Red Hat
Advanced Cluster Management
for Kubernetes

Key considerations for policy-based governance, risk, and compliance

Every organization is responsible for creating and enforcing a security posture that conforms to corporate and government policies and regulations. DevSecOps teams need to take a proactive approach to managing these security policies across clusters and applications. Here are three ways Red Hat® Advanced Cluster Management for Kubernetes can help.

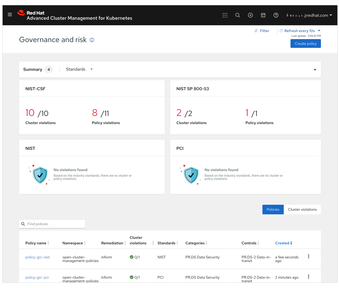
1. Track configuration drift and automate remediation across Kubernetes clusters

The ability to manage security configuration and state is now a requirement, not an option. It is even more important in a highly agile environment where things change very quickly.

With Red Hat Advanced Cluster Management, you can:

- **Automatically monitor and make sure security and configuration controls conform** to industry compliance and corporate standards using a policy-based governance and desired-state management engine.
- **Prevent unintentional or malicious configuration drift** that might expose threat vectors.
- **Report on or remediate policy** on Kubernetes cluster configuration, identity access management (IAM), and certificate management across clusters.
- **Streamline hardening** with out-of-the-box policies for faster time to value.
- **Create custom policy controllers** to augment default controllers (Kubernetes configuration, certificate management, and IAM).

Governance and risk posture overview



2. View and improve organizational compliance posture

As Kubernetes cluster environments grow, it becomes more difficult to view and maintain a compliance posture and monitor governance across the environment.

With Red Hat Advanced Cluster Management, you can:

- **View a consolidated Kubernetes environment compliance posture** through a governance and risk dashboard.
- **Collect cluster compliance details** and report on violations based on defined and enabled policies.
- **Use policies to automatically configure and maintain consistency** of security controls required by industry or other corporate standards like NIST, PCI, and HIPAA.[1]
- **Define custom policies** to best meet your specific organizational requirements and security best practices.
- **Identify and alert on security and compliance violations,** including Common Vulnerabilities and Exposures (CVEs), configuration drift, and version control.

[1] National Institute of Standards and Technology (NIST), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA)

Compliance policies and violation status

Policy name	Namespace	Remediation	Cluster violations	Standards
policy-certificatepolicy-1	call-center	inform	0/6	NIST, NIST CSF
policy-certificatepolicy-2	call-center	inform	0/3	NIST, NIST CSF
policy-rolebinding-1	default	inform	1/1	PCI
policy-koku-metrics-opera… disabled	koku-metrics-operator	inform	-	NIST CSF
policy-auth-provider	open-cluster-management-policies	enforce	0/4	NIST CSF

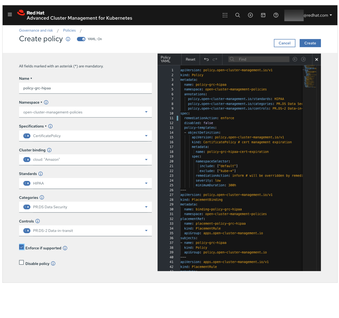
3. Support open source compliance technologies

Technologies like Open Policy Agent (OPA) and Open Security Content Automation Protocol (OpenSCAP) are gaining momentum. Organizations using these technologies need the ability to support and extend them.

With Red Hat Advanced Cluster Management, you can:

- **Enforce a desired state through remediation activities.** OPA is integrated to enforce OPA policies at runtime and receive policy violation information.
- **Unify policy enforcement** across the stack and use OPA to enforce policies in microservices and Kubernetes.
- **Automate scanning and reporting for vulnerabilities and misconfigurations.** Integration with the Compliance Operator, which is often deployed to Red Hat OpenShift® clusters, shows scanning and reporting information in a consolidated view.

Easily create and enforce policies



To learn more about Red Hat Advanced Cluster Management for Kubernetes, visit our YouTube channel.

Watch our videos on YouTube

Red Hat