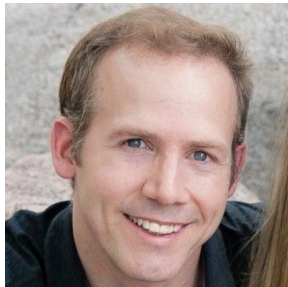


Introduction to Red Hat Advanced Cluster Management

Dean Peterson
Full Stack Solution Architect
dpeterso@redhat.com





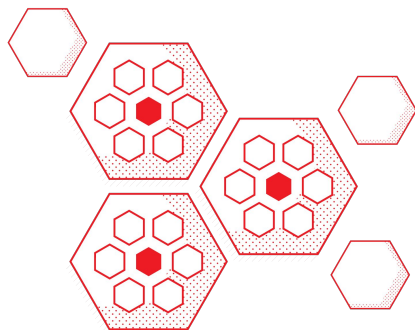
Dean Peterson

Specialist Solution Architect
dpeterso@redhat.com

What we'll discuss and show today

- ★ Why Multicloud Kubernetes?
- ★ Introduction to Advanced Cluster Management
- ★ Demo
 - Cluster Management
 - Application Lifecycle Management
 - Governance, Risk, and Compliance (GRC)
 - Cluster Visibility

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, multicloud, or edge deployments.”

Where is the growth in cluster deployments?



Small Scale Dev teams

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



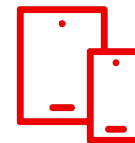
Medium Scale Organizations

- 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



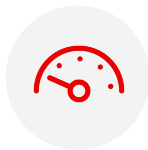
Edge Scale Telco

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

Reasons for deploying clusters



Application
availability



Reduced
latency



Address industry
standards



Geopolitical data
residency guidelines



Disaster
recovery



Edge
deployments



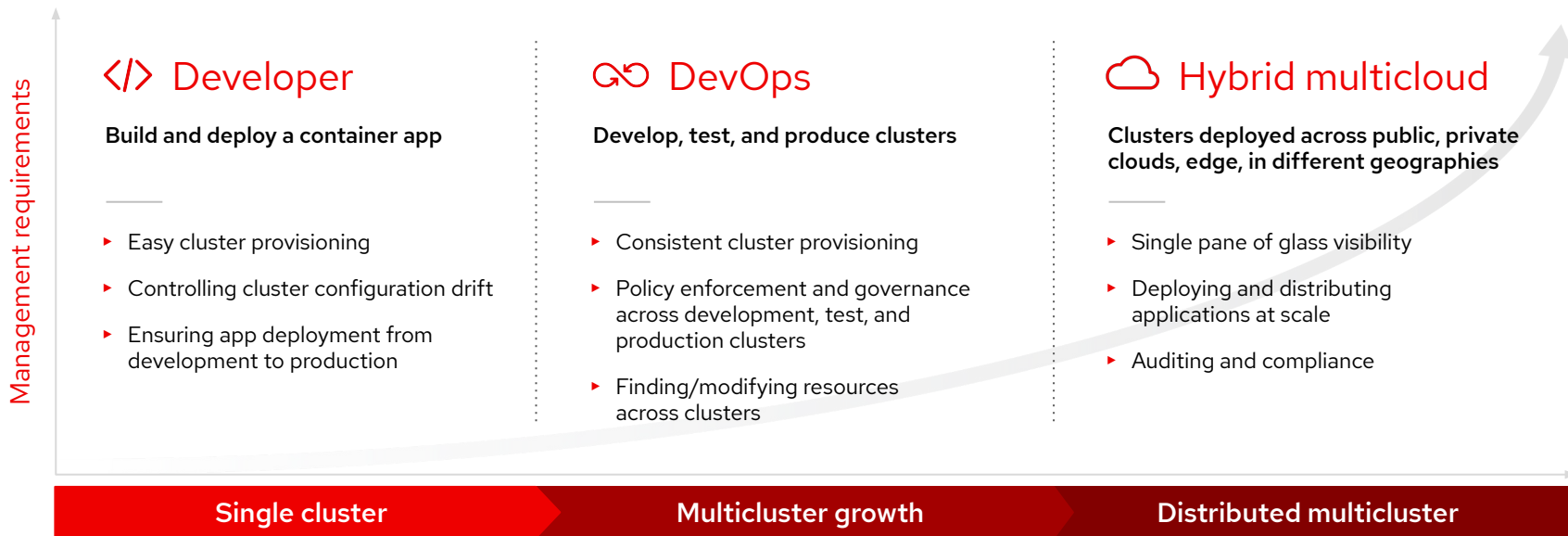
CapEx
cost reduction



Avoid vendor
lock-in

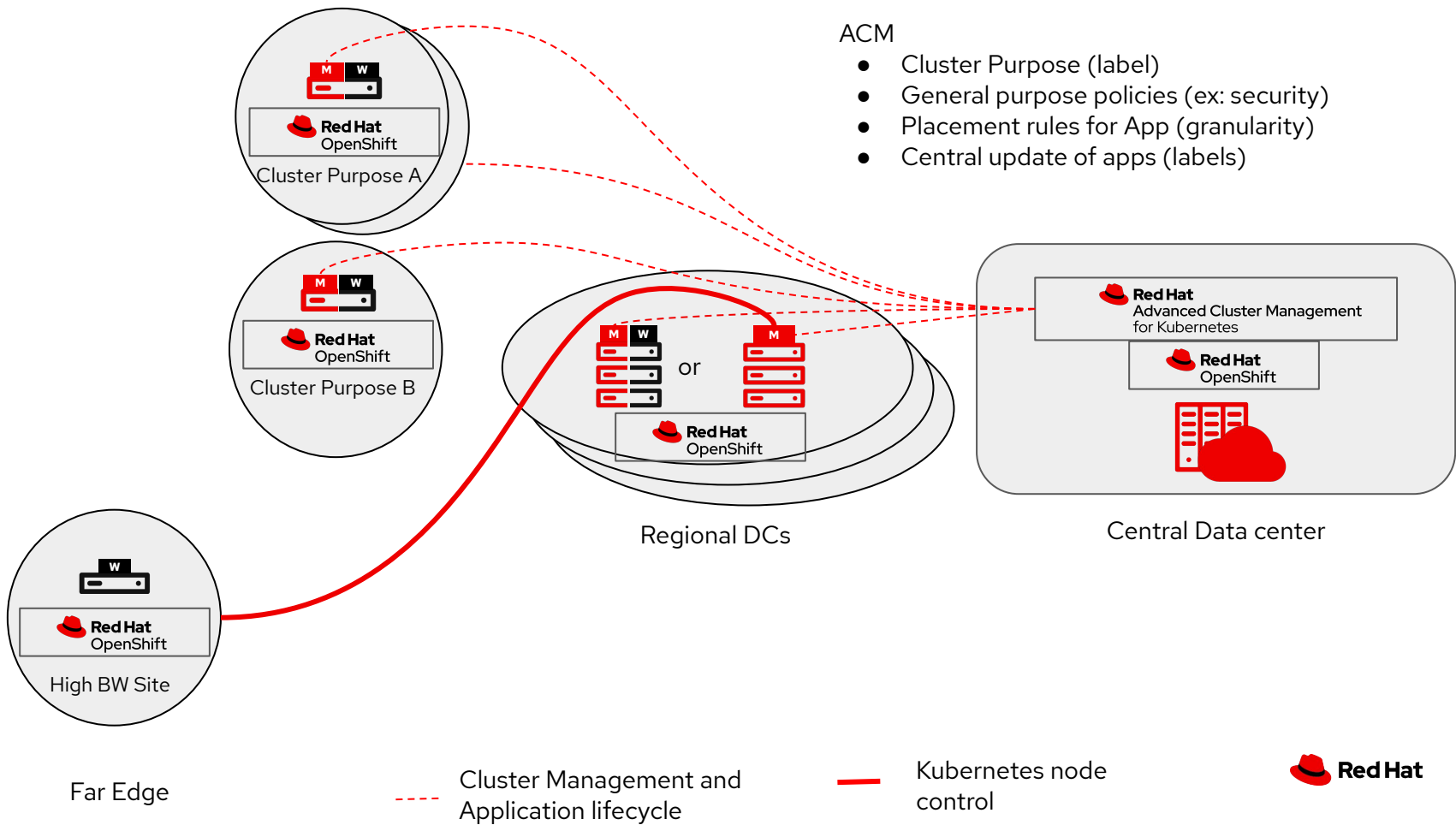
Multicluster management challenges

How do I normalize and centralize key functions across environments?



ACM and Edge deployment in a Nutshell

Edge computing with Red Hat





Red Hat Advanced Cluster Management for Kubernetes

Robust. Proven. Award winning.



Multicluster lifecycle
management



Policy driven governance,
risk, and compliance



Advanced application
lifecycle management

Key personas



IT Operations

- ▶ How can I manage the lifecycle of multiple clusters regardless of where they reside 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 on my application availability?
- ▶ How do I automate: provisioning/deprovisioning of my clusters, the placement of workloads based on capacity and policy, and the pushing of 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?

Unified Multi-Cluster Management

CONFIDENTIAL designator

Single Pane for all your Kubernetes Clusters

The screenshot displays the Red Hat ACM interface. The top section shows an overview of clusters categorized by provider: Azure (1 cluster: 01 AKS), Amazon (1 cluster: 01 RHOC), auto-detect (2 clusters: 01 Other), and MyDataCenter (1 cluster: 01 RHOC). Below this, a summary bar indicates 4 Apps, 5 Clusters, 3 Kubernetes types, 1 Region, 17 Nodes, and 646 Pods. A VCPU usage chart shows 100% compliance. The main section is a 'Clusters' table with the following data:

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-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=ICP	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%

- **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

Multi-Cluster Lifecycle Management

Overview

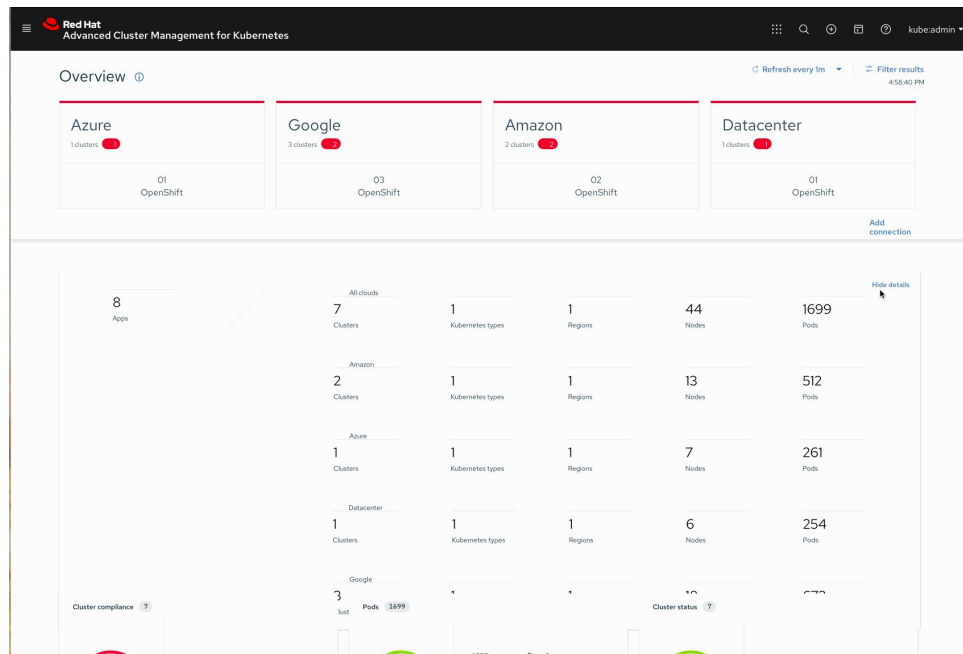
- Full Management of OCP Kubernetes
 - OpenShift 3.11, 4.1.x - 4.5.x
 - Public cloud hosted: OCP
- Public cloud managed kubernetes: EKS, AKS, GKE, IKS
 - Search, find and modify kubernetes resources.
- See high level summaries across all clusters
 - Misconfiguration
 - Pod status
 - Resource capacity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



Policy based Governance, Risk and Compliance

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

CONFIDENTIAL designator

The screenshot displays the 'Governance and risk' dashboard in the Red Hat ACM console. At the top, there are navigation options for 'Policies' and 'Standards'. A summary section shows '1/3 CLUSTER VIOLATIONS' and '3/3 POLICY VIOLATIONS'. A 'NIST SP 800 53' compliance card indicates 'No violations found'. Below this is a search bar for policies and a table of policy details.

Policy name	Namespace	Remediation	Cluster violations	Standards	Controls	Categories
policy-certificatpolicy-1	fraud-management	inform	0/3	NIST CSF	PR DS 2 Data In Transit, DE CM 8 Vulnerability Scans, PR AC 4 Access Control	PR DS Data Security
policy-auth-provider	open-cluster-management-policies	enforce	0/3	NIST CSF	PR IP 1 Baseline Configuration	PR IP Information Protection Processes And Procedures
policy-certificatpolicy	open-cluster-management-policies	inform	0/3	NIST CSF	PR DS 2 Data In Transit	PR DS Data Security
policy-consolelink	open-cluster-management-policies	enforce	0/3	NIST CSF	PR IP 1 Baseline Configuration	PR IP Information Protection Processes And Procedures
policy-iampolicy	open-cluster-management-policies	inform	1/1	NIST CSF	PR AC 4 Access Control	PR AC Identity Management Authentication And Access Control
policy-imagemanifestvuln	open-cluster-management-policies	enforce	0/1	NIST SP 800 53	SI 4 Information System Monitoring	SI System And Information Integrity
policy-namespace	open-cluster-management-policies	enforce	0/0	NIST CSF	PR IP 1 Baseline Configuration	PR IP Information Protection Processes And Procedures
policy-namespace-1	open-cluster-management-policies	enforce	0/2	NIST CSF	PR IP 1 Baseline Configuration	PR IP Information Protection Processes And Procedures
policy-rols	open-cluster-management-policies	inform	1/1	NIST CSF	PR AC 4 Access Control	PR AC Identity Management Authentication And Access Control
policy-rolebinding	open-cluster-management-policies	inform	1/1	NIST CSF	PR AC 4 Access Control	PR AC Identity Management Authentication And Access Control

- **Centrally** set & enforce policies for security, applications, & infrastructure
- <https://github.com/open-cluster-management/policy-collection>
- 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

Policy Driven Governance Risk and Compliance

Architecture Overview



Security Ops



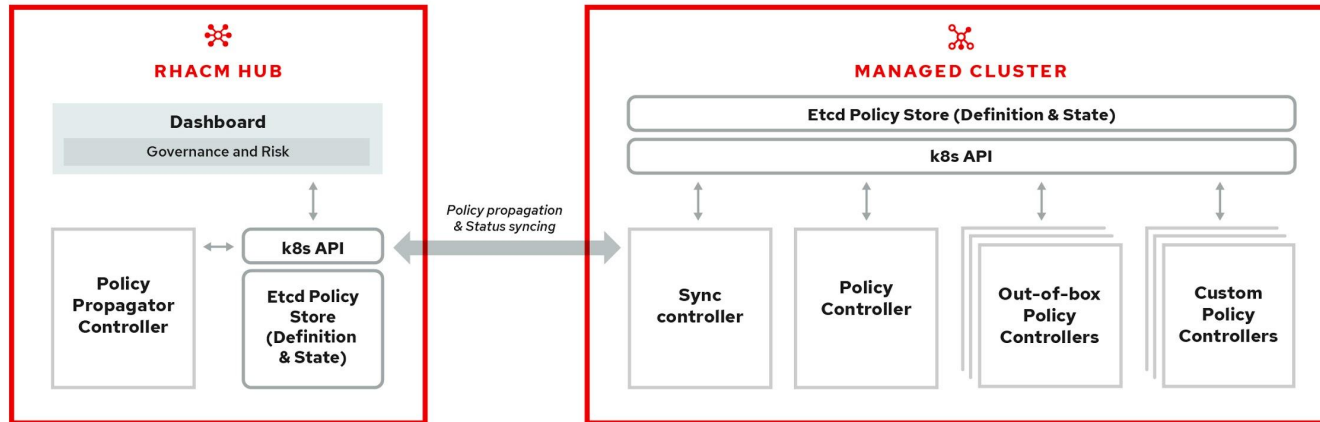
IT Operations

CONFIDENTIAL designer



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



- 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

- 17 • Use **inform** to view policy violations

- Use **enforce** to view violations and automatically remediate

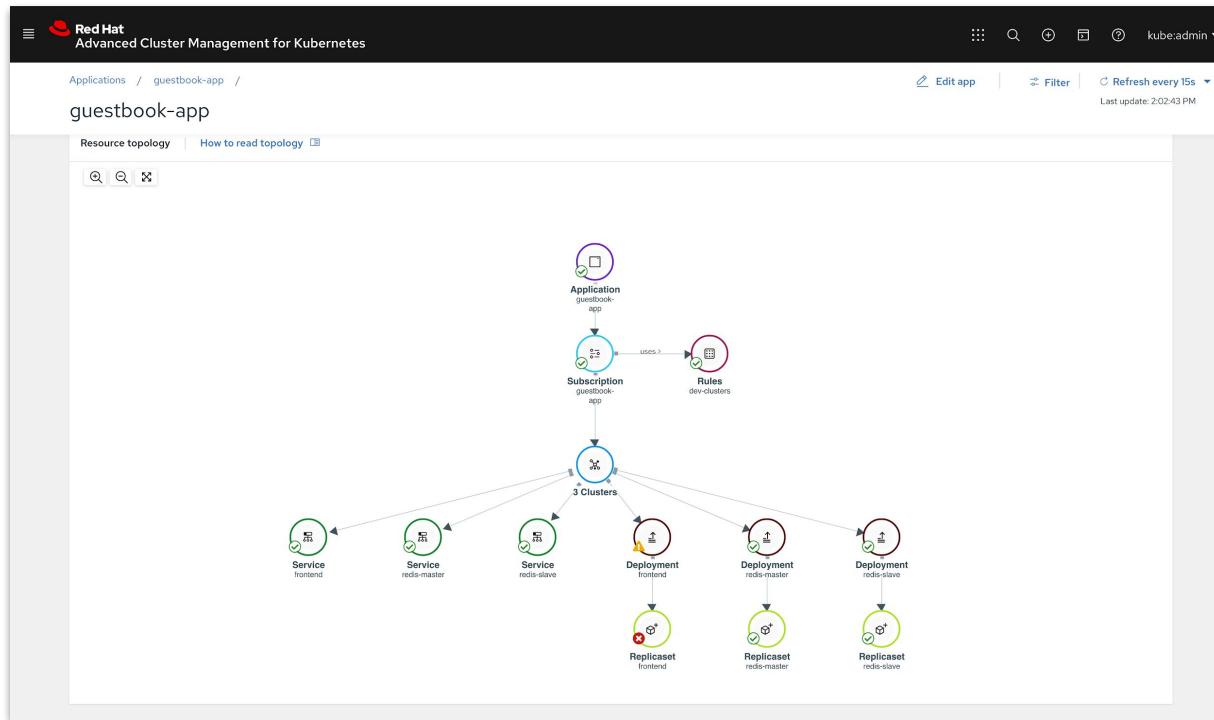
The screenshot shows the Red Hat Advanced Cluster Management for Kubernetes console. The top navigation bar includes the Red Hat logo and the text 'Advanced Cluster Management for Kubernetes'. The breadcrumb trail is 'Governance and risk / Policies /'. The main heading is 'Create policy' with a 'YAML On' toggle. There are 'Cancel' and 'Create' buttons. The form contains 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 appl...), '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 reported'. To the right, a 'Policy YAML' window is open, displaying 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

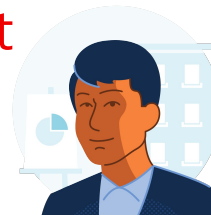
CONFIDENTIAL designer



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

Advanced Application Lifecycle Management

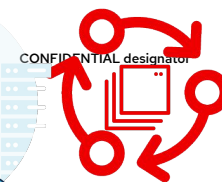
Subscriptions Bring Enterprise to Kubernetes



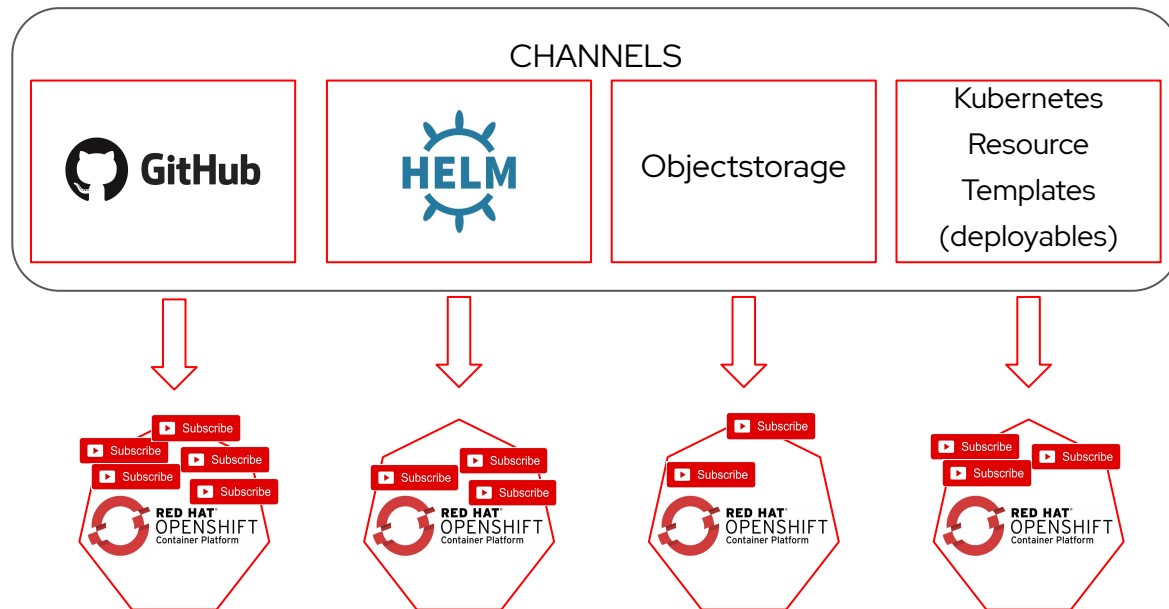
IT Operations



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



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



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

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

```
1 apiVersion: hive.openshift.io/v1
2 kind: ClusterDeployment
3 metadata:
4   name: mynewclus
5   namespace: mynewclus
6   labels:
7     clouds: ""
8   vendor: OpenShift
9 spec:
10  baseDomain:
11  clusterName: mynewclus
12  controlPlaneConfig: {}
13  servingCertificates: {}
14  installMode: false
15  platform:
16  provisioning:
17    installConfigSecretRef:
18      name: mynewclus-install-config
19      namespace: mynewclus
20    sshPrivateKeySecretRef:
21      name: mynewclus-ssh-private-key
22    pullSecretRef:
23      name: mynewclus-pull-secret
24  apiVersion: cluster.open-cluster-management.io/v1
25  kind: ManagedCluster
26  metadata:
27    labels:
28      name: mynewclus
29      vendor: OpenShift
30      namespace: mynewclus
31  spec:
32    hubSecretClient: true
33  ---
34  apiVersion: v1
35  kind: Secret
36  metadata:
37    name: mynewclus-install-config
38    namespace: mynewclus
39    type: Opaque
40  data:
41    # Base64 encoding of install-config.yaml
42    install-config.yaml:
43  ---
44  apiVersion: v1
45  kind: Secret
46  type: Opaque
47  ---
48  apiVersion: agent.open-cluster-management.io/v1
49  kind: ClusterRoleAddOnConfig
```

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 status:Pending,Error,Failed,Terminating,imagePullBackOff,CrashLoopBackOff,RunContainerError,ContainerCreating

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-6cb7f8b065-8tqz	guestbook-app	kilo-bravo	CrashLoopBackOff	35	10.0.135.156	10.129.2.79	3 hours ago	app:guestbook +2
frontend-6cb7f8b065-flj77	guestbook-app	kilo-alpha	CrashLoopBackOff	35	10.0.162717	10.129.2.61	3 hours ago	app:guestbook +2
frontend-6cb7f8b065-rvqkx	guestbook-app	kilo-alpha	CrashLoopBackOff	35	10.0.128.146	10.128.2.177	3 hours ago	app:guestbook +2
frontend-6cb7f8b065-4gqgn	guestbook-app	kilo-alpha	CrashLoopBackOff	35	10.0.147.26	10.131.0.172	3 hours ago	app:guestbook +2
frontend-6cb7f8b065-wpyzm	guestbook-app	kilo-bravo	CrashLoopBackOff	35	10.0.154.41	10.131.0.92	3 hours ago	app:guestbook +2
frontend-6cb7f8b065-kz7lc	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

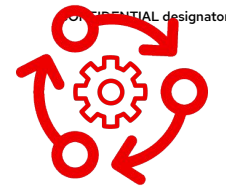
Visual Web Terminal



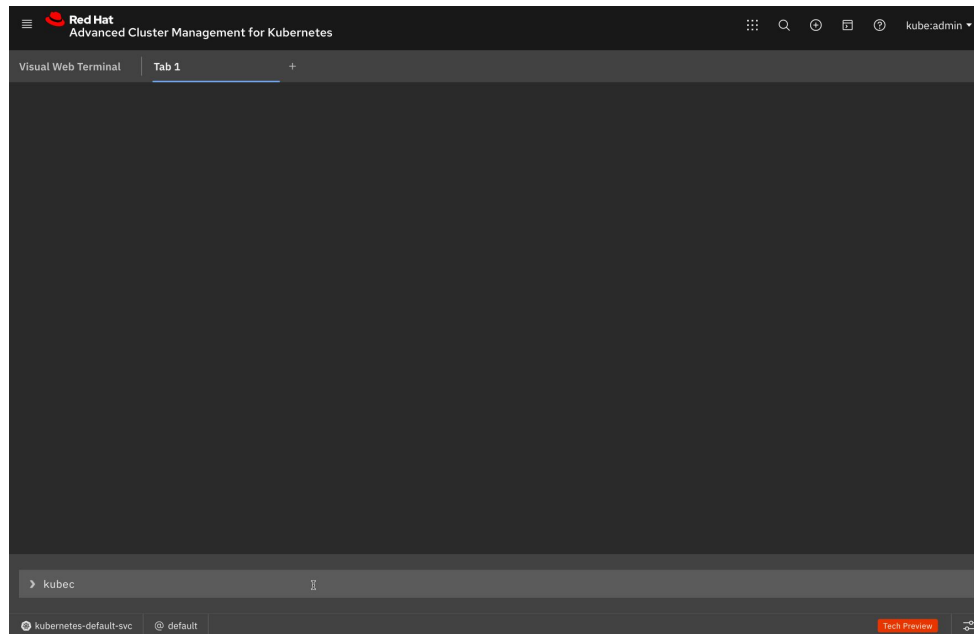
IT Operations



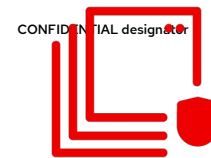
DevOps/SRE



- 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



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 based Governance, Risk and Compliance

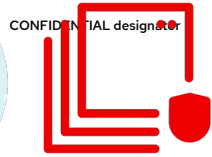
Don't wait for your security team to tap you on the shoulder



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

The screenshot displays the Red Hat Advanced Cluster Management for Kubernetes interface. The main section is titled 'Create policy' with a 'YAML On' toggle and 'Cancel' and 'Create' buttons. Below this, there are several dropdown menus for configuration: '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 appl...), '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'. On the right side, a 'Policy YAML' editor is open, showing two YAML snippets. The first snippet is for a 'Policy' resource with a remediation action of 'inform'. The second snippet is for a 'PlacementRule' resource with a status of 'True' and a cluster selector.

Advanced Application Lifecycle Management

CONFIDENTIAL designator



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.

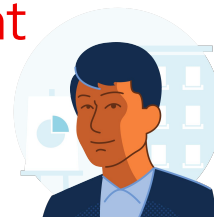


IT Operations

- 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



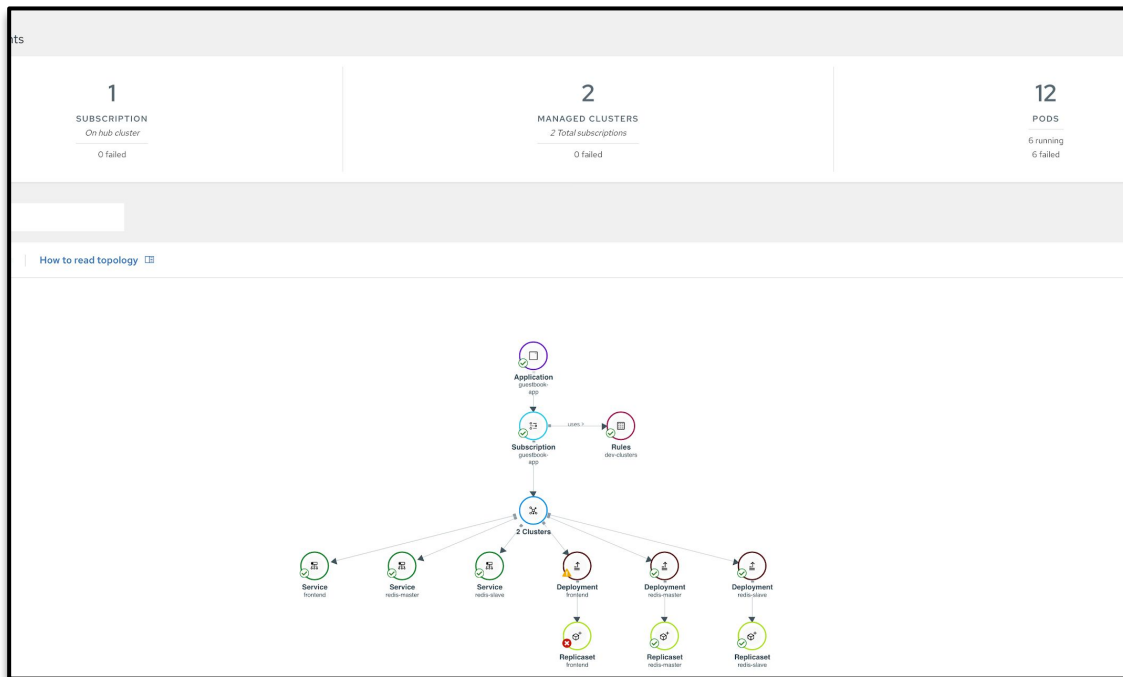
IT Operations



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

GitOps as the source of truth

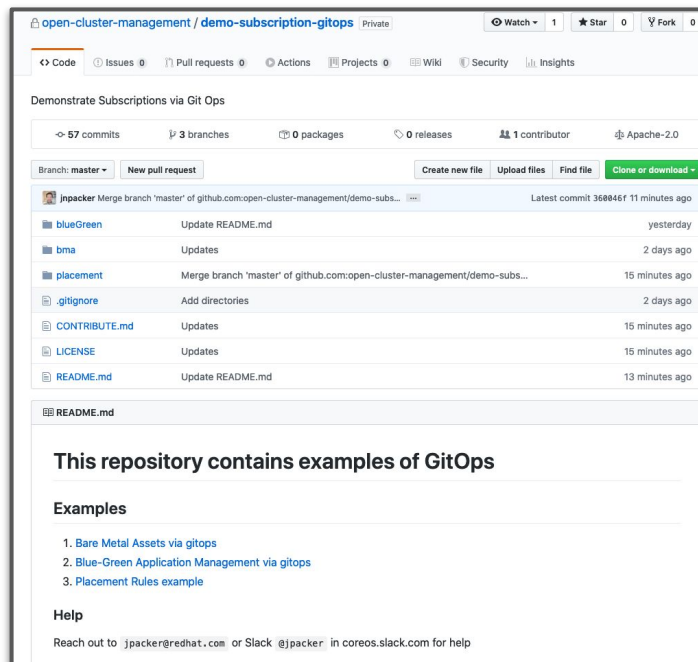
- Create, modify & delete, just as you would any source code. Git becomes your source of truth controlling your data center.
- Have a record of who, what & when for every change precipitated in your environments
- Through code Reviews & Approvals, take full control of all changes to your data center(s)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



IT Operations



DevOps/SRE



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

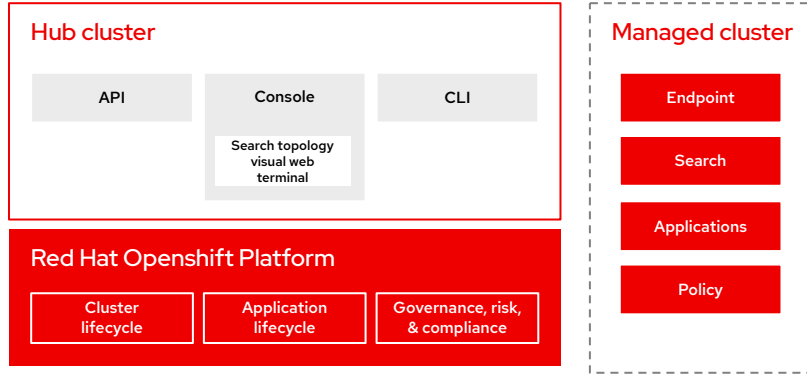
Architecture

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

Demo

