Red Hat

TechTalks

Networking & Security

Webinar-Serie: Next Generation Datacenter (NGDC)

16. September 2022, 11:00 CEST | Robert Bohne, Senior Specialist Solution Architect Openshfit

About me

Robert Bohne works as a **Senior Specialist Solution Architect** at Red Hat and a Subject-Matter Expert for **OpenShift** Container Platform. With over **10 years** of **middleware operating experience** from **automation** to **monitoring** and **more than 5 years of container** know-how, Robert primarily supports large German customers with their OpenShift adoption; starting with the introduction, **24x7 operations** up to the **migration** and **modernization** of complex **applications**.

Twitter
@RobertBohne

LinkedIn
https://www.linkedin.com/in/robertbohne/

Red Hat

Network & Security

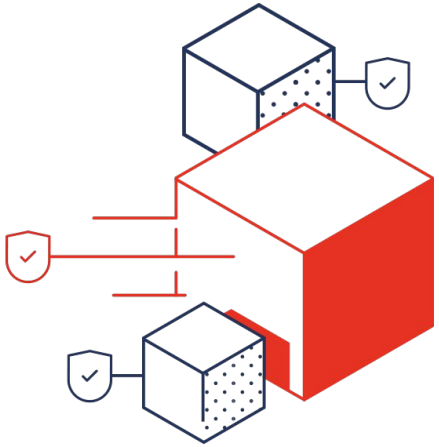
Overview: Das Next Generation Datacenter mit Red Hat gestalten
Franz Theisen
19.8.2022, 11.00 - 12.00 CEST

Compute: Virtualisierung und Container auf einer Platform
Domenico Piol
26.8.2022, 11.00 - 12.00 CEST

Management
Robert Baumgartner
2.9.2022, 11:00-12.00 CEST

Storage: MultiCloud, Unified, Converged oder klassisch
Matthias Rettl
9.9.2022, 11:00-12.00 CEST

Networking & Security
Robert Bohne
16.9.2022, 11:00-12.00 CEST

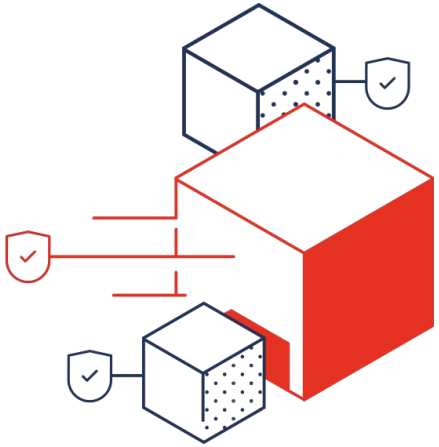


Red Hat

Upcoming Events

19. OpenShift Anwendertreffen

DACH OpenTour 2022



Delivering consistency and flexibility

Traditional apps & VM's

Cloud-native apps

AI/ML, Functions

Communities of Innovation | Ecosystems of Solutions

Red Hat OpenShift

Secure & Automated Infrastructure and Operations

Physical

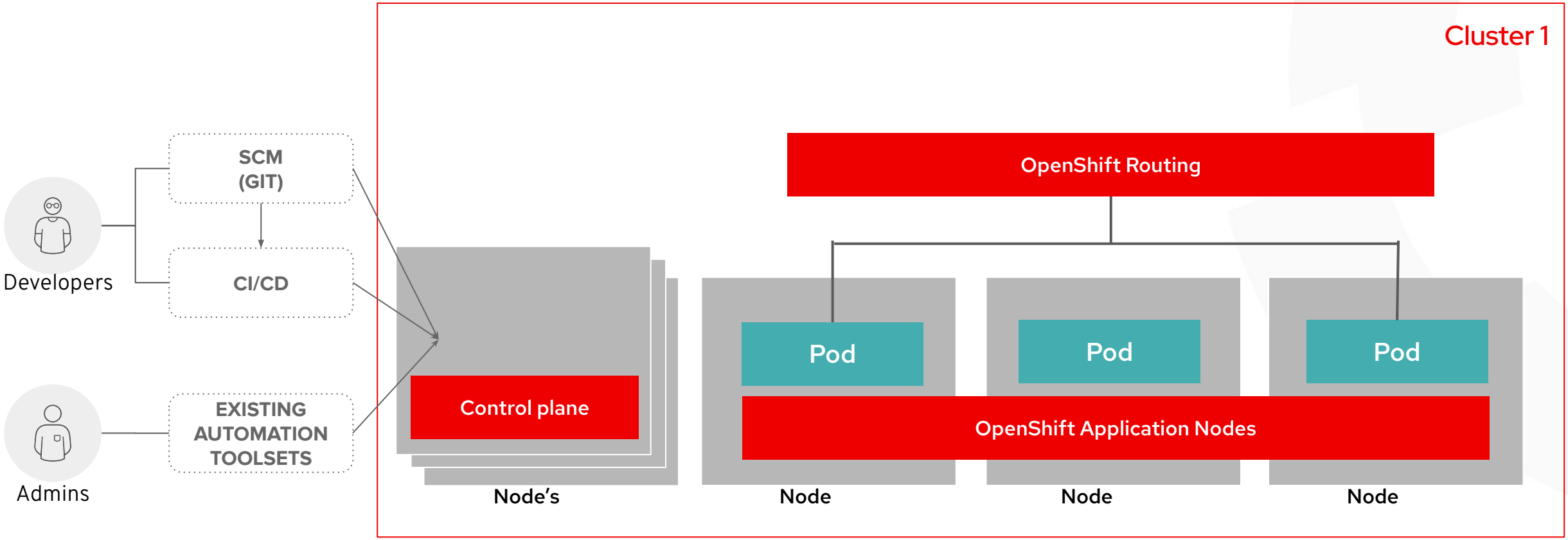
Virtual

Private cloud

Public cloud

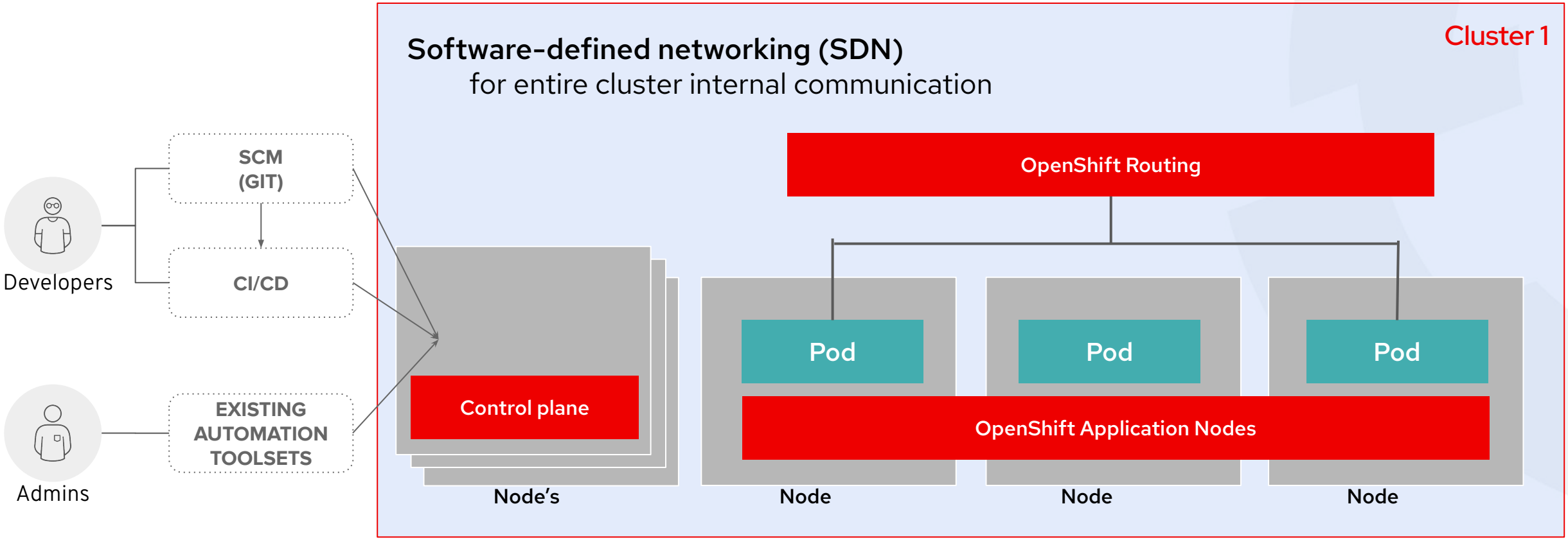
Edge

What is an OpenShift Cluster?



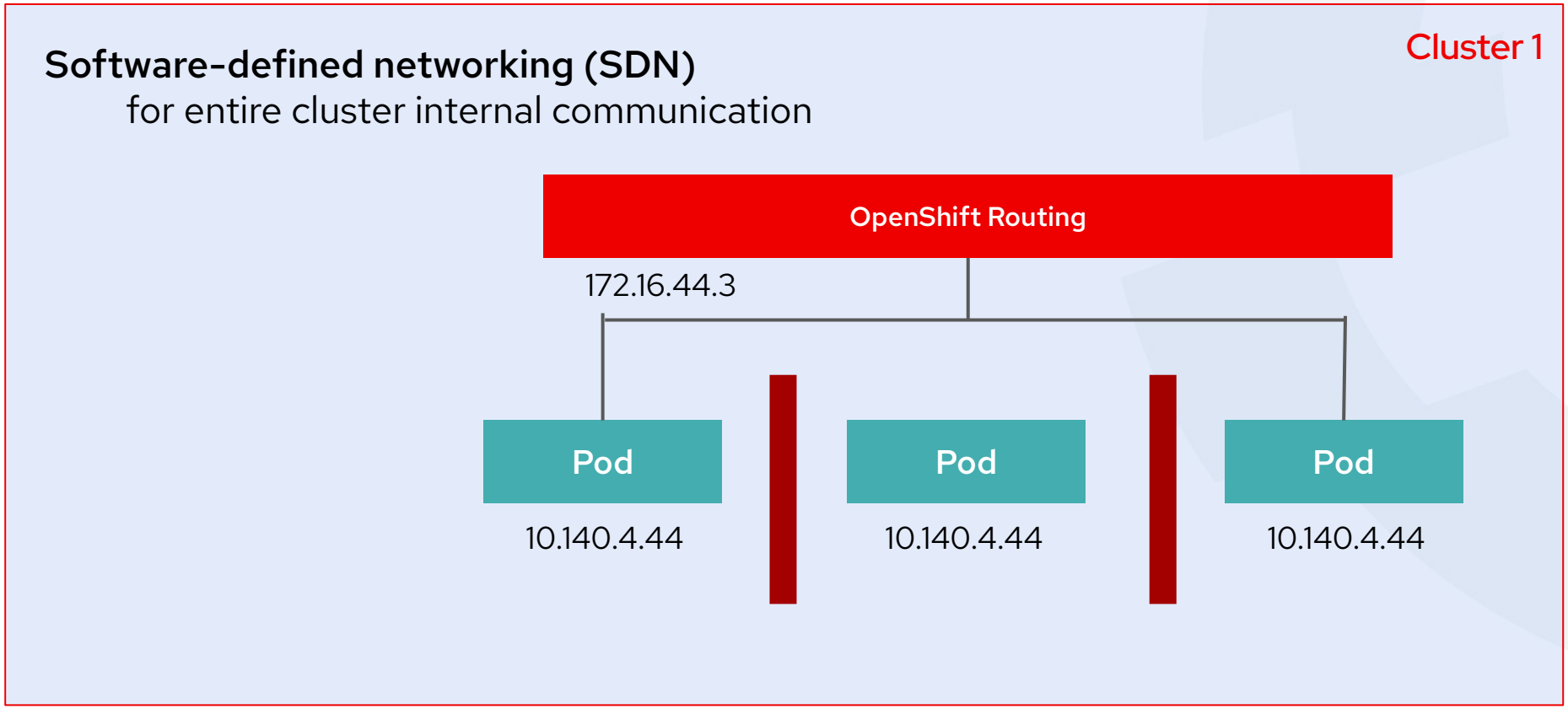
Red Hat
OpenShift

What is an OpenShift Cluster?



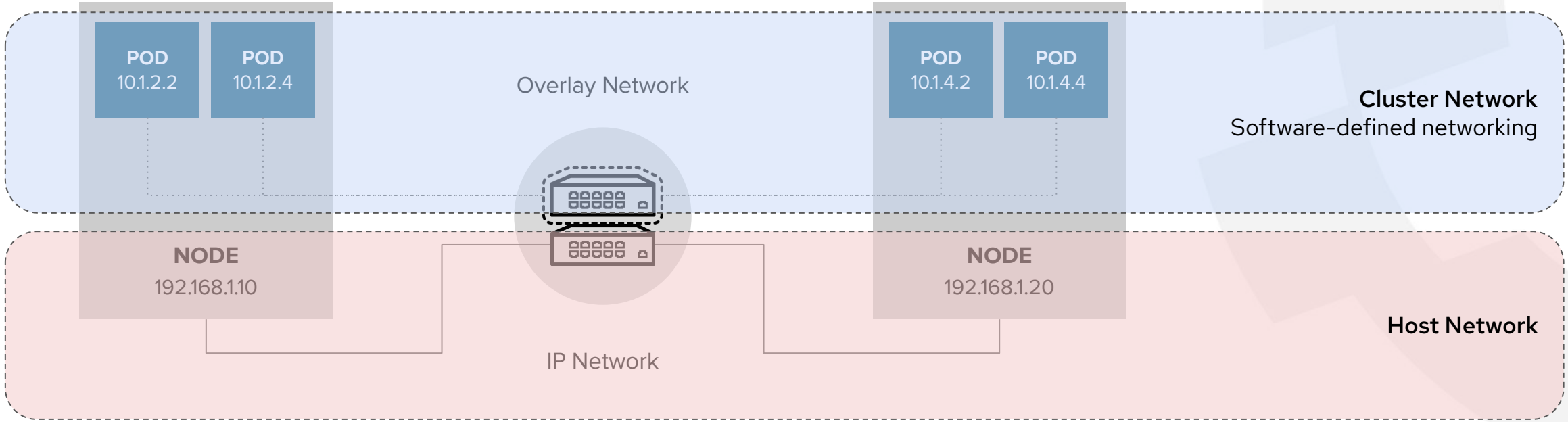
Red Hat OpenShift

Why do we need a Software-defined networking (SDN)?



Red Hat OpenShift

in Detail



Overlay Network exchangeable via OpenShift Network Plug-ins

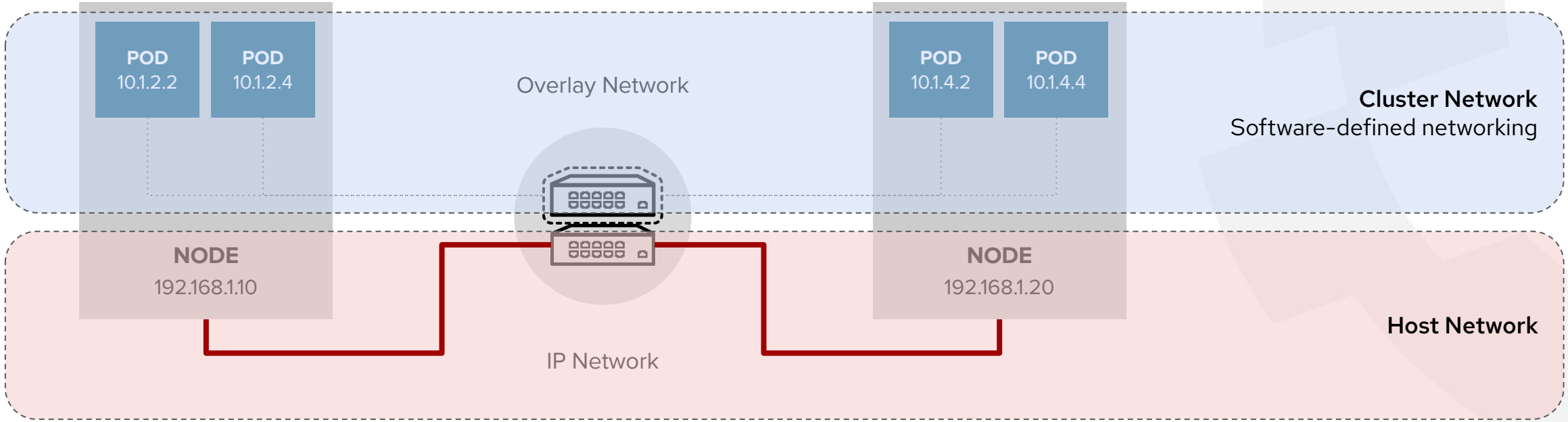
- Kubernetes **C**ontainer **N**etwork **I**nterface = CNI

CNI

https://github.com/containernetworking/cni
https://cncf-branding.netlify.app/projects/cni/

Red Hat OpenShift

🔐 Encrypted internode traffic (optional, IPSec)



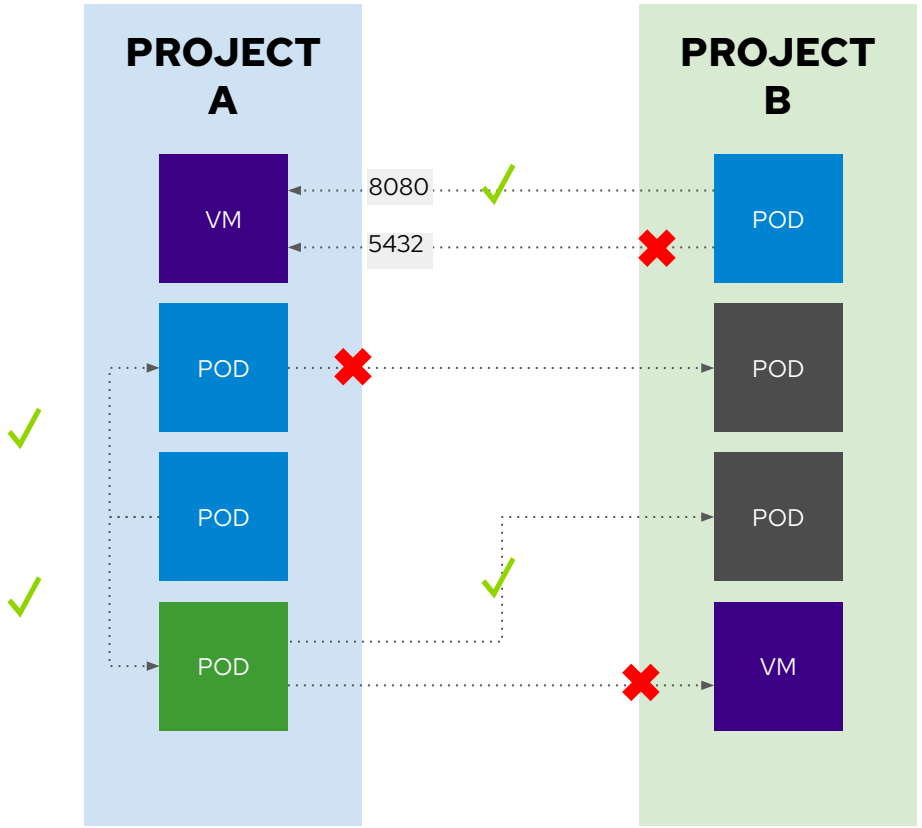
Overlay Network exchangeable via OpenShift Network Plug-ins

- Kubernetes **C**ontainer **N**etwork **I**nterface = CNI

CNI

https://github.com/containernetworking/cni
https://cncf-branding.netlify.app/projects/cni/

Isolation, (Micro) Segmentation, ...

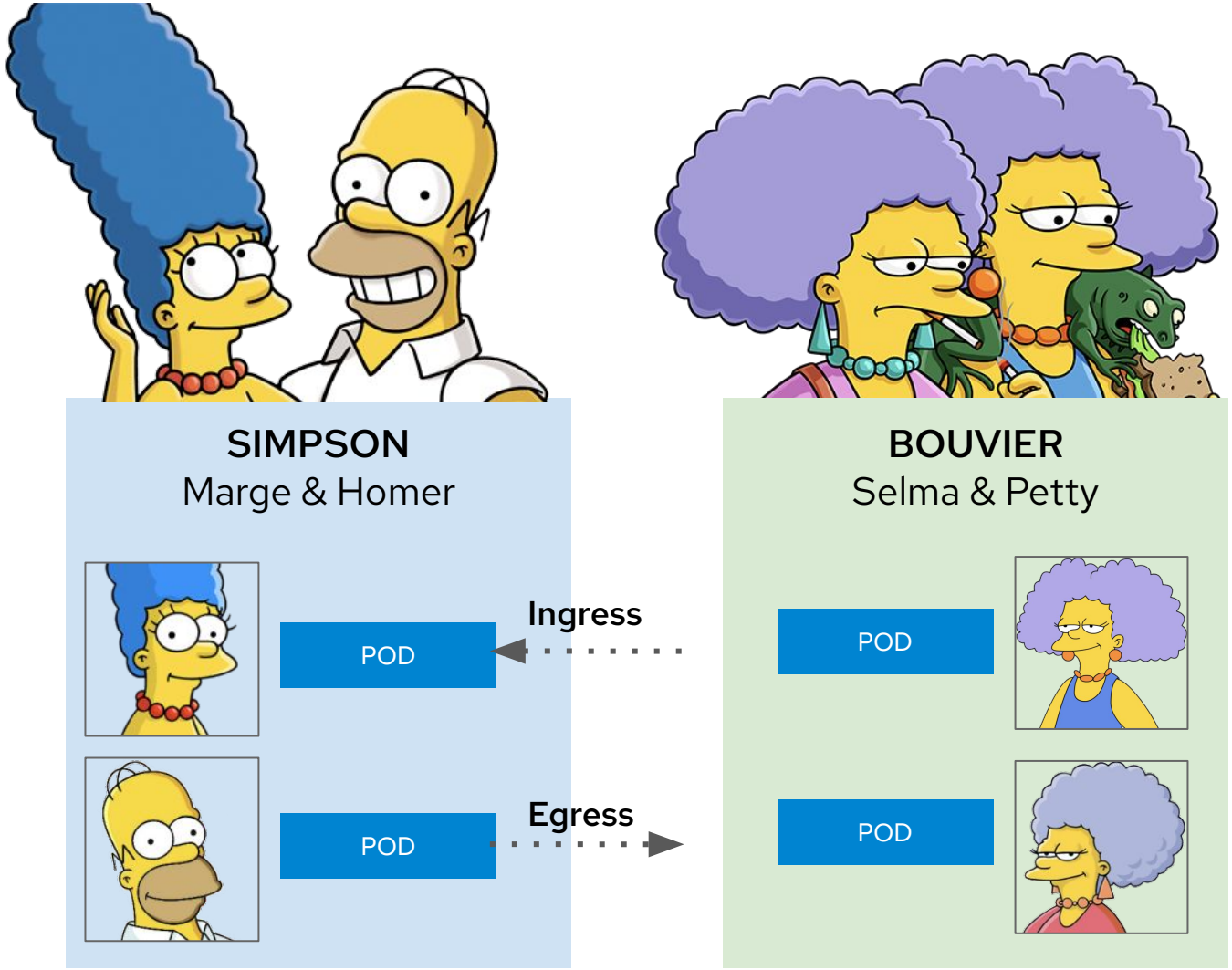


Network Policy

- Allow all traffic inside the project
- Allow traffic from green to gray
- Allow traffic to purple on 8080

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```

Network Policy



https://cloud.redhat.com/blog/guide-to-kubernetes-egress-network-policies
https://docs.openshift.com/container-platform/4.11/networking/network_policy/about-network-policy.html

Red Hat OpenShift

Demo

SIMPSON
Marge & Homer

POD

POD

BOUVIER
Selma & Petty

POD

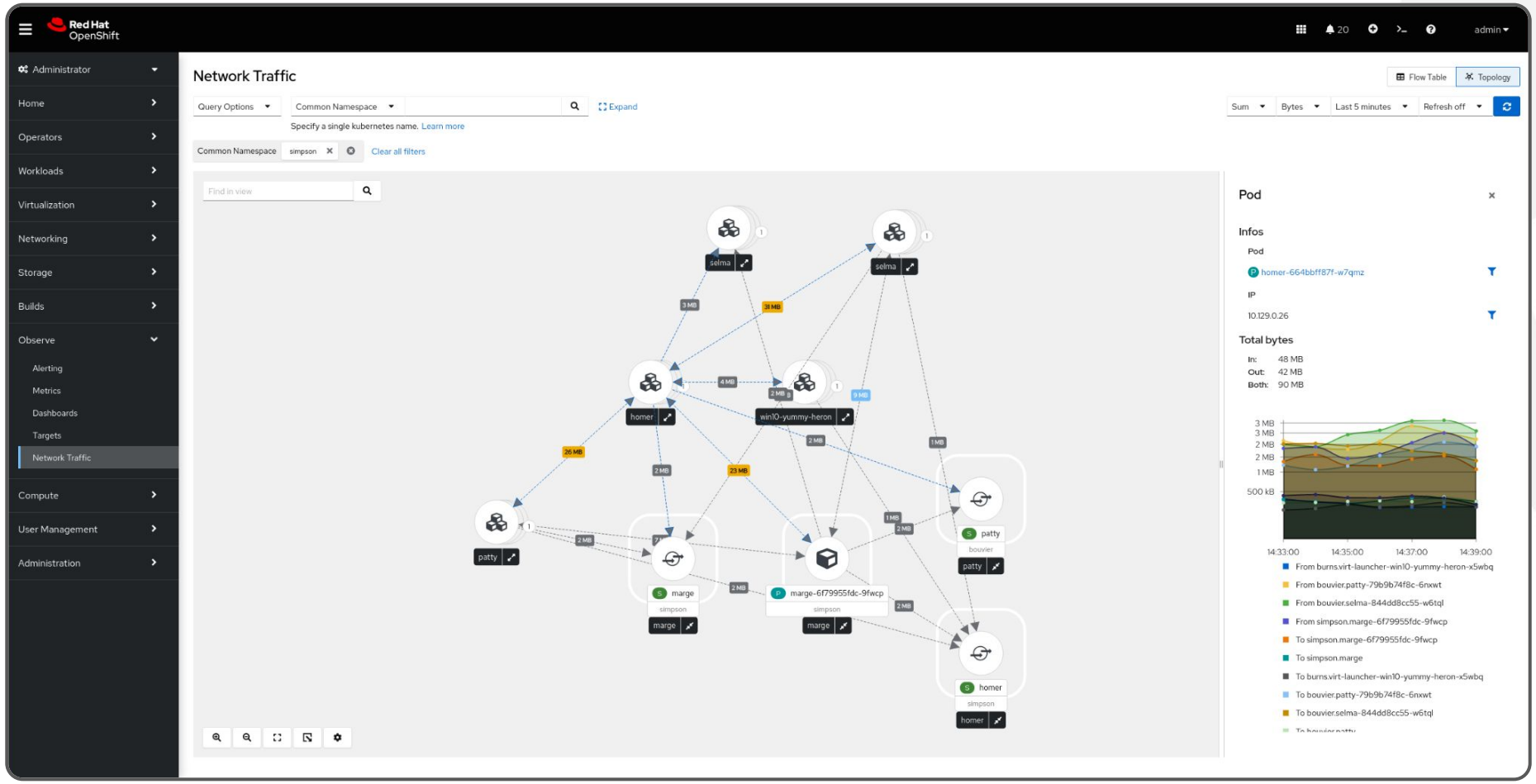
POD

BURNS
Monty

VM

Red Hat OpenShift

OpenShift Network Observability



https://github.com/netobserv

Red Hat OpenShift

Red Hat Advanced Cluster Security: Use Cases

Security across the entire application lifecycle

Vulnerability Management

Protect yourself against known vulnerabilities in images and running containers

Network Segmentation

Apply and manage network isolation and access controls for each application

Configuration Management

Ensure your deployments are configured according to security best practices

Compliance

Meet contractual and regulatory requirements and easily audit against them

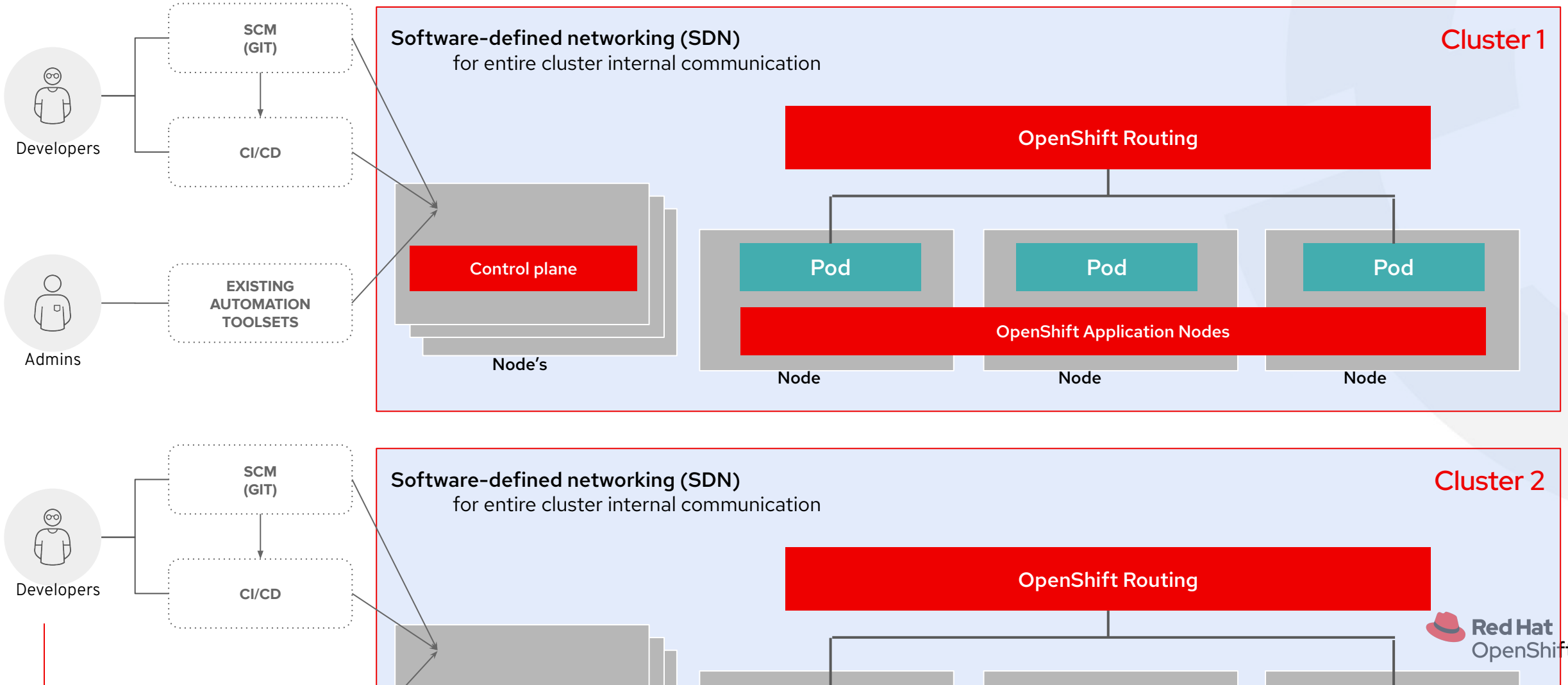
Risk Profiling

Gain context to prioritize security issues throughout OpenShift and Kubernetes clusters

Detection and Response

Carry out incident response to address active threats in your environment

What about multiple OpenShift Cluster?

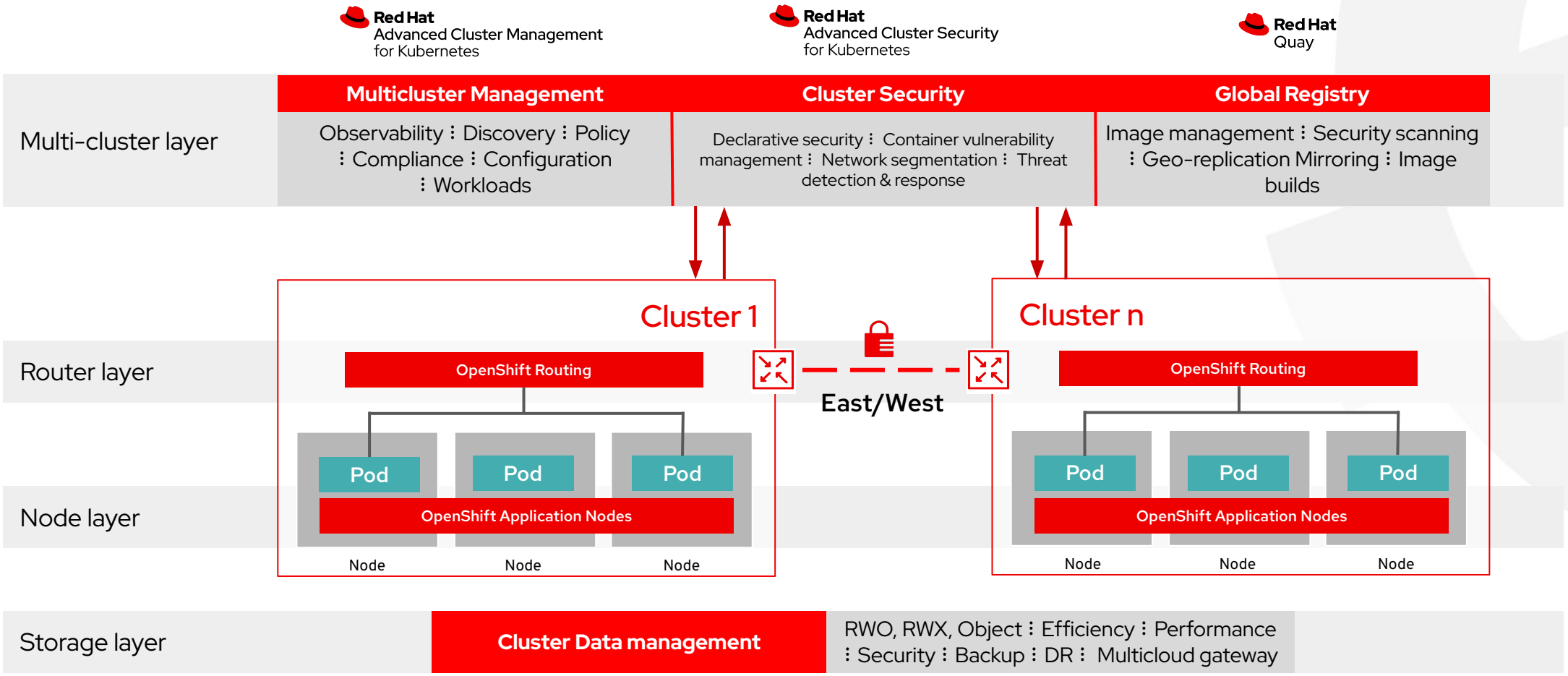


Cluster data management

RWO, RWX, Object | Efficiency | Performance | Security | Backup | DR Multicloud gateway

Red Hat OpenShift Platform Plus

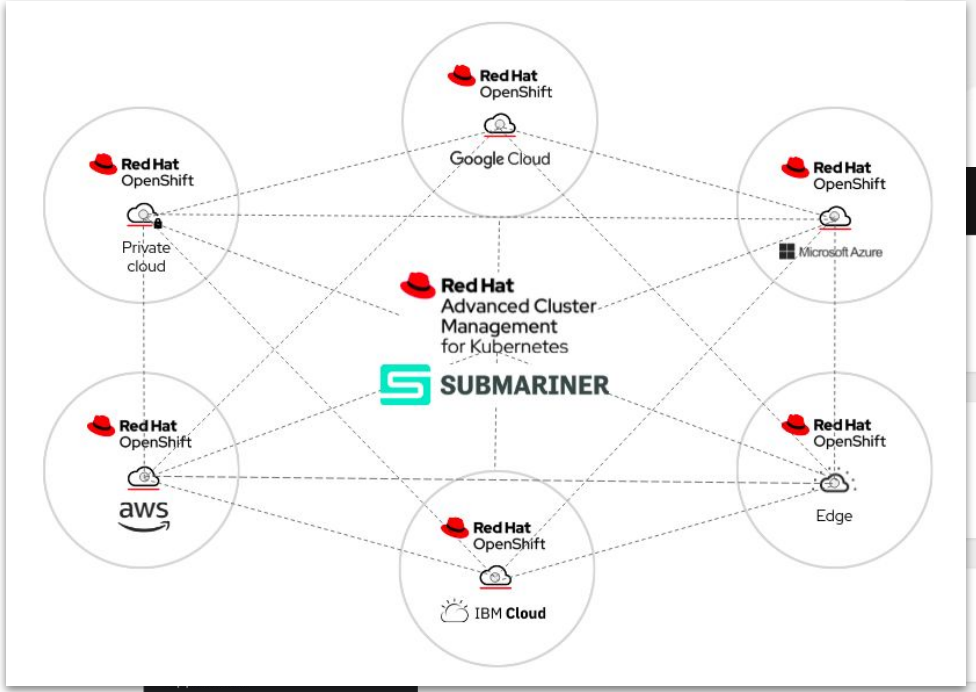
Enabling hybrid and multi-cloud deployments

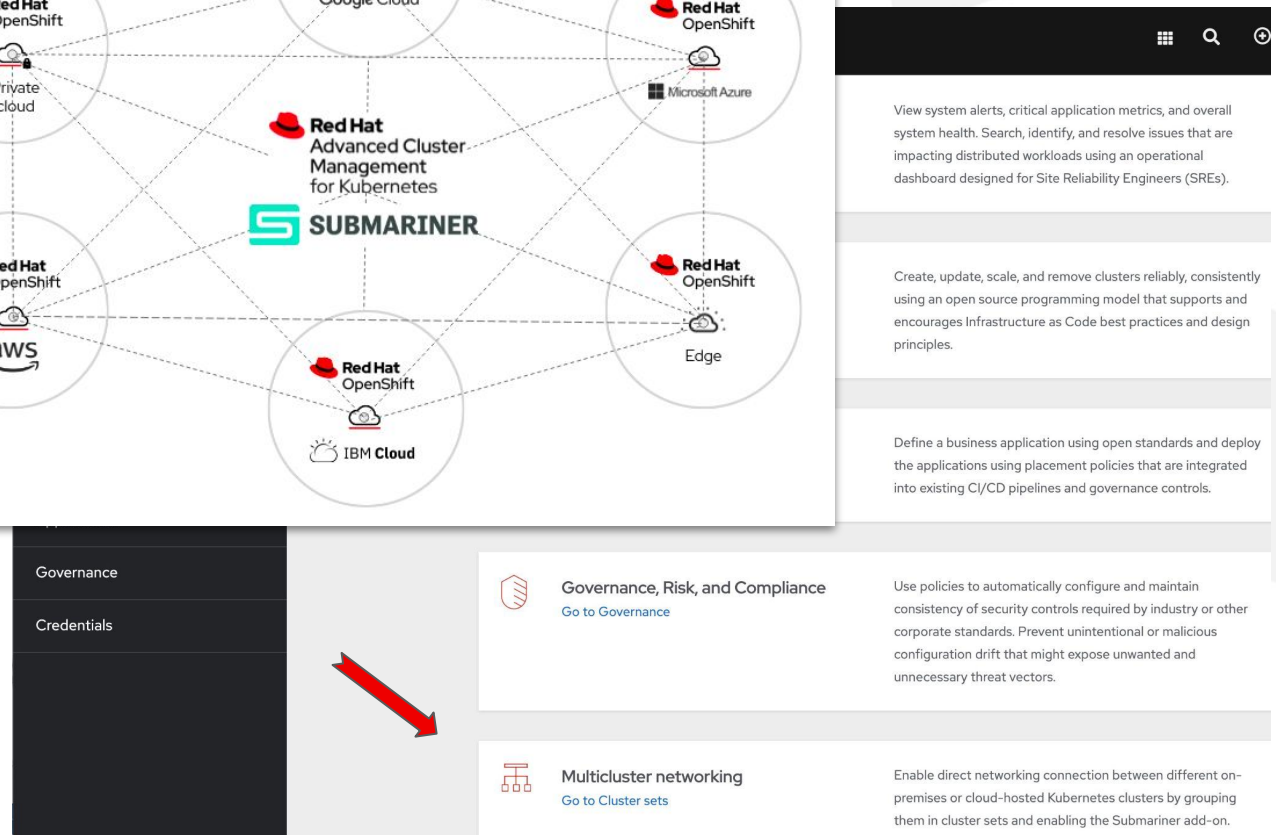


Red Hat OpenShift

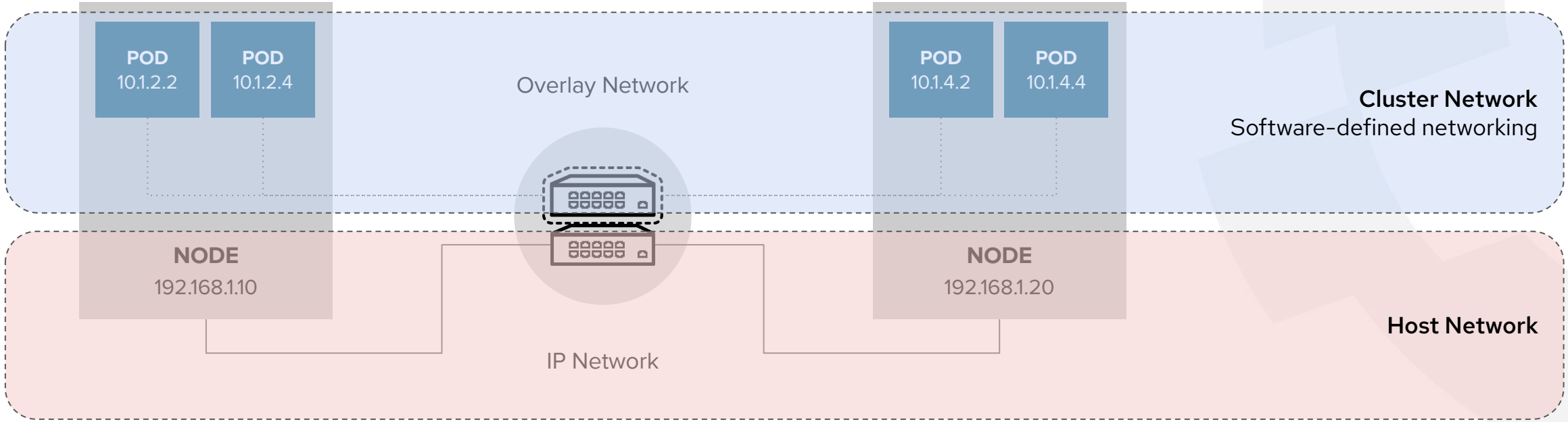
Multicluster Networking with Red Hat Advanced Cluster Management for Kubernetes

- Presenting **Submariner**: an CNCF open source project in the form of an **add-on** for RHACM, now generally available
- Enable **direct networking** between Pods in different Kubernetes clusters as well as **Service Discovery**, either on-premises or in the cloud
- **Globalnet** - Support for interconnecting clusters with overlapping CIDRs
- **Future work (subject to change)**
  - ACM Red Hat OpenShift Service mesh integration
  - Discovery Deploy & Configure Federation
  - Custom - upstream Istio, Gloo...

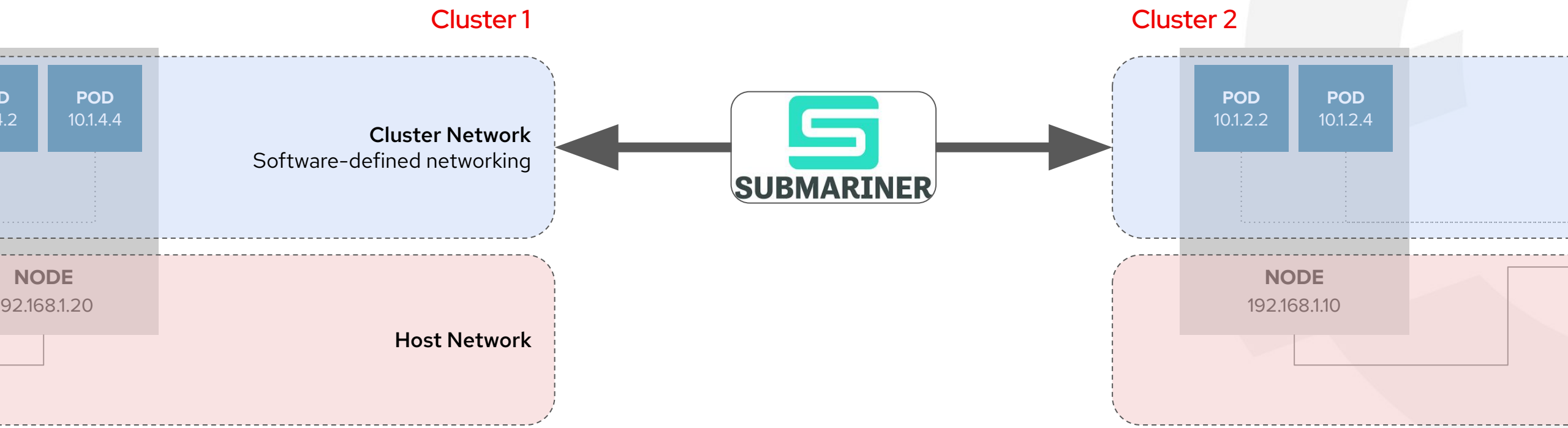




Where are we?



Where are we?



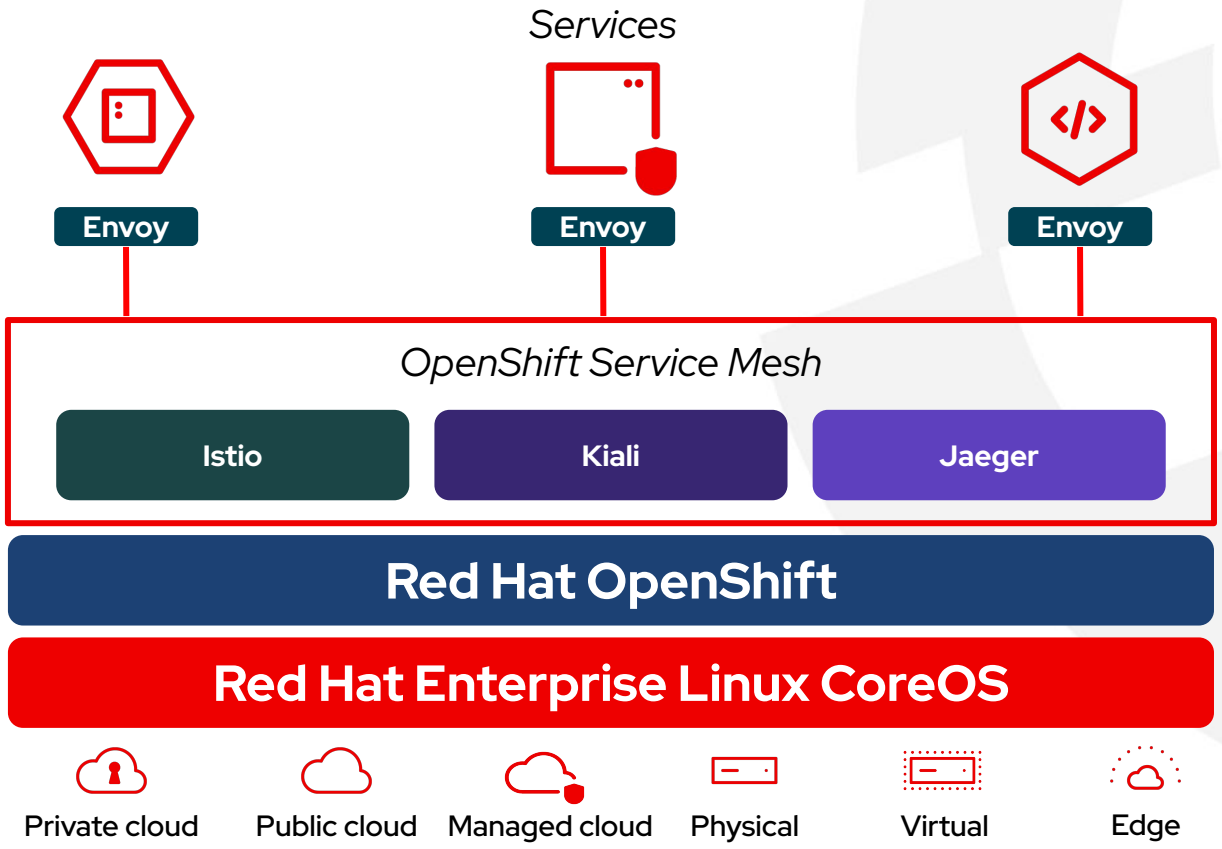
Red Hat OpenShift

Let’s move to application level

Red Hat

Connect, Secure, Control & Observe Services

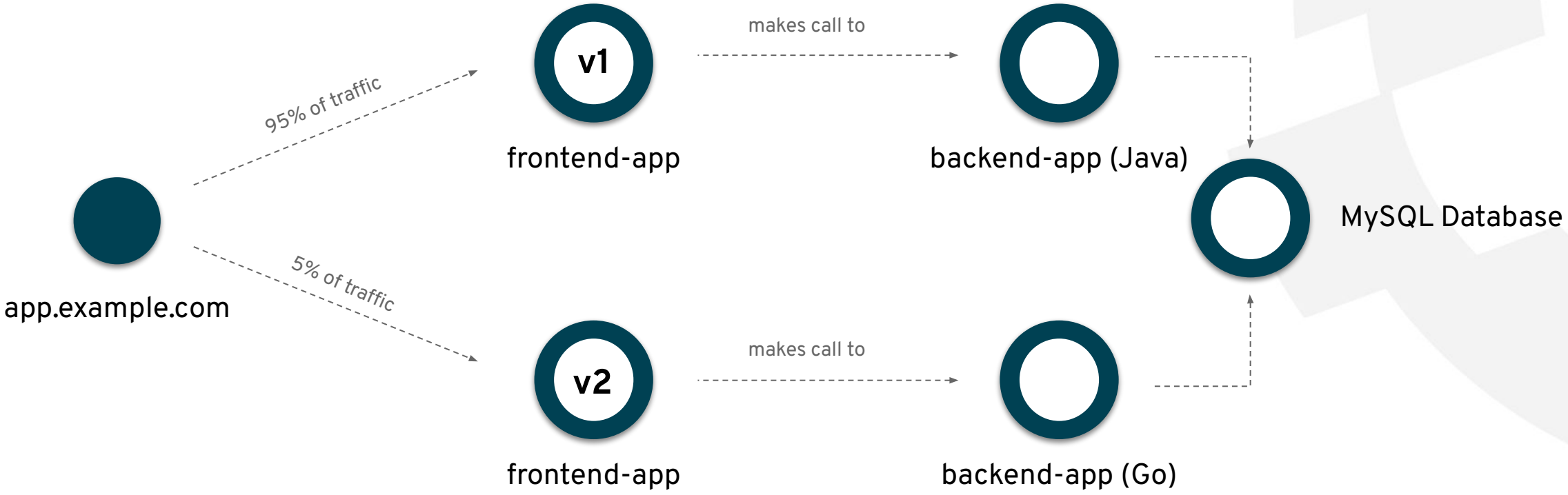
- **Connect** services securely with zero-trust network policies.
- Automatically **secure** your services with managed authentication, authorization and encryption.
- **Control** traffic to safely manage deployments, A/B testing, chaos engineering and more.
- See what's happening with out of the box distributed tracing, metrics and logging. (**Observe**)
- Manage OpenShift Service Mesh with the **Kiali** web console.



Red Hat OpenShift

Simplify the Mess With a Service Mesh

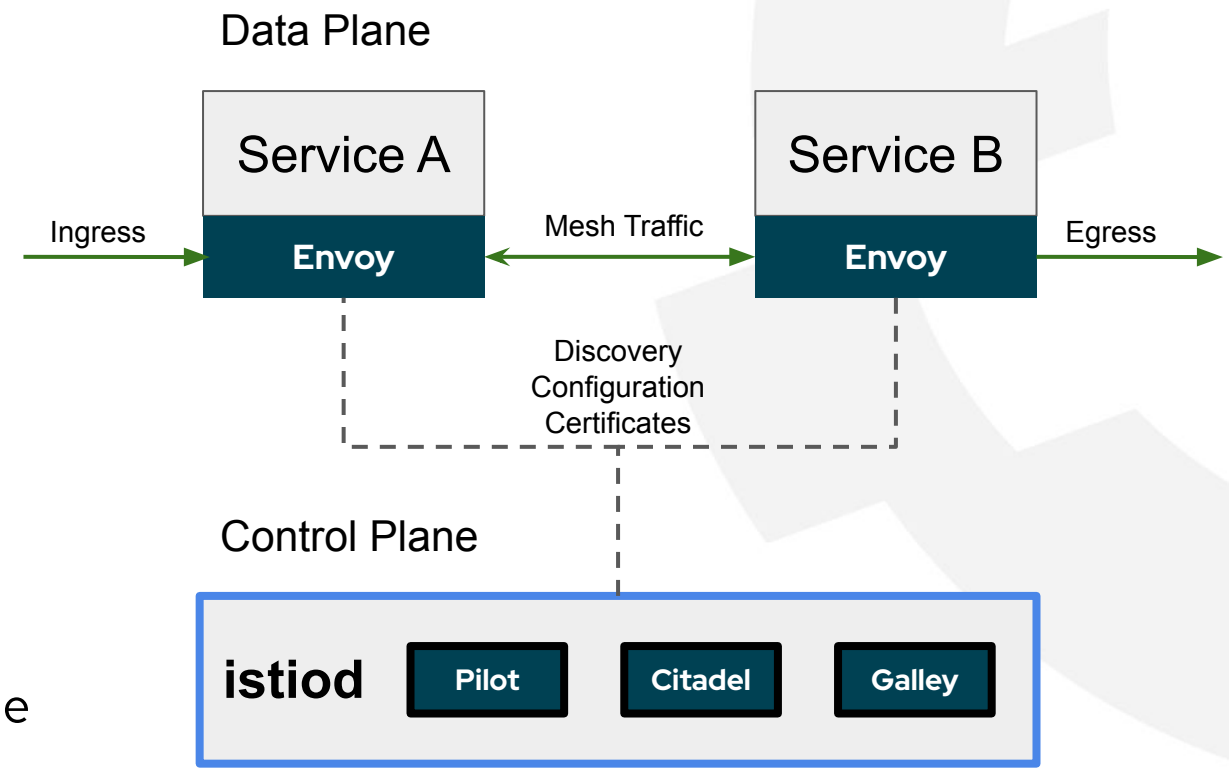
Control flow of traffic between application components



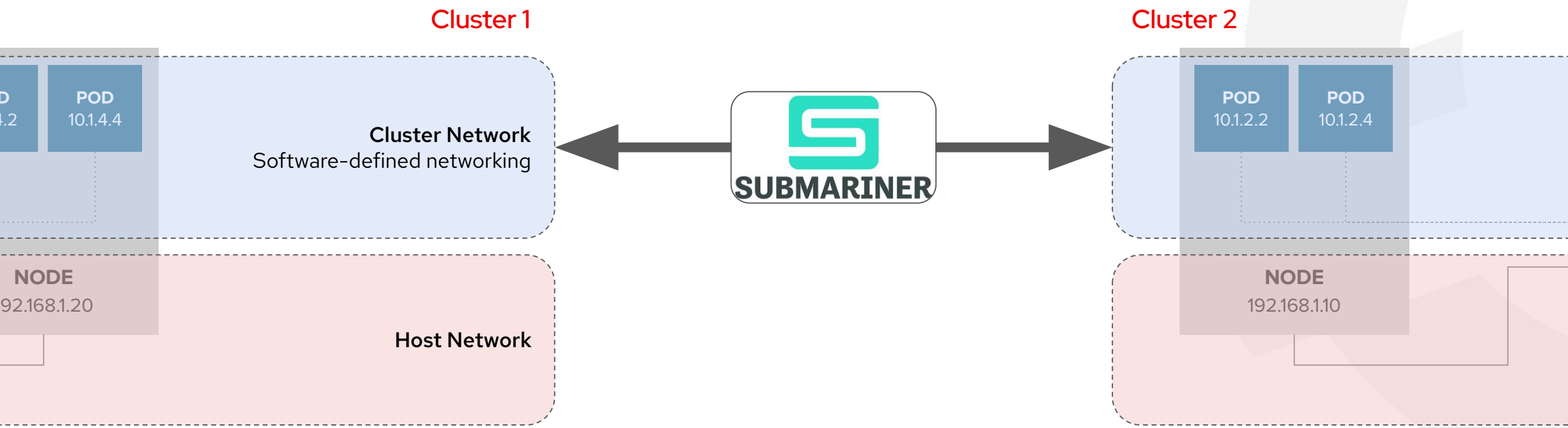
OpenShift Service Mesh

Control Plane Architecture

- Consolidates the Istio control plane components (Pilot, Galley, Citadel) into a single binary known as **istiod**.
- This provides multiple benefits:
  - Simplifies installation, upgrades and management of the Control Plane.
  - Reduces the Control Plane's resource usage and startup time.
  - Improves Control Plane performance due to a reduction in inter-control plane communication over networking.

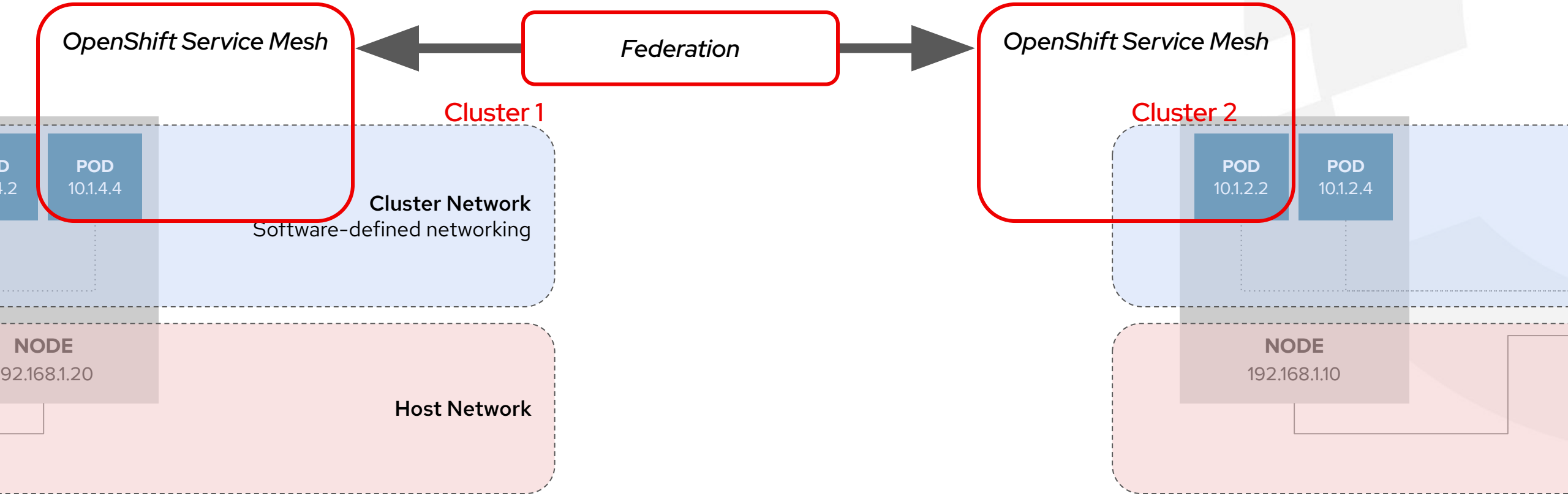


Where are we?



Red Hat OpenShift

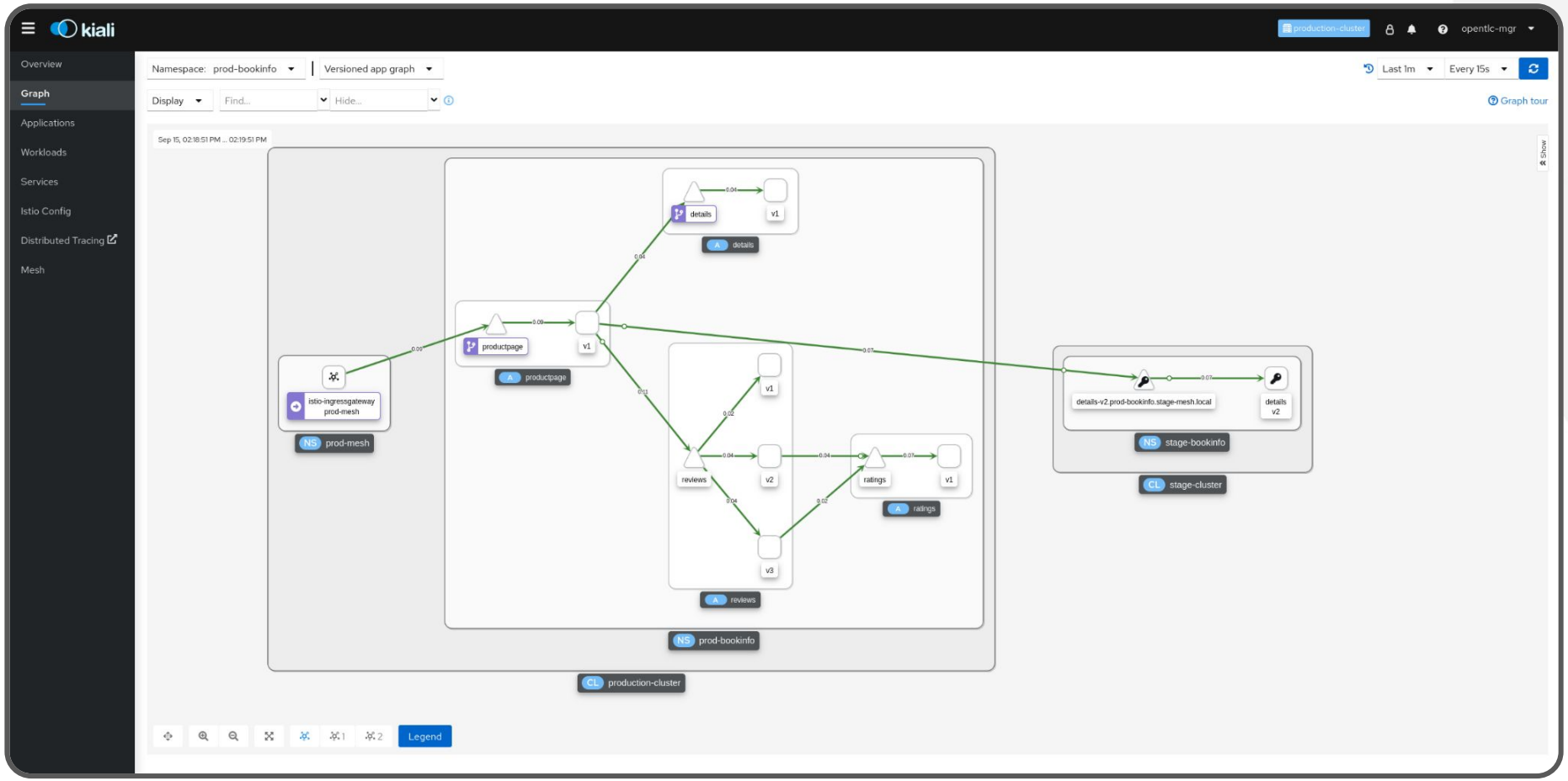
Where are we?



Red Hat OpenShift

Demo?

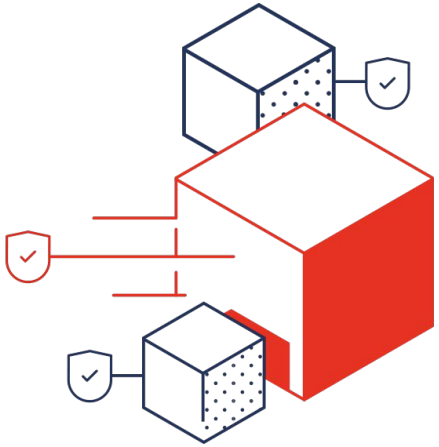
Getting started with OpenShift ServiceMesh Federation



Red Hat OpenShift

Network & Security
What did we learn today

- What is an OpenShift Cluster?
- Why do we need a Software-defined networking (SDN)?
- Container Network Interface = CNI
- Network Policy - w & w/o Advanced Cluster Security
- Network Observation
- Multicluster Networking with Advanced Cluster Manager
- Application level networking
    - OpenShift Service Mesh



Red Hat

Network & Security Q&A

Overview: Das Next Generation Datacenter mit Red Hat gestalten
Franz Theisen
19.8.2022, 11.00 - 12.00 CEST

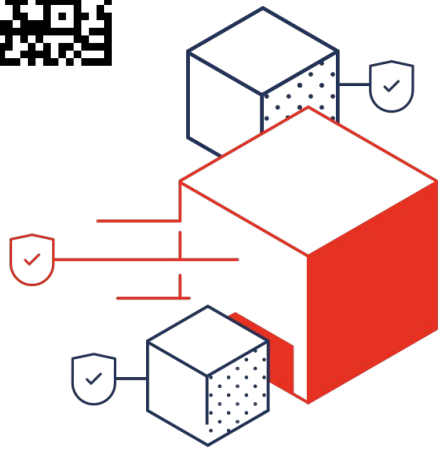
Compute: Virtualisierung und Container auf einer Platform
Domenico Piol
26.8.2022, 11.00 - 12.00 CEST

Management
Robert Baumgartner
2.9.2022, 11:00-12.00 CEST

Storage: MultiCloud, Unified, Converged oder klassisch
Matthias Rettl
9.9.2022, 11:00-12.00 CEST

Networking & Security
Robert Bohne
16.9.2022, 11:00-12.00 CEST

Recordings



Red Hat

Thank you

Red Hat