



**Red Hat**

Advanced Cluster Management  
for Kubernetes

# Red Hat Advanced Cluster Management for Kubernetes

Alfred Bach



**Red Hat**

# Introducing!

## Red Hat Advanced Cluster Management for Kubernetes

Robust, Proven, Award Winning



Multicluster Lifecycle  
Management



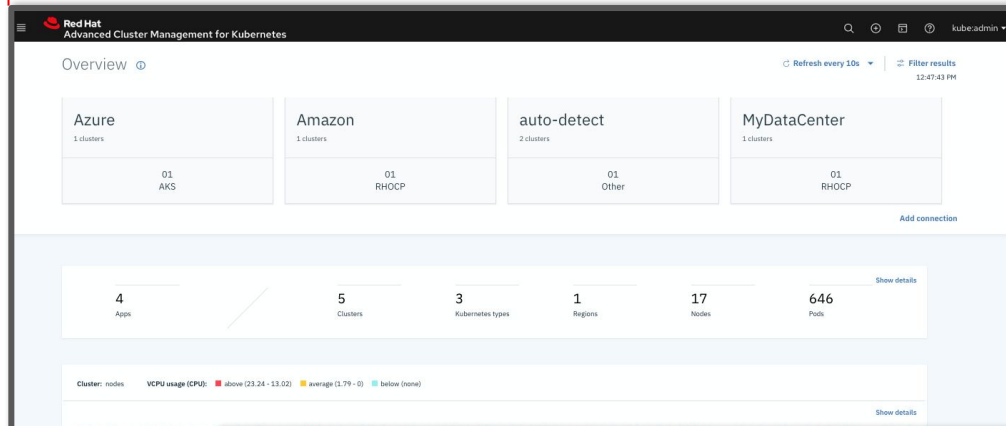
Policy Driven  
Governance, Risk and  
Compliance



Advanced Application  
Lifecycle Management

# Unified Multi-Cluster Management

Single Pane for all your Kubernetes Clusters



Clusters										
Search										
Name	Namespace	Labels	Endpoint	Status	Nodes	Kubernetes Version	Kubernetes Version	Storage	Memory	CPU
exec2-iks	mcm-exec2-iks	cloud=IBM datacenter=dal13 environment=dev name=exec2-iks region=US vendor=IKS	-	Offline	1	3.1.2-dev	v1.11.7-DKS	-	33%	70%
social-dev-1	mcm-social-dev-1	cloud=IBM datacenter=oregon environment=dev name=social-dev-1 owner=marketing region=us-west vendor=ICP	<a href="#">launch</a>	Ready	1	3.1.2	v1.11.5+icp-ee	100%	62%	45%
social-dev-2	mcm-social-dev-2	cloud=IBM datacenter=oregon environment=dev name=social-dev-2 owner=marketing region=us-west vendor=ICP	<a href="#">launch</a>	Offline	1	3.1.2	v1.11.1+icp-ee	100%	48%	47%
social-dev-gke	social-dev-gke	cloud=Google datacenter=us-central1-a environment=dev name=social-dev-gke owner=marketing region=US vendor=GKE	-	Ready	1	3.1.2-dev	v1.11.7-gke.12	-	6%	22%
social-prod-1	mcm-social-prod-1	cloud=IBM datacenter=oregon environment=Prod name=social-prod-1 owner=marketing region=us-west vendor=ICP	<a href="#">launch</a>	Ready	1	3.1.2	v1.11.1+icp-ee	100%	52%	34%
social-prod-eks	social-prod-eks	cloud=AWS datacenter=us-east-1 environment=Prod name=social-prod-eks owner=marketing	-	Ready	1	3.1.2-dev	v1.11.8-eks-7c34c0	-	1%	10%

- **Centrally** create, update and delete Kubernetes clusters **across multiple** private and public clouds
- 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

- **Centrally** set & enforce policies for security, applications, & infrastructure
- Quickly **visualize** detailed **auditing** on configuration of apps and clusters
- Built-in **CIS** compliance policies and audit checks
- **Immediate** visibility into your compliance posture based on **your** defined standards

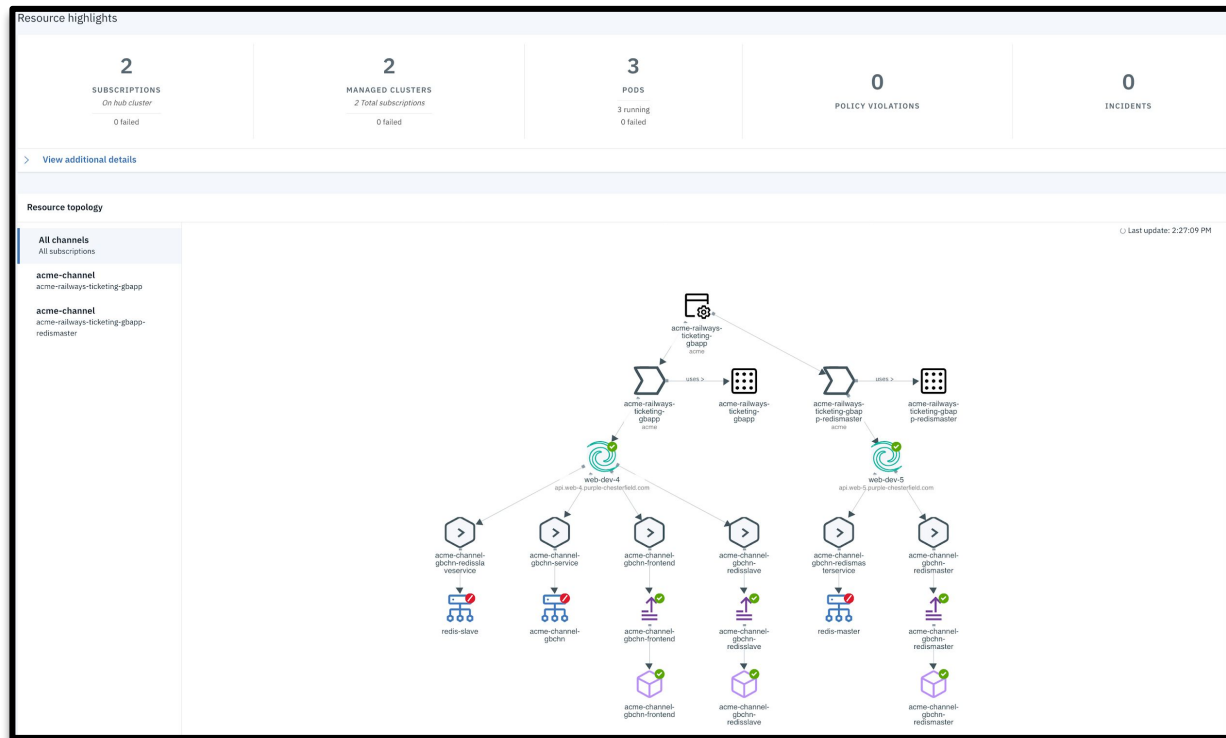
The screenshot displays the Red Hat Policy Guard interface. At the top, there are five tabs: POLICY VIOLATIONS (3), CLUSTER VIOLATIONS (1), HIGH SEVERITY FINDINGS (1), MEDIUM SEVERITY FINDINGS (1), and LOW SEVERITY FINDINGS (0). The main content area is divided into two sections: 'Top violations' and 'Top security findings'. The 'Top violations' section lists three policies: policy-cis, policy-gic, and policy-role, each with a count of 1. The 'Top security findings' section shows a 'Policy violation finding' with a count of 2, and a message stating 'No other security findings'. Below these sections is a 'Most impacted controls' section. On the left, there is a 'Key' section with 'Policy violations' and 'Security findings' indicators, and a 'Standard' dropdown menu set to 'AS'. A 'Policy summary' section is also visible. The bottom section, titled 'compliancePolicy', shows a table with columns: Name, Compliance Type, API version, Kind, Last Transition, and Compliant. The table lists three policies: restricted-mcm, deny-from-other-namespaces, and mem-limit-range. To the right of the table, there is a code editor showing the YAML configuration for the 'mem-limit-range' policy, including fields like 'podSelector', 'complianceType', 'objectDefinition', 'kind', 'metadata', 'spec', 'limits', 'default', 'memory', 'defaultRequest', 'memory', 'type', and 'remediationAction'.

Name	Compliance Type	API version	Kind	Last Transition	Compliant
restricted-mcm	musthave	policy/v1beta1	PodSecurityPolicy	-	-
deny-from-other-namespaces	musthave	networking.k8s.io/v1	NetworkPolicy	-	-
mem-limit-range	musthave	v1	LimitRange	-	-

```
11 - from:
12 - podSelector: {}
13 - podSelector:
14   matchLabels: null
15 - complianceType: musthave
16 - objectDefinition:
17   apiVersion: v1
18   kind: LimitRange
19   metadata:
20     name: mem-limit-range
21   spec:
22     limits:
23       - default:
24         memory: 512M
25         defaultRequest:
26         memory: 256M
27         type: Container
28     remediationAction: enforce
```

# Advanced Application Lifecycle Management

Simplify your Application Lifecycle



- **Easily** Deploy Applications at **Scale**
- Deploy Applications from **Multiple** Sources
- Quickly **visualize** application relationships **across** clusters and those that **span** clusters

## 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.

#### Ease Compliance

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

#### Increase Application Availability

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

#### Reduced Costs

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

# 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 clusters regardless of where they reside (on-prem, across public clouds) using a single control plane?



# Multi-Cluster Lifecycle Management

## Overview

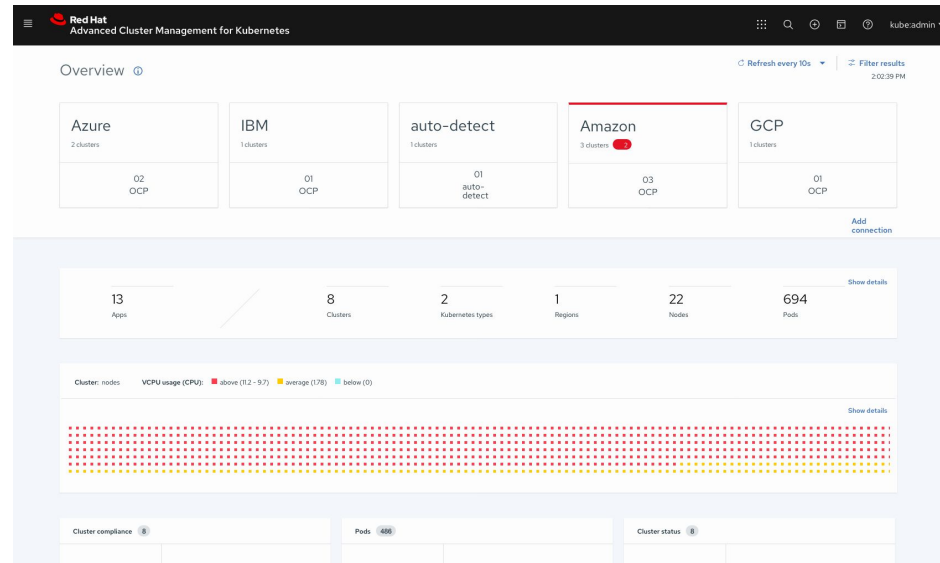
- Manage any Kubernetes compliant cluster
  - OpenShift 3.11, 4.1.x - 4.4.x
  - Public cloud hosted: OCP
  - Public cloud managed kubernetes: EKS, AKS, GKE, IKS
- Search, find and modify kubernetes resources across the management domain.
- IT Management as code with **YAML**
- See high level summaries 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



IT Operations



DevOps/SRE

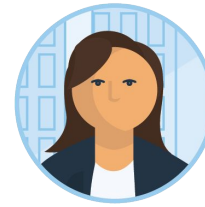


# Multi-Cluster Lifecycle Management

## Creating & Importing Clusters



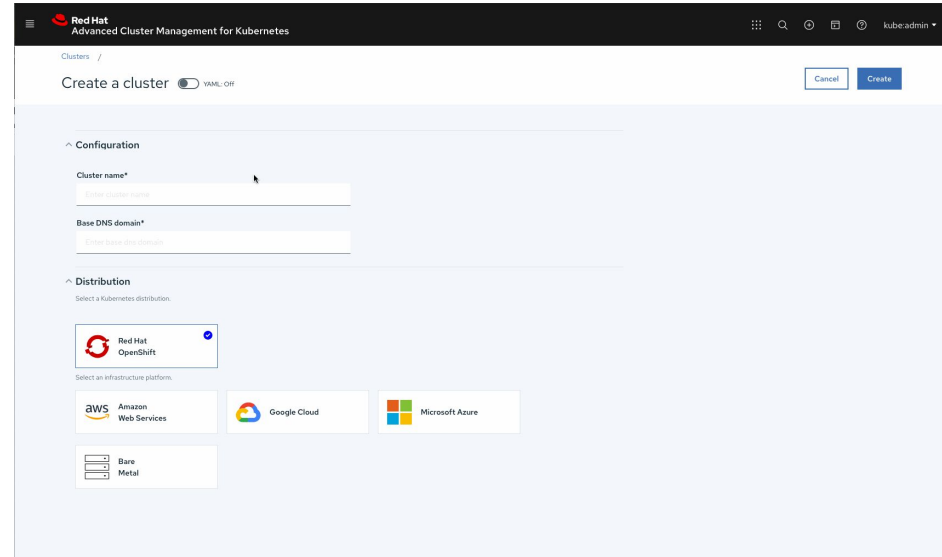
IT Operations



DevOps/SRE



- **Create, Upgrade** and **Destroy** OCP clusters running on **Bare-metal** as well as public cloud
- 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



# Multi-Cluster Lifecycle Management

## Dynamic Search



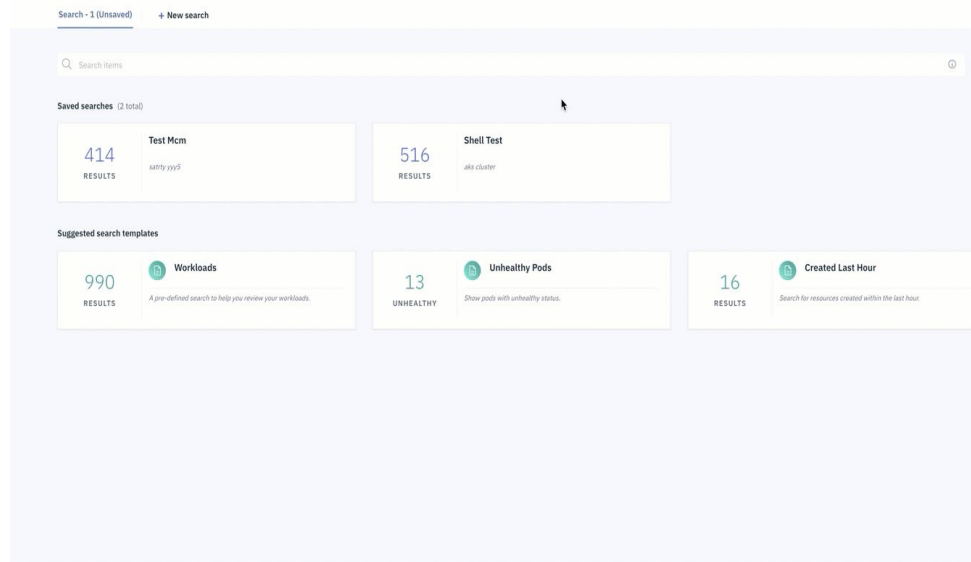
IT Operations



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



# Multi-Cluster Lifecycle Management

## Visual Web Terminal



IT Operations



DevOps/SRE



- Interactive terminal combines command input with visual output
- One **Terminal** for **all**
- Works with **helm**, **kubect****l**, **oc**, **istioct****l**
- Single interface for multi-cluster
- Drive ops directly from dashboards
- Bash commands allow for grep

Red Hat  
Advanced Cluster Management for Kubernetes

Welcome, let's get started.

Red Hat Advanced Cluster Management for Kubernetes provides the tools and capabilities to address various challenges with managing multiple clusters and consoles, distributed business applications, and inconsistent security controls across Kubernetes clusters that are deployed on-premises, or across public clouds.

**End-to-end visibility**  
System alerts and access to critical application metrics and overall system health. Providing an operational dashboard for SREs to search, identify, and resolve issues impacting distributed workloads.  
[Go to Overview](#)

**Cluster lifecycle**  
Creates, updates, scale, and remove clusters reliably, consistently using an open source programming model that supports and encourages Infrastructure as Code best practices and design principles.  
[Go to Clusters](#)

**Application lifecycle** Technology Preview  
Define a business application using open standards and deploy the applications using placement policies that are integrated into existing CI/CD pipelines and governance controls.  
[Go to Applications](#)

**Governance, Risk, and Compliance**  
Use policies to automatically configure and maintain consistency of security controls required by industry or other corporate standards. Prevent unintentional or malicious configuration drift that might expose unwanted and unnecessary threat vectors.  
[Go to Governance and risk](#)

Easy, simple, and secure.

Easy to use and simple to understand, Red Hat Advanced Cluster Management for Kubernetes provides the following mission critical capabilities based on open source projects:

<https://multicloud-console.apps.hotel.demo.red-hat-external.com/hui> [Kubernetes](#) [Policies](#) [Cluster landscape](#)



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 Driven Governance Risk and Compliance

## Architecture Overview



Security Ops

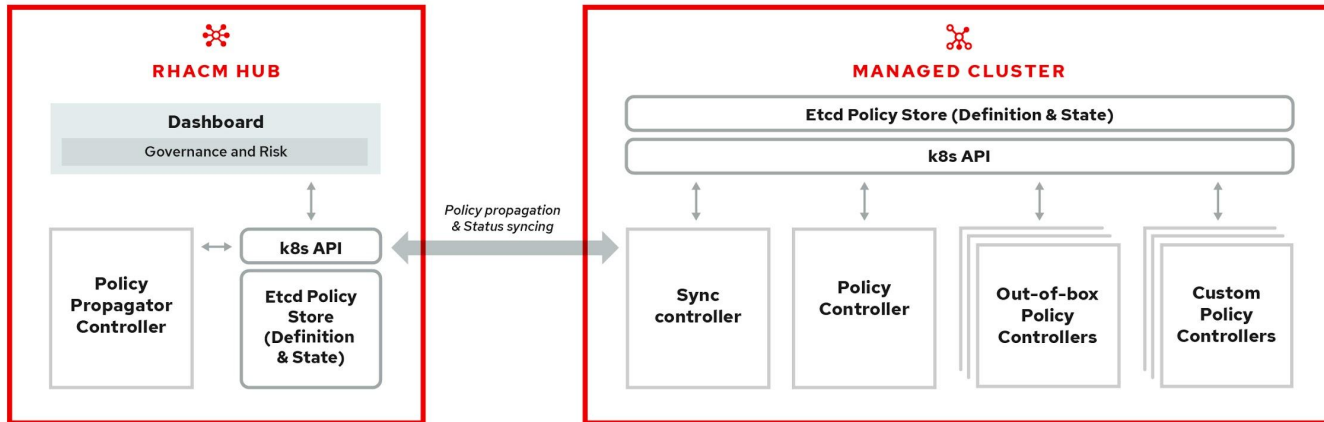


IT Operations



### 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 and an extensible policy framework



# Policy based Governance, Risk and Compliance

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



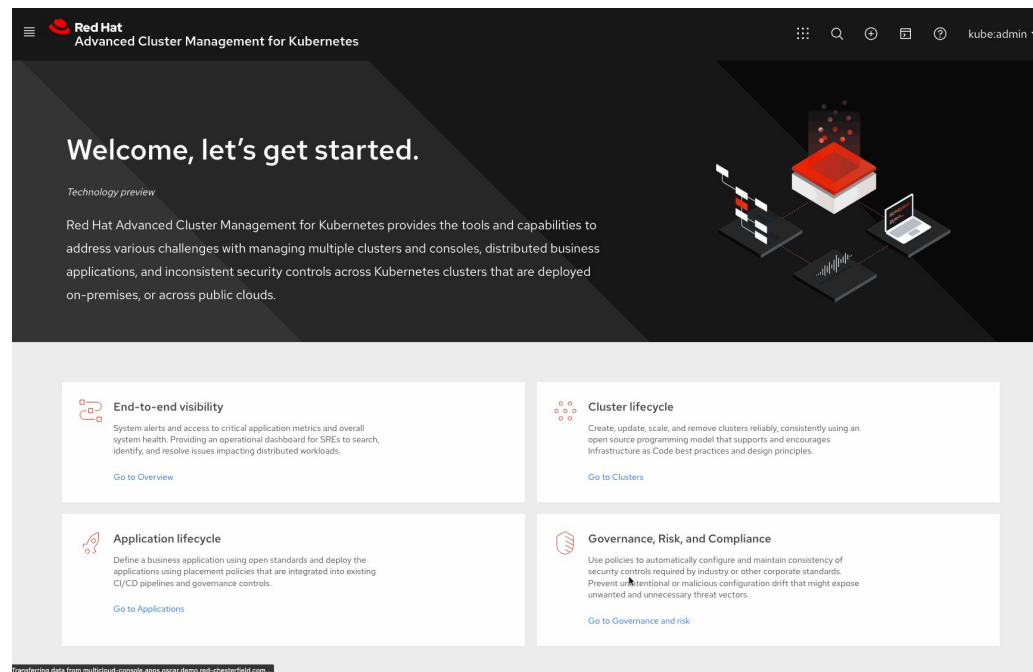
Security Ops



IT Operations



- Set and enforce policies for security, applications, & infrastructure
- Deep visibility for auditing configuration of apps and clusters
- Unique policy capabilities around CIS compliance
- Categorize violations based on your standards for immediate visibility into your compliance posture



# Policy based Governance, Risk and Compliance

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



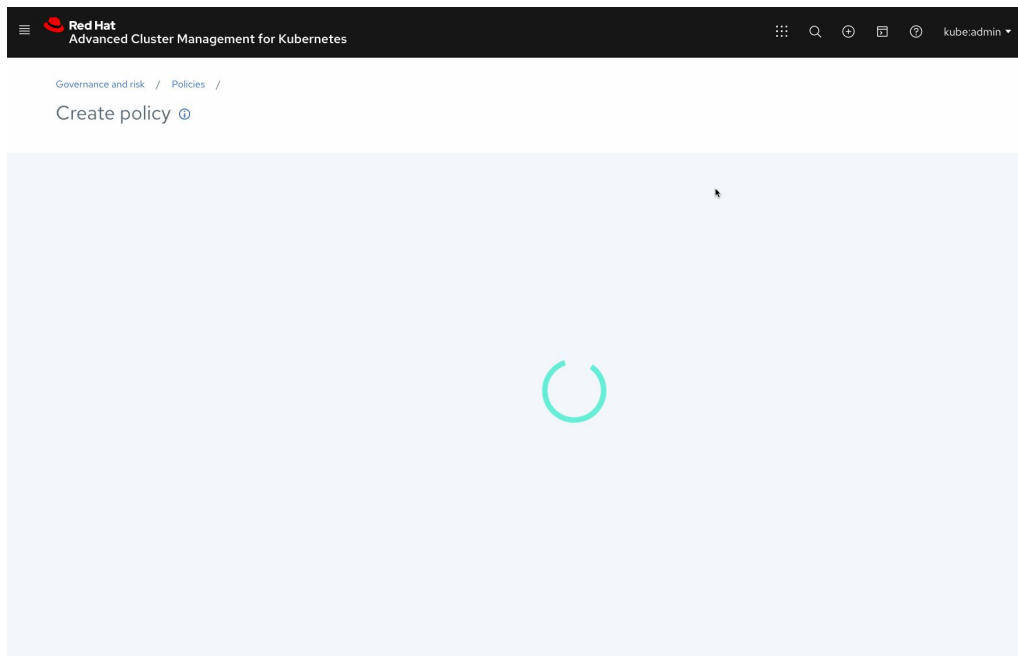
Security Ops



IT Operations



- 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





# 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.

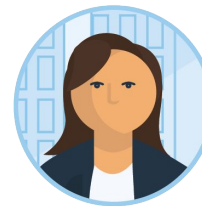


IT Operations

- 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

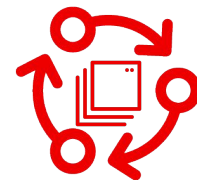
## Simplify your Application Lifecycle



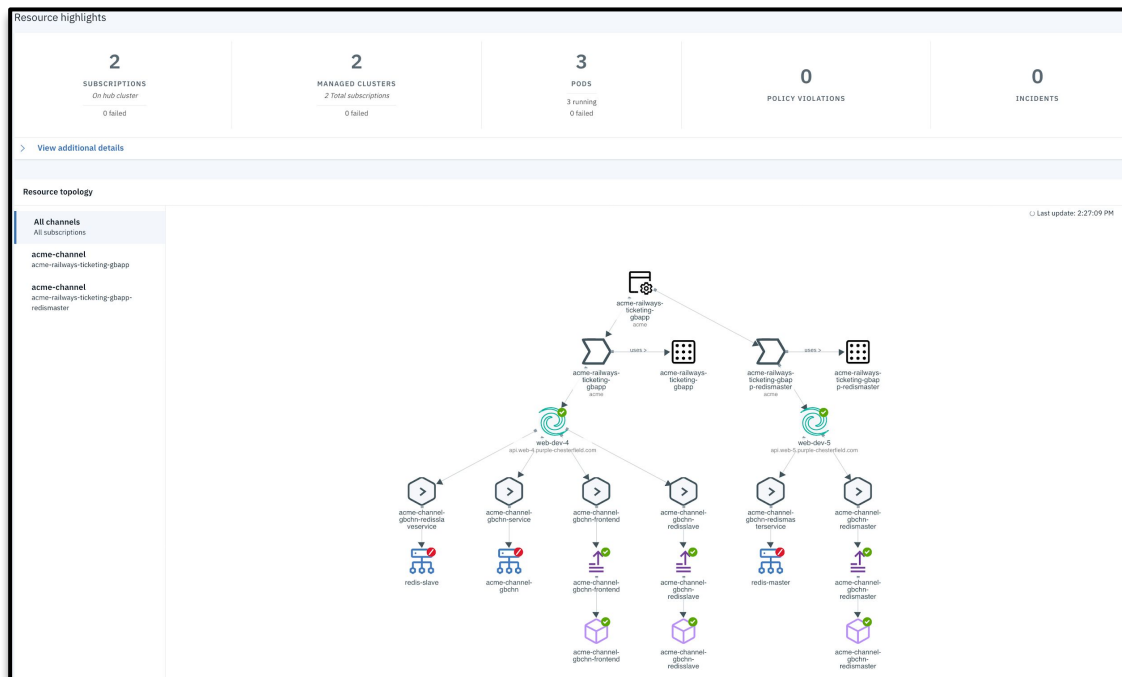
DevOps/SRE



IT Operations



- Deploy Applications at Scale
- Deploy Applications from Multiple Sources and Clusters
- Quickly Visualize Application Relationships
- Using the subscription & channel model, the latest application revisions are delivered to appropriate clusters, automatically.



# Advanced Application Lifecycle Management

## Subscriptions Bring Enterprise to Kubernetes



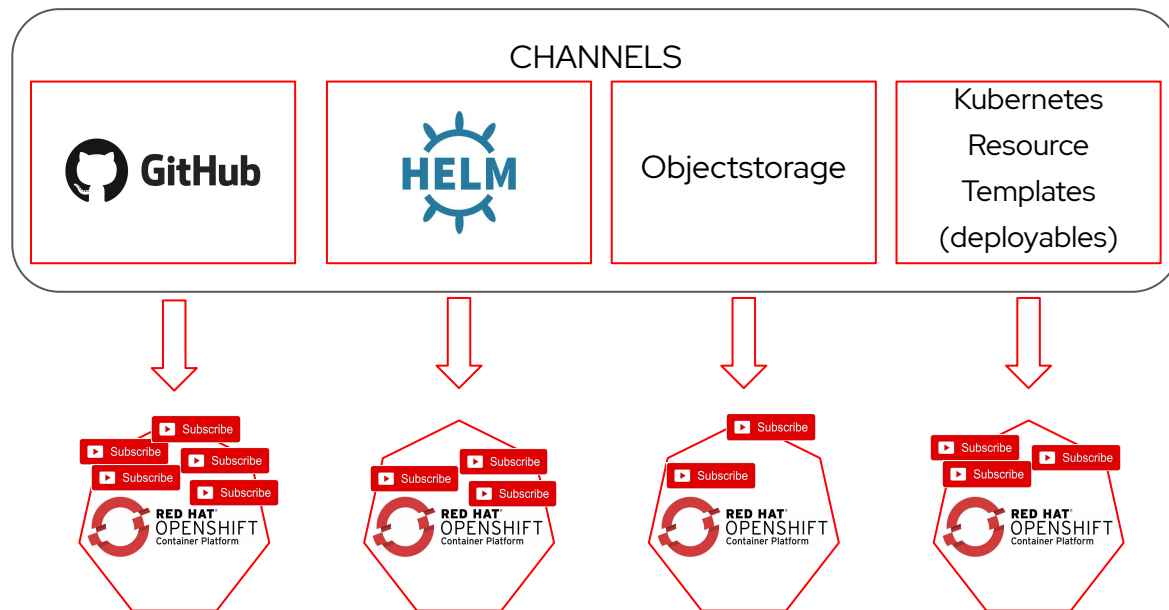
DevOps/SRE



IT Operations



- Extending the best of Enterprise into a desired state methodology
- Time Windows: New releases during your maintenance windows
- Rolling Updates: Control the rate and load on your growing infrastructure



# Advanced Application Lifecycle Management

## GitOps as the source of truth



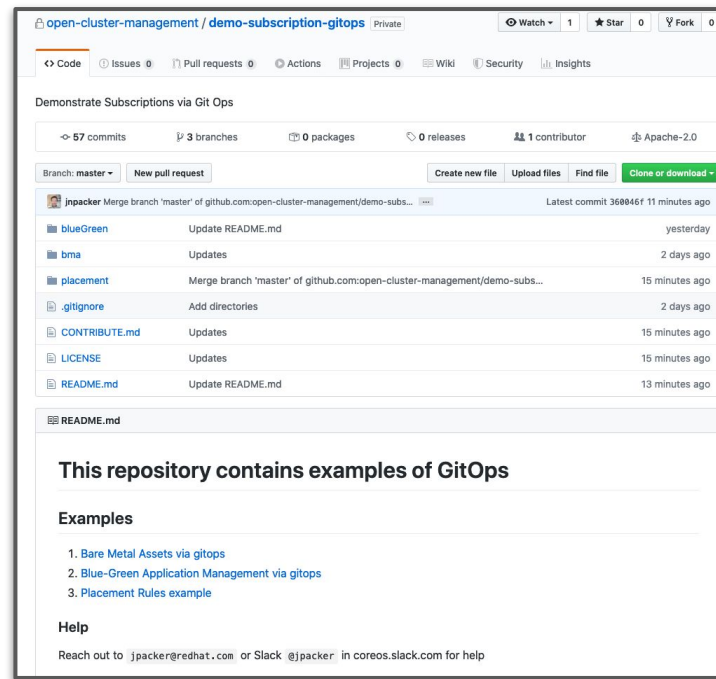
DevOps/SRE



IT Operations



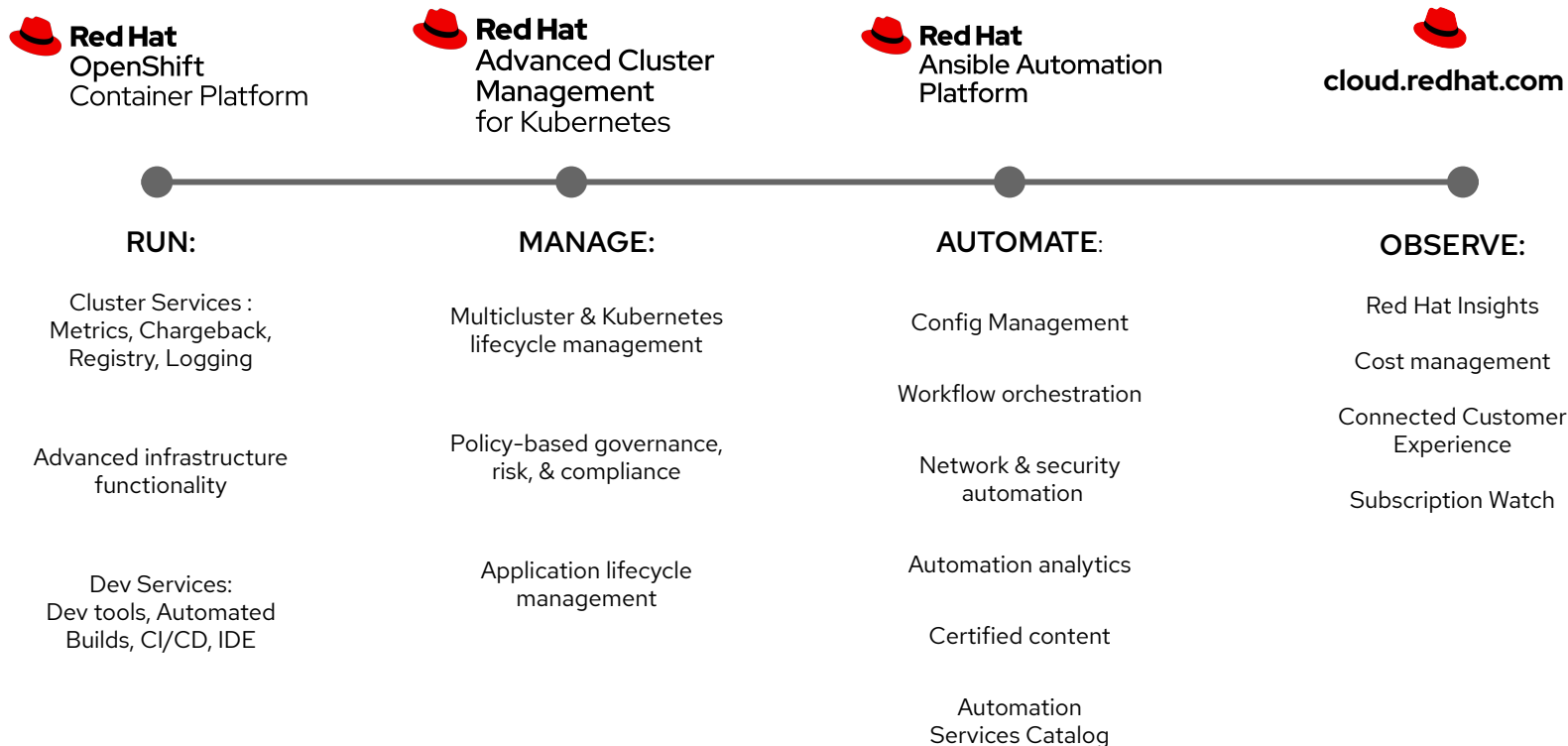
- Create, modify & delete, just as you would any source code. Git becomes your source of truth controlling your data center.
- Have a record of who, what & when for every change precipitated in your environments
- Through code Reviews & Approvals, take full control of all changes to your data center(s)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



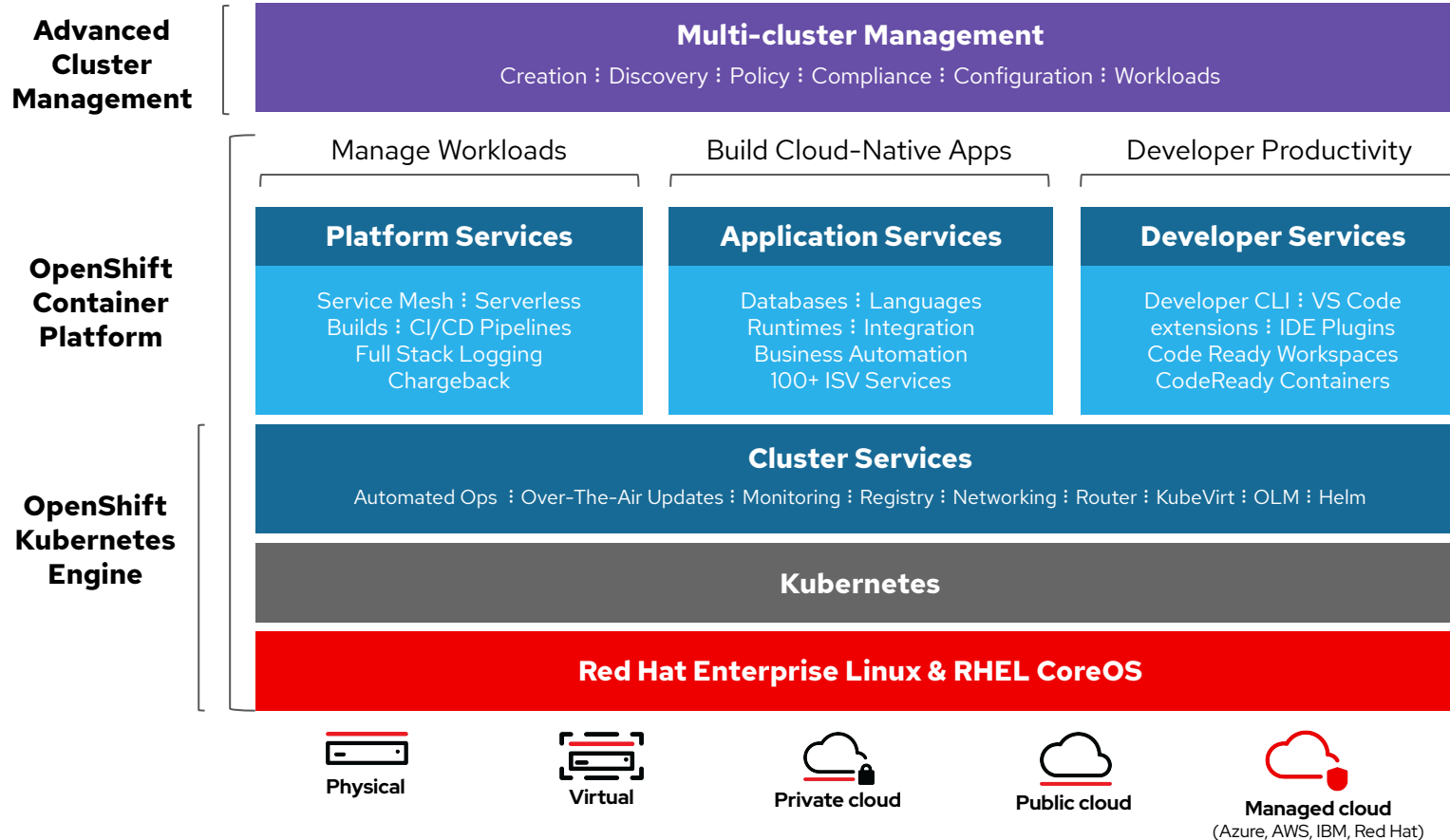
<https://github.com/open-cluster-management/demo-subscription-gitops>

# How it works with Openshift

# Supporting Application Modernization



# Draw Me a Picture!



# Architecture

Red Hat Advanced Cluster Management For  
Kubernetes



# Architecture Overview



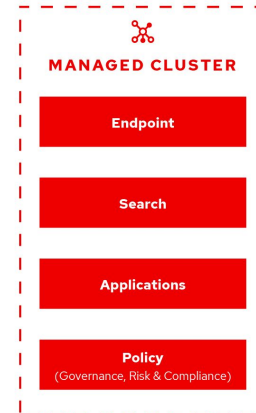
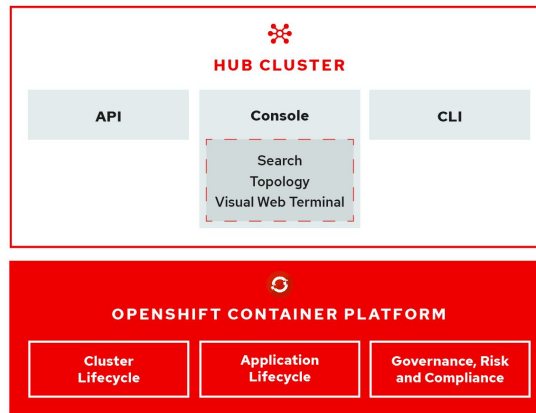
IT Operations

## Hub Architecture and Components

- RHACM uses the multicluster-hub operator and runs in the open-cluster-management namespace

## Managed Cluster Architecture and Components:

- RHACM managed clusters use the multi-cluster endpoint operator which runs in the multicluster-endpoint namespace



# Installation

Red Hat Advanced Cluster Management For  
Kubernetes

# Installation and Foundation

## Operator Install for Hub

### Hub Cluster

- Operator based installation
- Available on OperatorHub.io
- Requires OCP 4.3.5 or OCP 4.4.x

### Manage Kubernetes compliant clusters

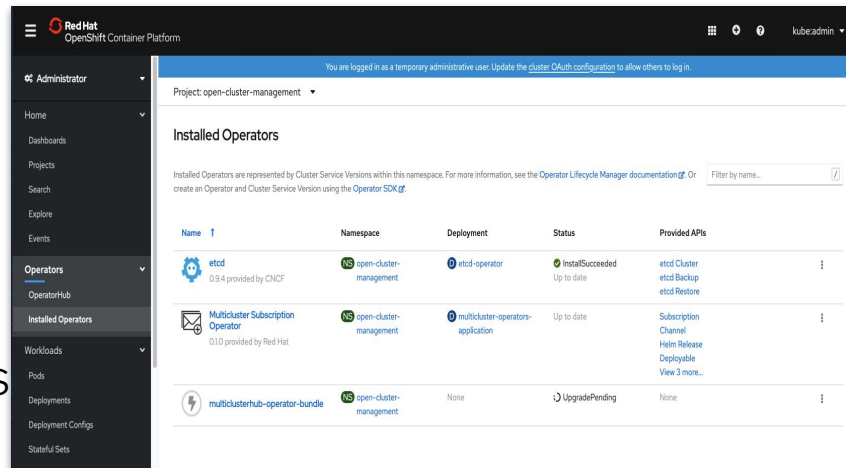
- OpenShift 3.11, 4.1.x - 4.4.x
- Public cloud hosted: OCP
- Public cloud managed kubernetes: EKS, AKS, GKE, IKS

### High Availability

- Supports OCP Availability Zone
- Limitation for Search component based on RedisGraph

### Resource Requirements

- Test: 1 master, 2 workers, 4CPU and 16GB RAM
- Production: 3 masters, 16CPU and 128GB RAM
  - Production requirements vary based on number of clusters in the management domain and types of workloads being run





IT Operations

### Managed Cluster

- The multicluster-endpoint operator controls the deployment of components on the managed cluster.
- List of included components:
  - Application Manager - agent for application management
  - Connection Manager - allows components to connect to the hub
  - Work Manager - executes remote actions from the hub
  - Policy Controller - agent for security GRC
  - Search Collector - agent for dynamic search
  - Service Registry - service discovery
  - IAM Policy controller - controller for IAM Policy
  - Certificate Policy Controller - controller for certificate expiration policy
  - CIS Policy Controller - controller for CIS policy

# 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.



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[twitter.com/RedHat](https://twitter.com/RedHat)