

Red Hat Advanced Cluster Management for Kubernetes

Presenter's Name
Title

Presenter's Name
Title

Why Red Hat Advanced Cluster Management is important

Why you should care

- ▶ App modernization is a top industry priority.
- ▶ Kubernetes is platform modernization.
- ▶ Enterprises are rapidly adopting Kubernetes.
- ▶ There is intense competition for Kubernetes.
- ▶ Not all Kubernetes solutions are equal.
- ▶ Kubernetes management is complicated.

Key solutions



Move quickly and win the platform



Use the best, most complete solution - OpenShift



Differentiate and win Red Hat OpenShift Container Platform



Recognize VMware as the biggest threat

But 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

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

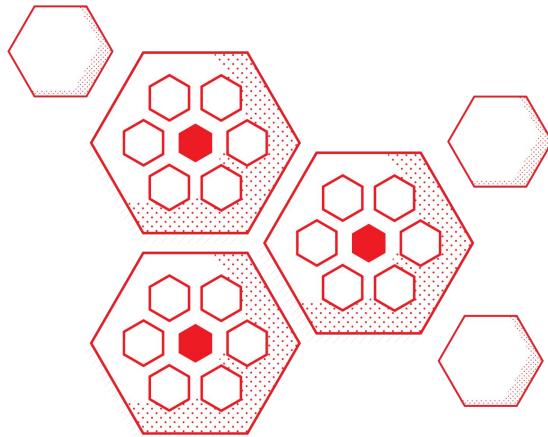


—
Using multiple infrastructure clouds*



—
Using multiple public clouds and one or more private/dedicated clouds*

Kubernetes adoption leads to multicloud



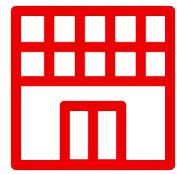
“As Kubernetes gains adoption across the industry, scenarios are arising in which I&O teams are finding **they must deploy and manage multiple clusters**, either in a single region on-premises or in the cloud, or across multiple regions....for a number of reasons, including multi-tenancy, disaster recovery, and with hybrid, multicloud, or edge deployments.”

Where is the growth in cluster deployments?



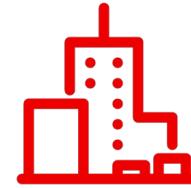
Small Scale Dev teams

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



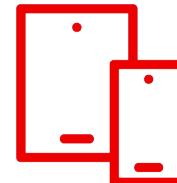
Medium Scale Organizations

- 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



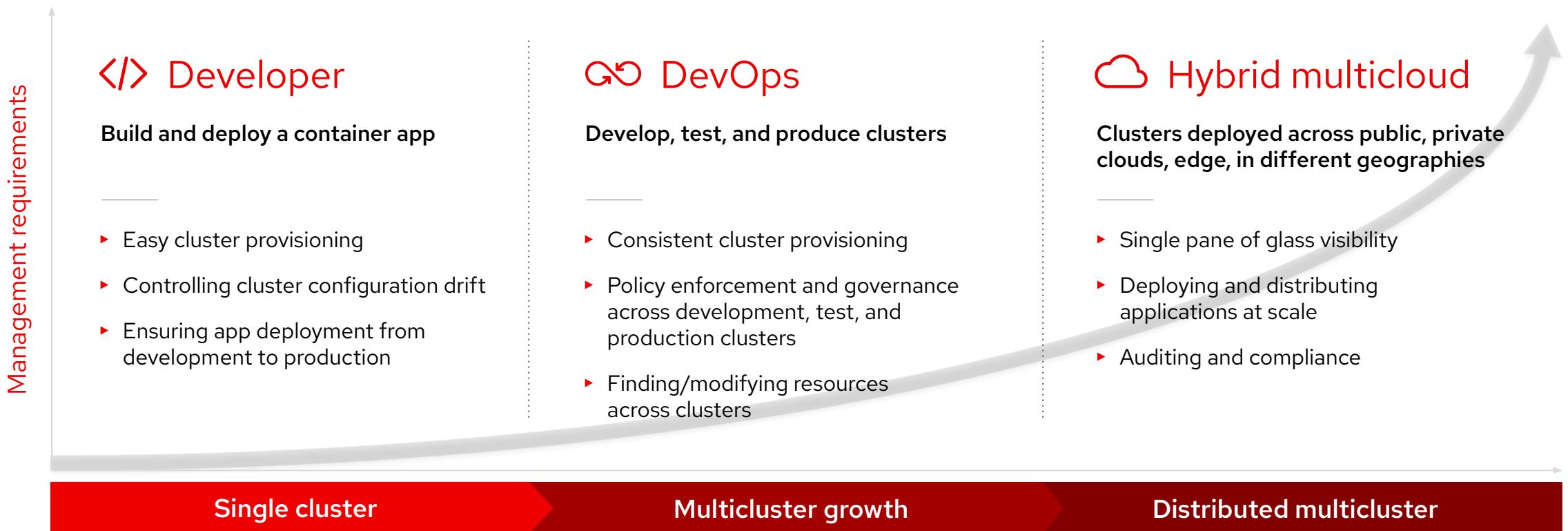
CapEx cost reduction

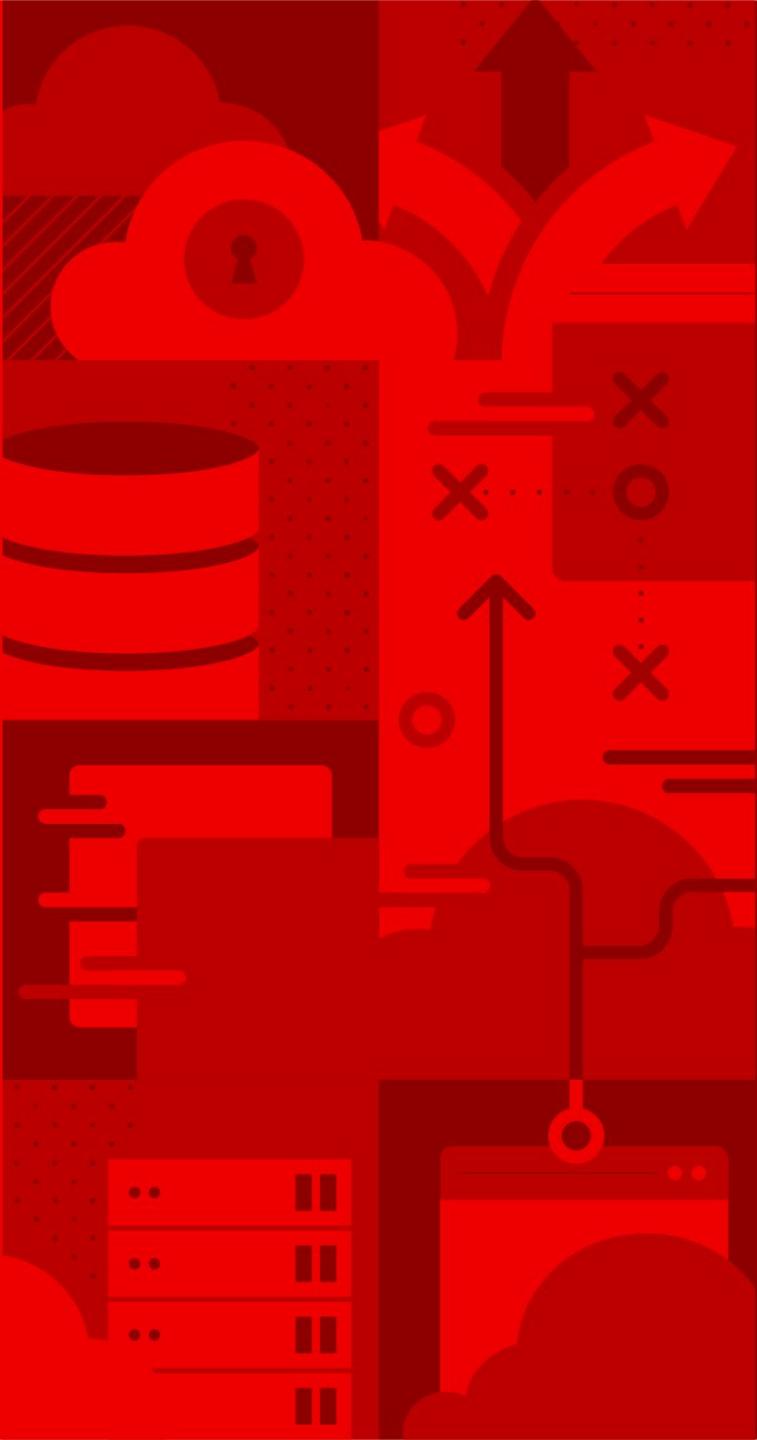


Avoid vendor lock-in

Multicloud management challenges

How do I normalize and centralize key functions across environments?





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



Multicloud observability for health and optimization

Red Hat Advanced Cluster Management for Kubernetes

Overview

Summary

4 Applications, 10 Clusters, 1 Kubernetes type, 5 Regions, 60 Nodes, 2513 Pods

Cluster compliance: 164, 66% Compliant (109 Compliant, 55 Non-compliant)

Pods: 2492, 100% Running (2483 Running, 4 Pending, 5 Failed)

Cluster status: 10, 100% Ready (10 Ready, 0 Offline)

Governance and risk

NIST-CSF: 10 / 10 Cluster violations, 8 / 11 Policy violations

NIST SP 800-53: 2 / 2 Cluster violations, 1 / 1 Policy violations

NIST: No violations found

PCI: No violations found

Find policies

Policy name	Namespace	Remediation	Cluster violations	Standards	Categories	Controls	Created
policy-grc-nist	open-cluster-management-policies	inform	0 / 1	NIST	PR/DS Data Security	PR/DS-2 Data-in-transit	21 hours ago
policy-grc-pci	open-cluster-management-policies	inform	0 / 1	PCI	PR/DS Data Security	PR/DS-2 Data-in-transit	21 hours ago
policy-no-gmail-users	open-cluster-management-policies	enforce	0 / 10	NIST-CSF	PR/IP Information Protection Processes and Procedures	PR/IP-1 Baseline Configuration	2 days ago
policy-hibernation_disabled	open-cluster-management-policies	enforce	▲ -	NIST-CSF	PR/IP Information Protection Processes and Procedures	PR/IP-1 Baseline configuration	2 days ago
policy-ansible-resource-operator	tower-policies	enforce	0 / 1	NIST-CSF	PR/IP Information Protection Processes and Procedures	PR/IP-1 Baseline configuration	3 days ago
policy-ansible-tower-prep	tower-policies	enforce	0 / 1	NIST-CSF	PR/IP Information Protection Processes and Procedures	PR/IP-1 Baseline configuration	3 days ago
policy-imagenmanifestival	open-cluster-management-policies	enforce	0 / 2	NIST SP 800-53	SI System and Information Integrity	SI-4 Information System Monitoring	6 days ago
policy-namespace-operatorgroup	open-cluster-management-policies	enforce	▲ -	NIST-CSF	PR/IP Information Protection Processes and Procedures	PR/IP-1 Baseline Configuration	6 days ago

Memory

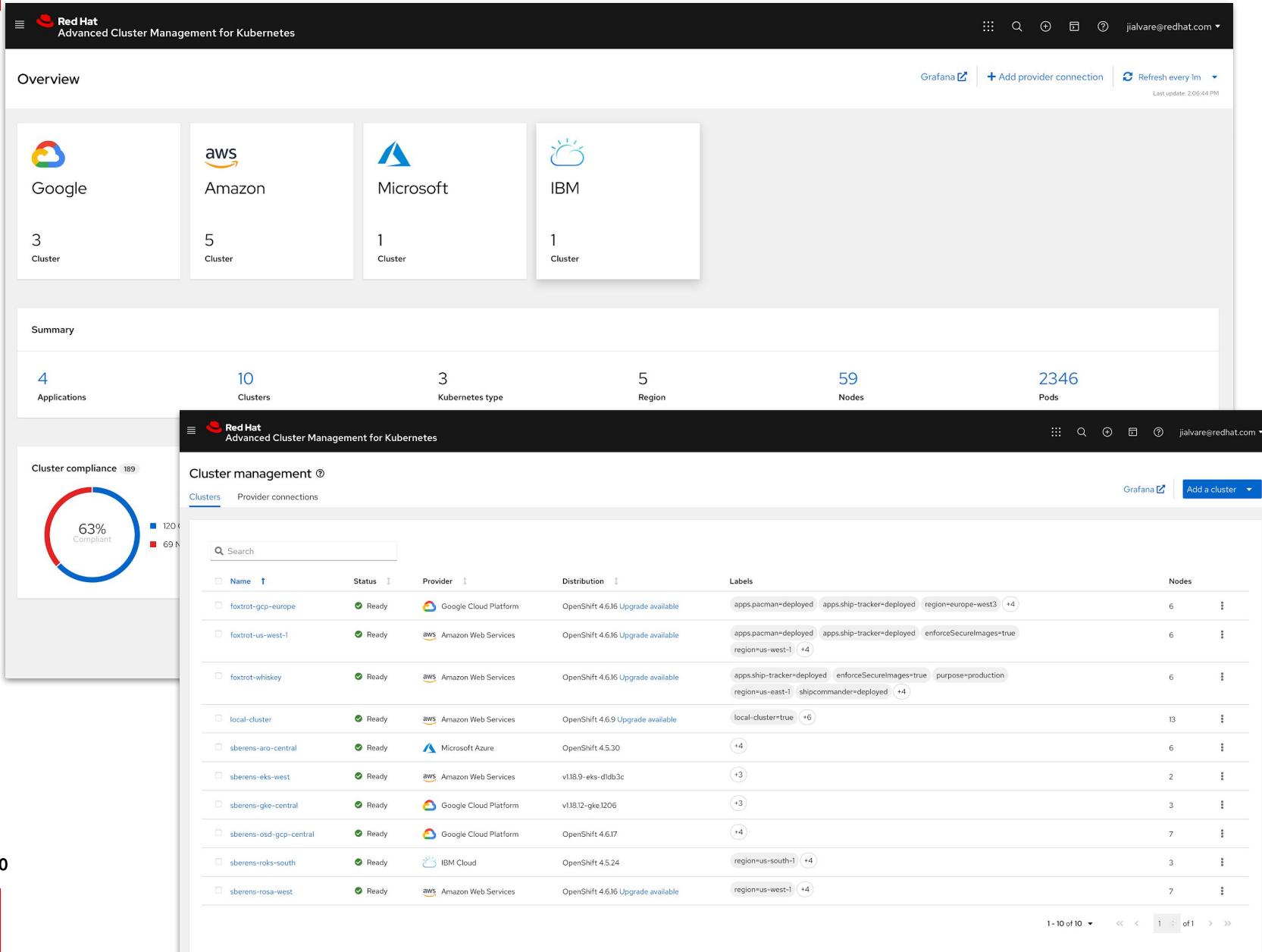
Cluster	Overutilization	Requested	Utilized
stage	37.42%	62.54%	25.12%
oregon2	19.21%	36.67%	17.66%
ocp-edge-bm-h27-1	30.92%	48.07%	17.15%
local-cluster	1.60%	29.98%	30.67%
challidoue-04	33.27%	49.93%	16.66%
stage3	43.93%	65.68%	21.75%
singapore	20.49%	39.34%	18.85%

Top 5 Utilized Clusters (% CPU usage)

Red Hat

Unified Multi-Cluster Management

Single Pane for all your Kubernetes Clusters



The screenshot displays the Red Hat Advanced Cluster Management for Kubernetes interface. At the top, there are four cards showing cluster counts for Google (3), Amazon (5), Microsoft (1), and IBM (1). Below this is a summary section with counts for Applications (4), Clusters (10), Kubernetes type (3), Region (5), Nodes (59), and Pods (2346). On the left, a 'Cluster compliance' section shows a 63% compliance rate with 120 compliant and 69 non-compliant clusters. The main area is a 'Cluster management' table listing 10 clusters, including 'foxtrot-gcp-europe', 'foxtrot-us-west-1', 'foxtrot-whiskey', 'local-cluster', 'sberens-aro-central', 'sberens-eks-west', 'sberens-gke-central', 'sberens-osd-gcp-central', 'sberens-roks-south', and 'sberens-rosa-west'. The table columns include Name, Status, Provider, Distribution, Labels, and Nodes. The 'Clusters' tab is selected in the navigation bar.

- **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

Governance and risk [ⓘ](#)

Summary [2](#) | Standards [▼](#)

NIST-CSF NIST SP 800-53

10 /10 Cluster violations 4 /11 Policy violations 2 /2 Cluster violations 1 /1 Policy violations

Filter Refresh every 10s Last update: 2:09:03 PM Create policy

Find policies

Policy name ⓘ	Namespace ⓘ	Remediation ⓘ	Cluster violations ⓘ	Standards ⓘ	Categories ⓘ	Controls ⓘ	Created ⓘ
policy-imagemanifestvuln	open-cluster-management-policies	enforce	1 /2	NIST SP 800-53	SI System and Information Integrity	SI-4 Information System Monitoring	12 days ago

Governance and risk / Policies / Create policy [ⓘ](#) YAML: On

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

Name [*](#) policy-pod

Namespace [ⓘ](#) default

Specifications [ⓘ](#) Pod

Cluster binding [ⓘ](#) Begin typing to search for cluster label to select. If not selected, all clusters will be applied.

Standards [ⓘ](#) FISMA, NIST-CSF

Categories [ⓘ](#) PR.DS Data Security, PR.IP Information Protection Processes and Procedures, PR...

Controls [ⓘ](#) PR.DS-2 Data-in-transit, PR.IP-1 Baseline Configuration, PR.PT-3 Least Functional...

Enforce if supported [ⓘ](#)

Disable policy [ⓘ](#)

Policy YAML

```
1 apiVersion: policy.open-cluster-management.io/v1
2 kind: Policy
3 metadata:
4   name: policy-pod
5   namespace: default
6 annotations:
7   | policy.open-cluster-management.io/standards: FISMA, NIST-CSF
8   | policy.open-cluster-management.io/categories: PR.DS Data Security, PR.IP Information Protection Processes and Protective Technology
9 spec:
10   remediationAction: inform
11   disabled: false
12   policyTemplate:
13     kind: ConfigurationPolicy
14     apiVersion: policy.open-cluster-management.io/v1
15     kind: ConfigurationPolicy
16     metadata:
17       name: policy-pod-nginx-pod
18     spec:
19       remediationActions: inform # will be overridden by remediationAction in parent policy
20       severity: low
21       namespaceSelector:
22         exclude: ["kube-*"]
23         include: ["default"]
24       objectDefinition:
25         - complianceType: mustHave
26           objectDefinition:
27             apiVersion: v1
28             kind: Pod # nginx pod must exist
29             metadata:
30               name: nginx-pod
31             spec:
32               containers:
33                 - image: nginx:1.7.9
34                 name: nginx
35                 ports:
36                   - containerPort: 80
37             ...
38         apiVersion: policy.open-cluster-management.io/v1
39         kind: PlacementBinding
40         metadata:
41           name: binding-policy-pod
42           namespace: default
43           placement:
44             name: placement-policy-pod
45             kind: PlacementRule
```

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

Advanced Application Lifecycle Management

Simplify your Application Lifecycle

The screenshot displays the Red Hat Application Builder interface, which includes the following components:

- Create an application:** A form for entering application details like Name (newapp) and Namespace (default).
- Application YAML:** A code editor showing the generated YAML configuration for the application.
- Repository location for resources:** A section for defining repository types and URLs. It shows a selected "Git" repository at <https://github.com/mdeleyo/test-repo>.
- Resource topology:** A visual graph showing the relationships between various application components like Application, Subscription, Placement, Cluster, Route, Service, Deployment, and PersistentVolume.
- Cluster details:** A panel showing the details of two clusters: "foxtrot-gcp-europe" and "foxtrot-us-west-1".

- **Easily deploy an Application using the Application Builder**
- **Deploy Applications from Multiple Sources (GIT / HELM / Object Storage)**
- **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.



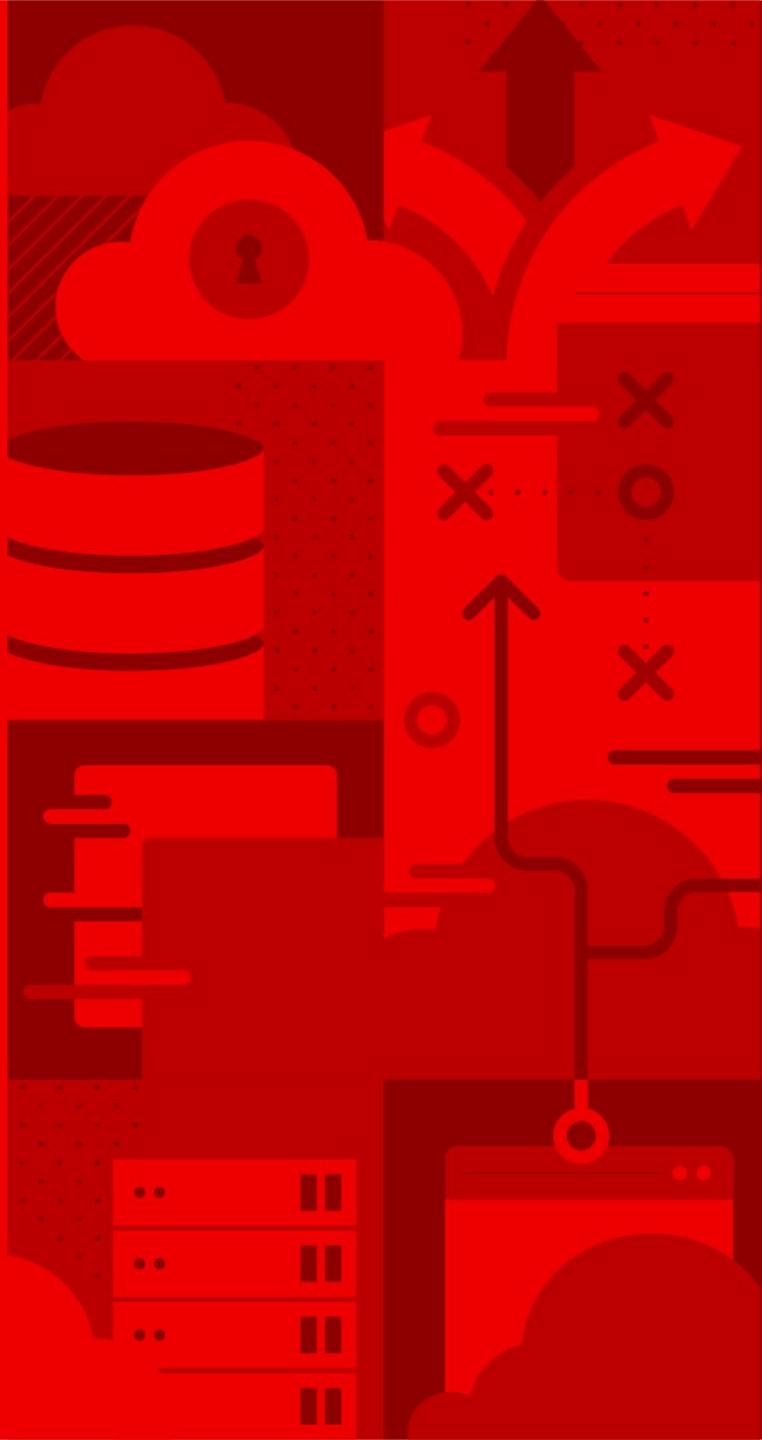
Reduce costs

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.



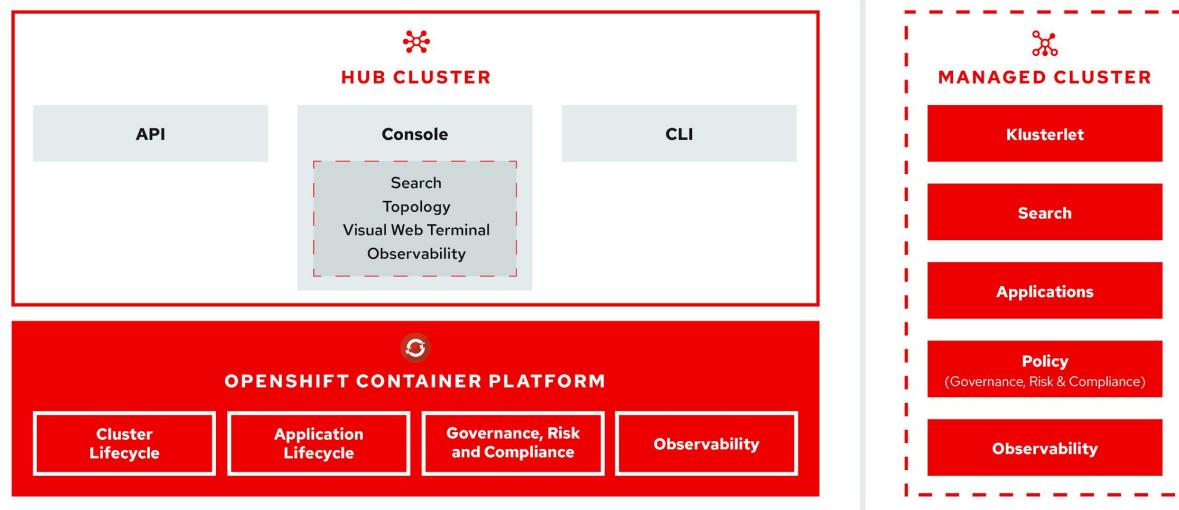
Architecture

Red Hat Advanced Cluster Management For
Kubernetes

Architecture overview



IT Operations



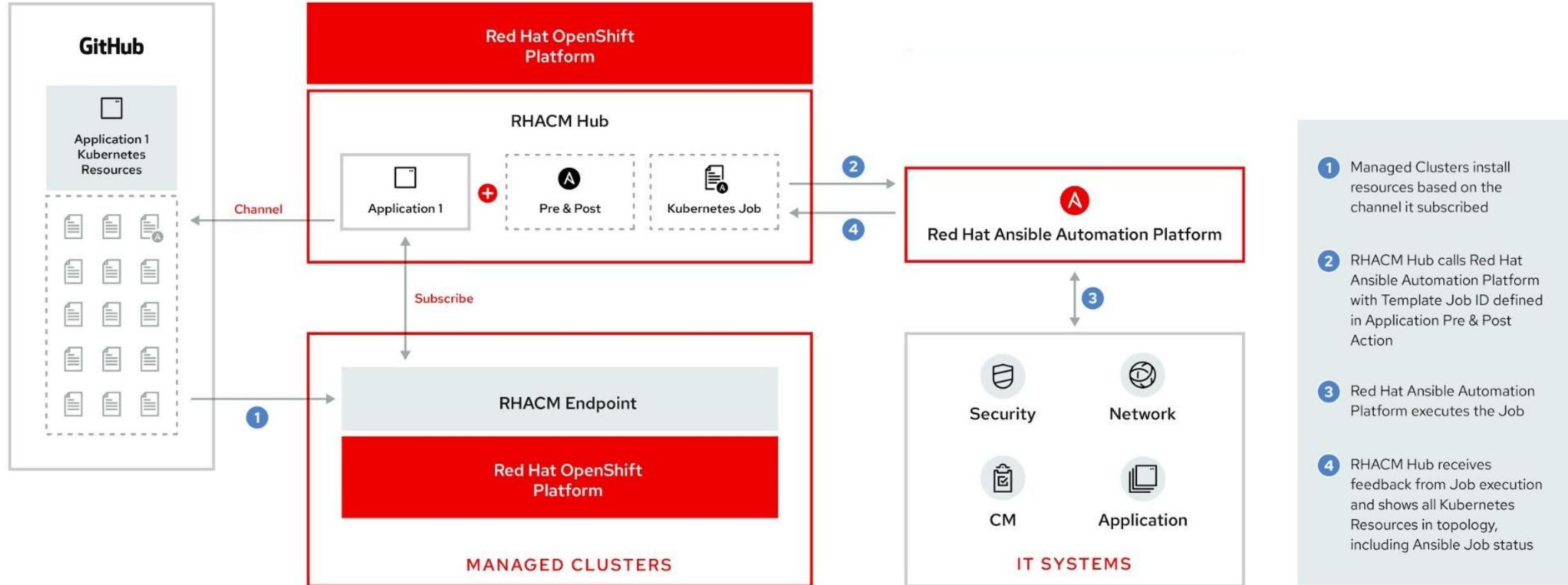
Hub architecture and components

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

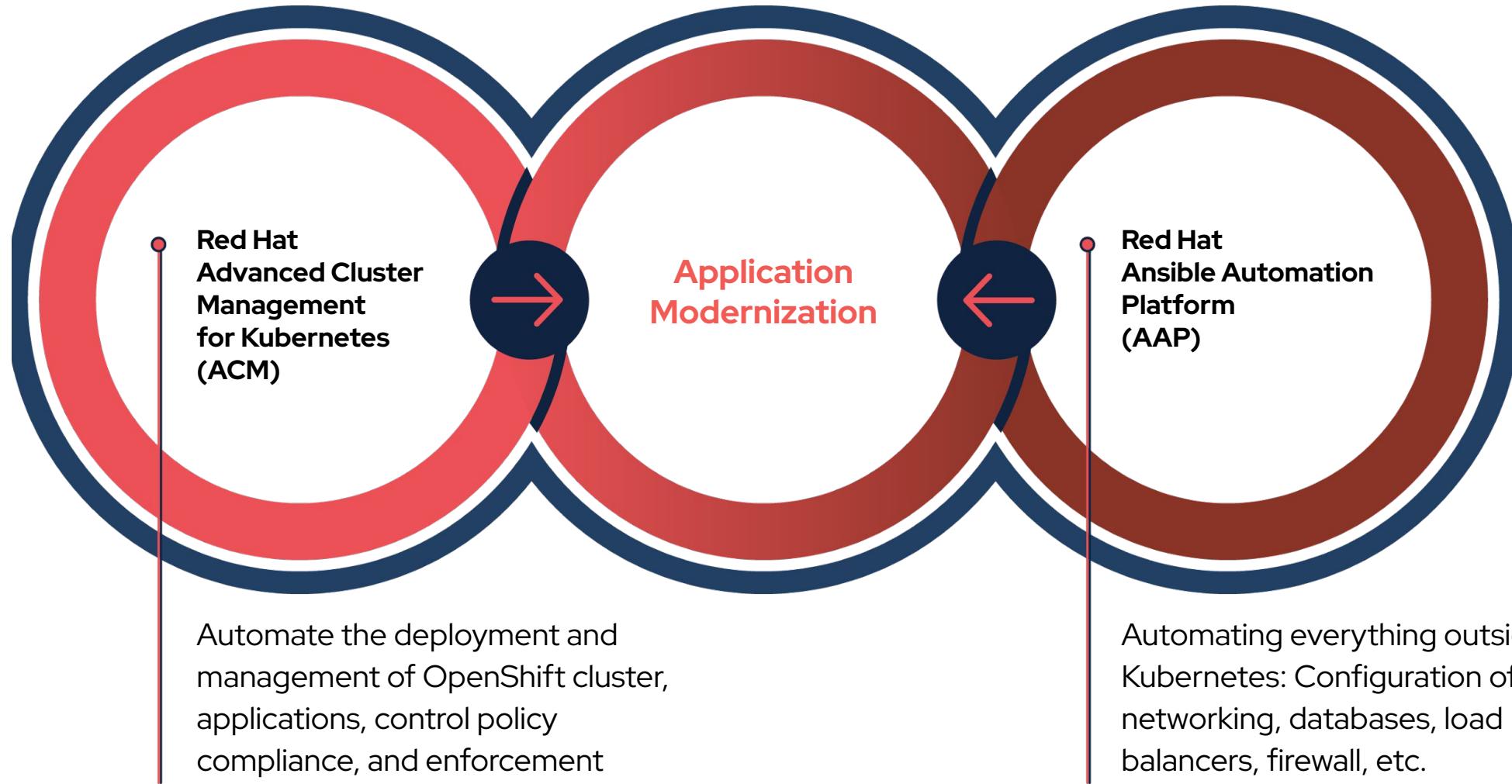
Managed cluster architecture and components

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

Architecture Overview for Application Lifecycle



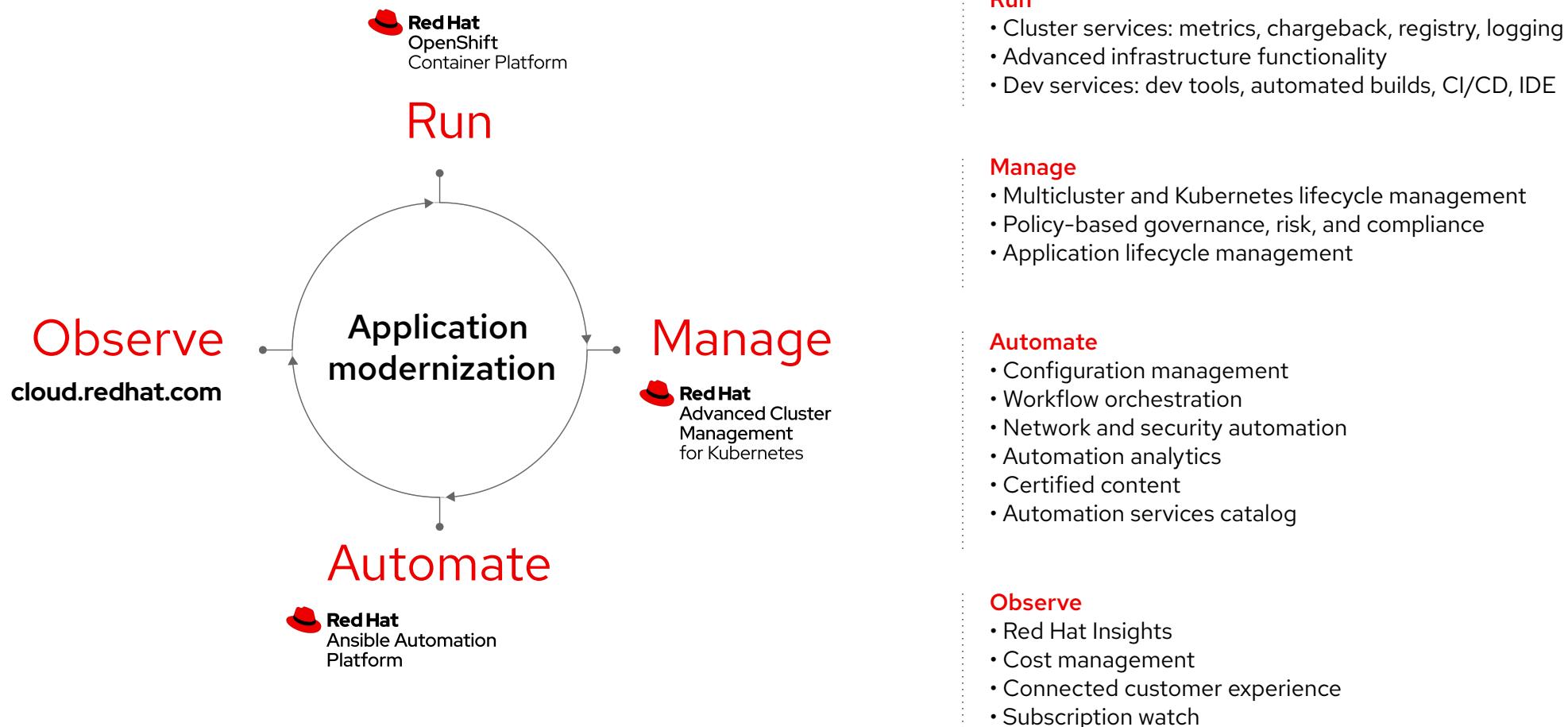
Application modernization driven by Automation of Kubernetes and beyond....





How ACM works with OpenShift

Supporting application modernization



Draw Me a Picture!

Advanced Cluster Management

Multi-cluster Management

Creation : Discovery : Policy : Compliance : Configuration : Workloads

OpenShift Container Platform

Manage Workloads

Build Cloud-Native Apps

Developer Productivity

Platform Services

Service Mesh : Serverless
Builds : CI/CD Pipelines
Full Stack Logging
Chargeback

Application Services

Databases : Languages
Runtimes : Integration
Business Automation
100+ ISV Services

Developer Services

Developer CLI : VS Code
extensions : IDE Plugins
Code Ready Workspaces
CodeReady Containers

OpenShift Kubernetes Engine

Cluster Services

Automated Ops : Over-The-Air Updates : Monitoring : Registry : Networking : Router : KubeVirt : OLM : Helm

Kubernetes

Red Hat Enterprise Linux & RHEL CoreOS



Physical



Edge



Virtual



Private cloud

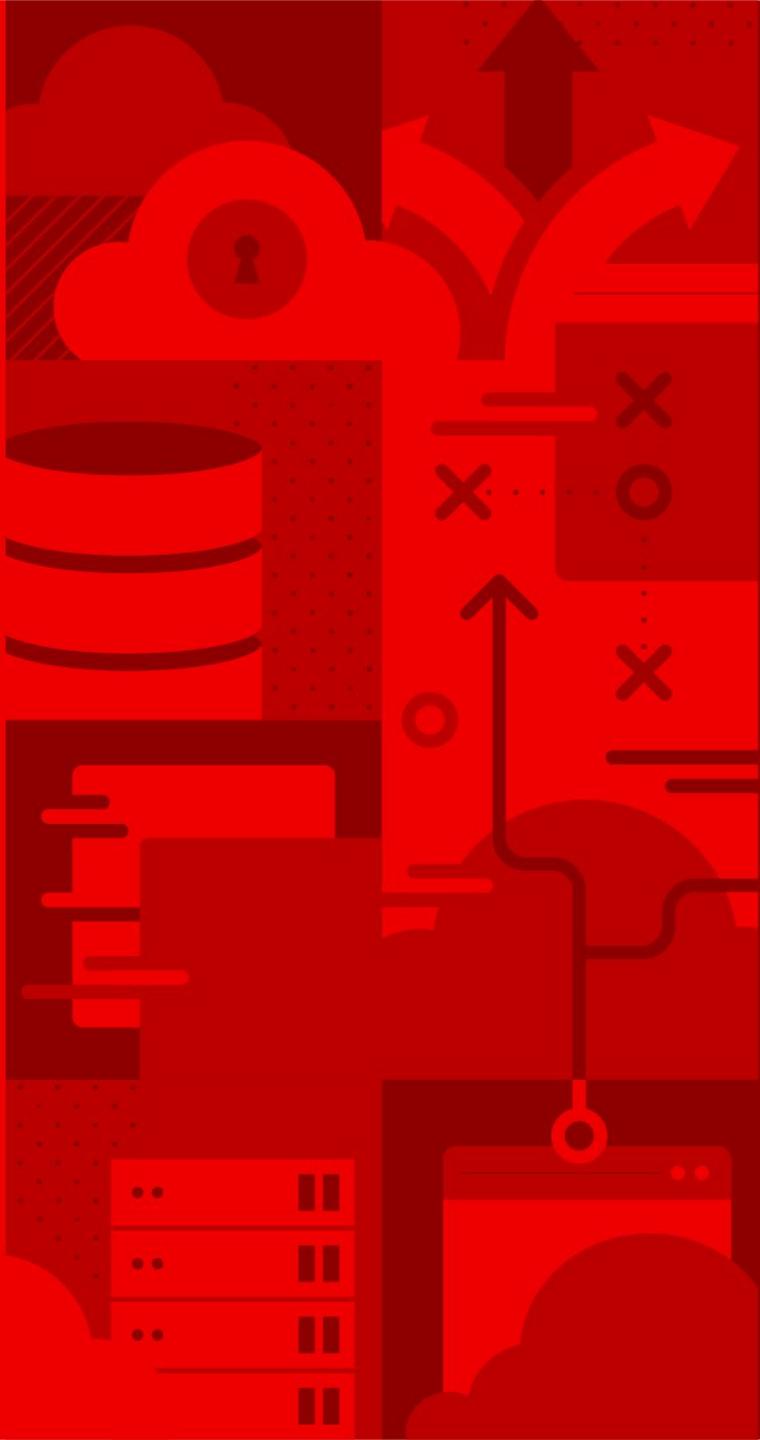


Public cloud



Managed cloud
(Azure, AWS, IBM, Red Hat)





Installation

Red Hat Advanced Cluster Management For
Kubernetes

Installation and Foundation

Operator Install for Hub



IT Operations

Hub Cluster

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

Full Management of OCP clusters

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

Limited Support for Public cloud managed Kubernetes

- EKS, AKS, GKE, IKS, ROKS

High Availability

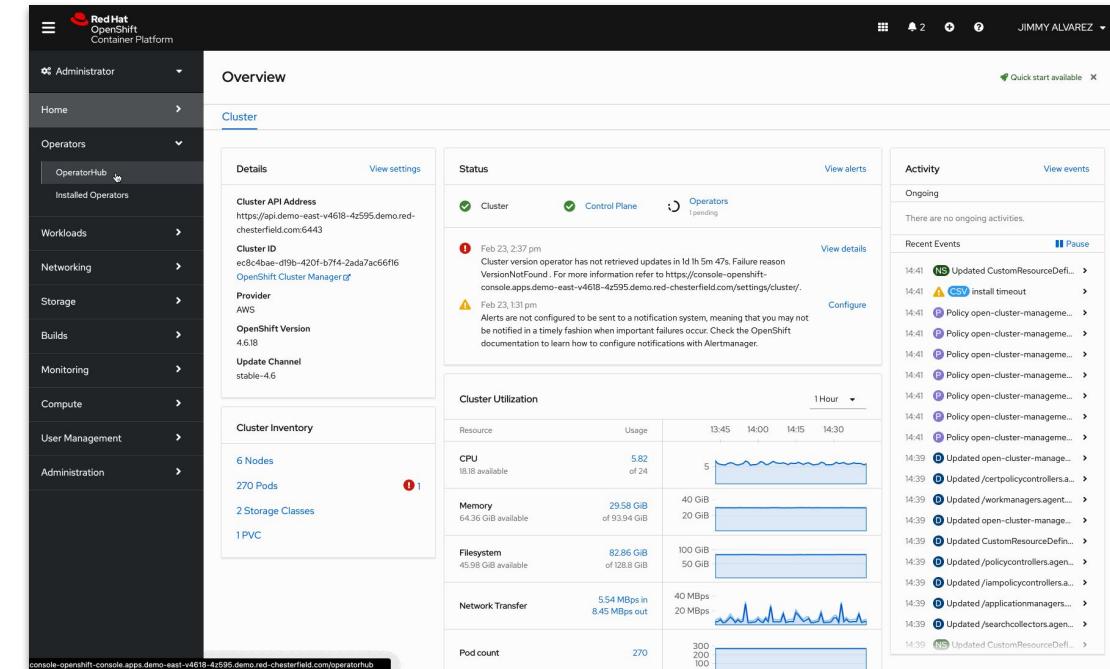
- Supports OCP Availability Zone
 - Limitation for Search component based on RedisGraph

Resource Requirements

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



CONFIDENTIAL designator

Security Ops

- RBAC in RHACM is based on kubernetes concepts and is enforced through openshift.
- Cluster-Admin Role is an Openshift super-user role and can perform all actions cluster-wide.
- Additional Roles are available out of the box to assign users Admin, Edit or View level access to RHACM artifacts, for more please see the [documentation](#)

Role	Description
open-cluster-management:cluster-manager-admin	A user with cluster-wide binding to this role, is an RHACM super user can perform any action on RHACM resources
open-cluster-management:admin:managed-cluster-x	A user with cluster binding to this role, has admin access to ManagedCluster "X" resource
open-cluster-management:view:managed-cluster-x	A user with cluster-wide binding to this role, has view access to ManagedCluster "X" resource
OCP Default admin / edit / view roles	A user with namespace binding to these roles has access to resources like policies, applications etc in that namespace or ManagedCluster. A user with cluster-wide binding to these roles has access to resources like policies, applications etc in all namespaces or for all ManagedClusters.

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