



Advanced Cluster Management for Kubernetes

Alfred Bach
PSA EMEA

Robust. Proven. Award winning.



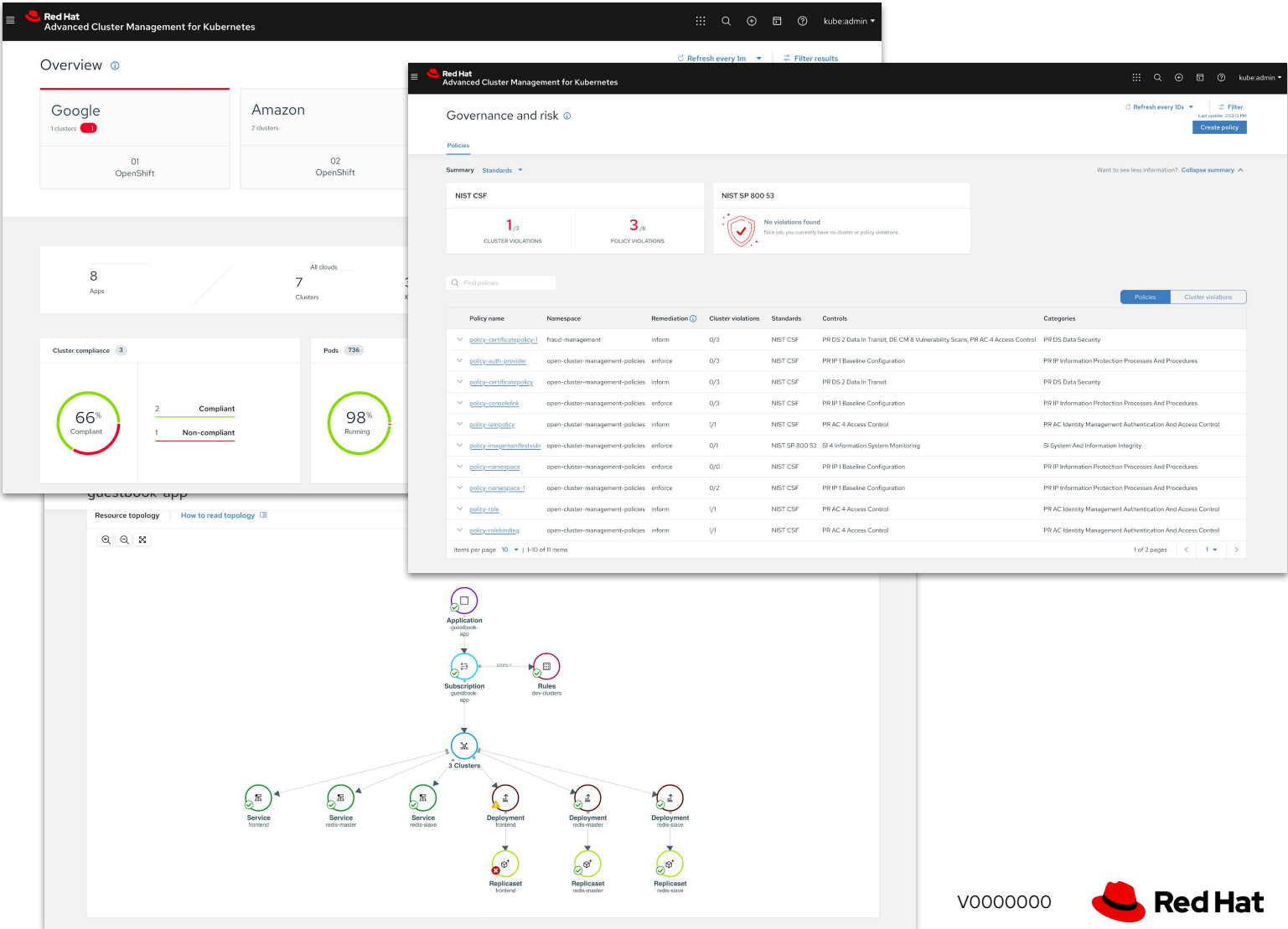
Multicloud lifecycle management



Policy driven governance, risk, and compliance



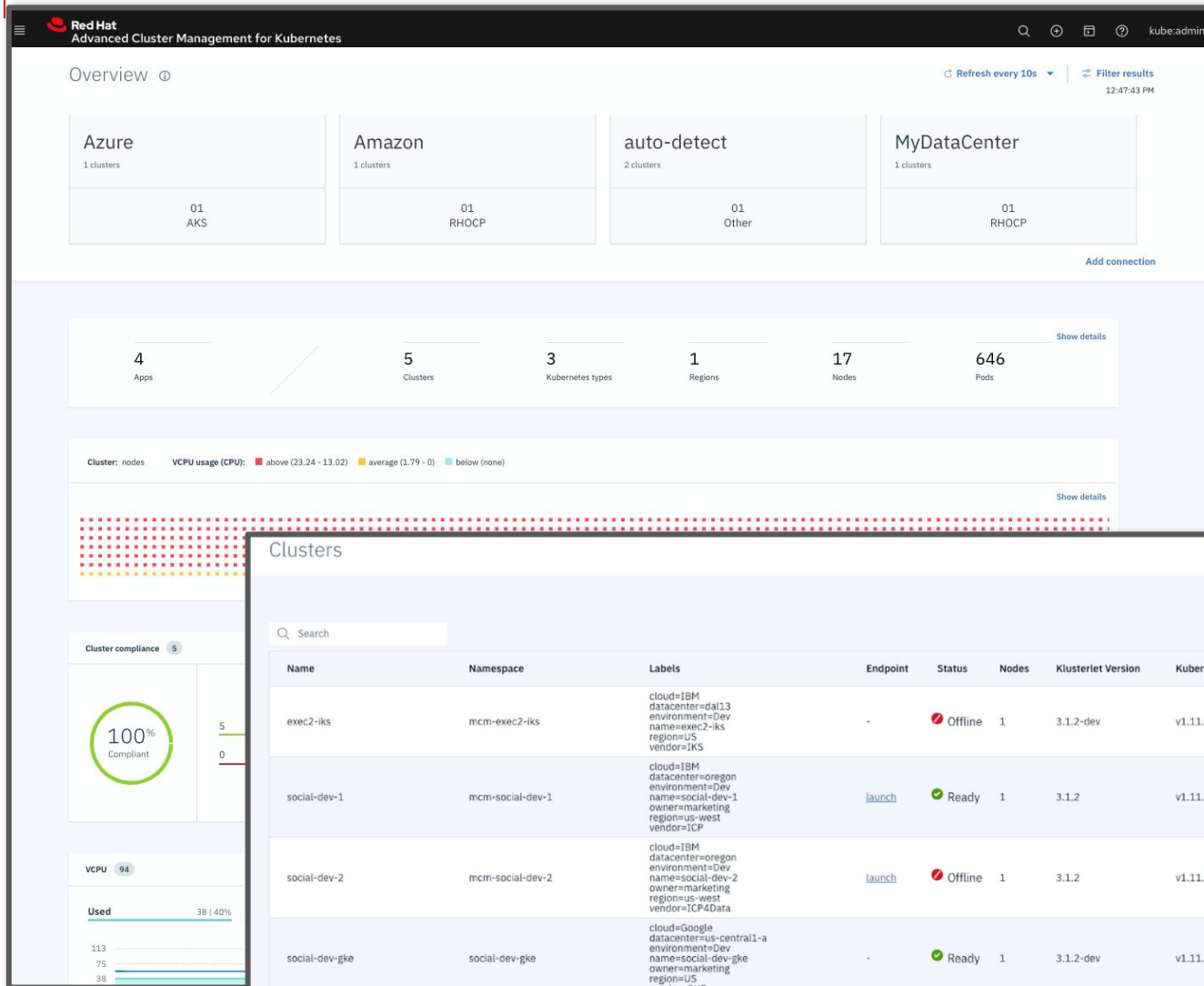
Advanced application lifecycle management



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

Policy based Governance, Risk and Compliance

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

CONFIDENTIAL designator

Top violations

Count	Policy Name	Training
1	policy-cis	training-1
1	policy-grc	training-2
1	policy-role	training-2

Top security findings

Count	Policy Name	Training
2	Policy violation finding	training-1 (2)

Most impacted controls

Key

- Policy violations
- Security findings

compliancePolicy

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
```

Object Templates

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	-	-

items per page 20 | 1-3 of 3 items

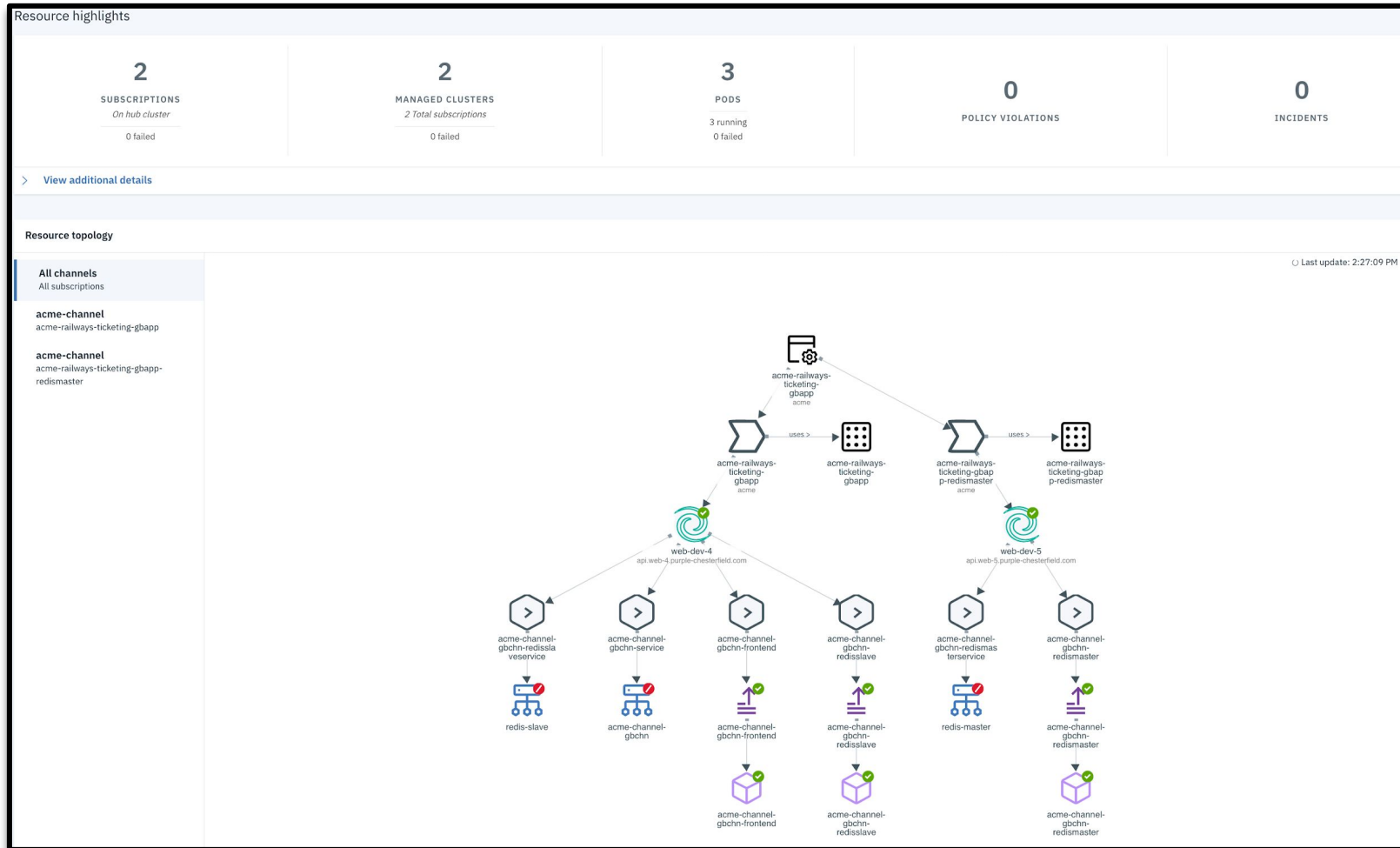
1 of 1 pages < 1 >

- **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

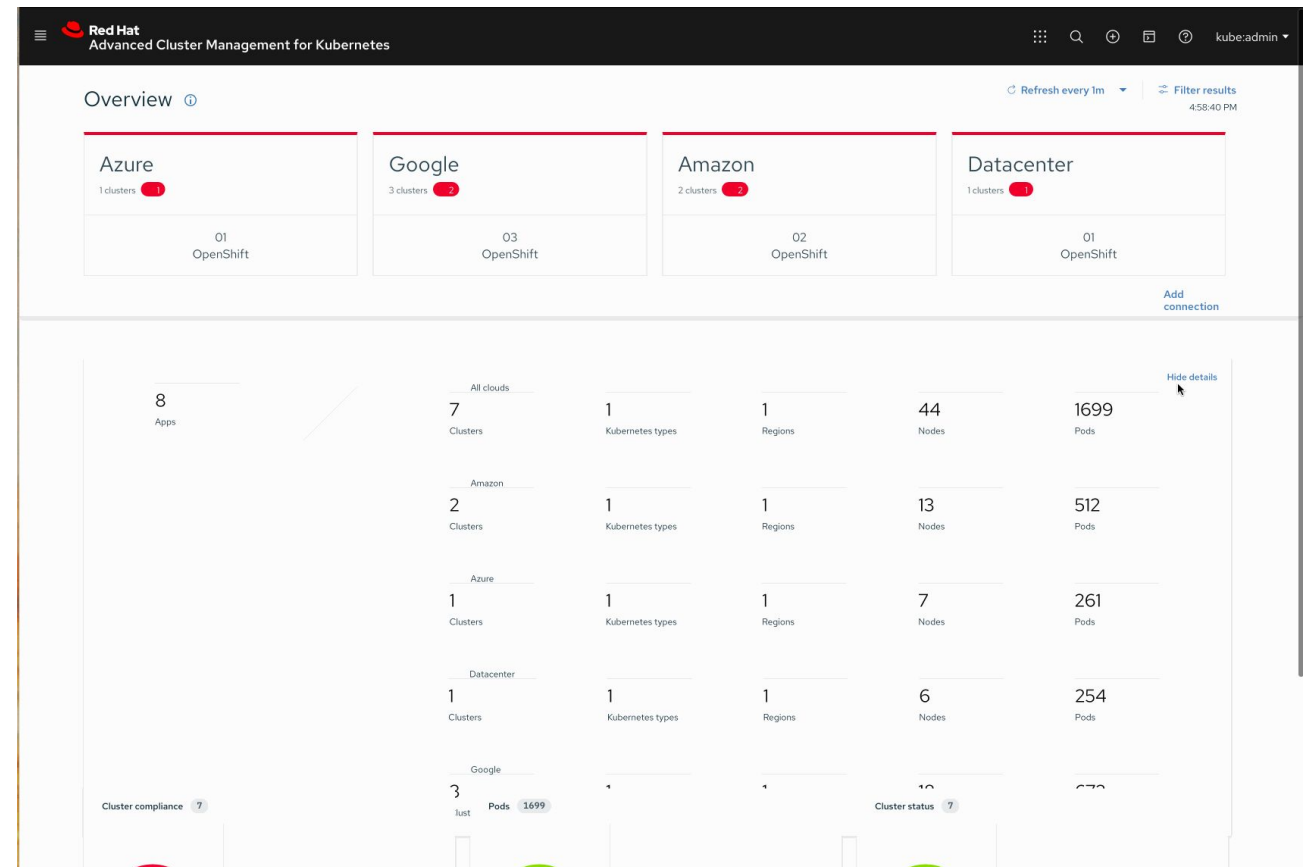
- Full Management of OCP Kubernetes
 - OpenShift 3.11, 4.1.x - 4.11.x
 - Public cloud hosted: OCP
- Public cloud managed kubernetes: EKS, AKS, GKE, IKS
 - Search, find and modify kubernetes resources.
- See high level summaries across all clusters
 - Misconfiguration
 - Pod status
 - Resource capacity
- 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

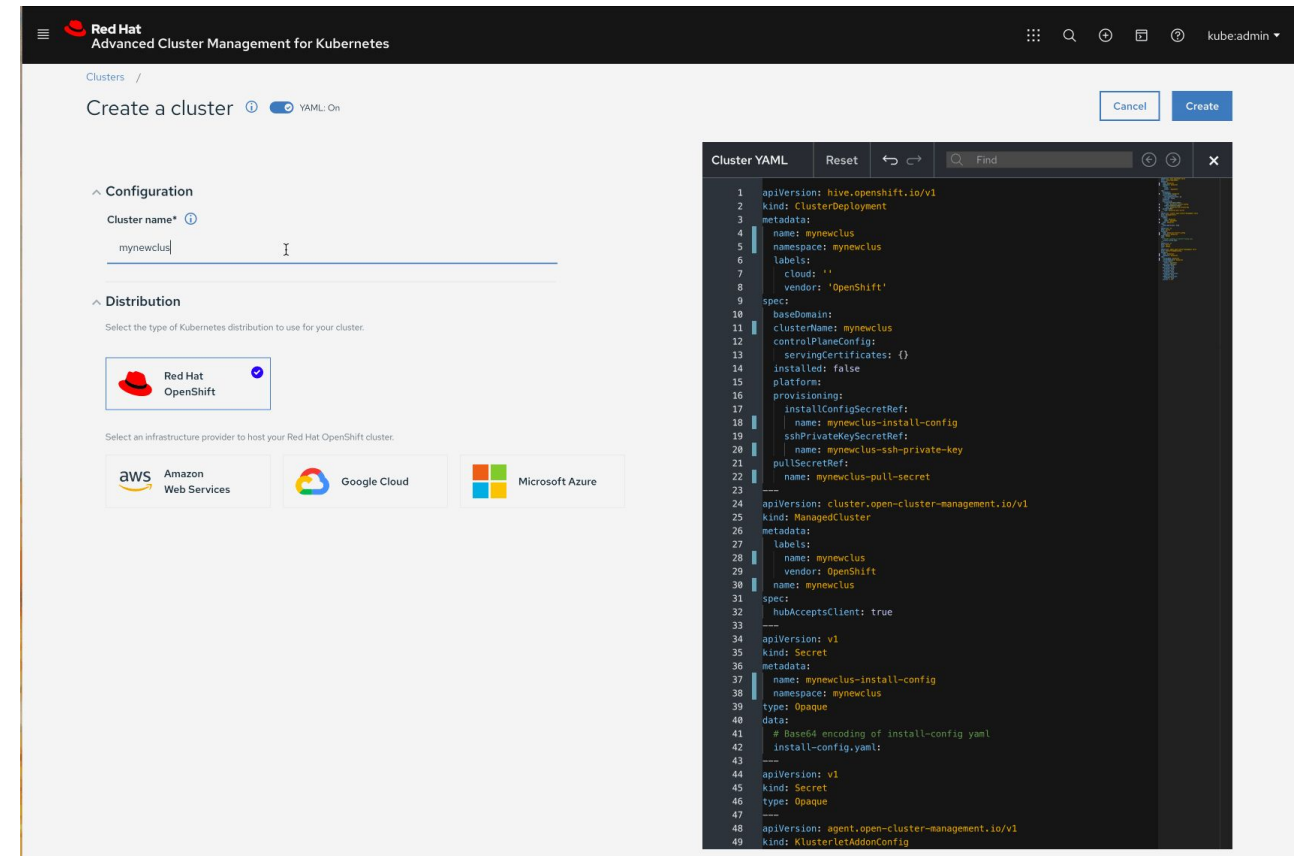
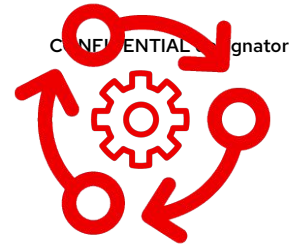
- **Create, Upgrade** and **Destroy** OCP clusters running on **Bare-metal** as well as public cloud
- Leverage **Hive API** for OCP cluster deployment
- Wizard or YAML based create cluster flow
- Launch to an OCP Console from ACM
- Access cluster login credentials and download kubeadmin configuration



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

The screenshot shows the Red Hat ACM console interface. At the top, there's a search bar with the text "Search". Below it, a dropdown menu shows "Unhealthy pods" selected. A search query is entered: "kind:pod X status:Pending,Error,Failed,Terminating,ImagePullBackOff,CrashLoopBackOff,RunContainerError,ContainerCreating". Below the search bar, there are several filters for related resources: 2 RELATED CLUSTER, 2 RELATED SECRET, 6 RELATED NODE, 1 RELATED APPLICATION, 2 RELATED DEPLOYMENT, 2 RELATED REPLICASET, 1 RELATED CHANNEL, 2 RELATED SERVICE, and 3 RELATED SUBSCRIPTION. Below these filters, a table titled "Pod (6)" shows a list of pods. The table has columns: Name, Namespace, Cluster, Status, Restarts, Host IP, Pod IP, Created, and Labels. The pods listed are all in the "guestbook-app" namespace and have a status of "CrashLoopBackOff".

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-6cb7f8bd65-4grgm	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

Multi-Cluster Lifecycle Management

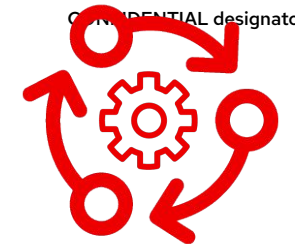
Visual Web Terminal **Tech-Preview**



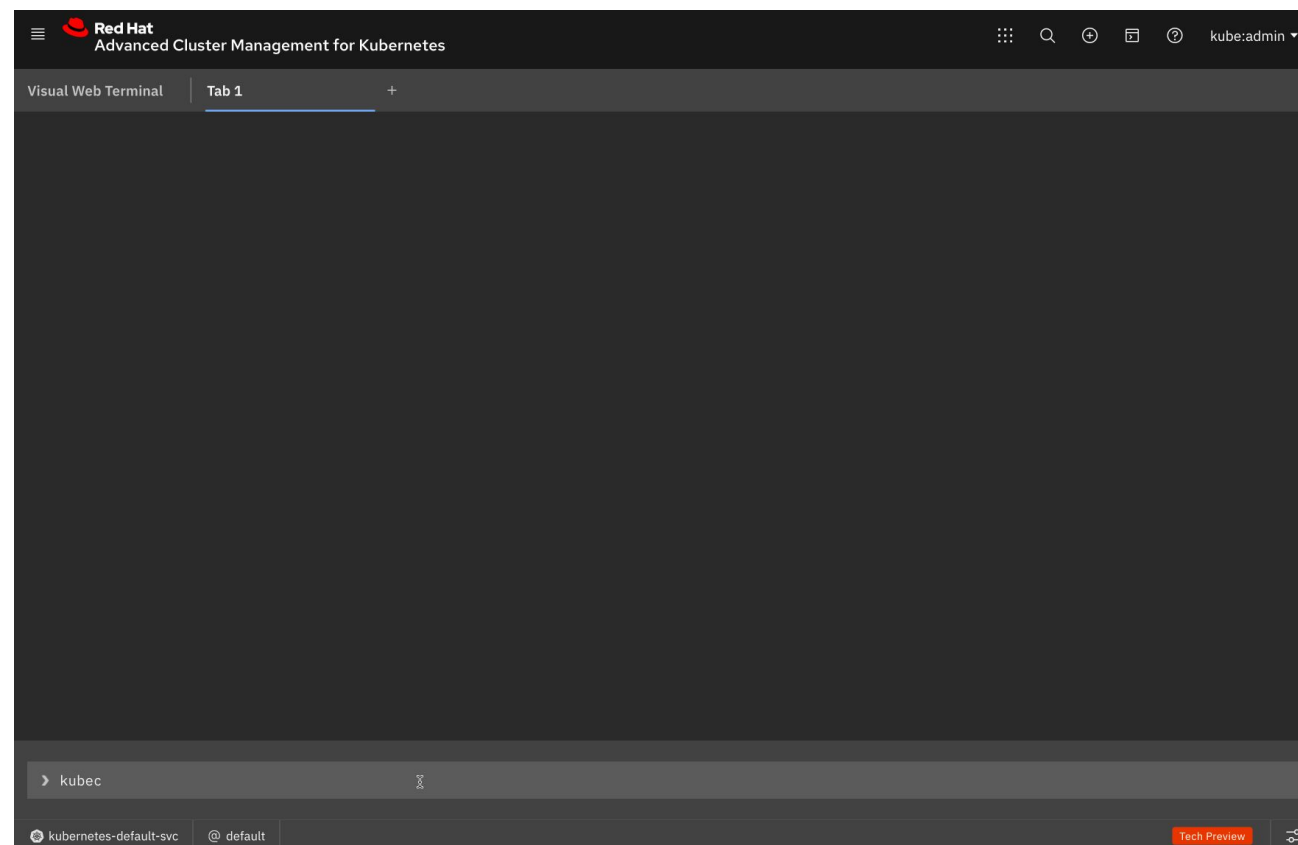
IT Operations



DevOps/SRE



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



Policy Driven Governance Risk and Compliance

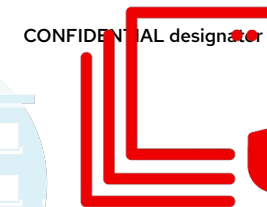
Architecture Overview



Security Ops

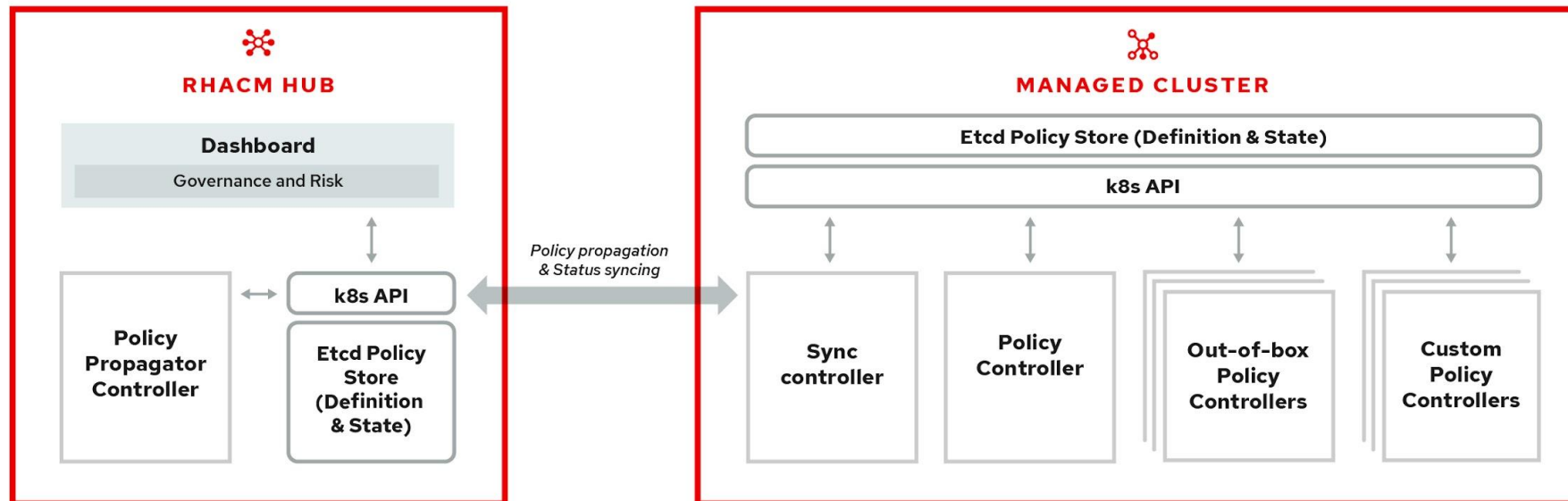


IT Operations



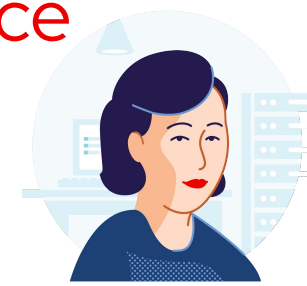
Managed Cluster and GRC Controllers

- 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

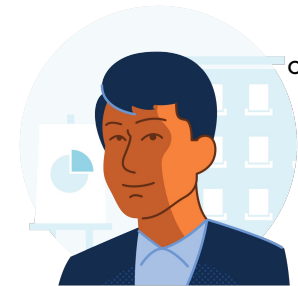


Policy based Governance, Risk and Compliance

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



Security Ops



IT Operations



- 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

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:
```

Policy based Governance, Risk and Compliance

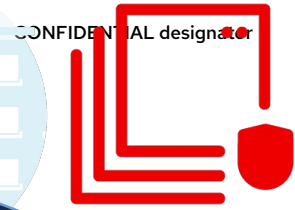
Don't wait for your security team to tap you on the shoulder



Security Ops



IT Operations



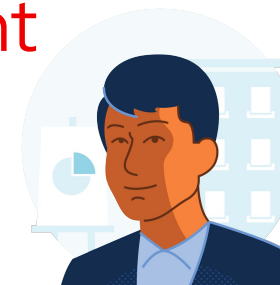
- Standard Policies out of the box
 - FISMA
 - HIPAA
 - NIST
 - PCI
- Leverage Different Categories to Represent more standards (if Needed)
- Use Labels to enforce policies against clusters
- Use **inform** to view policy violations
- Use **enforce** to view violations and automatically remediate

The screenshot shows the Red Hat Advanced Cluster Management for Kubernetes console. The main heading is 'Create policy' with a 'YAML: On' toggle. The form is divided into several sections: '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). At the bottom, there is a checkbox for 'Enforce if supported'. To the right, the 'Policy YAML' editor is open, showing the following code:

```
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

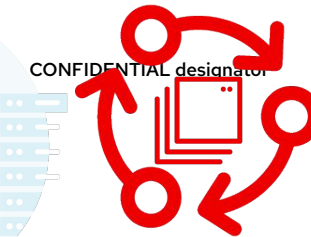
Simplify your Application Lifecycle



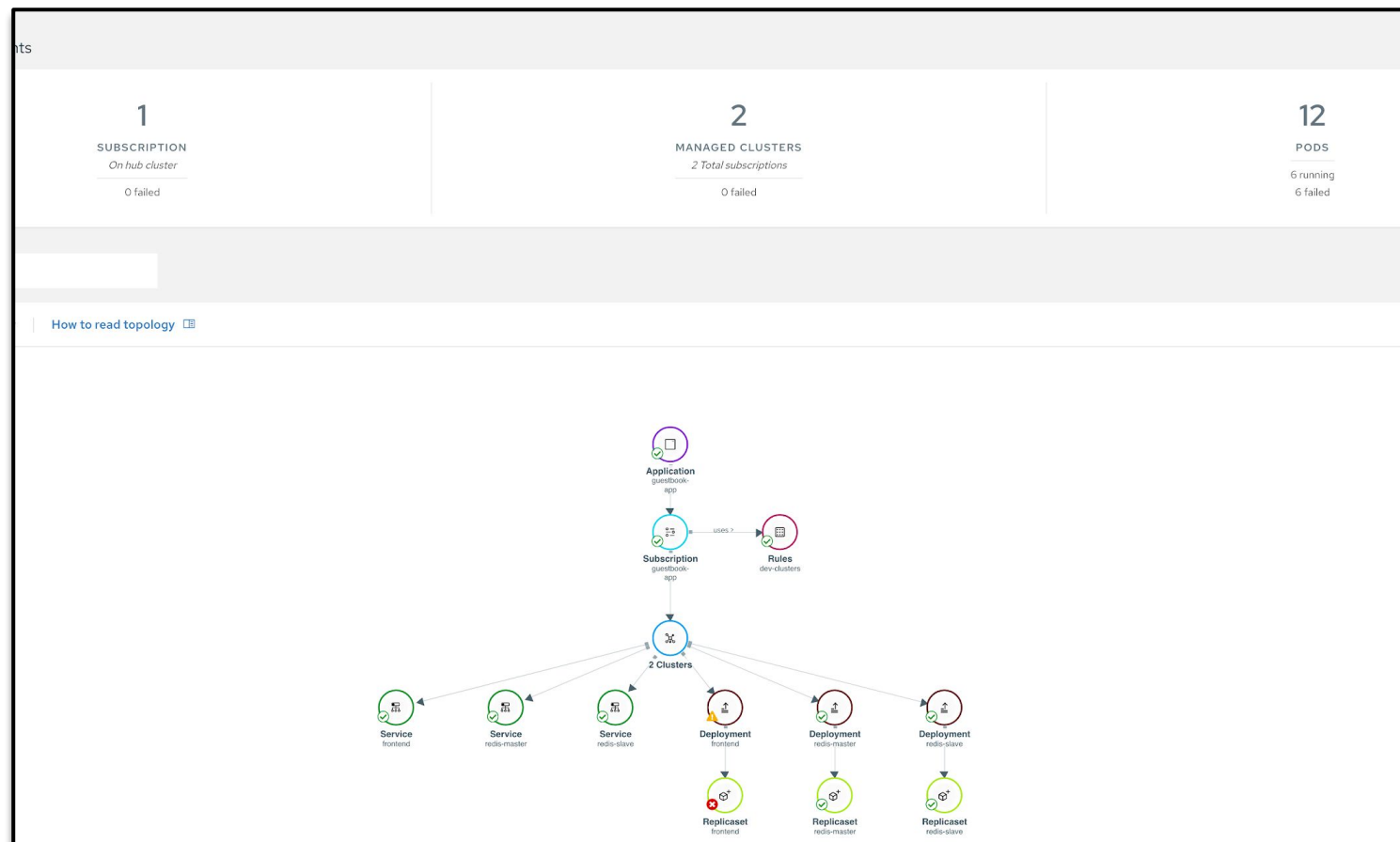
IT Operations



DevOps/SRE



- 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

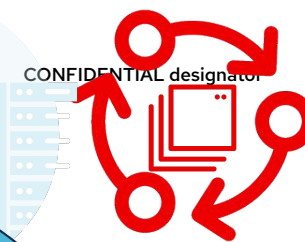
Subscriptions Bring Enterprise to Kubernetes



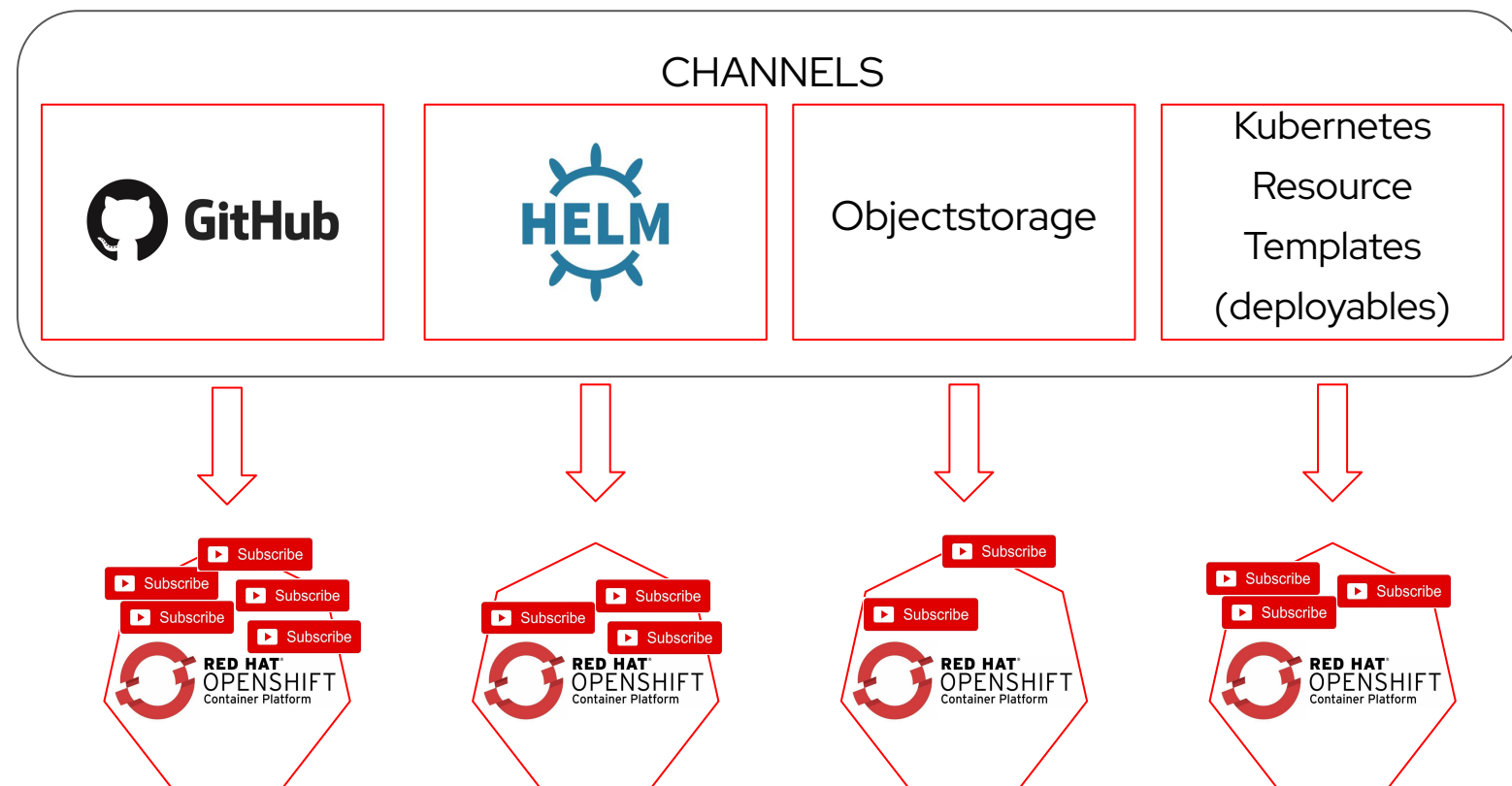
IT Operations



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

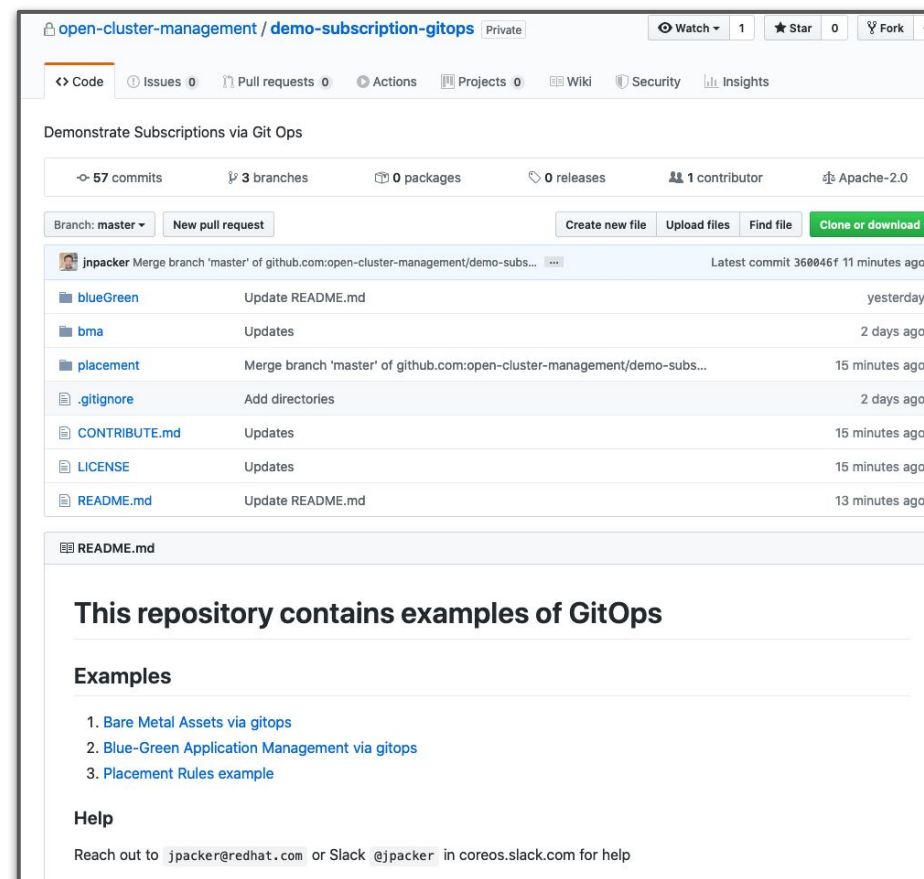
- Create, modify & delete, just as you would any source code. Git becomes your source of truth controlling your data center.
- Have a record of who, what & when for every change precipitated in your environments
- Through code Reviews & Approvals, take full control of all changes to your data center(s)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



IT Operations



DevOps/SRE



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

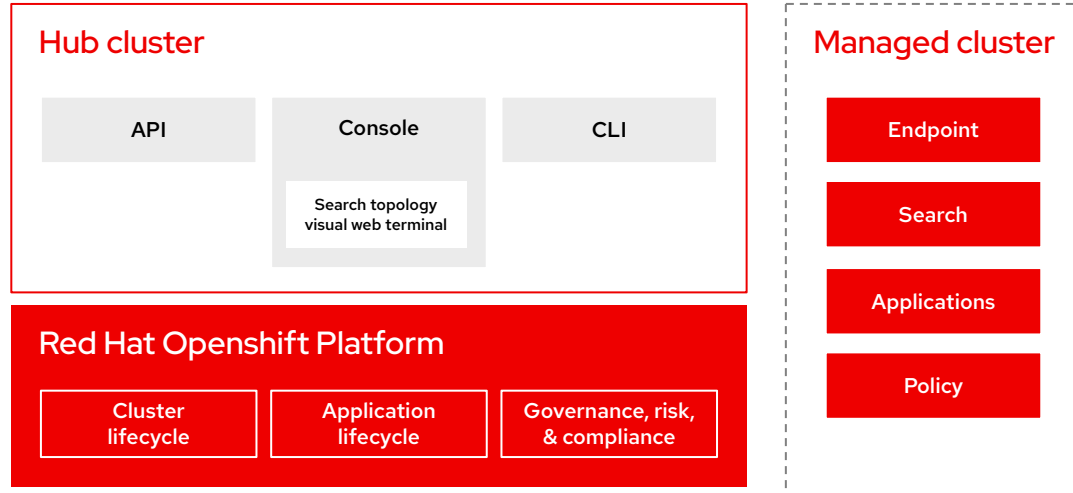
Architecture

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 ->

Full Management of OCP clusters

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

Limited Support for Public cloud managed Kubernetes

- EKS, AKS, GKE, IKS

High Availability

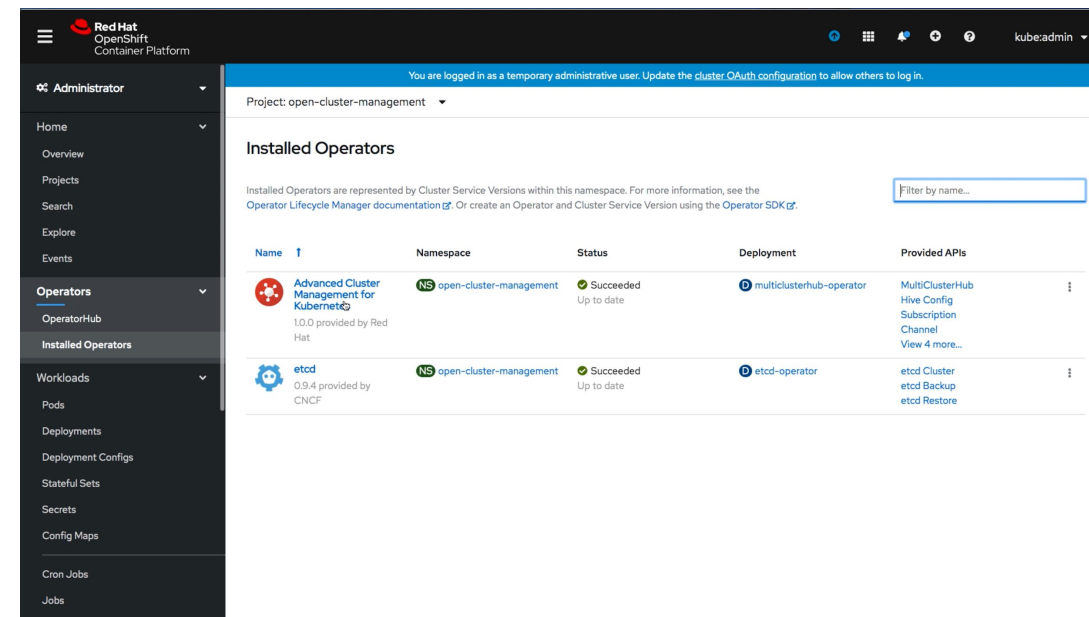
- Supports OCP Availability Zone
- Limitation for Search component based on RedisGraph

Resource Requirements

- **Test:** 3 master, 3 workers, 6 v CPU and 16GB RAM
- **Production:** 3 masters, 3 workers, 16vCPU and 24GB RAM*

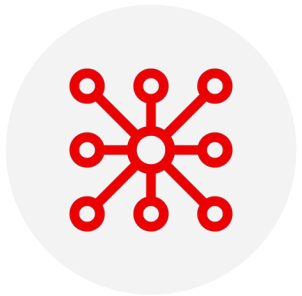
* Production requirements vary based on number of clusters in the management domain and types of workloads being run.

* 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

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