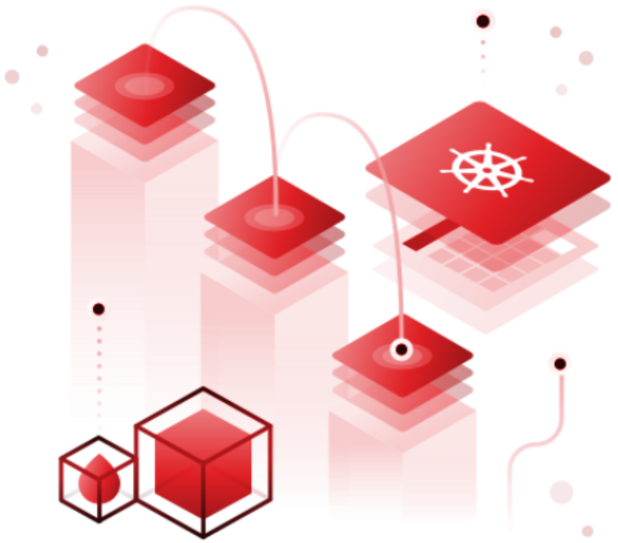
Kubernetes Security

getup

GROW IN THE CLOUD



Reliability

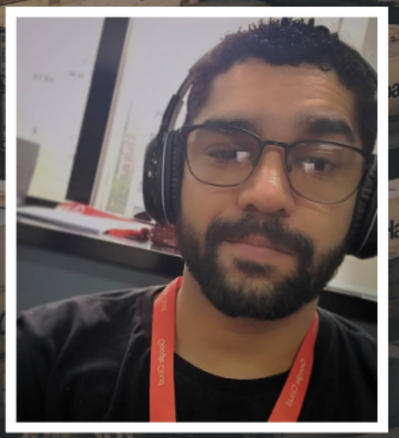
Kubernetes Security

Admission Controllers

Open Policies Agent - OPA

Vault

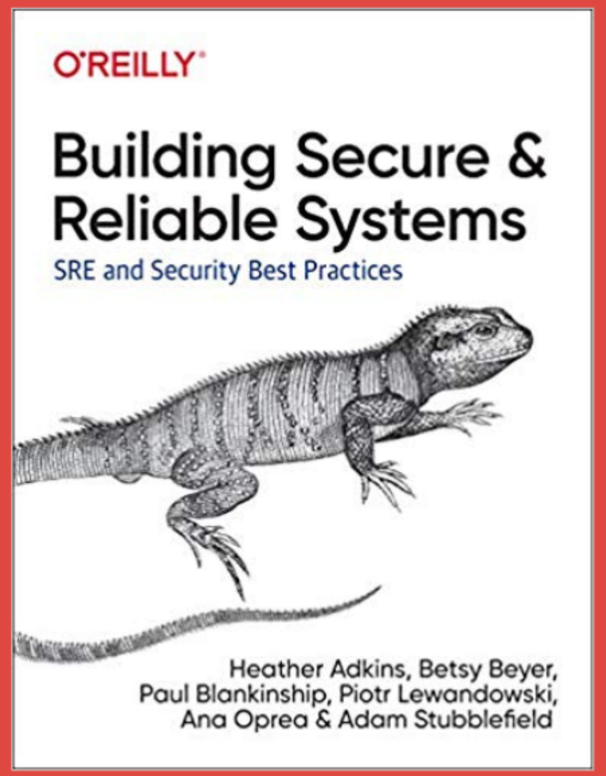
Network Policies



Bruno S. Brasil

Site Reliability Engineering

Reliability



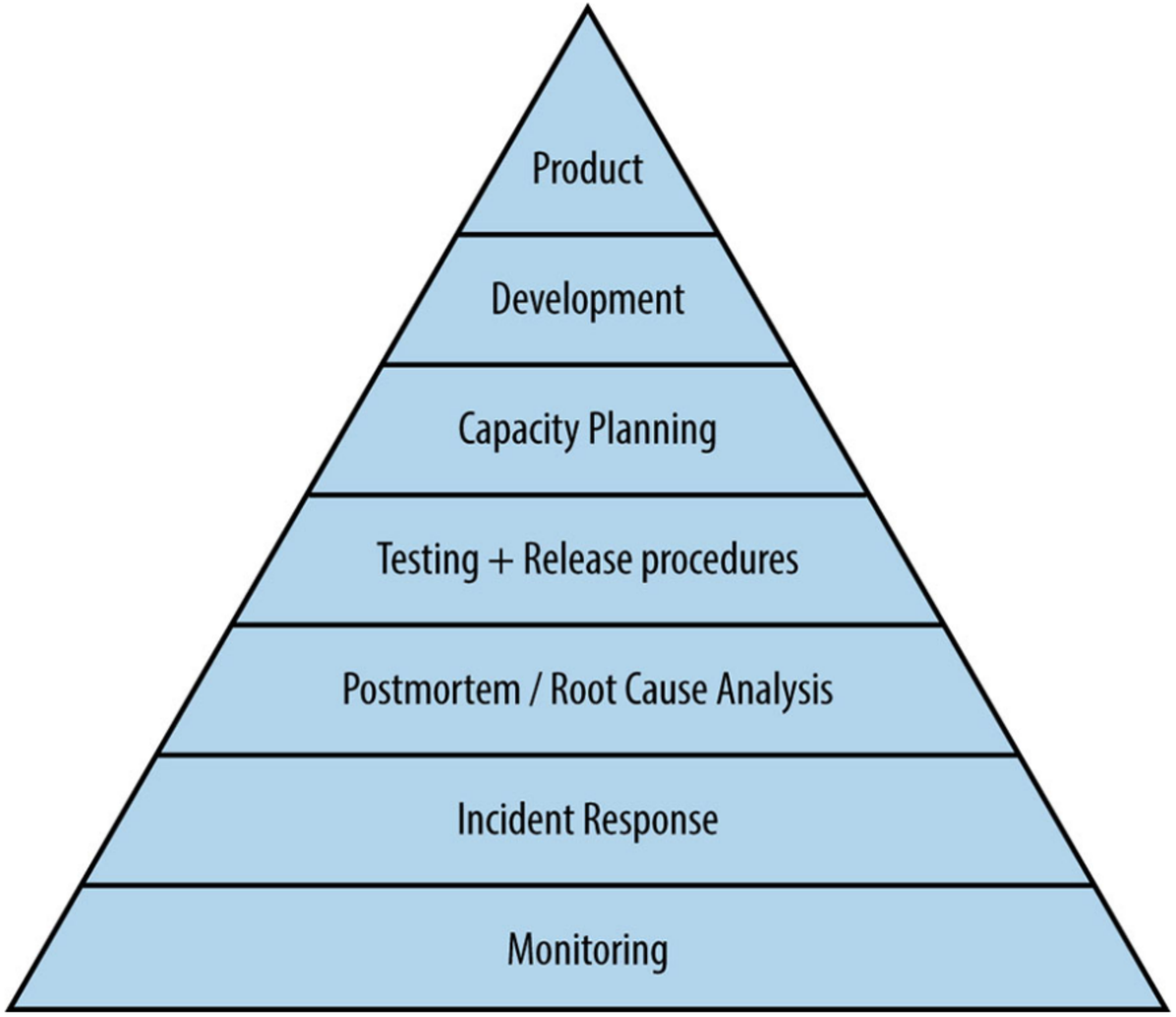
SRE Hierarchy

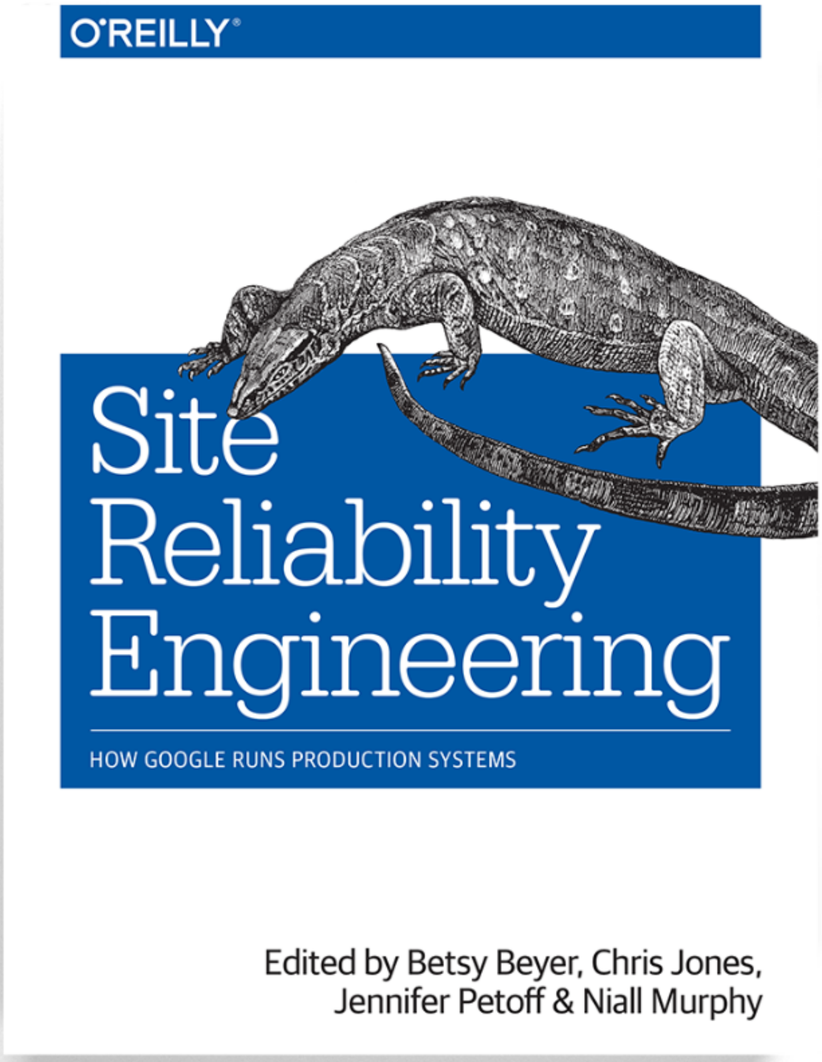
IT Security

Scan me

getup

SRE Hierarchy

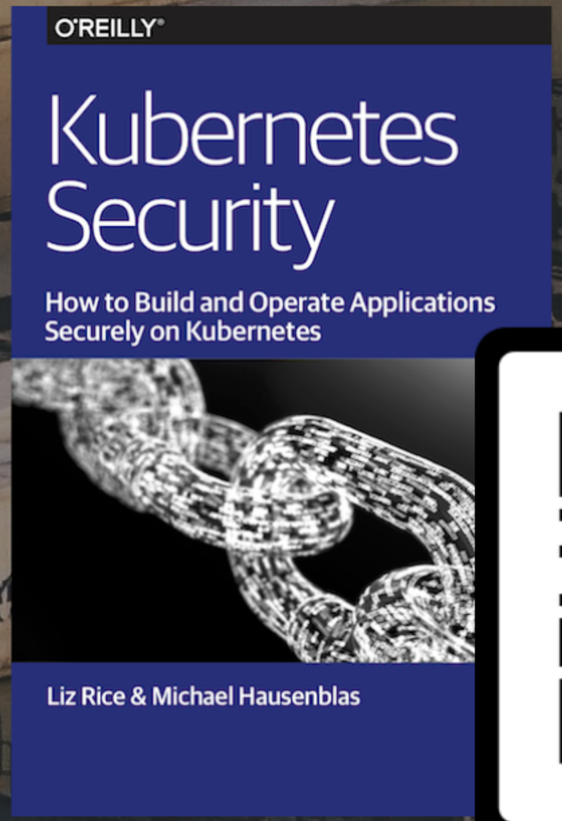




IT Security


Enlist your employees in the fight against breaches
Protect your assets according to the value at risk
Turn your information security department into a business-focused service provider
Ensure buy-in from top management
Establish an information security roadmap with a balanced budget
Use stress and penetration tests periodically
Go beyond benchmarking your peers: Cooperate with them
Automate processes and functions
Strategy
Organization
Processes
Technology
Culture

Kubernetes Security



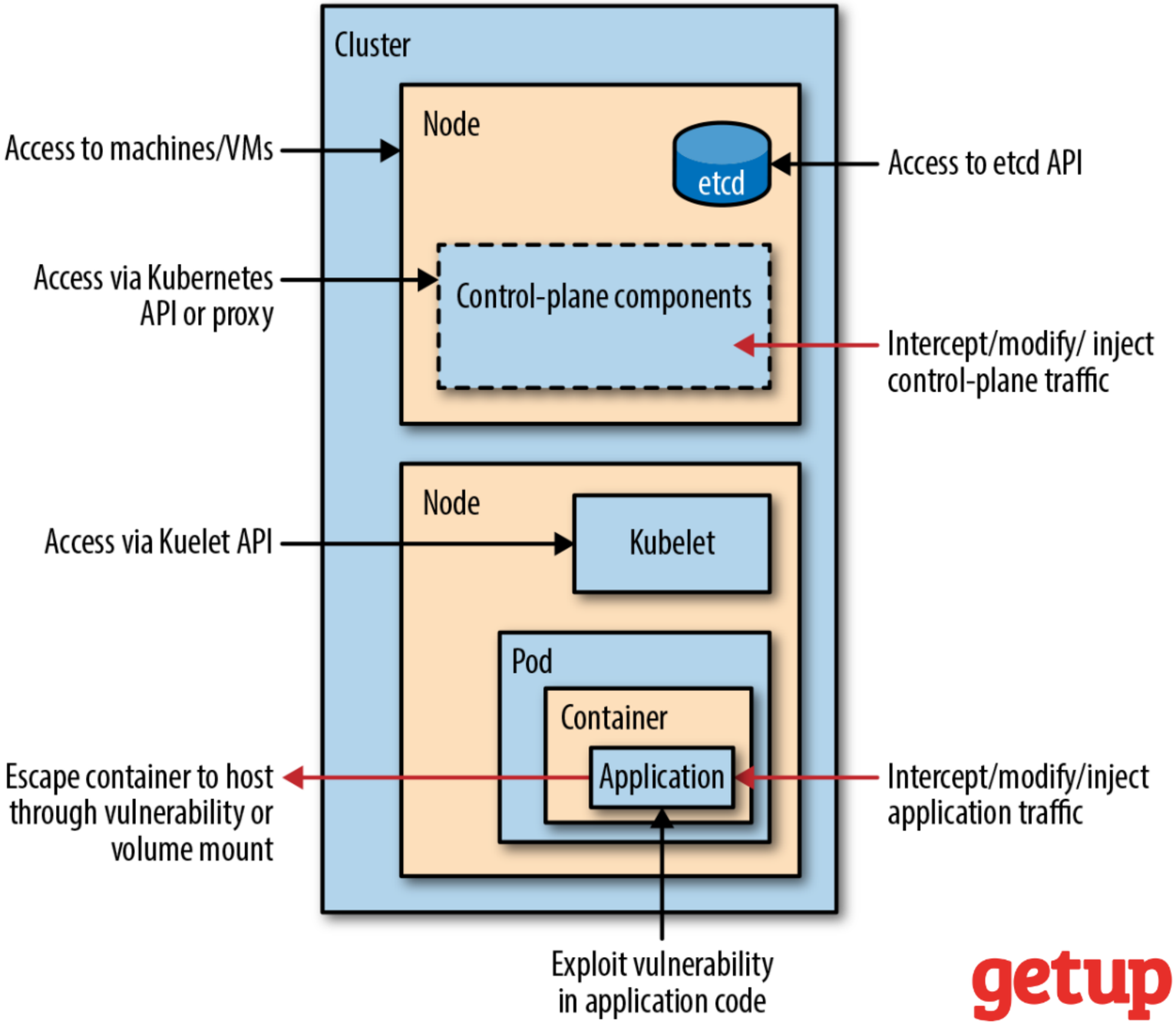
Scan me

getup

Possible Attacks

YouTube

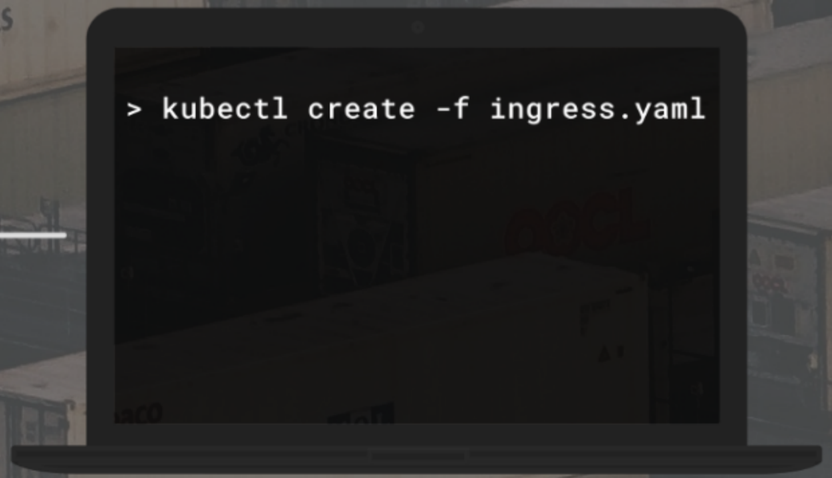
QRcode-pro.com



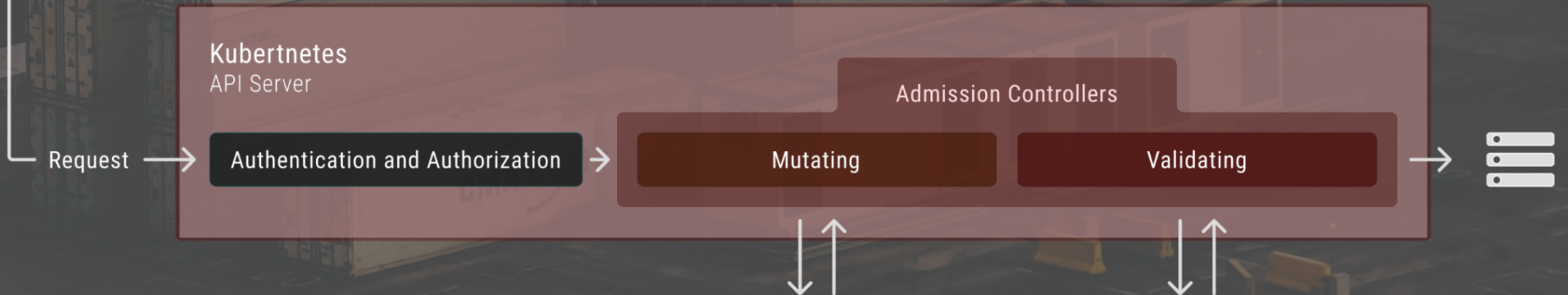
getup

Admission Controllers

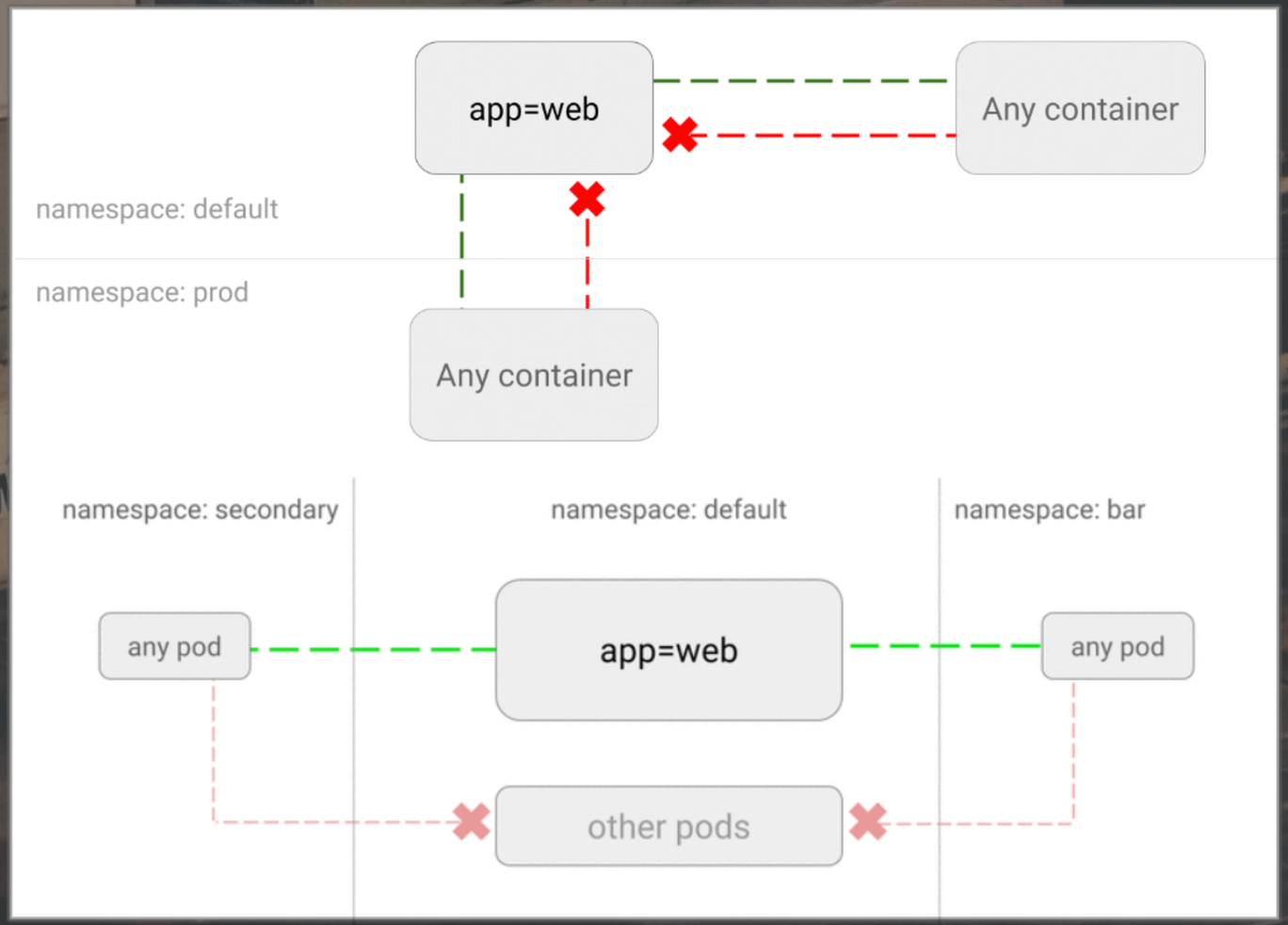
getup



Kubernetes
Admission Control

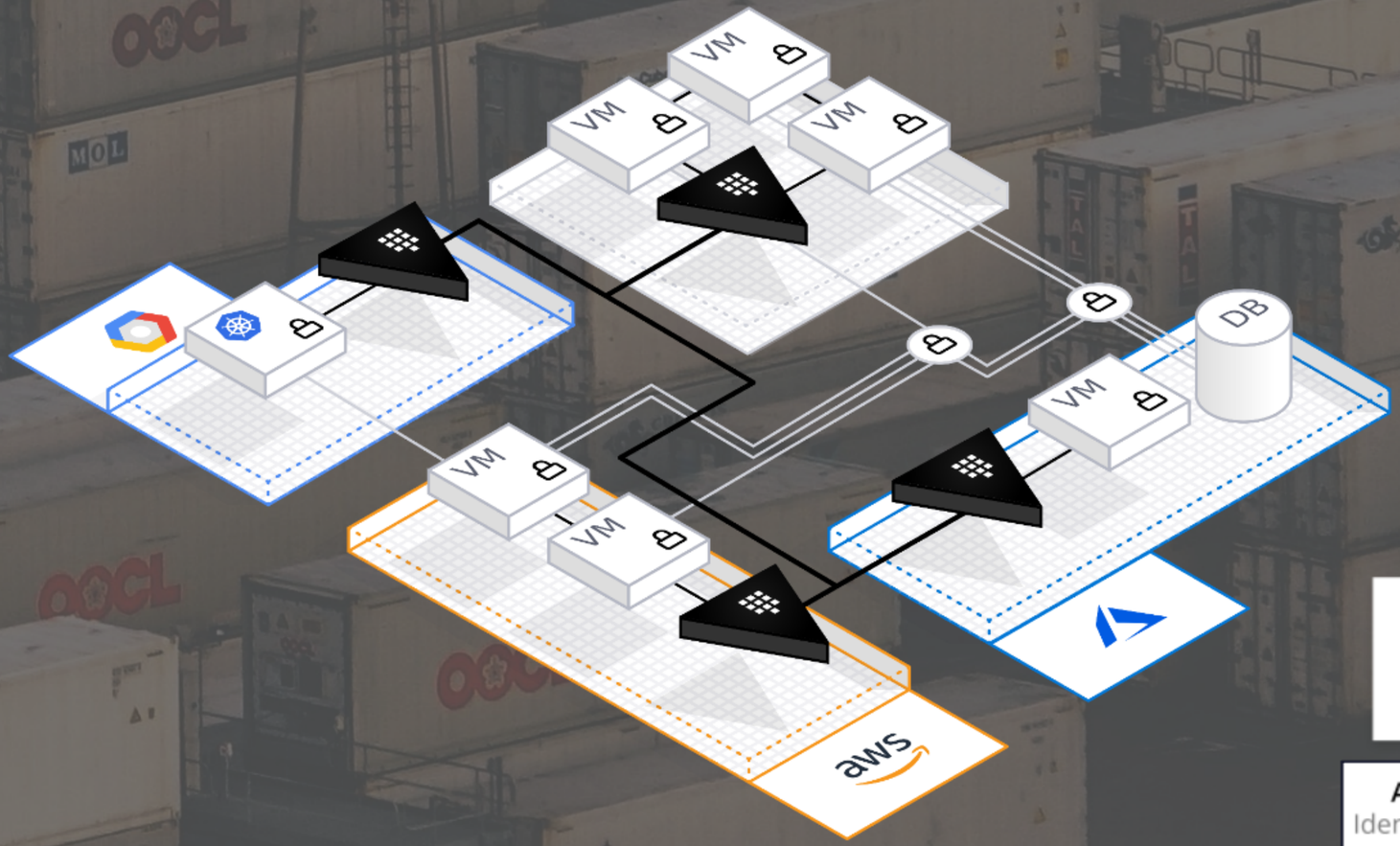


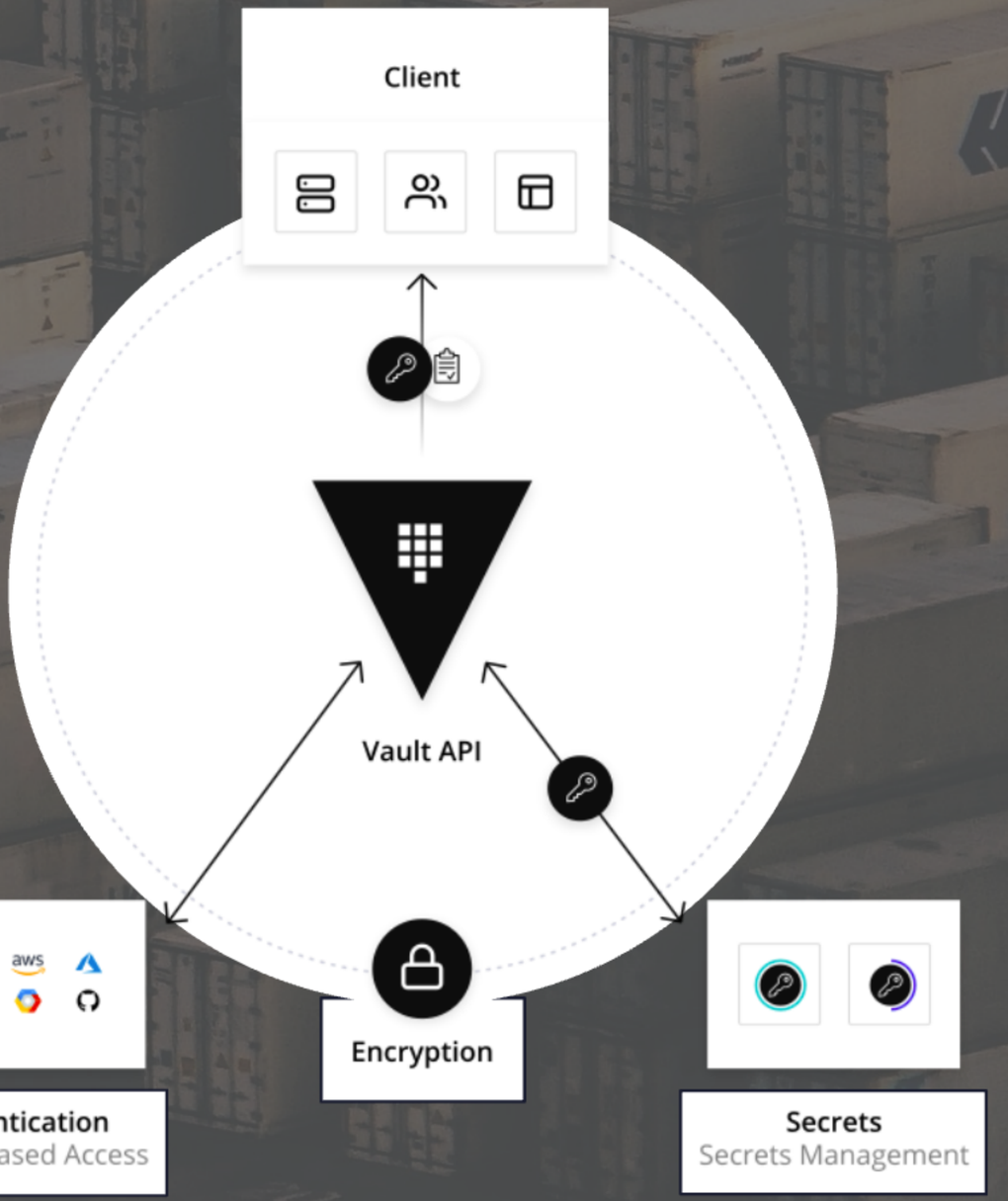
Network Policies




```yaml
---
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:
    matchLabels:
      role: db
  policyTypes:
  - Ingress
  - Egress
  ingress:
  - from:
    - ipBlock:
        cidr: 172.17.0.0/16
        except:
        - 172.17.1.0/24
    - namespaceSelector:
        matchLabels:
          project: myproject
    - podSelector:
        matchLabels:
          role: frontend
    ports:
    - protocol: TCP
      port: 6379
  egress:
  - to:
    - ipBlock:
        cidr: 10.0.0.0/24
    ports:
    - protocol: TCP
      port: 5978
---
```

Vault


VM
VM
VM
VM
VM
VM
DB
aws


Client
Vault API
Encryption
aws
Authentication
Identity-Based Access
Secrets
Secrets Management

Open Policies Agent - OPA

Admission Control

1 How Does OPA Work?

2 How Do I Write Policies?

3 How Do I Test Policies?

getup

Admission Control

getup

```
> kubectl create -f ingress.yaml
```

Kubernetes
Admission Control

Kubertnetes
API Server

Request

Authentication and Authorization

Admission Controllers

Mutating

Validating

Admission Control

Policies

Context

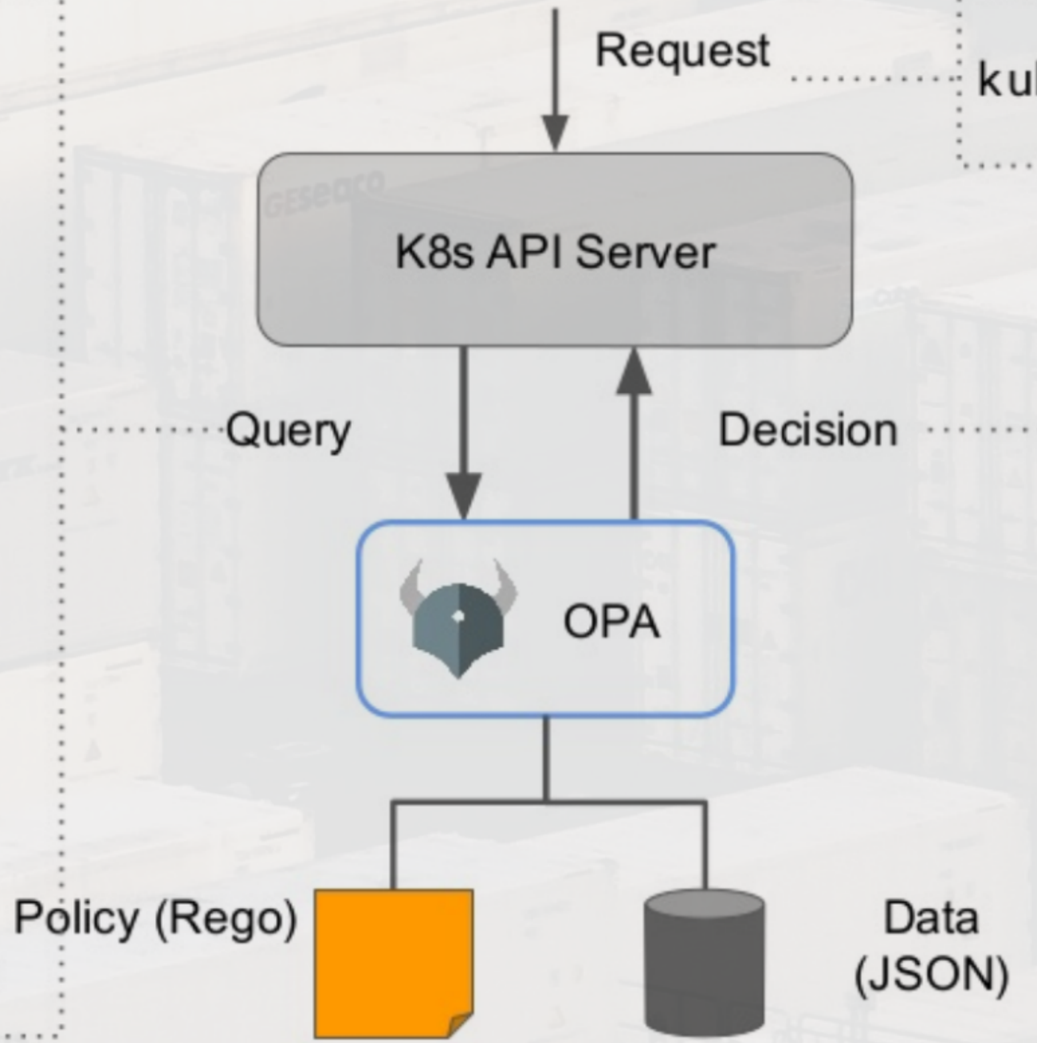
Admission Controller Input

Cached Kubernetes Data

Open Policy Agent
Webhook Admission Controller

How Does OPA Work?

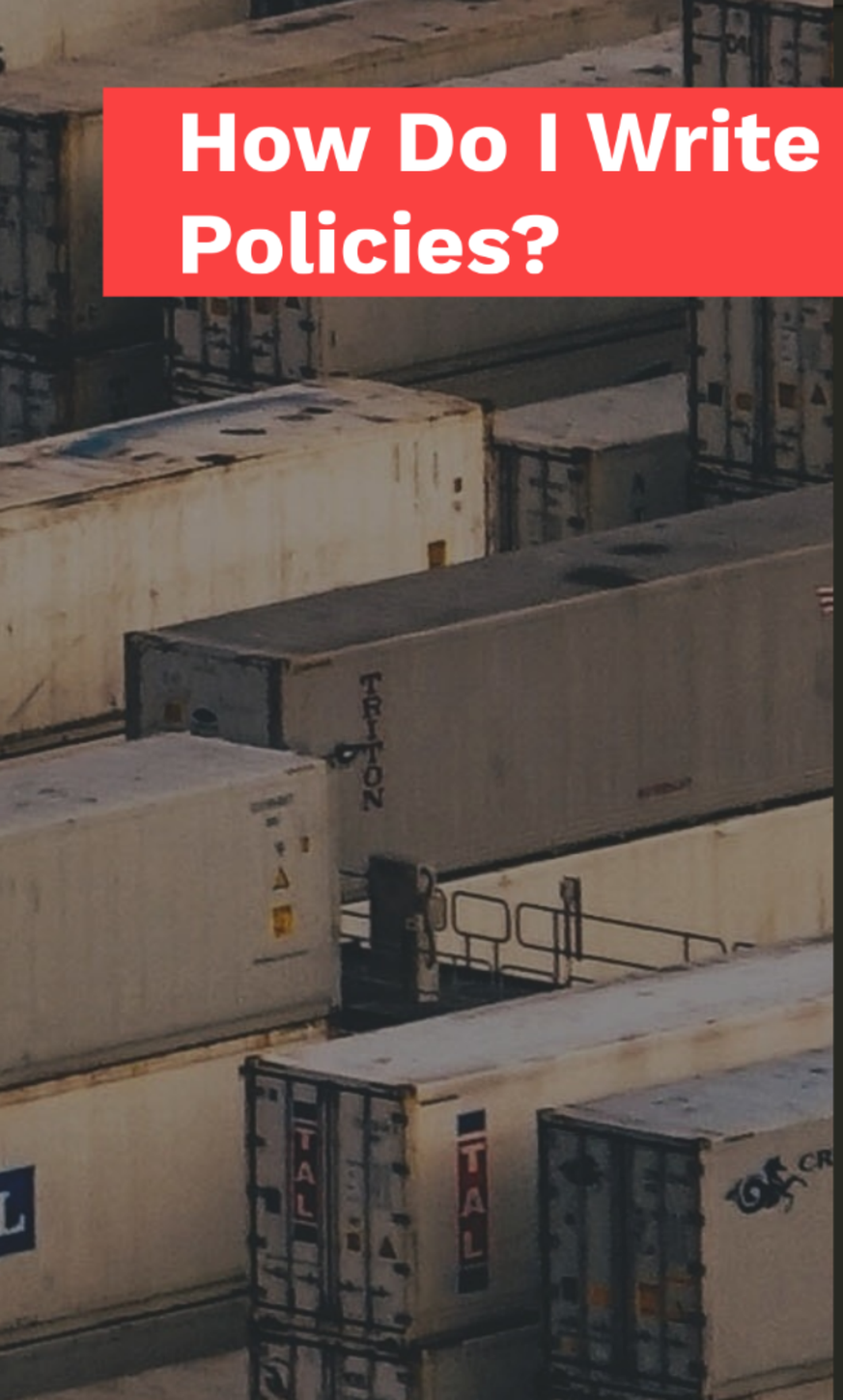
```
kind:
  kind: Deployment
request:
  object:
    metadata:
      name: nginx-deployment
    spec:
      replicas: 2
      selector:
        matchLabels:
          app: nginx
      template:
        metadata:
          labels:
            app: nginx
        spec:
          containers:
          - name: nginx
            image: nginx:1.7.9
```




```
kubectl create -f nginx.yaml
```

```
allow: false
reason: |
  no costcenter label
```

getup



How Do I Write Policies?

```
package kubernetes.admission

import data.kubernetes.namespaces

#- if not tag in image-name

deny[msg] {
    input.request.kind.kind = "Pod"
    input.request.operation = "CREATE"
    container = input.request.object.spec.containers[_]
    not contains(container.image, ":")
    msg = sprintf("No tag in image-name %q", [container.image])
}

#- check if image-name contain default latest tag

deny[msg] {
    input.request.kind.kind = "Pod"
    input.request.operation = "CREATE"
    container = input.request.object.spec.containers[_]
    [image_name, image_tag] = split(container.image, ":")
    image_tag = "latest"
    msg = sprintf("Invalid image tag - using default latest tag %q", [container.image])
}

#- check registry host name in image-name

deny[msg] {
    input.request.kind.kind = "Pod"
    input.request.operation = "CREATE"
    container = input.request.object.spec.containers[_]
    [image_name, image_tag] = split(container.image, ":")
    reg_name = split(image_name, "/")
    registry_name = reg_name[0]
    whitelist = namespaces[input.request.namespace].metadata.annotations["registry-whitelist"]
    not contains(whitelist, registry_name)
    msg = sprintf("[WARN] Invalid registry host [%q]", [container.image,registry_name])
}
```

How Do I Test Policies?

https://play.openpolicyagent.org

The Rego Playground

Input

```
{
  "apiVersion": "v1",
  "kind": "Pod",
  "metadata": {
    "name": "nginx",
    "labels": {
      "name": "nginx"
    }
  },
  "spec": {
    "containers": [
      {
        "name": "nginx",
        "image": "nginx:0.26",
        "ports": [
          {
            "containerPort": 80
          }
```

Output

```
# Evaluated package in 39.91 µs.
{
  "result": {
    "deny": []
  }
}
```

```
package kubernetes.admission

import data.kubernetes.namespaces

#- if not tag in image-name

deny[msg] {
    input.request.kind.kind = "Pod"
    input.request.operation = "CREATE"
    container = input.request.object.spec.conta
    not contains(container.image, ":")
    msg = sprintf("No tag in image-name %q", [c
}

#- check if image-name contain default latest tag

deny[msg] {
    input.request.kind.kind = "Pod"
    input.request.operation = "CREATE"
    container = input.request.object.spec.conta
    [image_name, image_tag] = split(container.i
    image_tag = "latest"
    msg = sprintf("Invalid image tag — using default latest tag %q", [container.image])
}

#- check registry host name in image-name

deny[msg] {
    input.request.kind.kind = "Pod"
    input.request.operation = "CREATE"
    container = input.request.object.spec.containers[_]
    [image_name, image_tag] = split(container.image, ":")
    reg_name = split(image_name, "/")
    registry_name = reg_name[0]
    whitelist = namespaces[input.request.namespace].metadata.annotations["registry-whitelist"]
    not contains(whitelist, registry_name)
    msg = sprintf("[WARN] Invalid registry host [%q]", [container.image,registry_name])
}
```

Scan me

Obrigado!! :)

Bruno S. Brasil

Site Reliability Engineer

linkedin.com/in/brunosb/

@bruhsb

@BrunoSBrasill

medium.com/@getupcloud

twitter.com/GetupCloud

Scan me

getup kubicast

getupcloud.com/kubicast

getup