IBM® Cloud Paks™ & Red Hat® OpenShift® Container Platform on IBM Z® & LinuxONE™

Advanced Technology Group
Technical Sales Support – Americas

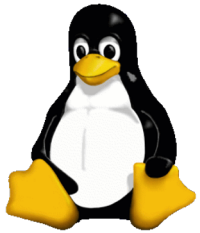
Workshop ID LXCS1 / ICPOZ1
IBM Advanced Technology Group (ATG) Wildfire Workshop Series

http://www.ibm.com/support/techdocs

3/9/21 2:10:26 PM

Wildfire
Technical Hands-On Workshops

Advanced Technology Group
Technical Sales Support – Americas



Special Notices and Trademarks

Special Notices

This presentation reflects the IBM Advanced Technical Skills organizations' understanding of the technical topic. It was produced and reviewed by the members of the IBM Advanced Technical Skills organization. This document is presented "As-Is" and IBM does not assume responsibility for the statements expressed herein. It reflects the opinions of the IBM Advanced Technical Skills organization. These opinions are based on the author's experiences. If you have questions about the contents of this document, please contact the author at linuxats@us.ibm.com

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

Any and all customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. References in this document to IBM products or services do not imply that IBM intends to make them available in every country. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Any proposed use of claims in this presentation outside of the United States must be reviewed by local IBM country counsel prior to such use.

The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.
Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk

Trademarks

The following are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

IBM, the IBM logo, DB2, Redbooks, Tivoli Enterprise Console, WebSphere, z/OS, System z, z/VM.
A full list of U.S. trademarks owned by IBM may be found at http://www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, Internet Explorer, and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.

Intel and Pentium are registered trademarks and MMX, Pentium II Xeon and Pentium III Xeon are trademarks of Intel Corporation in the United States and/or other countries.

Other company, product and service names may be trademarks or service marks of others.

IBM Cloud Paks & Red Hat OpenShift Container Platform on IBM Z & LinuxONE

Wildfire Technical Hands-On Workshops

Advanced Technology Group
Technical Sales Support – Americas

All labs and presentations can be found at:
`http://ibm.biz/wildfire-cloudpaks-ocp`

Please wait to access any lab systems until all presentations have concluded.

Schedule for the day

Start 11:00 AM Eastern

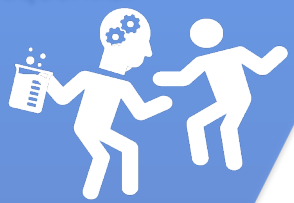
Presentation
Overview of OpenShift
Overview of IBM Cloud Paks

Presentation
- History of OpenShift

On break until 12:00 ET

Presentation
- OpenShift on Z technical deep dive

Hands-on Labs
- Self-paced
- Non-sequential



End 5:00 PM Eastern

Multitenancy

The main prerequisite: Thoughtful planning

Multitenancy in a nutshell

- Software architecture where a single software instance can serve multiple, distinct user groups.
- Software-as-a-service (SaaS) offerings are an example of multitenant architecture.
- In cloud computing, multitenancy can also refer to shared hosting, in which server resources are divided among different customers.
- Multitenancy is the opposite of single tenancy, when a software instance or computer system has one end-user or group of users.

When referring to a container orchestration platform such as Kubernetes, the term multitenancy usually means *a single cluster that serves multiple projects*. The cluster is configured so each project runs with some degree of isolation from the others.

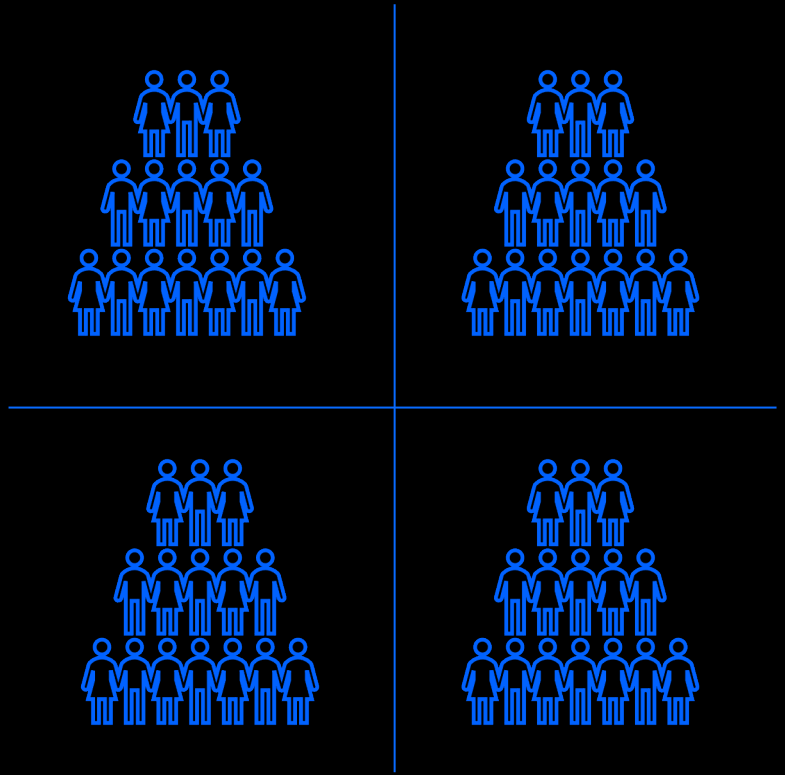
Multitenancy and Kubernetes

- When using Kubernetes for container orchestration, it's possible to set up multitenant environments using a single Kubernetes cluster.
- Separate each tenant into their own namespace
- Create policies that enforce tenant isolation.
- There are benefits and risks associated with this which need to be considered as part of the decision-making process.

Multitenant security is essential for enterprise-scale use of Kubernetes. Multitenancy allows you to have different teams use the same cluster while preventing unauthorized access to each other's environments.

Multitenancy and Red Hat OpenShift Container Platform version 4

Multitenancy and Red Hat OpenShift Container Platform



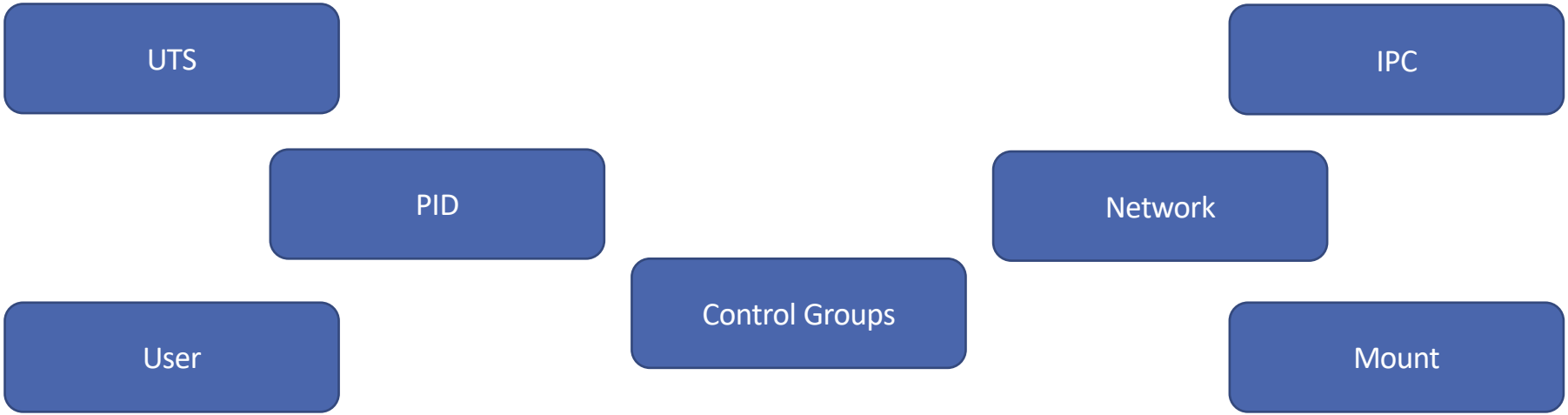
Red Hat OpenShift supports multitenancy through a combination of:

- Linux kernel namespaces
- SELinux
- Role-based Access Control (RBAC)
- Kubernetes namespaces
- Network policies.

Linux kernel Namespaces must not be conflated with Kubernetes Namespaces.

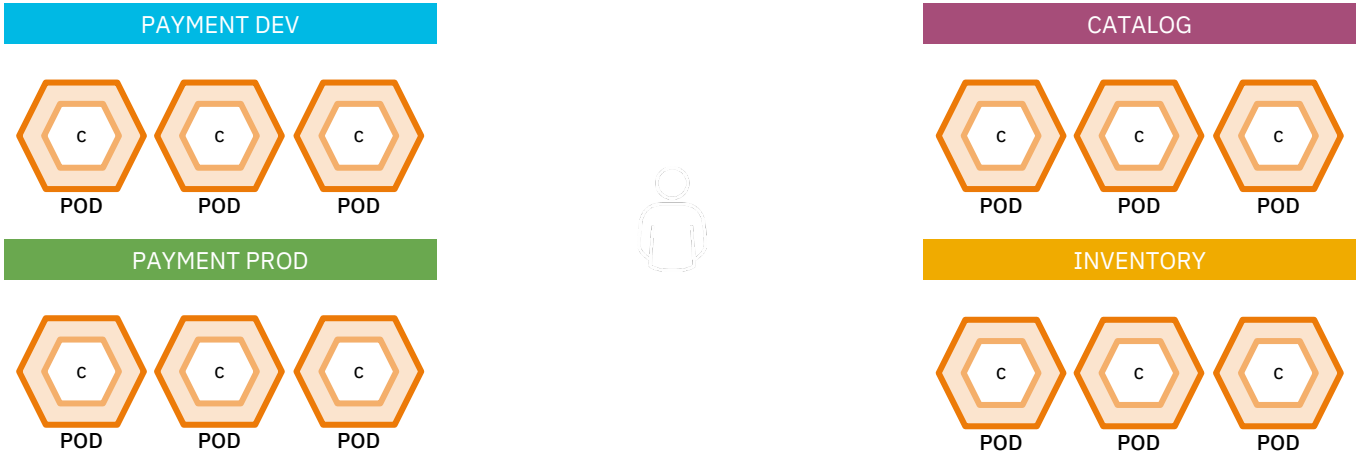
They are entirely different.

Linux kernel Namespaces are a set of seven abstraction wrappers for global system resources and in-scope processes.



https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/system_design_guide/what-namespaces-are_setting-limits-for-applications

Kubernetes Namespaces collate resources and isolate apps across environments, teams, groups and departments.

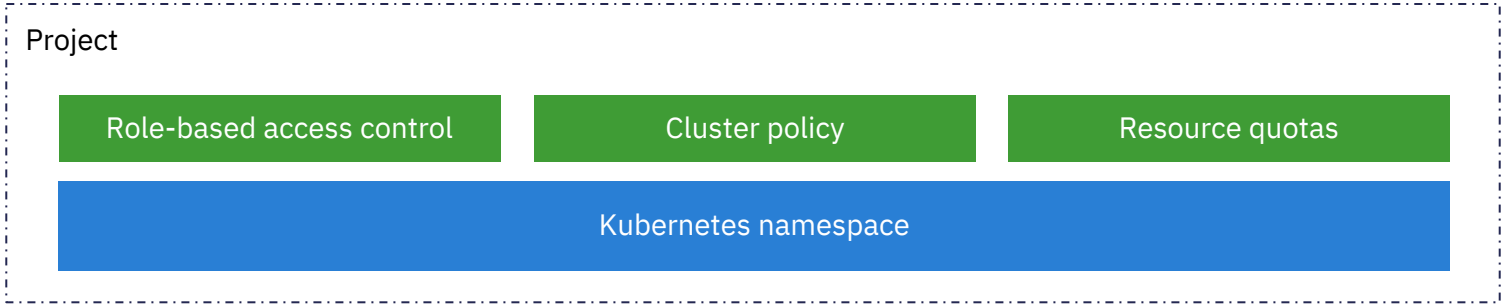


Namespaces were designed as a construct for cluster resource management, not security.

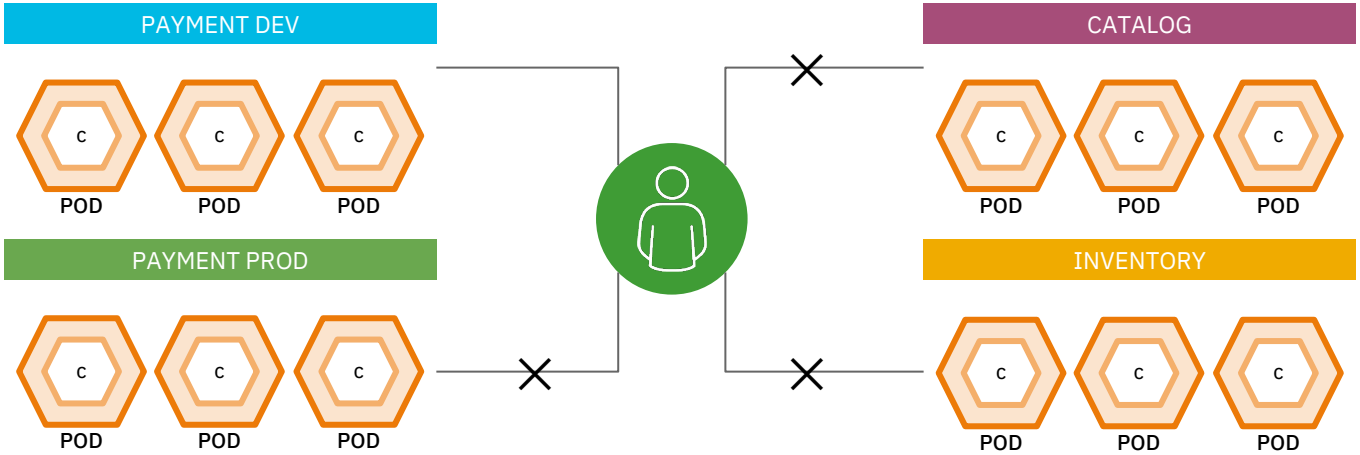
Do not rely on namespaces as a security feature outside of cluster internals within trusted domains.

Do not rely on namespaces to deny a cluster user access to resources in other namespaces.

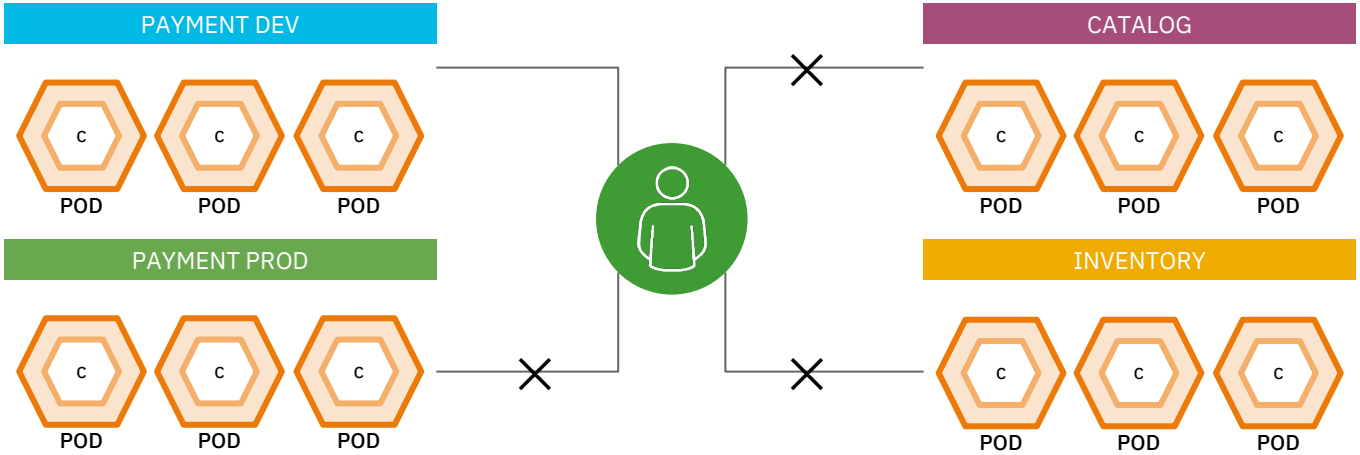
A namespace plus the RBAC layer and some other enhancements is a project



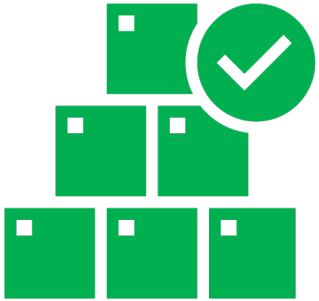
Projects isolate apps across environments, teams, groups and departments in a secure way.

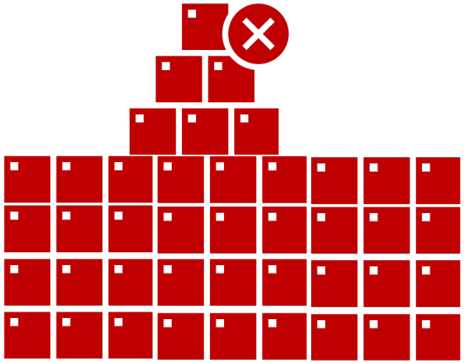


IBM Z and LinuxONE are the only platform where SECURE multi-tenant usage is possible



Embrace projects and use them on a sensible scale. Balance their performance enhancement against operational complexity.





Deep Dive

Virtualization considerations

KVM

Be mindful of the actual reality for slanted phrasing such as “specialized skills requirements”
Linux in an LPAR:

.... fun to install ....

utilization

waste
DR recovery considerations
Density delta

Hypervisors and Virtualization

PR/SM-LPARs IBM DPM

- Virtualization is built into the DNA of IBM Z
- PR/SM™ manages and virtualizes all the installed and enabled system resources as a single large SMP system
- Full sharing/partitioning of the installed resources with the highest levels of efficiency and utilization
- Scale up or scale out on demand with support for up to 85 partitions
- IBM Dynamic Partition Manager simplifies provisioning and management experience
- Workload isolation with design for highest EAL5+ security certification
- New dynamic optimization and scalability enhancements

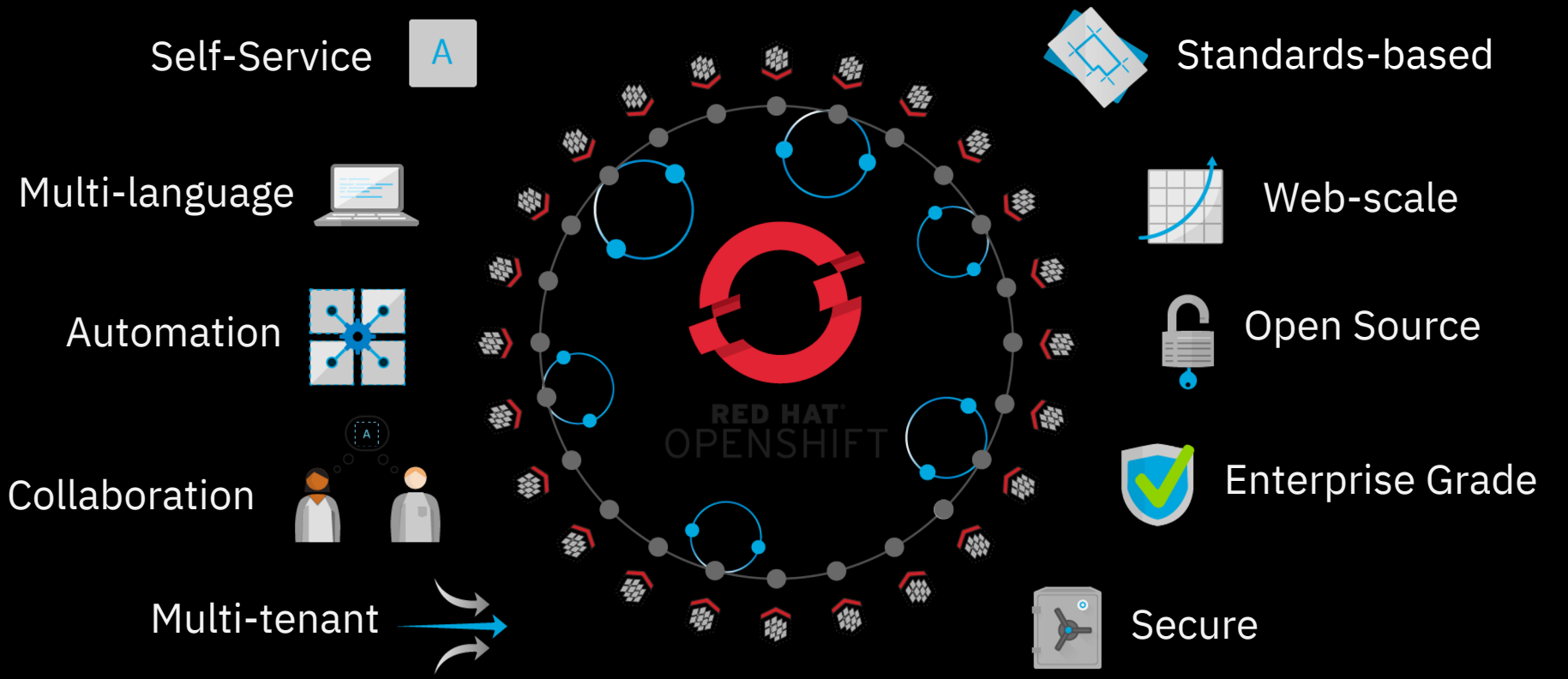
z/VM v7.x

- Enables extreme scalability, security and efficiency – Support for 2TB of memory, Dynamic Memory Downgrade,, 80 logical processors, and improved z/VM paging enabling workload consolidation, growth in memory-intensive applications, and superior levels of elasticity.
- Operational improvements by providing guest large page support and Guest TX (Transactional eXecution) support
- Z15 Support – Crypto Express7S, crypto enhancements, On-chip compression enabled for guest exploitation; Also supported by z/VM 6.4.
- IBM System Recover Boost – Boost general purpose processor speed during workload bring-up, quiesce, and system shutdown, with particular focus for z/VSE and z/TPF Guest environment
- z/VM 7.1 – Delivering a release cadence that improves z/VM's Continuous Delivery (CD) model. Includes Single System Image (SSI) support in the base product providing improved availability of z/VM systems by allowing clients to schedule outages without disrupting business critical applications

KVM on IBM Z

- Pass-through of Crypto Express adapter domains in KVM guests
- On-chip compression enabled for 'pervasive usage' with Linux guests
- Support of 16TB of host memory
- Improved performance via new vector instructions for different workloads
- Secure and protected business data with exploitation of elliptic-curve crypto (ECC)

Functional overview


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

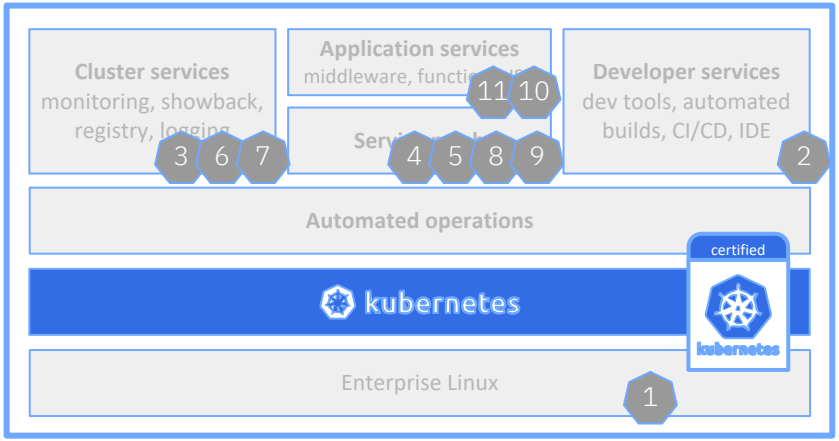
IBM | Red Hat

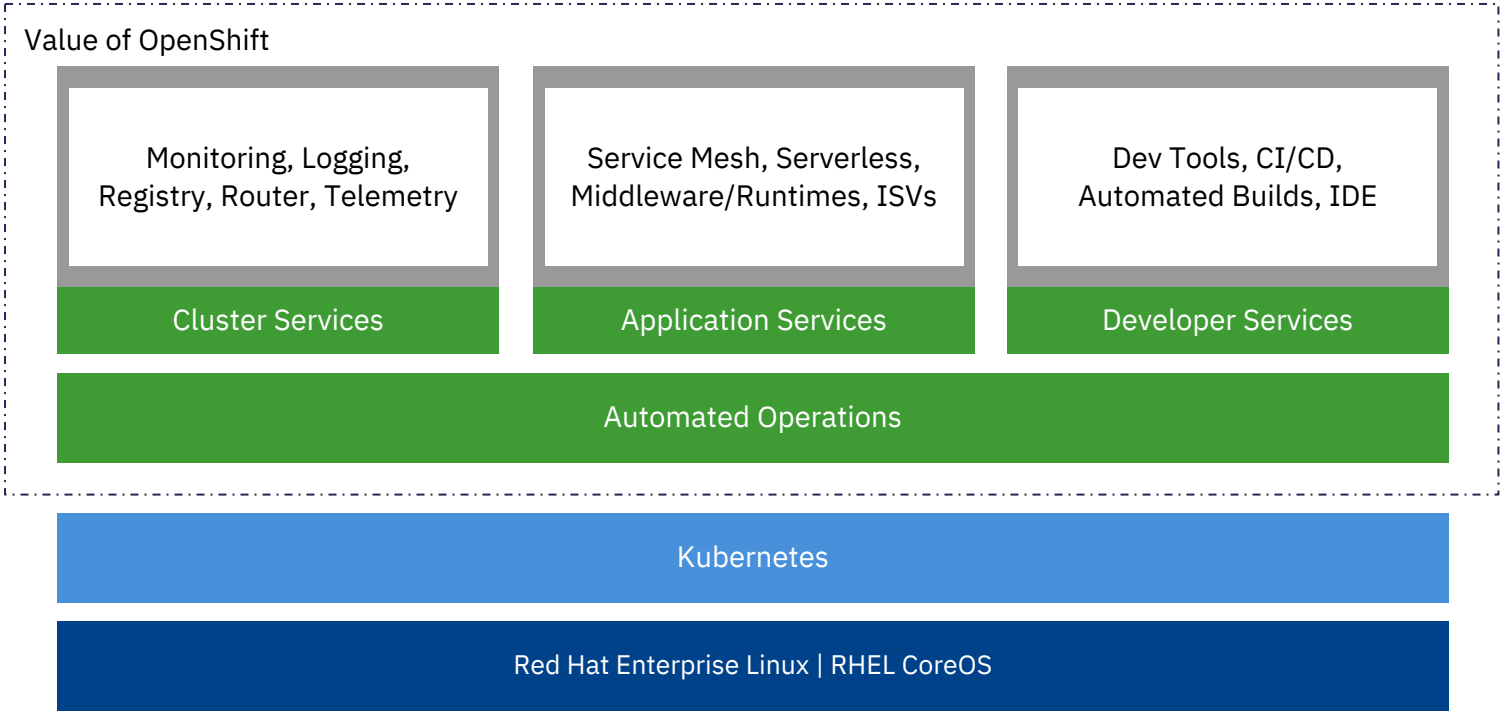
kubernetes

Lacks many essential components

1. Operating system
2. Container runtime (CRI-O, Containerd, Docker, etc).
3. Image registry
4. Software-defined networking
5. Load-balancer and routing
6. Log management
7. Container metrics and monitoring
8. DNS
9. Load balancing
10. Ingress
11. RBAC

The customer (or third-party) must configure, integrate, operate and support additional components to be fully operational.



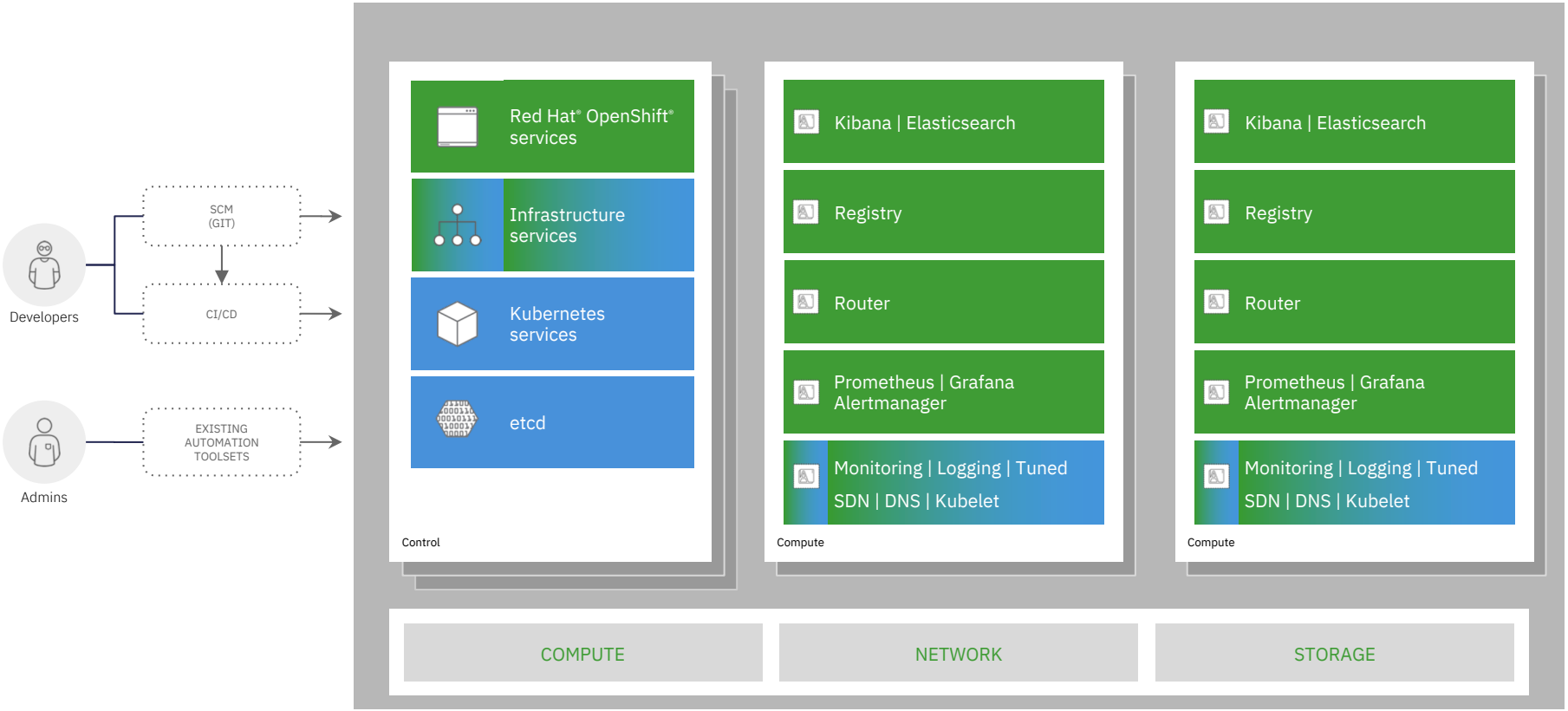


Best IT Ops Experience

CaaS ⟷ PaaS ⟷ FaaS

Best Developer Experience

A best-of-breed concept



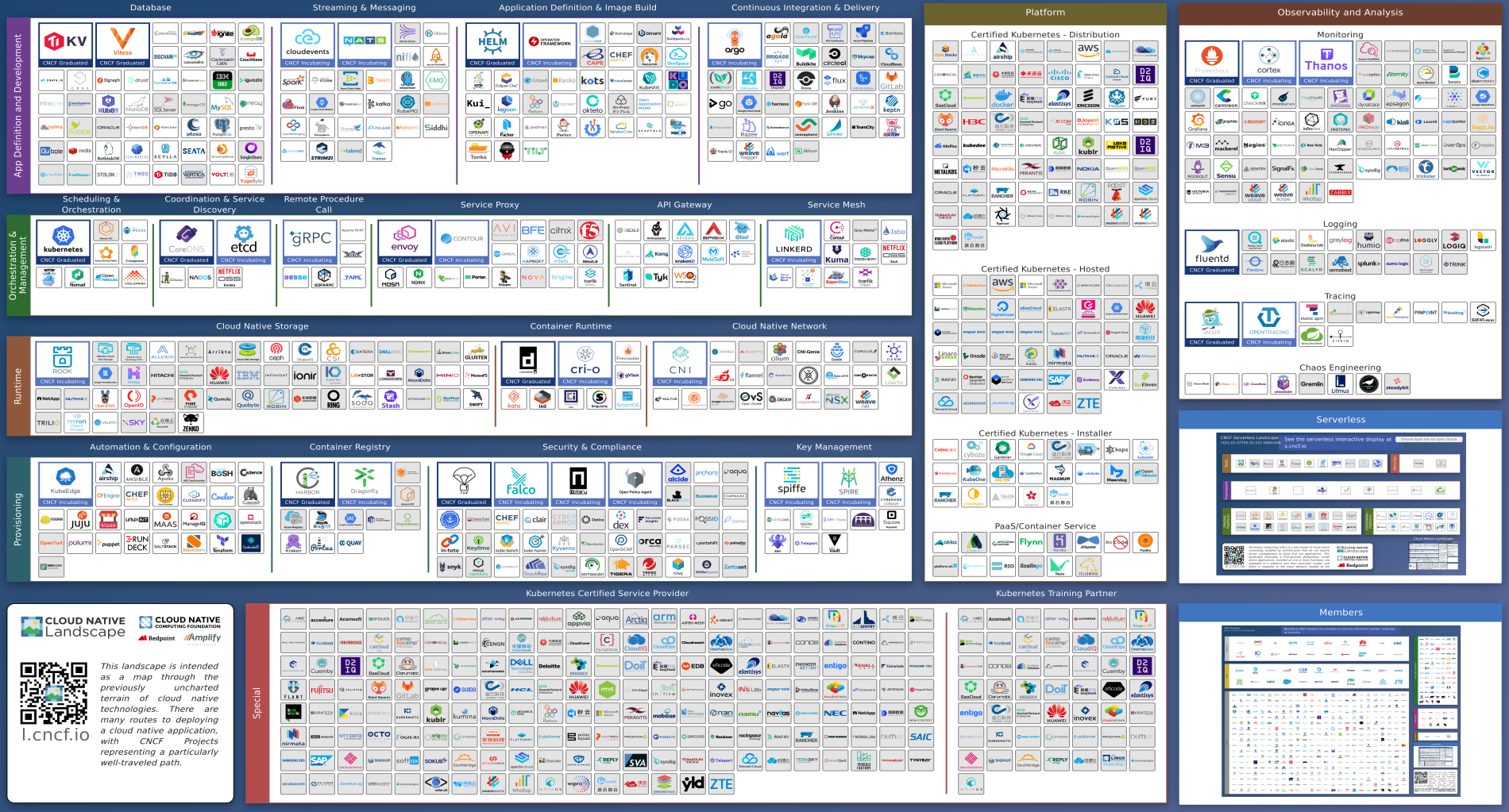
Architectural overview

CNCF Cloud Native Landscape

2021-01-07T00:35:31Z 0480c506

Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io

Greyed logos are not open source



CLOUD NATIVE Landscape

CLOUD NATIVE COMPUTING FOUNDATION

Redpoint Amplify Partners

l.cncf.io

This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path.

CLOUD NATIVE COMPUTING FOUNDATION

CLOUD NATIVE TRAIL MAP

The Cloud Native Landscape *l.cncf.io* has a large number of options. This Cloud Native Trail Map is a recommended process for leveraging open source, cloud native technologies. At each step, you can choose a vendor-supported offering or do it yourself, and everything after step #3 is optional based on your circumstances.

HELP ALONG THE WAY

A. Training and Certification

Consider training offerings from CNCF and then take the exam to become a Certified Kubernetes Administrator or a Certified Kubernetes Application Developer

cncf.io/training

B. Consulting Help

If you want assistance with Kubernetes and the surrounding ecosystem, consider leveraging a Kubernetes Certified Service Provider

cncf.io/kcsp

C. Join CNCF's End User Community

For companies that don't offer cloud native services externally

cncf.io/enduser

WHAT IS CLOUD NATIVE?

Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach.

These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.

The Cloud Native Computing Foundation seeks to drive adoption of this paradigm by fostering and sustaining an ecosystem of open source, vendor-neutral projects. We democratize state-of-the-art patterns to make these innovations accessible for everyone.

l.cncf.io

v20200501

1. CONTAINERIZATION

- Commonly done with Docker containers
- Any size application and dependencies (even PDP-11 code running on an emulator) can be containerized
- Over time, you should aspire towards splitting suitable applications and writing future functionality as microservices

2. CI/CD

- Setup Continuous Integration/Continuous Delivery (CI/CD) so that changes to your source code automatically result in a new container being built, tested, and deployed to staging and eventually, perhaps, to production
- Setup automated rollouts, roll backs and testing
- Argo is a set of Kubernetes-native tools for deploying and running jobs, applications, workflows, and events using GitOps paradigms such as continuous and progressive delivery and MLops

argo — CNCF Incubating

3. ORCHESTRATION & APPLICATION DEFINITION

- Kubernetes is the market-leading orchestration solution
- You should select a Certified Kubernetes Distribution, Hosted Platform, or Installer: cncf.io/ck
- Helm Charts help you define, install, and upgrade even the most complex Kubernetes application

kubernetes — CNCF Graduated

HELM — CNCF Graduated

4. OBSERVABILITY & ANALYSIS

- Pick solutions for monitoring, logging and tracing
- Consider CNCF projects Prometheus for monitoring, Fluentd for logging and Jaeger for Tracing
- For tracing, look for an OpenTracing-compatible implementation like Jaeger

Prometheus — CNCF Graduated

fluentd — CNCF Graduated

JAEGER — CNCF Graduated

OPENTRACING — CNCF Incubating

5. SERVICE PROXY, DISCOVERY, & MESH

- CoreDNS is a fast and flexible tool that is useful for service discovery
- Envoy and Linkerd each enable service mesh architectures
- They offer health checking, routing, and load balancing

envoy — CNCF Graduated

CoreDNS — CNCF Graduated

LINKERD — CNCF Incubating

6. NETWORKING, POLICY, & SECURITY

To enable more flexible networking, use a CNI-compliant network project like Calico, Flannel, or Weave Net. Open Policy Agent (OPA) is a general-purpose policy engine with uses ranging from authorization and admission control to data filtering. Falco is an anomaly detection engine for cloud native.

CNI — CNCF Incubating

Open Policy Agent — CNCF Incubating

Falco — CNCF Incubating

7. DISTRIBUTED DATABASE & STORAGE

When you need more resiliency and scalability than you can get from a single database, Vitess is a good option for running MySQL at scale through sharding. Rook is a storage orchestrator that integrates a diverse set of storage solutions into Kubernetes. Serving as the "brain" of Kubernetes, etcd provides a reliable way to store data across a cluster of machines. TiKV is a high performant distributed transactional key-value store written in Rust.

Vitess — CNCF Graduated

ROOK — CNCF Incubating

etcd — CNCF Incubating

TiKV — CNCF Incubating

8. STREAMING & MESSAGING

When you need higher performance than JSON-REST, consider using gRPC or NATS. gRPC is a universal RPC framework. NATS is a multi-modal messaging system that includes request/reply, pub/sub and load balanced queues. CloudEvents is a specification for describing event data in common ways.

gRPC — CNCF Incubating

NATS — CNCF Incubating

cloudevents — CNCF Incubating

9. CONTAINER REGISTRY & RUNTIME

Harbor is a registry that stores, signs, and scans content. You can use alternative container runtimes. The most common, both of which are OCI-compliant, are containerd and CRI-O.

containerd — CNCF Graduated

HARBOR — CNCF Incubating

cri-o — CNCF Incubating

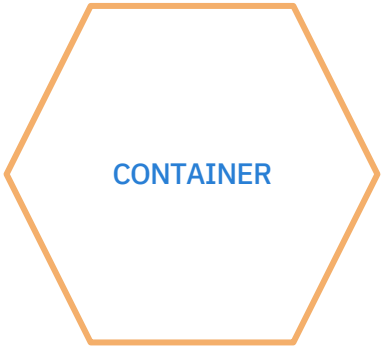
10. SOFTWARE DISTRIBUTION

If you need to do secure software distribution, evaluate Notary, an implementation of The Update Framework.

TUF — CNCF Graduated

Notary — CNCF Incubating

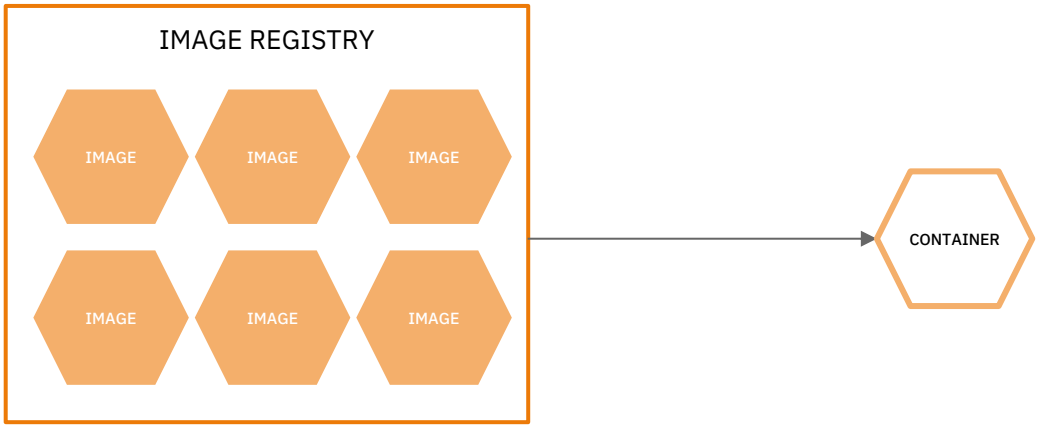
OpenShift and Kubernetes core concepts



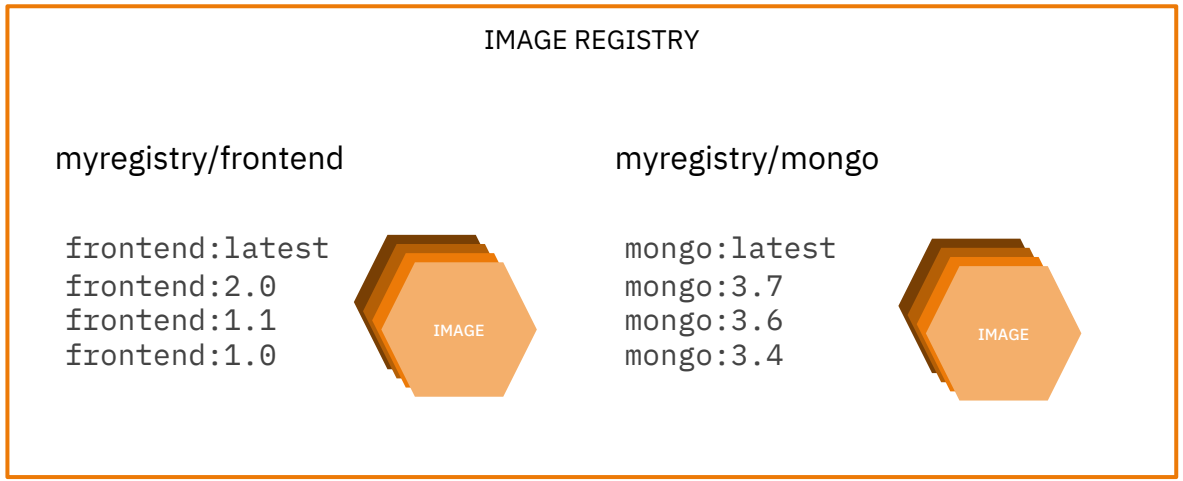
A container is the smallest compute unit

containers are created from container images

container images are stored in an image registry

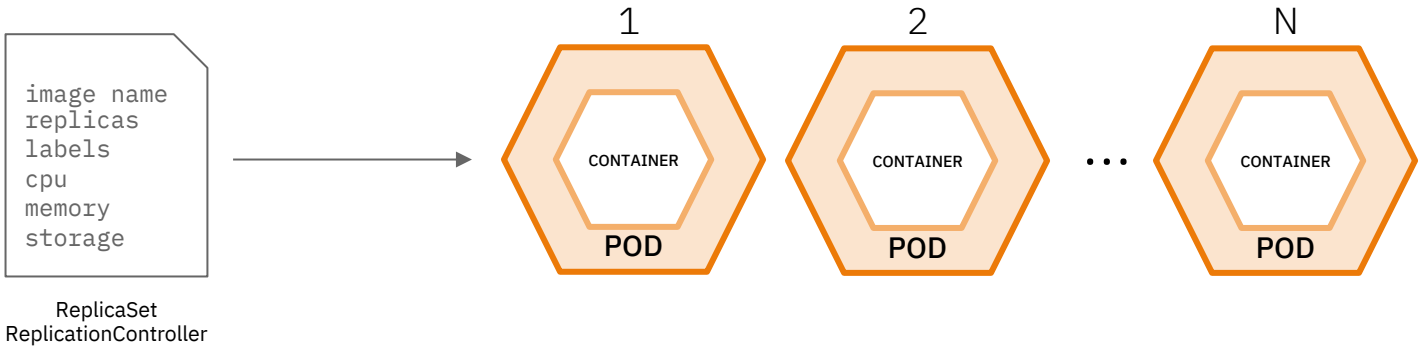


an image repository contains all versions of an image in the image registry

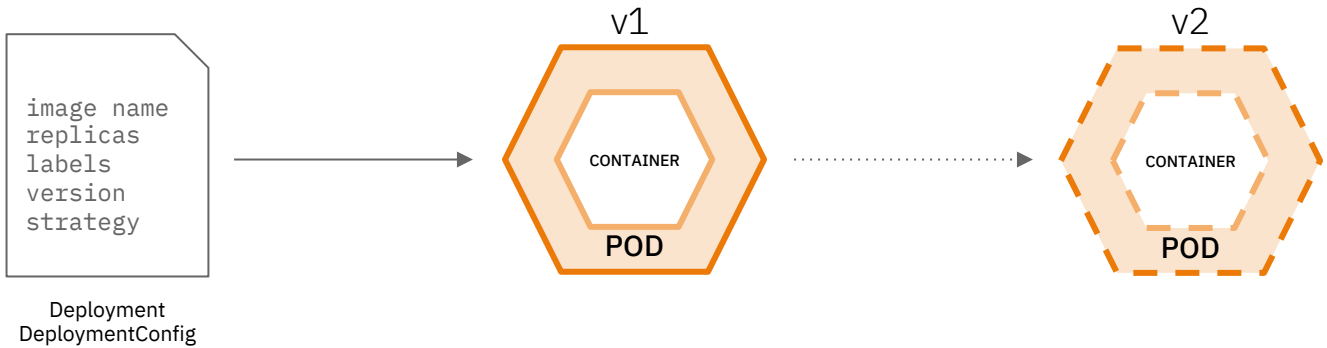


containers are wrapped in pods which are units of deployment and management

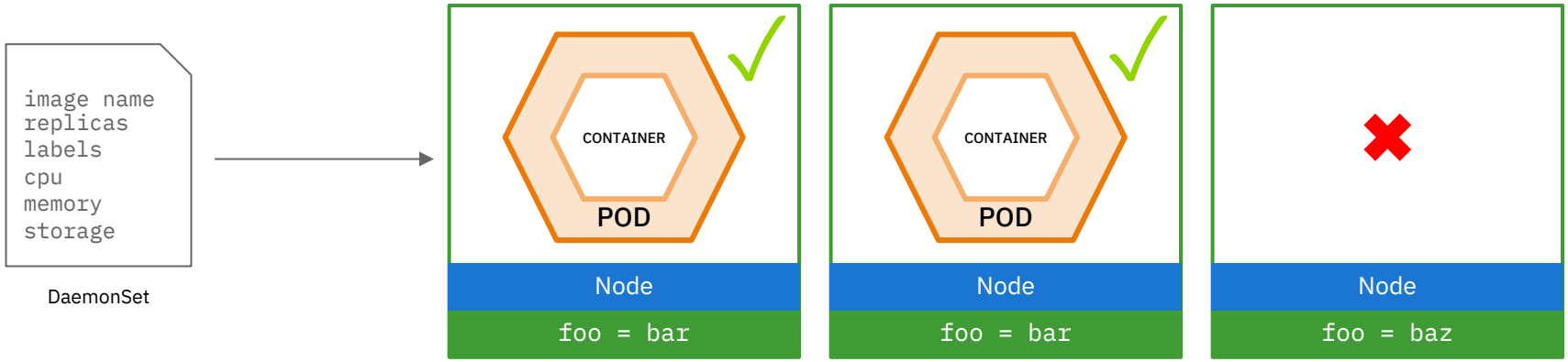
ReplicationControllers & ReplicaSets ensure a specified number of pods are running at any given time



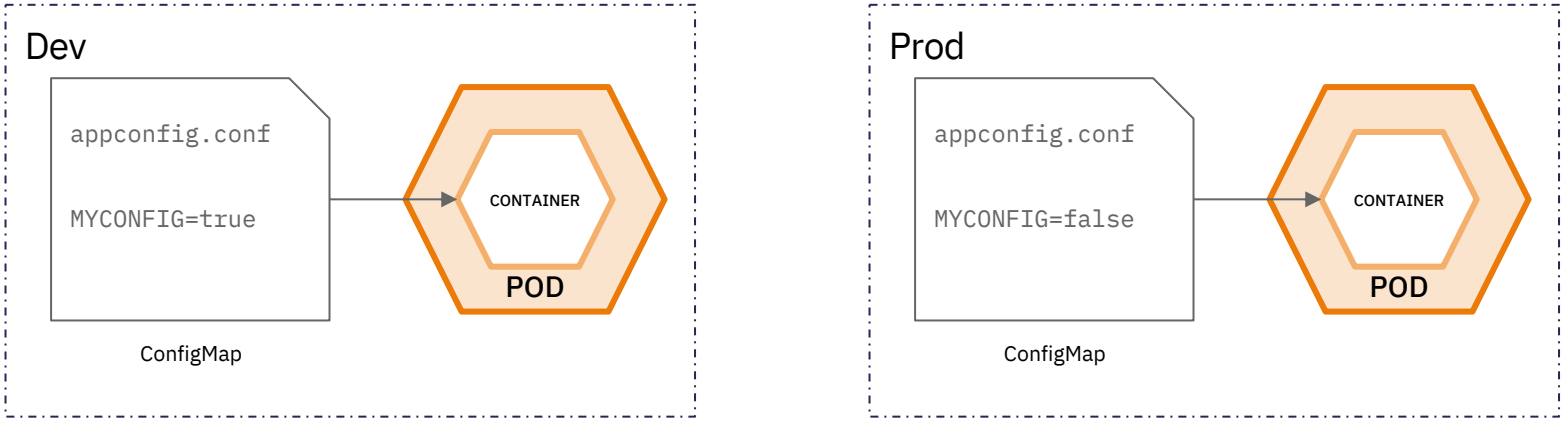
Deployments and DeploymentConfigurations define how to roll out new versions of Pods



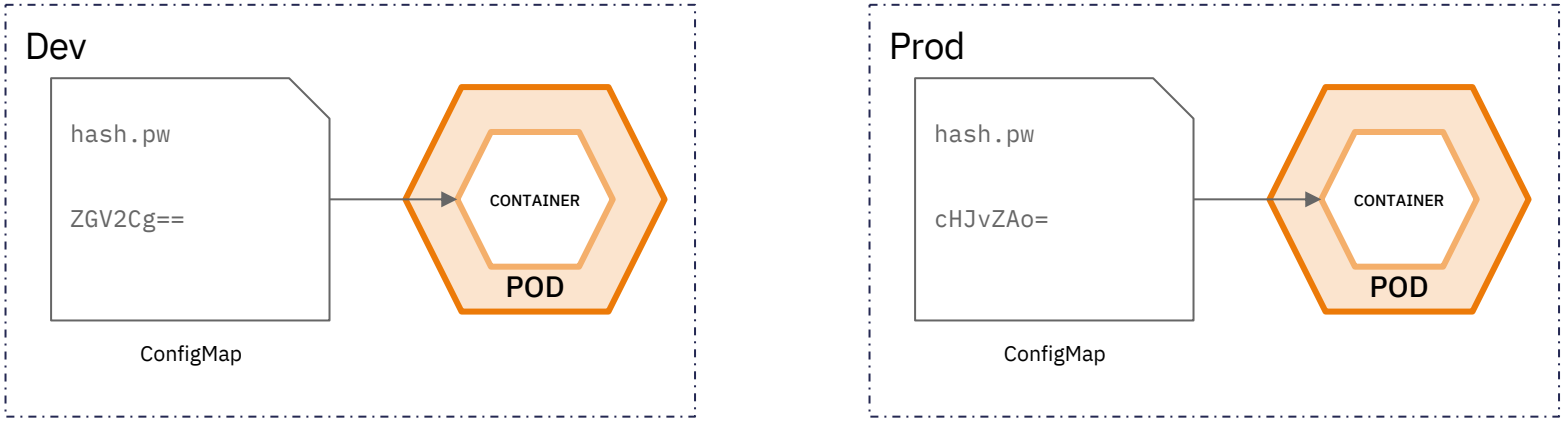
a `daemonset` ensures that all (or some) nodes run a copy of a pod

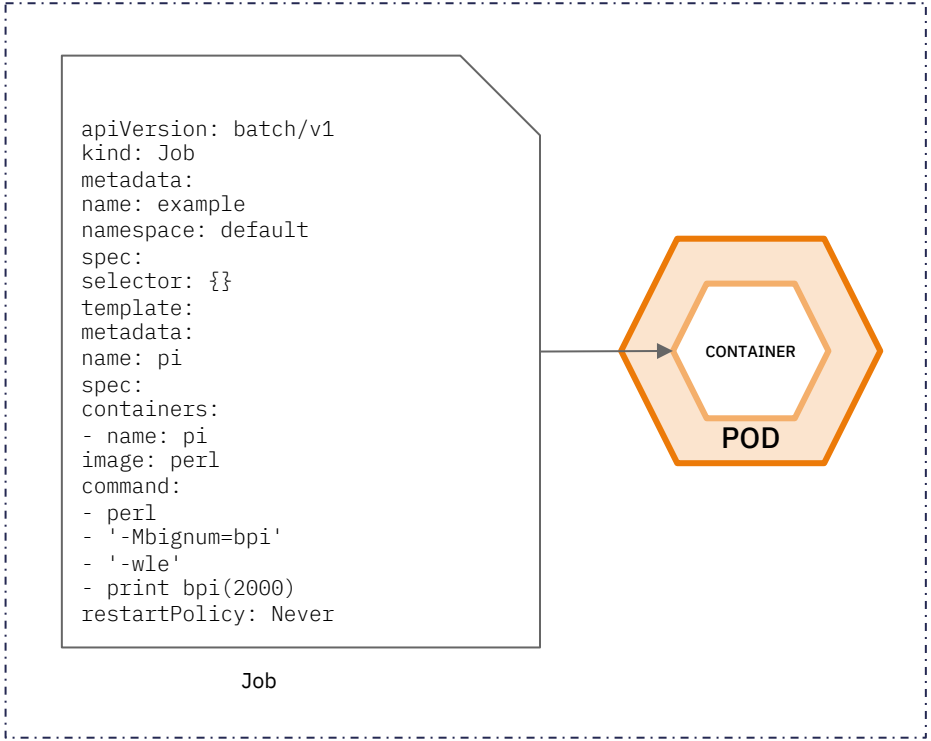


`configmaps` allow you to decouple configuration artifacts from image content

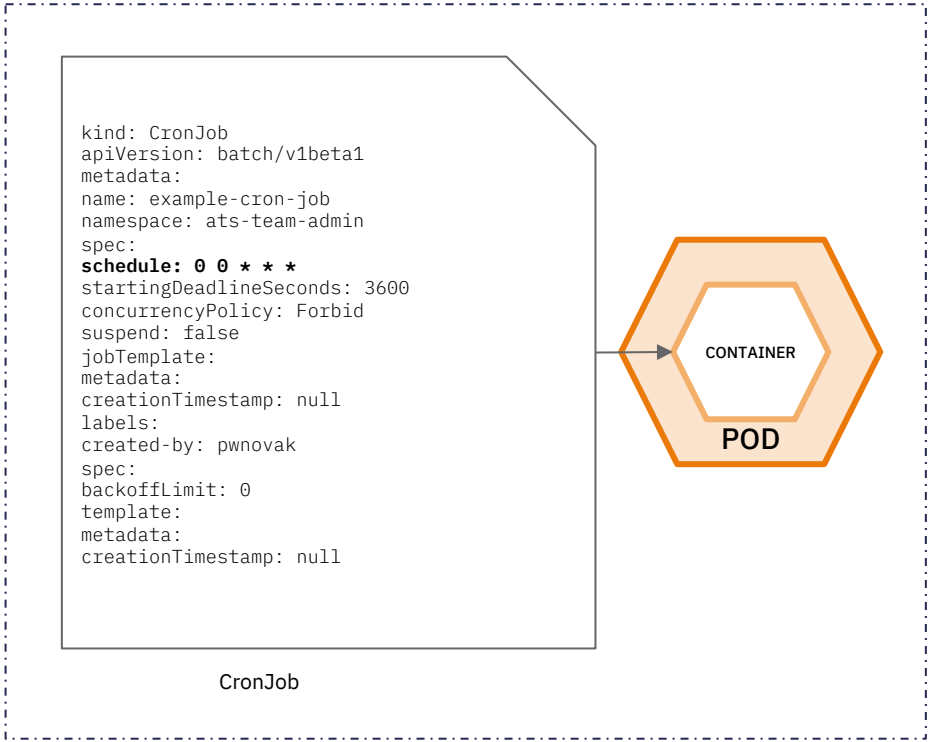


`secrets` provide a mechanism to hold sensitive information such as passwords





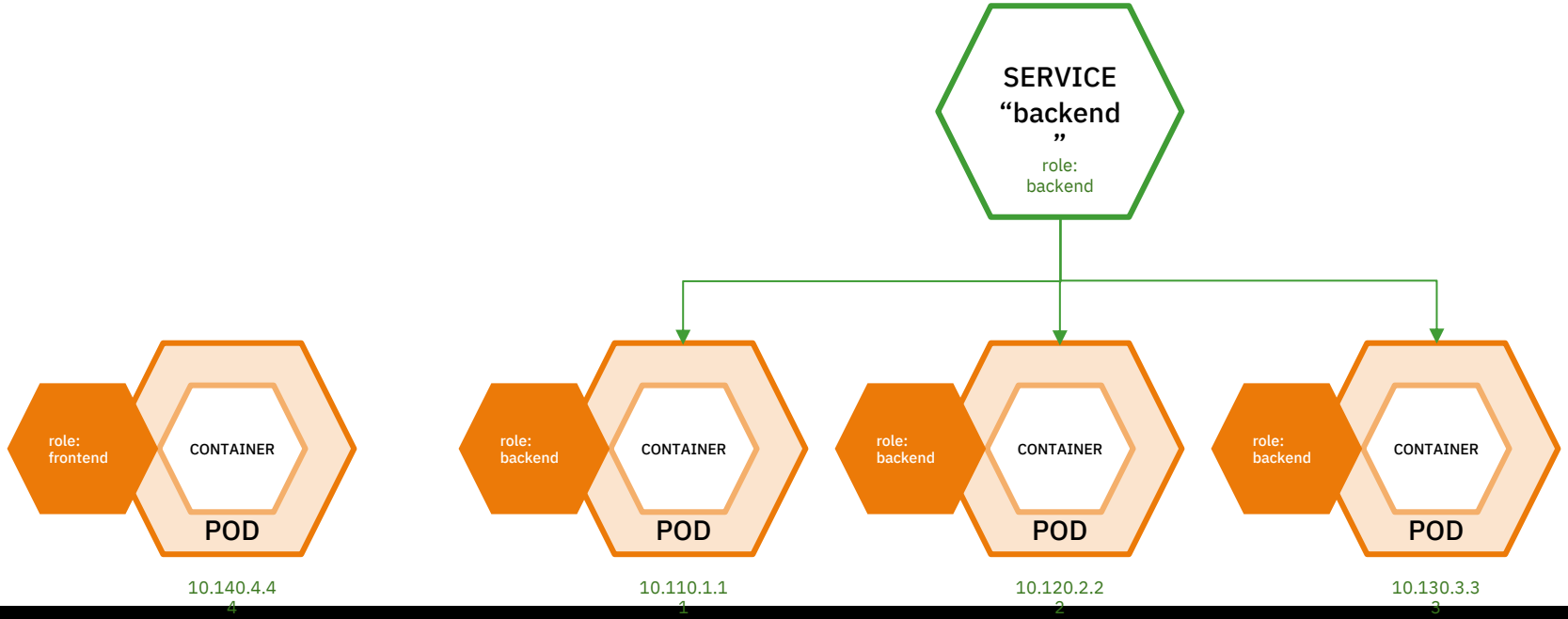
jobs are batch tasks that can be run either manually or via the cluster crontab.



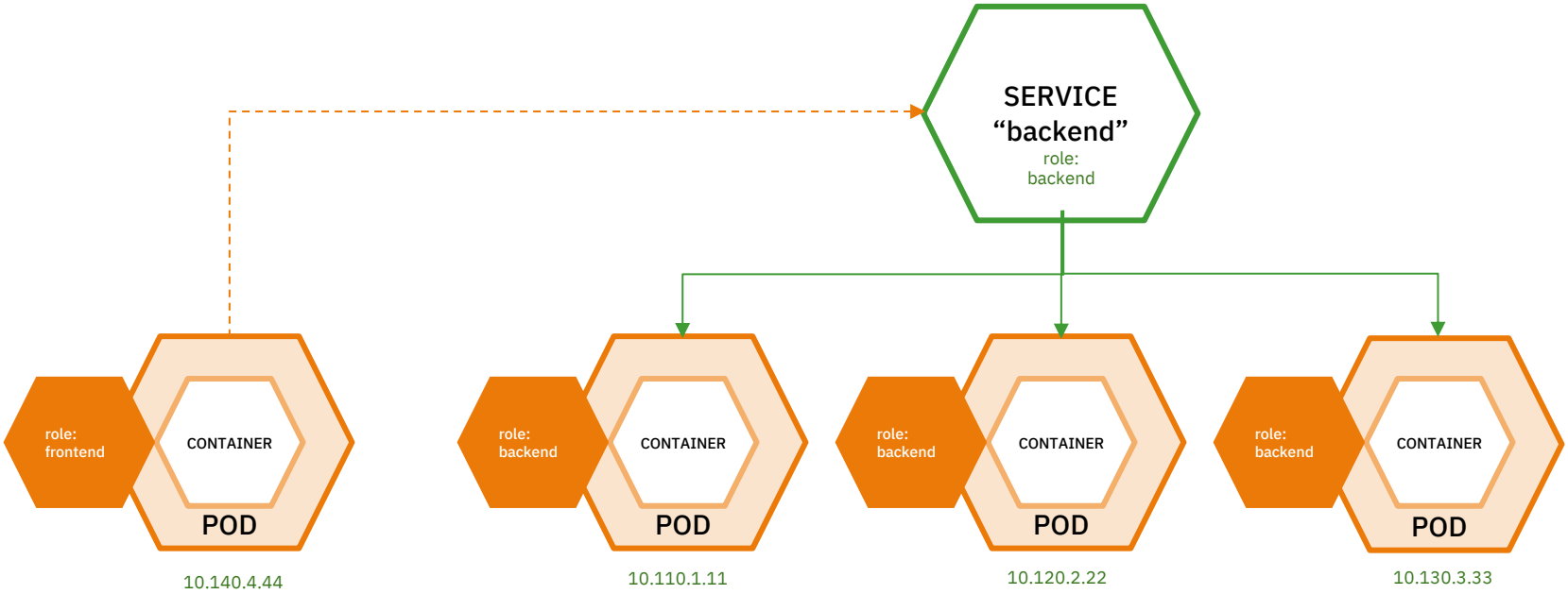
cronjobs are batch tasks run on a defined schedule via the cluster crontab.

Tip: You MUST stagger your scheduling!

services provide internal load-balancing and service discovery across pods

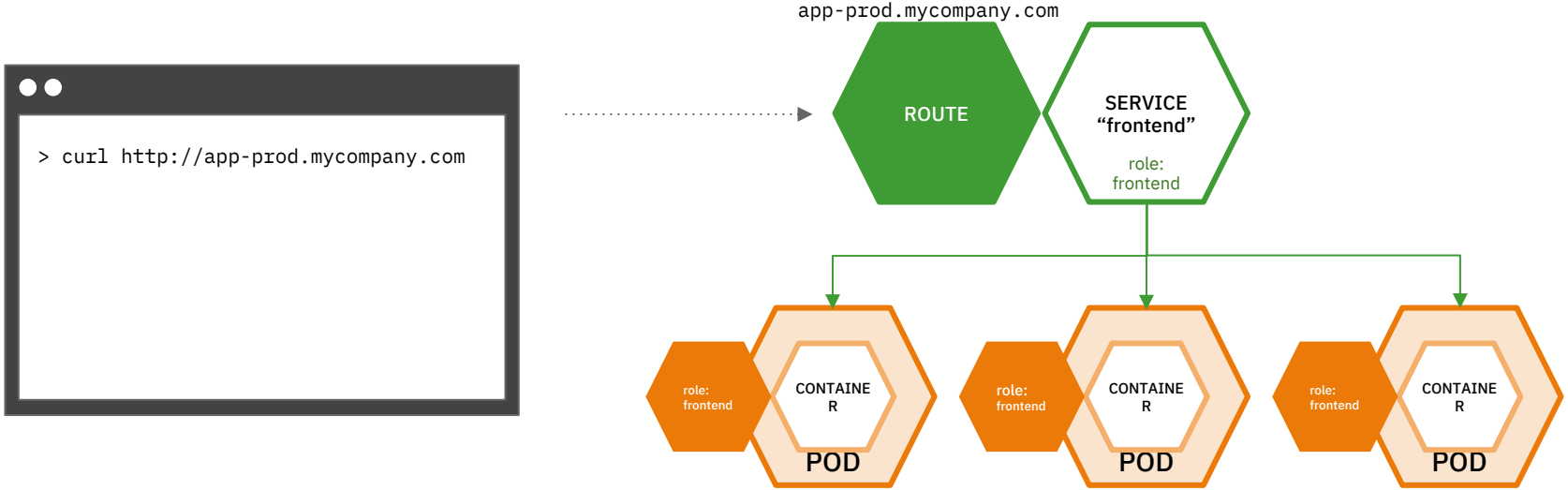


apps can talk to each other via services

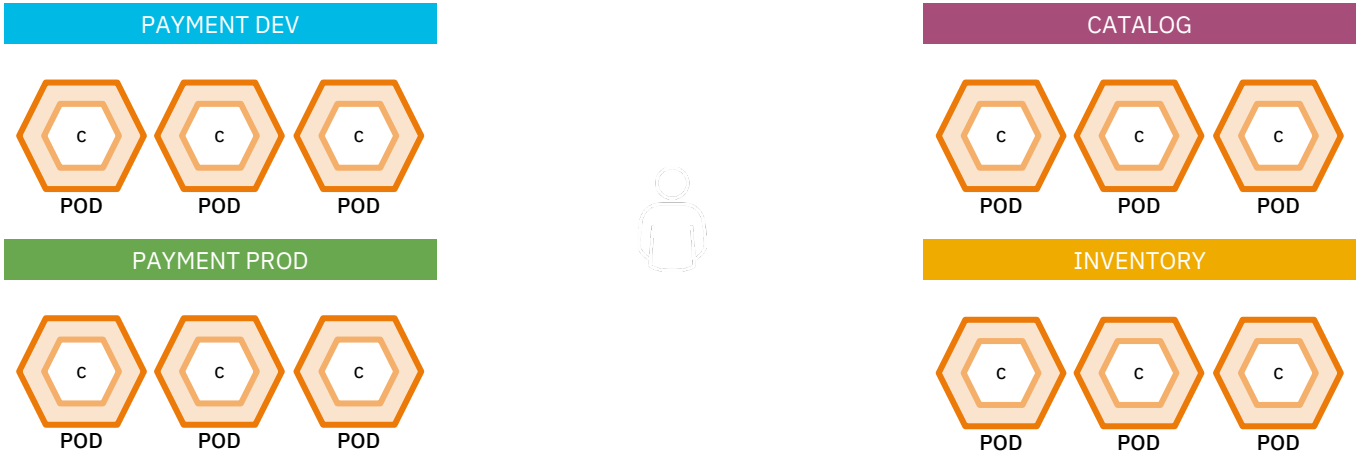


Service chatter

`routes` make services accessible to clients outside the environment via real-world URLs



Namespaces collate resources and isolate apps across environments, teams, groups and departments.



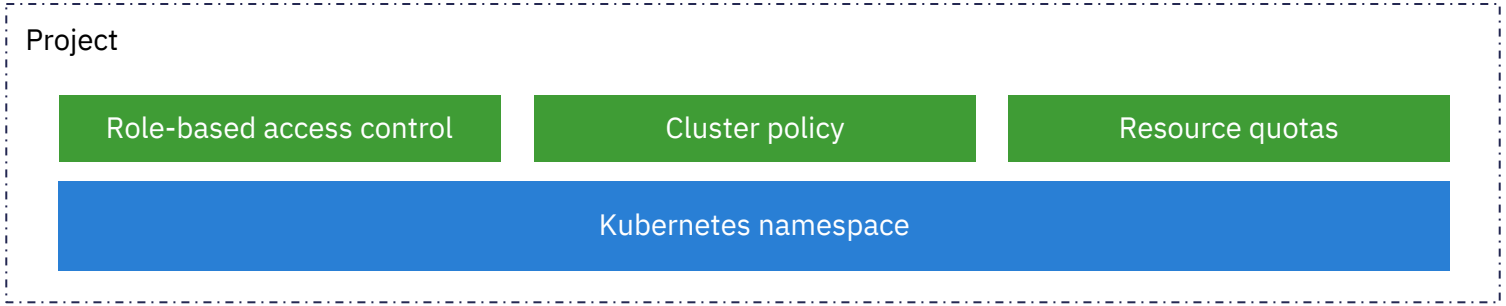
Kubernetes namespaces

Namespaces were designed as a construct for cluster resource management, not security.

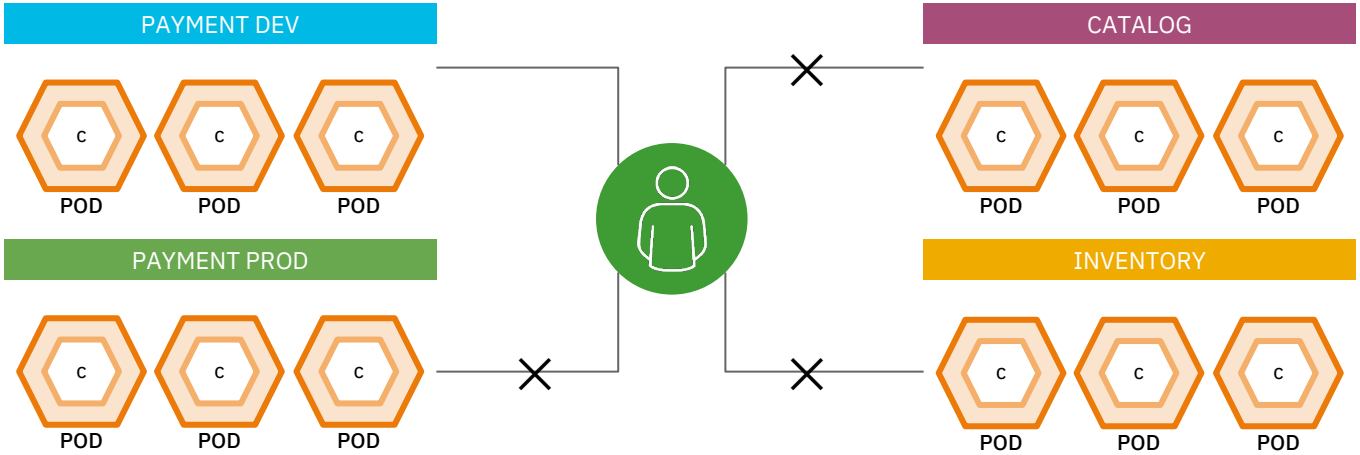
Do not rely on namespaces as a security feature outside of cluster internals within trusted domains.

Do not rely on namespaces to deny a cluster user access to resources in other namespaces.

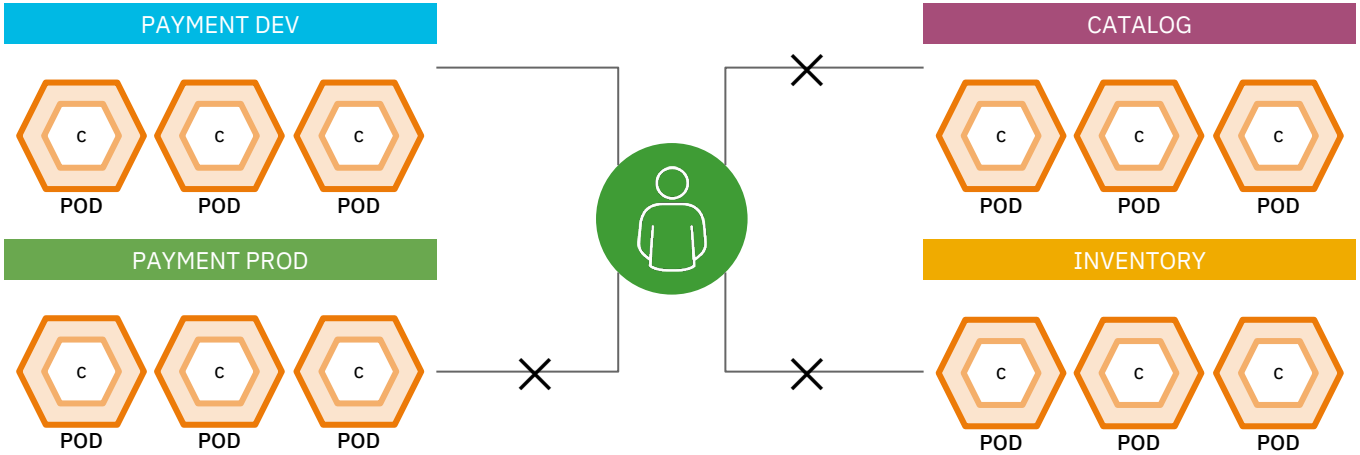
A namespace plus the RBAC layer and some other enhancements is a project



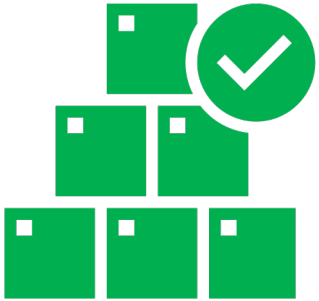
Projects isolate apps across environments, teams, groups and departments

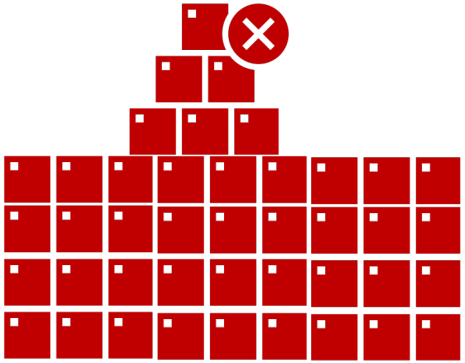


IBM Z and LinuxONE are the only platform where SECURE multi-tenant usage is possible



Embrace projects and use them on a sensible scale. Balance their performance enhancement against operational complexity.





OpenShift 4 Architecture

COMPUTE

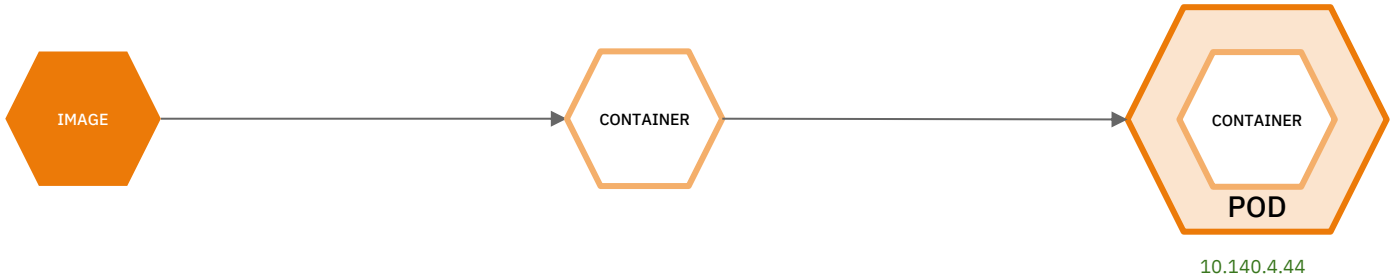
NETWORK

STORAGE

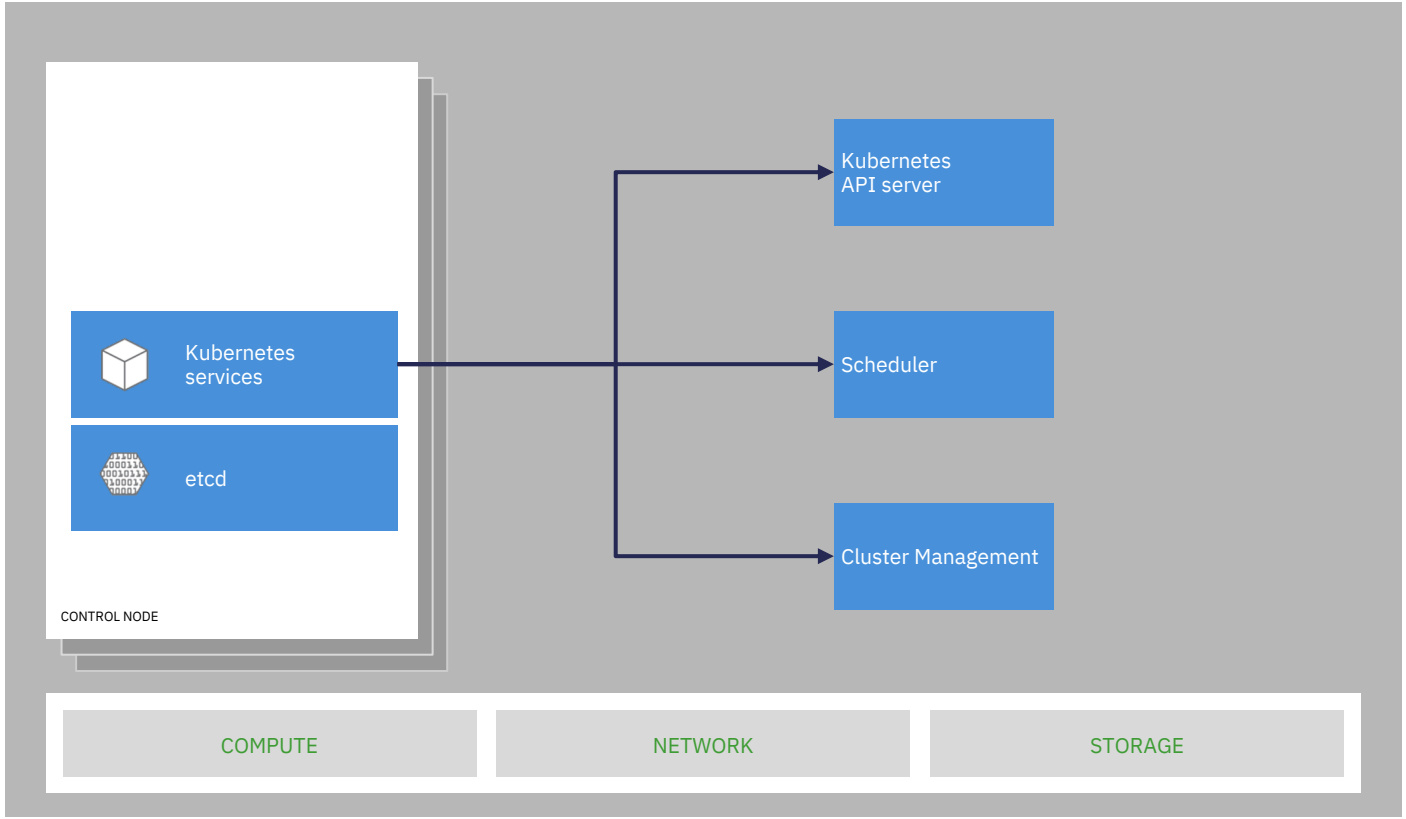
your choice of infrastructure

Compute nodes run workloads

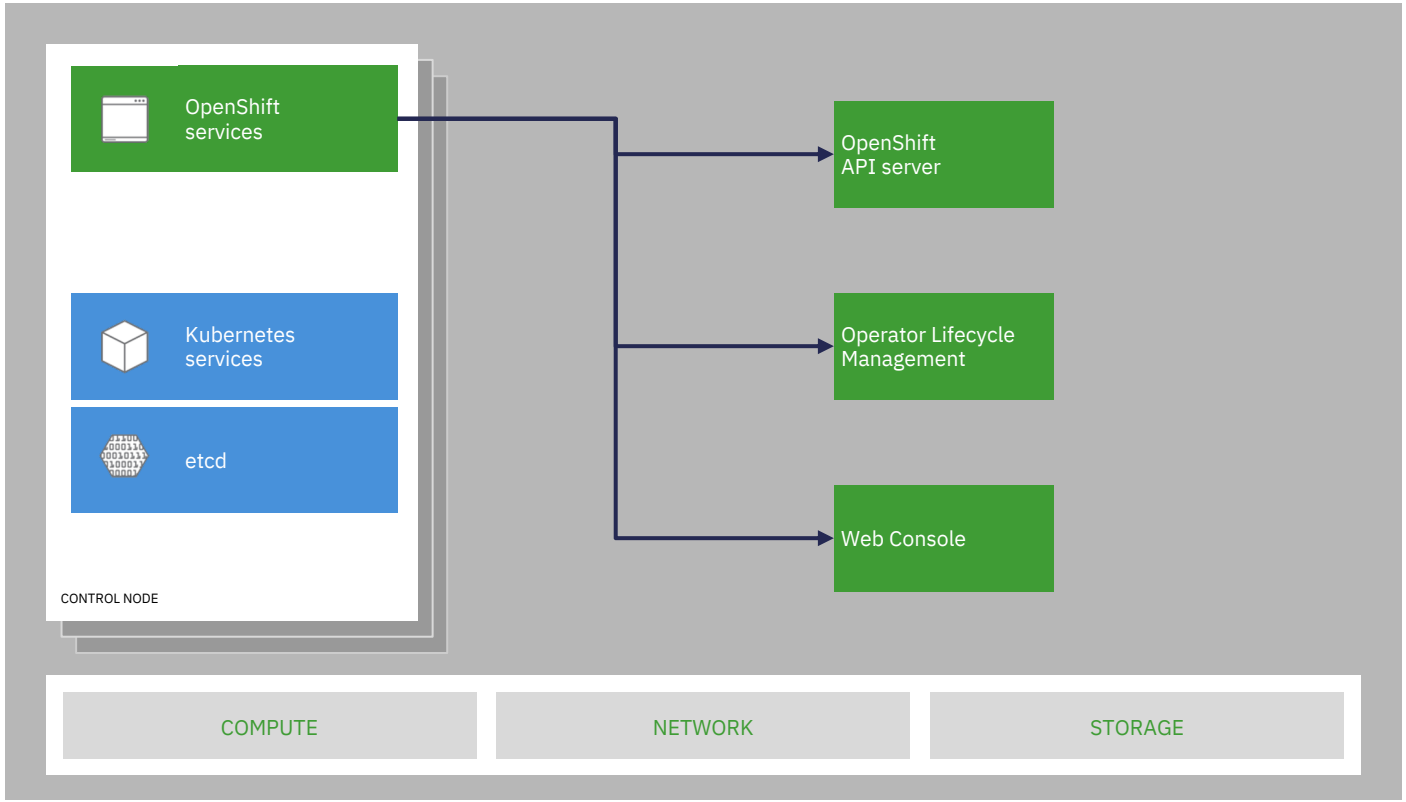
Control nodes



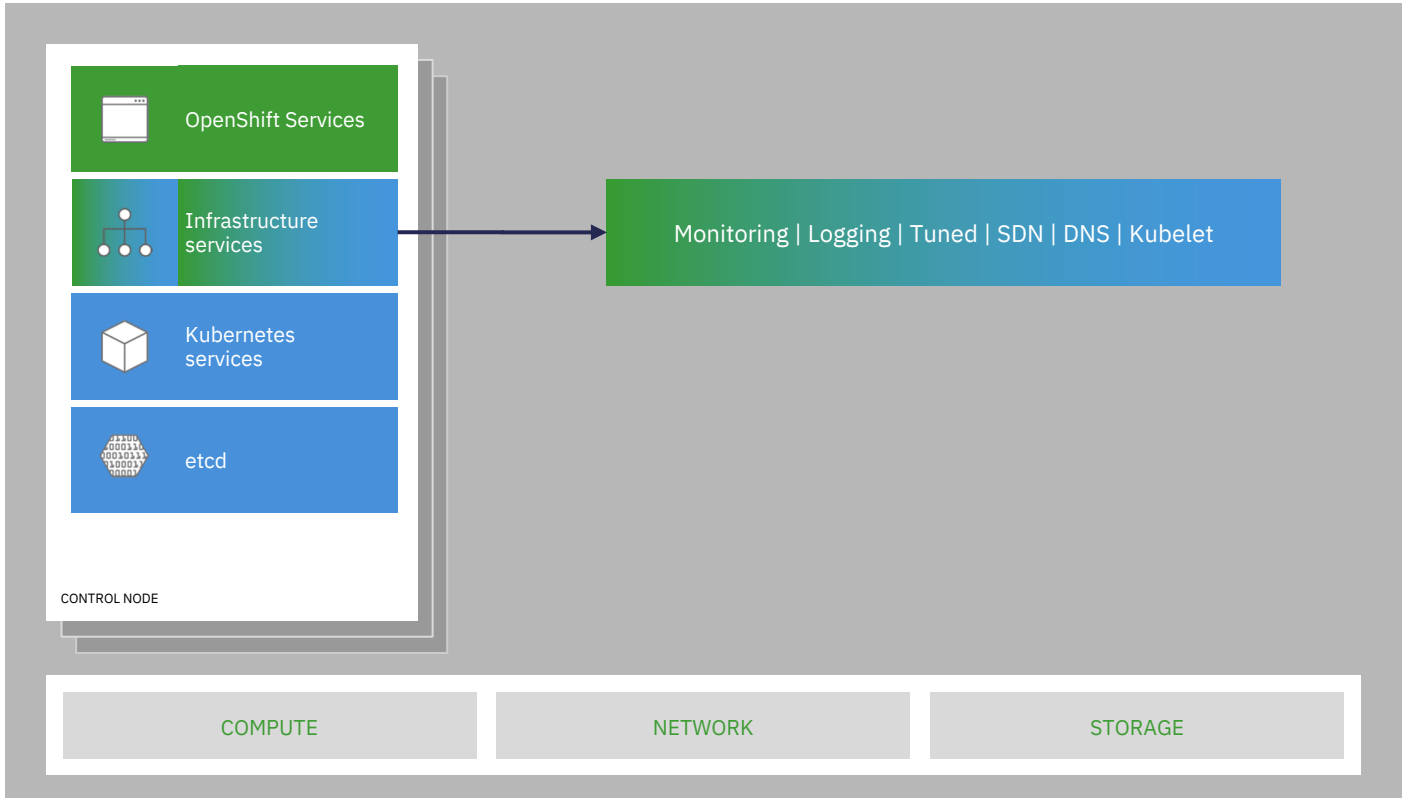
everything runs in pods



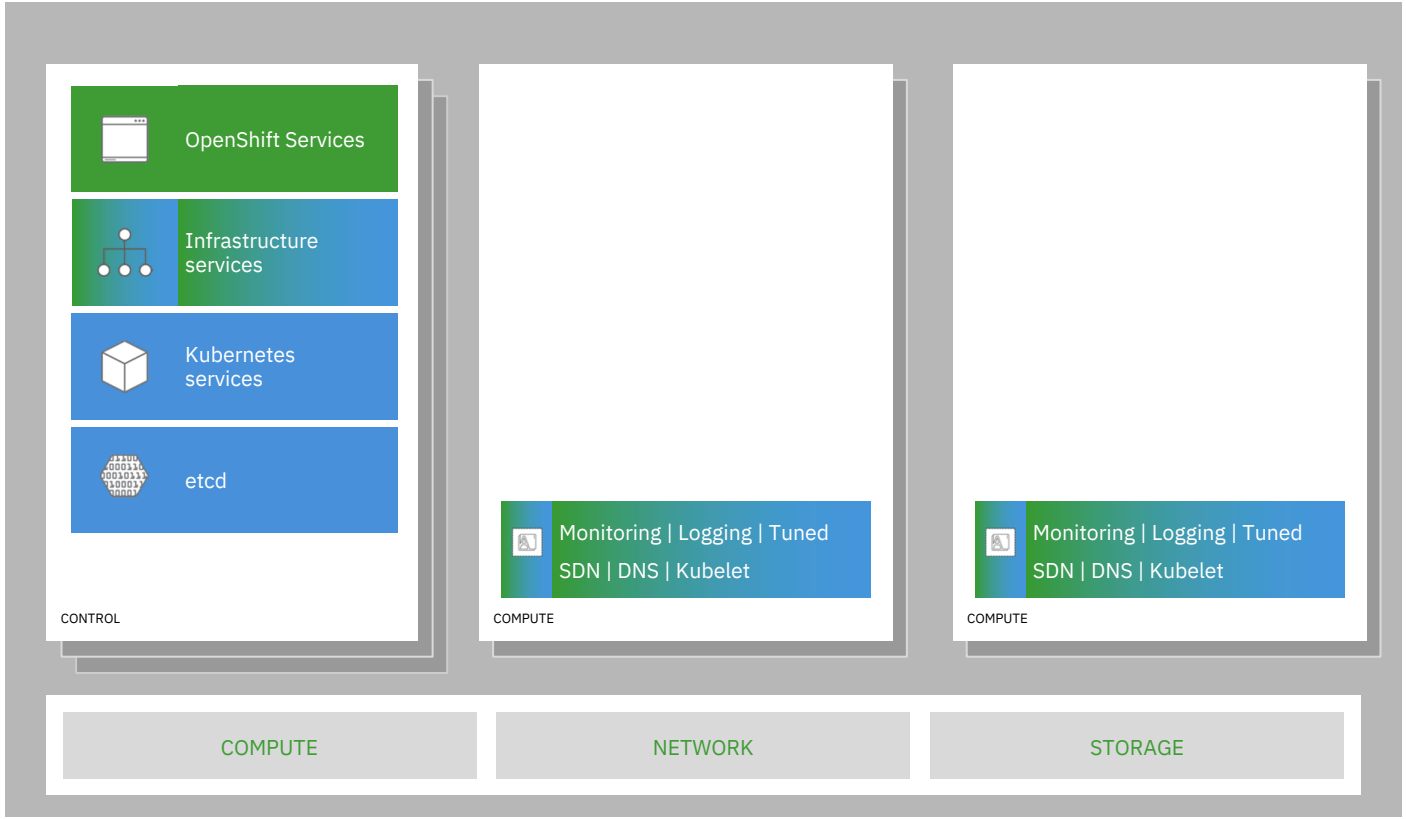
core kubernetes components



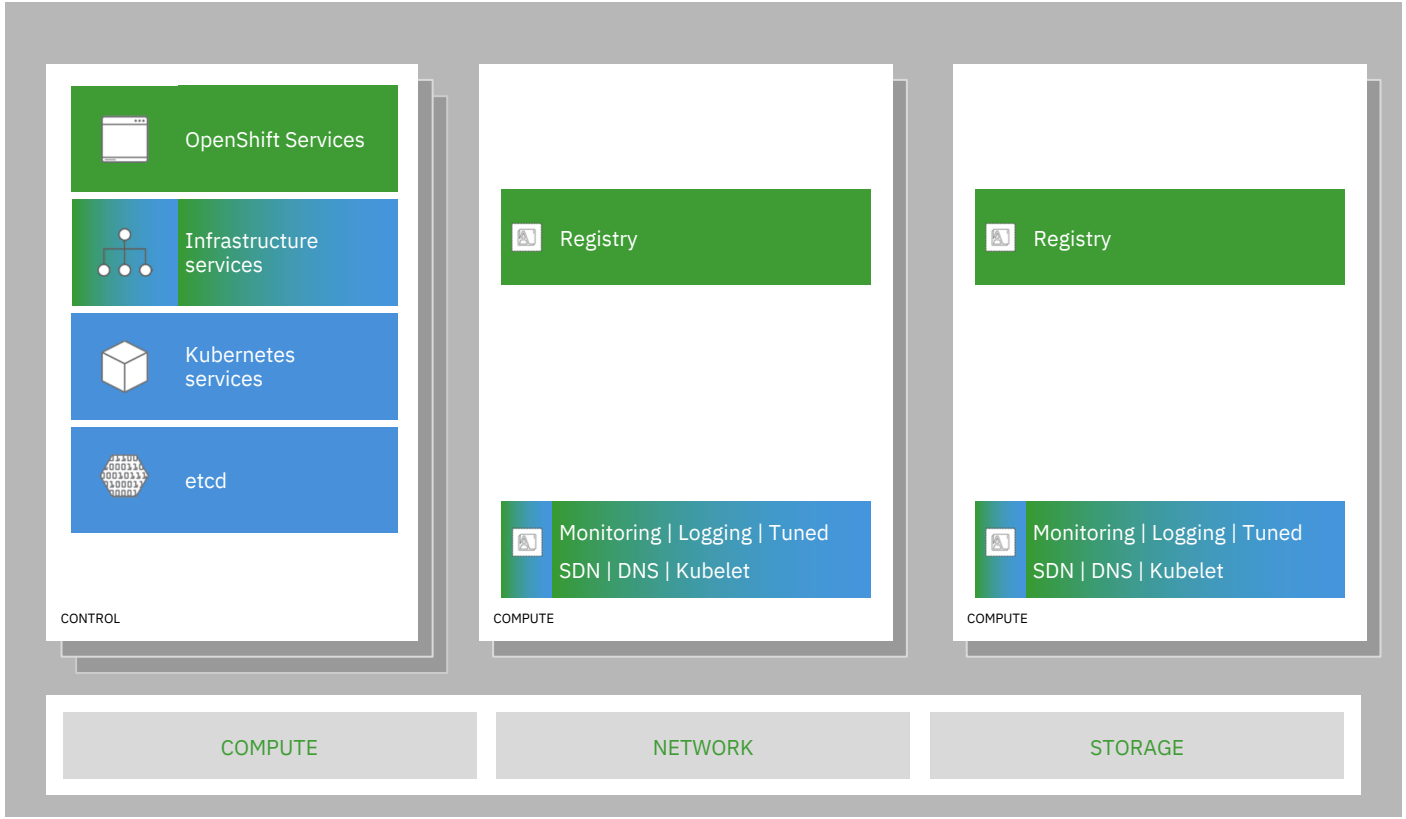
core OpenShift components



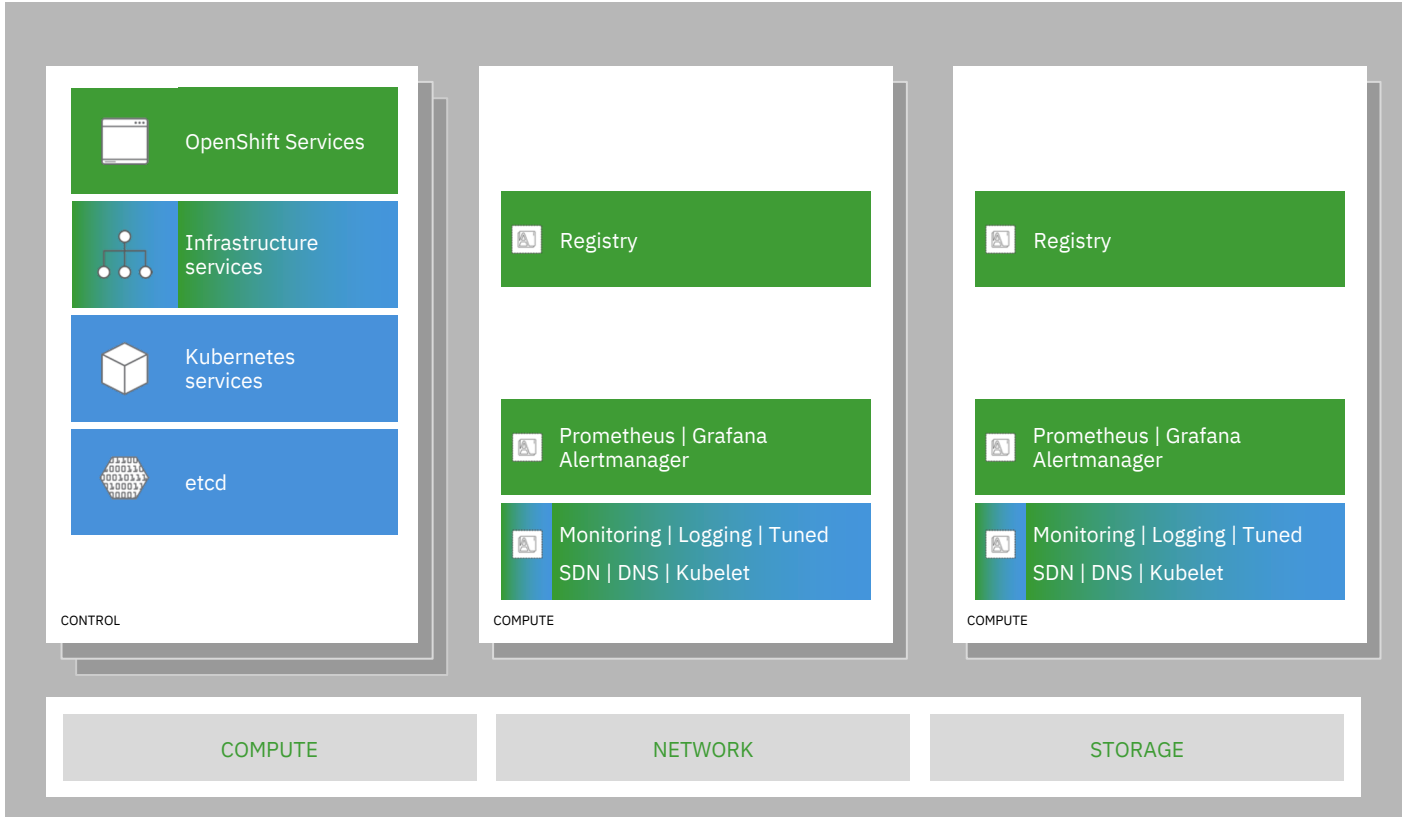
internal and support infrastructure services



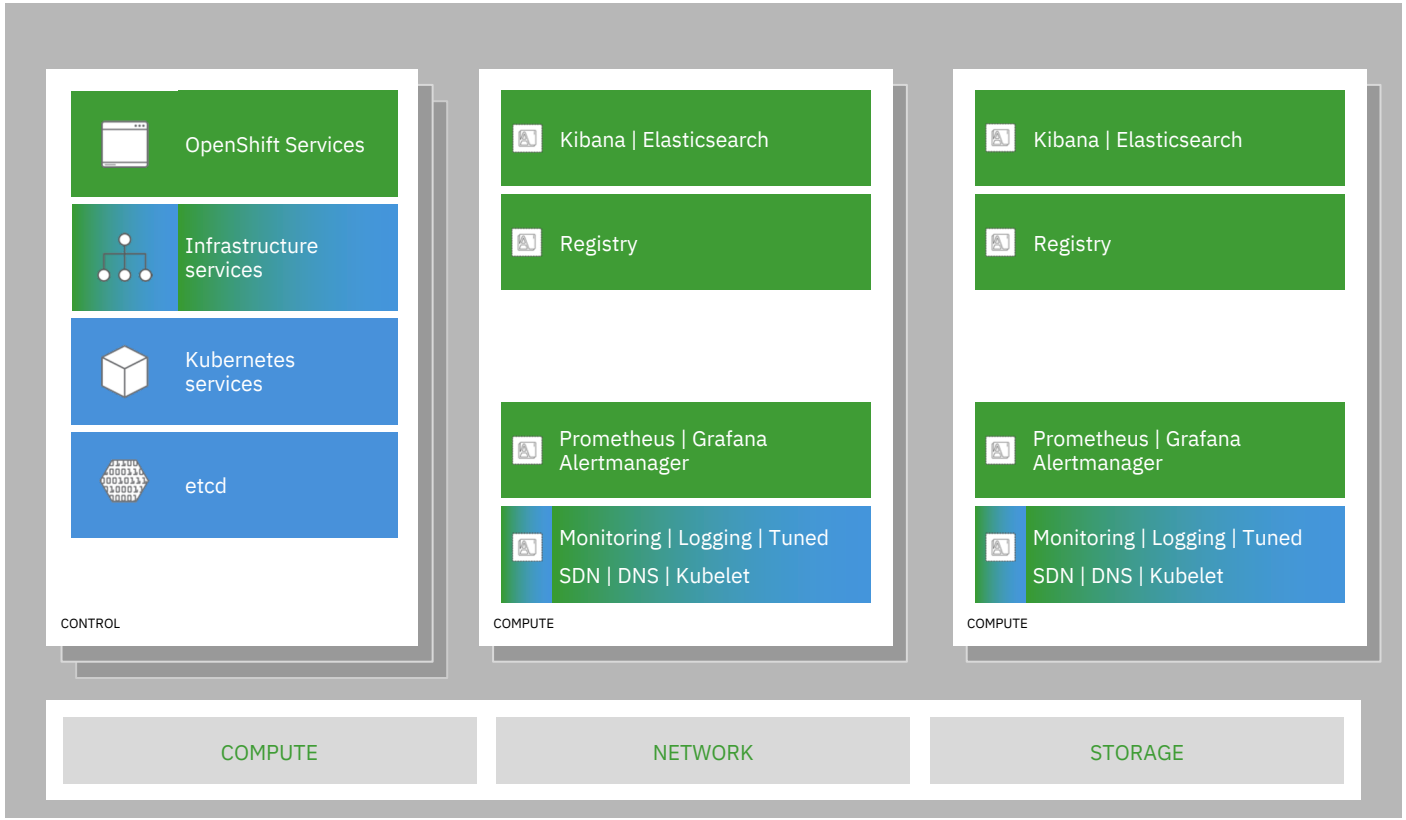
run on all hosts



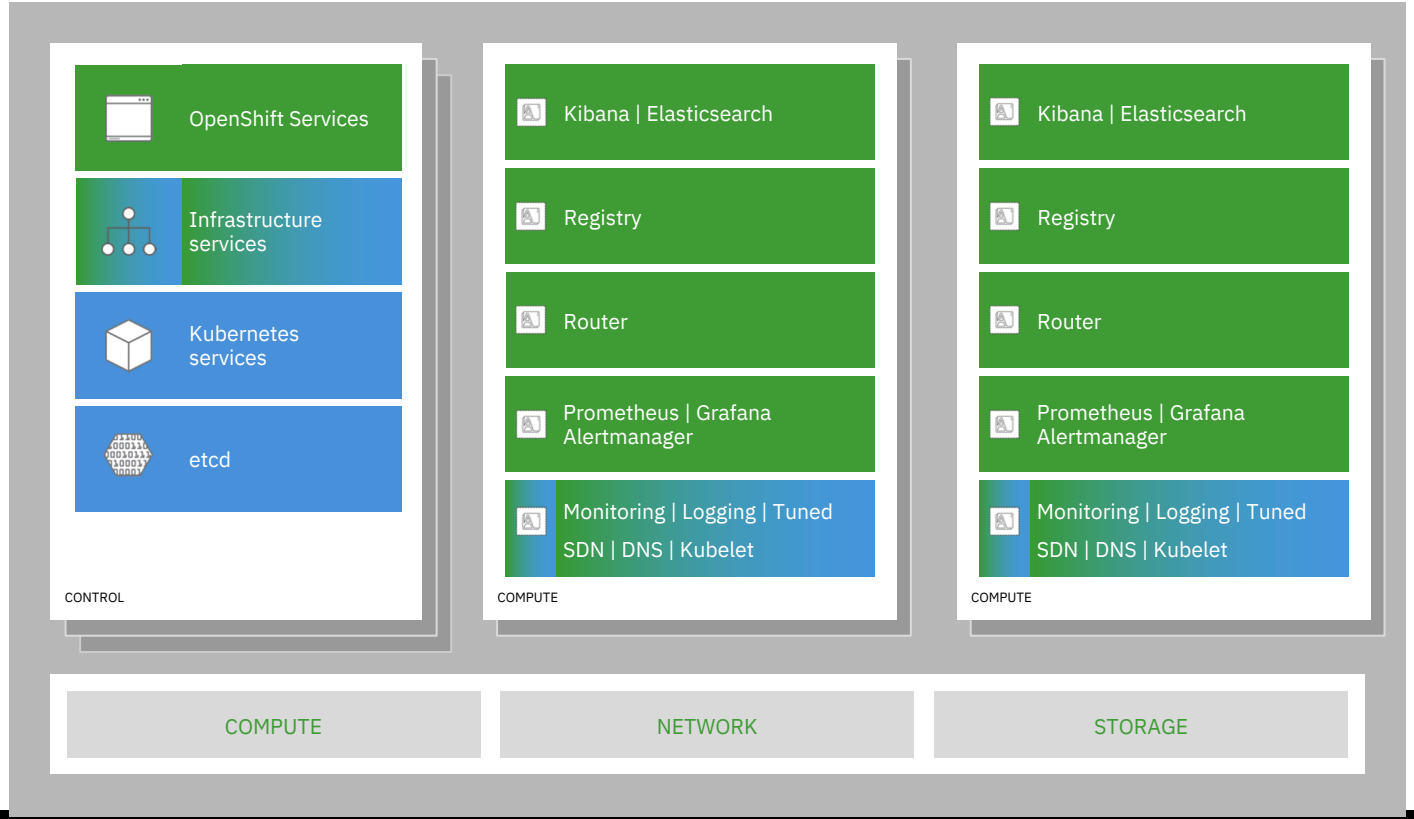
integrated image registry



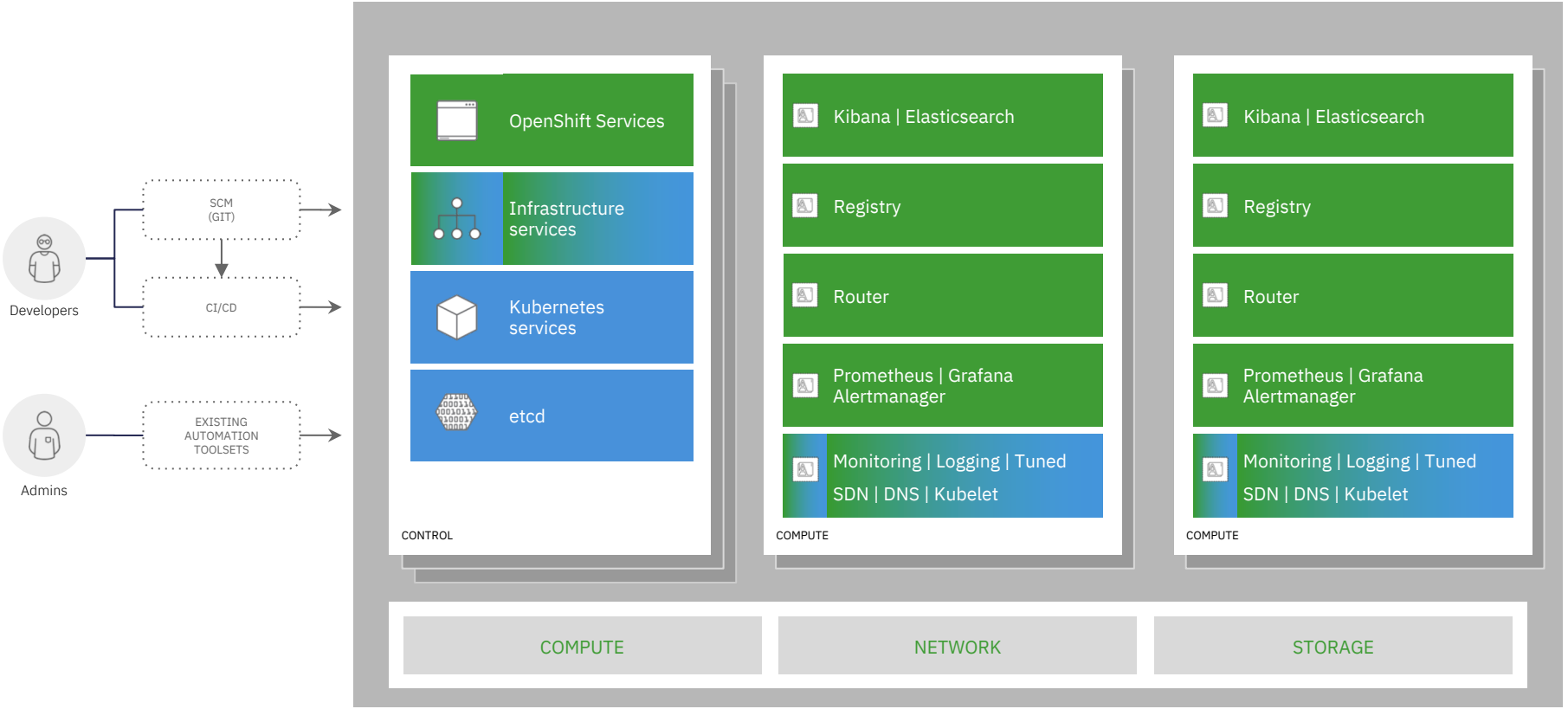
cluster monitoring



log aggregation



integrated routing



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

OpenShift lifecycle, installation & upgrades

OpenShift 4 Installation

Two new paradigms for deploying clusters

OPENSHIFT CONTAINER PLATFORM

Full Stack Automated

Simplified opinionated "Best Practices" for cluster provisioning

Fully automated installation and updates including host container OS.

Red Hat Enterprise Linux CoreOS

Pre-existing Infrastructure

Customer managed resources & infrastructure provisioning

Plug into existing DNS and security boundaries

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux

HOSTED OPENSHIFT

IBM Cloud Red Hat OpenShift

Get a powerful cluster in the IBM Cloud, fully managed by IBM engineers and support.

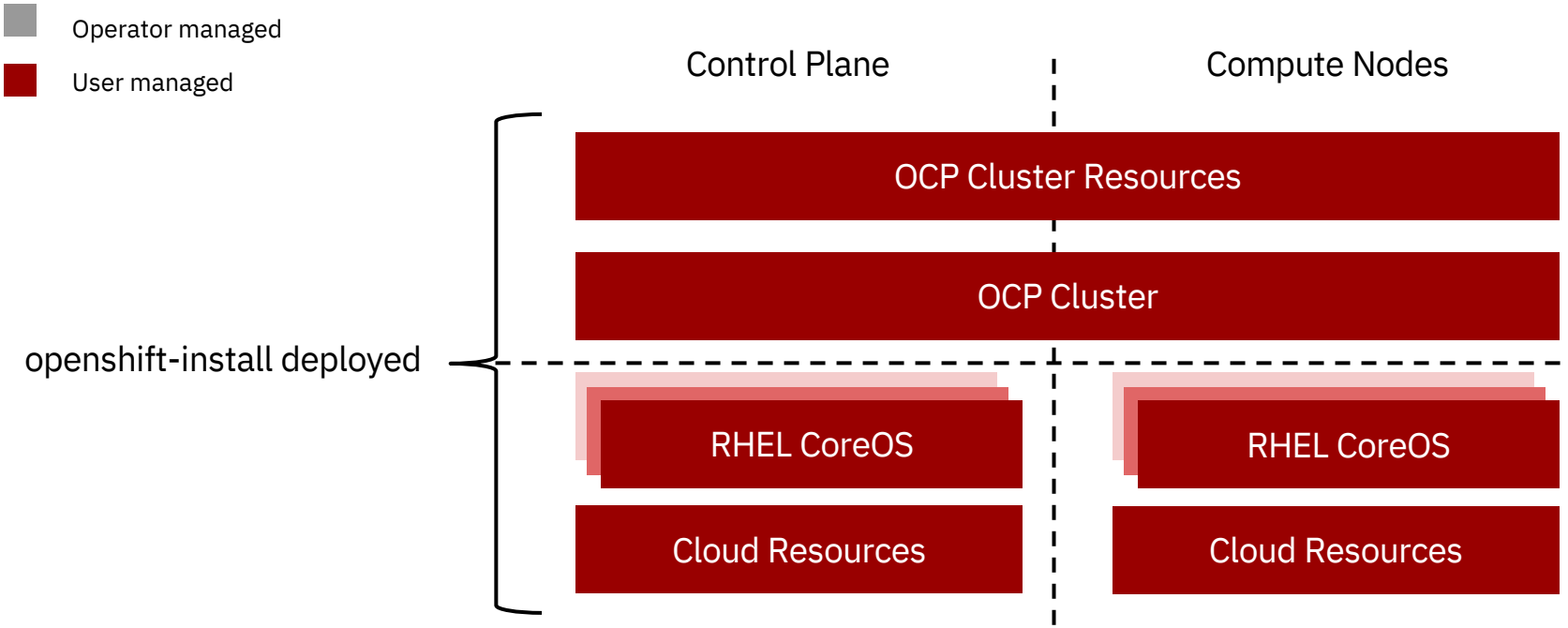
Azure Red Hat OpenShift

Deploy directly from the Azure console. Jointly managed by Red Hat and Microsoft Azure engineers.

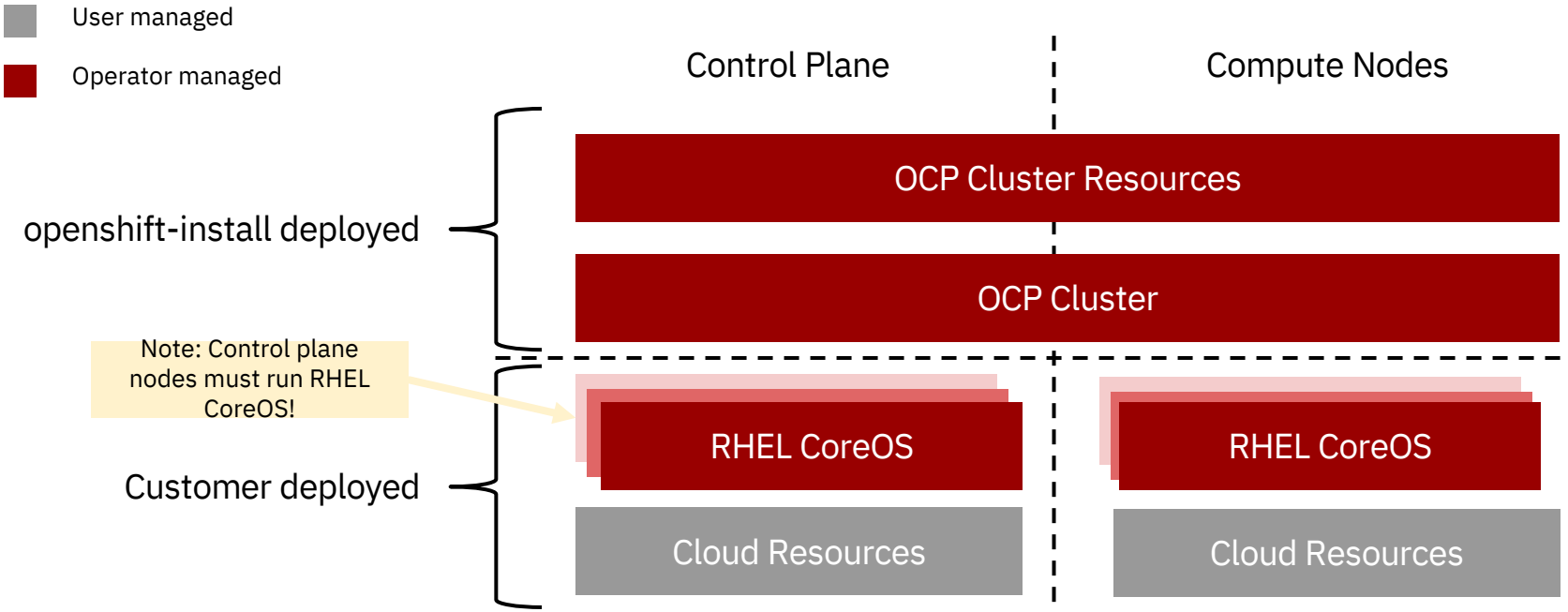
OpenShift Dedicated

Get a powerful cluster, fully managed by Red Hat engineers and support.

Installation Paradigms



Full-stack Automated Installation



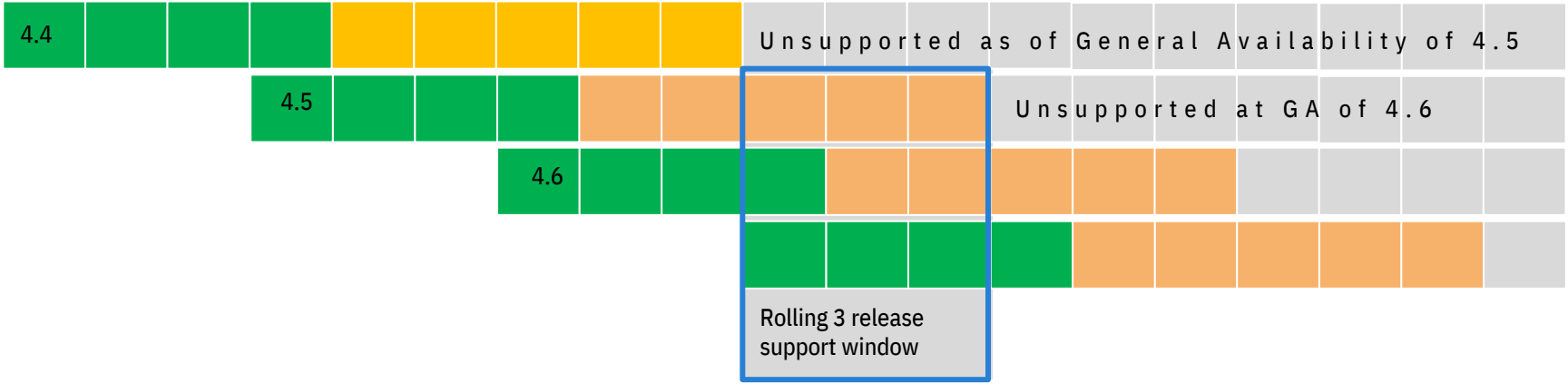
Pre-existing Infrastructure Installation

	Full Stack Automation	Pre-existing Infrastructure
Build Network	Installer	User
Setup Load Balancers	Installer	User
Configure DNS	Installer	User
Hardware/VM Provisioning	Installer	User
OS Installation	Installer	User
Generate Ignition Configs	Installer	Installer
OS Support	Installer: RHEL CoreOS	User: RHEL CoreOS
Node Provisioning / Autoscaling	Yes	Only for providers with OpenShift Machine API support

Comparison of Paradigms

Supported paths for upgrades and migrations

* Hypothetical timeline for discussion purposes



New model

Release based, not date based. Rolling three release window for support.

The overall 4 series will be supported for at least three years

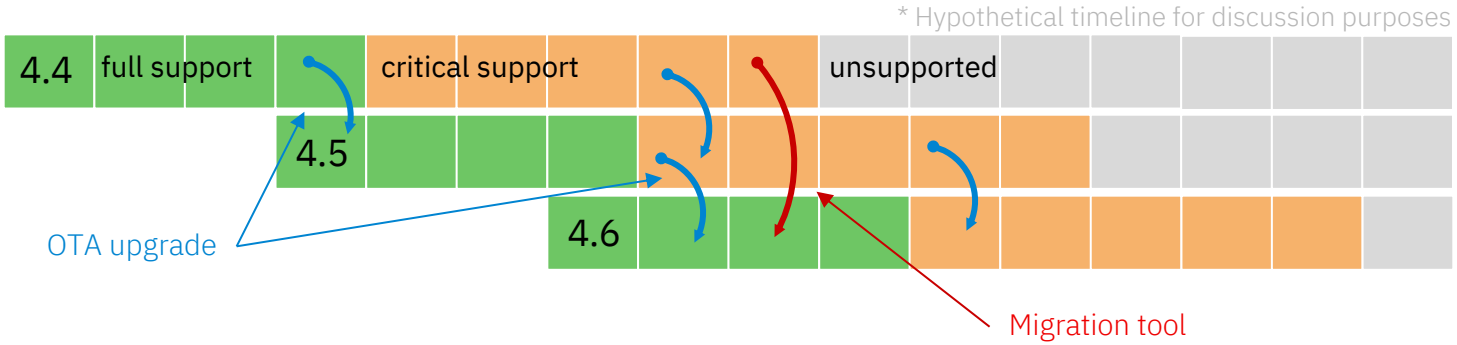
- Minimum two years full support (likely more)
- One year maintenance past the end of full support

EUS release planned

Supported for 14 months of critical bug and critical security fixes instead of the normal 5 months. If you stay on the EUS for its entire life, you must use the application migration tooling to move to a new cluster

https://access.redhat.com/support/policy/updates/openshift#ocp4_phases

Support Timelines



OTA Upgrades
Works between two minor releases in a serial manner.

Happy path = migrate through each version
On a regular cadence, migrate to the next supported version.

Optional path = migration tooling
If you fall more than two releases behind, you must use the application migration tooling to move to a new cluster.

Current minor release
Full support for all bugs and security issues
1 month full support overlap with next release to aid migrations

Previous minor release
Fixes for critical bugs and security issues for 5 months

Upgrades vs. Migrations

Operations and infrastructure deep dive

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux

	RED HAT® ENTERPRISE LINUX®	RED HAT® ENTERPRISE LINUX CoreOS
	General Purpose OS	Immutable container host
BENEFITS	• 10+ year enterprise life cycle • Industry standard security • High performance on any infrastructure • Customizable and compatible with wide ecosystem of partner solutions	• Self-managing, over-the-air updates • Immutable and tightly integrated with OpenShift • Host isolation is enforced via Containers • Optimized performance on popular infrastructure
WHEN TO USE	When customization and integration with additional solutions is required	When cloud-native, hands-free operations are a top priority

Immutable Operating System

Red Hat Enterprise Linux CoreOS is versioned with OpenShift

CoreOS is tested and shipped in conjunction with the platform. Red Hat runs thousands of tests against these configurations.

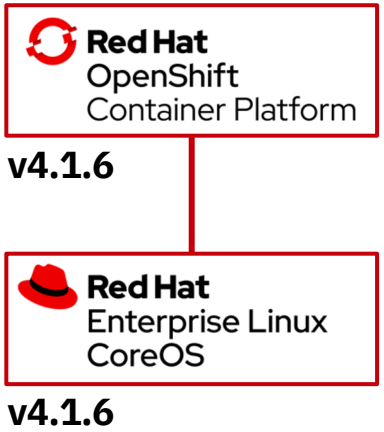
Red Hat Enterprise Linux CoreOS is managed by the cluster

The Operating system is operated as part of the cluster, with the config for components managed by Machine Config Operator:

- CRI-O config
- Kubelet config
- Authorized registries
- SSH config

RHEL CoreOS admins are responsible for:

Nothing. 😀🙌



More about CoreOS

Minimal and Secure Architecture

Optimized for Kubernetes

Runs any OCI-compliant image (including docker)

A lightweight, OCI-compliant container runtime

CRI-O tracks and versions identical to Kubernetes, simplifying support permutations

CRI-O Support in OpenShift

CRI-O 1.15 	Kubernetes 1.15 	OpenShift 4.5 
CRI-O 1.16 	Kubernetes 1.16 	OpenShift 4.6 
CRI-O 1.17 	Kubernetes 1.17 	OpenShift 4.7 

- Remote management API via Varlink
- Image/container tagging
- Advanced namespace isolation

- Integrated into OCP build pods
- Performance improvements for knative enablement
- Image signing improvements

OpenShift 4 installation

How to boot a self-managed cluster:

- OpenShift 4 is unique in that management extends all the way down to the operating system
- Every machine boots with a configuration that references resources hosted in the cluster it joins, enabling cluster to manage itself
- Downside is that every machine looking to join the cluster is waiting on the cluster to be created
- Dependency loop is broken using a bootstrap machine, which acts as a temporary control plane whose sole purpose is bringing up the permanent control plane nodes
- Permanent control plane nodes get booted and join the cluster leveraging the control plane on the bootstrap machine
- Once the pivot to the permanent control plane takes place, the remaining worker nodes can be booted and join the cluster

Bootstrapping process step by step:

1. Bootstrap machine boots and starts hosting the remote resources required for master machines to boot.
2. Control machines fetch the remote resources from the bootstrap machine and finish booting.
3. Control machines use the bootstrap node to form an etcd cluster.
4. Bootstrap node starts a temporary Kubernetes control plane using the newly-created etcd cluster.
5. Temporary control plane schedules the production control plane to the master machines.
6. Temporary control plane shuts down, yielding to the production control plane.
7. Bootstrap node injects OpenShift-specific components into the newly formed control plane.
8. Installer then tears down the bootstrap node or if user-provisioned, this needs to be performed by the administrator.

OpenShift Bootstrap Process: Self-Managed Kubernetes

Controls (Special)

- Terraform provisions initial masters on public cloud / full-stack automated installs. BaNWIS / Bastion on Z and LinuxONE
- Machine API adopts existing masters post-provision
- Each master is a standalone Machine object
- Termination protection (avoid self-destruction)

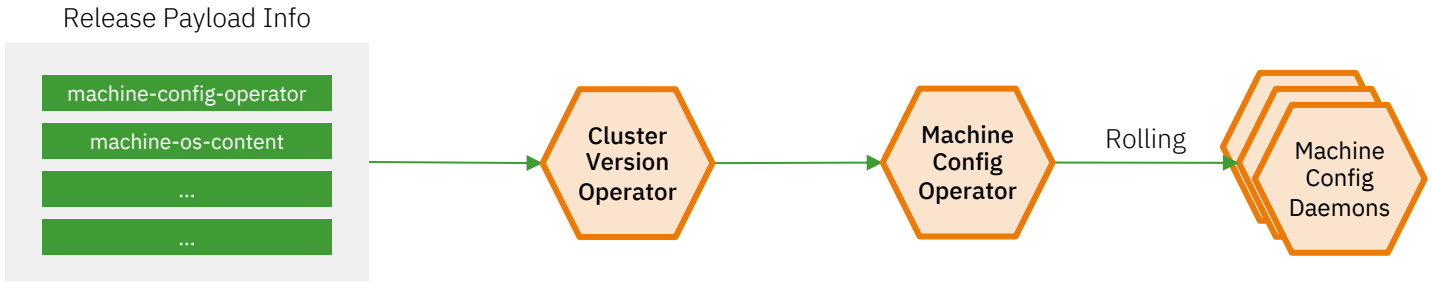
Computes

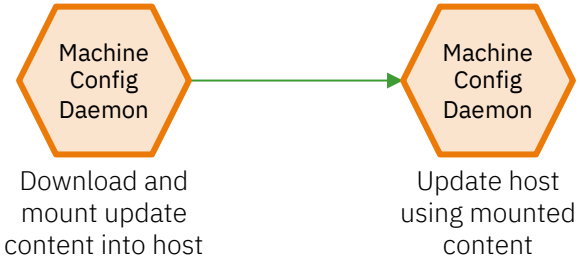
- Each Machine Pool corresponds to MachineSet
- Optionally autoscale (min,max) and health check (replace if not ready > X minutes) on public cloud. This is not much of a concern on Z and LinuxONE because hardware failure is such a remote possibility.

How everything deployed comes under management

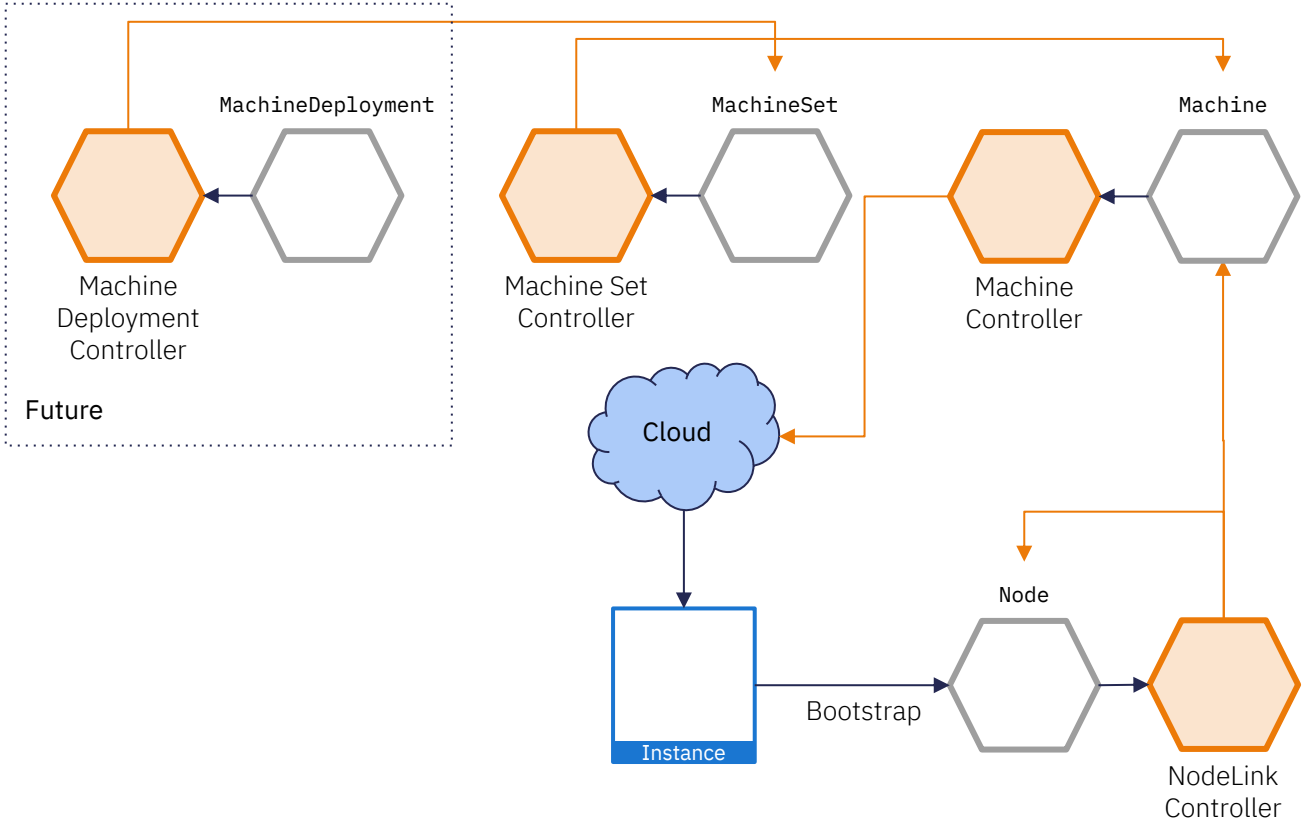
OpenShift 4 Cluster Management

Powered by Operators, OpenShift 4 automates many cluster management activities





Over-the-air updates



OpenShift Security

Features, mechanisms and processes for container and platform isolation

CONTROL
Application Security

- Container Content
- CI/CD Pipeline
- Container Registry
- Deployment Policies

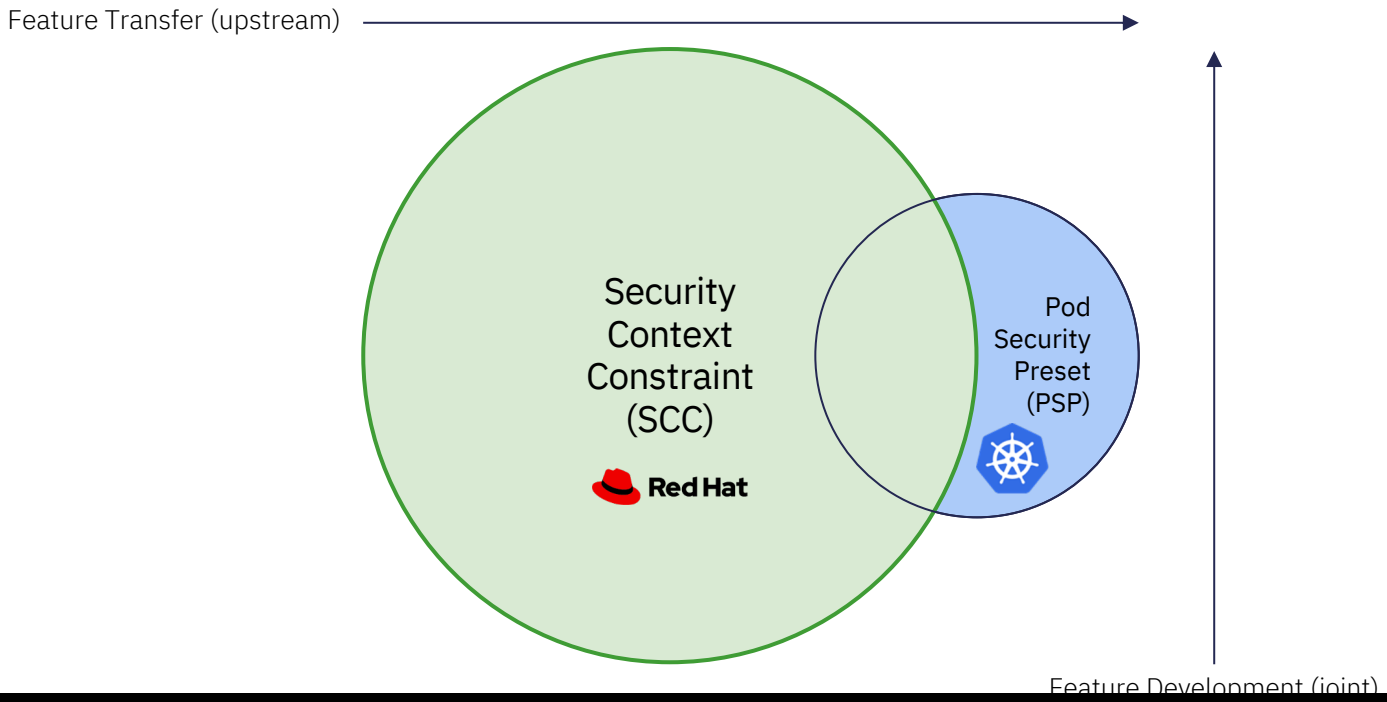
DEFEND
Infrastructure

- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

EXTEND

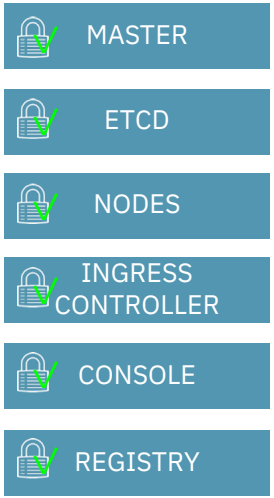
- Security Ecosystem

Security is built in

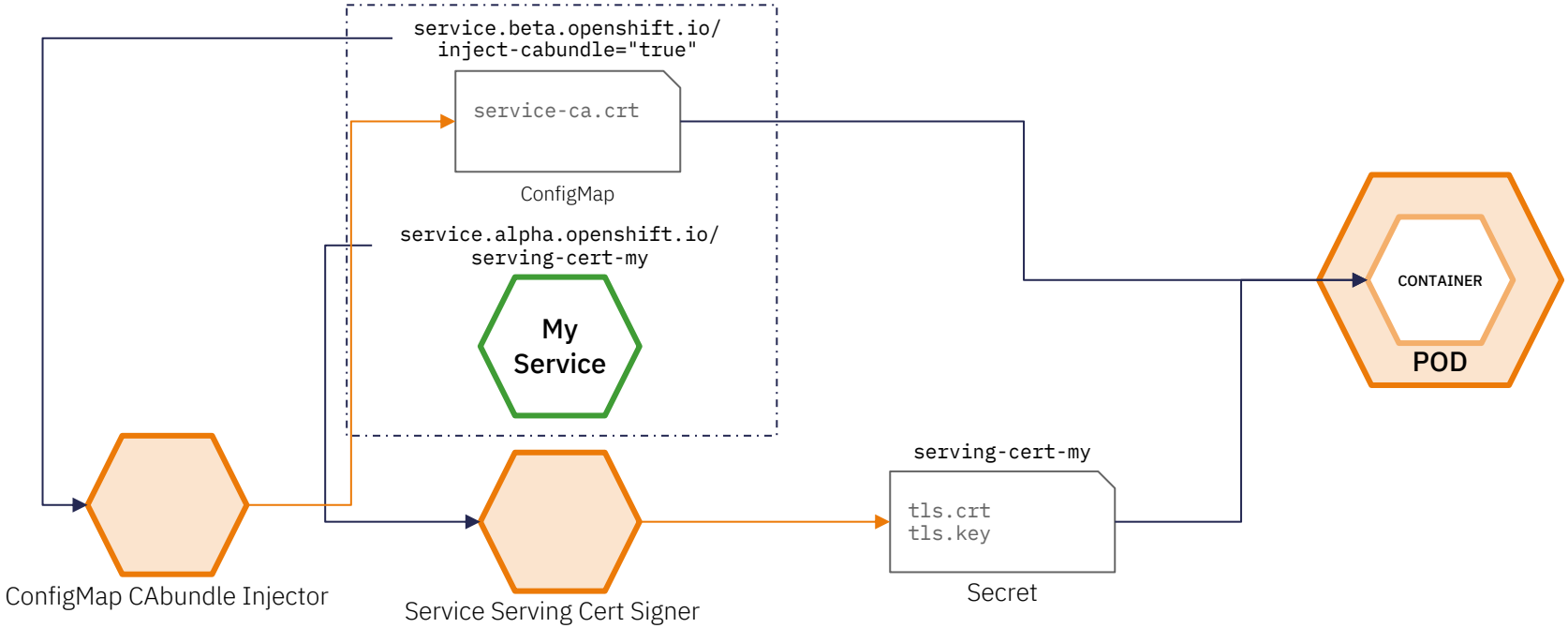


Extended Depth of Protection

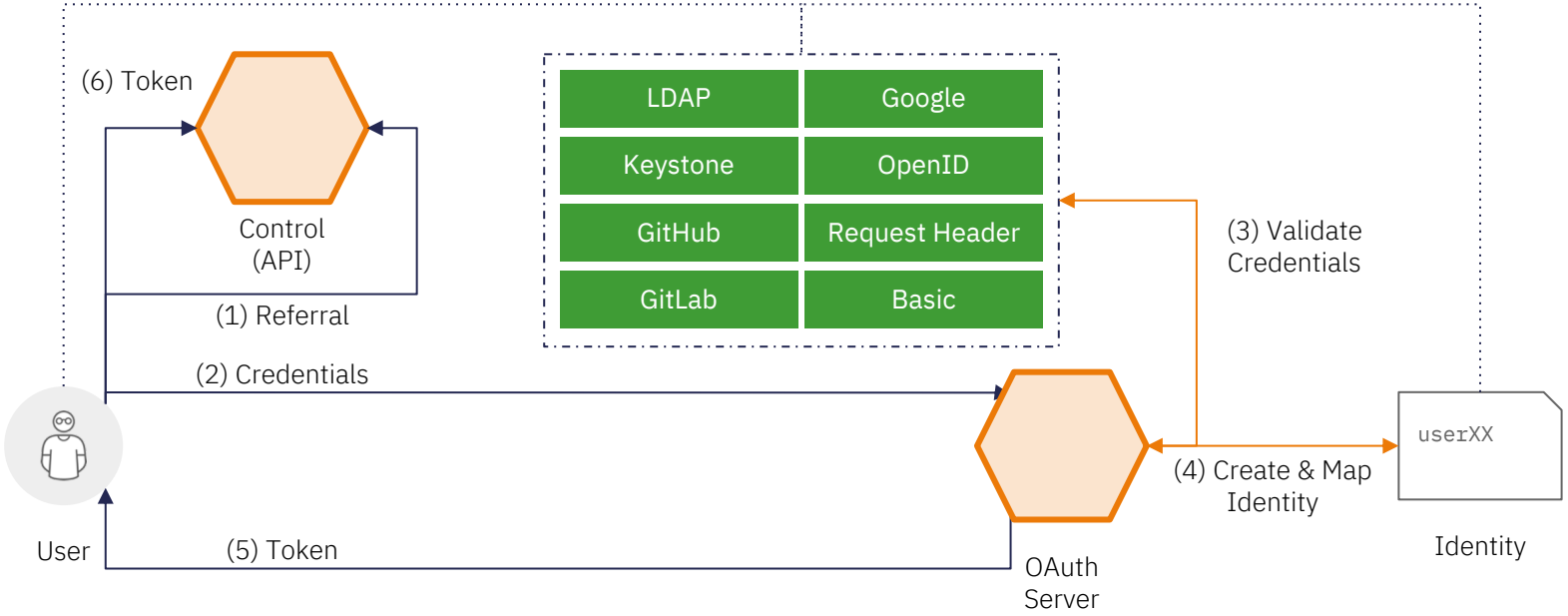
- OpenShift provides its own internal CA
- Certificates are used to provide secure connections to
  - master (APIs) and nodes
  - Ingress controller and registry
  - etcd
- Certificate rotation is automated
- Optionally configure external endpoints to use custom certificates



Certificates and Certificate Management



Service Certificates



- Project scope & cluster scope available
- Matches request attributes (verb,object,etc)
- If no roles match, request is denied (deny by default)
- Operator- and user-level roles are defined by default
- Custom roles are supported

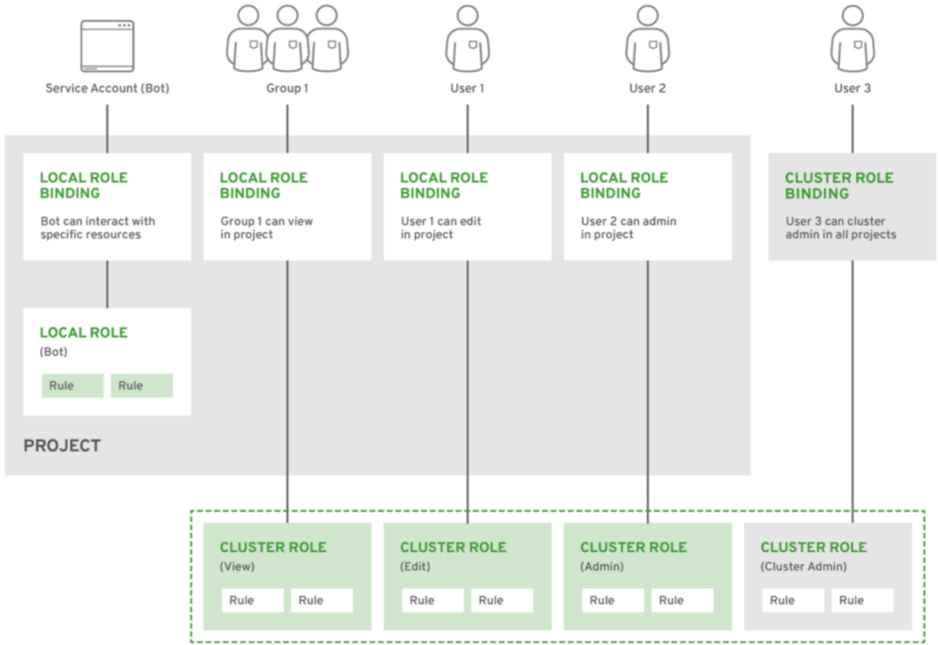


Figure 12 - Authorization Relationships

Fine-Grained RBAC

OpenShift Monitoring

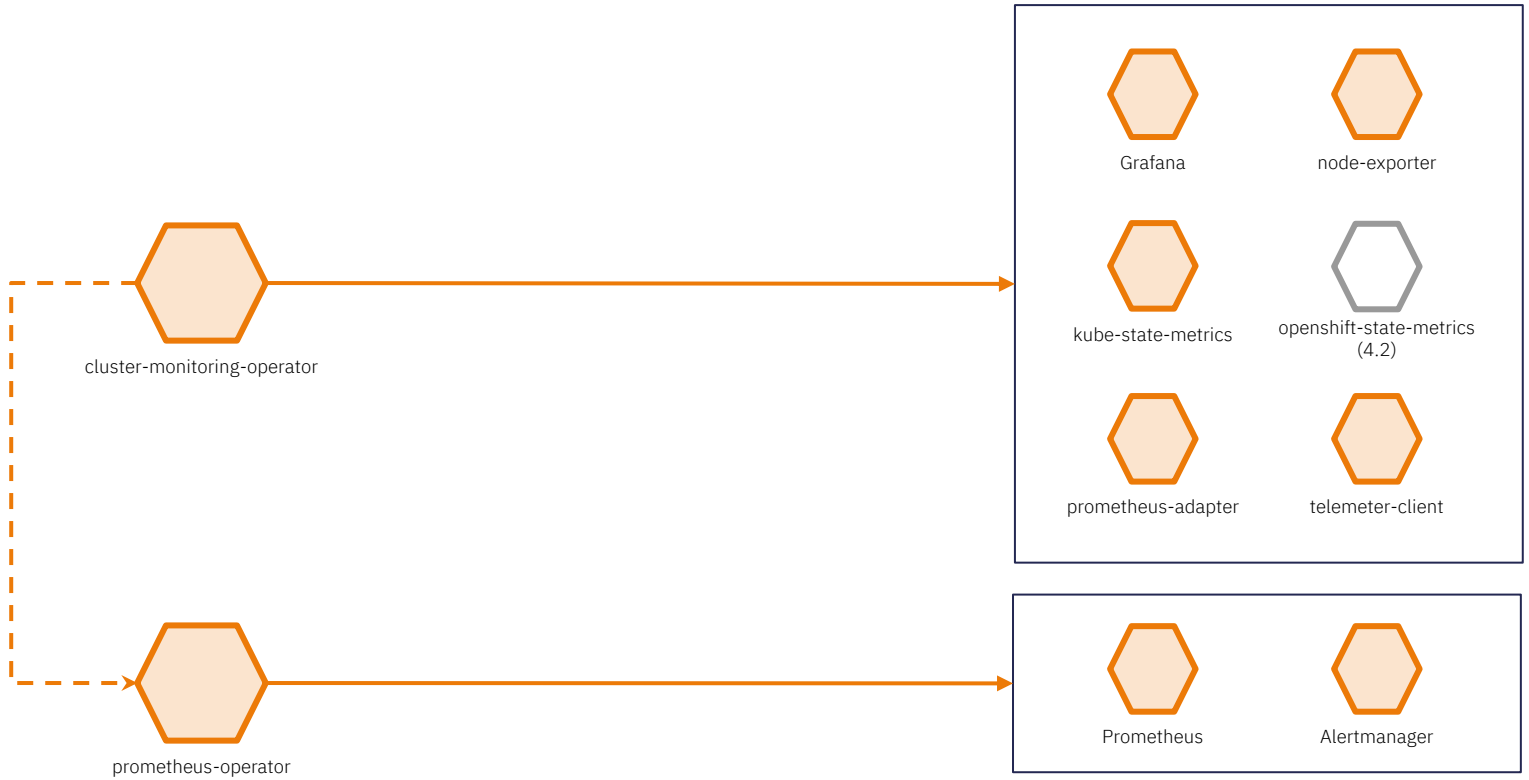
An integrated cluster monitoring and alerting stack

OpenShift Cluster Monitoring

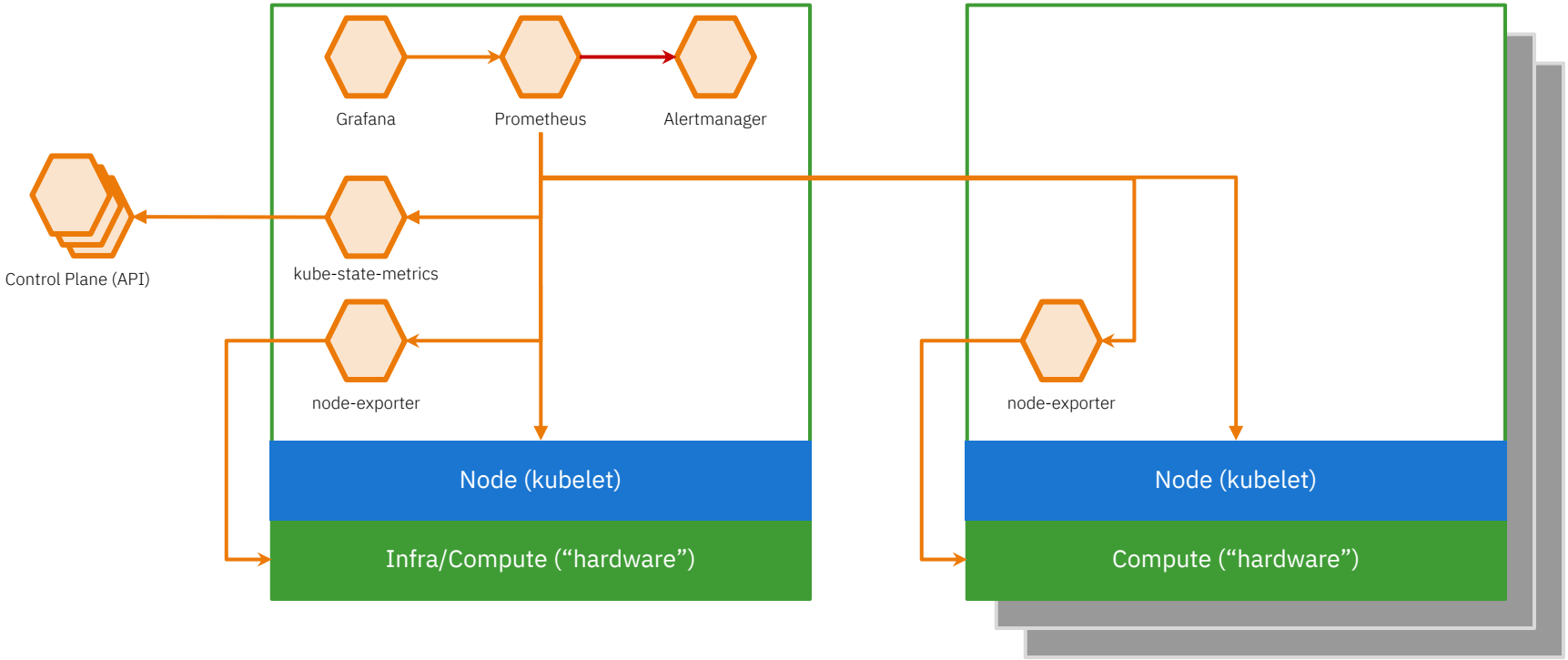
Metrics collection and storage via Prometheus, an open-source monitoring system time series database.

Alerting/notification via Prometheus' Alertmanager, an open-source tool that handles alerts send by Prometheus.

Metrics visualization via Grafana, the leading metrics visualization technology.



Monitoring relationships



The “plumbing”

OpenShift Logging

An integrated solution for exploring and corroborating application logs

Components

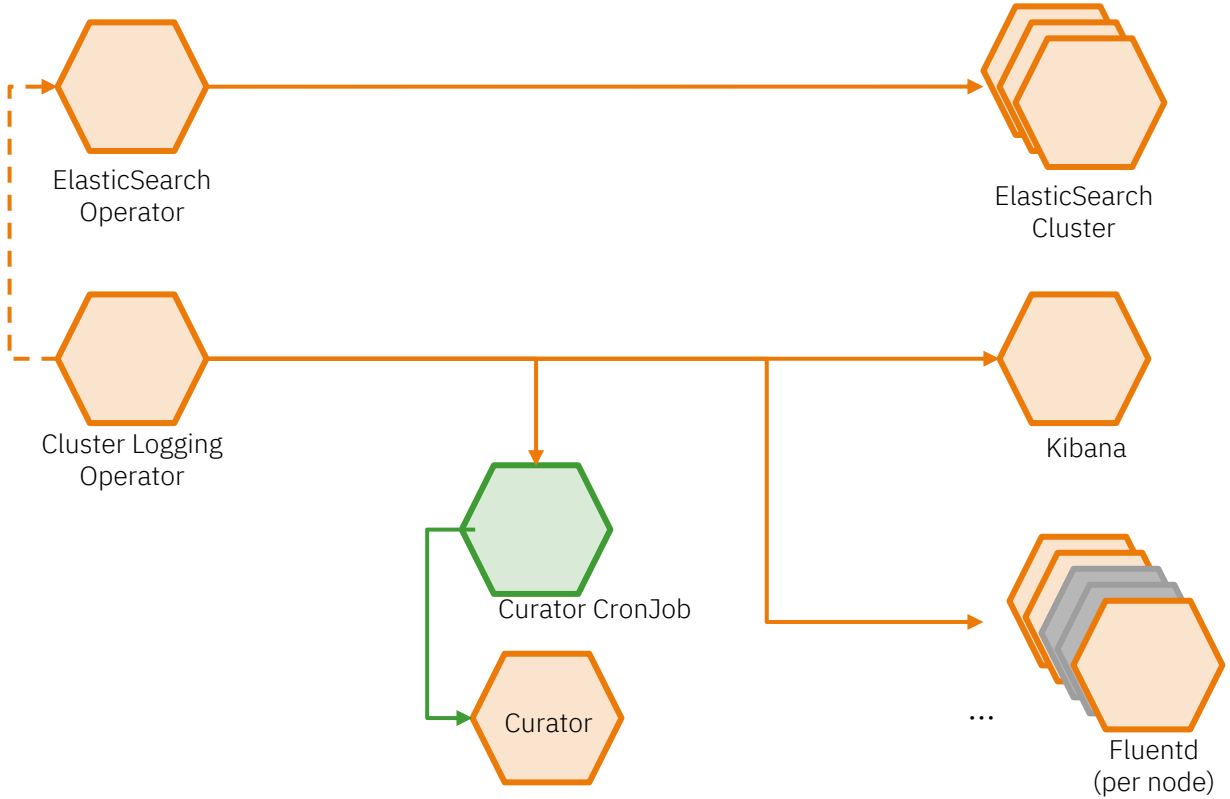
- **Elasticsearch:** a search and analytics engine to store logs
- **Fluentd:** gathers logs and sends to Elasticsearch.
- **Kibana:** A web UI for Elasticsearch.

Access control

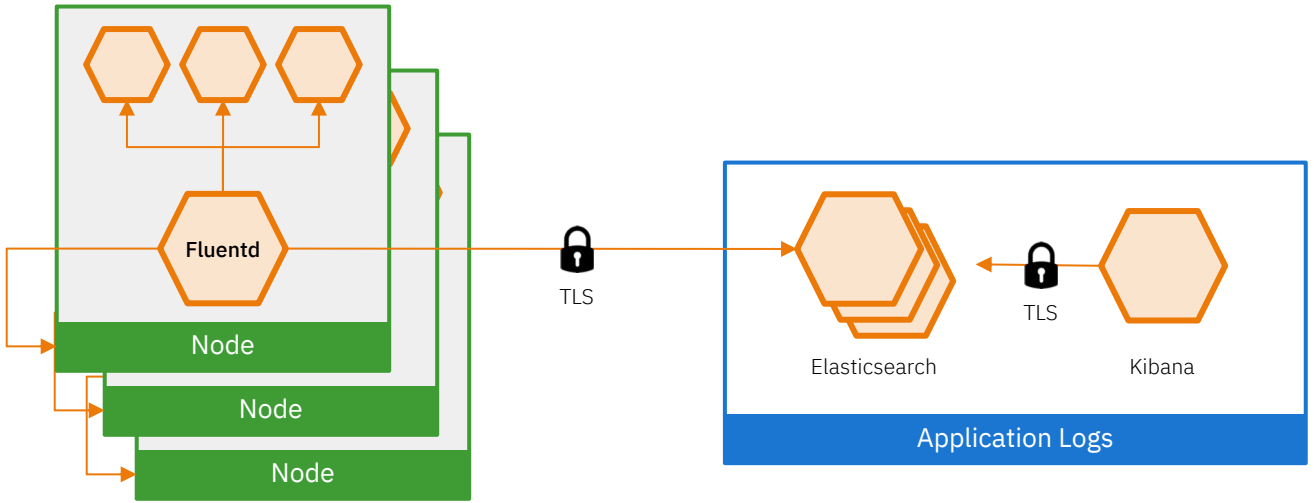
- Cluster administrators can view all logs
- Users can only view logs for their projects

Ability to forward logs elsewhere

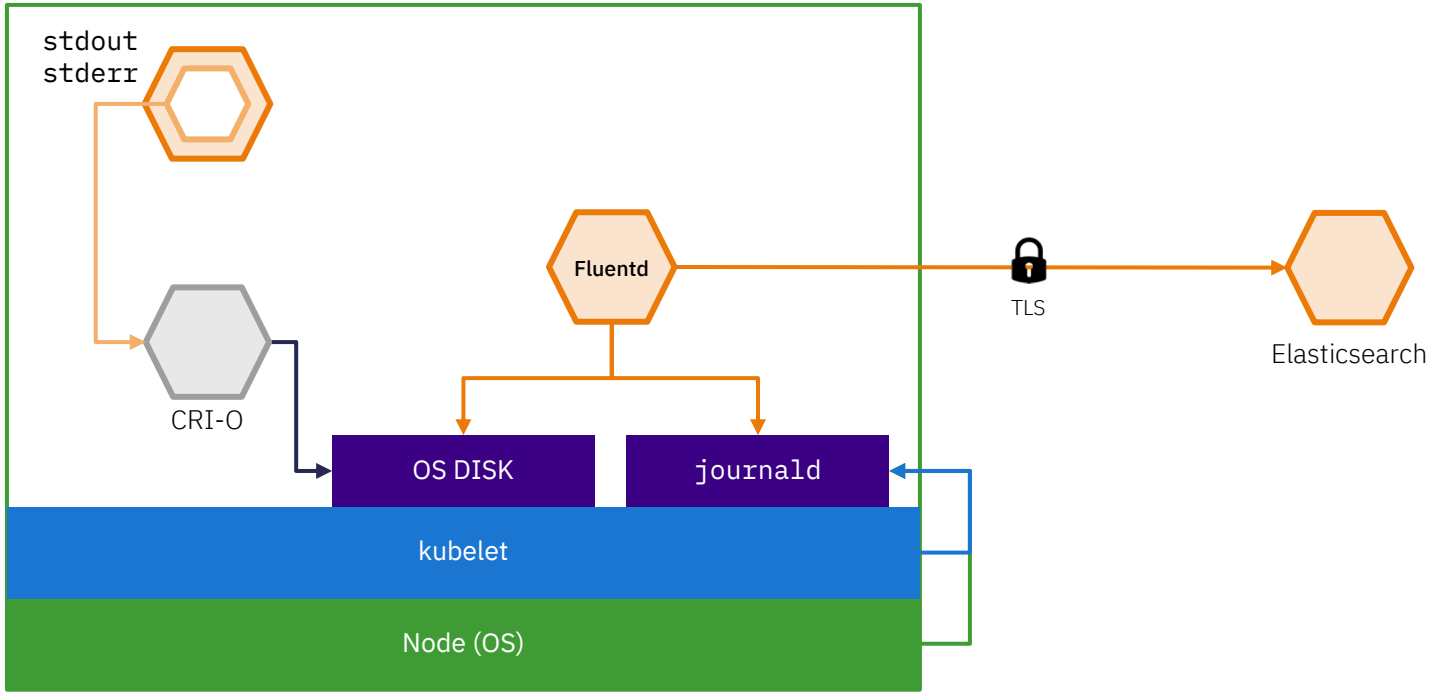
- External elasticsearch, Splunk, etc



Relationships for logging



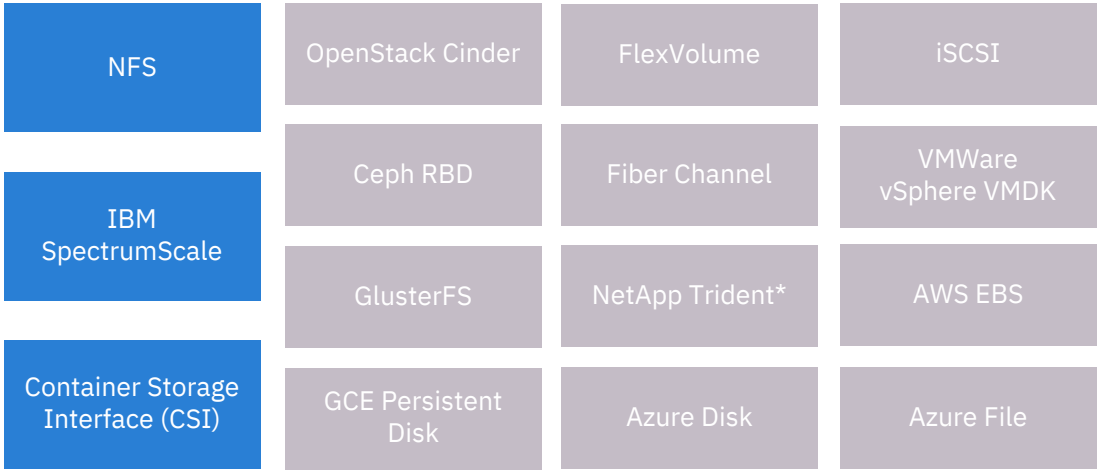
Log data flow in OpenShift



Log data flow in OpenShift

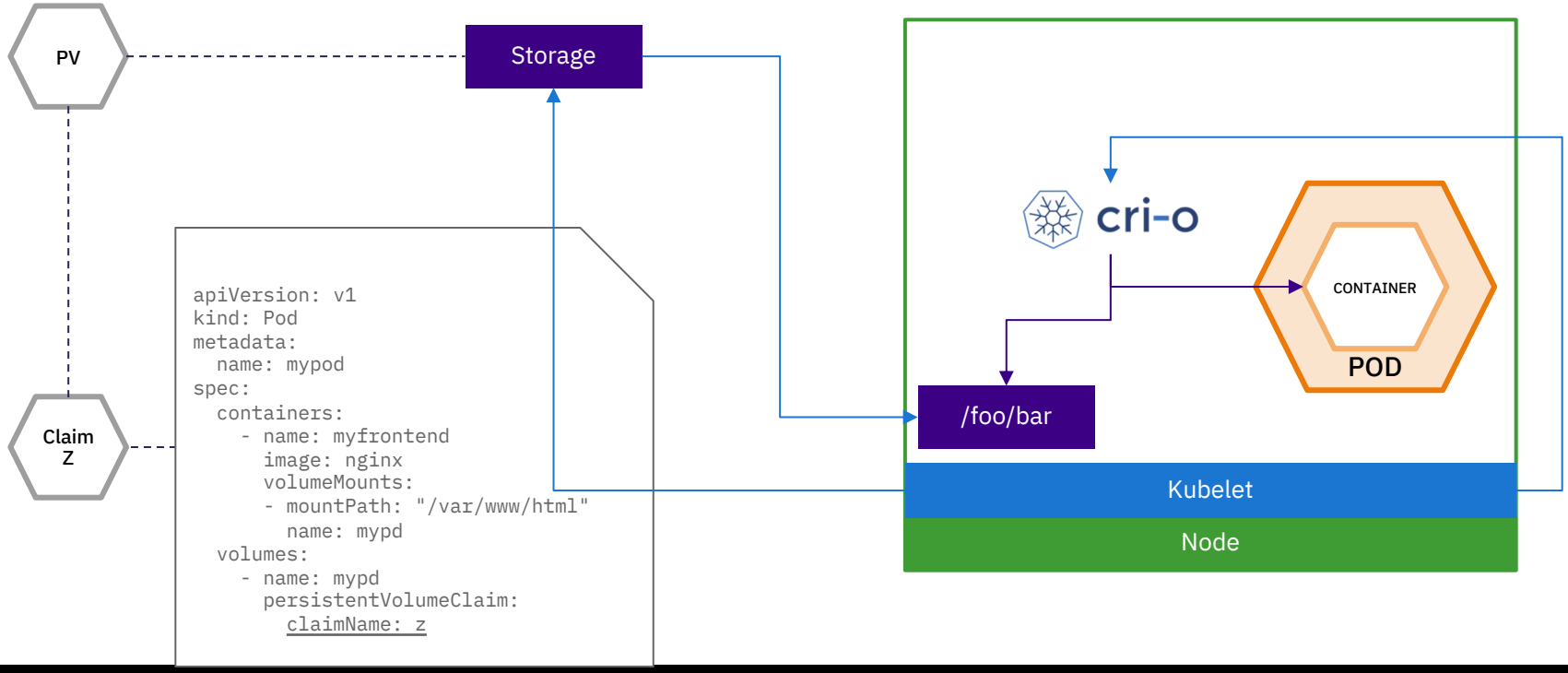
Persistent Storage

Connecting real-world storage to your containers to enable stateful applications

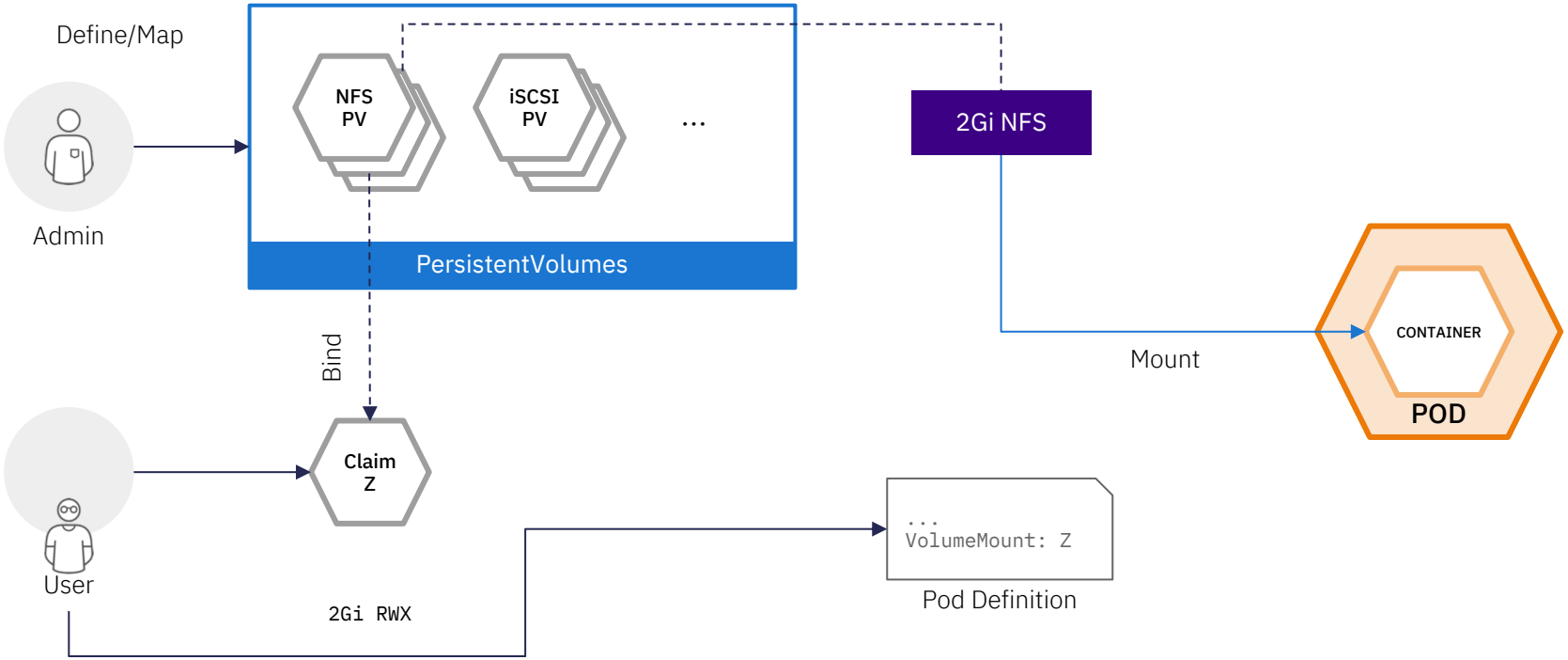


Tip: Using NFS? Don’t burden it with IPs in your exports configuration. Use the SDN firewall.

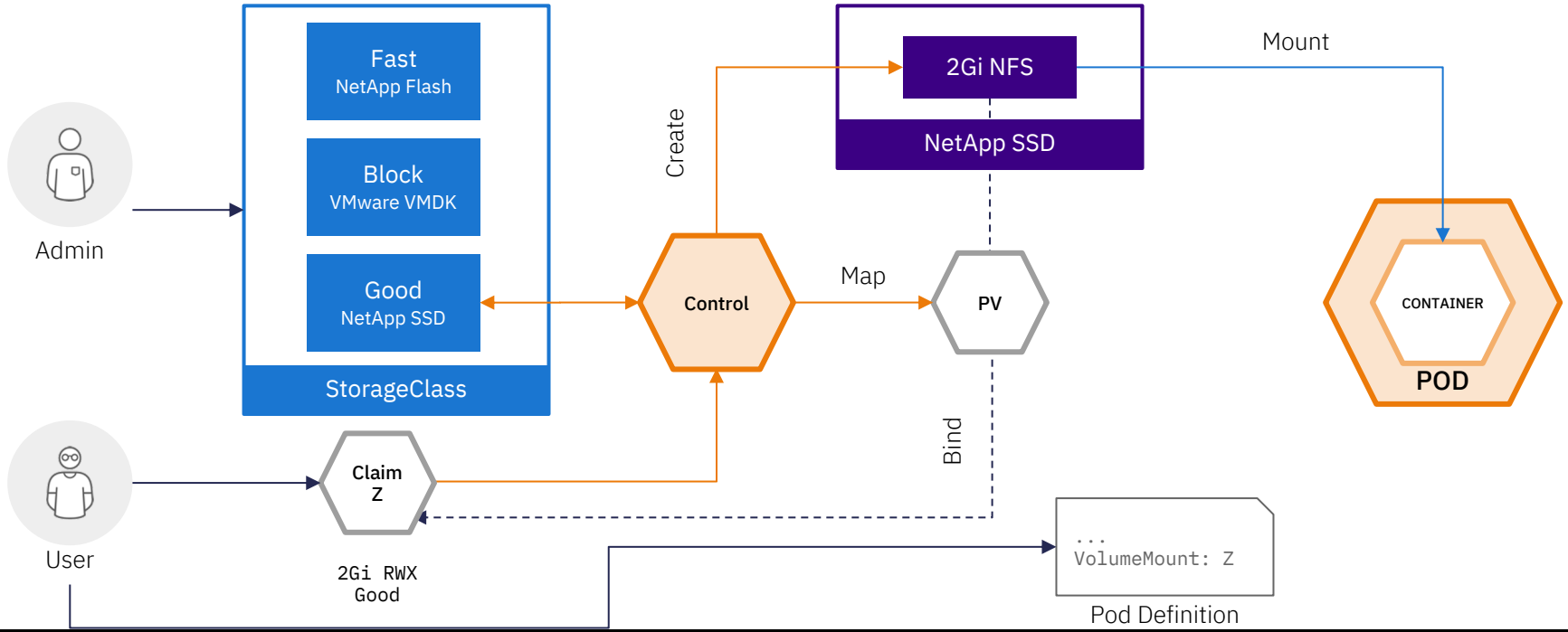
A broad spectrum of static & dynamic storage endpoints



PV Consumption



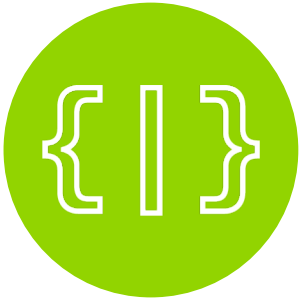
Static Storage Provisioning



Dynamic Storage Provisioning

Build and Deploy Container Images

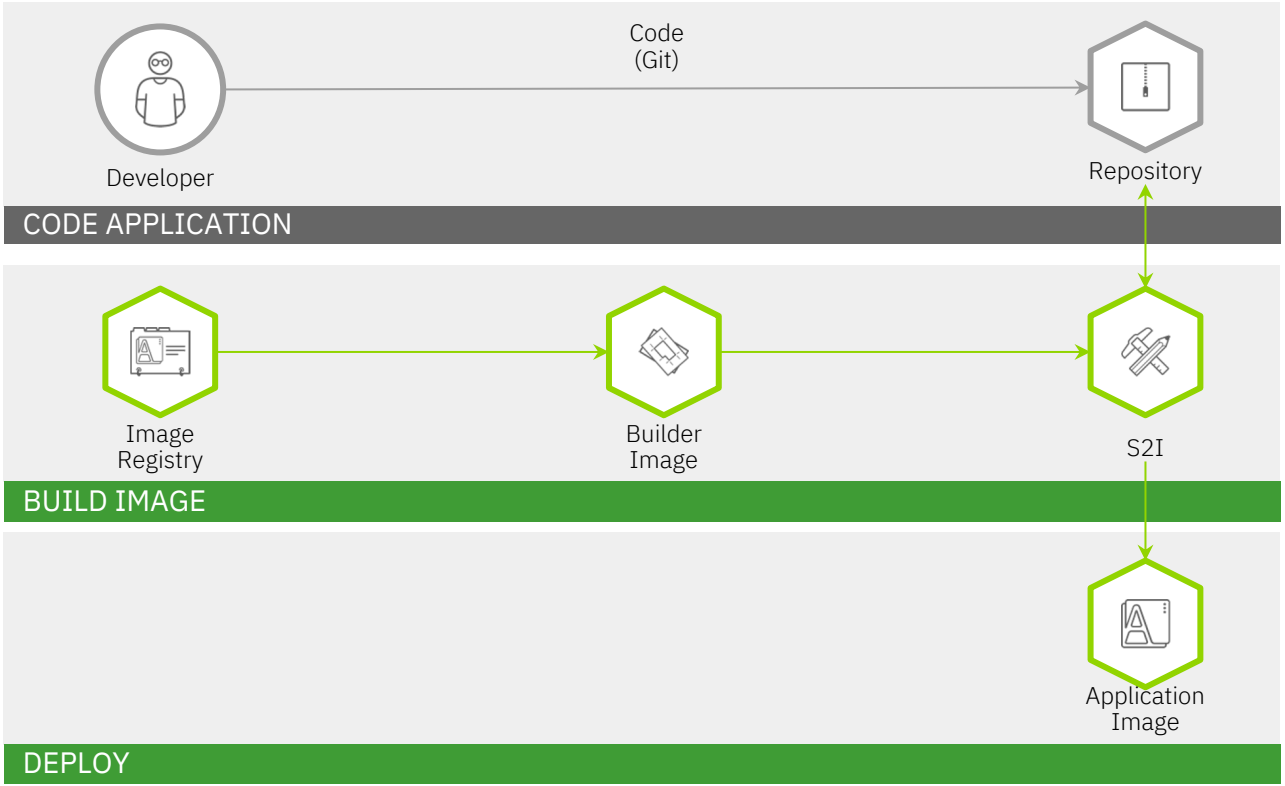
Tools and automation that makes developers productive quickly



DEPLOY YOUR SOURCE CODE

DEPLOY YOUR APP BINARY

DEPLOY YOUR CONTAINER IMAGE



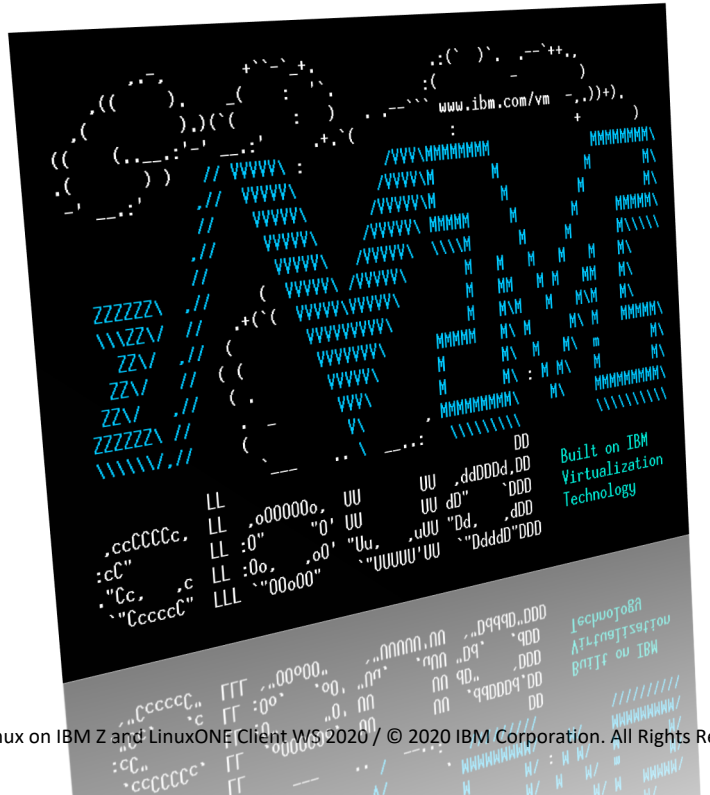
The Source-to-Image concept

Deployment considerations

- Hypervisor
  - z/VM Control Program (VM CP)
- Virtual servers
  - BANWIS / Bastion node (non-CoreOS)
  - OCP Member Nodes (running CoreOS)

- Setup
- Installation
- Configuration
- Tuning and optimization

Supported virtualization



- z/VM is the only supported virtualization hypervisor as of the current time.
- Red Hat has stated that they intend to support KVM in the future.
- If you are new to the platform and have not used either one, consider starting with z/VM:
  - Most functionally-rich with highest-density
  - Flexibility and performance
  - Easier to learn
- Be mindful of phrases with hidden undertones like “specialized skills required”
  - I/T specialists run the world, we’re not afraid of learning something new!

Setup considerations:

User experience

- ***User experience must be a primary consideration***
- OpenShift – and Kubernetes in general – were never intended to be the top of the architectural stack.
- OpenShift makes it exceptionally easy to deploy applications in a rapid fashion.
  - Unfortunately, it is also exceptionally easy to deploy applications in a manner which violates basic UXD (user experience design) principles.
- Why does any of this matter?
  - Cost, risk, and sustainability
- Needless exposure of complexity:
  - Is the enemy of productivity and user satisfaction.
  - Creates risk by encouraging undesirable user behavior.
  - Spawns additional needless workflow through supporting processes.

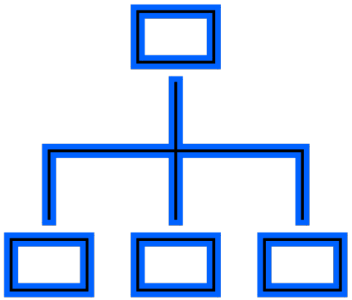
Masking complexity from users is an imperative!

Setup considerations: User experience

- Deploy an OCP cluster named ***cluster88*** in the network subdomain ***production.ciocloud.example.com***
- The cluster would operate under a cluster domain of ***cluster88.production.ciocloud.example.com***
- Applications deploy under cluster application domain of ***apps.cluster88.production.ciocloud.example.com***
- Deploy an application on this cluster named ***timecard***, in a project named ***hr-applications***, the OCP route would generate URLs that *start with* the following:
- *https://timecard-hr-applications.apps.cluster88.production.ciocloud.example.com/*
- You need governance – it is a must.
- Deploy applications with governance to ensure the messy complexity of the orchestration framework is hidden from users, and that every application is assigned a unique URI path it must remain entirely inside of.
- Never permit deployment URLs which use the server root. So I will deploy using the URL path /hr/timecard
- Why? This will not be seen by users. It needs to be served via a reverse proxy. More on that soon.
- Remember, nobody likes chaos.

considerations:

Supporting infrastructure



- Load balancing and reverse web proxy
- If you have enterprise load balancing and web proxy solutions, use them.
- If not, you will need to provide your own.
  - Load Balancer
    - Cluster address for your front-end reverse proxies.
    - Cluster addresses for your back-end OpenShift Container Platform.
  - Caching Proxy
    - Unified and consistent front-end service of Web traffic.
    - Consolidated trusted CA certificates can mean ongoing savings in the thousands of dollars.
- If you have purchased the IBM CloudPak for Applications:
  - Licensing for non-containerized IBM WebSphere Application Server Network Deployment may be included. If so, consider deploying WASND Edge Components in a High Availability model:
    - Edge Load Balancer
    - Edge Caching Proxy

considerations:

Supporting infrastructure

- BANWIS / Bastion
  - Using this as a hosting service core during a Proof of Concept is fine, but do not go into production with a single point of failure.
- If you plan to use this for NFS:
  - Create all your exports under /srv/nfs
  - Ensure you will have ample disk space and that /srv/nfs is part of an LVM.
  - Make sure you are creating full back ups of /srv/nfs frequently, and incremental backups even more so.
- If you plan to run your own DNS, you need an HA pair for production.

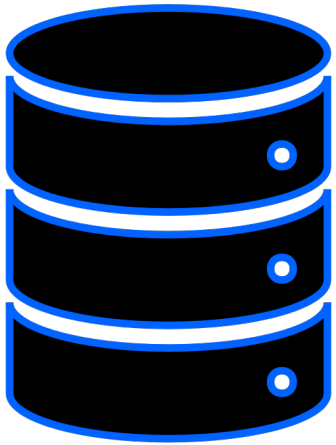
considerations:

Supporting infrastructure

- Identity and Access Management (IAM)
  - OpenShift Container platform requires a supporting IAM solution for the administrators and developers who will use and interact with it.
  - The IBM ATS/WSC team highly recommends using LDAP because it is so prevalent and well understood.
  - If you have an enterprise LDAP solution, use it. If that includes SAML integrations, even better.
  - If not, you will need to provide your own.
  - Your license for z/VM includes the z/VM LDAP server at **no additional charge**.
    - ATS/WSC highly recommends this solution also for the following reasons:
      - Extremely secure, scalable, and reliable.
      - If using RACF/VM for your ESM, the RACF LDAP connector means only one password to maintain for RACF, OCP, and Linux virtual servers.

Installation considerations:

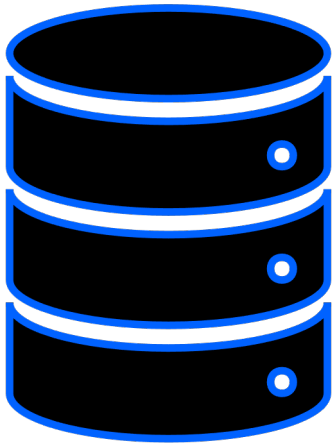
Disk



- OCP Member Nodes
- Run CoreOS as their operating system.
- Each requires at least 120 GB of disk.
  - More if deploying workload requiring extra local ephemeral disk such as blockchain.
    - Consider around 200 GB for these cases as your starting point.
- CoreOS does not use LVM. Your one and only disk must be of sufficient size.
  - Not resizable after installation
  - CoreOS multipath support for FCP/SCSI LUNs planned for the near future
  - You will need 3390-A Extended Address Volumes (EAV) plus aliases available for use.

Installation considerations:

Disk

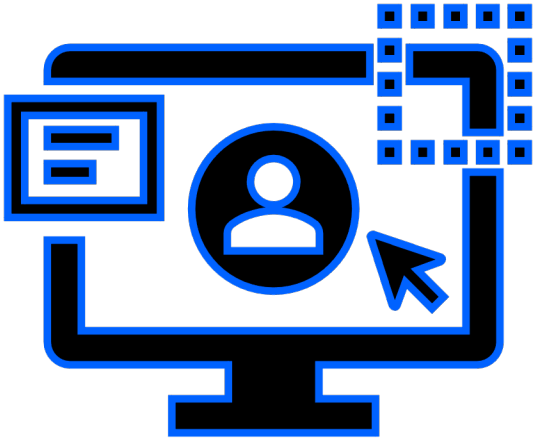


- OCP Member Nodes (continued)
- 3390-A EAV plus aliases:
  - Consider number of aliases per LPAR.
  - Keep in mind that aliases do not need to be dedicated.
  - Let z/VM virtualize the aliases.
  - Give each node 6 to 8 virtual aliases.
    - Ephemeral storage I/O intensive workloads need 8 to 10.

- BANWIS / Bastion and supporting infrastructure virtual systems
- Should follow your deployment standards for Linux virtual server
- The restrictions of CoreOS don’t apply here

Configuration considerations:

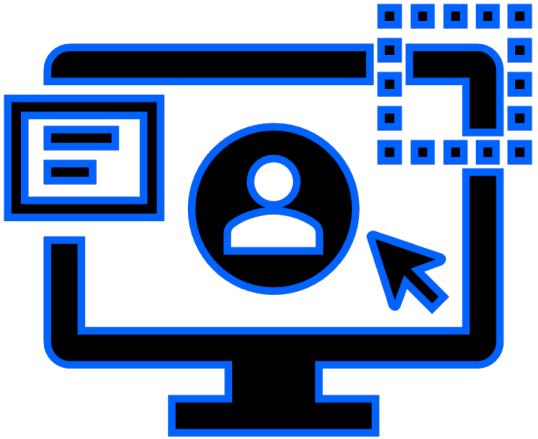
z/VM



- This is a cluster – consistency is very important.
- Consider using STP if you are not already.
- Use shared profiles in the z/VM user directory:
  - Control plane nodes.
  - Compute nodes.
  - Infrastructure (offload) nodes.
    - If or when you eventually go down this route.
- Attach minidisks as DEVNO to leverage HyperPAV.
- Memory (STORage, MAXSTORage, STANDBY) depends on node type. More on this coming up.

considerations:

z/VM shared profiles



- Again, consistency is very important.
  - Workloads are continually rebalanced.
  - In the event of a failure or maintenance, pods respawn on alternate nodes.
  - All of the nodes within the cluster should be consistent by respective type. Shared profiles are an easy way to do this.
- Examples of what shared profiles might look like are on the next two slides.

considerations:
Control plane shared profile

- Values here are shown as example only

```
PROFILE LPOCPCPN
***[ PROFILE: Linux | OCP ON Z | CONTROL PLANE NODE ]***
   CLASS G
   STORAGE 18G
   MAXSTORAGE 32G
   COMMAND DEFINE STORAGE STANDBY 6G RESERVED 0
   COMMAND SET RUN ON
   COMMAND TERM HOLD OFF
   COMMAND TERM MORE 001 000
   COMMAND SET PF12 RETR BACK
   COMMAND SET PF11 RETR FORW
   COMMAND SET VCONFIG MODE LINUX
   COMMAND DEFINE HYPERPAVALIAS A800 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A801 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A802 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A803 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A804 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A805 FOR BASE 0700
   COMMAND DEFINE CPU 00-05 TYPE IFL
   DATEFORMAT ISODATE
   IPL 190 PARM AUTOCR
   IUCV ALLOW
   IUCV ANY PRIORITY MSGLIMIT 2000
   LOGONBY HAYDEN PWNOVAK BADER MMONDICS SHALAWN
   MACHINE ESA 10
   OPTION APPLMON CHPIDV ONE
   XAUTOLOG LNCG4010 LNCG4020 LNCG4030 LNCG4030
   CONS 0009 3215 T OPMGRM1 OBSERVER
   NICDEF 0AD0 TYPE QDIO LAN SYSTEM VSWITCH3
   SPOOL 000C 2540 READER *
   SPOOL 000D 2540 PUNCH A
   SPOOL 000E 1403 A
   LINK OCPADMIN 0192 0192 RR
   LINK LNXMAINT 0191 0191 RR
```

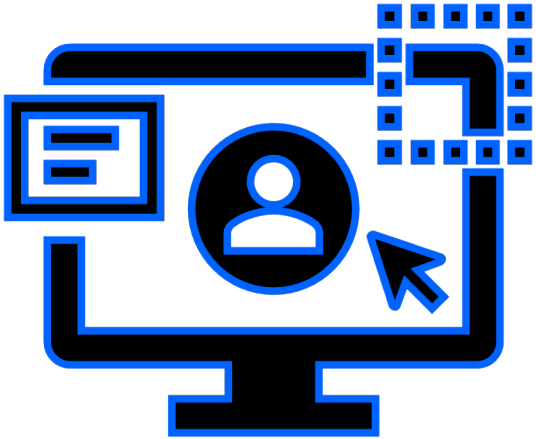
considerations:

Compute shared profile

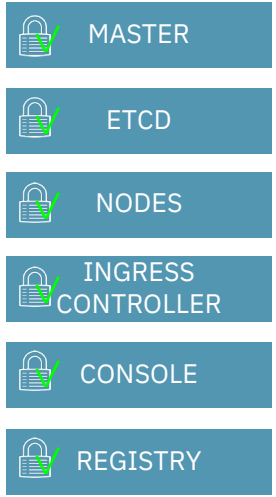
Values here are shown as example only

```
PROFILE LPOCPCON
***[ PROFILE: Linux | OCP ON Z | COMPUTE NODE ]***
   CLASS G
   STORAGE 12G
   MAXSTORAGE 64G
   COMMAND DEFINE STORAGE STANDBY 6G RESERVED 0
   COMMAND SET RUN ON
   COMMAND TERM HOLD OFF
   COMMAND TERM MORE 001 000
   COMMAND SET PF12 RETR BACK
   COMMAND SET PF11 RETR FORW
   COMMAND SET VCONFIG MODE LINUX
   COMMAND DEFINE HYPERPAVALIAS A800 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A801 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A802 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A803 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A804 FOR BASE 0700
   COMMAND DEFINE HYPERPAVALIAS A805 FOR BASE 0700
   COMMAND DEFINE CPU 00-05 TYPE IFL
   DATEFORMAT ISODATE
   IPL 190 PARM AUTOCR
   IUCV ALLOW
   IUCV ANY PRIORITY MSGLIMIT 2000
   LOGONBY HAYDEN PWNOVAK BADER MMONDICS SHALAWN
   MACHINE ESA 10
   OPTION APPLMON CHPIDV ONE
   XAUTOLOG LNCG4010 LNCG4020 LNCG4030 LNCG4030
   CONS 0009 3215 T OPMGRM1 OBSERVER
   NICDEF 0AD0 TYPE QDIO LAN SYSTEM VSWITCH3
   SPOOL 000C 2540 READER *
   SPOOL 000D 2540 PUNCH A
   SPOOL 000E 1403 A
   LINK OCPADMIN 0192 0192 RR
   LINK LNXMAINT 0191 0191 RR
```


Installation:
Certificates

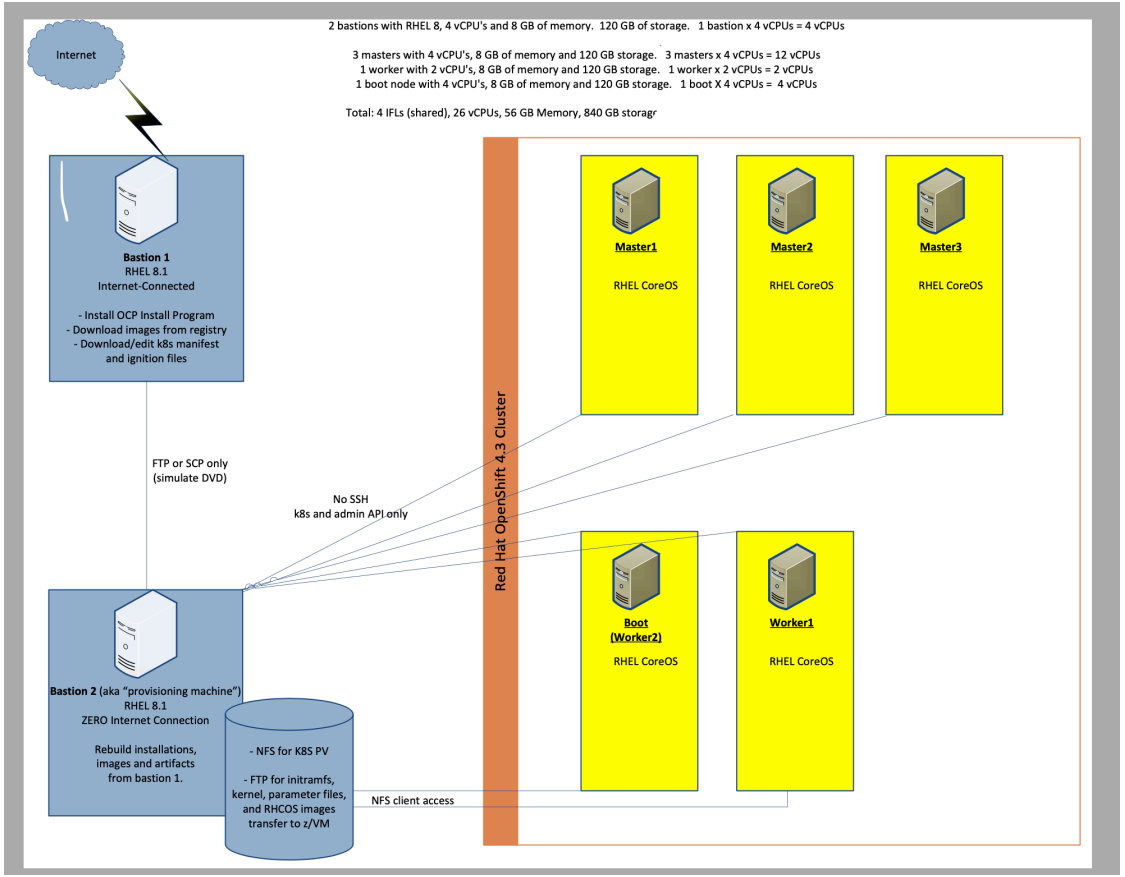


- OpenShift provides its own internal CA
- Certificates are used to provide secure connections to
  - master (APIs) and nodes
  - Ingress controller and registry
  - etcd
- Certificate rotation is automated
- Optionally configure external endpoints to use
  custom certificates
- Initial certs are good for 24 hours exactly. Rotation happens only when non-degraded though.



Installation:

Example lay



Installation:

Staging

- Collect the media, scripts, RHEL Linux repositories and container image repositories.
- Stage the oc and kubectl CLIs at /opt/openshift/4.x.x/install/ocp

```
[root@DHCODBN1(192.168.46.140) /opt/openshift/4.3.19/install/ocp [14:13:08] (0)]# ll
total 588960
-rwxr-xr-x 2 root root  84063376 May  4 08:37 kubectl-1.12.12
-rwxr-xr-x 2 root root  84063376 May  4 08:37 oc-4.3.19
-rw-r--r-- 1 root root  27122795 May  4 08:37 openshift-client-linux-4.3.19.tar.gz
lrwxrwxrwx 1 root root        36 May 11 12:45 openshift-cli-s390x -> openshift-client-linux-4.3.19.tar.gz
lrwxrwxrwx 1 root root        24 May 11 17:19 openshift-install -> openshift-install-4.3.19
-rwxr-xr-x 1 root root 326971520 May  4 08:46 openshift-install-4.3.19
-rw-r--r-- 1 root root  80856106 May  4 08:46 openshift-install-linux-4.3.19.tar.gz
lrwxrwxrwx 1 root root        37 May 11 12:46 openshift-install-s390x -> openshift-install-linux-4.3.19.tar.gz
-rw-r--r-- 1 root root       706 May  4 08:46 README.md
```

Installation:

Subscription

- RHEL Linux repositories
- If a Red Hat Satellite server is available to you in your air-gapped network, these steps, and the corresponding steps to stage these mirrored repositories on bastion2, should not be required. We did not have access to a Red Hat Satellite server in the air-gapped environment that we performed this test installation in.
- Apply your subscription:
- subscription-manager attach --pool=.....
- Successfully attached a subscription for: Red Hat OpenShift Container Platform Broker/Master Infrastructure
- Use reposync to download the repository contents:
- reposync --download-metadata --download-path=/opt/media --arch=s390x --repoid=rhel-8-for-s390x-appstream-rpms

Installation:

Subscription

```
dnf repolist
Updating Subscription Management repositories.
repo id                                                 repo name
RHEL8-AppStream                                         RHEL 8 - s390x - AppStream Updates
RHEL8-BaseOS                                                    RHEL 8 - s390x - BaseOS Updates
RHEL8-Supplementary                                             RHEL 8 - s390x - Supplementary
Updates
RHEL81-AppStream                                                RHEL 8.1 - s390x - AppStream
RHEL81-BaseOS                                                   RHEL 8.1 - s390x - BaseOS
Repos                                                           Repos
epel8                                                           Extra Packages for Enterprise Linux
8 - s390x
reposync --download-metadata --download-path=/opt/media --arch=s390x --repoid=RHEL8-BaseOS
reposync --download-metadata --download-path=/opt/media --arch=s390x --repoid=RHEL8-AppStream
reposync --download-metadata --download-path=/opt/media --arch=s390x --repoid=RHEL81-AppStream
reposync --download-metadata --download-path=/opt/media --arch=s390x --repoid=epel8

Needed to specify both the --arch=s390x as well as --arch=noarch
reposync --download-metadata --download-path=/opt/media --arch=noarch --repoid=RHEL8-BaseOS
reposync --download-metadata --download-path=/opt/media --arch=noarch --repoid=RHEL8-AppStream
reposync --download-metadata --download-path=/opt/media --arch=noarch --repoid=RHEL81-AppStream
reposync --download-metadata --download-path=/opt/media --arch=noarch --repoid=epel8

repomanage --old --keep 3 /opt/media | xargs rm -f '{}'
```

Installation:

Local repo

- Setting up docker local repository on bastion1:
-
- dnf install skopeo
- cd /opt/media
- cat mirror.sh
- #!/bin/bash -xe
- export OCP_RELEASE=4.3.19-s390x
- export LOCAL_REGISTRY='localhost:5000'
- export LOCAL_REPOSITORY='ocp4/openshift4'
- export PRODUCT_REPO='openshift-release-dev'
- export LOCAL_SECRET_JSON='/opt/openshift/4.3.19/data/.ocp4_pull_secret'
-
- # If using a nightly build, set to ocp-release-nightly
- export RELEASE_NAME="ocp-release"
-
- oc adm -a ${LOCAL_SECRET_JSON} release mirror \
- --insecure=true \
- --from=quay.io/${PRODUCT_REPO}/${RELEASE_NAME}:${OCP_RELEASE} \
- --to=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY} \
- --to-release-image=${LOCAL_REGISTRY}/${LOCAL_REPOSITORY}:${OCP_RELEASE}

installation:

Local pulls – not as root!

- `podman login registry.redhat.io`
- `skopeo copy docker://registry.redhat.io/openshift4/ose-docker-registry:v4.3 docker-archive:ose-docker-registry.v43.tar`
- `Getting image source signatures`
- `Copying blob b4e5f67d58c2 done`
- `.....`
- `Writing manifest to image destination`
- `Storing signatures`
- `skopeo copy docker-archive:ose-docker-registry.v43.tar containers-storage:registry.redhat.io/openshift4/ose-docker-registry:v4.3`
- `podman images`
- `REPOSITORY TAG IMAGE ID CREATED SIZE`
- `registry.redhat.io/openshift4/ose-docker-registry v4.3 d90d518cf6bc 7 days ago 337 MB`

Installation:

Local mirror

- mirror.sh
- + export OCP_RELEASE=4.3.19-s390x
- + OCP_RELEASE=4.3.19-s390x
- + export LOCAL_REGISTRY=localhost:5000
- + LOCAL_REGISTRY=localhost:5000
- + export LOCAL_REPOSITORY=ocp4/openshift4
- + LOCAL_REPOSITORY=ocp4/openshift4
- + export PRODUCT_REPO=openshift-release-dev
- + PRODUCT_REPO=openshift-release-dev
- + export LOCAL_SECRET_JSON=/opt/openshift/4.3.19/data/.ocp4_pull_secret
- + LOCAL_SECRET_JSON=/opt/openshift/4.3.19/data/.ocp4_pull_secret
- + export RELEASE_NAME=ocp-release
- + RELEASE_NAME=ocp-release
- + oc adm -a /opt/openshift/4.3.19/data/.ocp4_pull_secret release mirror --insecure=true --from=quay.io/openshift-release-dev/ocp-release:4.3.19-s390x --to=localhost:5000/ocp4/openshift4 --to-release-image=localhost:5000/ocp4/openshift4:4.3.19-s390x
- info: Mirroring 102 images to localhost:5000/ocp4/openshift4 ...
- localhost:5000/
- ocp4/openshift4
- blobs:
- quay.io/openshift-release-dev/ocp-release sha256:e1fef3d17a441646551dda3114f3c491445d954025711546147f3d7f720a14e8 1.604KiB
- info: Mirroring completed in 2m8.12s (30.86MB/s)

Installation:
Local mirror

- To use the new mirrored repository to install, add the following section to the install-config.yaml:
-
- ```
  imageContentSources:
  - mirrors:
    - localhost:5000/ocp4/openshift4
    source: quay.io/openshift-release-dev/ocp-release
  - mirrors:
    - localhost:5000/ocp4/openshift4
    source: quay.io/openshift-release-dev/ocp-v4.0-art-dev
  ```
- To use the new mirrored repository for upgrades, use the following to create an ImageContentSourcePolicy:
-
- ```
  apiVersion: operator.openshift.io/v1alpha1
  kind: ImageContentSourcePolicy
  metadata:
    name: example
  spec:
    repositoryDigestMirrors:
    - mirrors:
      - localhost:5000/ocp4/openshift4
      source: quay.io/openshift-release-dev/ocp-release
    - mirrors:
      - localhost:5000/ocp4/openshift4
      source: quay.io/openshift-release-dev/ocp-v4.0-art-dev
  ```

Installation:
What's next?

- It's the usual process from here. This entire process is covered in more detail in the IBM TechDocs Whitepaper from the WSC entitled

Linux containers and virtualization on IBM Z™ and LinuxONE™

Getting Started with Red Hat OpenShift™ Container Platform version 4 under z/VM on IBM Z™ and LinuxONE™

- Linux containers

- Kubernetes
- https://kubernetes.io/docs/tutorials/kubernetes-basics/

- IBM Cloud Paks
  - Cloud Pak for Applications
- https://www.ibm.com/demos/collection/Cloud-Pak-for-Applications/

- Red Hat OpenShift

IBM Washington Systems Center / ATS Americas

Our mission is to provide world-class subject matter expertise to IBM marketing and sales teams for the sale, design, sizing, implementation, optimization, and support of client solutions built on hardware, software, and services offerings from the IBM Storage, Spectrum Storage, Z, and LinuxONE brands.

This includes direct-to-field technical sales support, enablement, and development of the capacity, performance, and sizing (CPS) applications for z/Architecture systems.

Additionally, we provide no-charge knowledge transfer and skills enablement workshops and webinars to IBM customers seeking to enhance their knowledge of hardware, software, and services offerings from IBM Storage, Spectrum, Z, and LinuxONE. Contact your IBM representative to request enrollment in any of these workshops. Details can be found at the following URLs:

Accelerate with IBM Storage workshop series:
www.ibm.com/support/pages/washington-systems-center-accelerate-ibm-storage-technical-webinar-series

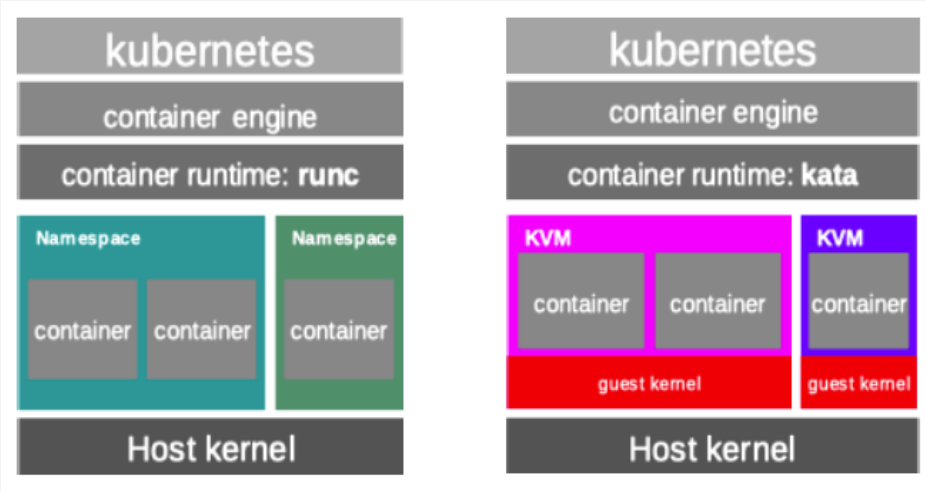
Wildfire workshop series for Z and LinuxONE hardware and software:
www.ibm.com/support/pages/node/6354049

Capabilities

- **Use Case Planning**
  - What do you want to do in the environment?
- **Pre-installation**
  - Infrastructure, architecture, and capability planning
- **Installation**
  - OpenShift, Cloud Paks, z/VM hypervisor, Disk, Networking, DNS, LDAP, optional extras
- **Post-Installation**
  - Advice on administrating and developing on the platform, setting up image registry, installing CLI, etc...

Kata Containers
The Speed of Containers, the Security of VMs

- Run containers inside a virtual machine to improve isolation
- Released end of December 2017, IBM Z support at the end of 2018
- Licensed under OpenStack Foundation and Apache 2.0 licenses
- Support for main container engines: Docker, cri-containerd, cri-o and Podman
- Support for Kubernetes
- Available via Snap
- No modifications of existing tools
- It can be used in parallel to standard containers



Questions so far?

Connect to the ATS/WSC lab network

1 Determine if Cisco® AnyConnect® is already installed on your system.

If it is, you should be able to locate and launch ***Cisco AnyConnect Secure Mobility Client*** under the *MacOS® Launchpad™*, Linux™ GUI menus, or *Windows® Start Menu™*. If not installed, visit `https://ssl.wsc.ihost.com` with your web browser. Log in using the VPN ID and password in step 3 below. You will be prompted to install software.

2 Launch the AnyConnect client and connect.

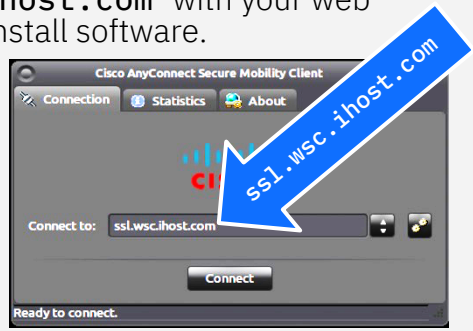
In the ***Connect to*** field, select `ssl.wsc.ihost.com` from the dropdown menu and click the **Connect** button. If ssl.wsc.ihost.com is not in the dropdown list, type it in manually.

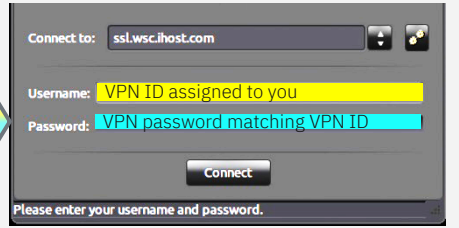
3 Log in using the VPN ID and associated password assigned to you.

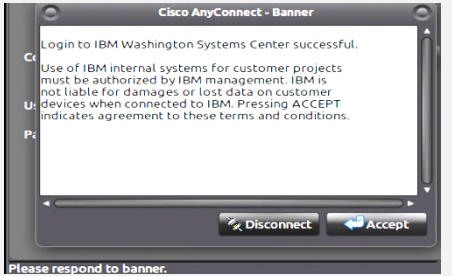
In the ***Username*** and ***Password*** fields, input the VPN ID and associated password beside your name in the table below. Click **Connect** , then **Accept** after reviewing the terms.

Participant	VPN ID	VPN Password
Ayers	vmsc01	hv=d+01Z
Schulz	vmsc02	hv=d+02Z
Fuller	vmsc03	hv=d+03Z
Hinckle	vmsc04	hv=d+04Z
Packer	vmsc05	hv=d+05Z
Brown	vmsc06	hv=d+06Z
Stoker	vmsc07	hv=d+07Z
Albitar	vmsc08	hv=d+08Z
Rane	vmsc09	hv=d+09Z
Mulvenna	vmsc10	hv=d+10Z
Swenson	vmsc11	hv=d+11Z
Kamel	vmsc12	hv=d+12Z
Sadanandam	vmsc13	hv=d+13Z
Smith	vmsc14	hv=d+14Z
Krakkus	vmsc15	hv=d+15Z
Tesla	vmsc16	hv=d+16Z

Participant	VPN ID	VPN Password
Atallah	vmsc17	hv=d+17Z
Ibrahim	vmsc18	hv=d+18Z
Rodolfi	vmsc19	hv=d+19Z
Tonia	vmsc20	hv=d+20Z
Conrad	vmsc21	hv=d+21Z
Giuliano	vmsc22	hv=d+22Z
Radaci	vmsc23	hv=d+23Z
Gunjal	vmsc24	hv=d+24Z
Rose	vmsc25	hv=d+25Z
Poppy	vmsc26	hv=d+26Z
Thorne	vmsc27	hv=d+27Z
Hawker	vmsc28	hv=d+28Z
Kramper	vmsc29	hv=d+29Z
Schprittzer	vmsc30	hv=d+30Z
Schleiden	vmsc31	hv=d+31Z
Schwann	vmsc32	hv=d+32Z



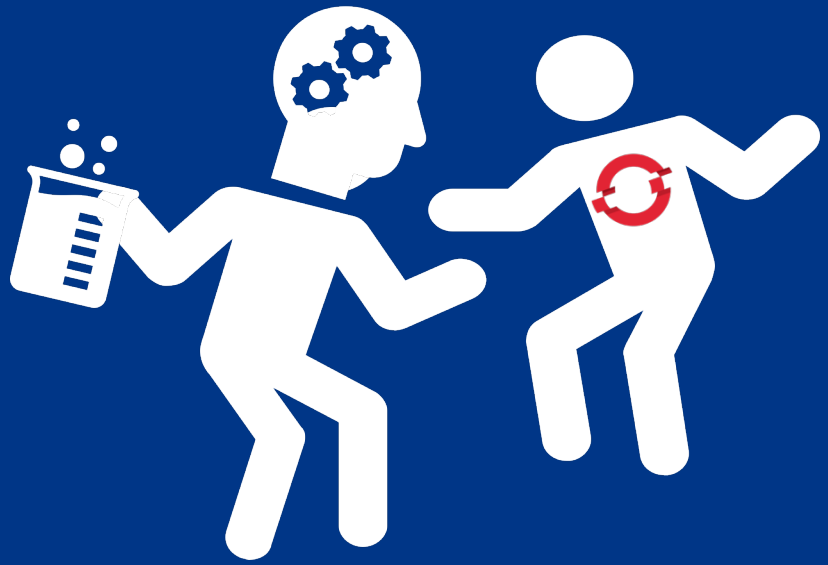




* **The VPN ID and password are *not* used for OpenShift!** See lab guide for details.

Workshop materials are available online at `http://ibm.biz/wildfire-cloudpaks-ocp`

Live demonstration



A proven way of introducing or supplementing knowledge of Mainframe systems technologies, each workshop delivers a series of lecture and labs that demonstrate how the cutting-edge, industry-leading IBM Z and LinuxONE systems can solve business problems in many different ways.

The workshops are *no-charge* to qualified customers. Details about the workshops we offer are outlined on IBM.com at:
http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS1778

Enroll today by contacting your IBM representative!

Additional information and where you can learn more

Where to find more information

Linux containers

Kubernetes

- https://kubernetes.io/docs/tutorials/kubernetes-basics/

IBM Cloud Paks

- Cloud Pak for Applications

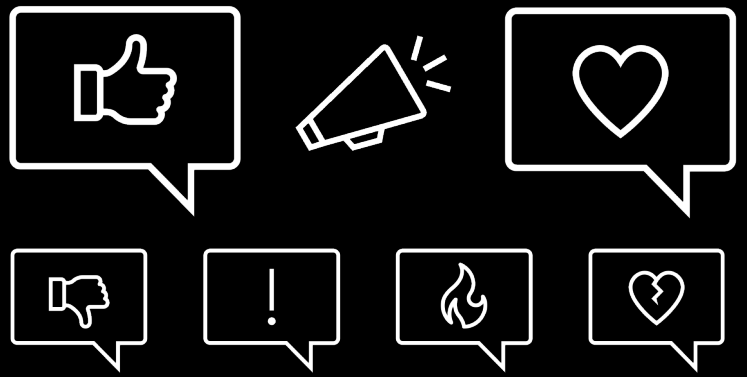
https://www.ibm.com/demos/collection/Cloud-Pak-for-Applications/

Red Hat OpenShift

Thanks for attending!

We kindly ask that you complete a survey before you depart.

Your opinion matters!



Feedback and comments are used to justify this no-charge Wildfire Workshop Series, shape the content to be most meaningful to you, and help us determine future topics.

Please let us know what you thought about today's workshop. Your feedback is greatly valued, especially written comments regarding any value the content will bring to you and your organization.

A very brief survey is available at the link below. Please be sure to click submit after you complete the survey. Thank you for attending!

https://survey.ibm-zcouncil.com/limesurvey/index.php/756758

Paul Novak
Senior IT Specialist
z/VM, Linux, Containers, Cloud

Washington Systems Center (ATS)
IBM Global Markets

Endicott – The Birthplace of IBM
1701 North Street
Endicott, NY 13760 USA

Tel +1 607 429 6186
pwnovak@us.ibm.com

Matt Mondics
Advisory IT Specialist
Private Cloud, Z and LinuxONE

Washington Systems Center (ATS)
IBM Global Markets

10500 Cedar Avenue
Cleveland, OH 44106 USA

Tel +1 614 551 7720
matt.mondics@ibm.com

Washington Systems Center
Advanced Technical Sales Support

www.ibm.com/support/techdocs

