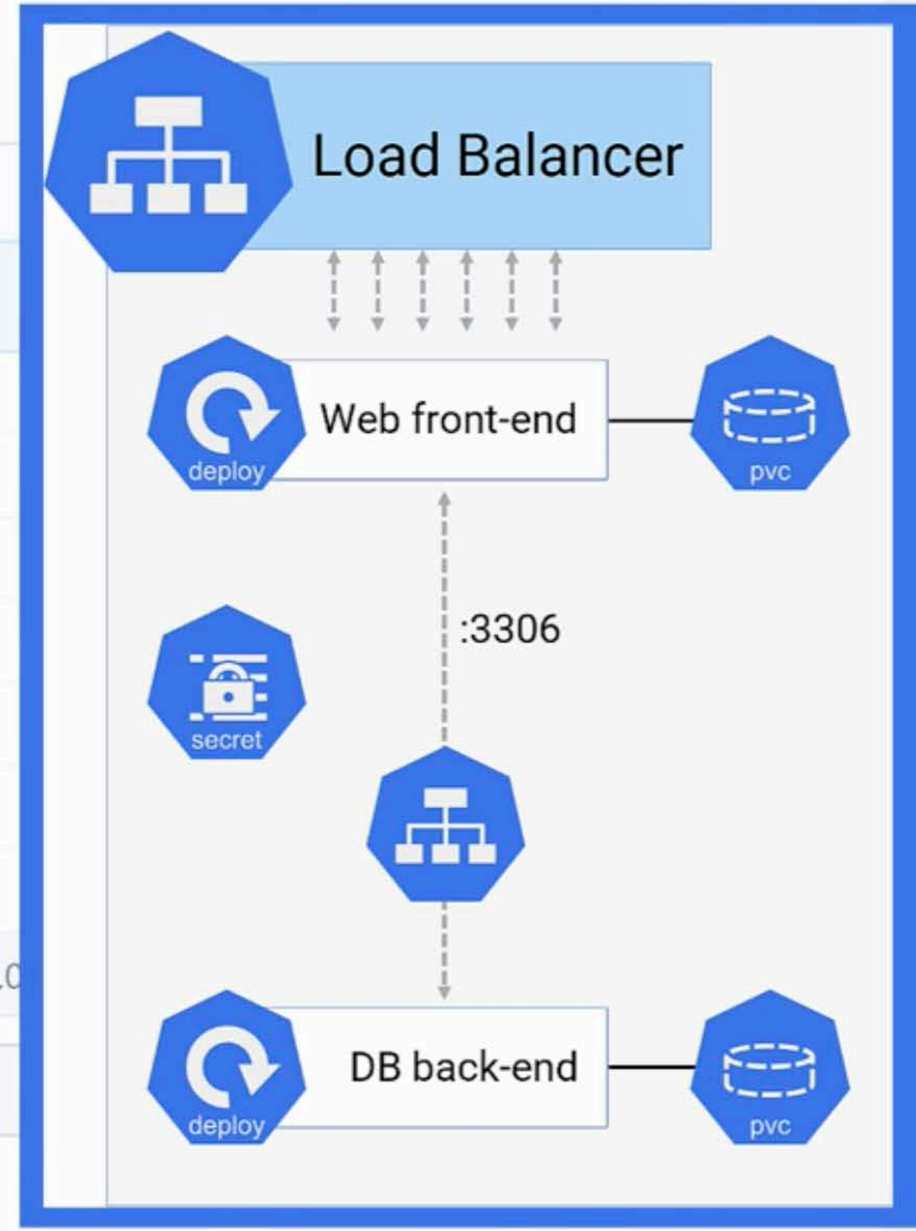
This branch is 28 commits behind kubernetes:master.

jheyduk and ahmetb add missing comment (#195)

..

OWNERS	Move maintained examples to root, update README
README.md	Redirect tutorials to the docs site (#85)
WordPress.png	Move maintained examples to root, update README
gce-volumes.yaml	Move maintained examples to root, update README
local-volumes.yaml	Move maintained examples to root, update README
mysql-deployment.yaml	add missing comment (#195)
wordpress-deployment.yaml	update all Deployment API version to apps/v1 in k8s v1.9.0

README.md

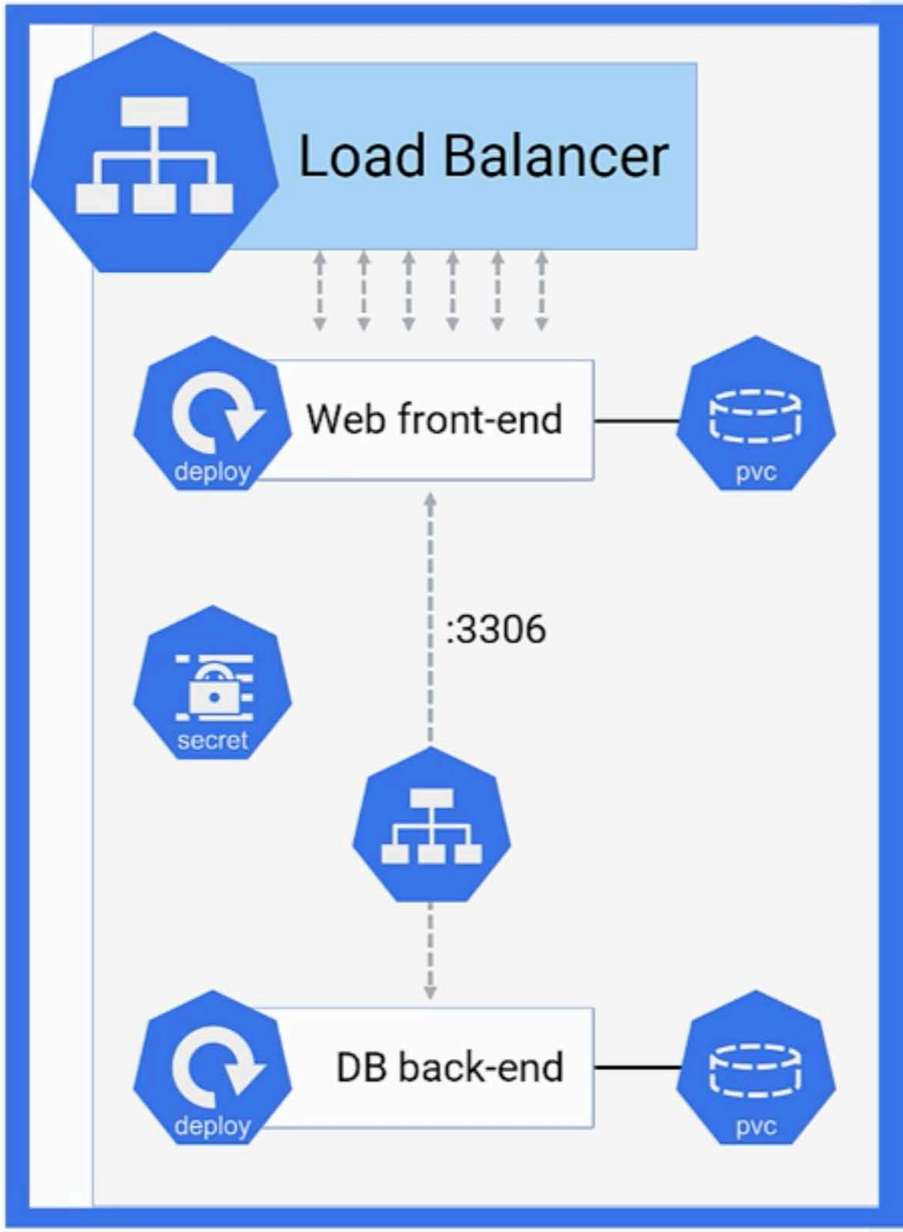


Example: WordPress and MySQL on Kubernetes

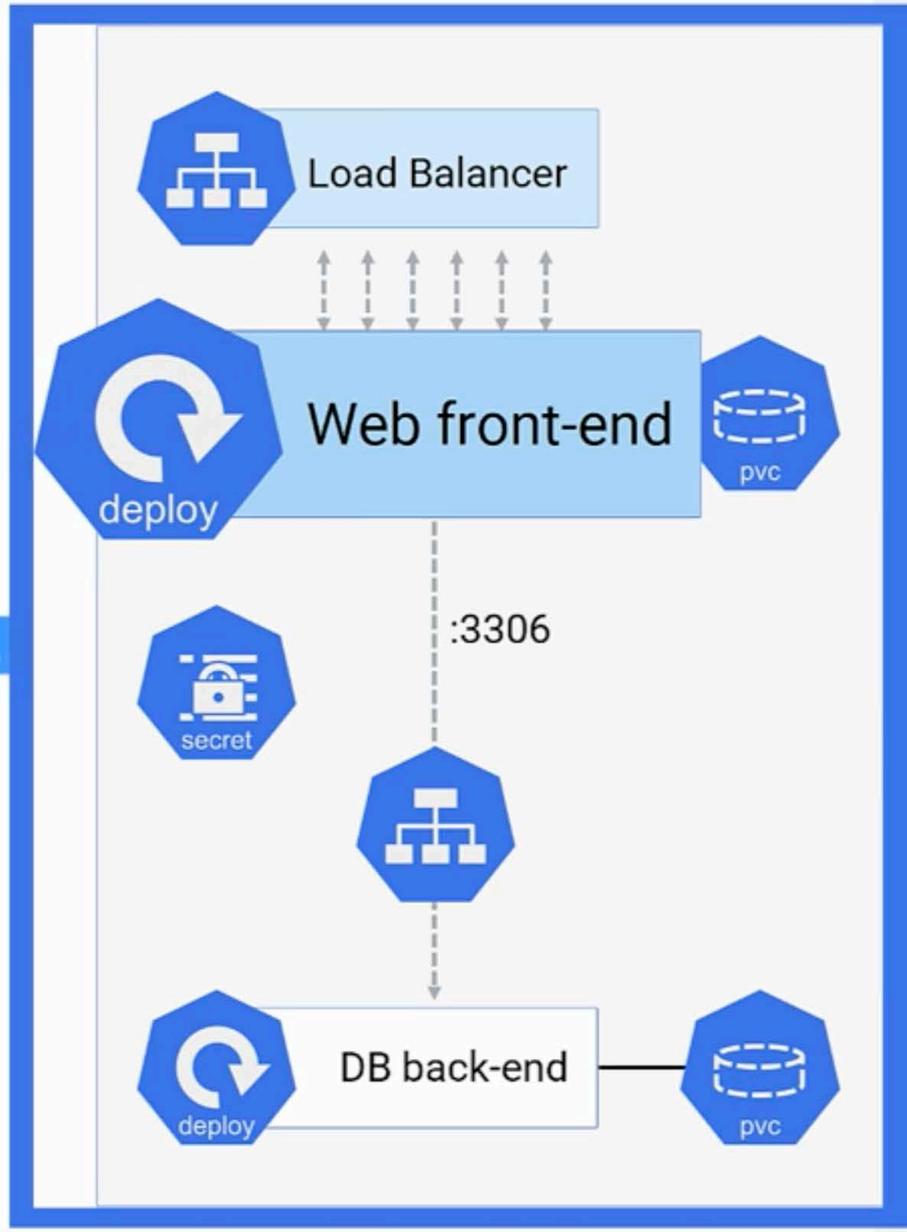
github.com/nigelpoulton/k8s-sample-apps/.../wordpress-deployment.yaml

Chrome File Edit View History Bookmarks Profiles Tab Window Help Mon Aug 16 4:42 PM

```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```

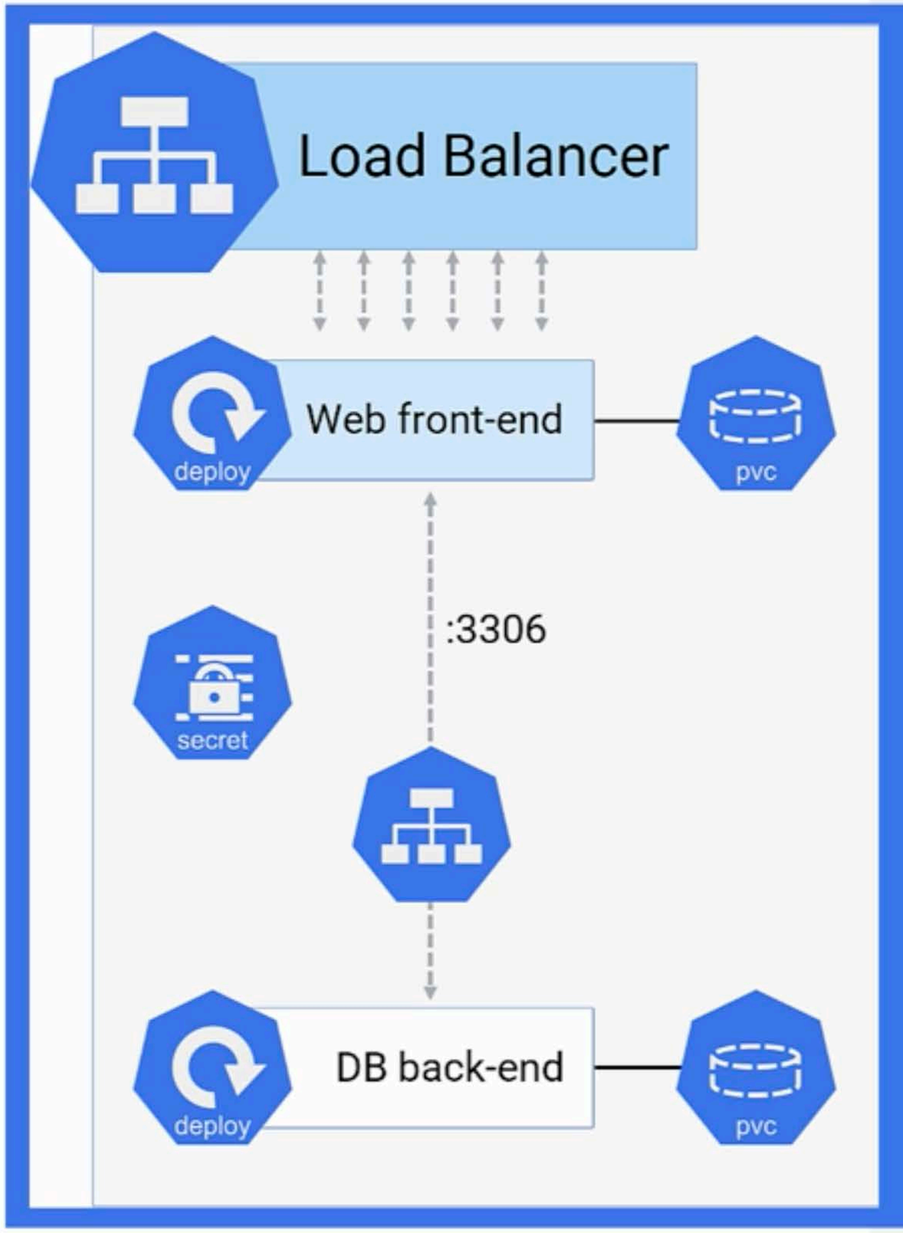


```yaml
    labels:
      app: wordpress
  spec:
    accessModes:
      - ReadWriteOnce
    resources:
      requests:
        storage: 20Gi
  ---
  apiVersion: apps/v1 #  for k8s versions before 1.
  kind: Deployment
  metadata:
    name: wordpress
    labels:
      app: wordpress
  spec:
    selector:
      matchLabels:
```

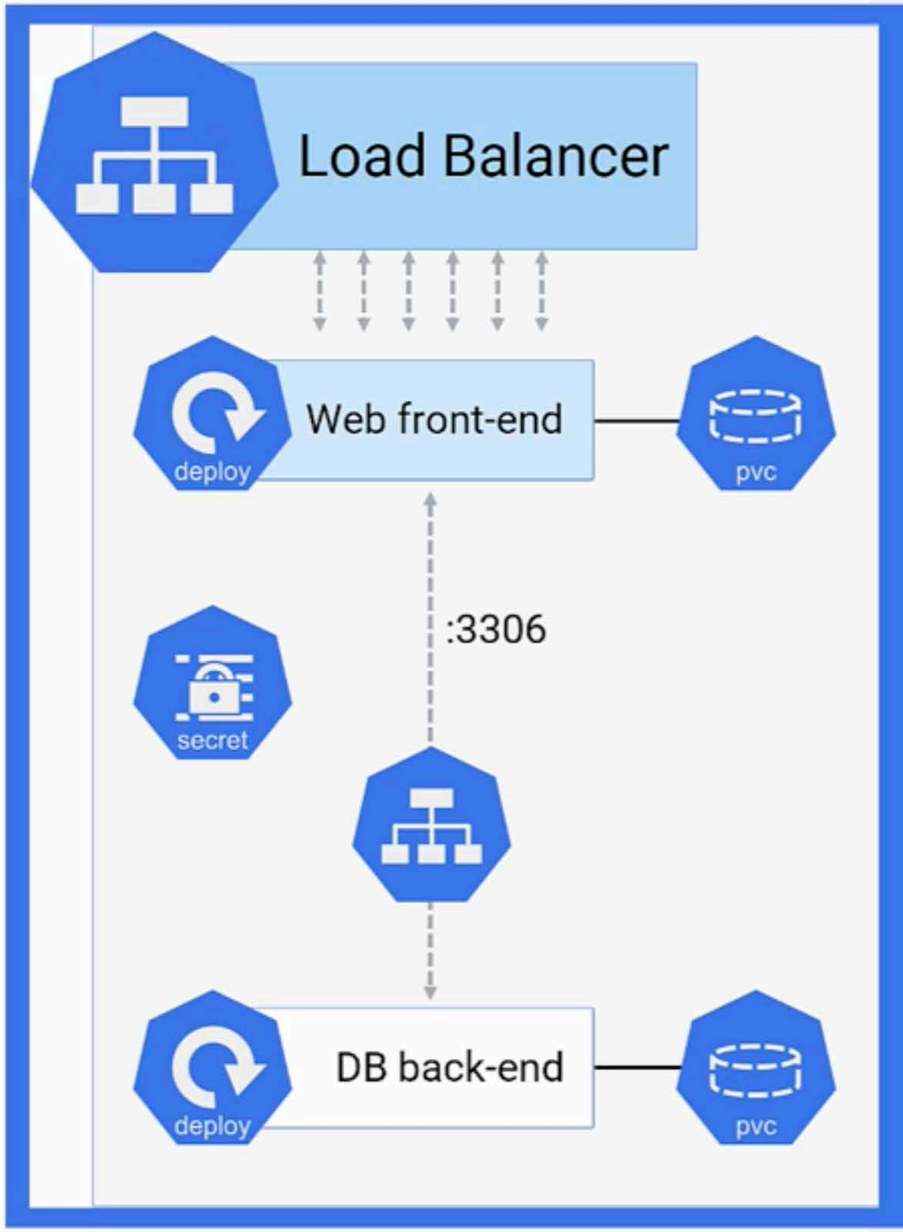


```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```

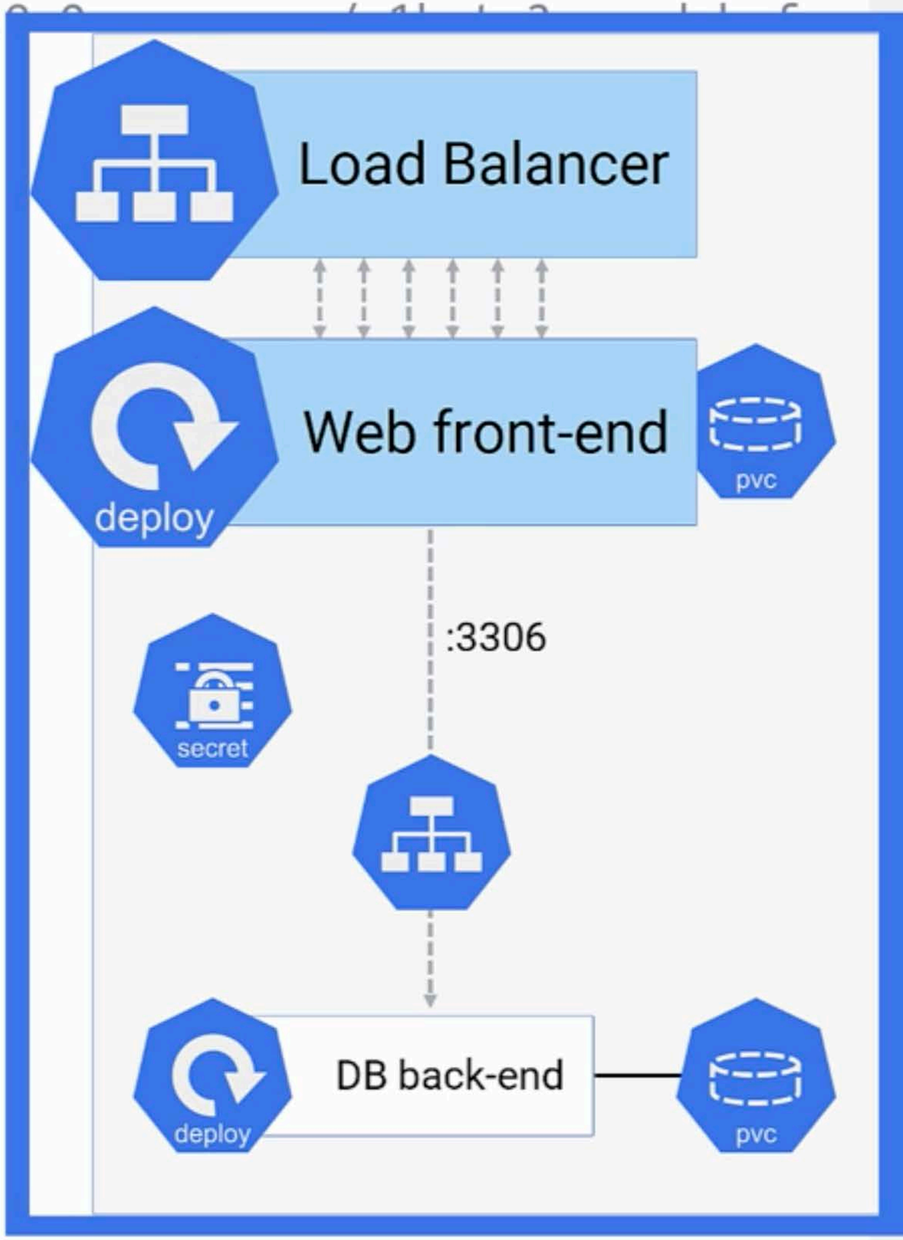
Create load-balancer on cloud platform



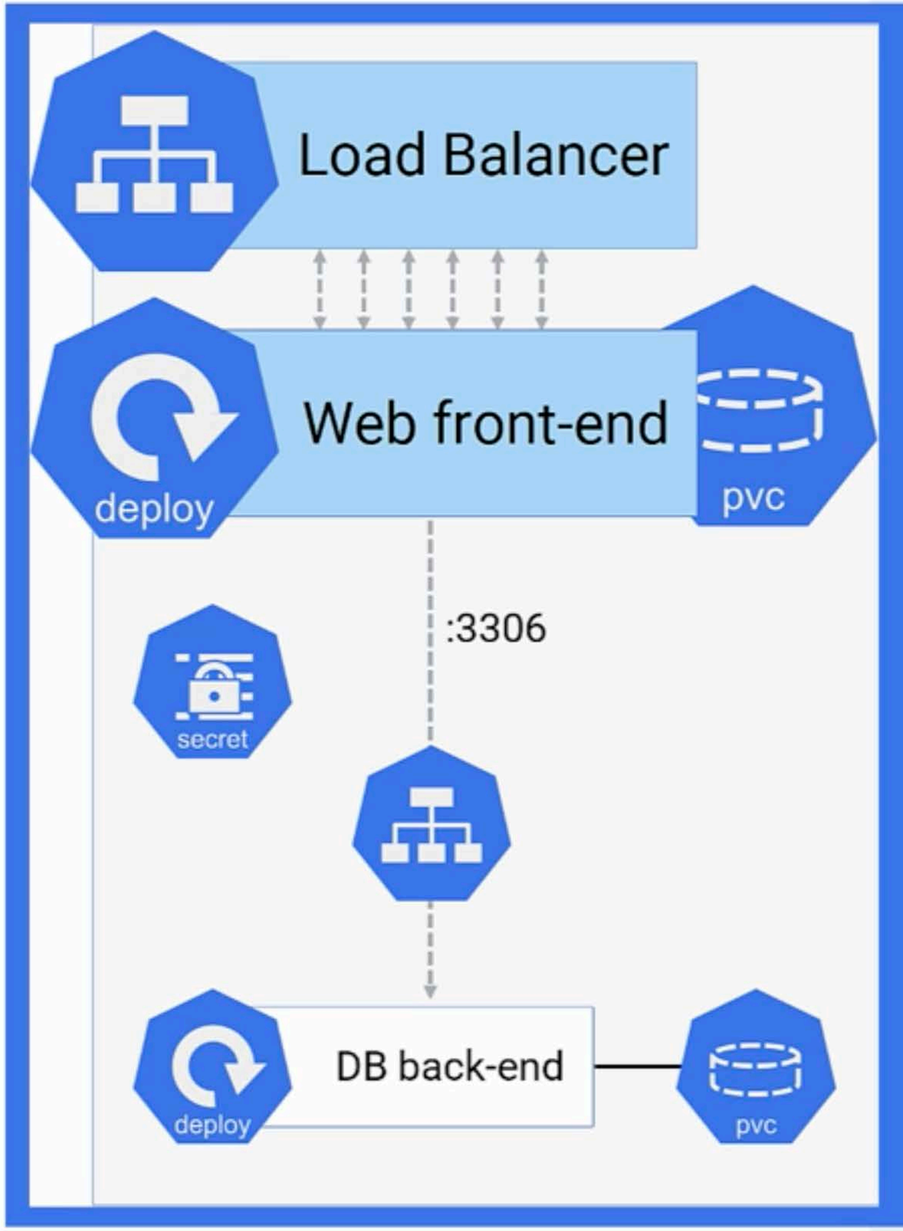
```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```



```yaml
---
apiVersion: apps/v1 #  for k8s versions before 1.
kind: Deployment
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  selector:
    matchLabels:
      app: wordpress
      tier: frontend
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
```

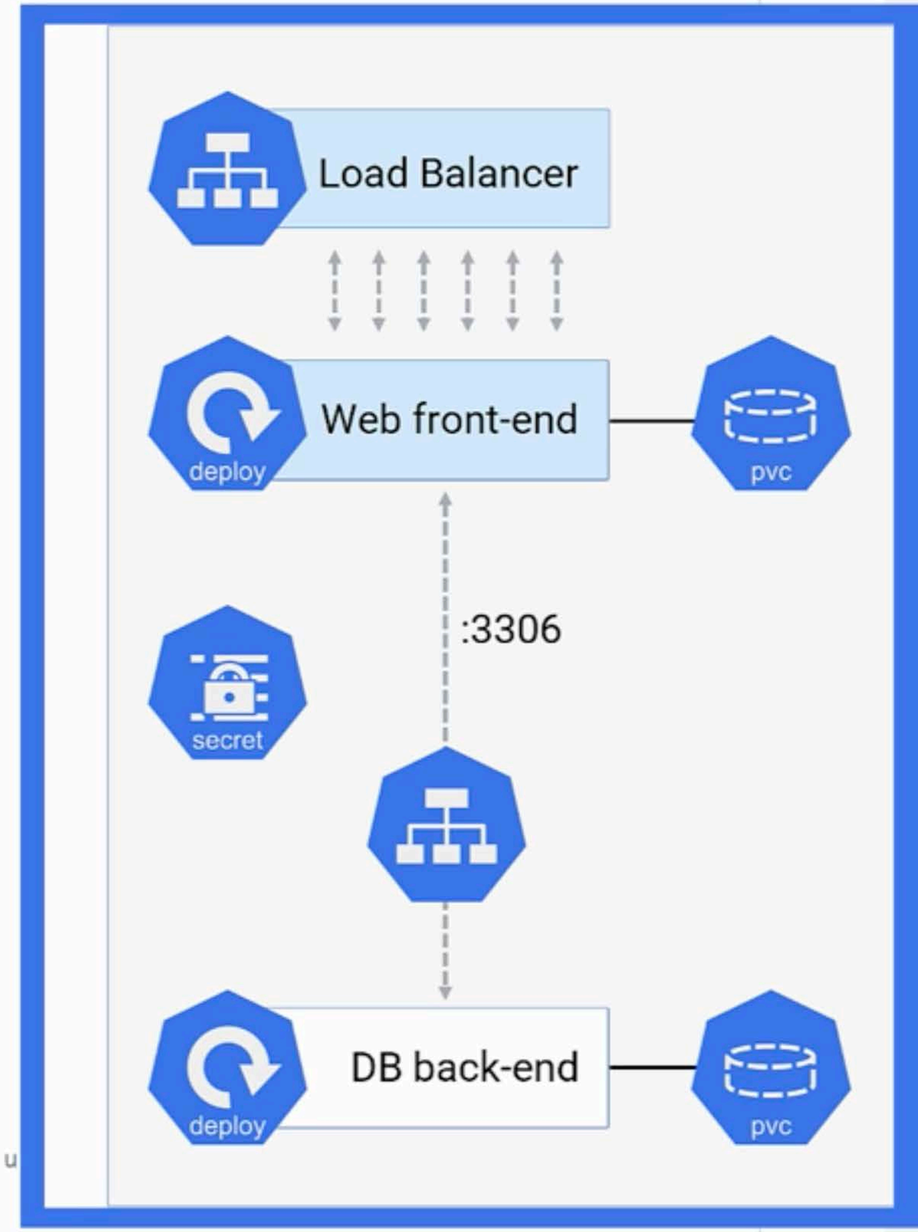


```yaml
      tier: frontend
    type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: wp-pv-claim
  labels:
    app: wordpress
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 20Gi
---
apiVersion: apps/v1 #  for k8s versions before 1.9.0 use apps/v1beta2  and before
```



Chrome File Edit View History Bookmarks Profiles Tab Window Help Mon Aug 16 4:44 PM

```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: wp-pv-claim
  labels:
    app: wordpress
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 20Gi
---
apiVersion: apps/v1 #  ns before 1.9.0 use apps/v1beta2  and before 1.8.0 u
kind: Deployment
metadata:
  name: wordpress
  labels:
```



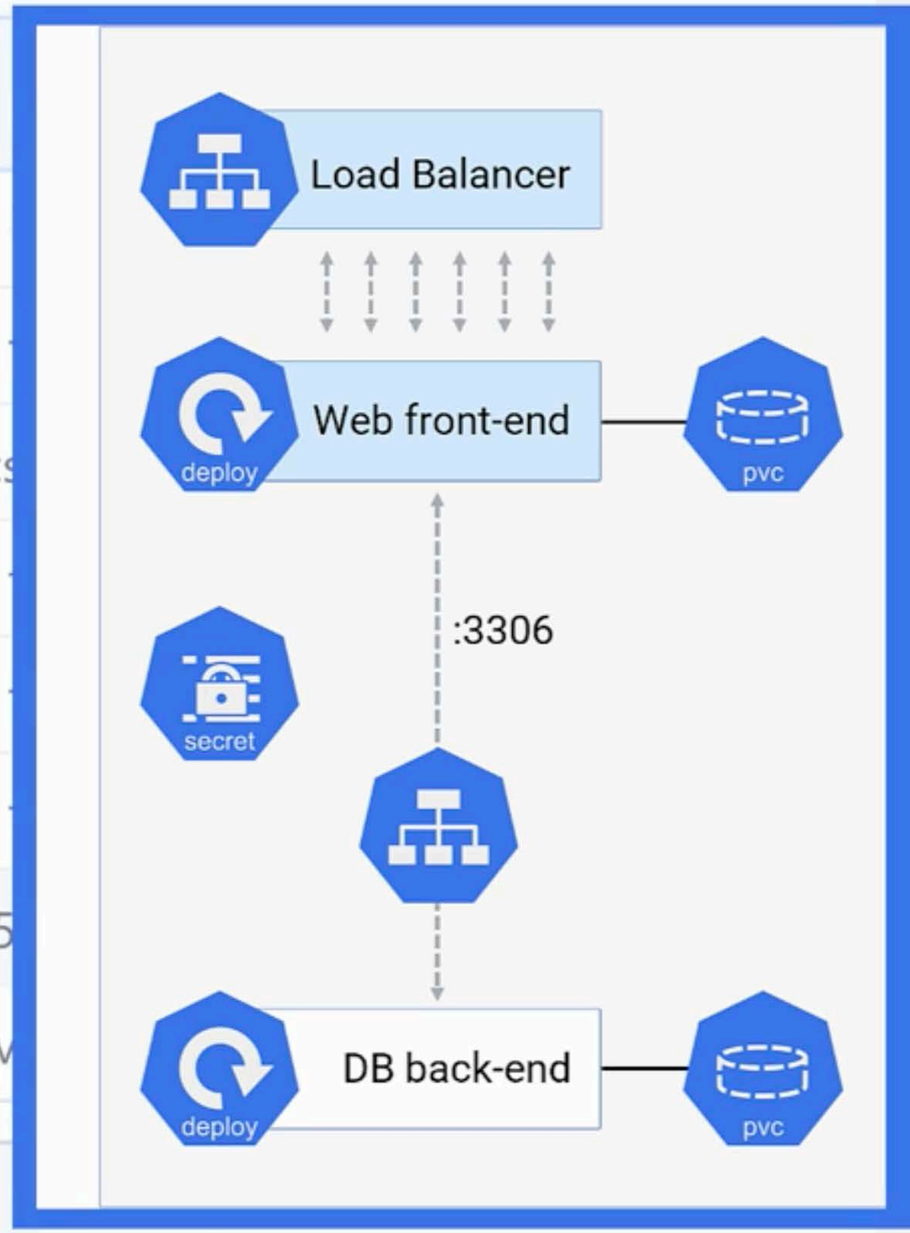
Chrome File Edit View History Bookmarks Profiles Tab Window Help Mon Aug 16 4:45 PM

This branch is 28 commits behind kubernetes:master.

jheyduk and ahmetb add missing comment (#195)

..

OWNERS	Move maintained examples
README.md	Redirect tutorials to the docs
WordPress.png	Move maintained examples
gce-volumes.yaml	Move maintained examples
local-volumes.yaml	Move maintained examples
mysql-deployment.yaml	add missing comment (#195
wordpress-deployment.yaml	update all Deployment API v



README.md

github.com/nigelpoulton/k8s-sample-apps/blob/.../mysql-deployment.yaml

Recap
A CLOUD GURU
15
15
00:03 / 02:23

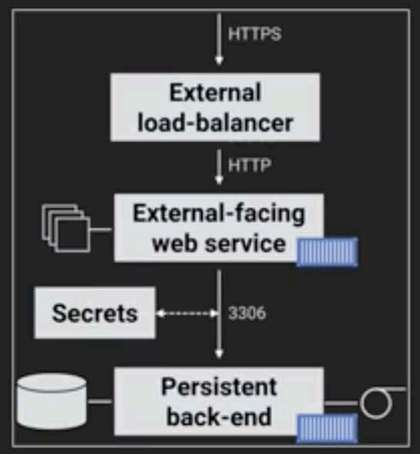
App Architecture

Recap

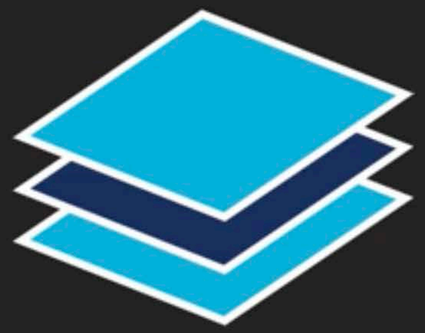
A CLOUD GURU

Ideas

Requirements



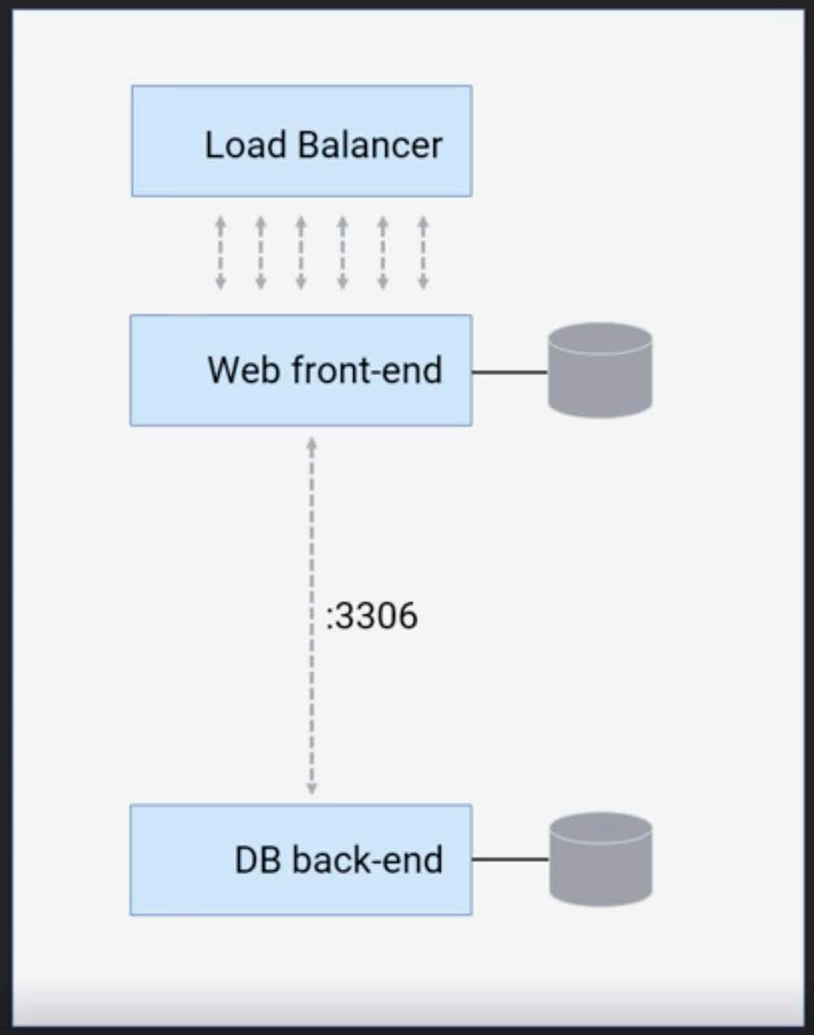

```
package main
import (
    "fmt"
    "reflect"
)
func main() {…
```



15 15 00:22 / 02:23

App Architecture

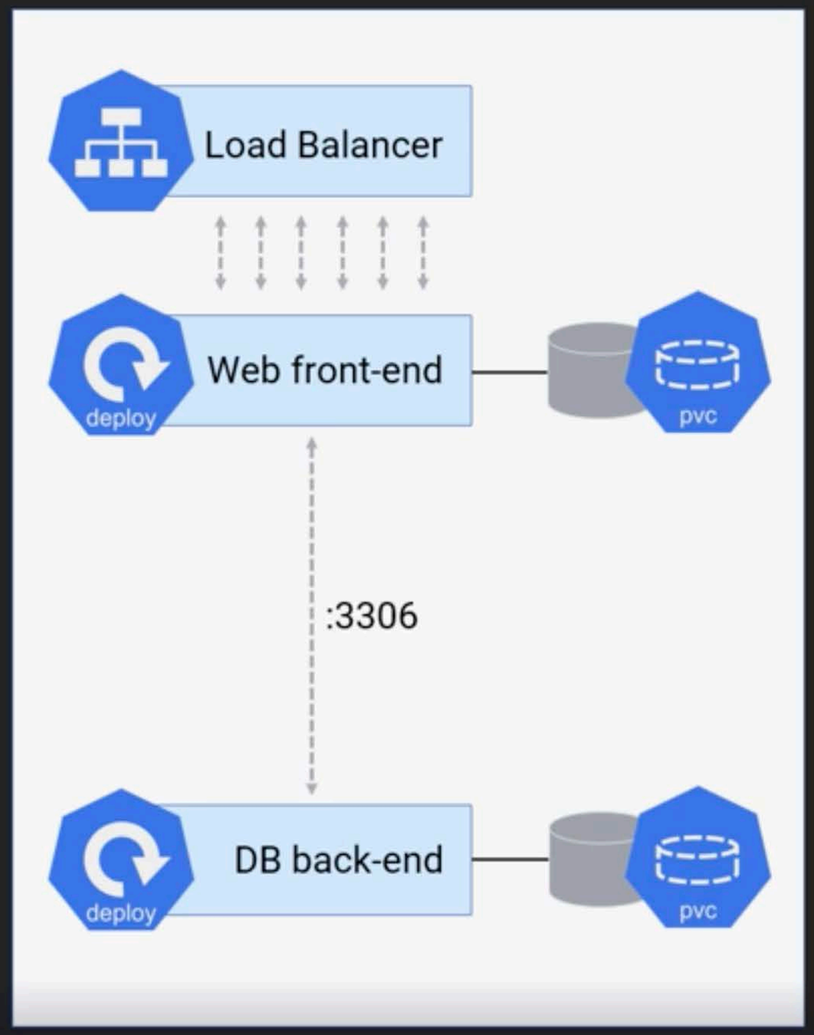
Recap



15 15 00:44 / 02:23

App Architecture

Recap



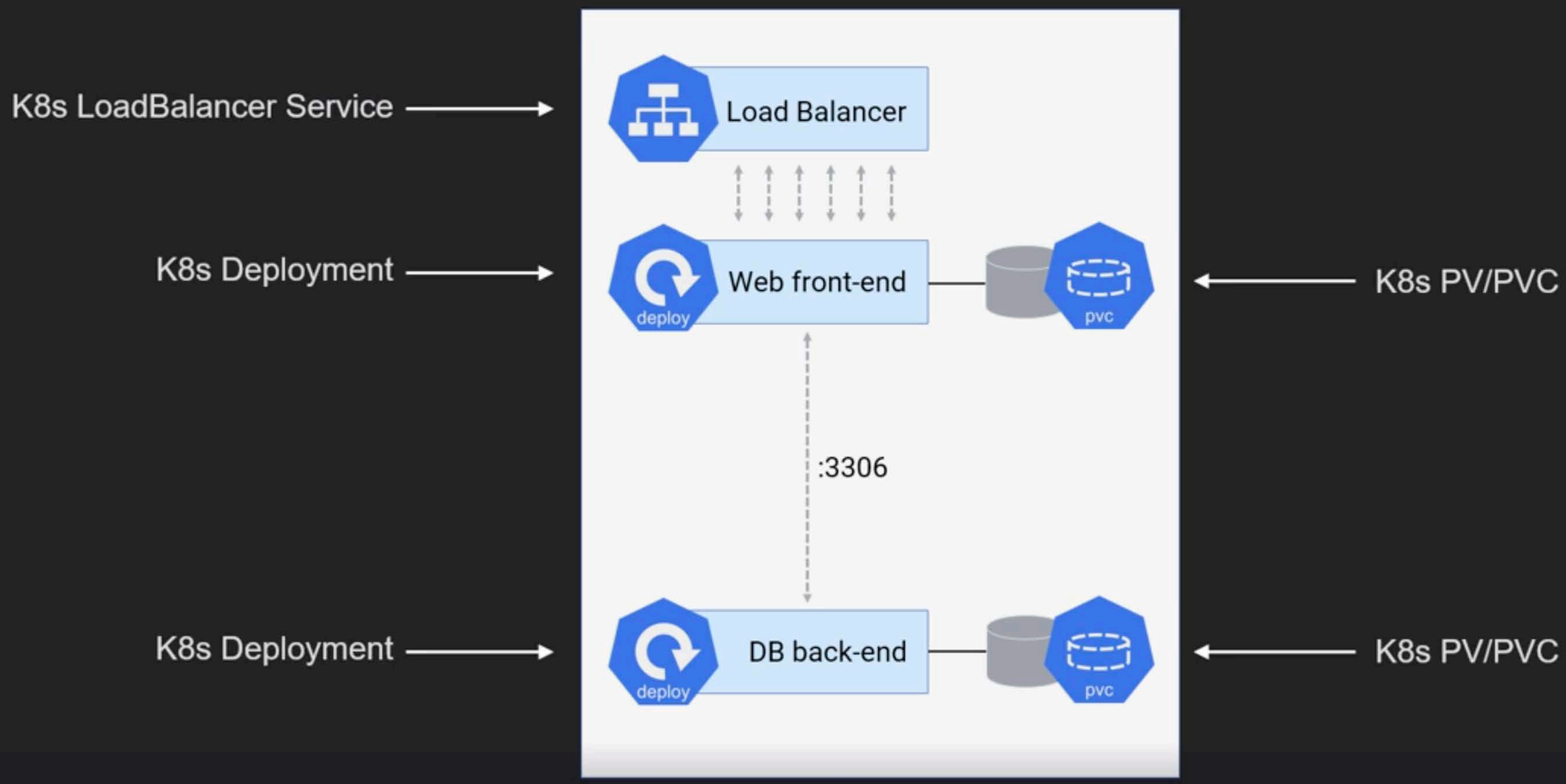
A CLOUD GURU

15 15 00:46 / 02:23

App Architecture

Recap

A CLOUD GURU

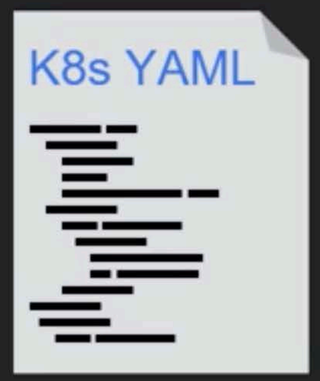


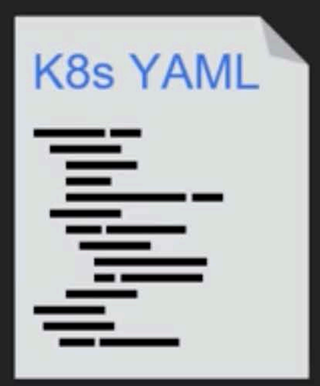
15 15 01:34 / 02:23

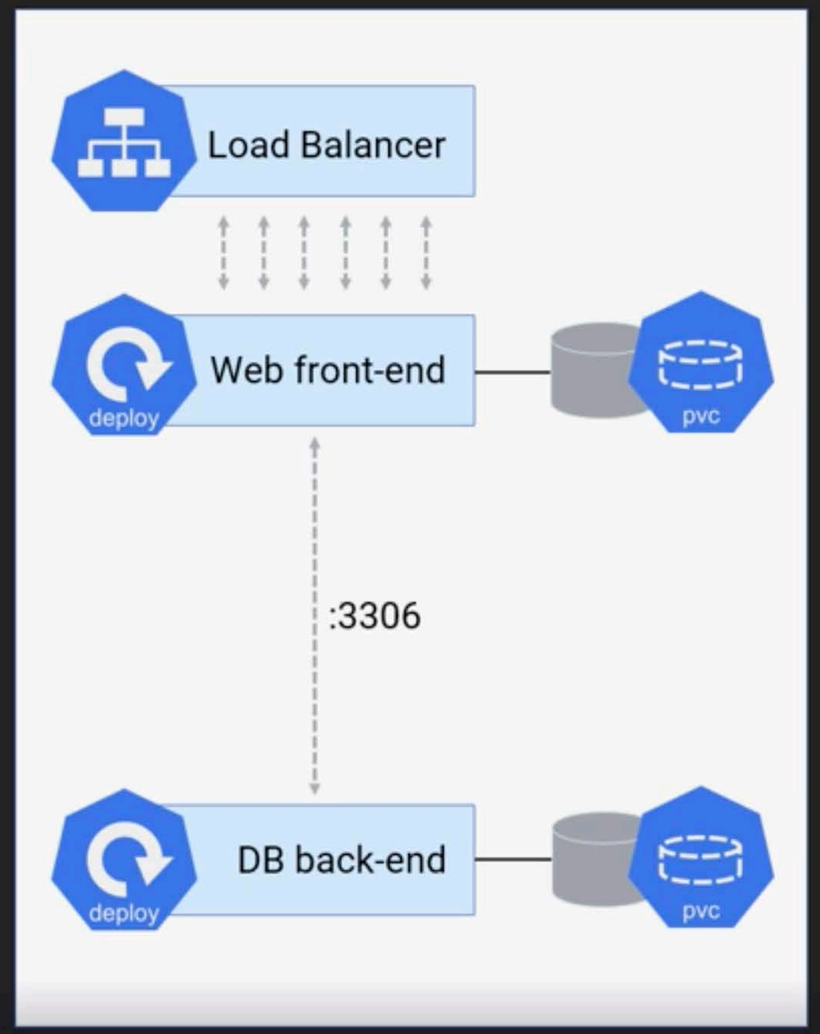
App Architecture

Recap

A CLOUD GURU





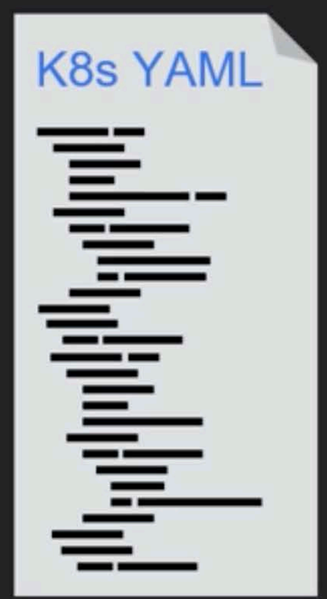


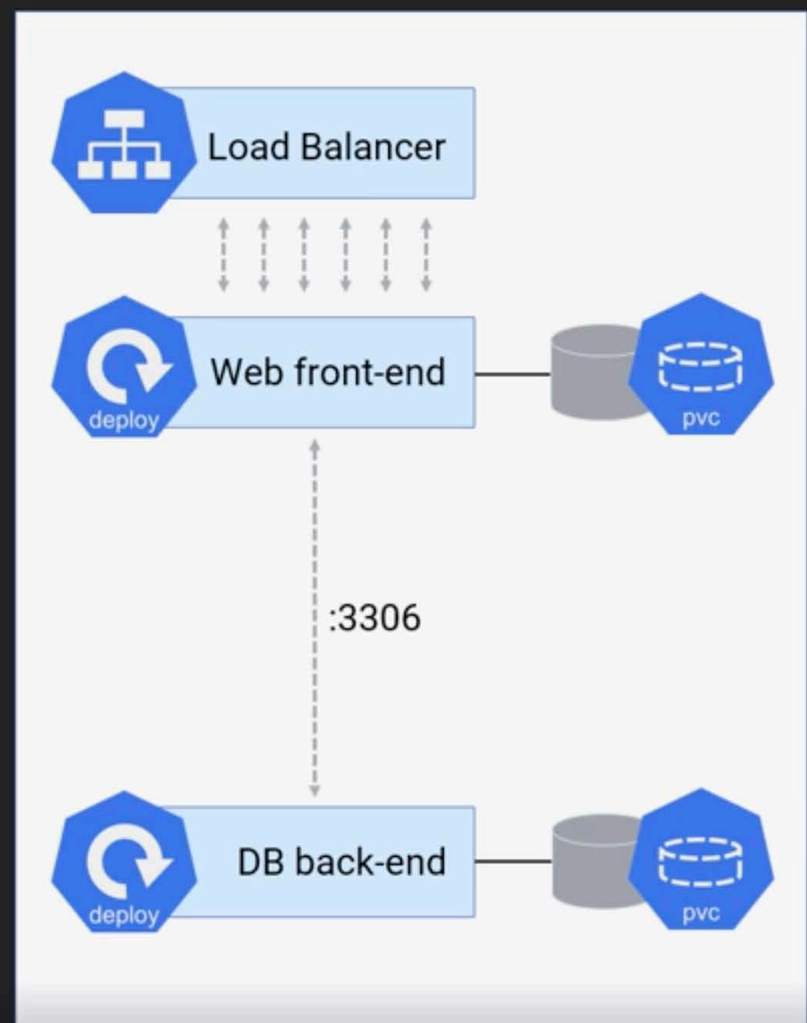
15 15 01:37 / 02:23

App Architecture

Recap

A CLOUD GURU





15 15 01:44 / 02:23

Kubernetes Networking

A CLOUD GURU

Lesson Plan

A CLOUD GURU

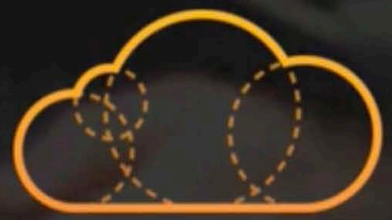
> Networking's important!
>
> Don't skip over this!

Lesson Plan

A CLOUD GURU

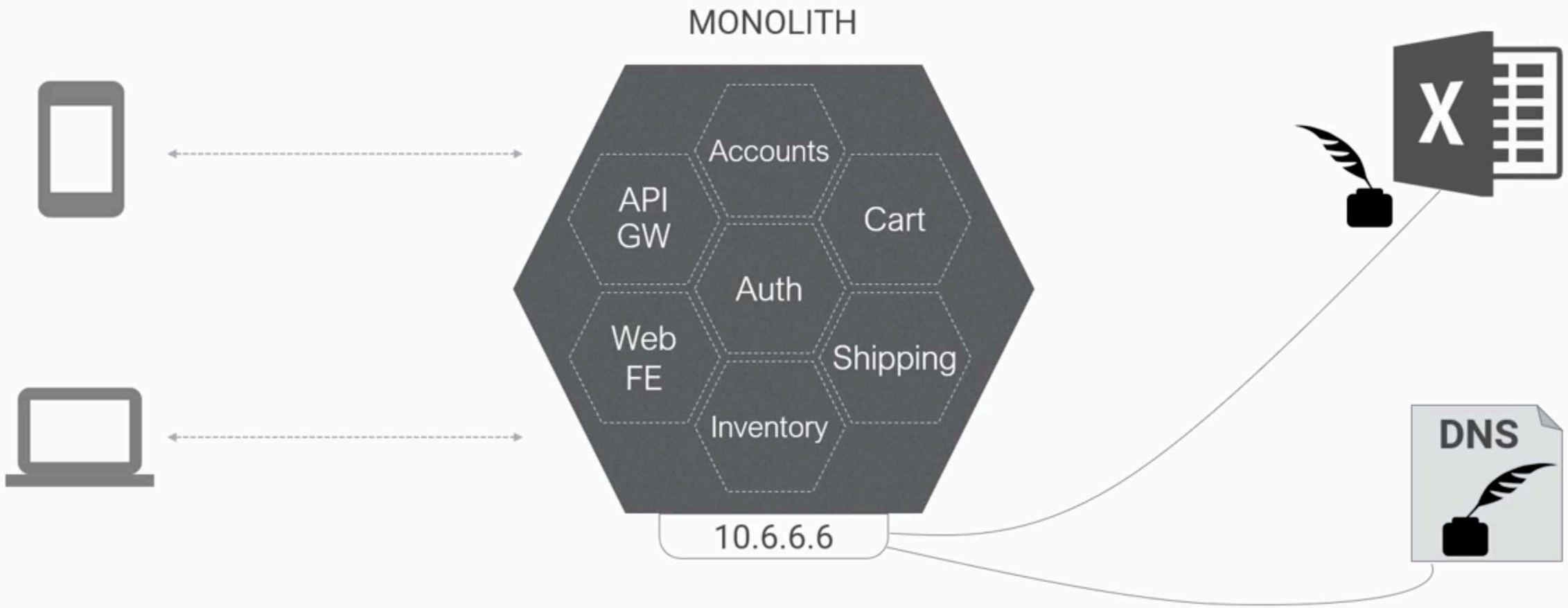
- Common Networking Requirements
- Networking in the Sample App
- Kubernetes Networking Basics
- Services
- Service Types
- The Service Network
- Lab
- Summary

Common Networking Requirements



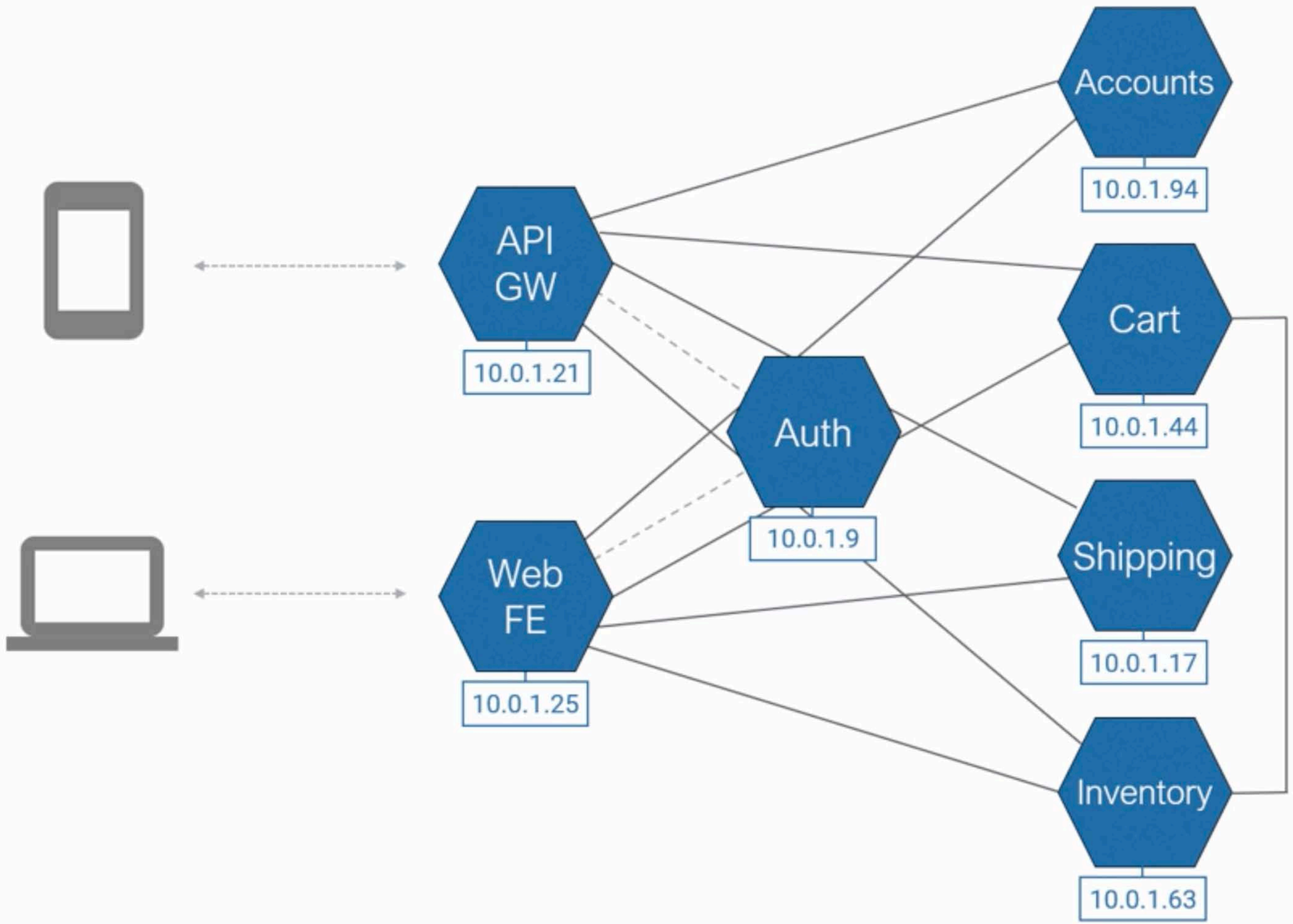
A CLOUD GURU

Common Networking Requirements

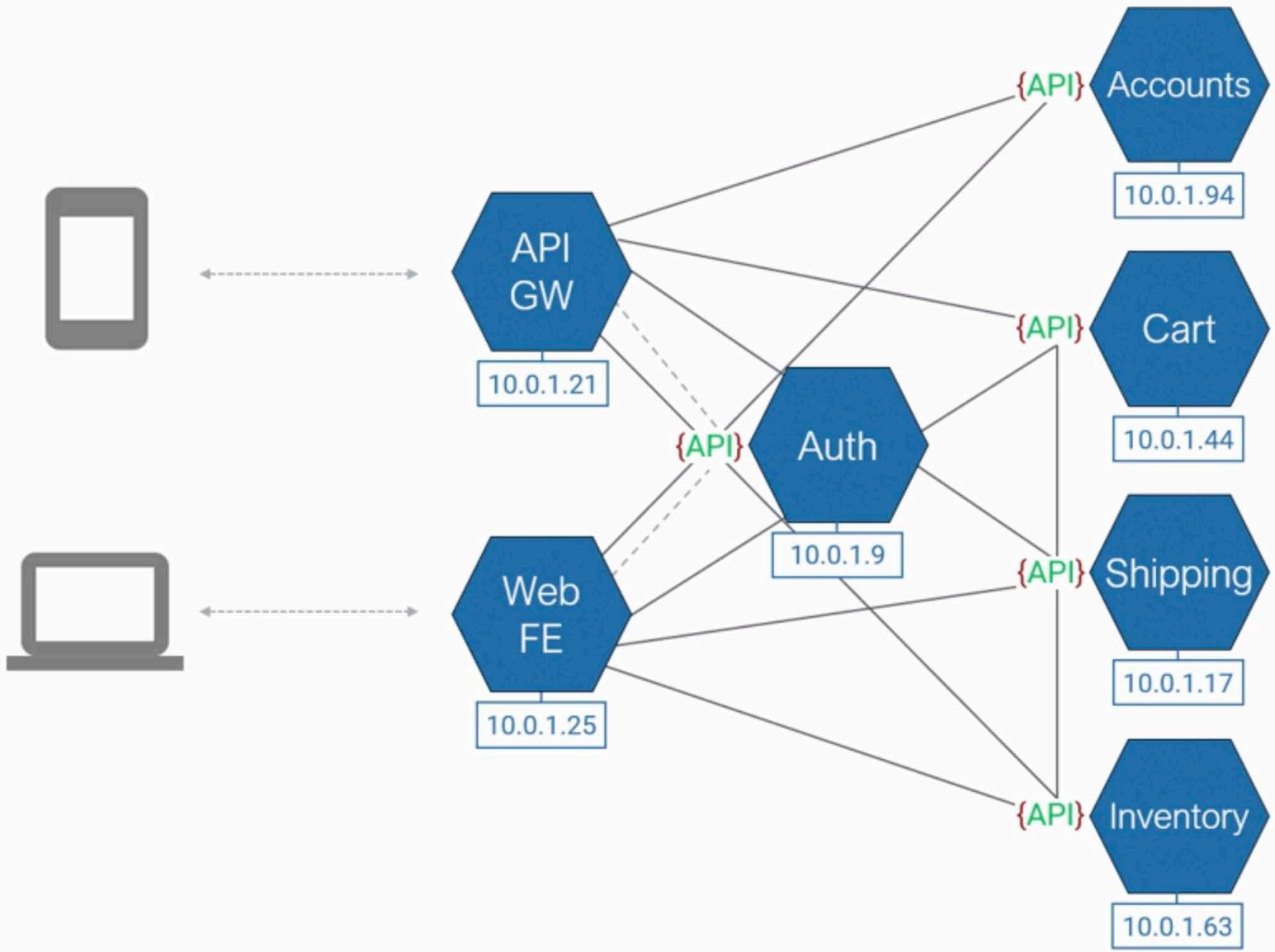


Common Networking Requirements

Common Networking Requirements



Common Networking Requirements



Common Networking Requirements

A CLOUD GURU

Highly dynamic networks are the **new normal!**

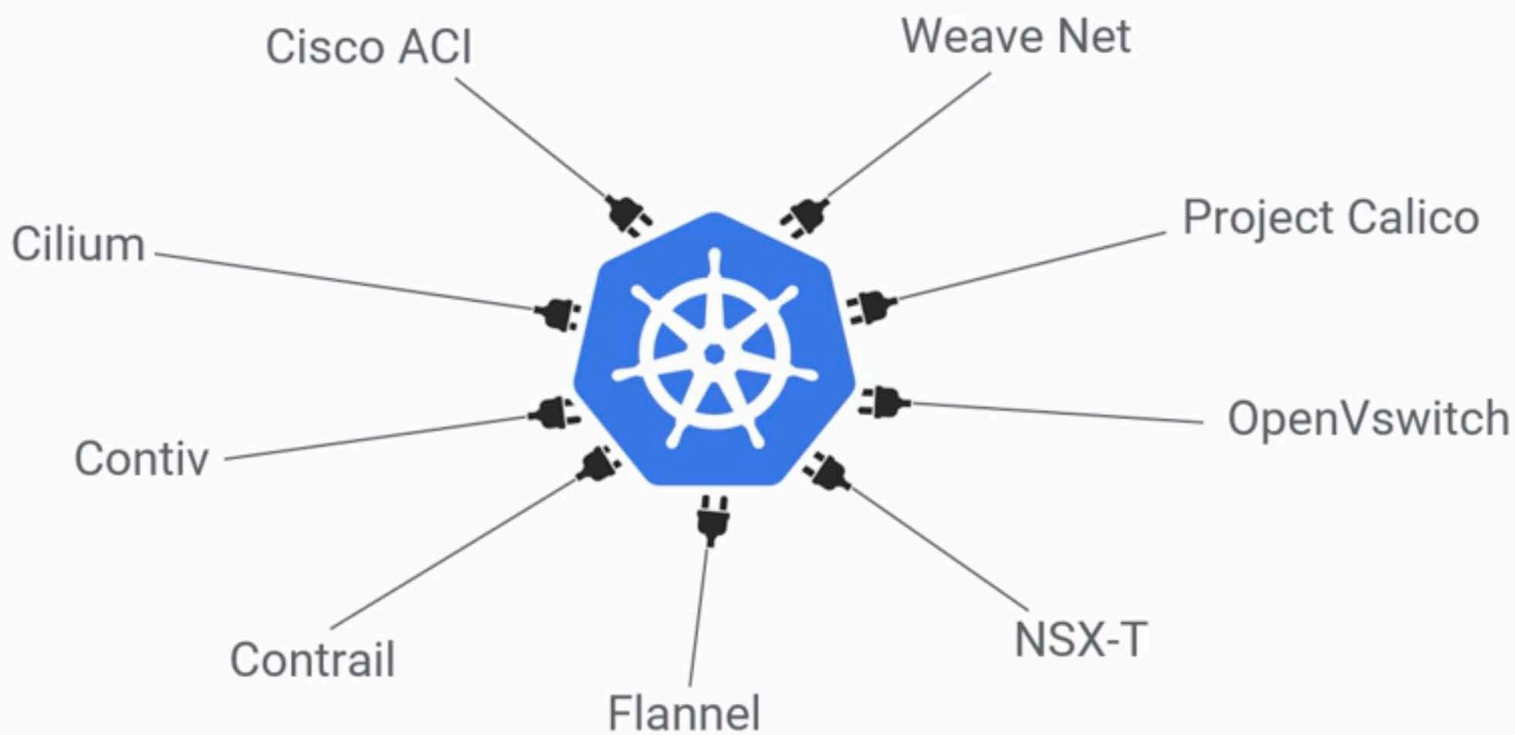
Common Networking Requirements

Highly dynamic networks are the **new normal!**

Common Networking Requirements

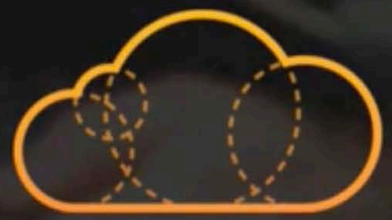
A CLOUD GURU

Highly dynamic networks are the **new normal!**



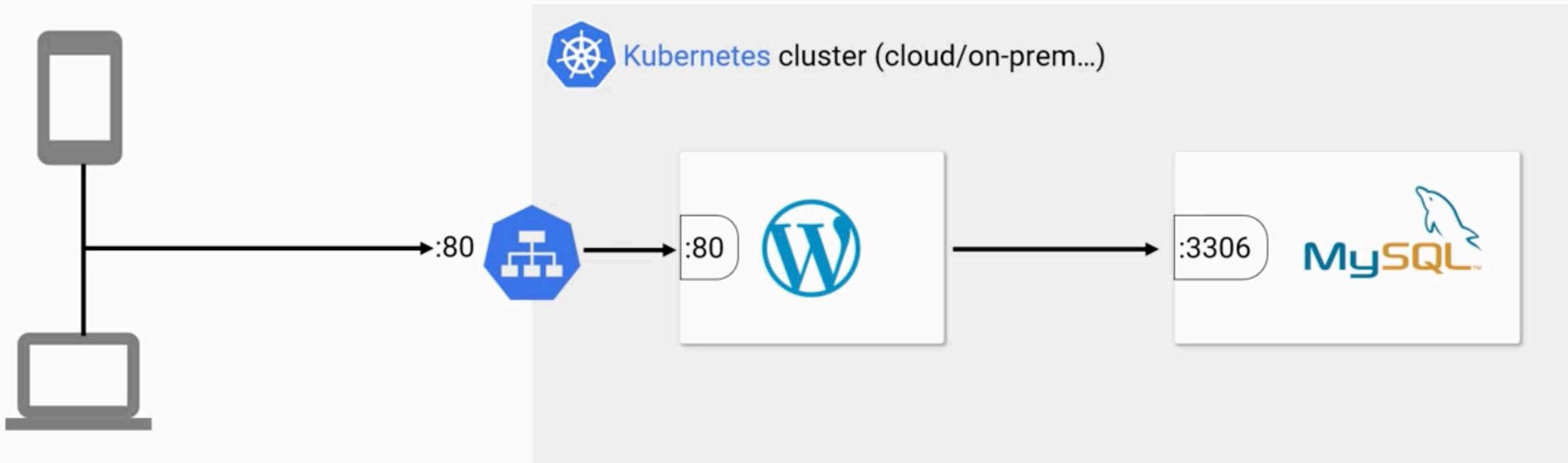
Some of the 3rd-party CNI plugins.
Others also exist.

Networking in the Sample App



A CLOUD GURU

Networking in the Sample App



Kubernetes application example tutorials

Edit

Add topics

1,840 commits | 2 branches | 0 releases | 323 contributors | Apache-2.0

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

This branch is 8 commits behind kubernetes:master. Pull request Compare

k8s-ci-robot Merge pull request #232 from adelton/create_psp_policy ... Latest commit 90145b4 on 24 May

cassandra	Merge pull request #201 from aledbf/docker	3 months ago
guestbook-go	[guestbook-go] Use multi-stage build (#211)	4 months ago
guestbook	update all Deployment API version to apps/v1 in k8s v1.9.0 and add ac...	5 months ago
mysql-wordpress-pd	add missing comment (#195)	5 months ago
staging	Creation of PSP by hack/local-up-cluster.sh is not as automatic as th...	2 months ago
.gitignore	We do not have a git ignore, modified version from core	a year ago
LICENSE	Initial commit	a year ago
OWNERS	Update owners for k/examples (#203)	4 months ago
README.md	Fix broken cassandra link in README	a year ago
code-of-conduct.md	Add code-of-conduct.md (#161)	7 months ago

github.com/nigelpoulton/k8s-sample-apps/tree/master/mysql-wordpress-pd

Search or jump to... / Pull requests Issues Marketplace Explore

nigelpoulton / k8s-sample-apps
forked from kubernetes/examples

Unwatch 1 | Star 0 | Fork 649

Code | Pull requests 0 | Projects 0 | Wiki | Insights | Settings

Branch: master | k8s-sample-apps / mysql-wordpress-pd / | Create new file | Upload files | Find file | History

This branch is 8 commits behind kubernetes:master. Pull request Compare

jheyduk and ahmetb add missing comment (#195) Latest commit 173927b on 12 Feb

..

OWNERS	Move maintained examples to root, update README	a year ago
README.md	Redirect tutorials to the docs site (#85)	10 months ago
WordPress.png	Move maintained examples to root, update README	a year ago
gce-volumes.yaml	Move maintained examples to root, update README	a year ago
local-volumes.yaml	Move maintained examples to root, update README	a year ago
mysql-deployment.yaml	add missing comment (#195)	5 months ago
wordpress-deployment.yaml	update all Deployment API version to apps/v1 in k8s v1.9.0 and add ac...	5 months ago

github.com/nigelpoulton/k8s-sample-apps/.../wordpress-deployment.yaml

```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: wp-pv-claim
  labels:
    app: wordpress
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 20Gi
---
apiVersion: apps/v1 #  for k8s versions before 1.9.0 use apps/v1beta2  and before 1.8.0 use extensions/v1beta1
```

Chrome File Edit View History Bookmarks Profiles Tab Window Help Tue Aug 17 9:43 AM

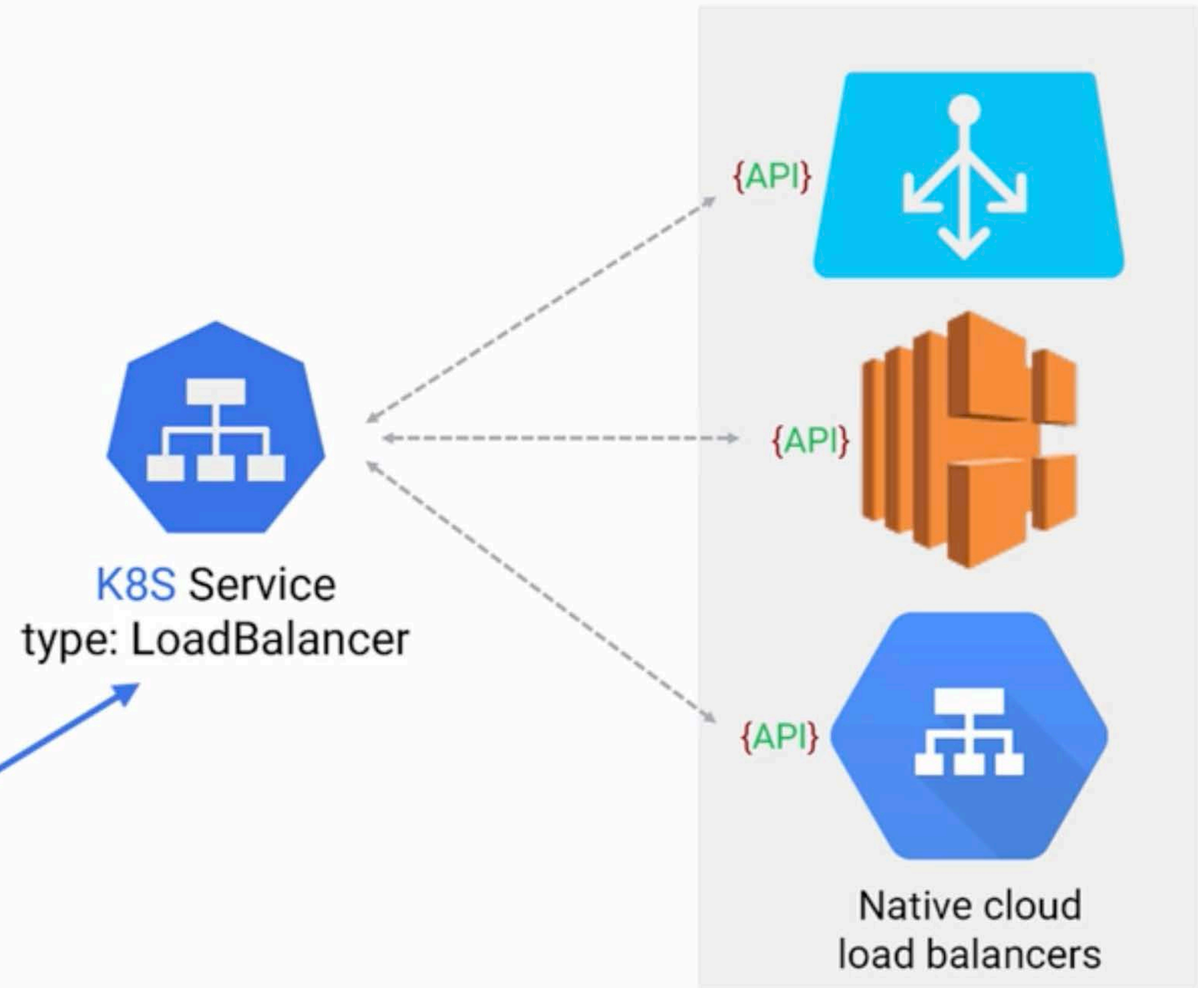
```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```

```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```

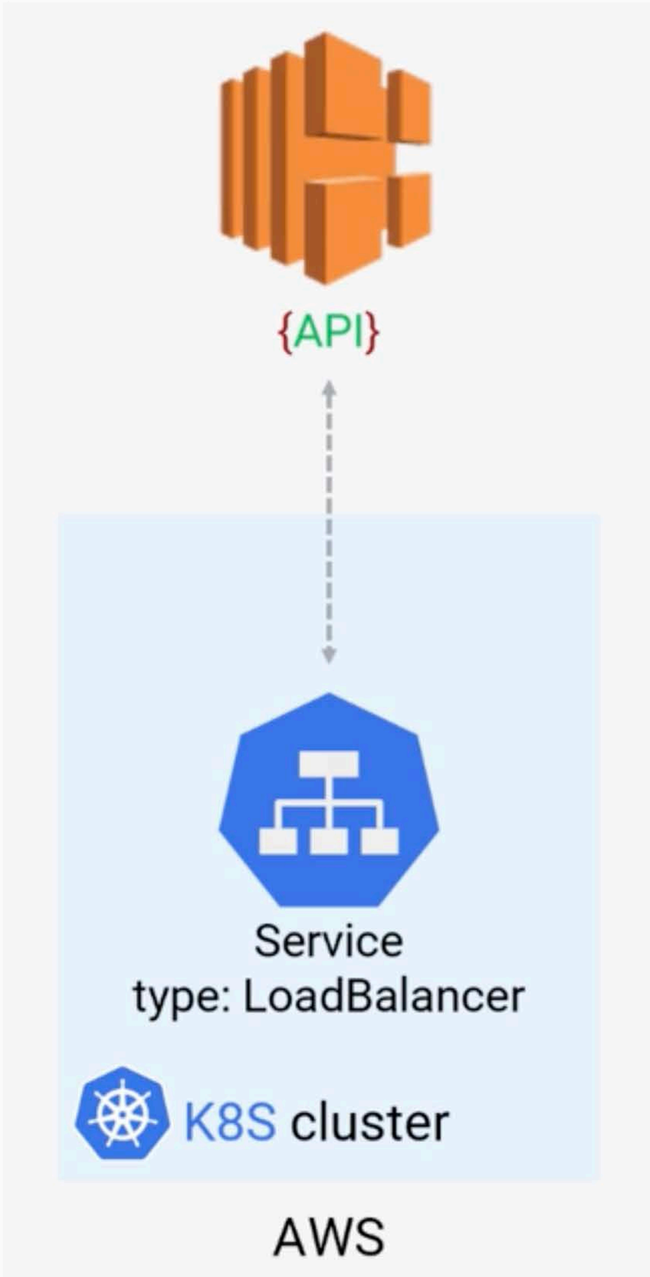
```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```

CoreDNS

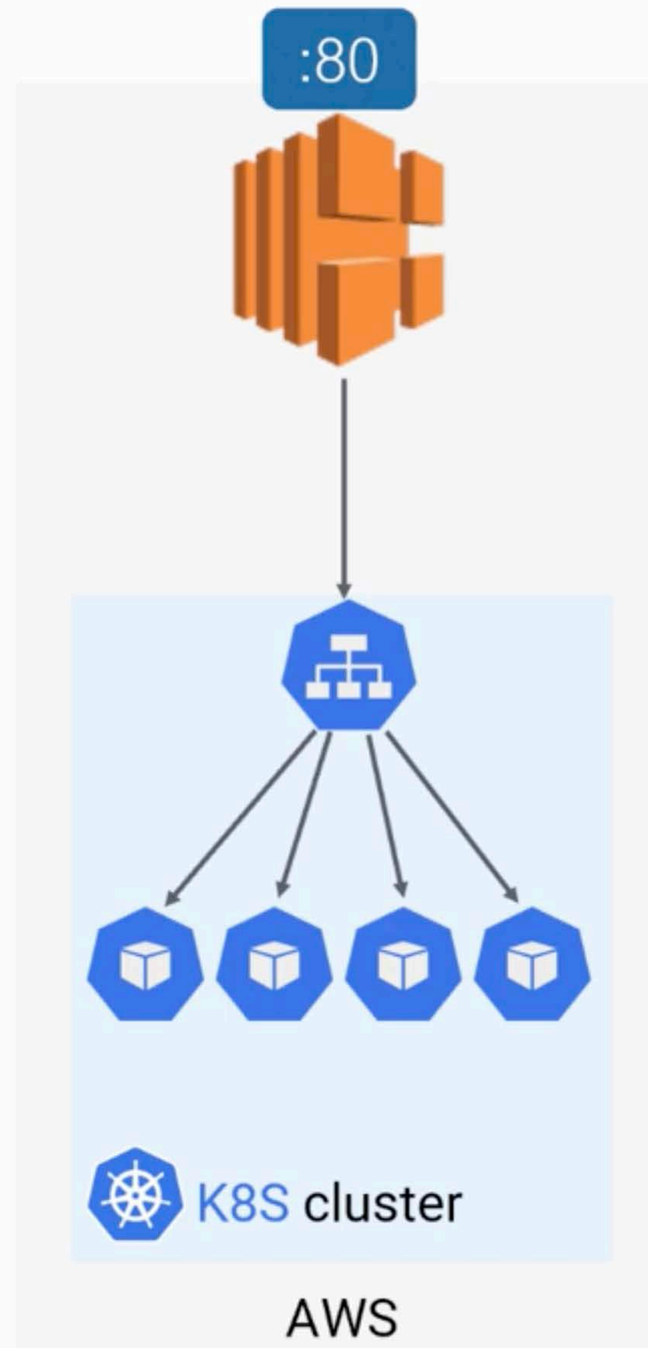
```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```



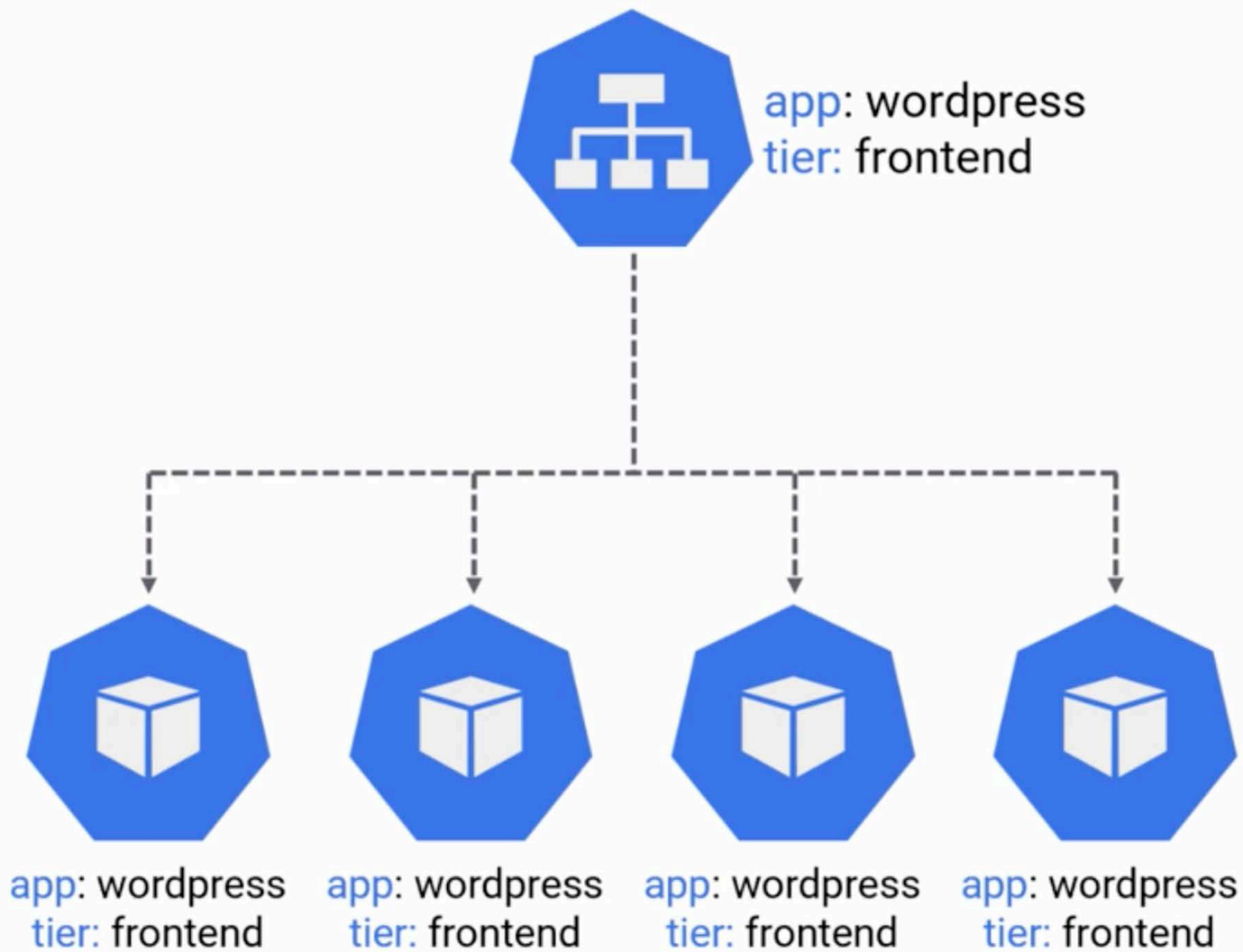
```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```



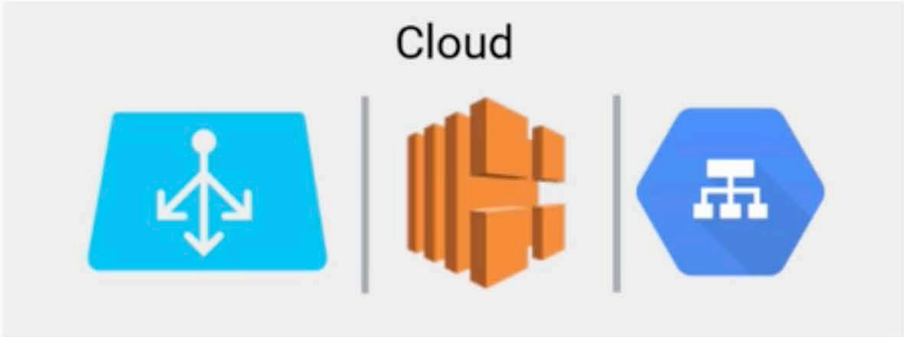
```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
```

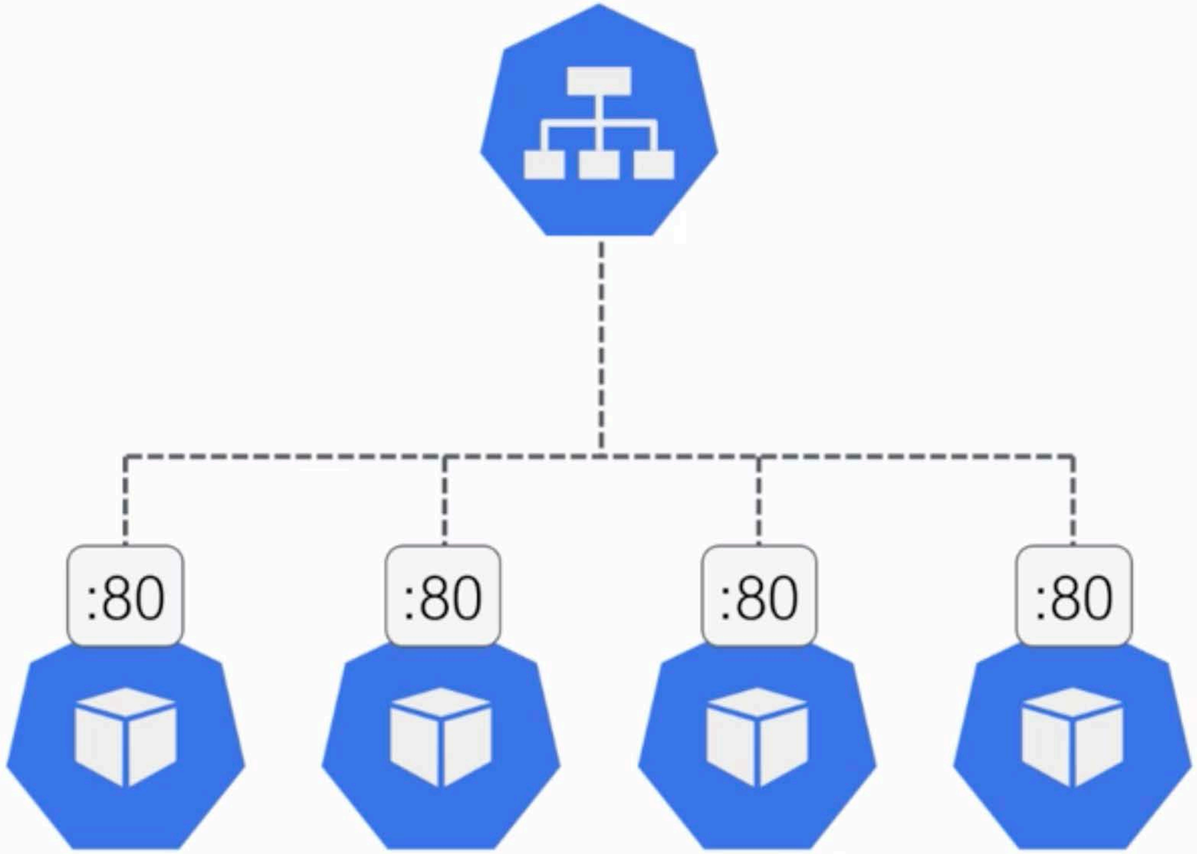


```yaml
apiVersion: apps/v1 #  for k8s versions before 1.9.0 use apps/v1beta2  and before 1.8.0 use extensions/v1beta1
kind: Deployment
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  selector:
    matchLabels:
      app: wordpress
      tier: frontend
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: wordpress
        tier: frontend
    spec:
      containers:
      - image: wordpress:4.8-apache
        name: wordpress
        env:
```



```yaml
apiVersion: apps/v1 #  for k8s versions before 1.9.0 use apps/v1beta2  and before 1.8.0 use extensions/v1beta1
kind: Deployment
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  selector:
    matchLabels:
      app: wordpress
      tier: frontend
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: wordpress
        tier: frontend
    spec:
      containers:
      - image: wordpress:4.8-apache
        name: wordpress
        env:
```





Kubernetes Networking Basics

A CLOUD GURU

House Rules

All Nodes can talk

All Pods can talk

(No NAT)

Every Pod gets its own IP

Kubernetes Networking Basics

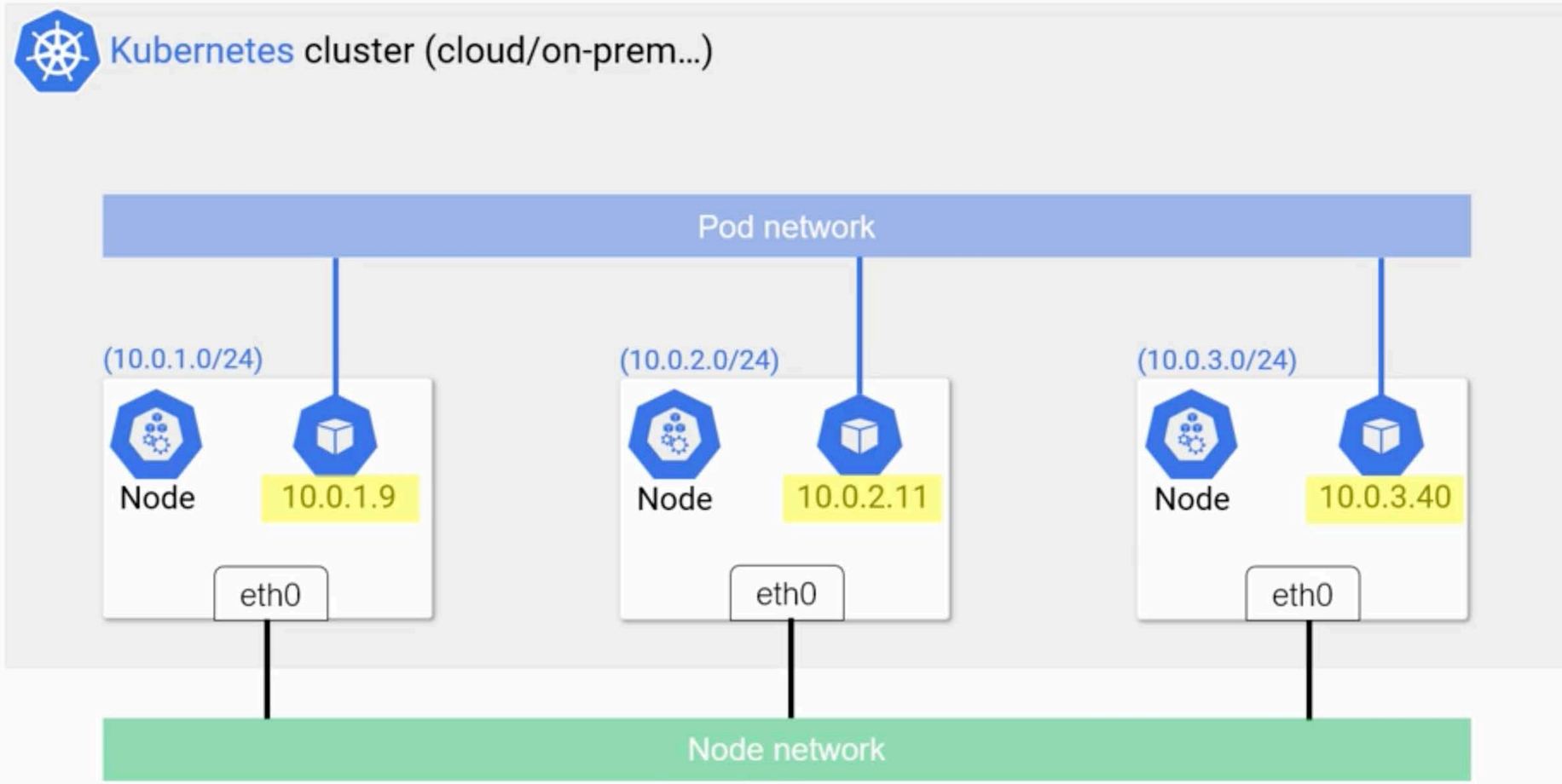
A CLOUD GURU

Pod network

CNI plugin
- Big flat network

Node network

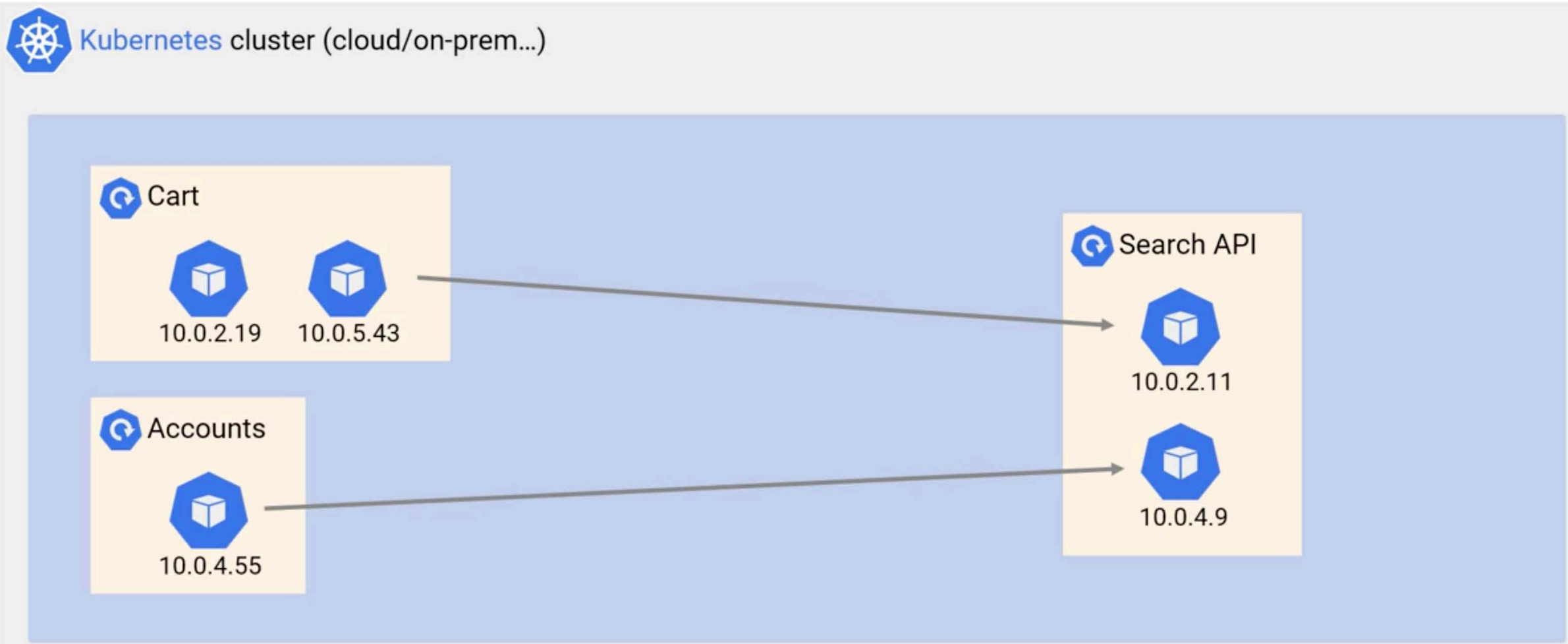
- 443 (HTTPS)
- Pod networking



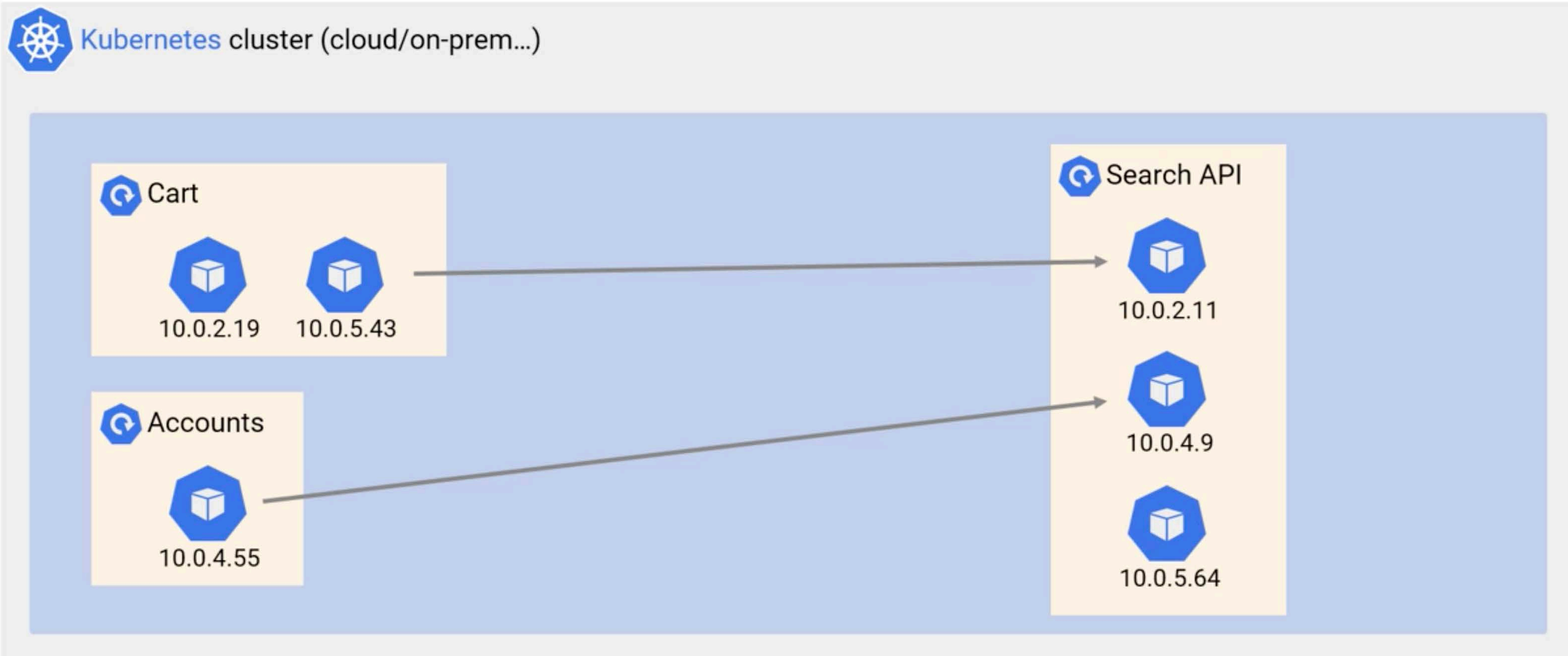
Kubernetes Services

A CLOUD GURU

Kubernetes Services

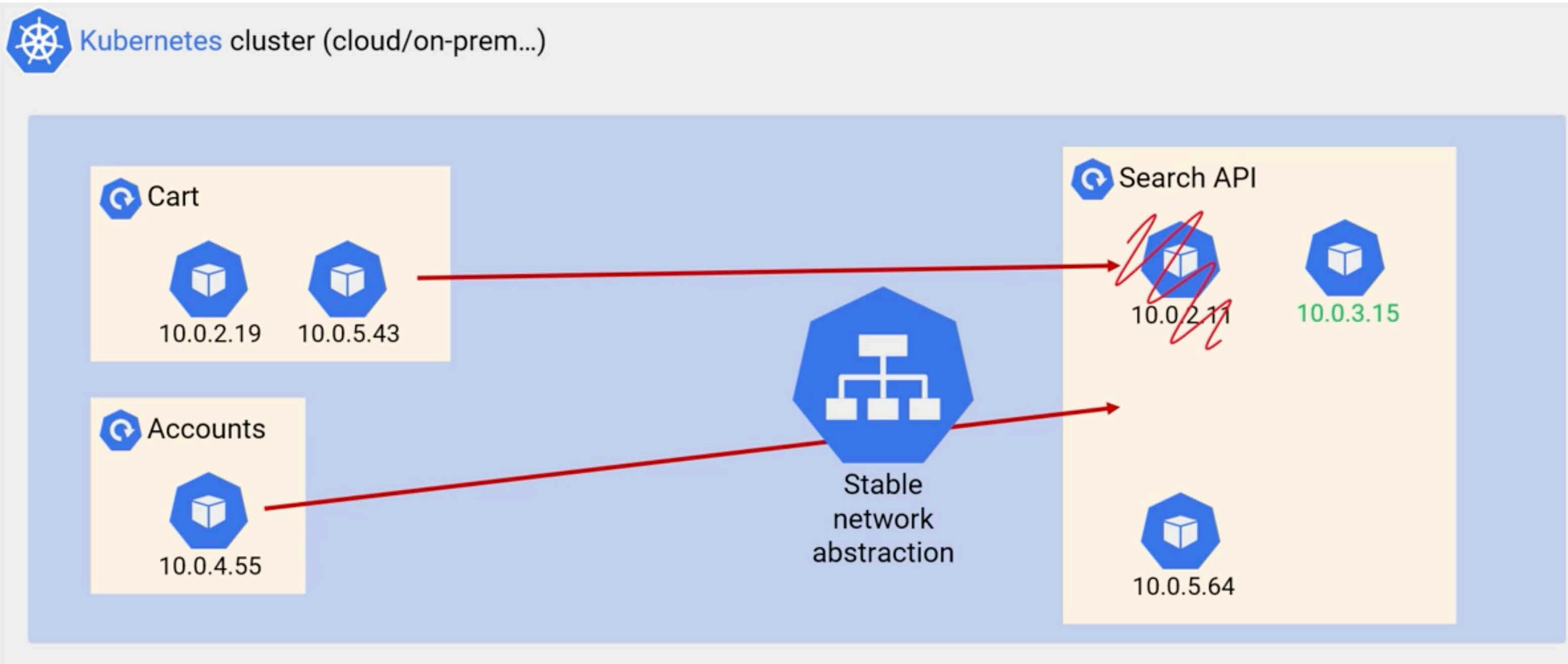


Kubernetes Services



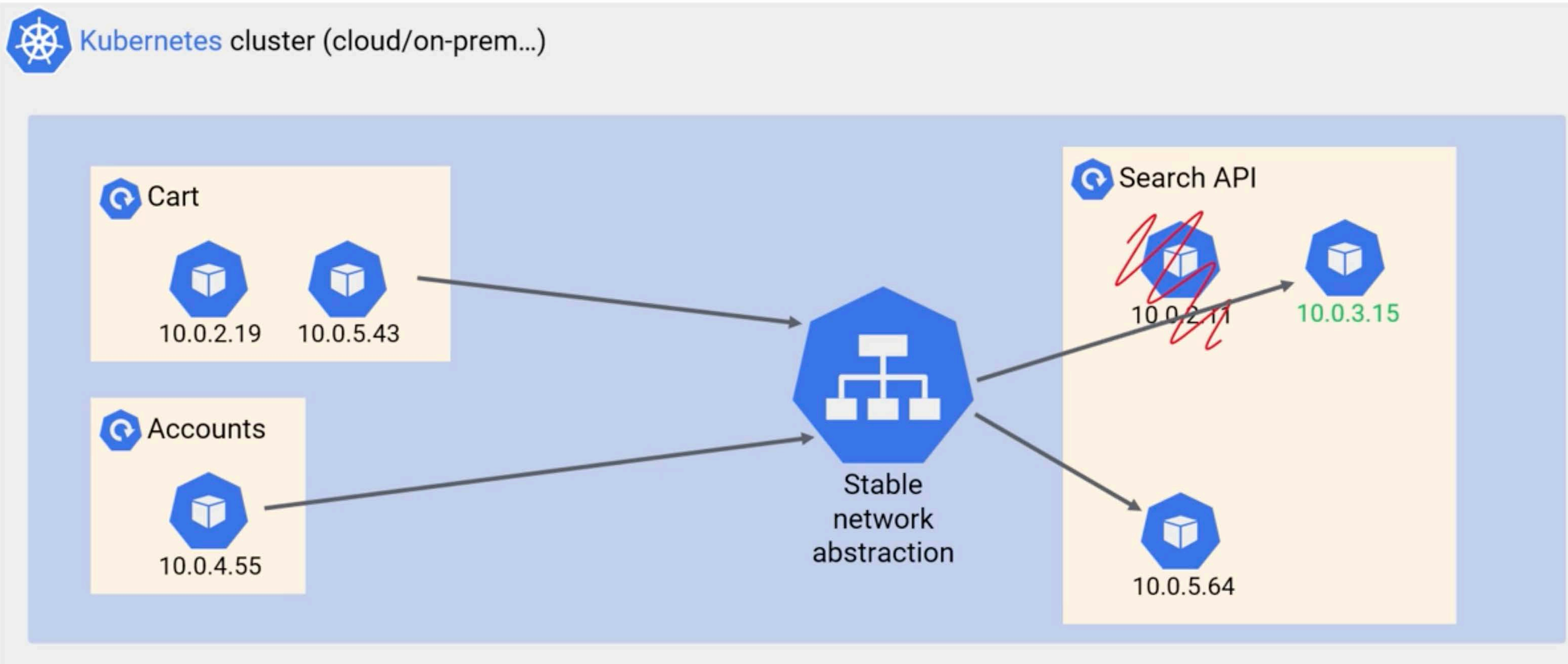
Kubernetes Services

A CLOUD GURU

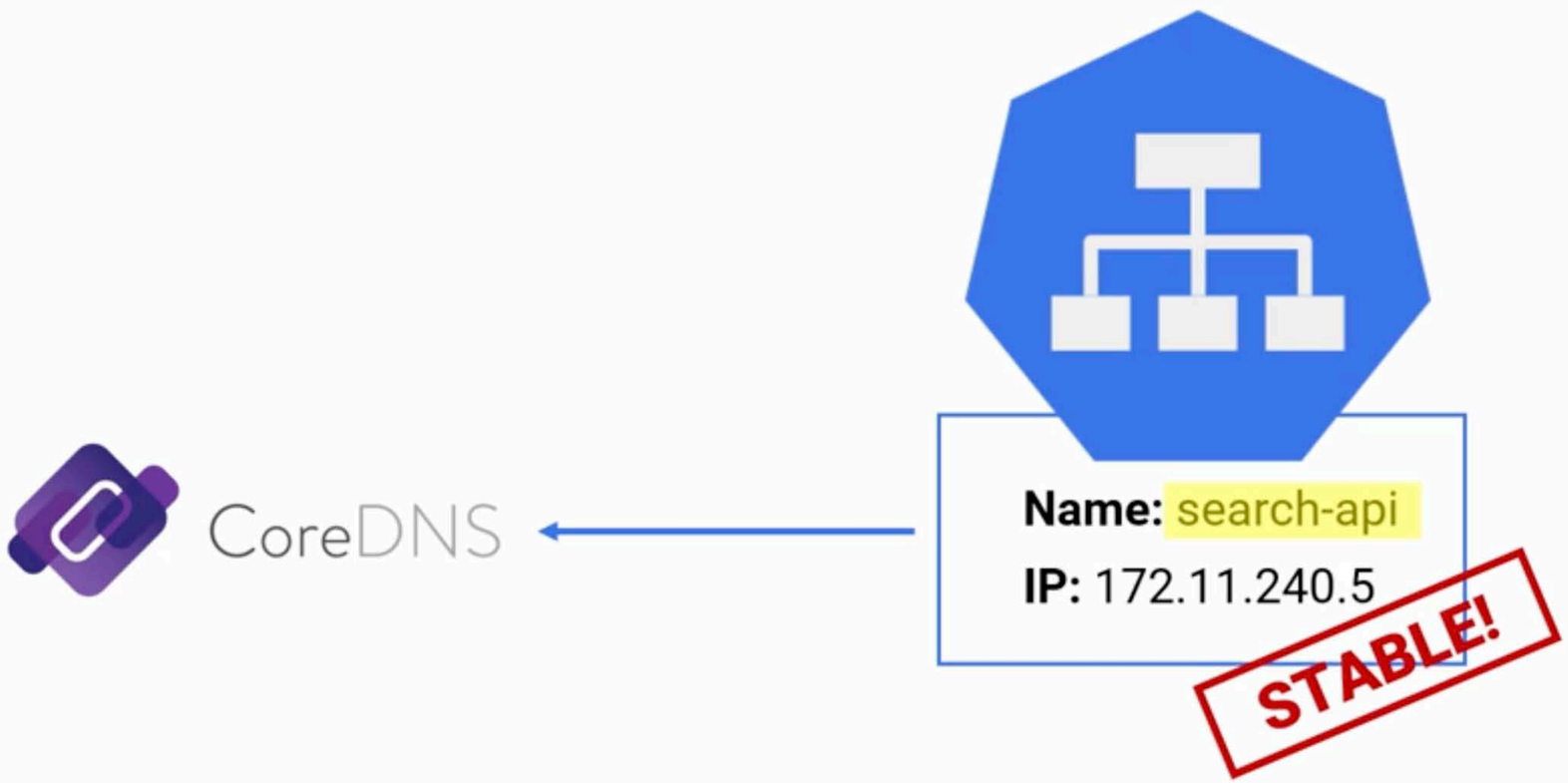


Kubernetes Services

A CLOUD GURU

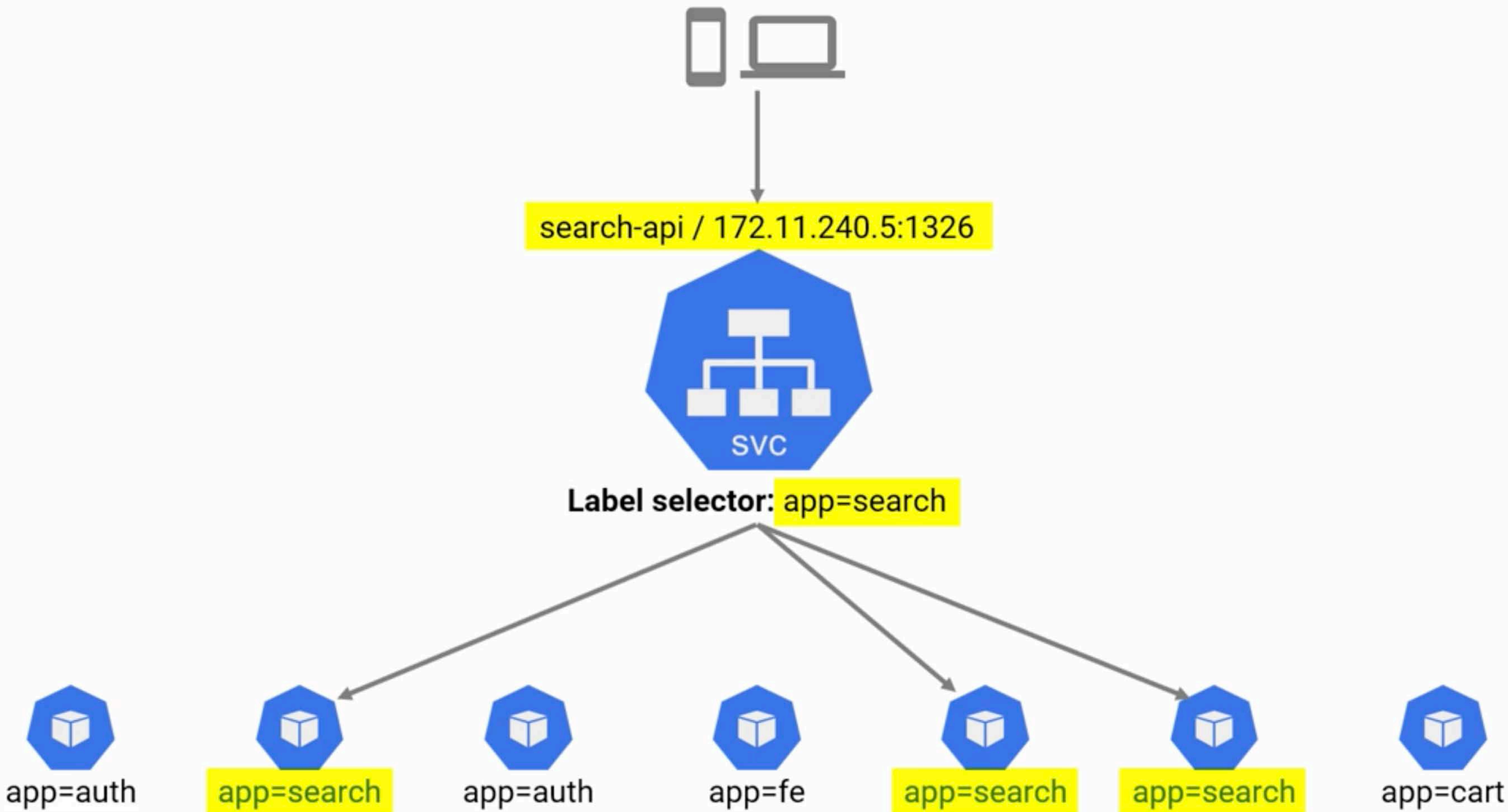


Kubernetes Services

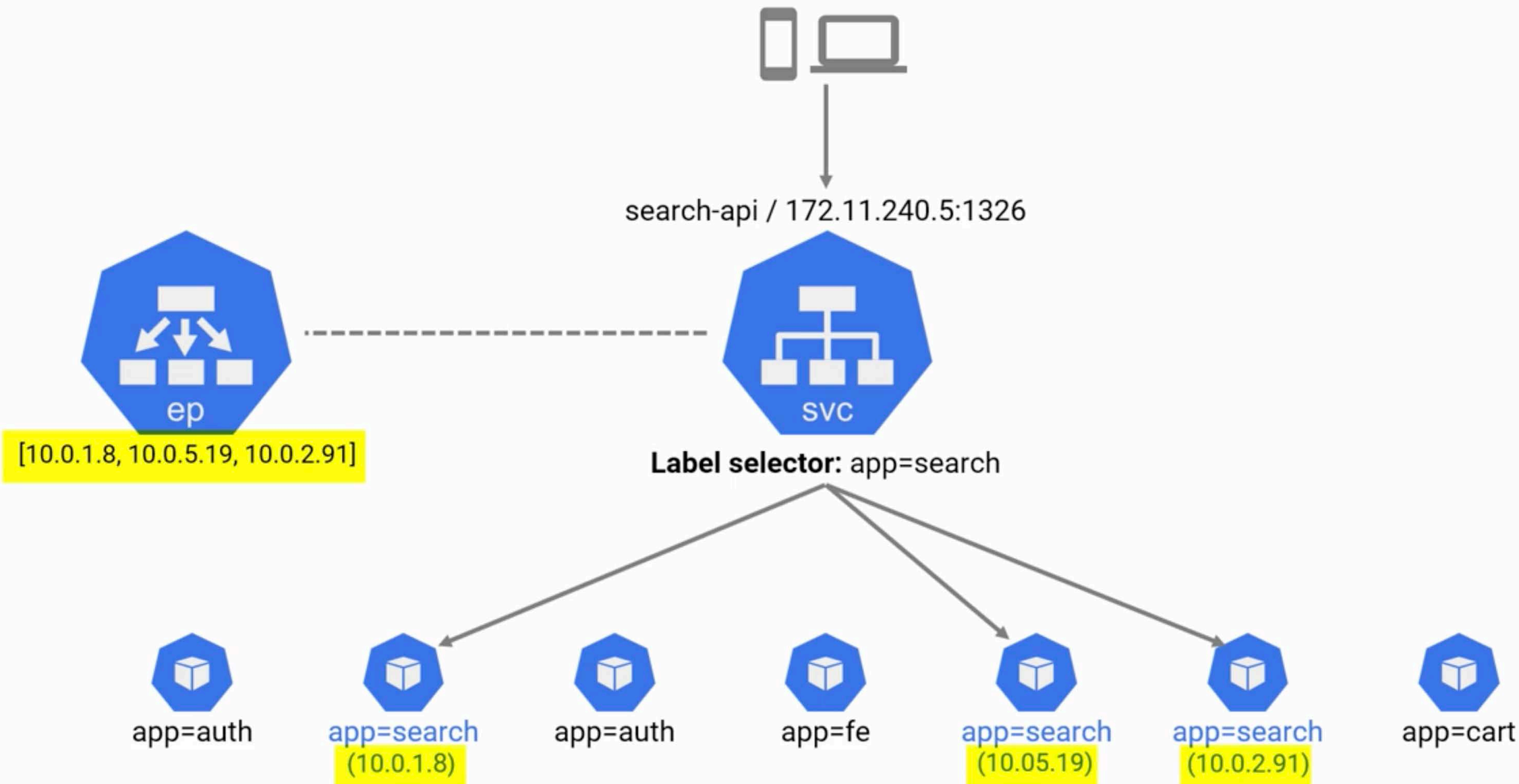


Kubernetes Services

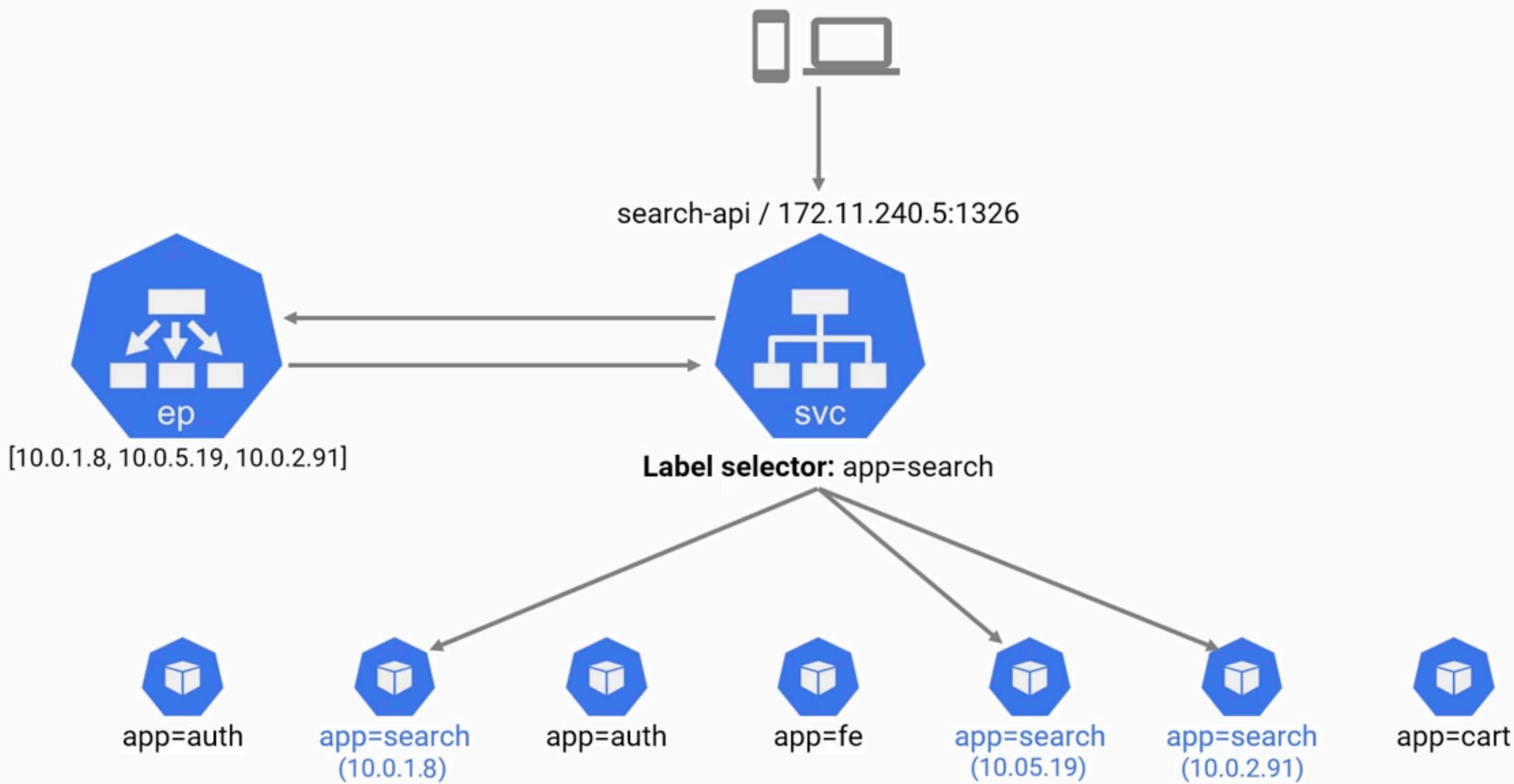
A CLOUD GURU



Kubernetes Services



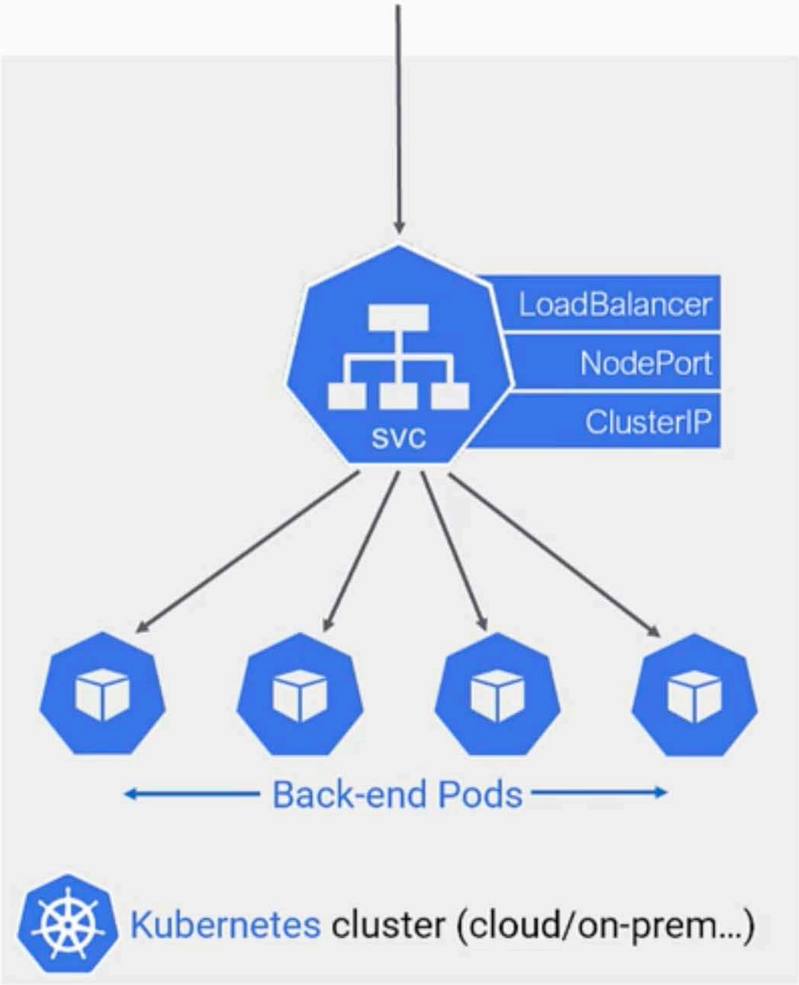
Kubernetes Services



Service Types

A CLOUD GURU

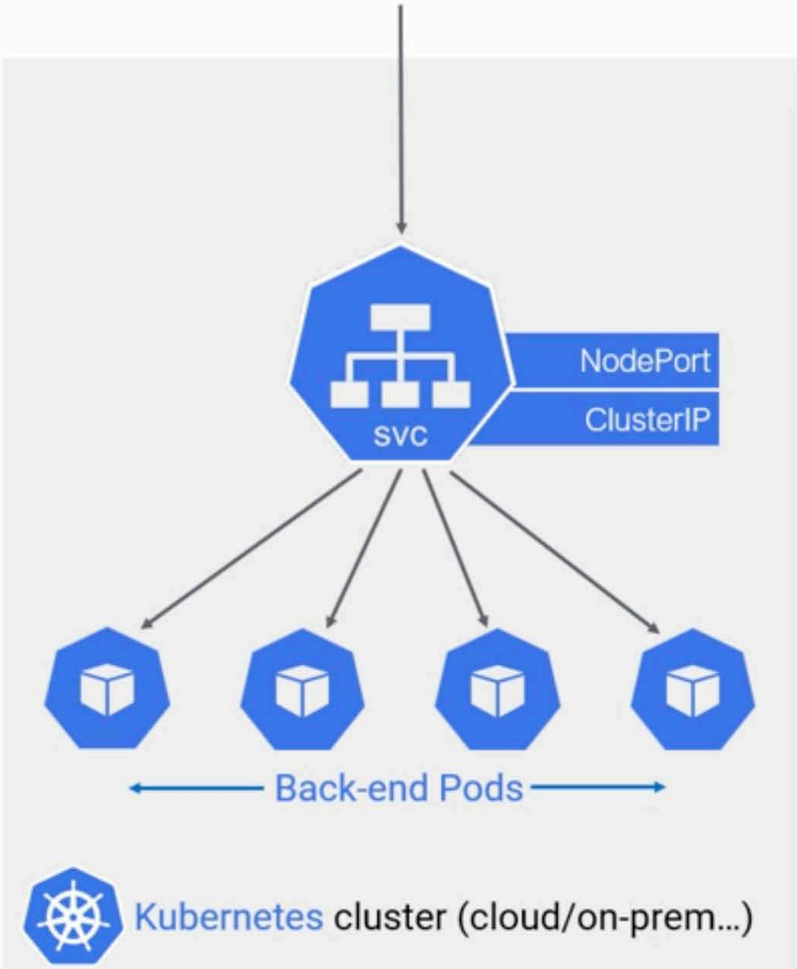
```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
---
```



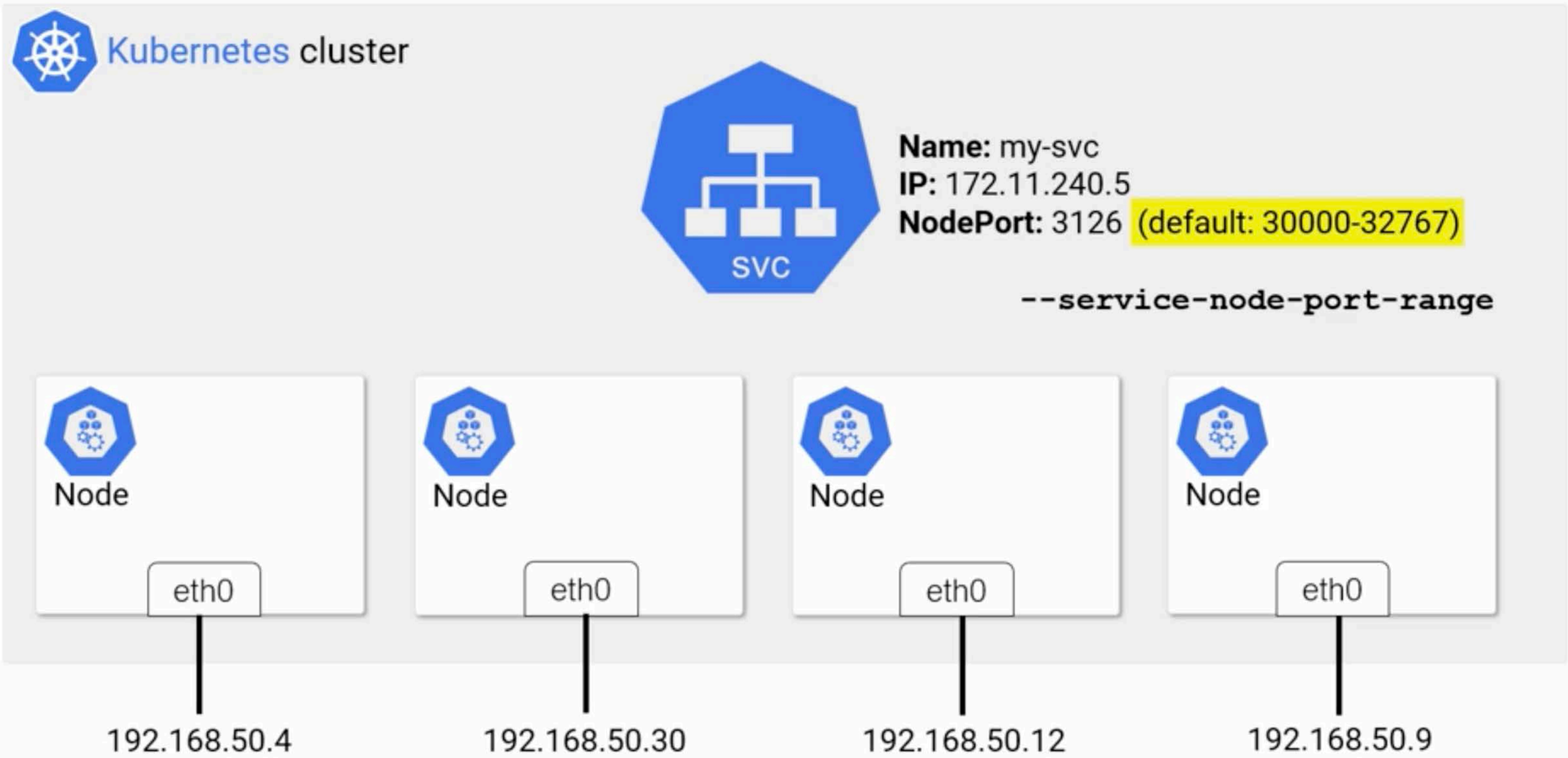
Kubernetes Services

NodePort:
- Gets cluster-wide **port**
- Also accessible from outside of cluster

ClusterIP (default):
- Gets own IP
- Only accessible from within cluster



Kubernetes Networking Basics



Welcome | nodeport.yml

```yaml
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  type: NodePort
  ports:
    - port: 80
      nodePort: 30080
  selector:
    app: wordpress
```

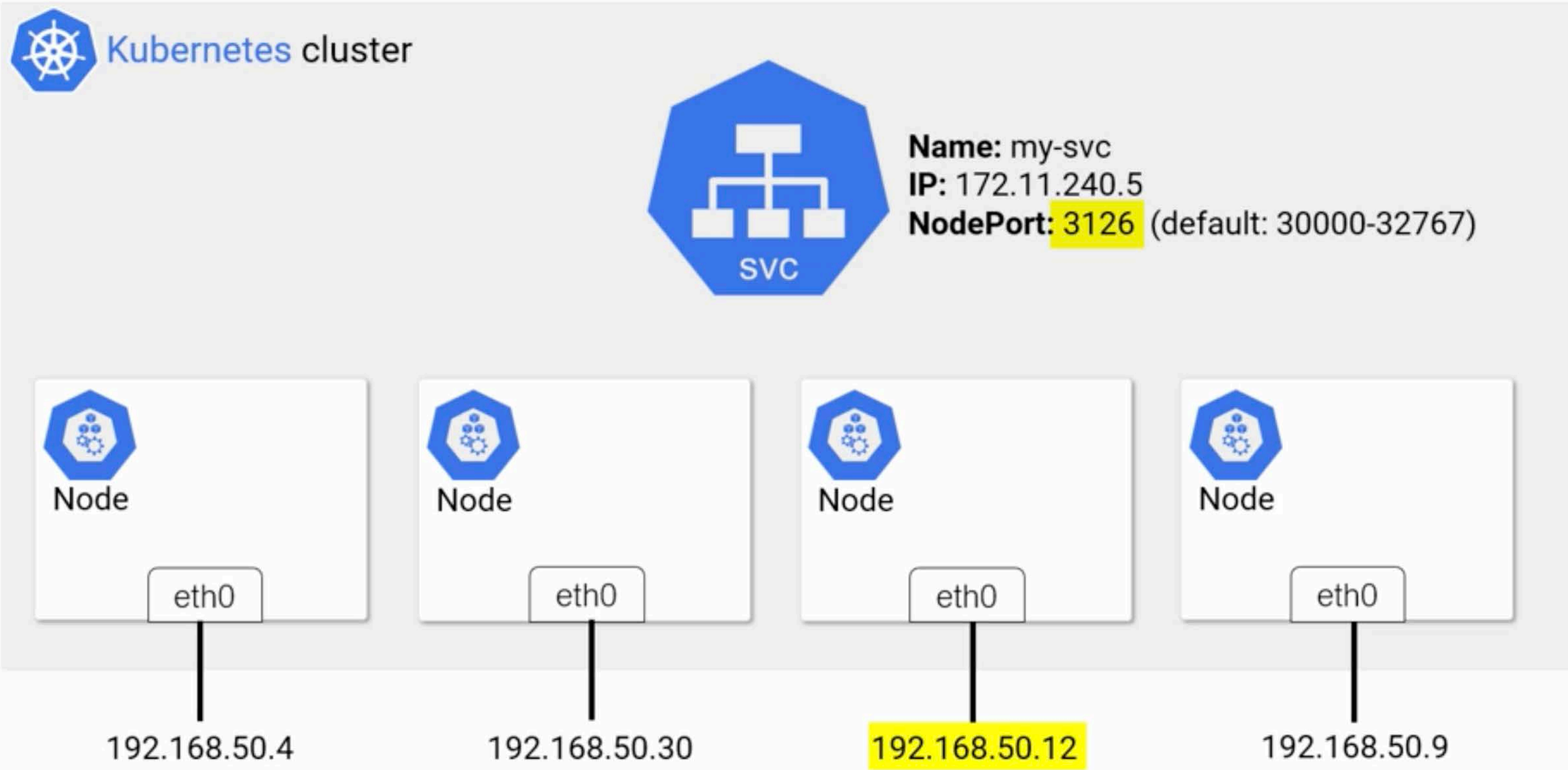
Port that the Pods are listening on

Cluster-wide port that the service listens on

0 0 | Ln 14, Col 6 | Spaces: 2 | UTF-8 | CRLF | YAML

Kubernetes Networking Basics

A CLOUD GURU

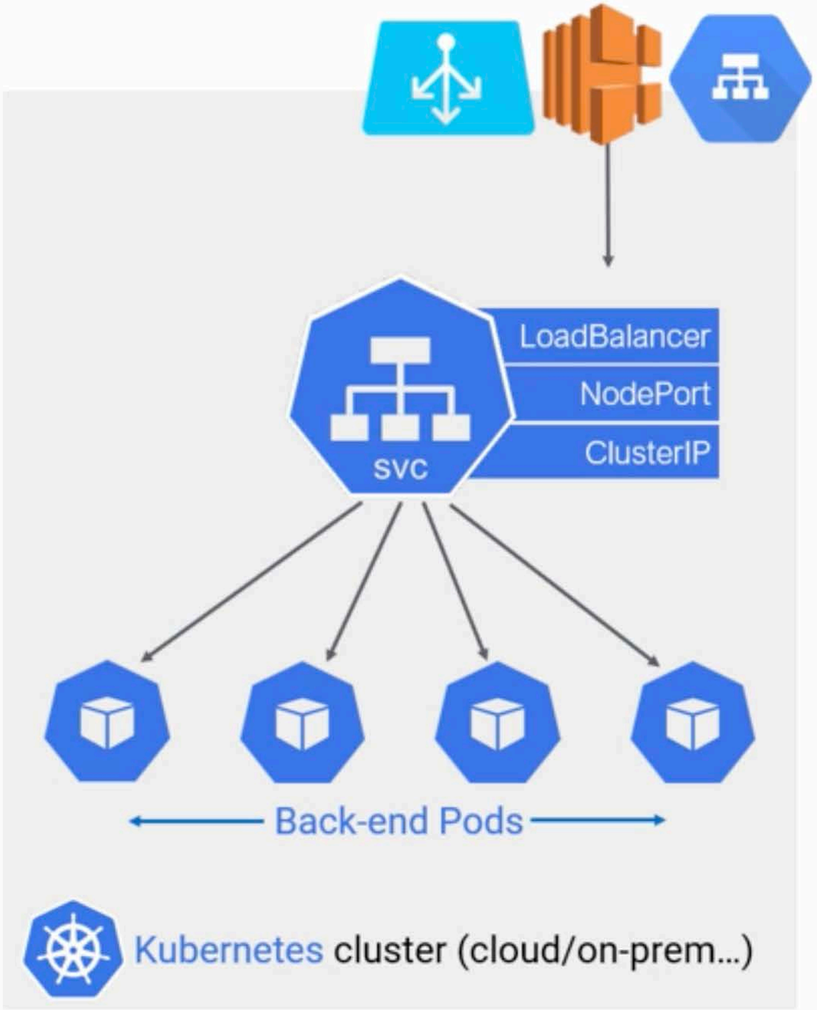


Kubernetes Services

LoadBalancer:
- Integrates with public cloud platform

NodePort:
- Gets cluster-wide **port**
- Also accessible from outside of cluster

ClusterIP (default):
- Gets own IP
- Only accessible from within cluster



The Service Network

A CLOUD GURU

Kubernetes Networking

The Service Network

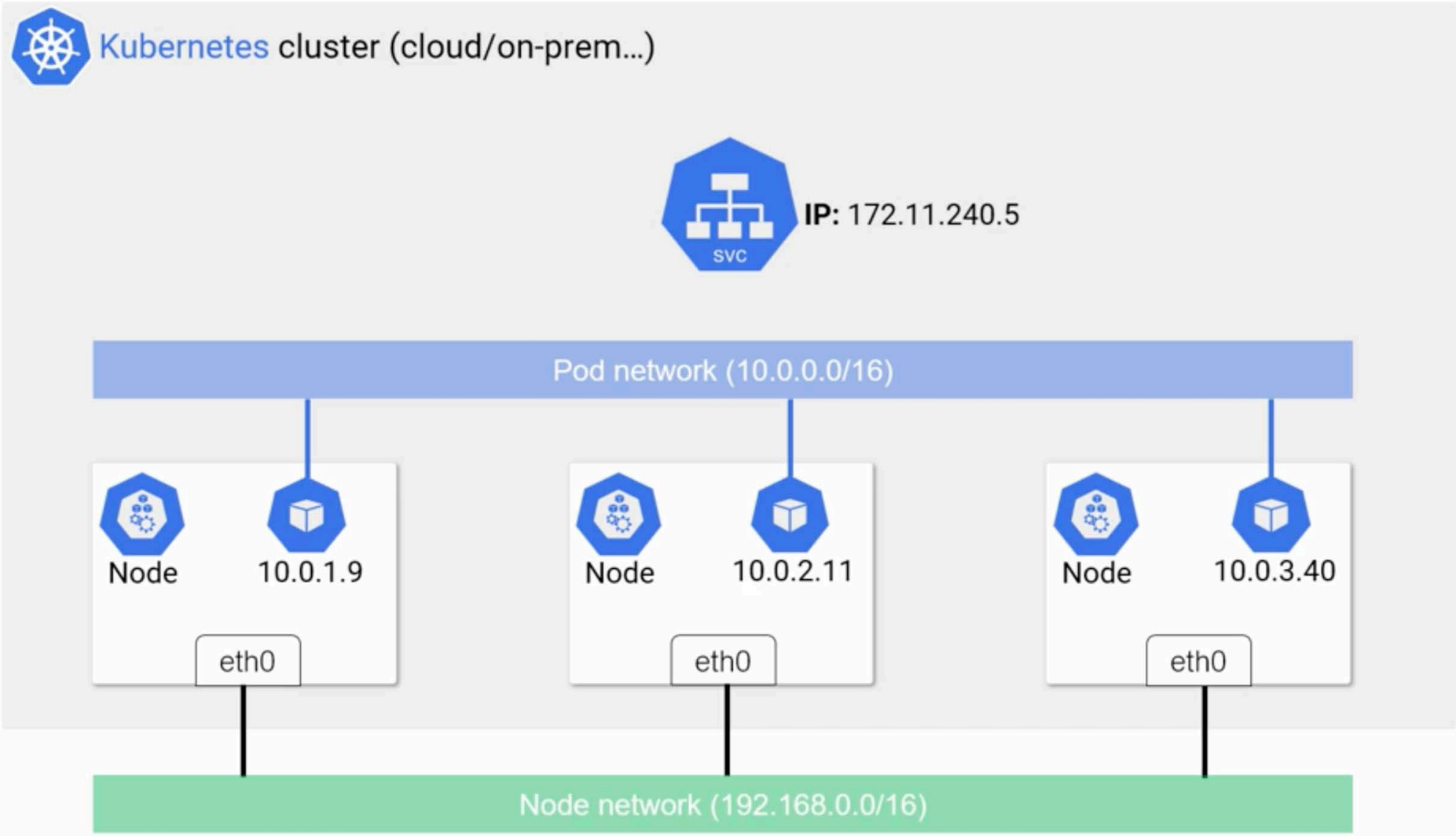
A CLOUD GURU

Pod network
- 10.0.0.0/16

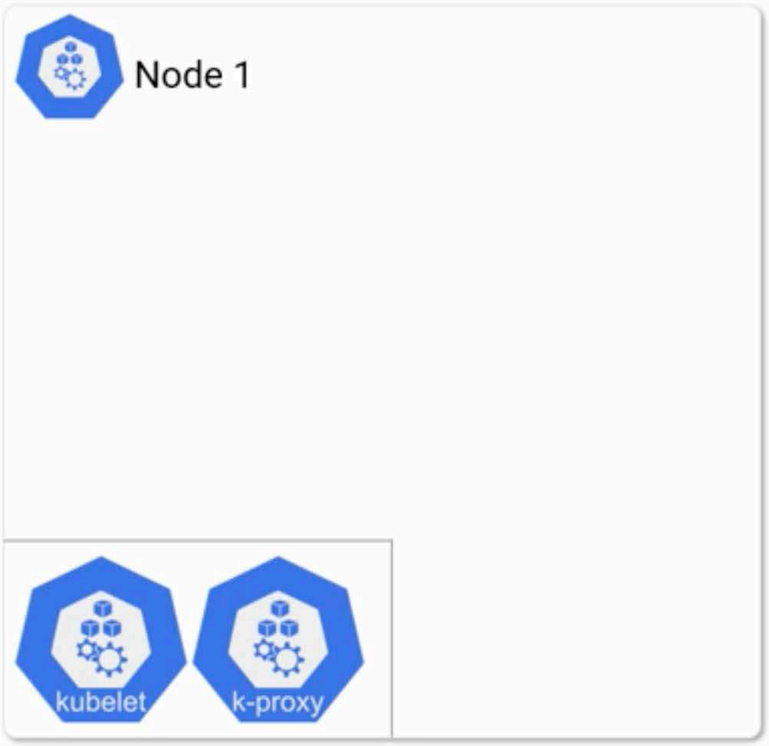
Node network
- 192.168.0.0/16

Service network
- 172.11.11.0/24

* Example network addresses for maximum clarity. Not the defaults that Kubernetes uses.



The Service ~~Network~~



"kube-proxy"

Kubernetes Networking

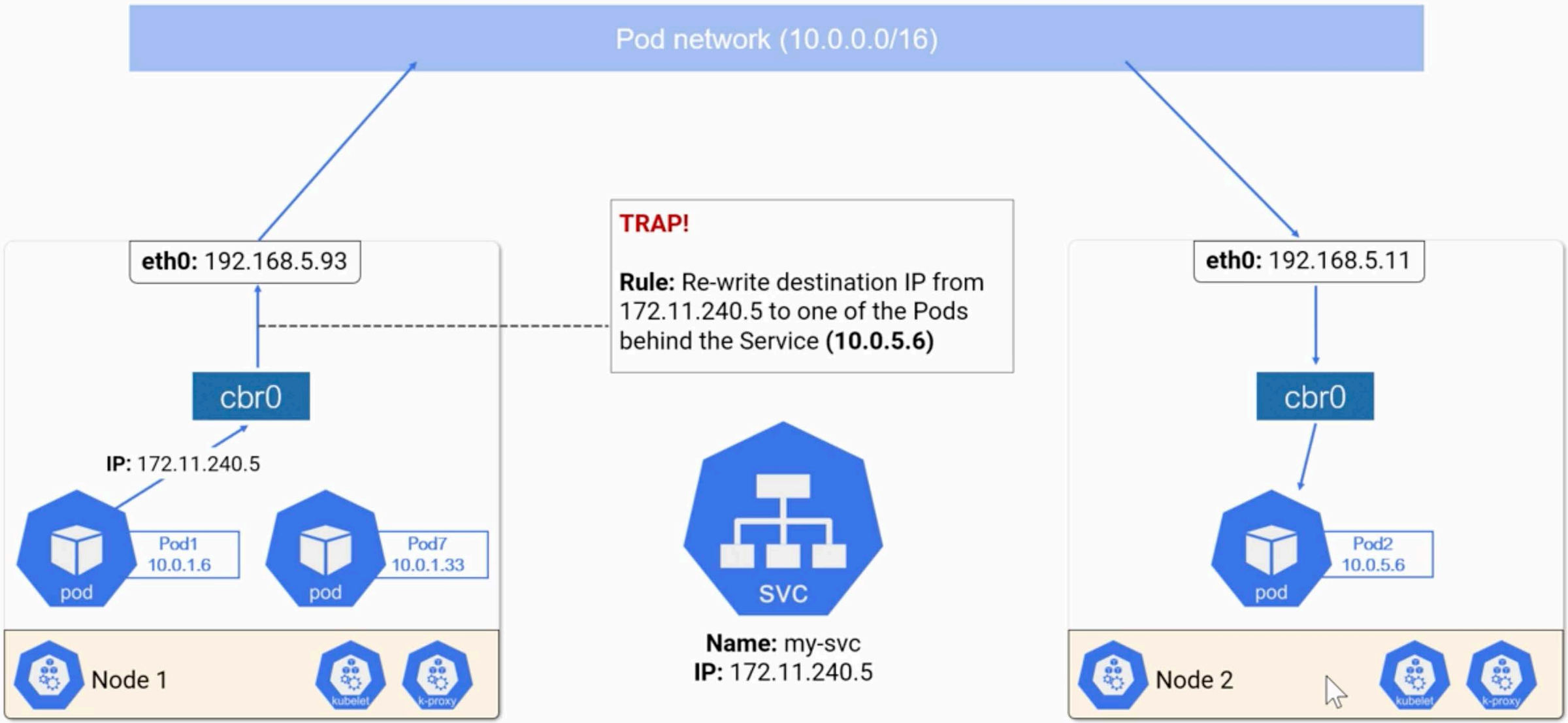
The Service Network

A CLOUD GURU

Kubernetes Networking

The Service Network

A CLOUD GURU



The Service ~~Network~~

Kube-proxy IPTABLES Mode

- Default since Kubernetes 1.2
- Doesn't scale well
- Not really designed for load balancing

Kube-proxy IPVS Mode

- Stable since Kubernetes 1.11
- Uses Linux kernel IP Virtual Server

The Service Network

Kube-proxy IPTABLES Mode

- Default since Kubernetes 1.2
- Doesn't scale well
- Not really designed for load balancing

Kube-proxy IPVS Mode

- Stable (GA) since Kubernetes 1.11
- Uses Linux kernel IP Virtual Server
- Native Layer-4 load balancer
- Supports more algorithms

Demo time!
A CLOUD GURU

Kubernetes Networking Recap

A CLOUD GURU

Recap

A CLOUD GURU

Node Network

All nodes need to be able to talk
- Kubelet ⟷ API Server
- Pod network ports

Not implemented by Kubernetes

Pod Network

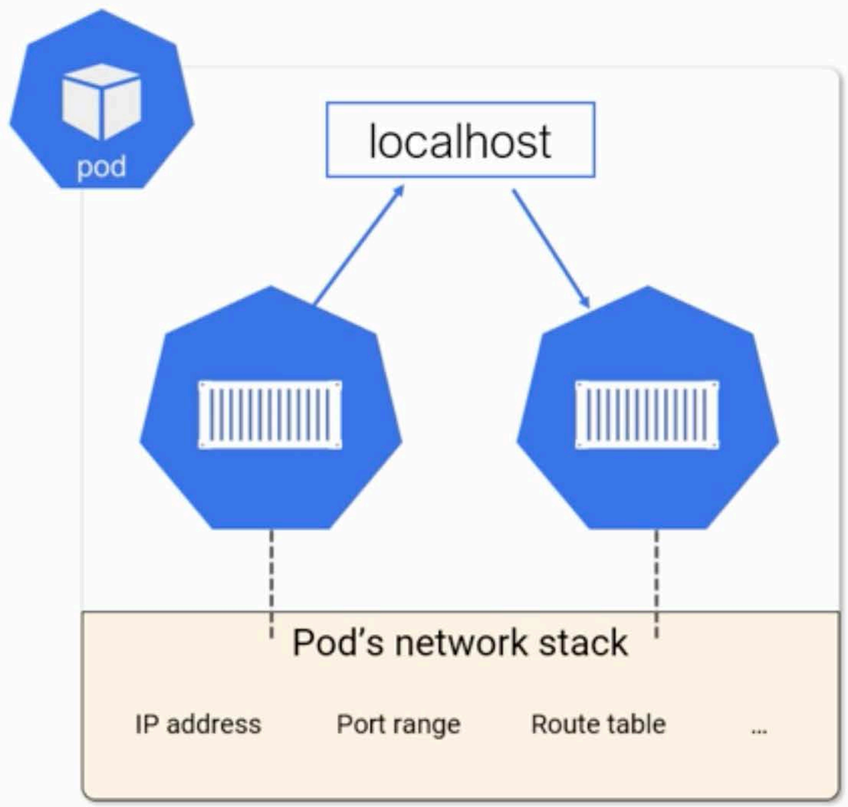
Implemented via CNI plugins

Big & flat

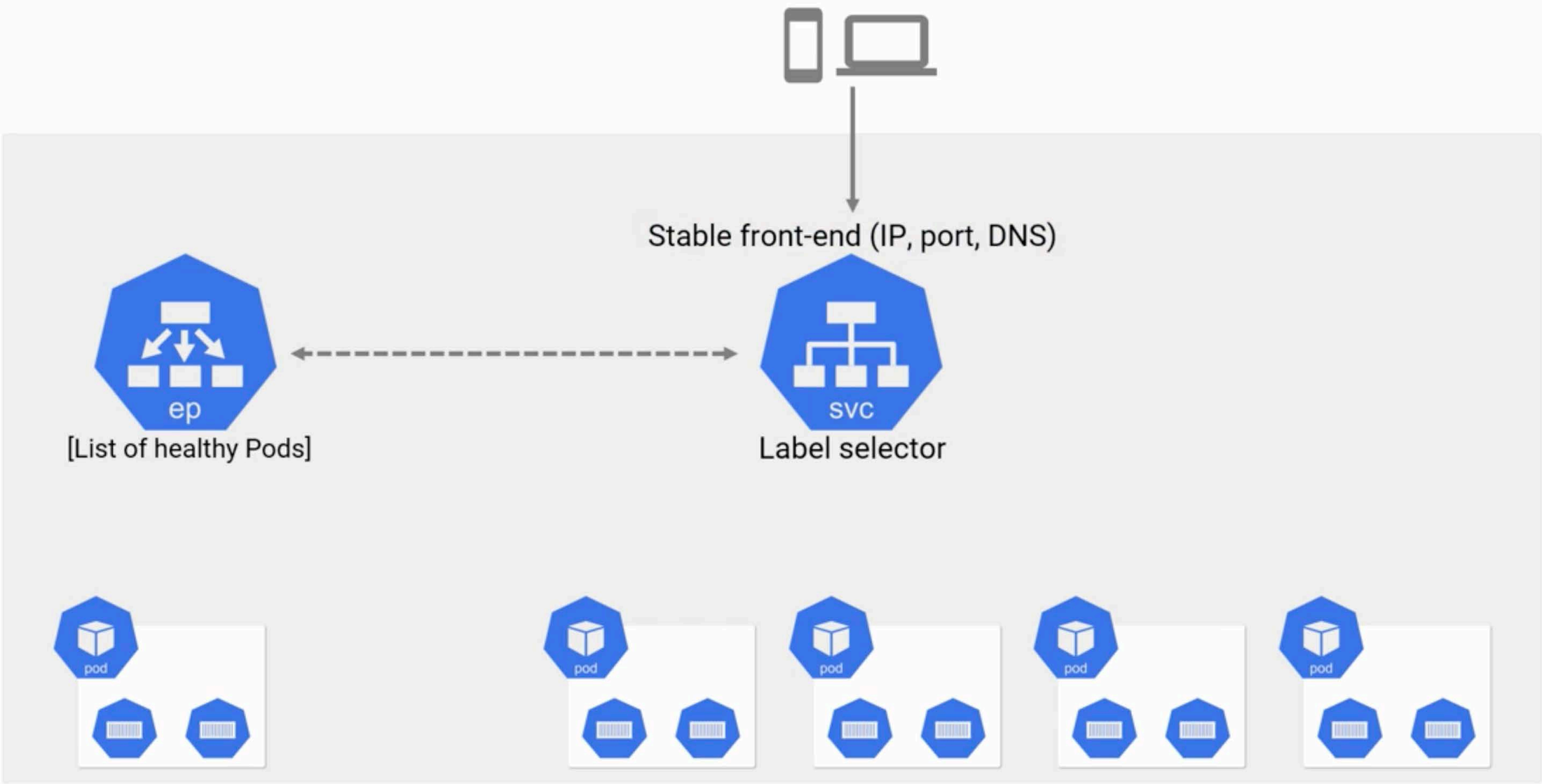
IP-per-Pod

All Pods can communicate

Recap


pod
localhost
Pod's network stack
IP address
Port range
Route table
...

Recap


Stable front-end (IP, port, DNS)
ep
[List of healthy Pods]
svc
Label selector
pod
pod
pod
pod
pod

Recap

A CLOUD GURU

The Service Network

(It's not really a network)

```
$ kubectl describe svc nginx-service
Name:                     my-svc
...
Type:                     ClusterIP
IP:                       10.11.240.5
Port:                     http    3080/TCP
Endpoints:                10.244.0.44:8080,10.244.1.39:8080
Session Affinity:         None


$ ipvsadm -ln
IP Virtual Server version 1.2.1 (size=4096)
Prot LocalAddress:Port Scheduler Flags
  -> RemoteAddress:Port           Forward Weight ActiveConn InActConn
TCP  10.11.240.5:3080  rr
  -> 10.244.0.44:8080             Masq    1      0          0
  -> 10.244.1.39:8080             Masq    1      0          0
```

* Kube-proxy in **IPVS** mode does create dummy interfaces on the *Service Network* (usually called `kube-ipvs0`). Kube-proxy in IPTABLES mode does not.

Storage in Kubernetes

A CLOUD GURU

Lesson Plan

A CLOUD GURU

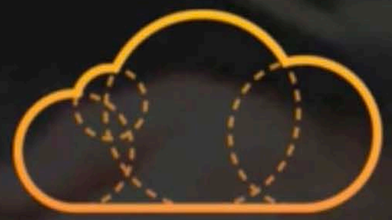
> Master a few concepts, and
> Kubernetes storage is a breeze!

Lesson Plan

A CLOUD GURU

- High-level storage requirements
- Container Storage Interface (CSI)
- The Kubernetes PersistentVolume Subsystem
- StorageClasses
- Lab/demo
- Recap

High-level Storage Requirements



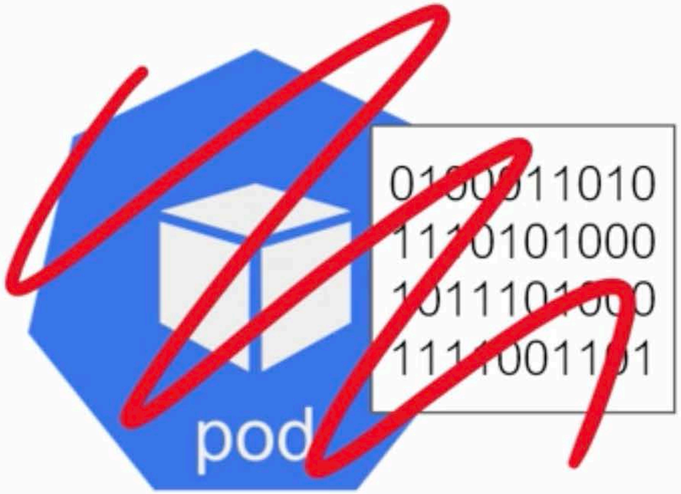
A CLOUD GURU

High-level Storage Requirements

A CLOUD GURU

Kubernetes Volumes

All about decoupling storage from Pods

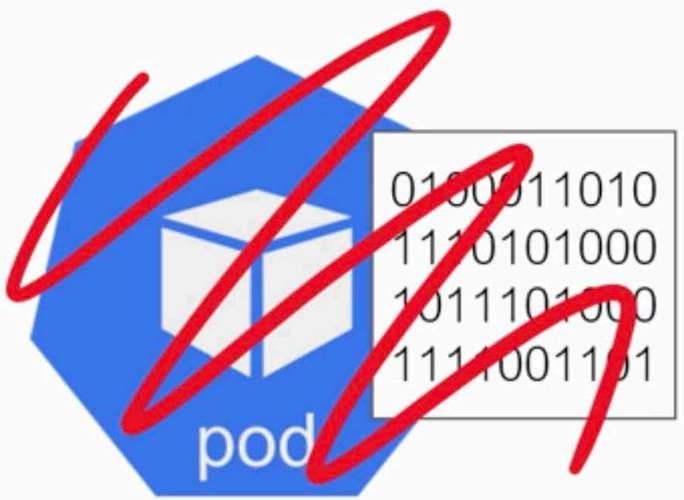


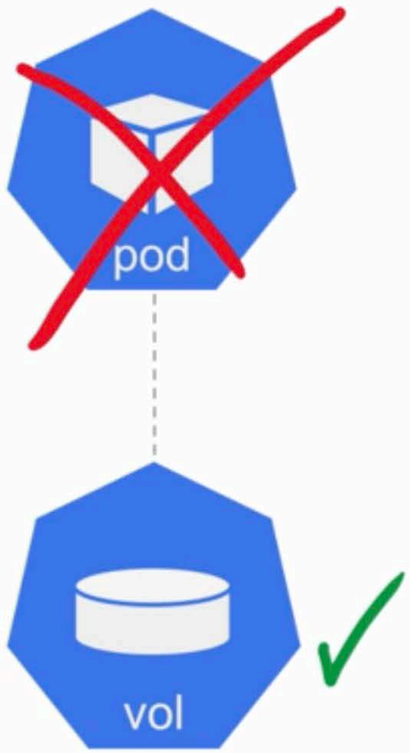
High-level Storage Requirements

A CLOUD GURU

High-level Storage Requirements

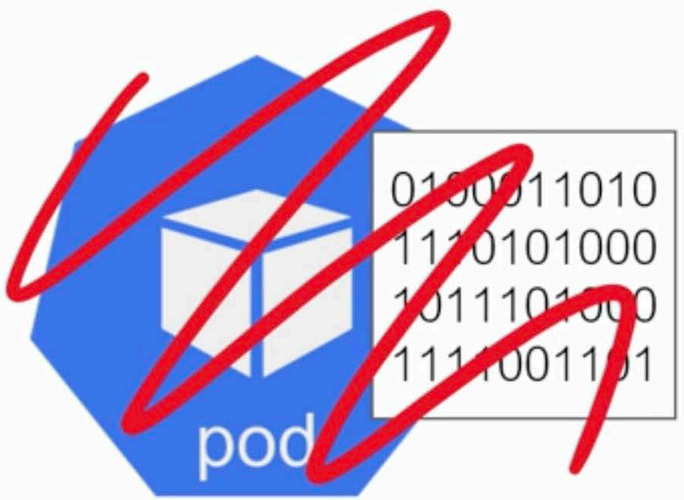
A CLOUD GURU

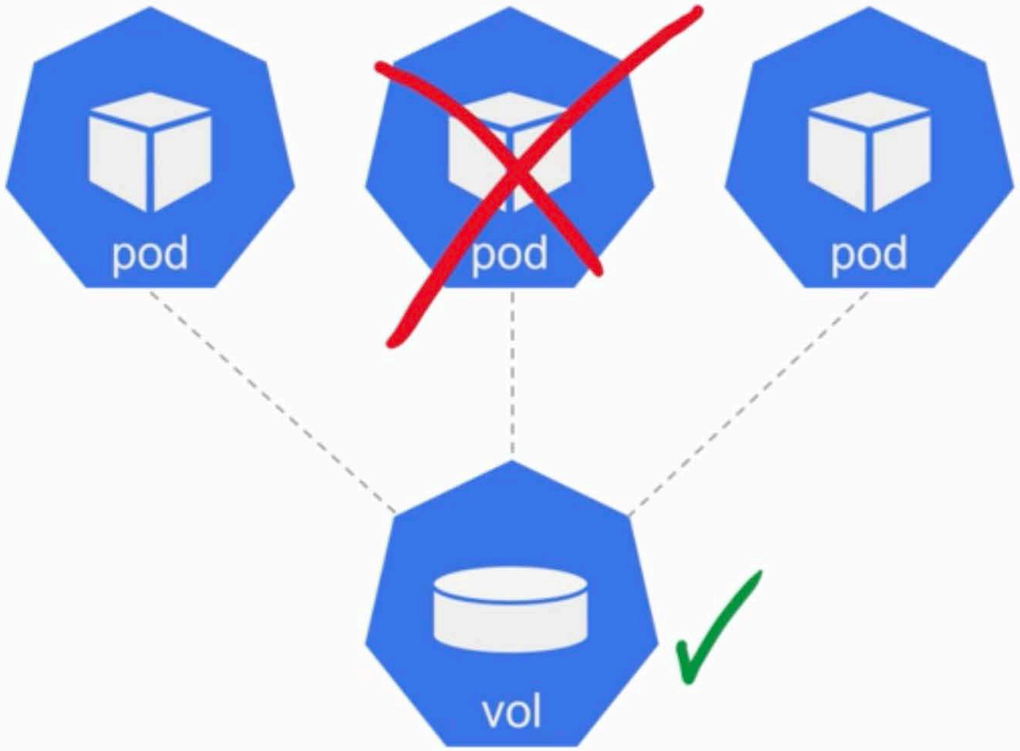




High-level Storage Requirements

A CLOUD GURU





High-level Storage Requirements

Volumes

[LUNs, devices, shares, mounts, spaces...]

High-level Storage Requirements

Storage is Vital!

File & Block
First-class Citizens in Kubernetes

High-level Storage Requirements

A CLOUD GURU

File & Block
First-class Citizens in
Kubernetes

- Standards-based
- Pluggable backend
- Rich API

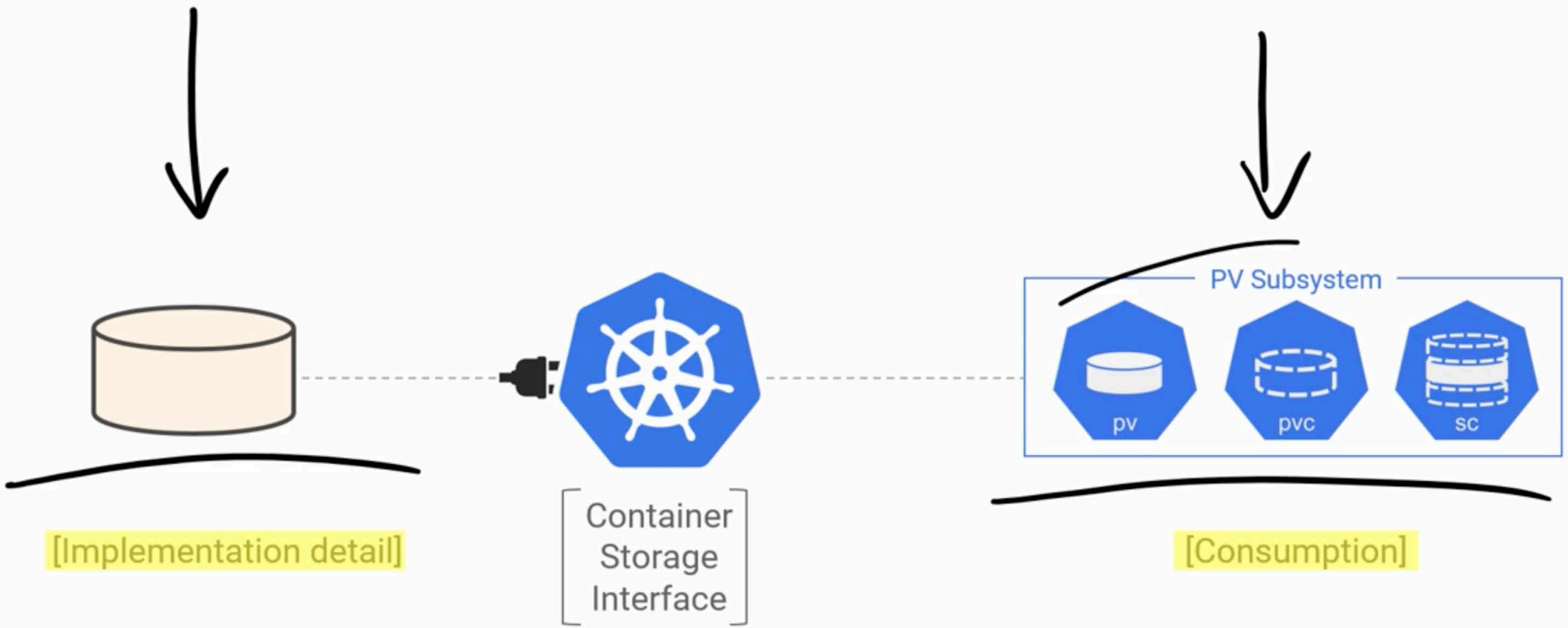
High-level Storage Requirements

Fundamental storage requirements

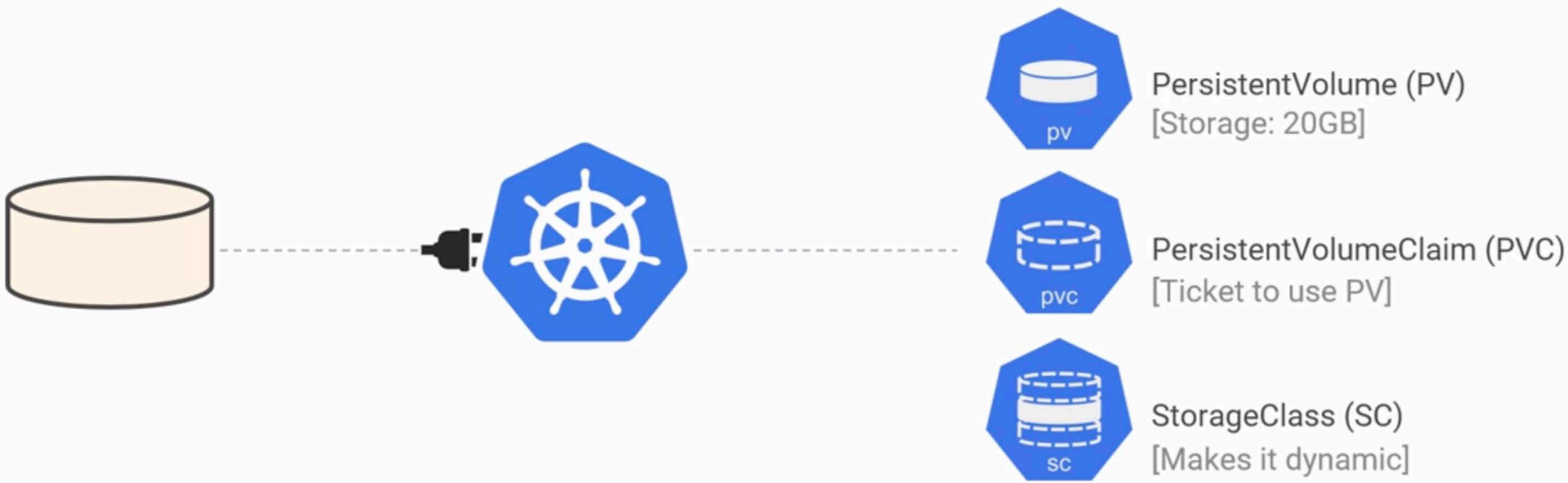
Storage Backend

Speed	Replicated	Resiliency	…

High-level Storage Requirements



High-level Storage Requirements



Container Storage Interface (CSI)

A CLOUD GURU

Container Storage Interface (CSI)

"Mare" = short for "nightmare"

Maintain external code in K8s

Tied to K8s release cycle

Driver code must be open-source

Container Storage Interface (CSI)

Out-of-tree

Open-standard

https://github.com/container-storage-interface/spec

Container Storage Interface (CSI)

A CLOUD GURU

@nigelpoulton

Out-of-tree

Open-standard

https://github.com/container-storage-interface/spec

Still Beta in K8s 1.11

The Kubernetes PersistentVolume Subsystem

A CLOUD GURU

Storage in Kubernetes

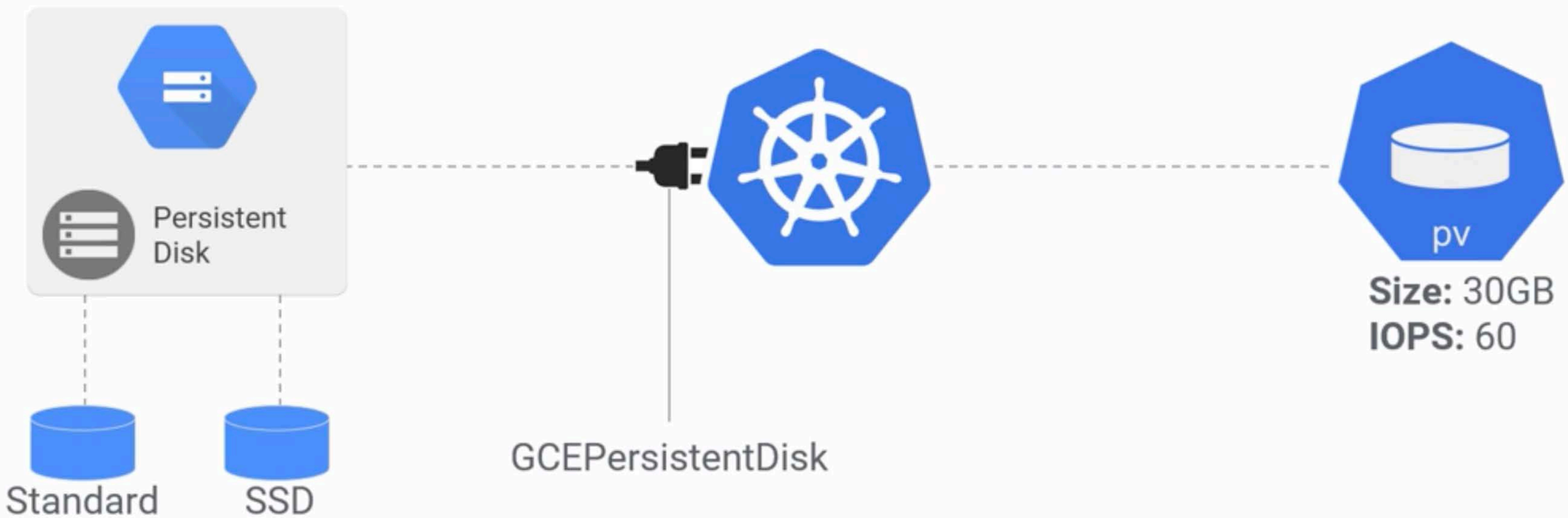
The K8s PersistentVolume Subsystem

A CLOUD GURU

Storage in Kubernetes

The K8s PersistentVolume Subsystem

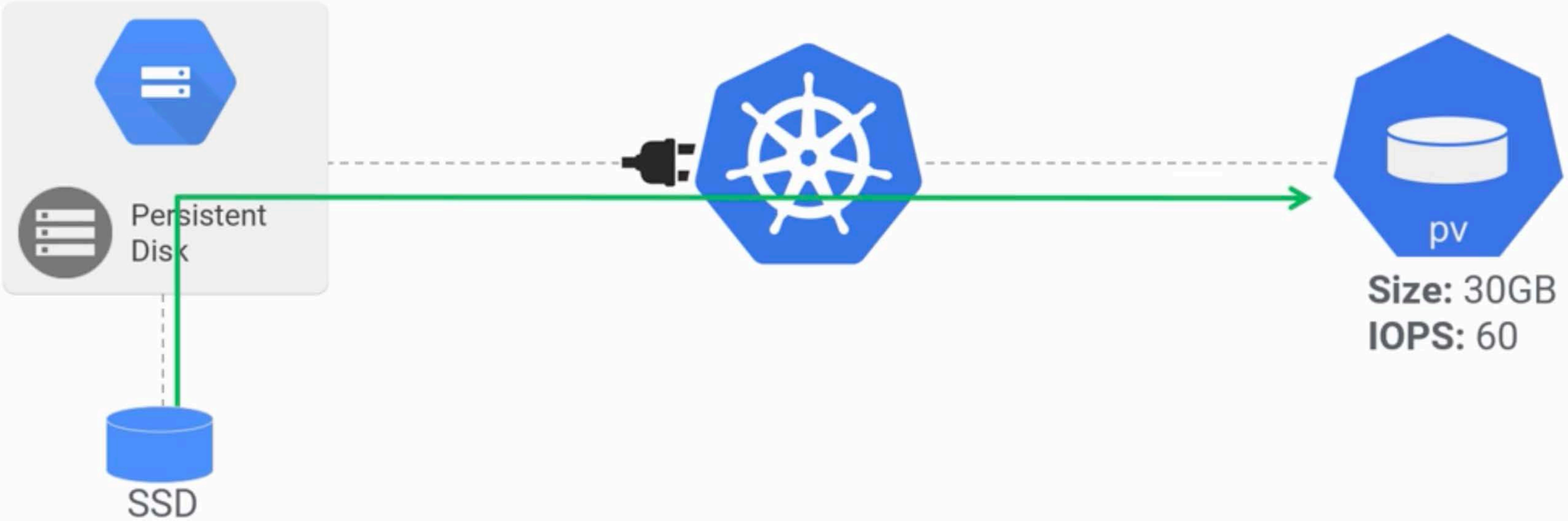
A CLOUD GURU



Storage in Kubernetes

The K8s PersistentVolume Subsystem

A CLOUD GURU

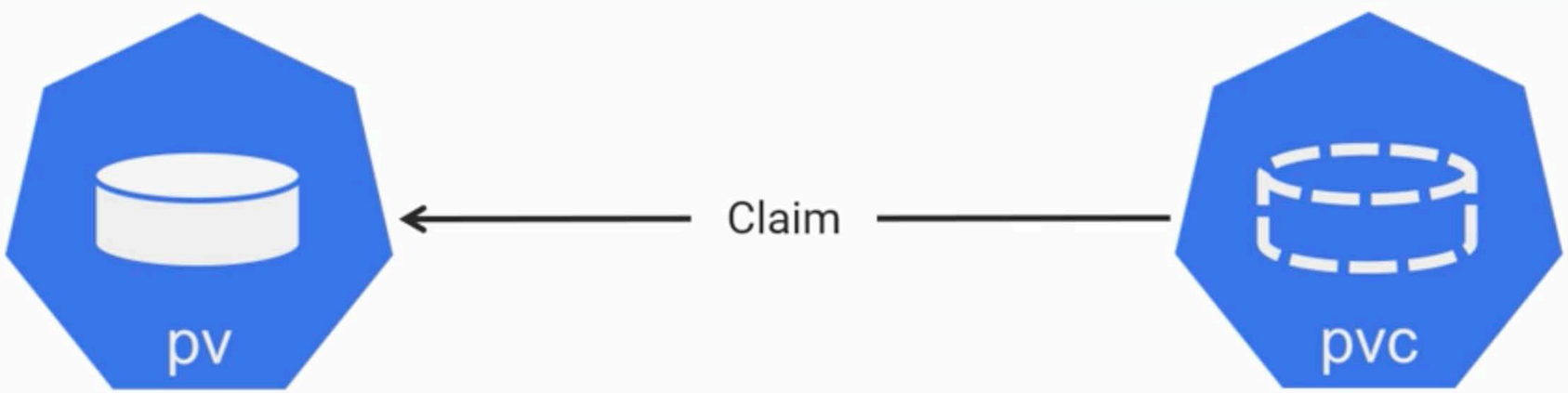


The K8s PersistentVolume Subsystem

A CLOUD GURU

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv1
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ssd
  capacity:
    storage: 10Gi
...
```

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc1
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ssd
  resources:
    requests:
      storage: 10Gi
```



Size: 30GB
IOPS: 60

gke-pv.yml ● | gke-pvc.yml | gke-volpod.yml

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv1
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ssd
  capacity:
    storage: 20Gi
  persistentVolumeReclaimPolicy: Retain
  gcePersistentDisk:
    pdName: uber-disk
```

0 0 | Ln 2, Col 23 (16 selected) | Spaces: 2 | UTF-8 | CRLF | YAML

gke-pv.yml ● | gke-pvc.yml | gke-volpod.yml

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv1
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ssd
  capacity:
    storage: 20Gi
  persistentVolumeReclaimPolicy: Retain
  gcePersistentDisk:
    pdName: uber-disk
```

0 0 | Ln 13, Col 25 (44 selected) | Spaces: 2 | UTF-8 | CRLF | YAML

Google Cloud Platform acg1

Disks

CREATE DISK REFRESH DELETE SHOW INFO PANEL

Filter resources Columns

Name	Type	Size	Zone	In use by
gke-cluster-1-70b82dc9-pvc-c2606c6d-899e-11e8-bb6b-42010a9a0089	Standard persistent disk	22 GB	europe-west2-b	
gke-cluster-1-default-pool-98763ba1-fht0	Standard persistent disk	100 GB	europe-west2-c	gke-cluster-1-default-pool-98763ba1-fht0
gke-cluster-1-default-pool-98763ba1-hw4j	Standard persistent disk	100 GB	europe-west2-c	gke-cluster-1-default-pool-98763ba1-hw4j
gke-cluster-1-default-pool-98763ba1-vdq7	Standard persistent disk	100 GB	europe-west2-c	gke-cluster-1-default-pool-98763ba1-vdq7
uber-disk	SSD persistent disk	20 GB	europe-west2-c	

Google Cloud Platform acg1

Disks

CREATE INSTANCE CREATE SNAPSHOT CREATE IMAGE EDIT DELETE

uber-disk

Description
Test PD for ACG storage lesson

Type
SSD persistent disk

Size
20 GB

Zone
europe-west2-c

Estimated performance

Operation type	Read	Write
Sustained random IOPS limit	600.00	600.00
Sustained throughput limit (MB/s)	9.60	9.60

Encryption type
Google managed

Equivalent REST

Select Windows PowerShell

```
PS C:\k8s\5>
PS C:\k8s\5>
PS C:\k8s\5> kubectl get nodes
NAME                                      STATUS    ROLES     AGE       VERSION
gke-cluster-1-default-pool-98763ba1-fht0  Ready     <none>    9m        v1.10.5-gke.2
gke-cluster-1-default-pool-98763ba1-hw4j  Ready     <none>    9m        v1.10.5-gke.2
gke-cluster-1-default-pool-98763ba1-vdq7  Ready     <none>    9m        v1.10.5-gke.2
PS C:\k8s\5>
PS C:\k8s\5>
PS C:\k8s\5> kubectl apply -f .\gke-pv.yml
persistentvolume "pv1" created
PS C:\k8s\5>
PS C:\k8s\5>
PS C:\k8s\5> kubectl get pv
NAME      CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS      CLAIM     STORAGECLASS   REASON    AGE
pv1       20Gi       RWO            Retain           Available               ssd                      8s
PS C:\k8s\5>
```

RWO: ReadWriteOnce
RWM: ReadWriteMany
ROM: ReadOnlyMany

*Not all volumes support all modes
*A PV can only have one active PVC/AccessMode

Select Windows PowerShell

```
PS C:\k8s\5>
PS C:\k8s\5>
PS C:\k8s\5> kubectl get nodes
NAME                                      STATUS    ROLES     AGE       VERSION
gke-cluster-1-default-pool-98763ba1-fht0  Ready     <none>    9m        v1.10.5-gke.2
gke-cluster-1-default-pool-98763ba1-hw4j  Ready     <none>    9m        v1.10.5-gke.2
gke-cluster-1-default-pool-98763ba1-vdq7  Ready     <none>    9m        v1.10.5-gke.2
PS C:\k8s\5>
PS C:\k8s\5>
PS C:\k8s\5> kubectl apply -f .\gke-pv.yml
persistentvolume "pv1" created
PS C:\k8s\5>
PS C:\k8s\5>
PS C:\k8s\5> kubectl get pv
NAME      CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS      CLAIM     STORAGECLASS   REASON    AGE
pv1       20Gi       RWO            Retain           Available             ssd                      8s
PS C:\k8s\5>
```

- Delete
- Retain

gke-pv.yml ● | gke-pvc.yml ✕ | gke-volpod.yml

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc1
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ssd
  resources:
    requests:
      storage: 20Gi
```

Ln 4, Col 13 (4 selected) Spaces: 2 UTF-8 CRLF YAML

05:35 / 08:30

Side-by-side compare of PVC and PV

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc1
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ssd
  resources:
    requests:
      storage: 20Gi
```

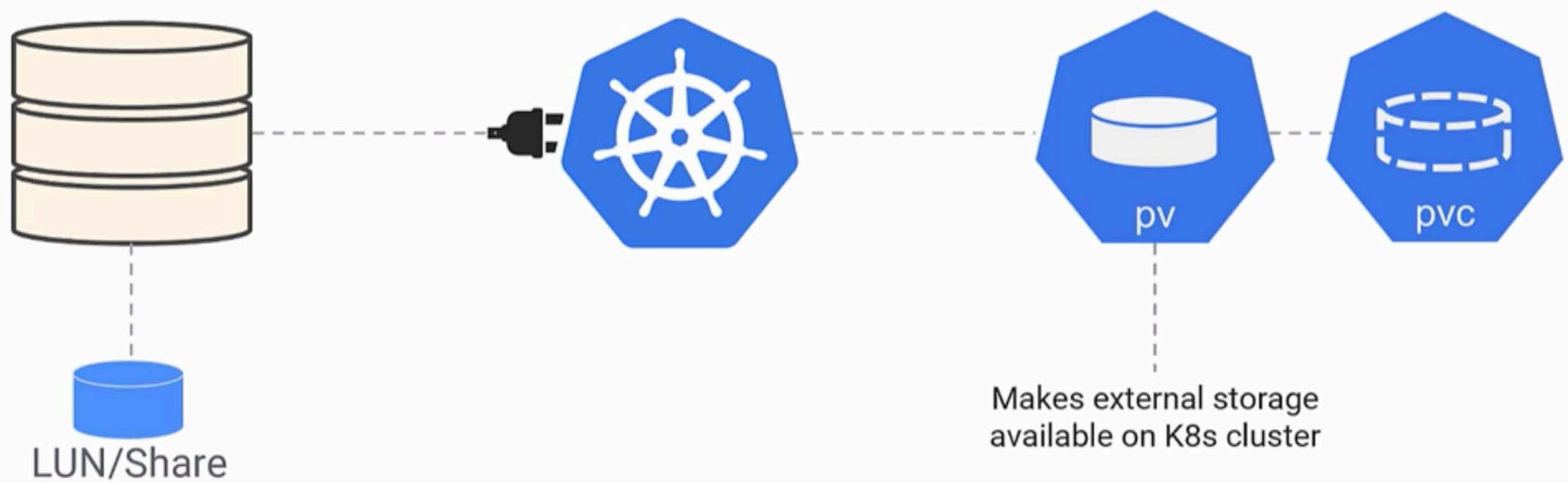
PVC

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv1
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ssd
  capacity:
    storage: 20Gi
  persistentVolumeReclaimPolicy: Retain
  gcePersistentDisk:
    pdName: uber-disk
```

PV

gke-pv.yml ● | gke-pvc.yml ✕ | gke-volpod.yml

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc1
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: ssd
  resources:
    requests:
      storage: 20Gi
```



0 0 | Ln 11, Col 20 (4 selected) | Spaces: 2 | UTF-8 | CRLF | YAML

gke-pv.yml ● | gke-pvc.yml | gke-volpod.yml ×

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: volpod
spec:
  volumes:
    - name: data
      persistentVolumeClaim:
        claimName: pvc1
  containers:
  - image: ubuntu:latest
    name: ubuntu-ctr
    command:
    - /bin/bash
    - "-c"
    - "sleep 60m"
    imagePullPolicy: IfNotPresent
    volumeMounts:
    - mountPath: /data
      name: data
```

0 ⚠ 0 | Ln 9, Col 24 (47 selected) | Spaces: 2 | UTF-8 | CRLF | YAML

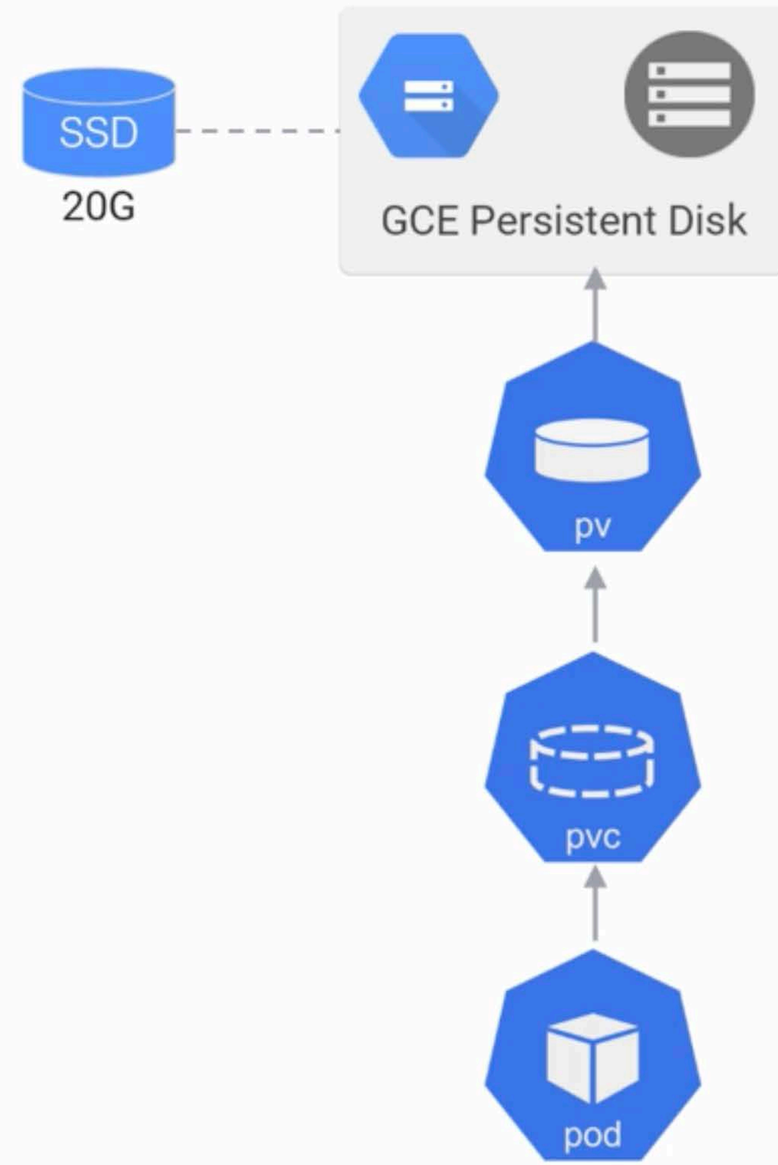
gke-pv.yml ● | gke-pvc.yml | gke-volpod.yml ×

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: volpod
spec:
  volumes:
    - name: data
      persistentVolumeClaim:
        claimName: pvc1
  containers:
  - image: ubuntu:latest
    name: ubuntu-ctr
    command:
    - /bin/bash
    - "-c"
    - "sleep 60m"
    imagePullPolicy: IfNotPresent
    volumeMounts:
    - mountPath: /data
      name: data
```

0 ⚠ 0 | Ln 20, Col 17 (56 selected) | Spaces: 2 | UTF-8 | CRLF | YAML

gke-pv.yml ● | gke-pvc.yml | gke-volpod.yml ✕

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: volpod
spec:
  volumes:
    - name: data
      persistentVolumeClaim:
        claimName: pvc1
  containers:
  - image: ubuntu:latest
    name: ubuntu-ctr
    command:
    - /bin/bash
    - "-c"
    - "sleep 60m"
    imagePullPolicy: IfNotPresent
    volumeMounts:
    - mountPath: /data
      name: data
```

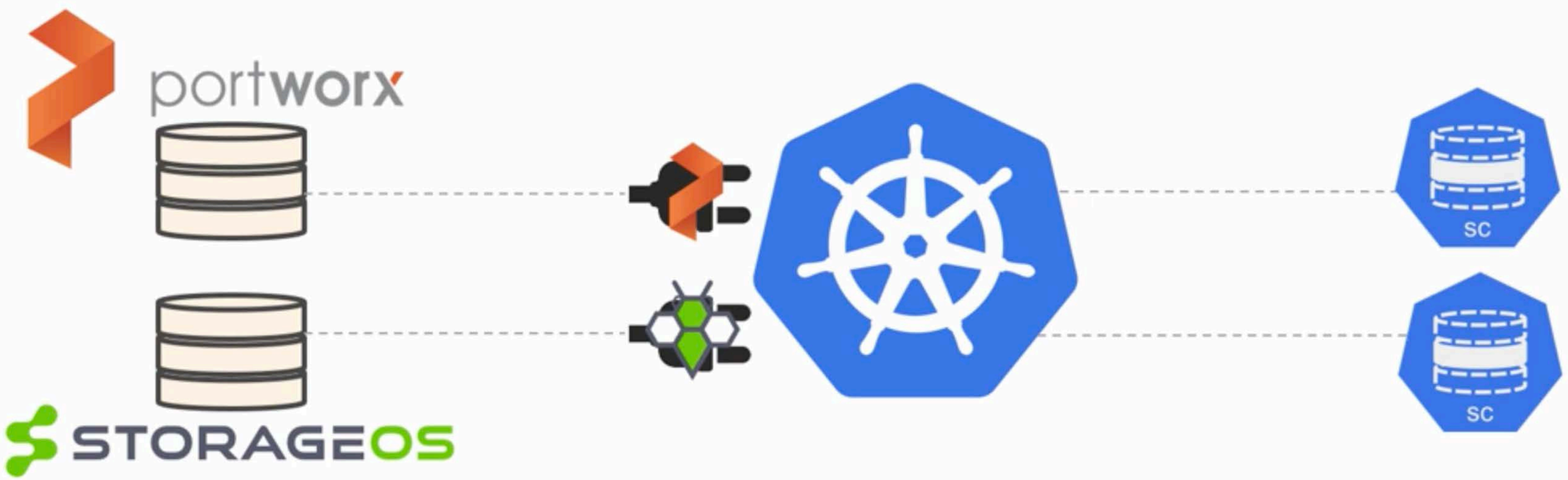


0 0 | Ln 20, Col 17 (56 selected) | Spaces: 2 | UTF-8 | CRLF | YAML

Dynamic Provisioning with StorageClasses

A CLOUD GURU

Dynamic Provisioning with StorageClasses



*Other storage backends do exist.

Dynamic Provisioning with StorageClasses

A CLOUD GURU

```yaml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: sc-fast
provisioner: kubernetes.io/aws-ebs
parameters:
  type: gp2
reclaimPolicy: Retain
```

Dynamic Provisioning with StorageClasses

A CLOUD GURU

```yaml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: sc-fast
provisioner: kubernetes.io/aws-ebs
parameters:
  type: pinkFluffySSD
reclaimPolicy: Retain
```

Dynamic Provisioning with StorageClasses

A CLOUD GURU

```yaml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: sc-fast
provisioner: kubernetes.io/aws-ebs
parameters:
  type: pinkFluffySSD
reclaimPolicy: Retain
```

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc1
…
storageClassName: sc-fast
```

```yaml
apiVersion: apps/v1
kind: Pod | Deployment
...
  spec:
  ...
    volumes:
    - name: my-vol
      persistentVolumeClaim:
        claimName: pvc1
```

sc.yml ● portworx.yml

```yaml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: fast
provisioner: kubernetes.io/aws-ebs
parameters:
  type: io1
  zones: eu-west-1a
  iopsPerGB: "10"
---
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: slow
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: kubernetes.io/aws-ebs
parameters:
  type: gp2
  zones: eu-west-1a
reclaimPolicy: Retain
mountOptions:
  - debug
```

0 0 Ln 23, Col 2 Spaces: 2 UTF-8 CRLF YAML

sc.yml ● portworx.yml

```yaml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: fast
provisioner: kubernetes.io/aws-ebs
parameters:
  type: io1
  zones: eu-west-1a
  iopsPerGB: "10"
---
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: slow
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: kubernetes.io/aws-ebs
parameters:
  type: gp2
  zones: eu-west-1a
reclaimPolicy: Retain
mountOptions:
  - debug
```

This is a feature of an AWS **io1** block device. It may not be available on other storage backends.

0 0 Ln 10, Col 1 (19 selected) Spaces: 2 UTF-8 CRLF YAML

sc.yml ● portworx.yml

```yaml
  type: io1
  zones: eu-west-1a
  iopsPerGB: "10"
---
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: slow
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: kubernetes.io/aws-ebs
parameters:
  type: gp2
  zones: eu-west-1a
reclaimPolicy: Retain
mountOptions:
  - debug
```

0 0 Ln 16, Col 56 (70 selected) Spaces: 2 UTF-8 CRLF YAML

sc.yml portworx.yml

```yaml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: fast
provisioner: kubernetes.io/aws-ebs
parameters:
  type: io1
  zones: eu-west-1a
  iopsPerGB: "10"
---
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: slow
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: kubernetes.io/aws-ebs
parameters:
  type: gp2
  zones: eu-west-1a
reclaimPolicy: Retain
mountOptions:
  - debug
```

0 0 Ln 10, Col 4 Spaces: 2 UTF-8 CRLF YAML

sc.yml ● portworx.yml ×

```yaml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: portworx-db-secure
provisioner: kubernetes.io/portworx-volume
parameters:
  fs: "xfs"
  block_size: "32"
  repl: "2"
  snap_interval: "30"
  io_priority:  "medium"
  secure: "true"
```

0 0 Ln 4, Col 27 (18 selected) Spaces: 2 UTF-8 CRLF YAML

ubuntu@mgr1: ~

```
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl get nodes
NAME                                          STATUS    ROLES     AGE       VERSION
ip-172-20-38-122.eu-west-1.compute.internal   Ready     master    8h        v1.11.0
ip-172-20-46-95.eu-west-1.compute.internal    Ready     node      8h        v1.11.0
ip-172-20-58-139.eu-west-1.compute.internal   Ready     node      8h        v1.11.0
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl get sc
No resources found.
ubuntu@mgr1:~$
```

ubuntu@mgr1: ~

```
No resources found.
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ cat sc.yml
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: fast
provisioner: kubernetes.io/aws-ebs
parameters:
  type: io1
  zones: eu-west-1a
  iopsPerGB: "10"
---
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: slow
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: kubernetes.io/aws-ebs
parameters:
  type: gp2
  zones: eu-west-1a
reclaimPolicy: Retain
mountOptions:
  - debug
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl apply -f sc.yml
```

ubuntu@mgr1: ~

```
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl apply -f sc.yml
storageclass.storage.k8s.io/fast created
storageclass.storage.k8s.io/slow created
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl get sc
NAME            PROVISIONER             AGE
fast            kubernetes.io/aws-ebs   6s
slow (default)  kubernetes.io/aws-ebs   6s
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl describe sc fast
Name:            fast
IsDefaultClass:  No
Annotations:     kubectl.kubernetes.io/last-applied-configuration={"apiVersion":"storage.k8s.io/v1","kind":"StorageClass","metad
ata":{"annotations":{},"name":"fast","namespace":""},"parameters":{"iopsPerGB":"10","type":"io1","zones":"eu-west-1a"},"provisio
ner":"kubernetes.io/aws-ebs"}

Provisioner:           kubernetes.io/aws-ebs
Parameters:            iopsPerGB=10,type=io1,zones=eu-west-1a
AllowVolumeExpansion:  <unset>
MountOptions:          <none>
ReclaimPolicy:         Delete
VolumeBindingMode:     Immediate
Events:                <none>
ubuntu@mgr1:~$
```

ubuntu@mgr1: ~

```
AllowVolumeExpansion:  <unset>
MountOptions:          <none>
ReclaimPolicy:         Delete
VolumeBindingMode:     Immediate
Events:                <none>
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl get pv
No resources found.
ubuntu@mgr1:~$ kubectl get pvc
No resources found.
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ cat aws-pvc.yml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: aws-fast
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: fast
  resources:
    requests:
      storage: 10Giubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
```

ubuntu@mgr1: ~

```
ReclaimPolicy:          Delete
VolumeBindingMode:      Immediate
Events:                 <none>
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl get pv
No resources found.
ubuntu@mgr1:~$ kubectl get pvc
No resources found.
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ cat aws-pvc.yml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: aws-fast
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: fast
  resources:
    requests:
      storage: 10Giubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl apply -f aws-pvc.yml
persistentvolumeclaim/aws-fast created
ubuntu@mgr1:~$
```

Name: aws-fast
Size: 10G
StorageClassName: fast

ubuntu@mgr1: ~

```
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl get pv
No resources found.
ubuntu@mgr1:~$ kubectl get pvc
No resources found.
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ cat aws-pvc.yml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: aws-fast
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: fast
  resources:
    requests:
      storage: 10Giubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl apply -f aws-pvc.yml
persistentvolumeclaim/aws-fast created
ubuntu@mgr1:~$ kubectl get pvc
NAME       STATUS    VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
aws-fast   Bound     pvc-3ec88edf-8ab6-11e8-8a01-060a650e58be   10Gi       RWO            fast           26s
ubuntu@mgr1:~$
```

Name: aws-fast
Size: 10G
StorageClassName: fast

EC2 Management Consol

Secure https://eu-west-1.console.aws.amazon.com/ec2/v2/home?region=eu-west-1#Volumes:sort=desc:createTime

aws Services Resource Groups EC2 CloudFormation VPC EKS Nigel Poulton Ireland Support

EC2 Dashboard
Events
Tags
Reports
Limits

INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances

IMAGES
AMIs
Bundle Tasks

ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager

NETWORK & SECURITY
Security Groups

Create Volume Actions

Filter by tags and attributes or search by keyword 1 to 9 of 9

Name	Volume ID	Size	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm Sta
acg.k8s.local-dyna...	vol-0b5d2fb5...	10 GiB	io1	100		July 18, 2018 at 7:1...	eu-west-1a	available	None
	vol-054e8ca...	128 GiB	gp2	384 / 3000	snap-0009045...	July 18, 2018 at 10:...	eu-west-1a	in-use	None
	vol-0136278...	128 GiB	gp2	384 / 3000	snap-0009045...	July 18, 2018 at 10:...	eu-west-1a	in-use	None
	vol-00bc557...	64 GiB	gp2	192 / 3000	snap-0009045...	July 18, 2018 at 10:...	eu-west-1a	in-use	None
a.etcd-main.acg.k8...	vol-071308c...	20 GiB	gp2	100 / 3000		July 18, 2018 at 10:...	eu-west-1a	in-use	None
a.etcd-events.acg.k...	vol-0f2c4e2b...	20 GiB	gp2	100 / 3000		July 18, 2018 at 10:...	eu-west-1a	in-use	None
	vol-0f152d66...	8 GiB	gp2	100 / 3000	snap-0a584c0...	July 17, 2018 at 3:0...	eu-west-1a	in-use	None
	vol-0a8bc77...	8 GiB	gp2	100 / 3000	snap-0a584c0...	July 17, 2018 at 3:0...	eu-west-1a	in-use	None
	vol-0ac9f520...	8 GiB	gp2	100 / 3000	snap-0a584c0...	July 17, 2018 at 3:0...	eu-west-1a	in-use	None

Volumes: vol-0b5d2fb58460a9e14 (acg.k8s.local-dynamic-pvc-3ec88edf-8ab6-11e8-8a01-060a650e58be)

Description Status Checks Monitoring Tags

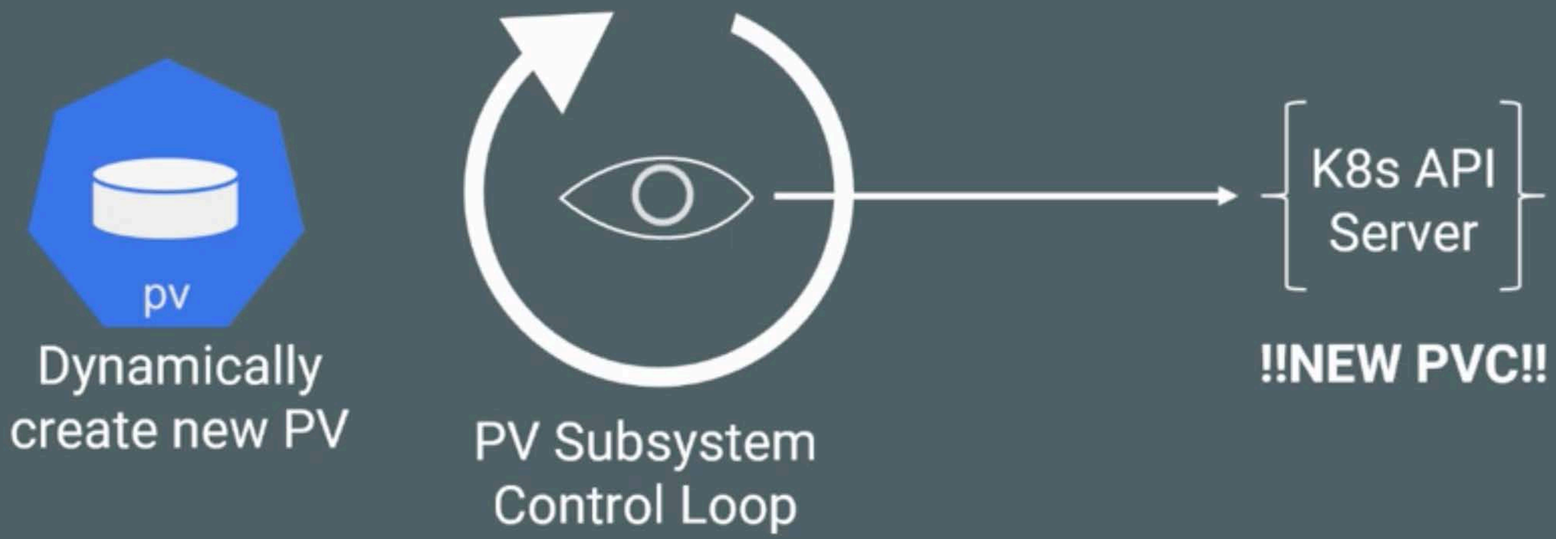
Volume ID vol-0b5d2fb58460a9e14
Size 10 GiB
Alarm status None
Snapshot -

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

ubuntu@mgr1: ~

```
ubuntu@mgr1:~$
ubuntu@mgr1:~$ cat aws-pvc.yml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: aws-fast
spec:
  accessModes:
  - ReadWriteOnce
  storageClassName: fast
  resources:
    requests:
      storage: 10Giubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl apply -f aws-pvc.yml
persistentvolumeclaim/aws-fast created
ubuntu@mgr1:~$ kubectl get pvc
NAME       STATUS    VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
aws-fast   Bound     pvc-3ec88edf-8ab6-11e8-8a01-060a650e58be   10Gi       RWO            fast           26s
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$
ubuntu@mgr1:~$ kubectl get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS    CLAIM              STORAGECLASS
  REASON    AGE
pvc-3ec88edf-8ab6-11e8-8a01-060a650e58be   10Gi       RWO            Delete           Bound     default/aws-fast   fast
            1m
ubuntu@mgr1:~$
```



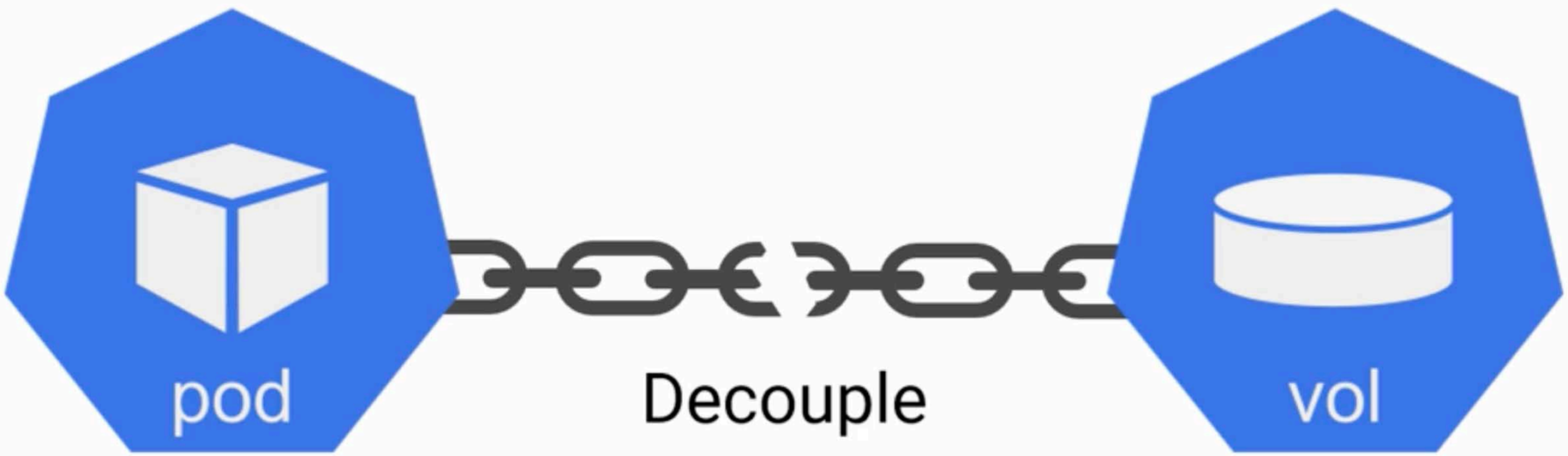
Demo/Lab

A CLOUD GURU

Recap

A CLOUD GURU

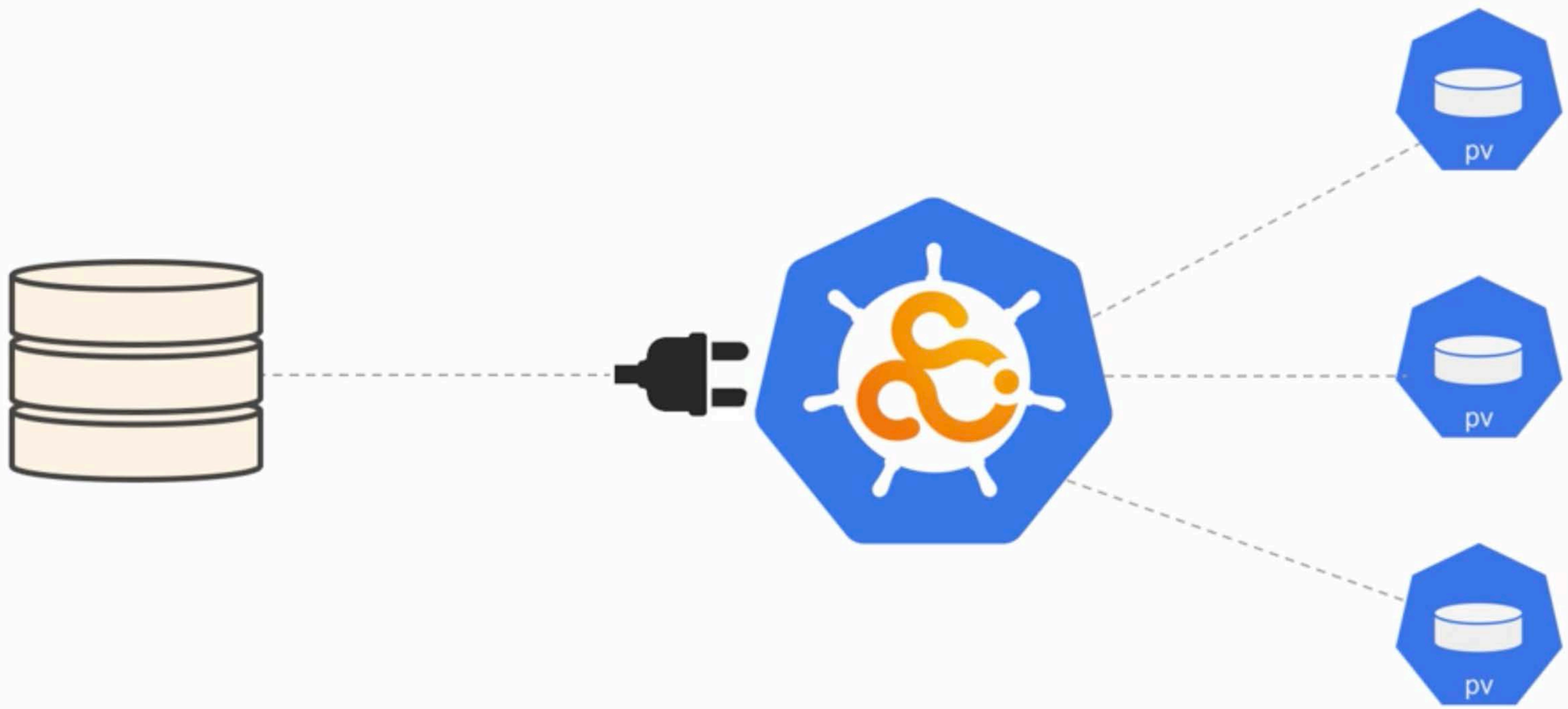
Recap



Recap

First Class Citizen

Recap



Recap

Recap

Making things dynamic!

Coming up next...

Code & Docker Images

From Code to Kubernetes

A CLOUD GURU

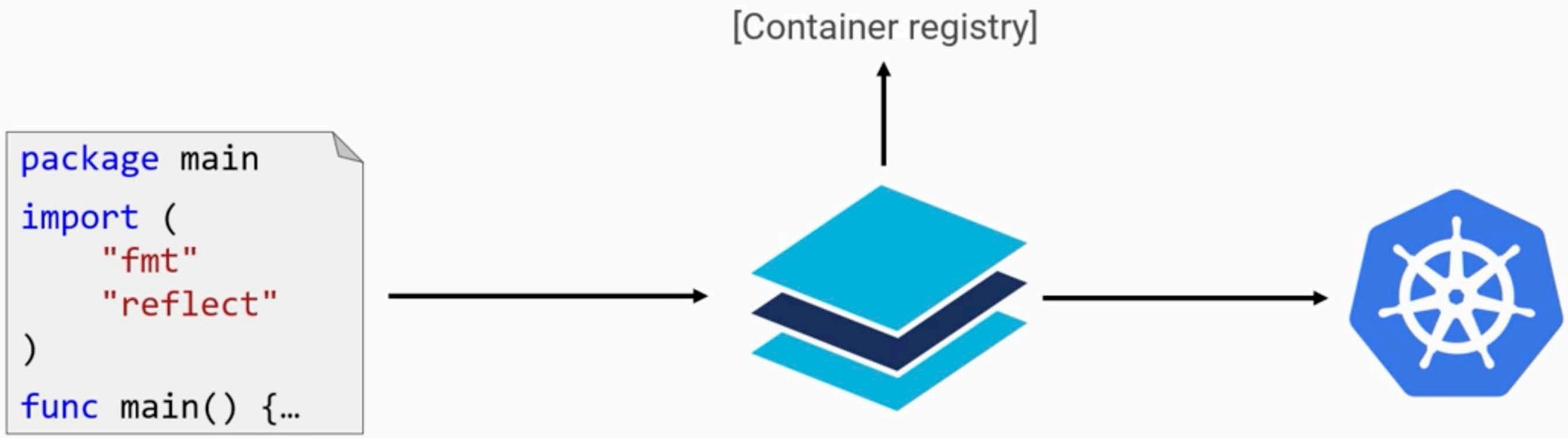
Lesson Plan

- Big Picture
- Walk-through example
- Recap

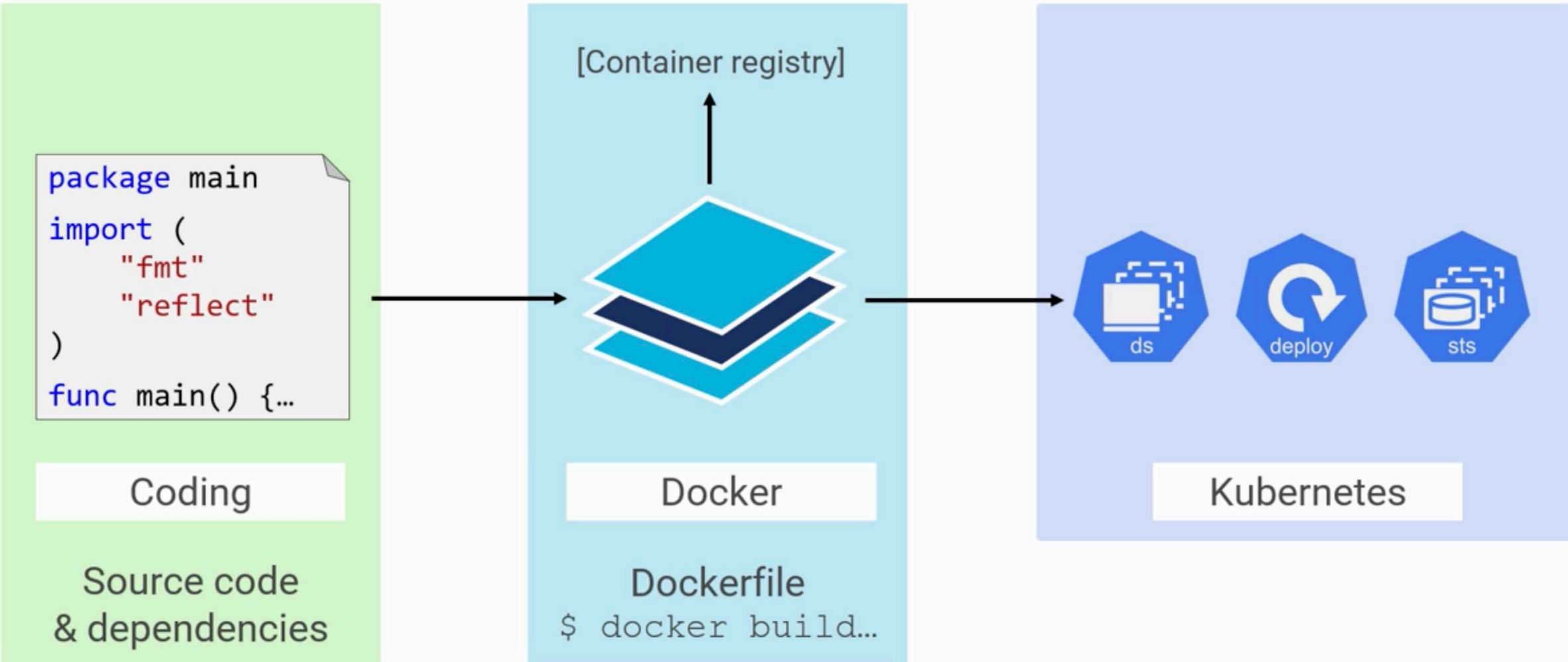
The Big Picture

A CLOUD GURU

The Big Picture



The Big Picture



The Big Picture

A CLOUD GURU

From code to Kubernetes

```
package main
import (
    "fmt"
    "reflect"
)
func main() {…
```

Coding

Source code
& dependencies

[Container registry]

Docker

Dockerfile
$ docker build…

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: acg-deploy
  labels:
    app: acg
spec:
  replicas: 3
  ...
  strategy:
  type: Recreate
  ...
```

Kubernetes

$ kubectl

Demo Time!
A CLOUD GURU

Recap

A CLOUD GURU

Recap


```go
package main
import (
    "fmt"
    "reflect"
)
func main() {…
```

```
LastWriteTime       Length Name
-------------       ------ ----
26/07/2018 12:41           views
26/07/2018 12:39     388   app.js
26/07/2018 20:07     508   Dockerfile
26/07/2018 12:36     345   package.json
26/07/2018 12:30     360   readme.md
26/07/2018 21:40     407   web-deploy.yml
26/07/2018 21:40     184   web-lb.yml
26/07/2018 12:22     197   web-nodeport.yml
```

```dockerfile
FROM centos:centos7
RUN yum -y install nodejs np
COPY . /src
RUN cd /src; npm install
EXPOSE 8080
CMD cd /src && node ./app.js
```

```
$ docker build…
```

[Container registry]

```
$ kubectl apply -f ...
```

Coming up next...

A CLOUD GURU

Deployments

Kubernetes Deployments

A CLOUD GURU

Lesson Plan

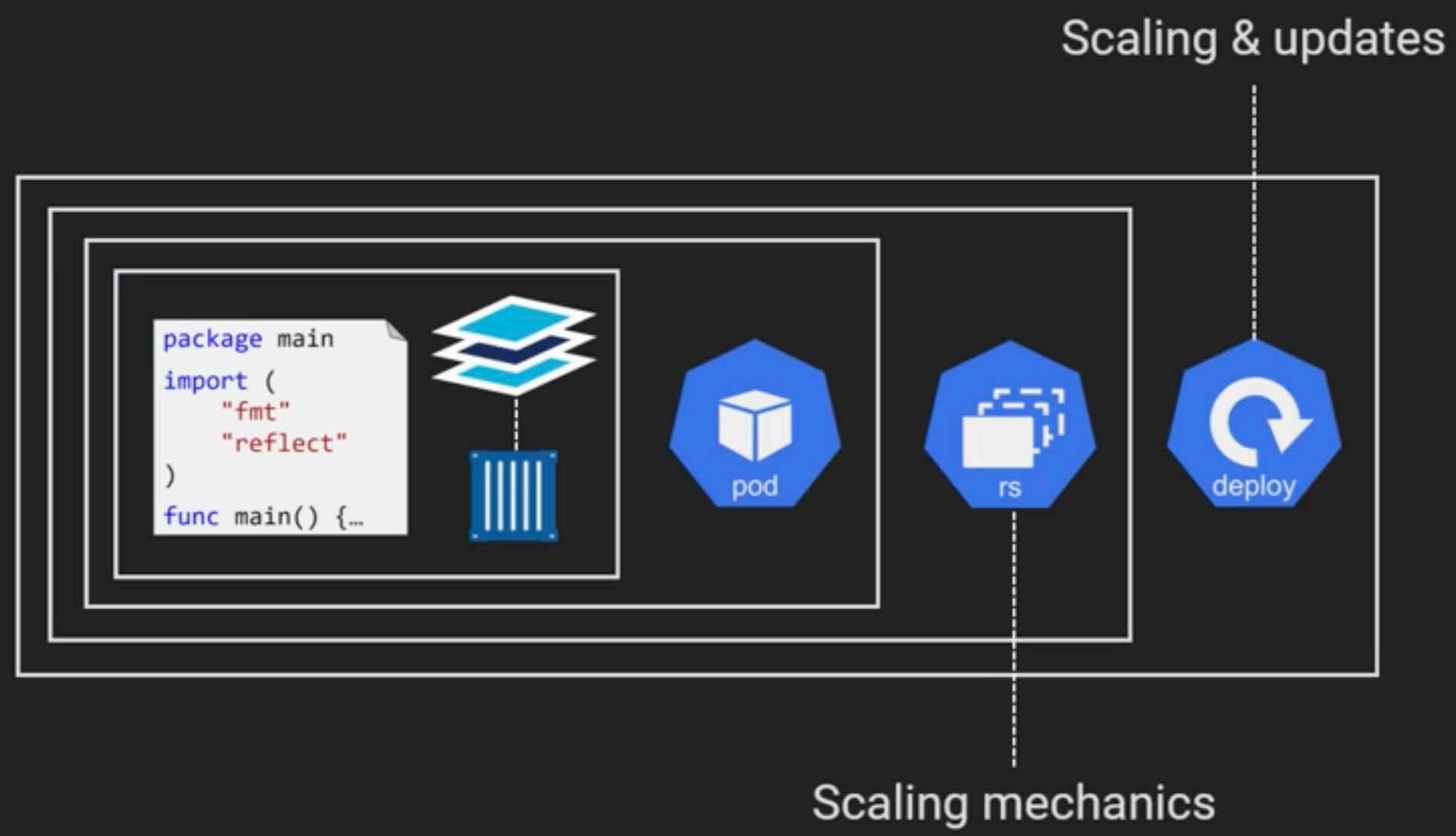
A CLOUD GURU

- Theory
- Demo
- Recap

Kubernetes Deployments

A CLOUD GURU

Deployment Theory



deployment.yml

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    run: prod-redis
  name: prod-redis
spec:
  selector:
    matchLabels:
      run: prod-redis
  replicas: 1
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
```

0 2 Ln 1, Col 1 Spaces: 2 UTF-8 CRLF YAML

deployment.yml

```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 1
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.0
        name: redis
```

0 2 Ln 25, Col 20 (71 selected) Spaces: 2 UTF-8 CRLF YAML

deployment.yml

```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 1
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.0
        name: redis
```

0 2 Ln 11, Col 14 (11 selected) Spaces: 2 UTF-8 CRLF YAML

deployment.yml

```yaml
8   selector:
9     matchLabels:
10      run: prod-redis
11  replicas: 3
12  minReadySeconds: 300
13  strategy:
14    rollingUpdate:
15      maxSurge: 1
16      maxUnavailable: 0
17    type: RollingUpdate
18  template:
19    metadata:
20      labels:
21        run: prod-redis
22    spec:
23      containers:
24      - image: redis:4.0
25        name: redis
26
```

Handled by ReplicaSet (RS)

0 2 Ln 11, Col 14 Spaces: 2 UTF-8 CRLF YAML

deployment.yml

```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
  strategy
    rollin
      maxS
      maxU
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.11
        name: redis
```

type (string)

Type of deployment. Can be "Recreate" or "RollingUpdate". Default is RollingUpdate.

0 2 Ln 17, Col 24 (19 selected) Spaces: 2 UTF-8 CRLF YAML

deployment.yml

```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.11
        name: redis
```

0 2 Ln 16, Col 24 (17 selected) Spaces: 2 UTF-8 CRLF YAML

deployment.yml

```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.11
        name: redis
```

0 2 Ln 16, Col 24 (17 selected) Spaces: 2 UTF-8 CRLF YAML

deployment.yml

```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.11
        name: redis
```

0 2 Ln 16, Col 24 (17 selected) Spaces: 2 UTF-8 CRLF YAML

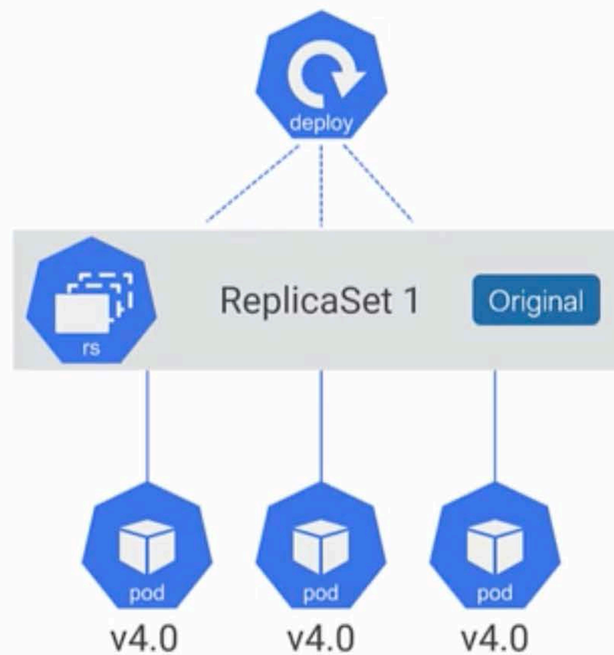
deployment.yml

```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.11
        name: redis
```

0 2 Ln 16, Col 24 (17 selected) Spaces: 2 UTF-8 CRLF YAML

deployment.yml

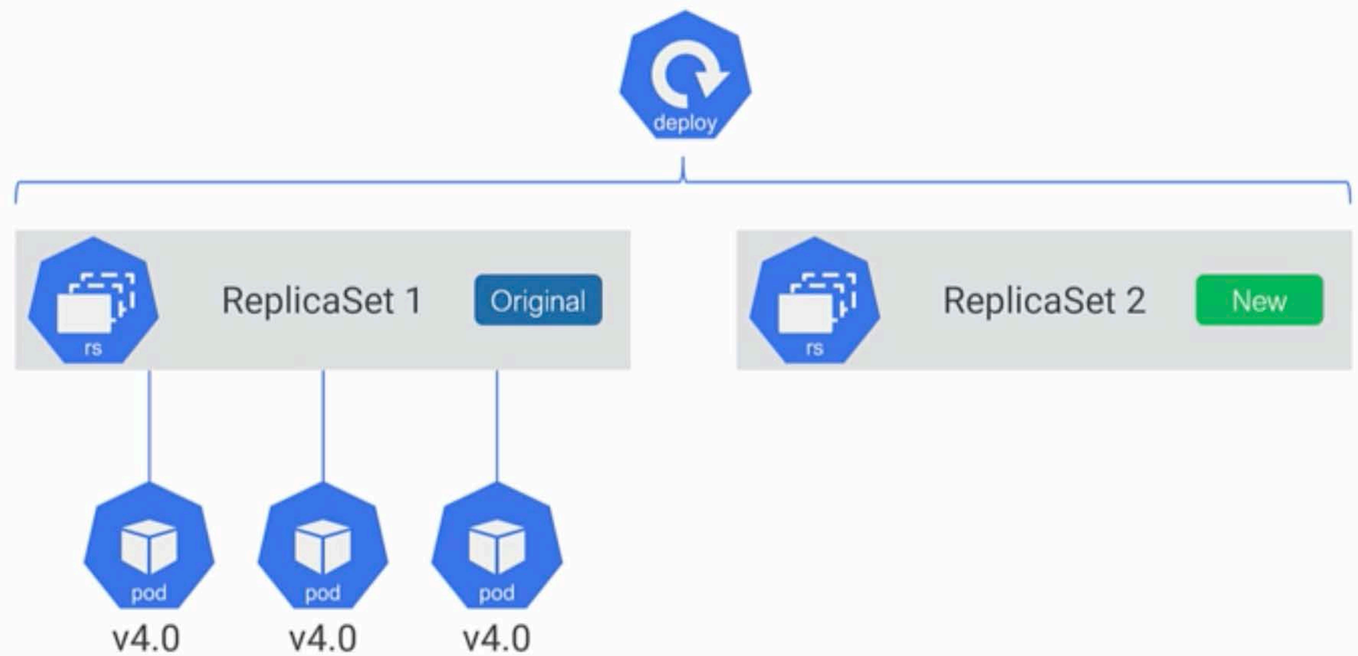
```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.11
        name: redis
```



0 2 Ln 16, Col 24 (17 selected) Spaces: 2 UTF-8 CRLF YAML

deployment.yml

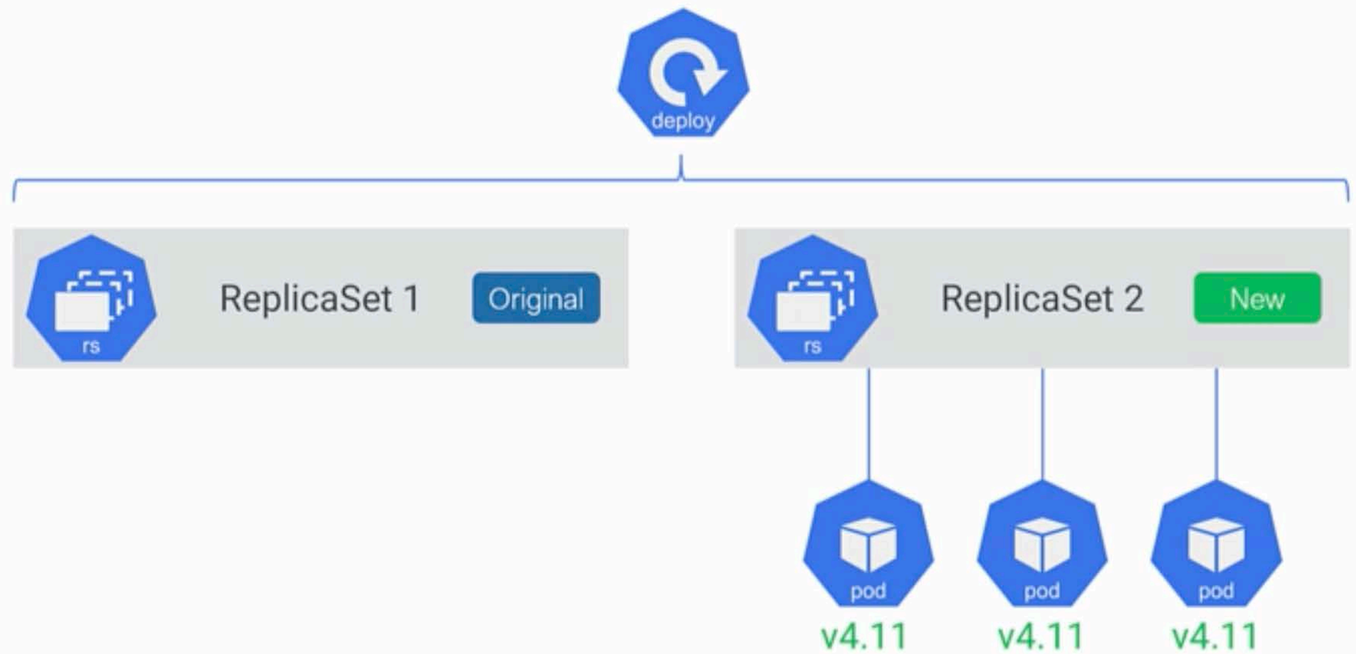
```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.11
        name: redis
```



0 2 Ln 16, Col 24 (17 selected) Spaces: 2 UTF-8 CRLF YAML

deployment.yml

```yaml
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 0
    type: RollingUpdate
  template:
    metadata:
      labels:
        run: prod-redis
    spec:
      containers:
      - image: redis:4.11
        name: redis
```



0 2 Ln 16, Col 24 (17 selected) Spaces: 2 UTF-8 CRLF YAML

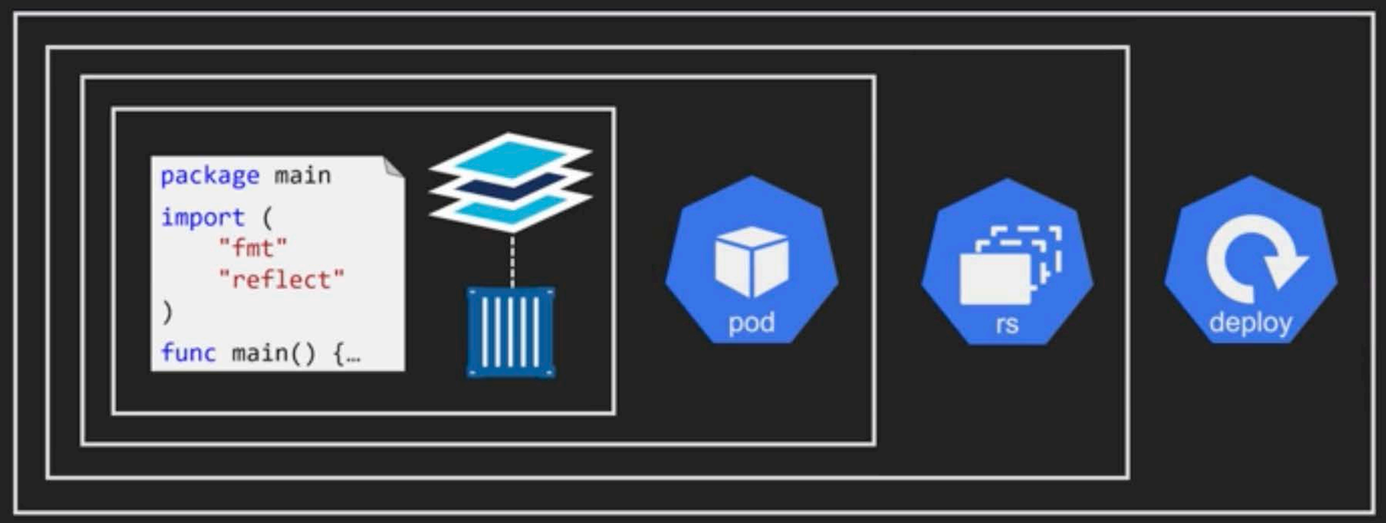
Demo Time!

A CLOUD GURU

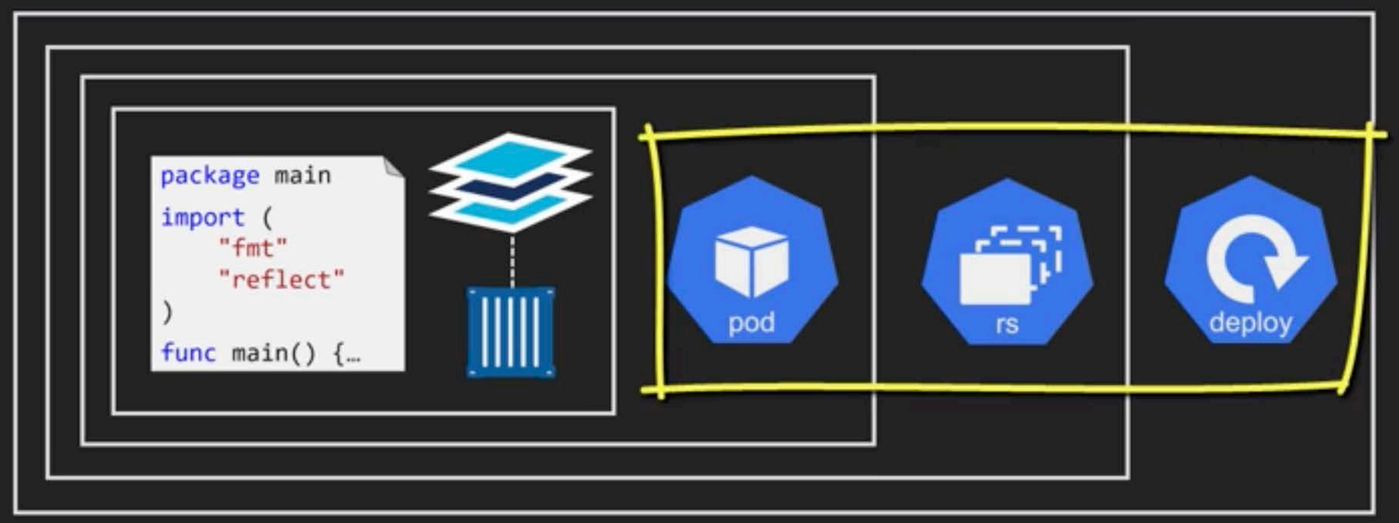
Recap

A CLOUD GURU

Recap

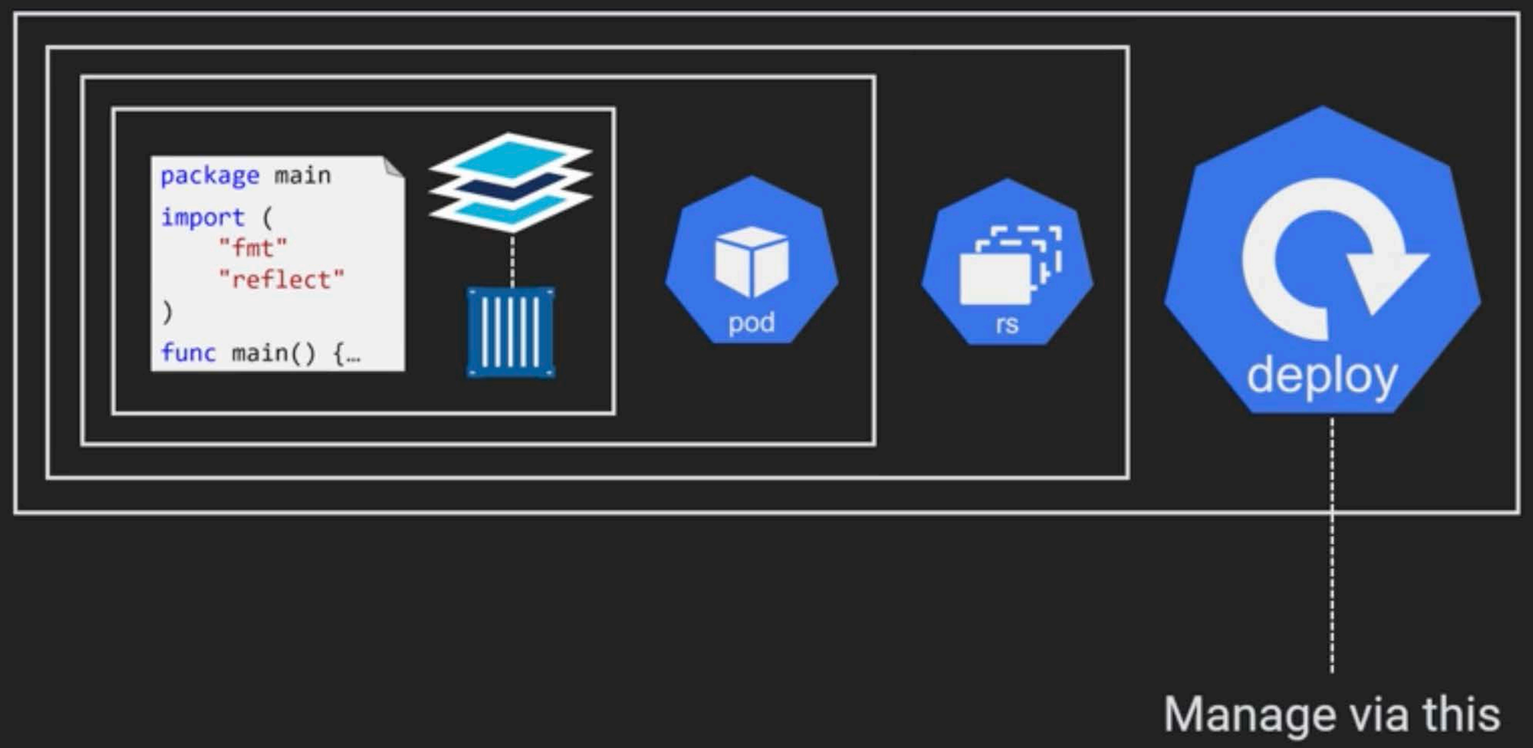


Recap

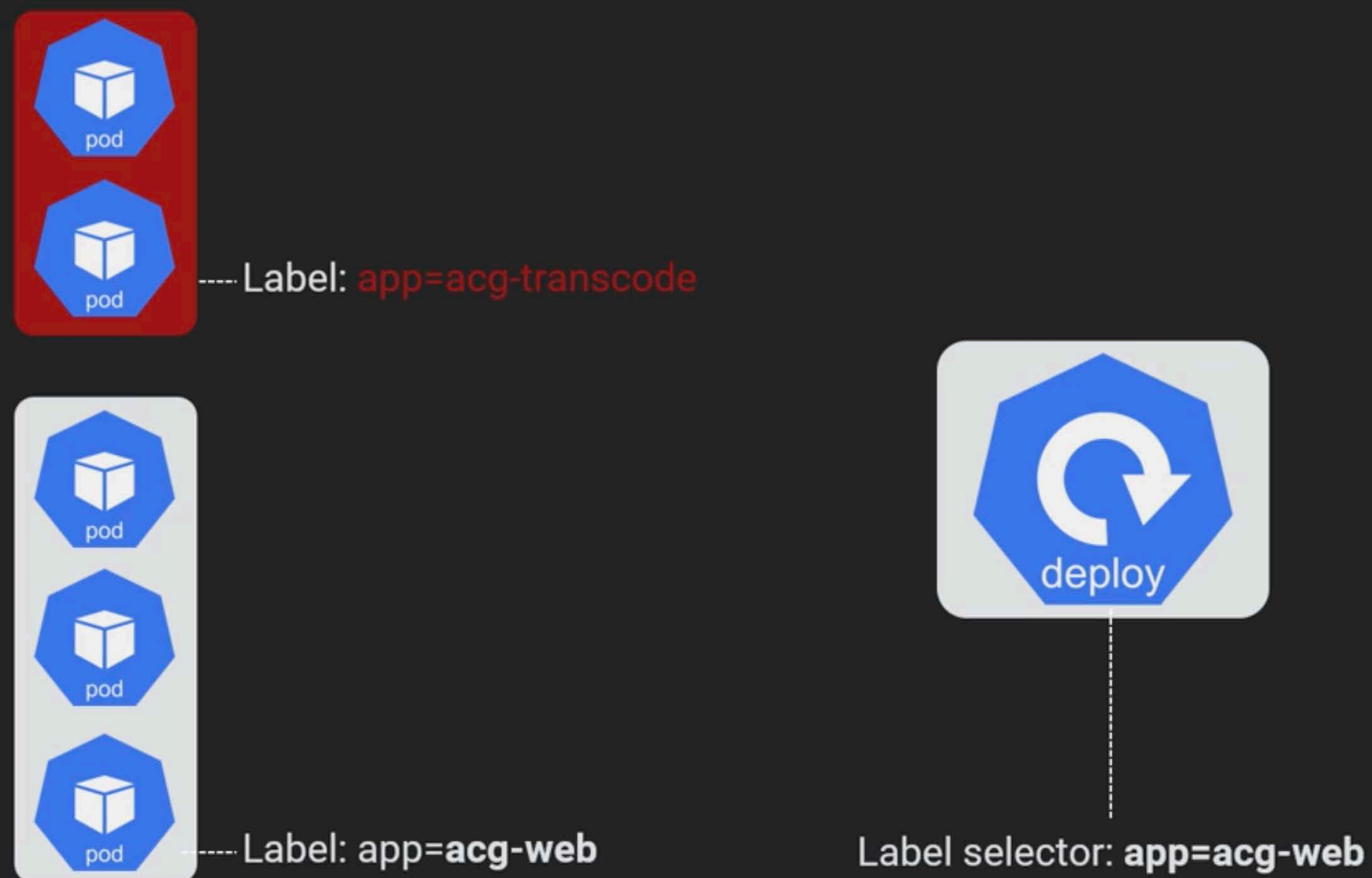


Kubernetes icons from
https://github.com/octo-technology/kubernetes-icons

Recap


package main
import (
"fmt"
"reflect"
)
func main() {…
pod
rs
deploy
Manage via this

Recap


pod
pod
Label: app=acg-transcode
pod
pod
pod
Label: app=acg-web
deploy
Label selector: app=acg-web

Recap

Declarative

Scaling Applications

A CLOUD GURU

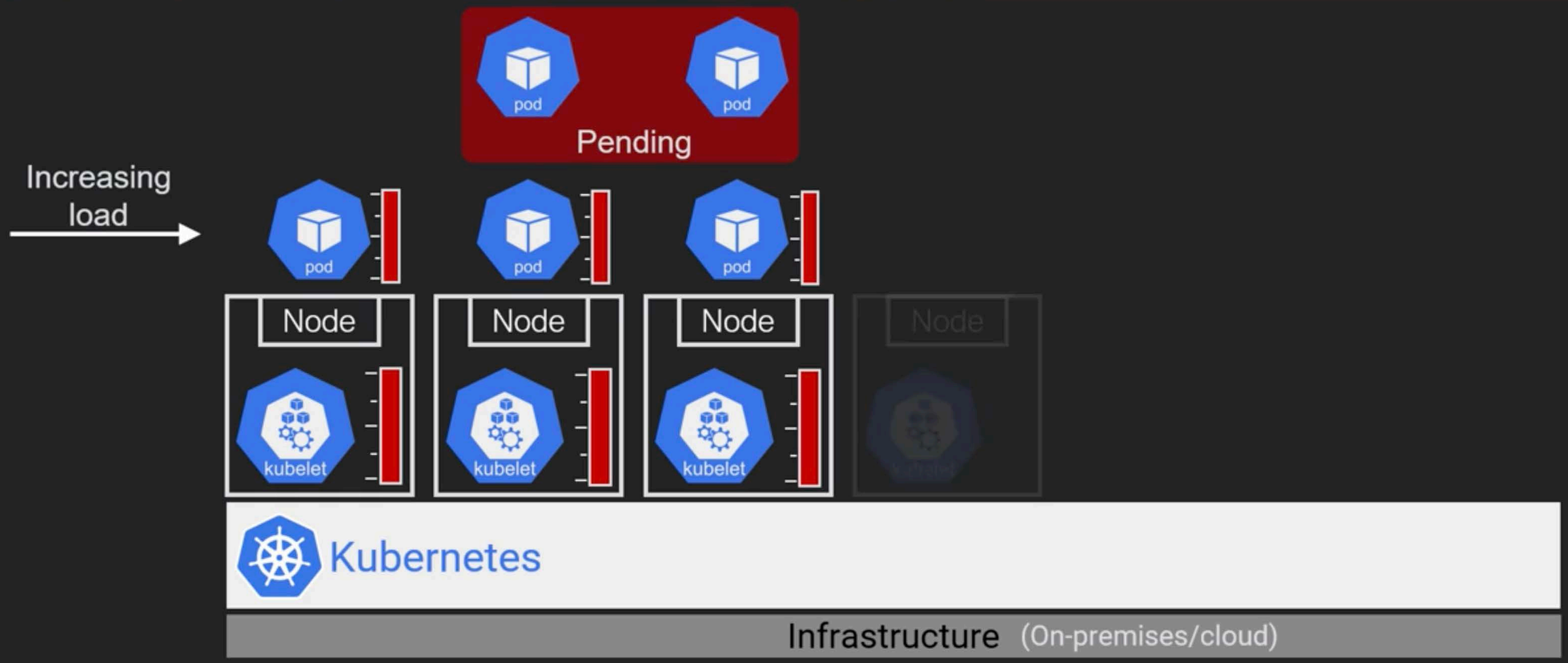
Lesson Plan

A CLOUD GURU

- Big Picture
- Horizontal Pod Autoscaler (HPA)
    - Theory
    - Demo
- Cluster Autoscaler(CA)
    - Theory
    - Demo
- Vertical Pod Autoscaler (VPA)
- Recap

Big Picture
A CLOUD GURU

Big Picture

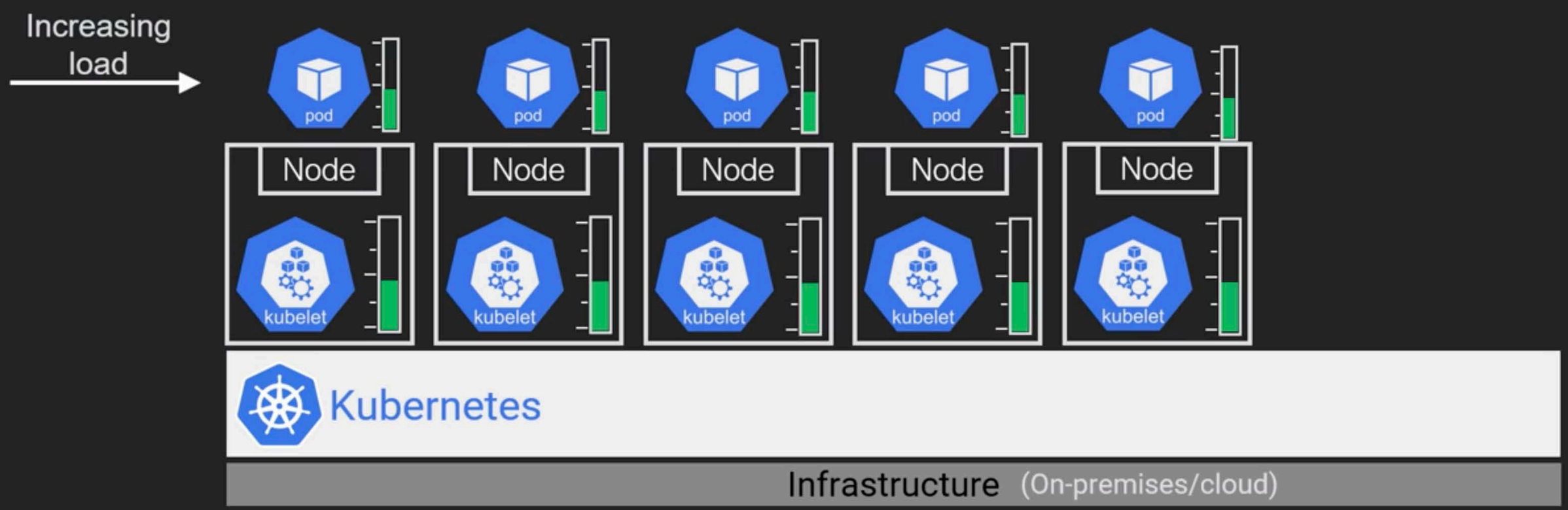


`autoscaling/v1` only supports CPU metric

`autoscaling/v2xx` adds support for memory and custom metrics

Big Picture

A CLOUD GURU



`autoscaling/v1` only supports CPU metric

`autoscaling/v2xx` adds support for memory and custom metrics

Big Picture

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    run: prod-redis
  name: prod-redis
spec:
  selector:
    matchLabels:
      run: prod-redis
  replicas: 3
  minReadySeconds: 300
```

Big Picture

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    run: prod-redis
  name: prod-redis
spec:
  selector:
    matchLabels:
      run: prod-redis
  replicas: 1 5
  minReadySeconds: 300
```

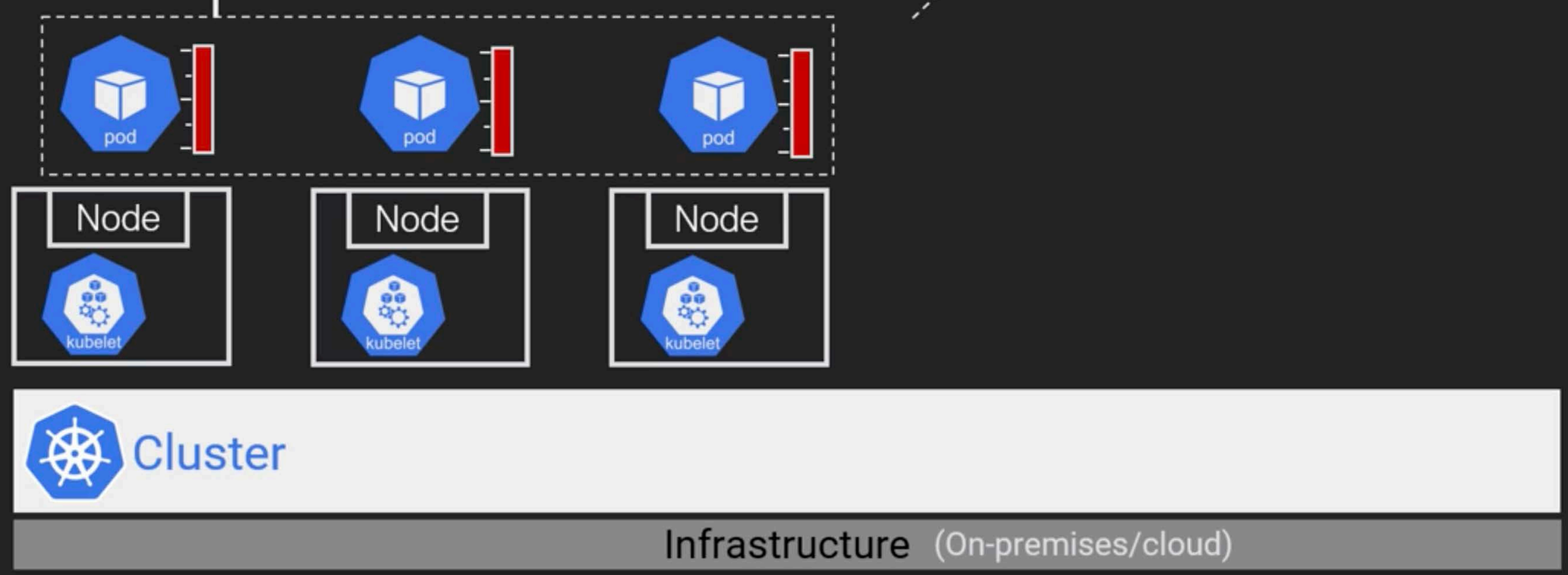
Big Picture

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
...
spec:
  replicas: 4
  ...
```

Scale to 4

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
...
spec:
  scaleTargetRef:
    name: my-deployment
    ...
```



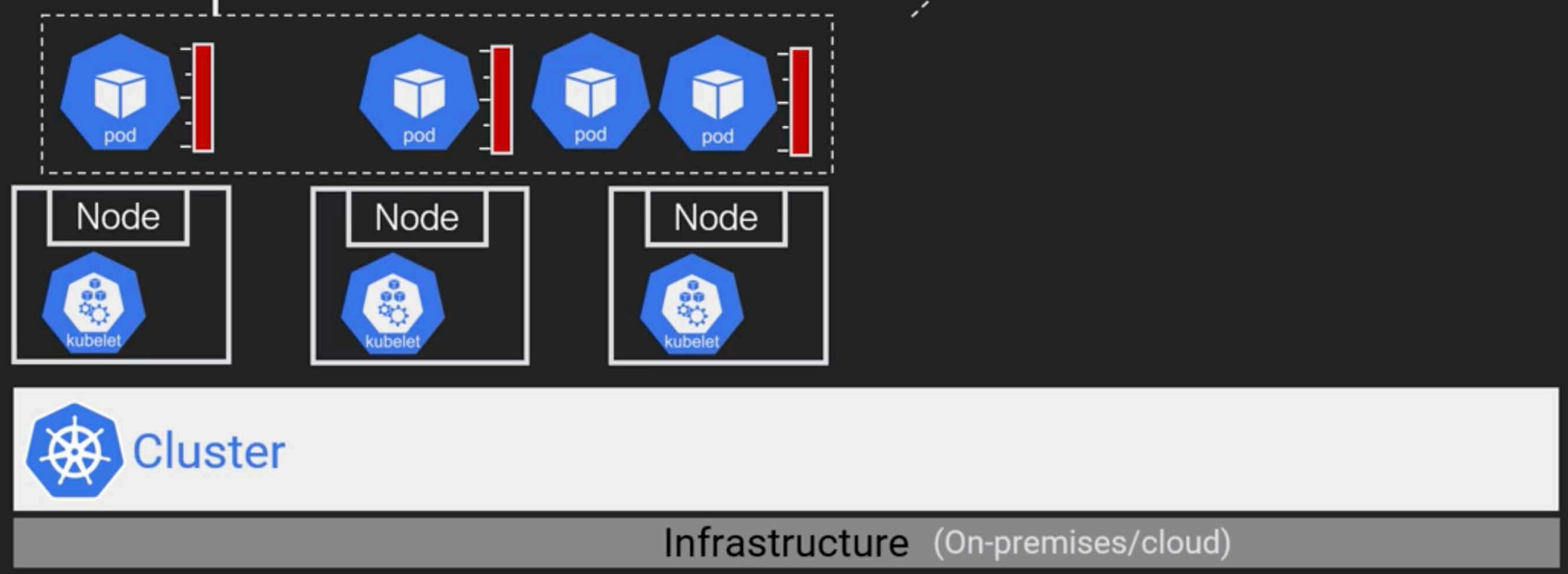
Big Picture

A CLOUD GURU

```
apiVersion: apps/v1
kind: Deployment
...
spec:
  replicas: 4
  ...
```

Scale to 4

```
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
...
spec:
  scaleTargetRef:
    name: my-deployment
    ...
```



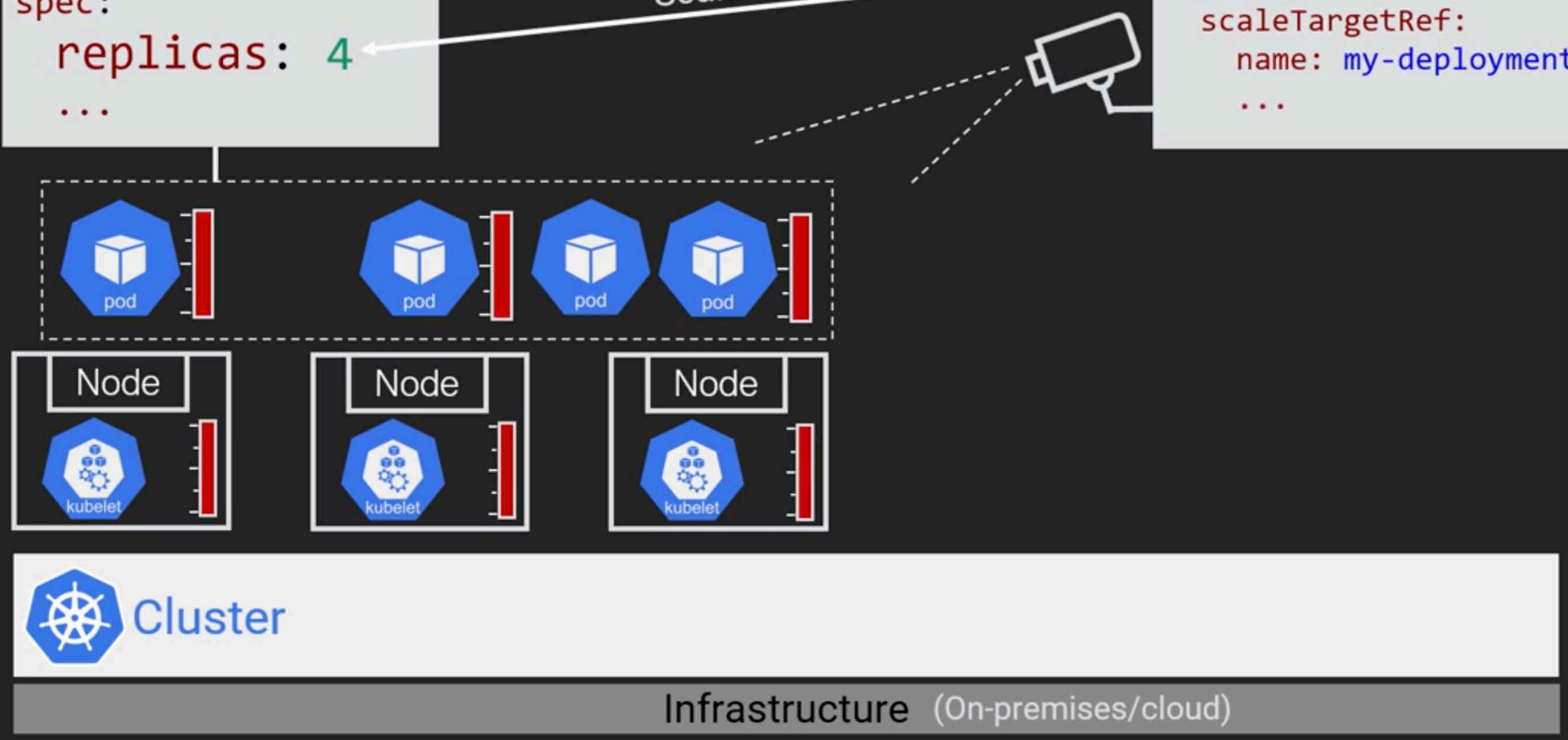
Big Picture

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
...
spec:
  replicas: 4
  ...
```

Scale to 4

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
...
spec:
  scaleTargetRef:
    name: my-deployment
    ...
```

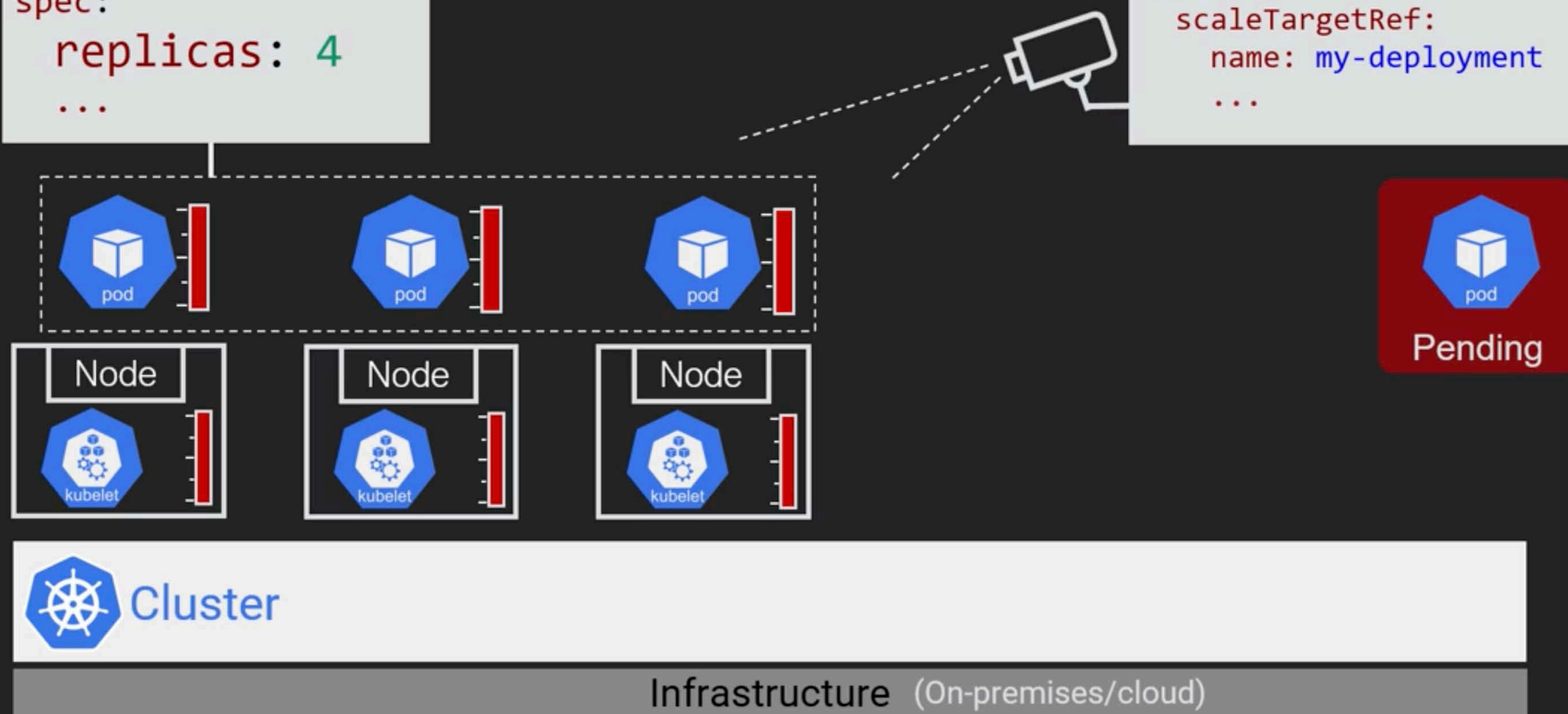


Big Picture

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
...
spec:
  replicas: 4
  ...
```

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
...
spec:
  scaleTargetRef:
    name: my-deployment
    ...
```

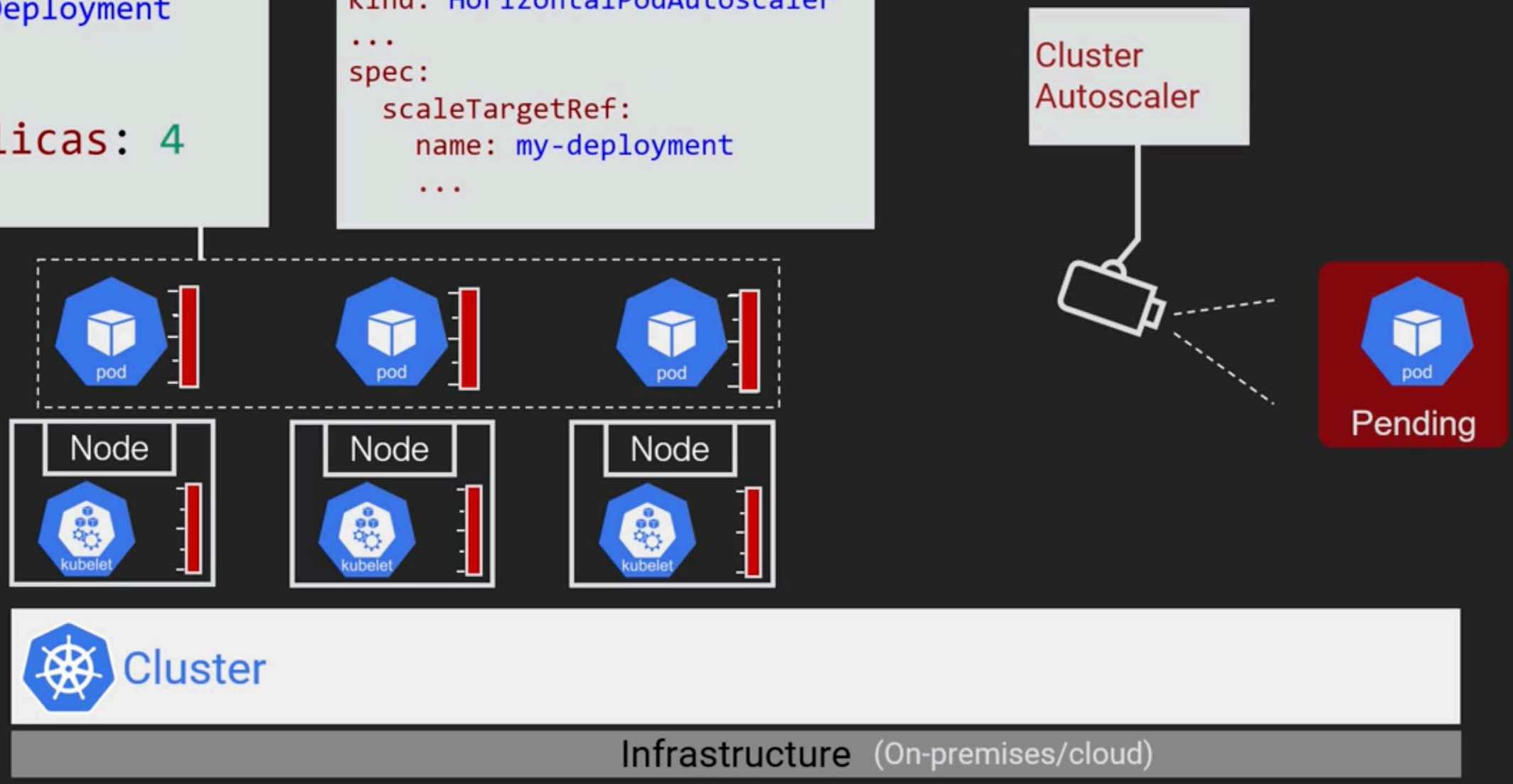


Big Picture

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
...
spec:
  replicas: 4
  ...
```

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
...
spec:
  scaleTargetRef:
    name: my-deployment
    ...
```

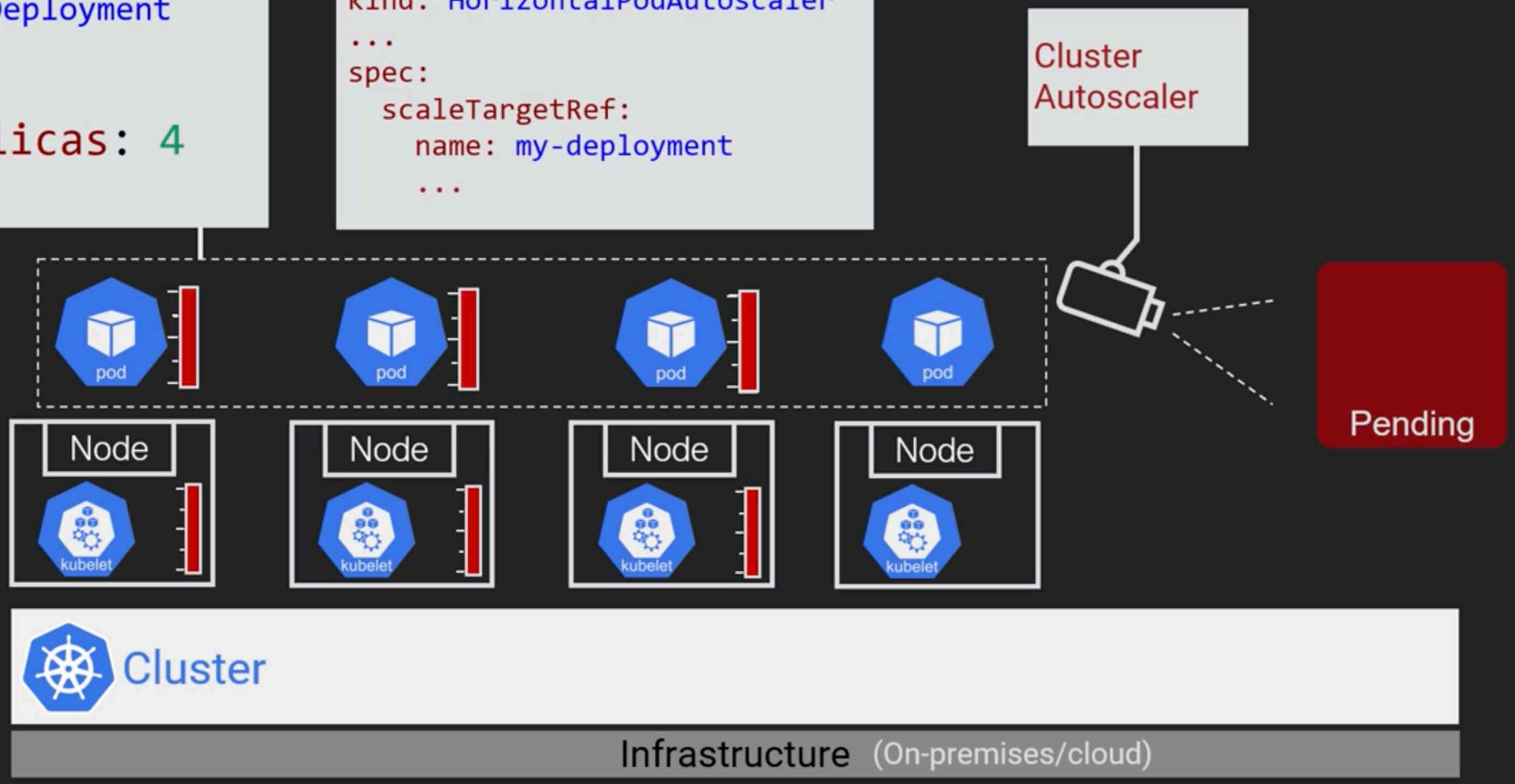


Big Picture

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
...
spec:
  replicas: 4
  ...
```

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
...
spec:
  scaleTargetRef:
    name: my-deployment
    ...
```

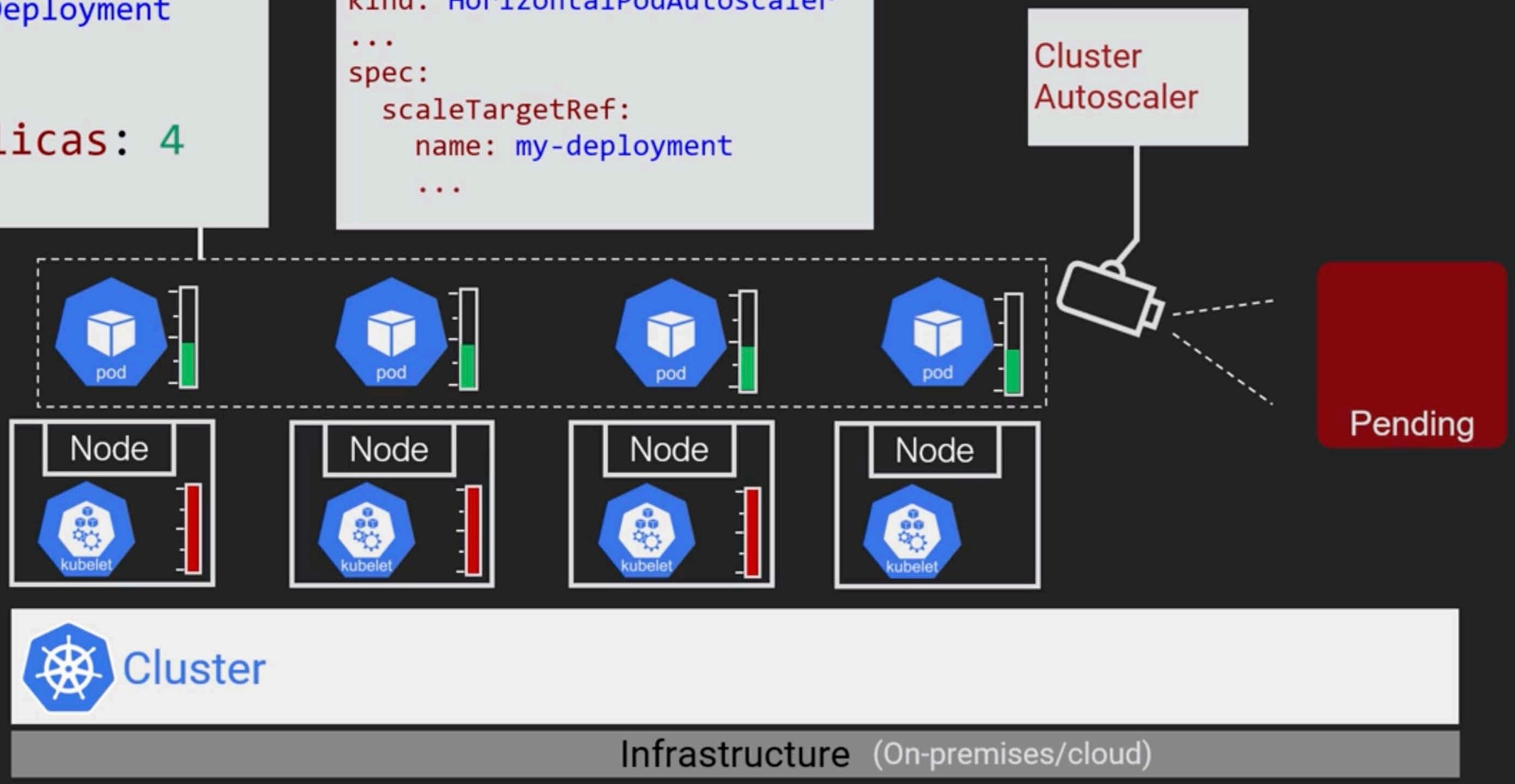


Big Picture

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
...
spec:
  replicas: 4
  ...
```

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
...
spec:
  scaleTargetRef:
    name: my-deployment
    ...
```



Big Picture

Vertical Pod Autoscaler (VPA)

Alpha product

Horizontal Pod Autoscaler Theory

A CLOUD GURU

Horizontal Pod Autoscaler - Theory

Horizontal Pod Autoscaler

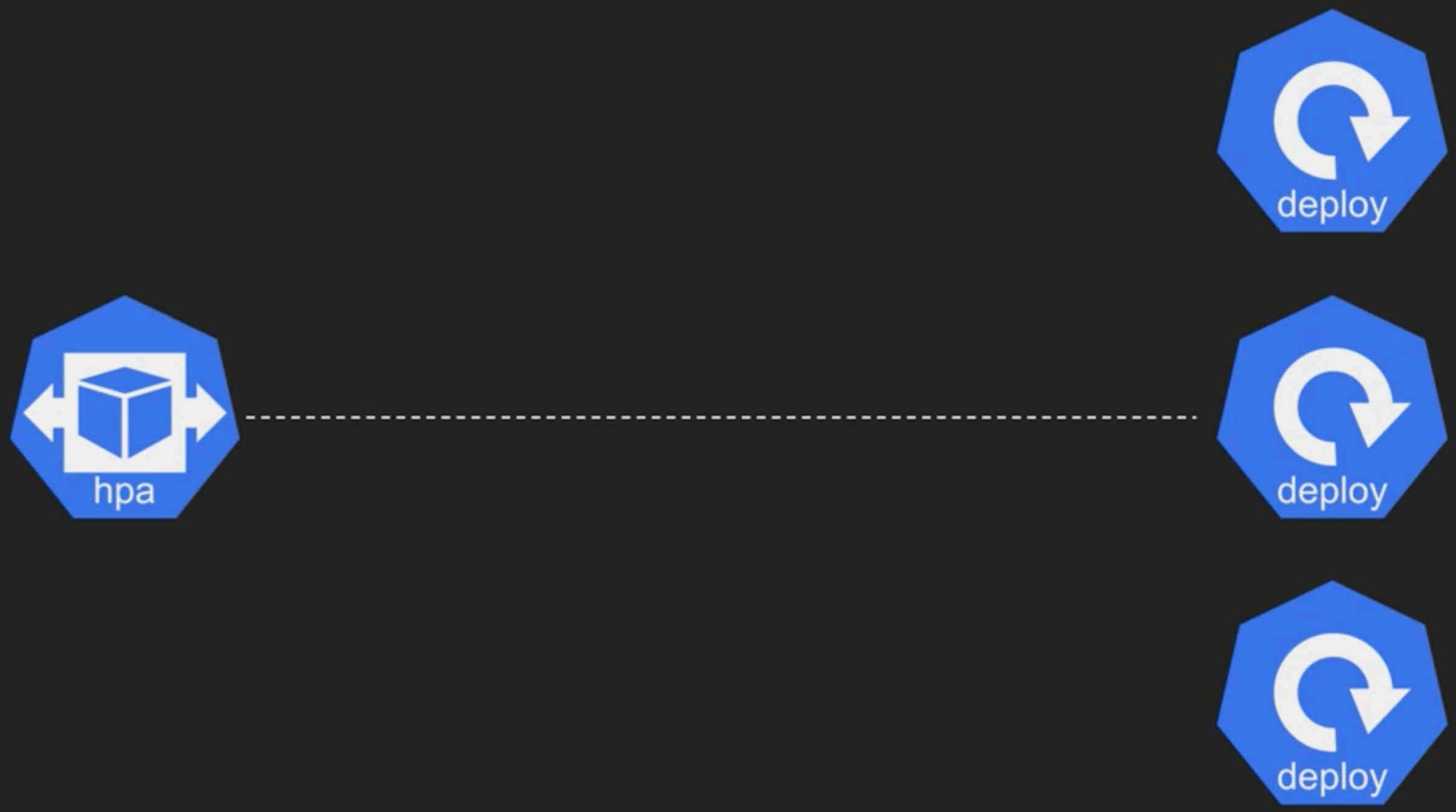
Horizontal Pod Autoscaler - Theory

Horizontal Pod Autoscaler

Horizontal Pod Autoscaler - Theory

Horizontal Pod **Autoscaler**

Horizontal Pod Autoscaler - Theory



Horizontal Pod Autoscaler - Theory

A CLOUD GURU

hpa

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: acg-test
  namespace: acg
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: acg-deploy
  minReplicas: 1
  maxReplicas: 10
targetCPUUtilizationPercentage: 50
```

deploy

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: acg-deploy
spec:
  replicas: 2
  ...
    spec:
      containers:
      - image: nginx:1.12
        name: nginx
        resources:
          limits:
            cpu: 1
          requests:
            cpu: 0.2
```

Horizontal Pod Autoscaler - Theory

A CLOUD GURU

hpa

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: acg-test
  namespace: acg
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: acg-deploy
  minReplicas: 1
  maxReplicas: 10
targetCPUUtilizationPercentage: 50
```

deploy

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: acg-deploy
spec:
  replicas: 2
  ...
    spec:
      containers:
      - image: nginx:1.12
        name: nginx
        resources:
          limits:
            cpu: 1
          requests:
            cpu: 0.2
```

Horizontal Pod Autoscaler - Theory

A CLOUD GURU

hpa

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: acg-test
  namespace: acg
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: acg-deploy
  minReplicas: 1
  maxReplicas: 10
targetCPUUtilizationPercentage: 50
```

```
1000m = 1CPU
1 = 1CPU

500m = ½CPU
0.5 = ½CPU

250m = ¼CPU
0.25 = ¼CPU
```

deploy

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: acg-deploy
spec:
  replicas: 2
  ...
    spec:
      containers:
      - image: nginx:1.12
        name: nginx
        resources:
          limits:
            cpu: 1
          requests:
            cpu: 0.2 “200m”
```

Horizontal Pod Autoscaler - Theory

A CLOUD GURU

hpa

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: acg-test
  namespace: acg
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: acg-deploy
  minReplicas: 1
  maxReplicas: 10
targetCPUUtilizationPercentage: 50
```

deploy

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: acg-deploy
spec:
  replicas: 2
  ...
    spec:
      containers:
      - image: nginx:1.12
        name: nginx
        resources:
          limits:
            cpu: 1
          requests:
            cpu: 0.2
```

Horizontal Pod Autoscaler - Theory

A CLOUD GURU

hpa

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: acg-test
  namespace: acg
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: acg-deploy
  minReplicas: 1
  maxReplicas: 10
targetCPUUtilizationPercentage: 50
```

50% of 20% of a CPU is 10% of a CPU :-D

deploy

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: acg-deploy
spec:
  replicas: 2
  ...
    spec:
      containers:
      - image: nginx:1.12
        name: nginx
        resources:
          limits:
            cpu: 1
          requests:
            cpu: 0.2
```

Horizontal Pod Autoscaler - Theory

A CLOUD GURU

hpa

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: acg-test
  namespace: acg
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: acg-deploy
  minReplicas: 1
  maxReplicas: 10
targetCPUUtilizationPercentage: 50
```

deploy

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: acg-deploy
spec:
  replicas: 2
  ...
    spec:
      containers:
      - image: nginx:1.12
        name: nginx
        resources:
          limits:
            cpu: 1
          requests:
            cpu: 0.2
```

The autoscaling/v2 API will bring custom metrics etc.

Horizontal Pod Autoscaler - Theory

A CLOUD GURU

hpa

```yaml
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: acg-test
  namespace: acg
spec:
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: acg-deploy
  minReplicas: 1
  maxReplicas: 10
targetCPUUtilizationPercentage: 50
```

deploy

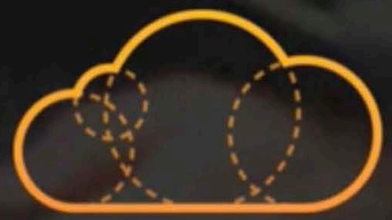
```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: acg-deploy
spec:
  replicas: 10
  ...
    spec:
      containers:
      - image: nginx:1.12
        name: nginx
        resources:
          limits:
            cpu: 1
          requests:
            cpu: 0.2
```

The autoscaling/v2 API will bring custom metrics etc.

Horizontal Pod Autoscaler Demo

A CLOUD GURU

Cluster Autoscaler Theory



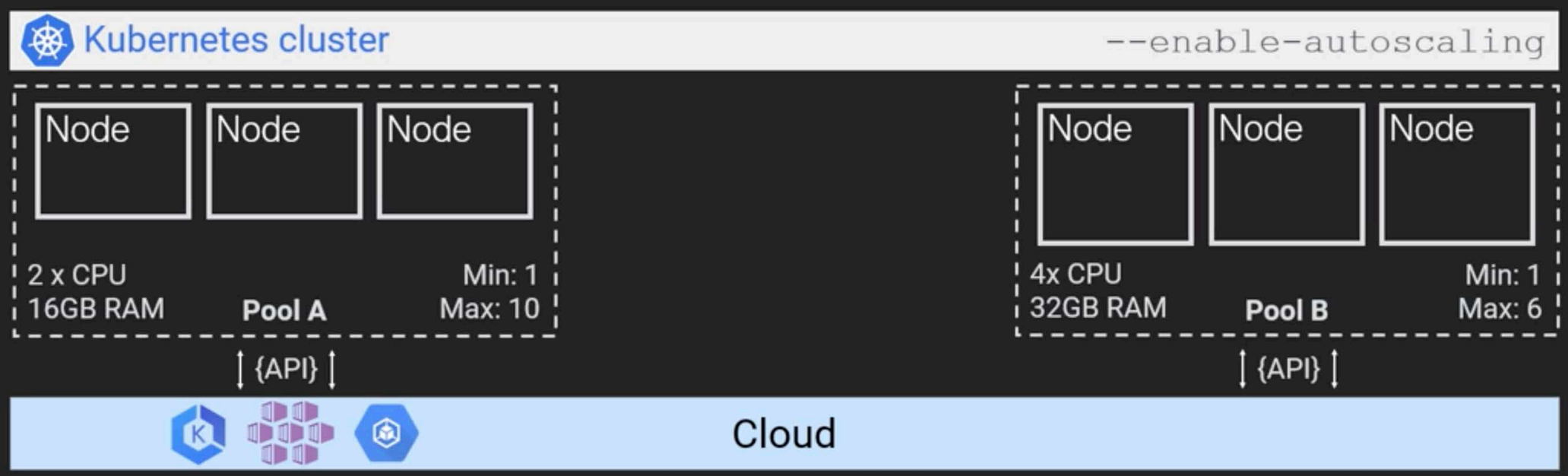
A CLOUD GURU

Cluster Autoscaler - Theory

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
spec:
...
    spec:
      resources:
        requests:
            cpu: 1
```

Always use
Pod Resource Requests

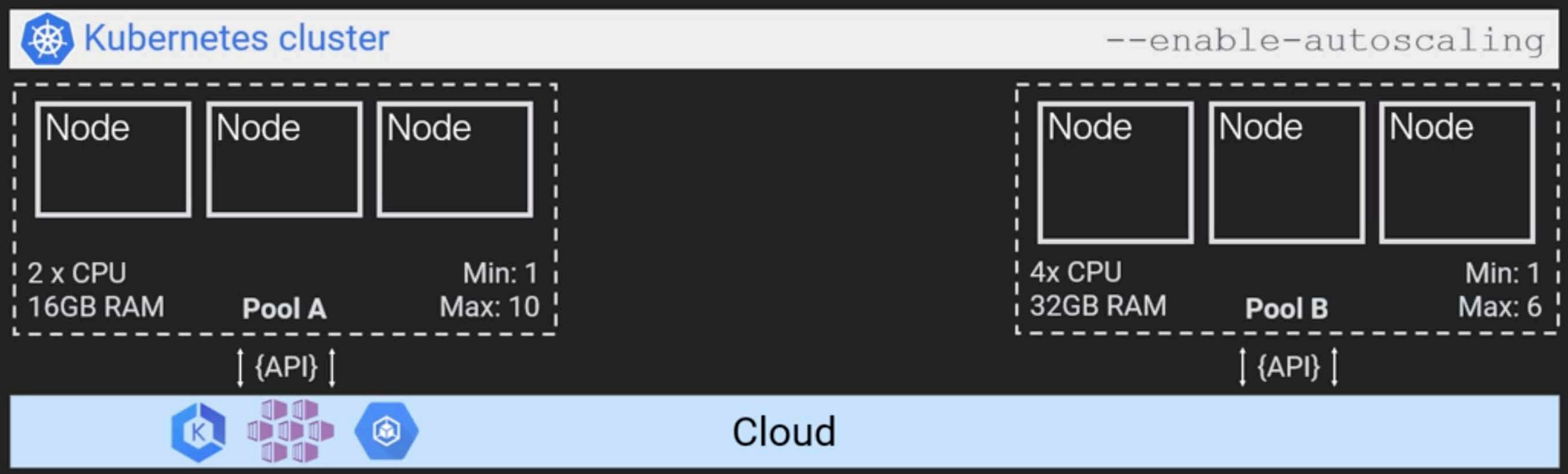


Cluster Autoscaler - Theory

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
spec:
...
    spec:
      resources:
        requests:
            cpu: 1
```

CPU=1



Cluster Autoscaler - Theory

```yaml
apiVersion: apps/v1
kind: Deployment
spec:
...
    spec:
      resources:
        requests:
          cpu: 1
```

Pending

Kubernetes cluster

`--enable-autoscaling`

Node Node Node

2 x CPU
16GB RAM

Pool A

Min: 1
Max: 10

Requested

Actual

Node Node Node

4x CPU
32GB RAM

Pool B

Min: 1
Max: 6

Requested

Actual

{API}

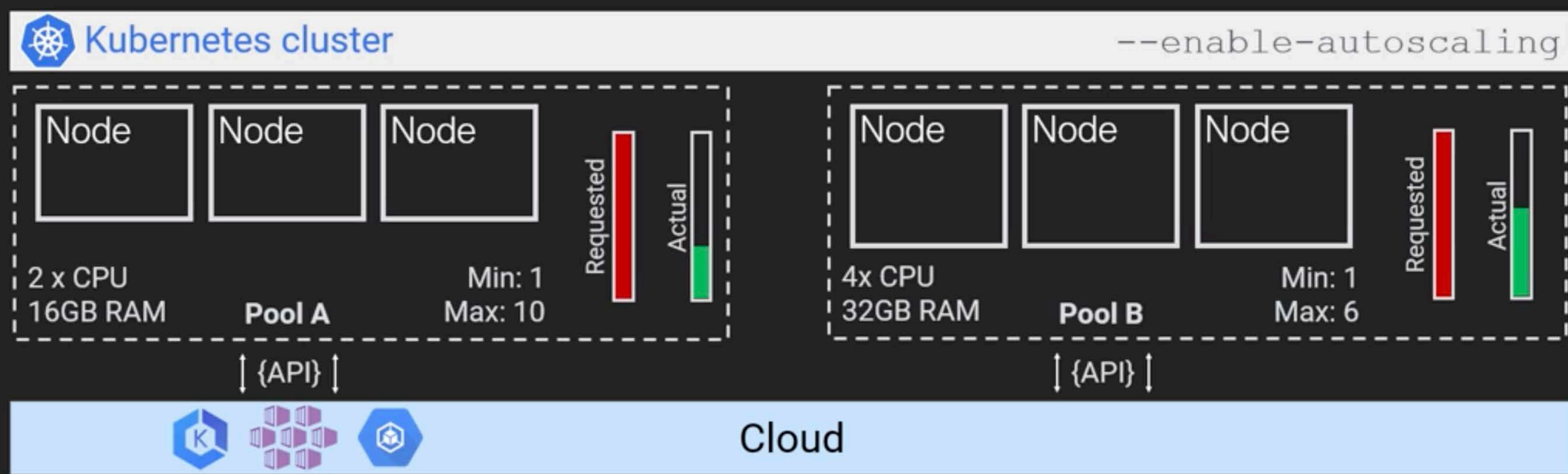
{API}

Cloud

Cluster Autoscaler - Theory

A CLOUD GURU

```yaml
apiVersion: apps/v1
kind: Deployment
spec:
...
    spec:
      resources:
        requests:
          cpu: 1
```



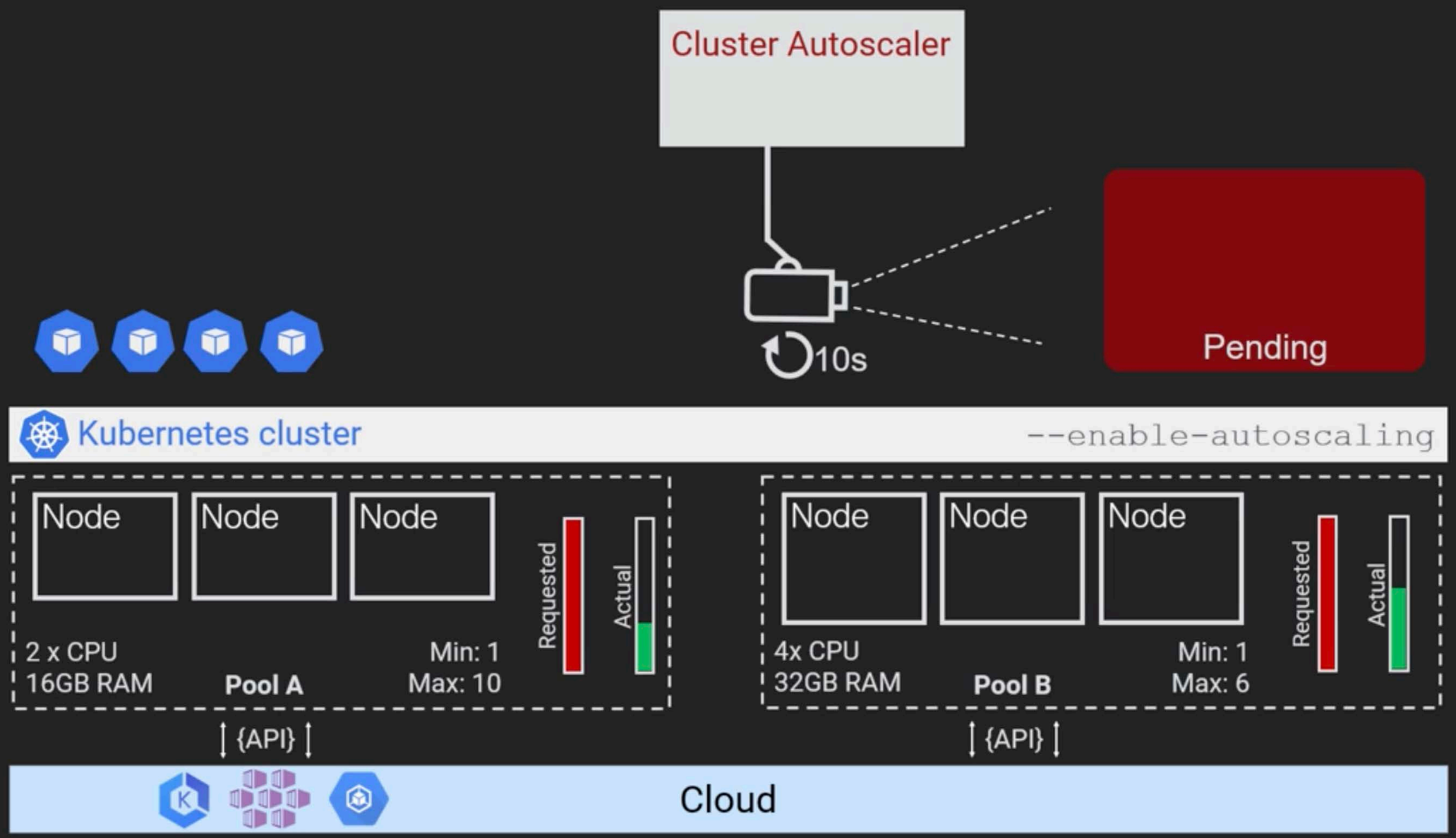
Cluster Autoscaler - Theory

A CLOUD GURU

Cluster Autoscaler	Works on **requested** values
Horizontal Pod Autoscaler	Works on **actual** values

Cluster Autoscaler - Theory

A CLOUD GURU



Cluster Autoscaler - Theory

Don’t mess with the node pools

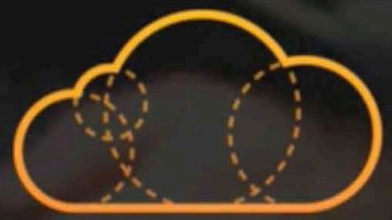
Check your cloud for support

Test performance on big clusters

Cluster Autoscaler Demo

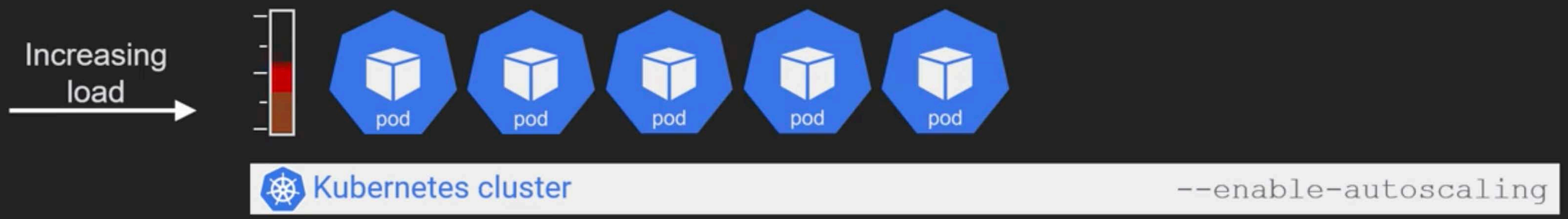
A CLOUD GURU

Recap

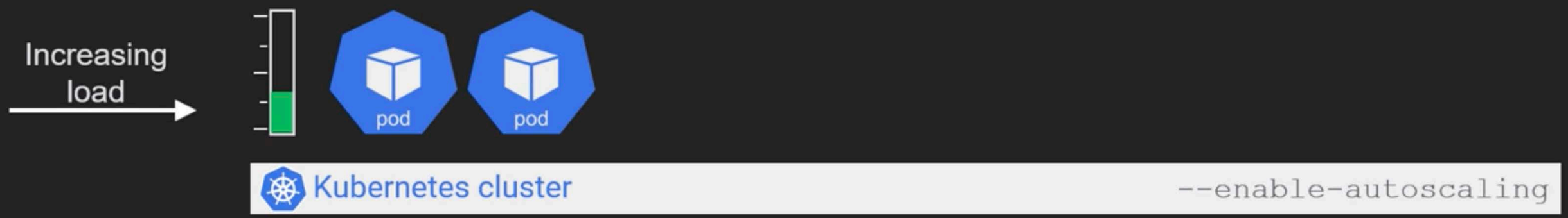


A CLOUD GURU

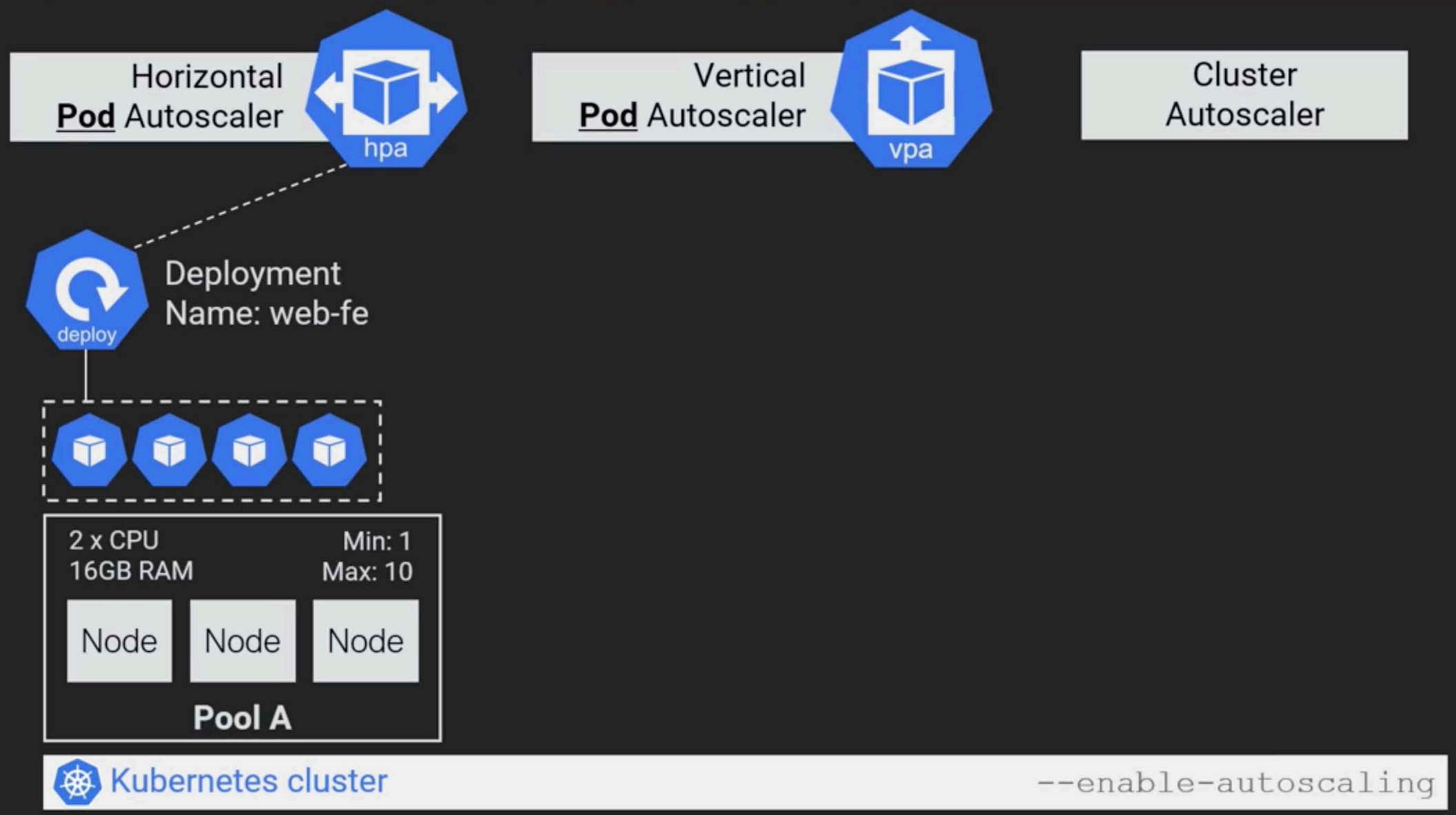
Recap


Increasing load
pod
pod
pod
pod
pod
Kubernetes cluster
--enable-autoscaling

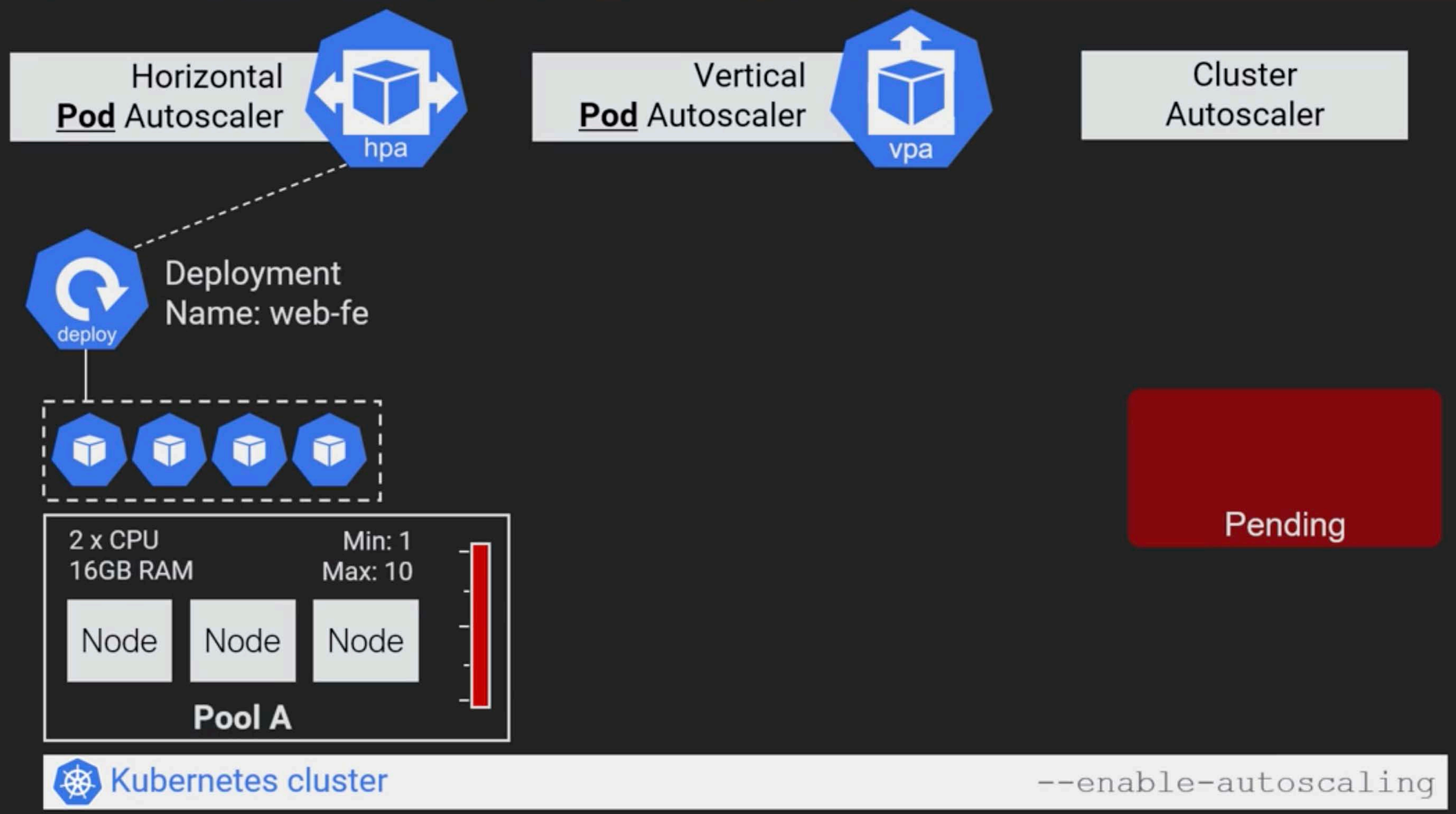
Recap


Increasing load
pod
pod
Kubernetes cluster
--enable-autoscaling

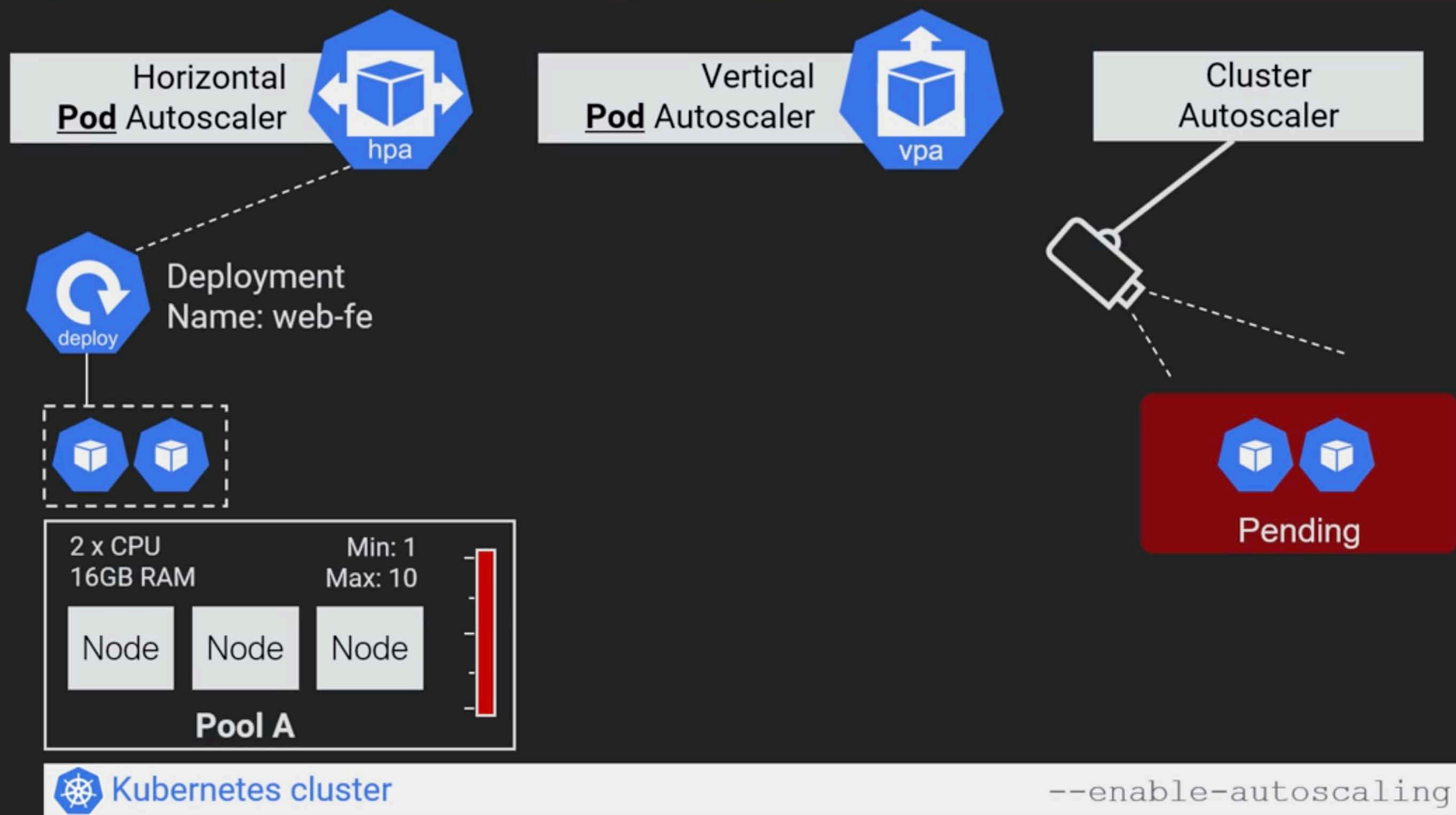
Recap


Horizontal
Pod Autoscaler
hpa
Vertical
Pod Autoscaler
vpa
Cluster
Autoscaler
deploy
Deployment
Name: web-fe
2 x CPU
16GB RAM
Min: 1
Max: 10
Node
Node
Node
Pool A
Kubernetes cluster
--enable-autoscaling

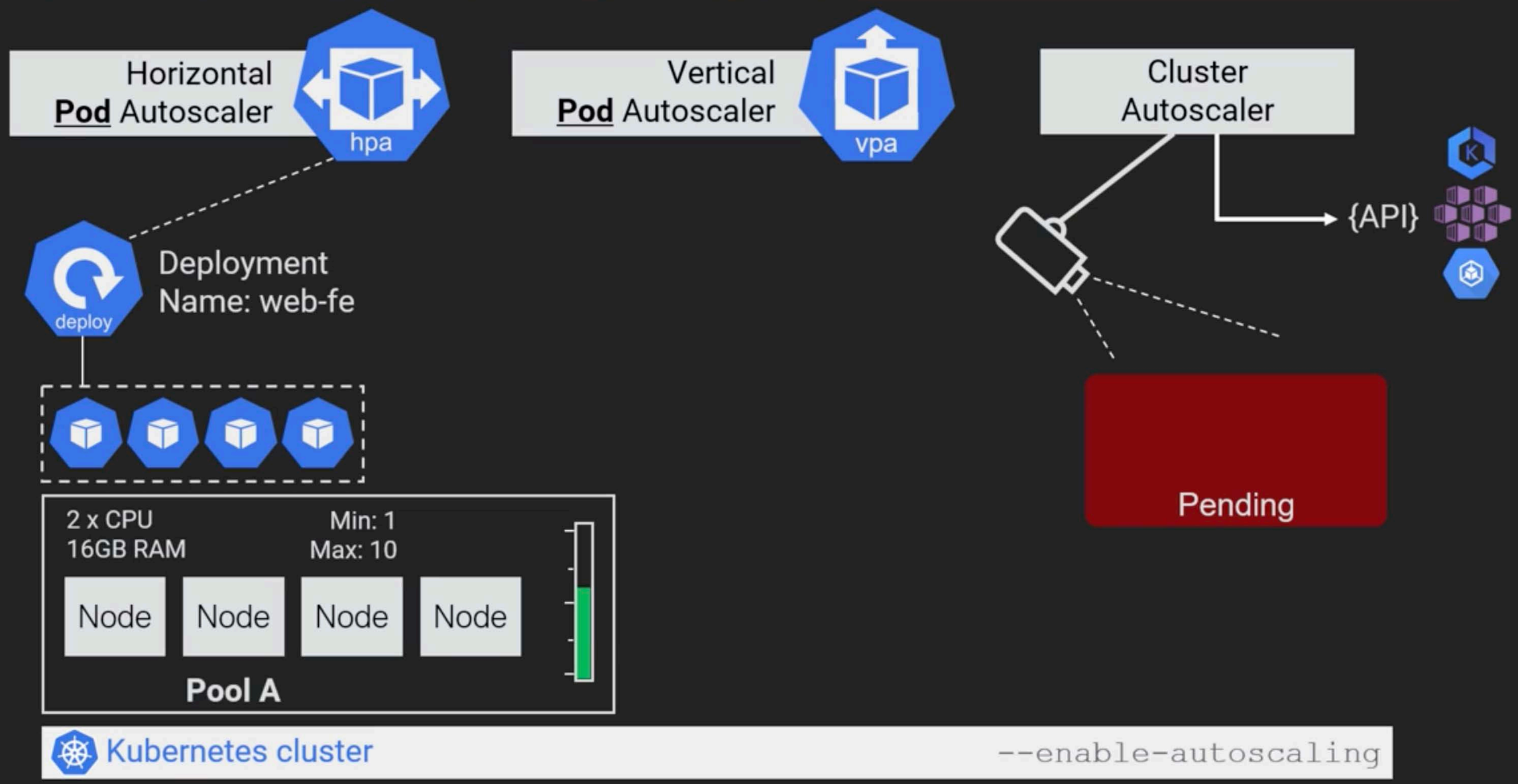
Recap


Horizontal
Pod Autoscaler
hpa
Vertical
Pod Autoscaler
vpa
Cluster
Autoscaler
deploy
Deployment
Name: web-fe
2 x CPU
16GB RAM
Min: 1
Max: 10
Node
Node
Node
Pool A
Pending
Kubernetes cluster
--enable-autoscaling

Recap


Horizontal
Pod Autoscaler
hpa
Vertical
Pod Autoscaler
vpa
Cluster
Autoscaler
deploy
Deployment
Name: web-fe
Pending
2 x CPU
16GB RAM
Min: 1
Max: 10
Node
Node
Node
Pool A
Kubernetes cluster
--enable-autoscaling

Recap


Horizontal
Pod Autoscaler
hpa
Vertical
Pod Autoscaler
vpa
Cluster
Autoscaler
{API}
deploy
Deployment
Name: web-fe
Pending
2 x CPU
16GB RAM
Min: 1
Max: 10
Node
Node
Node
Node
Pool A
Kubernetes cluster
--enable-autoscaling

Recap

`autoscaling/v1`
- CPU

`autoscaling/v2`
- CPU, memory, **custom metrics**

RBAC and Admission Control

A CLOUD GURU

Lesson Plan

A CLOUD GURU

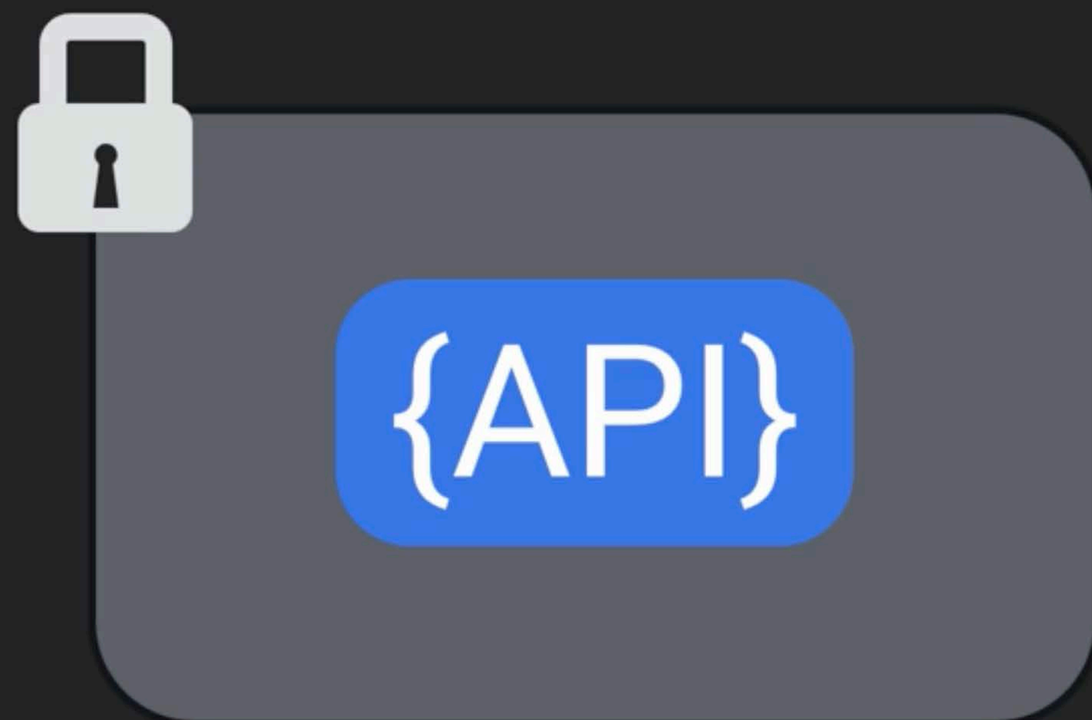
- Big Picture
- Authentication (AuthN)
- Authorization (AuthZ)
- Admission Control

Big Picture

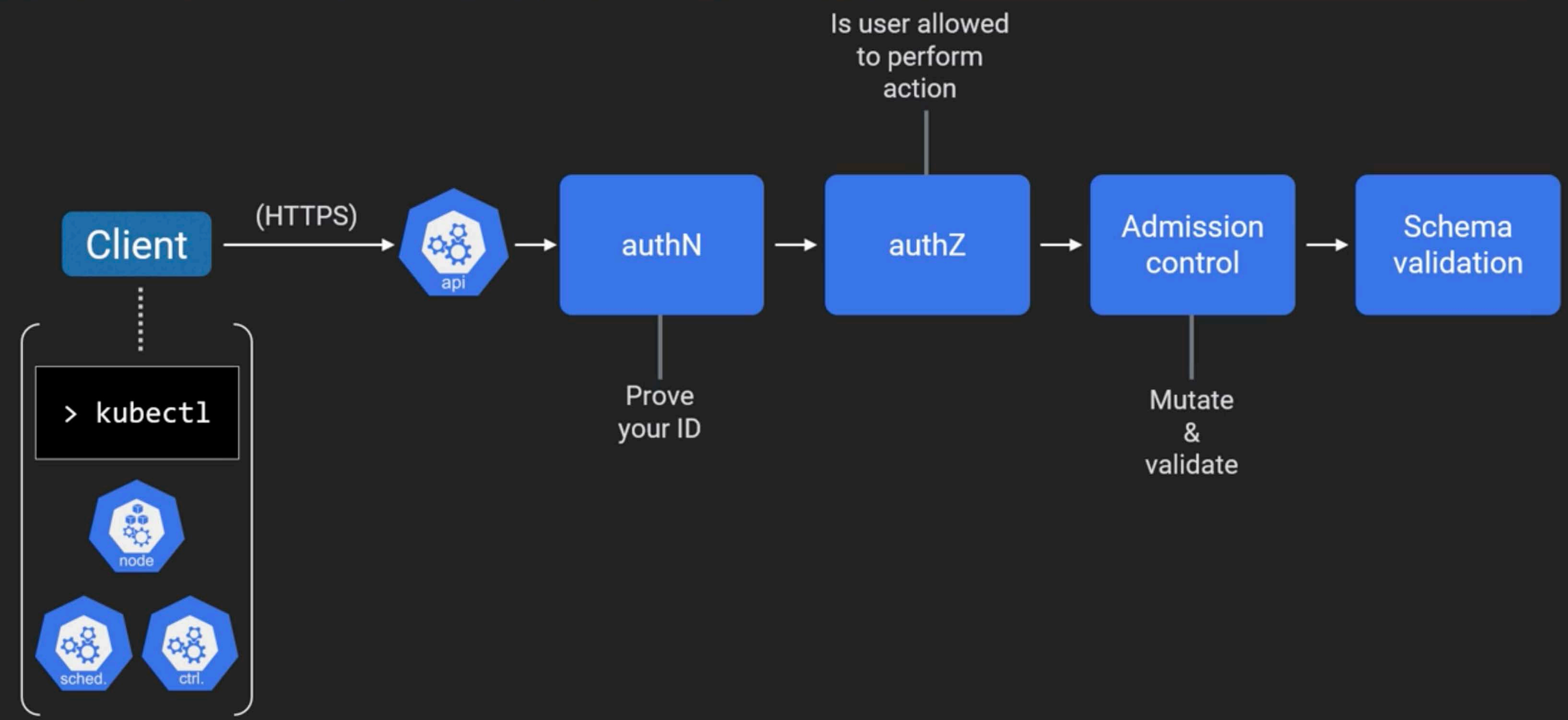
A CLOUD GURU

Big Picture

A CLOUD GURU

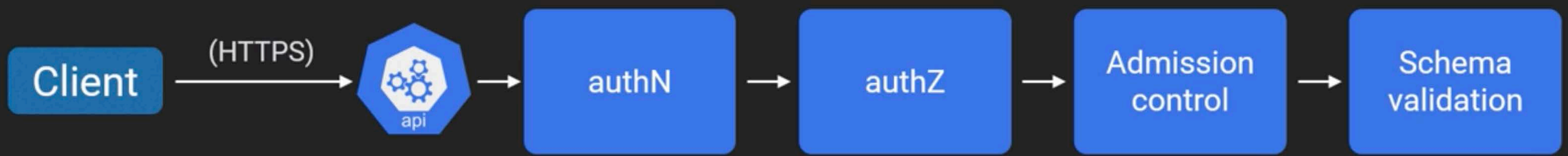


Big Picture


Is user allowed to perform action
Client
(HTTPS)
api
authN
authZ
Admission control
Schema validation
> kubectl
node
sched.
ctrl.
Prove your ID
Mutate & validate

Big Picture

A CLOUD GURU



Some clusters open an insecure local port!

Bypasses authN and authZ!!

Disable for prod!

Big Picture

RBAC

Enabled since 1.6

GA since 1.8

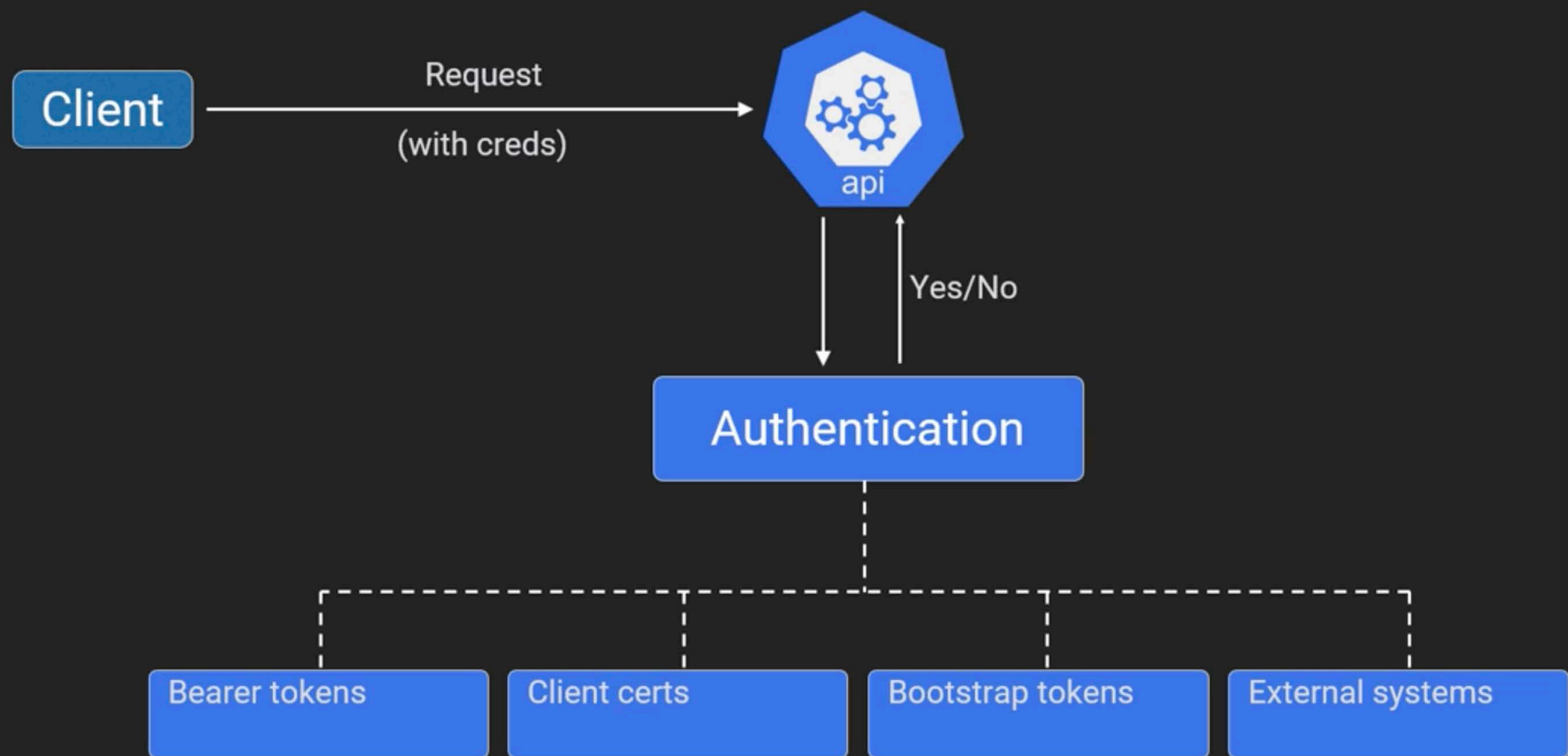
Deny-by-default

Authentication

(authN)

A CLOUD GURU

Authentication



Authentication

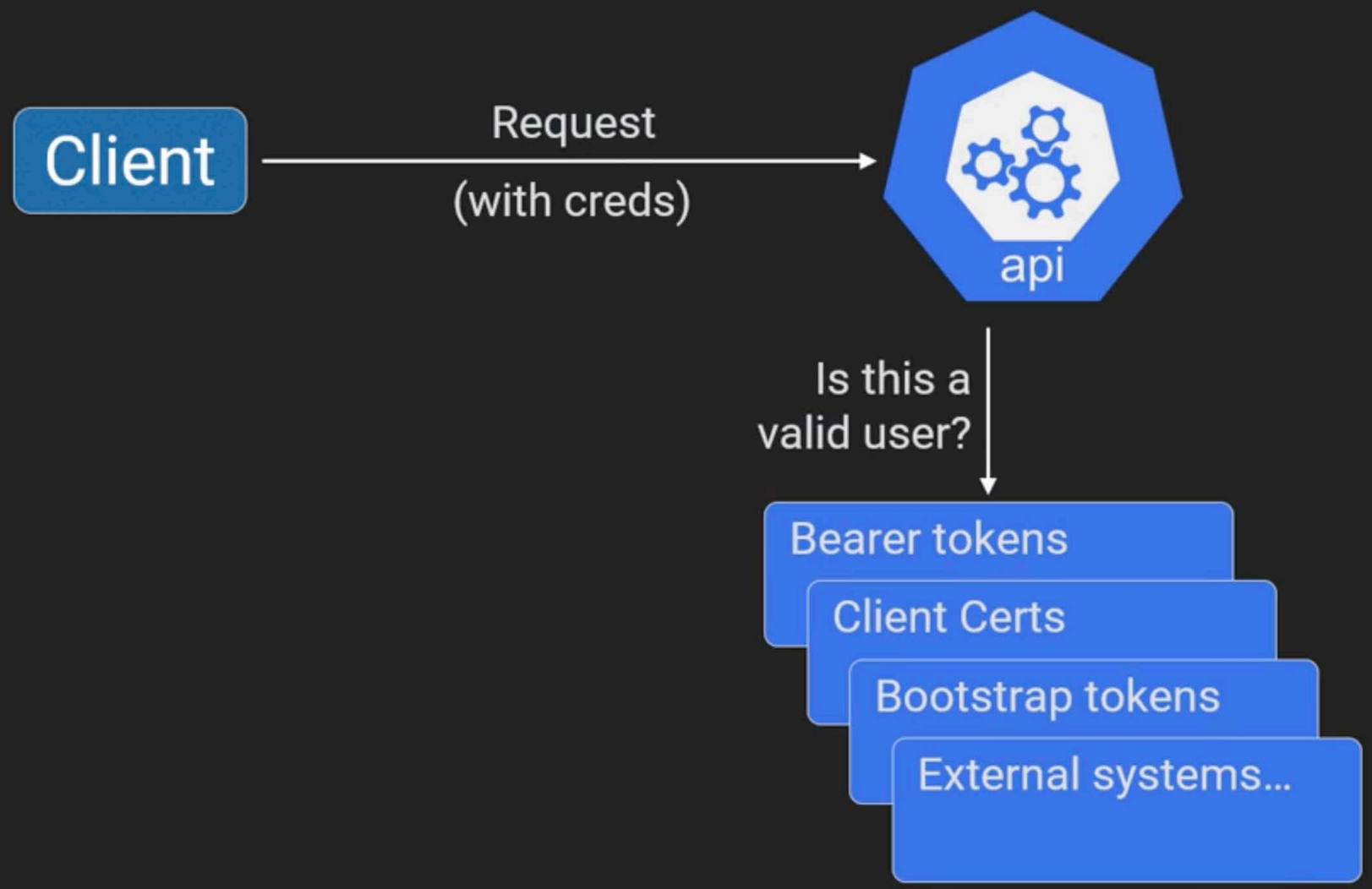
A CLOUD GURU

Kubernetes does **NOT** do Users!!

Manage Users externally

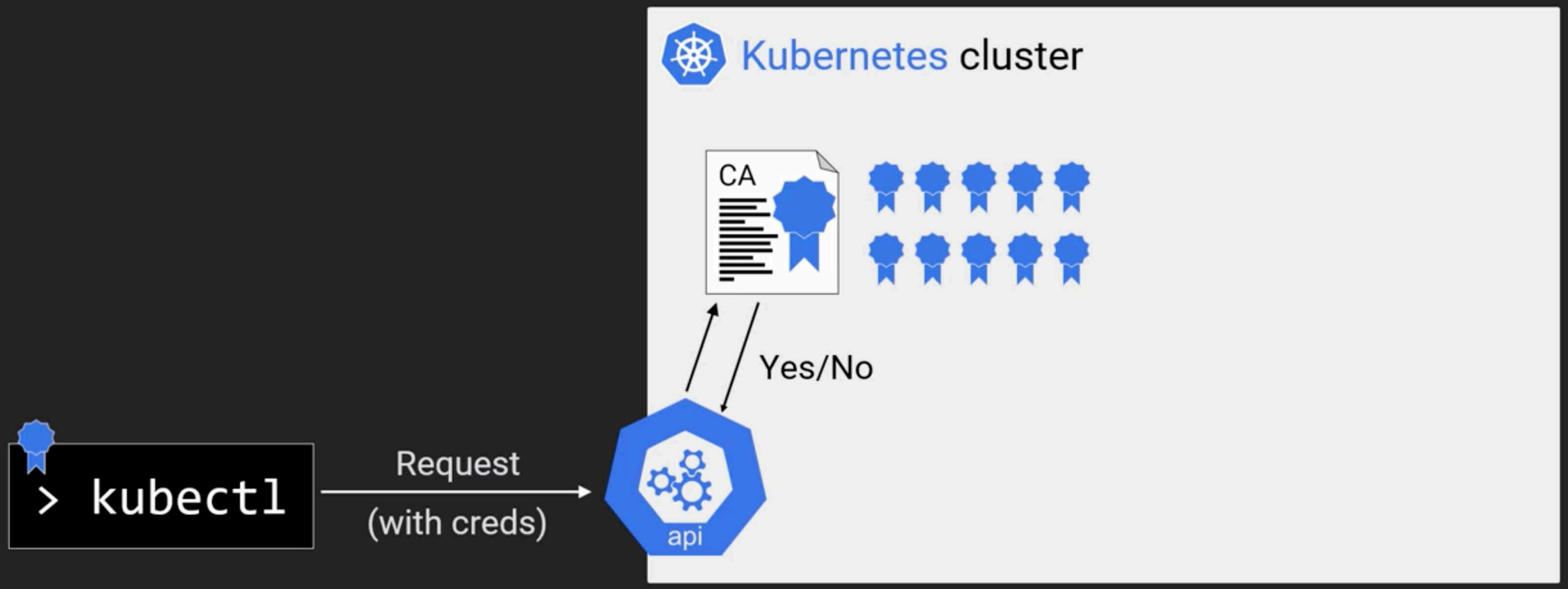
- Active Directory
- IAM
- Other...

Authentication



Authentication

A CLOUD GURU



A CLOUD GURU

Service Accounts

For `System` components

Managed by Kubernetes

You can (should) manage them

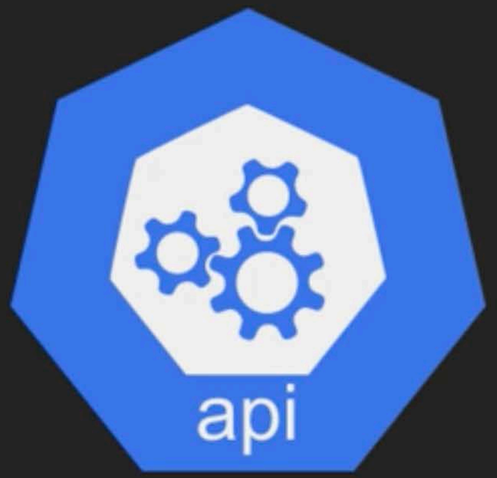
Authentication

A CLOUD GURU

```
> kubectl
```

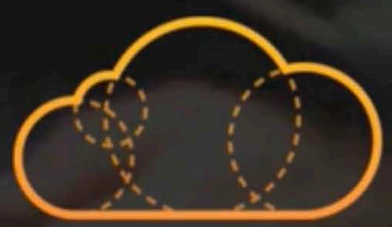
POST:
/apis/apps/v1/namespaces/acg-ns/deployments

Auth: Token FGg5dYFnsdY%351tg..
{"apiVersion":"1","kind":"Deployment"....}
...



API Group:	apps/v1
Subject:	nigel
Verb:	create (HTTP POST method)
Resource:	Deployments
Namespace:	acg

Authorization
(authz)



A CLOUD GURU

Authorization

A CLOUD GURU

Who can perform which actions on which resources?

Subject

lily
pushkar
sam
abi
system:authenticated

Verb

create
get
watch
delete
update

Resource

deployments
pods
services
crd

Authorization

Powerful default users
(Too powerful for production)

Roles & RoleBindings
(For *least privilege*)

Authorization

A CLOUD GURU

RBAC Role

```yaml
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
```

RBAC RoleBinding

```yaml
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
subjects:
- kind: User
  name: nigel@acg.com
  apiGroup: ""
roleRef:
  kind: Role
  name: acgrbac
  apiGroup: ""
```

Authorization

A CLOUD GURU

RBAC Role

```yaml
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
```

RBAC RoleBinding

```yaml
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
subjects:
- kind: User
  name: nigel@acg.com
  apiGroup: ""
- kind: Group
  name: ops
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: acgrbac
  apiGroup: ""
```

Authorization

A CLOUD GURU

RBAC Role

```yaml
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["*"]
  resources: ["*"]
  verbs: ["*"]
```

RBAC RoleBinding

```yaml
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
subjects:
- kind: User
  name: nigel@acg.com
  apiGroup: ""
- kind: Group
  name: ops
  apiGroup: rbac.authorization.k8s.io
- kind: Group
  name: system:masters
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: acgrbac
  apiGroup: ""
```

Authorization

A CLOUD GURU

Role | ClusterRole

```yaml
kind: Role | ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["*"]
  resources: ["*"]
  verbs: ["*"]
```

RoleBinding | ClusterRoleBinding

```yaml
kind: RoleBinding | ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
subjects:
- kind: User
  name: nigel@acg.com
  apiGroup: ""
- kind: Group
  name: ops
  apiGroup: rbac.authorization.k8s.io
- kind: Group
  name: system:masters
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: acgrbac
  apiGroup: ""
```

Authorization

A CLOUD GURU

Role | ClusterRole

```yaml
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["*"]
  resources: ["*"]
  verbs: ["*"]
```

RoleBinding | ClusterRoleBinding

```yaml
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
subjects:
- kind: User
  name: nigel@acg.com
  apiGroup: ""
- kind: Group
  name: ops
  apiGroup: rbac.authorization.k8s.io
- kind: Group
  name: system:masters
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: acgrbac
  apiGroup: ""
```

Authorization

A CLOUD GURU

ClusterRole

```yaml
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["*"]
  resources: ["*"]
  verbs: ["*"]
```

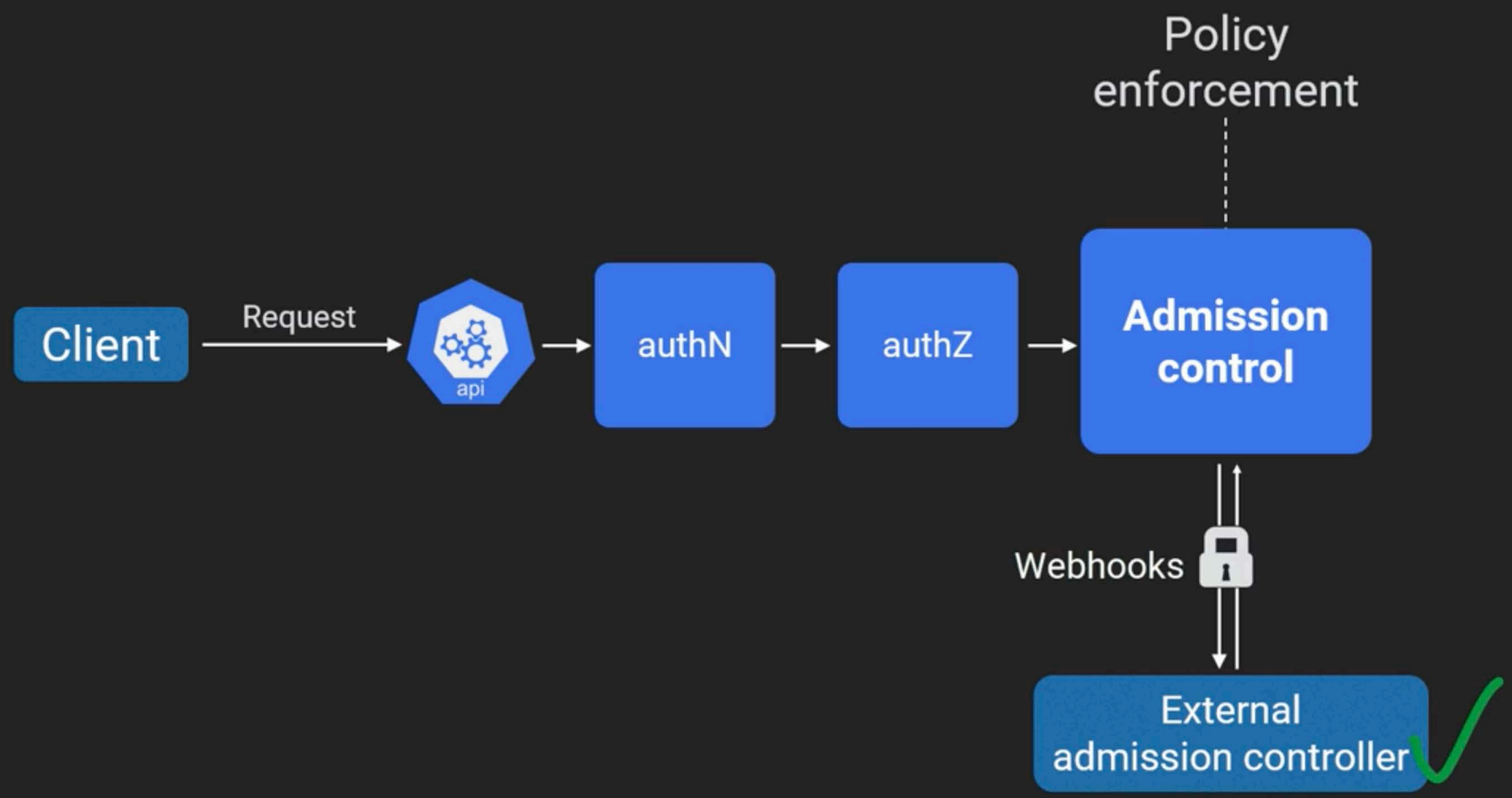
RoleBinding

```yaml
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
subjects:
- kind: User
  name: nigel@acg.com
  apiGroup: ""
- kind: Group
  name: ops
  apiGroup: rbac.authorization.k8s.io
- kind: Group
  name: system:masters
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: acgrbac
  apiGroup: ""
```

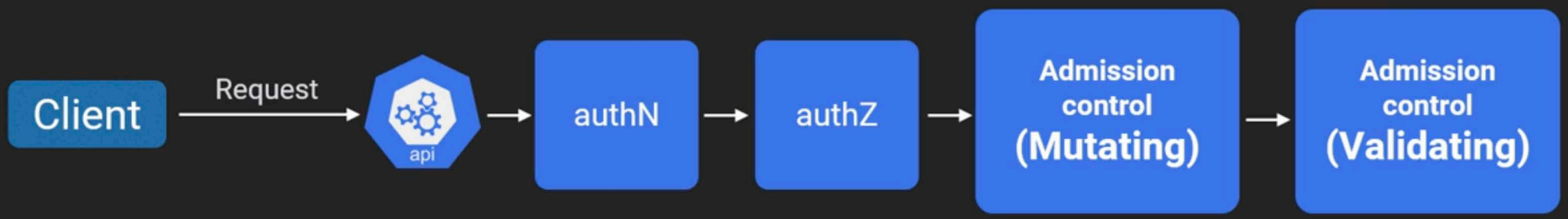
Admission Control

A CLOUD GURU

Admission Control



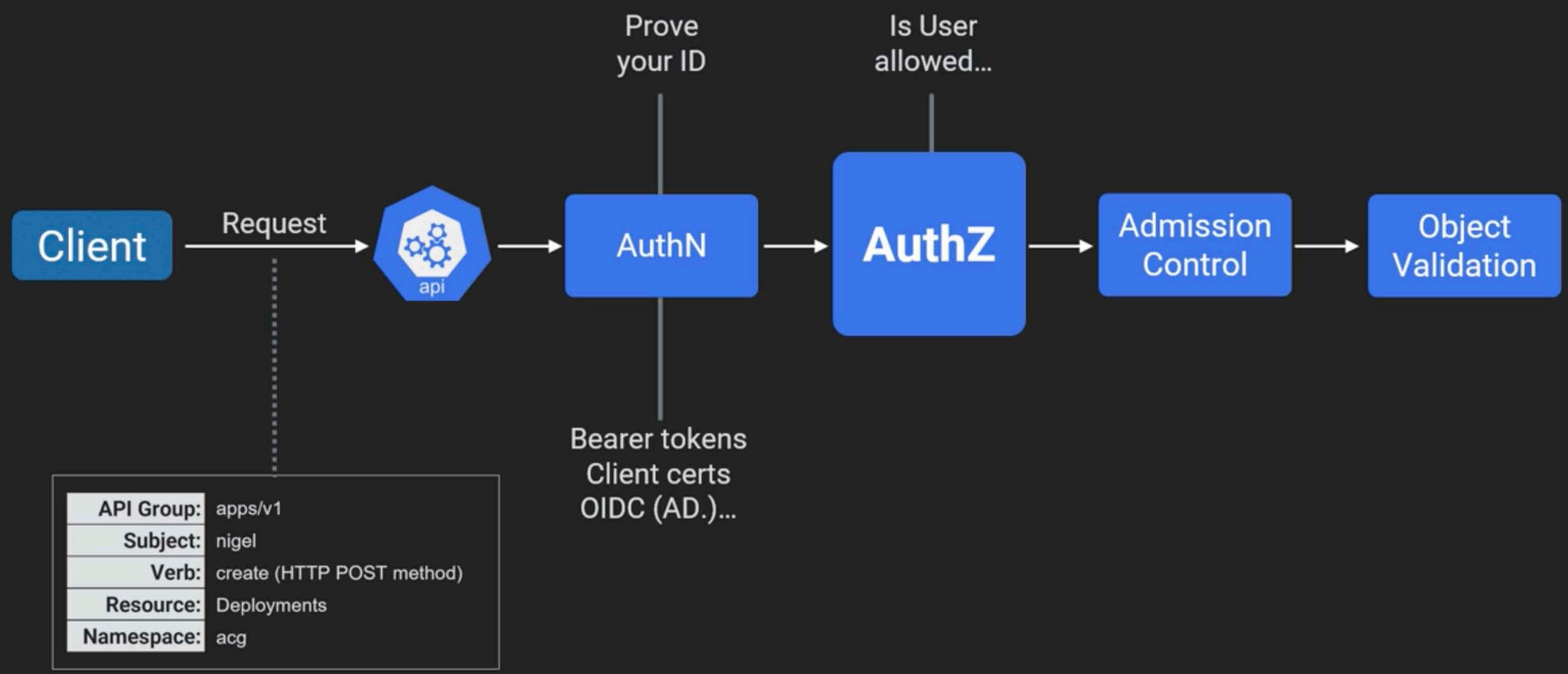
Admission Control



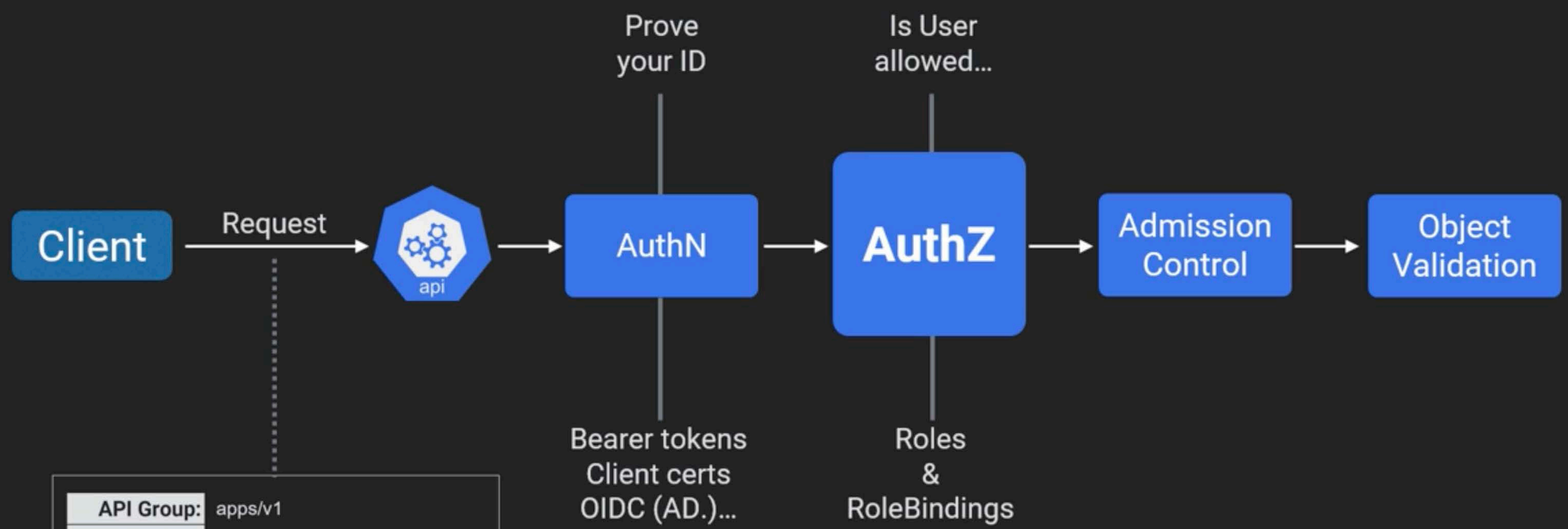
Recap

A CLOUD GURU

Recap


Client
Request
api
Prove your ID
AuthN
Is User allowed...
AuthZ
Admission Control
Object Validation
Bearer tokens
Client certs
OIDC (AD.)...
API Group: apps/v1
Subject: nigel
Verb: create (HTTP POST method)
Resource: Deployments
Namespace: acg

Recap



API Group:	apps/v1
Subject:	nigel
Verb:	create (HTTP POST method)
Resource:	Deployments
Namespace:	acg

Recap

A CLOUD GURU

RBAC Role

```yaml
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
rules:
- apiGroups: ["apps"]
  resources: ["deployments"]
  verbs: ["get", "list", "watch",
    "create", "update", "patch", "delete"]
```

RBAC RoleBinding

```yaml
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acg-test
  namespace: acg
subjects:
- kind: User
  name: nigel
  apiGroup: ""
roleRef:
  kind: Role
  name: acgrbac
  apiGroup: ""
```

Recap

A CLOUD GURU

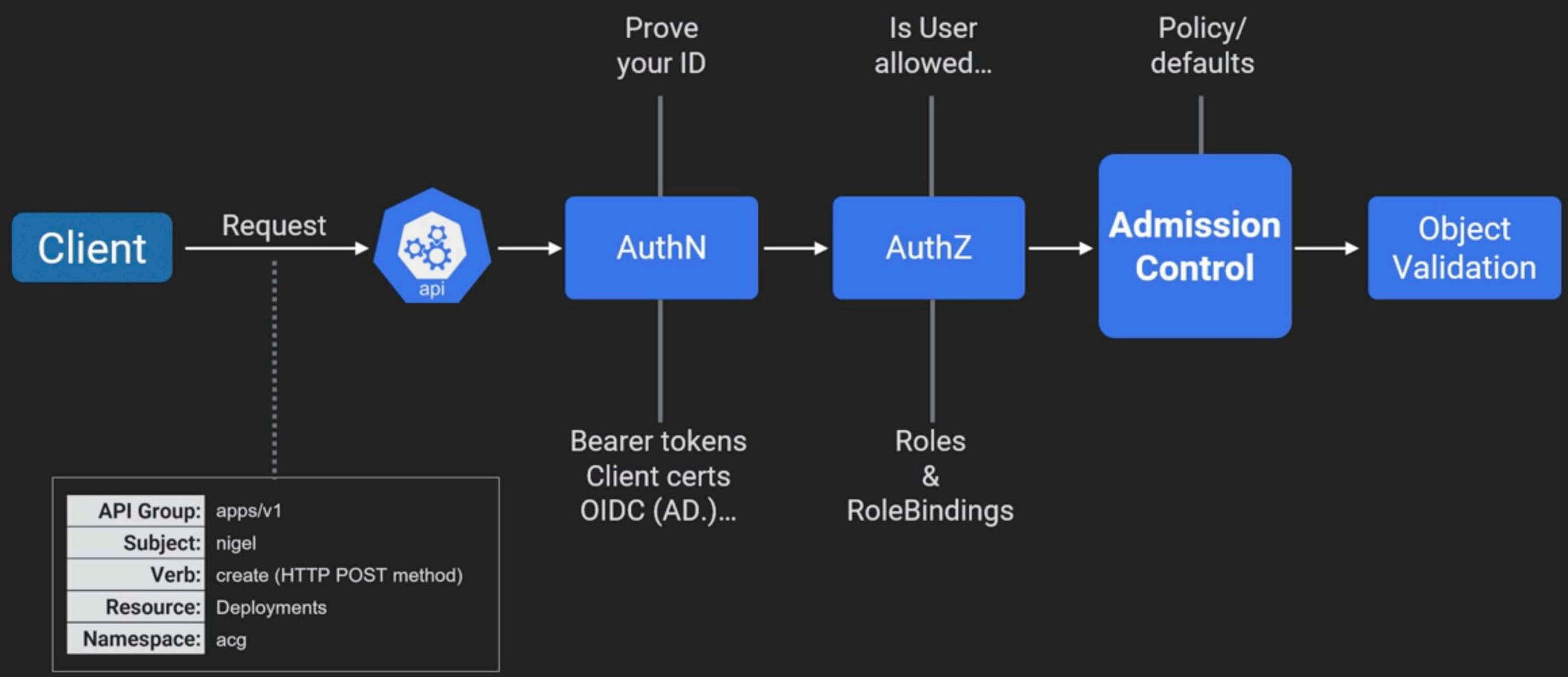
RBAC Role

```yaml
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acgrbac
  namespace: acg
rules:
- apiGroups: ["apps"]
  resources: ["deployments"]
  verbs: ["get", "list", "watch",
    "create", "update", "patch", "delete"]
```

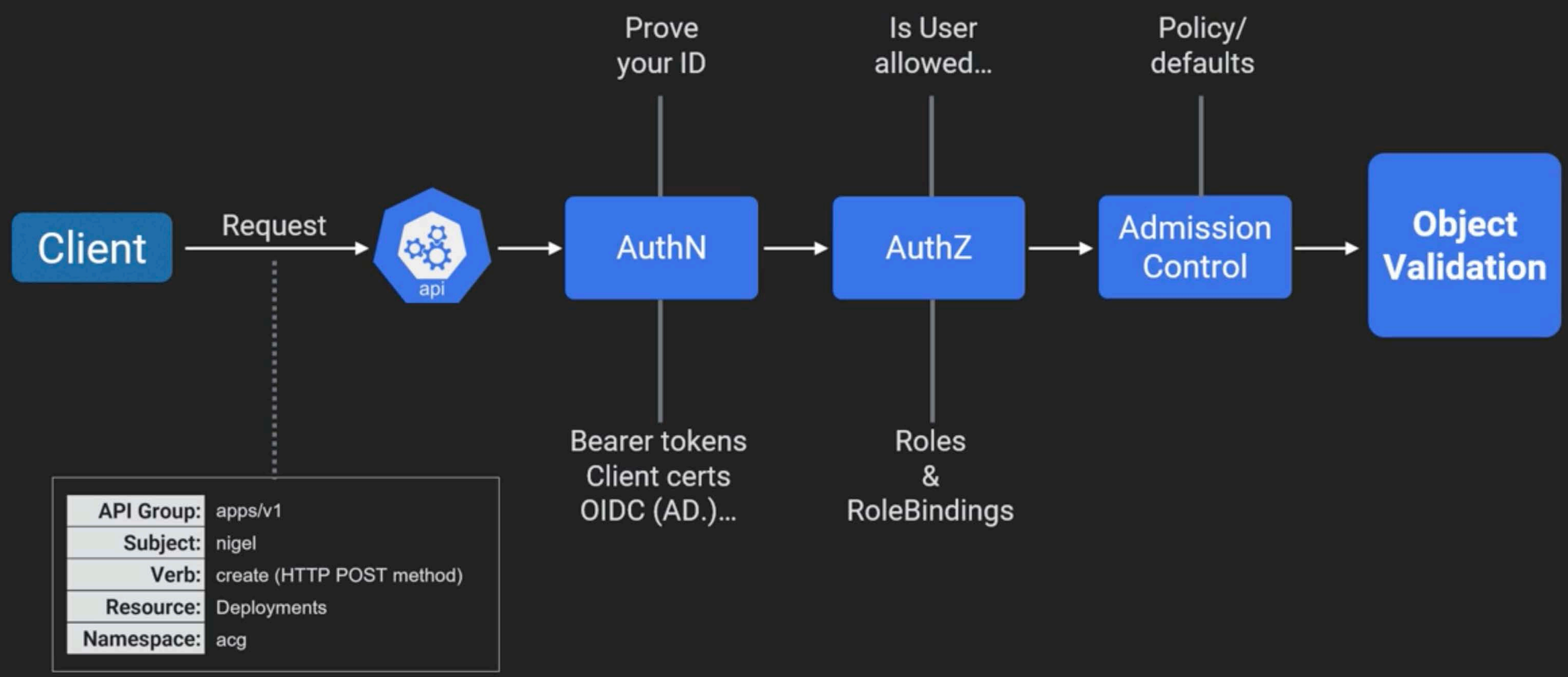
RBAC RoleBinding

```yaml
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: acg-test
  namespace: acg
subjects:
- kind: User
  name: nigel
  apiGroup: ""
roleRef:
  kind: Role
  name: acgrbac
  apiGroup: ""
```

Recap

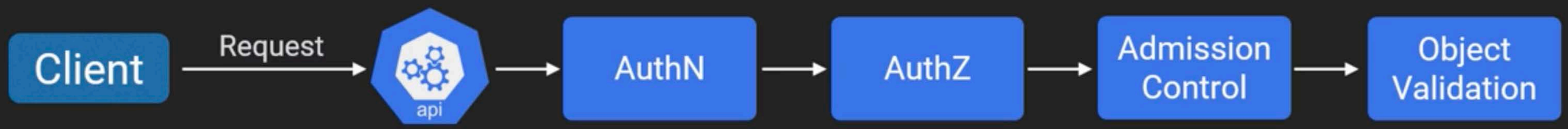

Prove your ID
Is User allowed...
Policy/ defaults
Client
Request
api
AuthN
AuthZ
Admission Control
Object Validation
Bearer tokens
Client certs
OIDC (AD.)...
Roles
&
RoleBindings
API Group: apps/v1
Subject: nigel
Verb: create (HTTP POST method)
Resource: Deployments
Namespace: acg

Recap


Client
Request
api
Prove your ID
AuthN
Is User allowed...
AuthZ
Policy/ defaults
Admission Control
Object Validation
Bearer tokens
Client certs
OIDC (AD.)...
Roles
&
RoleBindings
API Group: apps/v1
Subject: nigel
Verb: create (HTTP POST method)
Resource: Deployments
Namespace: acg

Recap

A CLOUD GURU



RBAC is stable

PLAN your implementation

Additive model

Other Kubernetes Stuff...

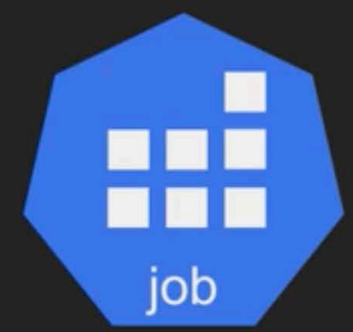
A CLOUD GURU

Other Kubernetes Stuff...

A CLOUD GURU

DaemonSet

StatefulSet



Job

CronJob

PodSecurityPolicy

Pod resource requests and limits

ResourceQuota

CustomResourceDefinition

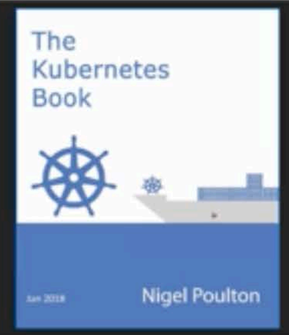
What Next...

A CLOUD GURU

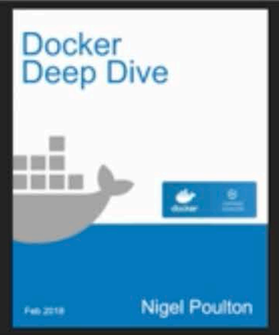
Kubernetes Deep Dive

What Next...

A CLOUD GURU



docker



Community

KubeCon

The PODCTL PODCAST

Kubernetes Podcast from Google

CERTIFIED kubernetes ADMINISTRATOR

OPENFAAS

Serverless

Service Meshes

Prometheus

{API}

```
> kubectl apply…
```

@nigelpoulton