



Red Hat

Advanced Cluster Management
for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes

Introduction

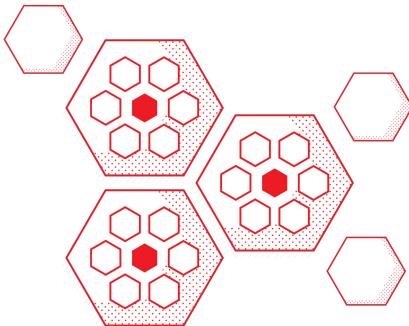
Alfred Bach

Red Hat



Market Trends and Challenges

Kubernetes adoption leads to multicloud



“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.”

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*

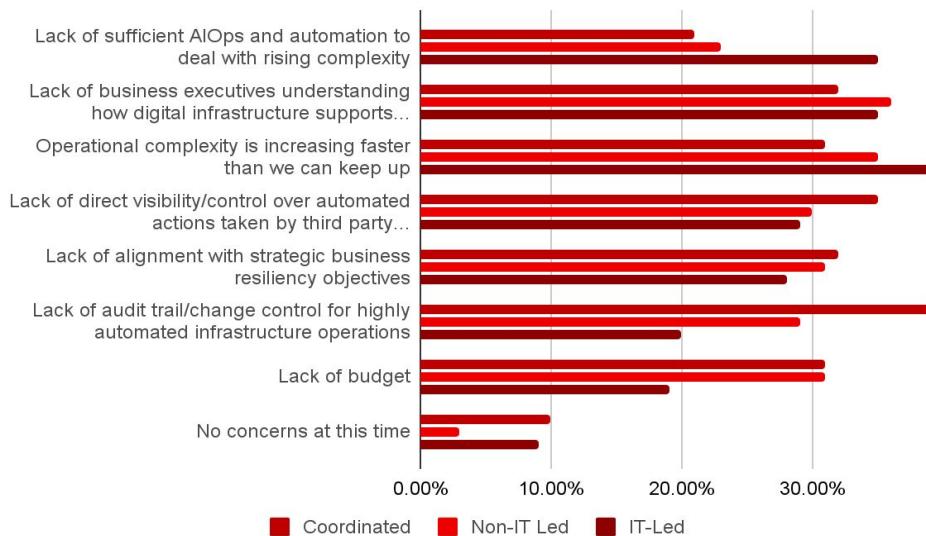


Using multiple public clouds and one or more private/dedicated clouds.*

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?



Remote container clusters are becoming modern-day LAN servers

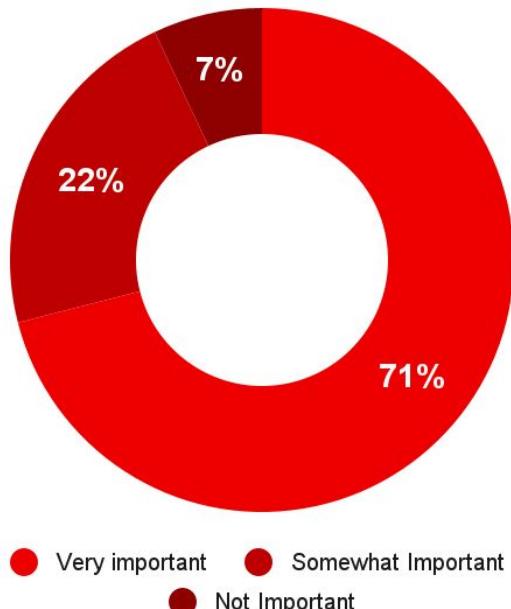
In many ways, remote container clusters are becoming modern-day LAN servers, which requires tooling for managing the distributed clusters.

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**

Unified, consistent, autonomous operations priorities

Importance of Unified Management Control Plane



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



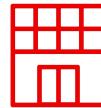
Improve data integration and data protection

Optimize infrastructure costs and usage

Where's the growth in cluster deployments?



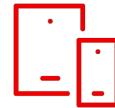
Small Scale Dev Teams



Medium Scaled Organizations



Large scale



Edge scale / Telco

- Managing and syncing across Dev/QE/Pre-Prod/Prod clusters can be difficult
- Retail with small clusters across 100s of locations
- Organizations with plan for growth 10-15 clusters moving to 100s
- Global organizations with 100s of clusters, hosting thousand of applications
- Large Retail with 1000s of stores
- 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

Multicloud management challenges

How do I normalize and centralize key functions across environments?



Solving real customer challenges



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

Seamless management and operations of the complete Kubernetes environment



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



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



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**



Introducing Red Hat Advanced Cluster Management



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

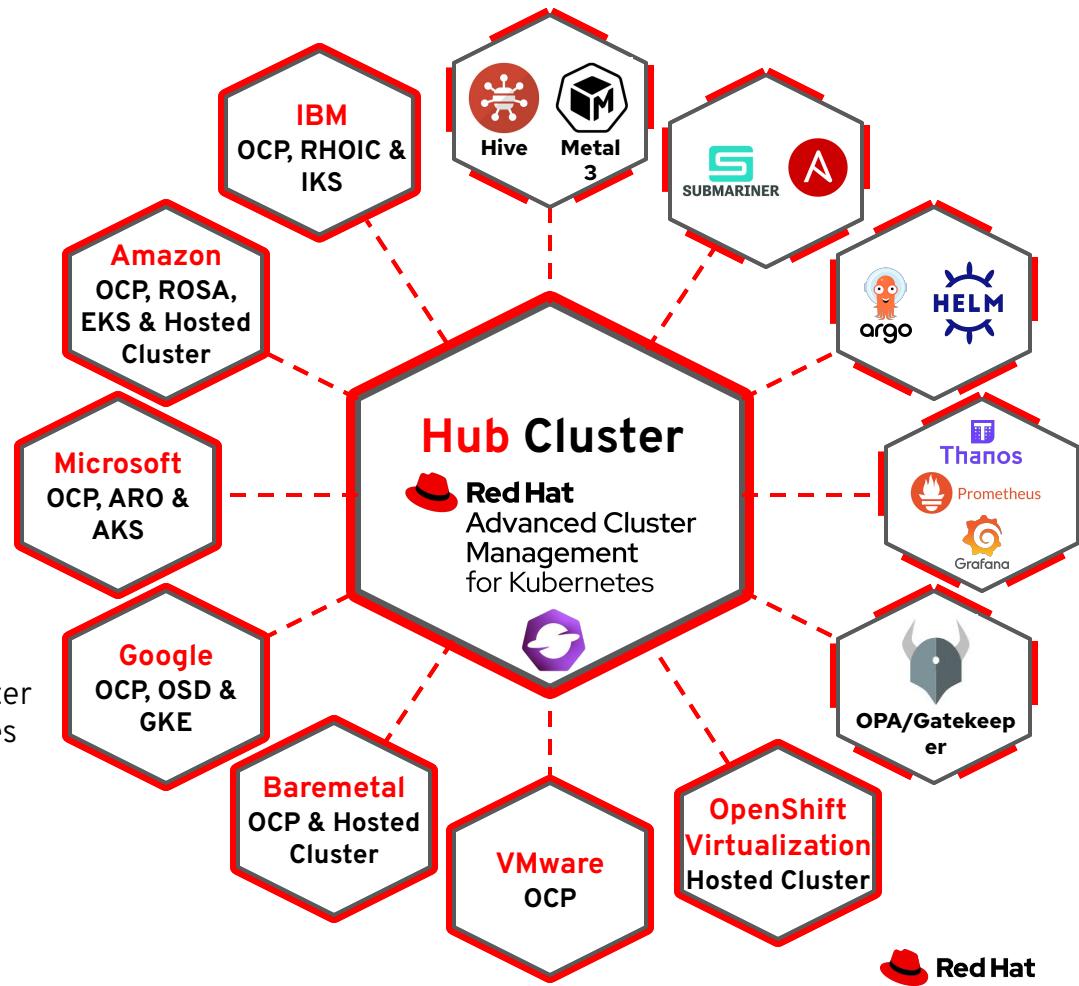
Like any other Kubernetes app, **easily run** and manage it on top of an OpenShift cluster.

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



Multicloud lifecycle management



Policy driven governance, risk, and compliance



Advanced application lifecycle management



Multicloud Observability and Search for health and optimization



Multicloud networking for interconnecting apps

The screenshot displays several key components of the Red Hat Advanced Cluster Management interface:

- Overview Dashboard:** Shows cluster counts by provider (AWS, Amazon, VMware, Other, Microsoft, IBM, Google), application counts (22), cluster counts (13), Kubernetes types (6), regions (2), and nodes (49). It also includes a chart of cluster violations (8%) and a summary of pods (99% healthy).
- Governance Dashboard:** Displays policy set violations (2) and policy violations (35) across various categories like ACM-Health, CA Security Assessment and Authorization, and CM Configuration Management.
- Clusters View:** Lists clusters with their status (e.g., rosecluster, local-cluster, migration, sberens-aro-central, sberens-rose-west, sberens-eks-west, carolina, sberens-arm64, dev-iks-eu, sberens-ako-central, sberens-x86-64, sberens-gke-central, testcluster) and provides controls for CA-7 Continuous Monitoring.
- Application Lifecycle Management:** A detailed diagram showing the flow from Application (pacman-app) through Subscription, Placement, Deployment, and Replicaset to a specific pod.
- Metrics and Monitoring:** Real-time monitoring of cluster metrics like CPU, Memory, and Disk usage, along with performance graphs for CPU and Memory.

Unified Multi Cluster Management

Single Management for all your Kubernetes Clusters

The screenshot displays the Red Hat OpenShift Multi Cluster Management interface. On the left, a navigation sidebar includes links for All Clusters, Home, Welcome, Overview, Search, Infrastructure, Applications, Governance, and Credentials. The main area has two tabs: 'Overview' and 'Summary'. The 'Overview' tab shows a grid of clouds representing different cloud providers: AWS (6 clusters), VMware (1 cluster), Other (2 clusters), Microsoft (2 clusters), IBM (1 cluster), and Google (1 cluster). The 'Summary' tab shows a list of clusters with columns for Name, Namespace, Status, Infrastructure, Control plane type, Distribution version, Labels, Nodes, and Creation date. The first cluster listed is 'carolina' (Namespace: carolina, Status: Ready, Infrastructure: VMware vSphere, Control plane type: Standalone, Distribution version: OpenShift 4.11.26, Labels: app=pacman-game, authdeployment=east, environment=prod, openshiftVersion-major=4, openshiftVersion-major-minor=4.11, upgrade-now, useglobal=true, Nodes: 3, Creation date: 09/09/2022, 19:44:46). The second cluster is 'dev-iks-eu' (Namespace: dev-iks-eu, Status: Ready, Infrastructure: IBM Cloud, Control plane type: Standalone, Distribution version: v1.23.16+KS, Labels: environment=dev, Nodes: 3, Creation date: 11/02/2022, 04:50:38). The third cluster is 'local-cluster' (Namespace: local-cluster, Status: Ready, Infrastructure: aws Amazon Web Services, Control plane type: Hub, Distribution version: OpenShift 4.11.9, Labels: authdeployment=east, environment=prod, gtops=true, openshiftVersion-major=4, openshiftVersion-major-minor=4.11, velero/ignore-backup=true, Nodes: 10, Creation date: 12/11/2021, 17:33:35). The fourth cluster is 'migration' (Namespace: migration, Status: Ready, Infrastructure: aws Amazon Web Services, Control plane type: Standalone, Distribution version: OpenShift 4.11.26, Labels: app=pacman-game, authdeployment=east, gtops=true, openshiftVersion-major=4, Nodes: 7, Creation date: 08/02/2022, 18:38:25).

- **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

Policy based Governance, Risk, and Compliance

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

Governance 

Overview Policy sets Policies

Policy set violations 2 Policy violations 57 Clusters

rosacluster local-cluster 1 A 22 14 14 1

2 Violations

Create policy  A policy generates reports and validates cluster compliance based on specified security standards, categories, and controls.

Standards

- ACM-Health
- CM-2 Baseline Configuration
- NIST
- NIST 800-53
- NIST SP 800-53
- NIST-CSF
- generic

1 Details

Name compliance-operator Namespace policies

2 Policy templates

3 Placement

4 Policy annotations

5 Review

Templates

Policy templates

- comp-operator-ns-2
- comp-operator-operator-group-2
- comp-operator-subscription-2
- comp-operator-status-2

Placement

Label expressions

name equals local-cluster

Policy annotations

Standards NIST SP 800-53

Categories CA Security Assessment and Authorization

Controls CA-2 Security Assessments CA-7 Continuous Monitoring

Submit Back Cancel

Policy YAML

```
1 apiVersion: policy.open-cluster-management.io/v1
2 kind: Policy
3 metadata:
4   name: compliance-operator
5   namespace: policies
6   annotations:
7     policy.open-cluster-management.io/categories: CA Security Assessment and Authorization
8     policy.open-cluster-management.io/standards: NIST SP 800-53
9     policy.open-cluster-management.io/controls: CA-2 Security Assessments, CA-7 Continuous Monitoring
10 spec:
11   disabled: false
12   policy-templates:
13     - objectDefinition:
14       apiVersion: policy.open-cluster-management.io/v1
15       kind: ConfigurationPolicy
16       metadata:
17         name: comp-operator-ns-2
18       spec:
19         remediationAction: inform
20         severity: high
21         object-templates:
22           - complianceType: musthave
23             objectDefinition:
24               apiVersion: v1
25               kind: Namespace
26               metadata:
27                 name: openshift-compliance
28           - objectDefinition:
29             apiVersion: policy.open-cluster-management.io/v1
30             kind: ConfigurationPolicy
31             metadata:
32               name: comp-operator-operator-group-2
33             spec:
34               remediationAction: inform
35               severity: high
36               object-templates:
37                 - complianceType: musthave
38                   objectDefinition:
39                     apiVersion: operators.coreos.com/v1
```

- **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

Advanced Application Lifecycle Management

Simplify your Application Lifecycle

Applications

Create application YAML: On

Name * Enter name

Namespace * Enter namespace

Repository location for resources

Repository types

rocketchat

Overview Topology

URL * Enter or select a Helm repository

Username

Application YML

```
1 apiVersion: app.k8s.io/v1beta1
2 kind: Application
3 metadata:
4   name:
5   namespace:
6 spec:
7   componentKinds:
8     - group: apps.open-cluster-management.io
9       kind: Subscription
10      descriptor: {}
11      selector:
12        matchExpressions:
```

Pod rocketchat-db

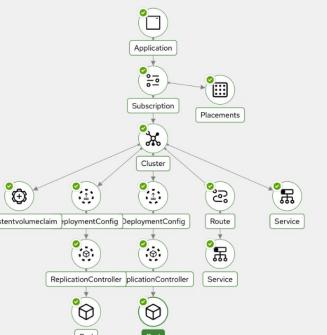
Launch resource in Search [View](#)

Details Logs YAML

Type: Pod
Namespace: rocketchat
Labels: app=rocketchat-db,deployment=rocketchat-db-1; deploymentconfig=rocketchat-db

Pod details for local-cluster

Pod: rocketchat-db-1-g/vst
Namespace: rocketchat
Status: Running
[View Pod YAML and Logs](#)
Restarts: 0
Host and Pod IP: 10.0.146.124, 10.129.2.114
Created: 2 hours ago



- **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

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

The screenshot shows a web-based interface for managing multiple Kubernetes clusters. The top navigation bar includes the Red Hat logo, the title 'Advanced Cluster Management for Kubernetes', and a user dropdown for 'kube/admin'. Below the header is a search bar and a toolbar with various icons. The main content area is titled 'Clusters' and displays a table of cluster information. The columns include the cluster name, status (e.g., Offline, Ready), version, and vendor information. A tooltip for the 'acmcdsan1' cluster indicates it is 'Ready' with 'OpenShift 4.5.2(Upgrade available)'. The interface also shows filtering options like 'cloud=Amazon', 'cloud=Azure', 'cloud=Google', and 'cloud=OpenStack'. At the bottom, there are pagination controls for items per page (20), total items (1-20 of 39), and navigation arrows.

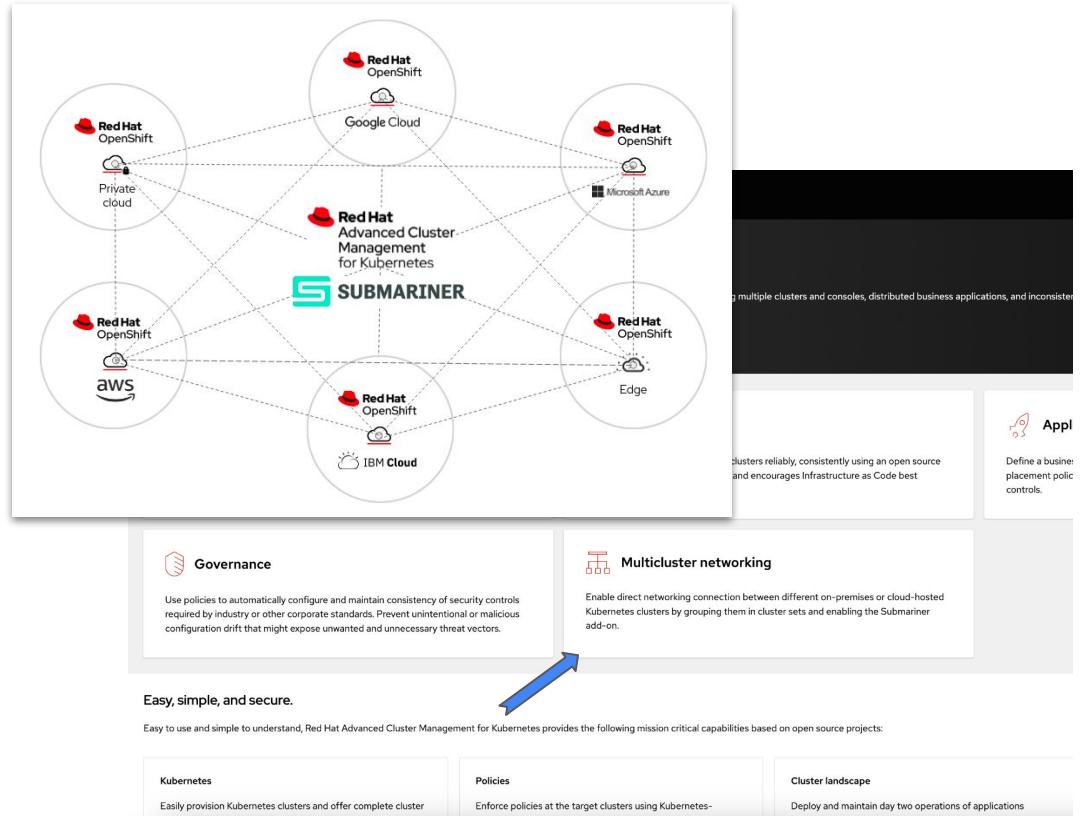
Cluster Name	Status	Version	Vendor	Actions
ctark-openshift40	Offline	OpenShift 4.6.0-rc.2	cloud=Amazon	...
sberens-azure	Offline	-	cloud=Azure	...
spoke50-ge2	Offline	v1.16.13-gke.401	cloud=Google vendor=GKE	...
acmcdsan1	Ready	OpenShift 4.5.2(Upgrade available)	cloud=OpenStack	...
acmcdsan2	Ready	OpenShift 4.5.2(Upgrade available)	cloud=OpenStack	...
dhaidue-01	Ready	OpenShift 4.3.38	cloud=Amazon	...
dhaidue-02	Ready	OpenShift 4.3.33(Upgrade available)	cloud=Amazon	...
dhaidue-03	Ready	OpenShift 4.5.11(Upgrade available)	cloud=Amazon	...
dhaidue-04	Ready	OpenShift 4.4.23(Upgrade available)	cloud=Amazon	...
dhaidue-eks-eu-central-1	Ready	v1.14.9-eks-058790	cloud=Amazon vendor=EKS	...
dhaidue-eks-eu-north-1	Ready	v1.14.9-eks-058790	cloud=Amazon vendor=EKS	...
dhaidue-eks-eu-west-1	Ready	v1.14.9-eks-058790	cloud=Amazon vendor=EKS	...
dhaidue-eks-eu-west-2	Ready	v1.14.9-eks-058790	cloud=Amazon vendor=EKS	...
dhaidue-eks-eu-west-3	Ready	v1.14.9-eks-058790	cloud=Amazon vendor=EKS	...
installer-test	Ready	OpenShift 4.5.5(Upgrade available)	cloud=Amazon	...
local-cluster	Ready	OpenShift 4.5.11(Upgrade available)	cloud=Amazon	...
lubbock	Ready	OpenShift 4.5.8(Upgrade available)	cloud=Amazon	...
oregon2	Ready	OpenShift 4.4.26(Upgrade available)	cloud=Amazon	...
sberens-eks1	Ready	v1.15.11-eks-065dce	cloud=Amazon vendor=EKS	...

Multicloud Networking

MCN features overview & look ahead

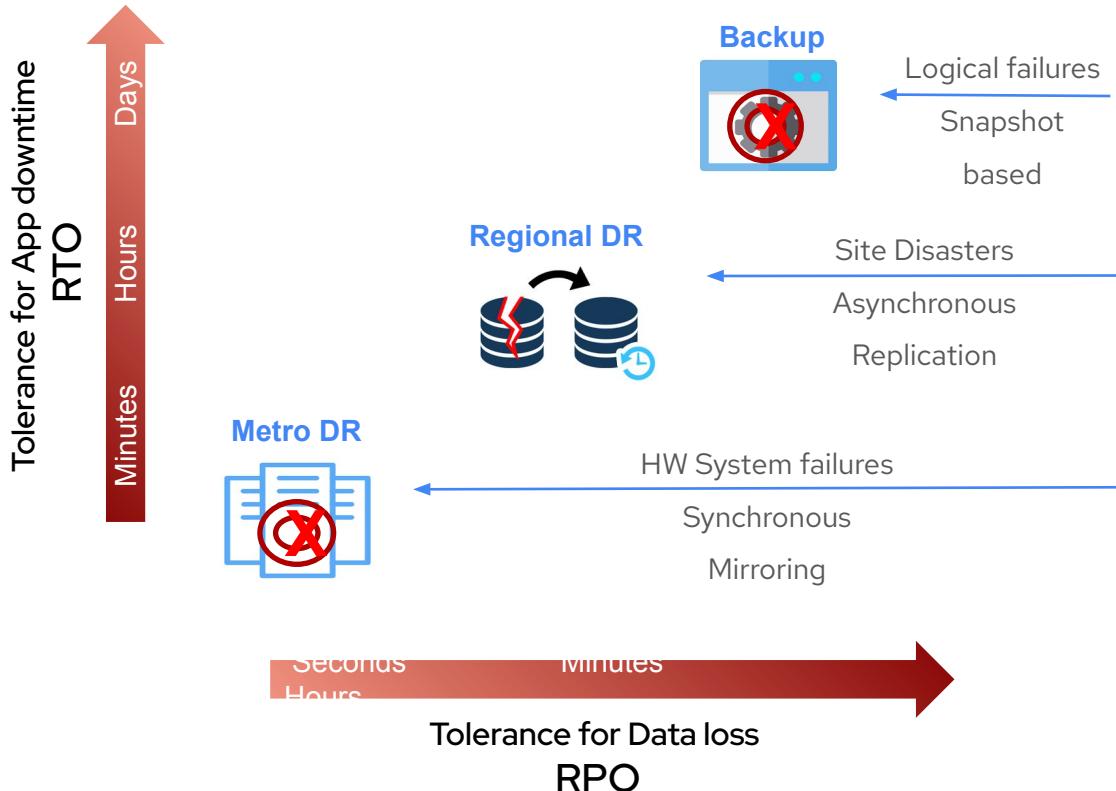
- **ACM MCN, aka 5th pillar**

- 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...



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.

- **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

Open Source commitment - Upstream project

The screenshot shows the official website for Open Cluster Management. At the top, there's a navigation bar with links for 'Community', 'Contribute', 'Document', and 'English'. Below the header, a large purple banner features a futuristic illustration of a person in a spacesuit working at a desk, surrounded by glowing hexagonal shapes and planets. The banner contains text: 'Make working with many Kubernetes clusters super easy regardless of where they are deployed' and a description of the project's focus on multicluster and multicloud scenarios. A 'Get Started' button and a GitHub link are also present.

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.
--	---	---	---

Strong open source community & ecosystem



OPA/Gatekeeper



Kyverno



Red Hat
Advanced Cluster
Management
for Kubernetes



HyperShift



Open Cluster
Management



Grafana



CAPI



metal3



SUBMARINER

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



 <p>IT Operations</p>	<p>How do I get a simplified understanding of my cluster health and the impact it may have on my application availability ?</p> <p>How do I automate provisioning and deprovisioning of my clusters?</p>
 <p>DevOps/SRE</p>	<p>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?</p>

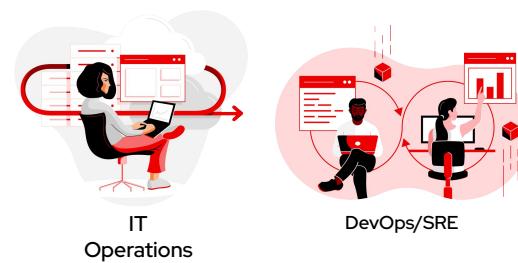


Multi-cluster Lifecycle Management



Overview

- **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



Clusters

Cluster list Cluster sets Cluster pools Discovered clusters

Get started with Multicloud Hub Grafana

Name	Namespace	Status	Infrastructure	Control plane type	Distribution version	Labels	Nodes	Add-ons	Creation date
aks-central	aks-central	Ready	Microsoft Azure	Standalone	v1.28.5	13 labels	2	9	05/01/2024, 21:26:08
aro-central	aro-central	Ready	Microsoft Azure	Standalone	OpenShift 4.13.9	app=pacman openshiftVersion=major... openshiftVersion=major... 15 more	6	9	28/02/2024, 23:13:04
boston	boston	Ready	VMware vSphere	Standalone	OpenShift 4.14.16 Upgrade available	openshiftVersion=major... openshiftVersion=major... 15 more	4	9	27/02/2024, 23:00:33
eks-west	eks-west	Ready	aws Amazon Web Services	Standalone	v1.28.7-eks-b99-9e6d7	13 labels	1	9	05/01/2024, 20:57:17
gke-central	gke-central	Ready	Google Cloud Platform	Standalone	v1.28.7-gke.1026000	13 labels	3	9	04/01/2024, 20:31:19
iks-eu	iks-eu	Ready	IBM Cloud	Standalone	v1.25.16+IKS	13 labels	3	9	10/04/2023, 22:59:35
local-cluster	local-cluster	Ready	aws Amazon Web Services	Hub	OpenShift 4.14.19	app=arm-sleep environment=prod install_acs=yes openshiftVersion=major... openshiftVersion=major...	7	8	10/04/2023, 18:32:16

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

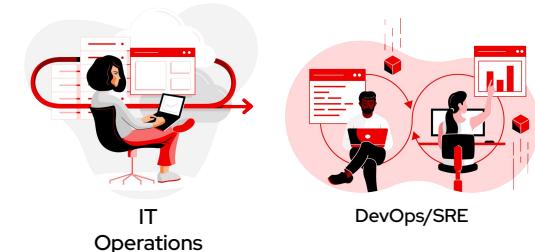
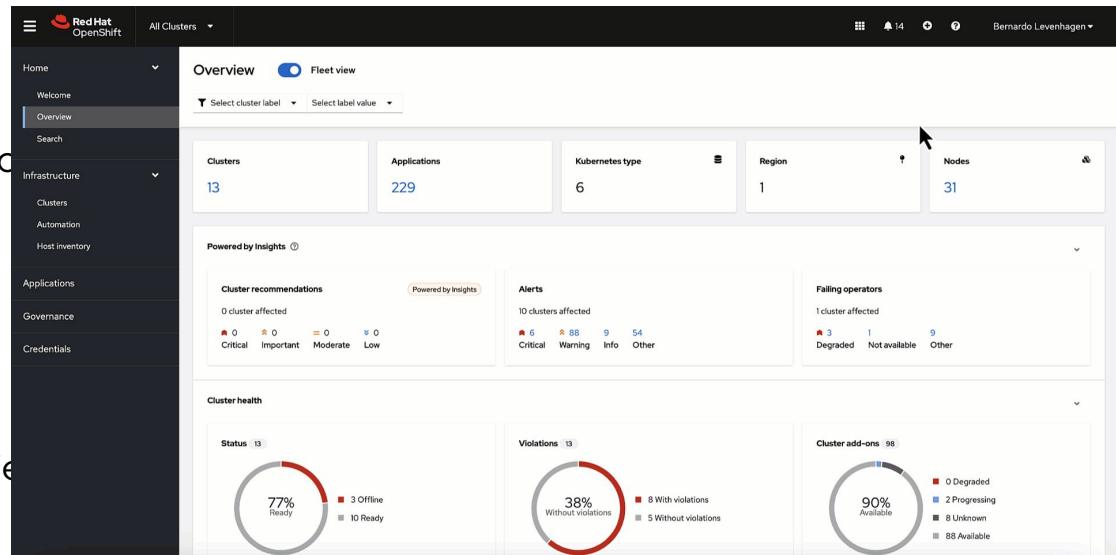


Multi-cluster Lifecycle Management



Dynamic Search

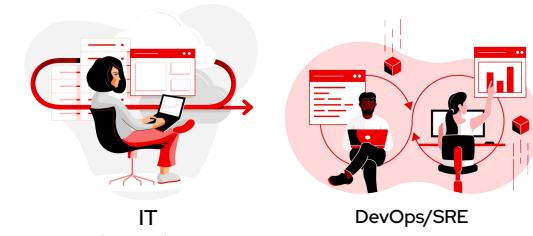
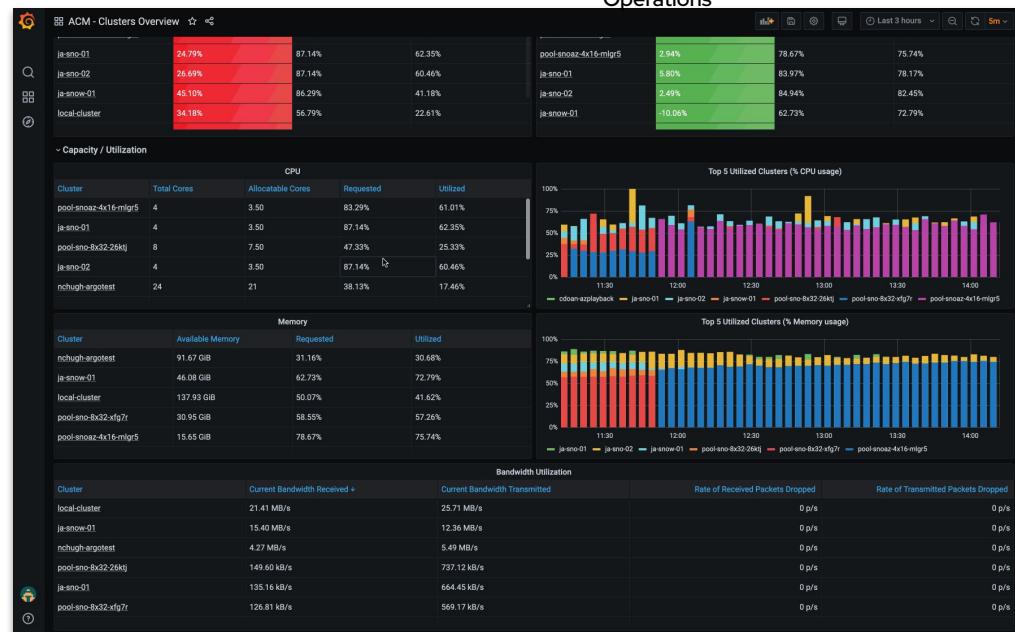
- Troubleshooting across clusters via relationships
- See all **unhealthy** pods
- See related application models to those pods
- See related Persistent Volumes
- See related secrets
- See related ***any*** kube resource object category



Multi-cluster Observability

Overview

- 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



Policy based Governance, Risk and Compliance



 <p>Security OPS</p>	<ul style="list-style-type: none">• 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?
 <p>IT Operations</p>	<ul style="list-style-type: none">• How do I ensure 99.9 % Uptime?• How do I drive more innovation at scale?

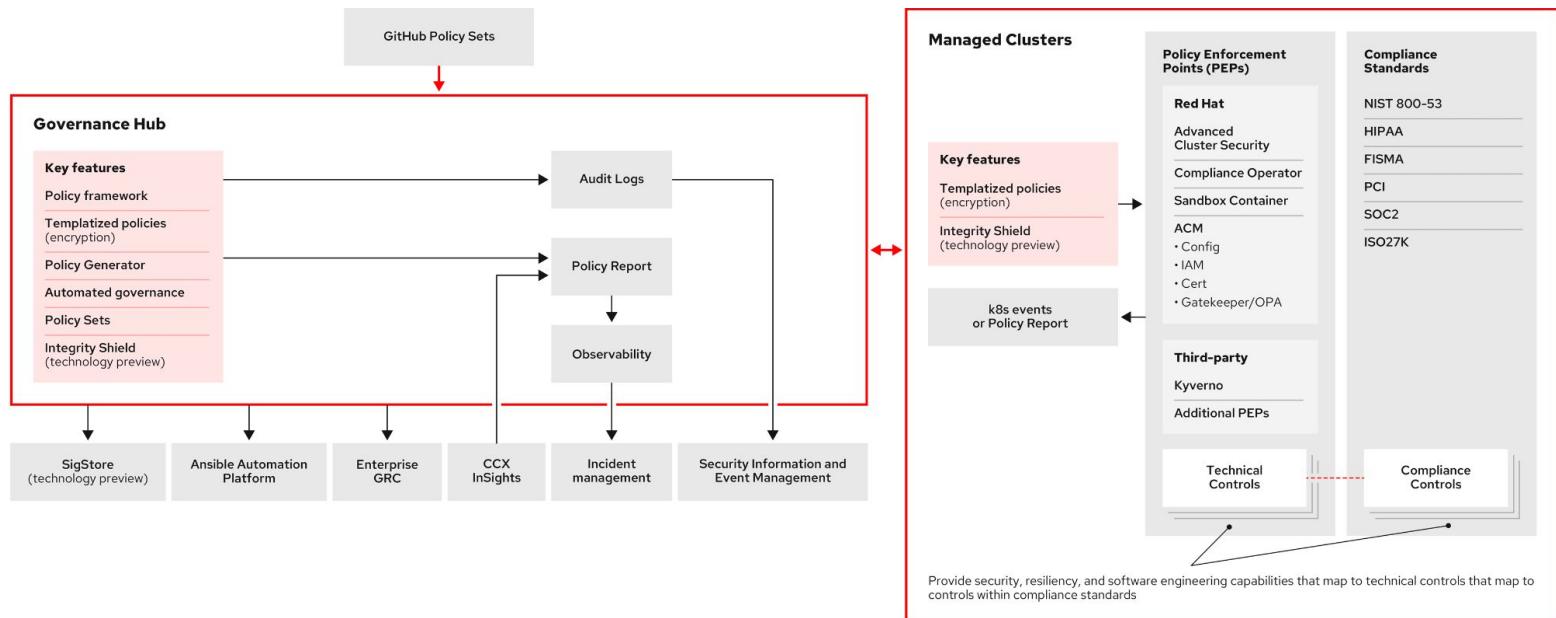
Policy based Governance, Risk and Compliance

Overview



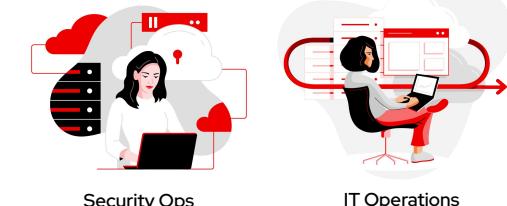
Managed Cluster and GRC Controllers

- 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](#)



Policy based Governance, Risk and Compliance

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



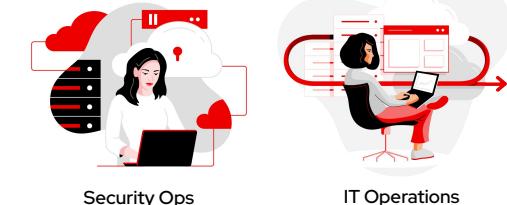
- **Set** and **enforce** policies for security, applications, & infrastructure
- **Deep visibility** for auditing configuration of apps and clusters
- **Custom view** for policies
- Categorize violations based on your standards for immediate visibility into your compliance posture
- Integrate with **OPA/Gatekeeper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

The screenshot shows the Red Hat OpenShift Governance interface. The top navigation bar includes the Red Hat OpenShift logo, a 'All Clusters' dropdown, and a user profile for 'Bernardo L...'. The left sidebar has sections for Home, Welcome, Overview, Search, Infrastructure (Clusters, Automation, Host inventory), Applications, Governance (selected), and Credentials. The main content area is titled 'Governance' with tabs for Overview, Policy sets, and Policies. It features two donut charts: 'Policy set violations' (1 violation) and 'Policy violations' (21 violations). Below these are sections for 'Standards' (NIST 800-53, NIST SP 800-53, NIST-CSF) and 'Categories' (AC Access Control, AU Audit and Accountability, CA Security Assessment and Authorization, CM Configuration Management, PR.IIP Information Protection Processes and Procedures, PR.PT Protective Technology, SC System and Communications). To the right is a 'Clusters' table and a 'Controls' table. The 'Clusters' table lists clusters like metal-hosted-cp, aks-central, gke-central, local-cluster, iks-eu, aro-central, eks-west, boston, sno-vm3, and rosa-hcp, each with status indicators. The 'Controls' table lists various compliance controls with their status (e.g., AC-3 Access Enforcement, AU-3 Content of Audit Records).

Control	Status
AC-3 Access Enforcement	1 ✓
AC-3 Access Enforcement	1 ⓘ
AU-3 Content of Audit Records	1 ✓
CA-3 Information Exchange	1 ⓘ

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

A screenshot of the Red Hat OpenShift Governance interface. The top navigation bar includes the Red Hat OpenShift logo, 'All Clusters' dropdown, and user information for 'Bernardo Levenhagen'. The left sidebar has sections for Home, Infrastructure (Clusters, Automation, Host inventory), Applications, Governance (selected), and Credentials. The main content area is titled 'Governance' and shows a table of policies. The table columns are: Name, Namespace, Remediation, Policy set, Cluster violations, Automation, and Actions. A cursor points to the 'Actions' column header. The table lists 10 policies, each with a small icon and some descriptive text. For example, one policy named 'admin-acks-413' is in the 'demo-policy' namespace, has 'enforce' remediation, and is part of the 'cluster-upgrade-412-413' policy set. It has 0 cluster violations and an 'Configure' button.

Advanced Application Lifecycle Management

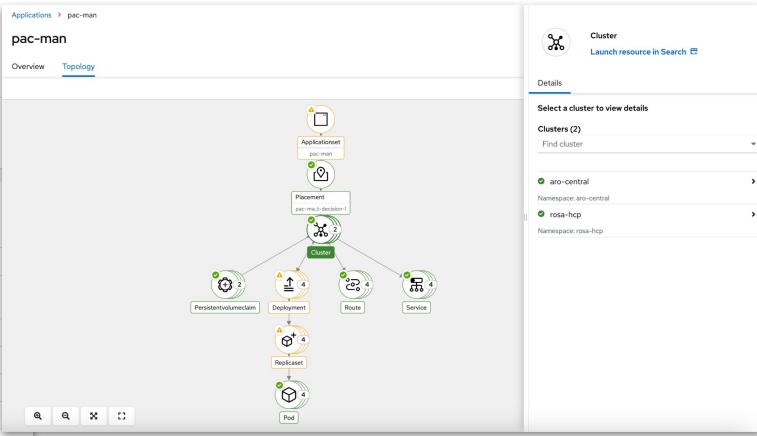
 <p>DevOps/SRE</p>	<ul style="list-style-type: none">• I want to quickly investigate application relationships with real time status, so that I can see where problems are.• With the Application Topology view, I can visually inspect application status labels and pod logs to understand if a part of the application is running or not, without having to connect to a cluster and gather any info.
 <p>IT Operations</p>	<ul style="list-style-type: none">• 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

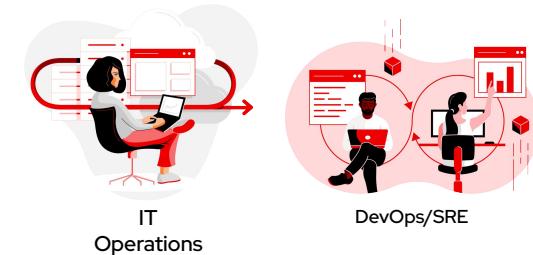
- **Deploy** applications at scale
- Deploy applications from **multiple sources**
(GitOps/Helm/ObjectStorage)
- Quickly visualize application relationships
- Integrate with the Red Hat Ansible Automation Platform
- Visualize Argo CD Applications in RHACM (Local and Remote)
- Support for **ApplicationSets**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

Name	Type	Namespace
guestbook	Argo CD ApplicationSet	guestbook
engineering-dev-guestbook	Argo CD ApplicationSet	guestbook
engineering-prod-guestbook	Argo CD ApplicationSet	guestbook
magchen-test	Argo CD ApplicationSet	
magchen-test2	Argo CD ApplicationSet	
nchugh-pacman	Discovered	default
pacman	Discovered	
pacman-app	Discovered	pacman-app
pre-kustomize-reversewords	Discovered	sre
rhacm-in40	Discovered	open-cluster-management
rhacm-op10	Discovered	open-cluster-management
spring-petclinic	Discovered	spring-petclinic

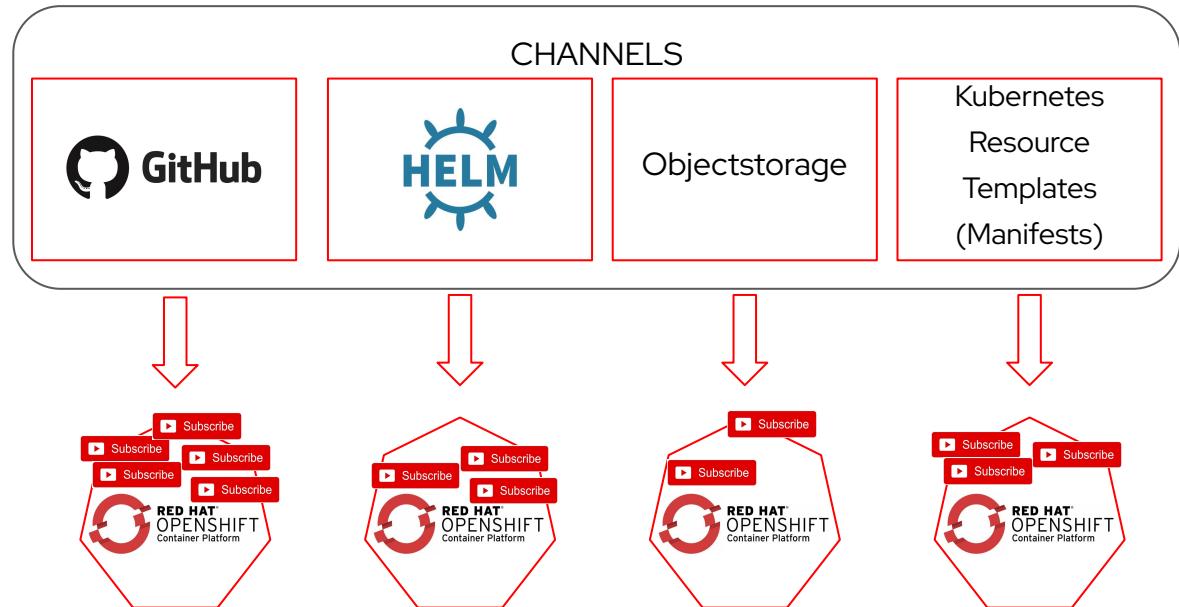


Advanced Application Lifecycle Management

Subscriptions bring enterprise to Kubernetes



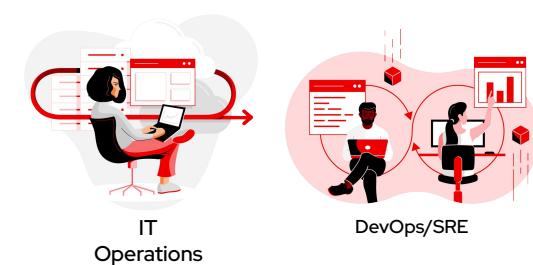
- Extending the best of Enterprise into a desired state methodology
- Time Windows: New releases during your maintenance windows
- Orchestrate actions with the integration of Ansible Automation Platform



Advanced Application Lifecycle Management

GitOps - Git as source of truth

- **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)



The screenshot shows a GitHub repository page for 'open-cluster-management / demo-subscription-gitops'. The repository has 57 commits, 3 branches, 0 packages, 0 releases, 1 contributor, and Apache-2.0 licensing. The 'Code' tab is selected. A recent commit from 'jnpacker' is shown, merging the 'master' branch from 'github.com:open-cluster-management/demo-subscription-gitops'. Below the commit list, a file viewer shows the 'README.md' file with the following content:

```
This repository contains examples of GitOps

Examples

1. Bare Metal Assets via gitops
2. Blue-Green Application Management via gitops
3. Placement Rules example

Help

Reach out to jnpacker@redhat.com or Slack @jnpacker in coreos.slack.com for help
```

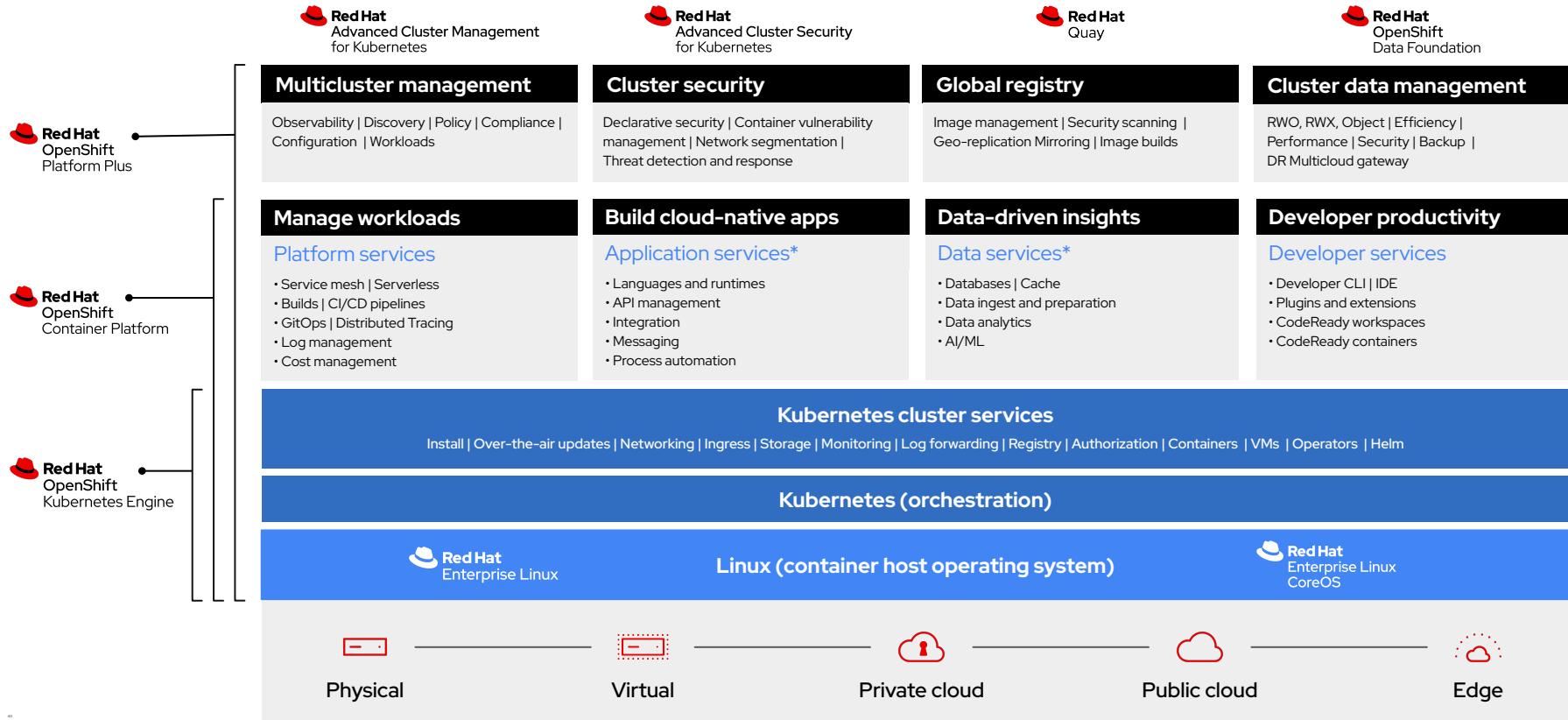
<https://github.com/open-cluster-management/demo-subscription-gitops>





How ACM works with OpenShift

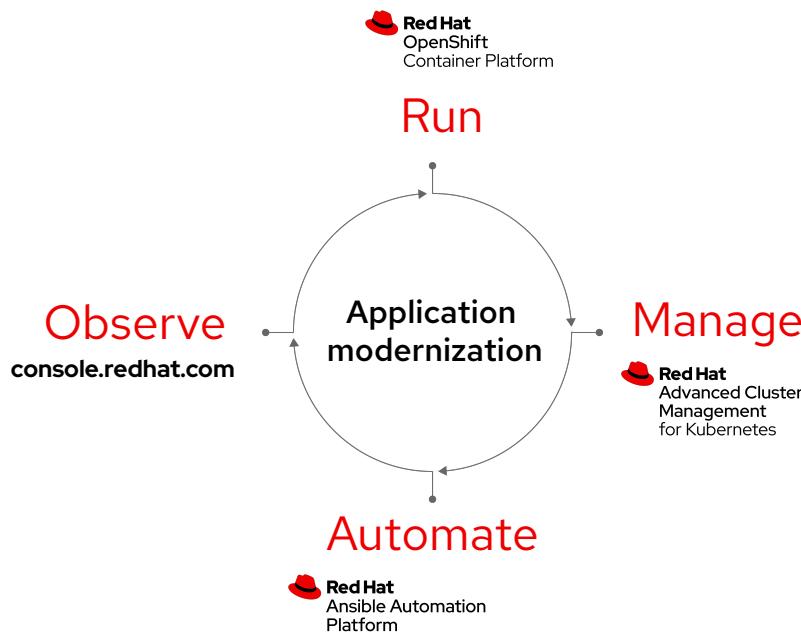
Bigger Picture: Red Hat Open Hybrid Cloud Platform



* 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

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

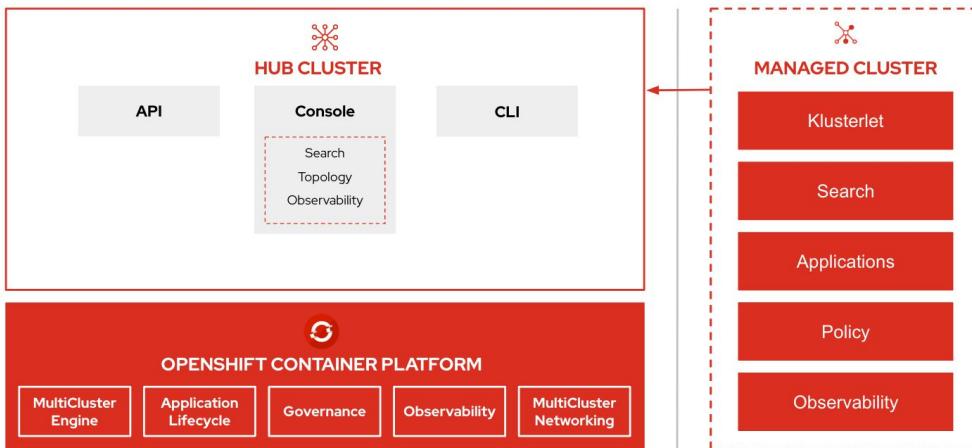
Architecture

Architecture Overview

Components



IT Operations



Hub architecture and components

Red Hat Advanced Cluster Management uses the **multicloudhub-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

* Multicloud 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.

Architecture Overview

Operator install for managed cluster



IT Operations



Managed cluster

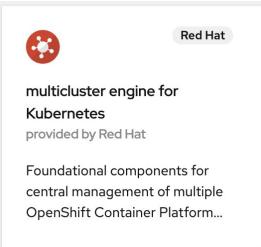
The [**klusterlet**](#) operator controls the deployment of components on the managed cluster.

List of included components:

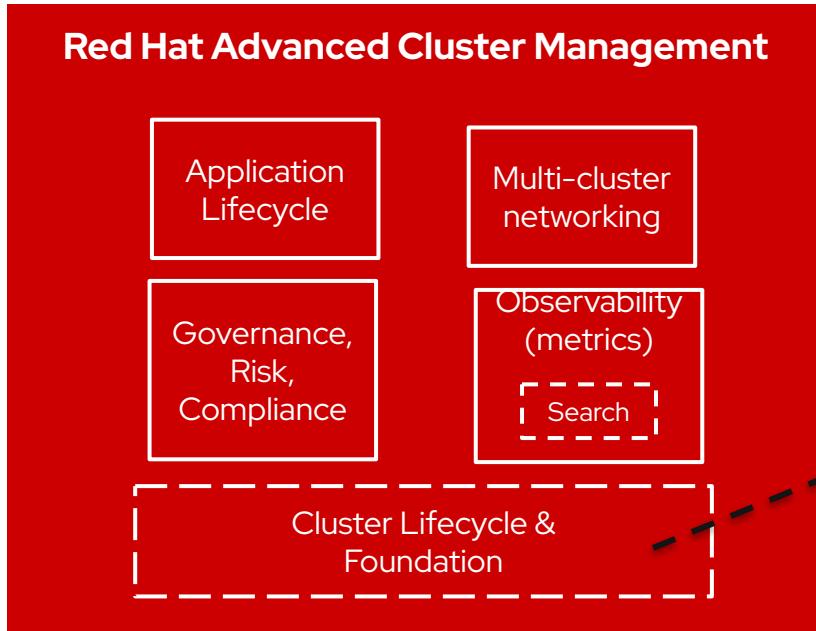
- ▶ Application manager
- ▶ Certificate controller
- ▶ Policy controller
- ▶ Registration agent
- ▶ Observability controller
- ▶ Search collector
- ▶ Cluster proxy
- ▶ IAM policy controller
- ▶ Work manager

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

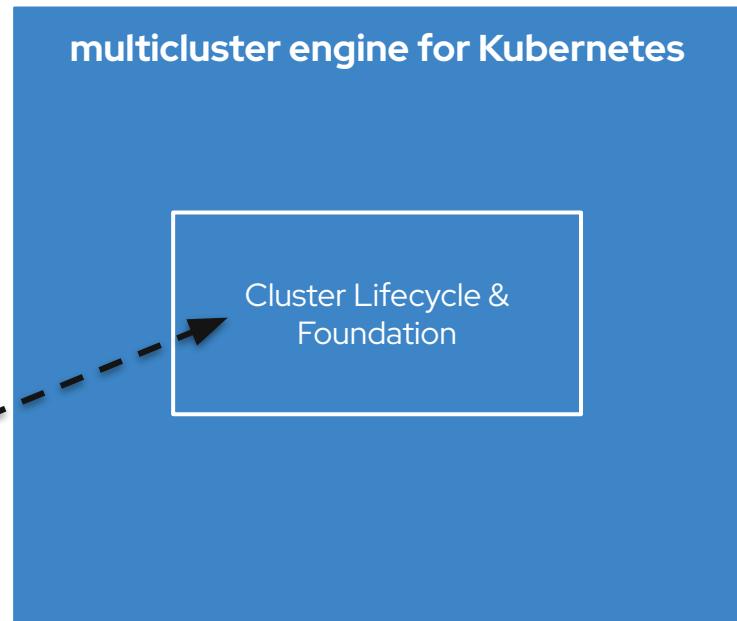
The **multicloud engine for Kubernetes** operator is entitled with OpenShift and it's installed automatically during a RHACM install.



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**.

multicluster engine for
Kubernetes
provided by Red Hat

Foundational components for
central management of multiple
OpenShift Container Platform...

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

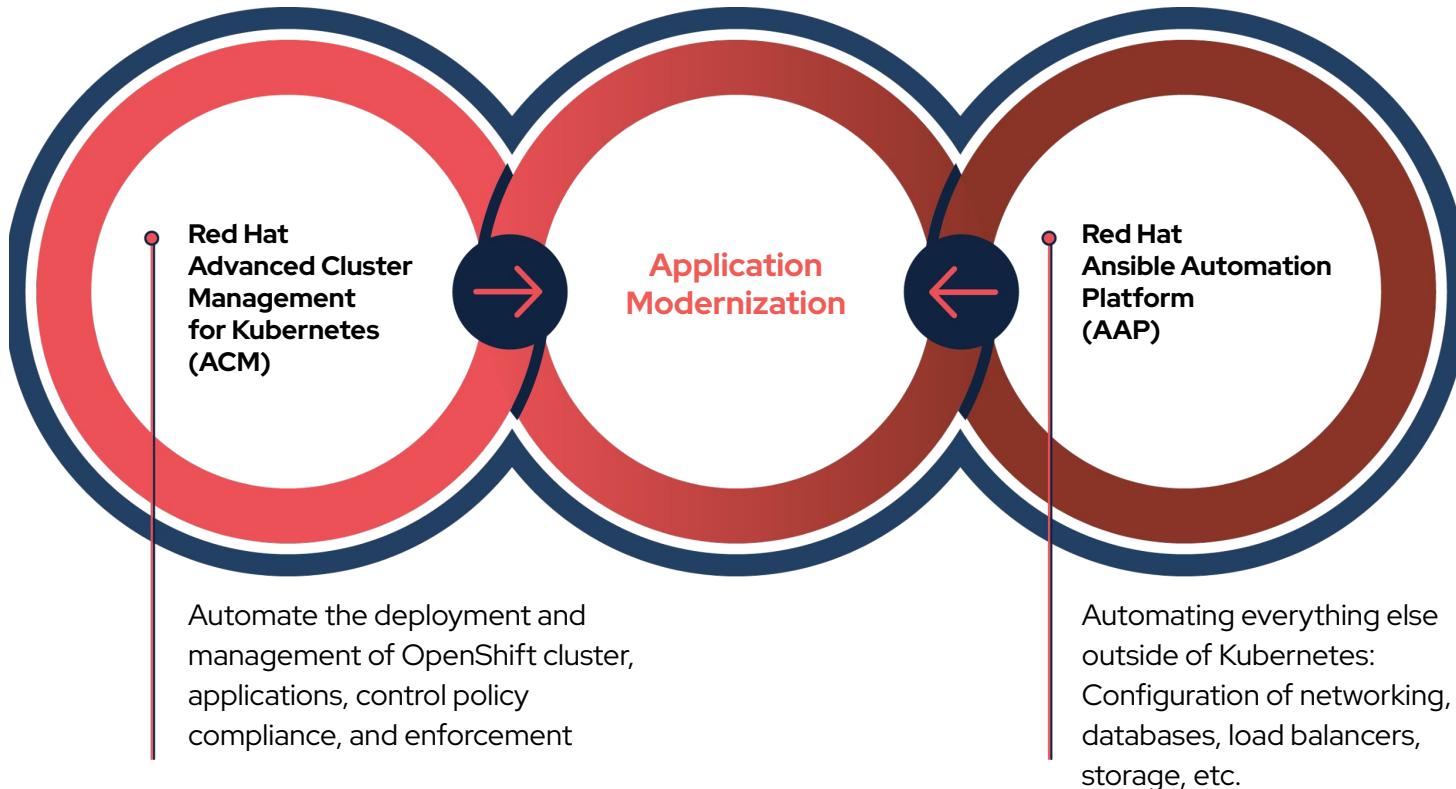
Hive

Central Infrastructure
Management & Infra Operator

Hosted Control Planes

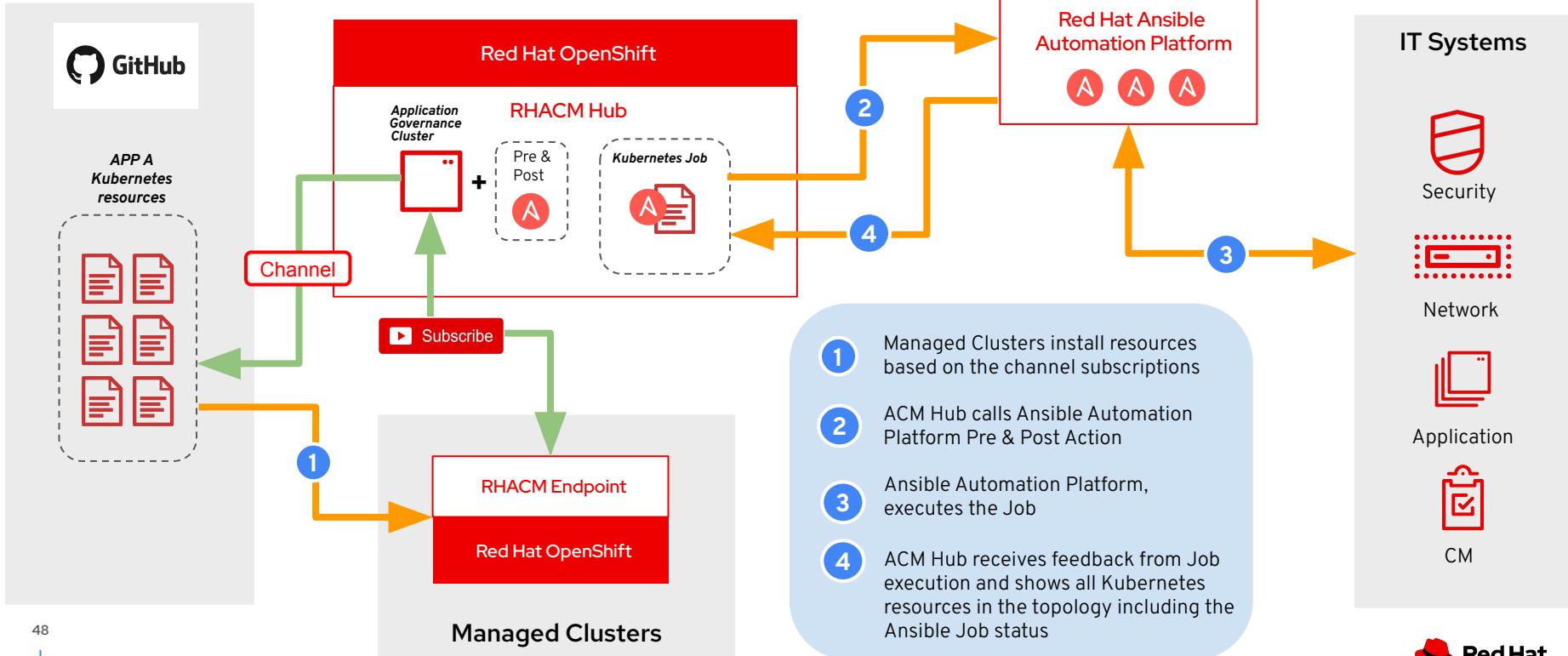


Application modernization driven by automation of Kubernetes and beyond....



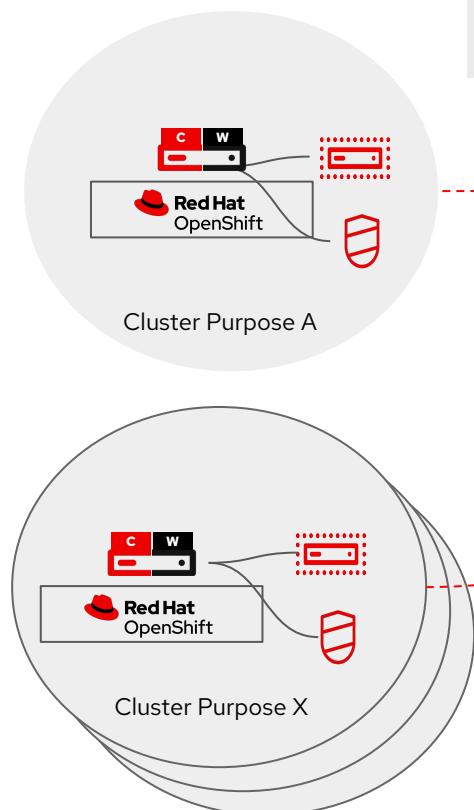
Complete Automation Platform

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



Complete Automation Platform

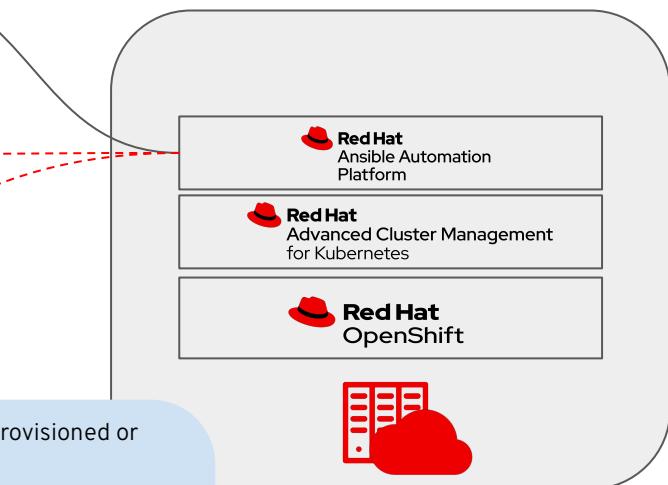
Use Case: Cluster Lifecycle Management



Management and
Application deployment

- 1
- 2
- 3
- 4

Managed Clusters provisioned or imported
ACM hub calls Ansible Automation Platform according to predefined pre & post provisioning actions.
Ansible Automation Platform executes job to update security, storage and more
Provisioning status and Ansible job execution represented in RHACM

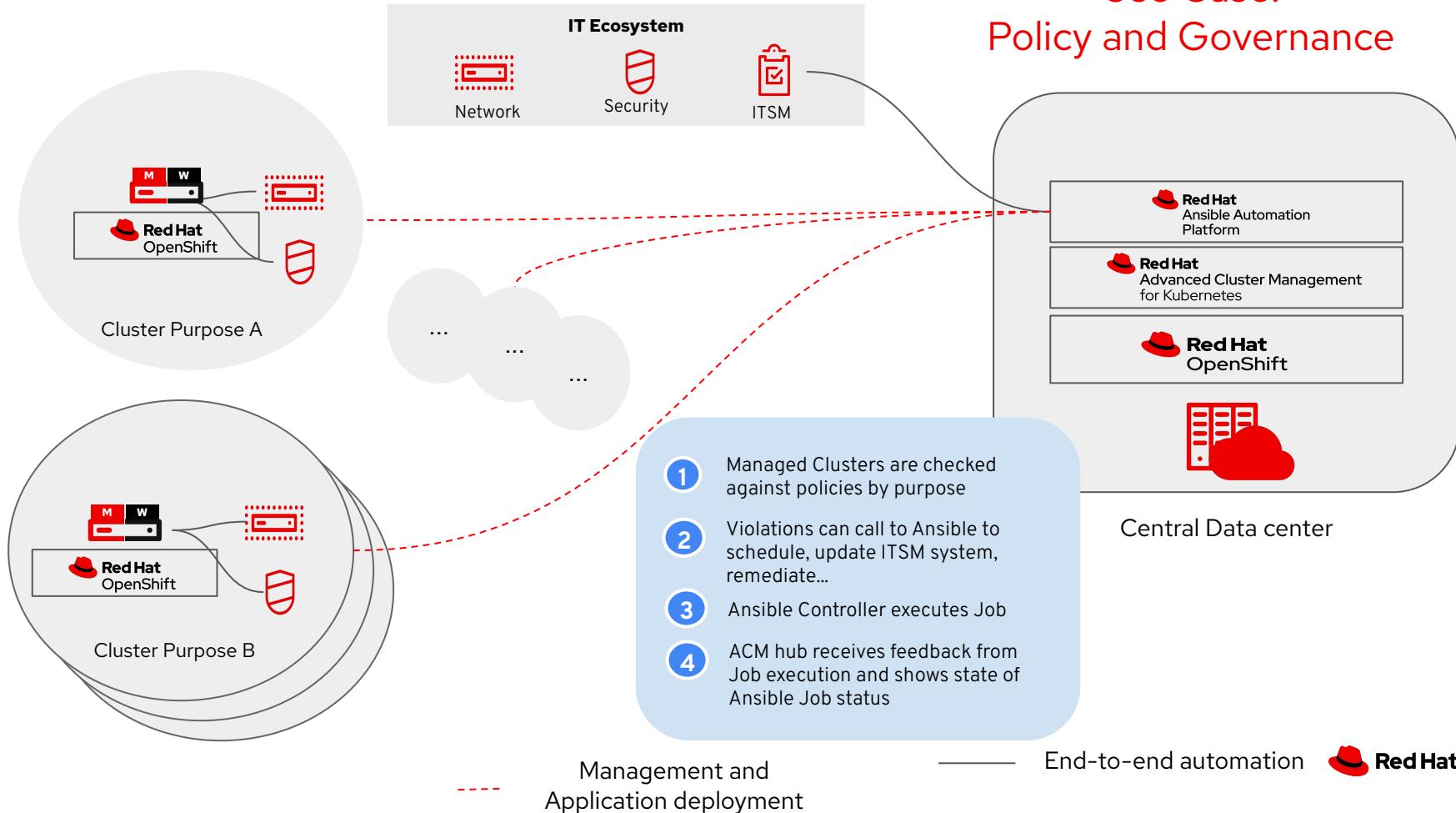


End-to-end automation



Complete Automation Platform

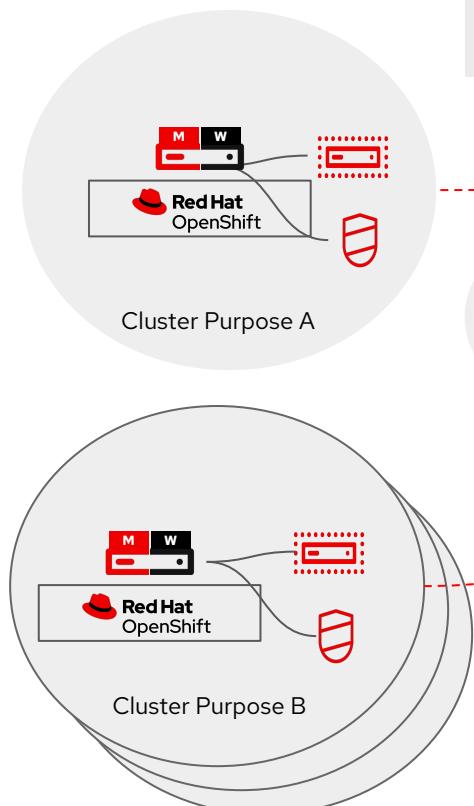
Use Case: Policy and Governance



Complete Automation Platform

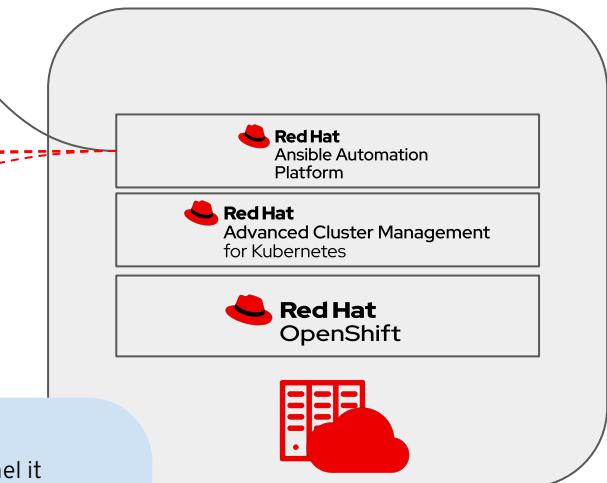
Use Case:

Advanced Application Lifecycle



Management and
Application deployment

- 1 Managed Clusters install resources based on channel it subscribed
- 2 ACM hub call Ansible Controller with Template Job ID define in Application Pre & Post Action
- 3 Ansible Controller executes Job
- 4 ACM hub receives feedback from Job execution and show all Kubernetes resources in topology including Ansible Job status



End-to-end automation





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.

The screenshot shows the Red Hat OpenShift web interface with a dark theme. The left sidebar has sections for Home, Overview, Projects, Search, API Explorer, Events, Operators (OperatorHub, Installed Operators), Workloads, Networking, Storage, and Builds. The main content area is titled 'Overview' and 'Cluster'. It includes sections for 'Getting started resources' (Set up your cluster, Build with guided documentation, Explore new admin features), 'Details' (Cluster API address: https://api.boston-dev02.red-chesterfield.com:643, Cluster ID: abe81fcc-2e44-45be-88c7-25ad320e0122, OpenShift Cluster Manager), 'Status' (Cluster, Control Plane, Operators, Insights, Dynamic Plugins, vSphere connection), and 'Activity' (Ongoing, Recent events, Updated open-cl...).

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