OpenShift Lifecycle update

- Time Is On Your Side: A Change to the OpenShift 4 Lifecycle
- Red Hat OpenShift Container Platform Life Cycle Policy

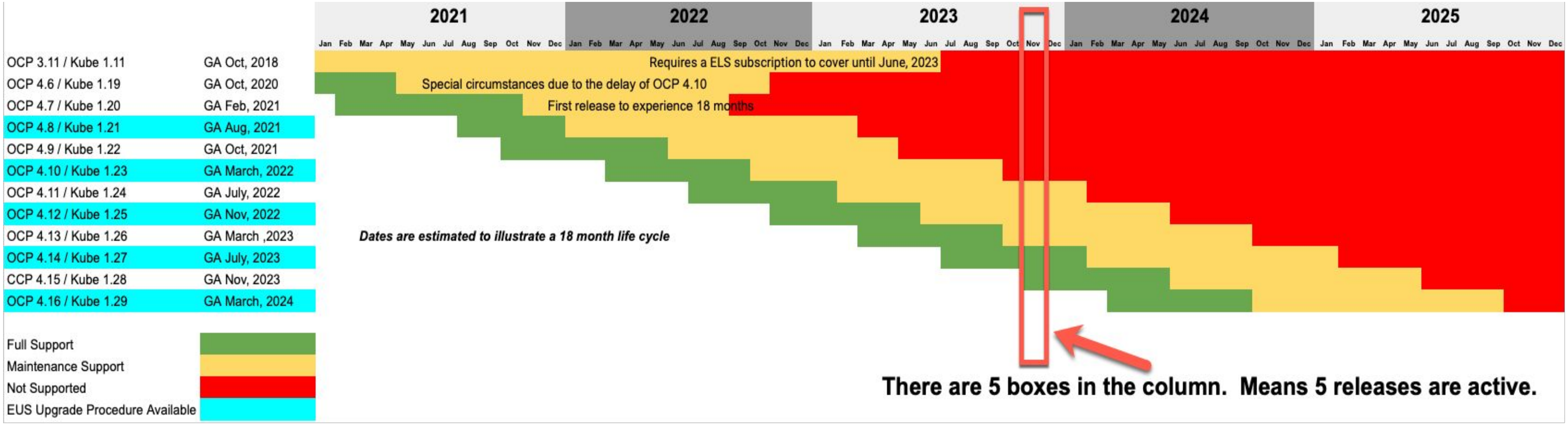
OpenShift Lifecycle Announcement

18.10'21

	Vor OpenShift 4.7	Neuerung ab OpenShift 4.7
OpenShift Lifecycle	~ 9 - 12 Monate Full- & Maintenance-Support	18 Monate Full- & Maintenance-Support
EUS	● Nur 4.6[1] mit Blick auf 4.10 ● Premium Subscription vorausgesetzt	Für alle geraden Releases ab 4.8
Upgrades	Jedes Minor-Release	Verlängerte Frist und Beschleunigung durch EUS >>> EUS
Timelines	Releasezyklen zu kurz	Planungssicherheit durch festgelegte Releasezyklen
Optimierung	Gehäufte Upgrades mussten in der Planung berücksichtigt werden	Schnellere Upgrades mit weniger Neustarts der OpenShift-Systeme

[1] OCP 4.6 ist heute die einzige EUS-Version, die bereits eine genehmigte und öffentlich dokumentierte Verlängerung des Lifecycles auf 24 Monate aufweist.
EUS = Extended Update Support

Die Bedeutung des Announcements für die Releaseplanung



OCP 3.11 / Kube 1.11	GA Oct, 2018
OCP 4.6 / Kube 1.19	GA Oct, 2020
OCP 4.7 / Kube 1.20	GA Feb, 2021
OCP 4.8 / Kube 1.21	GA Aug, 2021
OCP 4.9 / Kube 1.22	GA Oct, 2021
OCP 4.10 / Kube 1.23	GA March, 2022
OCP 4.11 / Kube 1.24	GA July, 2022
OCP 4.12 / Kube 1.25	GA Nov, 2022
OCP 4.13 / Kube 1.26	GA March ,2023
OCP 4.14 / Kube 1.27	GA July, 2023
CCP 4.15 / Kube 1.28	GA Nov, 2023
OCP 4.16 / Kube 1.29	GA March, 2024

Requires a ELS subscription to cover until June, 2023

Special circumstances due to the delay of OCP 4.10

First release to experience 18 months

Dates are estimated to illustrate a 18 month life cycle

Full Support	🟩
Maintenance Support	🟨
Not Supported	🟥
EUS Upgrade Procedure Available	🟦

There are 5 boxes in the column. Means 5 releases are active.

Source: https://cloud.redhat.com/blog/time-is-on-your-side-a-change-to-the-openshift-4-lifecycle

What’s New in OpenShift 4.9

OpenShift 4.9

INSTALLER FLEXIBILITY

Single Node UPI is GA

RHEL8 Worker & Infra Nodes

Azure Stack Hub using UPI

Bring your own Windows nodes

Kubernetes 1.22 & CRI-O 1.22

IMPROVED SECURITY

Shorter etcd TLS expiry + rotation

User customizable audit policy

mTLS: Ingress & Serverless↔Mesh

FIPS: ACM, Virtualization, & Sandboxed Containers

NEXT-GEN DEVELOPER TOOLS

Automatic RHEL entitlements

Certified Helm charts in Console

UI for GitOps pipelines as code

Custom domains for Serverless

Kubernetes 1.22

Major Themes and Features

- API deprecation
  - Affects many popular APIs (beta→stable)
  - Marked as deprecated for many releases, finally removed
- CSI for Windows nodes is GA
- Secure by default
  - New built-in admission controller replaces PodSecurityPolicy
  - PSP slated for removal in 1.25
  - CIS guidelines still call for using PSPs
  - OpenShift's SCCs are unaffected

CRI-O
1.22

Kubernetes
1.22

OpenShift
4.9

Blog: https://cloud.redhat.com/blog/whats-new-in-kubernetes-v1.22

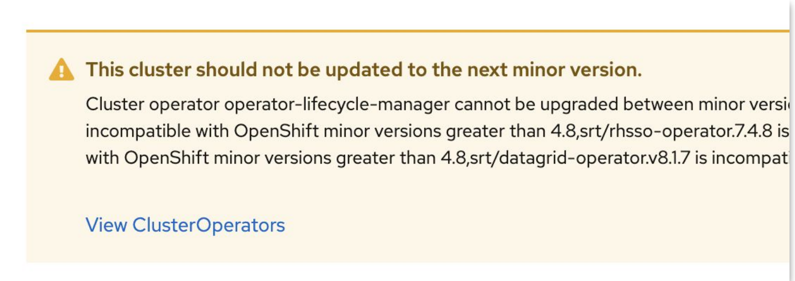
API Removal and Upgrade Behavior

Affected APIs

- CRD (beta→stable)
- CertificateSigningRequest (beta→stable)
- Mutating/ValidatingAdmissionWebhook (b→s)
- Full list and more details

Operators

- Change affects Operators that still use a beta CRD
- Partners and layered products have been audited and notified of updates they require
- Operators installed in 4.8 that do not have a compatible 4.9 release will block cluster upgrade

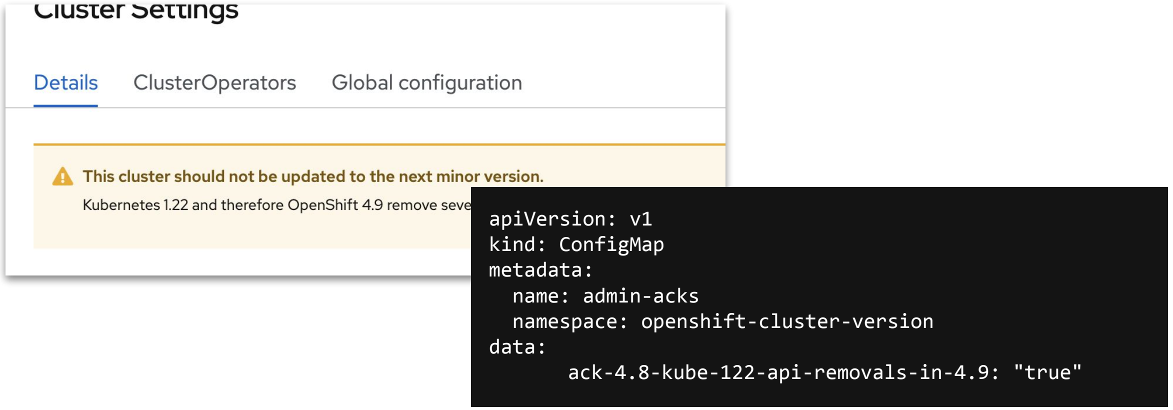


This cluster should not be updated to the next minor version.

Cluster operator operator-lifecycle-manager cannot be upgraded between minor versi
incompatible with OpenShift minor versions greater than 4.8,srt/rhsso-operator.7.4.8 is
with OpenShift minor versions greater than 4.8,srt/datagrid-operator.v8.1.7 is incompat

Confirming API usage during upgrade

- External software interacting with a cluster may use deprecated APIs.
- To prevent breakage, an admin will acknowledge external software has been updated prior to cluster upgrade
- This "ack" is a boolean on a ConfigMap
- We expect to use this functionality for similar changes of this magnitude in the future



This cluster should not be updated to the next minor version.

Kubernetes 1.22 and therefore OpenShift 4.9 remove seve

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: admin-acks
  namespace: openshift-cluster-version
data:
      ack-4.8-kube-122-api-removals-in-4.9: "true"
```

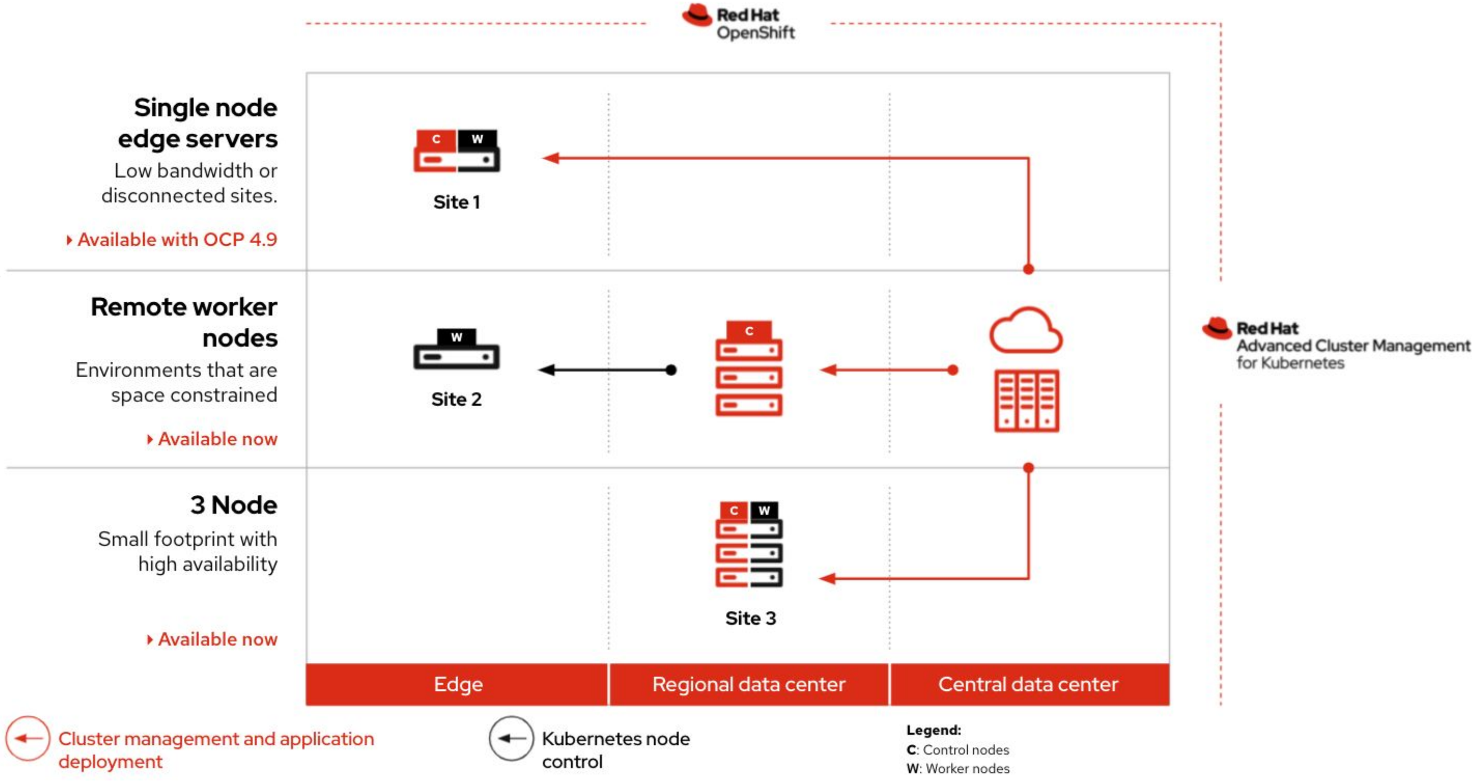
PM: Tony Wu

Single Node OpenShift

Consistent application platform from the datacenter to the edge

- Focused at production/edge use cases for Bare Metal
- Does not have a workload runtime dependency on a central control plane
- Bootstrap In Place - no additional bootstrap node needed
- Upgrade support
- Deployment via openshift-install (GA)
- Deployment via RHACM (ZTP/CIM) /Assisted installer (TP)
- OLM available to install Operators
- 8 cores 32GB mem minimal requirements
- ~2 cores 16GB platform footprint (vanilla OCP)

OpenShift for Edge



Single node edge servers
Low bandwidth or disconnected sites.
▸ Available with OCP 4.9

Remote worker nodes
Environments that are space constrained
▸ Available now

3 Node
Small footprint with high availability
▸ Available now

Legend:
C: Control nodes
W: Worker nodes

https://www.youtube.com/watch?v=QFf0yVAHQKc

PM: Moran Goldboim

MetalLB L2 Support

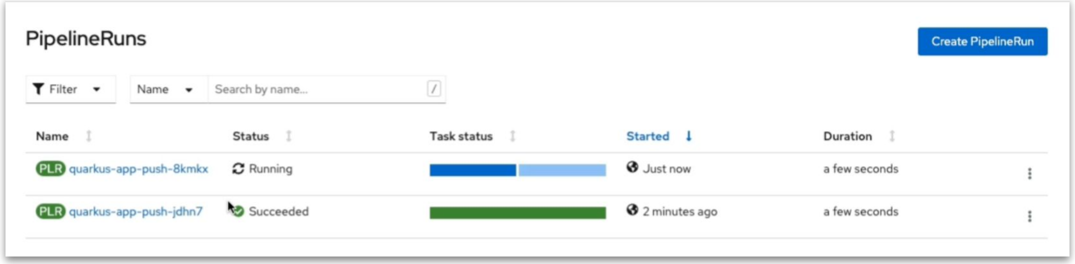
- MetalLB has two modes to announce reachability information for load balancer IP addresses:
  - Layer 2 (4.9)
  - BGP (4.10)
- Two components:
  - Controller - One per cluster
  - Speaker - Per Node (DaemonSet)
- L2 mode: ARP (IPv4) or NDP (IPv6) announces location of a LB'd IP address from the Speaker, then relies on Service load balancing within the cluster
- BGP mode: Traffic can target multiple nodes – routers can perform load balancing across the cluster using ECMP

```yaml
apiVersion: v1
kind: Service
metadata:
  name: nginx
spec:
  ports:
  - name: http
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: nginx
  type: LoadBalancer
```

PM: Marc Curry, Deepthi Dharwar

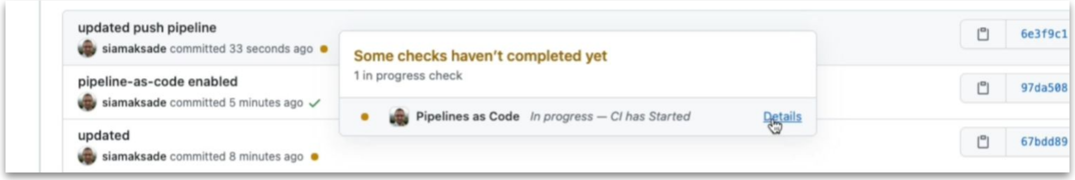
OpenShift Pipelines

- OpenShift Pipelines 1.6 released
- Tetkon Triggers GA
- Auto-pruning configurations per namespace
- Pipeline as code
  - Private Git repository support
  - Hosted BitBucket support
- Granular observability and metrics configurations
- CRD introduced for customizing Tekton configs
- (Dev Console) Search and install Tasks from TektonHub in the Pipeline builder
- (Dev Console) Repository list views for pipeline as code



PipelineRuns

Name	Status	Task status	Started	Duration
PLR quarkus-app-push-8kmkx	Running		Just now	a few seconds
PLR quarkus-app-push-jdhn7	Succeeded		2 minutes ago	a few seconds

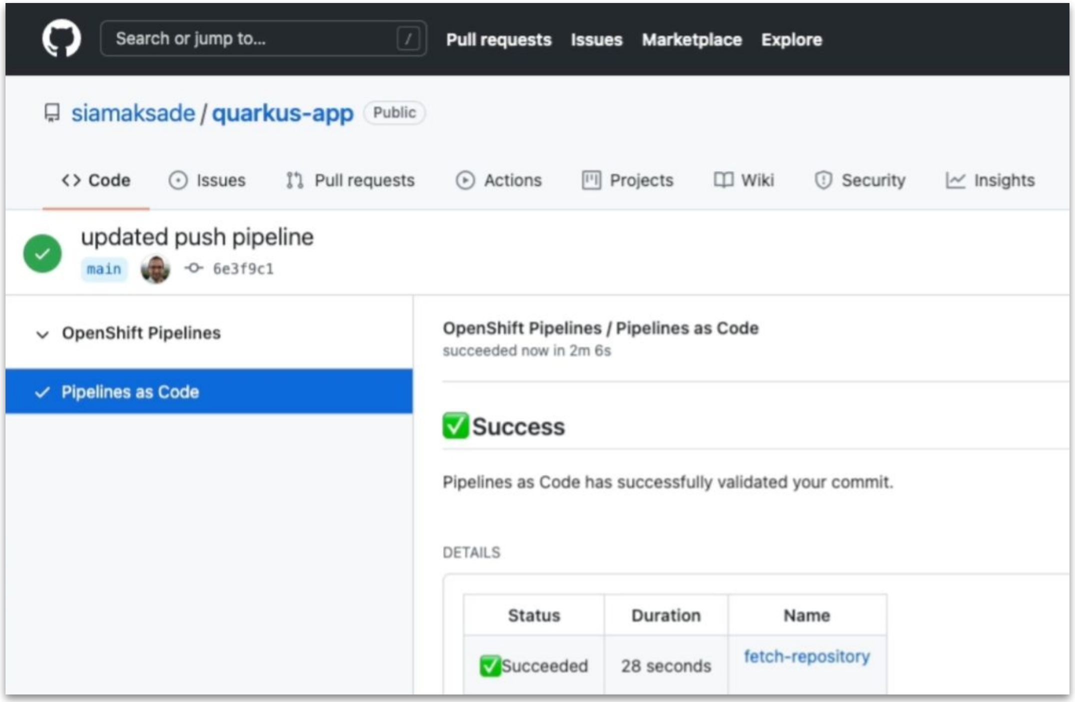


updated push pipeline
siamaksade committed 33 seconds ago ●

pipeline-as-code enabled
siamaksade committed 5 minutes ago ✓

updated
siamaksade committed 8 minutes ago ●

Some checks haven't completed yet
1 in progress check
● Pipelines as Code *In progress — CI has Started* Details



updated push pipeline
main 6e3f9c1

OpenShift Pipelines
✓ Pipelines as Code

OpenShift Pipelines / Pipelines as Code
succeeded now in 2m 6s

✅ Success

Pipelines as Code has successfully validated your commit.

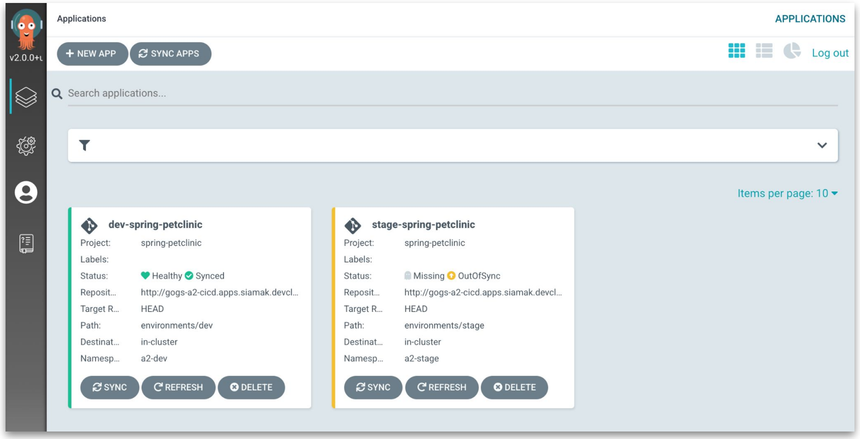
DETAILS

Status	Duration	Name
✅ Succeeded	28 seconds	fetch-repository

PM: Siamak Sadeghianfar

OpenShift GitOps

- OpenShift GitOps 1.3
- User groups and kube-admin support when log into Argo CD with OpenShift credentials
- ApplicationSet integration with RHACM for cluster lookup
- kustomize 4 support
- External cert manager support for TLS configs in Argo CD
- Router sharding for Argo CD
- (Dev Console) Application deployment environment details

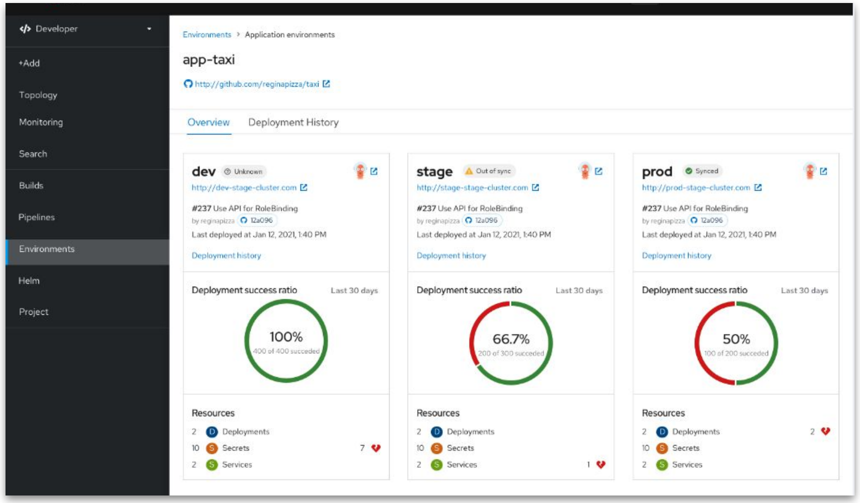


dev-spring-petclinic

Project: spring-petclinic
Labels:
Status: Healthy Synced
Reposit... http://gogs-a2-cicd.apps.siamak.devcl...
Target R... HEAD
Path: environments/dev
Destinat... in-cluster
Namesp... a2-dev

stage-spring-petclinic

Project: spring-petclinic
Labels:
Status: Missing OutOfSync
Reposit... http://gogs-a2-cicd.apps.siamak.devcl...
Target R... HEAD
Path: environments/stage
Destinat... in-cluster
Namesp... a2-stage



app-taxi

http://github.com/reginapizza/taxi

dev Unknown
http://dev-stage-cluster.com
#237 Use API for RoleBinding
by reginapizza 12a096
Last deployed at Jan 12, 2021, 1:40 PM
Deployment history
Deployment success ratio Last 30 days
100%
400 of 400 succeded
Resources
2 D Deployments
10 S Secrets 7
2 S Services

stage Out of sync
http://stage-stage-cluster.com
#237 Use API for RoleBinding
by reginapizza 12a096
Last deployed at Jan 12, 2021, 1:40 PM
Deployment history
Deployment success ratio Last 30 days
66.7%
200 of 300 succeded
Resources
2 D Deployments
10 S Secrets
2 S Services 1

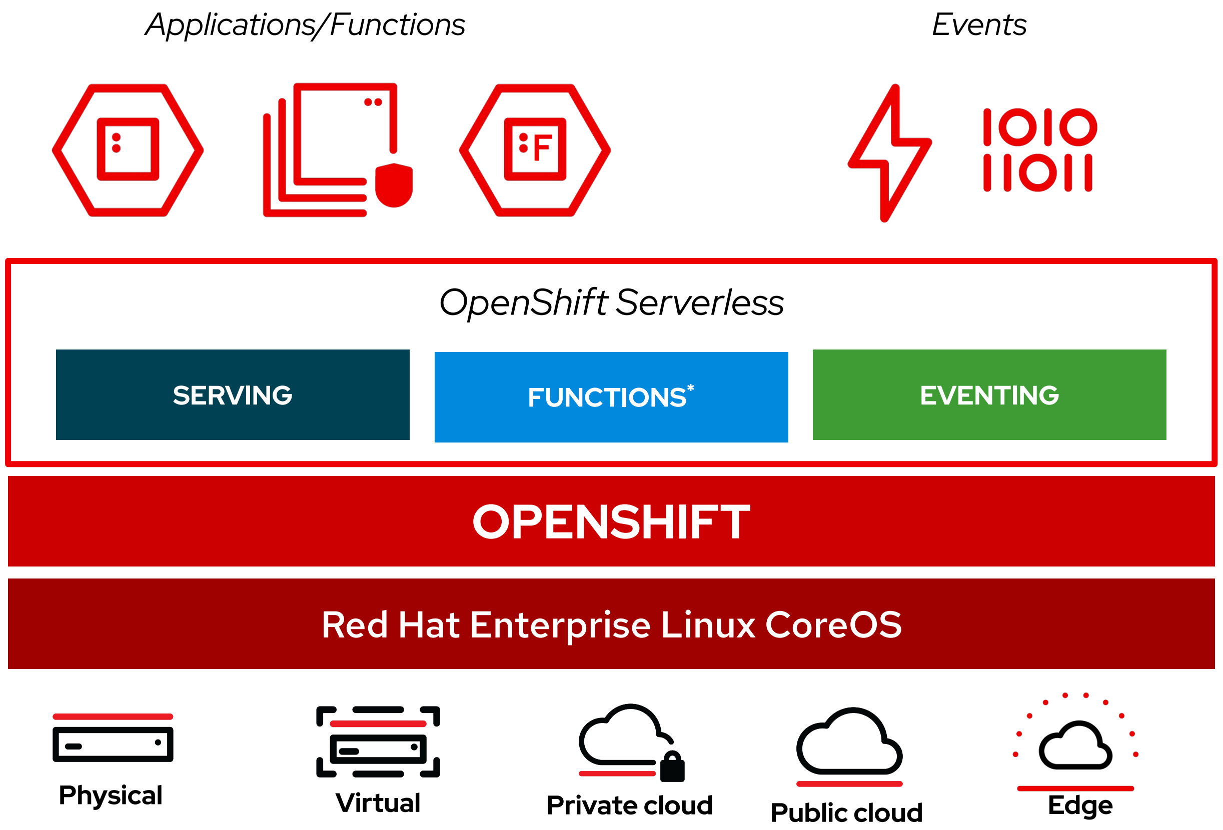
prod Synced
http://prod-stage-cluster.com
#237 Use API for RoleBinding
by reginapizza 12a096
Last deployed at Jan 12, 2021, 1:40 PM
Deployment history
Deployment success ratio Last 30 days
50%
100 of 200 succeded
Resources
2 D Deployments 2
10 S Secrets
2 S Services

PM: Siamak Sadeghianfar

OpenShift Serverless

Key Features & Updates

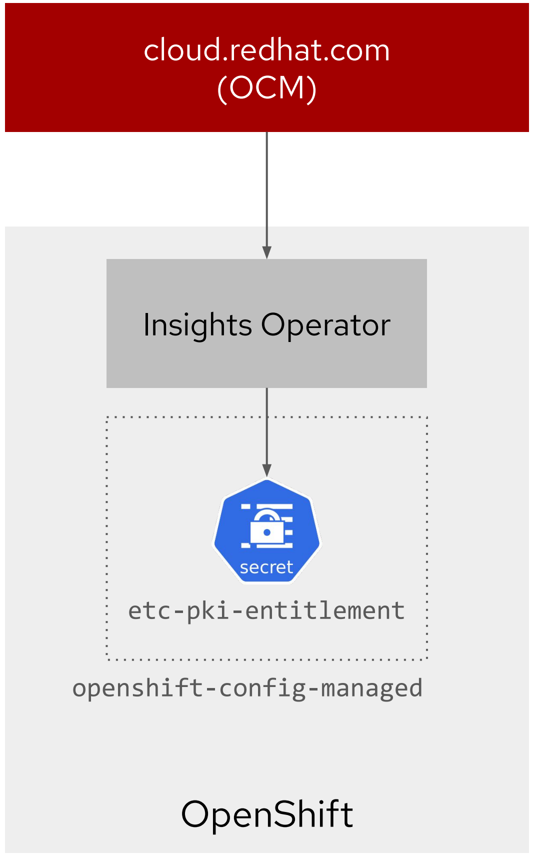
- Update to Knative 0.24
- **Security**: Encryption of Inflight Data with Service Mesh
- Custom Domain Mapping through DevConsole
- **Visualization**: New Monitoring Dashboards
  - CPU, Memory, Network Usage
  - Scaling Debugging
  - User workload monitoring through Knative Queue Proxy
- Support for emptyDir
  - Share files between sidecar and the main container
- **Functions Tech Preview**:
  - Node, Quarkus, Python, Go, SpringBoot, TypeScript^{New}, Rust^{New}
  - Access to data stored in secrets and config maps
  - Available on MacOS , RHEL, Windows with Docker and/or Podman



PM: Naina Singh

Automatic RHEL Entitlement Management for Builds

- Tech preview in 4.9
- Insights Operator pulls RHEL entitlements for OpenShift clusters
- Simple Content Access (SCA) must be enabled for customer's Red Hat account (by the customer)
- Entitlements stored as Secret named etc-pki-entitlement in the `openshift-config-managed` namespace
- Entitlements rotated and refreshed regularly
- Admin responsible to distribute entitlement secret to namespaces
- Mount entitlement secret into Pods and Tekton for entitled builds
- Mount entitlement and other credential secrets (or configmaps) in BuildConfigs for entitled builds



PM: Siamak Sadeghianfar

Simplified registry credentials management

Multi-component/microservice deployments before

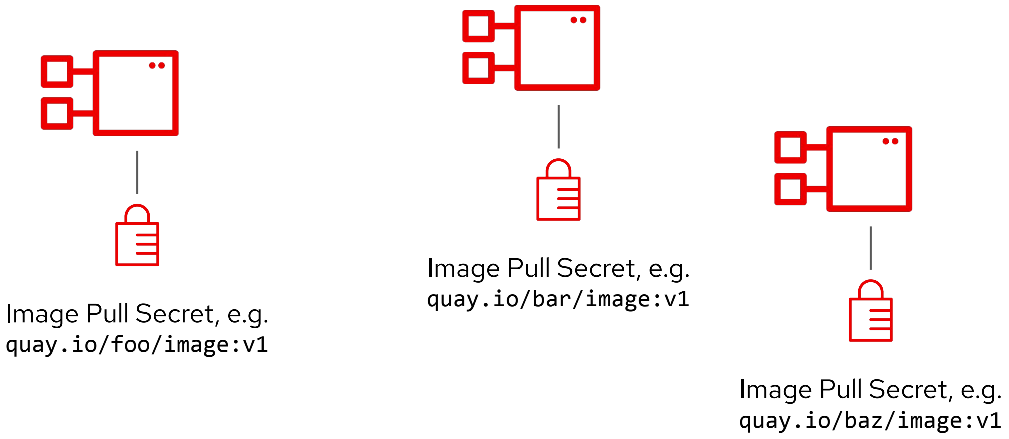


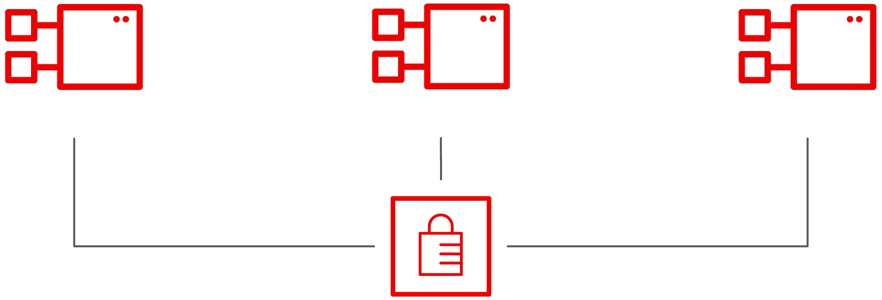
Image Pull Secret, e.g.
`quay.io/foo/image:v1`

Image Pull Secret, e.g.
`quay.io/bar/image:v1`

Image Pull Secret, e.g.
`quay.io/baz/image:v1`

Multiple `Secrets` containing different registry credentials per `Deployment` / image

New option: Multi-component/microservice deployments with 4.9



OpenShift Global Pull Secret:

```
- quay.io/openshift-release-dev
- quay.io/foo/
- quay.io/bar/
- quay.io/baz/image
```

Simplified registry credential management using a **single** `Secret` containing different logins, even for the same registry

Product Manager: Gaurav Singh

Installer Flexibility

4.9 Supported Providers

Full Stack Automation (IPI)

- amazon web services
- Microsoft Azure
- Google Cloud Platform
- vmware vSphere
- RED HAT OPENSTACK PLATFORM
- Bare Metal
- RED HAT VIRTUALIZATION

Pre-existing Infrastructure (UPI)

- amazon web services
- Microsoft Azure
- Google Cloud Platform
- Azure Stack Hub NEW
- RED HAT OPENSTACK PLATFORM
- vmware vSphere
- RED HAT VIRTUALIZATION
- Bare Metal
- IBM Power Systems
- IBM Z

Generally Available

Product Manager(s): Marcos Entenza (AWS, Azure, Azure Stack Hub, GCP), Maria Bracho (VMware), Peter Lauterbach (RHV & OCP Virtualization), Anita Tragler (OSP), Ramon Acedo Rodriguez (BM), & Duncan Hardie (IBM Z & Power)

RHEL 8 support for workers and infra nodes

Support of Red Hat Enterprise Linux 8

- RHEL 8 machines can be added to any **UPI or IPI** deployed cluster in **day-2.**
- **OCP 4.9** starts with **RHEL 8.4**.
- Adding **RHEL 7 machines** to OCP is **deprecated** and support for RHEL7 workers will be **removed** in **OCP 4.10**
- RHEL 7 compute machines **cannot be upgraded to RHEL 8**, new RHEL 8 compute machines must be deployed.

Red Hat
Enterprise
Linux 8

Product Manager: Marcos Entenza

Zero Touch Provisioning

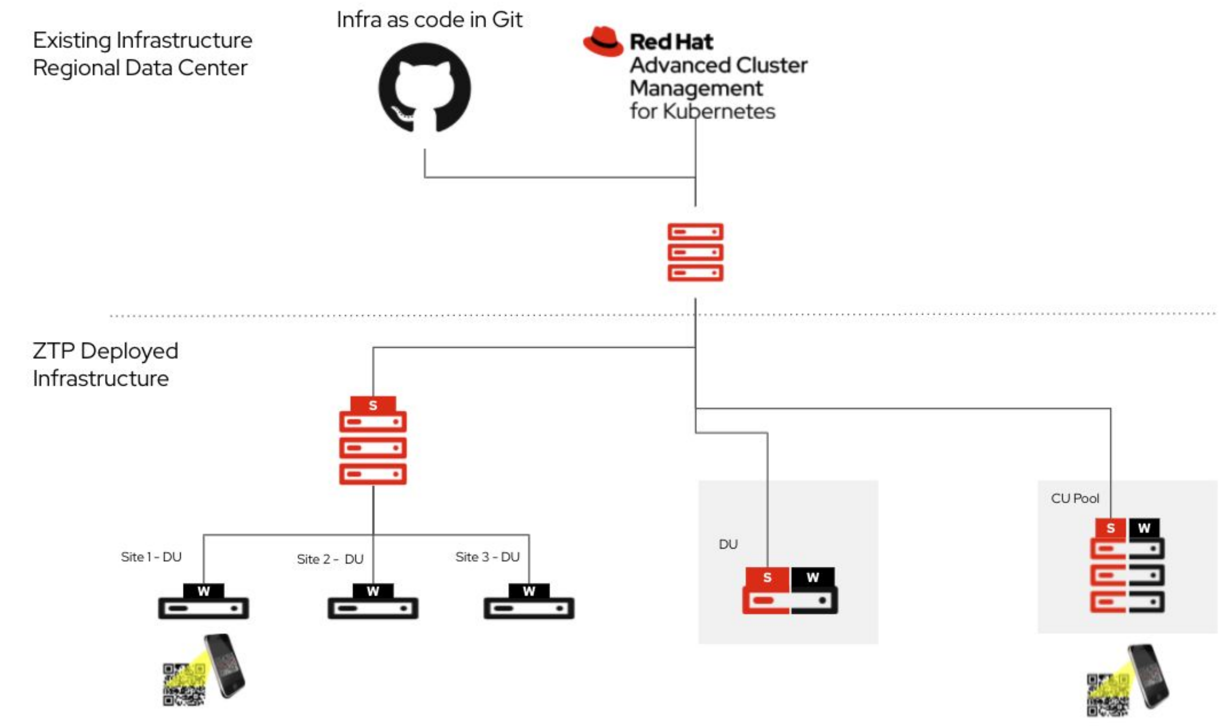
(Infrastructure Operator)

Tech-Preview in Advanced Cluster Management 2.4

Aimed at **regional distributed on-prem deployment.**

Enabling customer's **automated** path from **uninstalled infrastructure to application running on an OpenShift cluster.**

- **Integrates and leverages existing technology stack -** RHACM/Hive/Metal3/Assisted Installer
- **Minimal prerequisites**- deployment over L3 single network, no additional bootstrap node
- **Highly customized deployment** - Fits Connected/Disconnected, IPv4/IPv6, DHCP/Static, UPI/IPI deployment topologies
- **Edge focused** - no additional bootstrap node or external services needed for deployment.
- **GitOps enabled** - managed with kube-native declarative API
- **Any deployment topology** - SingleNodeOpenshift, Remote worker nodes, Compact clusters (3 nodes), multi-node



ZTP - Zero Touch Provisioning
DU - Distributed Unit (5G RAN)
CU - Central Unit (5G RAN)

PM: Moran Goldboim

Central Infrastructure Management

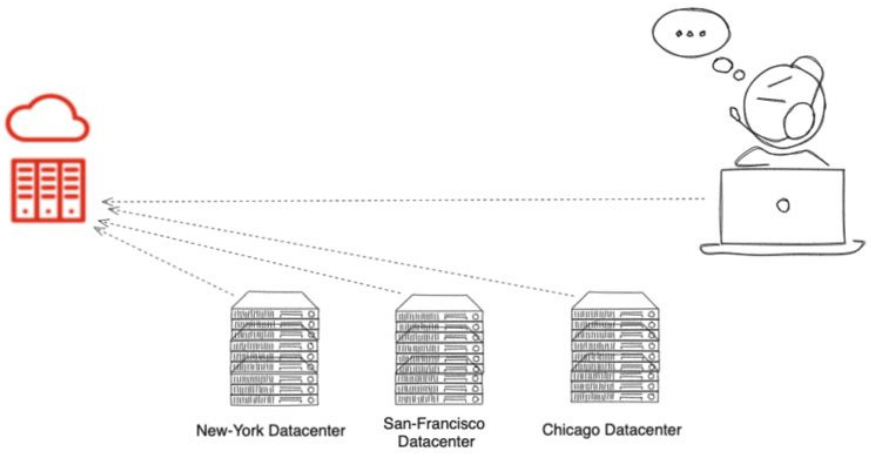
(Infrastructure Operator)

Tech-Preview in Advanced Cluster Management 2.4

Provides a separate interfaces for:
-***Infra-Admin (IT)*** - to manage on-prem compute across different datacenters/locations
-***Cluster creator (Dev/Ops)*** - to consume allocated compute resources for clusters creation

- **Fully integrated with ACM**
- **Consisted UXD with Assisted installer (SAAS)**
- **Integrated preflight checks, monitoring and eventing**
- **K8S native API**
- **Any type of OpenShift deployment (SNO, RWN, Compact..) for Bare metal and platform agnostic**

Infra Admin (IT) -
Adding managed compute resources for
OpenShift cluster creation



PM: Moran Goldboim

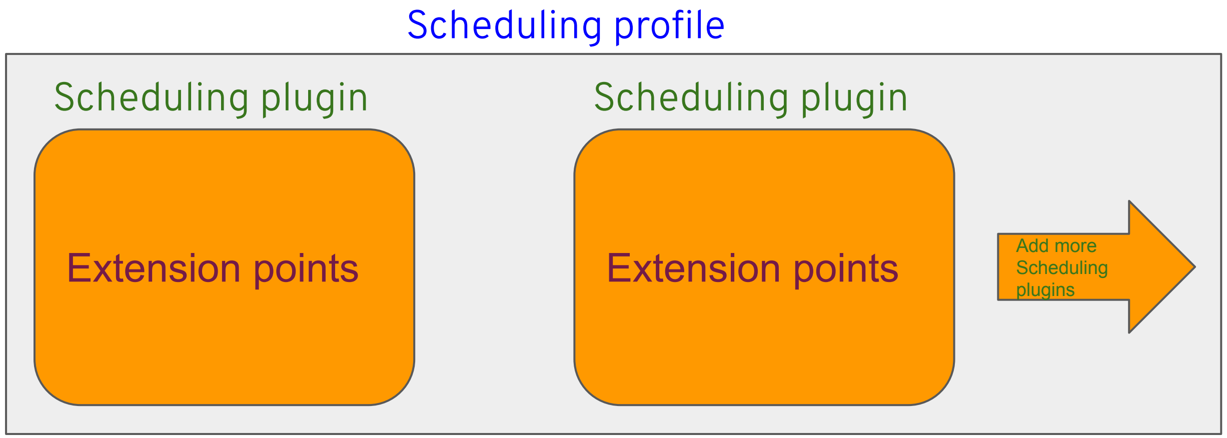
Scheduling Profiles Customization

Customize default out of box behaviour of openshift scheduler with Scheduling Profiles

Pre Build Profile

LowNodeUtilization	Spread pods evenly across nodes
HighNodeUtilization	Pack as many pods as possible on to as few nodes
NoScoring	Quickest scheduling cycle by disabling all score plugins

Build your own Profile



Scheduling profile : Openshift-scheduler can have only one profile
Scheduling plugin : Implements one or more extension points
Extension point : Plugins that define the scheduling logic

*Note: in OSP 4.7 customer can use both policy API and profiles but going forward policy API will be depreciated to profiles

Product Manager: Gaurav Singh

Custom Route Name and Certs for certain cluster components

- The default route name for OpenShift Cluster Components now allows for any level of flexibility in customers environments. The current <name>.apps.<cluster>.<domain> can be customized for the OAuth server and the the OCP console.
- The OAuth server route can be customized using the ingress config route configuration API. A custom hostname and a TLS certificate can be set using the spec.componentRoutes part of the configuration.Set the custom hostname and optionally configure the serving certificate and key.

```
apiVersion: config.openshift.io/v1
kind: Ingress
metadata:
  name: cluster
spec:
  componentRoutes:
    - name: oauth-openshift
      namespace: openshift-authentication
      hostname: <custom-hostname>
      servingCertKeyPairSecret:
        name: <secret-name>
```

Component	**Custom Route supported?**
OAuth	Yes (from 4.9)
Console	Yes (from 4.8)
Downloads	Yes (from 4.8)
Monitoring (AlertManager, Prometheus, Grafana, Thanos)	No
Image Registry	No

PM: Anand Chandramohan

Ingress Enhancements

Ingress Updates

Allow Setting mTLS Through the Ingress Operator Support

- Support client-TLS which enables router to verify client certificates.
- Admin must provide CA certificate to the router.

Support TLS 1.3 for OpenShift 4.x Ingress:

- Supports faster TLS handshake
- Simpler, secure cipher suites
- Better performance and stronger security.

Ingress Updates

HAProxy timeout Variables Customization

a. `clientTimeout/serverTimeout`
b. `clientFinTimeout/serverFinTimeout`
c. `tunnelTimeout`
d. `tlsInspectDelay`

Set as part of Ingress controller spec under tuning Options.

Global Options to Enforce HTTP Strict Transport Security [HSTS]

- Manual per-route annotations to enable HSTS is sub-optimal.
- Allow cluster admins to enforce this policy globally with ease and flexibility.

PM: Marc Curry, Deepthi Dharwar

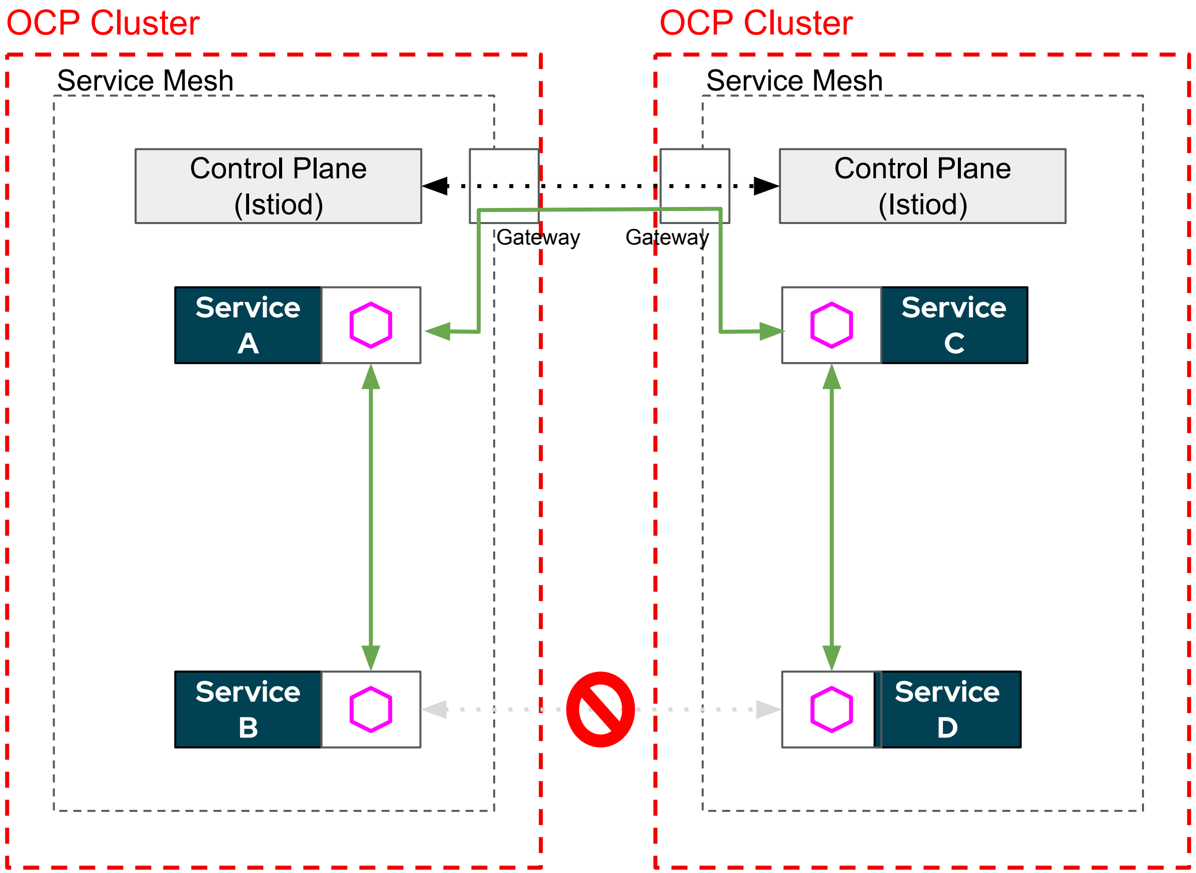
OpenShift Service Mesh 2.1

Key Features & Updates

- Update to Istio 1.9
- **New Feature: Service Mesh Federation**
  - ○ Securely connect service meshes across OCP clusters without the Kubernetes API Server
  - ○ Share services between meshes on a strict "need to know" basis
  - ○ Manage traffic with remote services as if they were local services
- ServiceMeshExtensions API becomes GA
  - ○ Extend service mesh API using Envoy's WebAssembly Extensions

- Service Mesh 2.1 Release Date: November 2021

Federated Service Meshes



PM: Jamie Longmuir

OpenShift Virtualization

Modernized workloads, support mixed applications with VMs, containers, and serverless

Public Cloud Support

- AWS Bare-metal (Tech Preview) - Consistent environment with on-premise VM workloads to support on-demand scaling and cloud migration

Enhanced Data Protection

- Crash-consistent online VM snapshots
- Improved Data Protection w/ upstream Velero plugin for VM backups (Tech Preview)

SAP HANA for test and non-production

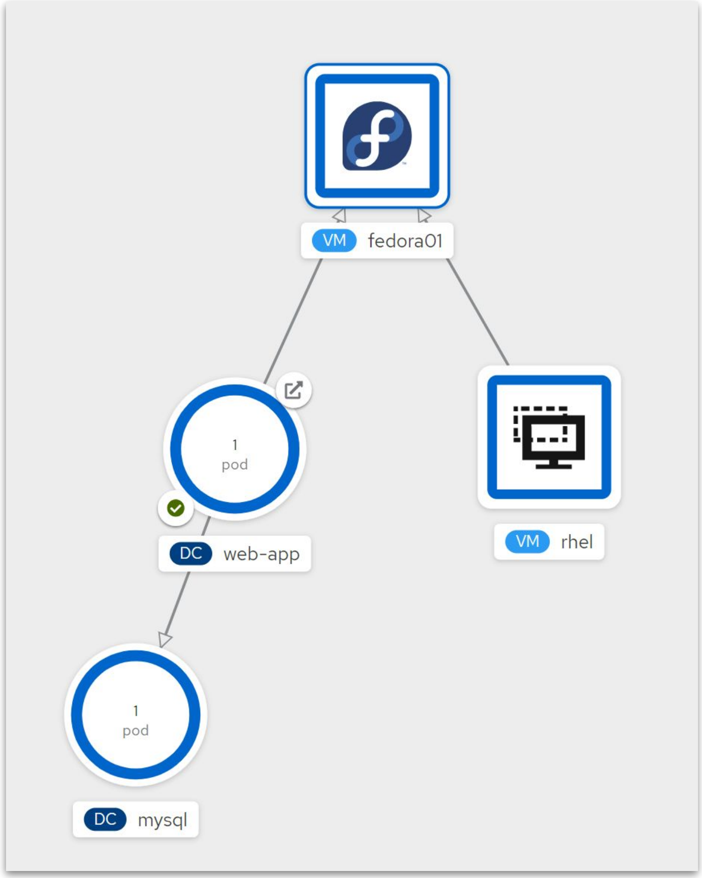
- SAP HANA enablement for testing and non-production deployments
  - production certification in a future release

Enhanced Security and Performance

- Additional modes to boot UEFI guests, High performance workloads with vNUMA
- VM workloads in a FIPS compliant OpenShift cluster

Operational Enhancements

- Hybrid workload with container and VMs in the same service mesh
- VM workflow management, easily configure Windows guests with sysprep

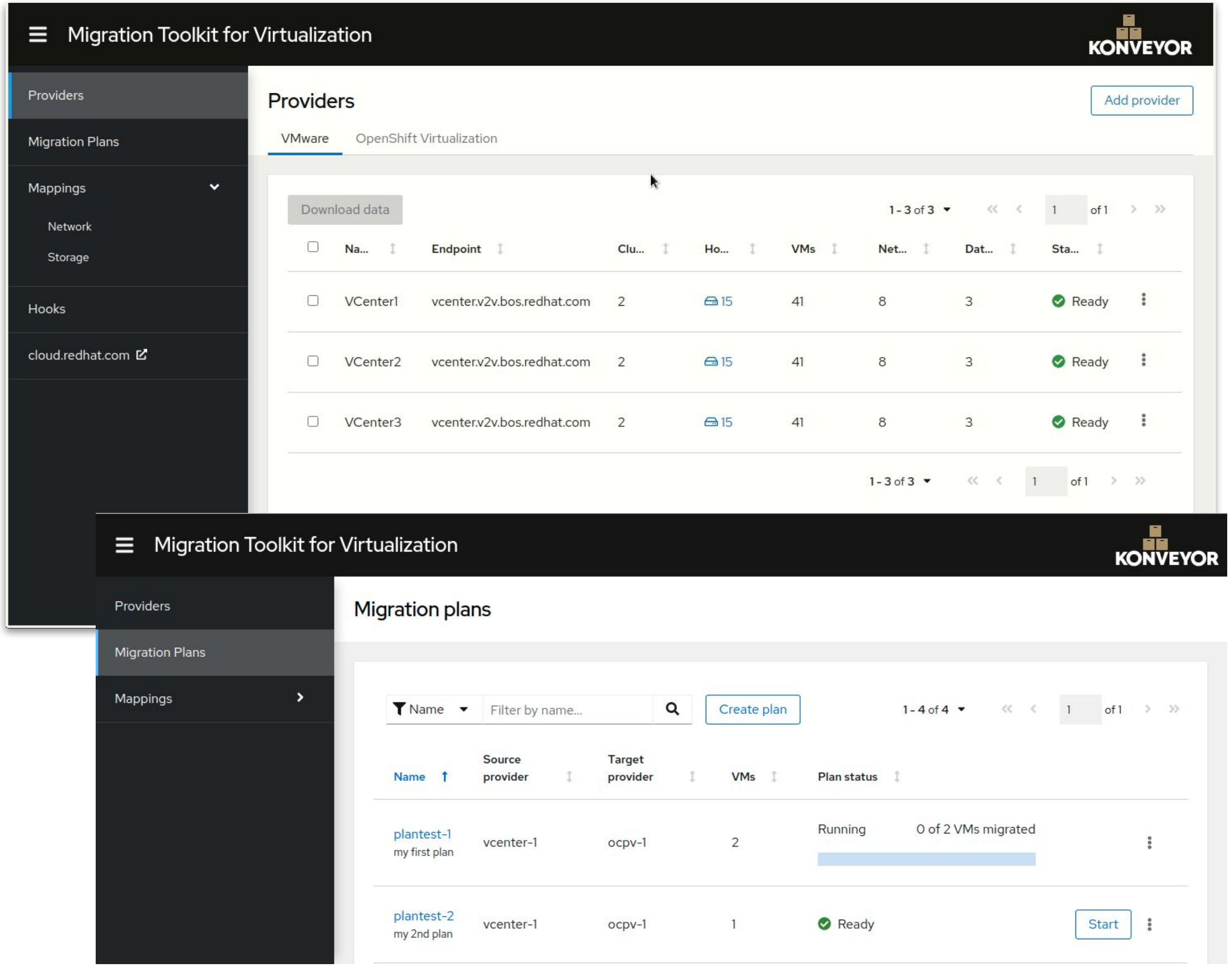


PM: Peter Lauterbach

VM lift-and-shift to OpenShift

Migration Toolkit for Virtualization 2.1

- Easy to use UI
- Mass migration of VMs from VMware and RHV to OpenShift
- Added Red Hat Virtualization as supported source provider (Cold Migration only)
- Validation service (Tech Preview): Includes SR-IOV cards and Opaque networks that are configured.
- Hooks: Automated tasks to be performed pre and post migration
- Must-Gather: specific add-ons created to help debug issues during migrations



Providers

Na...	Endpoint	Clu...	Ho...	VMs	Net...	Dat...	Sta...
VCenter1	vcenter.v2v.bos.redhat.com	2	15	41	8	3	Ready
VCenter2	vcenter.v2v.bos.redhat.com	2	15	41	8	3	Ready
VCenter3	vcenter.v2v.bos.redhat.com	2	15	41	8	3	Ready

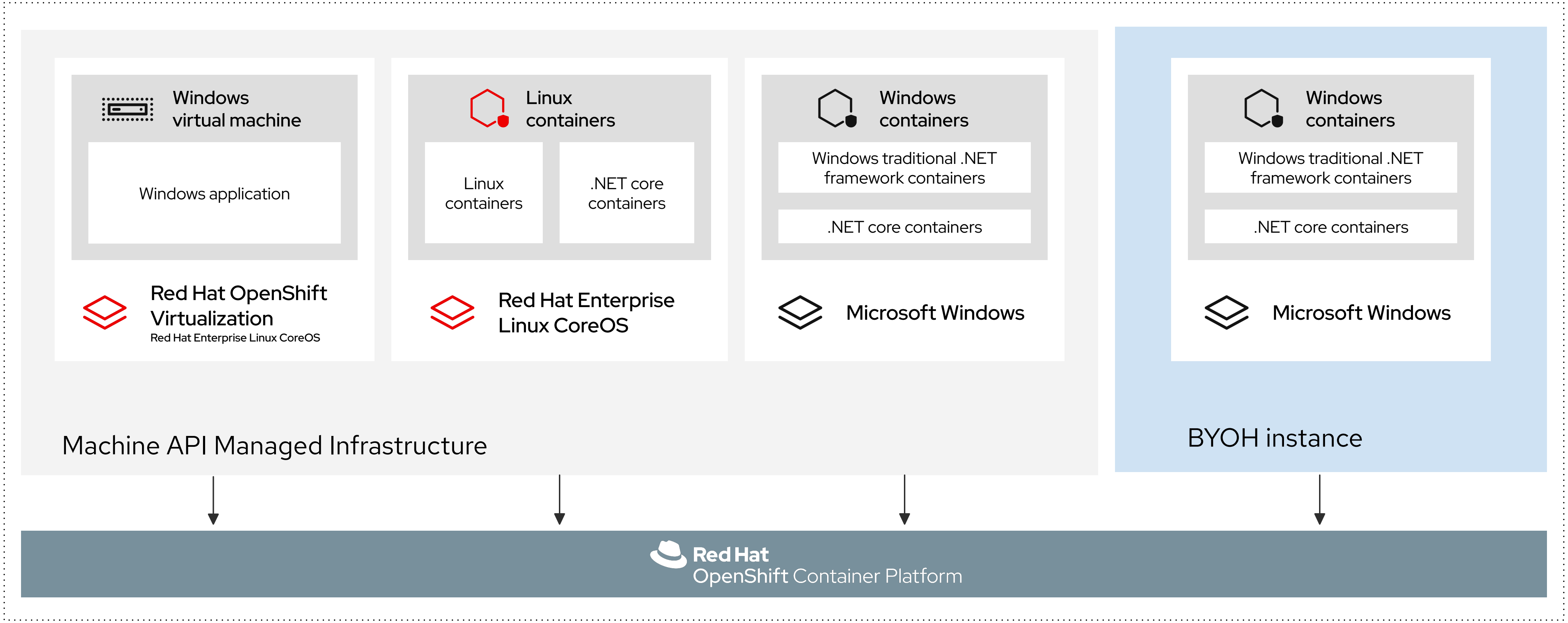
Migration plans

Name	Source provider	Target provider	VMs	Plan status
plantest-1 my first plan	vcenter-1	ocpv-1	2	Running 0 of 2 VMs migrated
plantest-2 my 2nd plan	vcenter-1	ocpv-1	1	Ready

PM: Miguel Pérez Colino

Bring Your Own Hosts (BYOH) for Windows Nodes

Mixed Windows and Linux workloads



Windows virtual machine
Windows application
Red Hat OpenShift Virtualization
Red Hat Enterprise Linux CoreOS
Linux containers
Linux containers
.NET core containers
Red Hat Enterprise Linux CoreOS
Windows containers
Windows traditional .NET framework containers
.NET core containers
Microsoft Windows
Windows containers
Windows traditional .NET framework containers
.NET core containers
Microsoft Windows
Machine API Managed Infrastructure
BYOH instance
Red Hat OpenShift Container Platform

- BYOH instance and Linux worker nodes on the cluster have to be on the same network
- The platform type for BYOH must match that set for the OCP cluster

PM: Anand Chandramohan

OpenShift sandboxed containers

Tech Preview

FIPS Compliance

Now you can run the OpenShift sandboxed containers operator on a FIPS enabled cluster without worrying about tainting its state. Our Operator, and Kata Containers are FIPS Validated.

Updates & Upgrades

You can now seamlessly upgrade a cluster, as well as the operator and its artifacts (Kata Containers + QEMU extensions).

Must Gather

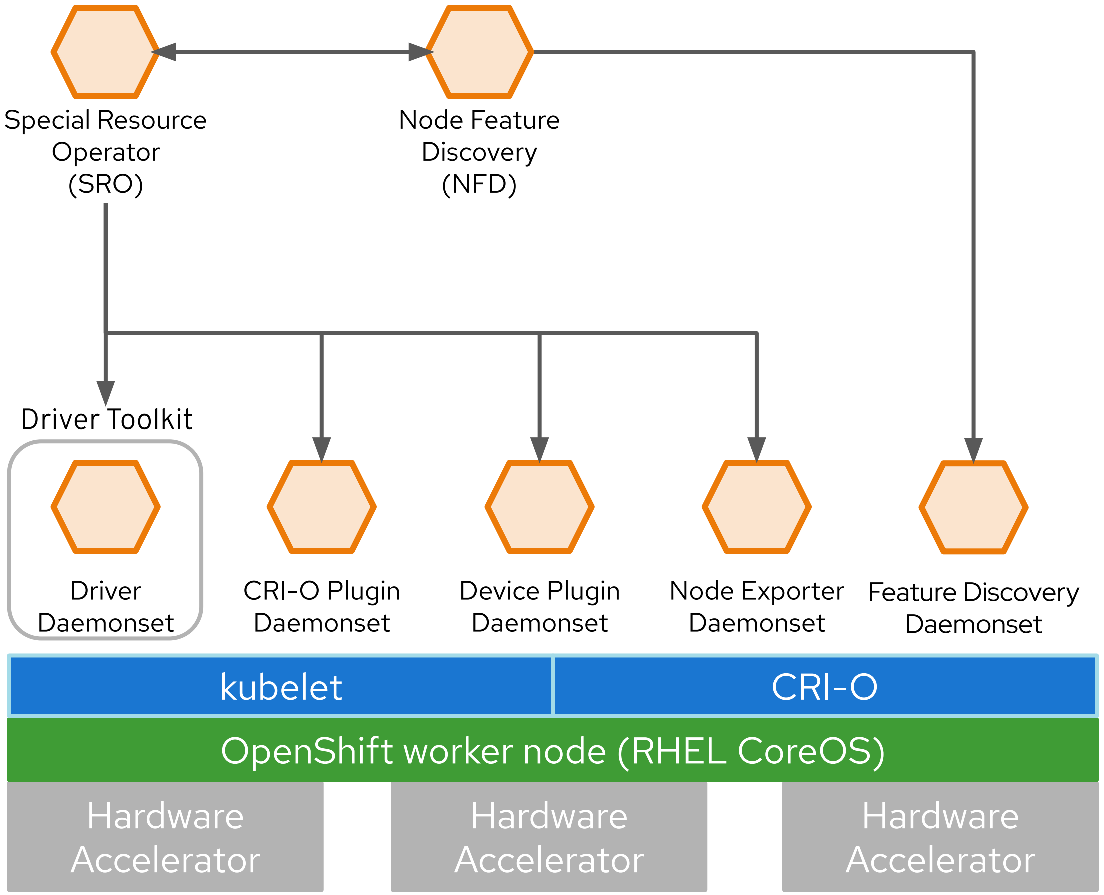
An initial version of must-gather will be available in this release. This will help automate data-collection for you to get a better support experience.

Disconnected Mode

Our operator now works in disconnected mode.

PM: Adel Zaalouk

Hardware Accelerators enablement



Special Resource Operator (SRO)

- Orchestrator to manages the deployment of software stacks for hardware accelerators
- SRO uses recipes to enable the out-of-tree driver and manage the driver life cycle
- Day 2 operations:
  - Building and loading a kernel module
  - Deploying the driver
  - Deploying one device plugin
  - Monitoring stack
- Red Hat third-party support and certification policies.
- Tech Preview in OpenShift 4.9

Driver Toolkit (DTK)

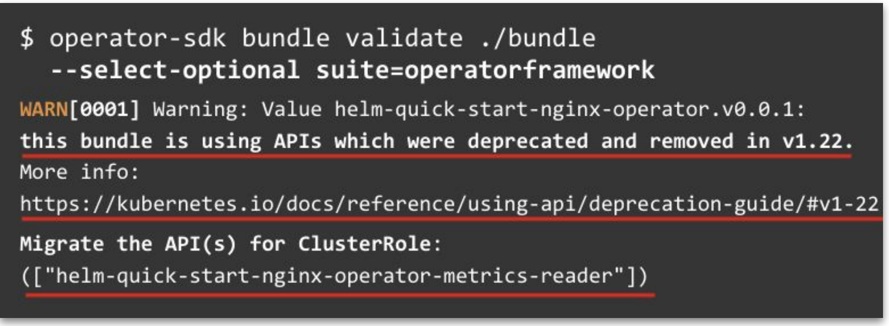
- The Driver Toolkit is a container image to be used as a base image for driver containers.
- The DTK contains tools and the kernel packages required to build or install kernel modules
- Usable for partner builds or local builds
- Reduce cluster entitlement requirements
- Tech Preview in OpenShift 4.9

PM: Erwan Gallen

Operator SDK Enhancements

Bundle validate: WARN on k8s removed APIs

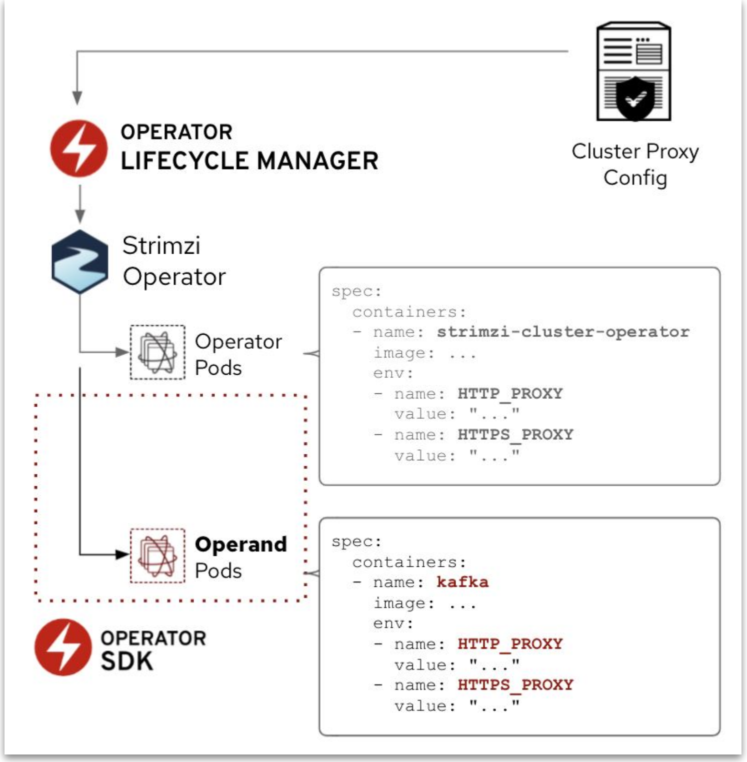
- Easily see and be aware of those **removed k8s APIs** in the bundled manifests.
- Get handy guidance on **how to migrate** per k8s upstream doc.



```
$ operator-sdk bundle validate ./bundle
  --select-optional suite=operatorframework
WARN[0001] Warning: Value helm-quick-start-nginx-operator.v0.0.1:
this bundle is using APIs which were deprecated and removed in v1.22.
More info:
https://kubernetes.io/docs/reference/using-api/deprecation-guide/#v1-22
Migrate the API(s) for ClusterRole:
(["helm-quick-start-nginx-operator-metrics-reader"])
```

Operator handles proxy settings in the pods for managed Operands

- Helper functions for reading proxy info so it can be passed down to Operands pods.
- Easier to build “**proxy-aware**” Operators for proxied cluster environment.

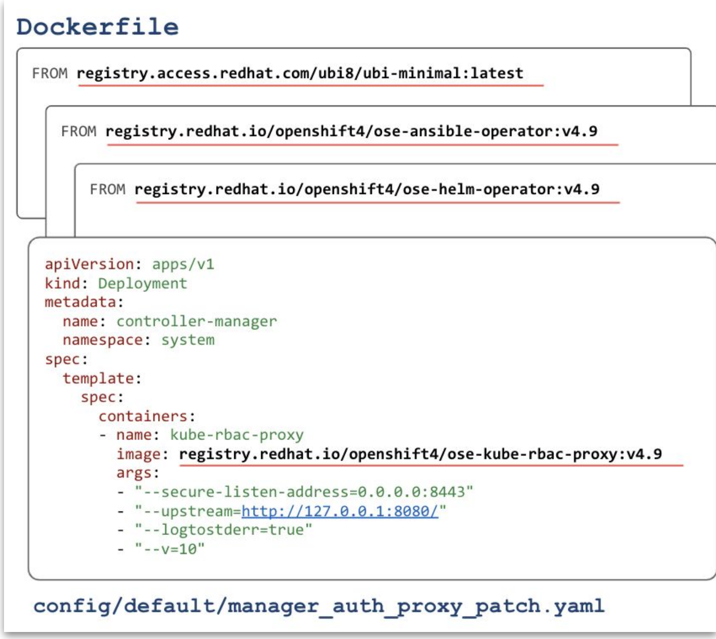


```
spec:
  containers:
  - name: strimzi-cluster-operator
    image: ...
    env:
    - name: HTTP_PROXY
      value: "..."
    - name: HTTPS_PROXY
      value: "..."
```

```
spec:
  containers:
  - name: kafka
    image: ...
    env:
    - name: HTTP_PROXY
      value: "..."
    - name: HTTPS_PROXY
      value: "..."
```

Uses UBI and other downstream images by default

- Base image (**v4.y**) is guaranteed with compatibility fixes in two OCP releases (**4.y** and **4.y+1**).
- Easier create and maintain Operator projects in a Red Hat supported way.



Dockerfile

```
FROM registry.access.redhat.com/ubi8/ubi-minimal:latest
```

```
FROM registry.redhat.io/openshift4/ose-ansible-operator:v4.9
```

```
FROM registry.redhat.io/openshift4/ose-helm-operator:v4.9
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: controller-manager
  namespace: system
spec:
  template:
    spec:
      containers:
      - name: kube-rbac-proxy
        image: registry.redhat.io/openshift4/ose-kube-rbac-proxy:v4.9
        args:
        - "--secure-listen-address=0.0.0.0:8443"
        - "--upstream=http://127.0.0.1:8080/"
        - "--logtostderr=true"
        - "--v=10"
```

config/default/manager_auth_proxy_patch.yaml

PM: Tony Wu

Operator Lifecycle Management Enhancements

Auto-switching of catalogs

Use Kubernetes/OCP-version specific operator catalogs and automatically switch during cluster updates, e.g.

```
"quay.io/org/catalog:v{kube_major_version}.{kube_minor_version}"
```

OpenShift Operator release compatibility

OpenShift release compatibility can be denoted via operator metadata, initially blocks cluster upgrades

```
metadata:
  annotations:
    operators.coreos.com/maxOpenShiftVersion: "4.8"
```

Support for "large" operator bundles

Bundles with lots of metadata (for example large CRD manifests) are now compressed to stay below the 1MB etcd limit

Reduced resource usage / Better troubleshooting

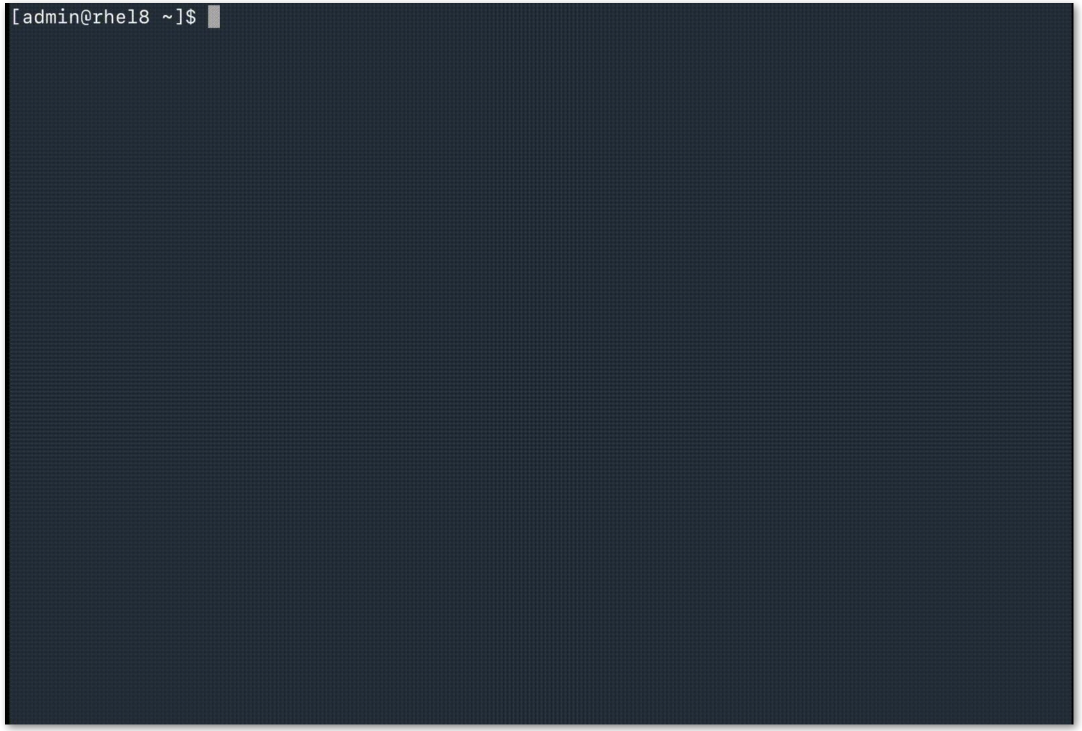
OLM catalog pods now use significantly less RAM. More status information in `OperatorGroup` and `Subscription` API, covering most install and update error scenarios.

PM: Daniel Messer

OpenShift Mirror Registry

Bootstrap registry for disconnected OpenShift cluster installations

- We prefer customers to run Quay on top of OCP
- But: disconnected clusters need a registry to store OCP release images and Operators before OCP can be installed
- Solution: tailored version of Quay helping customers to get a registry up and running quickly, mirroring is carried out via oc
- Local all-in-one Quay instance on RHEL 8
- Released as part of OpenShift, post 4.9 GA, included in every OCP subscription



```
[admin@rhel8 ~]$
```

PM: Daniel Messer

Nested repository support

Simplifying mass-mirroring and organization of registry content

Regular container image reference:

```
quay.local/organization/repository:tag
```

Nested container image references:

```
quay.local/organization/collection/repository:tag
```

```
quay.local/organization/folder/v1/repository:tag
```

```
quay.local/ocp/v4/redhat-pipelines/operator:v4.9
```

```
quay.local/ocp/v4/redhat-pipelines/tekton:v4.9
```

- **Audience:** Quay user / OpenShift administrator
- **Use Cases:**
  - Mirror content of multiple upstream registries into a single Quay* organization
  - Organize images into “subfolders” inside a single Quay organization
- **Benefit:** Eases skopeo mass mirroring, OpenShift Operator catalog mirroring
- **Caveat:** no hierarchical permission management

PM: Daniel Messer

* available in Quay 3.6 past OCP 4.9 GA, quay.io will get this towards the end of 2021

OpenShift Storage - Journey to CSI

- CSI Operators - plugable, built-in upgrade, could include new functionality
    - Azure Stack Hub (GA)
    - AWS EBS (GA)
    - AWS EFS (Tech Preview)
    - vSphere enhancements (Tech Preview)
- CSI Migration - allow easy move from using existing intree drivers to new CSI drivers
    - GCE Disk (Tech Preview)
    - Azure Disk (Tech Preview)
- Prepare for vSphere CSI transition
    - CSI Driver will be the only option in 4.11
    - New CSI Driver requires hardware version 15
        - And version 6.7u3 and later
    - Get your customers ready to upgrade
    - h/w version 15 will be default starting 4.9 (but h/w 13 is still supported)

CSI Operators		
Operator target	**Migration**	**Driver**
OpenStack Cinder	Tech Preview	Tech Preview
AWS EBS	Tech Preview	GA
AWS EFS	n/a	Tech Preview
GCE Disk	Tech Preview	GA
Azure Disk	Tech Preview	Tech Preview
Azure Stack Hub	n/a	GA
vSphere	-	Tech preview

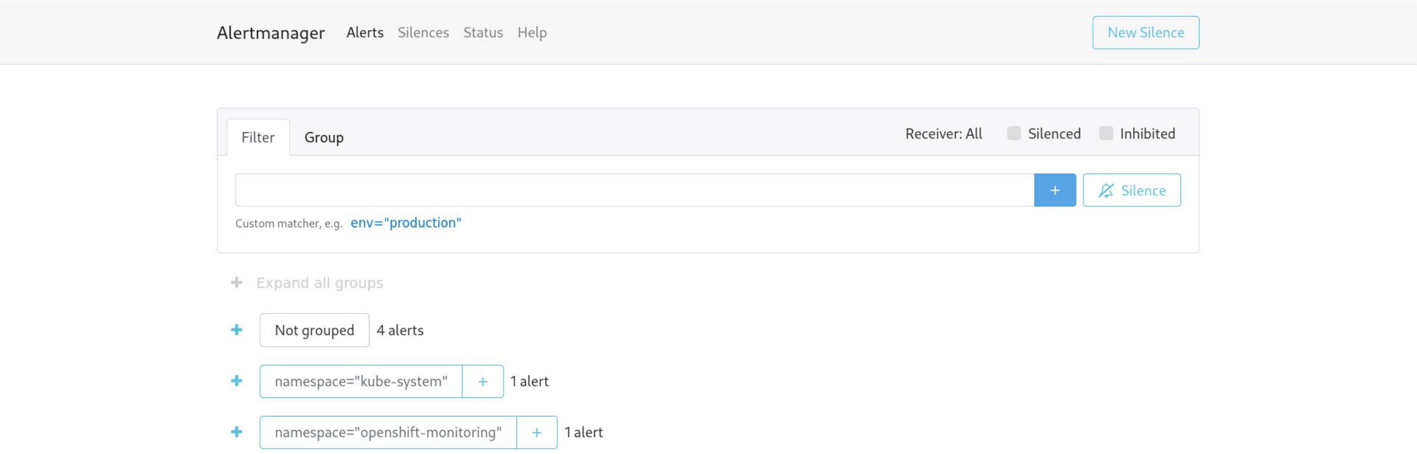
PM: Gregory Charot

New enhancement for OpenShift Monitoring

Enhanced capabilities to improve working with the OpenShift Console Monitoring Experience:

- Support for Prometheus 2.29.2 and Thanos 0.22.0
- Enhancements to Alert Manager Rules, Cluster Monitoring Operator and refined triggering conditions
  - Additional options to set Alerts on Cube States
  - Improvements to detect more quickly when disk space is running low
  - Expanded Alert rules for Kube Clier errors with Thanos queries
- Monitoring for User-Defined Projects
- Remote write storage for Prometheus Metrics

New Kube State Metrics & Alertmanager Functionality



Custom matcher, e.g. env="production"

Not grouped 4 alerts

namespace="kube-system" 1 alert

namespace="openshift-monitoring" 1 alert

Note: You can now disable the default Grafana dashboard deployment using a configuration option. https://github.com/openshift/cluster-monitoring-operator/pull/1241

PM: Shannon Wilber