

Red Hat Advanced Cluster Management for Kubernetes

Master Deck - OpenShift Anwendertreffen 26. Mai 2020

Matthias Pfützner
Solution Architect - Cloud

AGENDA

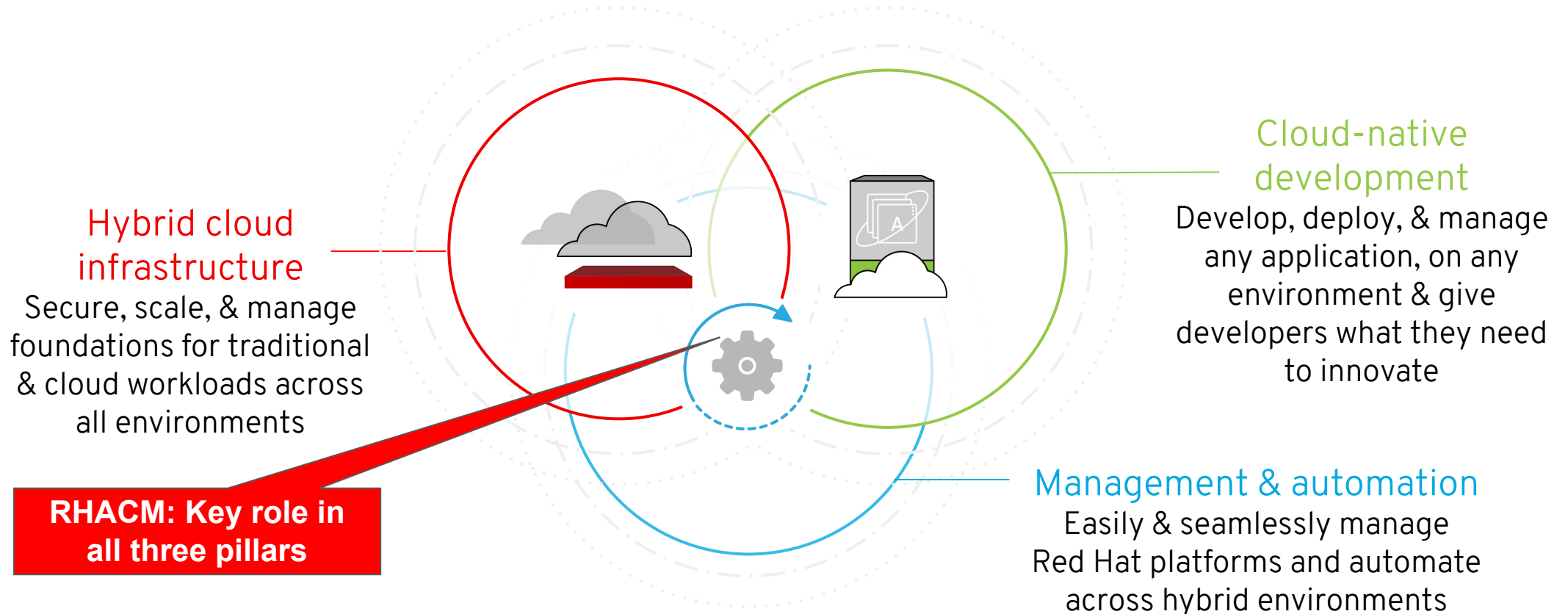
- ▶ Market Trends and Challenges
- ▶ Key Personas
- ▶ Introducing Red Hat Advanced Cluster Management for Kubernetes
- ▶ Detailed use cases
- ▶ ACM and OpenShift
- ▶ Architecture Overview
- ▶ Installation

Market Trends and Challenges

The Three Pillars of Red Hat

Open hybrid cloud

Red Hat's strategy and vision for its portfolio of software, tools, and services built in the open source development model and designed for future architectures that are open, secure, and agile across hybrid, multicloud.



Why Advanced Cluster Management Matters

App Modernization is Top Priority

•

Kubernetes is THE platform Modernization

•

Enterprises rapidly adopting Kubernetes

•

Need for multiple clusters required - adds scale,
scope, size, complexity

•

Not all Kubernetes solutions are equal

•

Multicloud management is hard - and
complicated

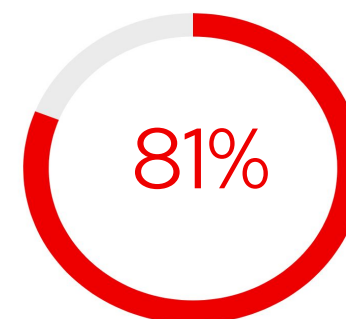
Hybrid, Multi-Cloud Management is Really Hard!!

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



Using multiple infrastructure clouds



Using multiple public clouds and 1 or more private/dedicated clouds

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

Source: IDC Multicloud Management Survey, 2019: Special Study, Doc # US45020919, April 2019

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, multi-cloud, or edge deployments.*

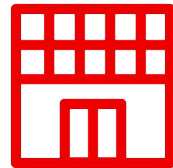
Source: Assessing Patterns for Deploying Distributed Kubernetes Clusters doc # G00465217, by Tony Iams

Where is the growth in cluster deployments?



Small Scale Dev teams

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



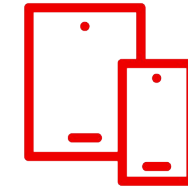
Medium Scale Organizations

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



Large Scale

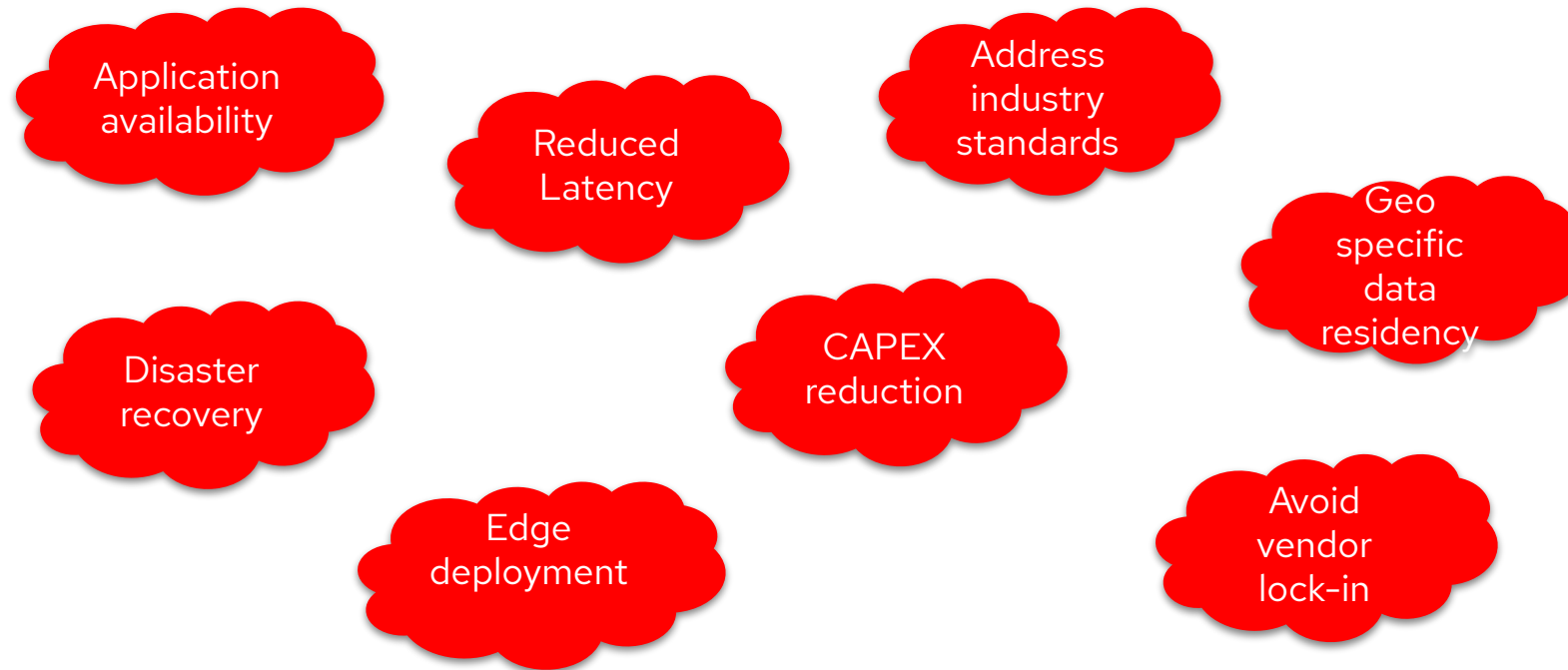
- Global organizations with 100s of clusters, hosting thousand of applications
- Large Retail with 1000s of stores



Edge Scale Telco

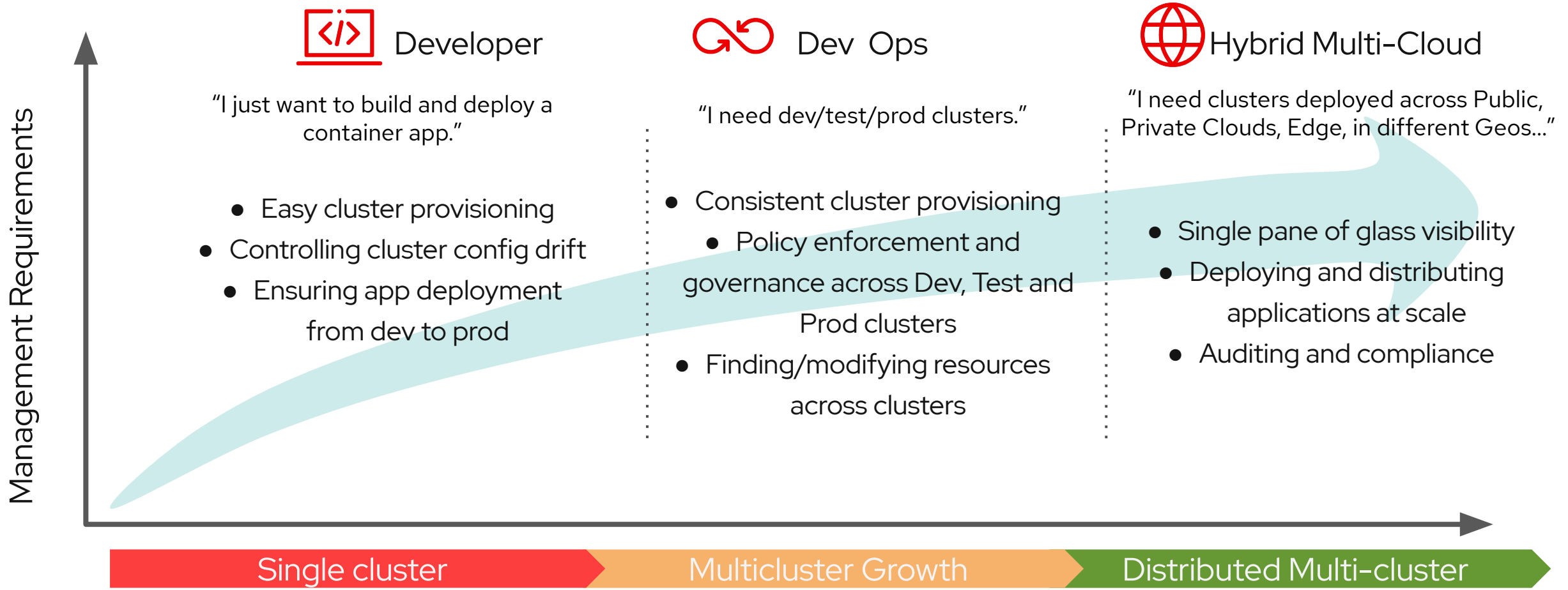
- 100s of zones, 1000s of clusters and nodes across complex topologies

Reasons for Deploying Clusters



Multi-cluster Management Challenges:

How do I normalize and centralize key functions across environments?



Key Personas

Key Personas - IT Operations



- How can I manage the lifecycle of multiple clusters regardless of where they reside (on-prem, across public clouds) using a single control plane?
- How can I quickly get to the root cause of failed components?
- How do I monitor usage across multiple clouds?

Key Personas - SRE/DevOps



- 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/ deprovisioning of my clusters?
- How can I automate the placement of workloads based on capacity, policy?
- How can I automate pushing application updates from dev to prod?

Key Personas - SecOps



- How do I ensure all my clusters are compliant with my defined policies?
- How do I set consistent security policies across diverse environments and ensure enforcement?
- How do I get alerted on any configuration drift and remediate it?

Introducing Red Hat Advanced Cluster Management for Kubernetes

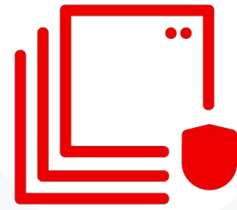
Introducing!

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

Overview

Azure 1 clusters
01 AKS

Amazon 1 clusters
01 RHOC

auto-detect 2 clusters
01 Other

MyDataCenter 1 clusters
01 RHOC

4 Apps

5 Clusters

3 Kubernetes types

1 Regions

17 Nodes

646 Pods

Cluster compliance 5

100% Compliant

VCPU 94

Used 38 | 40%

Clusters

Name	Namespace	Labels	Endpoint	Status	Nodes	Kubernetes Version	Storage	Memory	CPU
exec2-iks	mcm-exec2-iks	cloud=IBM datacenter=dat13 environment=Dev name=exec2-iks region=US vendor=IKS	-	Offline	1	3.1.2-dev	-	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	launch	Ready	1	3.1.2	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=ICP4Data	launch	Offline	1	3.1.2	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	-	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	launch	Ready	1	3.1.2	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	-	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

The dashboard provides a high-level overview of security posture. It features five main metrics: 3 Policy Violations, 1 Cluster Violation, 1 High Severity Finding, 1 Medium Severity Finding, and 0 Low Severity Findings. Below these metrics, there are two main sections: 'Top violations' and 'Top security findings'. The 'Top violations' section lists three items: 'policy-cis', 'policy-grc', and 'policy-rate', each with a count of 1. The 'Top security findings' section shows one 'Policy violation finding' with a count of 2, and a message stating 'No other security findings'.

This section provides a detailed view of a 'compliancePolicy' object template. It includes a table of fields, a code editor showing the underlying YAML configuration, and a table of object templates.

Type	Detail
Name	policy-prod
Message	-
Status	-
Enforcement	-
Exclude Namespaces	kube*
Include Namespaces	default

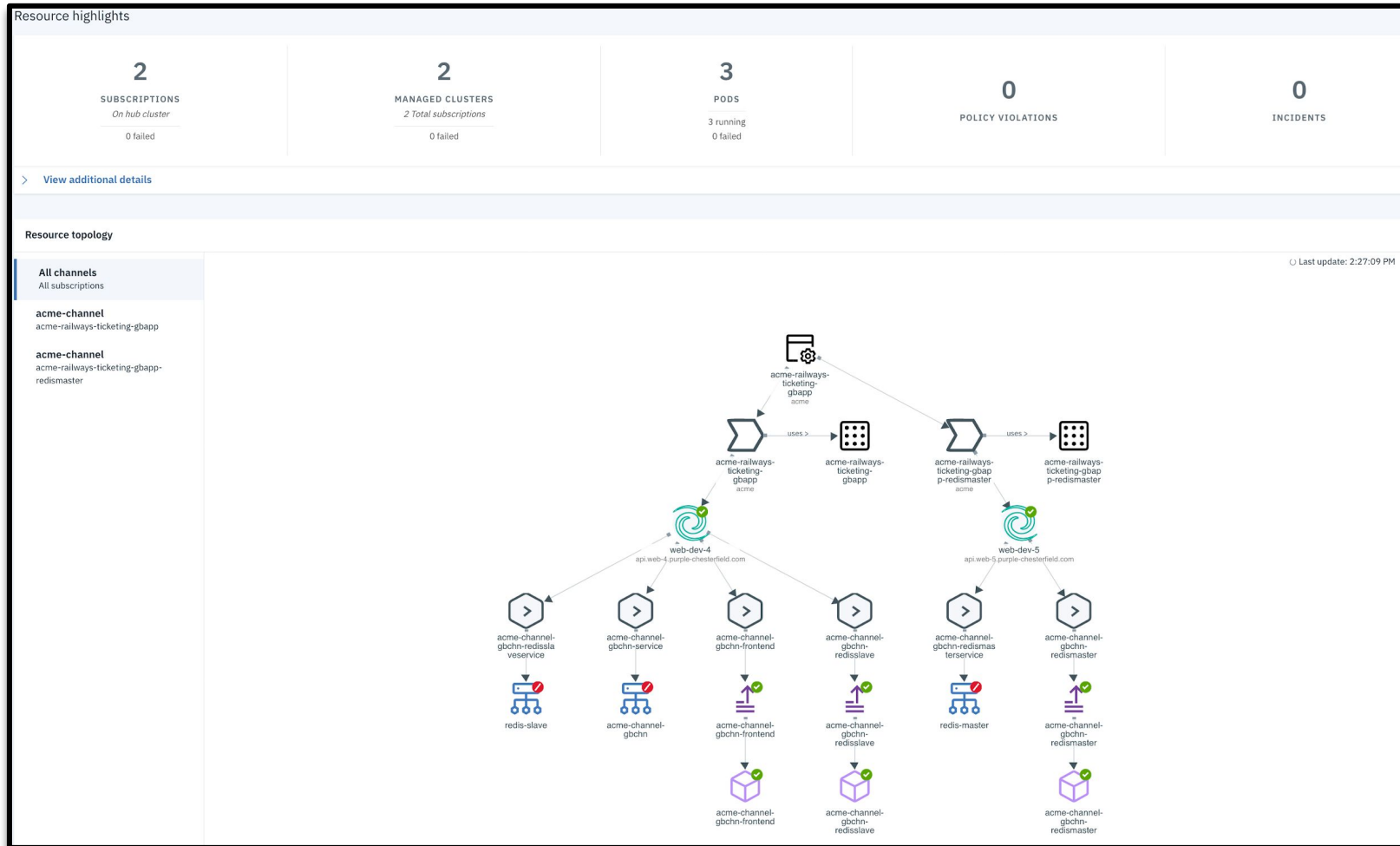
```
51 - from:
52   - podSelector: {}
53   podSelector:
54     matchLabels: null
55 - complianceType: musthave
56   objectDefinition:
57     apiVersion: v1
58     kind: LimitRange
59     metadata:
60       name: mem-limit-range
61     spec:
62       limits:
63         - default:
64             memory: 512Mi
65           defaultRequest:
66             memory: 256Mi
67         type: Container
68     remediationAction: enforce
69
```

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	-	-

- **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

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

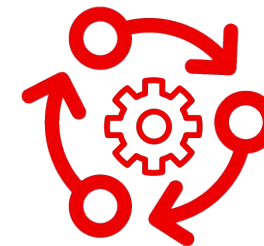
Placement rules can allow quick deployment of clusters and applications across distributed locations for availability, capacity, and security reasons.

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?

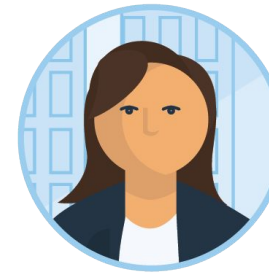
Multi-Cluster Lifecycle Management

Overview

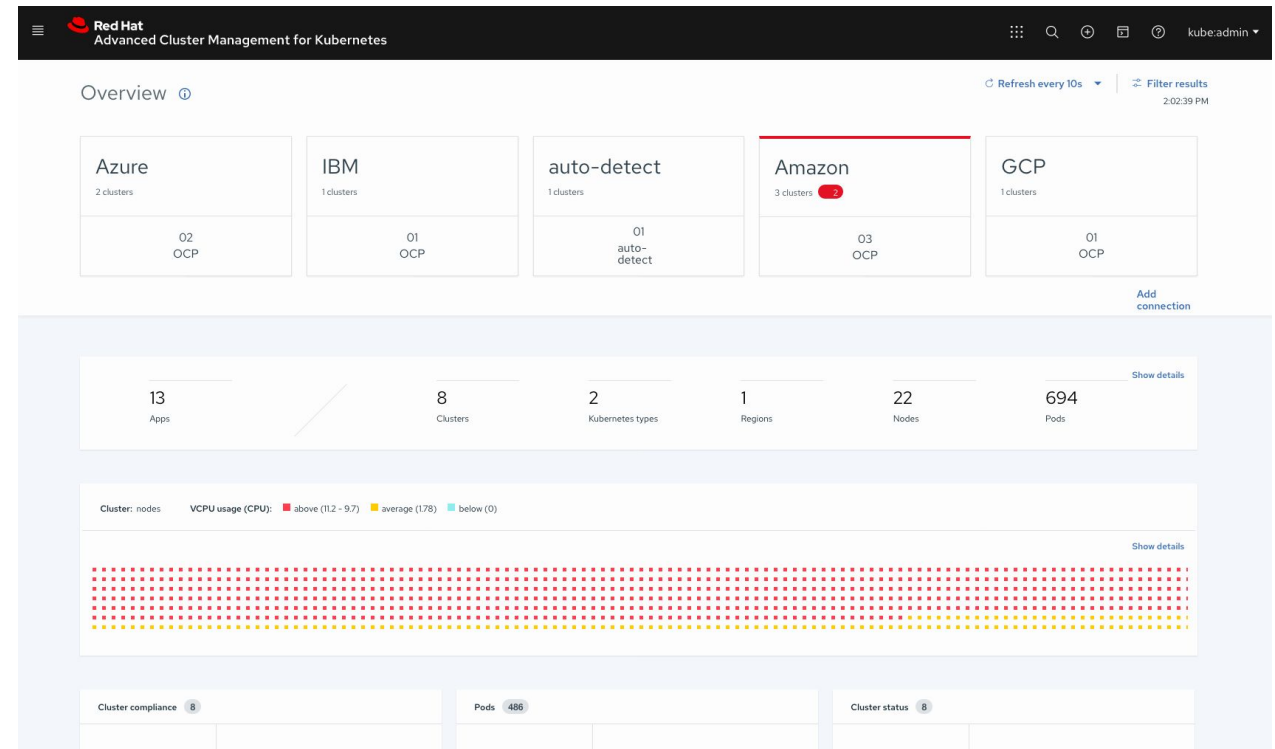
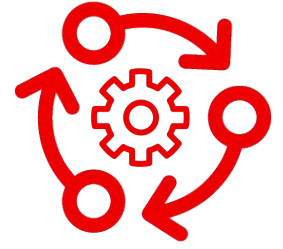
- Manage any Kubernetes compliant cluster
 - OpenShift 3.11, 4.1.x - 4.4.x
 - Public cloud hosted: OCP
 - Public cloud managed kubernetes: EKS, AKS, GKE, IKS
- Search, find and modify kubernetes resources across the management domain.
- IT Management as code with **YAML**
- See high level summaries across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

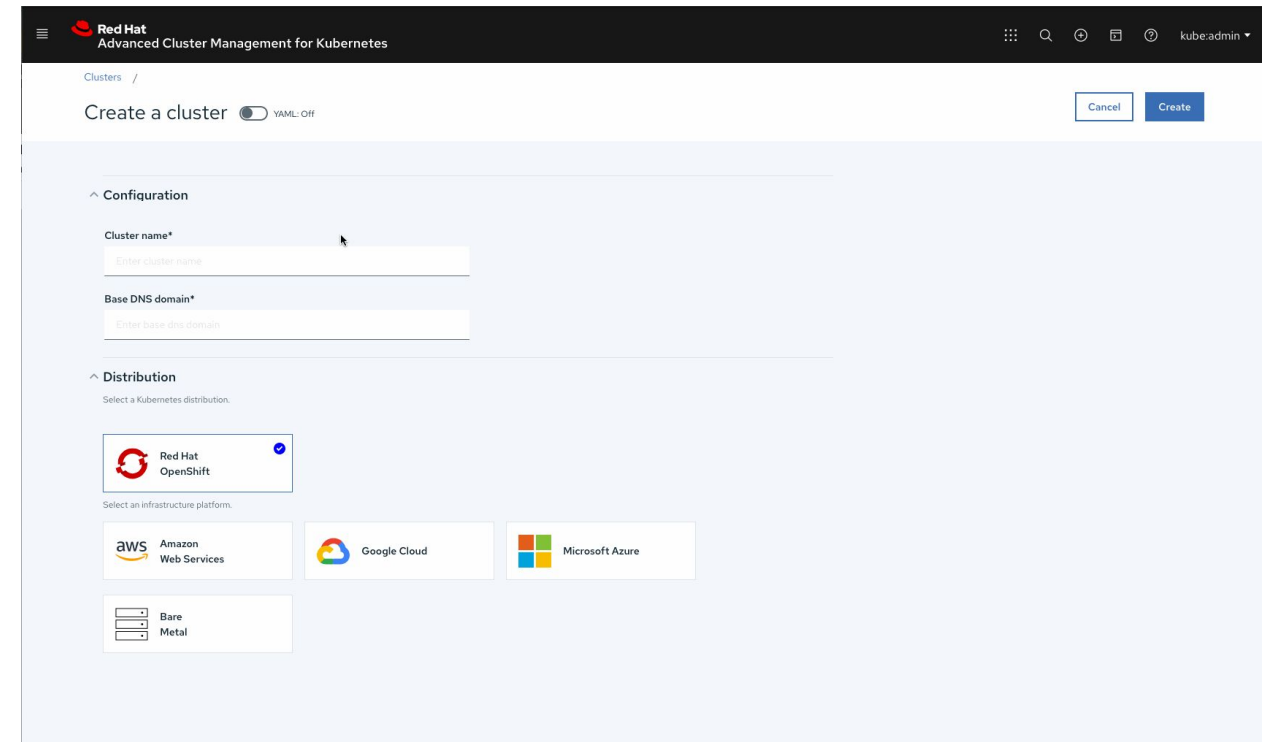
- **Create, Upgrade** and **Destroy** OCP clusters running on **Bare-metal** as well as public cloud
- Leverage [Hive API for OCP cluster deployment](#)
- Wizard or YAML based create cluster flow
- Launch to an OCP Console from ACM
- Access cluster login credentials and download kubeadmin configuration



IT Operations



DevOps/SRE



The screenshot shows the 'Create a cluster' wizard in the Red Hat Advanced Cluster Management for Kubernetes console. The interface is dark-themed with a light blue sidebar. The main content area is titled 'Create a cluster' and includes a 'YAML OFF' toggle and 'Cancel' and 'Create' buttons. The wizard is divided into sections: 'Configuration' with fields for 'Cluster name*' and 'Base DNS domain*', and 'Distribution' with a 'Select a Kubernetes distribution' section where 'Red Hat OpenShift' is selected. Below this is a 'Select an infrastructure platform' section with buttons for 'Amazon Web Services', 'Google Cloud', 'Microsoft Azure', 'Bare Metal', and 'Metal'.

Multi-Cluster Lifecycle Management

Dynamic Search



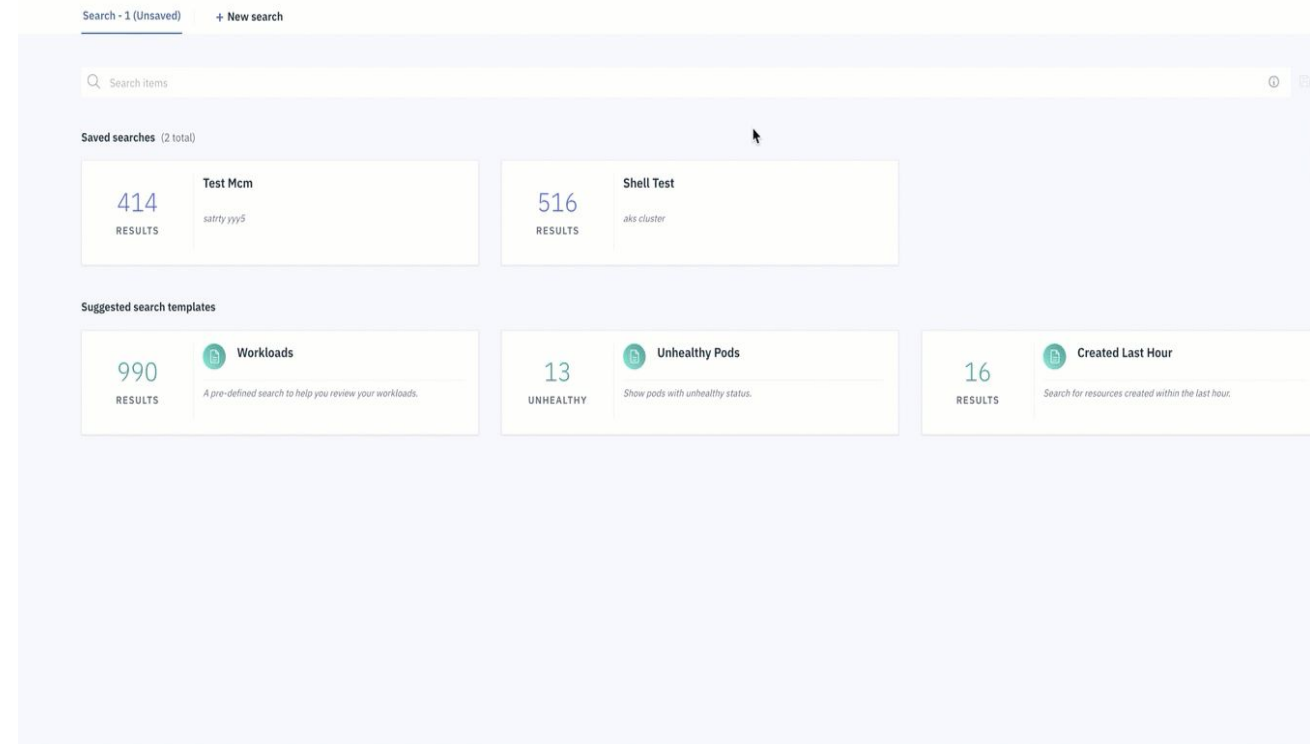
IT Operations



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**, **kubectrl**, **oc**, **istioctl**
- Single interface for multi-cluster
- Drive ops directly from dashboards
- Bash commands allow for grep

The screenshot shows the Red Hat Advanced Cluster Management for Kubernetes Visual Web Terminal interface. The header includes the Red Hat logo and the text "Advanced Cluster Management for Kubernetes". The main content area features a "Welcome, let's get started." message and a description of the tool's capabilities. Below this, there are four main sections: "End-to-end visibility", "Cluster lifecycle", "Application lifecycle" (marked as a Technology Preview), and "Governance, Risk, and Compliance". Each section includes a brief description and a "Go to" link. The interface is dark-themed with a navigation bar at the top right showing "kube:admin".

Policy Driven 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 Driven Governance Risk and Compliance

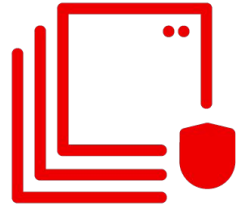
Architecture Overview



Security Ops

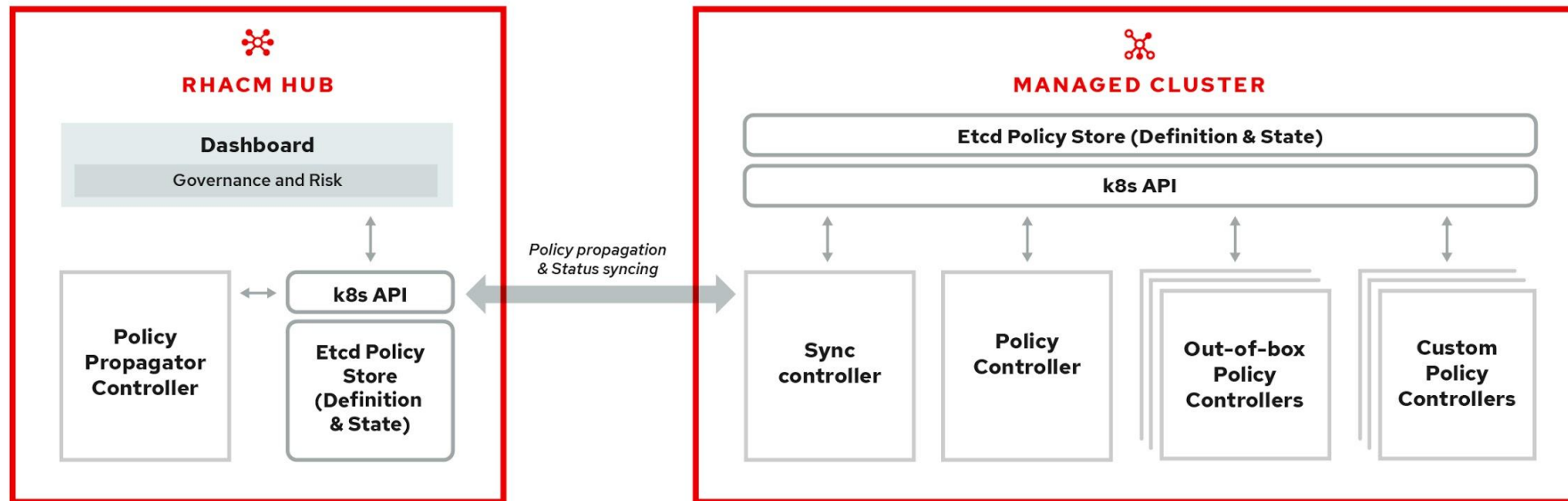


IT Operations



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

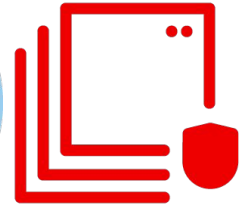
Don't wait for your security team to tap you on the shoulder



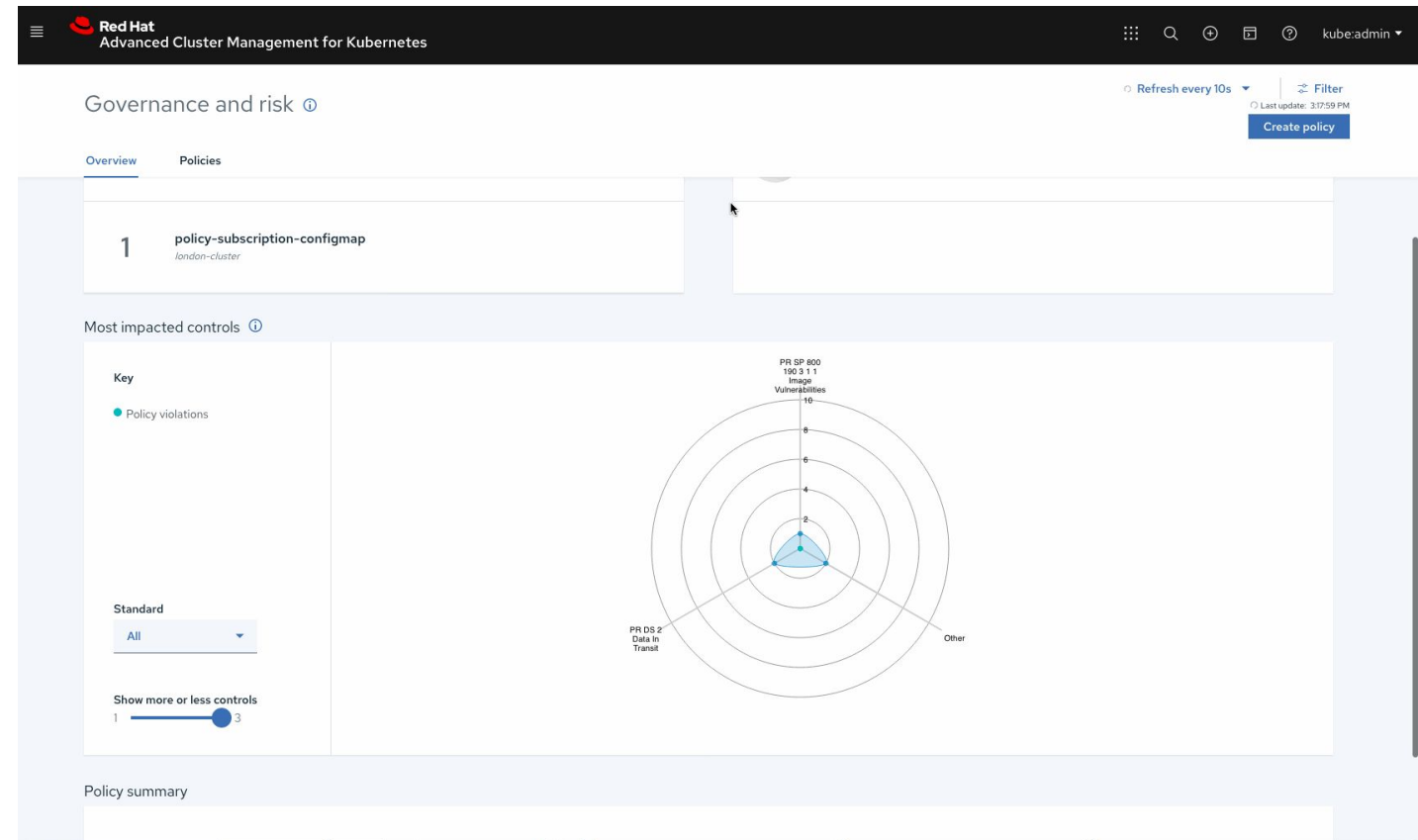
Security Ops



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

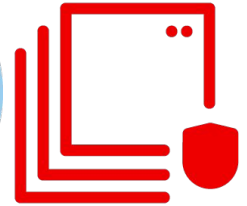
Don't wait for your security team to tap you on the shoulder



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

Red Hat Advanced Cluster Management for Kubernetes

Governance and risk ⓘ Refresh every 10s Last update: 3:36:19 PM Create policy

Overview Policies

1 policy-container-security london-cluster

1 policy-game-frontend-subscription san-francisco-cluster

1 policy-subscription-configmap london-cluster

3 policy-container-security, policy-subscription-configmap, policy-certificatepolicy

2 san-francisco-cluster policy-game-frontend-subscription, policy-certificatepolicy

No other policy violations We will continue to monitor and display any policy violations so you can easily find them here.

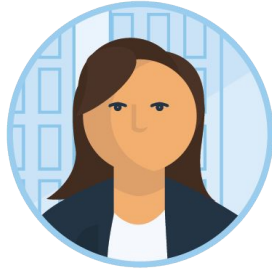
Most impacted controls ⓘ

Key Policy violations

Standard PR DS 2

PR SP 800 190 3 1.1 Image Vulnerabilities

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

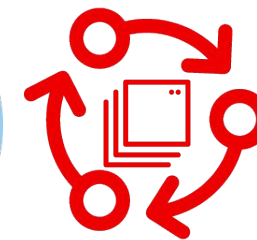
Simplify your Application Lifecycle



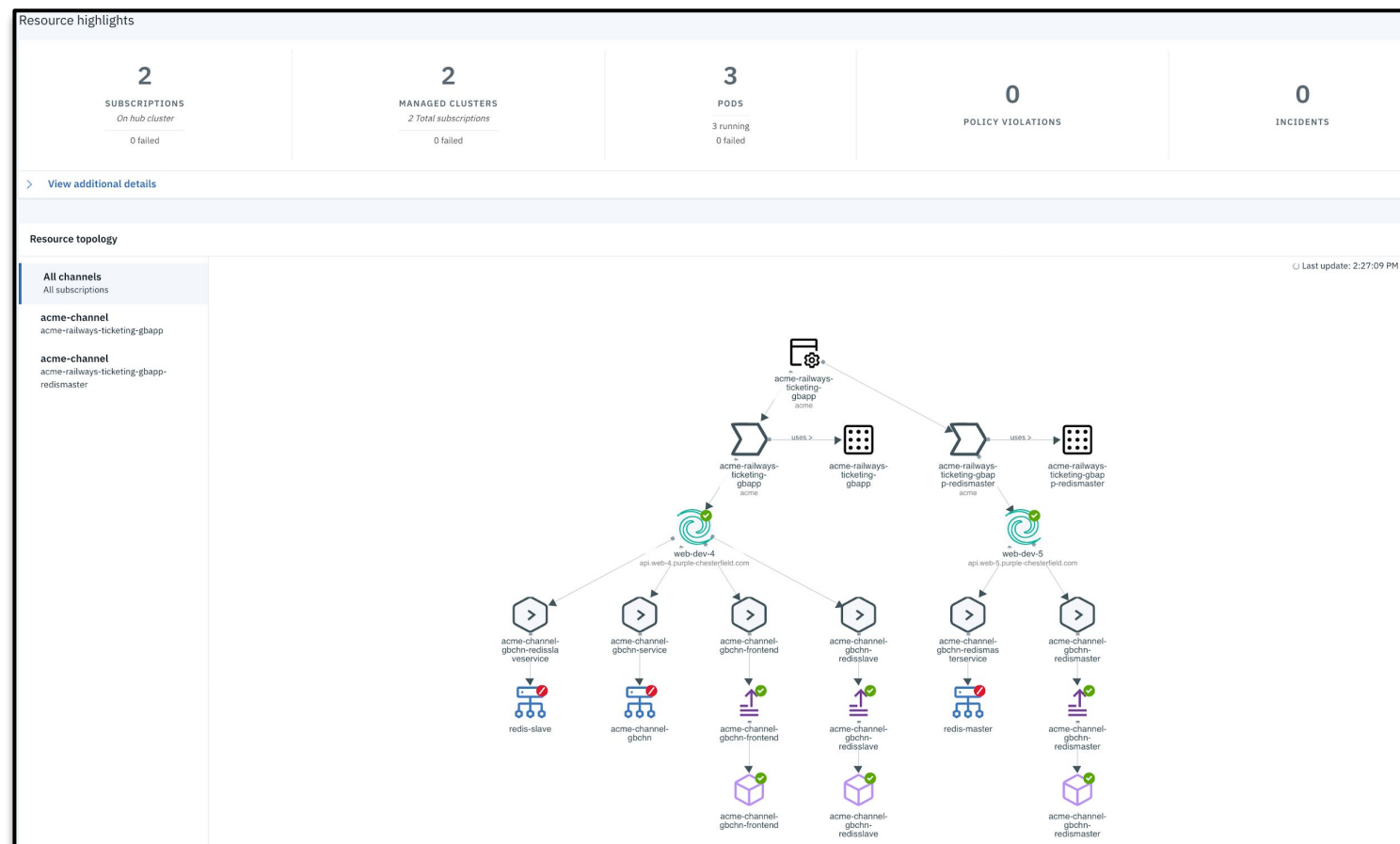
DevOps/SRE



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

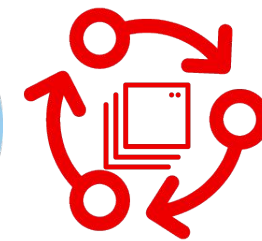
Subscriptions Bring Enterprise to Kubernetes



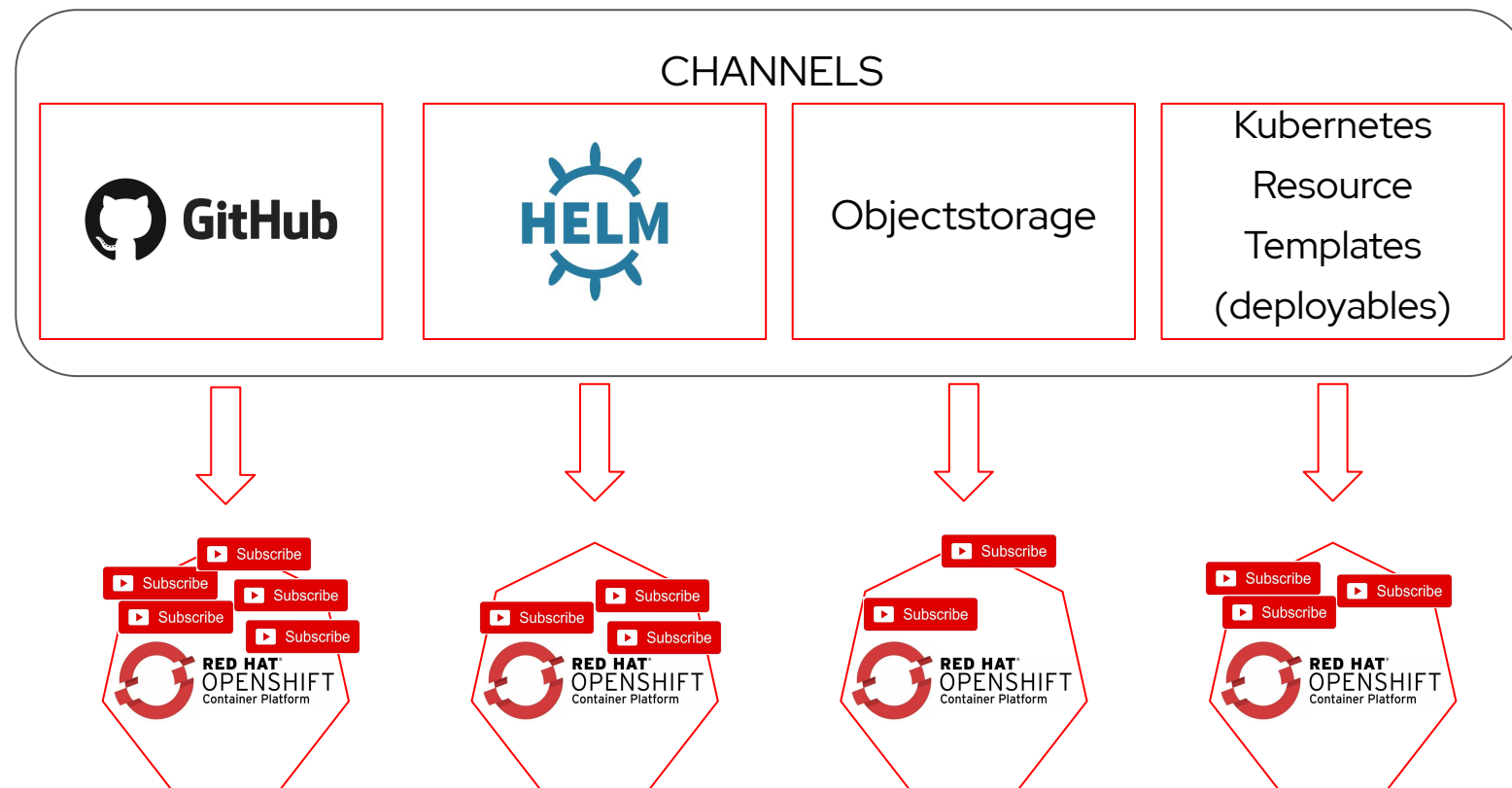
DevOps/SRE



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

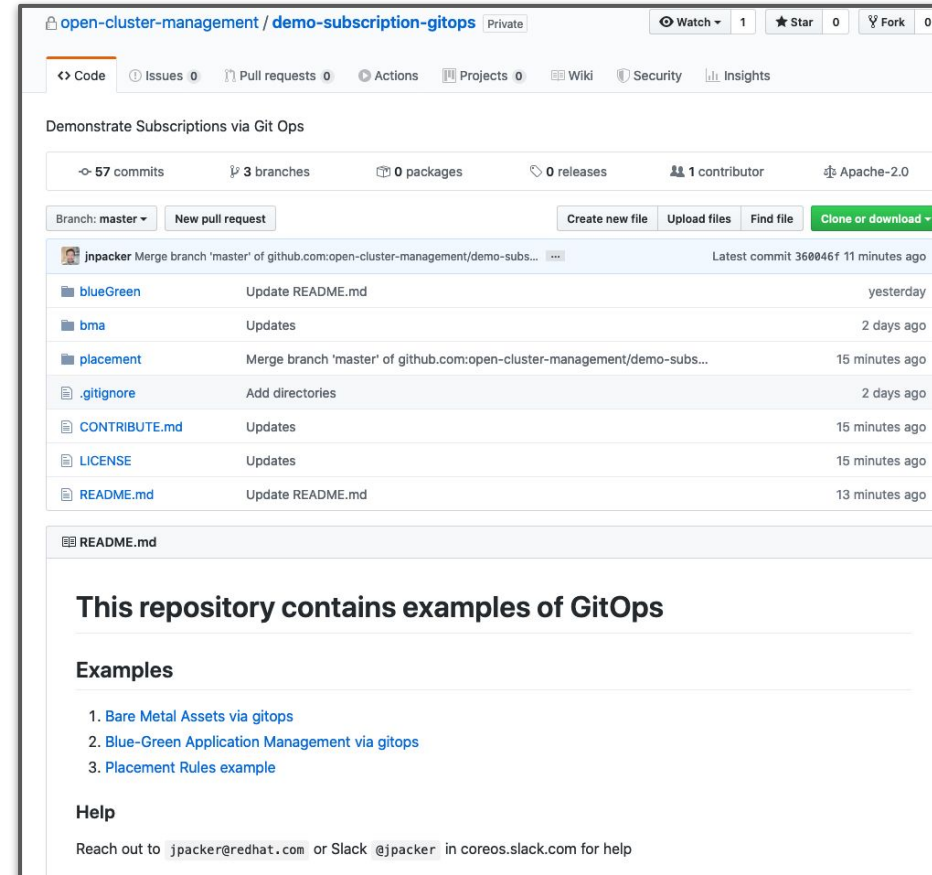
- Create, modify & delete, just as you would any source code. Git becomes your source of truth controlling your data center.
- Have a record of who, what & when for every change precipitated in your environments
- Through code Reviews & Approvals, take full control of all changes to your data center(s)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



DevOps/SRE



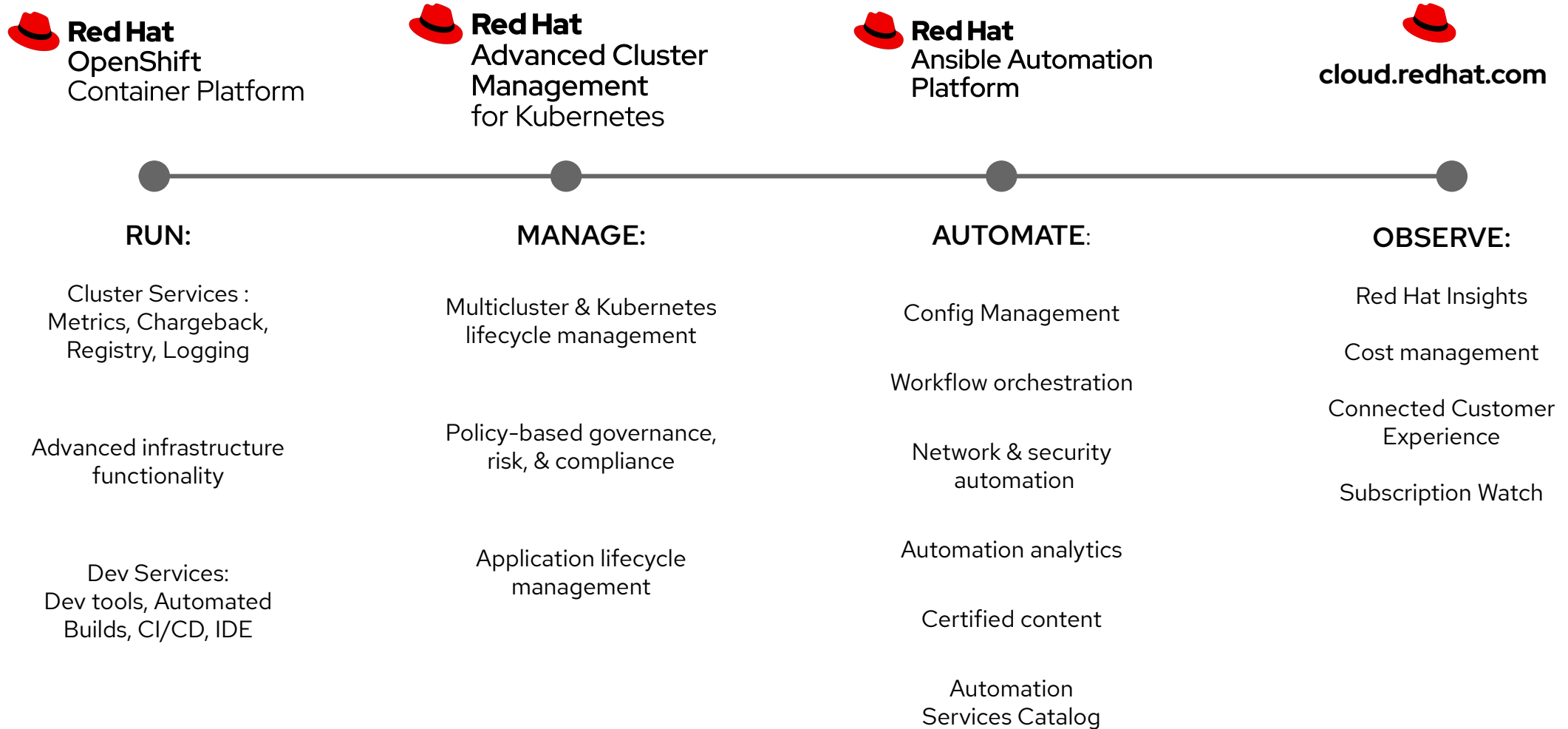
IT Operations



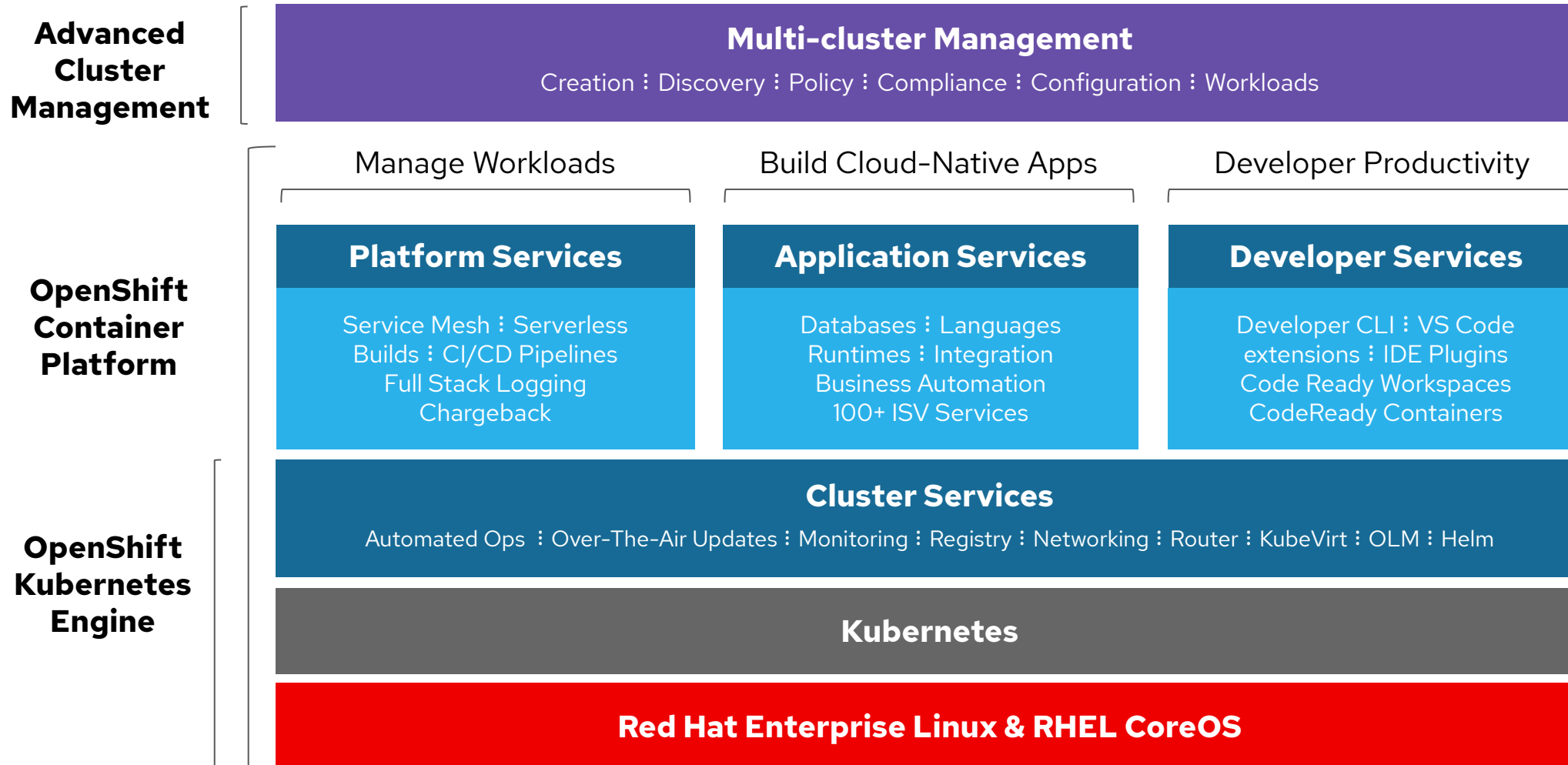
<https://github.com/open-cluster-management/demo-subscription-gitops>

ACM and Openshift

Supporting Application Modernization



Draw Me a Picture!



Architecture

Architecture Overview



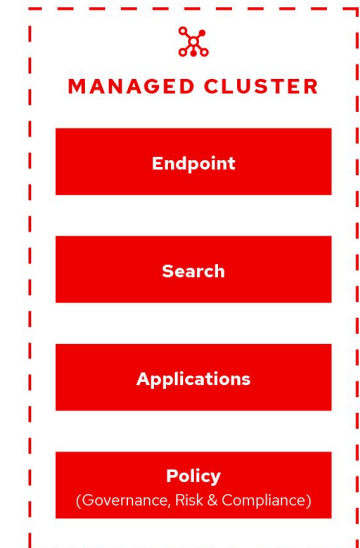
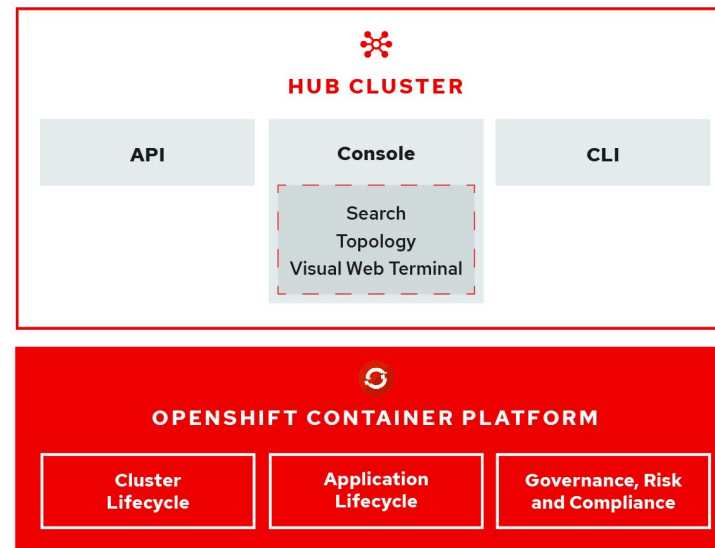
IT Operations

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

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

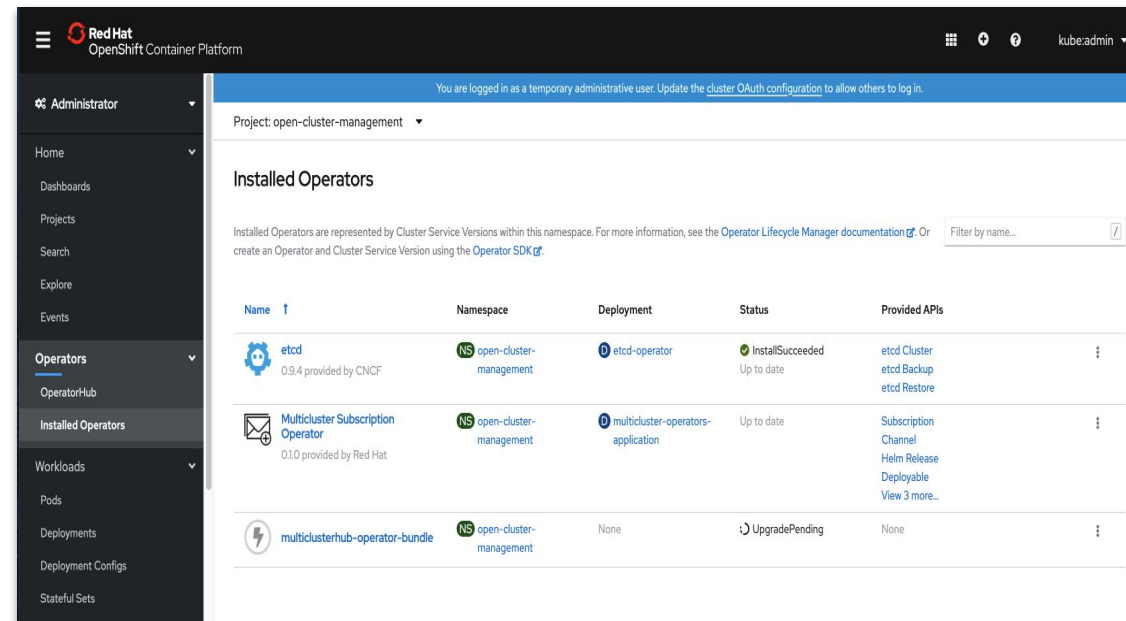
- OpenShift 3.11, 4.1.x - 4.4.x
- Public cloud hosted: OCP
- Public cloud managed kubernetes: EKS, AKS, GKE, IKS

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



Installation and Foundation

Operator Install for Managed Cluster



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

Demo

A Demo Video (from the 2020 Summit) is available here:

<https://content.onlinexperiences.com/FMSRecording/Production/MediaCollection/VideoCollection/3484/4/320174/DEMO 2 - Managing Kubernetes Clusters with Red Hat Advanced Cluster Manager for Kubernetes.mp4>

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://www.linkedin.com/company/red-hat)



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



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



twitter.com/RedHat