

ssh Mon 15:31 Niklaus Hirt 74° 0.4W

Charged

IBM Multicloud Manager

https://5.39.74.54:8443/multicloud/policies/create

Create resourceCatalog

Governance and risk / Policies /

Create policy ⓘ

CancelCreate

Name

demo-policy

Specifications ⓘ

Cluster selector ⓘ

Standards ⓘ

Categories ⓘ

Controls ⓘ

Begin typing to search for label to select

☐ Enforce if supported ⓘ

Policy YAML

Search

```
1 apiVersion: policy.mcm.ibm.com/v1alpha1
2 kind: Policy
3 metadata:
4   name: demo-policy
5   namespace: kube-system
6   annotations:
7     policy.mcm.ibm.com/standards: PCI
8     policy.mcm.ibm.com/categories: SystemAndCommunicationsProtections
9     policy.mcm.ibm.com/controls:
10 spec:
11   complianceType: musthave
12   remediationAction: inform
13   namespaces:
14     exclude: ["kube-*"]
15     include: ["default"]
16   role-templates:
17     - apiVersion: roletemplate.mcm.ibm.com/v1alpha1 # role must follow defined permissions
18       metadata:
19         namespace: "" # will be inferred
20         name: operator-role-policy
21       selector:
22         matchLabels:
23           dev: "true"
24       complianceType: musthave # at this level, it means the role must exist with the rules that it musthave below
25       rules:
26         - complianceType: musthave # at this level, it means if the role exists the rule is a musthave
27           policyRule:
28             apiGroups: ["extensions", "apps"]
29             resources: ["deployments"]
30             verbs: ["get", "list", "watch", "create", "delete", "patch"]
31         - complianceType: "mustnothave" # at this level, it means if the role exists the rule is a mustnothave
32           policyRule:
33             apiGroups: ["core"]
34             resources: ["secrets"]
35             verbs: ["get", "list", "watch", "delete", "create", "update", "patch"]
36
37 ---
38 apiVersion: mcm.ibm.com/v1alpha1
39 kind: PlacementBinding
40 metadata:
41   name: binding-demo-policy
42   namespace: kube-system
43 placementRef:
```

IBM Cloud Pak for Multicloud Management

Create resourceCatalog

Governance and risk / Policies /

Create policy ⓘ

CancelCreate

Name

demo-policy

Specifications ⓘ

1 x Role

☐ Limitrange-limit memory usage

☐ Mutationpolicy-no mutation allowed

☐ Namespace-must have namespace 'prod'

☐ Networkpolicy-deny network request

☐ Pod-nginx pod must exist

☐ Podsecuritypolicy-no privileged pods

☒ Role-role must follow defined permissions

☐ Rolebinding-role binding must exist

☐ Secretencryptionpolicy-Kubernetes secrets encryption

☐ Vulnerabilitypolicy-detect image vulnerabilities

☐ Enforce if supported ⓘ

Policy YAML

Search

```
1  apiVersion: policy.mcm.ibm.com/v1alpha1
2  kind: Policy
3  metadata:
4    name: demo-policy
5    namespace: kube-system
6    annotations:
7      policy.mcm.ibm.com/standards:
8      policy.mcm.ibm.com/categories:
9      policy.mcm.ibm.com/controls:
10 spec:
11   complianceType: musthave
12   remediationAction: inform
13   namespaces:
14     exclude: ["kube-*"]
15     include: ["default"]
16   role-templates:
17     - apiVersion: roletemplate.mcm.ibm.com/v1alpha1 # role must follow defined permissions
18       metadata:
19         namespace: "" # will be inferred
20         name: operator-role-policy
21       selector:
22         matchLabels:
23           dev: "true"
24       complianceType: musthave # at this level, it means the role must exist with the rules that it musthave below
25       rules:
26         - complianceType: musthave # at this level, it means if the role exists the rule is a musthave
27           policyRule:
28             apiGroups: ["extensions", "apps"]
29             resources: ["deployments"]
30             verbs: ["get", "list", "watch", "create", "delete", "patch"]
31         - complianceType: "mustnothave" # at this level, it means if the role exists the rule is a mustnothave
32           policyRule:
33             apiGroups: ["core"]
34             resources: ["secrets"]
35             verbs: ["get", "list", "watch", "delete", "create", "update", "patch"]
36 ---
37
38 apiVersion: mcm.ibm.com/v1alpha1
39 kind: PlacementBinding
40 metadata:
41   name: binding-demo-policy
42   namespace: kube-system
43 placementRef:
```