Kubernetes Governance using Kyverno

Anusha Hegde
Technical Product Manager
Nirmata

Agenda

- Governance in Kubernetes
- Kyverno Introduction
- Kubernetes Governance using Kyverno
- Q & A

What is Governance in Kubernetes?

https://www.cncf.io/blog/2020/05/29/kubernetes-governance-what-you-should-know/

Kubernetes Governance 101

- Be production-ready at scale
- Enforcing rules across Kubernetes clusters as well as applications running in those clusters.
- Governance dimensions
  - scope: where a specific rule should be applied, enforced or verified
  - target: what should be enforced or verified

Governance Scope

- Organizational units
  - departments, teams, groups, users
- Technical units
  - cloud provider, datacenter, region, group of clusters, namespaces, label selectors, etc.
- Both!

Governance Targets

- Security policies
  - access controls to users and teams
- Image management
  - production clearance for images
- Networking
  - pod security

Governance Targets

- Configuration constraints and policies
  - Kubernetes management tool configuration constraints
- Applications
  - app-level networking constraints, resources limits, usage etc.

Governance Implementation

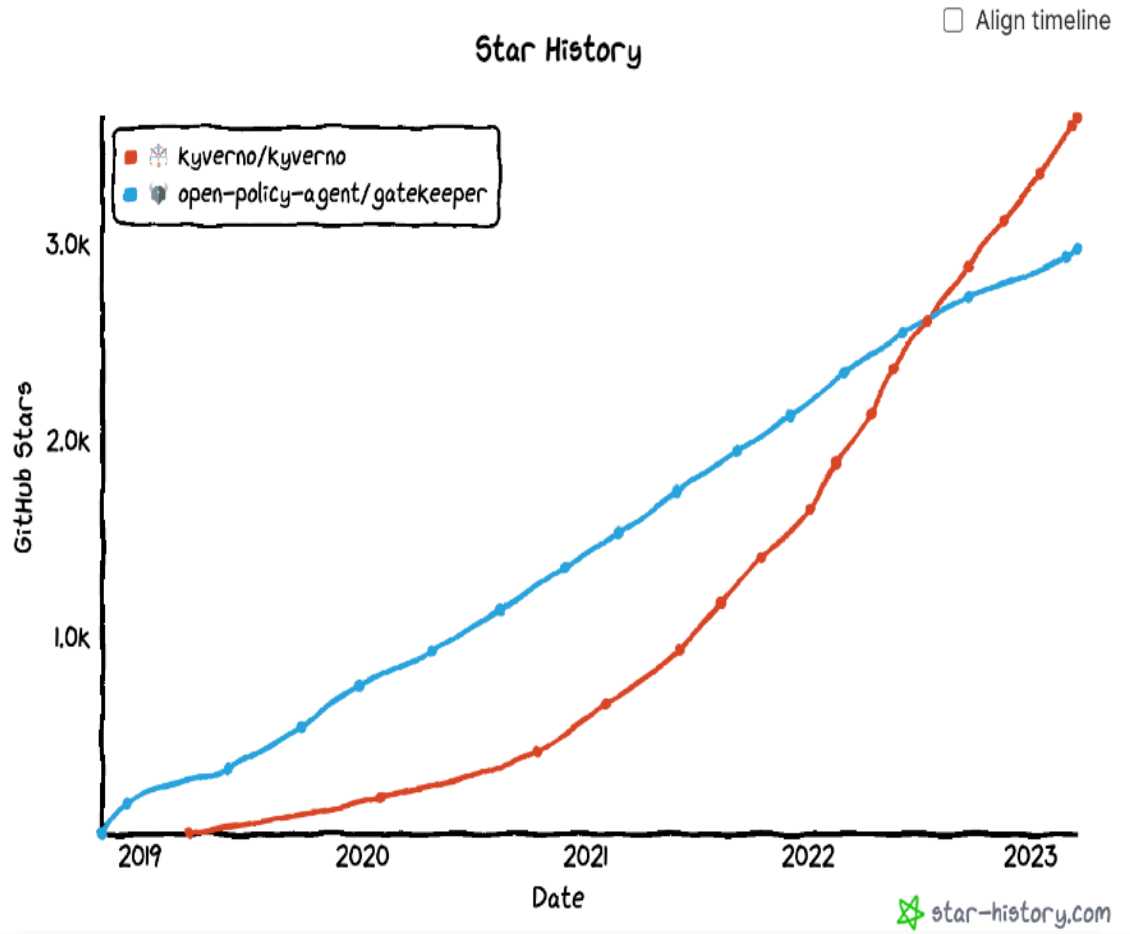
- Combine multiple specialized governance frameworks into a comprehensive solution
- Build your own framework on top of your centralized Kubernetes platform
- Select a Kubernetes platform that includes a comprehensive governance framework

Kyverno is the Kubernetes Native Policy Engine

A CNCF Incubating Project Created by Nirmata

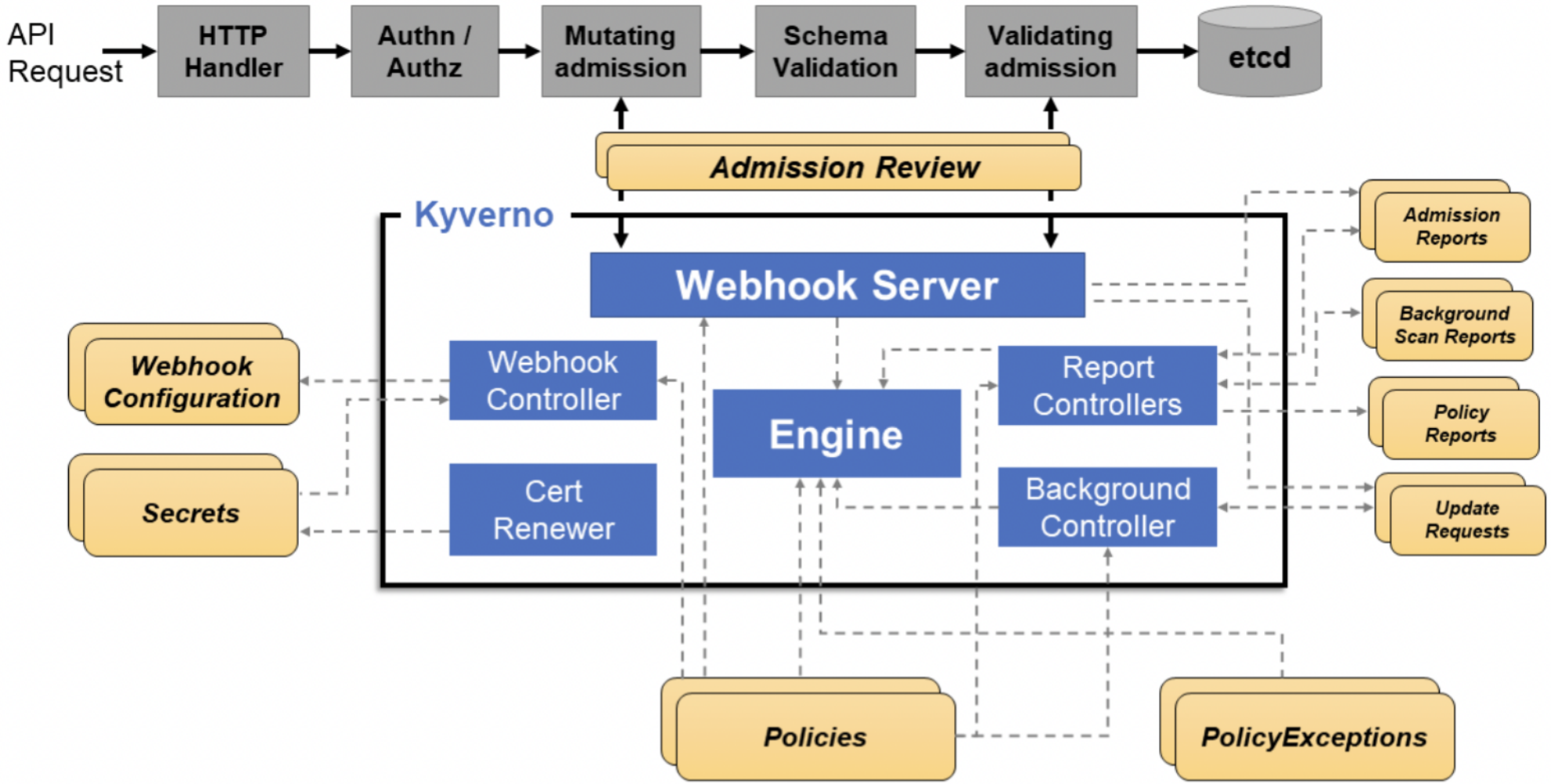
1. Cloud-Native Policy as Code
2. Map compliance controls to policies
3. Continuous compliance with background scans

2B+	image pulls
4.2K	GitHub Stars
300+	contributors
2000+	Slack members



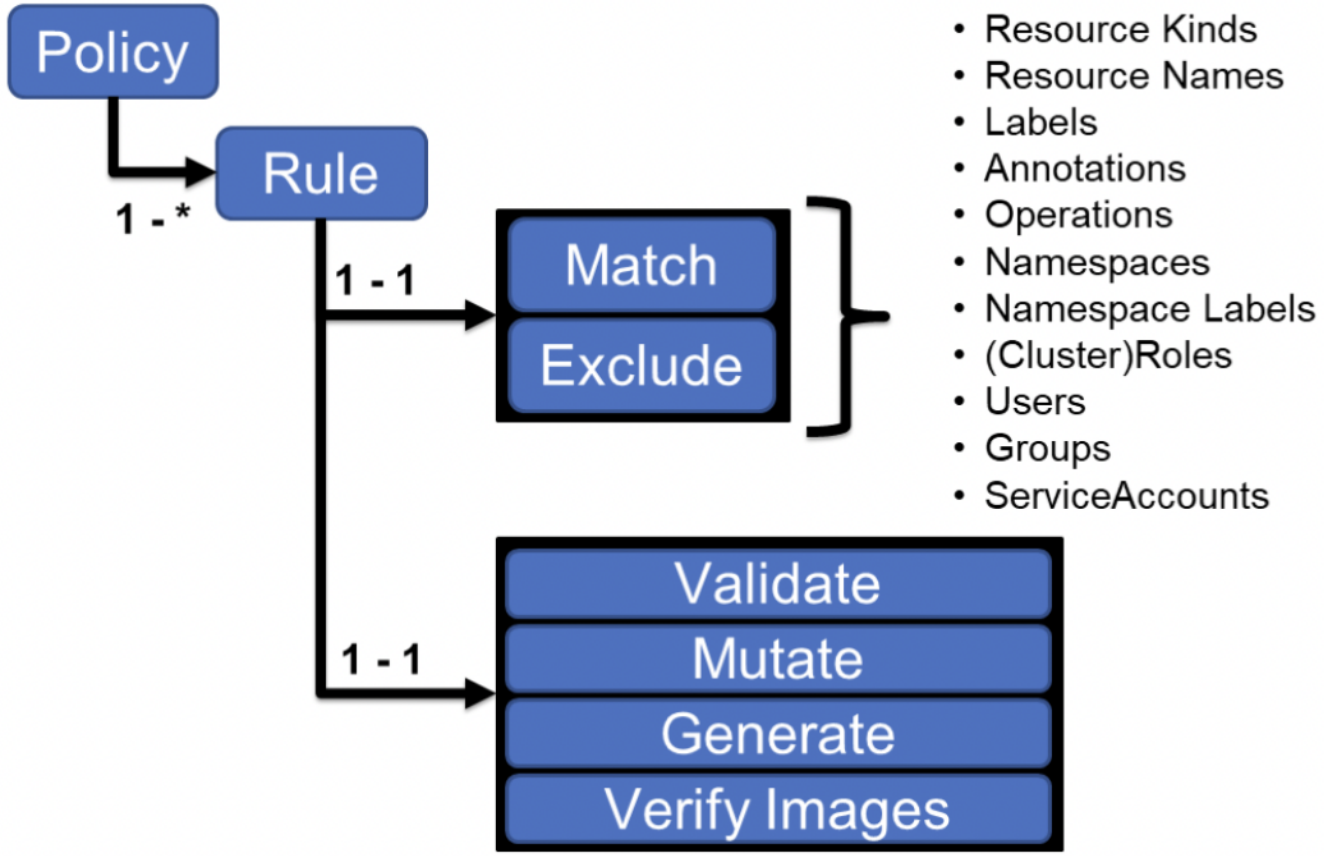
nirmata

Kyverno Architecture



nirmata

Kyverno Policy Anatomy



- Resource Kinds
- Resource Names
- Labels
- Annotations
- Operations
- Namespaces
- Namespace Labels
- (Cluster)Roles
- Users
- Groups
- ServiceAccounts

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: require-labels
spec:
  validationFailureAction: Audit
  background: true
  rules:
  - name: check-for-labels
    match:
      resources:
        kinds:
        - Pod
    validate:
      message: "The label `app.kubernetes.io/name` is required."
      pattern:
        metadata:
          labels:
            app.kubernetes.io/name: "?*"
```


nirmata

Benefits

- Automation and consistency
  - automate policy checks and violations
  - minimize human error
- Agility and flexibility
  - adapt to changing regulatory requirements

Benefits

- Enhanced security posture
  - define and enforce policies for security best practices
  - without hampering developer productivity
- DevOps Integration
  - enforce policies in development and deployment phases

Kyverno Use Cases for Governance (1/2)

- Pod Security Standards
  - baseline and restricted profiles
- Label and Annotation Validation
  - ensure proper identification and management of resources
- Policies for Infrastructure as Code
  - integration with Crossplane to enforce policies for cloud resources

…and many more @ **https://kyverno.io/policies**

Kyverno Use Cases for Governance (2/2)

- Cost Governance
  - enforce best practices for resource allocation, utilization, and cost optimization
- Software Supply Chain Security
  - define image verification policies
  - minimize the risk of unauthorized or tampered images

Summary

1. Kubernetes Governance is critical for being production-ready at scale

2. Policy-as-Code helps in automating security controls, compliances and operational best practices

3. Kyverno is Kubernetes-native and integrates seamlessly with other CNCF tools to achieve Governance across the board

4. Kyverno is easy to get started and try out!

Join the Kyverno Community

- The Kyverno docs & samples: https://kyverno.io
- Slack Channel: https://slack.k8s.io/#kyverno
- Monthly community meetings
- Weekly contributor meetings

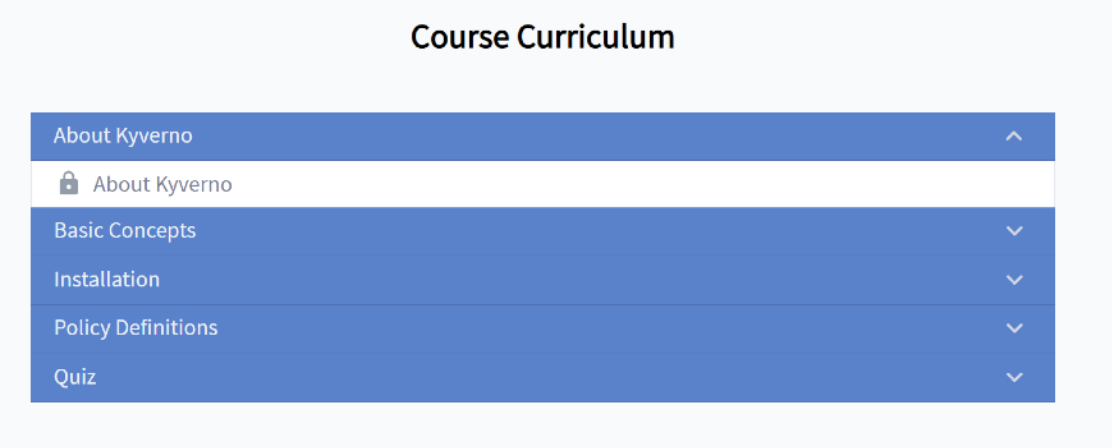
Join https://groups.google.com/g/kyverno

nirmata

Get Kyverno Certified!

- Free training and certification

https://learn.nirmata.com



nirmata

References

- Kyverno community site – https://kyverno.io
- Kyverno Policies - https://kyverno.io/policies/
- Kyverno playground - https://playground.kyverno.io/#/
- PolicyReport API: https://github.com/kubernetes-sigs/wg-policy-prototypes/tree/master/policy-report/pkg
- Open Security Controls Assessment Language (OSCAL): https://github.com/usnistgov/OSCAL

- 2023 Edition, The Ultimate Guide to Policy-based Governance, Security & Compliance for Kubernetes

  https://info.nirmata.com/guide-kubernetes-policy-governance-management

Thank-You!

https://try.nirmata.io