



Advanced Cluster Management for Kubernetes

Alfred Bach
PSA EMEA

Presenter's Name
Title

Introducing Red Hat Advanced Cluster Management For Kubernetes

Robust. Proven. Award winning.



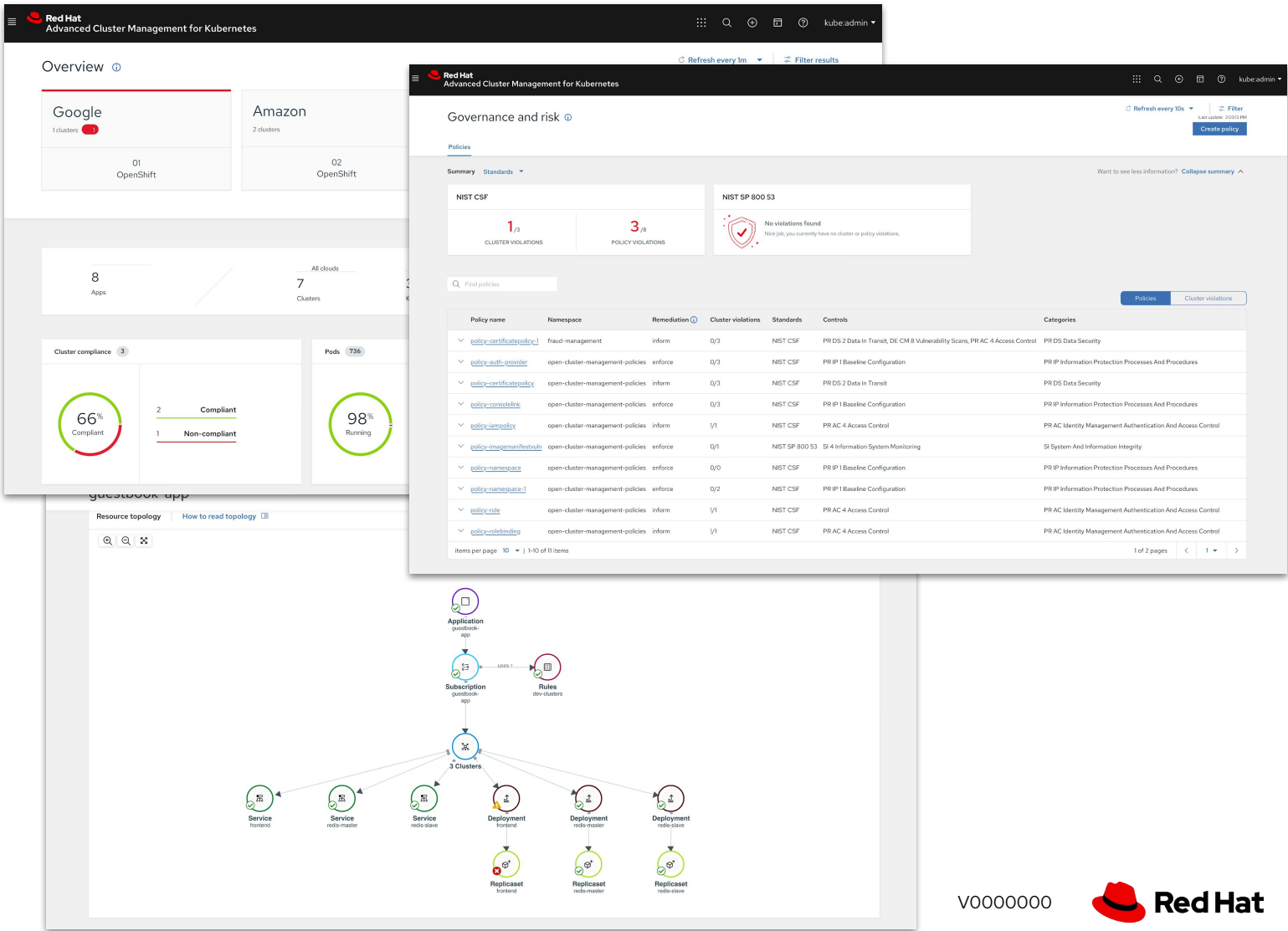
Multicloud lifecycle management



Policy driven governance, risk, and compliance



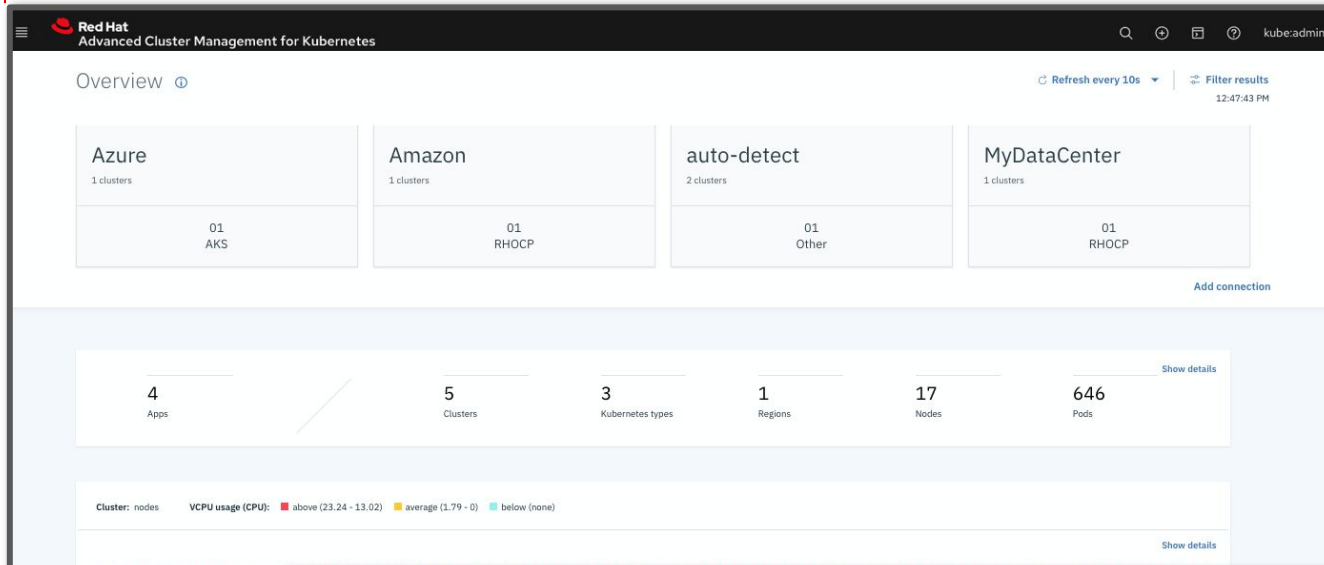
Advanced application lifecycle management



Unified Multi-Cluster Management

CONFIDENTIAL designator

Single Pane for all your Kubernetes Clusters



- **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

Name	Namespace	Labels	Endpoint	Status	Nodes	Kusterlet Version	Kubernetes Version	Storage	Memory	CPU
exec2-iks	mcm-exec2-iks	cloud=IBM datacenter=da13 environment=Dev name=exec2-iks region=US vendor=IKS	-	Offline	1	3.1.2-dev	v1.11.7+IKS	-	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	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=ICP4Data	launch	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	launch	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%

Policy based Governance, Risk and Compliance

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

CONFIDENTIAL designator

The dashboard provides a comprehensive overview of policy violations and security findings. It includes a summary of violations by severity (Policy Violations: 3, Cluster Violations: 1, High Severity Findings: 1, Medium Severity Findings: 1, Low Severity Findings: 1) and a detailed view of the most impacted controls. The 'compliancePolicy' section shows a table of policy details and a code editor for the policy definition. The 'Object Templates' section displays a table of policy 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
```

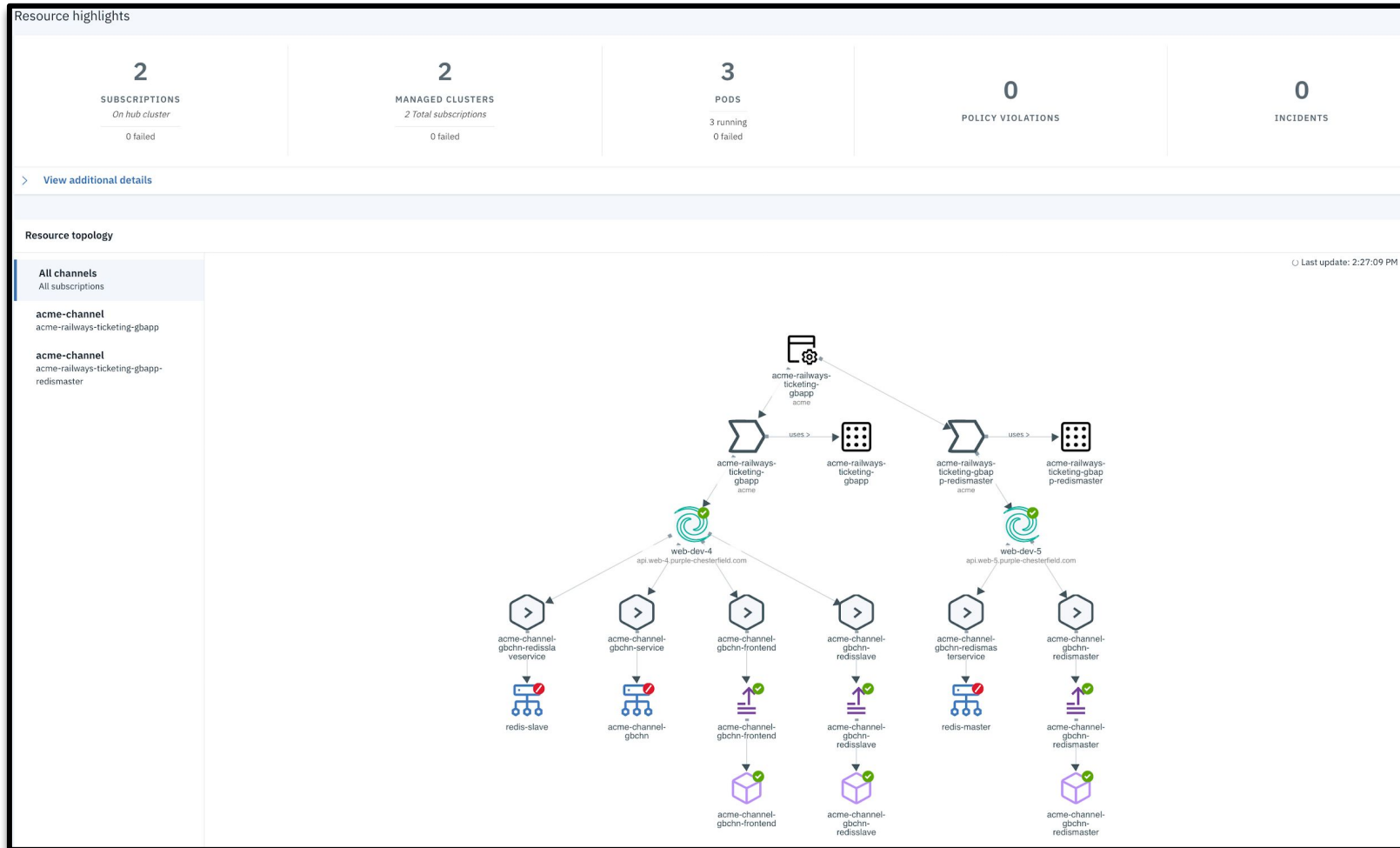
Name	Compliance Type	API version	Kind	Last Transition	Compliant
restricted-mcm	musthave	policy/v1beta1	PodSecurityPolicy	-	-
deny-from-other-namespaces	musthave	networking.k8s.io/v1	NetworkPolicy	-	-
mem-limit-range	musthave	v1	LimitRange	-	-

- **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

CONFIDENTIAL designator



- **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.



Increase application availability

Placement rules 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

Overview

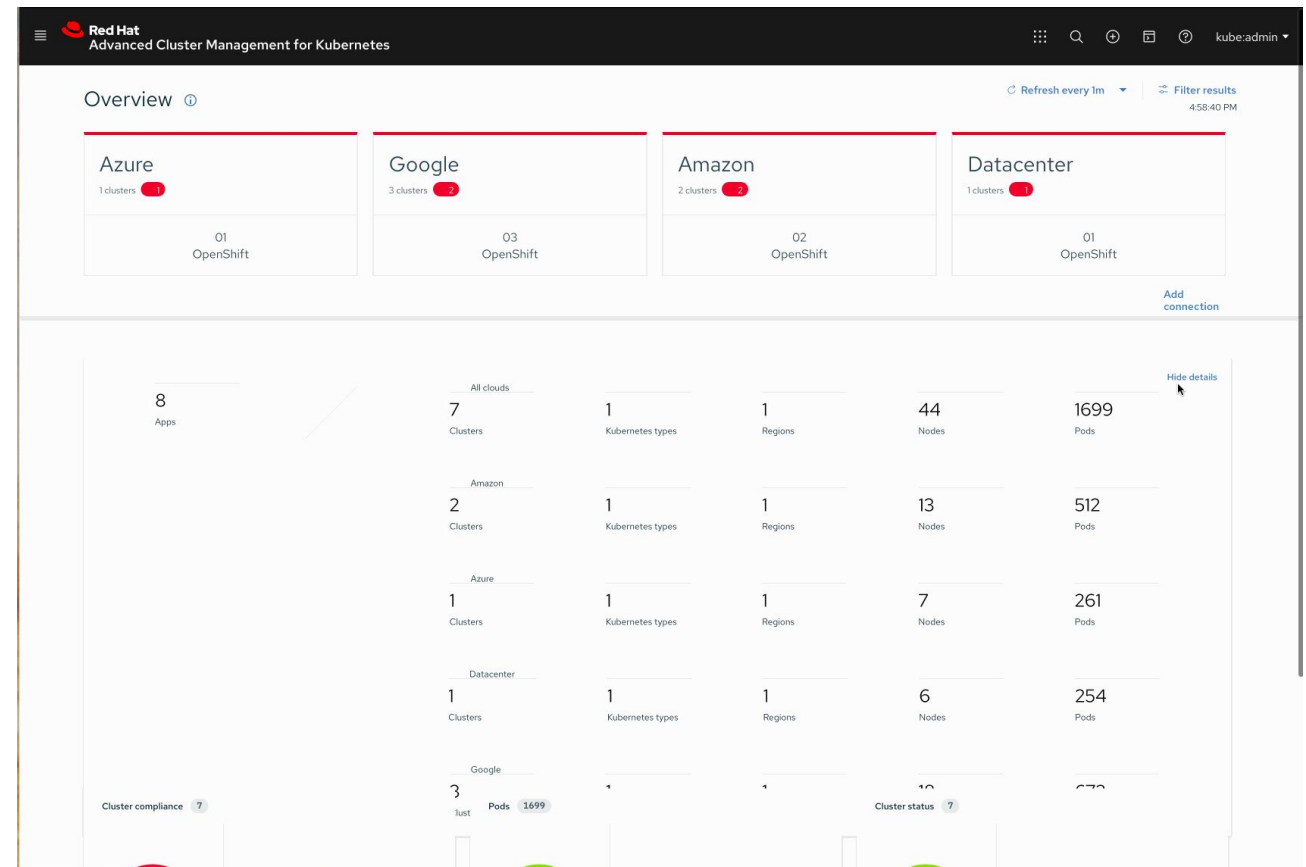
- Full Management of OCP Kubernetes
 - OpenShift 3.11, 4.1.x - 4.5.x
 - Public cloud hosted: OCP
- Public cloud managed kubernetes: EKS, AKS, GKE, IKS
 - Search, find and modify kubernetes resources.
- See high level summaries across all clusters
 - Misconfiguration
 - Pod status
 - Resource capacity
- 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



IT Operations



DevOps/SRE



Multi-Cluster Lifecycle Management

Creating & Importing Clusters

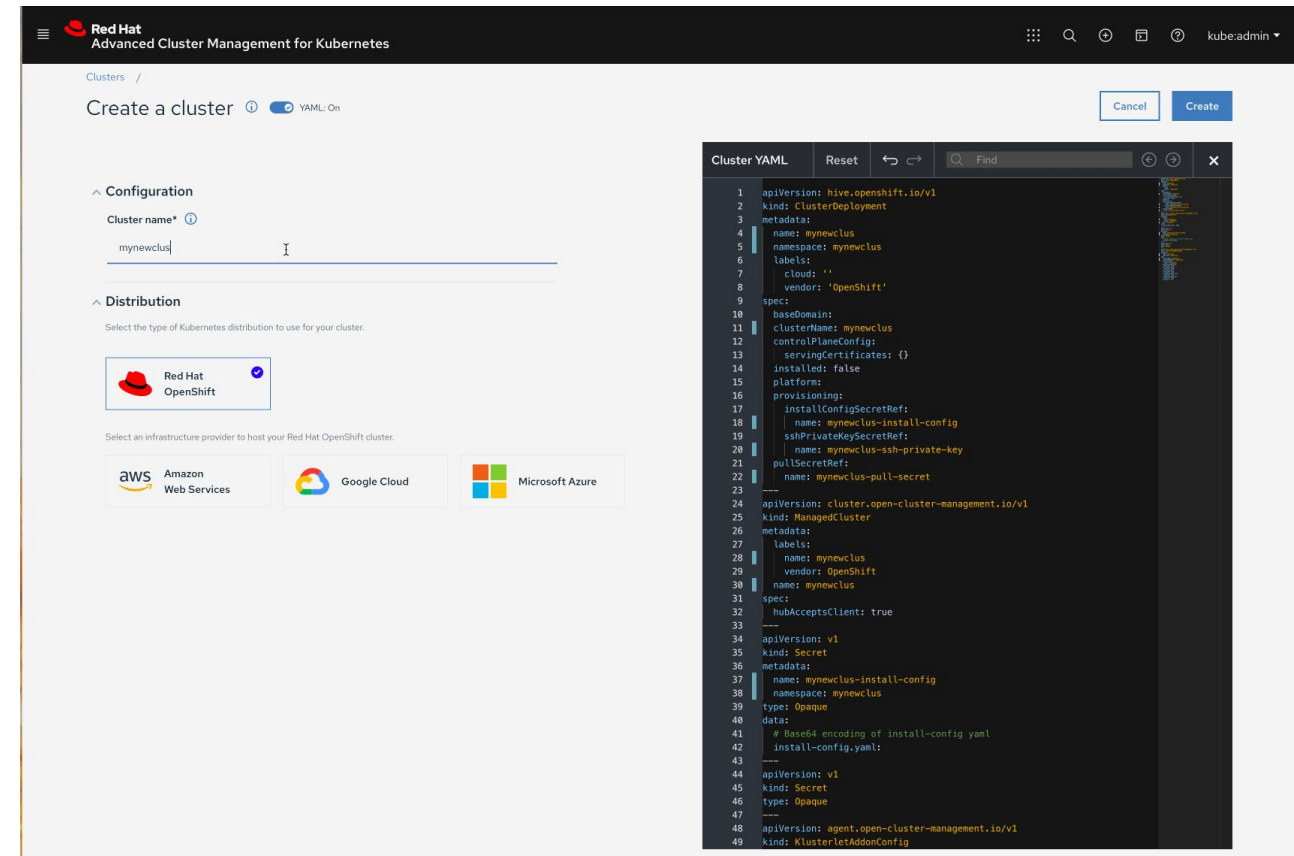
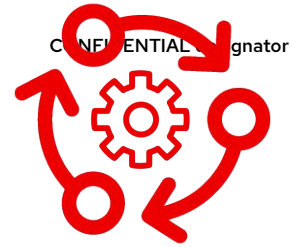
- **Create, Upgrade** and **Destroy** OCP clusters running on **Bare-metal** as well as public cloud
- Leverage **Hive** API for OCP cluster deployment
- Wizard or YAML based create cluster flow
- Launch to an OCP Console from ACM
- Access cluster login credentials and download kubeadmin configuration



IT Operations



DevOps/SRE



Multi-Cluster Lifecycle Management

Dynamic Search



IT Operations



DevOps/SRE



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

Red Hat Advanced Cluster Management for Kubernetes

Search

Unhealthy pods

kind:pod X status:Pending,Error,Failed,Terminating,ImagePullBackOff,CrashLoopBackOff,RunContainerError,ContainerCreating X

2 RELATED CLUSTER 2 RELATED SECRET 6 RELATED NODE 1 RELATED APPLICATION 2 RELATED DEPLOYMENT

2 RELATED REPLICASET 1 RELATED CHANNEL 2 RELATED SERVICE 3 RELATED SUBSCRIPTION

Pod (6)

Name	Namespace	Cluster	Status	Restarts	Host IP	Pod IP	Created	Labels
frontend-6cb7f8bd65-8lqz7	guestbook-app	kilo-bravo	CrashLoopBackOff	35	10.0.135.156	10.129.2.79	3 hours ago	app=guestbook +2
frontend-6cb7f8bd65-fjw77	guestbook-app	kilo-alpha	CrashLoopBackOff	35	10.0.167.117	10.129.2.161	3 hours ago	app=guestbook +2
frontend-6cb7f8bd65-rgqkx	guestbook-app	kilo-alpha	CrashLoopBackOff	35	10.0.128.146	10.128.2.177	3 hours ago	app=guestbook +2
frontend-6cb7f8bd65-4gqgm	guestbook-app	kilo-alpha	CrashLoopBackOff	35	10.0.147.26	10.131.0.172	3 hours ago	app=guestbook +2
frontend-6cb7f8bd65-wpv2m	guestbook-app	kilo-bravo	CrashLoopBackOff	35	10.0.154.41	10.131.0.92	3 hours ago	app=guestbook +2
frontend-6cb7f8bd65-kr7jc	guestbook-app	kilo-bravo	CrashLoopBackOff	35	10.0.174.99	10.128.2.36	3 hours ago	app=guestbook +2

Items per page 20 | 1-6 of 6 items

1 of 1 pages

Multi-Cluster Lifecycle Management

Visual Web Terminal **Tech-Preview**



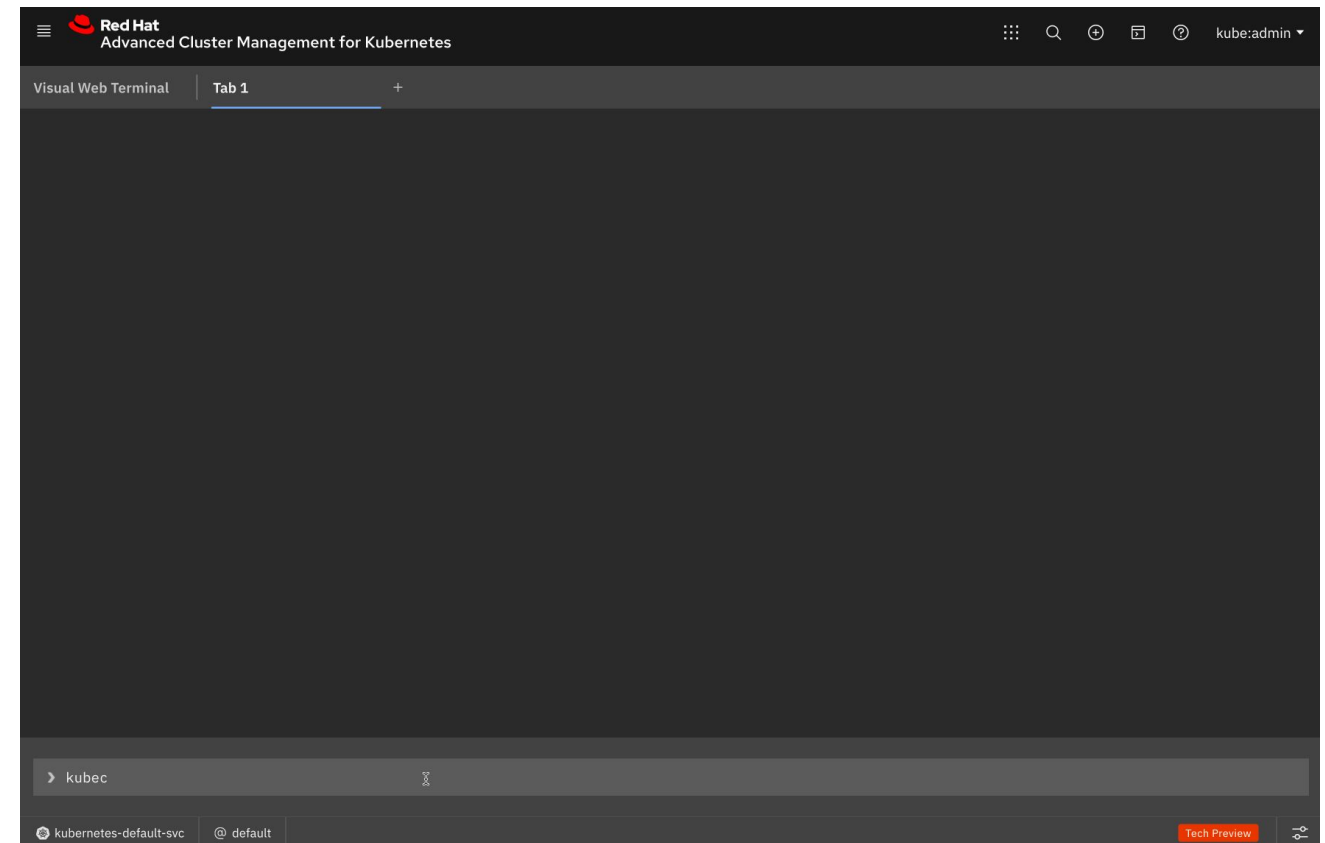
IT Operations



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



Policy Driven Governance Risk and Compliance

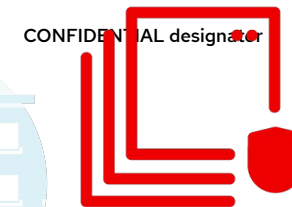
Architecture Overview



Security Ops

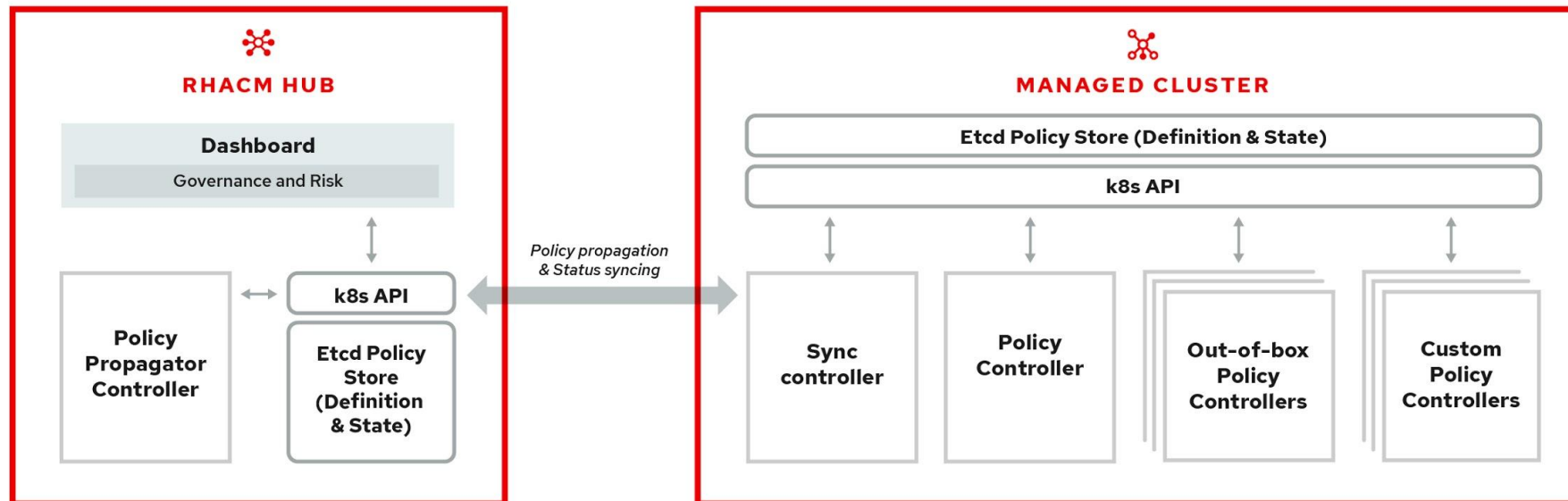


IT Operations



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

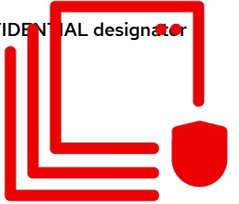


Security Ops



IT Operations

CONFIDENTIAL designator



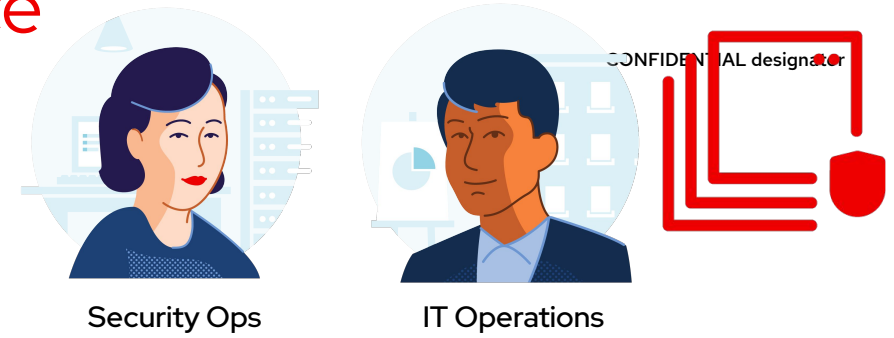
- Set and enforce policies for security, applications, & infrastructure
- Deep visibility for auditing configuration of apps and clusters
- Unique policy capabilities around CIS compliance
- Categorize violations based on your standards for immediate visibility into your compliance posture

The screenshot displays the Red Hat Advanced Cluster Management for Kubernetes console. The main heading is 'Create policy' with a 'YAML: On' toggle. The form includes fields for 'Name *' (policy-grc), 'Namespace *' (The namespace to create and store the policy on the hub cluster.), 'Specifications *' (Begin typing to search for template to select), 'Cluster binding' (Begin typing to search for cluster label to select. If not selected, all clusters will be appli...), 'Standards' (Begin typing to search for label to select), 'Categories' (Begin typing to search for label to select), and 'Controls' (Begin typing to search for label to select). A 'Cancel' button and a 'Create' button are at the top right. A 'Policy YAML' editor is open on the right, showing the following YAML content:

```
1  apiVersion: policy.open-cluster-management.io/v1
2  kind: Policy
3  metadata:
4    name: policy-grc
5    namespace:
6    annotations:
7      policy.open-cluster-management.io/standards:
8      policy.open-cluster-management.io/categories:
9      policy.open-cluster-management.io/controls:
10 spec:
11   remediationAction: inform
12   disabled: false
13 ---
14 apiVersion: policy.open-cluster-management.io/v1
15 kind: PlacementBinding
16 metadata:
17   name: binding-policy-grc
18   namespace:
19 placementRef:
20   name: placement-policy-grc
21   kind: PlacementRule
22   apiGroup: apps.open-cluster-management.io
23 subjects:
24   - name: policy-grc
25     kind: Policy
26     apiGroup: policy.open-cluster-management.io
27 ---
28 apiVersion: apps.open-cluster-management.io/v1
29 kind: PlacementRule
30 metadata:
31   name: placement-policy-grc
32   namespace:
33 spec:
34   clusterConditions:
35     - status: "True"
36       type: ManagedClusterConditionAvailable
37   clusterSelector:
38     matchExpressions:
```


Policy based Governance, Risk and Compliance

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



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

Red Hat Advanced Cluster Management for Kubernetes

Governance and risk / Policies /

Create policy ⓘ ☒ YAML: On

Cancel Create

All fields marked with an asterisk (*) are mandatory.

Name *
policy-grc

Namespace * ⓘ
The namespace to create and store the policy on the hub cluster.

Specifications * ⓘ
Begin typing to search for template to select

Cluster binding ⓘ
Begin typing to search for cluster label to select. If not selected, all clusters will be appli...

Standards ⓘ
Begin typing to search for label to select

Categories ⓘ
Begin typing to search for label to select

Controls ⓘ
Begin typing to search for label to select

☐ Enforce if supported ⓘ

Policy YAML

```
1 apiVersion: policy.open-cluster-management.io/v1
2 kind: Policy
3 metadata:
4   name: policy-grc
5   namespace:
6   annotations:
7     policy.open-cluster-management.io/standards:
8     policy.open-cluster-management.io/categories:
9     policy.open-cluster-management.io/controls:
10 spec:
11   remediationAction: inform
12   disabled: false
13
14 apiVersion: policy.open-cluster-management.io/v1
15 kind: PlacementBinding
16 metadata:
17   name: binding-policy-grc
18   namespace:
19 placementRef:
20   name: placement-policy-grc
21   kind: PlacementRule
22   apiGroup: apps.open-cluster-management.io
23 subjects:
24   - name: policy-grc
25     kind: Policy
26     apiGroup: policy.open-cluster-management.io
27
28 apiVersion: apps.open-cluster-management.io/v1
29 kind: PlacementRule
30 metadata:
31   name: placement-policy-grc
32   namespace:
33 spec:
34   clusterConditions:
35     - status: "True"
36     type: ManagedClusterConditionAvailable
37   clusterSelector:
38     matchExpressions:
```

Advanced Application Lifecycle Management

Simplify your Application Lifecycle

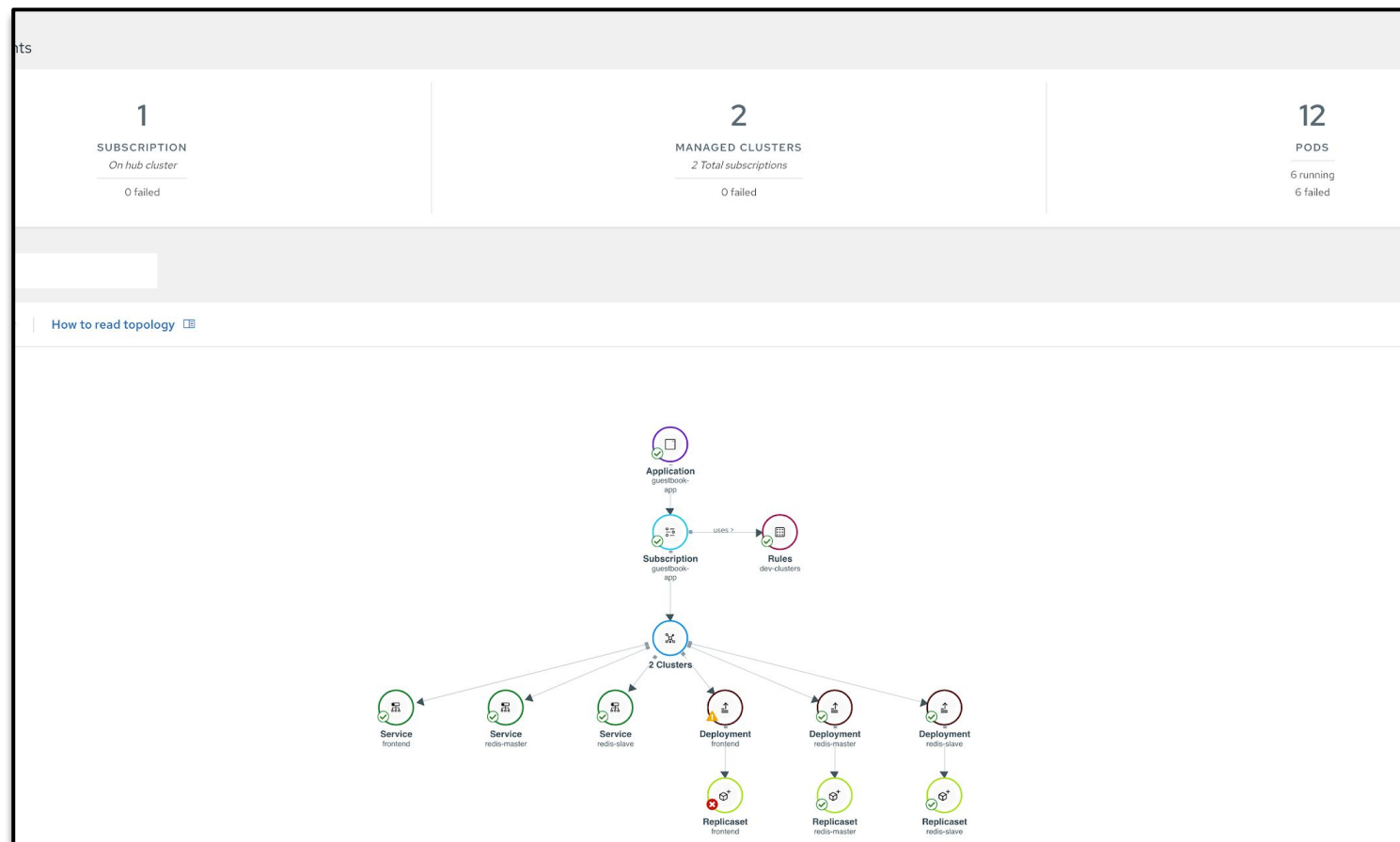
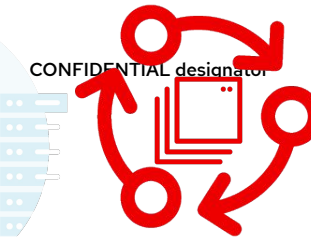
- Deploy Applications at Scale
- Deploy Applications from Multiple Sources and Clusters
- Quickly Visualize Application Relationships
- Using the subscription & channel model, the latest application revisions are delivered to appropriate clusters, automatically.



IT Operations

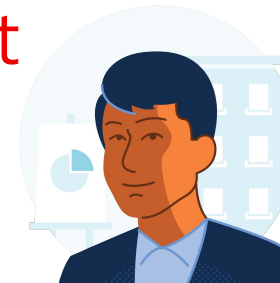


DevOps/SRE



Advanced Application Lifecycle Management

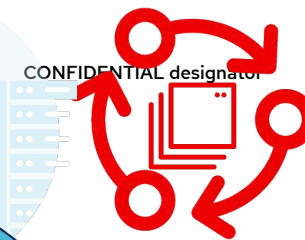
Subscriptions Bring Enterprise to Kubernetes



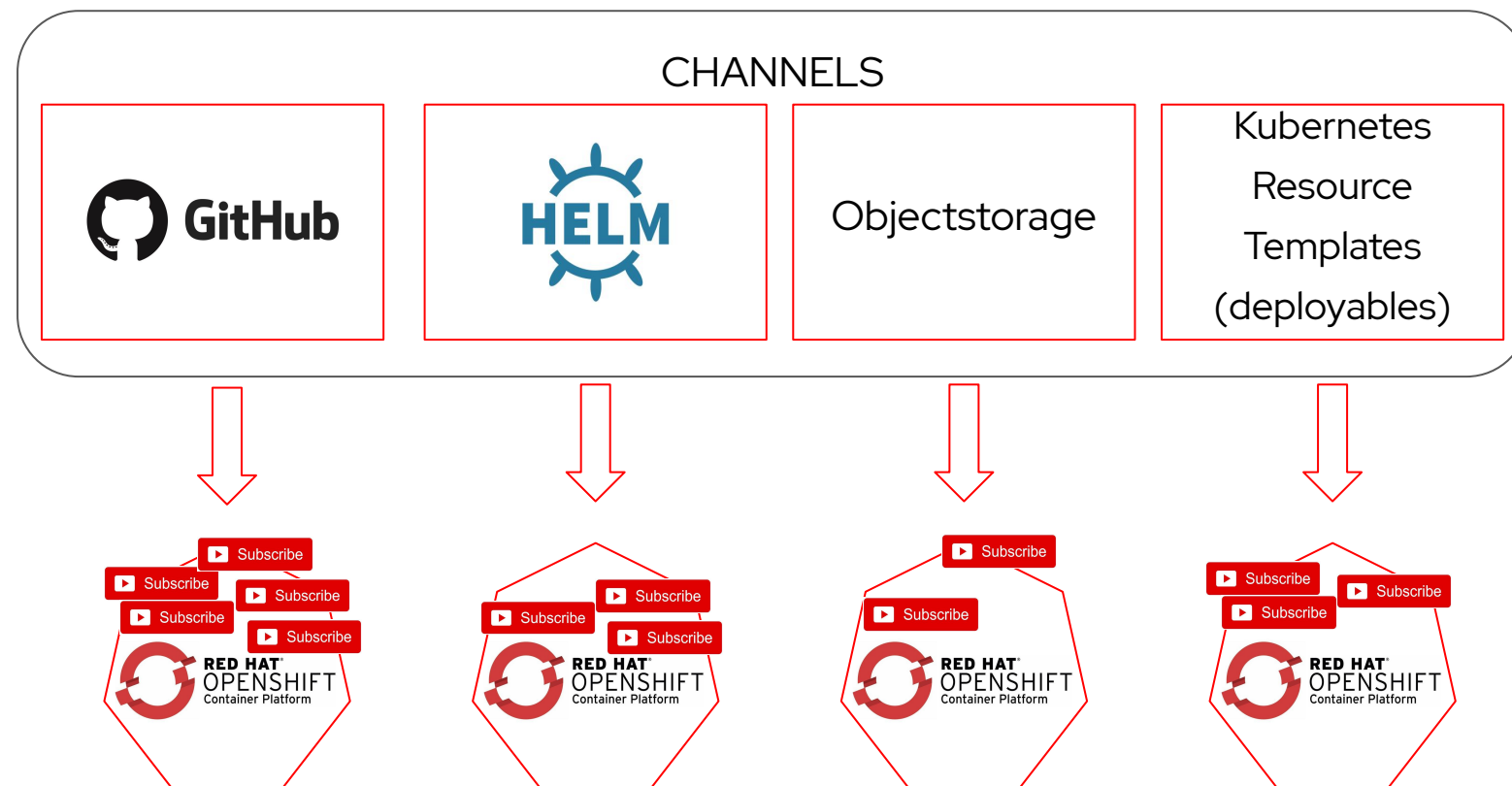
IT Operations



DevOps/SRE



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



Advanced Application Lifecycle Management

GitOps as the source of truth

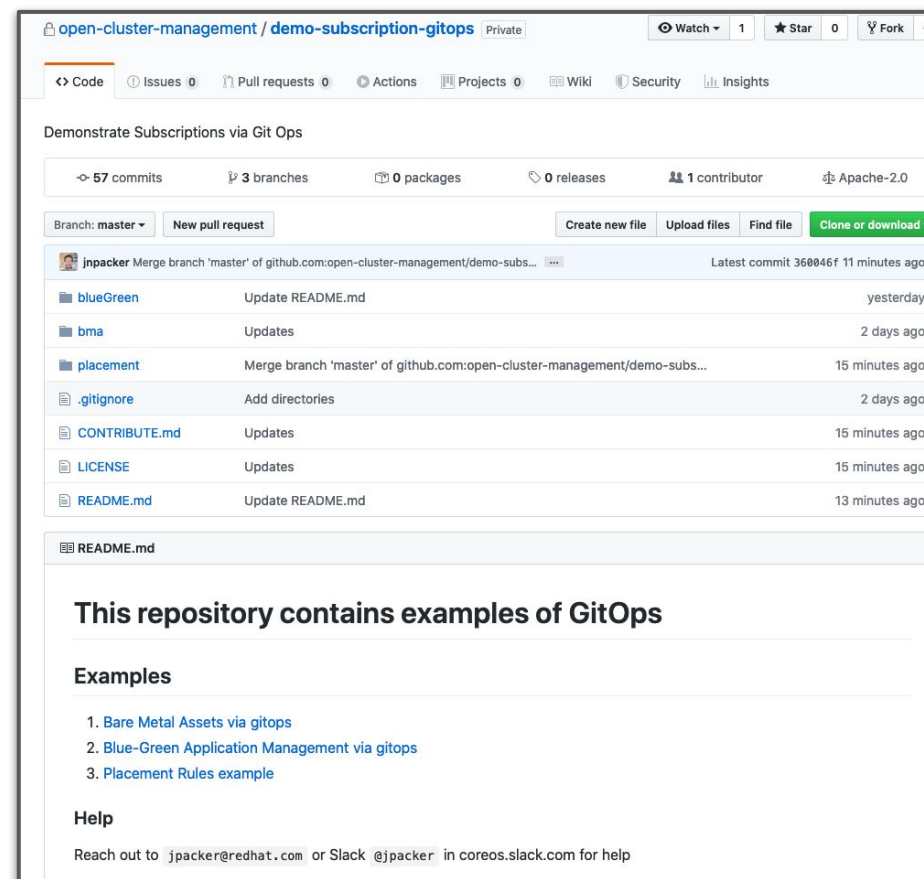
- Create, modify & delete, just as you would any source code. Git becomes your source of truth controlling your data center.
- Have a record of who, what & when for every change precipitated in your environments
- Through code Reviews & Approvals, take full control of all changes to your data center(s)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



IT Operations



DevOps/SRE



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

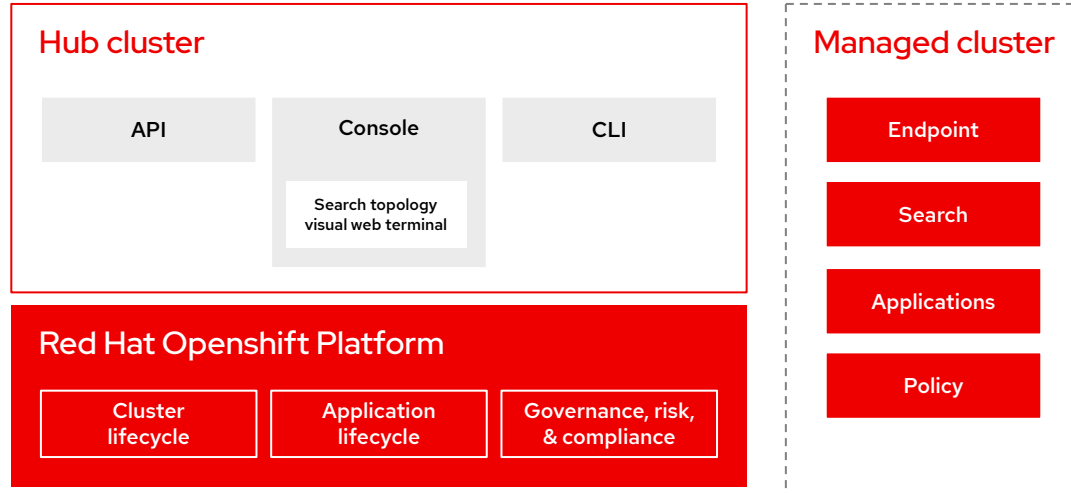
Architecture

Red Hat Advanced Cluster Management For Kubernetes

Architecture overview



IT Operations



Hub architecture and components

Red Hat Advanced Cluster Management uses the multicluster-hub operator and runs in the open-cluster-management namespace

Managed cluster architecture and components

Red Hat Advanced Cluster Management managed clusters use the multicluster-endpoint operator which runs in the multicluster-endpoint namespace

Installation

Advanced Cluster Management For Kubernetes

Installation and Foundation

Operator Install for Hub



CONFIDENTIAL designator

IT Operations

Hub Cluster

- Operator based installation
- Available on OperatorHub
- Requires OCP 4.3.x - 4.5.x

Full Management of OCP clusters

- OpenShift 3.11, 4.1.x - 4.5.x
- Public cloud hosted: OCP

Limited Support for Public cloud managed Kubernetes

- EKS, AKS, GKE, IKS

High Availability

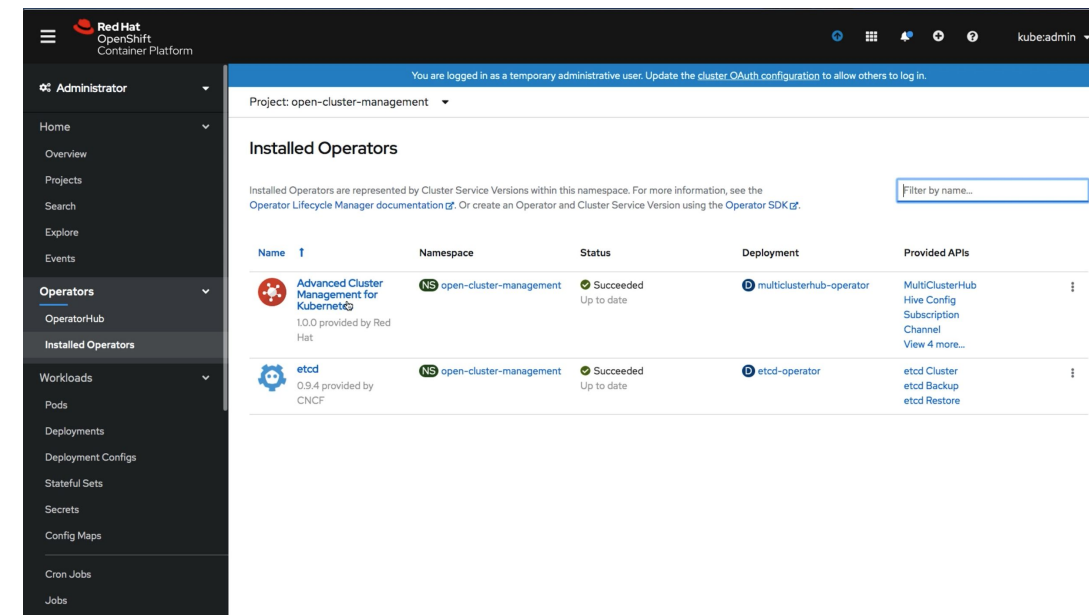
- Supports OCP Availability Zone
- Limitation for Search component based on RedisGraph

Resource Requirements

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



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
- ▶ Connection manager
- ▶ Work manager
- ▶ Policy controller
- ▶ Search collector
- ▶ Service registry
- ▶ IAM policy controller
- ▶ Certificate policy controller
- ▶ CIS policy controller

Role-Based Access Control

How to control User access



- There are no RHACM specific Roles or Personas, we rely on the default roles included in OCP
 - **Cluster Admin** - Super User can perform all actions
 - **Admin** - Can perform some actions
 - **Edit** - Read access
 - **View** - Read access
- Default User after installation is Kube Admin

UI Panel	Cluster Admin	Admin	Edit	View
Home Page	Read	Read	Read	Read
Overview Page	Read	Read	Read	Read
Topology View	Read	Read	Read	Read
Cluster View	CRUD*	Read	Read	Read
Manage Applications	CRUD*	CRUD*	Read	Read
Manage Policies	CRUD*	CRUD*	No Access	No Access

Pricing and Packaging

ACM SKUs

ALL ACM SKUs will be in the Private Pricebook until 1QCY21

- ▶ Ordering from the Private Pricebook requires a BU Guidance ticket
- ▶ Primary SKUs:

SKU	Offering Name	List Price (USD)
MCT3946	Red Hat Advanced Cluster Management for Kubernetes, Standard (2 Core or 4 vCPU)	\$675.00
MCT3945	Red Hat Advanced Cluster Management for Kubernetes, Premium (2 Core or 4 vCPU)	\$1,000.00

- ▶ Other SKUs are available, including SKUs for Telco, CSS, Cloud Suite add-ons, etc. but are not in the Private Pricebook until 4QCY20. Contact Greg Bowman for information and assistance. gbowman@redhat.com.

Refer to the [subscription and sizing guide for details](#)

Production SKUs

New SKU#	Existing SKUs Description
MCT3945	Red Hat Advanced Cluster Management for Kubernetes, Premium (2 Core or 4 vCPU)
MCT3946	Red Hat Advanced Cluster Management for Kubernetes, Standard (2 Core or 4 vCPU)
SER0599	60 Day Evaluation of Red Hat Advanced Cluster Management for Kubernetes, Self-Support (2 Cores or 4vCPU)
SER0600	60 Day Evaluation of Red Hat Advanced Cluster Management for Kubernetes, Standard (2 Cores or 4vCPU)
SER0601	Red Hat Advanced Cluster Management for Kubernetes, Self-Support (2 Cores or 4vCPUs, NFR, Partner Only)
SER0602	Red Hat Advanced Cluster Management for Kubernetes, Standard (2 Cores or 4vCPUs, NFR, Partner Only)

ACM Subscription Types

- ACM Subscriptions are only based on the number of logical cores in the Kubernetes clusters to be managed, so called *Managed Clusters*.
 - No cost per application managed
- One base subscription type:
 - Advanced Cluster Management - 2 Core
 - Available with Standard or Premium support
- **Stackable** (can be combined to cover “bigger” hosts/VMs)
- **Cannot split 2-core subscription**
 - Systems, when registered and subscribed in a managed cluster, consume in 2-core units
 - There is no way at present to consume one core from a subscription
 - If a system only effectively needs 3 cores, two 2-core subscriptions would be consumed.
- **Red Hat does not offer disaster recovery (DR)/cold backup type of subscription**
 - Any system with ACM installed, powered-on or powered-off, running workload or not, requires an active subscription.
- **ACM has Supported and Self-supported Evals as well as NFR SKUs.**
 - Supported Evals are available through the [Sales Assisted Eval](#) page
 - Self Supported Evals are available through the [main product page](#)

Cores vs. vCPUs and hyperthreading

- Virtual machines use virtualized CPUs.
- For hyperthreaded systems
 - To determine whether a particular system supports hyperthreading, visit <https://access.redhat.com/solutions/7714>
 - You can see two vCPU per underlying physical core
 - Red Hat calculates cores with a ratio of 2 core = 4 vCPUs
 - In other words, a 2-core subscription covers 4 virtual CPUs in a VM

Example: An 8 vCPU VM has 4 effective “cores”, and would need two (2) 2 core subscriptions.

- For non-hyperthreaded systems
 - You can see one vCPU per underlying physical core
 - Red Hat calculates cores with a ratio of 2 cores = 2 vCPUs
 - In other words, a 2-core of a subscription covers 2 virtual CPUs in a VM on a non-hyperthreaded system

Example: An 4 vCPU VM has 4 effective “cores”, and would need two (2) 2 core subscriptions.

Where can I run Red Hat ACM?

Anywhere OCP x86 is supported and tested:

- Bare metal (Tech Preview in RHACM 2.0)
- Virtual
 - VMware vSphere
 - Hyper-V
 - Red Hat Virtualization
- Private cloud
 - Red Hat OpenStack Platform
- Any OCP-certified public cloud
 - Amazon Web Services, Google Cloud Platform, Microsoft Azure, etc.
 - Cloud Access subscription transfer is required
 - <https://www.redhat.com/en/technologies/cloud-computing/cloud-access>
- For more information on tested platforms: [RHACM 2.0 Support Matrix](#)

Red Hat Advanced Cluster Management for Kubernetes

Roadmap :: 2020 And Beyond



Technical Preview 1.0

- Create, upgrade & delete OCP clusters with **Hive**
- Import and manage existing OCP, IKS, ROKS, EKS, AKS, GKE clusters
- Security compliance configuration, IAM, and certificate policies out of the box
- Multi-cluster application delivery with subscription and channel
- Disconnected installation for hub and managed clusters

May 2020

July 2020

General Availability 2.0

- Upstream strategic elements of the ACM control plane
- Application topology status improvements for SRE
- Validate upstream projects including **Cincinnati** (disconnected upgrades), and **Observatorium** (multi-cluster monitoring)
- Serviceability alignment with **Telemetry** and **Insights**
- *Tech Preview* Bare Metal Cluster Lifecycle with **Hive**

General Availability 2.1

- GA Bare Metal, vSphere, RHV, OpenStack IPI using **Hive**
- Discover and import OpenShift from cloud.redhat.com
- GitOps Collaboration with **ArgoCD** community
- GA Multi-cluster monitoring with Observatorium/**Thanos**
- Integrate **Ansible** into key ACM Lifecycle events.
- Improve the SRE user experience with Visual Web Terminal
- Compliance as code (**Compliance Operator**) Phase 1

Oct 2020

Beyond

- Cluster Lifecycle for ARO, OSD, MOA
- Lifecycle and portability for Stateful Applications HA/DR/Migration use cases
- Multi-cluster network configuration with **Service Mesh** and **Submariner**
- Management for OpenShift **Virtualization**
- Integrate **Cost Management** from OCM for Chargeback and App Placement use cases

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

 youtube.com/user/RedHatVideos

 facebook.com/redhatinc

 twitter.com/RedHat