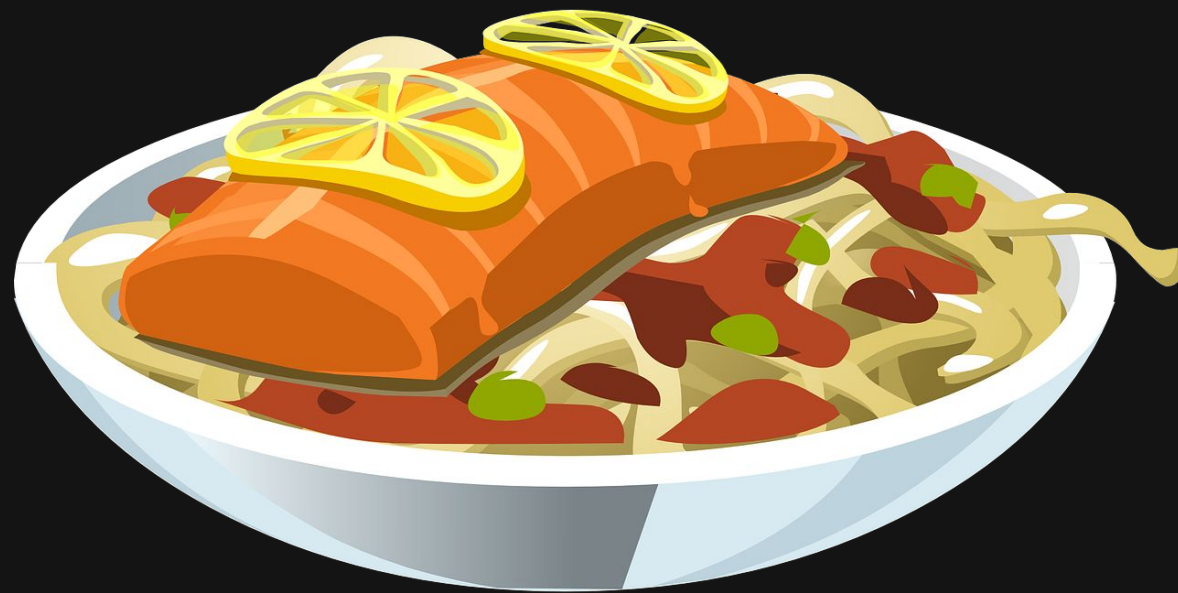
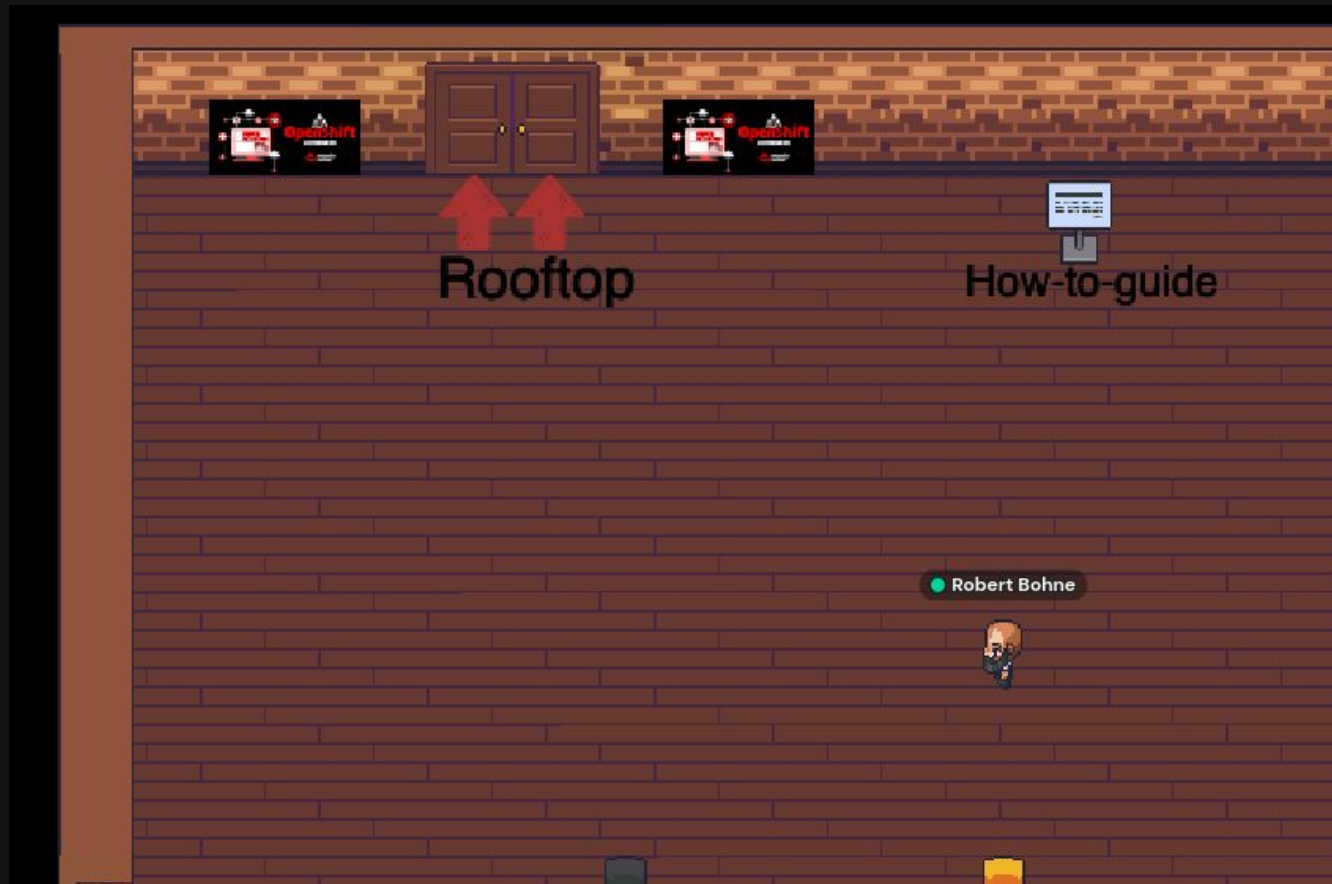




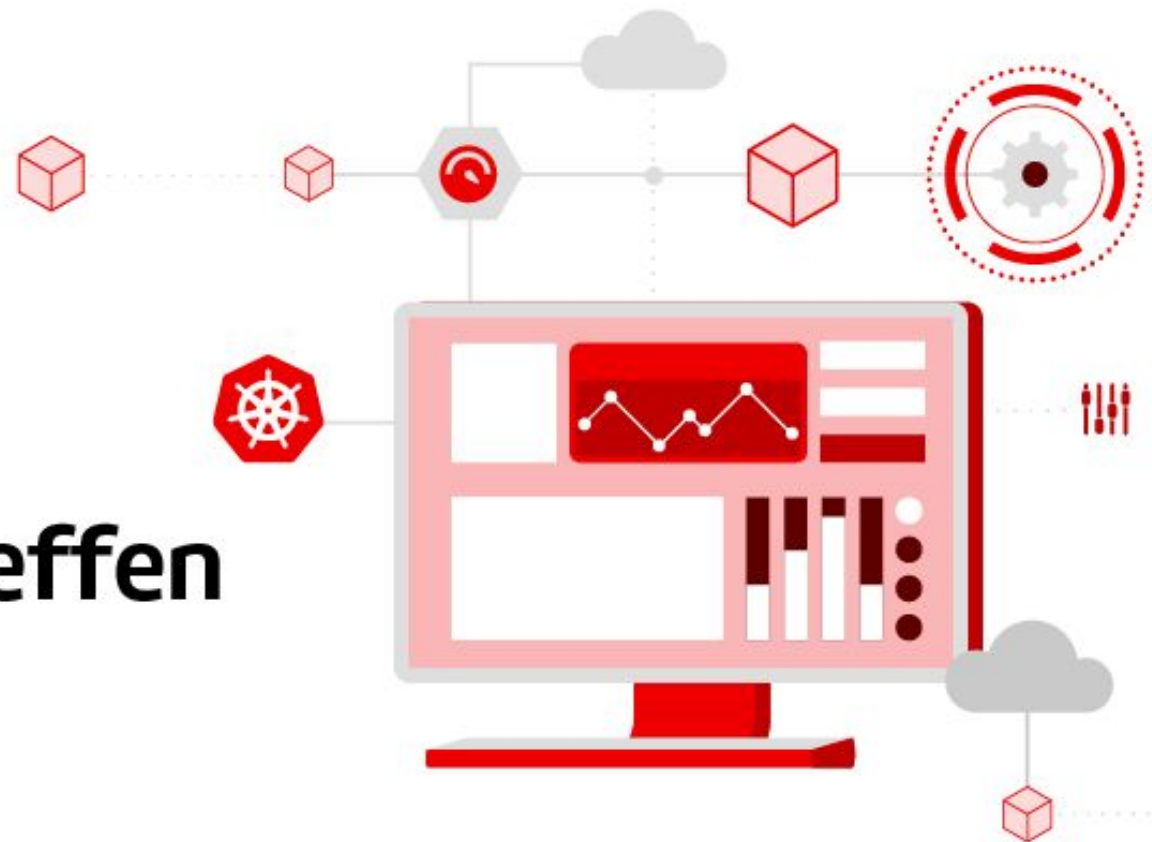
We'll be back at 13.00...

<https://www.openshift-anwender.de/live>



We'll be back at 15.00 in Gather.town

Link in chat



Robert Bohne, Red Hat

Organisatorisches

- **Veröffentlichung Foto und Video**
Folien werden im Nachgang über die Anwenderforum
Webseite (www.openshift-anwender.de) veröffentlicht
- ~~Raucherbereiche~~
- Fragen?

WE GROW WHEN WE SHARE.



Werde Teil der OpenShift Anwender Community!



Webseite

<http://www.openshift-anwender.de>

Slack Channel

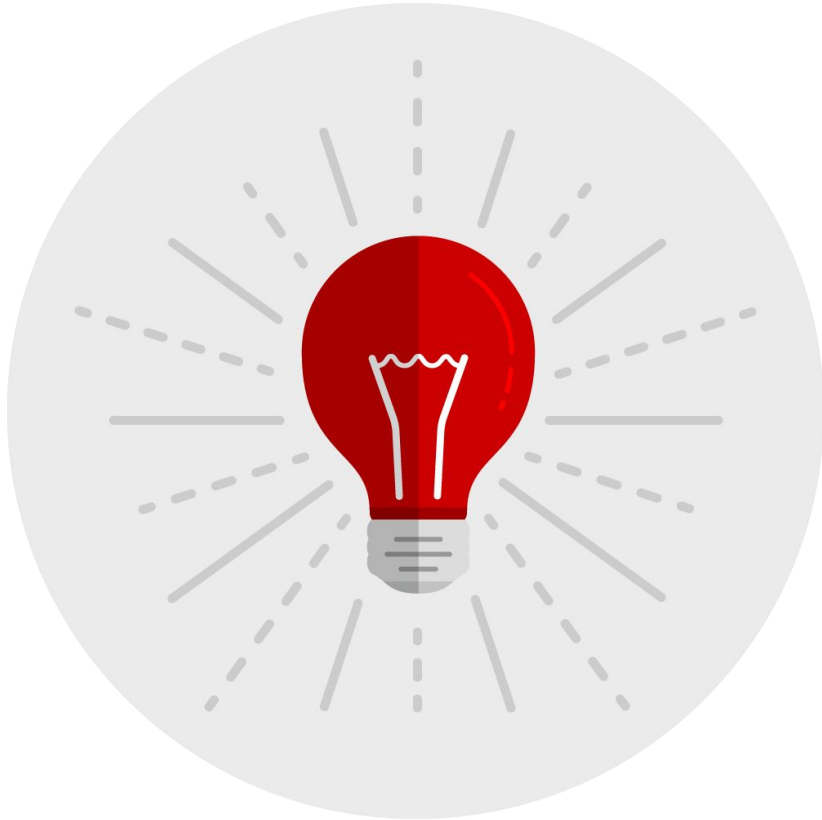
<http://openshift-de.slack.com>

Mailing Liste

openshift-anwender@redhat.com

Twitter

[#openshiftuser](https://twitter.com/openshiftuser)



Interactive Learning Portal for OpenShift

<https://learn.openshift.com>

Red Hat Developer Portal

<https://developers.redhat.com>

Try OpenShift

<https://try.openshift.com>

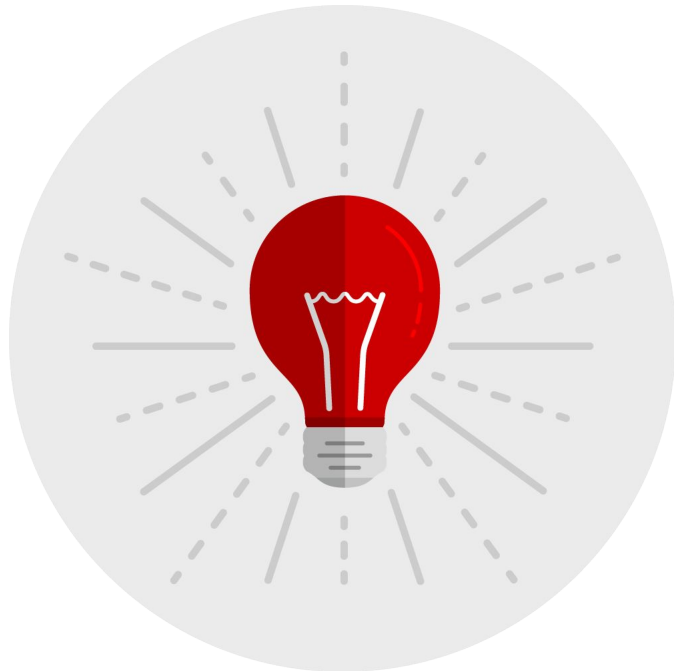
Agenda

Agenda

Time	Slot
11.00 – 12.00	 Einführung in Red Hat OpenShift*
	<i>Break</i>
13:00 – 13:45	 Willkommen, inklusive: Vorstellung Gather.Town & OpenShift What's next Jonas Janz
13:45 – 14:45	 Einführung SaaS „quay.io“ als zentrale Container Image Registry Andreas Letsche (Consol)
	<i>Break</i>
15:00 – 15:45	Room A  Anwendertreffen Continuous Improvement Jonas Janz
	Room B  Keycloak – Status and Evolution (with Q&A) Stian Thorgersen
15:45 – 16:30	Room A  Round Table: OpenShift in der public Cloud
	Room B  Open Demo: MicroShift Robert Bohne
16:30 – 17:00	Austausch & virtuelles 🍷 in Gather.town

* Sessions specifically for OpenShift beginners. / OpenShift Einsteiger Sessions

Breakout Themen



Anwendertreffen Continuous Improvement - Room A

Jonas Janz (Red Hat)

Keycloak - Status and Evolution (with Q&A) - Room B

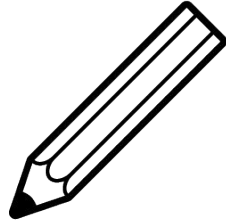
Stian Thorgerisson (Red Hat)

Round Table “Public Cloud” - Room A

Jonas Janz (Red Hat)

MicroShift Demo

Robert Bohne (Red Hat)



Feedback

<https://forms.gle/WGkKq53Z9hgFfe9L8>

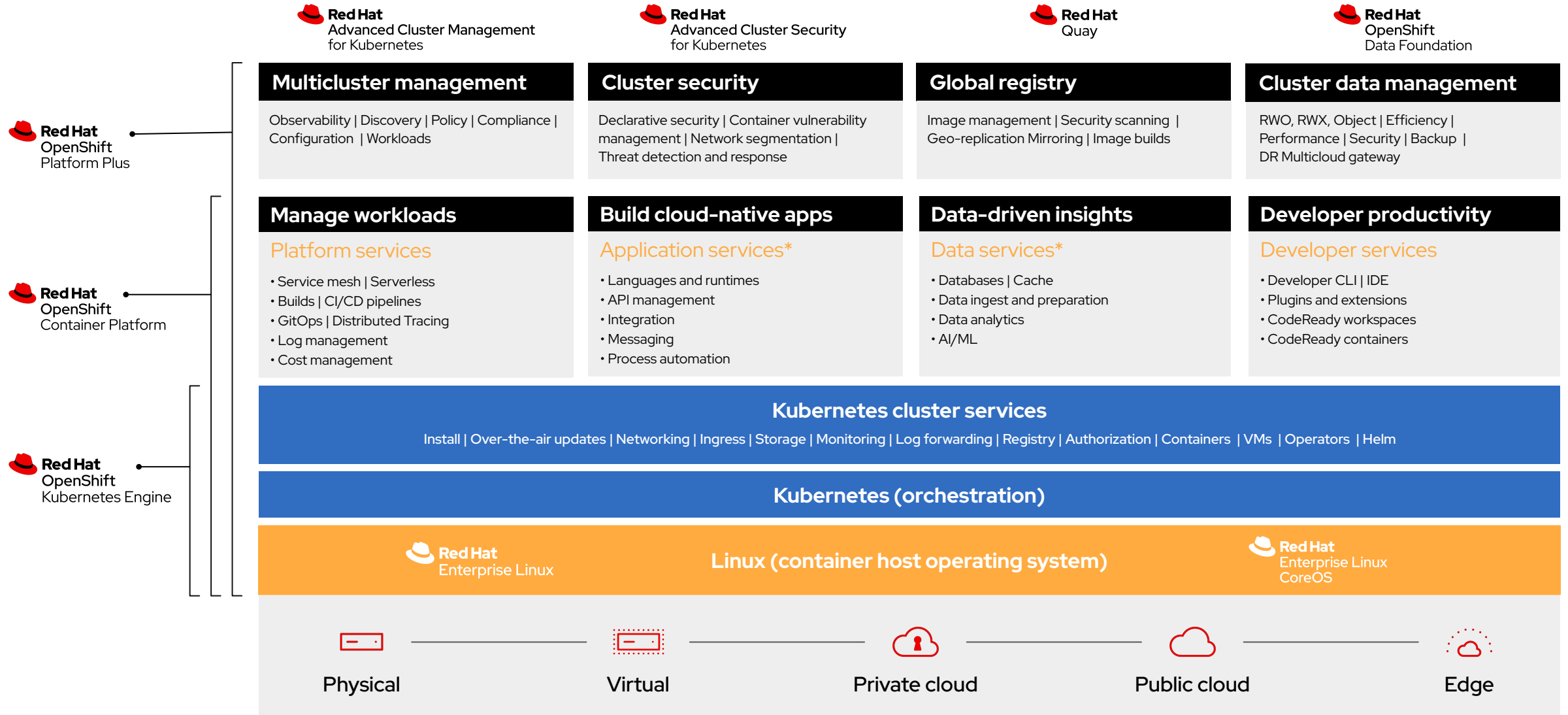




What's New in OpenShift 4.10

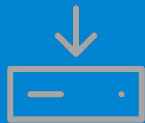
OpenShift Product Management

Red Hat open hybrid cloud platform



OpenShift 4.10

INSTALLER FLEXIBILITY



IBM Cloud (IPI) is GA
Azure Stack Hub (IPI) is GA
Alibaba Cloud (IPI) is Tech Preview
AWS on ARM is GA
Pre-install OCP at factory for OEMs

AUTOMATED OPERATIONS



Reduce worker reboots on EUS→EUS
Conditional cluster updates based on risk
New Mirror Registry for disconnected
Improved mirroring CLI workflow

WORKLOAD EXTENSIBILITY



New Compliance Operator profiles
Sandboxed Containers are GA
Virtualization supports Service Mesh
MetalLB with BGP for external services



Kubernetes 1.23

Major Themes and Features

- ▶ Clusters default to Dual Stack networking
 - ▶ Feature gate is removed, meaning IPv4 and IPv6 is default
 - ▶ In OpenShift, dual-stack has been GA since 4.8
- ▶ PodSecurity graduates to Beta
 - ▶ Red Hat is making upstream contributions here
 - ▶ OpenShift plans to introduce PodSecurity admission (tentatively 4.11) and plans to fully support it in the future along with SCCs side by side
- ▶ CSI Migration
 - ▶ Replacement of existing in-tree storage plugins with a corresponding CSI driver
 - ▶ OpenShift will seamlessly migrate in the future
- ▶ Software Supply Chain
 - ▶ SLSA Level 1 Compliance in the Kubernetes Release Process

CRI-O
1.23



Kubernetes
1.23



OpenShift
4.10



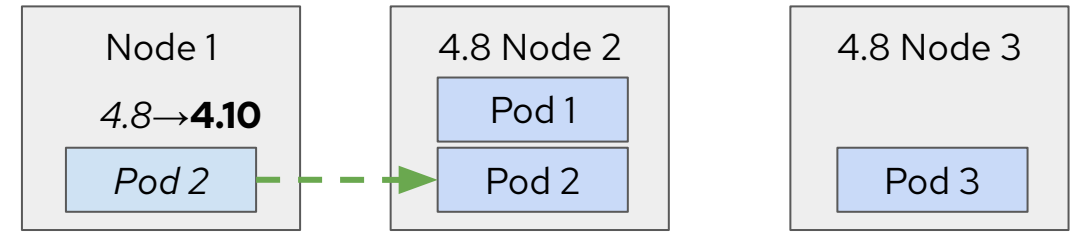
EUS to EUS Upgrade Experience

Quicker, Safer upgrades and less disruptions to workloads

EUS-aware Scheduler

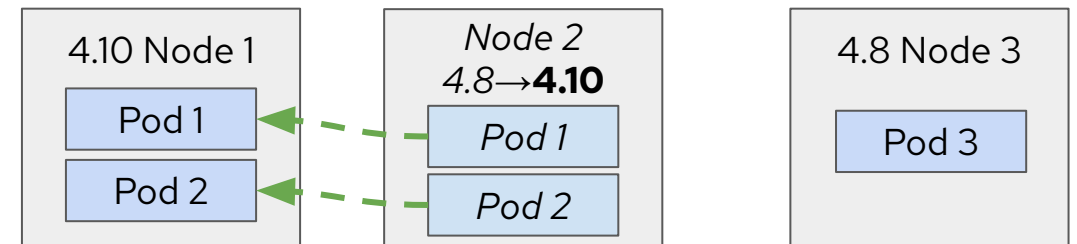
- ▶ EUS-to-EUS upgrade from 4.8.14+ to 4.10 incurs **single reboot** of non-master nodes
- ▶ **Upgrade-aware** scheduler steers rescheduled Pods to updated Nodes
- ▶ Pods restart **less frequently**

Upgrade drains Node1. Pod 1 moves from Node 1 to Node 2.



Pods relocate from Node 2 to Node 1.

Node 3 is ready to upgrade and will get new workloads afterwards.



OpenShift Roadmap

Q1 2022

DEV	- Unprivileged builds in OpenShift Pipelines - Custom Tekton Hub on OpenShift - Automatic pull of RHEL entitlements GA - BuildConfig CSI volume mounts - Tekton Chains (sigstore) TP - OpenShift sandboxed containers GA
APP	- Dynamic Plugins TP - Unified Console(ACM +OCP) TP - Serverless:Knative Kafka Broker and Sink TP - Operator SDK: Hybrid Helm Operator plugin TP - Operator SDK: Digest-based bundle (disconn.)
PLATFORM	- Alibaba Cloud (IPI) technology preview - IBM Cloud & Azure Stack Hub (IPI) - OpenShift on ARM (AWS and Bare Metal) - Zero Touch Provisioning and Central infrastructure Management in ACM is GA - External Control Planes with HyperShift in ACM TP - MetalLB BGP support - ExternalDNS technology preview - Disconnected mirroring simplification - Service Mesh on VMs
HOSTED	- ROSA: Cluster manager UI for ROSA provisioning - ROSA/OSD: Cluster hibernation - OCM: Updated OSD cluster creation UI - OSD: PrivateLink - ROSA: Cluster-wide proxy

Q2 2022

DEV	- Private Preview of App Studio, a hosted dev exp - OpenShift Serverless Functions IDE Experience - OpenShift Dev CLI (odo onboarding & more) - GitOps ApplicationSets GA - OpenShift Pipelines on Arm - Extended pipeline history - Custom Argo CD plugins support
APP	- OpenShift Serverless Functions GA - Encryption of inflight data natively in Serverless - Serverless:workflow orchestration TP - Serverless: Knative Kafka Broker and Sink GA - Operator Maturity increase via SDK - OLM operator update retries
PLATFORM	- Nutanix (UPI/IPI) - Alibaba Cloud (IPI) GA - SRO manages third party special devices - Additional capabilities for Windows containers: health management, 3rd party CNI (like Calico) - NetFlow/sFlow/IPFIX Collector - Introduce Gateway API
HOSTED	- ROSA/OSD: FedRAMP High on AWS GovCloud - ROSA/OSD/ARO: GPU Support - ROSA/OSD: ISO27017+ISO27018 - ROSA/OSD: Additional instance types - ARO: Upgrades through cluster manager - Cost management understands IBM Cloud IaaS

H2 2022+

DEV	- OpenShift Builds v2 & Buildpacks GA - Shared Resource CSI Driver GA - Image build cache - Pipelines: Manual approval, pipeline-as-code GA - Reusable Pipelines & concurrency control - GitOps on Power
APP	- File-based operator catalog management - Operator SDK for Java/Quarkus TP - Integration of Knative(Serverless) with KEDA - Multi Tenancy for Serverless - Serverless Cost Management
PLATFORM	- Azure China - Utilize cgroups v2 - Expand cloud providers for OpenShift on ARM - Enable user namespaces - Windows Containers: CSI proxy, improved monitoring/logging & more platforms supported - Gateway API / Ingress Controller support - Network Topology and Analysis Tooling - SmartNIC Integrations - eBPF Support - Network Policy v2 & OVN no-overlay option - BGP Advertised Services (FRR) - SigStore style image signature verification
HOSTED	- Cost mgmt integration to Subs Watch, ACM - Detailed Quota Usage in cluster manager - ROSA/OSD: AWS Dedicated instances - ROSA/OSD: Terraform provider



Notable Top RFE's and Components

Top Requests for Enhancement (RFEs)

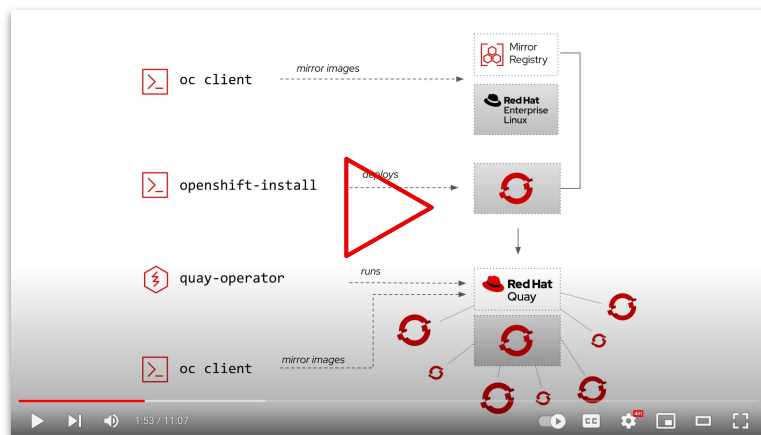
- ▶ Support for Day-2 changes in static network configuration
 - ▶ Static network configuration can become obsolete and need to be updated after cluster deployment.
- ▶ Capture MachineConfigDaemon Events in the Operator Events
 - ▶ Provides a way to check configuration regularly so admins know about potential problems sooner.
- ▶ Force write MachineConfig to Node
 - ▶ A way to align nodes configurations back to the rendered one in case the files monitored by MCO become misconfigured on UPI installations.
- ▶ Support for AvailabilitySets in MachineSets for Azure
 - ▶ Some Azure Regions do not support multiple zones, high availability can be achieved to some extent by using AvailabilitySets.
- ▶ Ability to change MTU of openshift-sdn post installation
 - ▶ Gives a way to adapt cluster setting to the environment on Day-2.

45 RFEs

shipped in
OpenShift 4.10
for customers

OpenShift Disconnected

New: Single command to get a registry



- ▶ Local all-in-one Quay instance on RHEL 8 to get customers a supported mirror registry at no additional cost for their first cluster
- ▶ More details: [Technical Enablement Deck](#)
- ▶ Next up (past 4.10 GA): Update support

New: Single command to mirror content



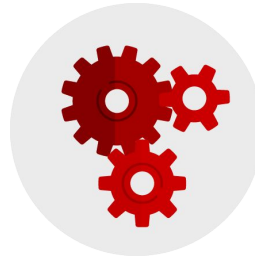
Tech Preview

- ▶ A single CLI tool to mirror all OCP content (images, operators, helm charts): `oc mirror`
- ▶ Smart: maintains update paths of OCP & operators
- ▶ Declarative: config to filter for particular OCP & operator catalogs / releases / channels
- ▶ Fast: Incremental mirroring



Three new Compliance Operator profiles

Customers will be able to Scan,
Report and Remediate
Compliance issues using the
following profiles



PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.



FedRAMP Moderate

FedRAMP moderate impact level is the standard for cloud computing security for controlled unclassified information across federal government agencies. The moderate impact level is appropriate for CSPs that will handle government data that is not publicly available.



NERC CIP

NERC Critical Infrastructure Protection (NERC CIP) is a set of requirements designed to secure the assets required for operating North America's bulk electric system to protect critical cyber assets and minimize risk and manipulation by bad actors seeking to cause damage.



OpenShift on Arm

- ▶ Announcing **GA** of support for OpenShift on Arm platforms
 - ▶ AWS Full Stack Automation (IPI)
 - ▶ Bare Metal Pre-existing Infrastructure(UPI)
- ▶ It's about choice, run on the architectures that best suit your workloads
- ▶ OpenShift "core" parts for this release
 - ▶ Logging
 - ▶ ACM
 - ▶ Storage: EBS, NFS only
- ▶ Hardware support
 - ▶ What RHEL supports
 - ▶ Certified systems on HCL for best experience but ...
 - ▶ Also systems that meet Arm SystemReady/ServerReady specification*

Fully Automated Installers (IPI)	✓
Customizable Installers (UPI)	✓
RHEL or CoreOS entitlement	✓
CRIO Runtime	✓
Over the Air Smart Upgrades	✓
Operating System (CoreOS) Management	✓
Enterprise Secured Kubernetes	✓
Kubectl and oc automated command line	✓
Auth Integrations	✓
Operator Lifecycle Manager (OLM)	✓
Administrator Web console	✓
Node Feature Discovery	✓
Embedded OperatorHub	✓
Embedded Marketplace	✓
Embedded Registry	✓
Helm	✓

Cluster Monitoring	✓
Log Forwarding	✓
Telemeter and Insights	✓
OVS and OVN SDN	✓
HAProxy Ingress Controller	✓
Ingress Cluster Wide Firewall	✓
Egress Pod	✓
Ingress Non-Standard Ports	✓
Network Policies	✓
IPv6 Single and Dual Stack	✓
CNI Plugin ISV Compatibility	✓
CSI Plugin ISV Compatibility	✓
Service Binding Operator	✓
Platform Logging	✓
OpenShift Elasticsearch Operator	✓
Developer Web Console	✓



MetalLB BGP Support

- ▶ MetalLB has two modes to announce reachability information for load balancer IP addresses:
 - ▶ Layer 2 (4.9)
 - ▶ BGP (4.10)
- ▶ BGP (FRR) mode: Traffic can target multiple nodes – routers can perform load balancing across the cluster using ECMP
 - ▶ Active / Active configuration handled by the external routers
 - ▶ Extra configuration required to establish BGP sessions
 - ▶ BFD Support
 - ▶ Refusing incoming routes
 - ▶ BGP Peer node selector
 - ▶ iBGP and eBGP, single and multihop

```
apiVersion: metallb.io/v1beta1
kind: AddressPool
metadata:
  name: addresspool-sample1
  namespace: metallb-system
spec:
  protocol: bgp
  addresses:
    - 172.18.0.100-172.18.0.255
```

```
apiVersion: metallb.io/v1beta1
kind: BGPPeer
metadata:
  name: peer-sample1
  namespace: metallb-system
spec:
  peerAddress: 10.0.0.1
  peerASN: 64501
  myASN: 64500
  peerPort: 179
  holdTime: "180s"
  keepaliveTime: "180s"
  password: "test"
```

RHEL entitlement management for image builds

Pull entitlements

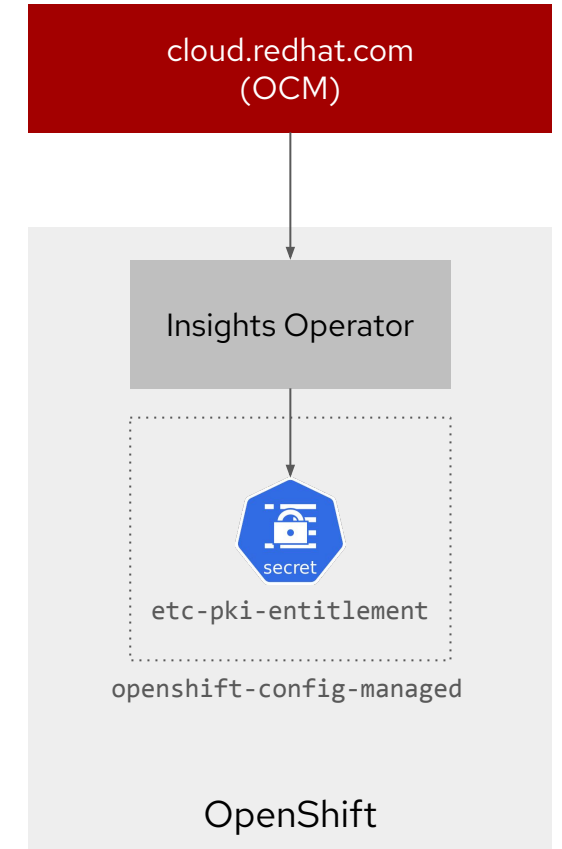
- ▶ Insights Operator manages and refreshes cluster entitlements **(GA)**
- ▶ Simple Content Access (SCA) must be enabled on customer's account
- ▶ NOT available for OSD/ROSA/ARO

Manage access

- ▶ Shared Resource CSI Driver **(Tech Preview)**
- ▶ Provide tenants access to entitlements without sharing certificates

Use entitlements

- ▶ Mount shared entitlements in BuildConfigs **(Tech Preview)**
- ▶ Mount entitlement secret in BuildConfigs, Pipelines, Pods, etc **(GA)**



Multi-Cluster Focused

Selectable Cluster Inventory

Tech Preview

What is this console integration?

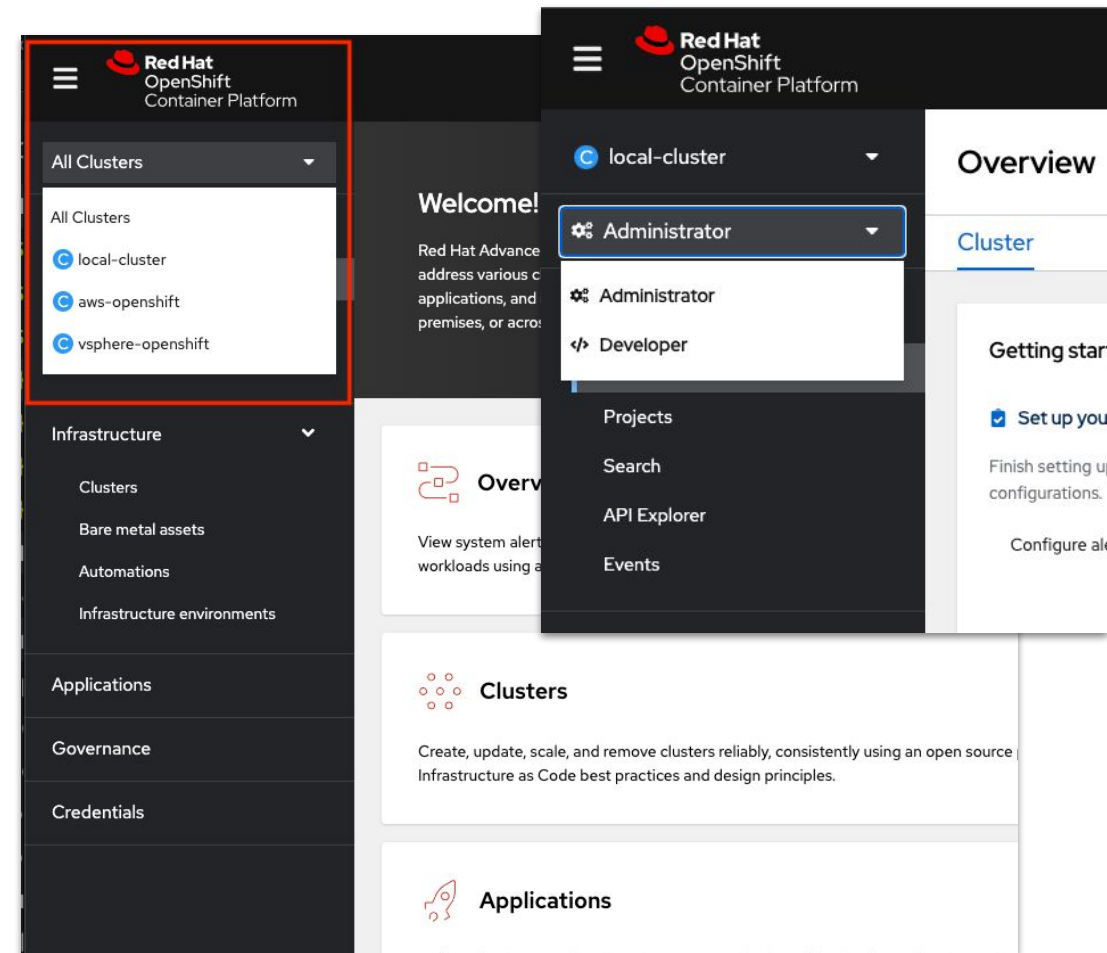
Experience allows users to select clusters across their company as they enter the hub cluster's OCP console! Bringing together 3 tools into one UX:

- ▶ OpenShift Console (OCP) - main user experience for all individual clusters
- ▶ Multicluster Engine (MCE) - offers basic cluster inventory/create/update/destroy
- ▶ Advanced Cluster Management (ACM) - full multi-cluster management

Moving from single cluster to a fleet of OpenShift:

1. Start deploying apps on a single OpenShift cluster
2. Use the Multicluster Engine to create more clusters and enable RBAC controlled multi-cluster views
3. Upgrade with Advanced Cluster Management to simplify multi-cluster configuration, application deployment, observability, networking, and more.

All OCP customers get MCE included in their subscription



Console Extensibility

Dynamic Plugins

Tech Preview

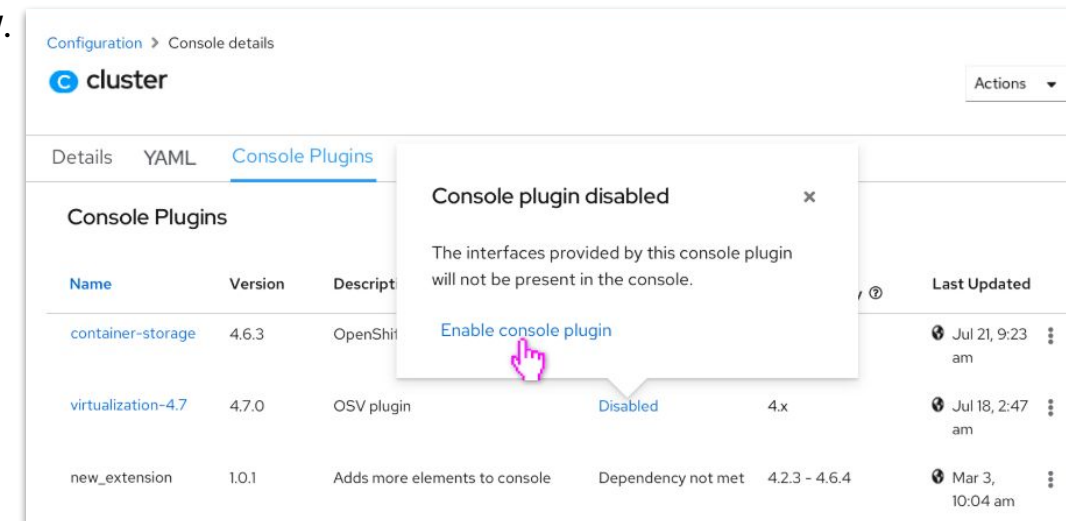
What is a dynamic plugin?

- ▶ Dynamic Plugin enables partners & customers to build high quality, unique user experiences **natively** in the OCP Console !
- ▶ Update existing perspectives
 - ▶ Add new flows, pages, actions, to either the Admin or Dev perspectives
- ▶ Add new perspectives
 - ▶ Create persona or task based perspectives based on your needs

Dynamic Plugin Technical Details

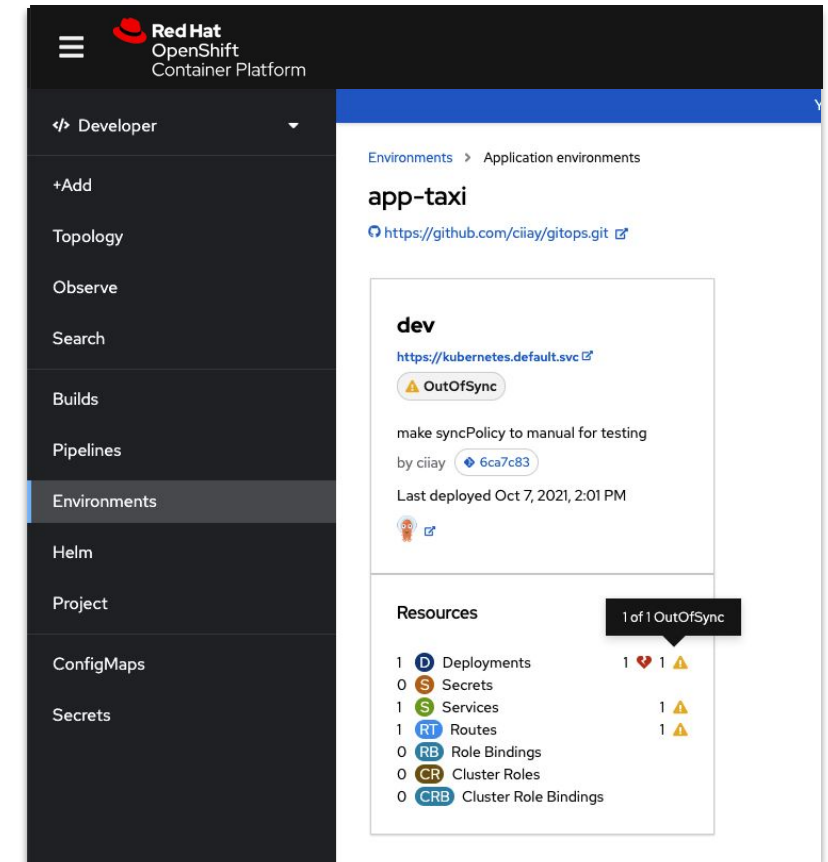
How does it work?

- ▶ Based on [webpack 5 module federation](#)
- ▶ Built with [PatternFly 4](#) components
- ▶ Plugins are dynamically loaded at runtime & dis/enabled via Console UI
- ▶ Plugins can be updated independently of the host application
- ▶ Plugins provide extension points or whole perspectives
- ▶ ACM is built with Dynamic Plugins and will give us the ability to extend the Multi Cluster view.



OpenShift GitOps

- ▶ OpenShift GitOps 1.5
- ▶ Provides Argo CD 2.3
- ▶ New generators in ApplicationSets
 - ▶ Generate Application for pull requests
 - ▶ Merge result of multiple generators
- ▶ Support for ignoring managed fields by specific managers
- ▶ Respects “ignore differences” setup during sync for objects and fields owned or mutated by operators
- ▶ [Dev Console] Health status for resources added

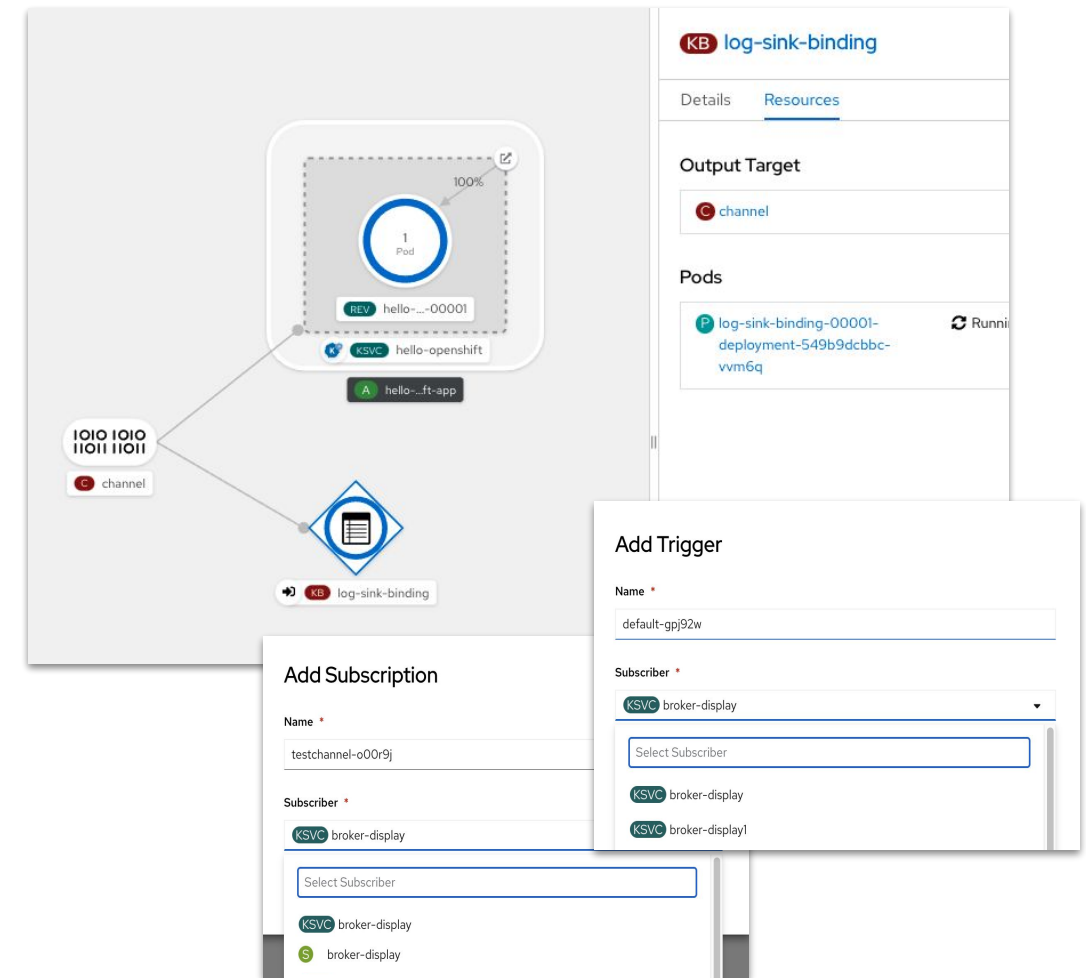


OpenShift Serverless

Key Features & Updates

- ▶ Update to Knative 1.0
- ▶ Apache Kafka based Knative Broker (**Tech Preview**)
 - ▶ Maximises Kafka performance and avoids events duplications
 - ▶ Prevents tight coupling with Kafka and eliminated the use of Kafka client by event producers
- ▶ Knative Kafka Sink (**Tech Preview**)
 - ▶ Recieve CloudEvents from Source/Subscription/Trigger on a Kafka topic, without writing custom code
- ▶ Developer Experience:
 - ▶ Support for developing, debugging and testing EDA applications by sending CloudEvents via the kn CLI (**Tech Preview**)
 - ▶ Visualization of Event Sink on Dev Console
- ▶ Functions (**Tech Preview**)
 - ▶ Node.js, TypeScript, Quarkus, Python, Rust, Go & Spring Boot
 - ▶ Available on MacOS , RHEL, Windows with Docker and/or Podman
 - ▶ Local Development and Testing for quick iteration

Event Sink & Event Source visualization



Conditional Updates

Evaluate risk before updating

- ▶ Update Service declares **conditionally recommended updates** associated with known risks
- ▶ Cluster Version Operator (CVO) **continually evaluates known risks** associated with updates
- ▶ Update recommended when no risks found

```
# View description of the update when it is not
recommended because a risk might apply.

$ oc adm upgrade --include-not-recommended

# Evaluate for potential known risks and decide if
acceptable for current cluster, then waive safety guards
and proceed the update.
# <version> is the supported but not recommended update
version you obtained from the output of the previous
command.

$ oc adm upgrade --allow-not-recommended --to <version>
```



Syncing group membership from identity providers

Connect Groups to RBAC

- ▶ 4.10 release introduces support for synchronizing group membership from an OpenID Connect provider to OpenShift Container Platform upon user login.
- ▶ You can enable this by configuring the groups claim in the OpenShift Container Platform OpenID Connect identity provider configuration.

```
apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
  name: cluster
spec:
  identityProviders:
    - name: oidcidp
      mappingMethod: claim
      type: OpenID
      openID:
        clientID: ...
        clientSecret:
          name: idp-secret
        claims:
          preferredUsername:
            - preferred_username
          name:
            - name
          groups:
            - groups
      issuer: https://www.idp-issuer.com
```



OpenShift Virtualization

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

Enhanced Data Protection

- ▶ VM backup and restore built into OADP
- ▶ Disaster recovery workflows coordinated through ACM

Additional Deployment Options

- ▶ Small footprint in resource constrained deployments e.g. SNO
- ▶ IBM Public Cloud Bare Metal (**Tech Preview**)

Operational Enhancements

- ▶ Composite applications (container & VM) in same Service Mesh
- ▶ Enhanced Virtual Machine Workflow Management

Workload Acceleration

- ▶ Accelerate compute and 3D apps with shared vGPU resources

"Red Hat technology stands out from the competition in terms of its ability to run virtualized workloads and container workloads in a streamlined and well-integrated manner. Red Hat allows us to deliver value to our users more quickly, minimizing time to market and accelerating the software development lifecycle."

Gökhan Ergül
CTO,
sahibinden.com

sahibinden.com



Application VMs
to Kubernetes



Cloud-native
VMs



Support GPU
acceleration



Telco - path to
Kubernetes or
remain as VM



Compact
clusters
at the edge

VM lift-and-shift to OpenShift

Migration Toolkit for Virtualization 2.3

MTV 2.3 is adding **warm migration** capabilities for both VMware and RHV to OpenShift Virtualization

Warm migration reduced the amount of downtime by pre-copying the data from disks before the final shutdown and reboot of your VM on the destination platform.

The image displays two screenshots of the Migration Toolkit for Virtualization (MTV) 2.3 web interface. The top screenshot shows the 'Providers' page under the 'VMware' tab, listing three vCenter instances (VCenter1, VCenter2, VCenter3) with their endpoints, cluster counts, host counts, VM counts, network counts, data counts, and status (Ready). The bottom screenshot shows the 'Migration plans' page, listing two plans: 'plantest-1' (Running) and 'plantest-2' (Ready). The 'plantest-1' plan shows a progress bar for '0 of 2 VMs migrated'.

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



Vielen Dank!
Thank you!
Merci!



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat