Red Hat OpenShift

ARCHITECTURAL OVERVIEW

Alfred Bach
Principal Solution Architect

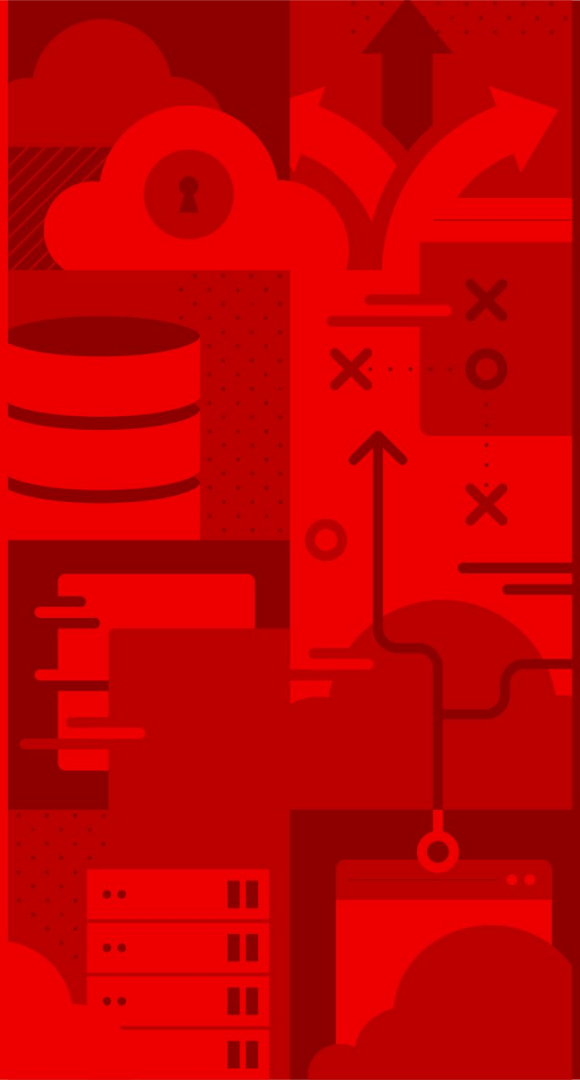
linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

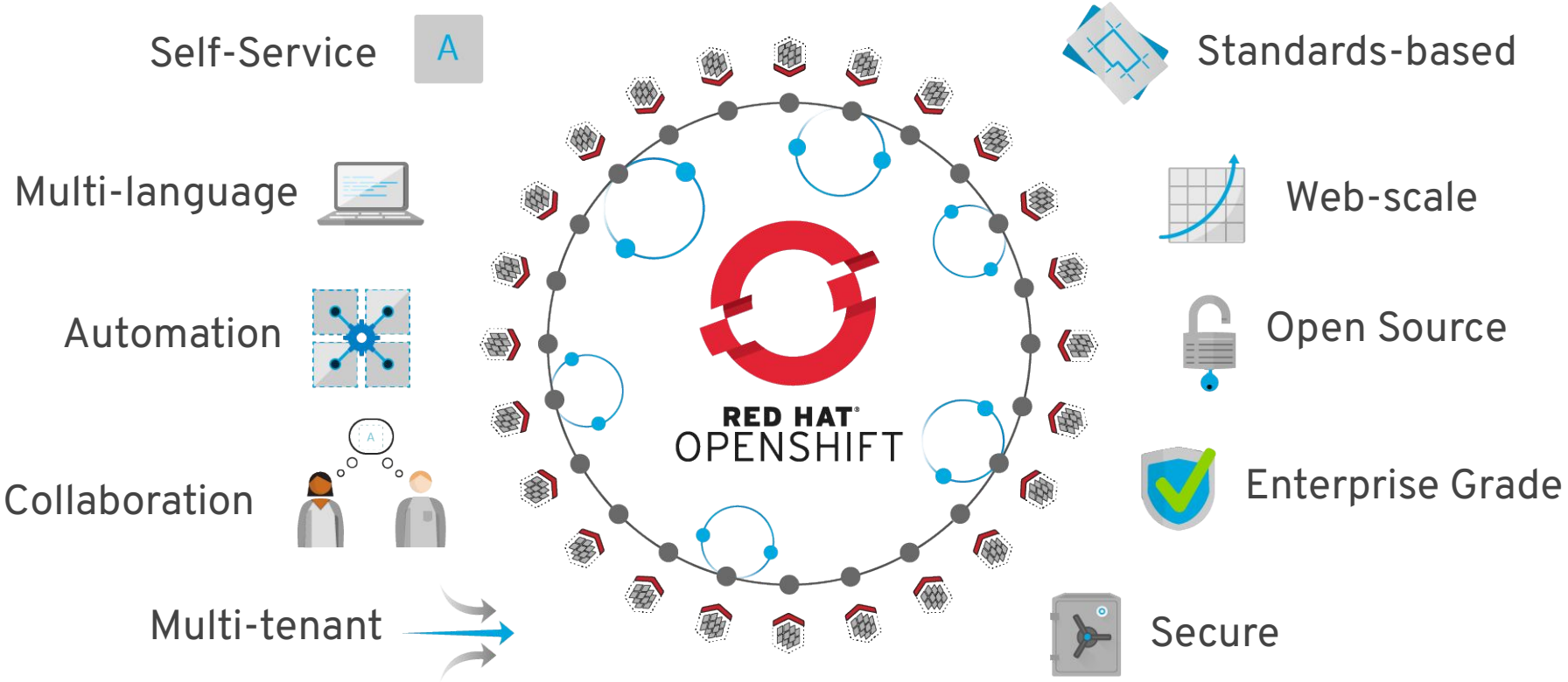
twitter.com/RedHat

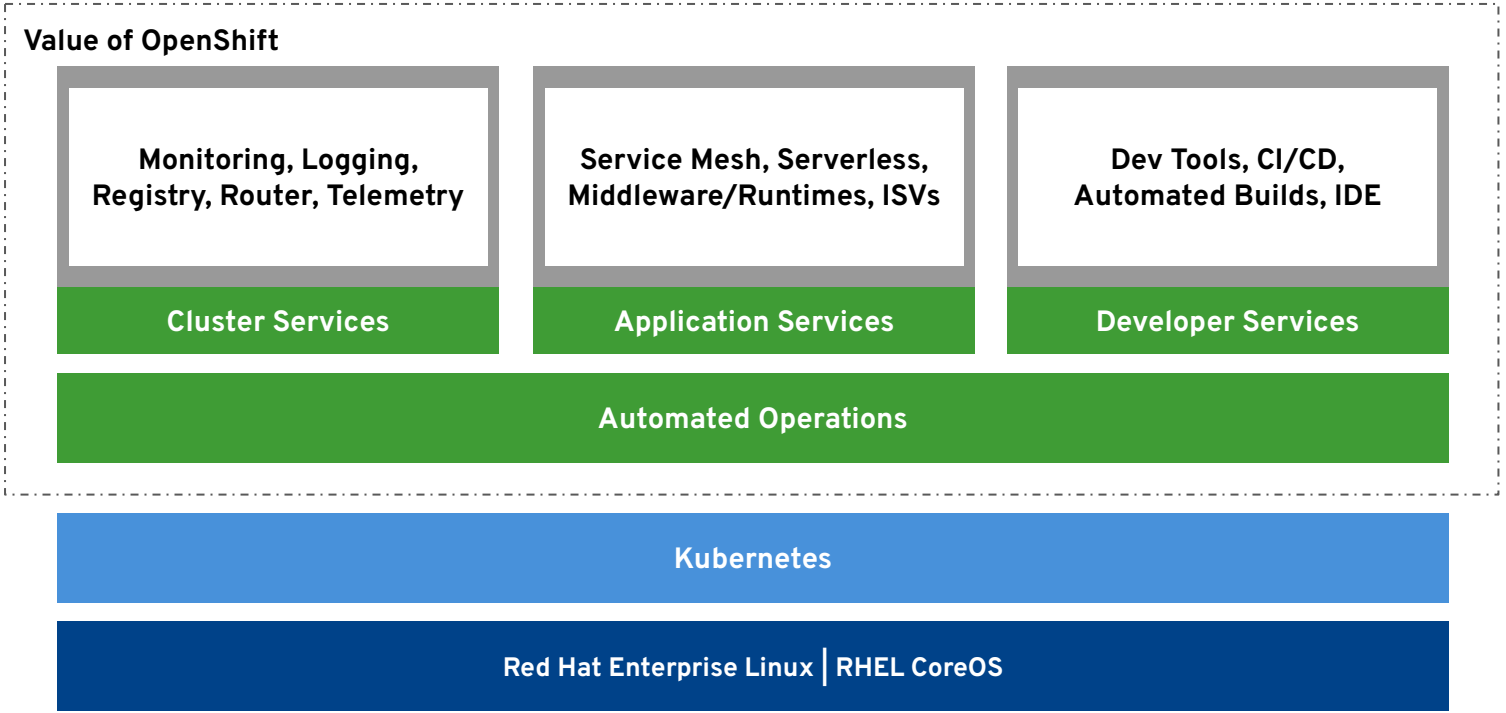
Red Hat



Functional overview

Red Hat


Self-Service
Multi-language
Automation
Collaboration
Multi-tenant
RED HAT
OPENSHIFT
Standards-based
Web-scale
Open Source
Enterprise Grade
Secure

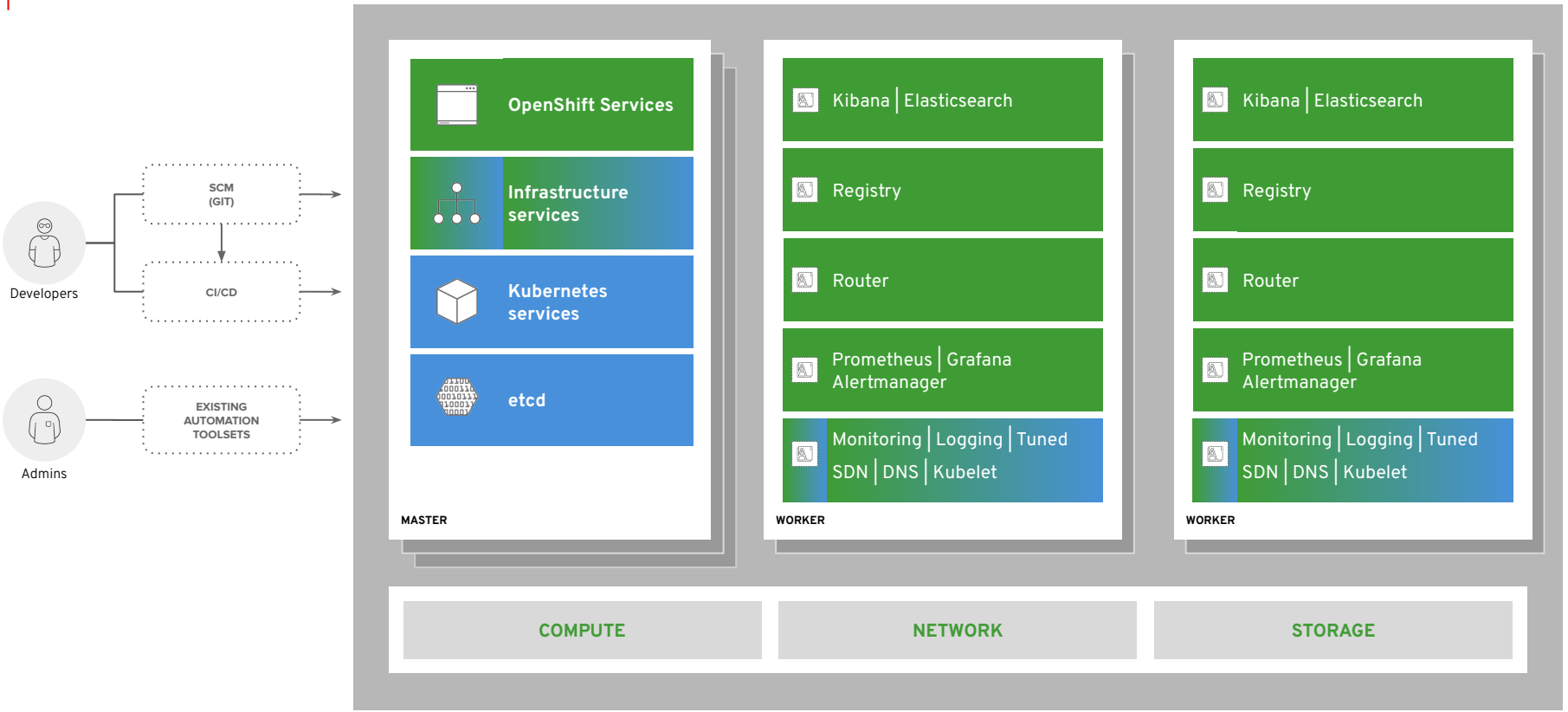


Best IT Ops Experience

CaaS ⟷ PaaS ⟷ FaaS

Best Developer Experience

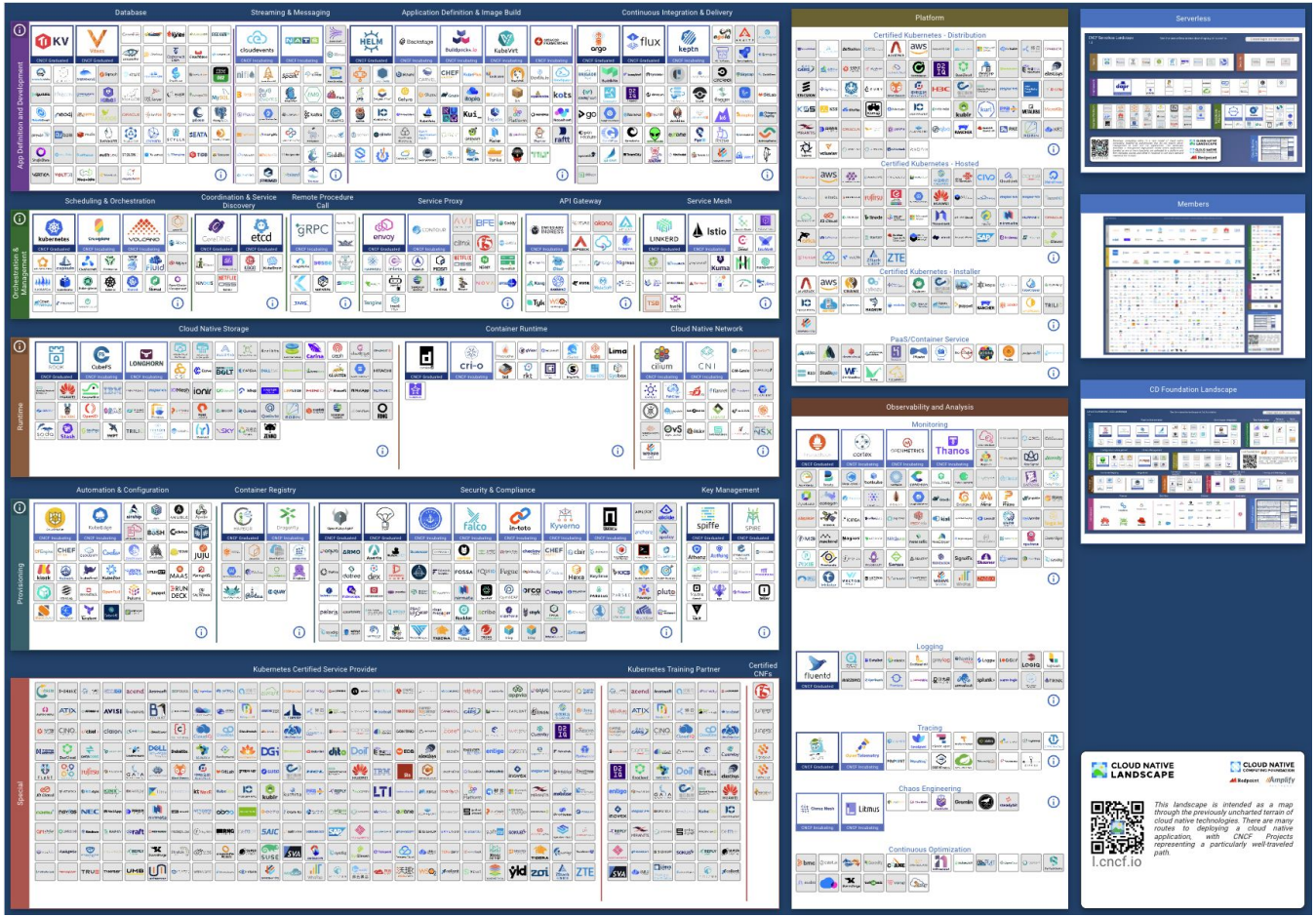
Red Hat


SCM (GIT)
CI/CD
Developers
EXISTING AUTOMATION TOOLSETS
Admins
OpenShift Services
Infrastructure services
Kubernetes services
etcd
MASTER
Kibana | Elasticsearch
Registry
Router
Prometheus | Grafana Alertmanager
Monitoring | Logging | Tuned
SDN | DNS | Kubelet
WORKER
Kibana | Elasticsearch
Registry
Router
Prometheus | Grafana Alertmanager
Monitoring | Logging | Tuned
SDN | DNS | Kubelet
WORKER
COMPUTE
NETWORK
STORAGE

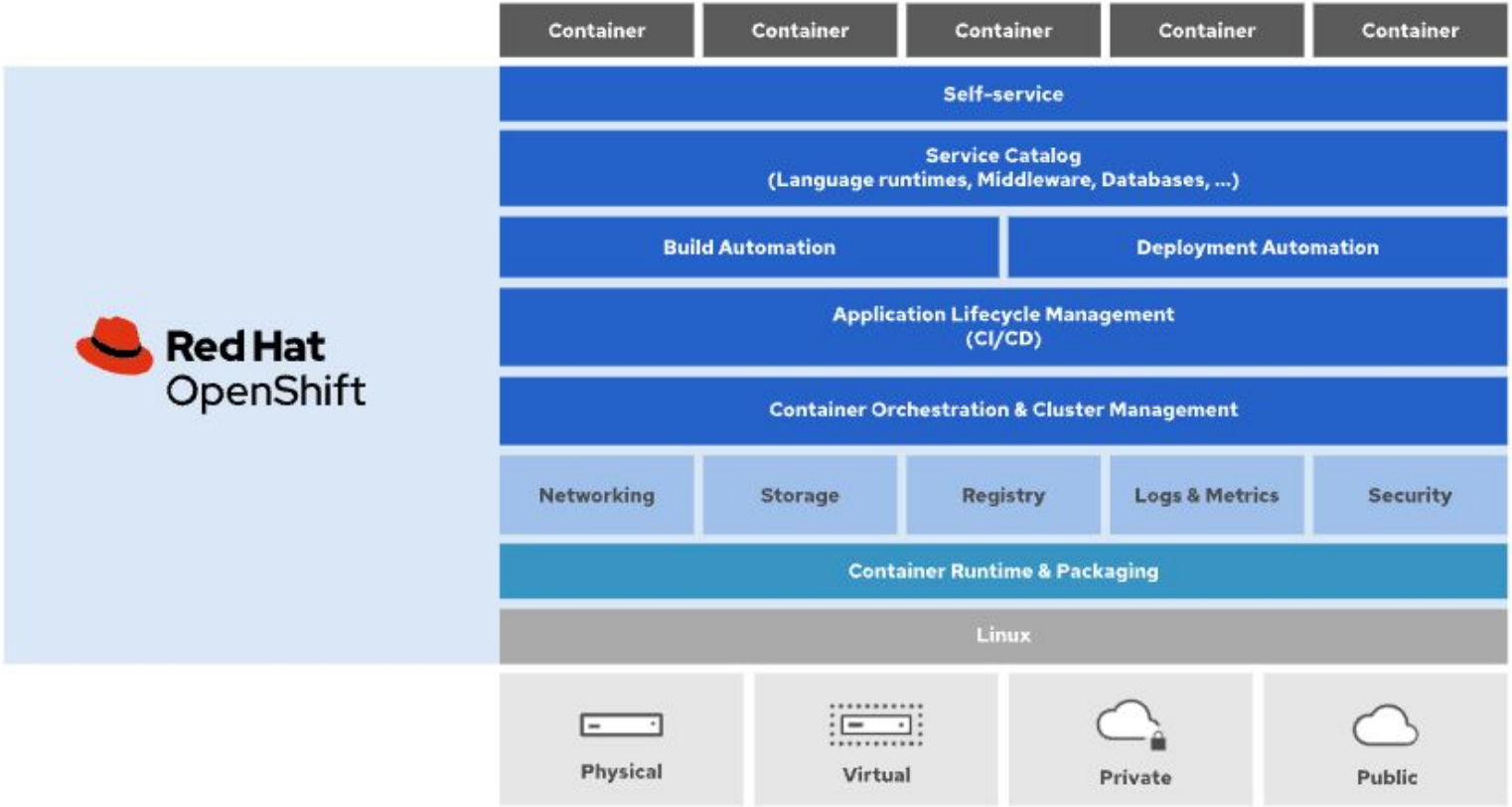
Red Hat

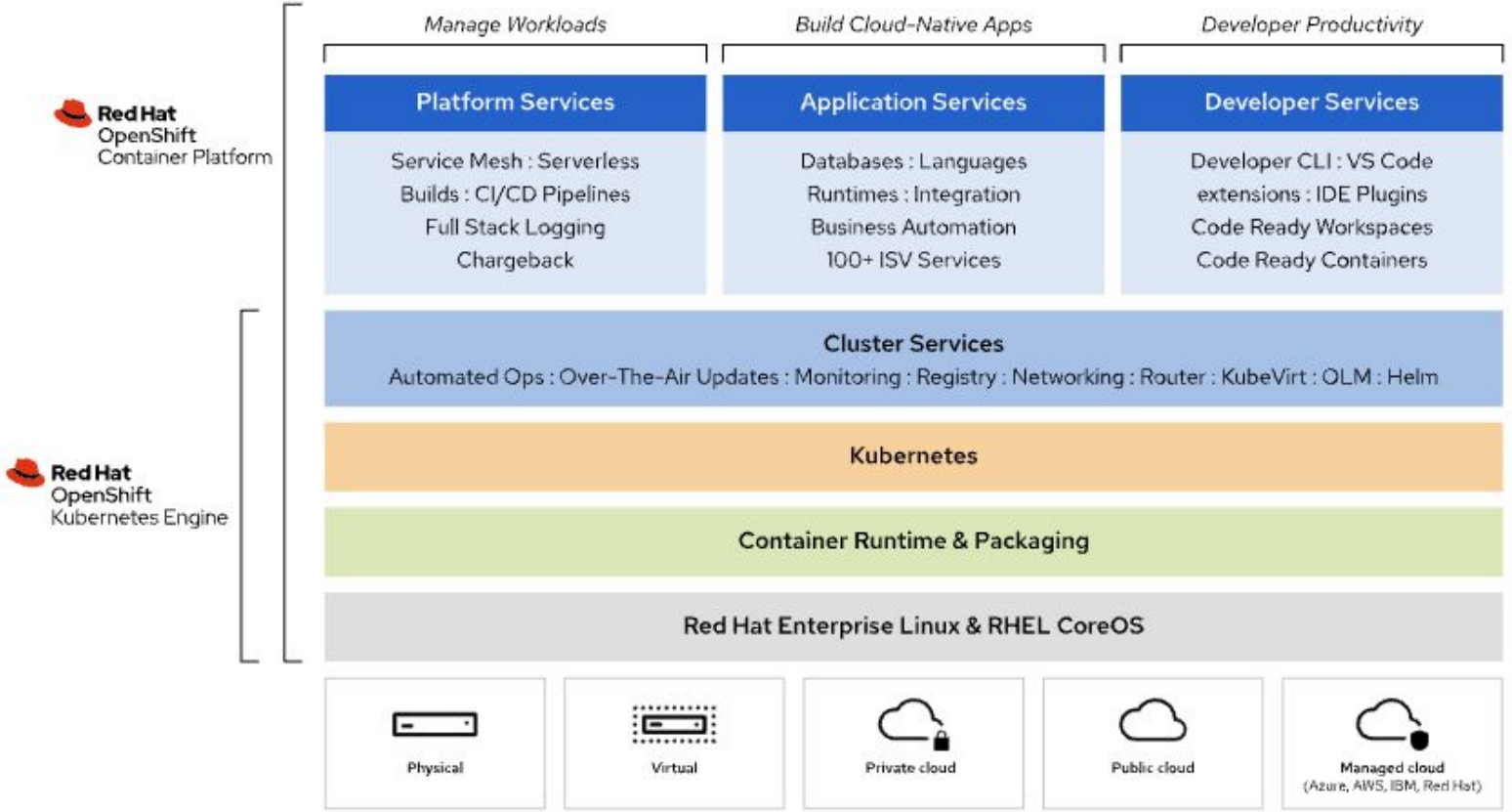
CLOUD NATIVE LANDSCAPE

CNCF Ecosystem Slide

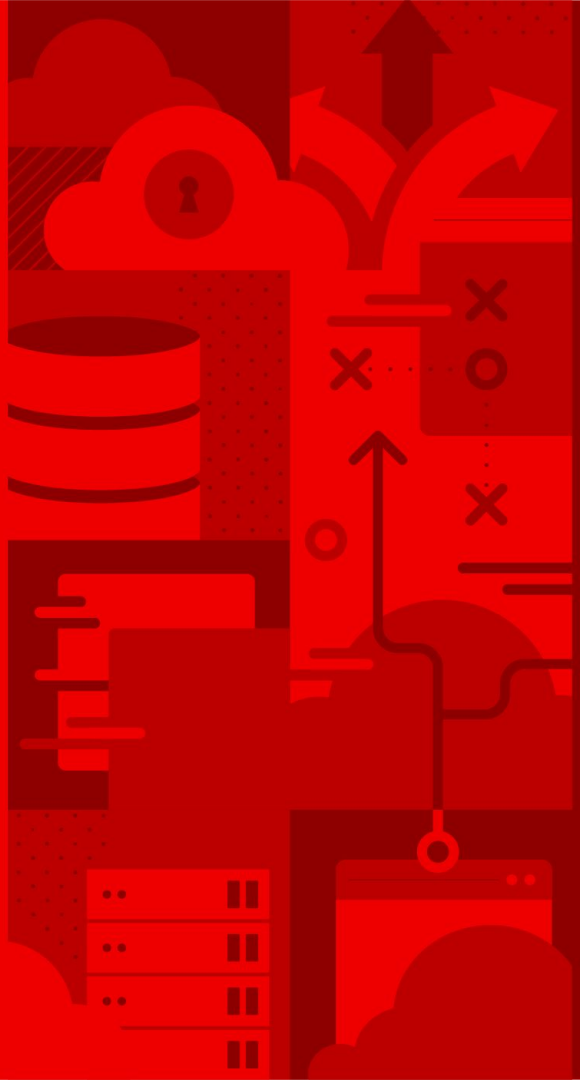


Red Hat


Container
Container
Container
Container
Container
Self-service
Service Catalog
(Language runtimes, Middleware, Databases, ...)
Build Automation
Deployment Automation
Application Lifecycle Management
(CI/CD)
Container Orchestration & Cluster Management
Networking
Storage
Registry
Logs & Metrics
Security
Container Runtime & Packaging
Linux
Red Hat
OpenShift
Physical
Virtual
Private
Public


Red Hat OpenShift Container Platform
Red Hat OpenShift Kubernetes Engine
Manage Workloads
Build Cloud-Native Apps
Developer Productivity
Platform Services
Service Mesh : Serverless
Builds : CI/CD Pipelines
Full Stack Logging
Chargeback
Application Services
Databases : Languages
Runtimes : Integration
Business Automation
100+ ISV Services
Developer Services
Developer CLI : VS Code
extensions : IDE Plugins
Code Ready Workspaces
Code Ready Containers
Cluster Services
Automated Ops : Over-The-Air Updates : Monitoring : Registry : Networking : Router : KubeVirt : OLM : Helm
Kubernetes
Container Runtime & Packaging
Red Hat Enterprise Linux & RHEL CoreOS
Physical
Virtual
Private cloud
Public cloud
Managed cloud
(Azure, AWS, IBM, Red Hat)

Red Hat



OpenShift 4 Architecture

Red Hat

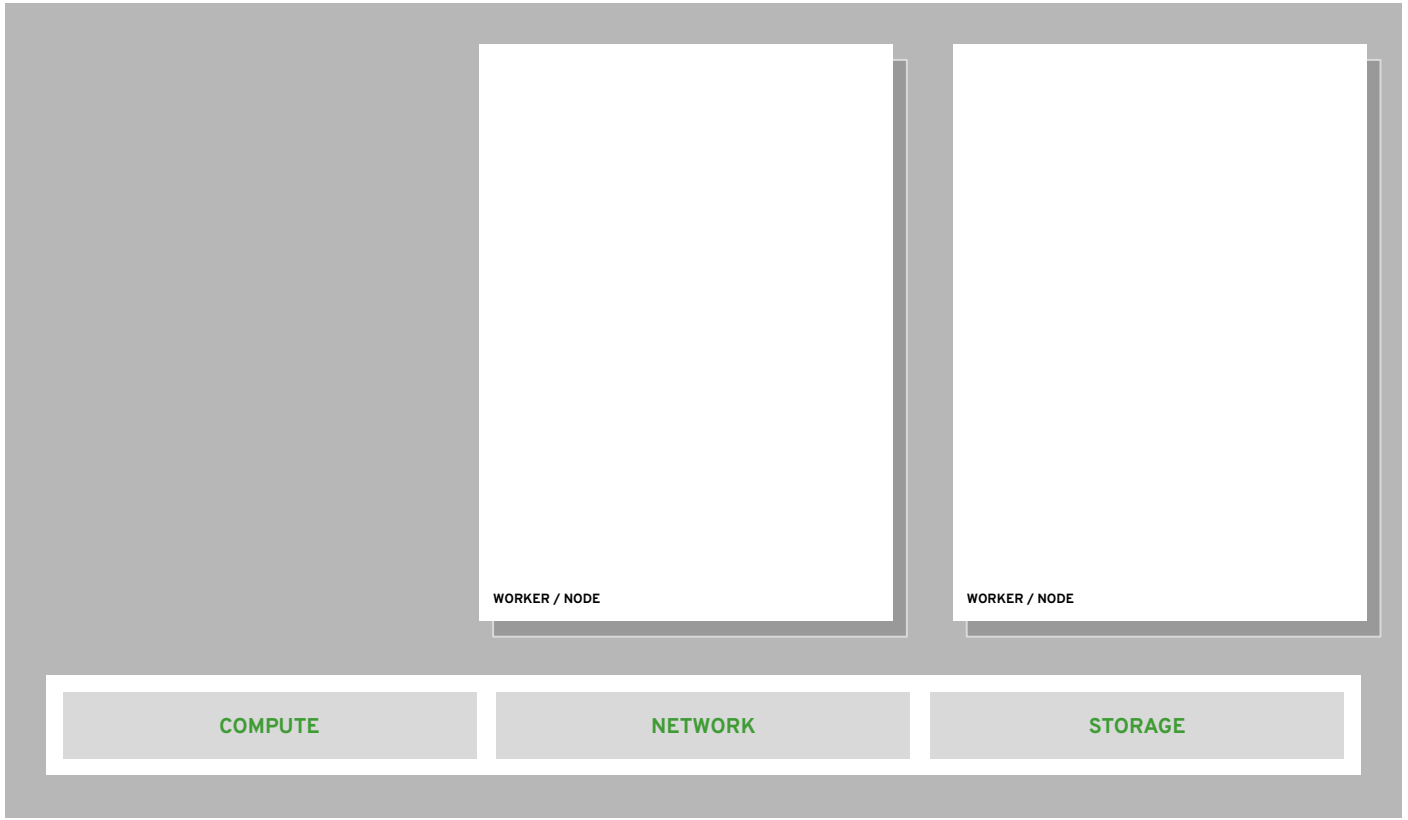
your choice of infrastructure

COMPUTE

NETWORK

STORAGE

workers run workloads

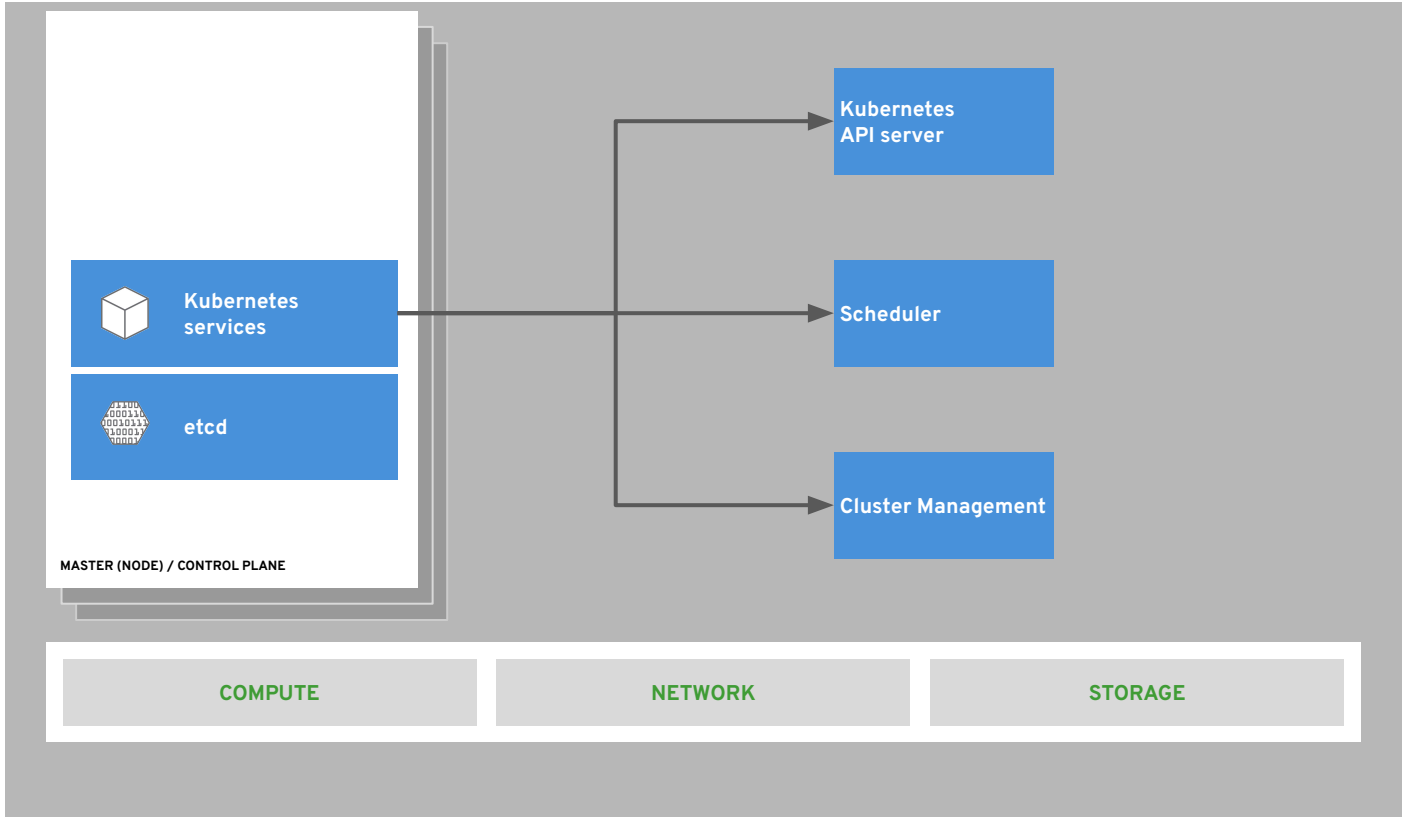


masters are the control plane

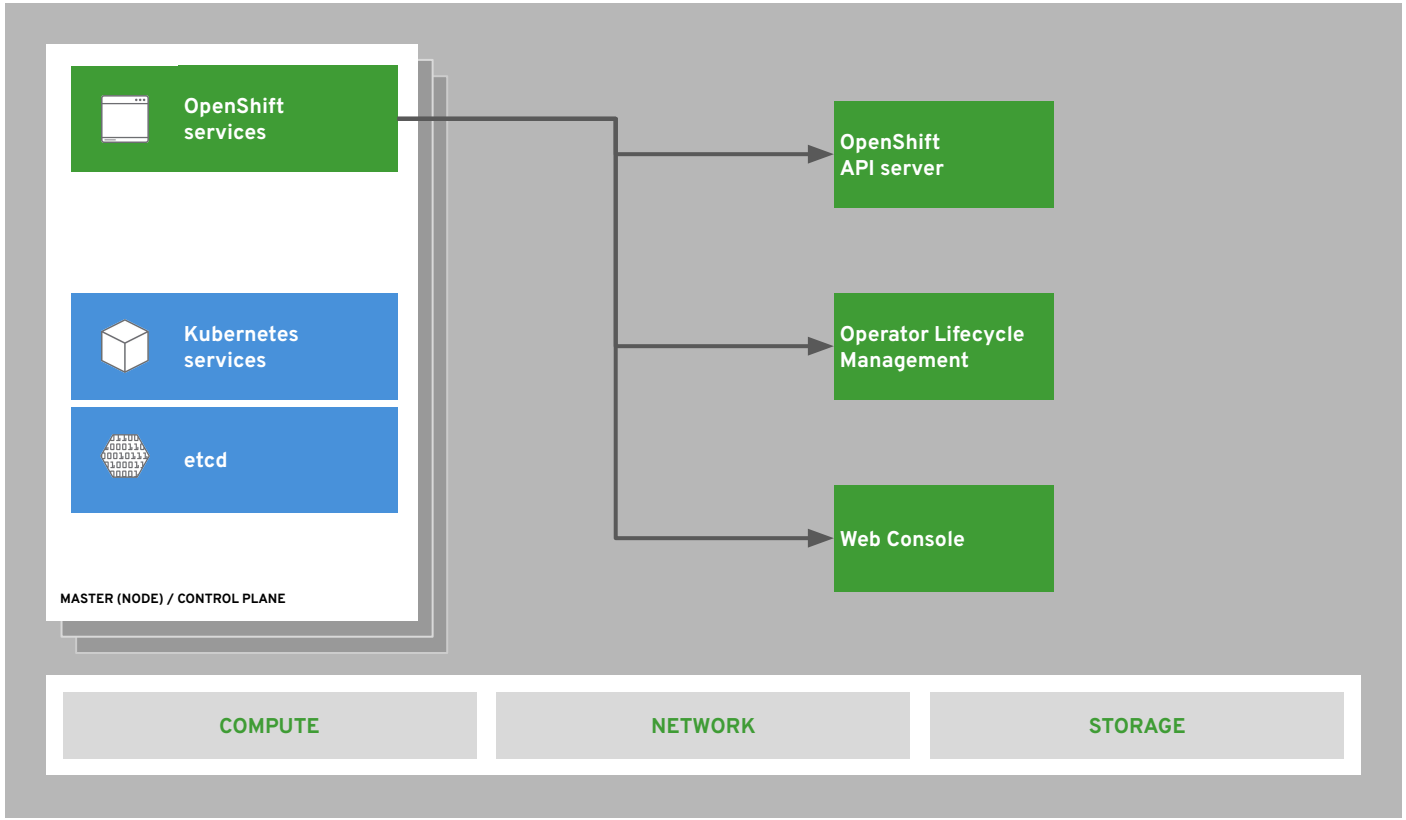
Red Hat

state of everything

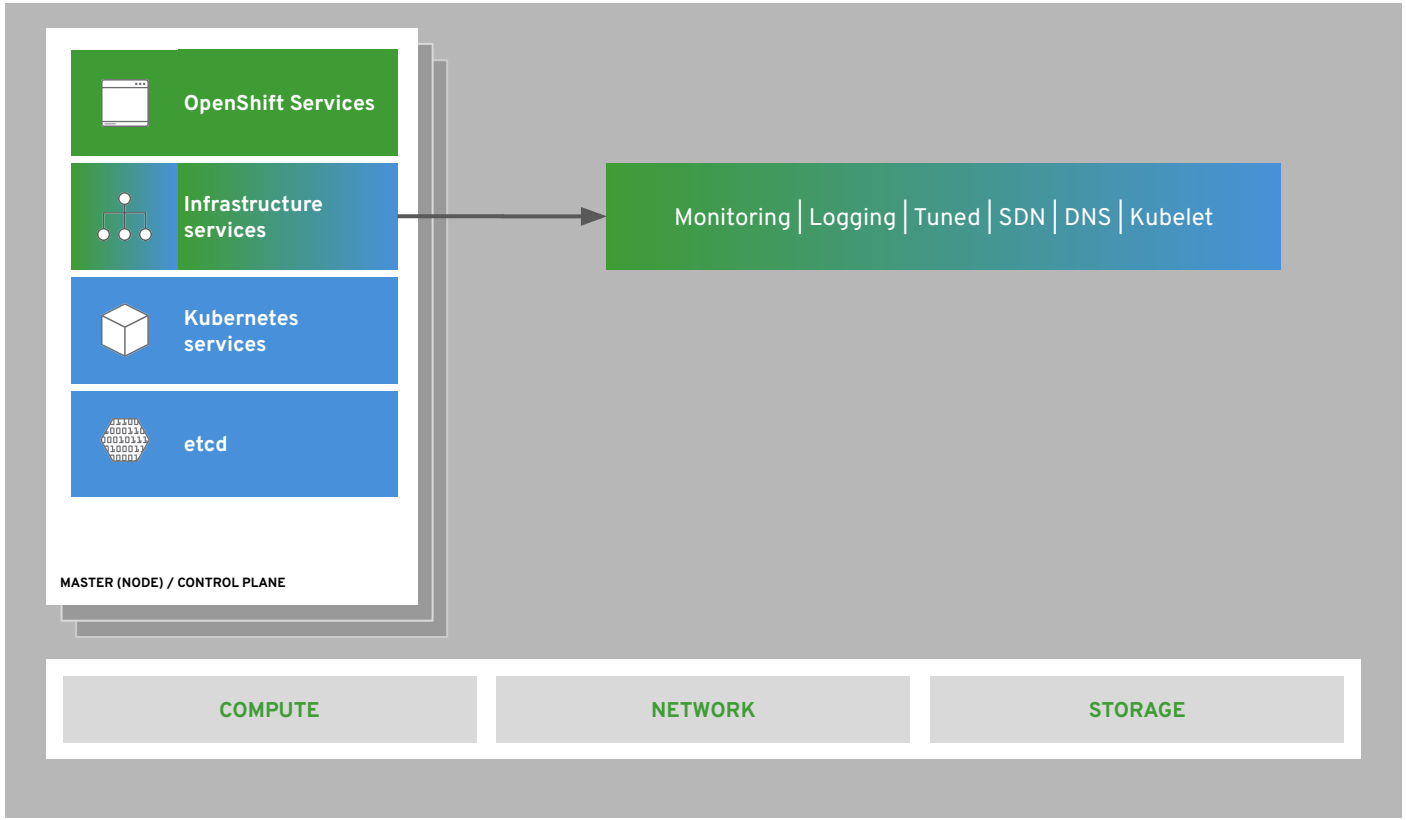
core kubernetes components



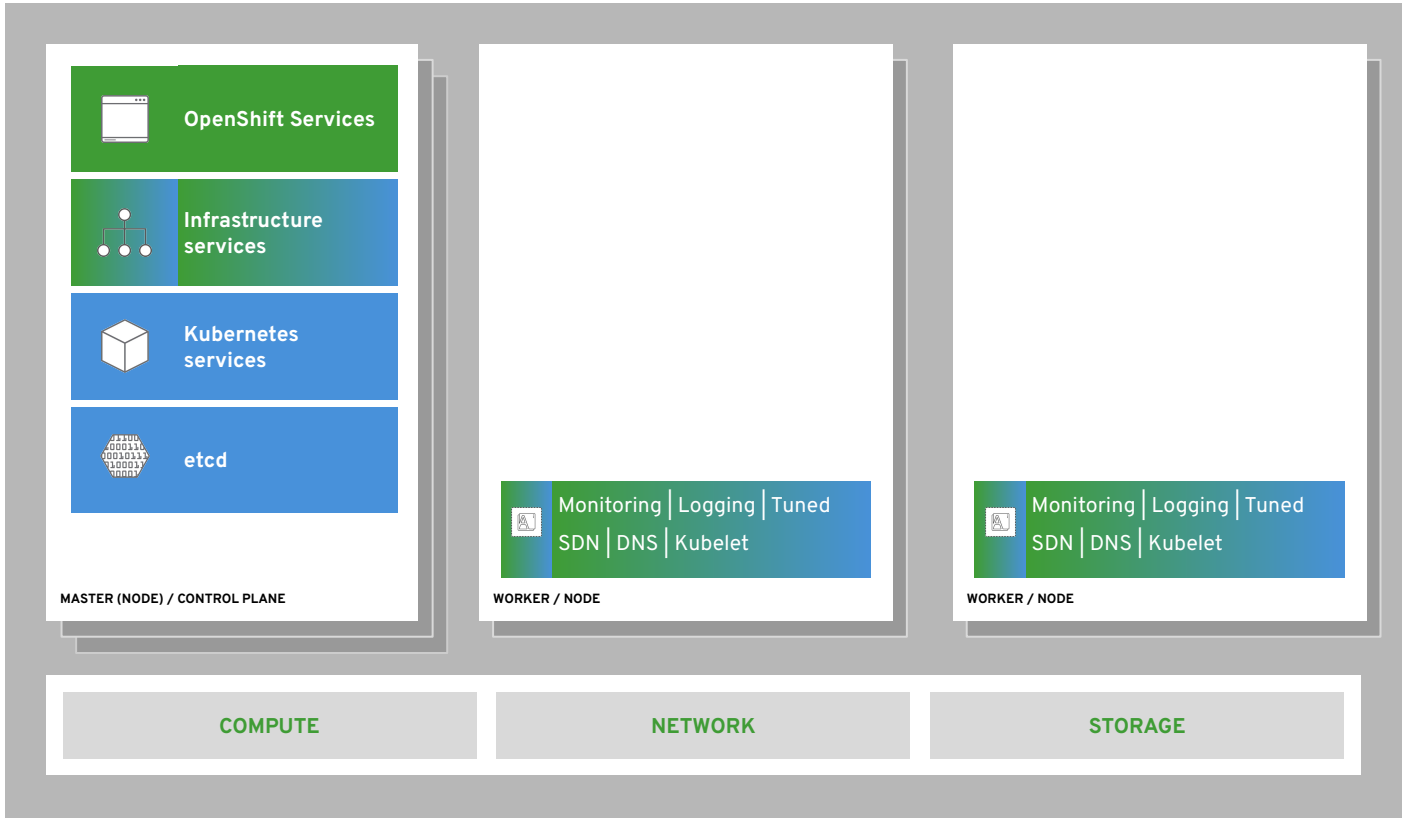
core OpenShift components



internal and support infrastructure services

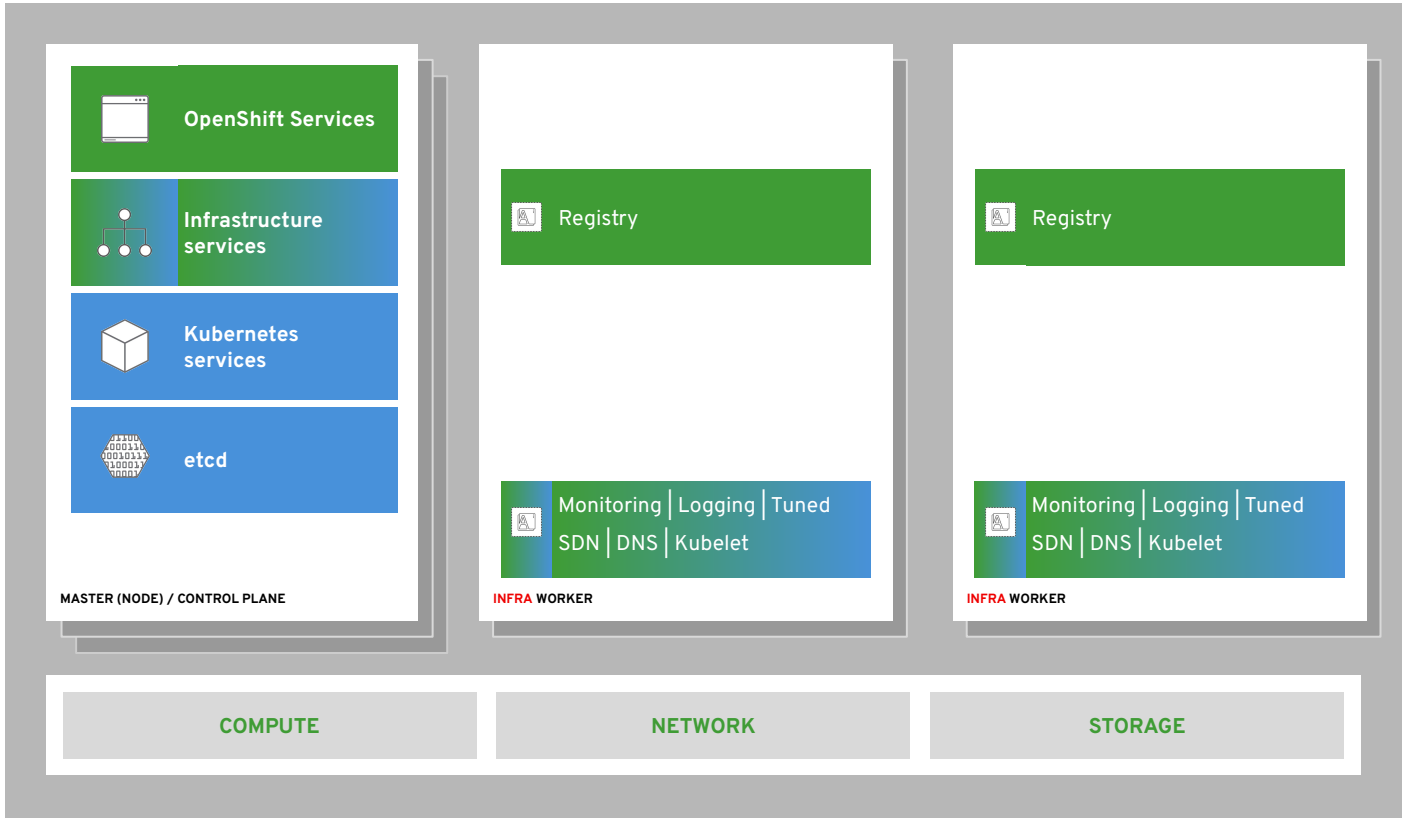


run on all hosts



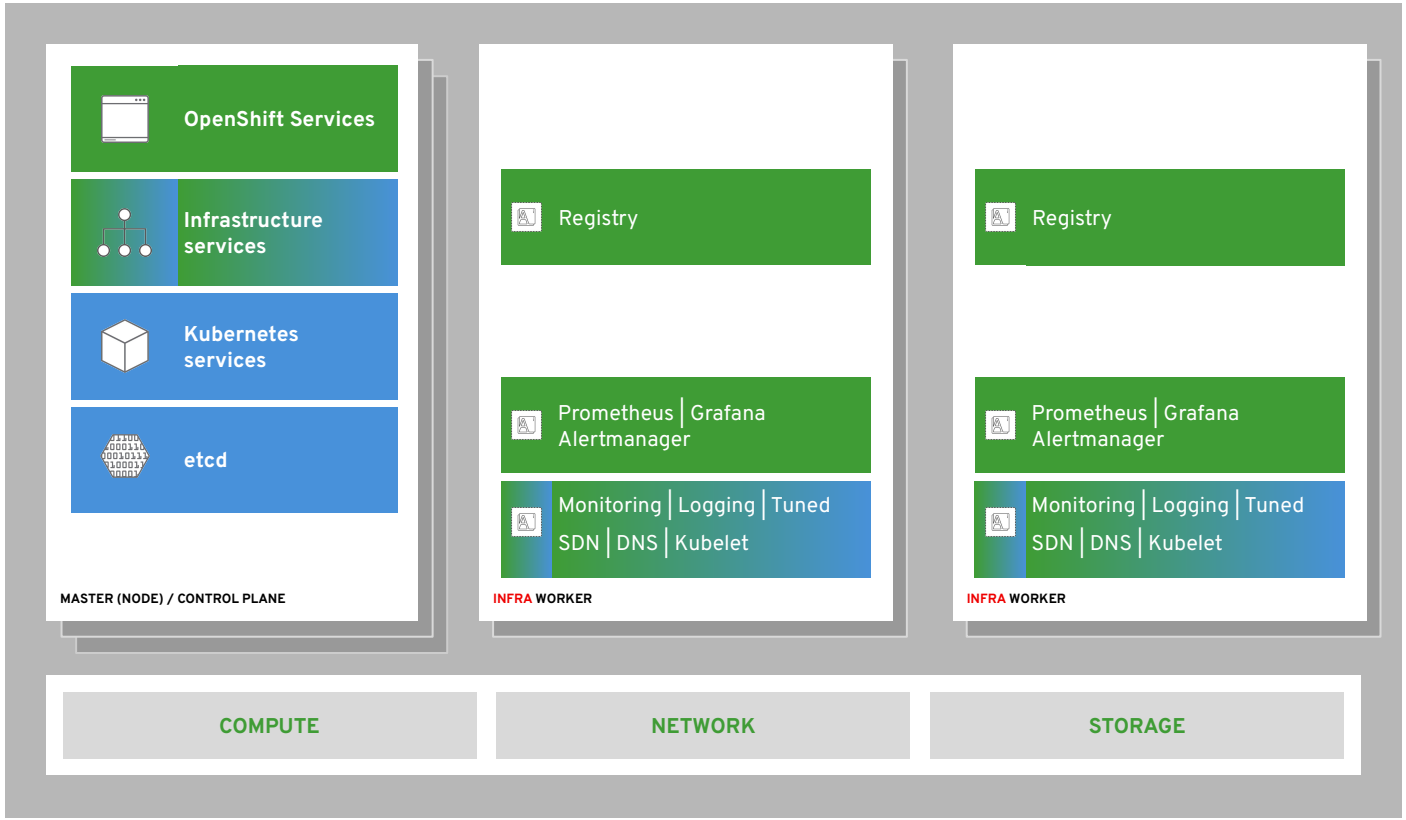
Red Hat

integrated image registry

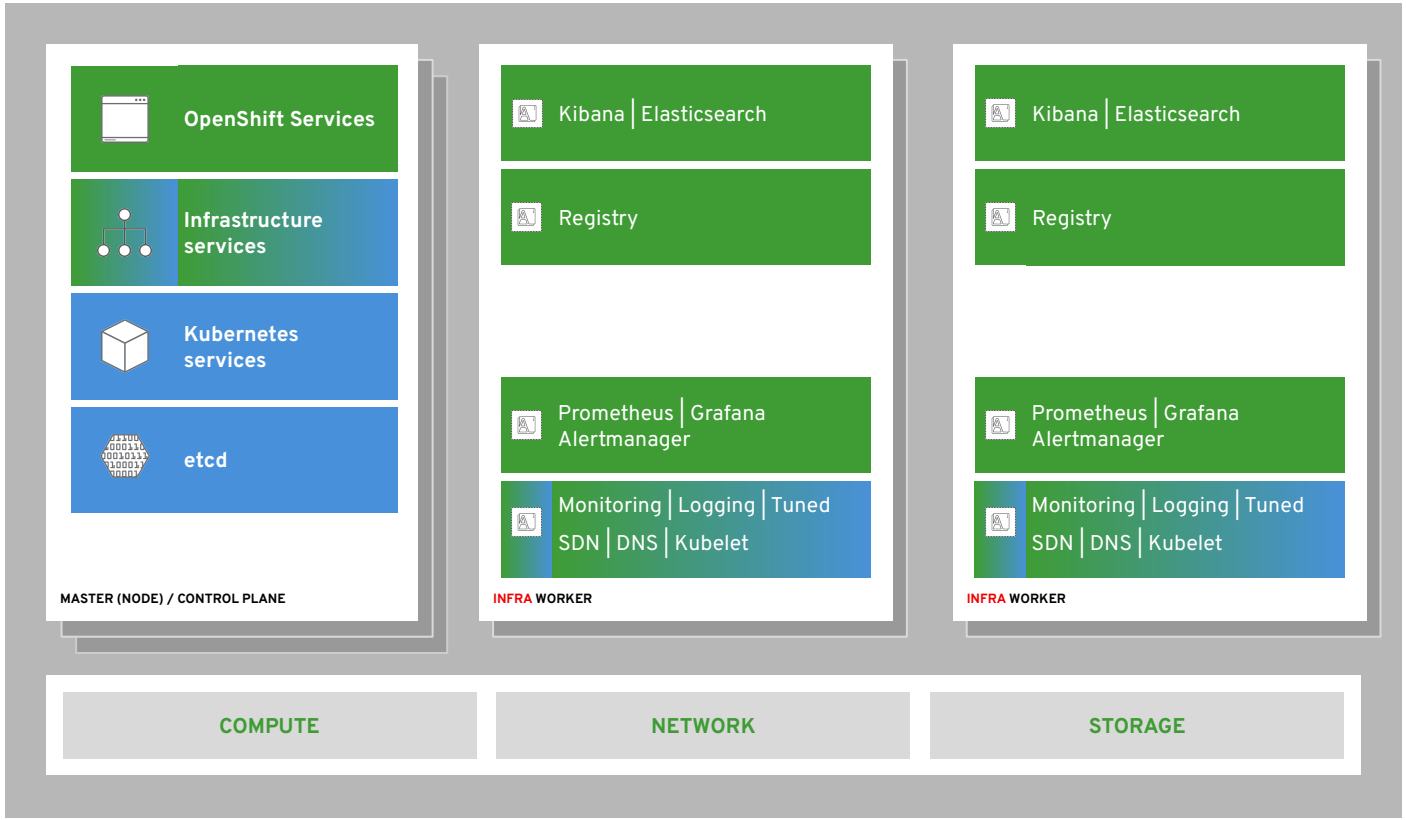


Red Hat

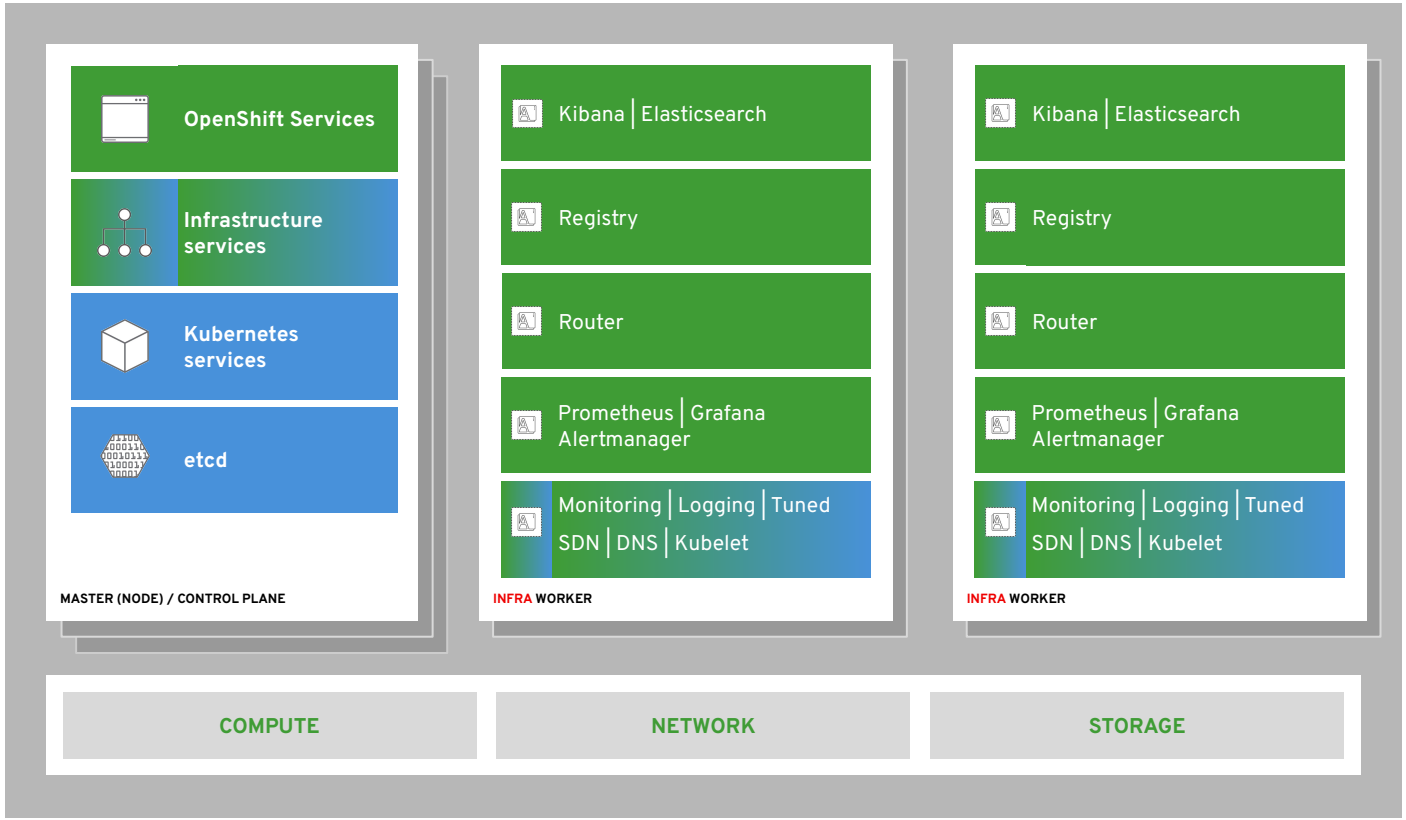
cluster monitoring



log aggregation

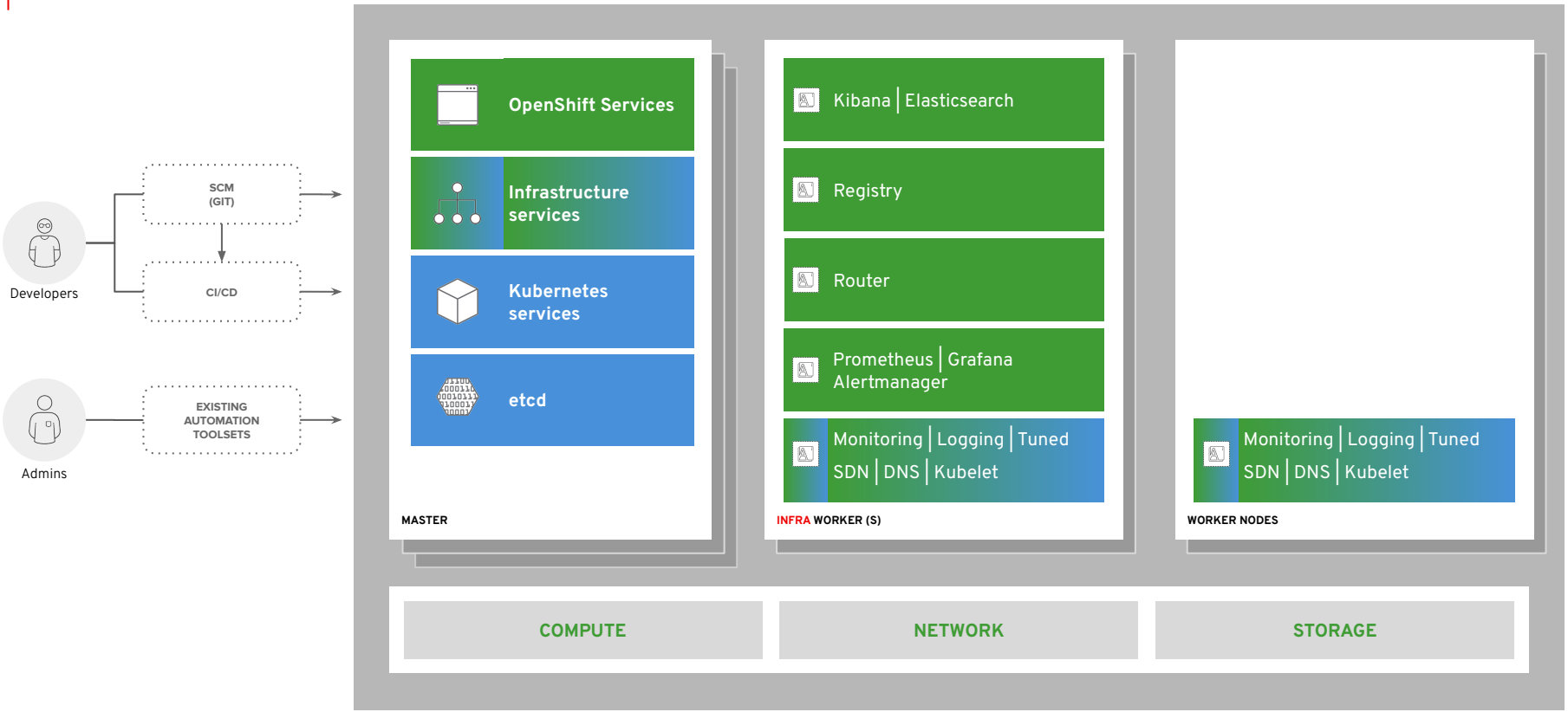


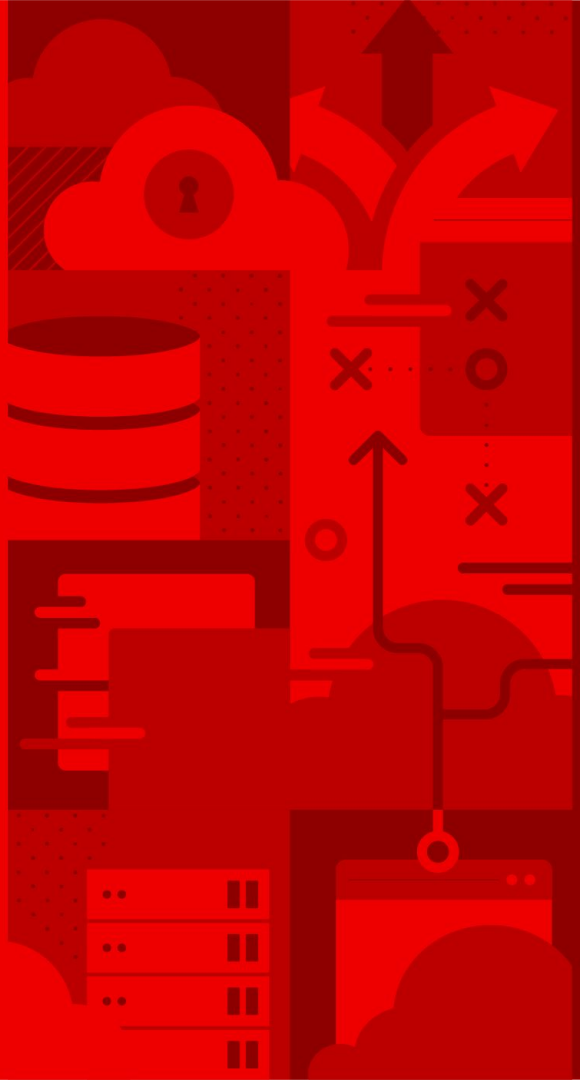
integrated routing



Red Hat

dev and ops via web, cli, API, and IDE



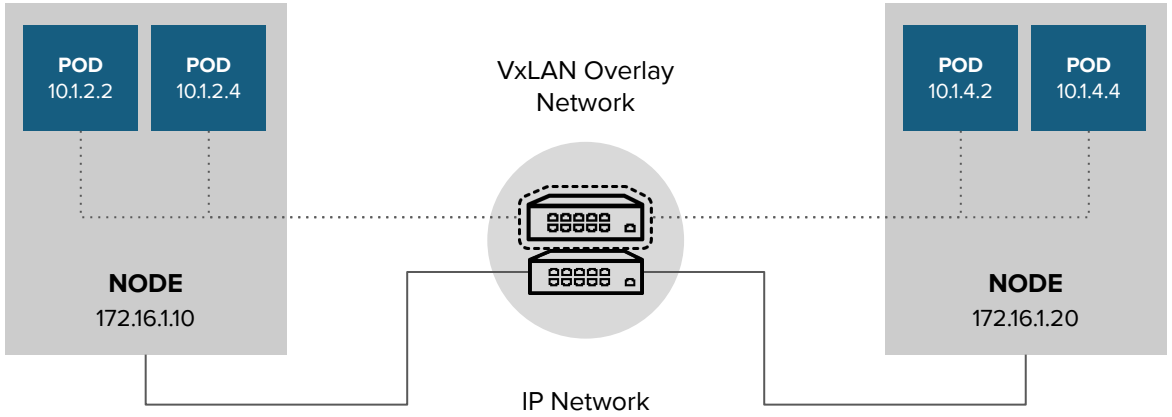


Networking

A pluggable model for network interface controls in kubernetes

Red Hat

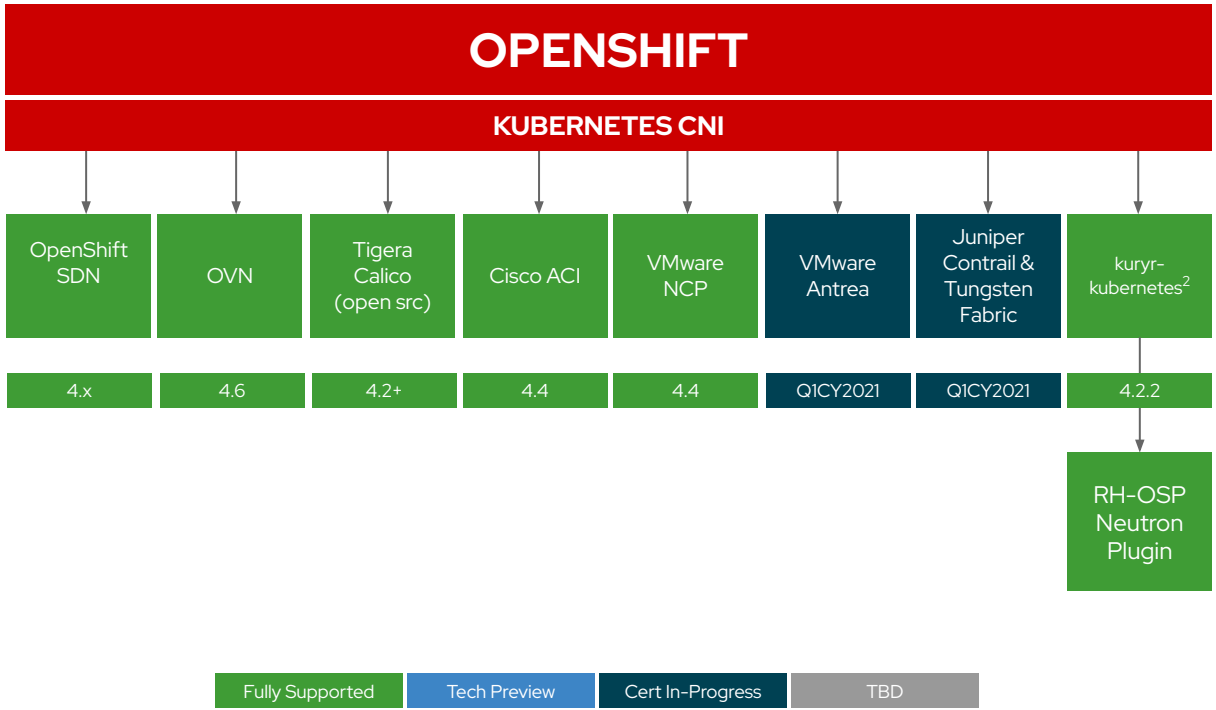
OpenShift SDN high-level architecture



OpenShift Networking Plug-ins

3rd-party Kubernetes CNI plug-in certification primarily consists of:

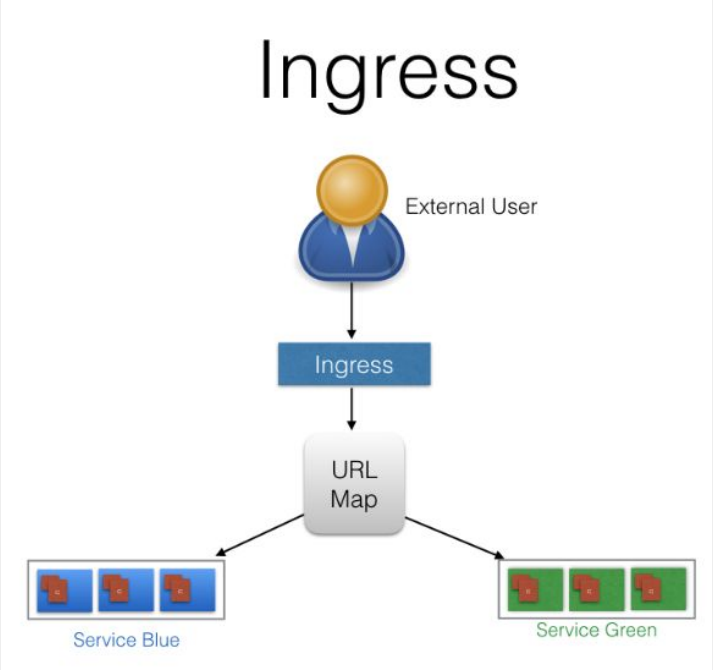
1. Formalizing the partnership
2. Certifying the container(s)
3. Certifying the Operator
4. Successfully passing the same Kubernetes networking conformance tests that OpenShift uses to validate its own SDN



Product Manager: Marc Curry

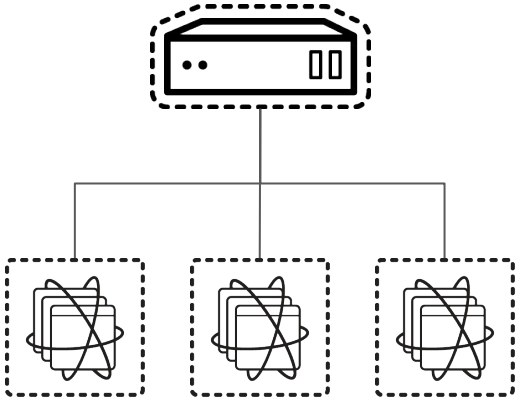
routes and ingress

How traffic enters the cluster



Routing and Load Balancing

- Pluggable routing architecture
  - HAProxy Router
  - F5 Router
- Multiple-routers with traffic sharding
- Router supported protocols
  - HTTP/HTTPS
  - WebSockets
  - TLS with SNI
- Non-standard ports via cloud load-balancers, external IP, and NodePort

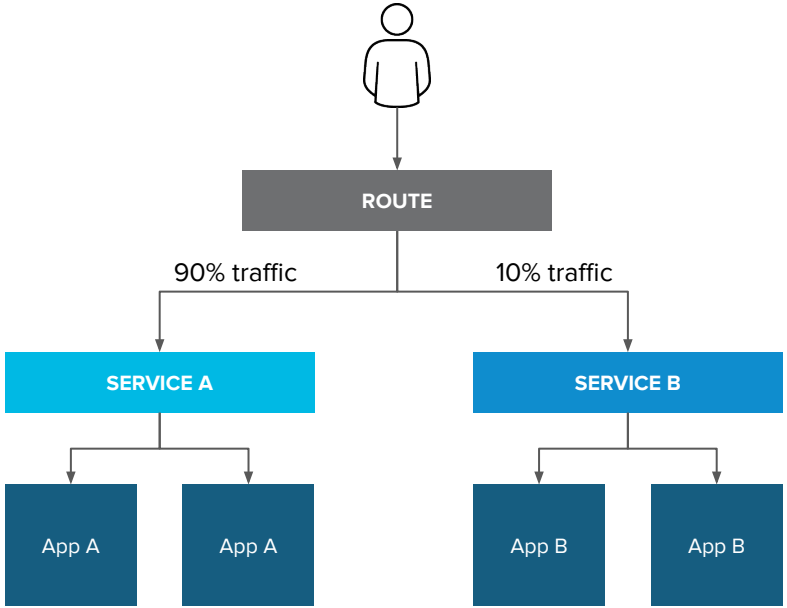


Routes vs Ingress

Feature	Ingress	Route
Standard Kubernetes object	X	
External access to services	X	X
Persistent (sticky) sessions	X	X
Load-balancing strategies (e.g. round robin)	X	X
Rate-limit and throttling	X	X
IP whitelisting	X	X
TLS edge termination	X	X
TLS re-encryption	X	X
TLS passthrough	X	X
Multiple weighted backends (split traffic)		X
Generated pattern-based hostnames		X
Wildcard domains		X

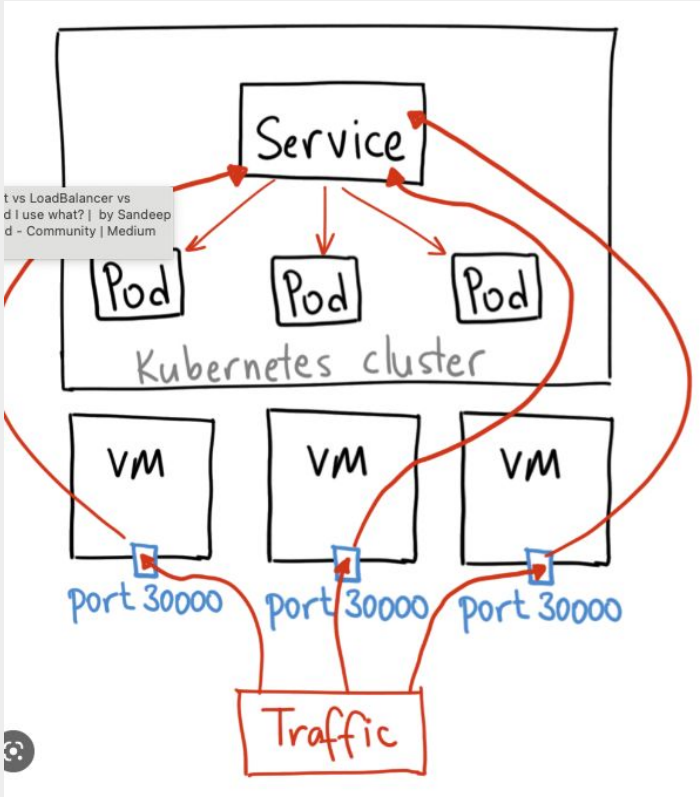
Router-based deployment methodologies

Split Traffic Between Multiple Services For A/B Testing, Blue/Green and Canary Deployments



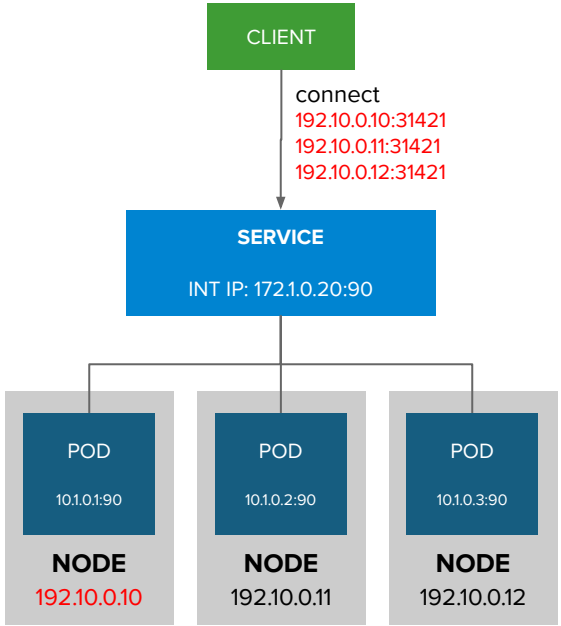
Alternative methods for ingress

Different ways that traffic can enter the cluster without the router



Entering the cluster on a random port with service nodeports

- NodePort binds a service to a unique port on all the nodes
- Traffic received on any node redirects to a node with the running service
- Ports in 30K-60K range which usually differs from the service
- Firewall rules must allow traffic to all nodes on the specific port



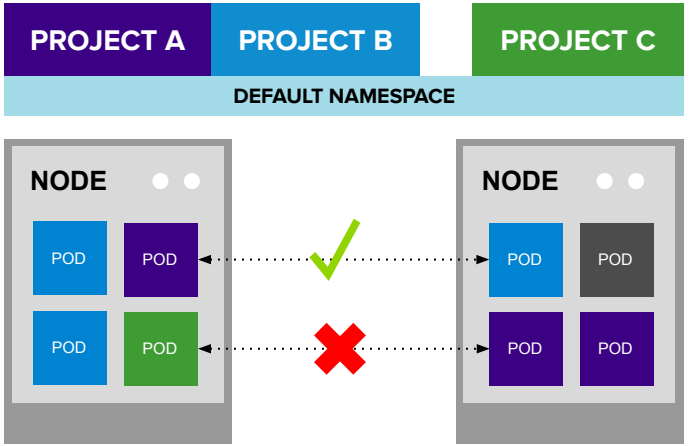
OpenShift SDN “flavors”

OPEN NETWORK **(Default)**

- All pods can communicate with each other across projects

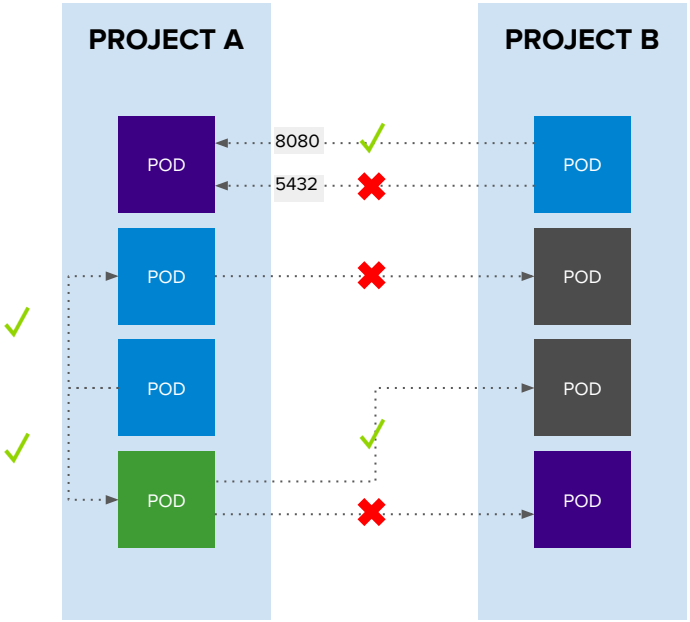
MULTI-TENANT NETWORK

- Project-level network isolation
- Multicast support
- Egress network policies



Multi-Tenant Network

NetworkPolicy



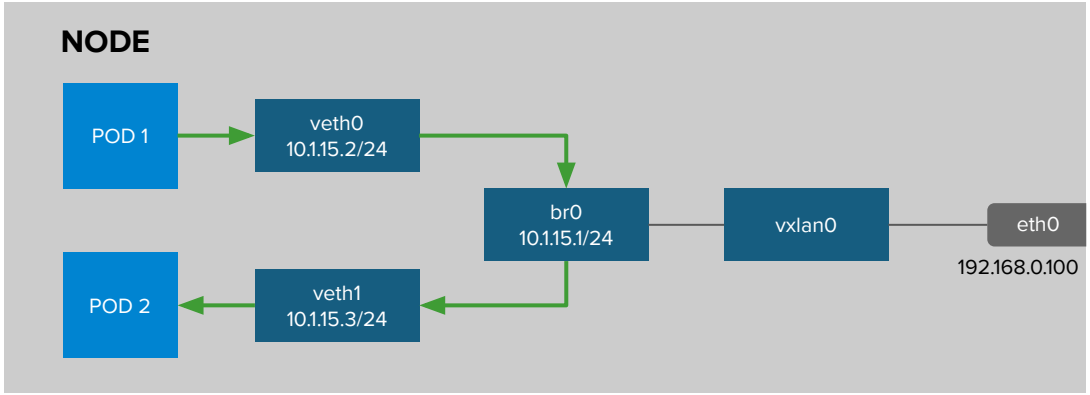
Example Policies

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

```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```

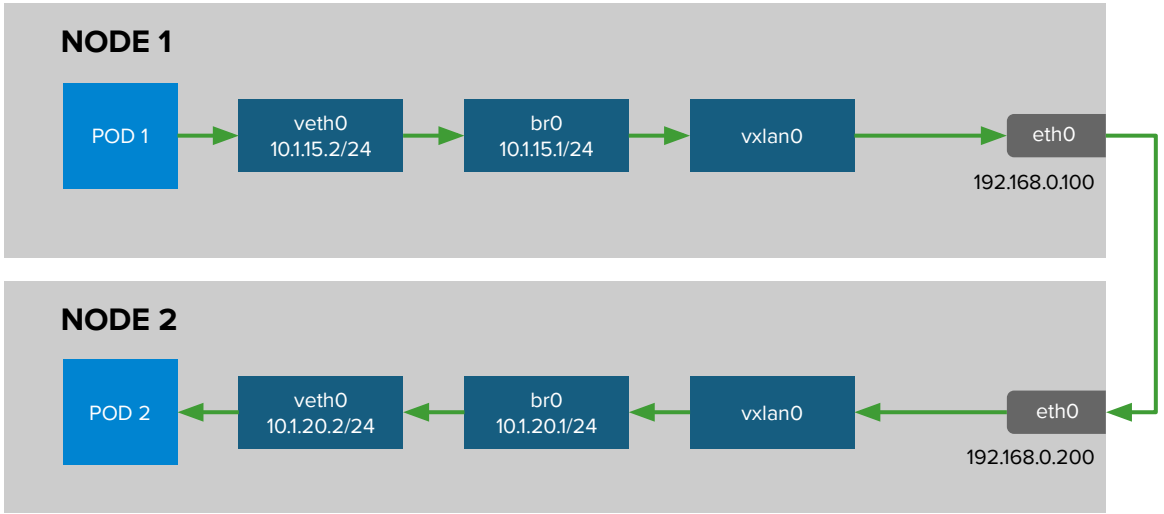
OpenShift SDN packet flows

container-container on same host



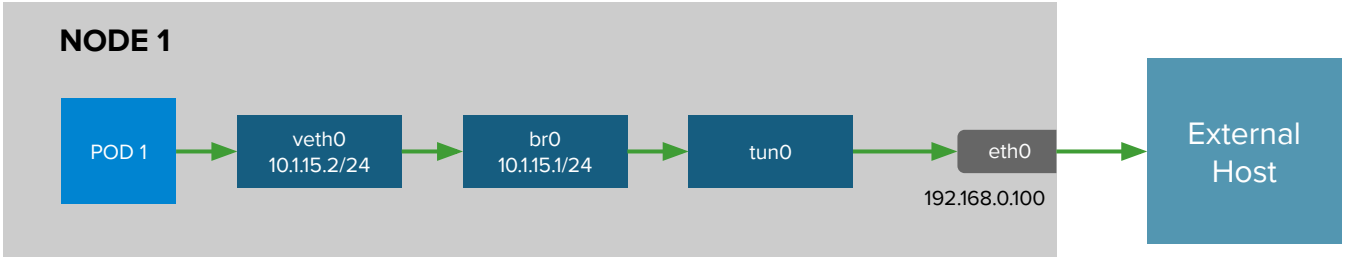
OpenShift SDN packet flows

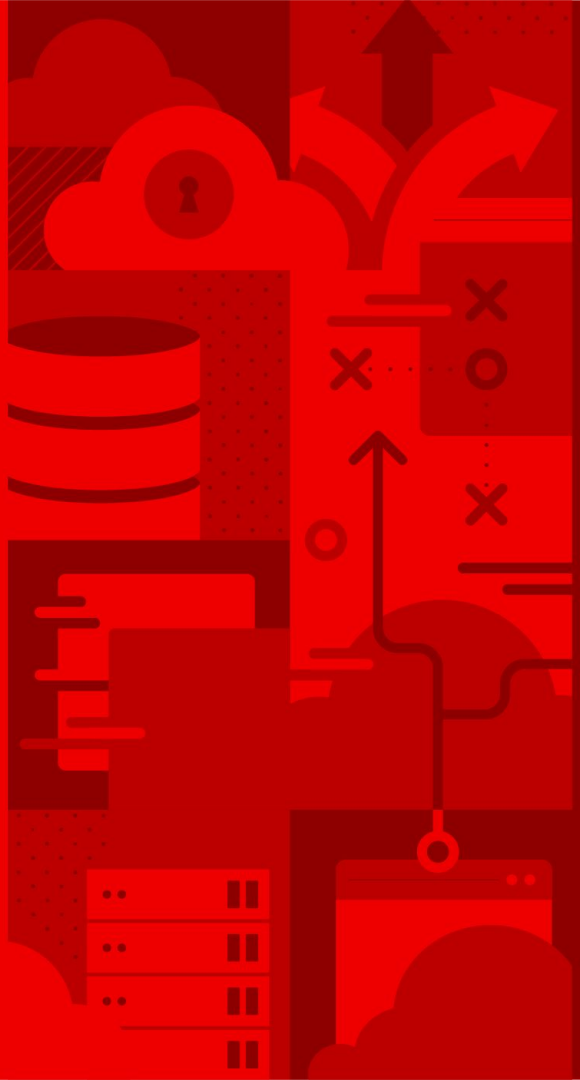
container-container across hosts



OpenShift SDN packet flows

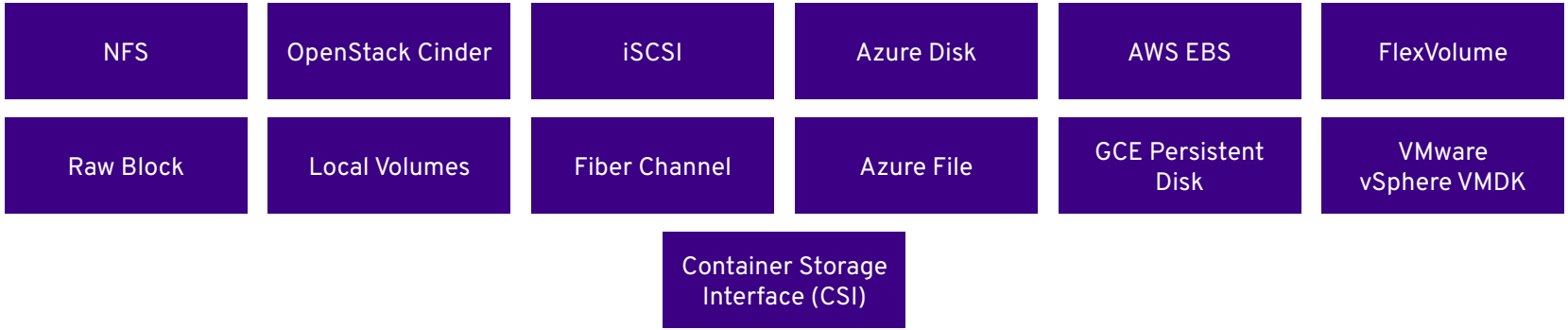
container leaving the host



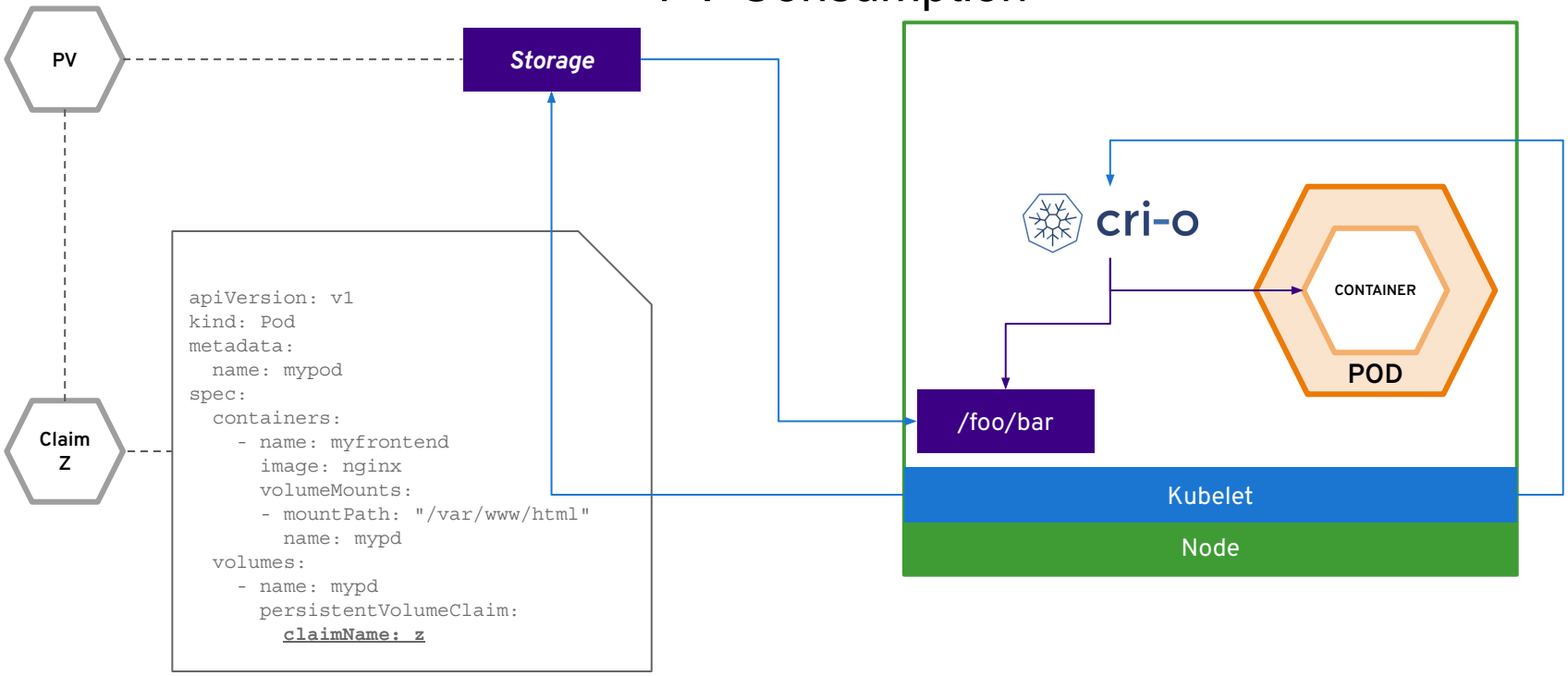


Persistent Storage

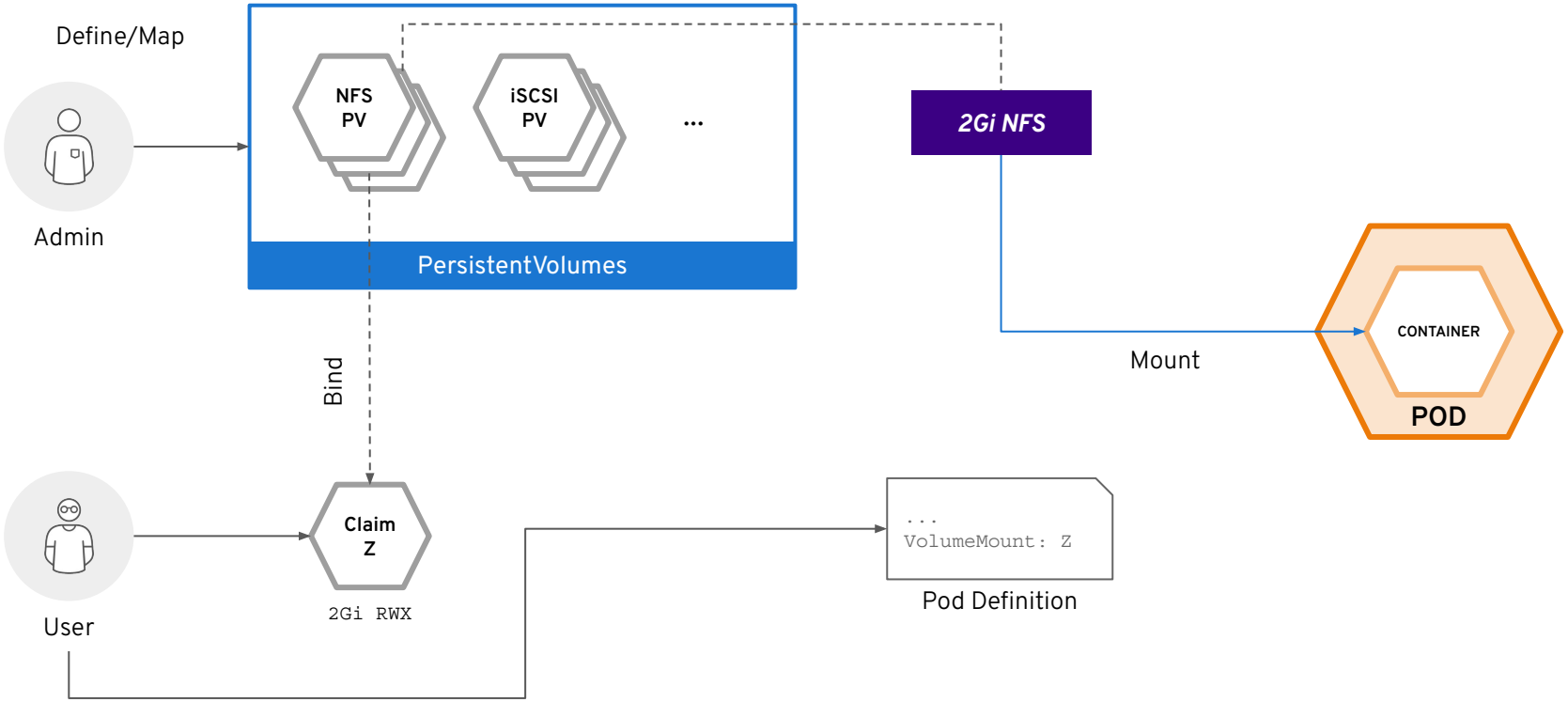
A broad spectrum of static and dynamic storage endpoints



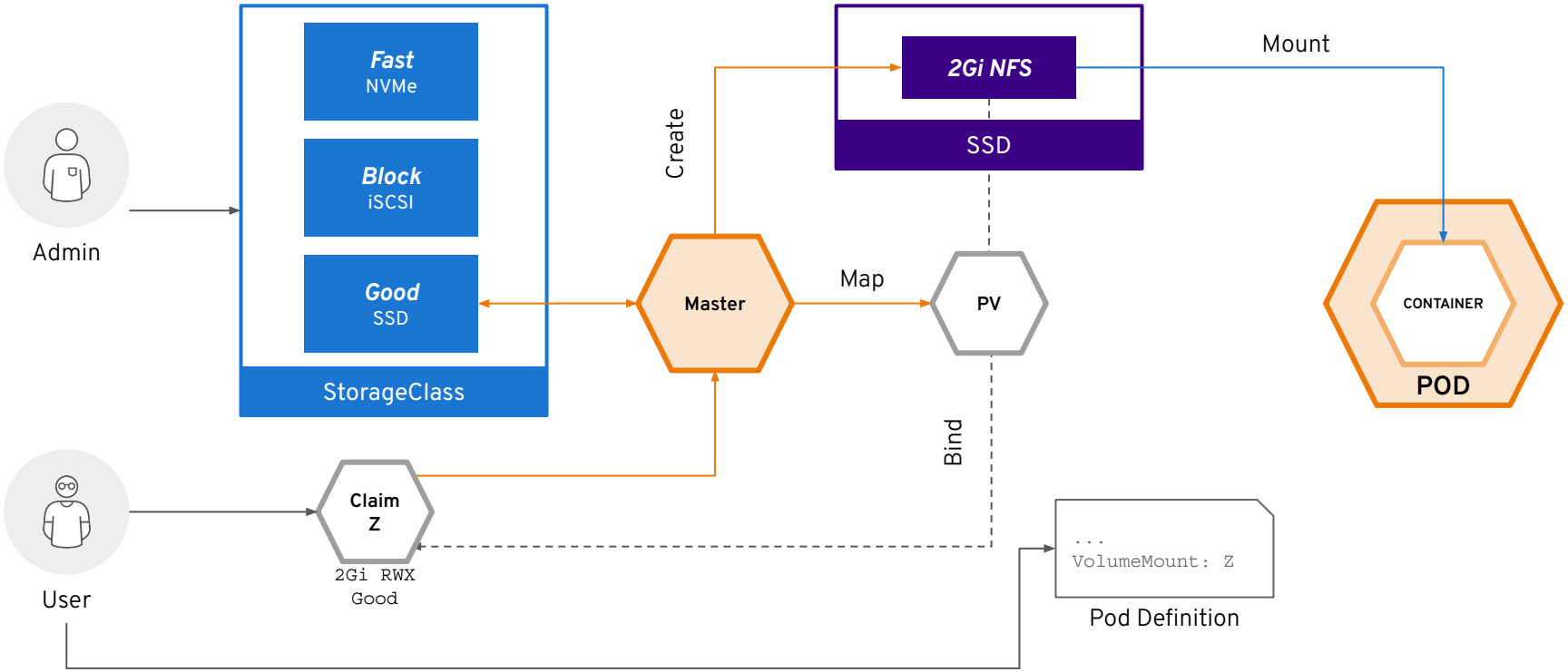
PV Consumption

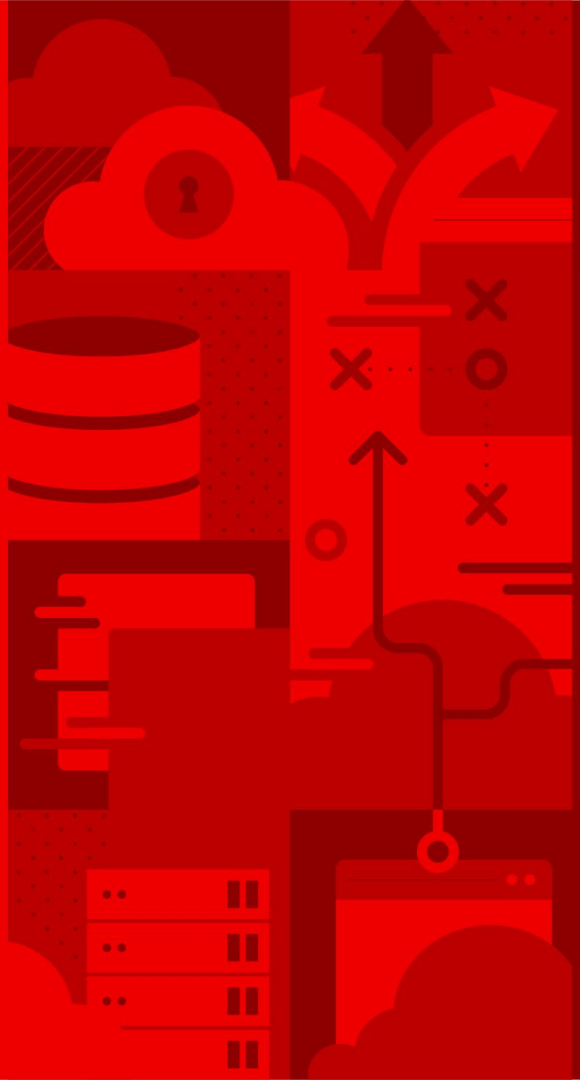


Static Storage Provisioning



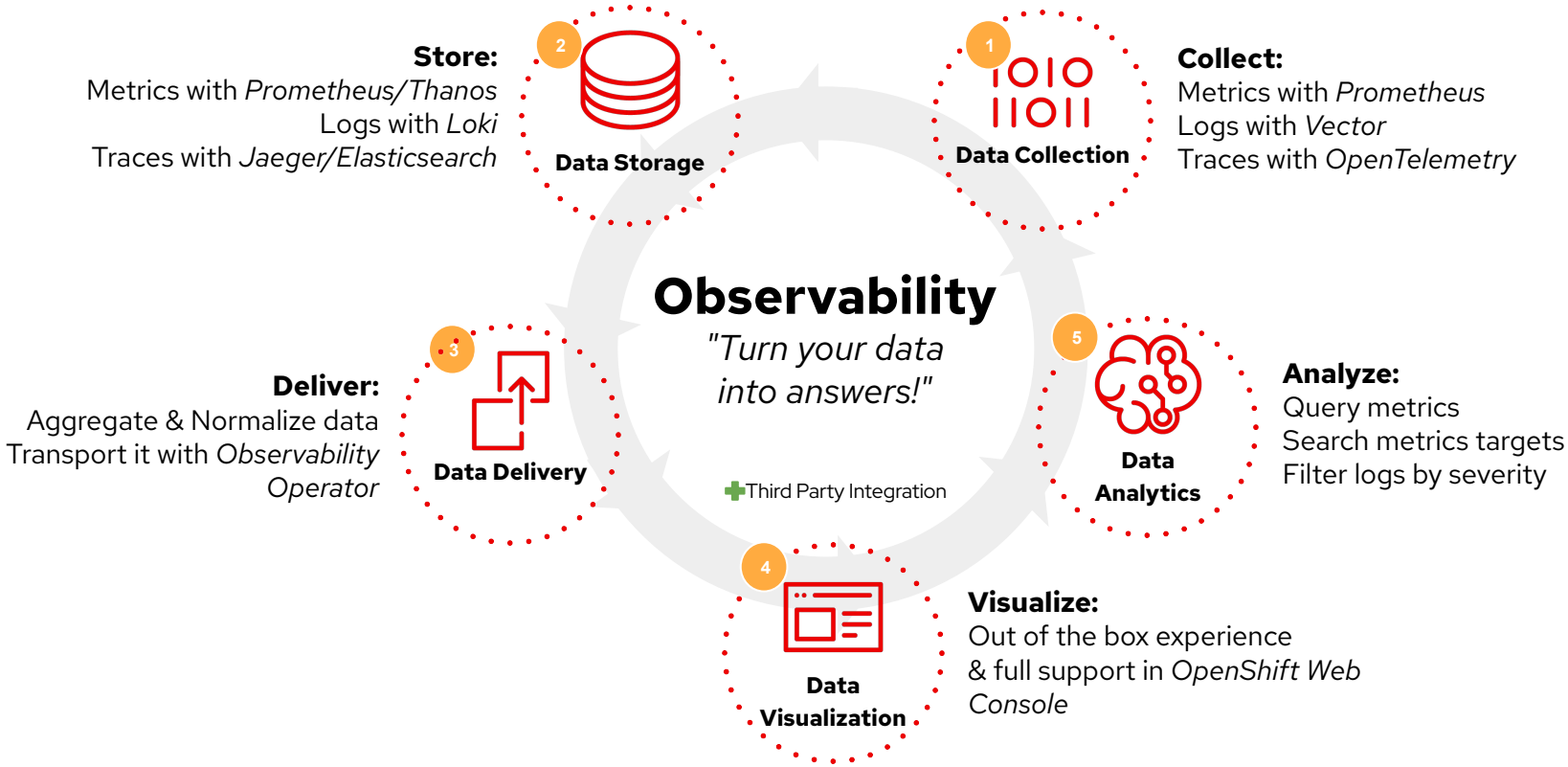
Dynamic Storage Provisioning





Observability

OpenShift Observability: Five Pillars



Store:
Metrics with *Prometheus/Thanos*
Logs with *Loki*
Traces with *Jaeger/Elasticsearch*

Collect:
Metrics with *Prometheus*
Logs with *Vector*
Traces with *OpenTelemetry*

Deliver:
Aggregate & Normalize data
Transport it with *Observability Operator*

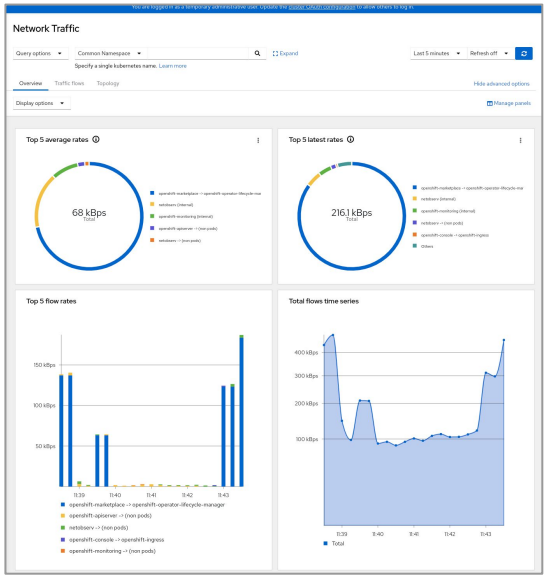
Analyze:
Query metrics
Search metrics targets
Filter logs by severity

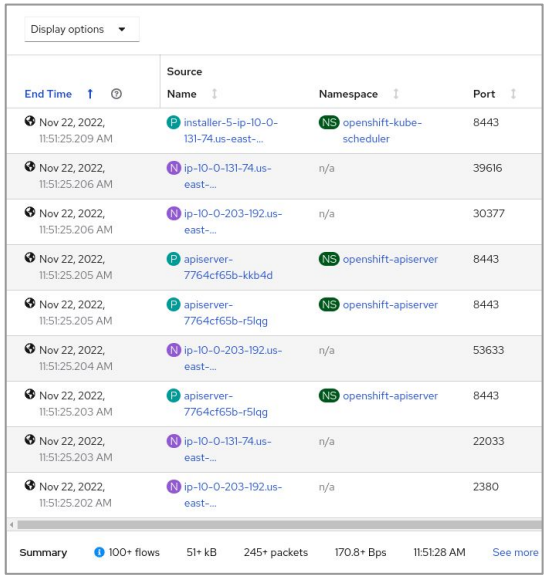
Visualize:
Out of the box experience
& full support in *OpenShift Web Console*

Network Observability

Network Observability GAs at 4.12 for all supported versions of OpenShift at 4.10 or newer

- Integrated with the larger Observability ecosystem, this optional Operator focuses on networking information for a single cluster
- Uses an **eBPF-based** agent on cluster nodes to collect metrics
- Provides observable network traffic metrics, flows, topology and tracing





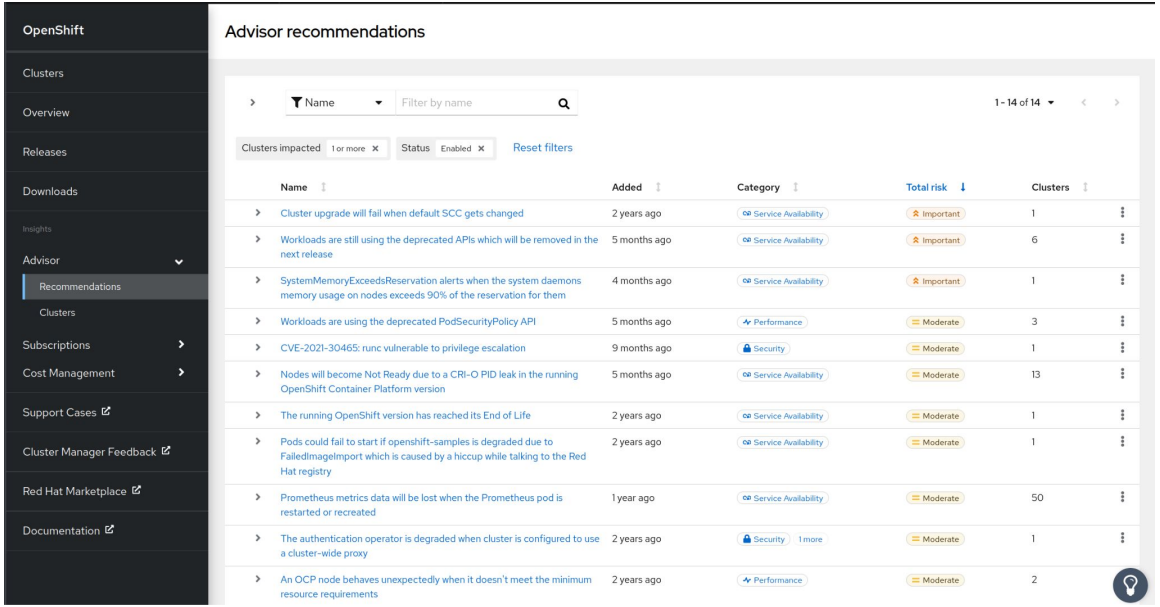
PM: Marc Curry, Deepthi Dharwar

Red Hat

Insights Advisor for OpenShift

- **Free service leveraging Red Hat experience with supporting and operating OpenShift**
- New recommendations based on analysis of Kubernetes YAML files (available for managed OpenShift only ATM)
- Alerts in OpenShift WebConsole for most critical recommendations
- **New recommendations** focused on storage performance, etcd issues etc.
- Improved internal integrations for more stable upgrades

https://console.redhat.com/openshift/advisor
https://console.redhat.com/settings/notifications/openshift

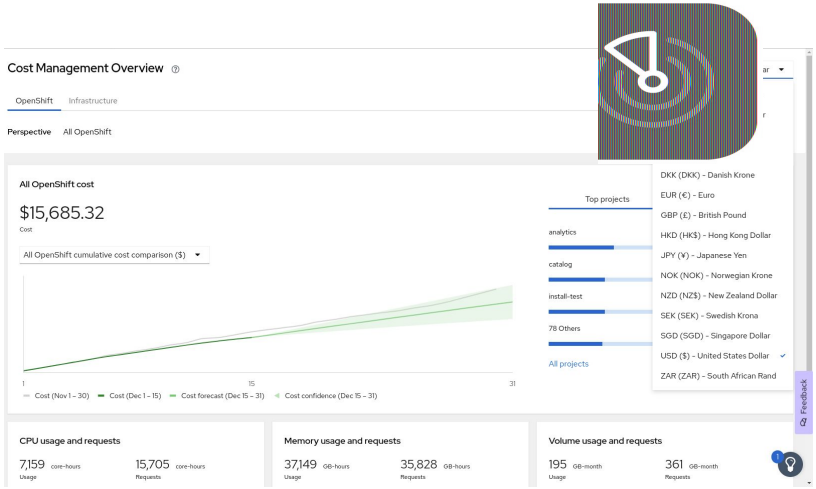


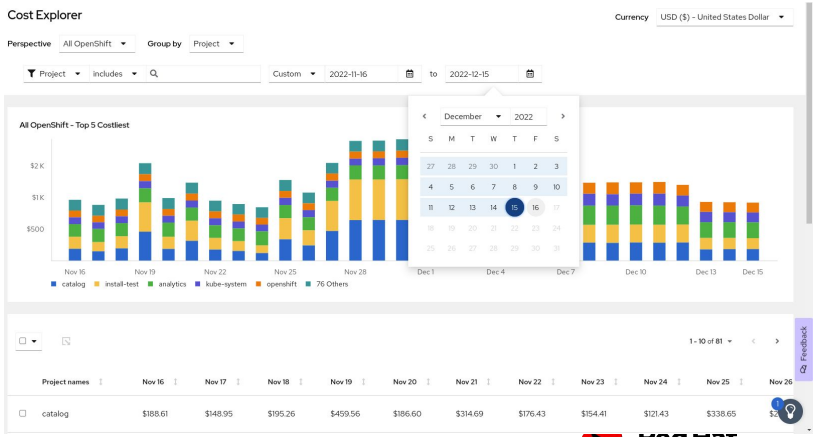
PM: Tomas Dosek

Red Hat

Insights Cost Management

- **Free service to monitor per-project and per-cluster spending**
- Currency support
- Marketplace services reported including ROSA, ARO, RHEL, ODF, 3rd parties, etc
- ROSA and ARO costs distributed to projects
- Costs now distributed according to the same resource consumption criteria in every view
- Cost of unallocated capacity accounted (both workers and platform)
- Filtering gained exclude capabilities (“negative filtering”)
- AWS costs default to amortized when Savings Plans are involved
- Previous month report and custom date picker in Cost Explorer
- Performance improvements for OCP clusters running on GCP
- Integration with console.redhat.com notifications





https://console.redhat.com/openshift/cost-management
https://console.redhat.com/settings/applications/cost-management
https://console.redhat.com/settings/notifications/openshift

PM: Pau Garcia Quiles

Red Hat

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat