What's Next in OpenShift

Q4 CY2024

OpenShift Product Management

Speakers

Oren Kashi

Duncan Hardie

Radek Vokal

Shreyans Mulkutkar

Maria Simon

August Simonelli

Ali Mobrem

Hari Rakotoranto

Red Hat

Creating value depends on the ability to develop and deliver high-quality applications (*and AI models*) faster on any cloud

Improve digital
customer experience

Gain competitive
advantage

Mitigate risks

Red Hat

The Challenges

Application Modernization

80%

of enterprise technologists surveyed **plan to modernize** more than half of their legacy applications **in the next 2 years**.

Source: The Newstack

Rise of Generative AI

80%

of Enterprises will have deployed **Generative AI-Enabled Applications** by 2026

Source: Gartner

Developer Productivity

76%

of organizations say the **cognitive load is so high** that it is a **source of low productivity**. **Gartner** predicts **75%** of companies will establish platform teams for application delivery.

Source: Salesforce
Source: Gartner

Software Supply Chain Security

742%

Average **annual increase in software supply chain attacks** over the past three years. **45%** of organizations will experience attacks. **Is a matter of when, not if.**

Source: Sonatype

Red Hat

You need an application platform that is...

Trusted — **Comprehensive** — **Consistent**

Container engine   Application platform   Across hybrid cloud

| Reduce Risk | Improve Productivity | Increase Flexibility |

Red Hat is *a Leader* in the 2024 Gartner® Magic Quadrant™: Container Management and 2024 Gartner® Magic Quadrant™: Cloud Application Platforms

Source: Gartner, "Magic Quadrant for Container Management," Dennis Smith, Tony Iams, Wataru Katsurashima, Michael Warrilow, Richard Watson, 10 September 2024

Source: Gartner, "Magic Quadrant for Cloud Application Platforms," By Tigran Egiazarov, Mukul Saha, Anne Thomas, Steve Schwent, 4 November 2024

The Road Ahead

Manage at Scale

Multicluster management and governance
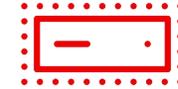
Cloud Services

Edge

Modernize Applications

Developer productivity

AI/ML (OpenShift AI, Lightspeed)
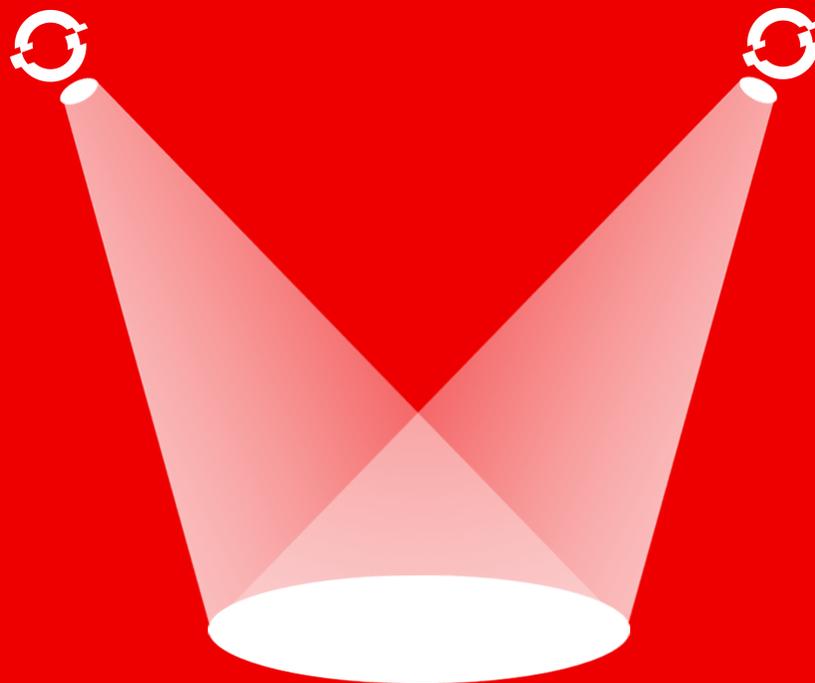
Simplify app connectivity

Modernize Infrastructure

OpenShift Virtualization

Universal Connectivity

OpenStack Services on OpenShift

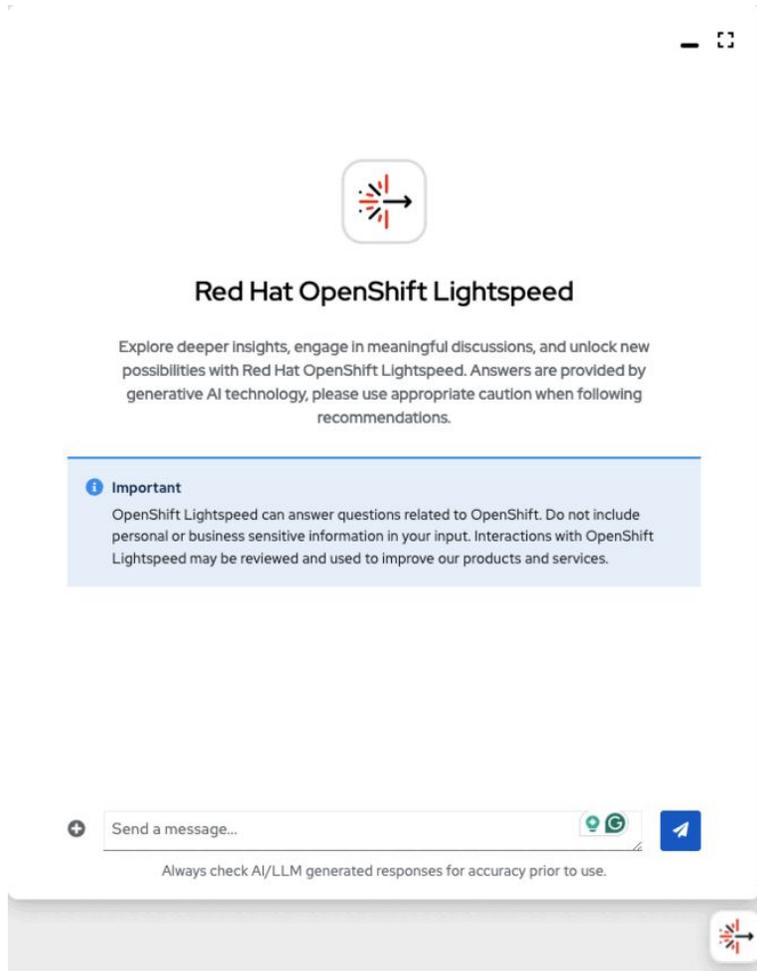Platform, Application, Security (Zero Trust, Trusted Supply Chain)

Red Hat

Spotlight Features

OpenShift Lightspeed
(Technology Preview)
Generative AI based chat assistant

Red Hat OpenShift Lightspeed

Explore deeper insights, engage in meaningful discussions, and unlock new possibilities with Red Hat OpenShift Lightspeed. Answers are provided by generative AI technology, please use appropriate caution when following recommendations.

> ℹ **Important**
> OpenShift Lightspeed can answer questions related to OpenShift. Do not include personal or business sensitive information in your input. Interactions with OpenShift Lightspeed may be reviewed and used to improve our products and services.

Send a message...

Always check AI/LLM generated responses for accuracy prior to use.

Help where you need it
Integrated directly into the Red Hat OpenShift web console

Explain, investigate and learn more
Provides assistance with explaining and investigating cluster resources

Generative AI
Powerful, pluggable LLMs combined with the latest OpenShift documentation
- RHEL AI
- Red Hat OpenShift AI
- OpenAI
- Azure AI
- Watson X

9

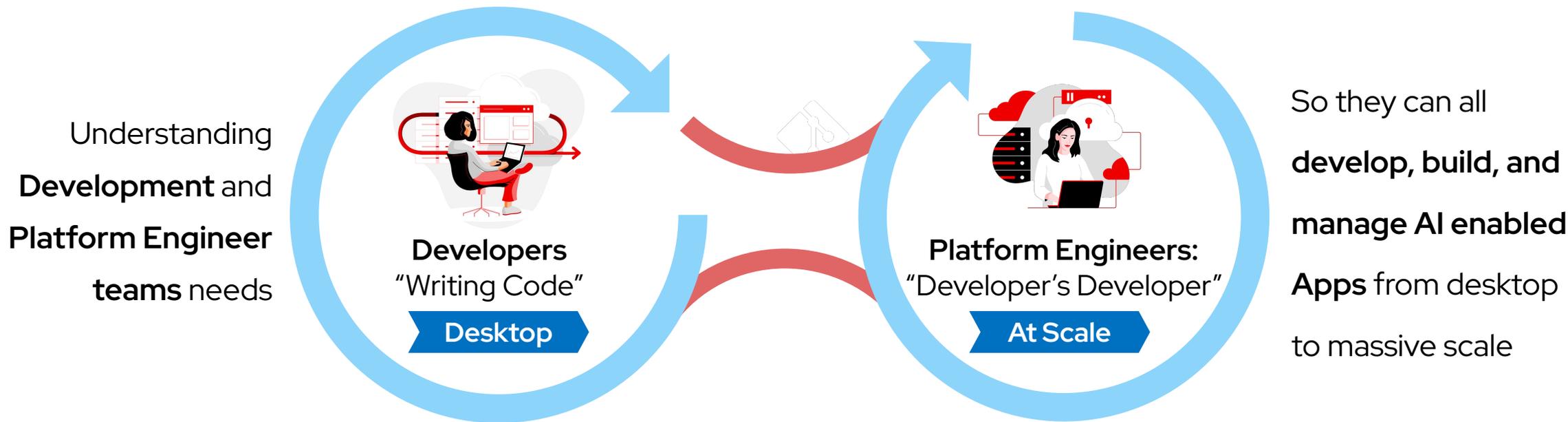**OpenShift Lightspeed**

OpenShift Lightspeed Roadmap

Now

- Interactive OCP documentation/help
- Attach feature to explain pod yaml , and debug log and alerts
- Disconnected cluster support
- Self-hosted model support through OpenShift AI's & RHEL AI's vLLM model serving runtime

Next

- Cluster-awareness and cluster interrogation
- BYO Knowledge
- Additional OpenShift products and knowledge sources
- Red Hat Insights integration
- Predictive Maintenance and Proactive Self-Healing

10

Application Services and Developers

Understanding **Development** and **Platform Engineer teams** needs

Developers
"Writing Code"

Desktop

Platform Engineers:
"Developer's Developer"

At Scale

So they can all **develop, build, and manage AI enabled Apps** from desktop to massive scale

---

Red Hat
Application Foundations

- Modernize existing Java EE/Jakarta EE investments:
  Red Hat JBoss EAP 8
- Accelerate workload migration to OpenShift:
  Migration Toolkits (MTV/MTA)
- Develop Cloud Native Java apps:
  Red Hat build of Quarkus
- Connect data across applications and services with
  3scale API Management, Red Hat build of Camel and **streams for Apache Kafka**

Red Hat
OpenShift Developer Services

- Internal Developer Portal (IDP):
  Red Hat Developer Hub
- Improve Containers Developer Desktop Experience:
  Podman Desktop
- IDE Tools:
  Red Hat IDE Plugins and **Red Hat OpenShift Dev Spaces**
- Secure and Trusted Software Supply Chain:
  Trusted Application Pipeline | Trusted Artifact Signer | Trusted Profile Analyzer

Red Hat
OpenShift AI

- Platform for AI enabled applications:
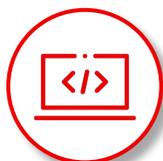 **OpenShift AI**

AI Enablement Tools: Code recommendations on Ansible: **Ansible Lightspeed** | **Coming in 2024:** AI to refactor Applications: **MTA (Migration Toolkit for Applications)**, AI Studio in **Podman Desktop**

AI and OpenShift

Run isolated AI/ML workloads

GPU support in **OpenShift sandboxed containers** via peer-pods

Protect data in use

Deploy AI apps in **Confidential Containers** to secure sensitive data

Improve GPU efficiency

DRA, Instaslice efforts, leverage **NVIDIA MPS GPU sharing** in OpenShift

Accelerate GenAI deployments anywhere and Deploy faster

Custom models with **NVIDIA NIM**, faster deployments with **precompiled signed drivers**

Provide Fair Scheduling

Bring **Kueue** into the OpenShift ecosystem providing best of breed

Provide choice and flexibility

A broad ecosystem of hardware accelerators with **AMD, Intel, and more**

Red Hat

OpenShift AI

MLOps platform for artificial intelligence/machine learning (AI/ML) use cases

MLOps

- ▸ Model registry enhancements
- ▸ NVIDIA Triton certified serving runtime
- ▸ Model serving inference graphs, A/B testing, canary rollouts
- ▸ AI explainability
- ▸ Data drift detection

GenAI

- ▸ RHEL AI / RHOAI integration – OOTB DS Pipelines, model registry integration
- ▸ Multi-node serving
- ▸ E2E tuning & eval experience
- ▸ LLM guardrails
- ▸ Distributed workloads Integration with Data Science Pipelines

Model development

- ▸ VS Code local IDE integration
- ▸ Feature Store
- ▸ Custom Workbenches enhancements

Platform and integrations

- ▸ AMD GPUs, Intel Gaudi Devices, IBM AIU
- ▸ Enhance data/model connections
- ▸ Fractional GPUs
- ▸ Expand admin UI config capabilities
- ▸ Designed for FIPS
- ▸ Public API and enhance GitOps support

13

Red Hat

OpenShift Virtualization

Modern infrastructure with proven KVM virtualization

Simplicity

- Enhancements to dedicated VM Admin view for easier navigation
- OpenShift Lightspeed offers guidance for VM workflow
- Workload mobility across clusters
- Expanded Guest OS migration for broader set of workloads

Enterprise Networking and Storage

- Improve tenant isolation with overlay tenant networks, with overlapping subnets
- Load balancing in ingress, microsegmentation, IPAM, and static IPs
- localnet and self-service overlay networks

Multi-cluster and Hybrid Cloud

- Multi-cluster Observability for VM management at scale
- Multi-cluster lifecycle operations enhancement
- Support for additional Public Clouds with bare metal installation
- Multi-arch support for Arm and LinuxONE s390 platforms

User Defined Networks (UDN)

A better solution for the monolithic layer 3 Kubernetes pod network

▶ Full support in OVN–Kubernetes

▶ A default network for OVN–Kubernetes components + VRF support for additional **isolated-by-default** UDNs

▶ One or more namespaces in each UDN (tenant)

▶ A pod or VM can be connected to different UDNs, each meant for a specific purpose

▶ Extend UDN into provider networks, so a VM can be directly referenced by its L2 network address, rather than requiring NAT translation at the cluster edge

▶ Support for:
- (Admin) Network Policy
- L2 & L3 UDN topologies
- BGP + EVPN w/ directly-referenceable VM static IPs
- VPC-like multicluster L3-to-L3 UDN connectivity (post–4.19)
- primary (default-route) and secondary UDNs
- overlapping pod IPs across UDNs
- clusterIP services and external services
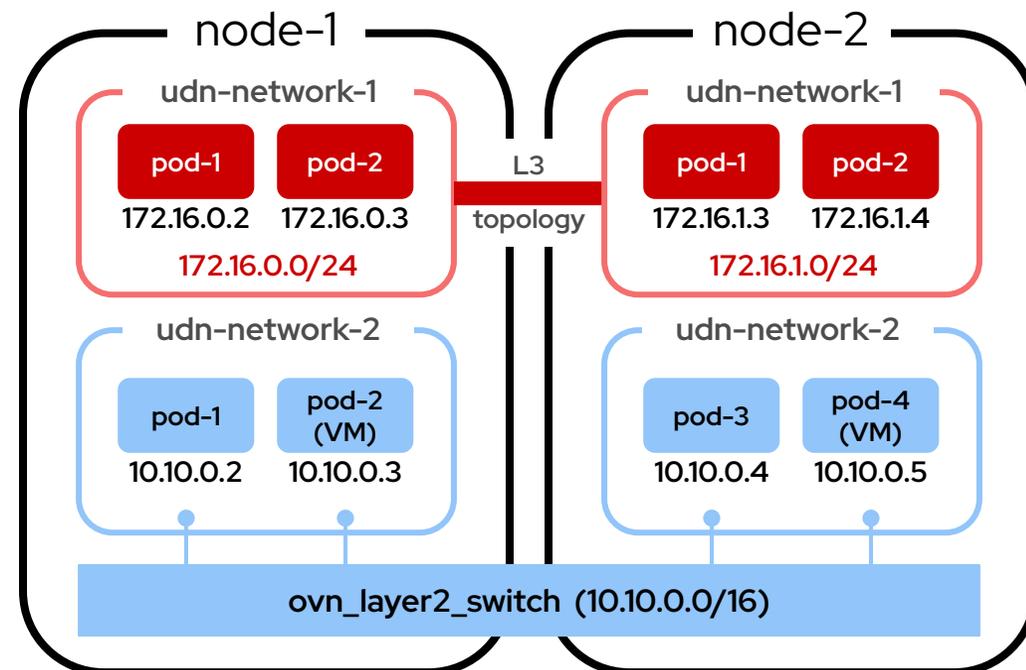
Core platform

Core platform

Provider Integrations, Installation and Updates

Platforms

- ▸ Add new clouds and platforms
- ▸ Add new regions
- ▸ Multiple architectures
- ▸ Enable third party integrations

⇨ **Enable Hybrid Cloud**

Installation

- ▸ Hosted Control Planes
- ▸ Composable installation
- ▸ New capabilities
- ▸ More flexibility

⇨ **Optimize onboarding**

Updates

- ▸ Improve update user experience
- ▸ N+3 skew updates
- ▸ Update progress monitoring

⇨ **Mitigate risk**

aws

Azure

IBM Cloud

Google Cloud

ORACLE CLOUD

17

Red Hat

Cloud

Consistency Across the Hybrid Cloud

aws

- Dual stack support
- Dedicated Host support
- User managed External DNS support
- Additional disks at install time
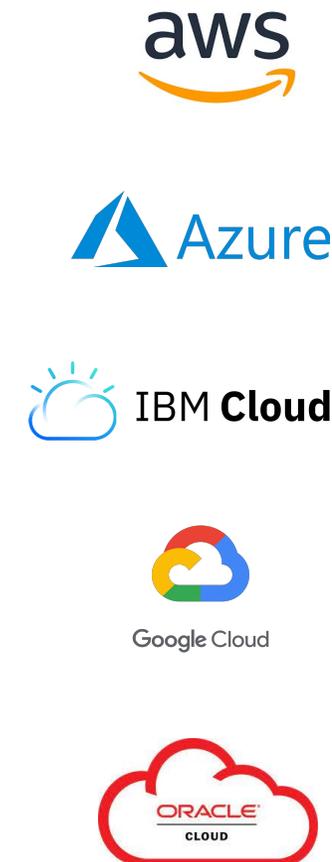
Google Cloud

- Dual stack support
- GCP bare metal support
- Support for OpenShift Virtualization

Azure

- Confidential VMs on Azure
- Dual stack support
- Dedicated Host support
- User managed External DNS support
- Additional disks at install time

ORACLE Cloud

- Oracle Cloud Infrastructure bare metal
- Oracle Private Cloud Appliance
- Oracle Compute Cloud @ Customer
- Support for OpenShift Virtualization

18

Red Hat

On-premises

Consistency Across the Hybrid Cloud

Bare Metal

- Day 2 firmware settings reconfiguration and firmware updates
- Hardware RAID support via Redfish
- BareMetalHost with self-signed CA certs for BMCs
- Bare Metal as a Service (BMaaS)
- Support for Network Controller Sideband Interface (NC-SI)

vmware vSphere

- OpenShift Zones support with Host Groups
- MachineSet support for more than one disk
- IPI support for multi-NIC VM
- Support for Multi-vCenter without shared storage

NUTANIX

- Static IP assignment
- Simplify add nodes on day 2 with Agent-based Installer

Red Hat OpenStack Services on OpenShift

- ShiftonStack on Red Hat OpenStack Services on OpenShift (RHOSO) architecture
- RHOSO multi cluster resource orchestration
- RHOSO multi-Openstack deployments
  - Under HCP
  - Under NameSpace isolation
- RHOSO Campus HA
  - RHOSO CTLPlane AZ awareness (stretched)
  - Dataplane AZ awareness

IBM Power Systems IBM Z and IBM LinuxONE

- Expand Compliance Operator Profile Support – PCI-DSS v4
- NFD support for nodes with Power
- Secure Execution for Agent-Based Installer on Z
- CSI driver support of IBM Z ICIC Management
- System Identification on IBM Z and LinuxONE

19

Hosted Control Planes and the Core Platform

Hosted Control Planes (HCP)

- **Streamlined** upgrades
- **Automated scaling** and delivery
- **Proactive debugging tools** for seamless installation and upgrades
- **IPSec/networking config parity** with standalone
- Expanded **metrics, alerts, and cost visibility** for better monitoring.
- Cross-management cluster **backup/restore**

Core

- Custom RHCOS **boot images**
- **Minimize workload disruption**
- Swap support for containers
- In-place **pod update**
- In-place **Vertical Pod Autoscaler update**
- Machine API to **Cluster API** migration

Storage

- **SMB CSI** GA
- **SecretStore CSI** GA
- **VolumeGroup Snapshot API** GA
- VolumeAttributeClass TP
- GCP hyperdisk support GA

Autoscaling

- Scale nodes with **Karpenter**

20

Control Plane Scalability and Resilience

- ▸ Cluster hibernation for up to 6 months

- ▸ Optimizations for recoverability of the control-plane

  - Automated control plane recovery procedure

  - Control-plane recovery on expired certificates

  - Automated backup of etcd database (BackupAPI)

- ▸ Selectable etcd database sizes

- ▸ Add Control Plane documentation section

- ▸ Hitless TLS Certificate Rotation for Kubernetes API

21

Red Hat

Red Hat Cloud Services

Red Hat OpenShift Cloud Services

Azure Red Hat OpenShift (ARO)

1. Managed Identities
2. Hosted Control Planes
3. Azure Lockbox Enhancements
4. Expanded regions and instance types
5. Support for SDN to OVN migration
6. Expanded instance type support

Red Hat OpenShift Service on AWS (ROSA)

1. Install/Operate HCP Clusters with No Public Egress required
2. Shared-VPC deployment
3. Support for SDN to OVN migration
4. AWS Windows license support
5. Capacity Reservation and Capacity Blocks for ML
6. New regions: Calgary, Tel Aviv, Malaysia
7. Expanded cluster image registry configuration

Product Managers: Aaren de Jong, Abhishek Gupta,, Bala Chandrasekaran, Jerome Boutaud, Oren Kashi, Shreyans Mulkutkar

Red Hat OpenShift Cloud Services

OpenShift Dedicated - Google Cloud
1. Support for upto 249 compute nodes
2. Wide range of GPU-enabled instances with deployment flexibility
3. OCP-Virt on OSD-GCP
4. Out of the box integration with Google Cloud NetApp Volumes

Product Managers: Aaren de Jong, Abhishek Gupta,, Bala Chandrasekaran, Jerome Boutaud, Oren Kashi, Shreyans Mulkutkar

Batteries Included...

(Workloads and Layered Offerings)

Red Hat

OpenShift Console

Building for the **future!**

- Content Security policy (CSP) for Console & Dynamic Plugins

- Gen AI Template offered in ODC

- Merge & Simplify Admin + Dev Perspective

- OLM v1 support in Console

- Support for Themes (PF6)

- Deprecation Pattern Fly 4

- Dynamic Plugin improved versioning support for multiple OpenShift releases

- RHDH Software Template Generator for OCP Applications

- Gen AI generated UI

Near Term

Long Term

Red Hat

OpenShift Service Mesh

- General availability of Red Hat **OpenShift Service Mesh 3.0!**
  - Istio multi-cluster support
  - Istio revisions & canary control plane upgrade support
  - Kiali 2.0
  - Istioctl support
  - IPv4/IPv6 dual-stack technology preview
  - Istio ambient mode (sidecar-less) developer preview

- Istio-csr support

- Istio ambient mode (sidecar-less) technology preview

- General availability of IPv4/IPv6 Dual Stack

- Istio ambient mode (sidecar-less) general availability

- External (Off Kubernetes) workload integration

- Multi-cluster service mesh management with Red Hat Advanced Cluster Management

- SPIRE + Istio support

Near Term

Long Term

Red Hat

OpenShift GitOps

- FIPS support
- Argo agent + ACM integration (Developer Preview)
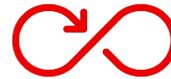
- Progressive sync GA
- Rollouts in OpenShift console
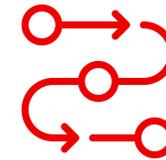
- Image updater GA
- Environment promotion and rollback

Near Term   **Long Term**

Red Hat

OpenShift Pipelines

Tekton's Path Forward

- TektonCD Pruner TP
- Tekton Results GA
- Concurrency Control with Pipelines As Code

- Expose more Tekton Metrics, Ship Tekton Metrics dashboard with Openshift Pipeline
- Caching Support for resolvers
- Pipelines in Pipelines

- Pipelines-as-code in multi-cluster environments
- Unified Tekton UI for a multi cluster environment

Near Term

Long Term

Red Hat

Product Managers: Koustav Saha

OpenShift Serverless

- General Availability for End to End encryption for services
- Function template – Python for AI
- Event Mesh
    - Auto Event Discovery
    - Catalog of pre factored Event Source and Event Sinks

- Serverless Workflow for AI Agent Composition
- Support for AWS Lambda Migration
- AI model Drift Detection

- Support integration of AI Services
- Knative Auto Scaler with KEDA
- Event Streaming Support
- Serverless on Edge

Near Term   **Long Term**

Red Hat

Builds for OpenShift

UX

- Create Shipwright Build flow in Console
- Migration guide form BuildConfigs

New ways to build

- Shipwright Builds on Arm, P/Z
- Build multi-arch images on multi-arch clusters
- Expanding community build strategies

Buildpacks

- Buildpacks build strategy GA
- UBI Buildpacks for Node.js and Quarkus

Red Hat

Operator Framework

*The future of the **next-gen OLM** → **OLM v1**, a more **robust** and **flexible** management experience*

Trusted

Comprehensive

Consistent

- **Declarative Operations**: Simplified APIs and **GitOps**/**ZTP friendly** operator management.

- **Platform-Wide Signature Trust**: Ensured **integrity** and **authenticity** of operator content.

- **Expanded Content Support**: Broader **interoperability** with **existing catalogs** and K8s manifests/**Helm charts**.

- **Efficient Catalog Content Service**: Optimized UI and CLI performance through **efficient metadata retrieval**.
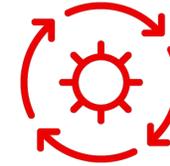
- **Standardized Interface**: **Predictable** user experience **regardless** of **packaging format**.

- **Standardized Operations**: **Declarative** workflows for install, update, and removal **across packages** and **infrastructures**.

Product Managers: Tony Wu, Daniel Messer

Red Hat

Red Hat Quay
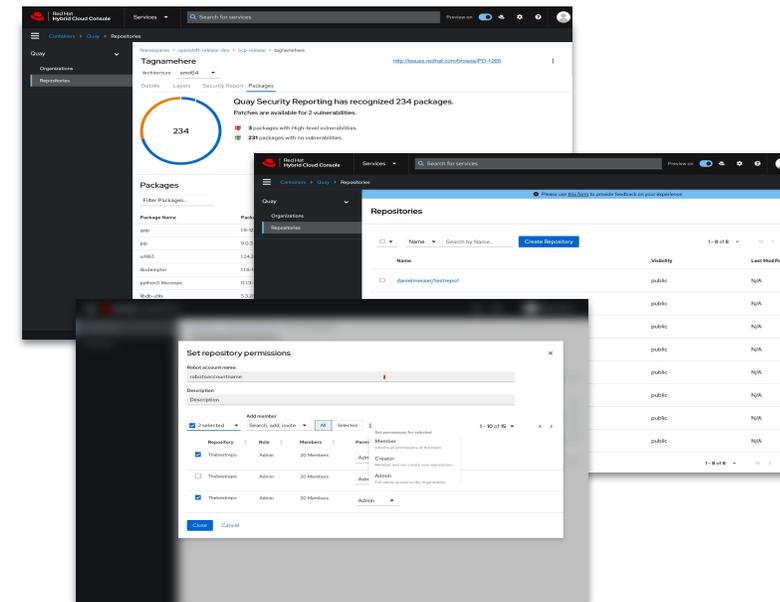## Next Gen Storage and UI

ML Model Storage

Quay and Openshift Model Registry teams will collaborate to support ML model storage
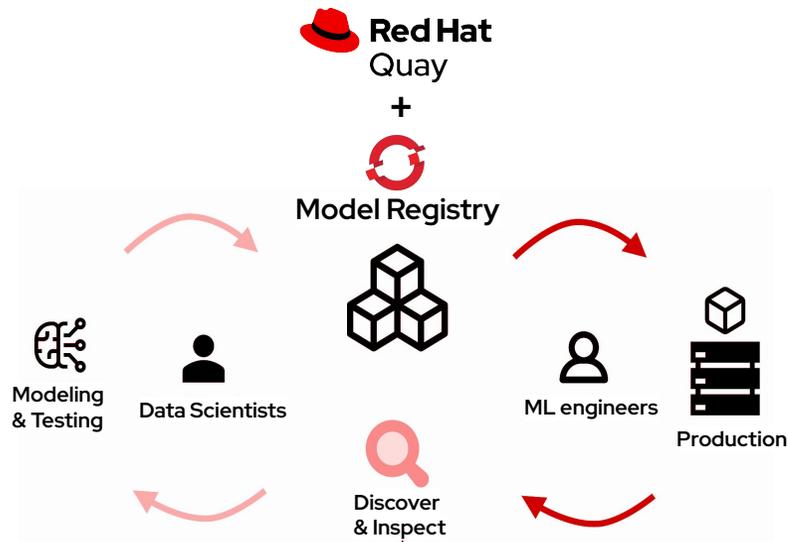
First-Class New UX

When parity is met with the old UI, all investment will go towards building functionality **only** on top of the new default UI
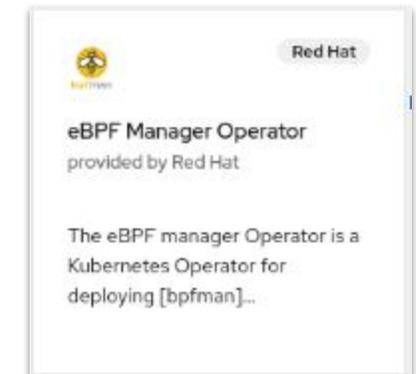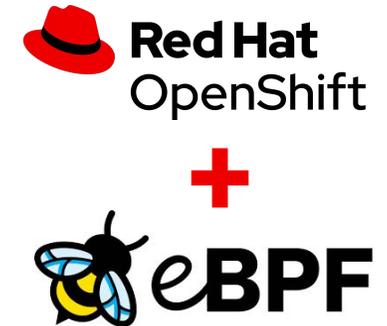
Networking and Observability

Product Managers: Marc Curry, Deepthi Dharwar, Roger Floren, Jose Gomez-Selles, Vanessa Martini, Jamie Parker, Radek Vokal

eBPF Manager

An eBPF program **manager** and **gatekeeper**

- ▶ 2nd Technology Preview release at OpenShift 4.18

- ▶ eBPF Manager (upstream: "bpfman") notable features:

  - **System Overview** (provide insights on eBPF programs)
  - **eBPF Program Loader**
  - **eBPF Filesystem Management**   ensure the secure deployment of eBPF applications

- ▶ Optionally installed from Operator Hub

- ▶ Secure and manage all user and OpenShift eBPF implementations

  - e.g. Ingress Node Firewall, Network Observability Operator

- ▶ Currently in CNCF Sandbox

bpf man

Red Hat

eBPF Manager Operator
provided by Red Hat

The eBPF manager Operator is a
Kubernetes Operator for
deploying [bpfman]...

35

Next-gen Ingress and Network Observability

gateway api

- aka Kubernetes "Ingress API v2"
- Optional enablement (HAProxy is default)
- Expressive, portable, and extensible API
- Role-based configuration layers
- Simplified configuration
- Enhanced scalability
- Advanced traffic management
- Increased security
- More information

Ingress Component Analogs

OpenShift router ➔ Istio
HAProxy ➔ Envoy
IngressController ➔ Gateway
Route ➔ HTTPRoute

Network Observability (targeting v1.18+)

- Move the Operator into OpenShift console/core
- UDN enablement
- Multi-cluster enablement
- OpenShift AI deployment-specific metrics
- eBPF enhancements (modern TCx hook in kernel)
- korrel8r (combinatorial correlation between the Observability tools)
- Packet tracing
- IPsec / mTLS

36
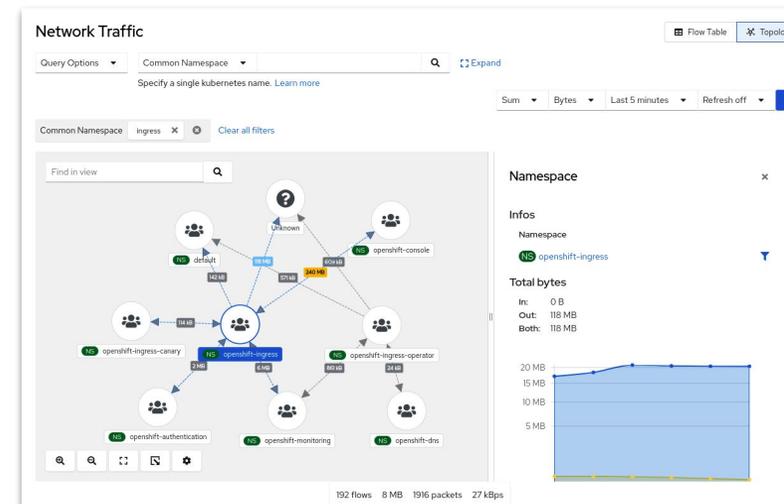
Observability Roadmap

redhat.com/observability

▸ **Building blocks** – for collecting, storing, and delivering relevant signals for our customers

▸ **Analytics solutions** to troubleshoot faster no matter the number of clusters to be managed

▸ **Single-pane-of-glass** for Observability no matter the number of clusters to be managed

▸ **Solution focused guidance** across Red Hat and 3rd party products
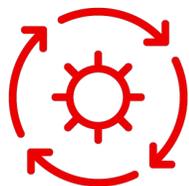
Collection, Storage & Delivery Mechanisms in OCP:

Expanding on **Cluster Observability Operator** – single and simple way to enable observability stack

Observability visualization in OCP:

Traces UI (GA)

Traces UI in **Developer Perspective**

Traces in **Pod** Page

APM Dashboards

OpenTelemetry support in **Logs UI**

Observability troubleshooting journey in OCP:

Incident detection / Red Hat Insights (TP) observability **signal correlation** (GA)

Incident detection & observability **signal correlation** integration

Observability

Enhancing Sustainability & OPP

Sustainability

Collect, Store & Aggregate

- New power monitoring capabilities incoming, such as **AMD & ARM CPU, & NVidia GPU**
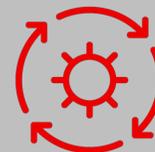
Analyze

- Upcoming improvements allow for **monitoring & optimizing performance metrics** – particularly Kube API load

Visualize

- Dashboards can display **total energy consumption** by a cluster in the last 24 hours & the amount of power consumed by the **top 10 namespaces** in a cluster in the last 24 hours

OpenShift Platform Plus

Collect, Store & Aggregate

- Cluster Logging Operator delivered in ACM via the **MultiCluster Observability AddOn (MCOA)** – Dev Preview

Analyze

- Improved **troubleshooting journey** with Incident Detection
- Consolidated **Right Sizing** recommendations

Visualize

- Unified & customizable **dashboards** in RHACM Console / Perses – Dev Preview
- Improved **Observe>Alerting UI** in RHACM console

38

Observability

Enabling Virtualization & AI

Virtualization

Collect, Store & Aggregate

- **Aggregate logs** from OpenShift Virtualization via rsyslog and HTTP with Cluster Logging Operator
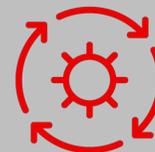
Analyze

- **Right Sizing** recommendations for OpenShift Virtualization (ACM)

Visualize

- Perses integration – more supported **charts** & a unified/customizable dashboarding experience (ACM) – Dev Preview

AI

Collect, Store & Aggregate

- OpenTelemetry integration story for **RHOAI, OpenLLmetry** & more

Analyze

- **OpenShift Lightspeed** & **Observability** integration story – ongoing PoC (OCP)

Visualize

- Dedicated **accelerators** dashboard in OCP web console

39

Red Hat

Observability connected

Insights services for OpenShift

Advisor

- Predicting risks, recommending actions
- Leveraging Red Hat experience with running/supporting OpenShift

Coming soon

- ▶ Incident detection for OCP
  - · <u>Development preview</u> available already, test it out!
- ▶ Rapid recommendations
  - · High quality proactive recommendations faster

Cost Management

- Visualize and distribute costs and into business-meaningful items
- Cost visibility and allocation for cloud, OpenShift and VMs (incl. non-RHEL)
- Cost models enable flexible cost distribution

Coming soon

- ▶ Itemized cost of AWS EC2 instances (incl. non-RHEL)
- ▶ Itemized cost of OpenShift Virtualization VMs (incl. non-RHEL)
- ▶ Support ROSA Classic + HCP combined private offers
- ▶ Release Cost Management Metrics Operator through the Konflux secure development pipeline

Observability & Networking for AI

AI Workloads and AI–Powered

AI-Optimized Infra

▶ Support the specific networking behavior, configurability and observability required for common AI workload

▶ AI hardware (e.g. GPU, HPU) enablement

- OpenShift AI-certified partner solution integrations, SR-IOV for Arm
- Resource optimizations, capacity planning

▶ Based on specific industry's workload needs

- for example, high-throughput between GPUs, multiple networks

▶ OTEL instrumentation, resource optimization, cost management

OpenShift Lightspeed

▶ Develop prompts to simplify networking complexity

- e.g. "human language" to generate YAML (and the reverse operation)

▶ Tailored recommendations

41

Red Hat

Security

Platform Security and Red Hat Advanced Cluster Security
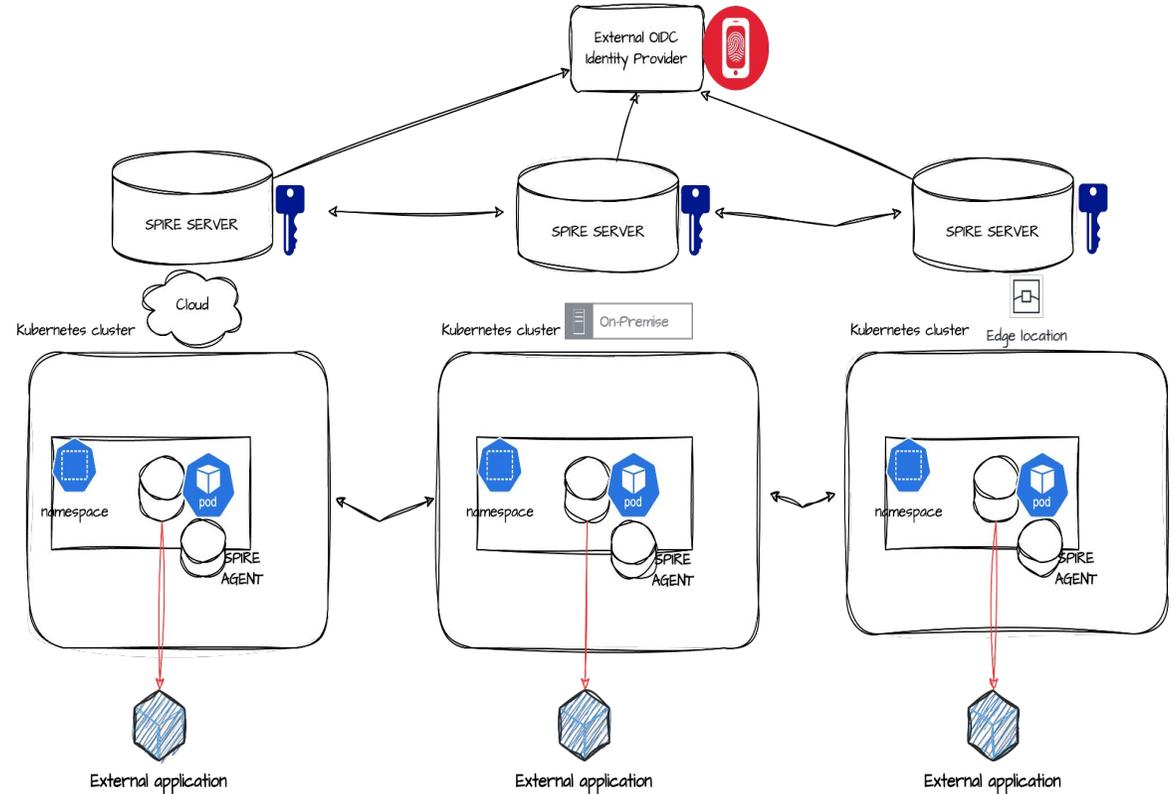
Red Hat

Trusted and Secure Platform

- **Bring Your Own external OIDC** for seamless multi-cloud authentication

- Pod Security Admission Integration - **Restricted Enforcement**

- **User namespace** support (GA)

- **Kube-KMS** support

- **Cert-Manager** enhancements - istio-csr integration, disconnected support, trust-manager integration

- **External Secrets Operator** support

- **SigStore** toolchain to sign and verify signed artifacts in OpenShift

- **Secret Store CSI Driver** GA with Cloud Secret Store CSI Providers

- **Confidential computing** enhancements

43

Red Hat

Multi-cloud Workload Identity with SPIFFE/SPIRE

Workload Identity Across Multi-Cloud and Multi-Cluster Environments

- **SPIFFE/SPIRE** for short-lived cryptographically-verifiable identities for Workloads.
- Supports OIDC Federation with External OIDC Identity issuers, SPIRE<>SPIRE Federation support for Cross-Cloud, Cross-Cluster usecases
- Works across On-prem, Cloud Hyperscalers, Edge
- Identity can be provided to VMs and Containers
- Node and Workload attestation before providing identities
- Day-2 Operator for Workloads-Only
- Integrates with existing solutions such as OpenShift Service Mesh, Identity Providers, *KS
- SPIFFE/SPIRE are Graduated-CNCF Projects that have been used in production. Tornjak for SPIRE User management is IBM-donated CNCF project.

External OIDC Identity Provider

SPIRE SERVER — SPIRE SERVER — SPIRE SERVER

Cloud — On-Premise — Edge location

Kubernetes cluster — Kubernetes cluster — Kubernetes cluster

namespace / pod / SPIRE AGENT

External application — External application — External application

Product Manager: Anjali Telang

Red Hat

Red Hat Advanced Cluster Security

Security across the entire application lifecycle

Vulnerability Management

Near term

- ▶ SBOM Generation based on scanned container images
- ▶ Enriched vulnerability data with exploit prediction scoring
- ▶ Z-stream based remediation guidance for RH OCP
- ▶ Scanning SBOMs for vulnerability reporting

Long term

Risk Profiling

- ▶ Action Driven Risk
  - · Custom rules support
  - · AI recommendations
  - · Improve Scoring

Compliance

- ▶ Compliance schedule reporting
- ▶ Workload Compliance
- ▶ Tailored profiles support
- ▶ Compliance trending

45

Product Manager: Maria Simon

Red Hat Advanced Cluster Security

Security across the entire application lifecycle

Security Policy Guardrails

Near term

- OpenShift GitOps (ArgoCD) support
- Policy as code API and roxctl support
- Violations reporting
- VAP Integration and additional policy engines

Long term

Network & Runtime

- External Entity IP visualization and threat detection
- Automatic alert on suspicious process and network activity
- Improved isolation insights with BANP/ANP and User Defined Networks
- Isolation for OCP Virt

Platform

- ACS data in Global Hub (ACM)
- ARM based secured cluster
- Runtime configuration
- Auto-rotation of ACS Internal Certs

46

Product Manager: Maria Simon

What's Next in Multicluster Management

With Red Hat Advanced Cluster Management

Product management team: Scott Berens, Sho Weimer, Christian Stark, Bradd Weidenbenner, August Simonelli

47

Red Hat Advanced Cluster Management

Roadmap Highlights

Cluster Lifecycle	Governance	Observability
• Cluster lifecycle for ROSA HCP • Backup and restore for local hosted control planes with ACM	• Display Kyverno Policies in Governance UI* • Support for ValidatingAdmissionPolicy in Governance UI	• Alert Management UI in ACM • Incident Detection based on Alert Grouping • Enhanced Observability with OpenShift Virt (network traffic, snapshots)
• Cluster lifecycle for ARO • Global Hub event driven workflow enhancements	• Governance dashboard refresh, integrated with multiple policy engines.	• MultiCluster Observability Addon (Logging, Tracing) • Unified Observability Dashboards within console (with Perses!)
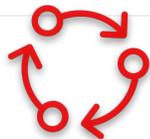
NEXT

FUTURE

Red Hat

* Red Hat support for Kyverno as a run-time policy engine is not being offered

Red Hat Advanced Cluster Management

Roadmap Highlights

|	Virtualization	App Lifecycle	Edge
NEXT	• Enhanced UI Integration of OpenShift Virtualization • Right Sizing for OpenShift Virtualization red.ht/ACMRightSize	• ACM addons to improve Gitops Integration with Argo	• Integration of Edge Management tooling (formerly known as Flight Control) into ACM.
FUTURE	• Create VMs from the ACM UI • Fine-grained RBAC for OCP Virtualization	• Argo CD agent and Addon for efficient deployments at scale • Progressive sync of Application Sets for reliable deployments at scale.	
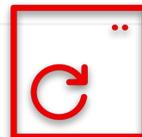
OpenShift for Telco and Edge

Product Managers: Franck Baudin, Daniel Fröhlich, Philippe Huet, Robert Love, Michal Zasepa, Hari Rakotoranto

EDGE

Red Hat Device Edge and MicroShift
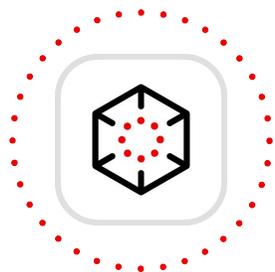
Extend Capabilities

Auto-Recover
TLS and Cypher Config
Gateway API (Dev Preview)
ISA 62443 compliance
Cert-manager
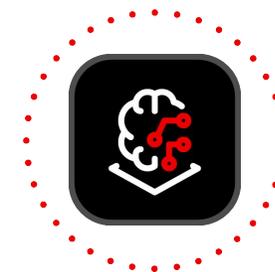
Simplify day2

Maintain the Base

Support RHEL Image Mode
Base Images for Image Mode
RHEL 9.6 and 10.x
Long Term RHEL9 support for
ISA V2

Stability and Simplification

Edgy AI Workload

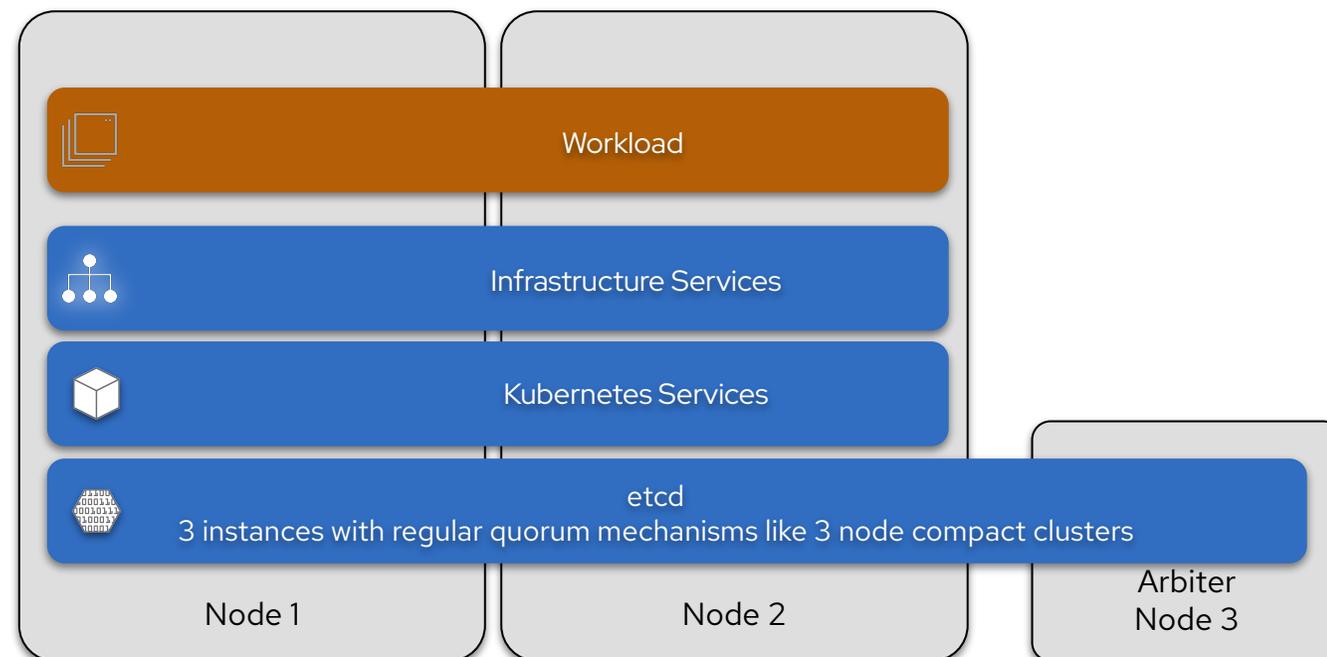Model Serving at the edge
with
OpenShift AI

Innovative use cases

# 2+1 **O**penShift with (*local)* **a**rbiter (OLA)

Approach:

- Two node solution for cost sensitive customers
- Small arbiter node, running only 3d etcd instance
- Behaves like a 3 node compact cluster
- Arbiter Node is a regular node and could be used to run additional components/workload
- Arbiter node can be co-located (e.g Dell PowerEdge XR4000 with witness sled)
- Arbiter node has to be within <500msec max effective end to end latency (incl. Disc io)
- OCP Virtualisation fully supported
- Hyperconverged Storage / SDS via Partners

Workload

Infrastructure Services

Kubernetes Services

etcd
3 instances with regular quorum mechanisms like 3 node compact clusters

Node 1

Node 2

Arbiter Node 3

Example HW appliance (all certified HW is okay) :

Dell XR4000

Arbiter Node

Timeline Targets:

- V4.18 Technology Preview, X86+Arm Bare Metal only
- V4.19 General Availability, X86+Arm Bare Metal only

Hat
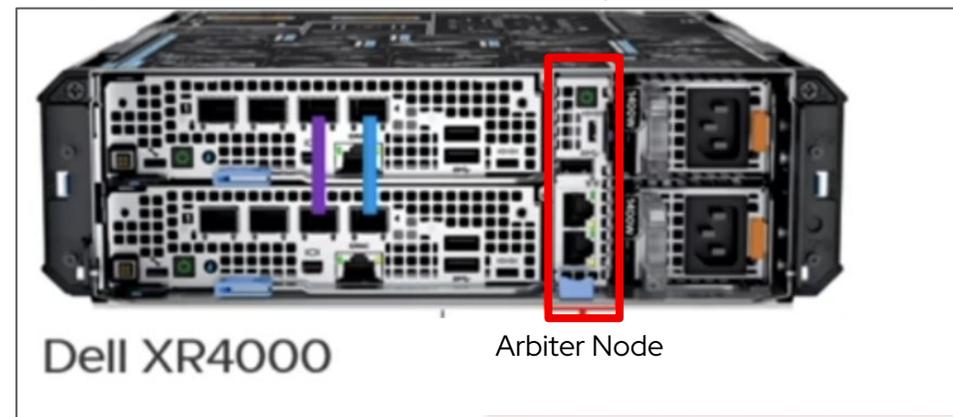
Two Node OpenShift with fencing (2NO)

Approach:
- True two node solution for cost sensitive customers
- Relies on proven RHEL–HA technologies (corosync, pacemaker) to provide etcd HA
- Uses fencing to protect against split brain situations
- Requires a Base Management Controller (BMC) that supporters RedFish for fencing
- Node local storage supported (e.g. LVMS)

Timeline Targets:
- V4.19 Technology Preview X86_64 only

Workload

Infrastructure Services

Kubernetes Services

etcd (Lead)

etcd (Follow)

RHEL HA
(Corosync, Pacemaker)

Node 1

Node 2

BMC used
for fencing
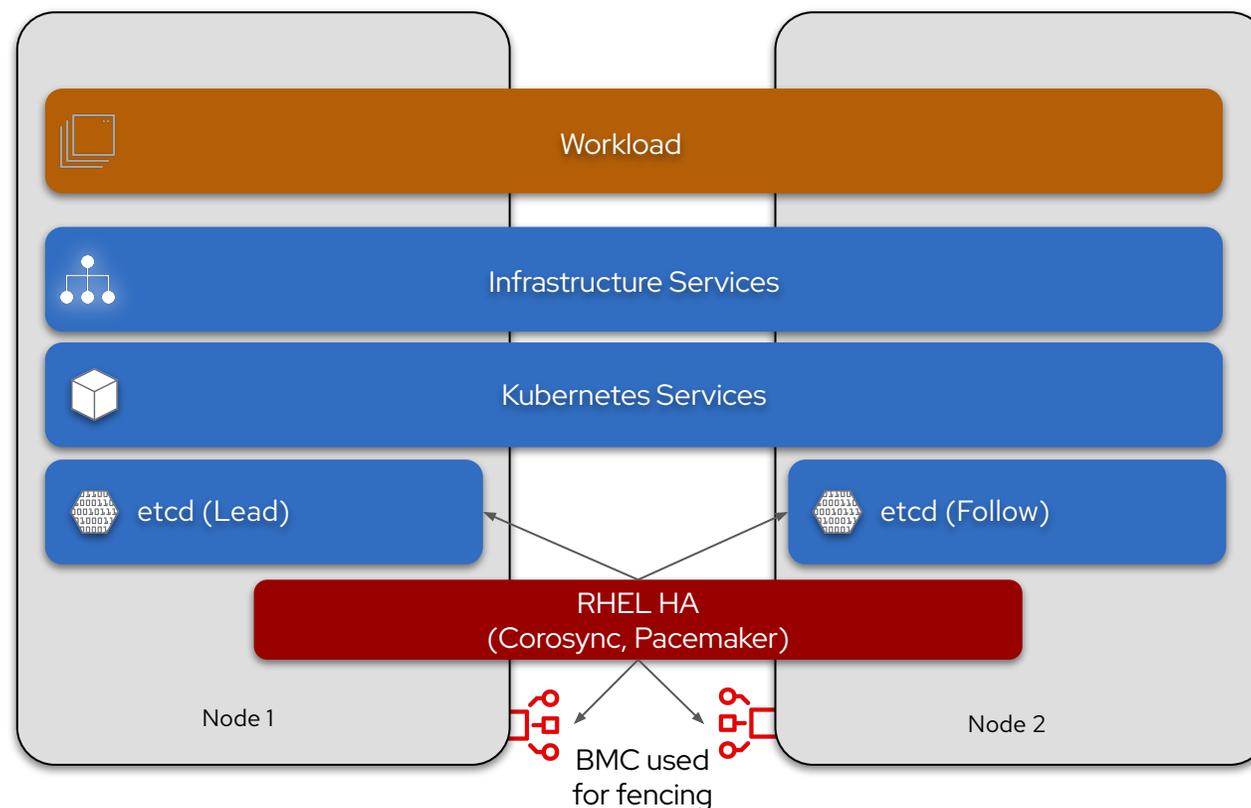
Steps to replace a DU-configured Single Node OpenShift using Image Based Break Fix (IBBF)

STEP 1
A seed-image generated from DU-configured Single Node OpenShift installation

STEP 2
The seed-image is then installed to any number of Far Edge servers

Staging Facility

STEP 3
Far Edge server shipped to Far Edge site, racked cabled and booted

STEP 4
Provisioning triggered by committing SiteConfig to git.

Config Repo

STEP 5
Hub Cluster components orchestrate SNO provisioning

Hub Cluster

STEP 6
Image Based Install Operator and Lifecycle Agent Operator orchestrate site-specific configuration for the new SNO

STEP 7
(CNF / Orchestrator functionality)
Orchestrator orchestrates CNF restoration process

Radio Site

- Procedurally similar to Image Based Install

Commercial DU site preparation

- Server is shipped to the Far Edge site

Technician Delivers Server

- Procedurally similar to Image Based Install
- Cluster identifiers retained from previous installation to maintain manageability and observability continuity

Commercial DU site upgrade

Activities which should be done before hardware failure.

Activities which are done after hardware failure.

Developer Preview to be available in 4.18

54

Telco - O-RAN

Problem statement: CSPs work on or consider Open RAN and O-RAN architecture implementation. They expect: better TCO, the same or better quality, and shorter TTM.

Red Hat Way to Standardized O-Cloud

## Continued Involvement in O-RAN

WG 6 (O-Cloud):
- Promote Kubernetes declarative paradigms and best practices
- Standardize a Cluster Template and O2ims provisioning/LCM API
- Drive the discussion about Energy Saving
- Continue participation in PTP and HW Acceleration

WG11 (Security):
- Continue participating in mTLS and OAuth 2.0

O-RAN Software Community:
- Work on the reference architecture with open-source components
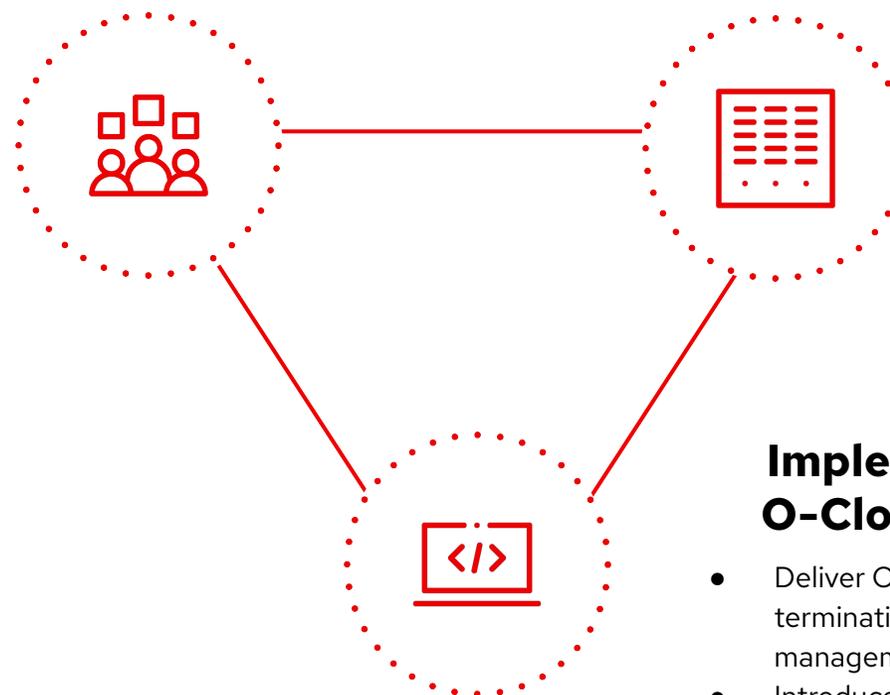
Cooperation with Partners

- Hardware vendor - to deliver together an O-Cloud, which manages CaaS and Hardware
- RAN Application vendors- to validate O-Cloud with RAN applications
- SMO vendors - to check the E2E O-RAN concept

Implementation of O-Cloud Use Cases

- Deliver O-Cloud Manager for O2ims termination and O-Cloud workflow management
- Introduce the Cluster Template concept and the SNO with DU profile deployment use case

55

Advanced IP traffic steering: scale up, simplify, keep enhancing
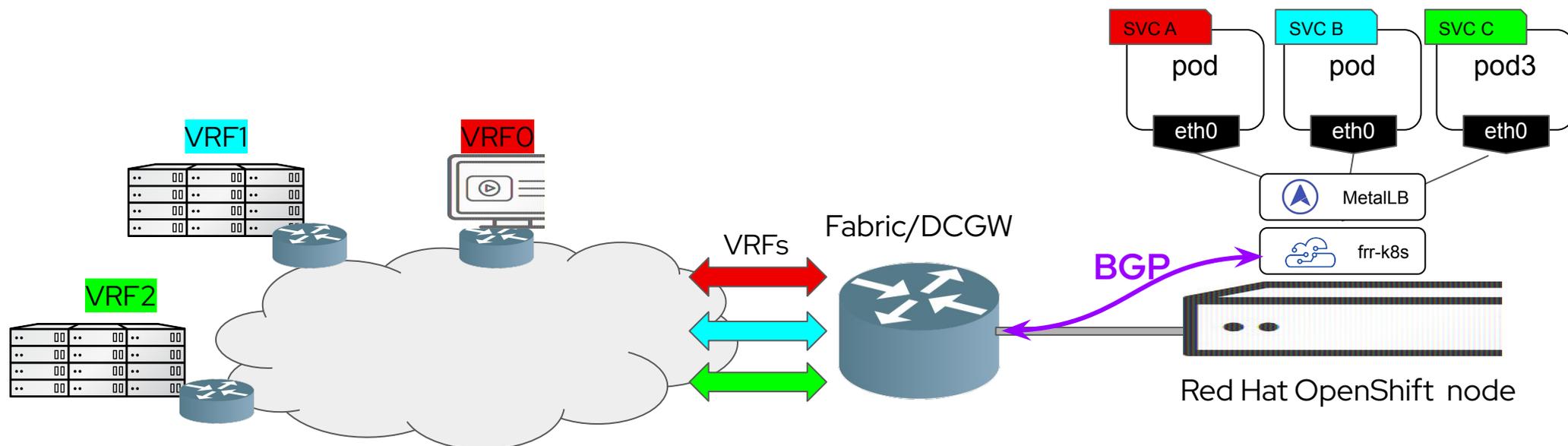
- ▶ Unnumbered BGP peering
- ▶ BGP Graceful Restart
- ▶ Dynamic AS number
- ▶ Egress IP as SVC
- ▶ Linux VRF

Thank you for joining!

What's New and What's Next

red.ht/whatsnew

Guided demos of new features on a real cluster

learn.openshift.com

OpenShift info, documentation and more

try.openshift.com

OpenShift Commons: Where users, partners, and contributors come together

commons.openshift.org

Red Hat