Red Hat Summit

Connect

What's New OpenShift

Journey to cloud

Mario Mendoza
Principal Solution Architect

Asier Cidón
Senior Cloud Architect

Red Hat | intel

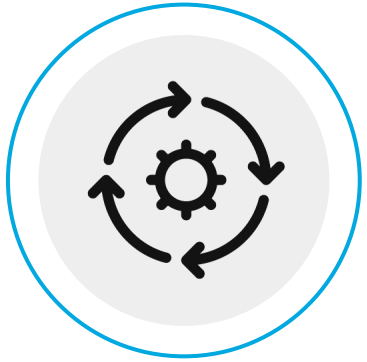
Red Hat customers have common needs & challenges

Hybrid cloud infrastructure

Build the foundation for the future, while managing costs to speed progress

Cloud-native development

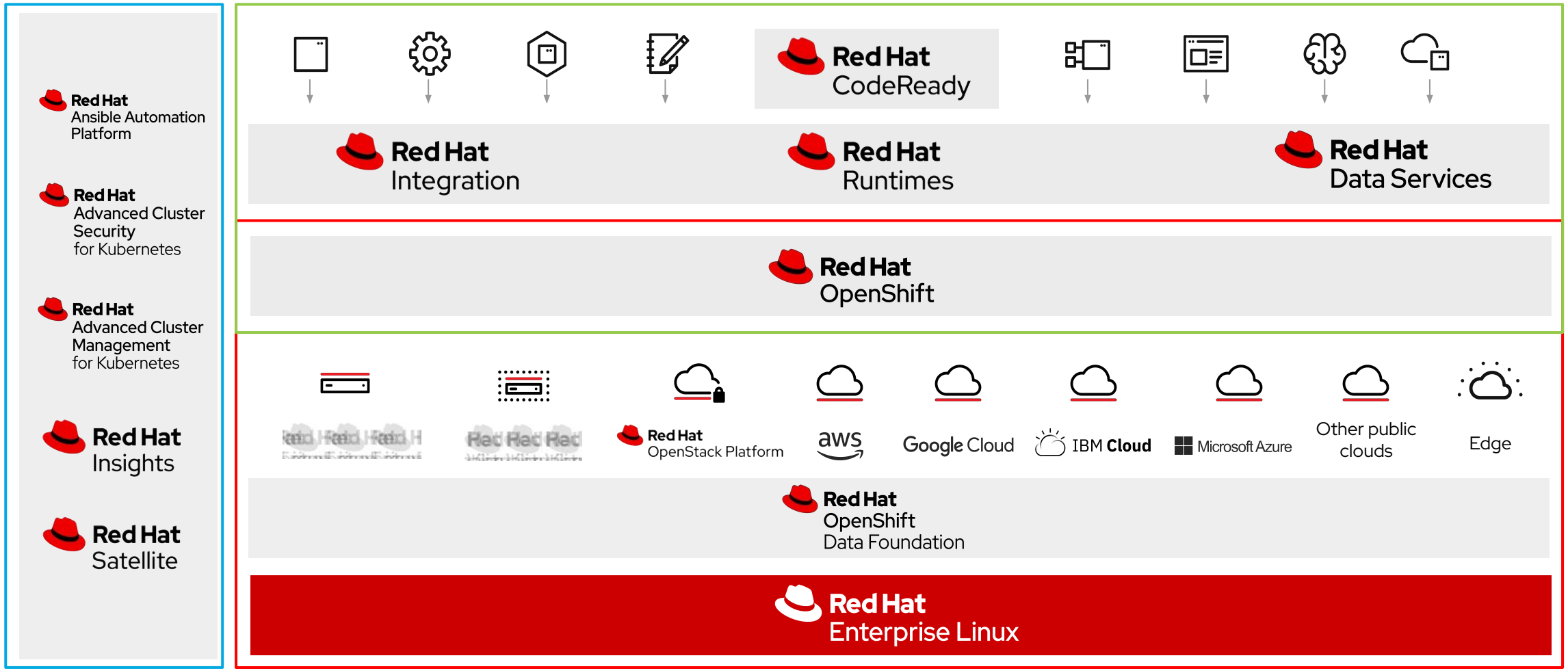
Accelerate application development, innovation, & delivery

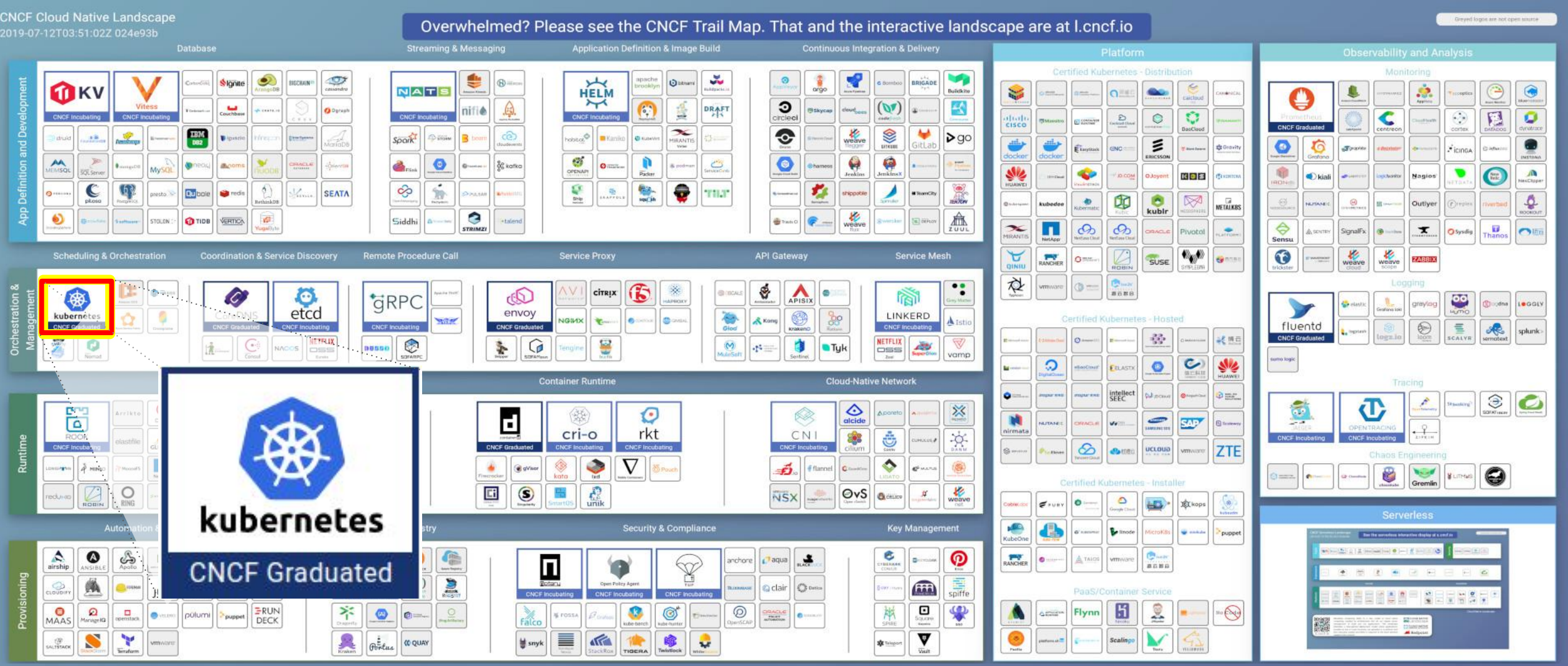


IT automation & management

Automate infrastructure & applications so you can do more without sacrificing stability

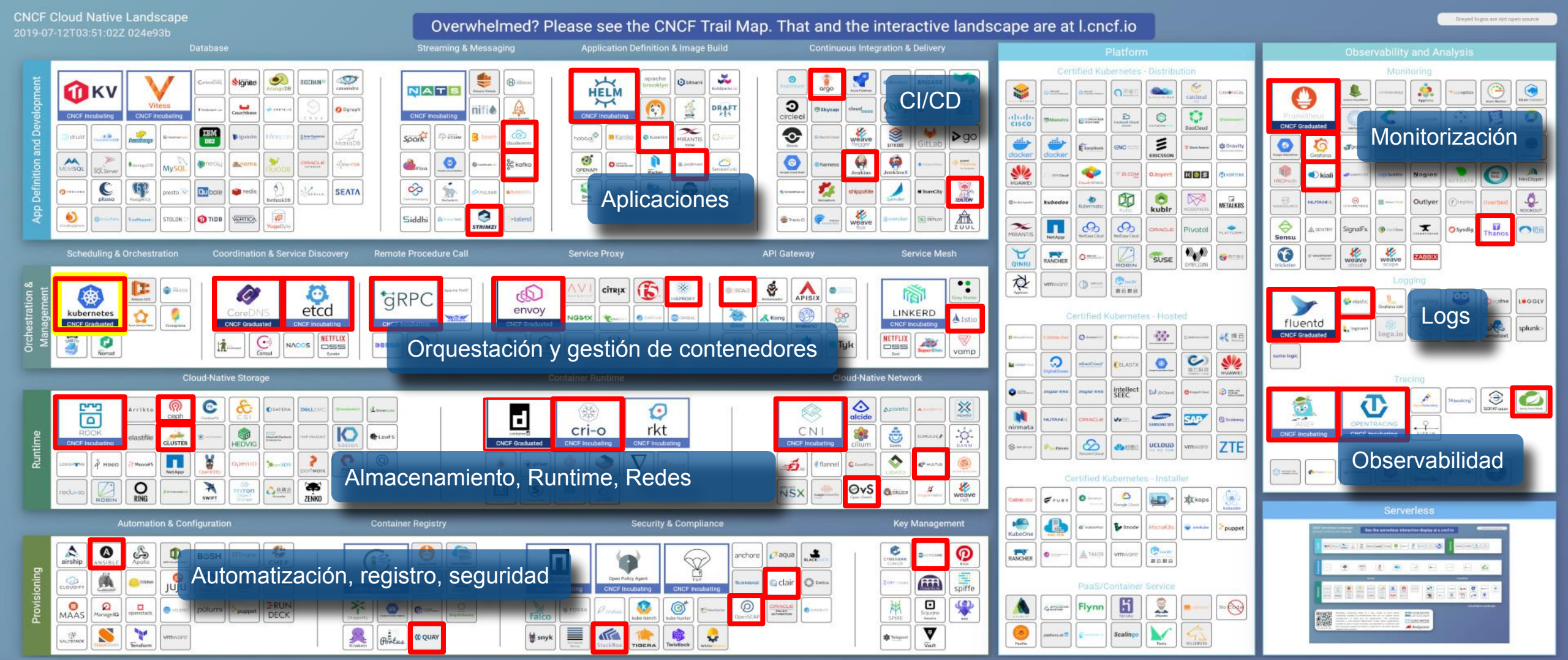
Addressing these challenges with a broad portfolio





CNCF is the open source, vendor-neutral hub of cloud native computing, hosting projects like Kubernetes and Prometheus to make cloud native universal and sustainable.

Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds.



Innovation
Standards
APIs

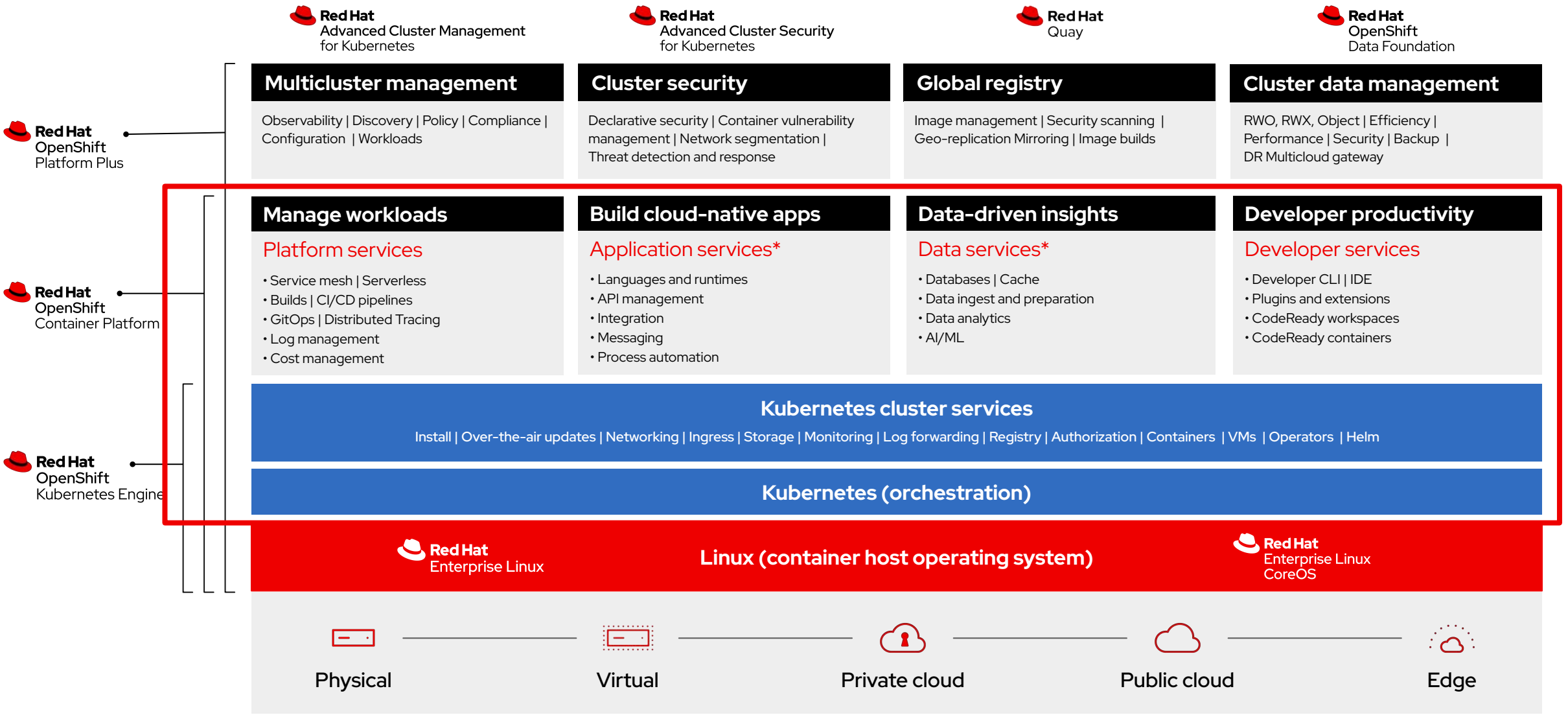
Community Projects

PARTICIPATE → **INTEGRATE** → **STABILIZE**

Enterprise Products

Support
Updates
Security
K.Base
Certification
Roadmap

Red Hat open hybrid cloud platform



Red Hat | intel

Red Hat open hybrid cloud platform

Red Hat OpenShift Platform Plus

Red Hat Advanced Cluster Management for Kubernetes	Red Hat Advanced Cluster Security for Kubernetes	Red Hat Quay	Red Hat OpenShift Data Foundation
Multicluster management	**Cluster security**	**Global registry**	**Cluster data management**
Observability | Discovery | Policy | Compliance | Configuration | Workloads	Declarative security | Container vulnerability management | Network segmentation | Threat detection and response	Image management | Security scanning | Geo-replication Mirroring | Image builds	RWO, RWX, Object | Efficiency | Performance | Security | Backup | DR Multicloud gateway

Red Hat OpenShift Container Platform

Manage workloads	Build cloud-native apps	Data-driven insights	Developer productivity
Platform services	Application services*	Data services*	Developer services
• Service mesh | Serverless • Builds | CI/CD pipelines • GitOps | Distributed Tracing • Log management • Cost management	• Languages and runtimes • API management • Integration • Messaging • Process automation	• Databases | Cache • Data ingest and preparation • Data analytics • AI/ML	• Developer CLI | IDE • Plugins and extensions • CodeReady workspaces • CodeReady containers

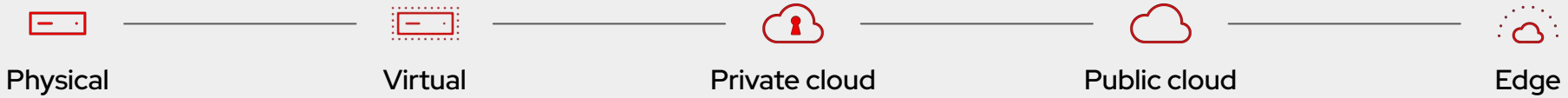
Red Hat OpenShift Kubernetes Engine

Kubernetes cluster services

Install | Over-the-air updates | Networking | Ingress | Storage | Monitoring | Log forwarding | Registry | Authorization | Containers | VMs | Operators | Helm

Kubernetes (orchestration)

Red Hat Enterprise Linux — **Linux (container host operating system)** — Red Hat Enterprise Linux CoreOS



Red Hat | intel

Hybrid Cloud

Red Hat | intel

What are Hybrid Cloud biggest challenges?

Be able to move workloads between environments

The platforms are often distributed across geographies for failover or data protection which comprise one or more types of operating systems, virtualization systems, private cloud deployments, or containerized infrastructure.

Orchestrate processes with the help of automation

Automation makes cloud infrastructure and applications more streamlined and less complex

Universal developer frameworks and tools

Develop and deploy apps as collections of small, independent, and loosely coupled services.

Incorporate a single, unified management tool

A unified management platform lets you view and manage private and public cloud resources, allocate resources, perform capacity planning tasks, monitor resource allocations and quotas, and a whole lot more from a single console.

Openshift 4.11 Supported Providers

Self Managed OpenShift

Red Hat OpenShift Container Platform

Everywhere
Baremetal, OpenStack, AWS, Azure, IBM Cloud, GCP, vSphere, Nutanix etc...

Provided by:
Red Hat/Partner
Managed by:
Cliente / Partners

Azure
aws
IBM Cloud
Alibaba Cloud
Google Cloud
Bare Metal
Azure Stack Hub
NUTANIX
IBM Z
IBM Power Systems
vmware vSphere
RED HAT OPENSTACK PLATFORM
RED HAT VIRTUALIZATION

The same platform on any environment, on-prem, private cloud, public cloud, self managed or managed by the cloud provider with Red Hat support

Provider Managed OpenShift

Self Managed OpenShift

Red Hat OpenShift Container Platform

Everywhere
Baremetal, OpenStack, AWS, Azure, IBM Cloud, GCP, vSphere, Nutanix etc...

Provided by:
Red Hat/Partner
Managed by:
Cliente / Partners

Red Hat OpenShift Dedicated

Red Hat OpenShift Container Platform

aws Google Cloud Platform

Provided and Managed by:
Red Hat

Azure Red Hat OpenShift

Red Hat OpenShift Container Platform

Microsoft Azure

Provided and Managed by:
Azure

Red Hat OpenShift Service on AWS

Red Hat OpenShift Container Platform

aws

Provided and Managed by:
AWS

RHOIC (aka ROKS)

Red **H**at **O**penShift on **I**BM **C**loud

Red Hat OpenShift Container Platform

IBM **Cloud**

Provided and Managed by:
IBM

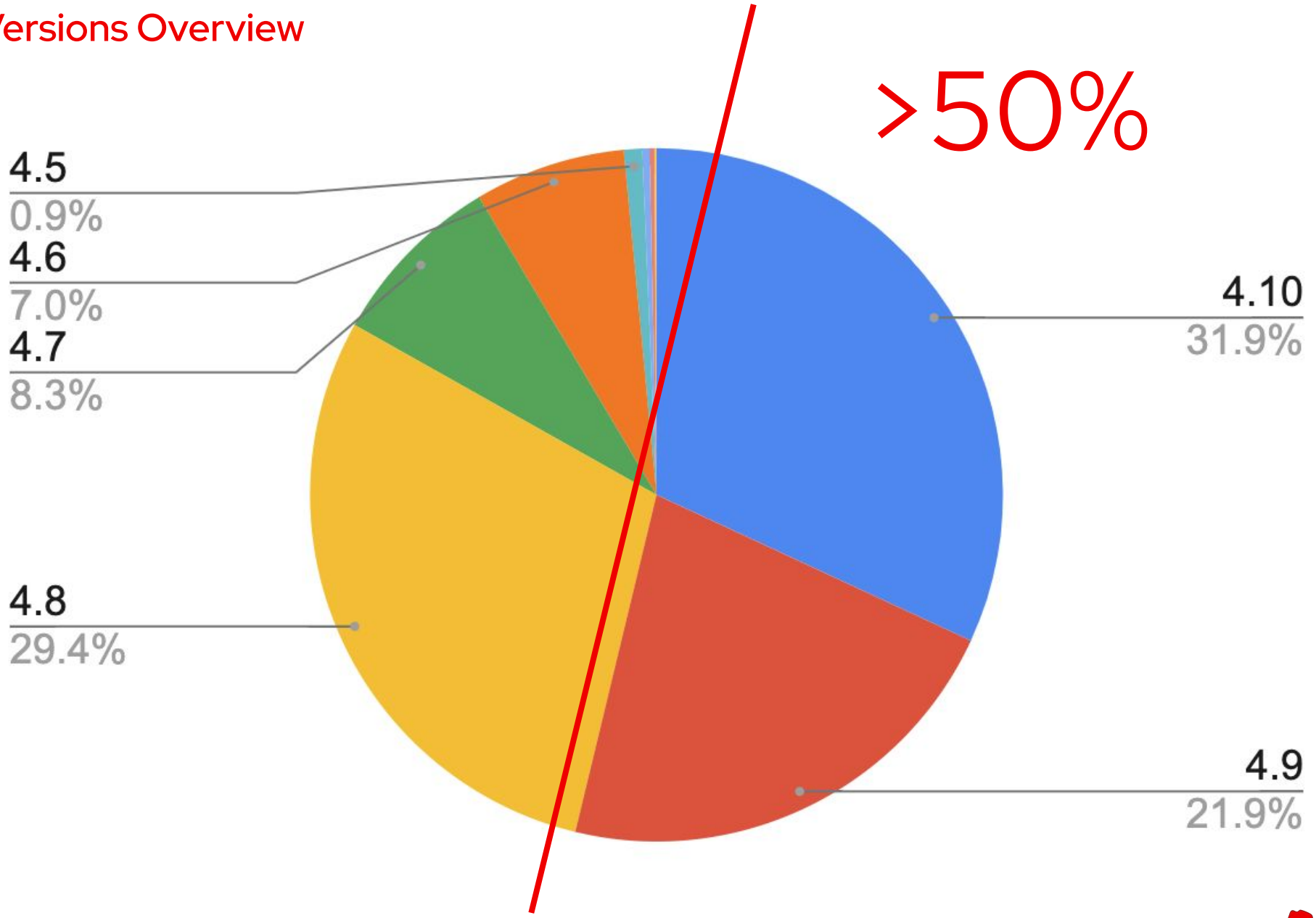
The same platform on any environment, on-prem, private cloud, public cloud, self managed or managed by the cloud provider with Red Hat support

Red Hat | intel

OpenShift 4.11 Supported Providers & Installation Experiences

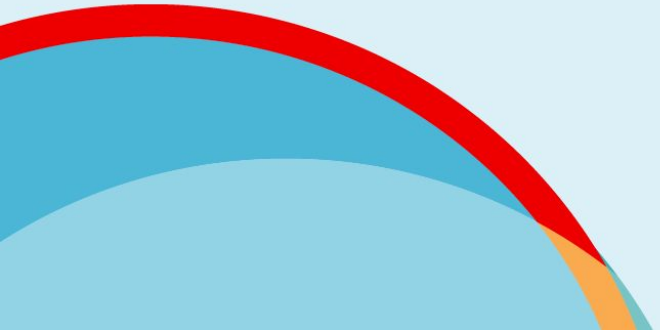
Provider	Full Stack Automation (installer-provisioned infrastructure) **IPI**	Pre-existing Infrastructure (user-provisioned infrastructure) **UPI**	Interactive **Connected** *(Assisted Installer)*	Interactive **Disconnected** *Agent-based Installer* Developer Preview
Alibaba Technology Preview	x			
AWS	x	x		
Azure	x	x		
Azure Stack Hub	x	x		
Bare Metal	x	x	x	x
Google Cloud Platform	x	x		
IBM Cloud Technology Preview	x			
IBM Power Systems		x		
IBM Z		x		
Nutanix AOS	x			
Red Hat OpenStack Platform	x	x		
Red Hat Virtualization	x	x		
VMware vSphere	x	x	x	

Fleet Versions Overview



Red Hat | intel.

Applications Architecture



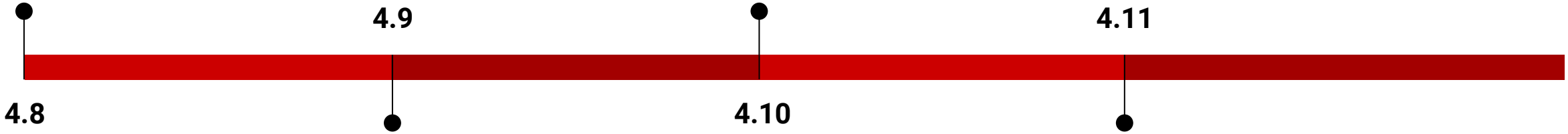
Red Hat | intel.

Cloud Native Apps Journey

Roadmap

- OpenShift Serverless Functions
- OpenShift Sandbox Containers TP
- Performance profile creator
- Vertical Pods Autoscaler
- Quarkus, Node.js, Python, Go and Spring Boot in Serverless

- OpenShift Sandbox Containers GA
- Virtualization supports Service Mesh
- OpenShift Event Bus Advancements for RAN Workloads

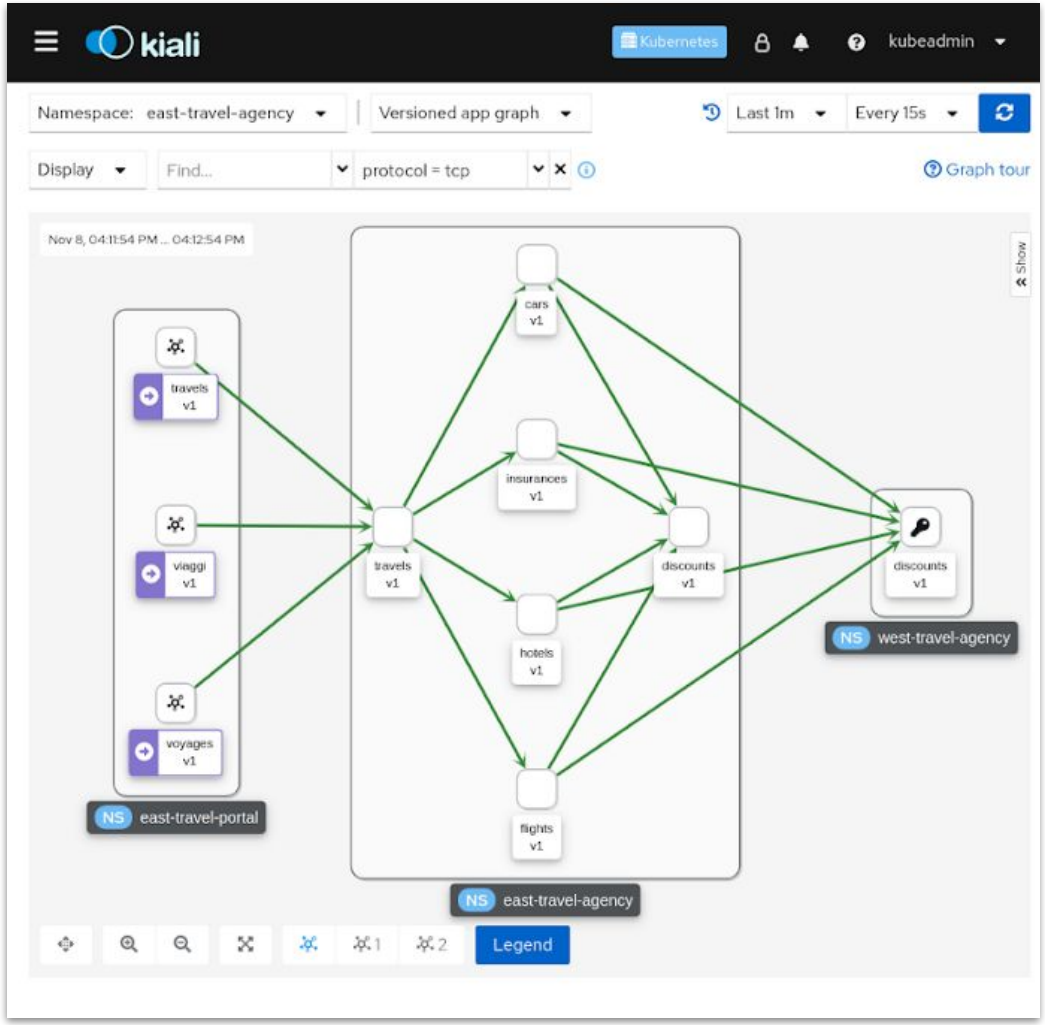


- OpenShift Serverless security and visualization enhancers
- OpenShift Service Mesh 2.1 Federation
- Openshift Virtualization
- Migration Toolkit for Virtualization 2.1
- OpenShift Mirror Registry (Quay)
- CSI Operators - plugable, built-in upgrade, could include new functionality (ODF)

- Custom Metric Autoscaler TP with KEDA
- Openshift Serverless Support for Init Containers and PVC
- Serverless integration with Cost Management Service and Distributed Tracing
- Metro Disaster Recovery TP (ODF)
- Online expansion including FileSystem (ODF)

OpenShift Service Mesh

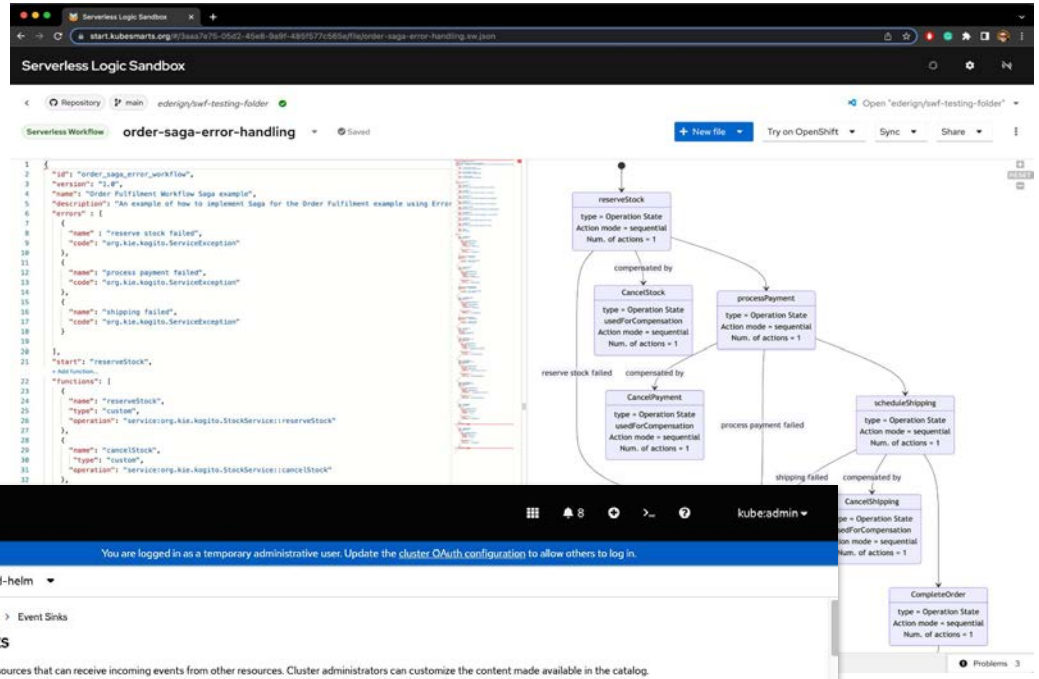
- OpenShift Service Mesh 2.2 is now available.
- Based on **Istio 1.12** and **Kiali 1.48**.
- Service Mesh, including **federation**, is now supported on Red Hat OpenShift on AWS (ROSA)
- Istio 1.12 introduces **WasmPlugin** API which deprecates the ServiceMeshExtensions API.
- **Kiali** updates in Service Mesh 2.2:
  - Improved views for larger service meshes
  - View internal certificate information
  - Set Envoy proxy log levels
- New **Istio** *Tech preview* features to try:
  - Kubernetes **Gateway API**
  - **AuthPolicy** "dry run"
  - gRPC "Proxyless" service mesh

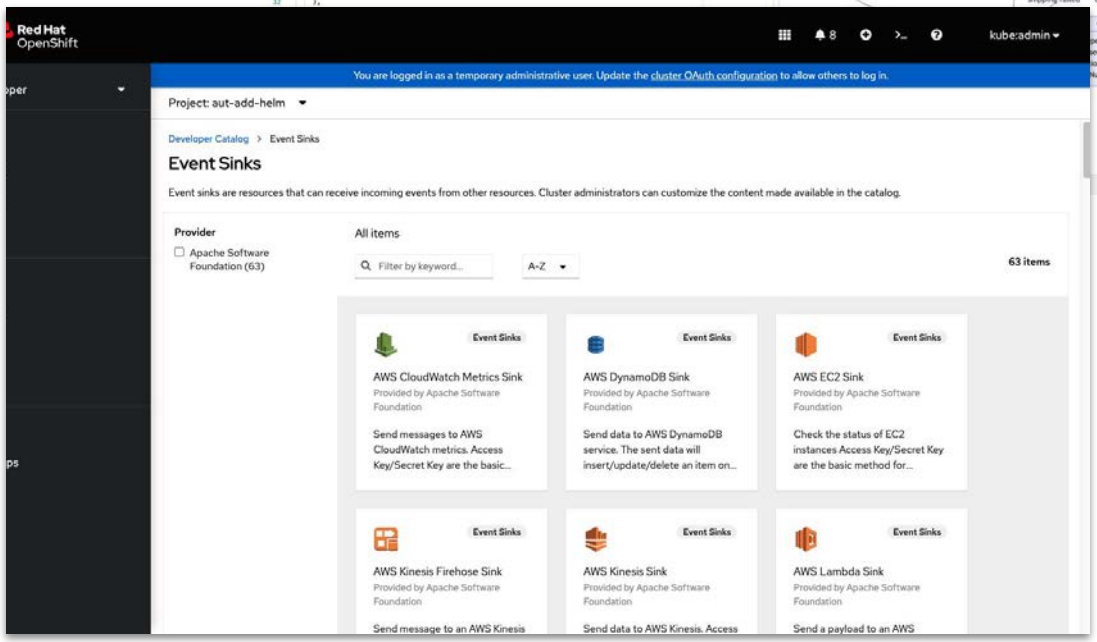


Red Hat | intel.

OpenShift Serverless

- Update to Knative 1.3
- Support for **Init Containers** and PVC (Tech Preview)
- Serverless integration with Cost Management Service and Distributed Tracing
- Connection to externally managed **Kafka** Topic (Tech Preview)
- Developer Experience:
  - Addition of Event Sink on Dev Console
  - **Serverless Dashboard** for Developers perspective
- **Functions** (Tech Preview)
  - On cluster build using OpenShift Pipelines
  - Multiple build strategy support
  - IDE plugin for creating Functions (VScode & IntelliJ)
- Serverless Logic (Dev Preview)
  - Orchestration for **Functions and Services**
  - CLI and Workflow Editor(UX)





Red Hat | intel

OpenShift Virtualization

Modernize workloads, bring VMs to Kubernetes

Enterprise Virtualization Enhancements

- Windows 11 and RHEL 9 Guest Support
- Improved new VM wizard & VM catalog
- VM overview page to manage individual VMs

VMs and Containers in Private/Hybrid Cloud

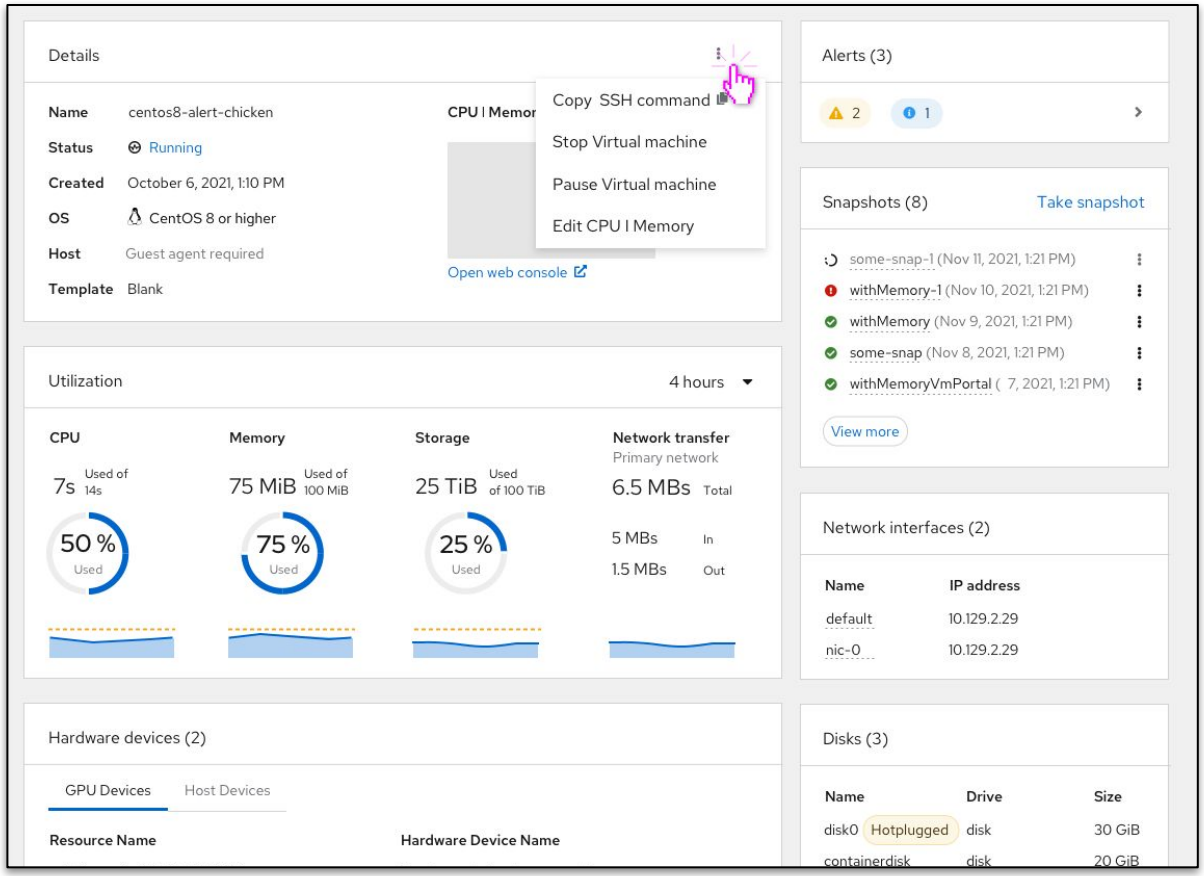
- RBAC control on VM templates
- Container & VM applications in same Service Mesh
- Easily share vGPU w/ NVIDIA operator

Enhanced Data Protection

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

Proven Performance

- Workload Acceleration
- Accelerate compute and 3D apps with vGPU resources

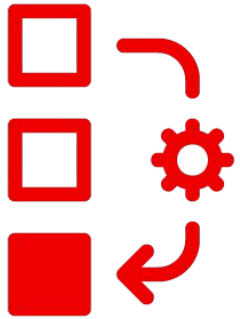


Red Hat | intel

Custom Metric Autoscaler (Technology Preview)

Scale workloads horizontally based on custom metrics

- Custom Metric Autoscaler is built on CNCF project **KEDA**
- Use Scalers example **Prometheus** , Apache **Kafka** and many more on which **custom metric autoscaler** can scale based on
- Manages workloads to scale to 0
- Registers itself as k8s Metric Adapter
- Provides metrics for Horizontal Pod Autoscaler (HPA) to scale on



Red Hat Modernization and Migration Solutions

Tools and Web Services Overview

Migration Toolkit for Applications

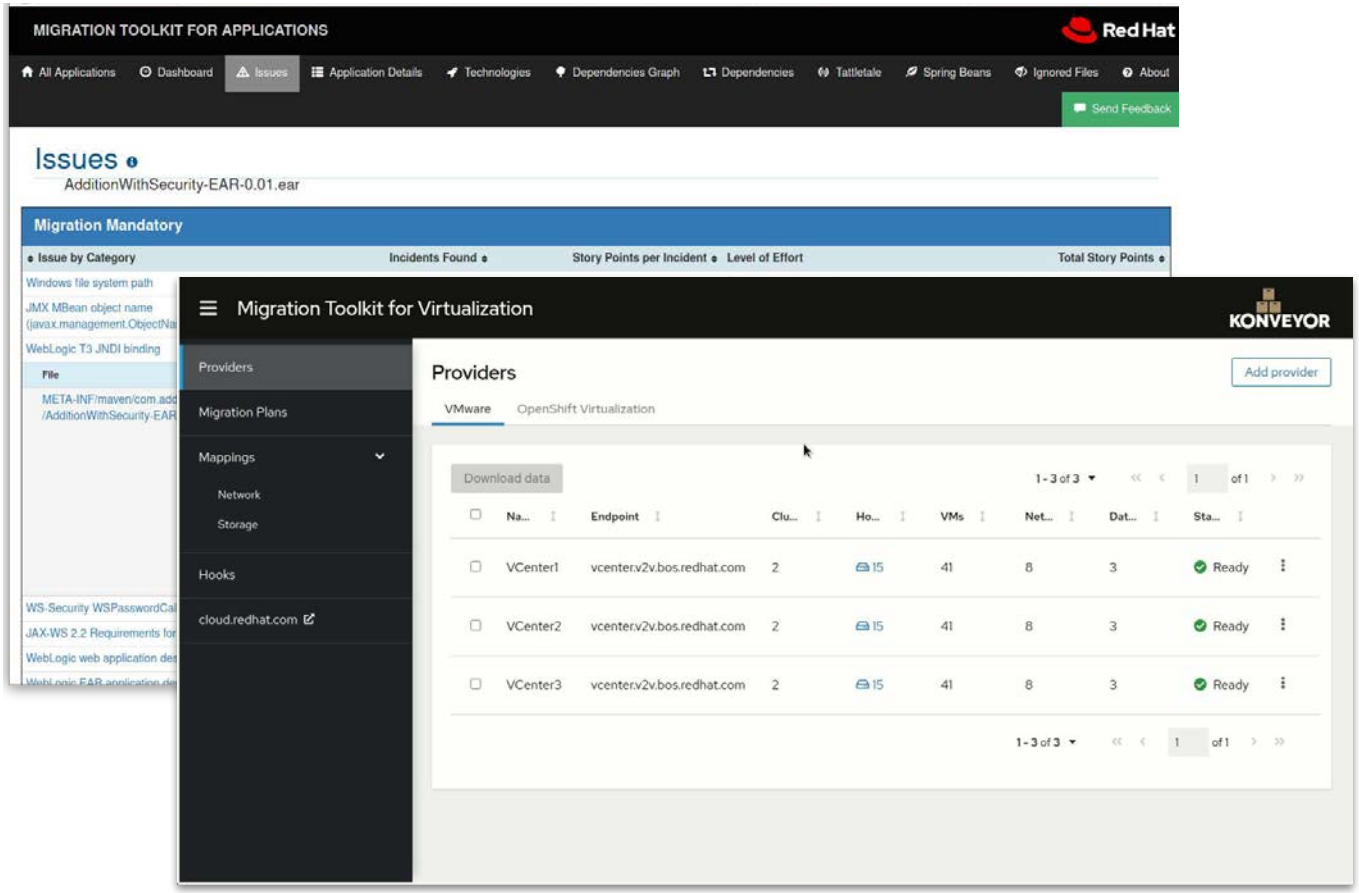
Tools and services that help customers migrate and modernize applications with a focus on adopting OpenShift

Migration Toolkit for Containers

Tools and services that help users migrate containers between OpenShift clusters

Migration Toolkit for Virtualization

Tools and services that help customers migrate to OpenShift Virtualization

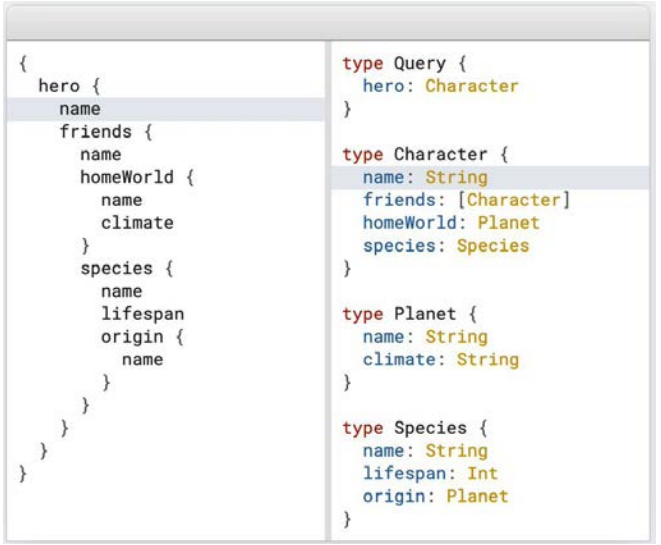


Red Hat | intel.

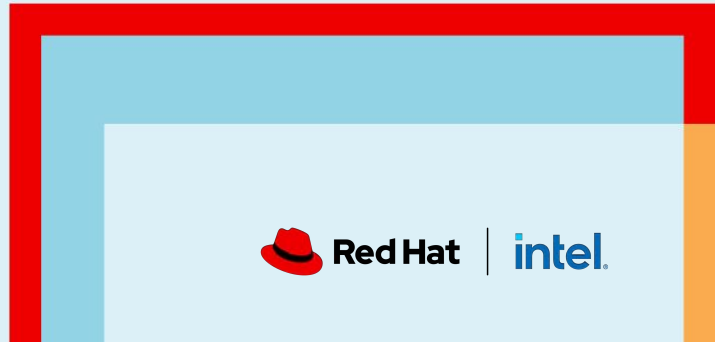
Kube Native Java with Quarkus

- **Java 17** support for *native* executables (Tech Preview)
- **GraphQL** Support
  - Only return data that was requested -> Prevents Over-fetching
  - Combines many resources in the same request -> Prevents Under-fetching
  - Includes Quarkus Dev UI integration
  - Reactive GraphQL Support (Tech Preview)
- Enhanced Search with **Hibernate Search**
  - Automatically extracts data from Hibernate ORM entities to push it to Elasticsearch/OpenSearch indexes.
  - Full text search for entities, including “sounds like”
- Intelligent service discovery and selection with **Stork**
  - Write applications with a pluggable service discovery implementation (out of the box: static, K8s, Consul)
  - App-side load balancing (round robin, random, least used, least response time, etc)

GraphQL in the Dev UI



Application Lifecycle

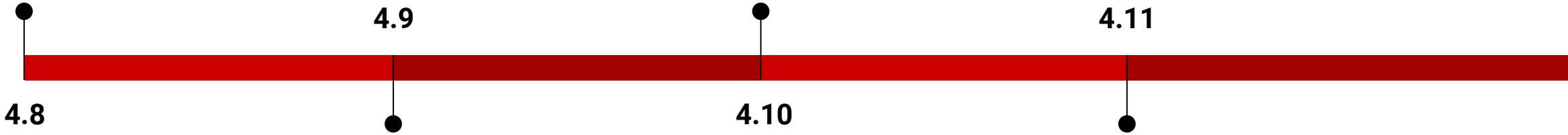


Build & Deploy Cloud NativeApps

Roadmap

- Pipeline as code with GitHub DP
- Auto-pruning PipelineRuns and TaskRuns
- Ability to customize default ClusterTasks and Pipeline templates
- ArgoCD auth integrated with OpenShift via RH SSO
- RHACM and ArgoCD integrations

- TaskRun and image signing with Tekton Chains
- Triggers emit events in the user namespace to simplify debugging
- New generators in ApplicationSets
- Respects “ignore differences” setup during sync for objects and fields owned or mutated by operators
- Shared Resource CSI Driver TP
- Mount CSI volumes in BuildConfigs



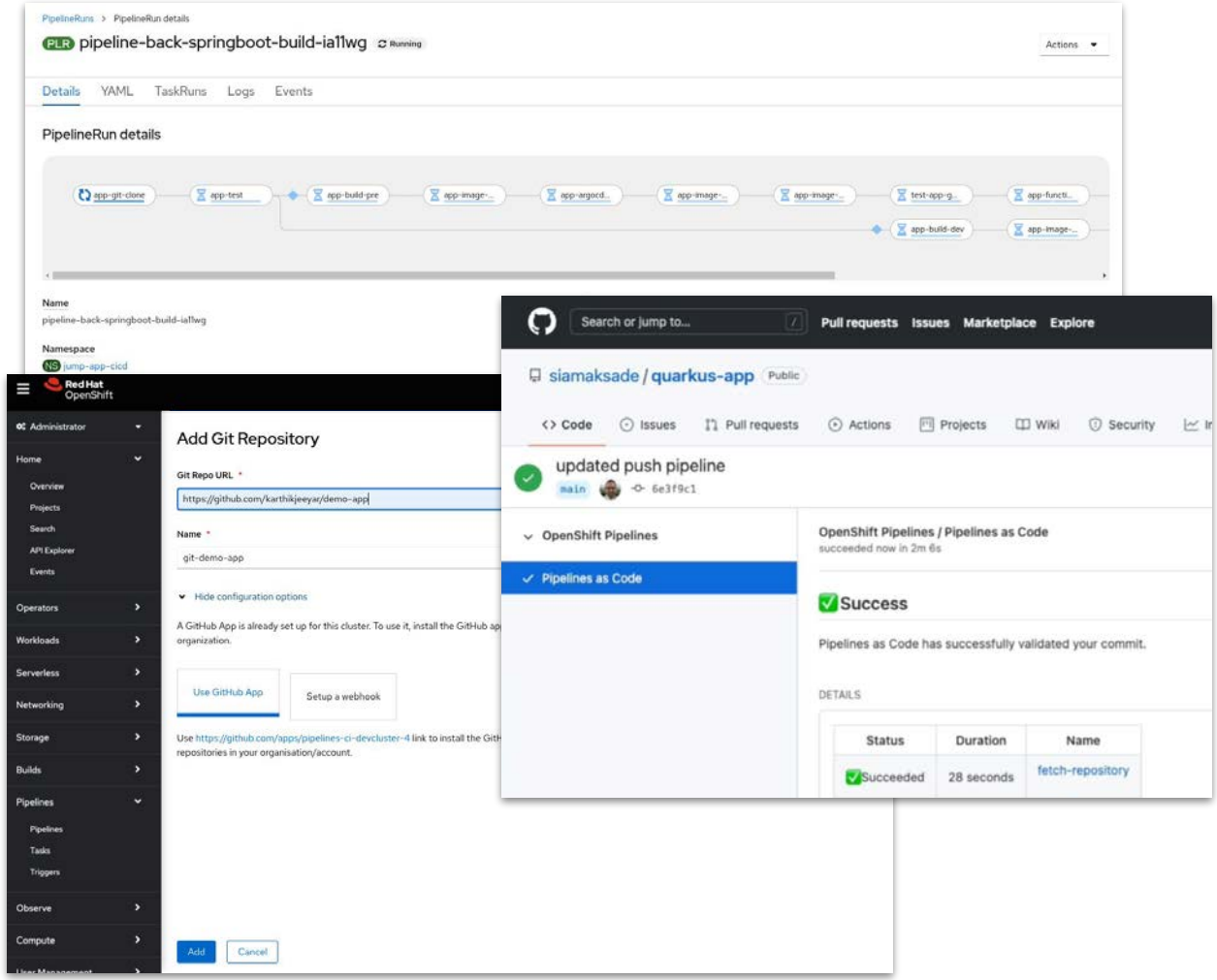
- Tetkon Triggers GA
- Pipeline as code TP (Private repositories and BitBucket)
- Search and install Tasks from TektonHub in the Pipeline builder
- Repository list views for pipeline as code
- kustomize 4 support
- External cert manager support for TLS configs in ArgoCD

- External database support in Tekton Hub
- Pipelines on Arm architecture TP
- Trigger multiple pipelines for Git event
- ApplicationSets GA
- Notifications TP
- Custom plugins in Argo CD

Red Hat | intel

OpenShift Pipelines

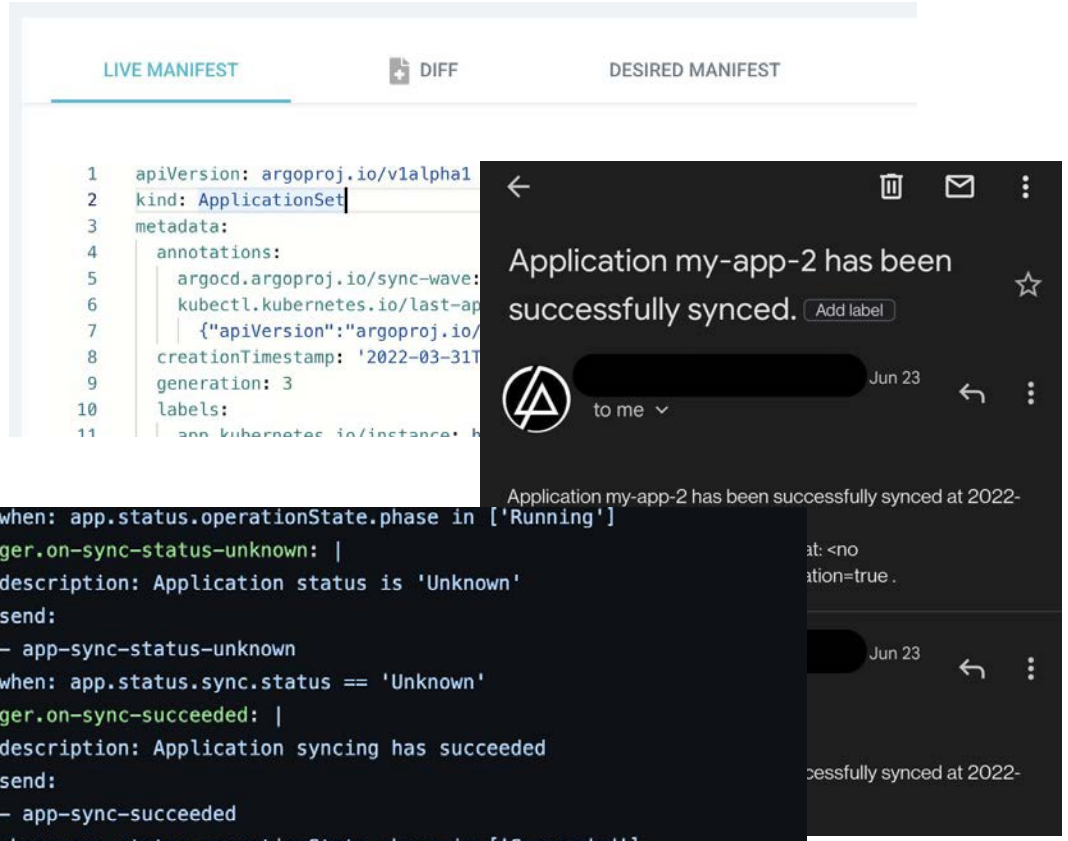
- OpenShift Pipelines 1.8
- External database support in **Tekton Hub**
- Pipelines on **Arm** architecture TP
- **Pipelines as code** enhancements
  - Trigger multiple pipelines for Git event
  - GitLab and BitBucket support
  - CLI commands for configuring webhooks
  - Manual and third-party triggers
- **Dev Console** enhancements
  - Configure Git repositories with pipelines as code
  - Create GitHub App for pipelines as code



PM: Koustav Saha

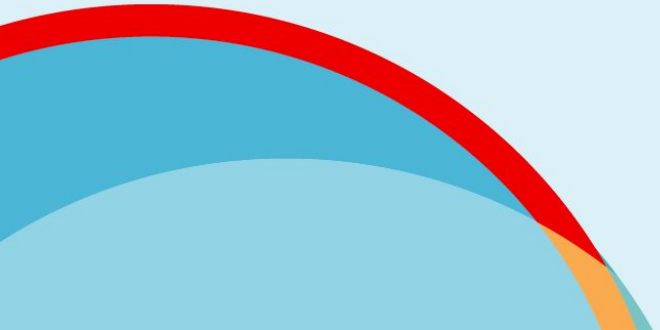
OpenShift GitOps

- OpenShift GitOps 1.6 (Argo CD 2.4)
- ApplicationSets GA
- **Notifications** TP
- Secret management guide
- **Custom plugins** in Argo CD
- **Encrypted** comms with Redis
- Deployment history in **Dev console**
- Support for running on IBM Power and IBM Z



Red Hat | intel.

Developer Experience



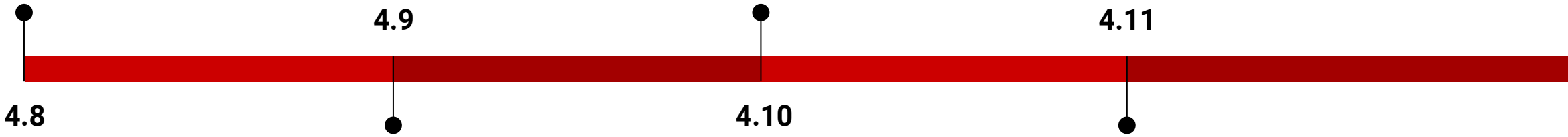
Red Hat | intel

Unified Developer Experience

Roadmap

- Expanded UI for Serverless (Cloud functions, autoscale, etc)
- Improved onboarding & Quick Start features
- Customize the Developer Experience
- Certified Helm Charts
- Console routes supports custom & wildcard certificates

- Multi-Cluster Focused with ACM
- Console Extensibility (Add new flows, pages, actions, …. to either the Admin or Dev perspectives based on webpack 5)
- Pod Debug Mode
- Improved Quota Visibility
- Hybrid Helm Operator SDK plugin TP



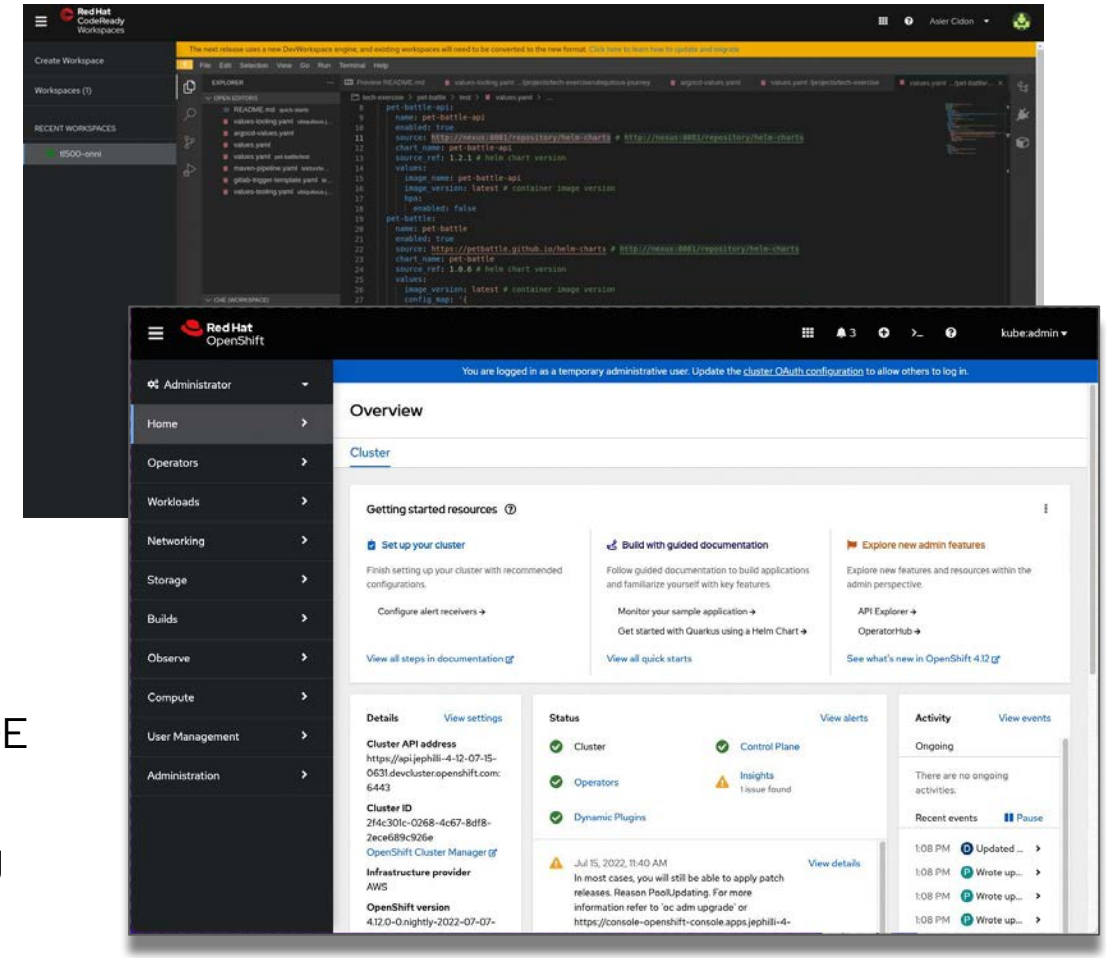
- Focus on the projects you care about
- Set your individual preferences for the console experience
- Troubleshoot Node-level problems directly from the Console
- New features & UX enhancements (Apps Observability, Export Applications, Builds, etc)
- New Serverless UIs (Domain Mapping Support, Community Kamelets Availables, etc)

- Cluster Upgrade Improvements
- Pod Disruption Budget integration
- Dark mode
- Form Based Experiences (Configmaps, routes, etc)
- Web Terminal improvements
- Java Operator SDK plugin TP

Developer Experience

Watch the ***What's New - Developer Edition***

- **Developer Perspective** in OpenShift Console
- **odo v3 beta 1** with improved dev flows
- New container tooling initiatives to expand our footprint
  - **Podman Desktop** early development
  - **Docker Desktop extension** for OpenShift
- **OpenShift Dev Spaces 3.0** *(formerly known as CodeReady Workspaces)*
- **OpenShift Local** (formerly known as CodeReady Containers)
- **Certified Helm Charts** available from our Partners
- Enhanced application development and deployment around IDE experience in Visual Studio Code, IntelliJ and Eclipse Tooling
- Richer experience in VSCode Java, Quarkus and YAML tooling



Red Hat | intel.

Console Extensibility

Dynamic Plugins

Tech Preview

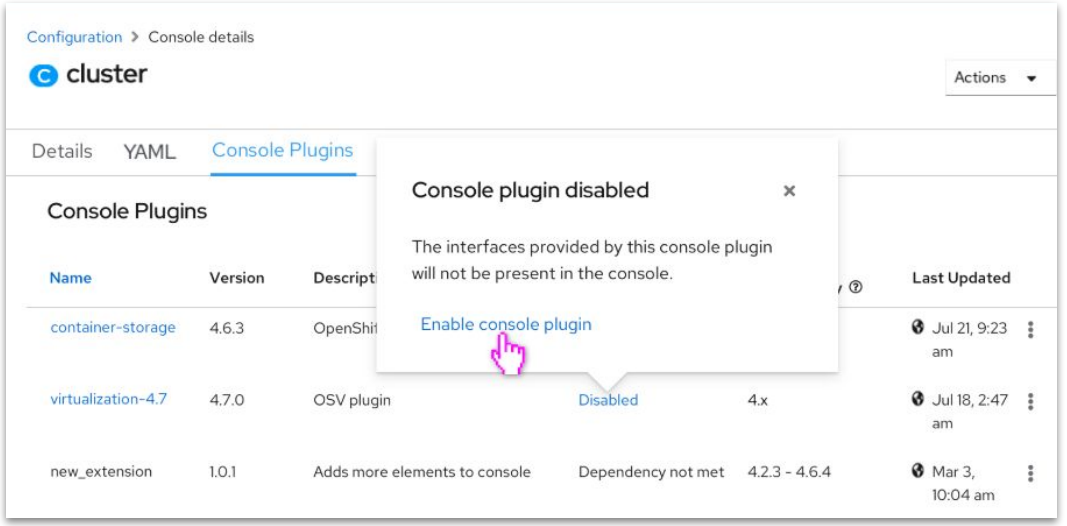
What is a dynamic plugin?

- 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.

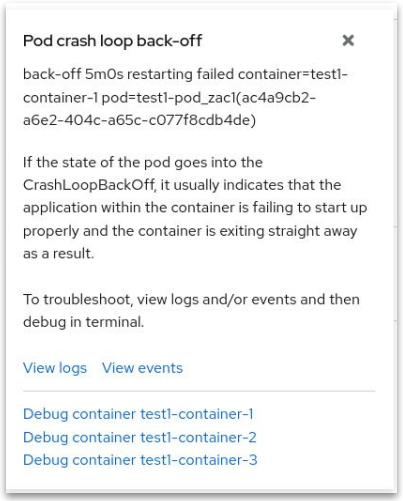


Common Console Updates

Pod Debug Mode

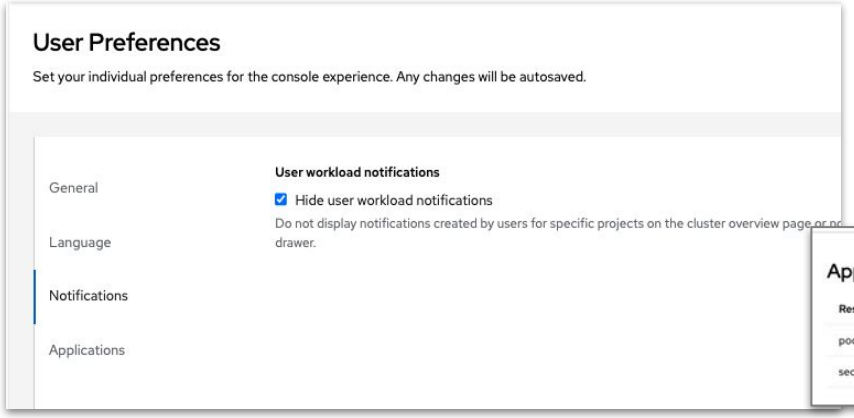
How do I debug a application that fails on startup?

- Quickly troubleshoot miss behaving pods from the UI CrashLoopBackOff
  - Same as running oc debug pod
  - Starts each container in a interactive shell
    - Stops the pod from CrashLooping
    - Check environment variables, config files, …
    - Access to logs & events

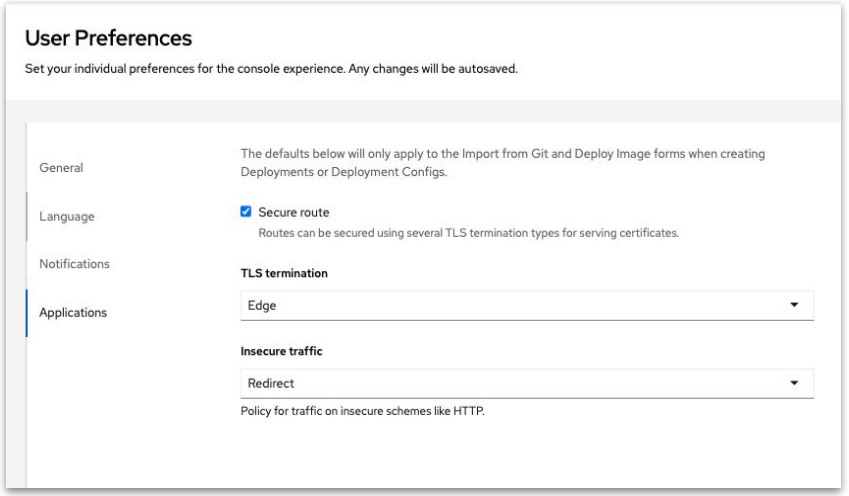


User Preferences updates

How do I hide user workload notifications?



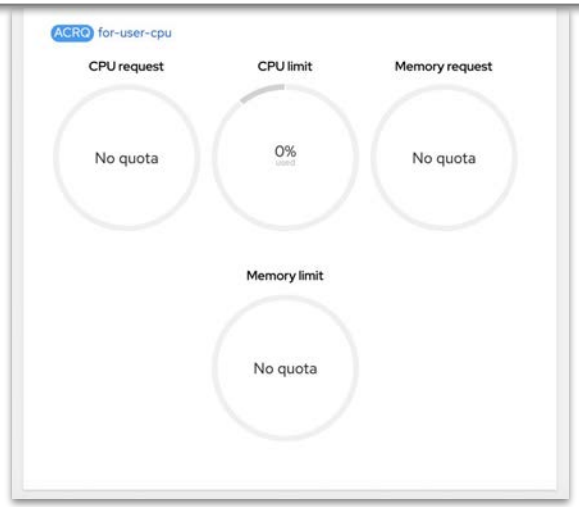
Change your defaults for route creation in creation flows!



Improved Quota Visibility

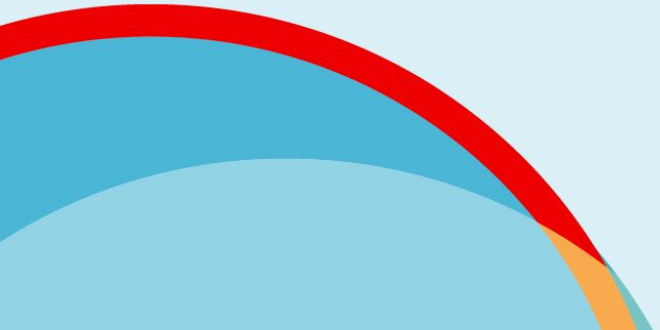
How do I see how much quota is left?

- Non admin users can now see their usage of the AppliedClusterResourceQuota



Red Hat | intel

Observability



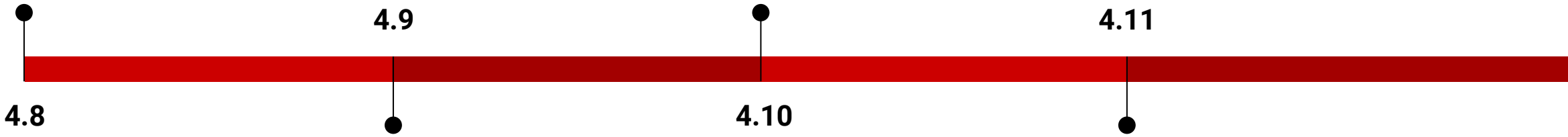
Red Hat | intel.

Metrics, logs, and traces integrated

Roadmap

- New enhancement inside the OpenShift Console (Group dependent charts, show multiple data points in one view or allow filtering for absolute time ranges instead of using relative ranges)
- More flexibility to select and filter certain logs to forward

- New Support for enabling Audit Logging in Prometheus Adapter
- Prometheus Client Certificate Authentication for Scraping Metrics
- Integrated Alerting with Alertmanager in the Openshift Console
- New Prometheus Targets Endpoints Provided within the OpenShift Console
- Distributed tracing based on Jaeger and OpenTelemetry



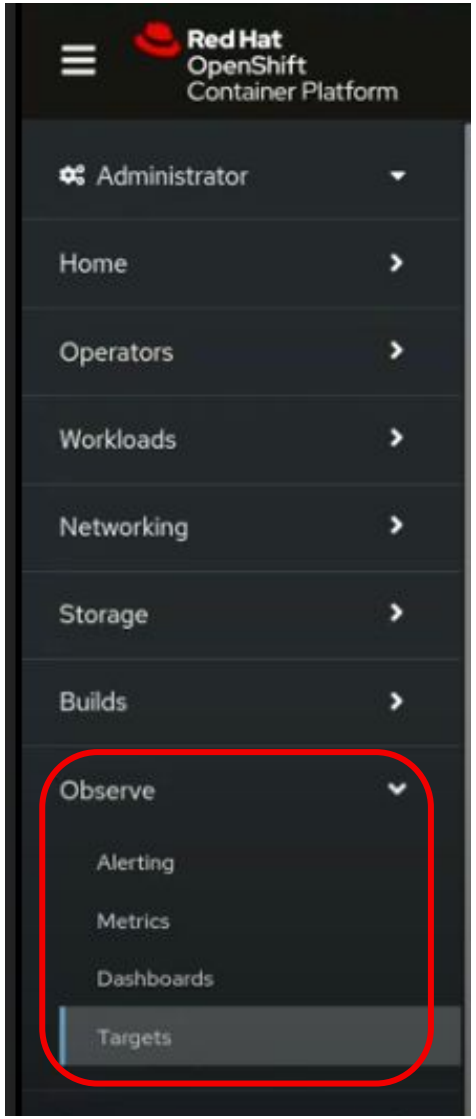
- Enhancements to Alert Manager Rules, Cluster Monitoring Operator and refined triggering conditions
- Remote write storage for Prometheus Metrics
- Monitoring for User-Defined Projects
- New Support and Capabilities for Loki
- New Added Logging Support and Flexibility (Fluentd to Vector) TP

- Improving the overall Monitoring experience inside the OpenShift Console
- Expand upon Vector as an alternate Collector and Loki as an alternate log store
- Logging view in the Observe Section of the OpenShift Console

Improved OpenShift Monitoring UI Experience

OpenShift Console Monitoring Experience

- Console Monitoring User Experience Enhancements to Observe OpenShift:
  - **Observe > Metrics**: Query Browser UX (e.g., autocomplete feature > now showing functions and metrics suggestions to users)
  - **Observe > Dashboards**: Higher data sampling rate > now showing more details to users
  - **Observe > Alerting:** Users can manage Alertmanager for user-defined alerts
  - **Observe > Targets:** Users can have a single view of all OpenShift Console Integrated Monitored Scrape Endpoints



Notes:

Prometheus user interfaces have been deprecated > console redirect for Prometheus alert backlinks added

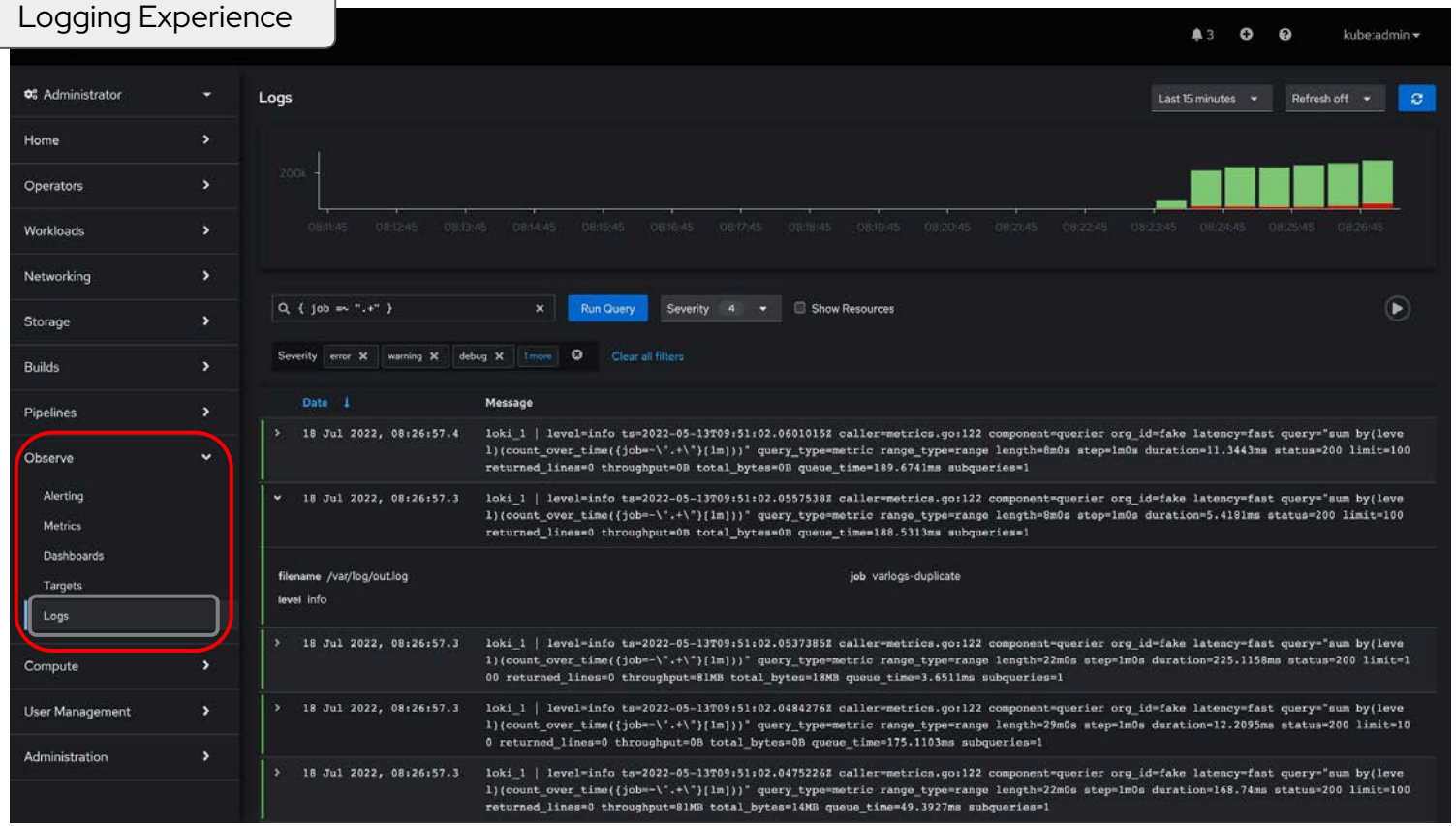
Grafana dashboards for visualization/customization out of the box are no longer provided

Logging 5.5: OpenShift Logging UI Experience

OpenShift Console Logging Experience

- Continue to work towards a consistent and simplified Observability User Experience by introducing a logging view in the console:
  - **Observe > Logs**: exposes log information from the underlying storage via an API, queried by the console to retrieve contextualized logs

Logging Experience



Logging 5.5 for OpenShift 4.11

<< NEW >>

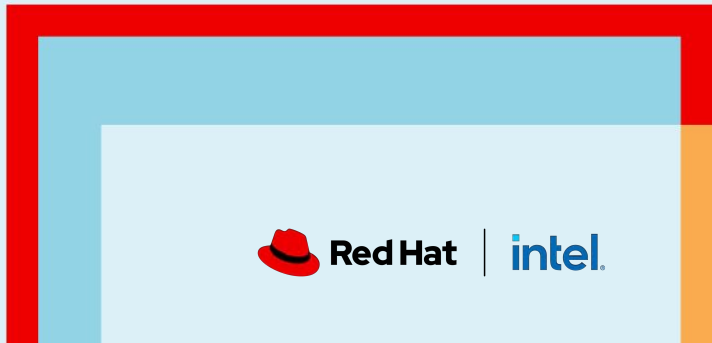
Vector as alternate collector

Loki as alternate log store

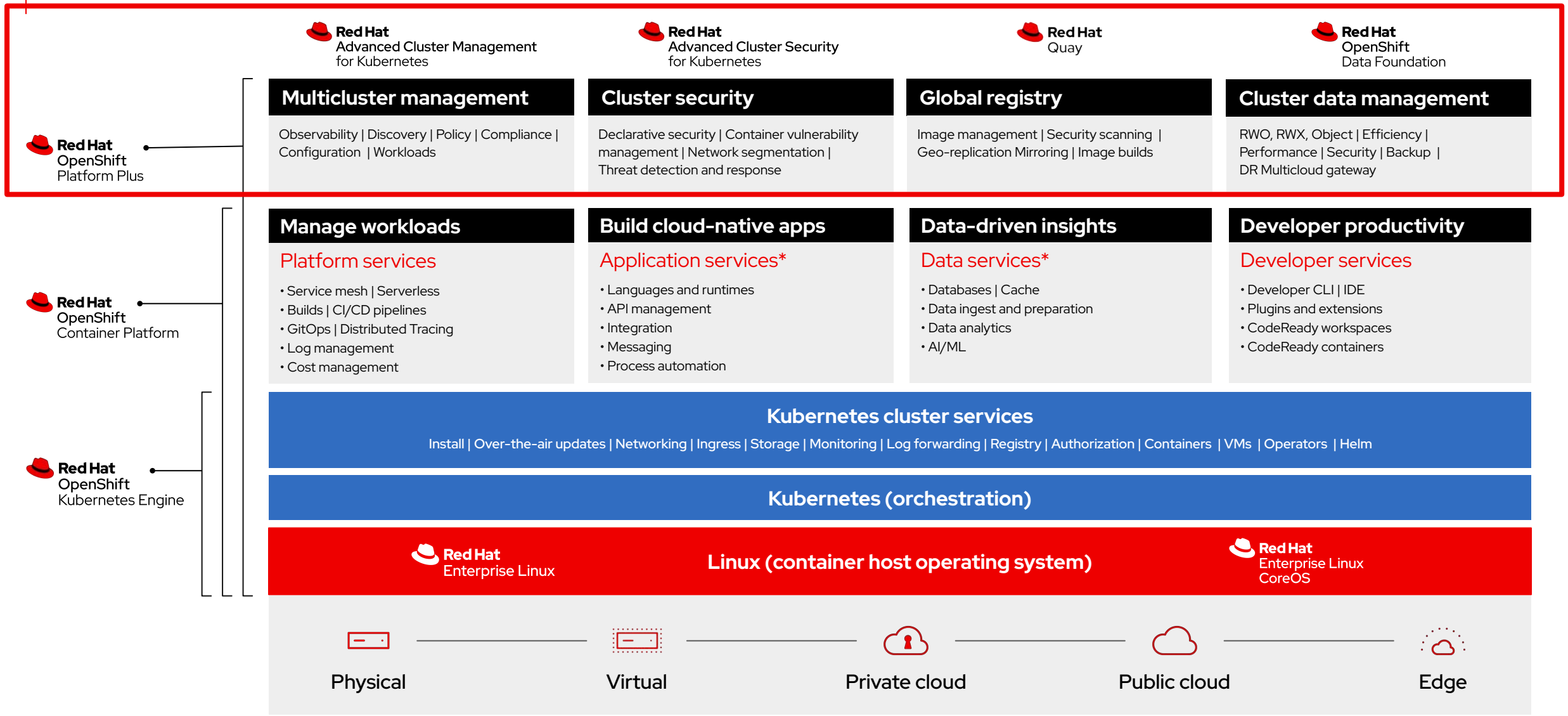
Major updates and features

- maxUnavailable of 'collector' daemonset reducing upgrade time
- Log exploration natively inside the OpenShift Console
- Upgrade fluent to ruby 2.7 and latest dependencies
- Pod labels for k8s are preserved
- Support Cloudwatch output for Vector
- CloudWatch log forwarding add-on supports STS installations

Governance



Red Hat open hybrid cloud platform



Red Hat | intel

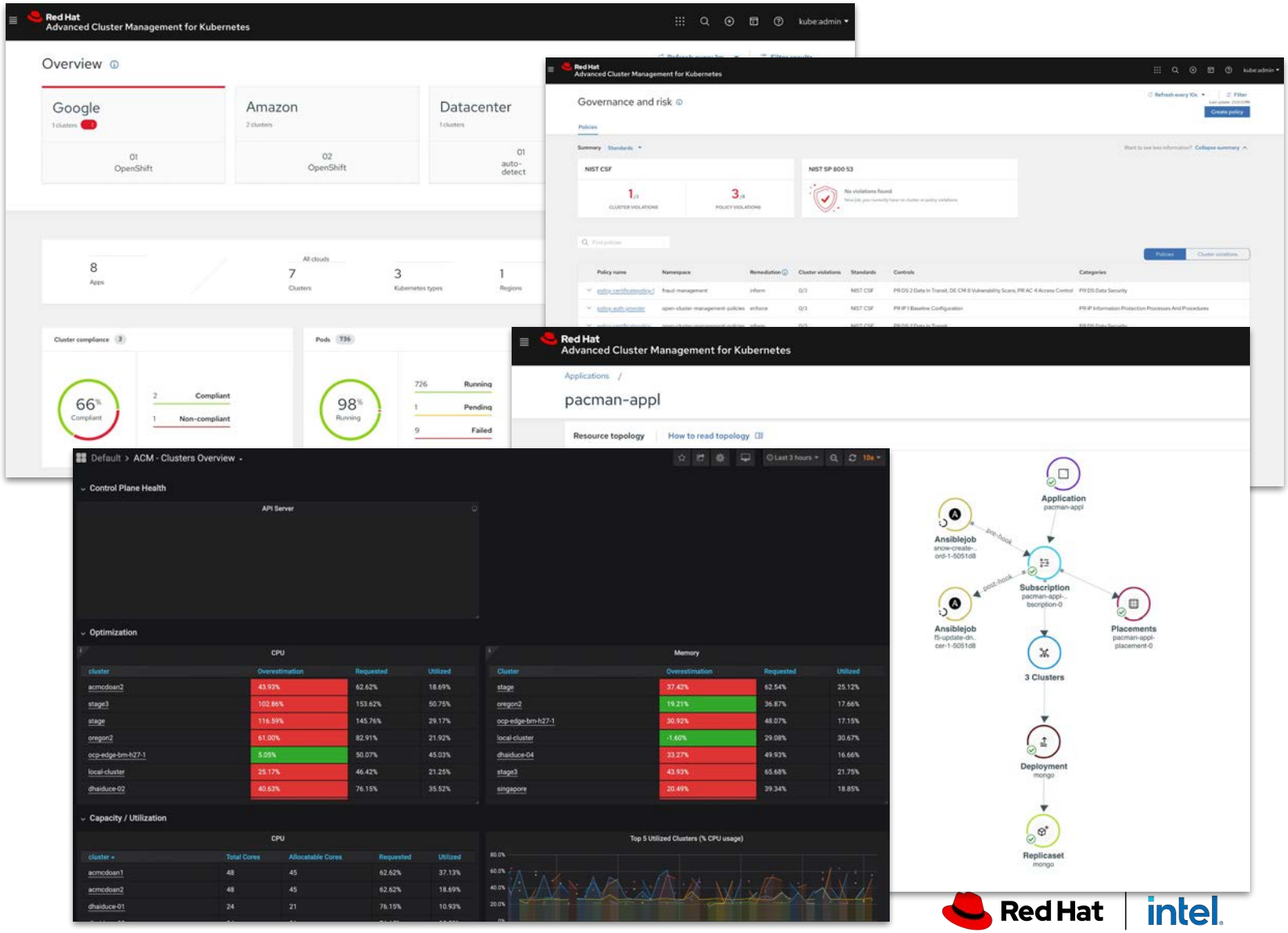
Red Hat
Advanced Cluster Management
for Kubernetes

Multicluster lifecycle management

Policy driven governance, risk, and compliance

Application lifecycle management + GitOps

Multicluster observability for health and optimization

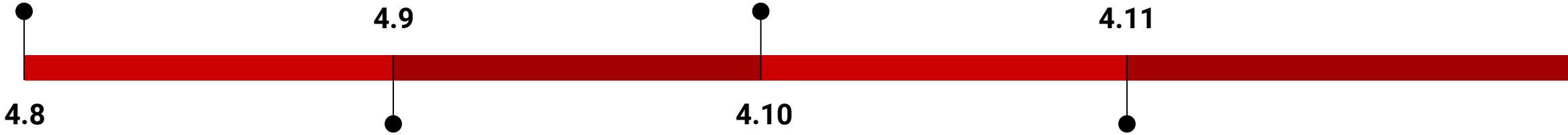


Red Hat | intel

Red Hat Advanced Cluster Management

Roadmap

- **Enhanced Multi-Cluster Deployments**
  - Provision OCP on Red Hat OpenStack
  - Import and manage Red Hat OpenShift on Amazon (ROSA) & OpenShift IBM Power
  - Improve managed OCP clusters upgrades
- Improve **Multi-Cluster Observability** (Alert Forwarding from Managed Clusters to the ACM Hub Cluster…)
- RHACM is now **Fully Open Source**



- Centralized **Infrastructure Management** (CIM) for Bare Metal Deployments TP
- **Single Node** OpenShift management (SNO)
- Meeting the needs of customers in Public Sector (NAPS), whether on premise with **FIPS** compliance or in the cloud with Microsoft Azure Gov
- **Advanced image registry configurations** for managed clusters in public clouds

- Support for OpenShift **GitOps ApplicationSets**
- **Gatekeeper Mutating Webhooks** can change resources upon admission
- Central **Infrastructure Management** (GA)
- Application **Disaster Recovery** capabilities using Red Hat OpenShift Data Foundation (ODF) across two distinct OCP clusters separated by distance

- **Kyverno and Gatekeeper** community PolicySets
- Manage RHACM clusters from **Ansible** (AAP) TP
- Deploy & manage 2500 SNO
- Configurable dynamic metrics collection
- Metro-DR with **Failover Automation** TP

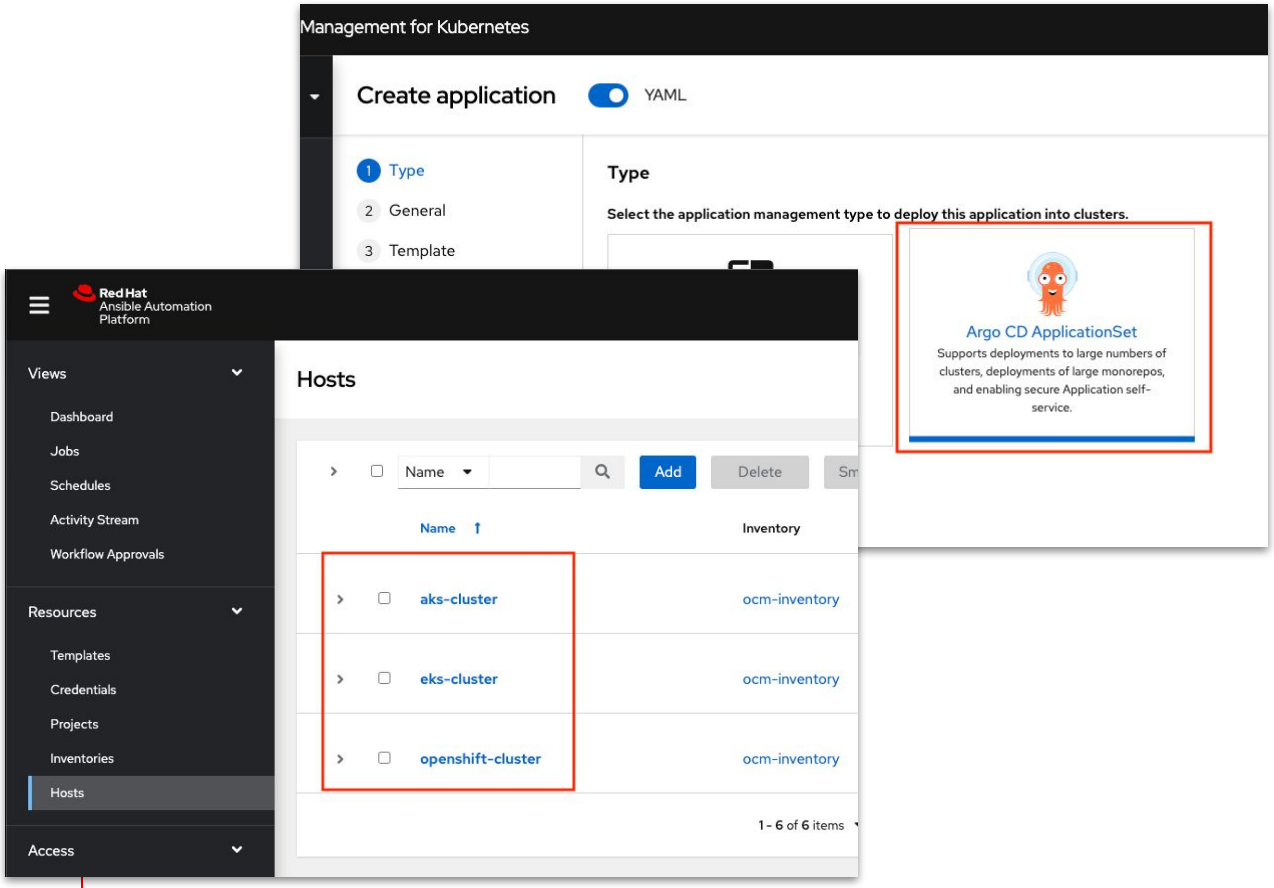
Red Hat | intel

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM

Better Together

Red Hat Advanced Cluster Management brings together Ansible and OpenShift Platform Plus, including OpenShift GitOps, Red Hat Advanced Cluster Security, Red Hat OpenShift Data Foundation across cloud vendors all from a single-pane of glass.



- **OpenShift GitOps Integration:** Improves visibility, control and resiliency of ArgoCD when deployed on RHACM managed clusters.
- **RHAAP Integration:** RHACM cluster inventory and API available from Ansible Automation Platform: AAP has access to ACM functionality using the Ansible collections.
- **RHACS Integration:** Provide PolicySets for ACS and OpenShift+ Integration
- **RHODF Integration:** Provides Backup/Restore functionality and Automates Disaster Recovery for Metro and Multi-Regional Openshift Clusters and Applications

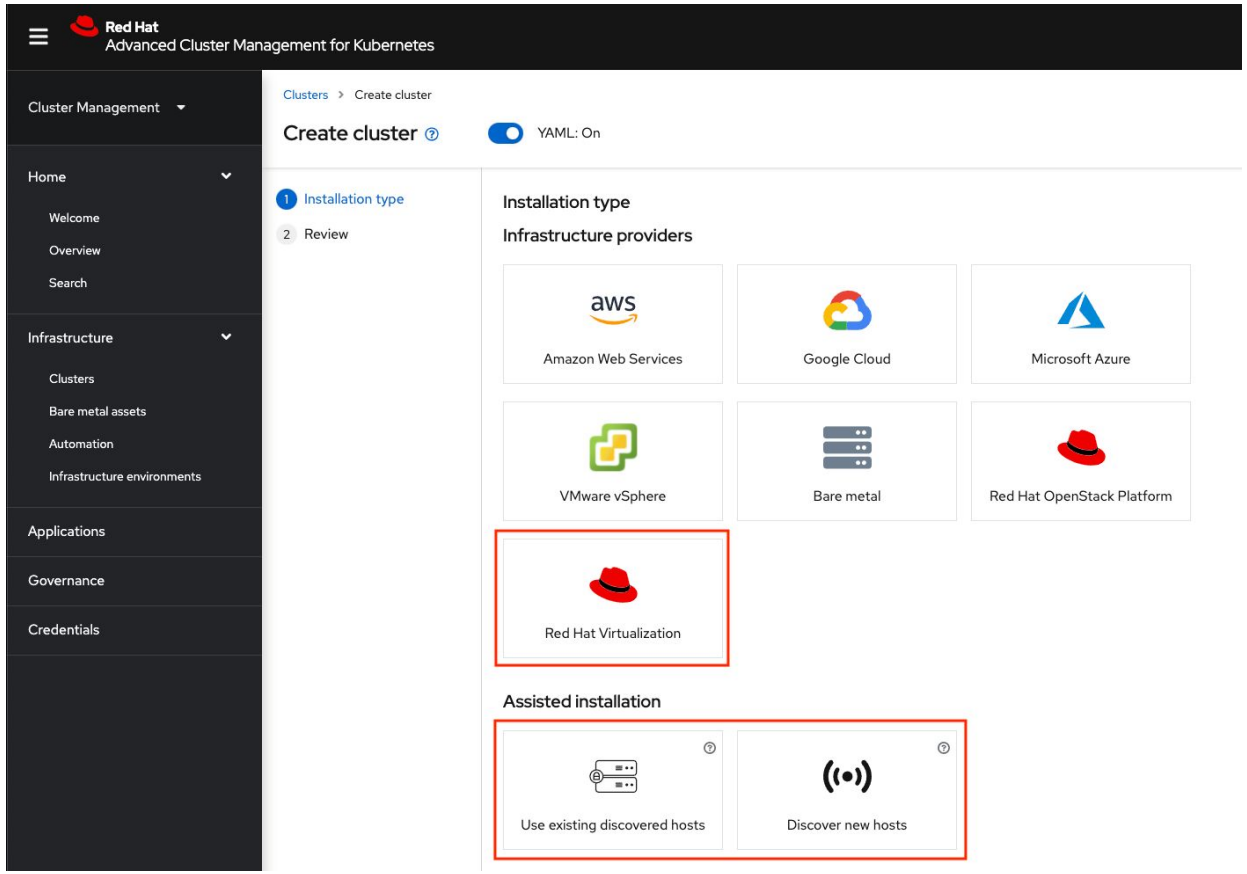
Red Hat | intel

Red Hat Advanced Cluster Management for Kubernetes

What's new in RHACM

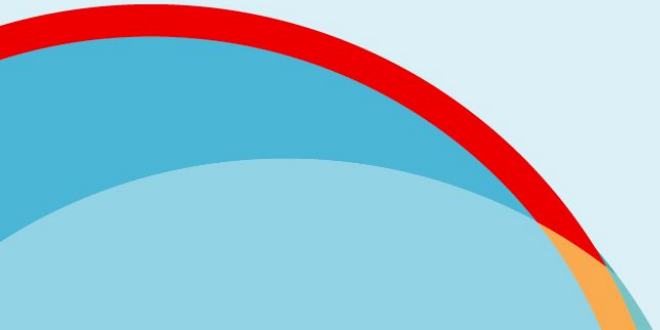
Manage OpenShift Everywhere

Meeting the needs of customers across all sectors, whether on premise with Red Hat Virtualization, bare metal, or in the cloud with AWS GovCloud (US).



- **Arm architecture:** Deploy an ACM hub on Arm, as well as import and manage OpenShift clusters leveraging Arm for low power consumption.
- **Cluster health metrics** for non-OCP: EKS, GKE, AKS.
- **HyperShift:** Host and provision containerized OpenShift control planes at scale, reducing cost, hardware footprint, and time to provision.
- **Central Infrastructure Management:** Enables access to bare metal hosts for OCP cluster provisioning.
- **Submariner** enhancements on Azure and OVN SDN
- **FIPS-Compliance**

Storage



Red Hat | intel.

OpenShift Data Foundation roadmap

4.9

- Extended control plane with IBM Flashsystem
- **MCG namespace mirroring (Object)**
- MCG auto scale
- LSO Health and maintainability
- Overprovision Level Policy Control
- RBD PV encryption service account
- Hashicorp **KMS** for PVs at rest encryption keys

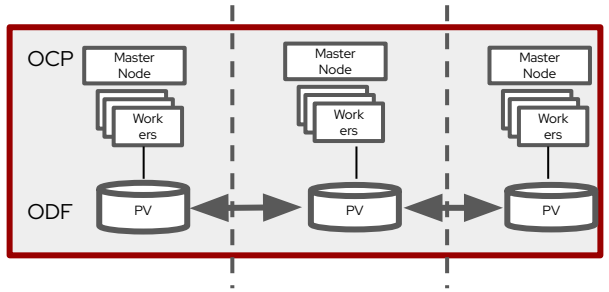
4.10

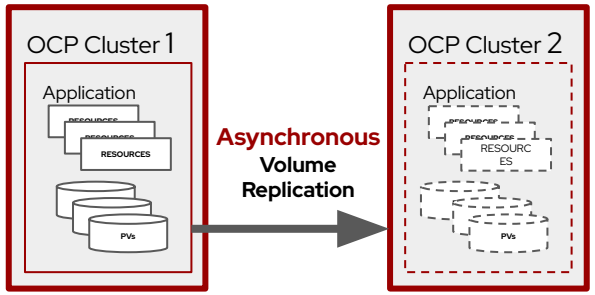
- Regional DR with ACM based management
- AWS gp3/gp2 csi support as backing storage
- **MCG support for namespace on top of filesystem**
- Cluster wide encryption - Service Account
- Support for IBM HPCS **KMS**

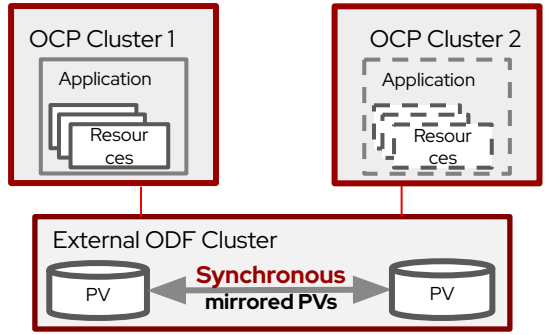
4.11

- Data Resiliency
  - **Metro DR with ACM**
  - **Regional DR with ACM UI**
- Single Node OpenShift Cluster
  - Snapshots/Clone
  - Thin provisioning
- Multi-Cluster ODF monitoring with ACM UI

Summary OCP+ODF DR options

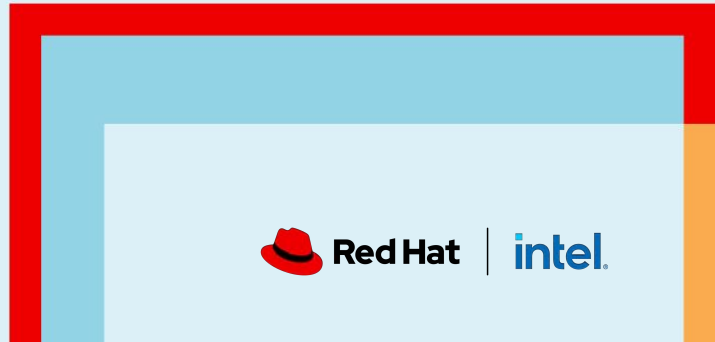






	Cluster HA	Regional-DR	Metro-DR
Topology	Single OCP+ODF clusters deployed over multiple AZs in a single region	Multi OCP + ODF clusters spread over multiple regions	Multi OCP clusters + single external ODF stretched cluster deployed over low latency networks
RTO (Downtime)	RTO=0 (Continuous)	RTO = minutes DR Automation from ACM+ODF reduces RTO	RTO = minutes DR Automation from ACM+ODF reduces RTO
RPO (Data loss exposure)	RPO=0 No Data loss due due to Synchronous mirroring of ODF data	RPO > 0; Usually 5 min or higher Depends upon network bandwidth & change rate	RPO=0 No data loss due to synchronous mirroring of ODF data
Infra Requirements	Multi-AZ deployment recommended No network latency limits	All ODF supported platforms No network latency limits	On-prem only (vSphere or bare-metal) <10ms network latency between sites (<5 recomm.)

Security



Security & Compliance

Roadmap

4.8

- Enabling managed Secure Boot with installer-provisioned clusters
- TLS security profile for the Kubernetes control plane
- RHACS - Improved Vulnerability Scanner
- oc-compliance plug-in is now available and makes the interaction with the Compliance Operator API and other components easier

4.9

- Configuring the audit log policy with custom rules
- RHACS - Enhanced protections for the Kubernetes API server
- RHACS - Accelerates security use case adoption in the cloud with certified testing and support for **ROSA** and **ARO**
- RHACS - Improve cybersecurity gap analysis and incident response prioritization by aligning security policies & alerts with the **MITRE ATT&CK** Framework

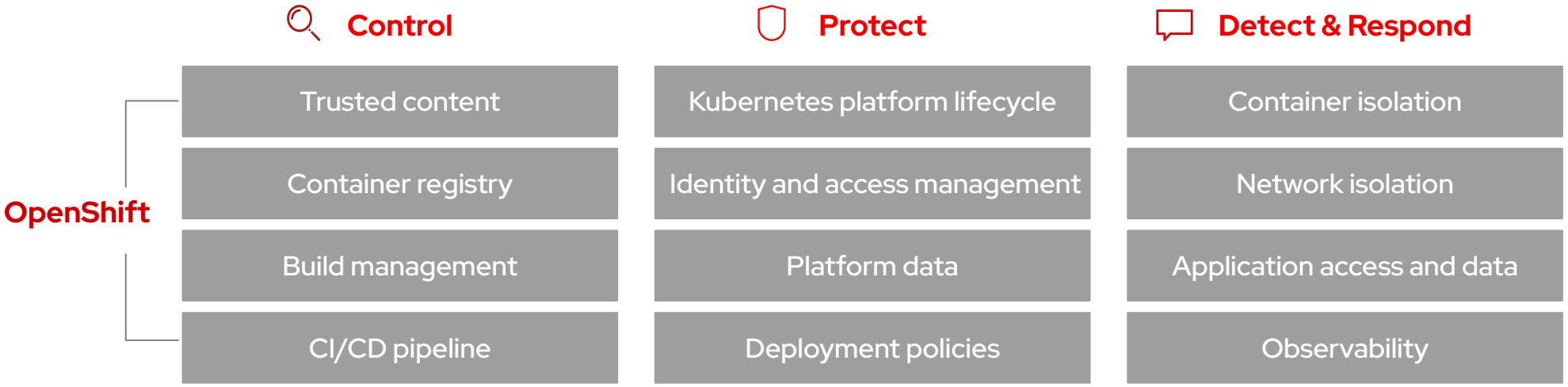
4.10

- Automate certificate management in cloud native environments with **cert-manager**
- RHACS - Enable developers to streamline risk management by marking vulnerabilities as false positives or accept risk
- RHACS - Send additional details to system notifiers and SIEMs about the timelines of runtime policy violations and risks.

4.11

- Audit logs now include OAuth server audit events
- RHACS - Verify image signatures against **Cosign** public keys (DevSecOps improvements)
- RHACS - Identify Missing Kubernetes Network Policies
- RHACS - **Identify Spring critical vulnerabilities**

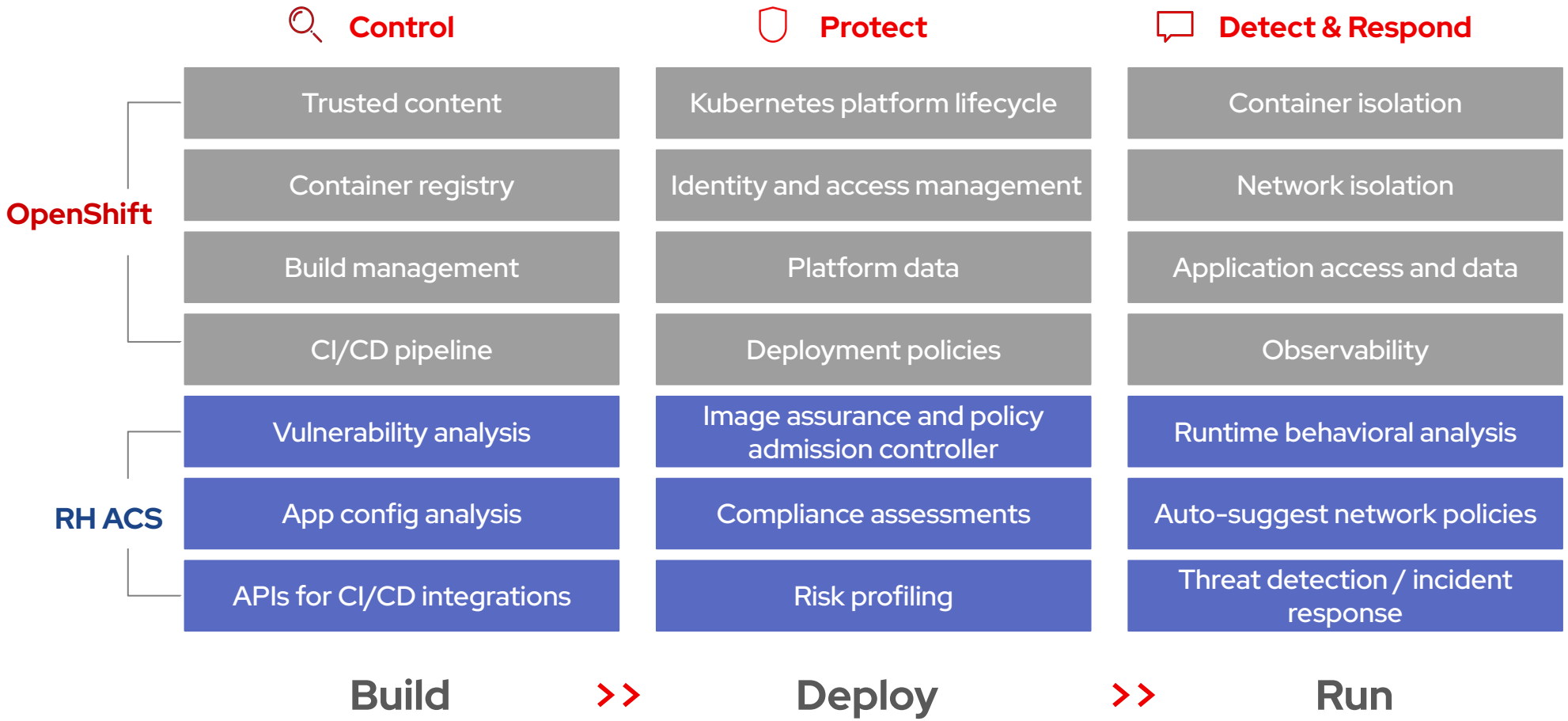
Red Hat Advanced Cluster Security for Kubernetes



- OpenShift **Compliance** Operator
- OpenShift **Cert-Manager** Operator
- **FedRAMP** High for Compliance Operator
- **Disconnected** Mirroring Workflow
- Audit Log **custom configuration & OAuth**
- Kerberos support on **CoreOS** nodes
- Multiple enhancements in Red Hat Single Sign-On

Red Hat | intel

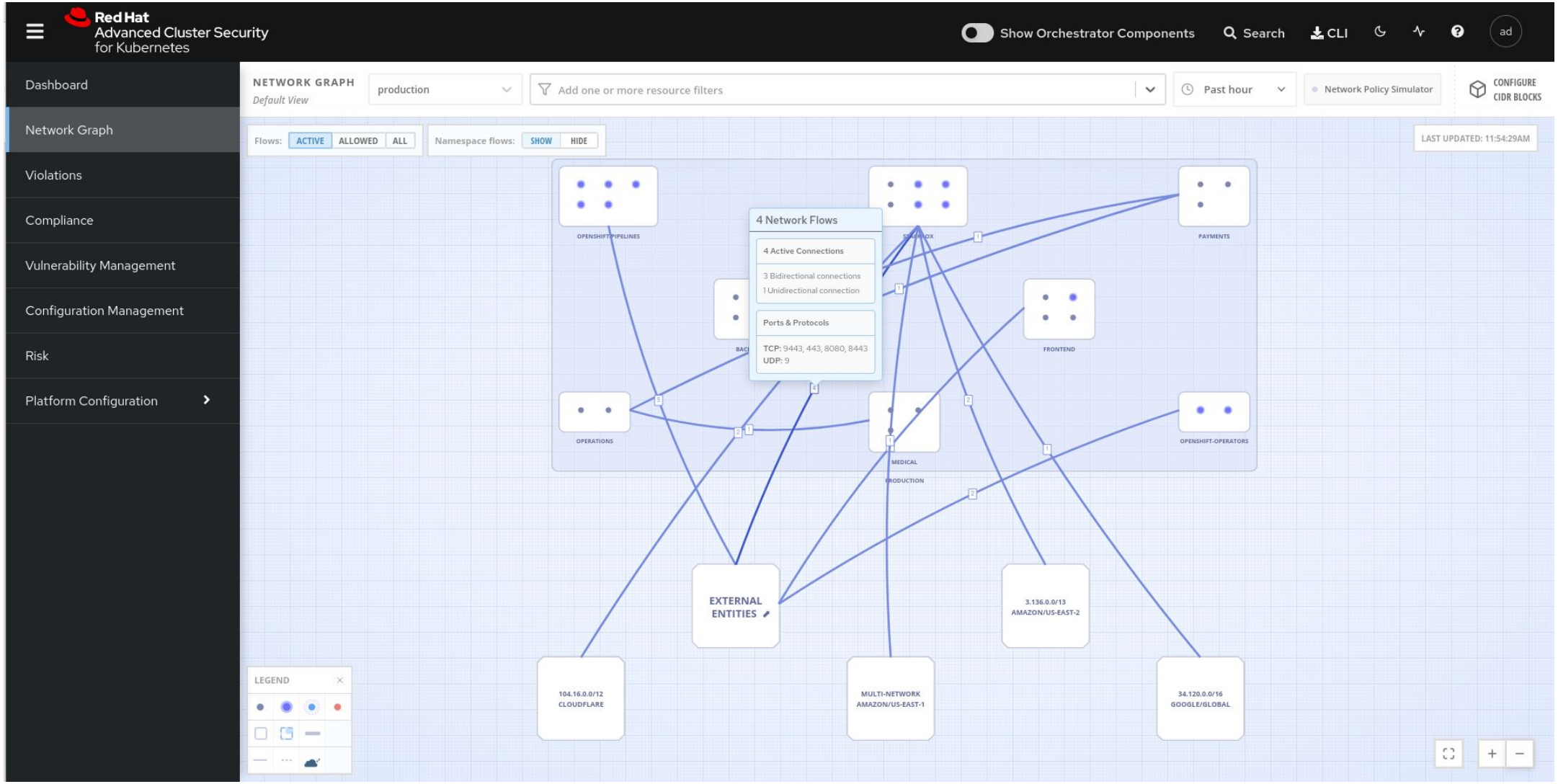
Red Hat Advanced Cluster Security for Kubernetes



DevSecOps

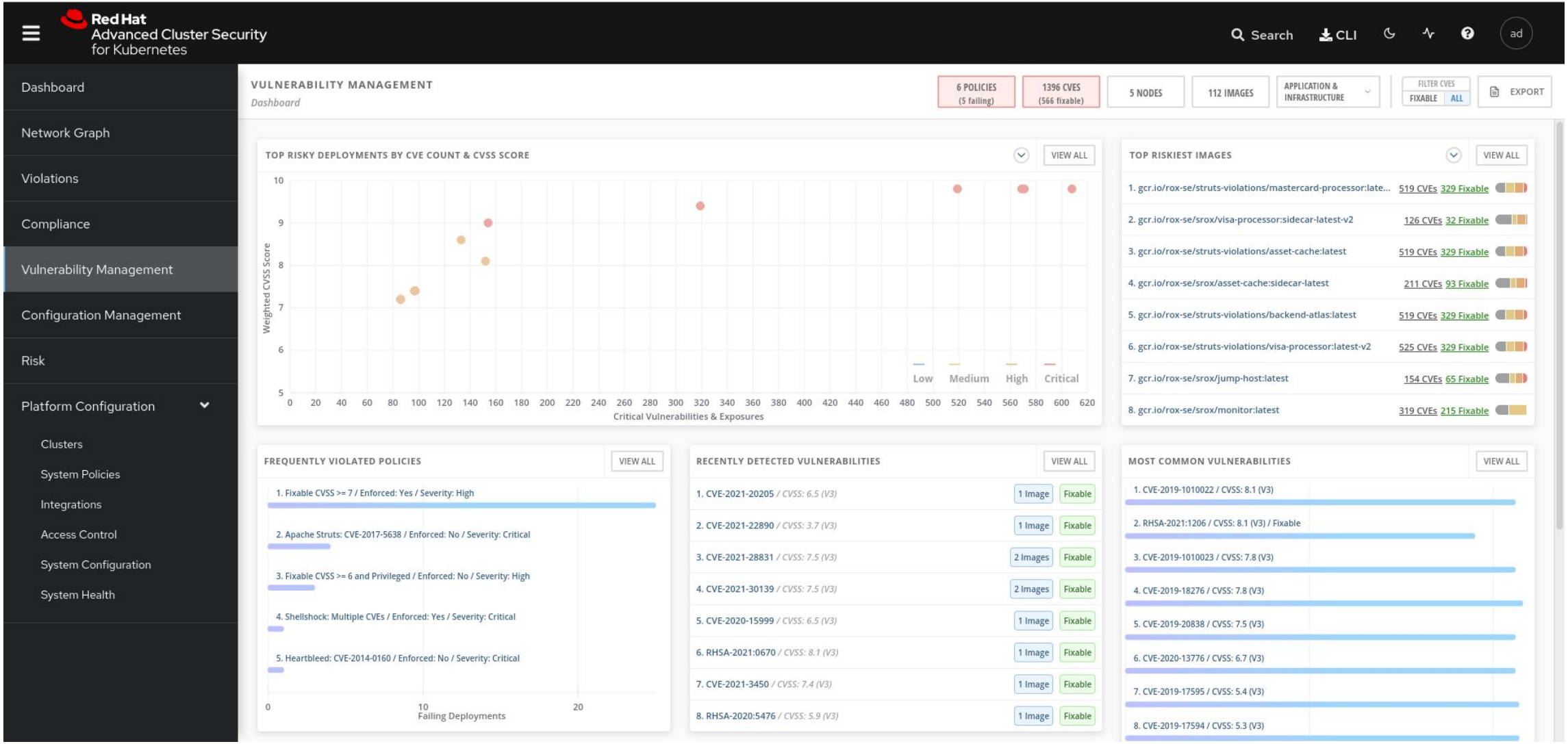
Red Hat | intel

Visibility (network policies auto-discovery & edition)

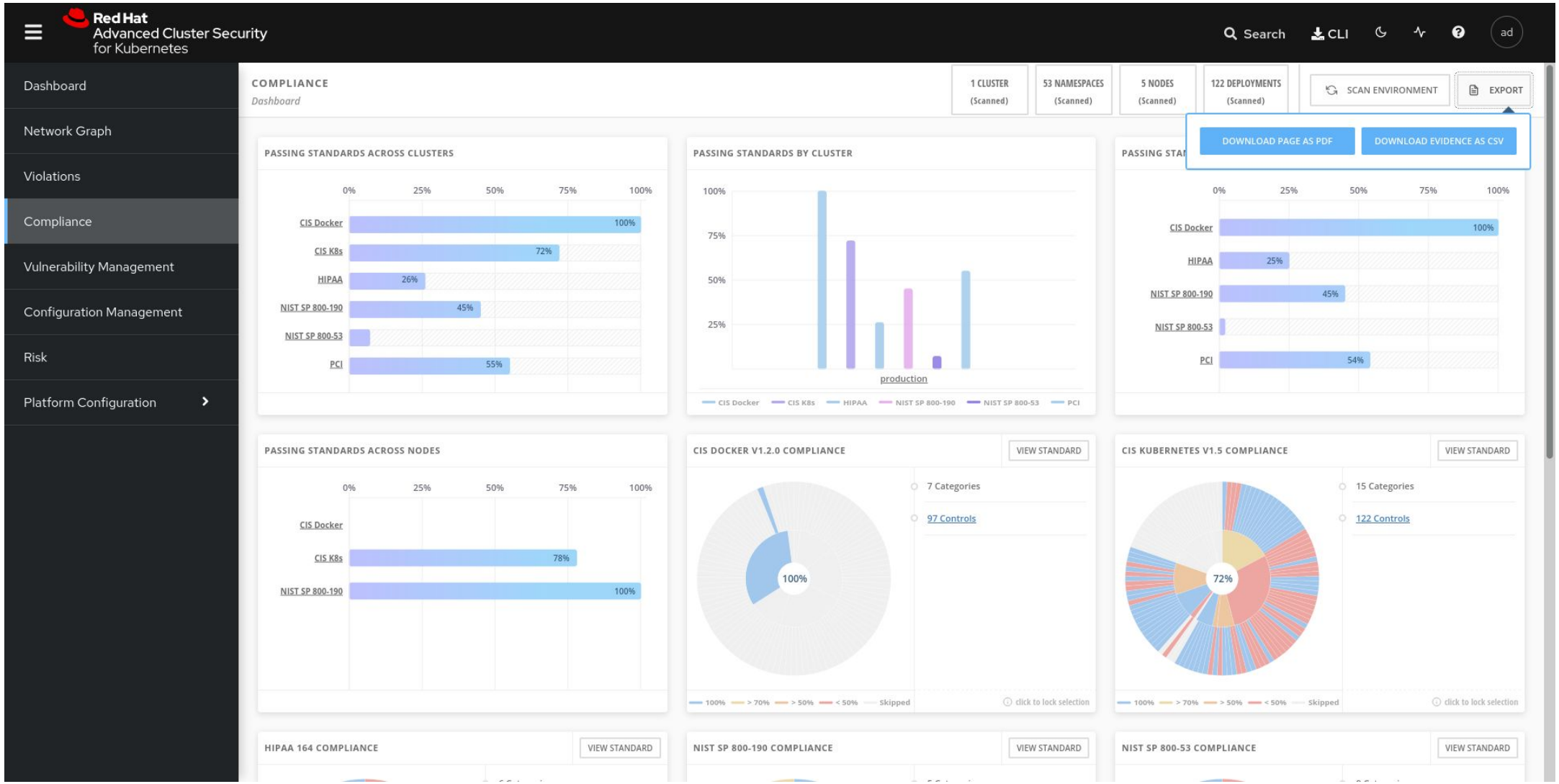


Red Hat | intel

Vulnerability Management



Compliance


Red Hat
Advanced Cluster Security
for Kubernetes
Search
CLI
ad
Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration
COMPLIANCE
Dashboard
1 CLUSTER (Scanned)
53 NAMESPACES (Scanned)
5 NODES (Scanned)
122 DEPLOYMENTS (Scanned)
SCAN ENVIRONMENT
EXPORT
DOWNLOAD PAGE AS PDF
DOWNLOAD EVIDENCE AS CSV
PASSING STANDARDS ACROSS CLUSTERS
CIS Docker 100%
CIS K8s 72%
HIPAA 26%
NIST SP 800-190 45%
NIST SP 800-53
PCI 55%
PASSING STANDARDS BY CLUSTER
production
PASSING STANDARDS ACROSS NODES
CIS Docker
CIS K8s 78%
NIST SP 800-190 100%
CIS DOCKER V1.2.0 COMPLIANCE
VIEW STANDARD
7 Categories
97 Controls
100%
CIS KUBERNETES V1.5 COMPLIANCE
15 Categories
122 Controls
72%
HIPAA 164 COMPLIANCE
NIST SP 800-190 COMPLIANCE
NIST SP 800-53 COMPLIANCE

Red Hat Advanced Cluster Security for Kubernetes

Release 3.69.1

- Security
  - Improved **detection of Spring vulnerabilities**
  - Scanning of the **OpenShift Integrated Registry**
- DevSecOps
  - Identify inactive software component
- Policy
  - Operational deployment readiness

Release 3.70

- Security
  - Supply Chain: Verify image signatures against **Cosign** public keys
  - Network segmentation: Identify **Missing** Kubernetes Network Policies
- DevSecOps
  - Automatic **Amazon ECR** registry integration for AWS clusters
- Performance
  - **eBPF** as default collector method
- Policy
  - **Identify Spring critical vulnerabilities**
  - Improved validation of Pod Security Context

Red Hat | intel

OpenShift sandboxed containers

Kernel Isolation for containerized workloads

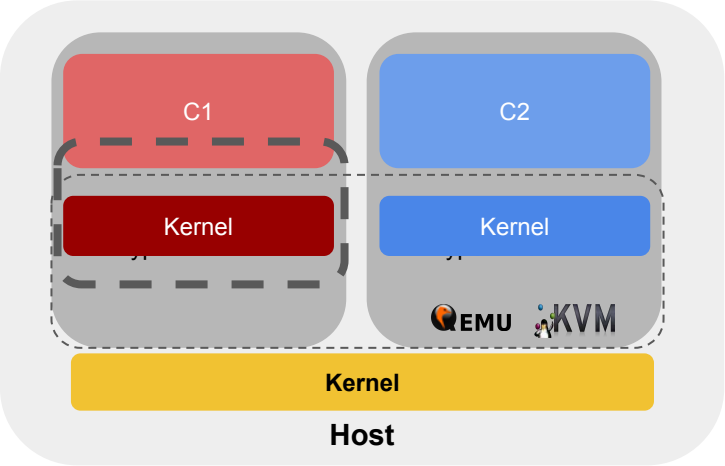
Edge and Cloud Support

- Bare metal support on AWS - Tech Preview
  Ability to install OpenShift sandboxed containers on AWS BM instances

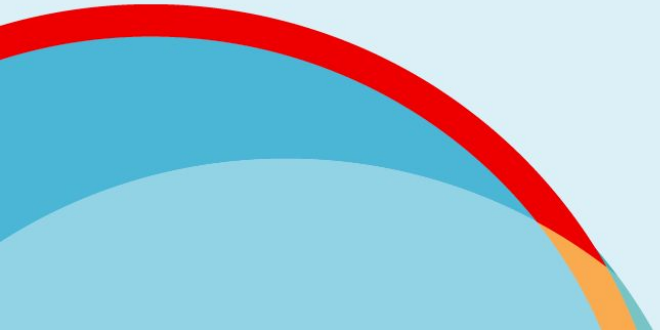
- Sandboxed Containers available and supported on SNO
  Ensured that Sandboxed Containers can run on SNO

Enhanced Observability

- Additionals Upstream Kata Specific Metrics
  Better administration with visible metrics on performance, health or potential bottlenecks



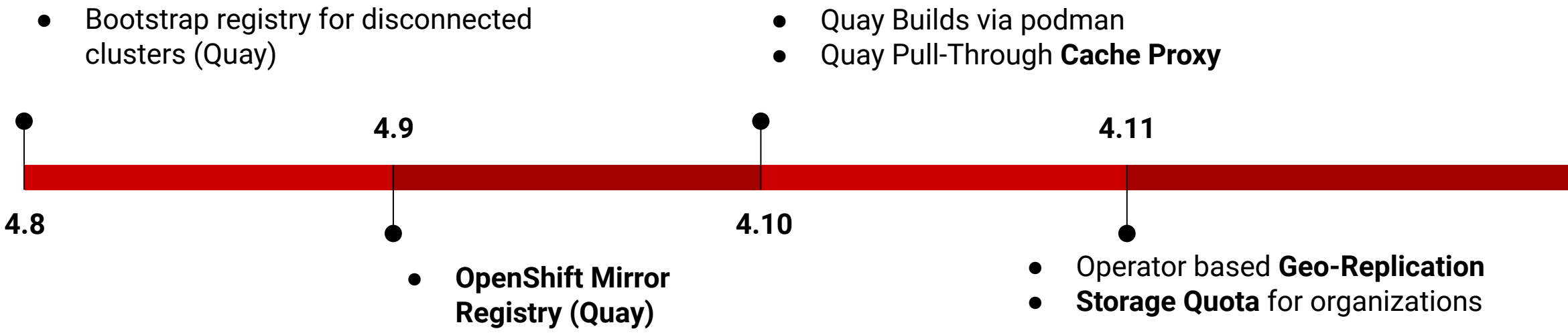
Quay



Red Hat | intel.

Quay Registry

Roadmap



Quay Registry

Storage Quota on Organizations

Control and contain storage growth of your container registry with reporting and enforcement.

Transparent pull-thru cache proxy

Use Quay as a transparent cache for other registry for improved performance and resiliency.

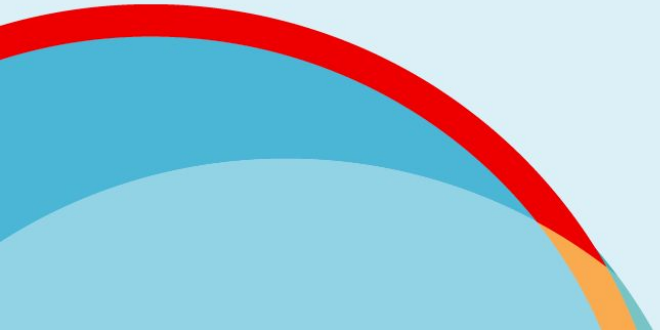
Geo-replication with the operator

Deploy a geographically dispersed container registry across two or more OpenShift clusters.

Disconnected Install and Update

Support for disconnected environments by adhering to ImageContentSourcePolicy and cluster-wide proxy settings. Improved credential management.

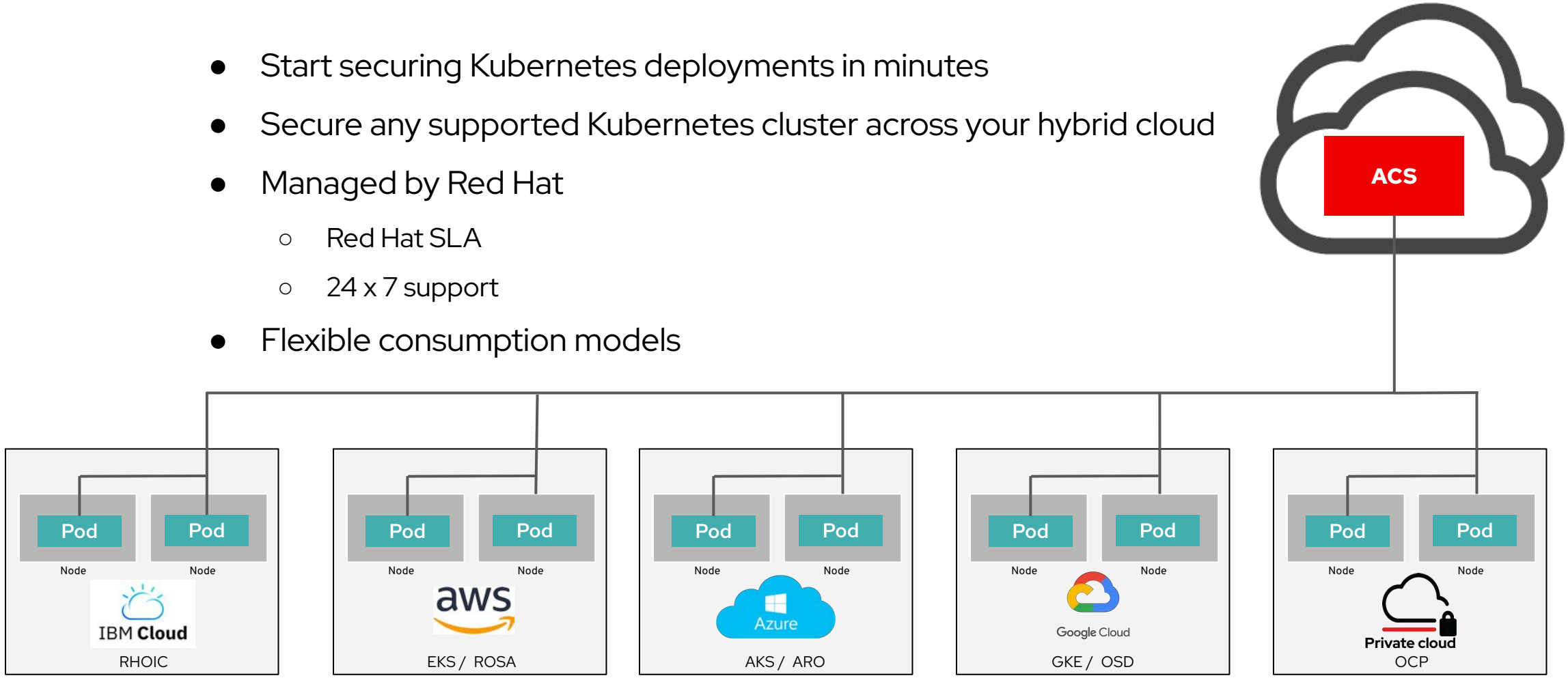
What’s next



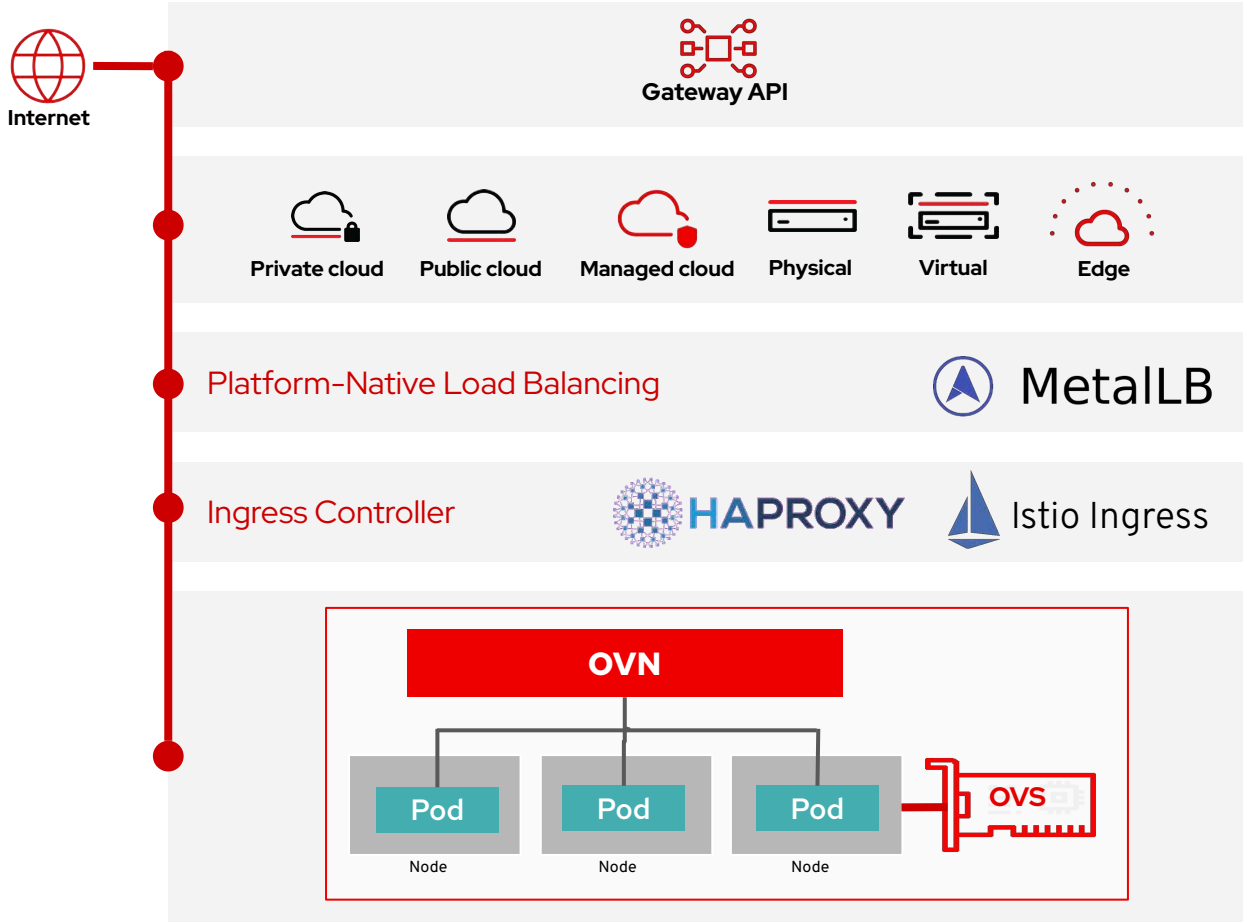
Red Hat | intel.

Introducing Advanced Cluster Security **as a Service**

- Start securing Kubernetes deployments in minutes
- Secure any supported Kubernetes cluster across your hybrid cloud
- Managed by Red Hat
  - Red Hat SLA
  - 24 x 7 support
- Flexible consumption models



Multi-cluster End-to-End Networking



- Unified traffic handling so you configure all your traffic the same way
- Any supported platform – add or swap easily, hybrid scenarios
- Flexibility to use native traffic distribution and filtering (e.g. WAF) for optimal performance
- Your traffic, your way: L3-L7, Envoy, by-pass, custom HTTP header support
- OVN for advanced traffic workloads
- IPv6 single/dual stack across all platforms that support it
- eBPF for policy, traffic control, tooling, debugging, observability
- Advanced host-level firewall functionality
- Observability enhancements across all networking (e.g. SR-IOV)
- Multi-NIC support to align host networking
- HW Offload (OVS, IPsec, ...) for performance
- Submariner

Red Hat | intel

Observability

Networking

Unified Experience

Network Traffic Metrics and Tracing

Whether one cluster or one hundred, developers and cluster administrators require seamless connectivity across applications.

Security Everywhere

Network Policy and Governance

Security and regulatory compliance requires governance of traffic in, around, and out of networks.

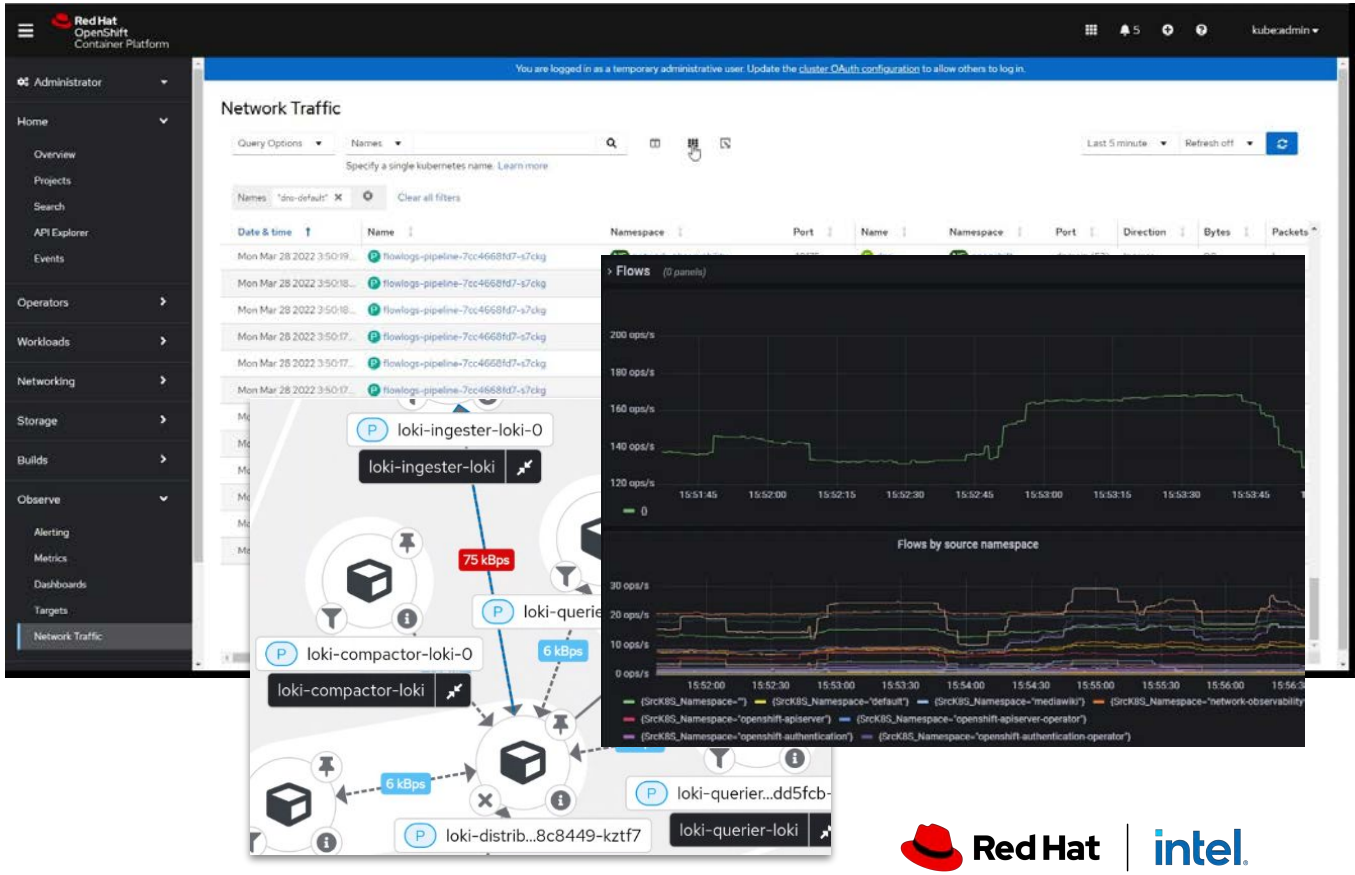
Platform Consistency

Network Traffic Flow and Topology

Developers and administrators require a common understanding of their traffic within and across cluster boundaries.

Network Flow Data – New Insight & Presentation

Tabular Netflow data, NOC Dashboard, Pod/Service/Node-specific Topology, New Metrics, Export options



OpenShift on Bare Metal

Hardware support for nodes

More hardware supported through Redfish improvements.

Hardware integration Improvements

SaaS Installer

Hosted Assisted Installer will be promoted to GA from Tech Preview.

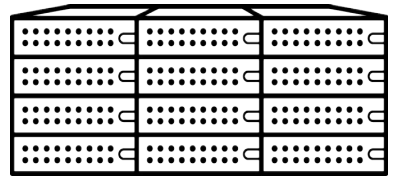
Assisted Installer GA

Agent-based Installer

Agent-based installer to easily create initial cluster. Automate on-premises clusters installations. Install via UI.

Faster, easier on-premises installations

Metal³



OpenShift Support for Windows Containers

Platform Consistency

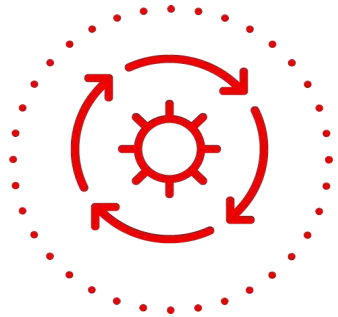
Windows nodes will move to Containerd as the runtime, and CSI for storage, thus future proofing consistency and application portability for Windows

Consistent experience with upstream

Unified Experience

Health Management of Windows Nodes with self healing will allow for better resiliency of the Windows nodes (e.g. recovering from a Kubelet crash). Horizontal Pod Autoscaling of Windows pods to will enable workloads to be scaled to match demand

Easy Management of Windows apps



Expanding Ecosystem

Support for **Windows Server 2022**, more networking plugins (Calico etc) to provide additional platform choices for Windows applications running on OpenShift

Broader compatibility

Red Hat | intel

OpenShift Virtualization

Unified Experience

New VM creation Wizard flow

VM centric overview page

Performance tuned VM templates

Improved flexibility with live migration policies

Support RHEL High Availability

Manage VMs at Scale

Security Everywhere

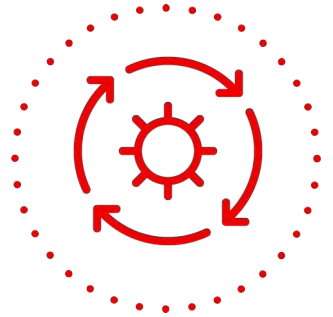
RBAC for VM templates

Isolate Live Migration with dedicated network

Multi-tenant virtual OpenShift clusters with Hosted Control Planes (HyperShift)

Enhanced secondary network using micro-segmentation on OVN

Enhanced security and controls for VMs



Platform Consistency

More depl choices with Public Cloud & Bare Metal providers

RHEL 9 & Windows 11 guests

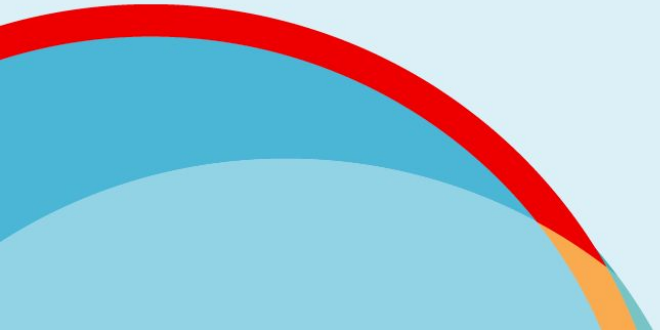
Network latency checks for telco and high performance workloads

Enhanced Ecosystem of Data Protection partners

Broader Compatibility

Red Hat | intel.

Muchas gracias !!



Red Hat | intel.