Enabling Automation and Governance for Red Hat OpenShift using Kyverno

Red Hat® OpenShift® Container Platform is the industry-leading hybrid cloud platform powered by containers and Kubernetes. Using the OpenShift Container Platform simplifies and accelerates the development, delivery, and lifecycle management of a hybrid mix of applications, consistently anywhere across on-premises, public clouds, and edge. OpenShift Container Platform is designed to deliver continuous innovation and speed at any scale, helping organizations to be ready for today and build for the future.

OpenShift provides a great experience for development, operations, and security teams to build, deploy, and securely run containerized workloads and accelerate container application deployment. While OpenShift is secure by default, operations and security teams often have different requirements for automation, governance and security. Operations teams want to ensure Kubernetes best practices are followed by development teams and ensure that they build security into the platform with tools for configuration security, runtime security, admission controls, pod security policies and network policies. Security teams need to continuously monitor OpenShift environments for vulnerabilities, policy violations and compliance issues.

Kyverno, a Kubernetes-native policy engine, is the ideal solution to enable automation, governance and security for the OpenShift Container Platform. Kyverno runs as a dynamic admission controller in an OpenShift cluster. Kyverno receives validating and mutating admission webhook HTTP callbacks from the kube-apiserver and applies matching policies to return results that enforce admission policies or reject requests. Kyverno policies are written in Kubernetes-native YAML, significantly reducing the learning curve required to write custom policies. Kyverno policies can match resources using the resource kind, name, and label selectors to trigger actions such as validate, mutate, generate and image verification for container signing and software supply chain attestations.

Key highlights

Kyveno is a completely open source solution that helps improve security, governance and compliance for OpenShift.

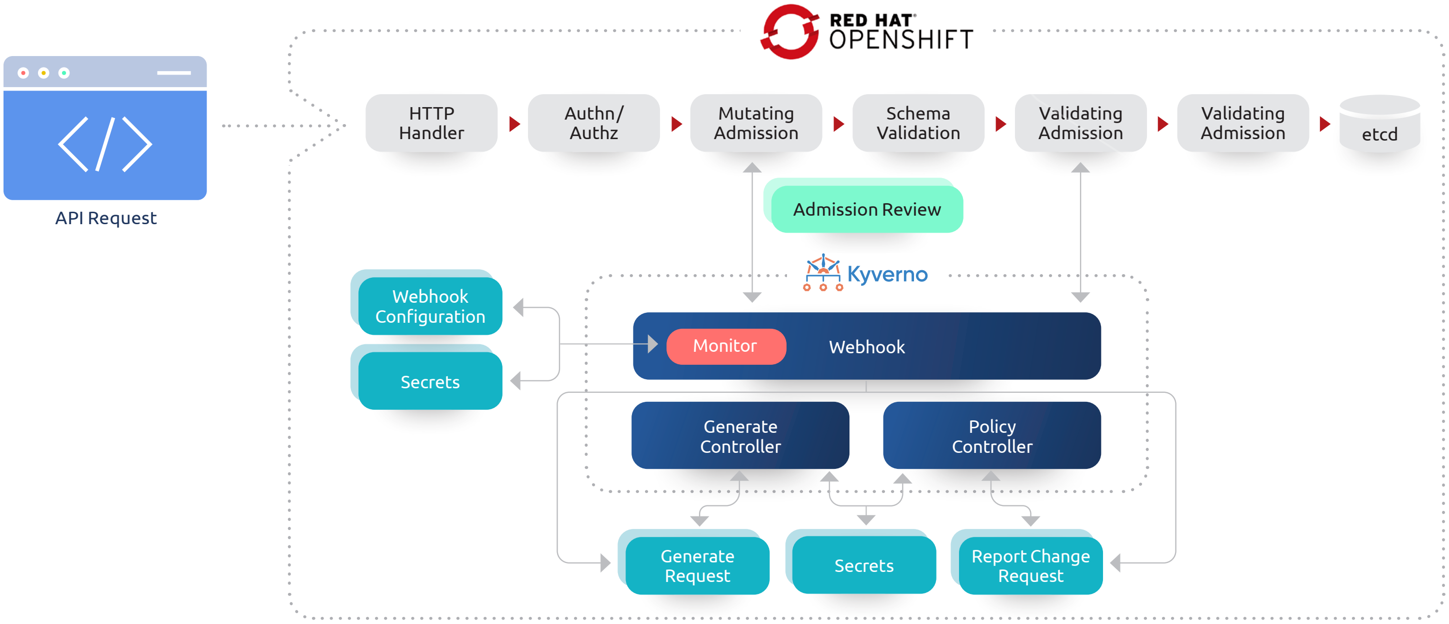
Kyverno community has build hundreds of policies that can be easily leveraged by OpenShift users.

Kyverno is a highly scalable and high performance admission controller for OpenShift.

Kyverno policies are easy to learn and write for OpenShift users.

Kyverno policies can be used to validate, mutate and generate OpenShift configuration.

Kyverno can be used for image verification in software supply chains.



HERE ARE SOME EXAMPLES OF HOW KYVERNO POLICIES CAN BE USED:

Automation

Kyverno's policies can be used to automatically generate Kubernetes resources based on a trigger. OpenShift administrators can:

- Automatically create a backup policy when a persistent volume claim is created
- Automatically add secrets for image repositories
- Automatically add certificates for ingress rule

Configuration Security

Kyverno's policies can be used to block insecure configurations. OpenShift administrators can configure policies to:

- Prevent pods with root privileges from being deployed
- Prevent pods that mount host volumes from being deployed
- Prevent pods that use host networking from being deployed

Governance

Kyverno's validate and mutate policies can be used to ensure that best practices are followed and configuration errors are detected early in the deployment pipeline. OpenShift administrators can configure best practice policies to:

- Ensure that required labels are always present on resources
- Ensure duplicate host names are not used in ingress
- Ensure duplicate routes are not used in ingress

Supply Chain Security

Kyverno can be used to secure software supply chains for OpenShift clusters. By leveraging the image verification capability of Kyverno, only signed and attested images from allowed image registries can be deployed to the cluster. This capability ensures that any image that was tampered with in the build pipeline does not get deployed on the cluster, thus enabling an additional layer of security in OpenShift environments.

Kyverno is a swiss-army knife for Kubernetes policy management and provides an extremely flexible and open solution for automation, security and governance in OpenShift environments. Kyverno community members have contributed over one hundred policies and several of them can be used by OpenShift users.

Nirmata, the company behind the CNCF open source project Kyverno, provides commercial tools, solutions, support and training from Kyverno. If you are interested in learning more about how to benefit from incorporating Kyverno in your OpenShift environment, please contact us at info@nirmata.com.

CONTACT US!

CLOUD NATIVE
COMPUTING FOUNDATION

Nirmata is a proud member of the Kubernetes community

Learn More