NYRHUG
Red Hat Advanced Cluster Management for Kubernetes

Harshil Sabhnani - Consulting Architect FSI
05/17/2023

Red Hat

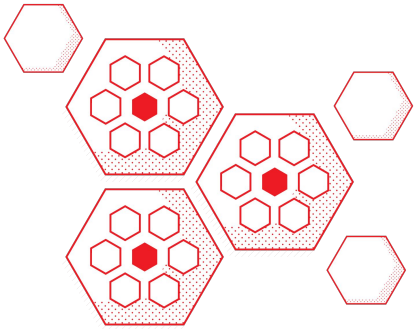
Speaker Biography

Agenda

- Market Trends and Challenges
- Key Personas
- Introducing Red Hat Advanced Cluster Management for Kubernetes
- Architecture
- Installation Demonstration
- Featureset Demo
- Resources and Next Steps

Market Trends and Challenges

Kubernetes adoption leads to multicluster



"As Kubernetes gains adoption across the industry, scenarios are arising in which I&O teams are finding they must deploy and manage multiple clusters, either in a single region on-premises or in the cloud, or across multiple regions….for a number of reasons, including multi-tenancy, disaster recovery, and with hybrid, multicloud, or edge deployments."

Source:
Assessing Patterns for Deploying Distributed Kubernetes Clusters doc # G00465217, by Tony Iams

Reasons for deploying clusters

Application availability

Reduced latency

Address industry standards

Geopolitical data residency guidelines

Disaster recovery

Edge deployments

CapEx cost reduction

Avoid vendor lock-in

Hybrid Multicloud management is really hard

As organizations deploy more across multiple clouds, new challenges arise.

- **Difficult and error prone** to manage at scale
- **Inconsistent security controls** across environments
- **Overwhelming to verify** components, configurations, policies, and compliance

IDC Survey of 200 US-based $1B companies actively using two or more "infrastructure clouds" for production applications

Using multiple infrastructure clouds*

Using multiple public clouds and one or more private/dedicated clouds*

Source:
IDC Multicloud Management Survey, 2019: Special Study, Doc # US45020919, April 2019
*IDC Survey of 200 US-based $1B companies actively using two or more "infrastructure clouds" for production applications

Red Hat

Where's the growth in cluster deployments?

Small Scale Dev Teams

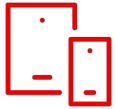
- Managing and syncing across Dev/QE/Pre-Prod/Prod clusters can be difficult

Medium Scaled Organizations

- Retail with small clusters across 100s of locations
- Organizations with plan for growth 10-15 clusters moving to 100s

Large scale

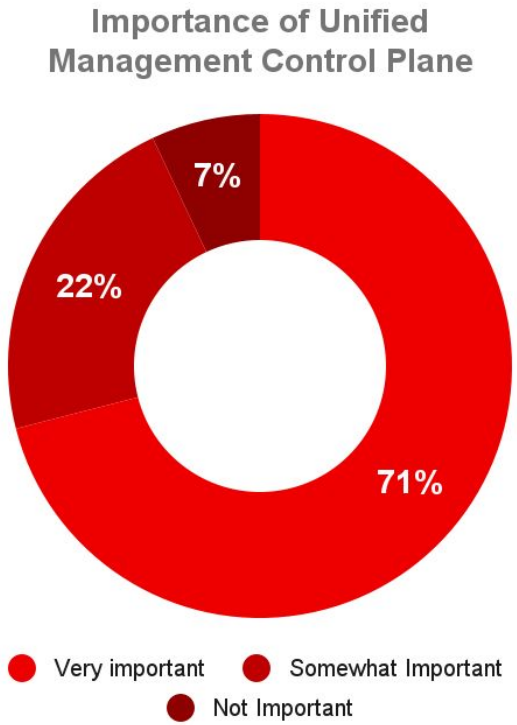
- Global organizations with 100s of clusters, hosting thousand of applications
- Large Retail with 1000s of stores



Edge scale / Telco

- 100s of zones, 1000s of clusters and nodes across complex and air-gapped topologies

Unified, consistent, autonomous operations priorities



*Most important reasons organizations need a unified management control plane for all digital infrastructure resource is to

42%

Improve data integration and data protection

41%

Optimize infrastructure costs and usage

*Source:
Future of Digital Infrastructure Agenda Q2 Survey 2021, IDC, June, 2021. n = 254 US decision makers.

Red Hat

Key Personas

IT Operations

"How can I manage the lifecycle of multiple clusters regardless of where they reside using a single control plane?"

"How can I quickly get to the root cause of failed components?"

"How do I monitor usage across multiple clouds?"

SRE/DevOps

"How do I get a simplified understanding of my cluster health and the impact on my application availability?"

"How do I automate provisioning and destroying of my clusters, workload placement based on capacity and policies, and the pushing of application from dev to prod?"

SecOps

"How do I ensure all my clusters are compliant with my defined policies?"

"How do I set consistent security policies across diverse environments and ensure enforcement?"

"How do I get alerted on any configuration drift and remediate it?"

Introducing Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes

Simplified operation and maintenance

View, manage, operate and solve issues all through a single console.

Runs on OpenShift

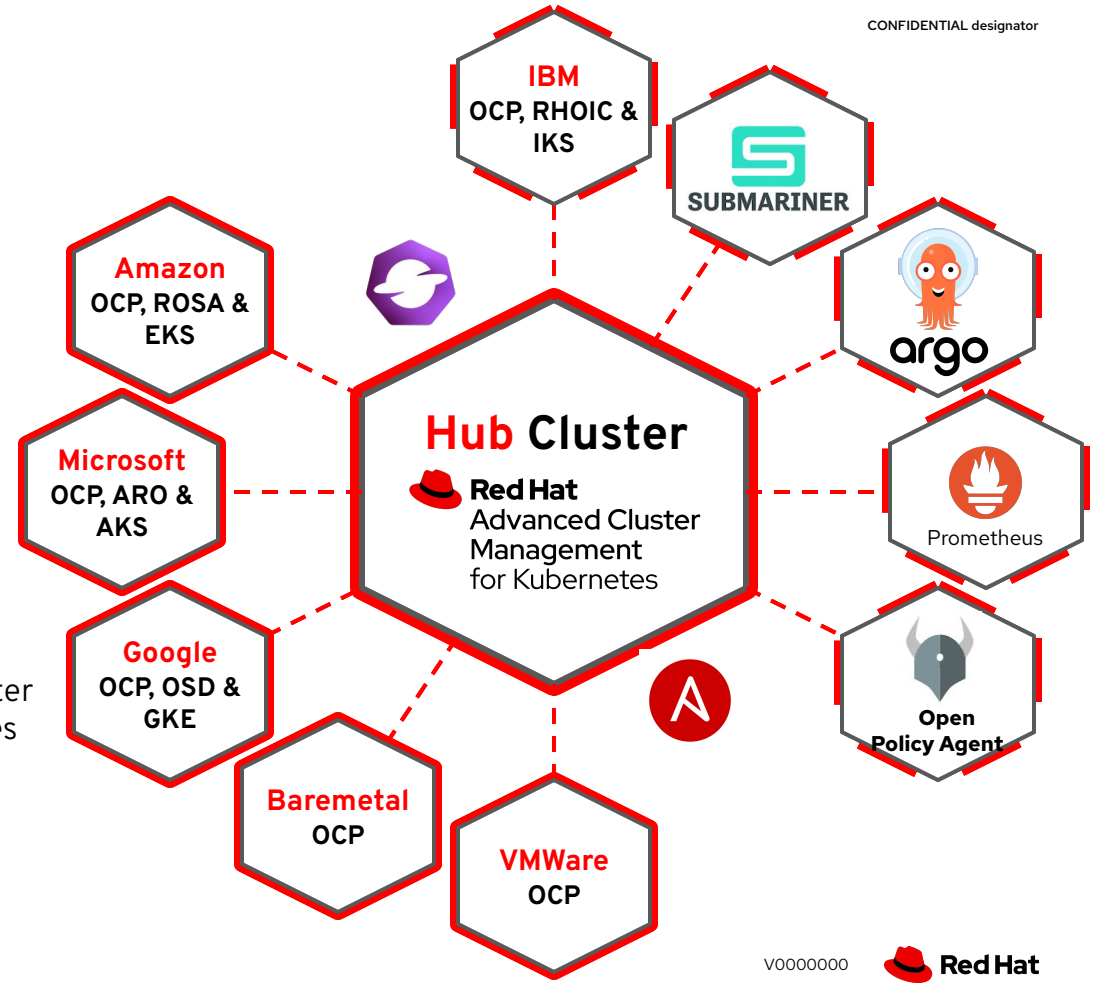
Like any other Kubernetes app, easily run and manage it on top of a OpenShift cluster.

Hub-Spoke architecture

Have all configurations managed by the Hub cluster component and seamlessly add Spoke Kubernetes clusters to the central hub.

Tight Integration

RHACM comes with a rich API, add-ons and it can integrate with some key other enterprise tools.

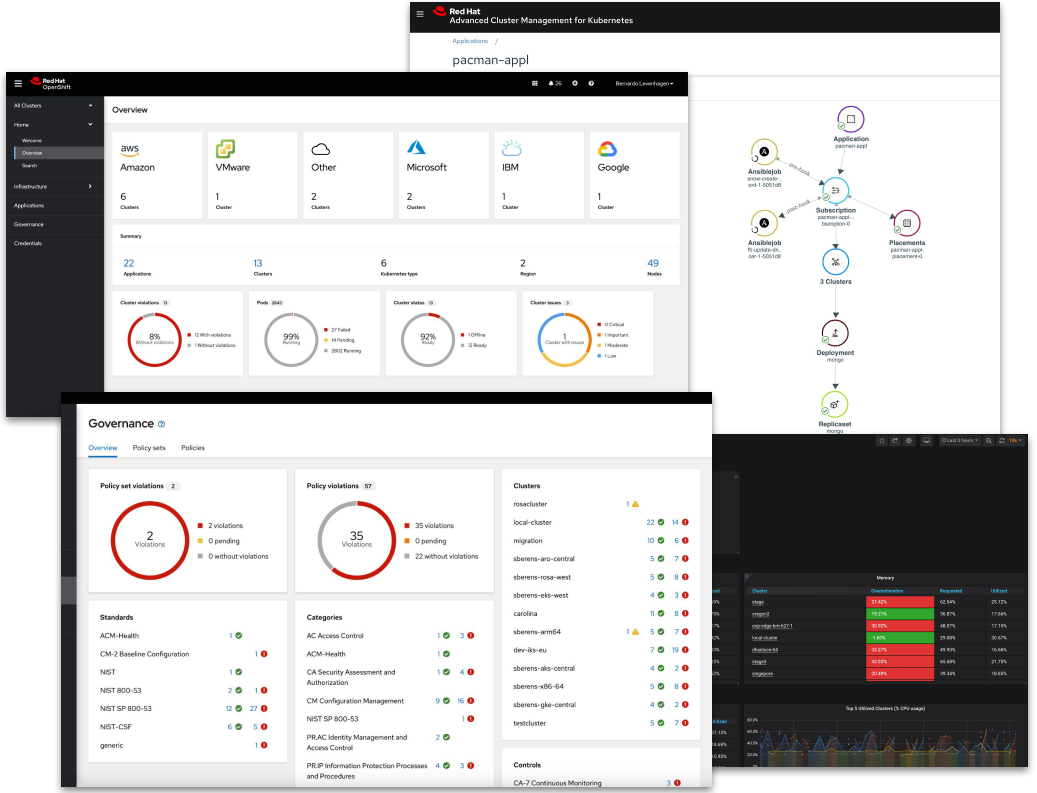


Red Hat

Robust & Proven

End-to-end automation with Red Hat Ansible Automation Platform integration

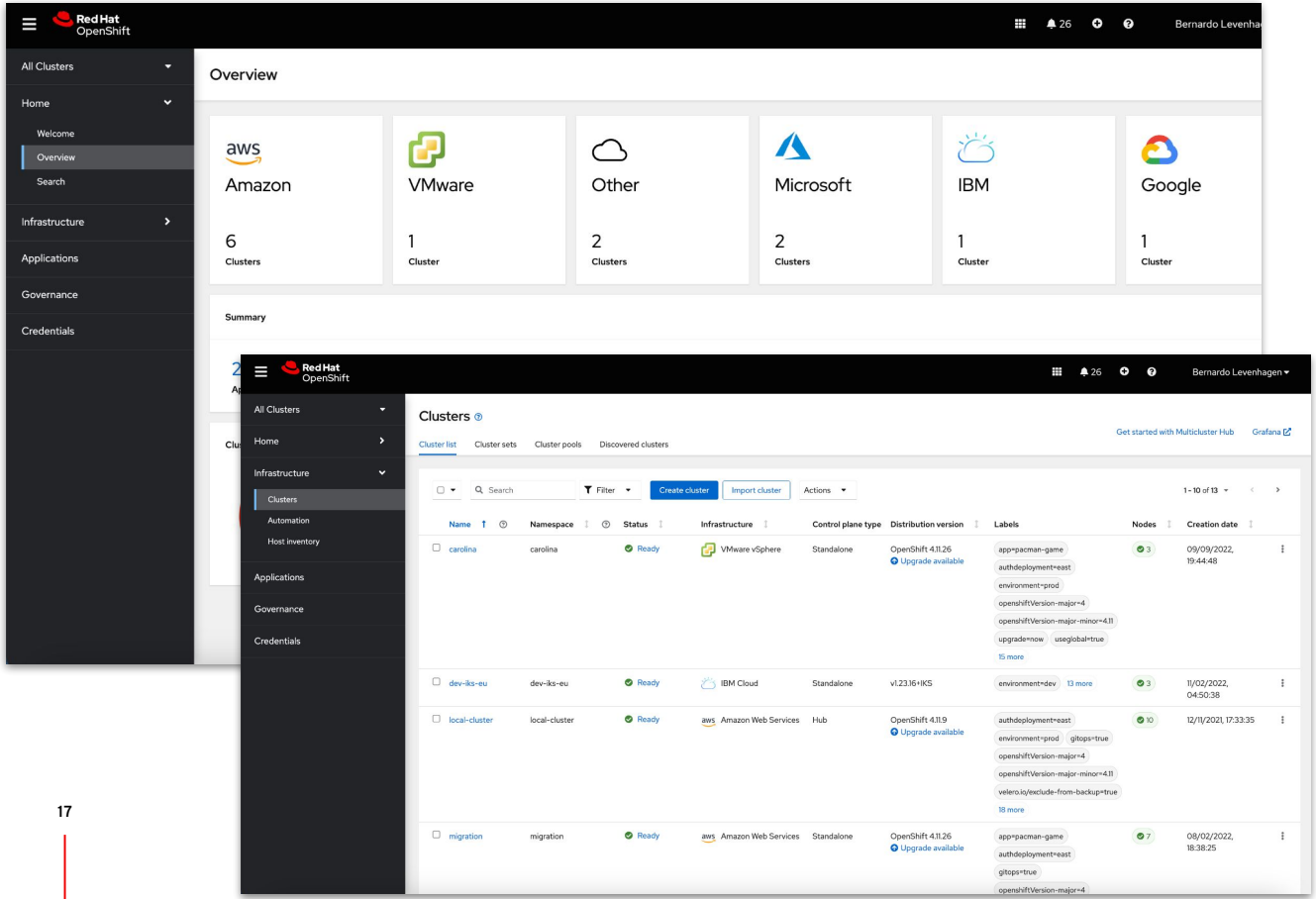
- Multicluster lifecycle management
- Policy driven governance, risk, and compliance
- Advanced application lifecycle management
- Multicluster observability for health and optimization
- Multicluster networking for interconnecting



Red Hat

Unified Multi Cluster Management

Single Management for all your Kubernetes Clusters

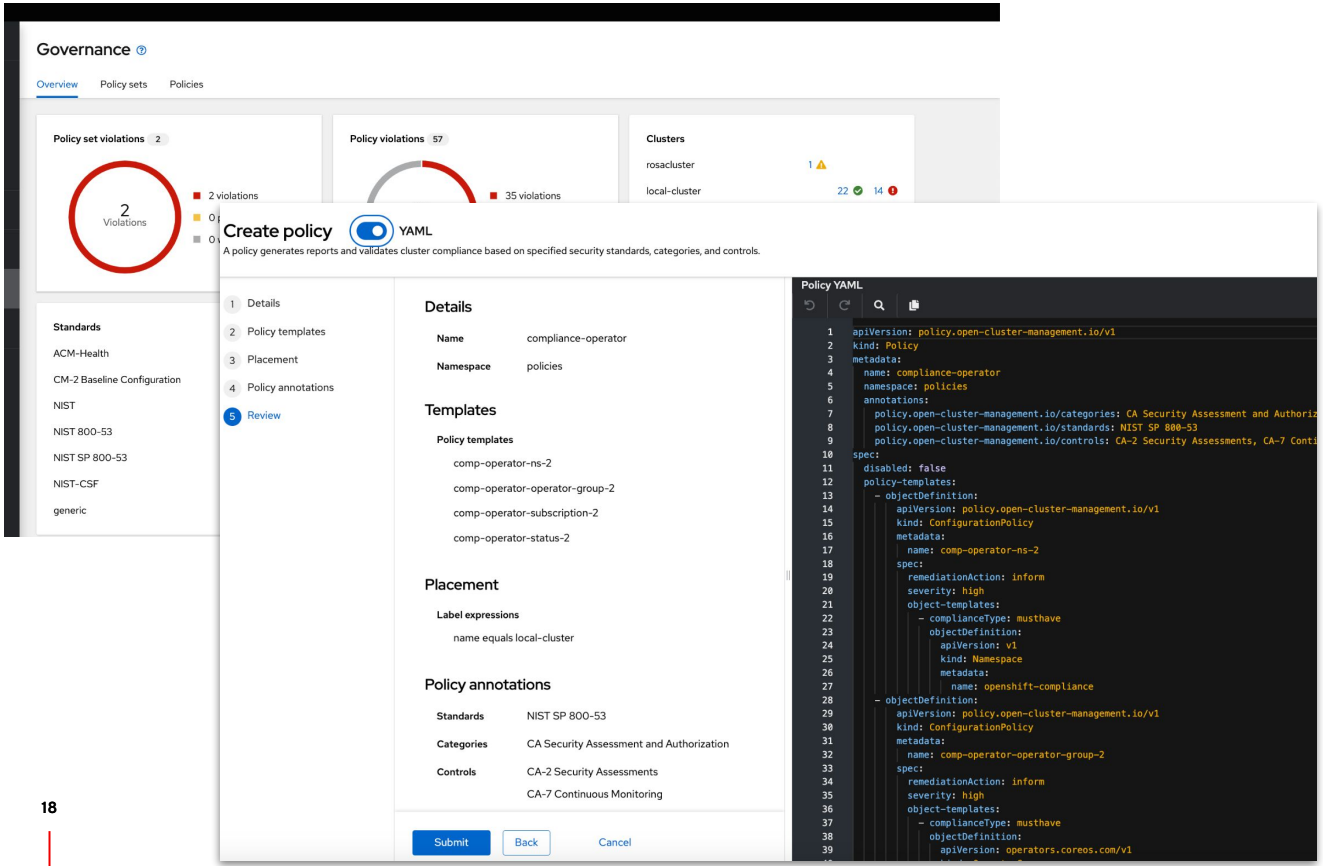


- **Centrally** create, update and delete Kubernetes clusters **across multiple** private and public clouds
- **Hibernate / resume** OCP Clusters across your domain
- **Configure ClusterSets & Cluster Pools** for simplified OCP cluster management
- Search, find and modify **any** kubernetes resource across the **entire** domain
- **Quickly** troubleshoot and resolve issues across your **federated** domain

Red Hat

Policy based Governance, Risk, and Compliance

Don’t wait for your security team to tap you on the shoulder

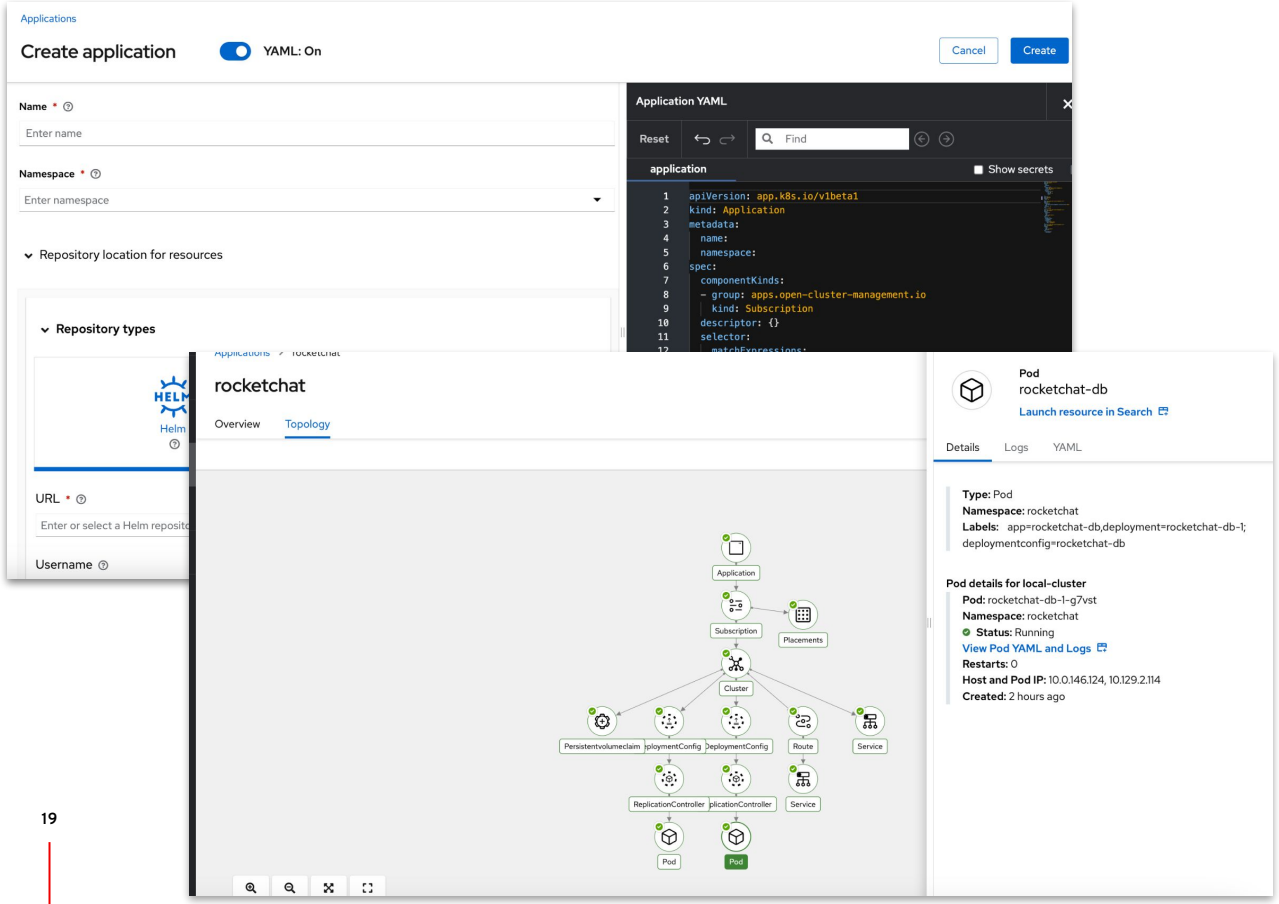


- **Centrally** set & enforce policies for security, applications, & infrastructure
- Quickly **visualize** detailed **auditing** on configuration of apps and clusters
- Perform remediation actions by leveraging **Ansible Automation Platform** integration.
- Built-in **compliance policies** and audit checks, including **GitOps** integration.
- **Immediate** visibility into your compliance posture based on **your** defined standards

Red Hat

Advanced Application Lifecycle Management

Simplify your Application Lifecycle



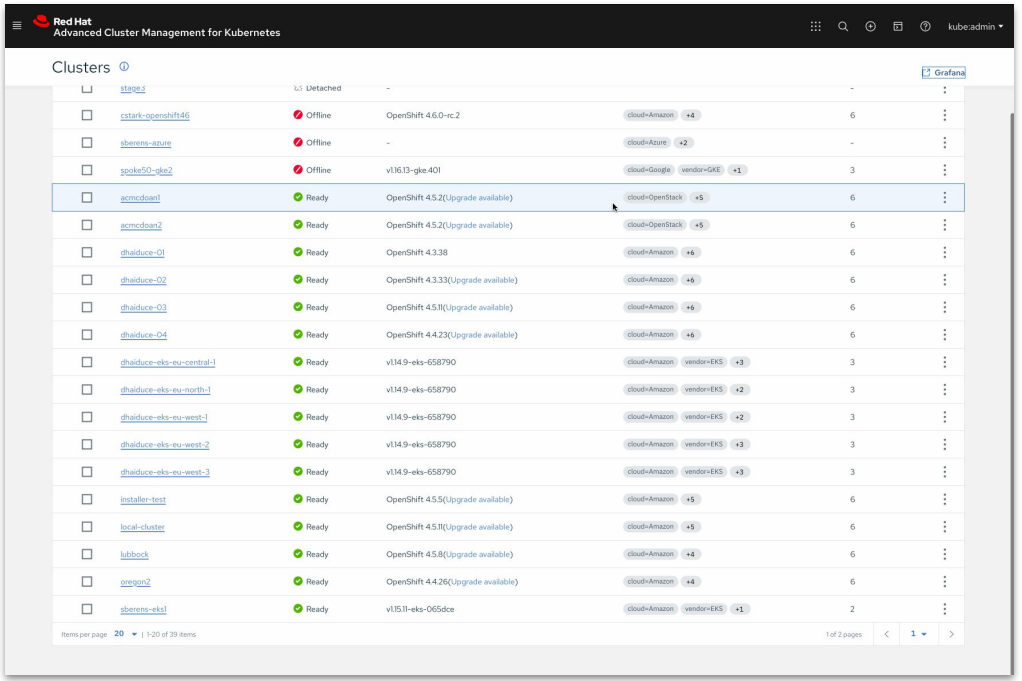
- **Easily** deploy an Application using the **Application Builder** (Subscription)
- Deploy applications from **multiple** Sources (Git/Helm/Object Storage)
- Integrate with **OpenShift GitOps** (Argo CD).
- Automatically **detect and visualize Argo CD** Applications in RHACM
- Quickly **visualize** application relationships **across** clusters and those that **span** clusters

Red Hat

Multicluster Observability

Overview

- Global Query view with **Grafana** for OCP Clusters
  - Out of the Box multi cluster health monitoring dashboards
  - PromQL compliant - Build your own queries
- **Centralize Alerts** and notifications on the **RHACM Hub**. Forward to 3rd Party Systems (PagerDuty / Slack)
- Centralized **Database**
  - Optimized set of metrics collected from managed clusters
  - Focused on Cluster Management
- Unlimited **Data Retention**
  - Observe Metric trends
  - Set Alert Patterns
  - Supported Object Storage
    - AWS S3 (and compatible)
    - Ceph for on-premise
    - Google Cloud Storage
    - Azure Storage

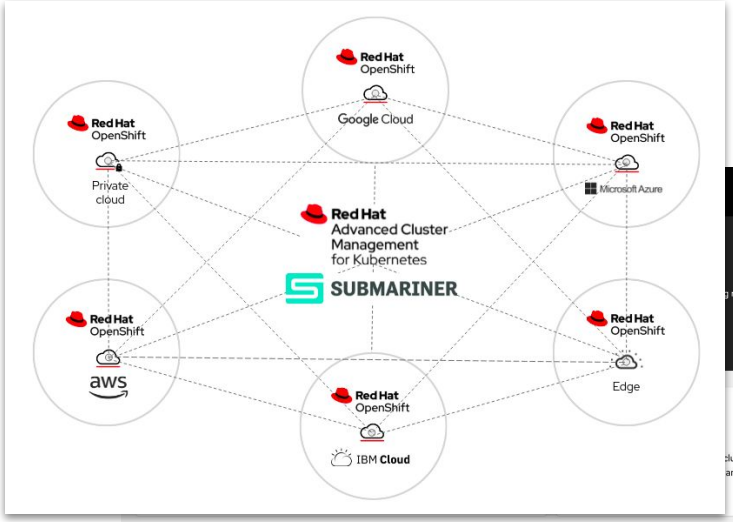


Red Hat

Multicluster Networking

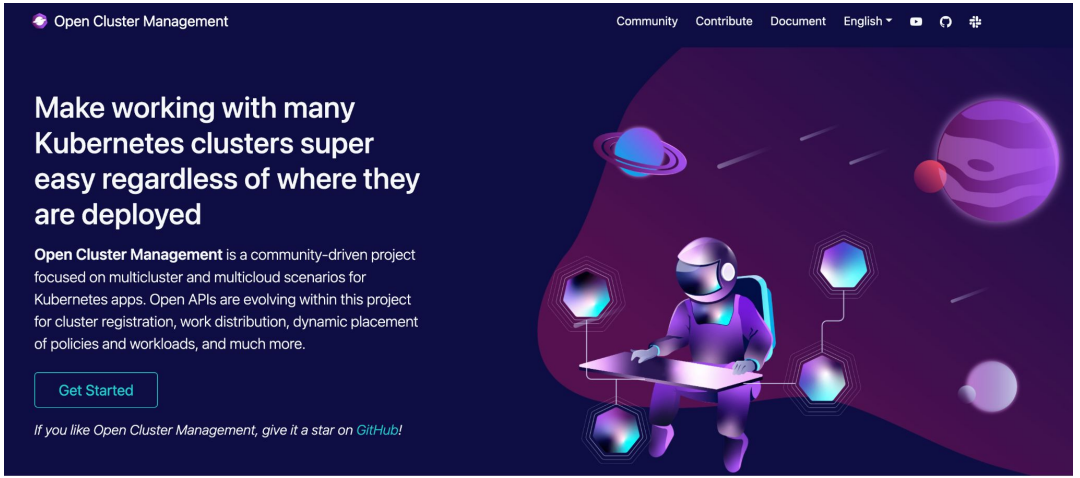
MCN features overview & look ahead

- **ACM MCN, aka 5th pillar**
- Presenting **Submariner**: an CNCF open source project in the form of an **add-on** for RHACM, now generally available
- Enable **direct networking** between Pods in different Kubernetes clusters as well as **Service Discovery**, either on-premises or in the cloud
- Leverage **Cluster Sets** - All done via a group of clusters with a high degree of mutual trust that share services
- **Globalnet** – Support for interconnecting clusters with overlapping CIDRs
- **Future work (subject to change)**
  - ACM Red Hat OpenShift Service mesh integration
  - Discovery Deploy & Configure Federation
  - Custom - upstream Istio, Gloo…



Open Source commitment - Upstream project

- **Open Cluster Management** has been accepted as a **CNCF Sandbox**
  - https://www.cncf.io/projects/open-cluster-management/
- Collaboration in key **Kubernetes Special Interest Groups (SIGs)**
  - Sig-MultiCluster
  - Sig-Application
  - Sig-Policy
- Growing together with support from partners and contributors
  - Ant Group
  - Alibaba
  - Tencent
  - Microsoft **



Feature Overview

Cluster inventory
Registration of multiple clusters to a hub cluster to place them for management.

Work distribution
The work API that enables resources to be applied to managed clusters from a hub cluster.

Content placement
Dynamic placement of content and behavior across multiple clusters.

Vendor neutral APIs
Avoid vendor lock-in by using APIs that are not tied to any cloud providers or proprietary platforms.

https://open-cluster-management.io

Red Hat

Strong open source community & ecosystem

OPA/Gatekeeper

Hive

metal3

Open Cluster
Management

Benefits

Red Hat OpenShift and Red Hat Advanced Cluster Management for Kubernetes

Accelerate development to production

Self-service provisioning allows app dev teams to request clusters directly from a catalog removing central IT as a bottleneck.

Reduce costs

Centralized management of clusters reduces operational cost, makes the environment consistent, and removes the need to manually manage individual clusters.

Increase application availability

Placement rules can allow quick deployment of clusters across distributed locations for availability, capacity, and security reasons.

Ease Compliance

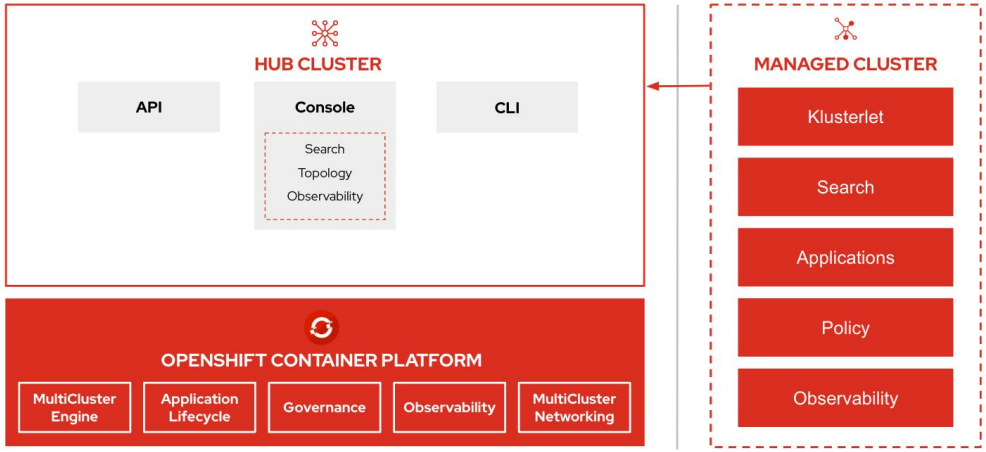
Policies can be written by the security team and enforced at each cluster, allowing environments to conform to your policy.

Architecture

Architecture Overview

Components

IT Operations



Hub architecture and components

Red Hat Advanced Cluster Management uses the **multiclusterhub-operator** and other operator and runs in the **open-cluster-management** namespace

Managed cluster architecture and components

Red Hat Advanced Cluster Management managed clusters use the **klusterlet** operator which runs in the **open-cluster-management-agent** namespace

* Multicluster Engine is the cluster lifecycle operator that provides cluster management capabilities for OpenShift Container Platform and Red Hat Advanced Cluster Management hub clusters. MCE, for short, is entitled within OCP subscriptions and is installed automatically along with an ACM operator deployment.

Red Hat

Architecture Overview

Operator install for managed cluster

IT Operations

Managed cluster

The **klusterlet** operator controls the deployment of components on the managed cluster.

List of included components:

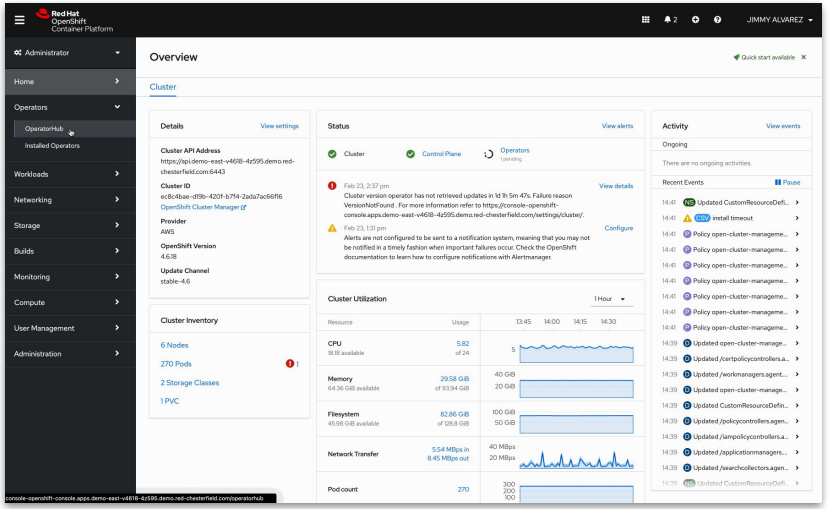
- Application manager
- Certificate controller
- Policy controller
- Registration agent
- Observability controller
- Search collector
- Cluster proxy
- IAM policy controller
- Work manager

Installation

Installation and Foundation

Operator-based installation for Hub cluster

IT Operations



Hub Cluster

- Operator-based installation
- Available on OperatorHub
- Requires OCP 4.10.x - **Latest**

Full Lifecycle Management of OCP clusters

- Deploy OpenShift 4.8.x - **Latest**

Import and Management of OCP clusters

- OpenShift 3.11*, OpenShift 4.8.x - **Latest**
- Cloud hosted OCP: ROSA / OSD / ARO / RHOIC

Import and Limited Management for cloud Kubernetes

- EKS, AKS, GKE, IKS

High Availability

- Supports OCP Availability Zone

Resource Requirements

- **Test**: 3 master, 3 workers, 6 vCPU and 16GB RAM
- **Production**: 3 masters, 3 workers, 16 vCPU and 24GB RAM*

  * Production requirements vary based on number of clusters in the management domain and types of workloads being run.

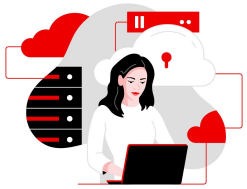
  * vCPU/RAM Numbers are per node.

29

Red Hat

Role-Based Access Control

How to control user access



- RBAC in RHACM is based on kubernetes concepts and is enforced through Openshift.
- Cluster-Admin Role is an Openshift super-user role and can perform all actions cluster-wide.
- Additional Roles are available out of the box to assign users Admin, Edit or View level access to RHACM artifacts, for more please see the documentation. See some examples below:

Role	Description
open-cluster-management:cluster-manager-admin	A user with cluster-wide binding to this role, is an RHACM super user can perform any action on RHACM resources
open-cluster-management:admin:managed-cluster-x	A user with cluster binding to this role, has admin access to ManagedCluster "X" resource
open-cluster-management:view:managed-cluster-x	A user with cluster-wide binding to this role, has view access to ManagedCluster "X" resource
OCP Default admin / edit / view roles	A user with namespace binding to these roles has access to resources like policies, applications etc in that namespace or ManagedCluster. A user with cluster-wide binding to these roles has access to resources like policies, applications etc in all namespaces or for all ManagedClusters.

ACM Featureset

Multi-cluster Lifecycle Management

 **IT Operations**	How do I get a simplified understanding of my cluster health and the impact it may have on my application availability ? How do I automate provisioning and deprovisioning of my clusters?
 **DevOps/SRE**	How can I manage the life cycle of multiple applications regardless of where they reside (on-prem, across public clouds) using a single control plane?

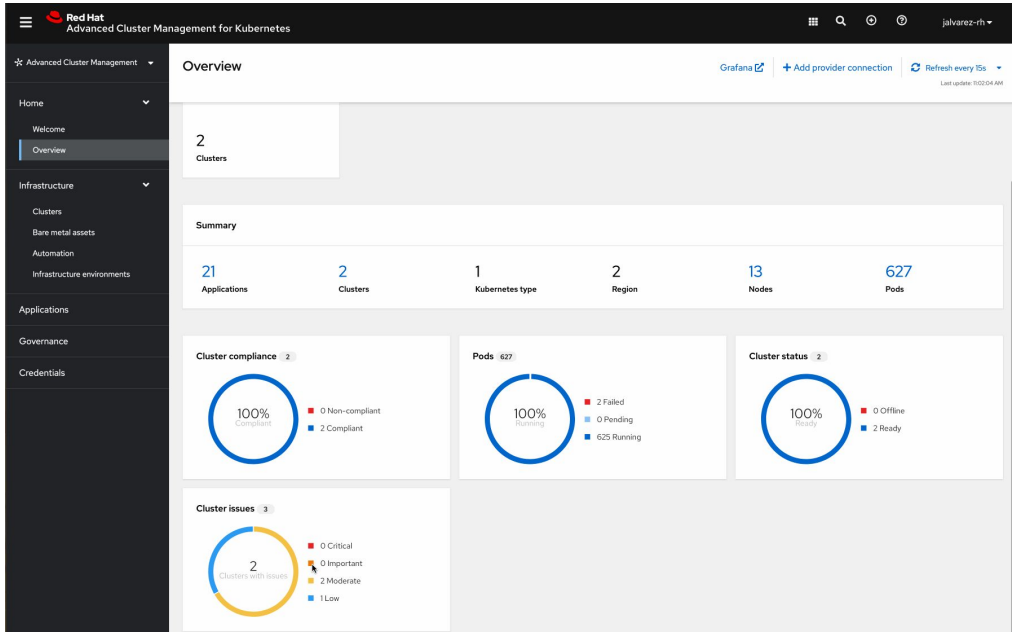
Multi-cluster Lifecycle Management

Overview

IT Operations

DevOps/SRE

- **Full Management of OCP Kubernetes**
  - Provision new OCP 4.12.x and above
  - Manage existing **OCP 3.11 (Limited Support)** 4.12.x and above
  - Support for OCP 4.12+ Single Node (SNO)
- **Public cloud managed kubernetes**: EKS, AKS, GKE, IKS, ROKS, ROSA, ARO, OSD.
  - Deploy Policies and Applications, Search, find and modify kubernetes resources.
- See **high level summaries** across all clusters
  - Misconfiguration
  - Pod status
  - Resource capacity
- **Troubleshoot and resolve** issues across the federated domain
  - See in dashboard or via a list/table form
  - Table shows custom tagging
  - Regions
  - Business Purpose
  - Version



Red Hat

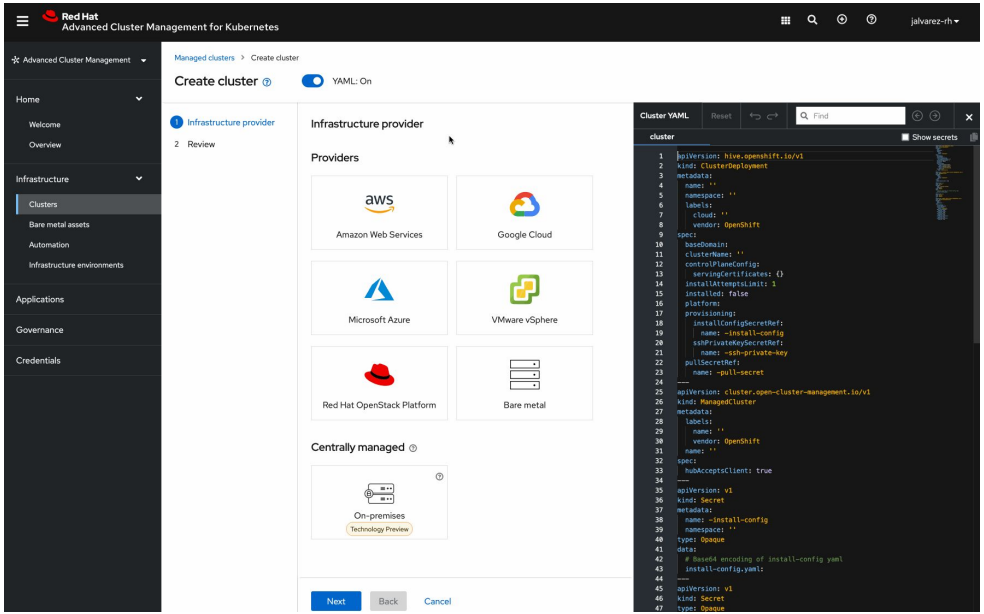
Multi-cluster Lifecycle Management

Creating & Importing clusters

IT Operations

DevOps/SRE

- **Create**, **Upgrade** and **Destroy** OCP clusters running on **vSphere**, **Bare-metal** as well as **Public cloud**.
- Import **OCP Clusters** that can be discovered from **OCM** (OpenShift Cluster Manager)
- Leverage Hive API for OCP cluster deployment
- Wizard or YAML based create cluster flow
- Launch to an OCP Console from ACM
- Access cluster login credentials and download **kubeadmin** configuration **kubeconfig**
- Integrate with Ansible Automation Platform
- Centrally Manage your On-Prem Infrastructure (CIM) / Host Inventory



Red Hat

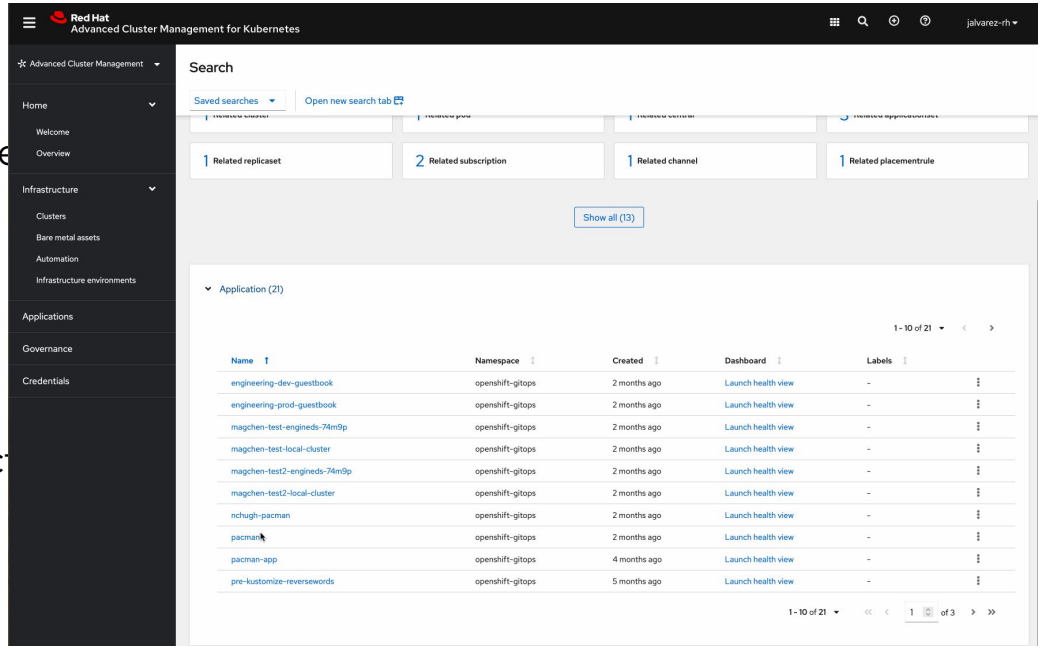
Multi-cluster Lifecycle Management

Dynamic Search

IT Operations

DevOps/SRE

- Troubleshooting across clusters via relationships
- See all **unhealthy** pods
- See related application models to those pods
- See related Persistent Volumes
- See related secrets
- See related ***any*** kube resource object category



Red Hat

Multi-cluster Observability

 IT Operations	Resource Utilization across all my Clusters. A Central place to manage alerts. Insights into key metrics.
 DevOps/SRE	App teams want to onboard to k8s, where should I place the workload. I want to create dashboards in grafana for identifying trends and anomalies in my environment. What's my SLI/SLO

Multi-cluster Observability

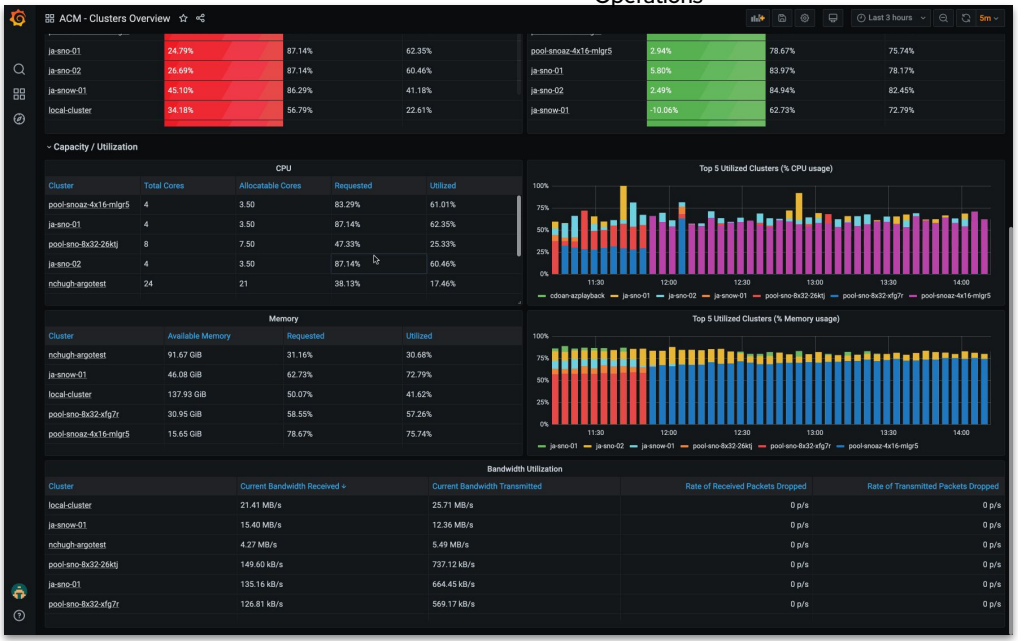
Overview

IT Operations

DevOps/SRE

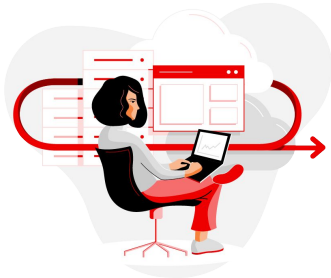
- Enhanced Multi-cluster **OpenShift and non-OpenShift** metric aggregation with customized allowlist
  - Enhanced multi-cluster metric aggregation
  - Custom metrics and pre defined metrics

- **Customize** your own Grafana dashboards for fleet management
  - Optimized set of metrics collected from managed clusters
  - Focused on Cluster Management
  - Unlimited Data Retention
  - Set Alert patterns



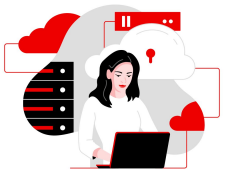
Red Hat

Policy based Governance, Risk and Compliance

 Security OPS	• How do I ensure all my clusters are compliant with standard and custom policies? • How do I set consistent security policies across diverse environments and ensure enforcement? • How do I get alerted on any configuration drift and remediate it?
 IT Operations	• How do I ensure 99.9 % Uptime? • How do I drive more innovation at scale?

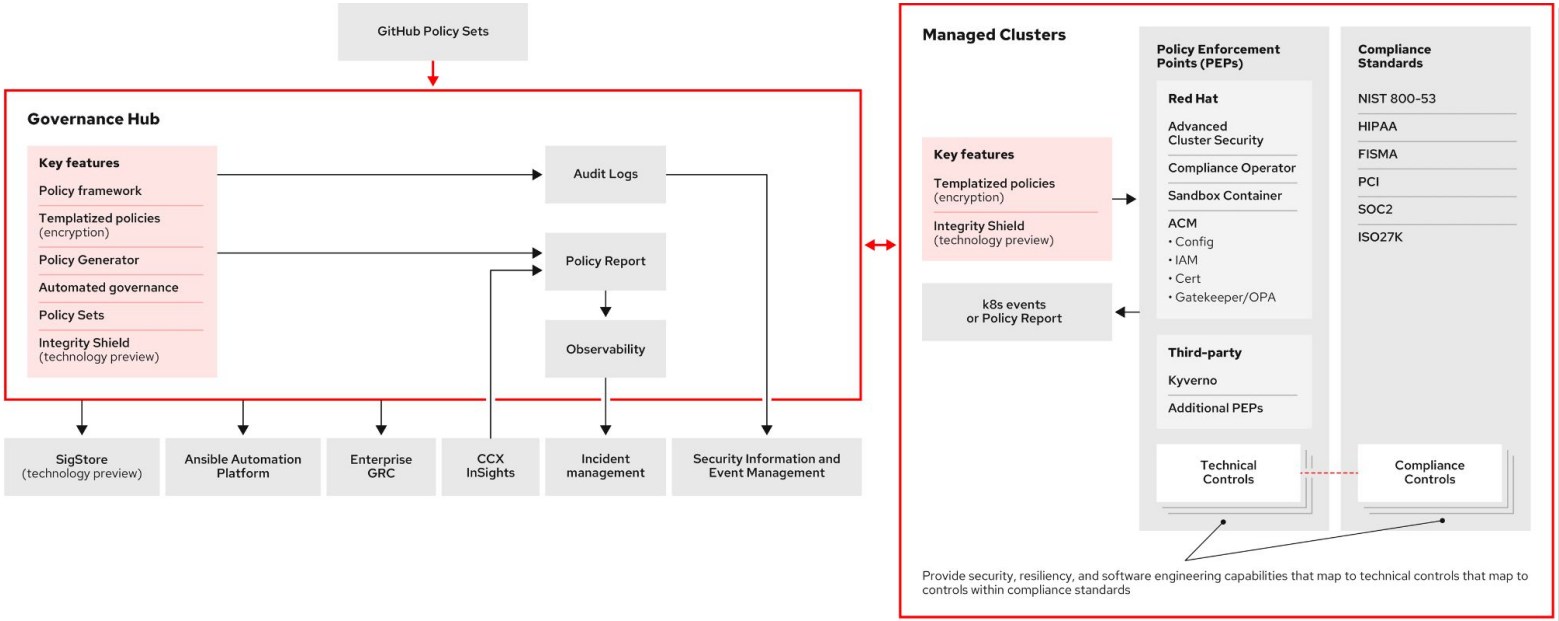
Policy based Governance, Risk and Compliance

Overview



Managed Cluster and GRC Controllers

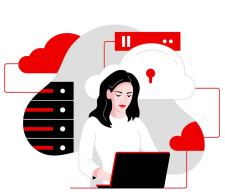
- Driven by Kubernetes CRDs and controllers
- Governance capability for managed clusters covering both security and configuration aspects.
- Out of box policies in GitHub and an extensible policy framework
- Community based policies in GitHub



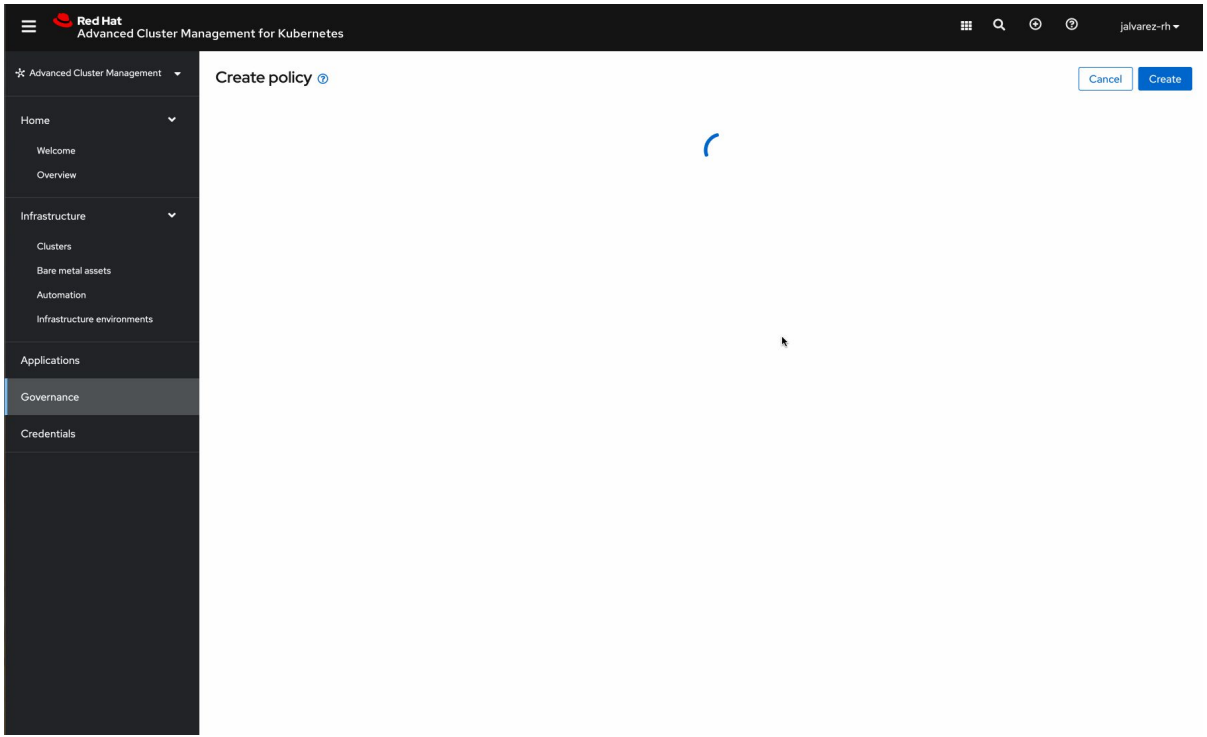
Red Hat

Policy based Governance, Risk and Compliance

Don’t wait for your security team to tap you on the shoulder

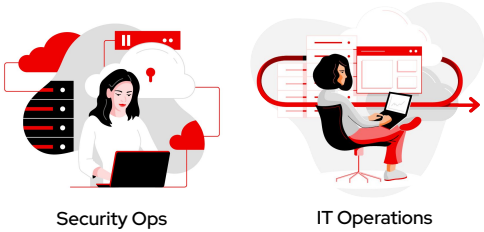


- Set and enforce policies for security, applications, & infrastructure
- Deep visibility for auditing configuration of apps and clusters
- Unique policy capabilities around compliance
- Categorize violations based on your standards for immediate visibility into your compliance posture
- Integrate with OPA / Gatekeeper & Compliance Operator
- Integrate with Ansible Automation Platform at the Policy Level

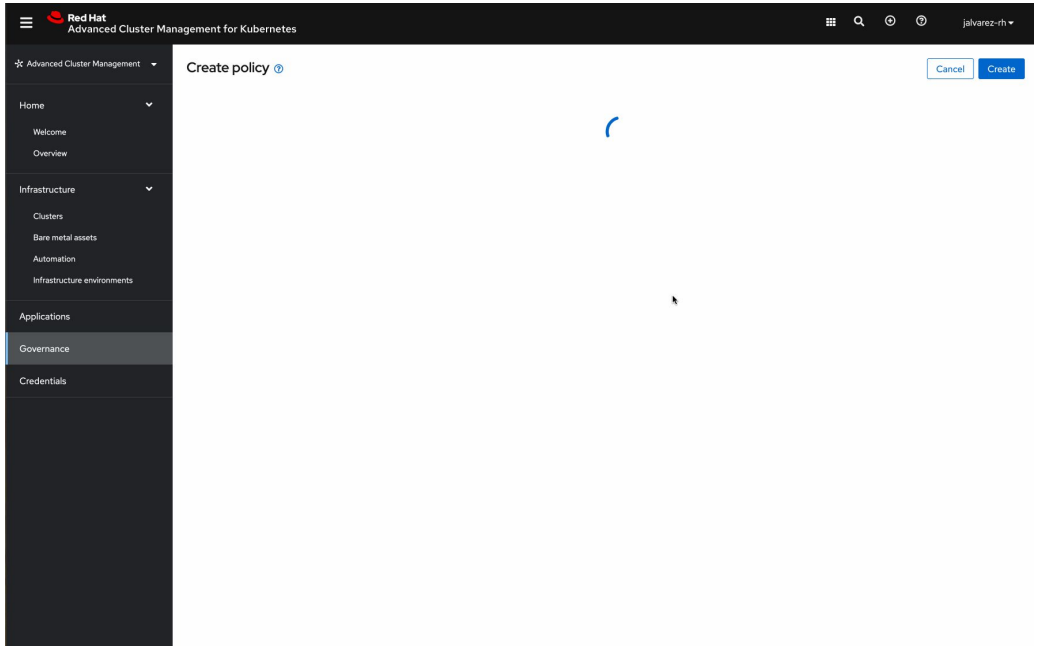


Policy based Governance, Risk and Compliance

Don’t wait for your security team to tap you on the shoulder



- Standard Policies out of the box
  - FISMA
  - HIPAA
  - NIST
  - PCI
- Leverage Different Categories to Represent more standards (if Needed)
- Use Labels to enforce policies against clusters
- Use **inform** to view policy violations
- Use **enforce** to view violations and automatically remediate



Red Hat

Advanced Application Lifecycle Management

 **DevOps/SRE**	• I want to quickly investigate application relationships with real time status, so that I can see where problems are. • With the Application Topology view, I can visually inspect application status labels and pod logs to understand if a part of the application is running or not, without having to connect to a cluster and gather any info.
 **IT Operations**	• I want new clusters to be deployed with a set of known configurations and required applications. • With the assignment of a label at cluster deploy time, the necessary configurations and applications will be automatically deployed and running without any additional manual effort.

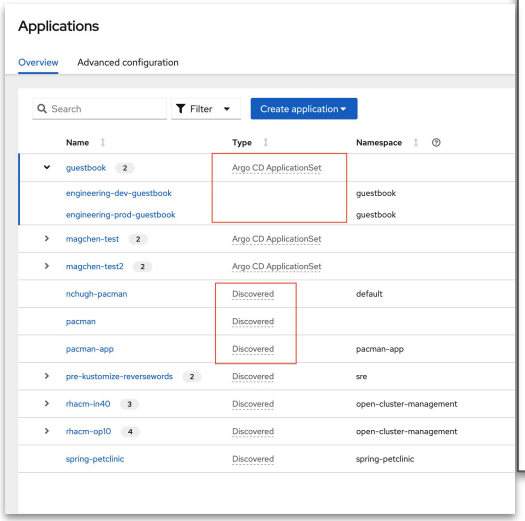
Advanced Application Lifecycle Management

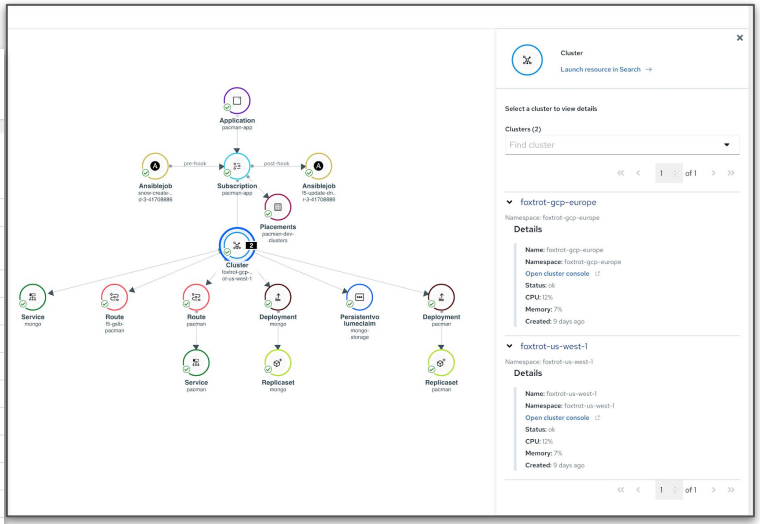
Simplify your Application Lifecycle

IT Operations

DevOps/SRE

- **Deploy** applications at scale
- Deploy applications from **multiple sources** (GitOps/Helm/OjectStorage)
- Quickly visualize application relationships
- Integrate with the Red Hat Ansible Automation Platform
- Visualize Argo CD Applications in RHACM (Local and Remote)
- Support for **ApplicationSets** (ArgoCD)

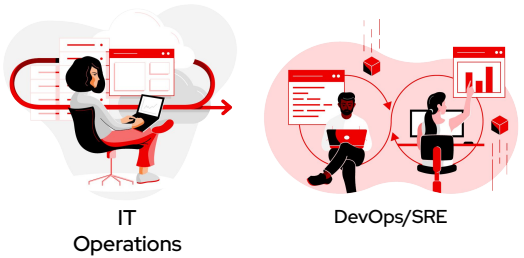




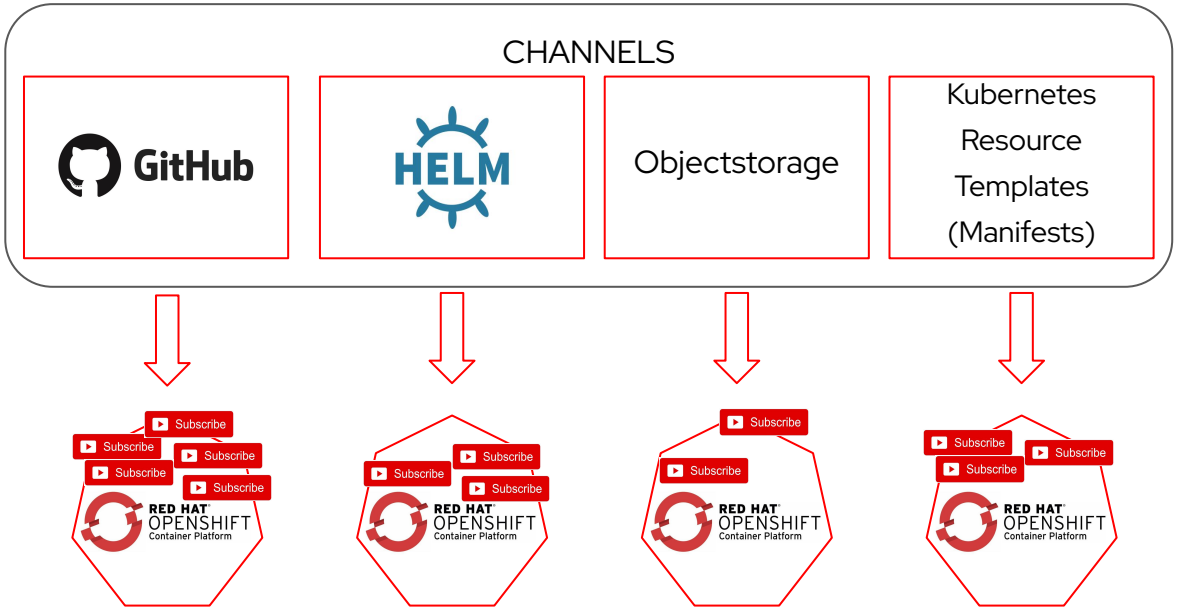
Red Hat

Advanced Application Lifecycle Management

Subscriptions bring enterprise to Kubernetes



- Extending the best of Enterprise into a desired state methodology
- Time Windows: New releases during your maintenance windows
- Orchestrate actions with the integration of Ansible Automation Platform



Red Hat

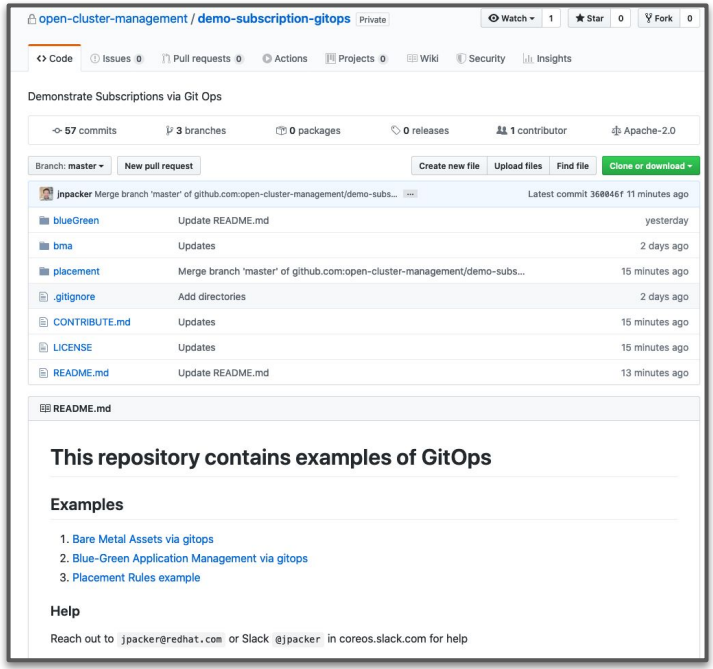
Advanced Application Lifecycle Management

GitOps - Git as source of truth

IT Operations

DevOps/SRE

- **Create, modify & delete**, just as you would any source code. Git becomes your source of truth controlling your data center.
- Have a record of **who, what & when** for every change precipitated in your environments
- Through code Reviews & Approvals, take full control of all changes to your data center(s)
- Restore your environment, via the Git commit history (system of record)



https://github.com/open-cluster-management/demo-subscription-gitops

Red Hat

Resources and next steps

Resources

External Resources

Webpage

YouTube Playlist

Datasheet

Twitch Playlist

Infographic

External FAQ

Ebook: Managing your Kubernetes clusters for Dummies'

Checklist: 5 considerations for managing your Kubernetes clusters

IDC paper: Digital business success depends on effective multicluster Kubernetes management

Questions

Thank You


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat