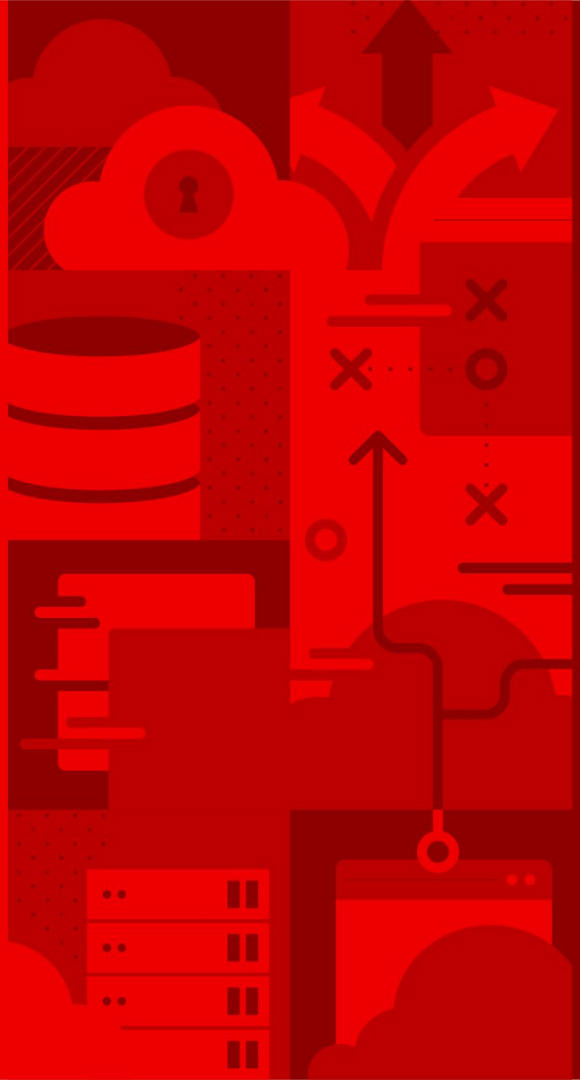
Red Hat
Advanced Cluster Management
for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes

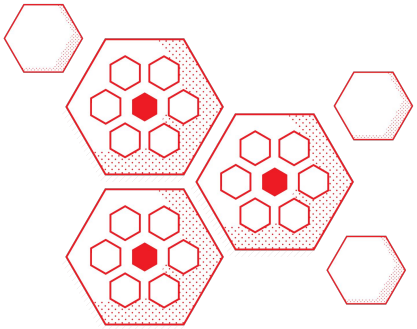
Introduction

Alfred Bach
Red Hat



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

Hybrid multi cloud 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*

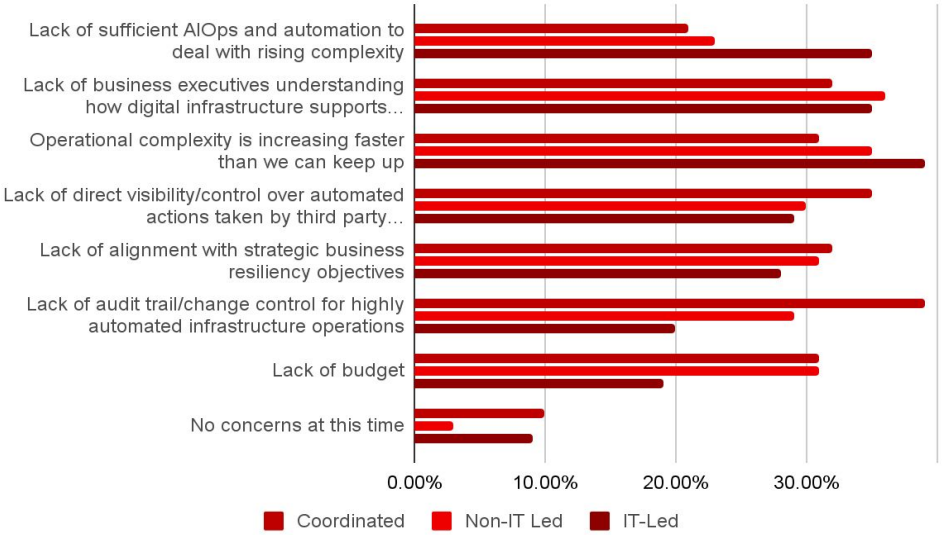
Using multiple public clouds and one or more private/dedicated clouds*

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

Digital infrastructure concerns are around automation

Smaller, IT-Led organizations are concerned about lack of automation and AIOps while larger, more collaborative organizations are more concerned about lack of change control and limited business executive understanding of how digital infrastructure supports business resiliency

What are the greatest concerns regarding organizations' overall digital infrastructure strategy being able to fully support business resiliency plans?



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

Remote container clusters are becoming modern-day LAN servers

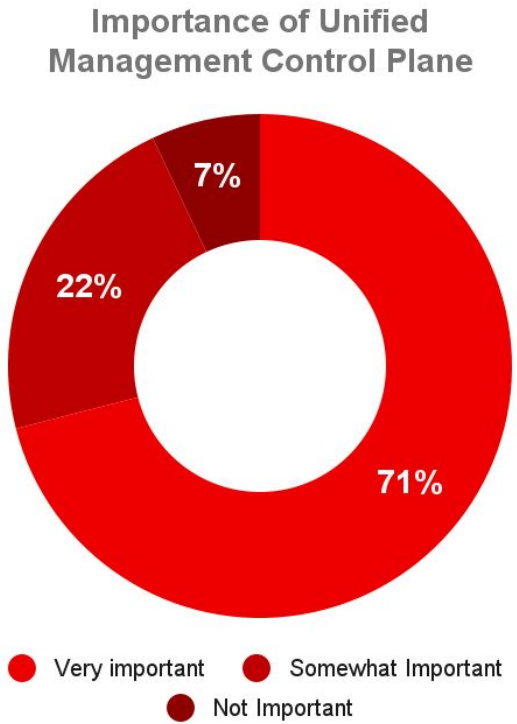
In many ways, remote container clusters are becoming modern-day LAN servers, which requires tooling for managing the distributed clusters.

Software and service providers are differentiating their offerings by providing more complete solutions, adding capabilities such as

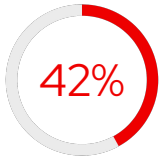
- **Distributed management of multiple clusters**
- **Application lifecycle integration**
- **Policy management**
- **Monitoring and security to the foundational container orchestration capabilities**

Source:
Market Guide for Container Management, Gartner, 2021.

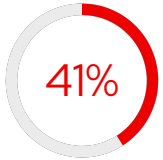
Unified, consistent, autonomous operations priorities



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



Improve data integration and data protection



Optimize infrastructure costs and usage

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

Where’s the growth in cluster deployments?

Small Scale Dev Teams

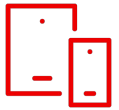
- Managing and syncing across Dev/QE/Pre-Prod/Prod clusters can be difficult

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

Reasons for deploying clusters

Application availability

Reduced latency

Address industry standards

Geopolitical data residency guidelines

Disaster recovery

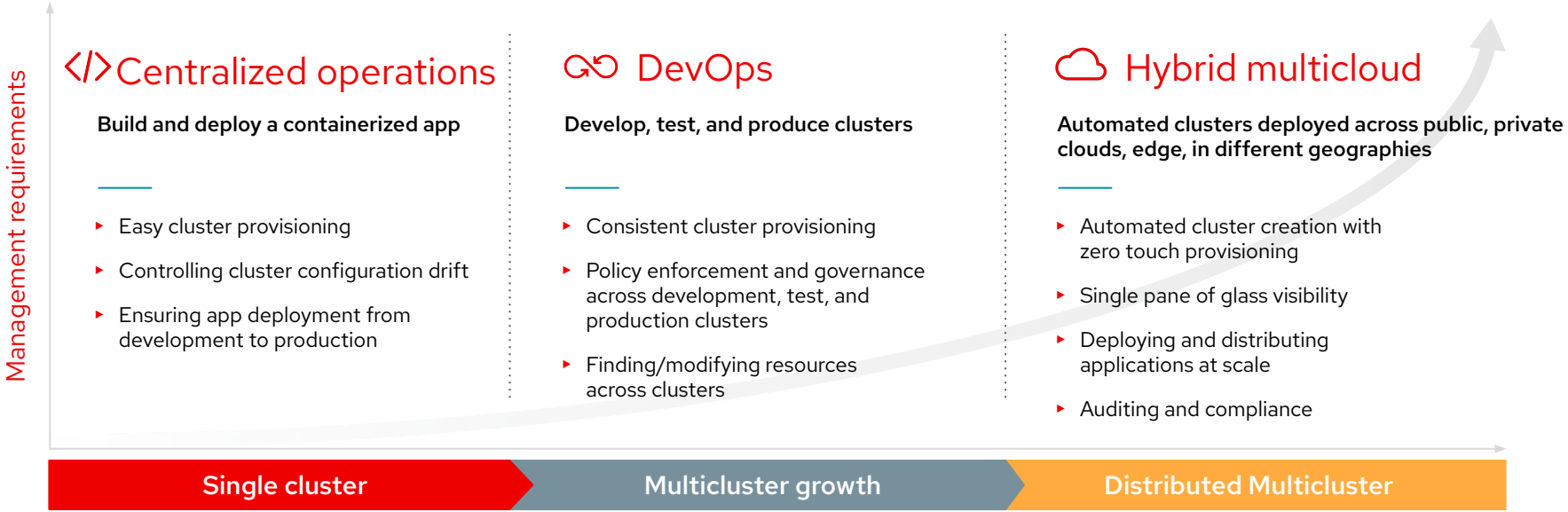
Edge deployments

CapEx cost reduction

Avoid vendor lock-in

Multicluster management challenges

How do I normalize and centralize key functions across environments?



Red Hat

Solving real customer challenges

DISCOVER

Enforced policies at scale across clusters using the governance and risk framework in RHACM

Automated deployment and ease of managing clusters and applications at scale

verizon

Seamless management and operations of the complete Kubernetes environment

vodafone Ziggo

End-to-end multi-cloud management, visibility, and compliance enforcement for multiple clusters at scale

ORANGELIFE

Transformed several applications to become cloud-native and prepared for a full migration to cloud

Telefónica

Increased observability and control for managing the Kubernetes environment

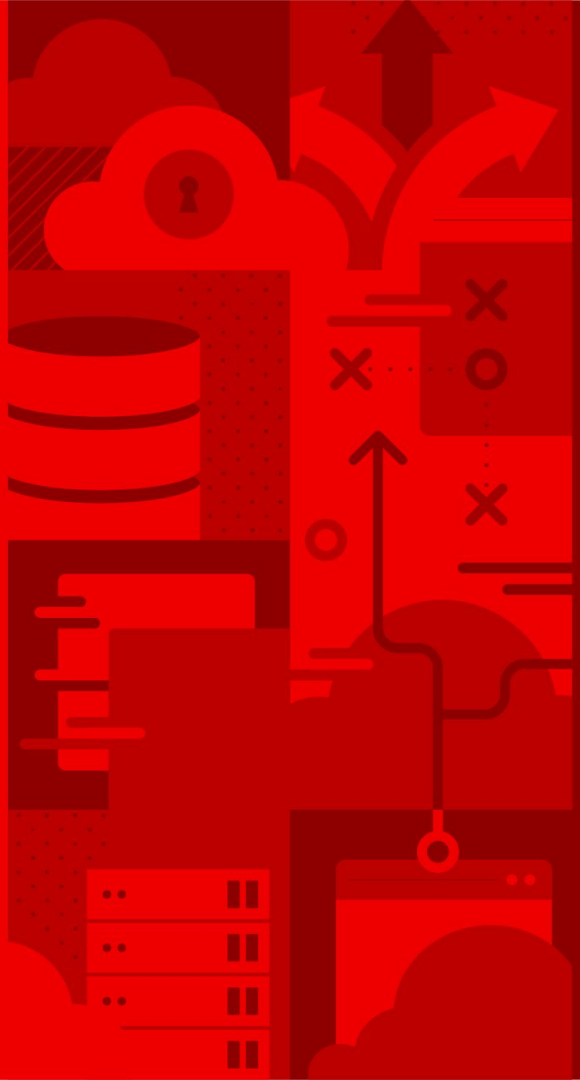
Our open hybrid cloud portfolio accelerates digital transformation

Red Hat Advanced Cluster Management for Kubernetes enables enterprises to build highly agile, scalable architectures with enhanced cluster security that can be deployed at any location.

Red Hat aims to scale automation across enterprise through a three-pronged strategy comprising: business-critical workload automation, Red Hat Ansible Automation for infrastructure and Red Hat Advanced Cluster Manager for container management.

- **Innovative container management**
- **Deeper integration with Red Hat Ansible Automation Platform for container automation**

Source:
Red Hat's Open Hybrid Cloud Portfolio Can Accelerate Digital Transformation, Gartner, May, 2021.



Introducing Red Hat Advanced Cluster Management

Red Hat

Red Hat Advanced Cluster Management for Kubernetes

Simplified operation and maintenance

View, manage, operate and solve issues across your kubernetes fleet through a **single console**.

Runs on OpenShift

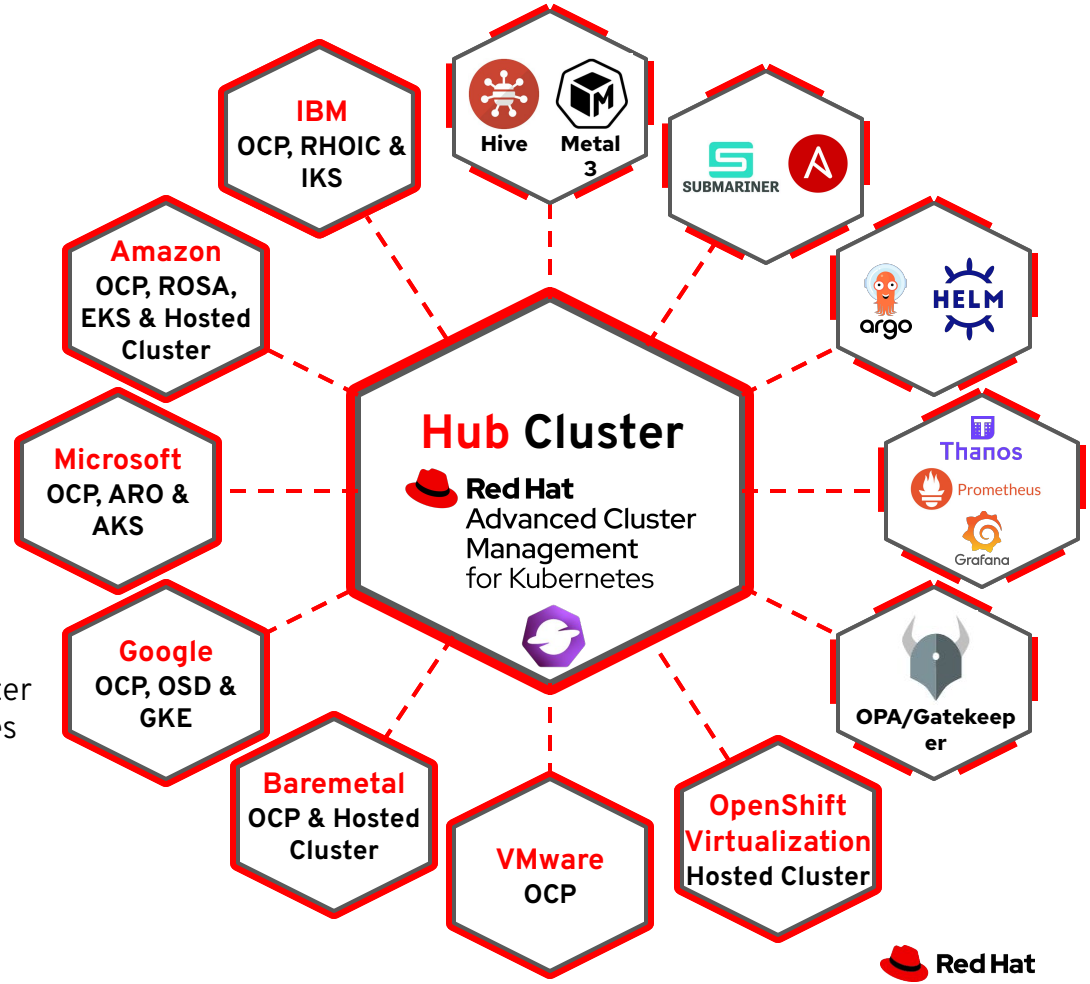
Like any other Kubernetes app, **easily run** and manage it on top of an OpenShift cluster.

Hub-Spoke architecture

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

Tight Integration

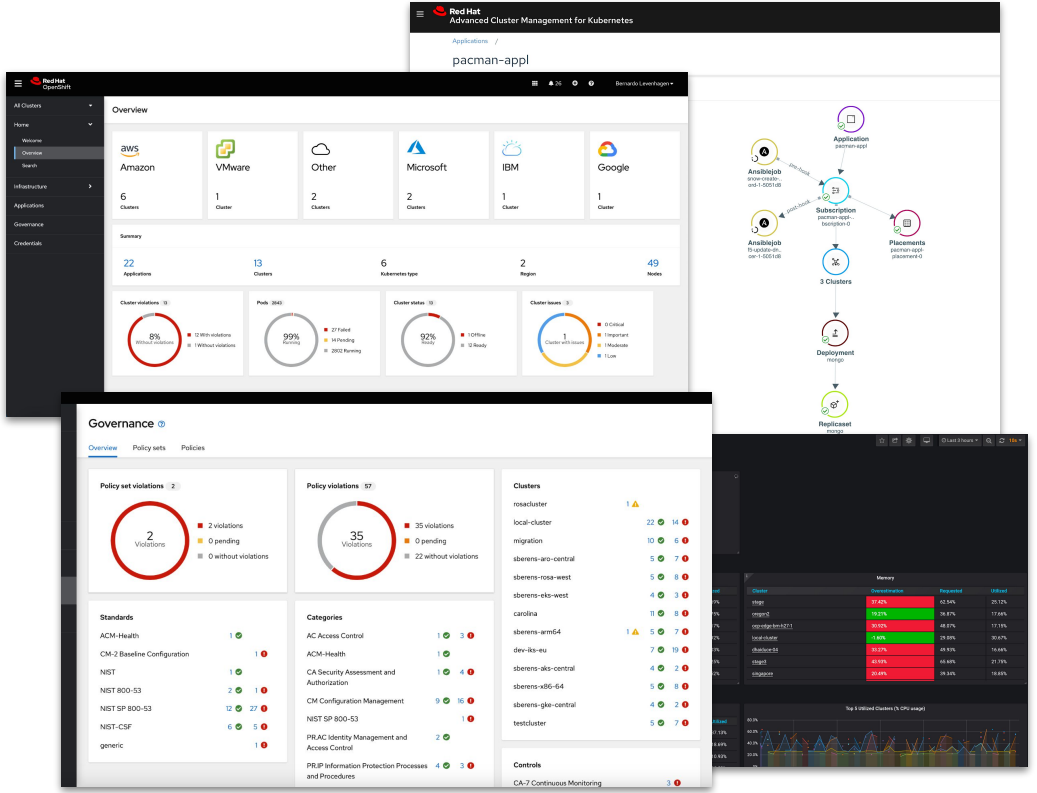
RHACM comes with a rich API, add-ons and it can **integrate** with some other key enterprise solutions and open source tools.



Robust & Proven

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

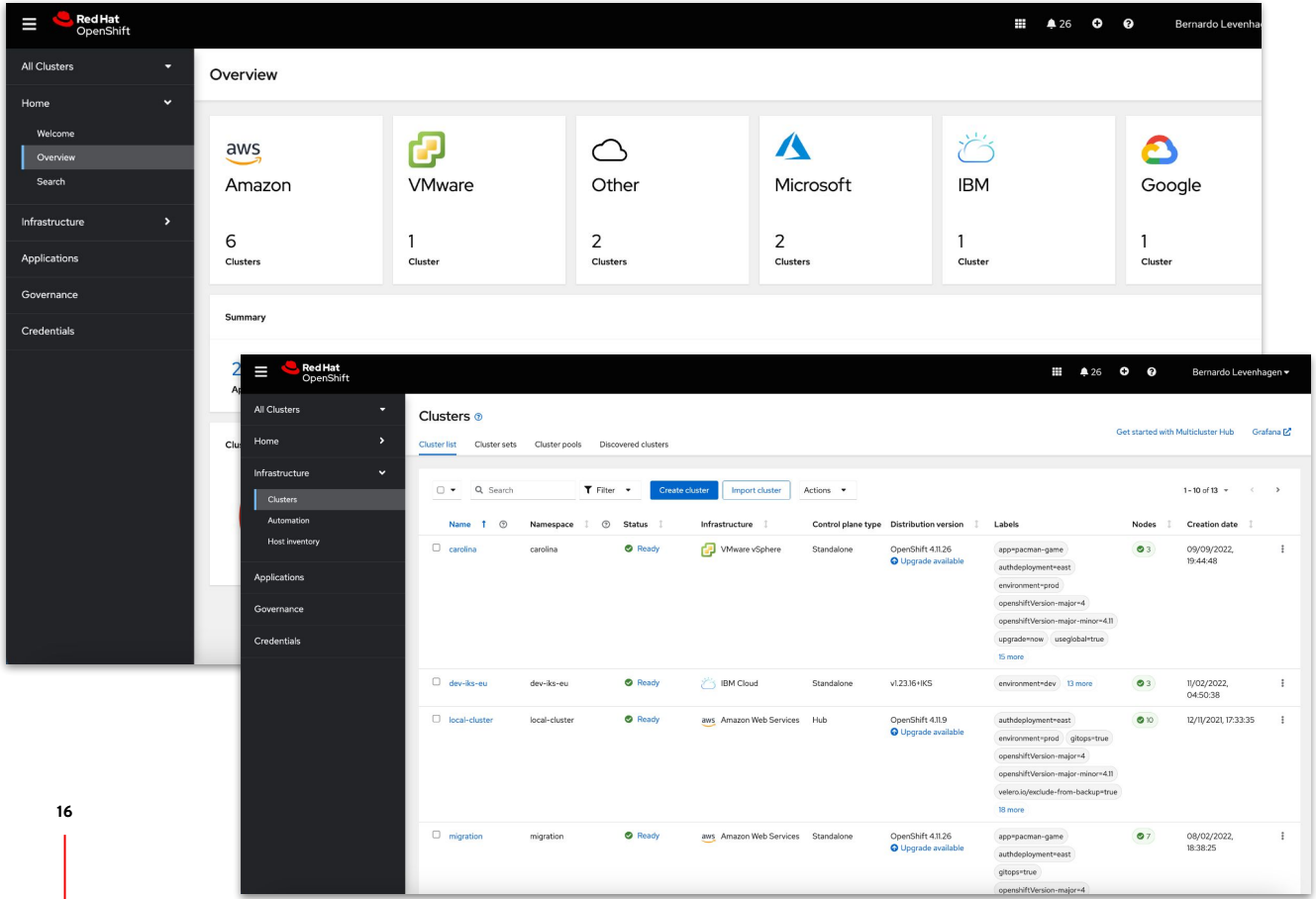
- Multicluster lifecycle management
- Policy driven governance, risk, and compliance
- Advanced application lifecycle management
- Multicluster Observability and Search for health and optimization
- Multicluster networking for interconnecting apps



Red Hat

Unified Multi Cluster Management

Single Management for all your Kubernetes Clusters

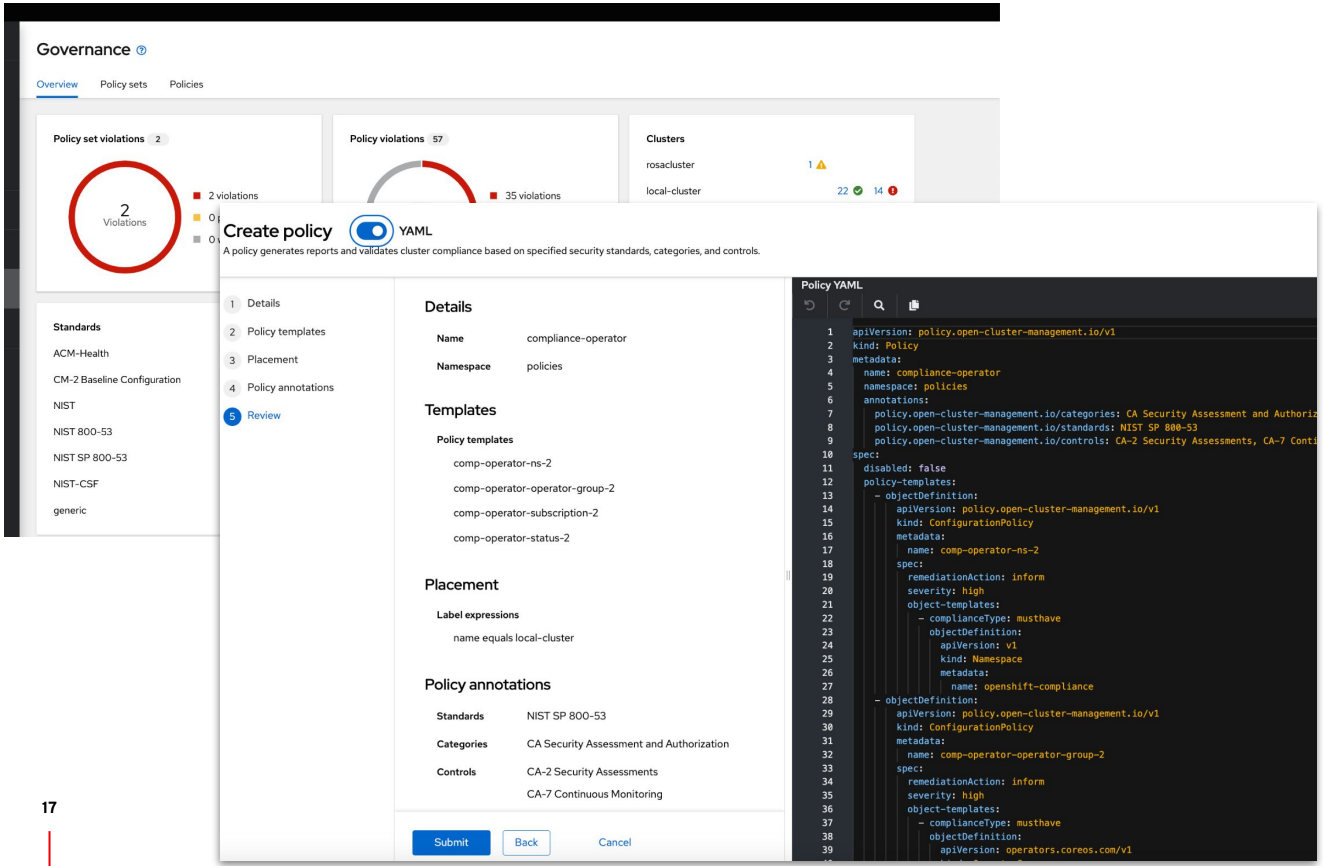


- **Centrally** create, update and delete Kubernetes clusters **across multiple** private and public clouds
- **Hibernate / resume** OCP Clusters across your domain
- **Configure ClusterSets & Cluster Pools** for simplified OCP cluster management
- Search, find and modify **any** kubernetes resource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

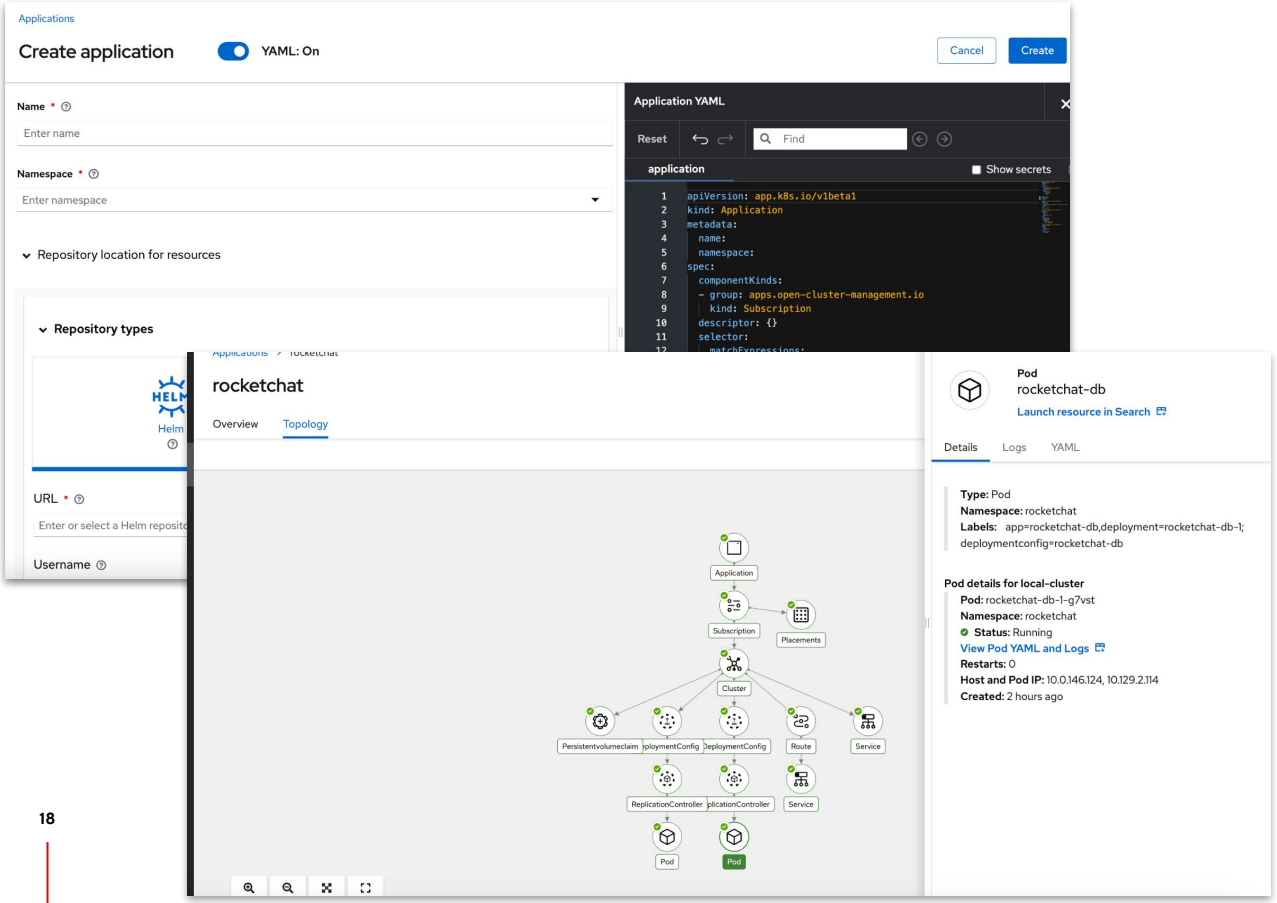


- **Centrally** set & enforce policies for security, applications, & infrastructure
- Quickly **visualize** detailed **auditing** on configuration of apps and clusters
- Perform remediation actions by leveraging **Ansible Automation Platform** integration.
- Built-in **compliance policies** and audit 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



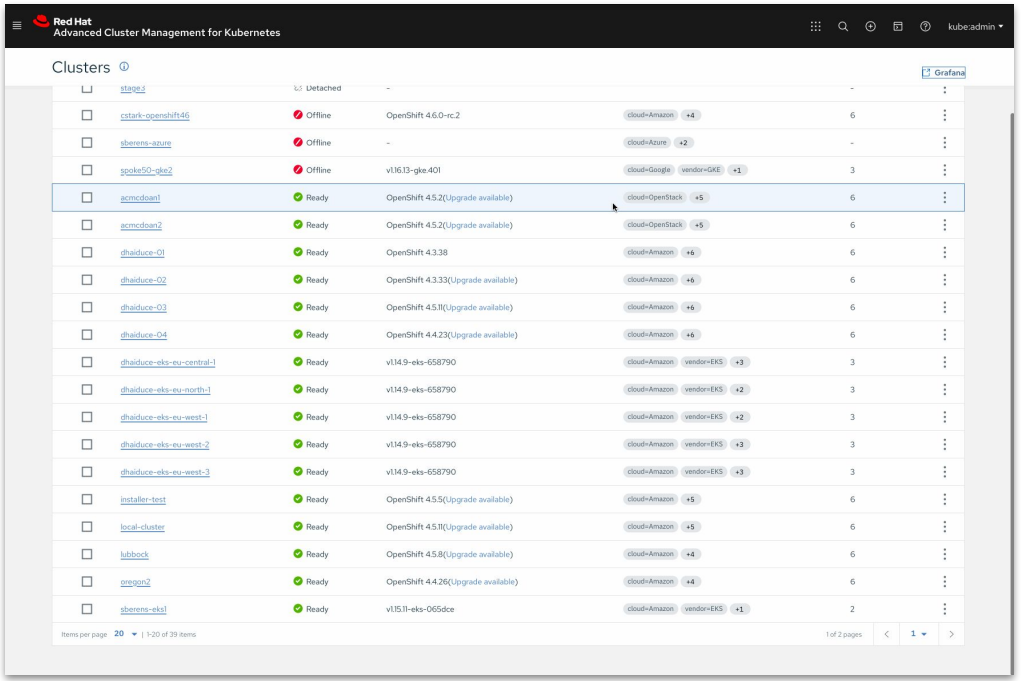
- **Easily** deploy an Application using the **Application Builder** (Subscription)
- Deploy applications from **multiple** Sources (Git/Helm/Object Storage)
- Integrate with **OpenShift GitOps** (Argo CD).
- Automatically **detect and visualize Argo CD** Applications in RHACM
- Quickly **visualize** 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
- Long Term **Data Retention**
  - Observe Metric trends
  - Set Alert Patterns
  - Supported Object Storage
    - AWS S3 (and compatible)
    - Ceph for on-premise
    - Google Cloud Storage
    - Azure Storage

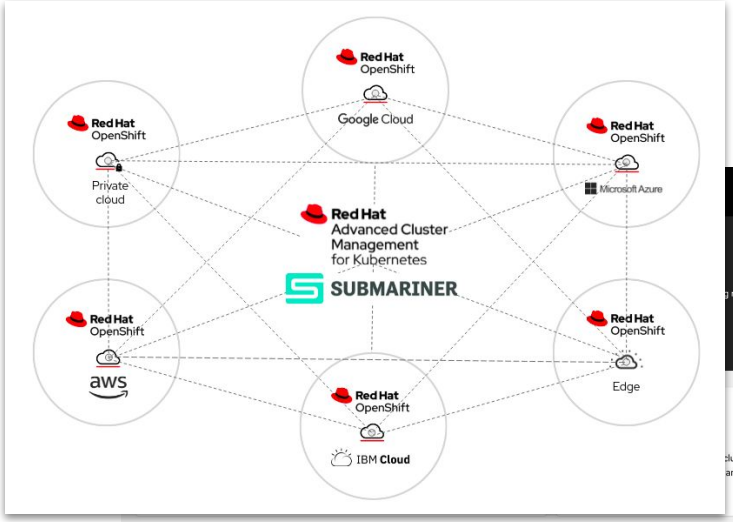


Red Hat

Multicluster Networking

MCN features overview & look ahead

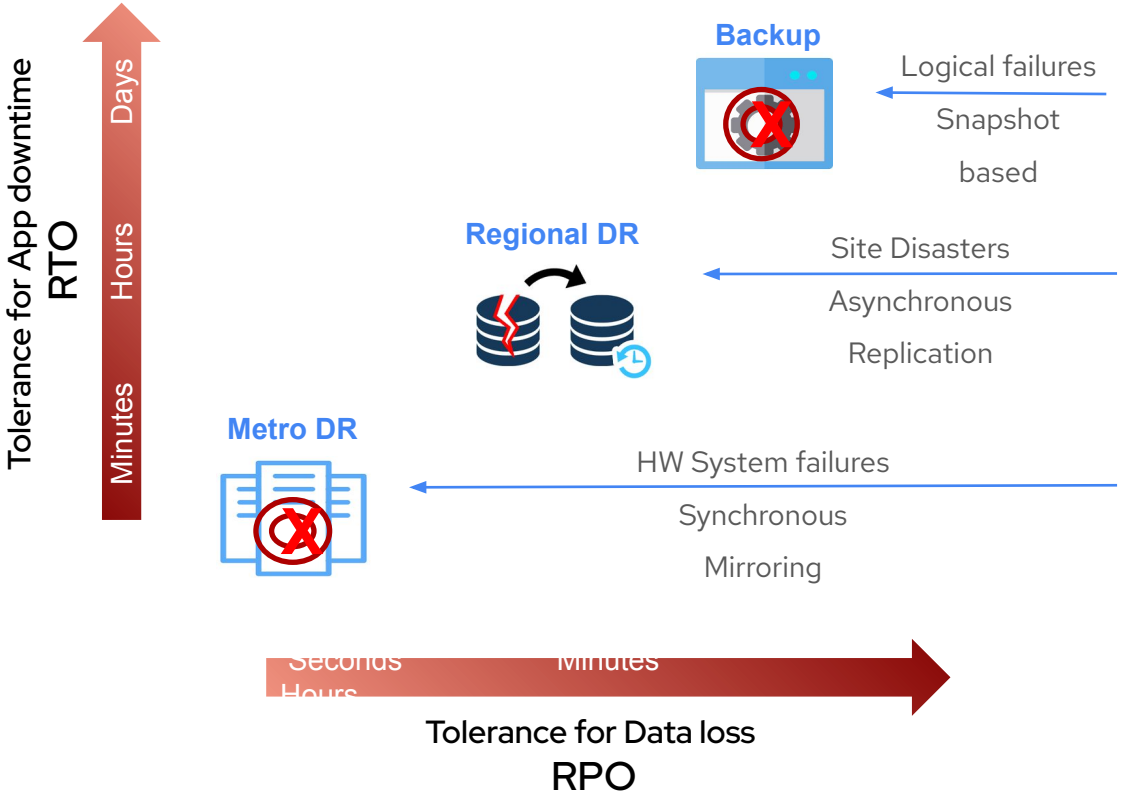
- **ACM MCN, aka 5th pillar**
- Presenting **Submariner**: an CNCF open source project in the form of an **add-on** for RHACM, now generally available
- Enable **direct networking** between Pods in different Kubernetes clusters as well as **Service Discovery**, either on-premises or in the cloud
- Leverage **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...



Red Hat

Ways to achieve **Business Continuity** with RHACM

Comprehensive protection solutions against wide spectrum of failures

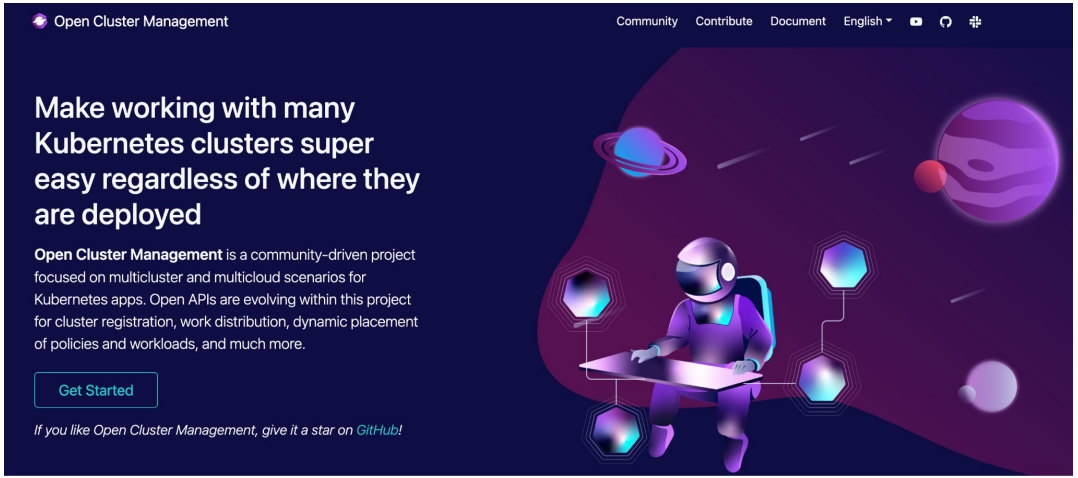


- **OADP**(DataMover) & **Volsync** facilitates time-based copies of application state. Data replication can be applied to different storage types and vendors.
- **ACM** & **ODF** integrated stack offers **Regional-DR.** It ensures continuity during the unavailability accepting some loss of data in a predictable amount. In the public cloud these would be akin to protecting from a region failure.
- **ACM** & **ODF** integrated stack introduces **Metro-DR.** It ensures continuity during the unavailability with no data loss. In the public cloud these would be akin to protecting from an Availability Zone failure.

Red Hat

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



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

Strong open source community & ecosystem

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.

Increase application availability

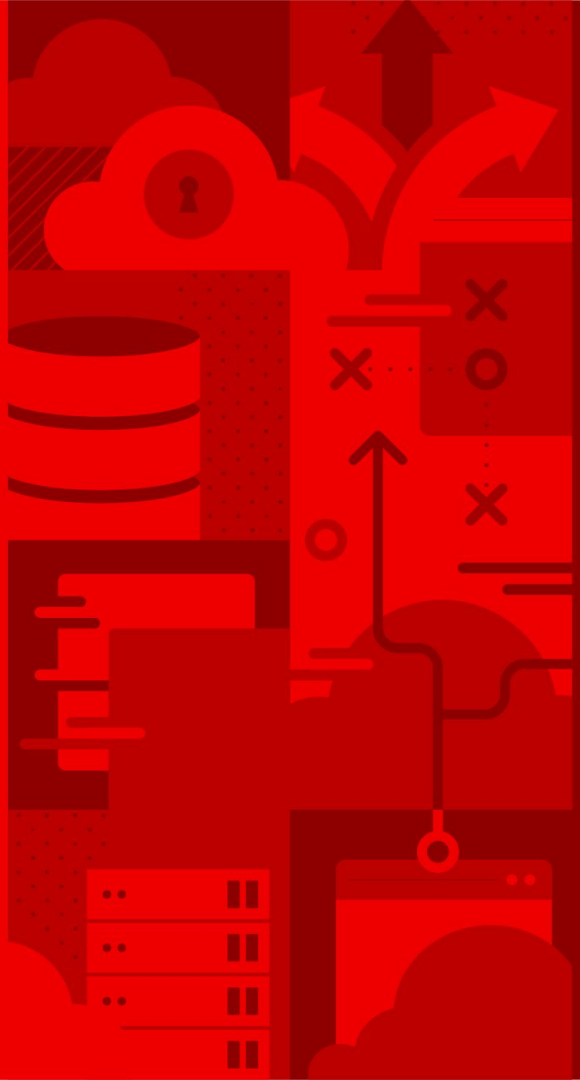
Placement API can allow quick deployment of clusters across distributed locations for availability, capacity, and security reasons.

Reduce costs

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

Ease Compliance

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



Detailed Use Cases

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?

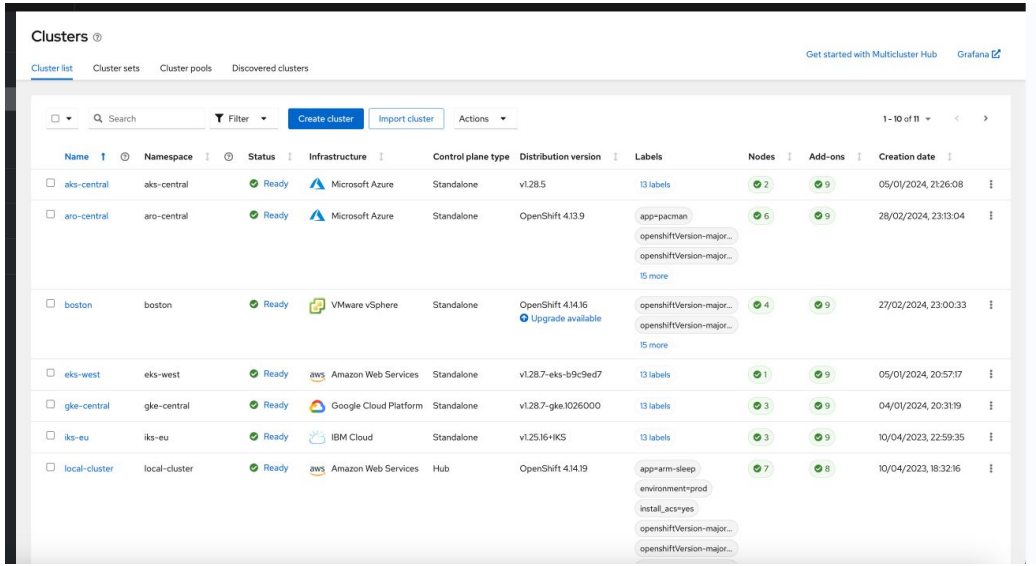
Multi-cluster Lifecycle Management

Overview

IT Operations

DevOps/SRE

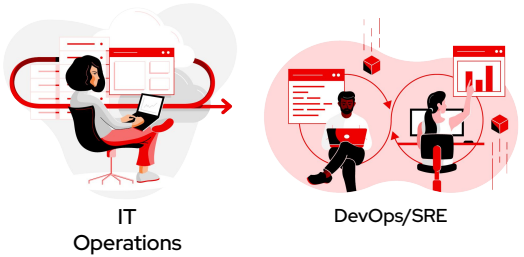
- **Full Management of OpenShift**
  - Provision new OpenShift 4.13.x and above
  - Manage existing **OpenShift 3.11 (Limited Support)**, 4.13.x and above
  - Support for Single Node OpenShift (SNO)
  - Hosted Control Planes
- **Public cloud managed kubernetes**: EKS, AKS, GKE, IKS, ROKS, ROSA, ARO, 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



- **Create**, **Upgrade** and **Destroy** OpenShift clusters running on **vSphere**, **Bare-metal** as well as **Public cloud**.
- Import **OpenShift Clusters** that can be discovered from **OCM** (OpenShift Cluster Manager at https://console.redhat.com/openshift/)
- Leverage Hive API for OpenShift Cluster Deployment
- Wizard or YAML-based create cluster flow
- Launch to an OpenShift 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

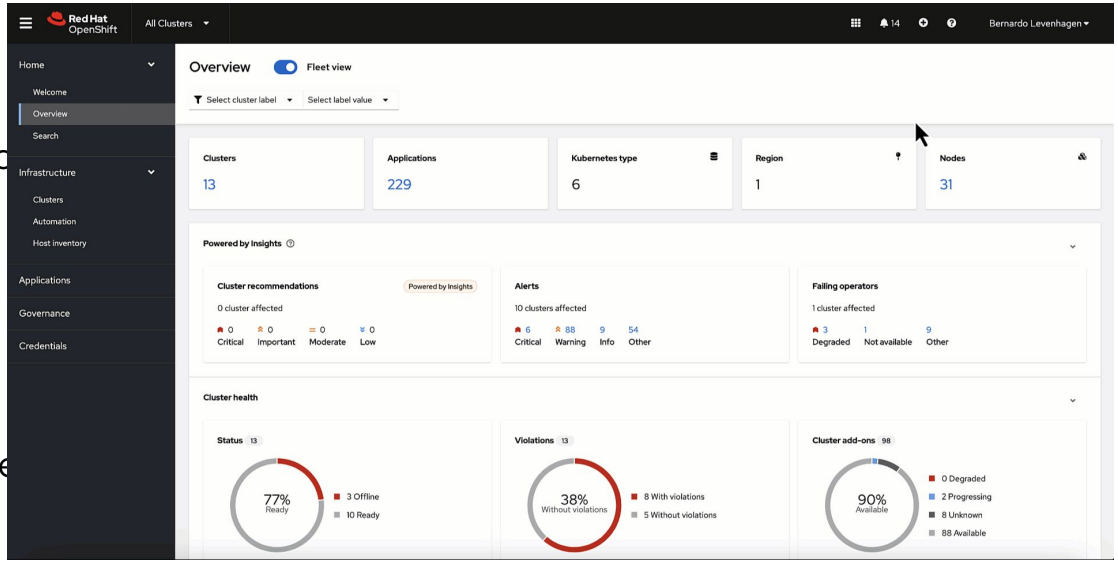
Multi-cluster Lifecycle Management

Dynamic Search

IT Operations

DevOps/SRE

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



Red Hat

Multi-cluster Observability

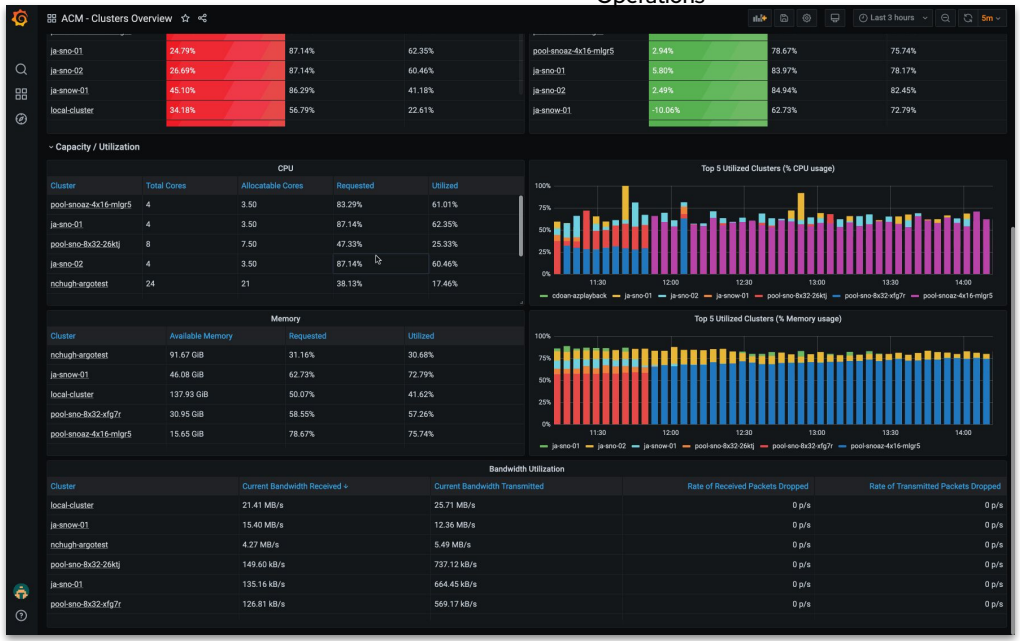
Overview

IT Operations

DevOps/SRE

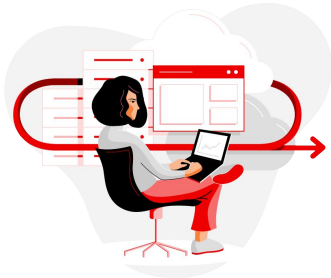
- Enhanced Multi-cluster **OpenShift and non-OpenShift** metric aggregation with customized allowlist
  - Enhanced multi-cluster metric aggregation
  - Custom metrics and pre-defined metrics

- **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



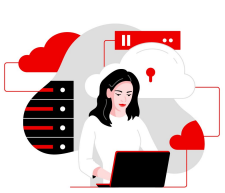
Red Hat

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?

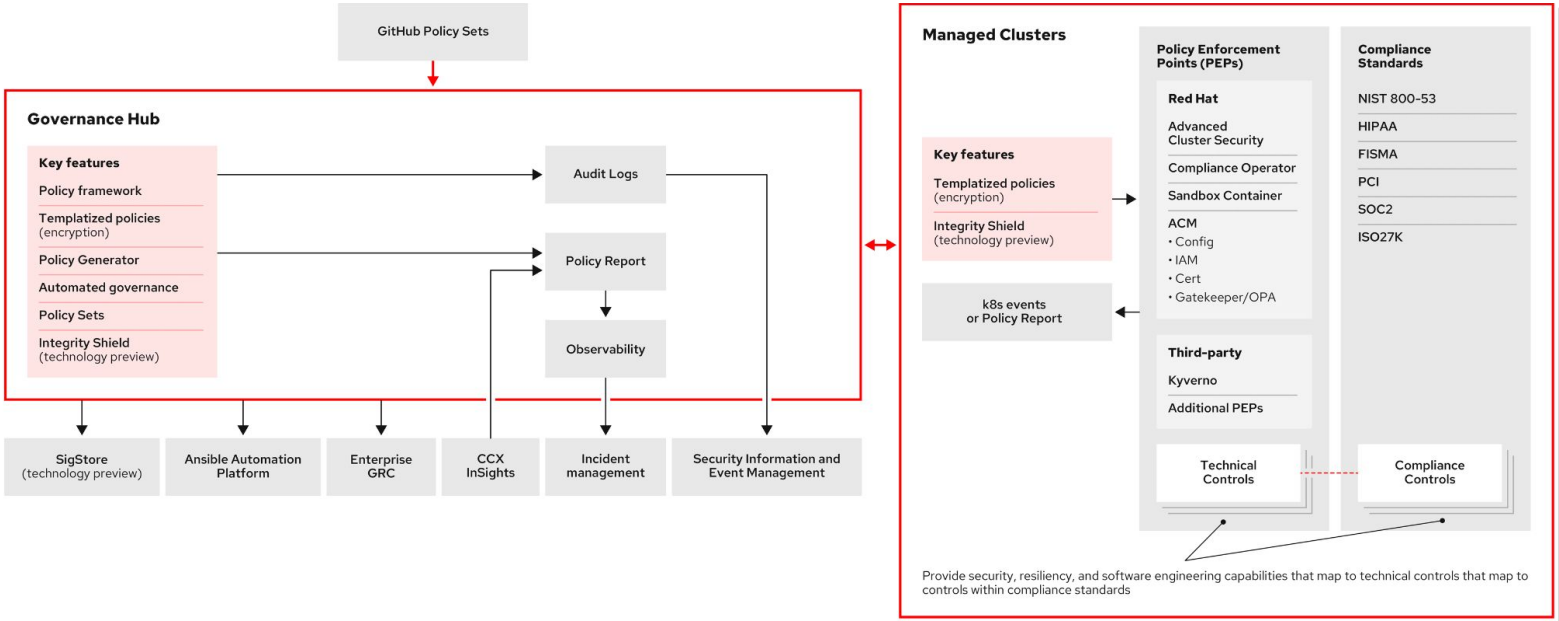
Policy based Governance, Risk and Compliance

Overview



Managed Cluster and GRC Controllers

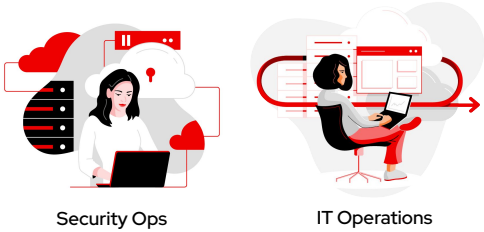
- Driven by Kubernetes CRDs and controllers
- Governance capability for managed clusters covering both security and configuration aspects.
- Out of box policies in GitHub and an extensible policy framework
- Community based policies in GitHub



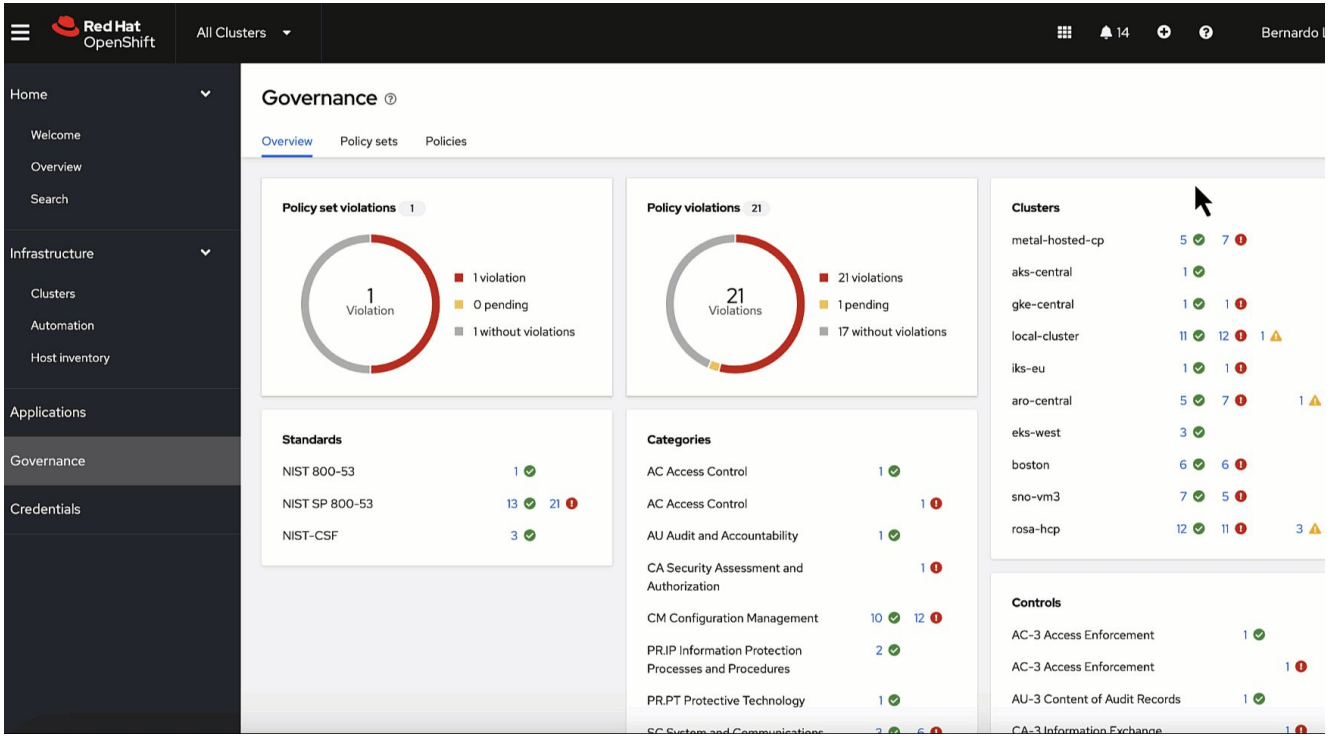
Red Hat

Policy based Governance, Risk and Compliance

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

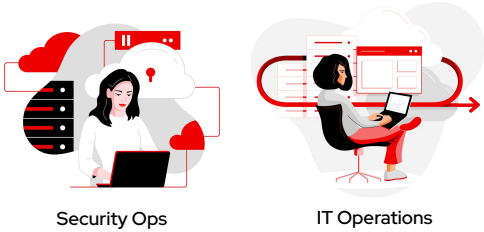


- **Set** and **enforce** policies for security, applications, & infrastructure
- **Deep visibility** for auditing configuration of apps and clusters
- **Custom view** for policies
- Categorize violations based on your standards for immediate visibility into your compliance posture
- Integrate with **OPA/Gatekeeper** & **Compliance Operator**
- Leverage **PolicySets** for a grouping policies with a single purpose

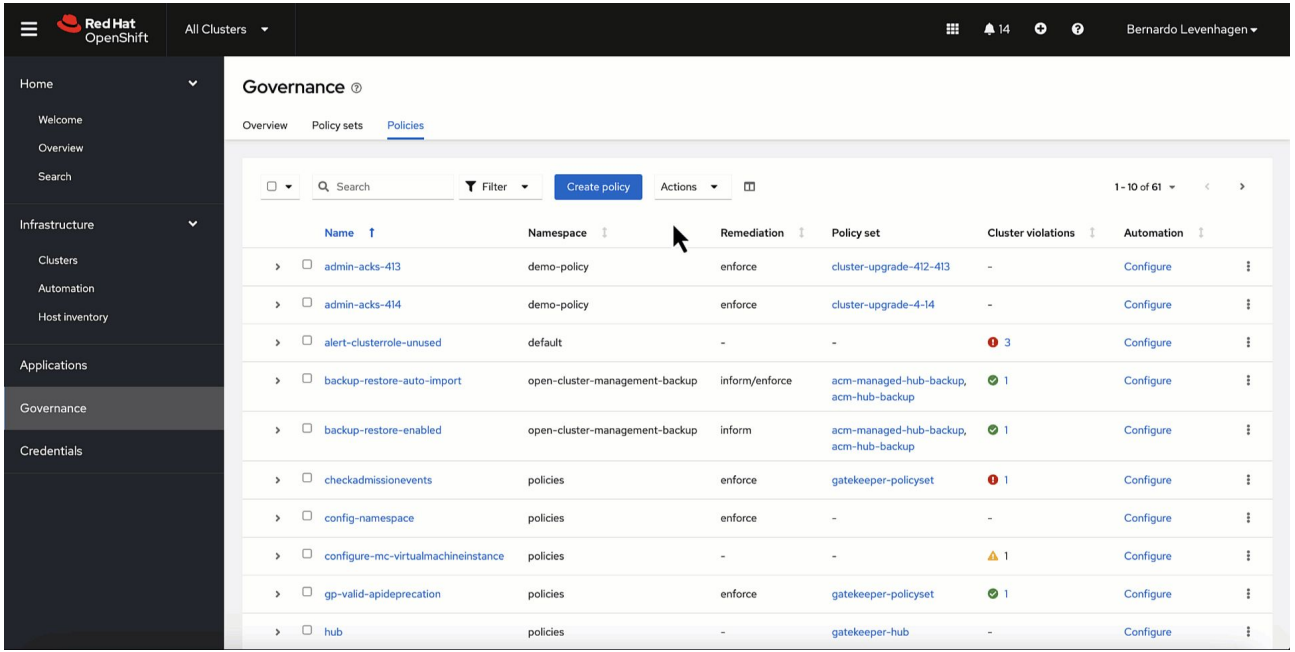


Policy based Governance, Risk and Compliance

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



- Unique, standardized policy capabilities around **compliance**
  - FISMA
  - HIPAA
  - NIST
  - PCI
- Integrate with **Ansible Automation Platform** at the Policy Level
- 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.

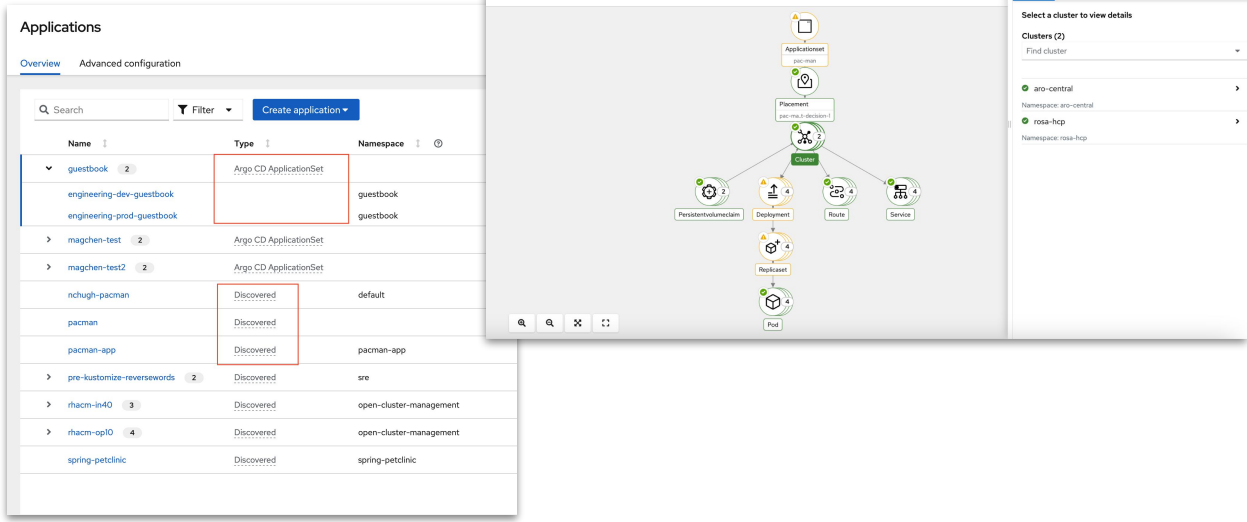
Advanced Application Lifecycle Management

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

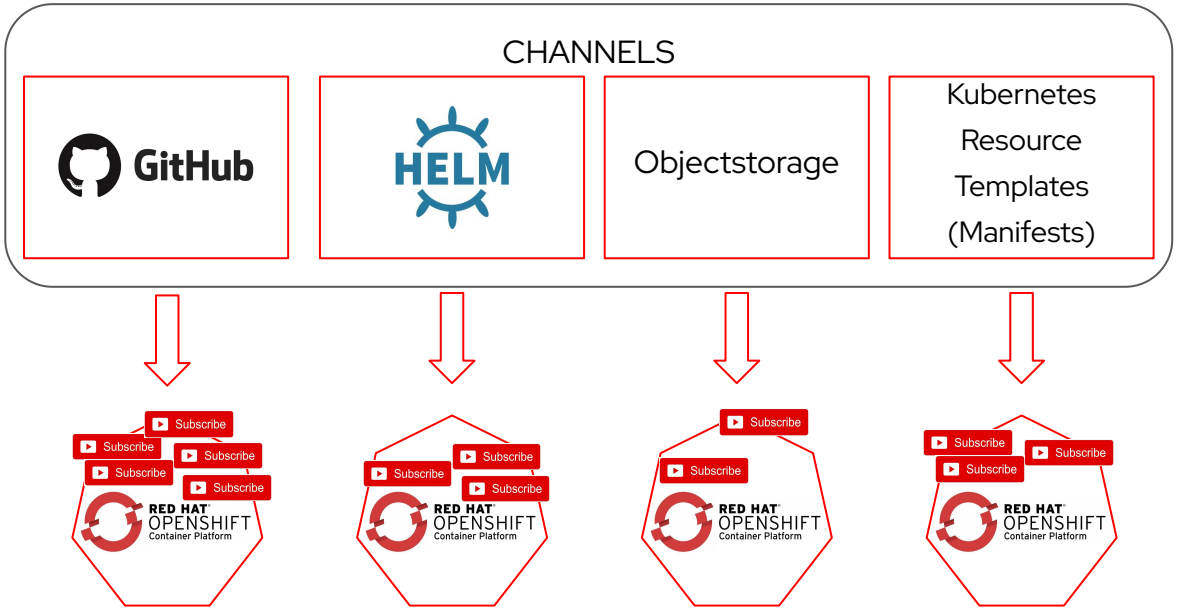
Advanced Application Lifecycle Management

Subscriptions bring enterprise to Kubernetes

IT Operations

DevOps/SRE

- 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

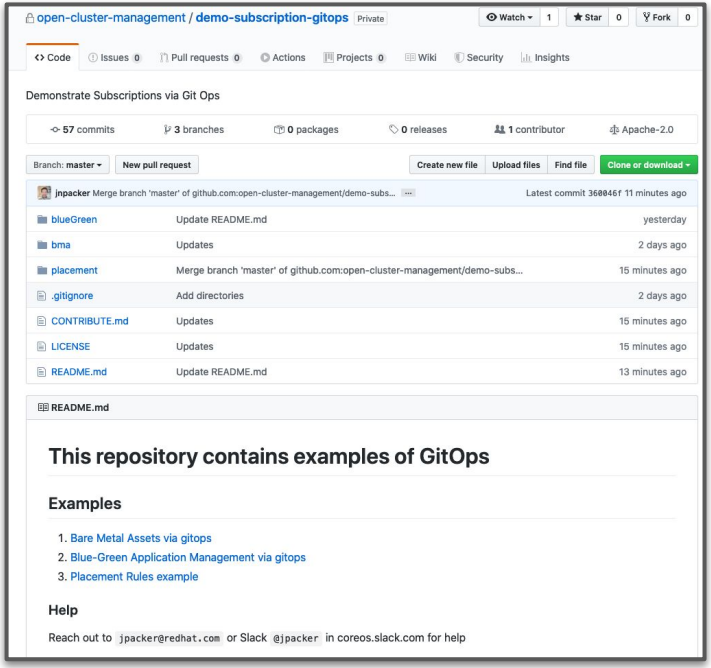
Advanced Application Lifecycle Management

GitOps - Git as source of truth

IT Operations

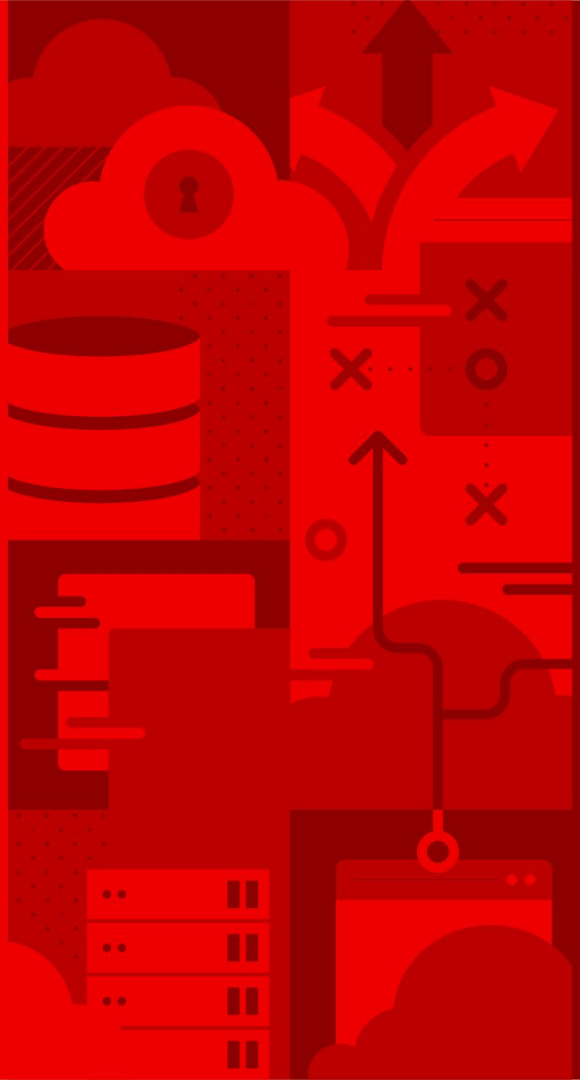
DevOps/SRE

- **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

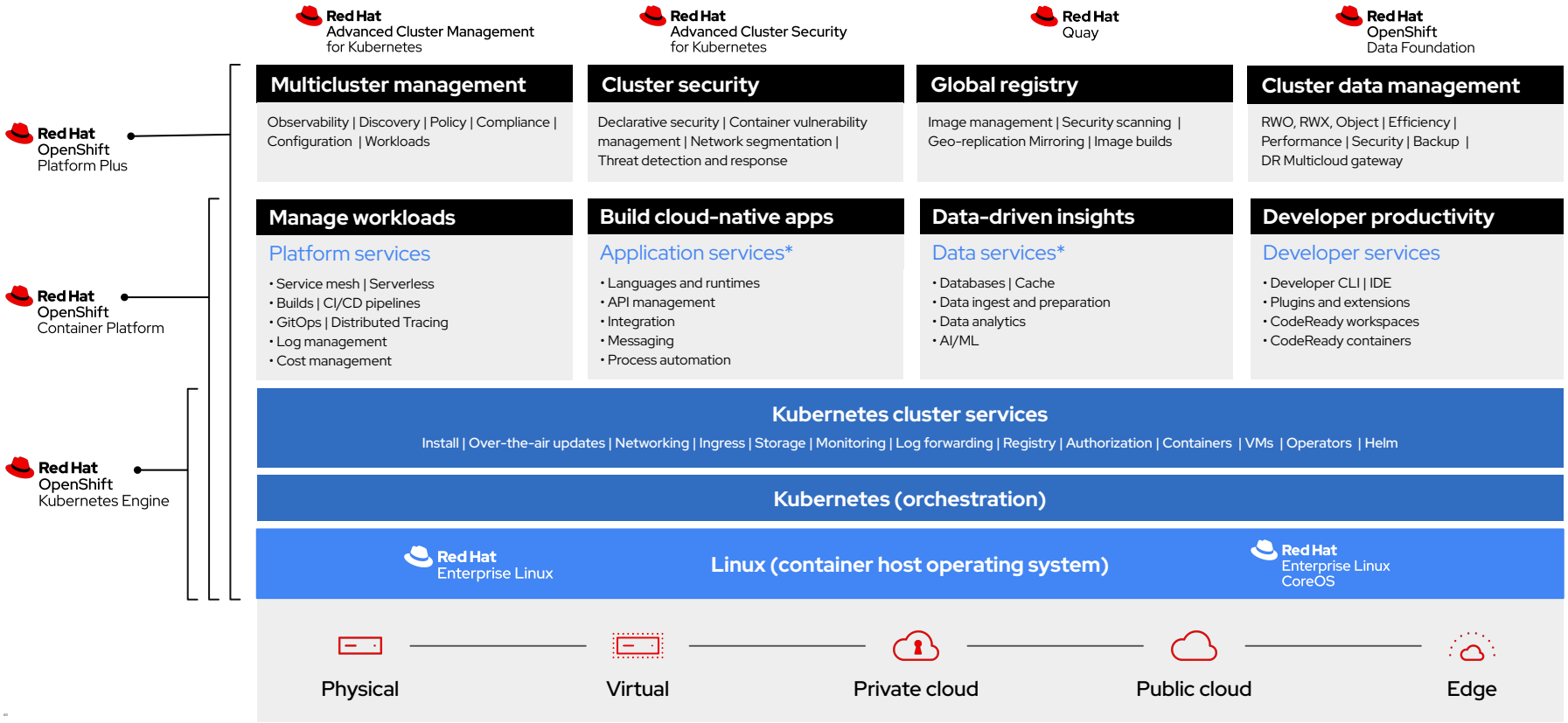
Red Hat



How ACM works with OpenShift

Red Hat

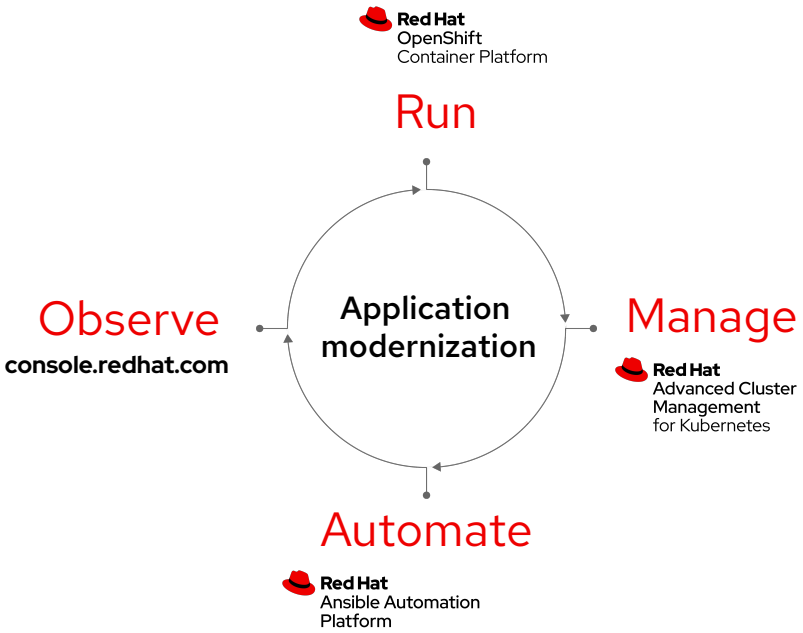
Bigger Picture: Red Hat Open Hybrid Cloud Platform



* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application Services and Red Hat Data Services portfolios.
** Disaster recovery, volume and multicloud encryption, key management service, and support for multiple clusters and off-cluster workloads requires OpenShift Data Foundation Advanced

Red Hat

Supporting application modernization



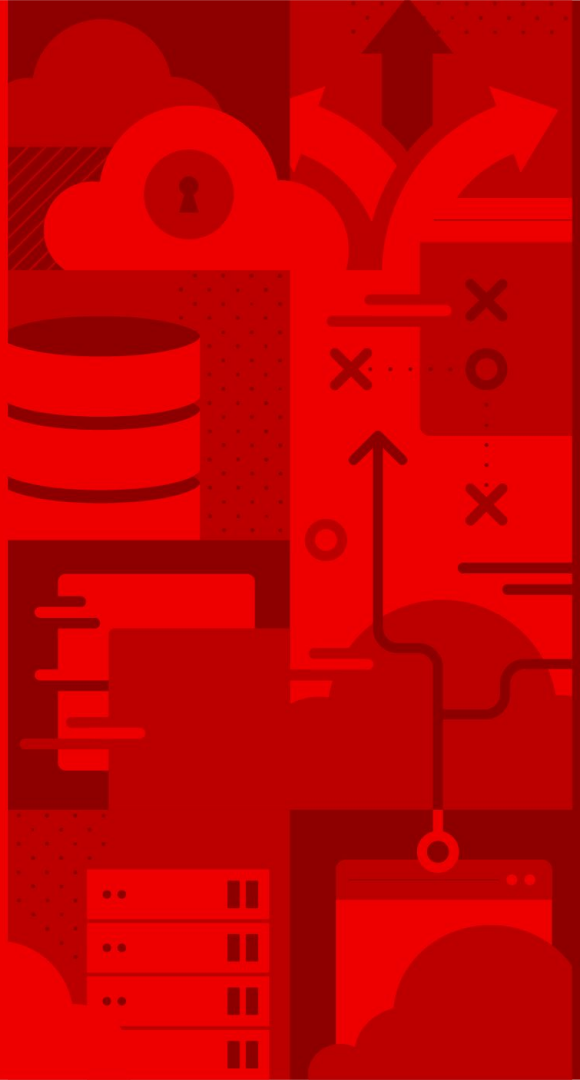
Run
- Cluster services: metrics, chargeback, registry, logging
- Advanced infrastructure functionality
- Dev services: dev tools, automated builds, CI/CD, IDE

Manage
- Multicluster and Kubernetes lifecycle management
- Policy-based governance, risk, and compliance
- Application lifecycle management
- ODF integration for Disaster Recovery of stateful apps

Automate
- Workflow orchestration
- Network and security automation
- Automation analytics
- Certified content
- Automation services catalog

Observe
- Red Hat Insights for OpenShift
- Connected customer experience
- Subscription watch
- Red Hat Cloud Services

Red Hat

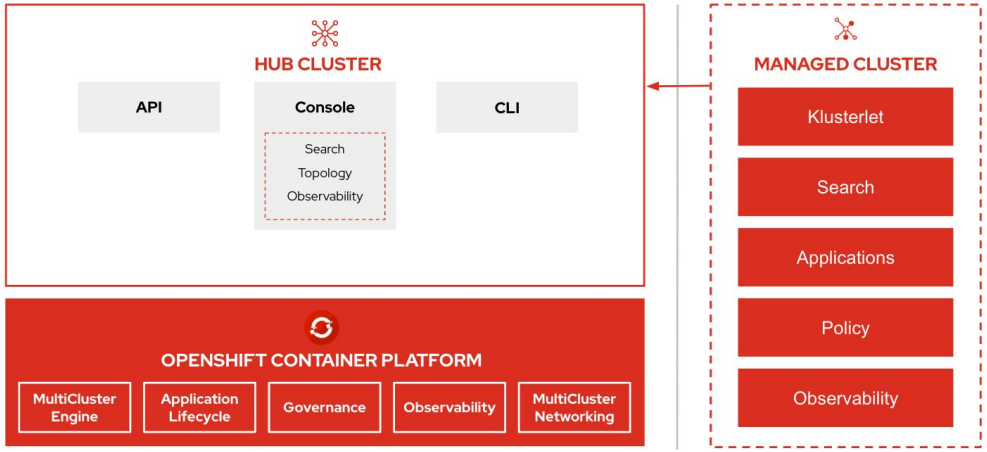


Architecture

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

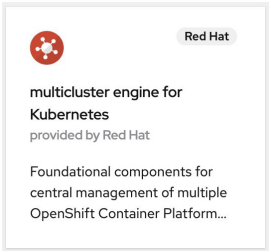
Managed cluster

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

List of included components:

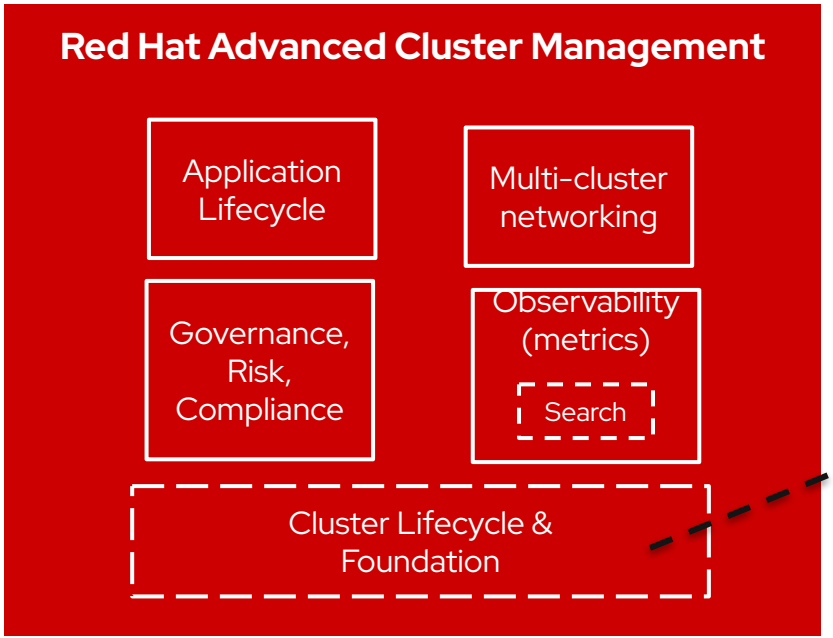
- Application manager
- Certificate controller
- Policy controller
- Registration agent
- Observability controller
- Search collector
- Cluster proxy
- IAM policy controller
- Work manager

With MCE, ACM has re- packaged core multi-cluster functionality into a new operator

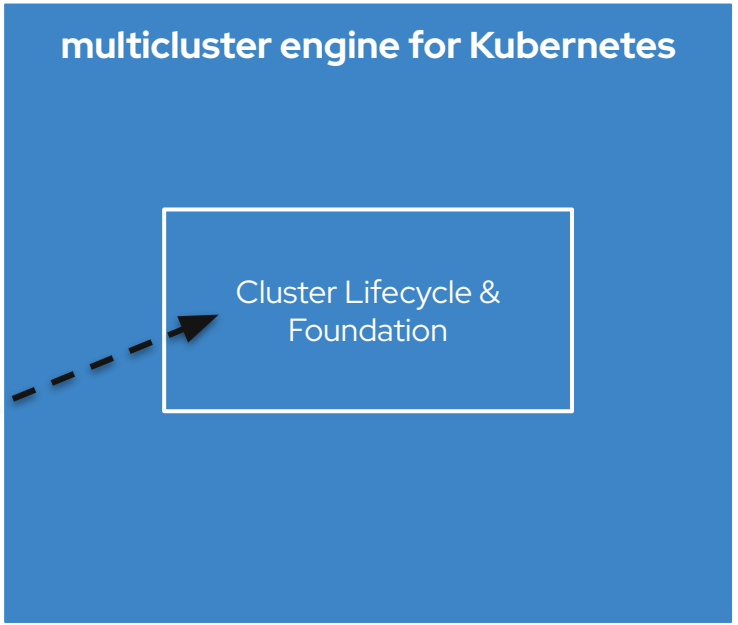


The **multicluster engine for Kubernetes** operator is entitled with OpenShift and it's installed automatically during a RHACM install.

ACM 2.4 (and earlier)



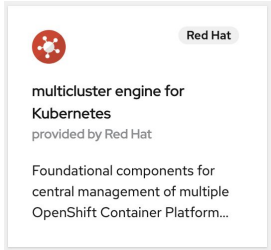
MCE 1.0 (and later)



Red Hat

ACM is “Consumer One” of MCE

RHACM is built on top of the **multicluster engine operator**.



ACM 2.5, 2.6, 2.7, 2.8, 2.9, 2.10

ADVANCED CLUSTER MANAGEMENT

- Application Lifecycle
- Governance, Risk, Compliance
- Observability & Search
- Multi-cluster networking

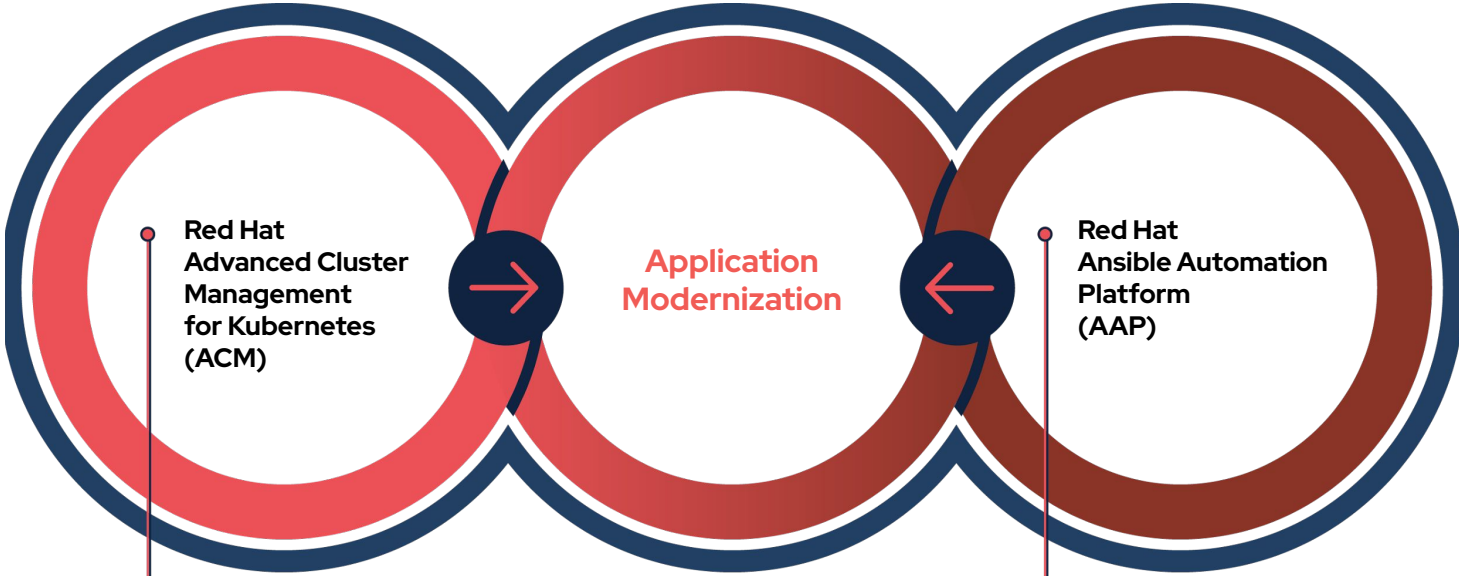
MCE 2.0, 2.1, 2.2, 2.3, 2.4, 2.5

MULTICLUSTER ENGINE

- Cluster Manager (Inventory, Work, Placement)
- Klusterlet
- Discovery
- Hive
- Central Infrastructure Management & Infra Operator
- Hosted Control Planes

Red Hat

Application modernization driven by automation of Kubernetes and beyond….



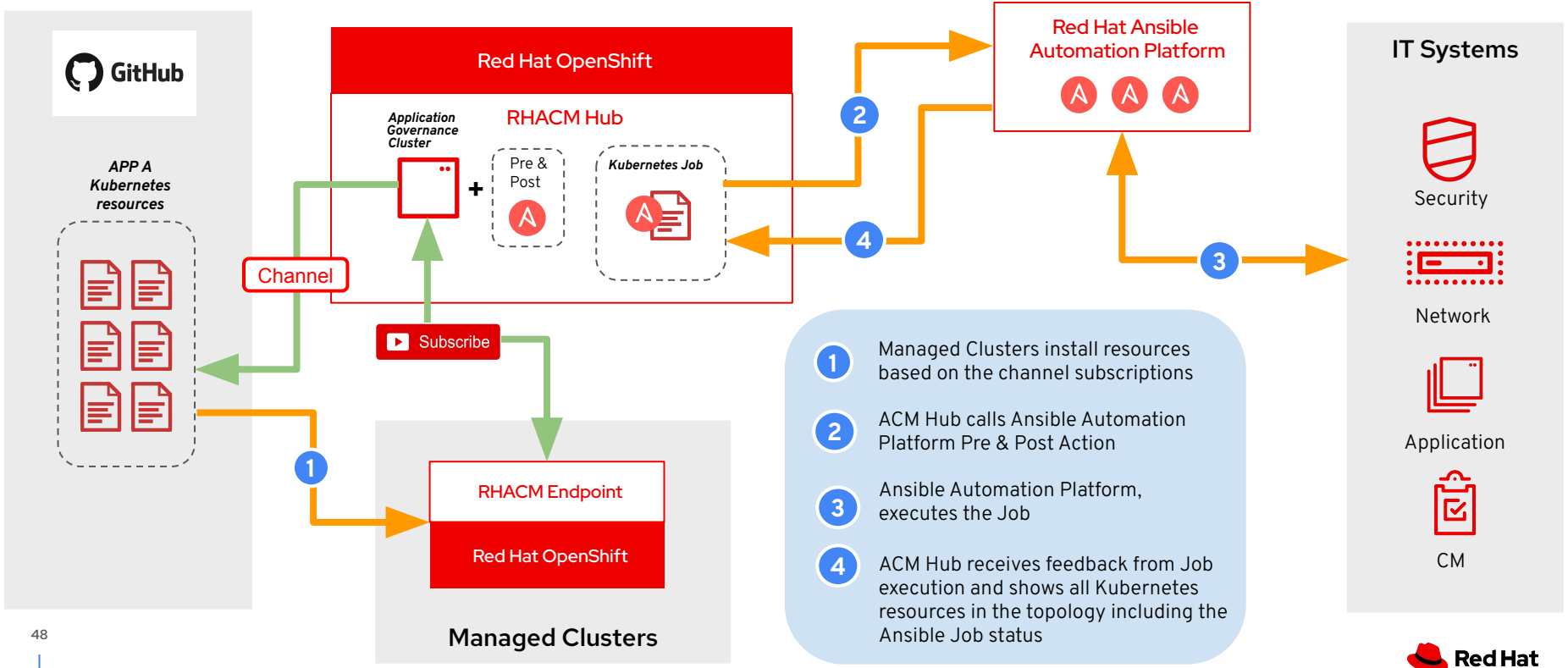
Automate the deployment and management of OpenShift cluster, applications, control policy compliance, and enforcement

Automating everything else outside of Kubernetes: Configuration of networking, databases, load balancers, storage, etc.

Red Hat

Complete Automation Platform

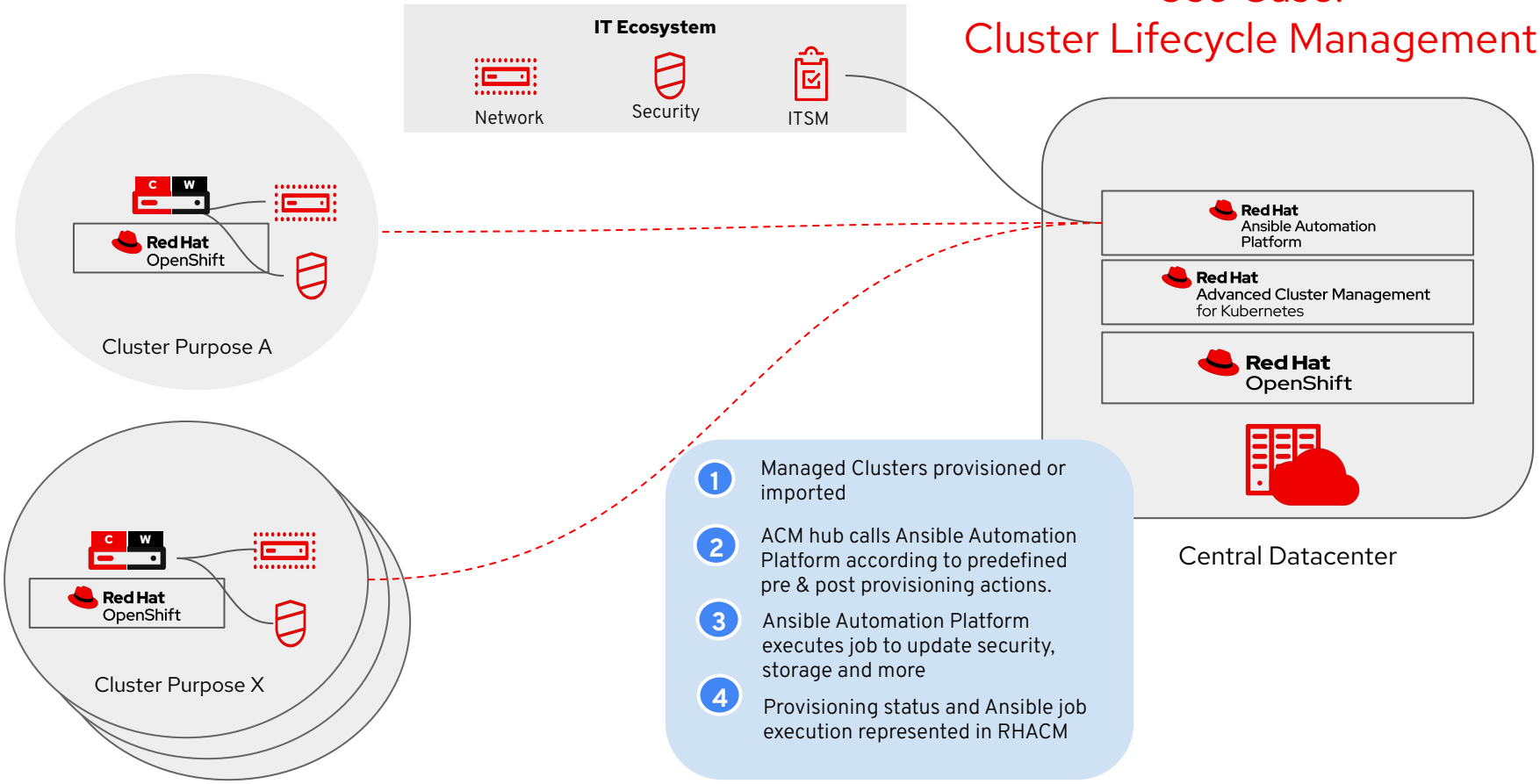
ACM - Ansible Automation Platform Integration through all the use-cases



Red Hat

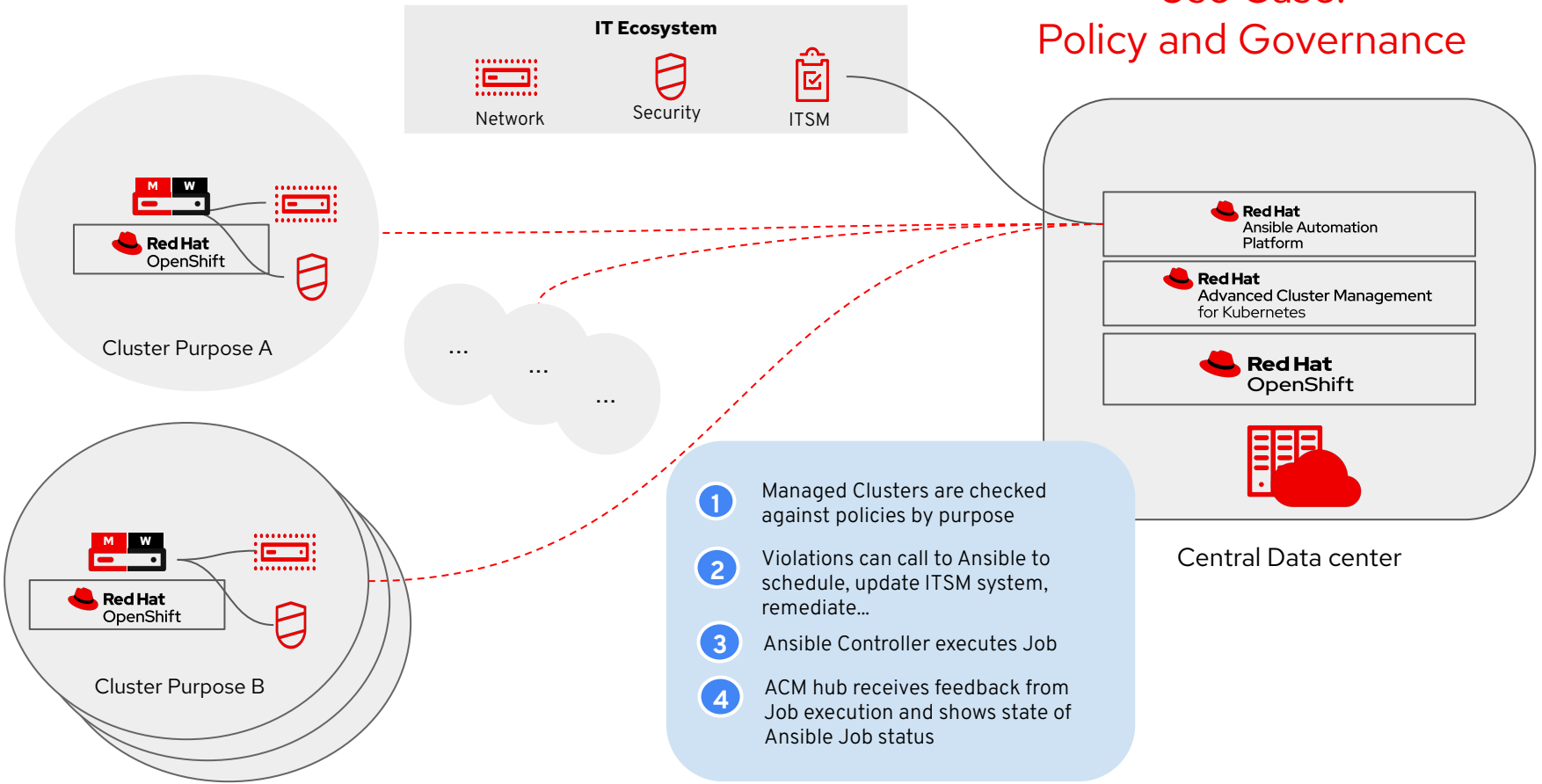
Complete Automation Platform

Use Case: Cluster Lifecycle Management



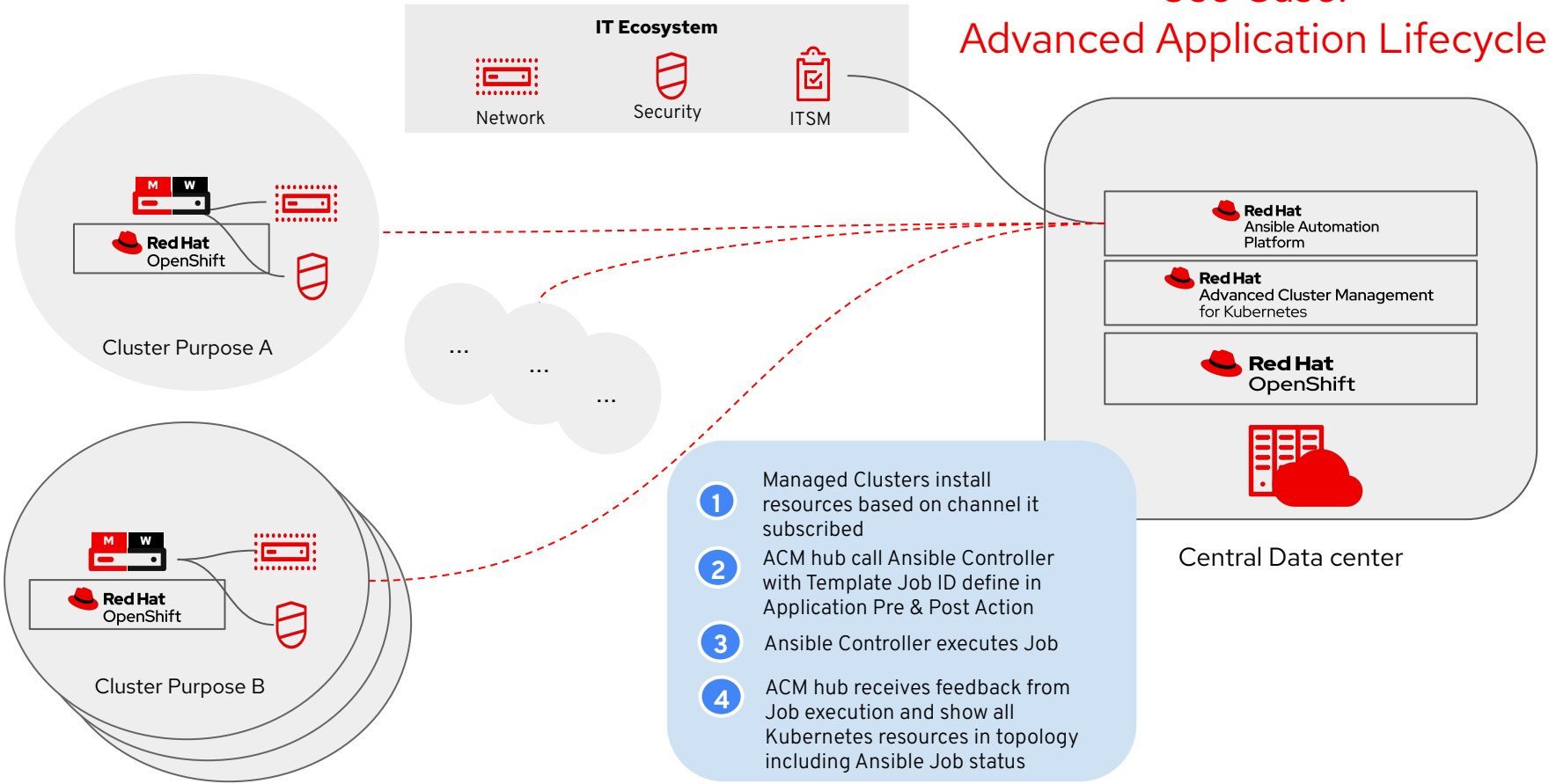
Complete Automation Platform

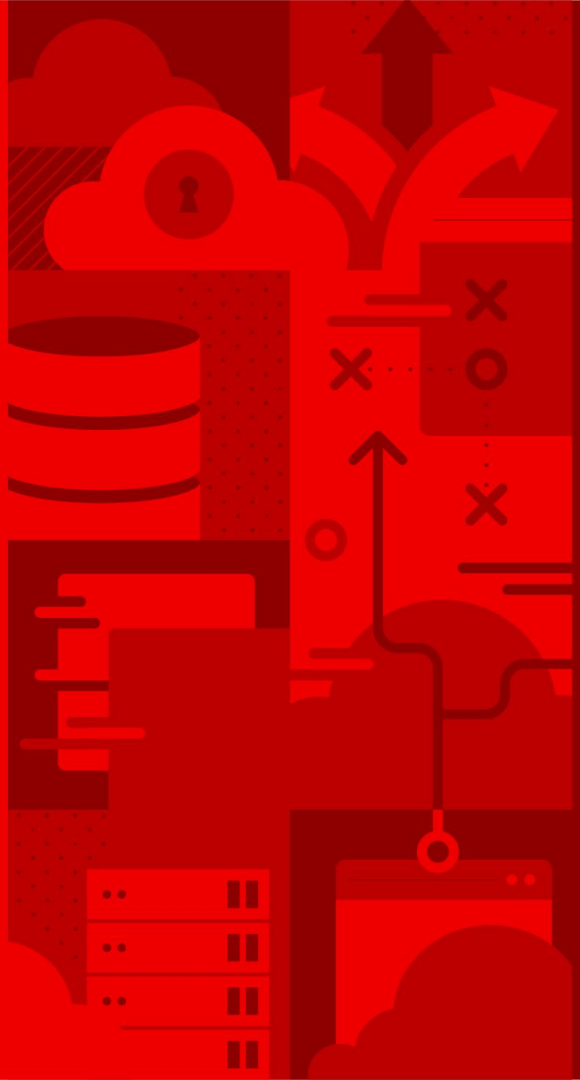
Use Case: Policy and Governance



Complete Automation Platform

Use Case: Advanced Application Lifecycle





Installation

Installation and Foundation

Operator-based installation for Hub cluster

IT Operations

Hub Cluster

- Operator-based installation
- Available on OperatorHub
- Requires OCP 4.13.x - **Latest**

Full Lifecycle Management of OCP clusters

- Deploy OpenShift 4.13.x - **Latest**

Import and Management of OCP clusters

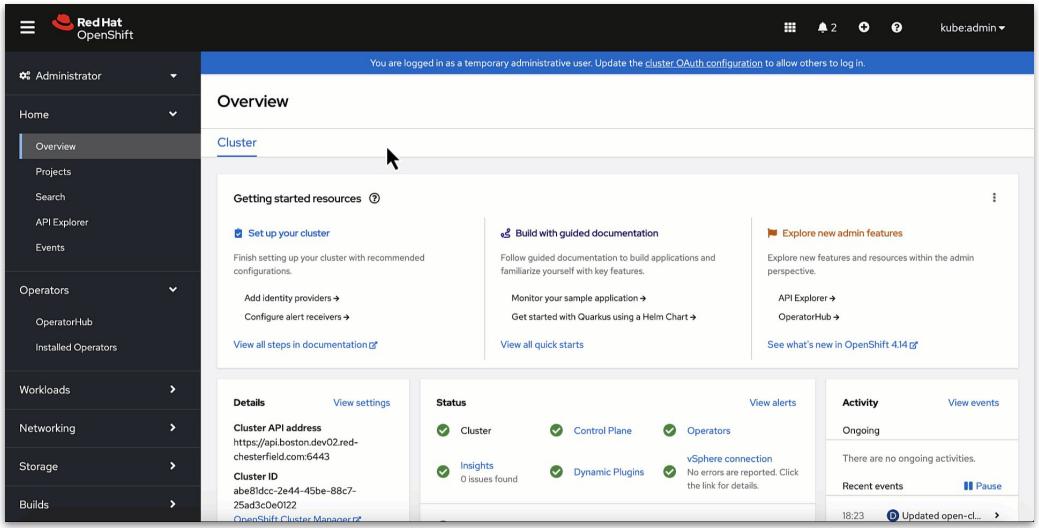
- OpenShift 3.11*, OpenShift 4.13.x - **Latest**
- Cloud hosted OCP: ROSA / OSD / ARO / RHOIC

Import and Limited Management for public 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*

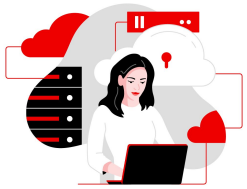
  * Production requirements vary based on number of clusters in the management domain and types of workloads being run.

  * vCPU/RAM Numbers are per node.

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.

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make
Red Hat a trusted adviser to the Fortune 500.

Stay Connected acm-contact@redhat.com


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat