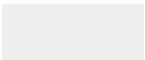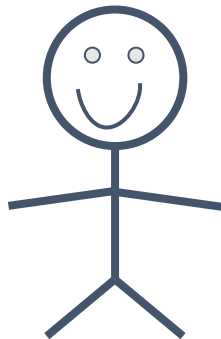# Submariner: Multi Cluster Networking for Kubernetes

Nir Yechiel, Red Hat

@nyechiel

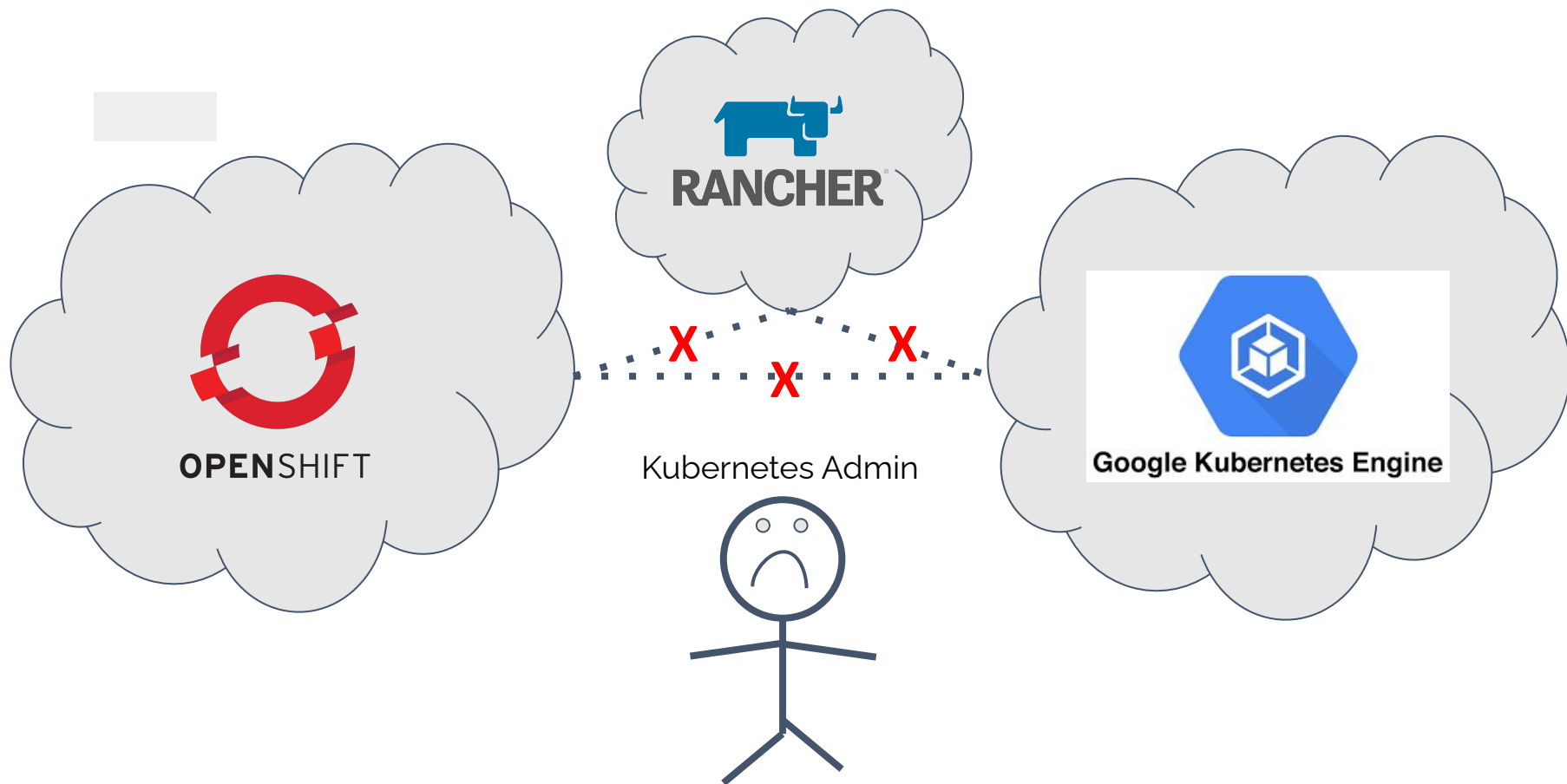Developer Community TLV
December 17, 2020

Kubernetes Admin

Kubernetes Admin

Submariner: Multi Cluster Networking for Kubernetes
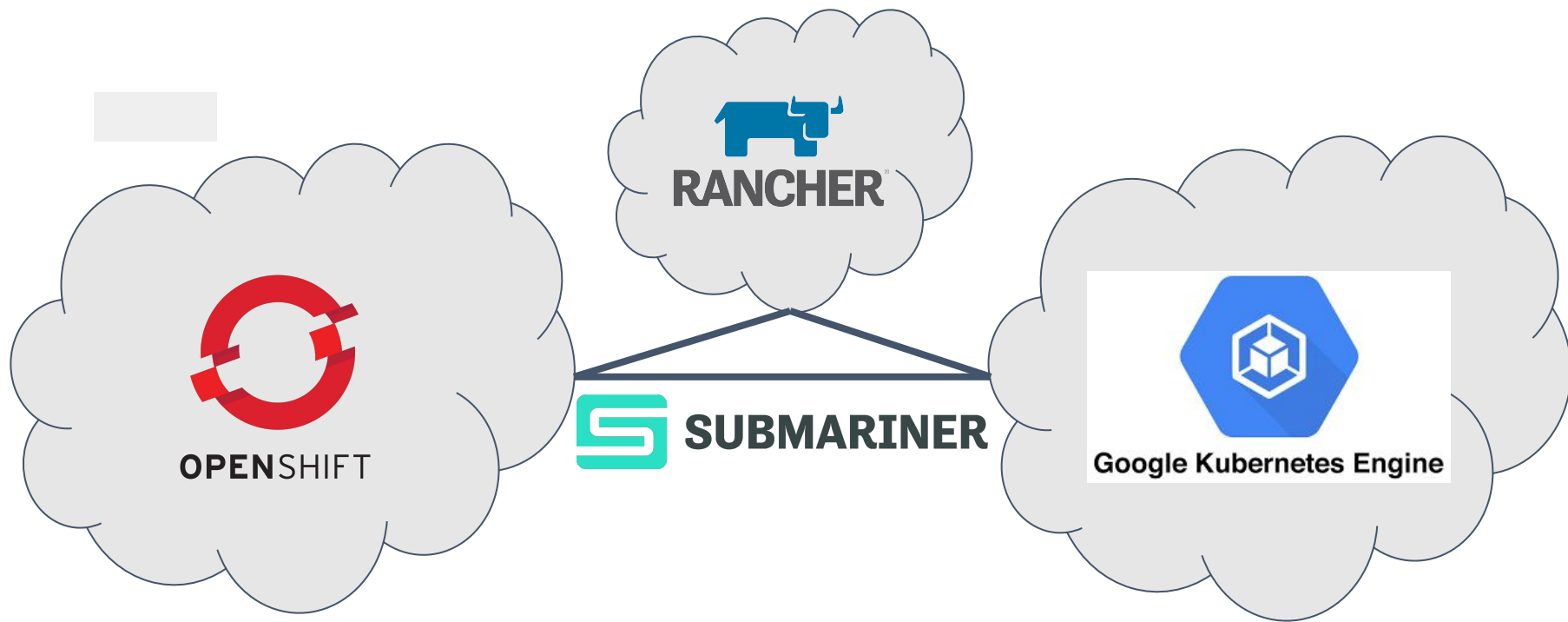
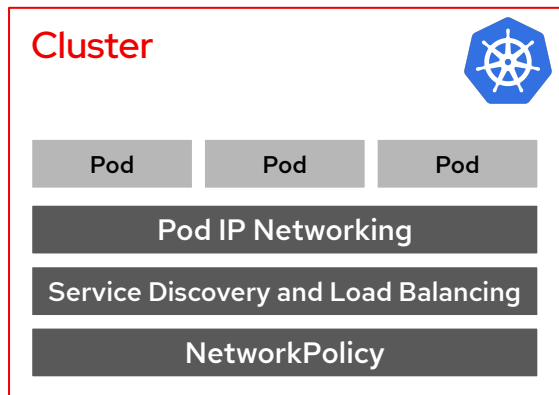Submariner: Multi Cluster Networking for Kubernetes

What is Submariner?

- Enables direct network connectivity between multiple Kubernetes clusters

- Exposes a set of new custom resources (CRDs) backed by the Kubernetes datastore

- Open source, vendor neutral project: https://submariner.io/

- Can be deployed using Operator, Helm and `subctl`

Kubernetes cluster networking

Cluster

Pod | Pod | Pod

Pod IP Networking

Service Discovery and Load Balancing

NetworkPolicy

Submariner: Multi Cluster Networking for Kubernetes

Multi cluster networking with Submariner

Submariner: Multi Cluster Networking for Kubernetes
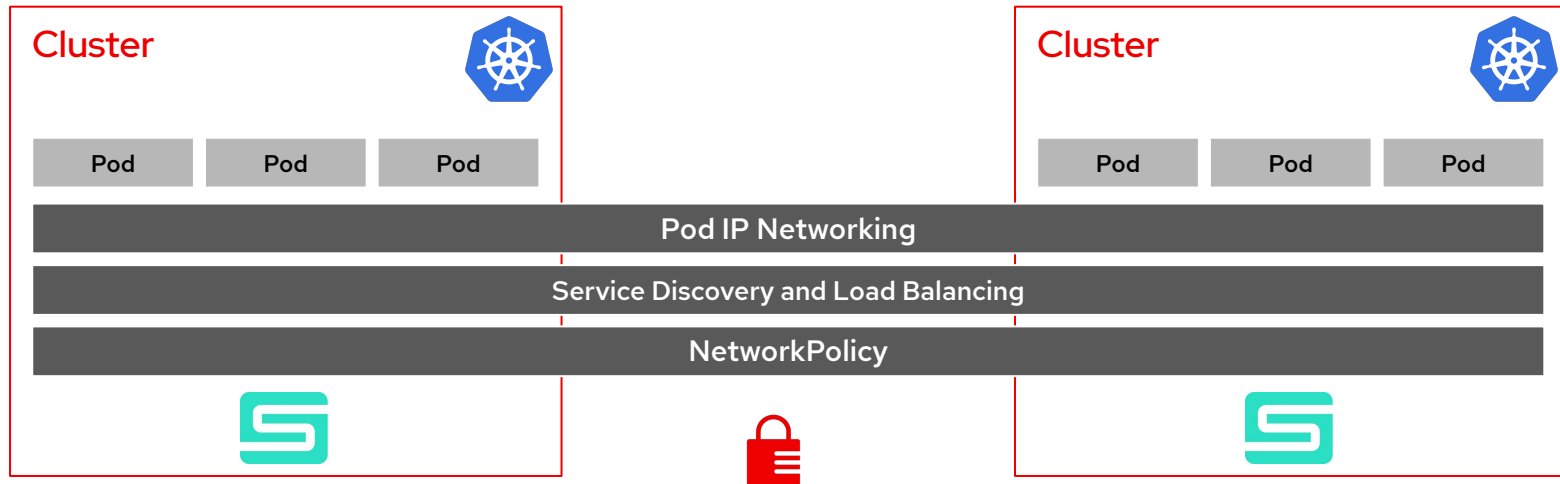
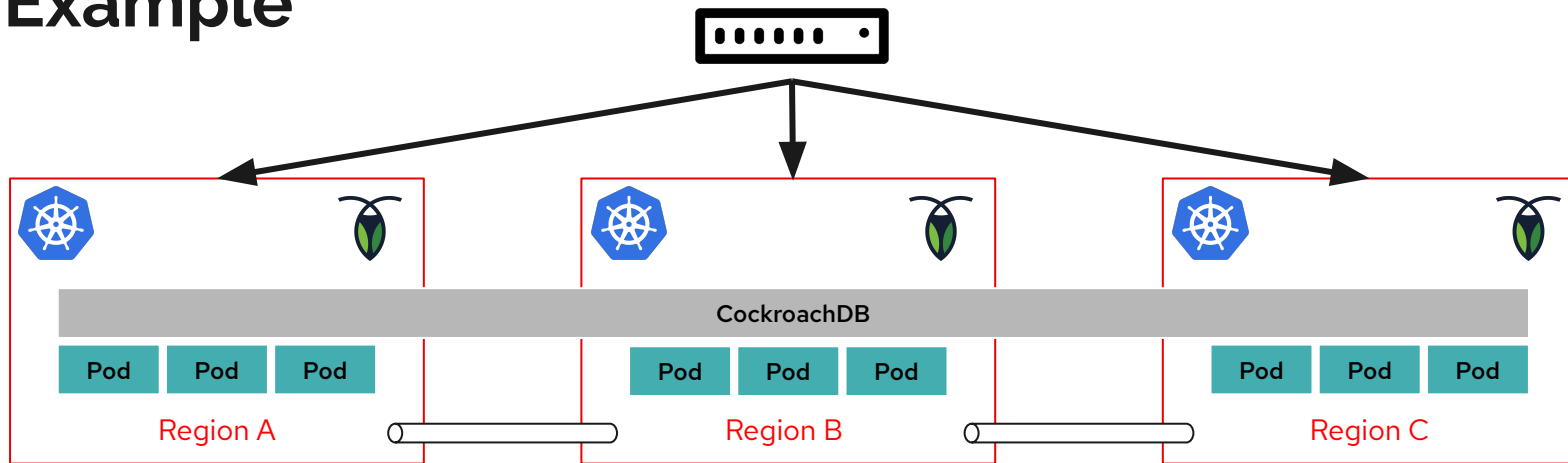# Common use cases

- Application availability

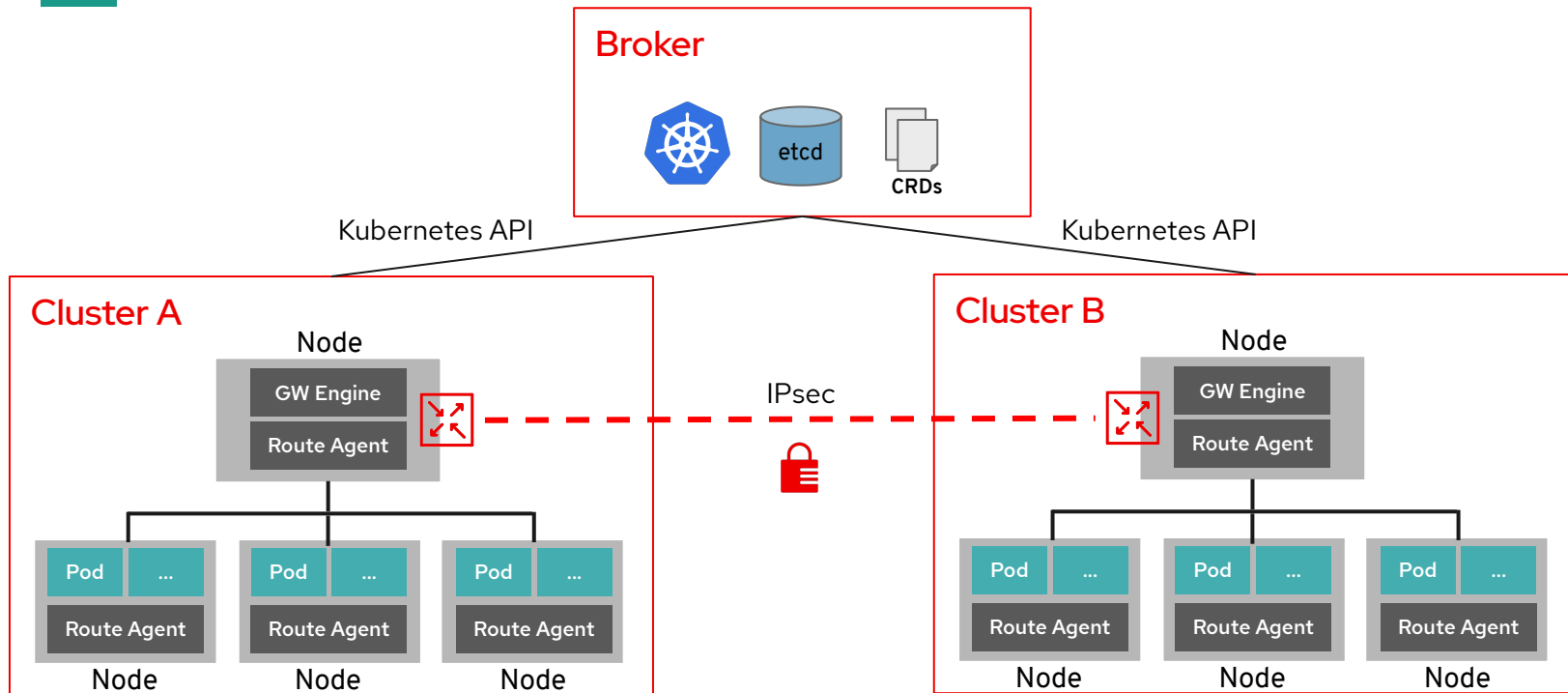- Disaster Recovery (DR)

- Data residency guidelines

Example

- Example: multi-region CockroachDB cluster
- Kubernetes clusters in multiple regions, with replicas of the same service running in each cluster
- Goal: keep data close to the user, while reducing latency and fault tolerance to improve user experience

Benefits

- Direct east/west Pod-to-Pod and Pod-to-Service routing across clusters
  - … without requiring proxies or exposing your backend services to the internet
- Works with any Kubernetes cluster, compatible with different network (CNI) providers
- Deploy services across clusters
  - Beyond connectivity, also address Service Discovery (Lighthouse) and NetworkPolicy (Coastguard)
- Enhanced security
  - Cross-cluster traffic is encrypted with IPsec by default; WireGuard also supported

High level architecture

Broker

etcd

CRDs

Kubernetes API

Kubernetes API

Cluster A

Node

GW Engine

Route Agent

IPsec

Cluster B

Node

GW Engine

Route Agent

Pod | ...
Route Agent
Node

Pod | ...
Route Agent
Node

Pod | ...
Route Agent
Node

Pod | ...
Route Agent
Node

Pod | ...
Route Agent
Node

Pod | ...
Route Agent
Node

Submariner: Multi Cluster Networking for Kubernetes

Service Discovery (DNS)

- Lighthouse is an implementation of the Kubernetes Multi-Cluster Service API

- **clusterset** - a group of clusters with a high degree of mutual trust that share services
  - Within a `clusterset`, all namespaces with a given name are considered to be the same

- `ServiceExport` (CRD) - used to specify which services should be exposed across clusters
  - To export a service, a ServiceExport should be *explicitly* created within the cluster
  - When a ServiceExport is created, this will cause a domain name of `<service>.<ns>.svc.clusterset.local` for the multi-cluster service to become accessible

- `ServiceImport` (CRD) – in-cluster representation of a multi-cluster service

subctl

- A command-line utility to ease deployment and verification of Submariner

```
# subctl join --kubeconfig output/kubeconfigs/config-cluster1 broker-info.subm
```

```
# subctl join --kubeconfig output/kubeconfigs/config-cluster1 broker-info.subm
```

Try Submariner

- Website: https://submariner.io
  - https://submariner.io/getting_started/quickstart/
- GitHub: https://github.com/submariner-io
- YouTube: https://tinyurl.com/submariner-youtube
- Slack (Kubernetes space): #submariner