Red Hat® Advanced Cluster Management: Kubernetes Kümelerinde Uçtan Uca Kontrol ve Uyum

2023

www.gantek.com

Ajanda

- Red Hat® Advanced Cluster Management Nedir ?
- Mimari Genel Bakış
- Politika Tabanlı Yönetim
- Gantek Sizin İçin Neler Yapabilir ?
- Soru & Cevap
- DEMO

Gantek Teknoloji Hakkında

Rekabetçi Avantajlar

Güçlü marka ve güçlü referanslara dayalı **40+ yıllık** deneyim

Kurumsal referanslar ve odaklı yaklaşım ile **Lekelenmemiş Repütasyon**

Müşteriler ve önde gelen üreticiler ile adanmış, uzun süreli ve mükemmel **İş Birlikteliği**

Yerel Destek ve **Bölgesel Mevcudiyet'in** gücü

Güvenilir, sağlam & uzun süreli iş ortağı

TURKİYE & AVRASYA bölgesinin önde gelen Kurumlarında kurulu sistemler

Yetkinlikler

99,9% Seviyesinde 7x24 Destek

Geniş ve Etkin **Çözüm Portföyü**

Katma Değerli Sistem Entegrasyonu

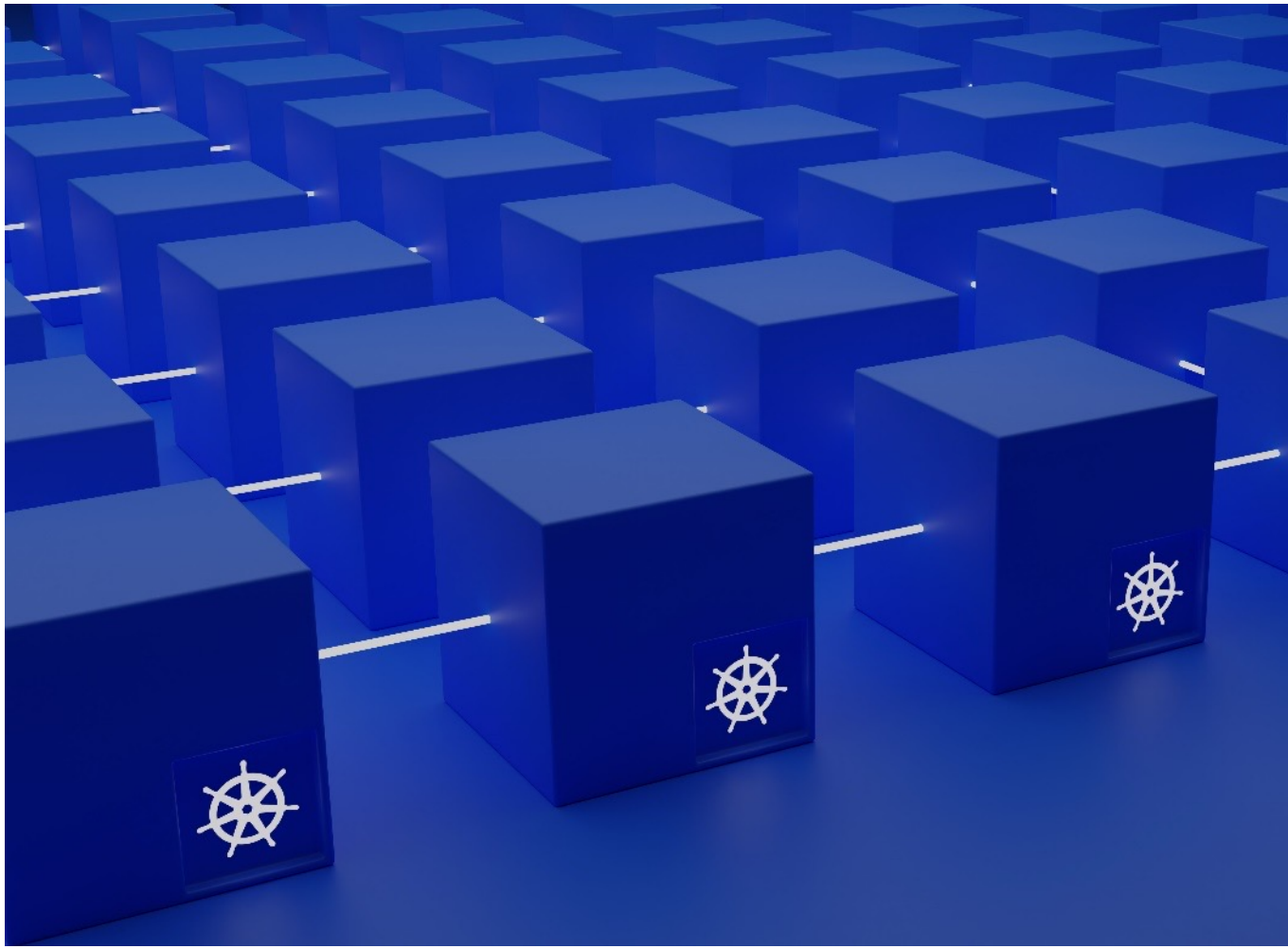
Yüksek **Müşteri Memnuniyet** Oranları

Görev Kritik Projeler için **Yerinde Destek** Servisleri, **Yönetilen Hizmetler**

Yerel/ Bölgesel Mevcudiyet ve Küresel Yöntemler

Çoklu Küme Yönetimi Neden Zor

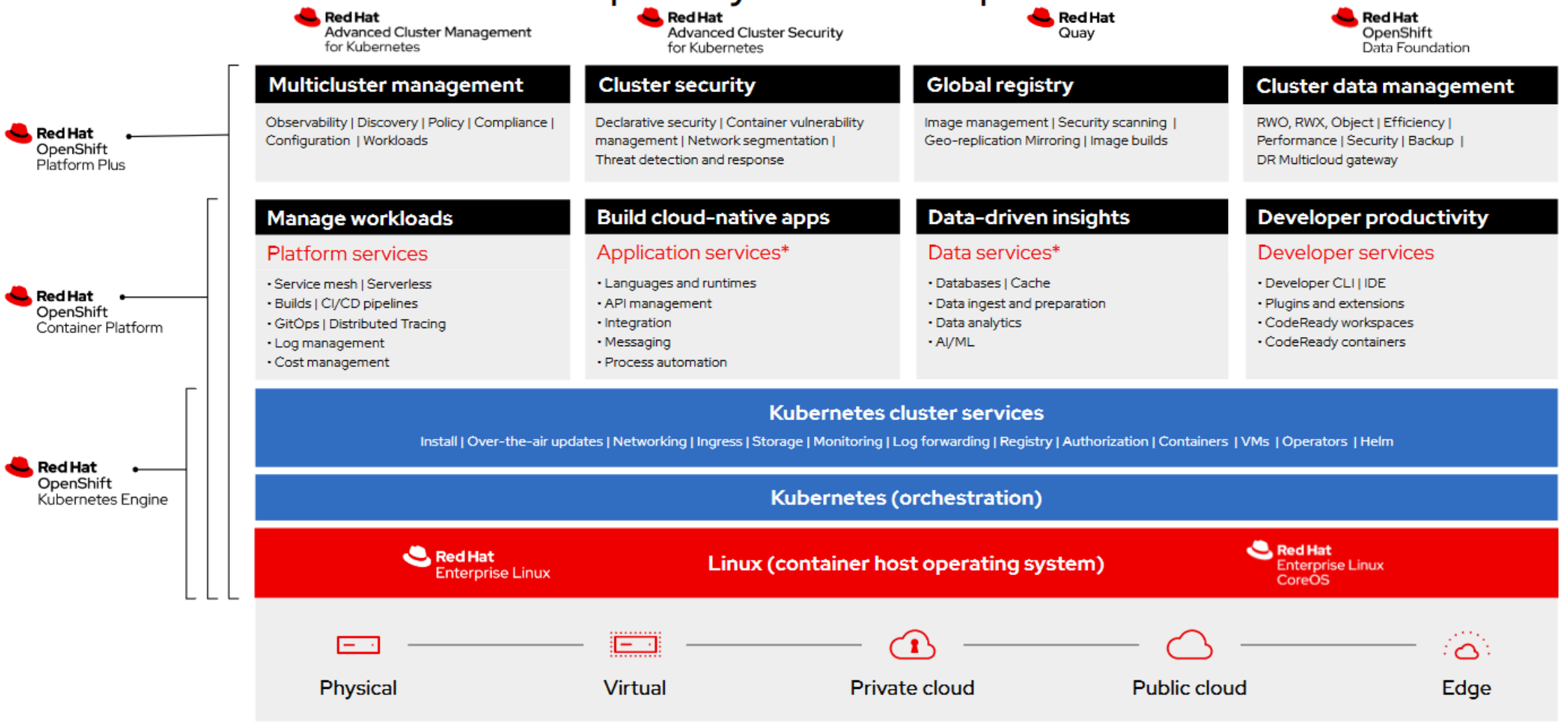
- Büyük ölçekli yönetim zorlayıcı ve hatalara açık
- Farklı platformlarda güvenlik önlemlerinin değişkenliği
- Bileşenlerin, ayarların ve mevzuata uygunluğun bütünlüğünü sağlamak için karmaşık süreç



Neden Çoklu Kümeye İhtiyacınız Var ?

- Uygulama uptime sürelerinin sağlanması
- Felaket kurtarma
- Düşük gecikme süreleri elde etme
- Sektör standartlarına uyum
- Izolasyon ve güvenlik
- Performans yönetimi

Red Hat open hybrid cloud platform



Feature Overview

Cluster inventory

Registration of multiple clusters to a hub cluster to place them for management.

Work distribution

The work API that enables resources to be applied to managed clusters from a hub cluster.

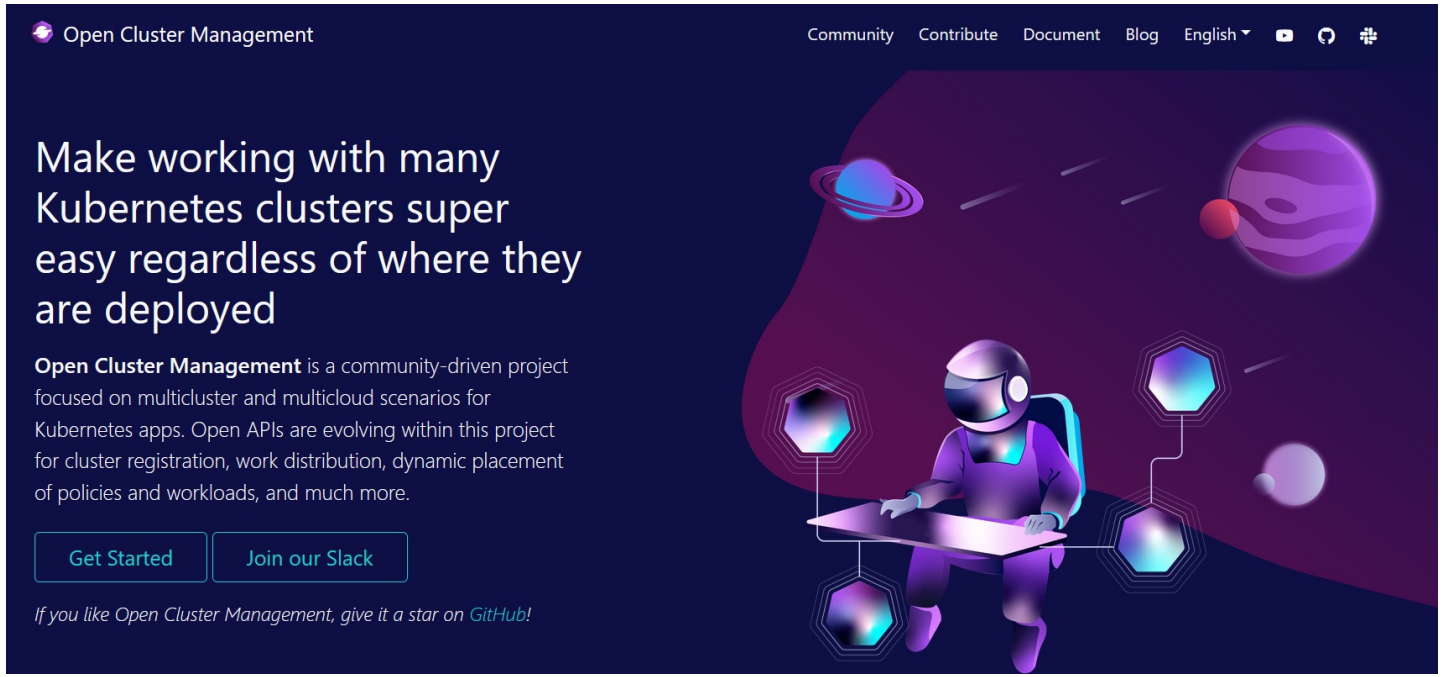
Content placement

Dynamic placement of content and behavior across multiple clusters.

Vendor neutral APIs

Avoid vendor lock-in by using APIs that are not tied to any cloud providers or proprietary platforms.

Open Cluster Management, 9 Kasım 2021 tarihinde Sandbox olgunluk seviyesinde CNCF'ye kabul edilmiştir.



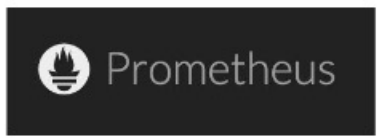
Open Policy Agent

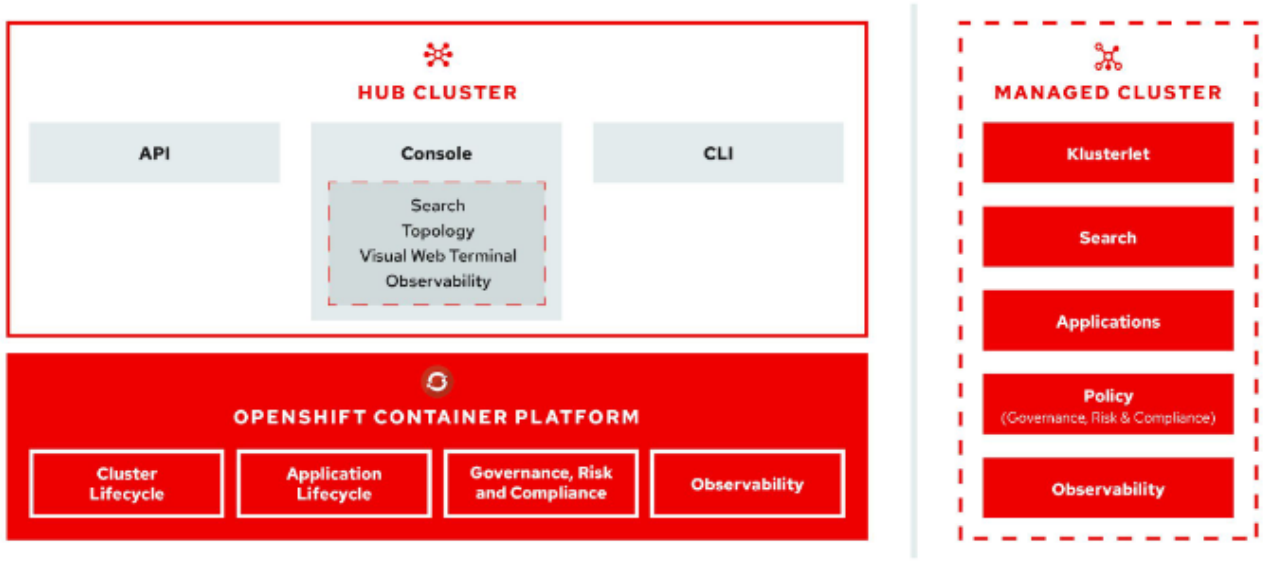
Hive

Red Hat
Advanced Cluster
Management
for Kubernetes

metal3

Open Cluster
Management





Hub architecture and components

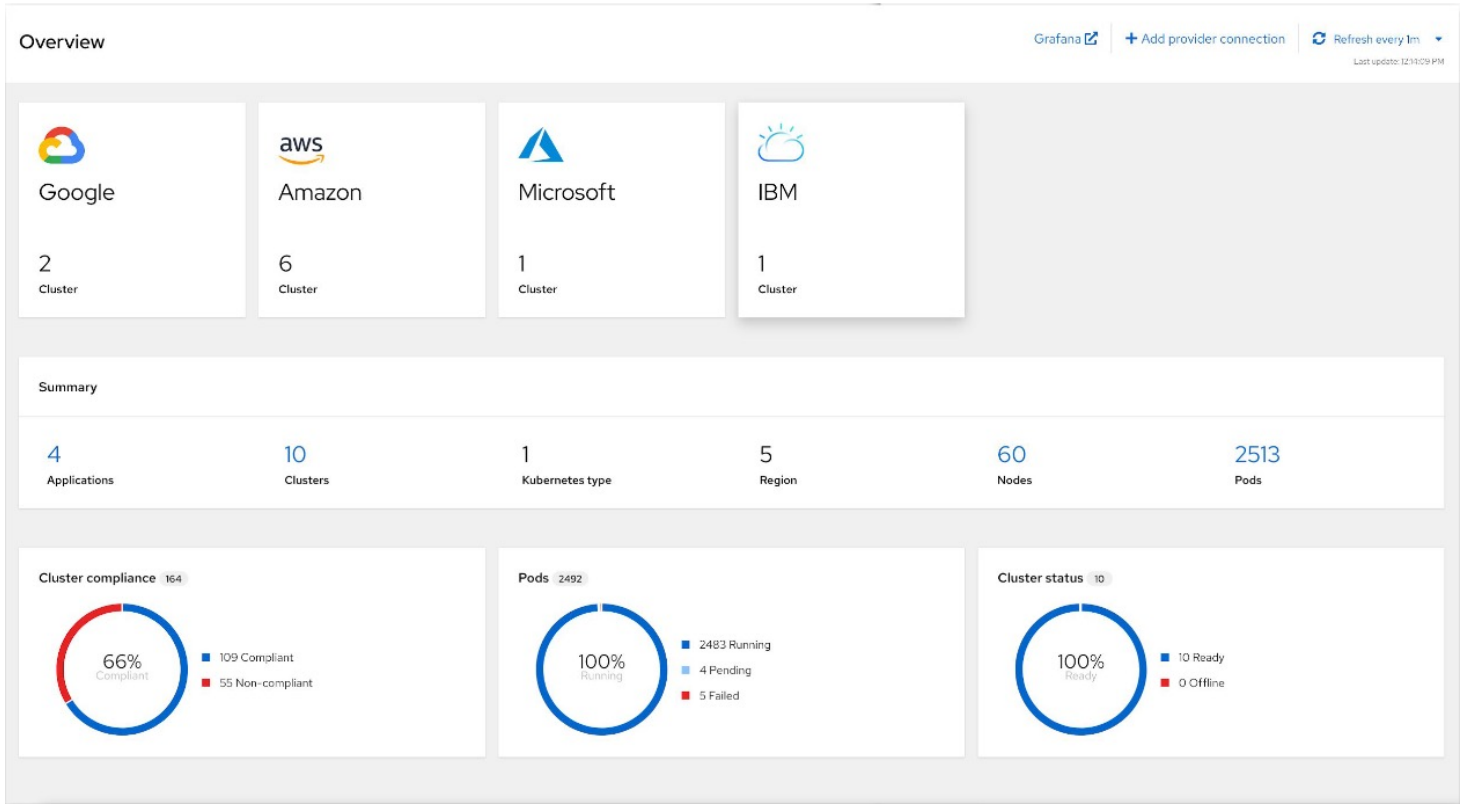
Red Hat Advanced Cluster Management uses the **multicluster-hub** operator and runs in the **open-cluster-management** namespace

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

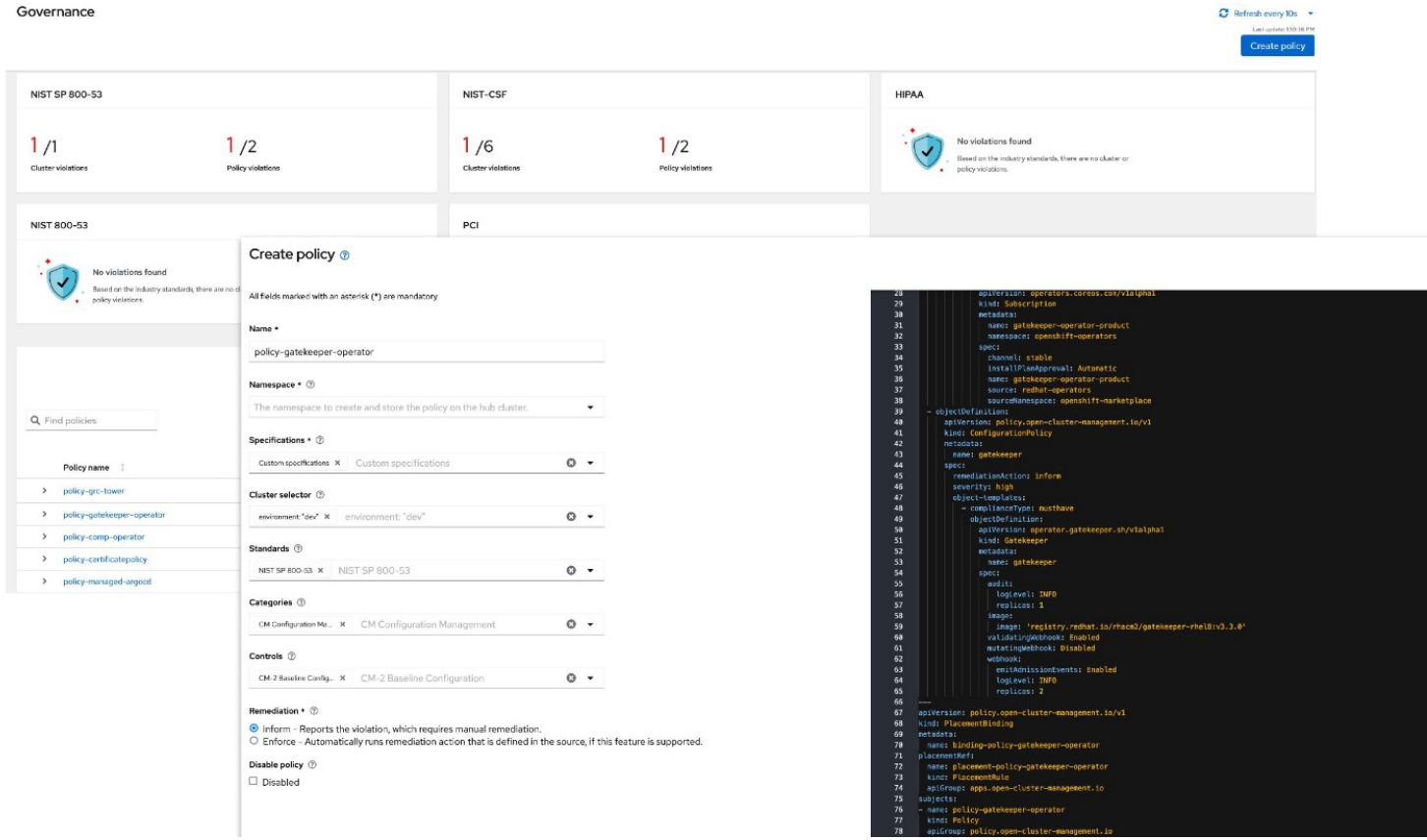
ACM Genel Kabiliyetler

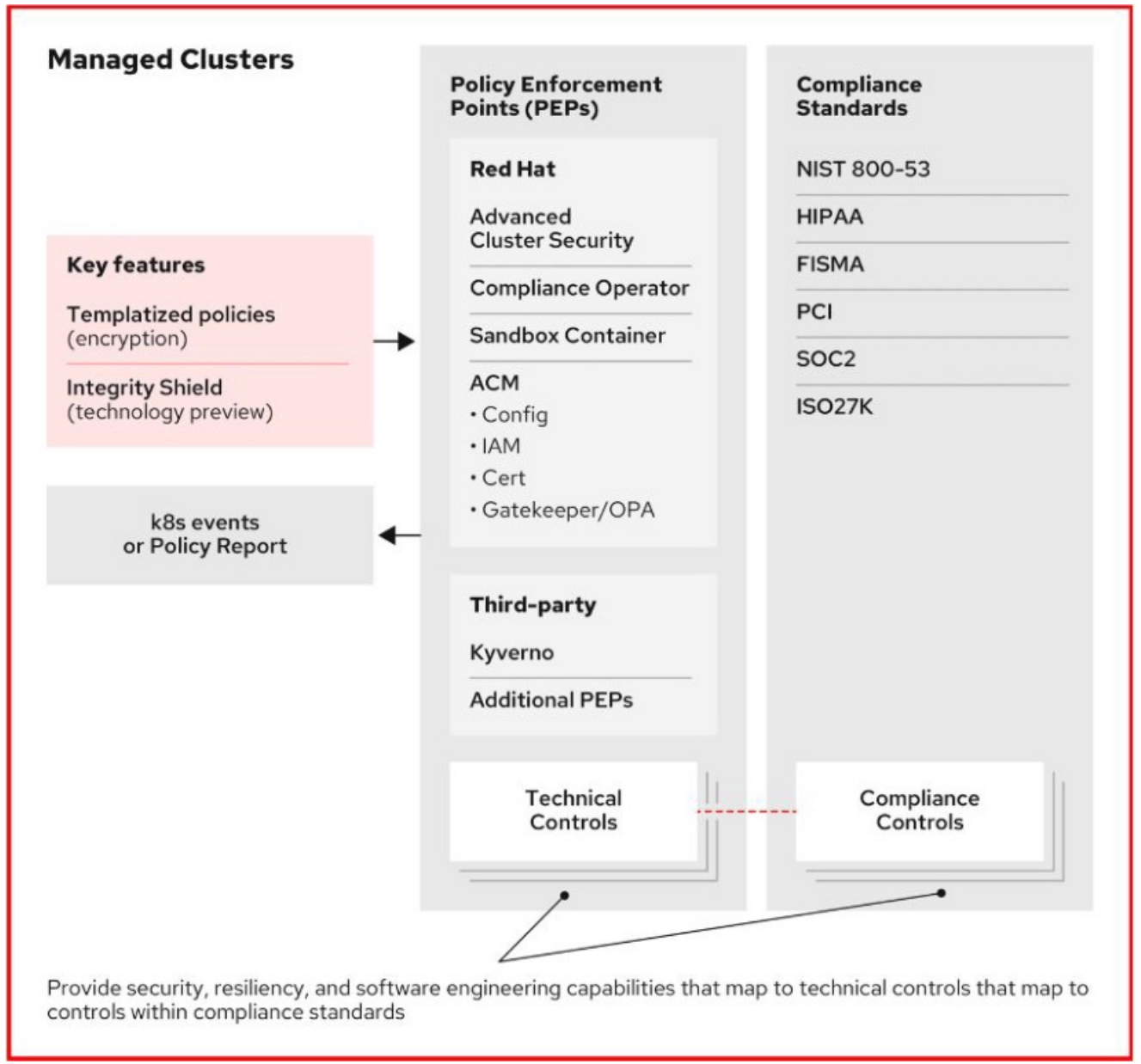
- Çoklu küme yaşam döngüsü yönetimi
- Politika odaklı yönetim, risk ve uyum
- Gelişmiş uygulama yaşam döngüsü yönetimi
- Sağlık ve optimizasyon için çoklu küme gözlemlenebilirliği
- Çoklu küme network ağı



Politika Tabanlı Yönetim, Risk ve Uyum

- Güvenlik ve Altyapı politikalarının merkezi olarak uygulanması ve düzenlenmesi
- Uygulama ve küme yapılandırma denetimlerinin hızlı görselleştirilmesi
- GitOps mantığı ile politikaların tek bir kaynaktan yönetilmesi




Managed Clusters
Policy Enforcement Points (PEPs)
Compliance Standards
Red Hat
Advanced Cluster Security
Compliance Operator
Sandbox Container
ACM
• Config
• IAM
• Cert
• Gatekeeper/OPA
Key features
Templatized policies (encryption)
Integrity Shield (technology preview)
k8s events or Policy Report
Third-party
Kyverno
Additional PEPs
NIST 800-53
HIPAA
FISMA
PCI
SOC2
ISO27K
Technical Controls
Compliance Controls
Provide security, resiliency, and software engineering capabilities that map to technical controls that map to controls within compliance standards

Policy Örneği

```yaml
apiVersion: policy.open-cluster-management.io/v1
kind: Policy
metadata:
  name: policy-role
  annotations:
    policy.open-cluster-management.io/standards: NIST SP 800-53
    policy.open-cluster-management.io/categories: AC Access Control
    policy.open-cluster-management.io/controls: AC-3 Access Enforcement
    policy.open-cluster-management.io/description:
spec:
  remediationAction: inform
  disabled: false
  policy-templates:
    - objectDefinition:
        apiVersion: policy.open-cluster-management.io/v1
        kind: ConfigurationPolicy
        metadata:
          name: policy-role-example
        spec:
          remediationAction: inform # the policy-template spec.remediationActio
          severity: high
          namespaceSelector:
            include: ["default"]
          object-templates:
            - complianceType: mustonlyhave # role definition should exact match
              objectDefinition:
                apiVersion: rbac.authorization.k8s.io/v1
                kind: Role
                metadata:
                  name: sample-role
                rules:
                  - apiGroups: ["extensions", "apps"]
                    resources: ["deployments"]
                    verbs: ["get", "list", "watch", "delete","patch"]
```

```yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PlacementBinding
metadata:
  name: binding-policy-role
placementRef:
  name: placement-policy-role
  kind: PlacementRule
  apiGroup: apps.open-cluster-management.io
subjects:
- name: policy-role
  kind: Policy
  apiGroup: policy.open-cluster-management.io
```

```yaml
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: placement-policy-role
spec:
  clusterConditions:
  - status: "True"
    type: ManagedClusterConditionAvailable
  clusterSelector:
    matchExpressions:
      - {key: environment, operator: In, values: ["dev"]}
```

Ön Tanımlı Gelen Politikalar

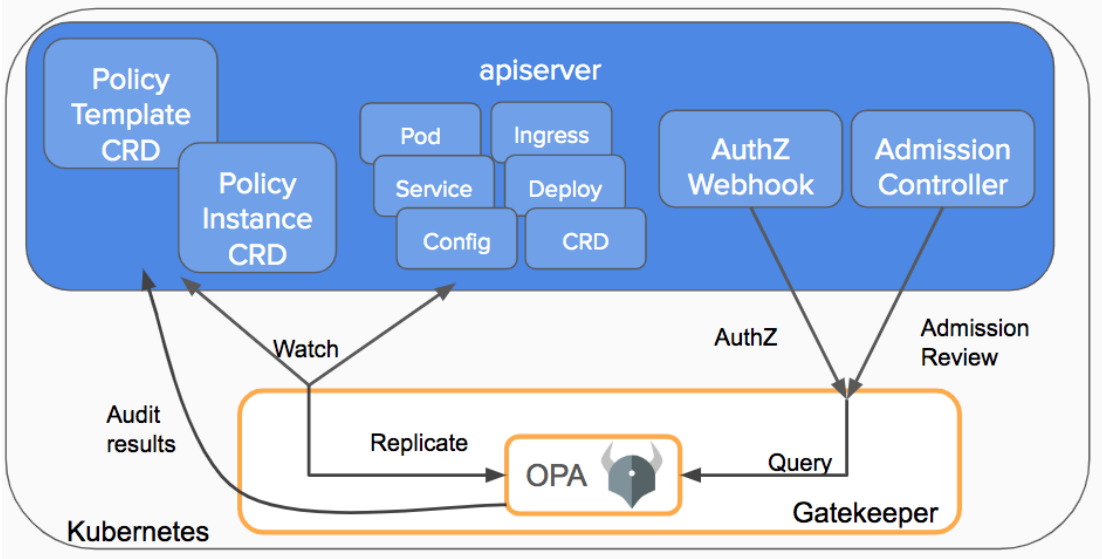
Policy sample	Description
Namespace policy	Ensure consistent environment isolation and naming with Namespaces. See the Kubernetes Namespace documentation.
Pod policy	Ensure cluster workload configuration. See the Kubernetes Pod documentation.
Memory usage policy	Limit workload resource usage using Limit Ranges. See the Limit Range documentation.
Pod security policy (Deprecated)	Ensure consistent workload security. See the Kubernetes Pod security policy documentation.
Role policy Role binding policy	Manage role permissions and bindings using roles and role bindings. See the Kubernetes RBAC documentation.
Security content constraints (SCC) policy	Manage workload permissions with Security Context Constraints. See Managing Security Context Constraints documentation in the OpenShift Container Platform documentation.
ETCD encryption policy	Ensure data security with etcd encryption. See Encrypting etcd data in the OpenShift Container Platform documentation.
Compliance operator policy	Deploy the Compliance Operator to scan and enforce the compliance state of clusters leveraging OpenSCAP. See Understanding the Compliance Operator in the OpenShift Container Platform documentation.
Compliance operator E8 scan	After applying the Compliance operator policy, deploy an Essential 8 (E8) scan to check for compliance with E8 security profiles. See Understanding the Compliance Operator in the OpenShift Container Platform documentation.
Compliance operator CIS scan	After applying the Compliance operator policy, deploy a Center for Internet Security (CIS) scan to check for compliance with CIS security profiles. See Understanding the Compliance Operator in the OpenShift Container Platform documentation.
Image vulnerability policy	Deploy the Container Security Operator and detect known image vulnerabilities in pods running on the cluster. See the Container Security Operator GitHub repository.
Gatekeeper operator deployment	Gatekeeper is an admission webhook that enforces custom resource definition (CRD)-based policies executed by the Open Policy Agent (OPA) policy engine. See the Gatekeeper documentation.
Gatekeeper compliance policy	After deploying Gatekeeper to the clusters, deploy this sample Gatekeeper policy that ensures namespaces that are created on the cluster are labeled as specified.

Politikaları Extend Etmek

OPA Gatekeeper

Gatekeeper OPA

- Temelde Admission Controller prensibini kullanır.
- Her request gatekeeper aracılığı ile OPA tarafından control edilir.
- İstek OPA politikalarına uymaz ise apiserver “reject” eder.



OPA Politika Örneği

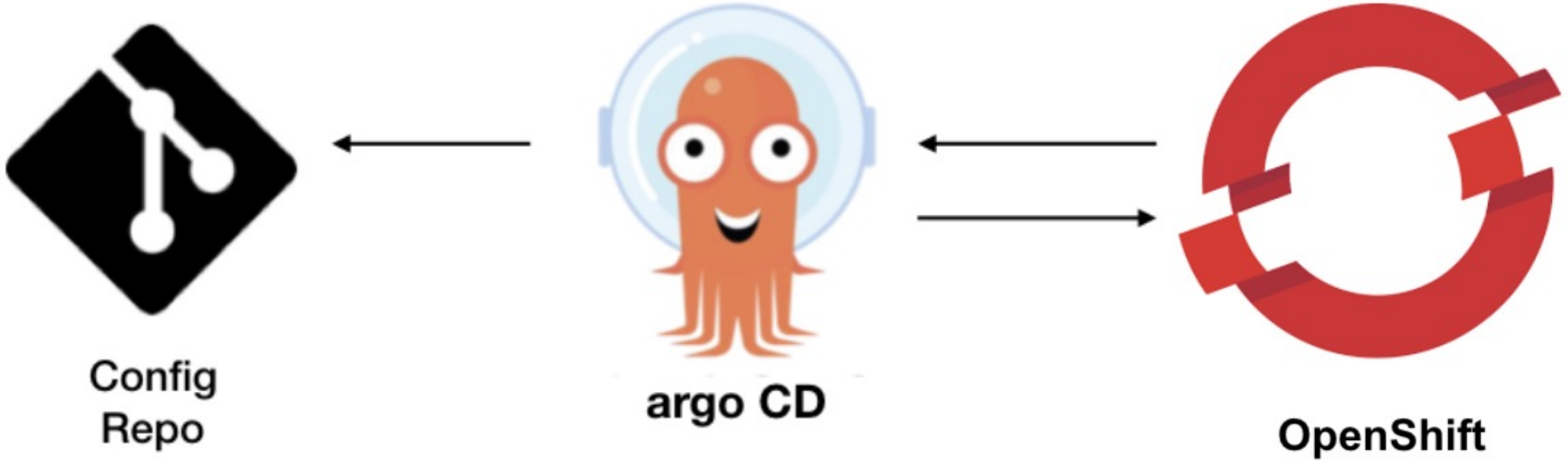
```yaml
apiVersion: templates.gatekeeper.sh/v1
kind: ConstraintTemplate
metadata:
  name: k8sblocknodeport
  annotations:
    metadata.gatekeeper.sh/title: "Block NodePort"
    metadata.gatekeeper.sh/version: 1.0.0
    description: >-
      Disallows all Services with type NodePort.

      https://kubernetes.io/docs/concepts/services-networking/service/#nodeport
spec:
  crd:
    spec:
      names:
        kind: K8sBlockNodePort
  targets:
    - target: admission.k8s.gatekeeper.sh
      rego: |
        package k8sblocknodeport

        violation[{"msg": msg}] {
          input.review.kind.kind == "Service"
          input.review.object.spec.type == "NodePort"
          msg := "User is not allowed to create service of type NodePort"
        }
```

```yaml
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sBlockNodePort
metadata:
  name: block-node-port
spec:
  match:
    kinds:
      - apiGroups: [""]
        kinds: ["Service"]
```

OpenShift GitOps Entegrasyonu



```yaml
apiVersion: policy.open-cluster-management.io/v1
kind: ConfigurationPolicy
metadata:
  name: create-infra-machineset
spec:
  remediationAction: enforce
  severity: low
  object-templates-raw: |
    {{- /* Specify the parameters needed to create the MachineSet  */ -}}
    {{- $machineset_role := "infra" }}
    {{- $region := "ap-southeast-1" }}
    {{- $zones := list "ap-southeast-1a" "ap-southeast-1b" "ap-southeast-1c" }}
    {{- $infrastructure_id := (lookup "config.openshift.io/v1" "Infrastructure" "" "cluster").status.infrastructureName }}
    {{- $worker_ms := (index (lookup "machine.openshift.io/v1beta1" "MachineSet" "openshift-machine-api" "").items 0) }}
    {{- /* Generate the MachineSet for each zone as specified  */ -}}
    {{- range $zone := $zones }}
    - complianceType: musthave
      objectDefinition:
        apiVersion: machine.openshift.io/v1beta1
        kind: MachineSet
        metadata:
          labels:
            machine.openshift.io/cluster-api-cluster: {{ $infrastructure_id }}
          name: {{ $infrastructure_id }}-{{ $machineset_role }}-{{ $zone }}
          namespace: openshift-machine-api
        spec:
          replicas: 1
          selector:
            matchLabels:
              machine.openshift.io/cluster-api-cluster: {{ $infrastructure_id }}
              machine.openshift.io/cluster-api-machineset: {{ $infrastructure_id }}-{{ $machineset_role }}-{{ $zone }}
          template:
            metadata:
              labels:
                machine.openshift.io/cluster-api-cluster: {{ $infrastructure_id }}
                machine.openshift.io/cluster-api-machine-role: {{ $machineset_role }}
                machine.openshift.io/cluster-api-machine-type: {{ $machineset_role }}
                machine.openshift.io/cluster-api-machineset: {{ $infrastructure_id }}-{{ $machineset_role }}-{{ $zone }}
```

Gantek Sizin İçin Neler Yapabilir ?

- ACM çoklu küme yönetimi konusunda danışmanlık.
- Kurumunuza özel politika geliştirilmesi ve uygulanması.
- Ansible Automation Platform ile entegrasyonu.
- Çoklu küme monitoring kurgulanması.
- Submariner ile network genişletme.
- ODF DR senaryoların kurgulanması.


DEMO

Red Hat OpenShift

Güvenli değil | https://console-openshift-console.apps.ocp4.ocp.imt/multicloud/home/welcome

Red Hat OpenShift

19 admin1

All Clusters

Home

Infrastructure

Applications

Governance

Credentials

Welcome! Let's get started.

Red Hat Advanced Cluster Management for Kubernetes provides the tools and capabilities to address various challenges with managing multiple clusters and consoles, distributed business applications, and inconsistent security controls across Kubernetes clusters that are deployed on-premises, or across public clouds.

Overview

View system alerts, critical application metrics, and overall system health. Search, identify, and resolve issues that are impacting distributed workloads using an operational dashboard designed for Site Reliability Engineers (SREs).

Clusters

Create, update, scale, and remove clusters reliably, consistently using an open source programming model that supports and encourages Infrastructure as Code best practices and design principles.

Applications

Define a business application using open standards and deploy the applications using placement policies that are integrated into existing CI/CD pipelines and governance controls.

Governance

Use policies to automatically configure and maintain consistency of security controls required by industry or other corporate standards. Prevent unintentional or malicious configuration drift that might expose unwanted and unnecessary threat vectors.

Multicluster networking

Enable direct networking connection between different on-premises or cloud-hosted Kubernetes clusters by grouping them in cluster sets and enabling the Submariner add-on.

Easy, simple, and secure.

Easy to use and simple to understand, Red Hat Advanced Cluster Management for Kubernetes provides the following mission critical capabilities based on open source projects:

Kubernetes

Easily provision Kubernetes clusters and offer complete cluster lifecycle management in a single console.

Policies

Enforce policies at the target clusters using Kubernetes-supported custom resource definitions.

Cluster landscape

Deploy and maintain day two operations of applications distributed across your cluster landscape.

Range of environments

Work across a range of environments, including multiple data centers, and private and public clouds.

Application topology

Quickly view service endpoints, pods, and dependant resources that comprise your application topology.

Cluster labels and placement rules

Use cluster labels and application placement rules to easily move workloads across clusters, even between multiple cloud providers.

Teşekkürler

Daha fazla bilgi için lütfen www.gantek.com adresini ziyaret ediniz.

www.gantek.com | info@gantek.com

GANTEK