Personas

Platform

Security

Custom Policies and Governance Dashboard

Use Case 08

Create a custom policy for least privilege roles which is a part of the AC-Access Control under NIST 800-53 Control Family standards.

#hub-spoke-model #fleet-management #policy #governance #risk #compliance

Red Hat OpenShift

Red Hat Advanced Cluster Management

Create your own custom policy

- Make Sure all tenants namespaces have label “type” and report all violations.
- Based on namespace type, platform team will push the namespace baseline configuration

ConstraintTemplate

Define your policy using rego, the OPA’s native query language Rego

```
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
metadata:
 name: k8srequiredlabels
spec:
 crd:
   spec:
     names:
       kind: K8sRequiredLabels
 targets:
   - target: admission.k8s.gatekeeper.sh
     rego: |
      package k8srequiredlabels

      violation[{"msg": msg}] {
        provided := {label | input.review.object.metadata.labels[label]}
        required := {label | label := input.parameters.labels[_]}
        missing := required - provided
        count(missing) > 0
        msg := sprintf("Missing required labels: %v", [missing])
      }
```

Policy

To add the template to RHACM Policy engine

```
apiVersion: policy.open-cluster-management.io/v1
kind: Policy
metadata:
 name: type-labels-on-tenant-ns
 namespace: cicd
spec:
 remediationAction: inform
 disabled: false
 policy-templates:
   - objectDefinition:
       apiVersion: constraints.gatekeeper.sh/v1beta1
       kind: K8sRequiredLabels
       metadata:
         name: ns-must-have-type-label
         annotations:
           policy.open-cluster-management.io/severity: low
       spec:
         enforcementAction: dryrun
         match:
           kinds:
             - apiGroups: [""]
               kinds: ["Namespace"]
           name: "team*"
         parameters:
           labels: ["type"]
```

Use Case Catalog

Day 1

1. UC01 : Cluster as a service
2. UC02: VM as a service
3. UC03: Namespace as a service
4. UC04: Container as a service
5. UC05: Cloud native as a service
6. UC06: VM migration as a service
7. UC07: Baseline Configuration
8. UC08: Custom Policies
9. UC09: Control Policy Scope
10. UC10: AuthN and Identity Providers
11. UC11: Authorization and RBAC
12. UC12: Zero Trust enforcement
13. UC13: Workload network policies

Day 2

14. UC14: Cross provider connectivity
15. UC15: Hybrid workload
16. UC16: Workload scalability
17. UC17: Cluster autoscaling
18. UC18: Metrics and Logging
19. UC19: Network graphs
20. UC20: Policy violation dashboard
21. UC21: Day 2 Operations
22. UC22: Cluster upgrades
23. UC23: Developer onboarding
24. UC24: Trusted SW supply chain

Day 3 (hands-on workshop)

25. UC25: Node Resiliency
26. UC26: Cluster and site resiliency
27. UC27: Backup & Restore

Hands-on labs

1. UC02: VM as a service
2. UC04: Container as a service
3. UC06: VM migration as a service
4. UC11: Authorization and RBAC
5. UC12: Zero Trust enforcement
6. UC16: Workload scalability
7. UC24: Trusted SW supply chain