

Governance and risk / Policies /

# Create policy ⓘ

Cancel Create

Name

demo-policy

Specifications ⓘ

1 x Role

Cluster selector ⓘ

1 x cloud: "RHOCp"

Standards ⓘ

1 x PCI

Categories ⓘ

1 x SystemAndCommunicationsProtections

Controls ⓘ

Begin typing to search for label to select

☐ Enforce if supported ⓘ

Policy YAML

Search

```
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:
44   name: placement-demo-policy
45   kind: PlacementPolicy
46   apiGroup: mcm.ibm.com
47 subjects:
48   - name: demo-policy
49     kind: Policy
50     apiGroup: policy.mcm.ibm.com
51 ---
52 apiVersion: mcm.ibm.com/v1alpha1
53 kind: PlacementPolicy
54 metadata:
55   name: placement-demo-policy
56   namespace: kube-system
57 spec:
58   clusterLabels:
59     matchExpressions:
60     - {key: cloud, operator: In, values: ["RHOCp"]}
```

Governance and risk ⓘ

Refresh every 10s | Filter  
Last update: 9:52:10 AM

Overview Policies Security findings

Summary Standards ▾

Want to see less information? Collapse summary ^

PCI

7 / 8

CLUSTER FINDINGS

7 / 7

HIGH SEVERITY

NIST

1 / 8

CLUSTER FINDINGS

1 / 1

HIGH SEVERITY

Search security findings

Security findings Cluster findings

Description	Resources	Severity	Cluster	Standards	Controls	Categories	Update time
Policy that is not compliant	Policy: policy-demo	High	rhocp5	PCI	-	System And Information Integrity	16 minutes ago
Policy that is not compliant	Policy: policy-prod	High	rhocp5	PCI	-	System And Communications Protections, System And Information Integrity	16 minutes ago ...
Policy that is not compliant	Policy: policy-network	High	fyre-prod	NIST	-	System And Communications Protections	31 minutes ago
Policy that is not compliant	Policy: policy-dev	High	rhocp5	PCI	-	System And Information Integrity	33 minutes ago
Policy that is not compliant	Policy: policy-dev	High	ibm-rhocp	PCI	-	System And Information Integrity	4 days ago
Policy that is not compliant	Policy: policy-dev	High	rhocp5	PCI	-	System And Information Integrity	11 days ago
Policy that is not compliant	Policy: policy-dev	High	rhocp5	PCI	-	System And Information Integrity	11 days ago
Policy that is not compliant	Policy: policy-dev	High	rhocp5	PCI	-	System And Information Integrity	11 days ago

Governance and risk ⓘ

Refresh every 10s | Filter

Last update: 9:52:02 AM

Overview Policies Security findings

Create policy

Summary Standards Want to see less information? Collapse summary ^

PCI


1 / 2

CLUSTER VIOLATIONS

1 / 1


POLICY VIOLATIONS

FISMA



No violations

NIST



No violations

Search policies Policies Cluster violations

Policy name	Remediation	Cluster violations	Standards	Controls	Categories
policy-all	inform	0/1	NIST	-	System And Information Integrity
policy-mcm	inform	0/3	FISMA	-	System And Communications Protections
policy-network	inform	0/1	NIST	-	System And Communications Protections
policy-prod	inform	1/2	PCI	-	System And Communications Protections, System And Information Integrity
policy-rhocp-sdn	inform	0/2	FISMA	-	System And Communications Protections

items per page 10 | 1-5 of 5 items



Governance and risk / Policies /

# Create policy ⓘ

Cancel Create

Name

demo-policy

Specifications ⓘ

1 x Role

Cluster selector ⓘ

1 x cloud: "RHOC"

Standards ⓘ

1 x PCI

Categories ⓘ

1 x SystemAndCommunicationsProtections

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:
```



# Welcome, let's get started.

The IBM® Cloud Pak for Multicloud Management, running on Red Hat® OpenShift®, provides consistent visibility, governance, and automation from on premises to the edge. Enterprises gain capabilities such as multicluster management, event management, application management and infrastructure management. Enterprises can use this IBM Cloud Pak to help increase operational efficiency that is driven by intelligent data, analysis, and predictive golden signals, and gain built-in support for their compliance management.



## Define and deploy your own applications

Use policy based deployment to automate across environments.

[Docs](#)



## Be notified when problems occur

Set up procedures and automation.

[Docs](#)



## Monitor your application performance

As well as your infrastructure, including components in and outside Kubernetes.

[Docs](#)



## Automate cloud provisioning

Customize how you want to provision clusters and infrastructure.

[Docs](#)