KubeCon | CloudNativeCon

Europe 2023

Policy Matters!

Kubernetes Policy Working Group
Introduction and Deep Dive

Agenda

- **Kubernetes & policy-based configuration management**
- **Policy Working Group Charter and Projects**
- **Policy Report API**
- **Policy Reporter Overview and Demo**

About us

nirmata

- Co-founder and CEO, Nirmata
- Co-chair Kubernetes Policy and Multi-tenancy Working Groups
- Kyverno Co-creator and Maintainer

LOVOO

- Senior Software Engineer, LOVOO
- Creator & maintainer of Policy Reporter
- CKA and a CKAD; OSS Contributor for Falco and Kyverno

Code of Conduct

Remember the **Golden Rule**: Treat others as you would want to be treated - with kindness and respect

Scan the QR code to access and review the **CNCF Code of Conduct**:

SCAN ME

Virtual Audience Closed Captioning

Closed captioning for the virtual audience is available during each session through Wordly. The Wordly functionality can be found under the “Translations” tab on the session page.

Wordly will default to English. If another language is needed, simply click the dropdown at the bottom of the “Translations” tab and choose from one of 26+ languages available so you don’t miss a beat from our presenters.

*Note: Closed captioning is ONLY available during the scheduled live sessions and will not be available for the recordings on-demand within the virtual conference platform.

Session Q+A

- Virtual attendees may submit questions to speakers through the CNCF Slack channel: **#2-Kubecon-sessions**

- Please create a thread and tag the speaker(s) with questions about their talk.

- Questions will be answered by the speaker and/or other community members after the session concludes.

Sponsor Shout-Out!

Thank you to our Session Recording Sponsor:

Kubernetes Policy Management

What is a policy?

Policies are configurations that govern other configurations or runtime behaviors

Network Policy: defines rules for traffic flows

Resource Quota: defines how much of a resource is consumed

Why are policies required?

- Kubernetes configuration are complex
- Kubernetes has multiple roles i.e., dev-sec-ops
- Policies act as a digital contract across roles
- Policies simplify Kubernetes configuration management
- Policies prevent misconfigurations

Kubernetes policy types

1. API Objects
2. Built-in admission controllers
3. ValidatingAdmissionPolicy
4. Dynamic Admission Controls

Kubernetes Policy Working Group (WG)

Provide an overall architecture that describes both the current policy related implementations as well as future policy related proposals in Kubernetes.

Through a collaborative method, we want to present both dev and end user a universal view of policy architecture in Kubernetes.

https://github.com/kubernetes/community/tree/master/wg-policy

Policy WG Projects

1. Policy Report API Completed
2. Kubernetes Policy Management Paper Completed
3. Kubernetes GRC Paper In Progress
4. Compliance mappings In discussion
5. Kubernetes docs updates In dicussion

Kubernetes Policy Management Paper

https://github.com/kubernetes/sig-security/blob/main/sig-security-docs/papers/policy/CNCF_Kubernetes_Policy_Management_WhitePaper_v1.

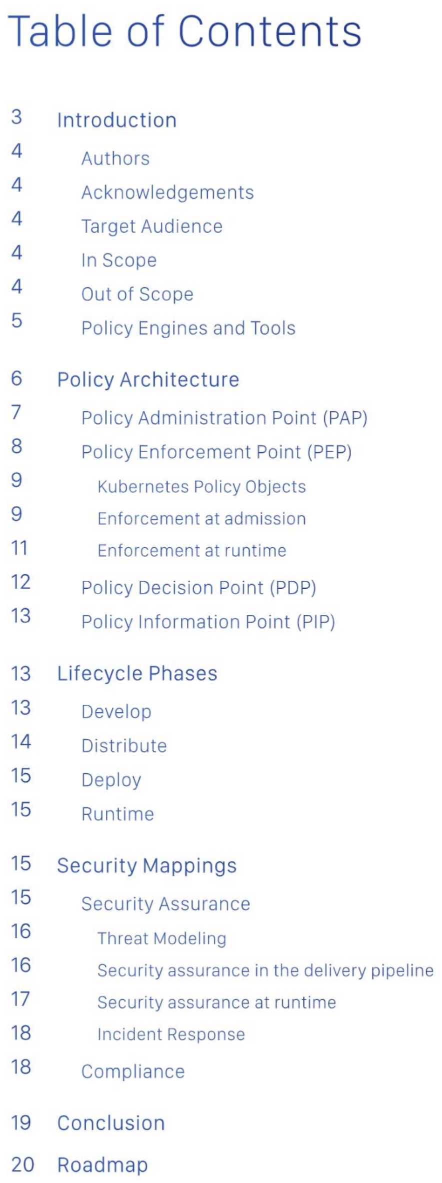


Table of Contents

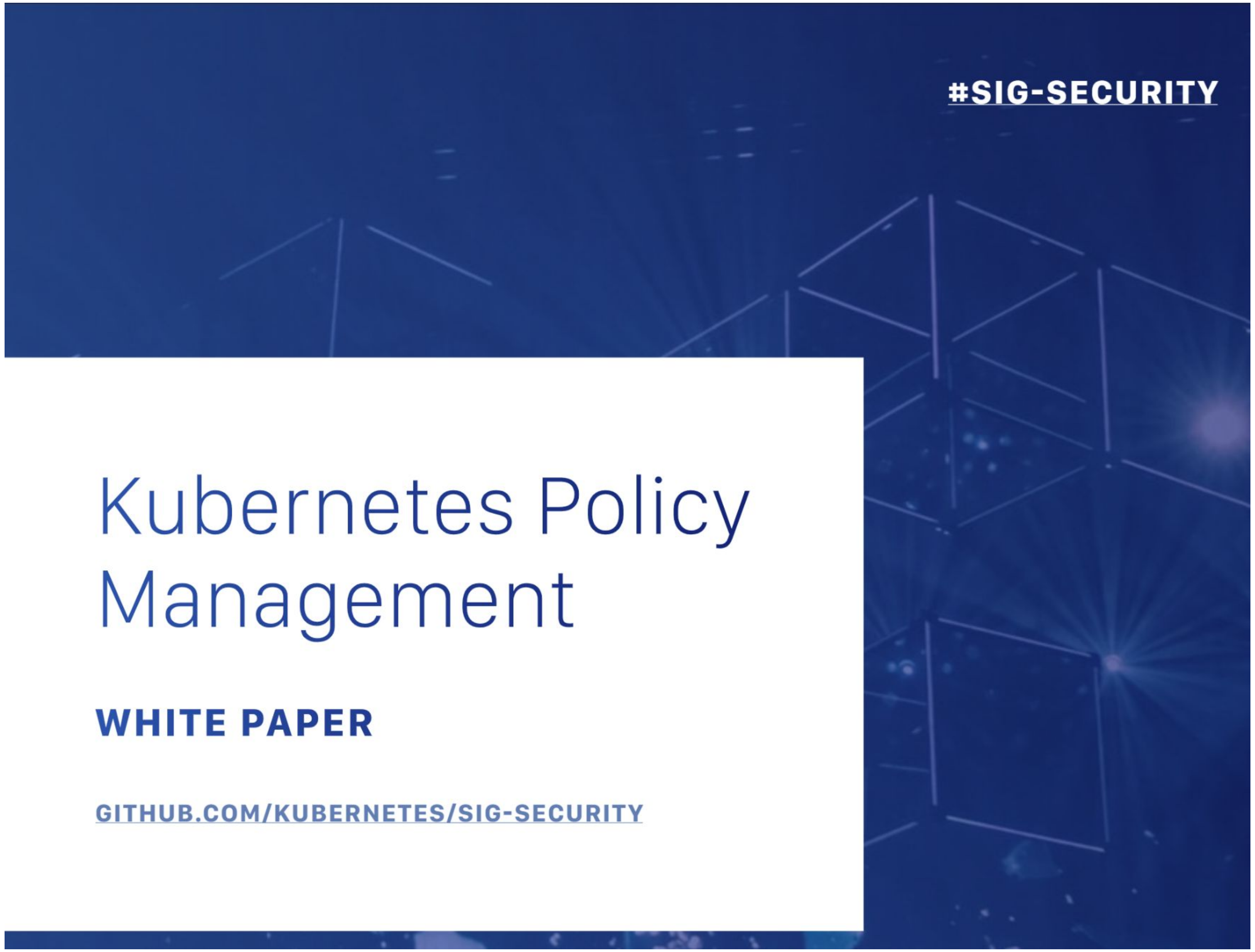
3 Introduction
4 Authors
4 Acknowledgements
4 Target Audience
4 In Scope
4 Out of Scope
5 Policy Engines and Tools

6 Policy Architecture
7 Policy Administration Point (PAP)
8 Policy Enforcement Point (PEP)
9 Kubernetes Policy Objects
9 Enforcement at admission
11 Enforcement at runtime
12 Policy Decision Point (PDP)
13 Policy Information Point (PIP)

13 Lifecycle Phases
13 Develop
14 Distribute
15 Deploy
15 Runtime

15 Security Mappings
15 Security Assurance
16 Threat Modeling
16 Security assurance in the delivery pipeline
17 Security assurance at runtime
18 Incident Response
18 Compliance

19 Conclusion
20 Roadmap



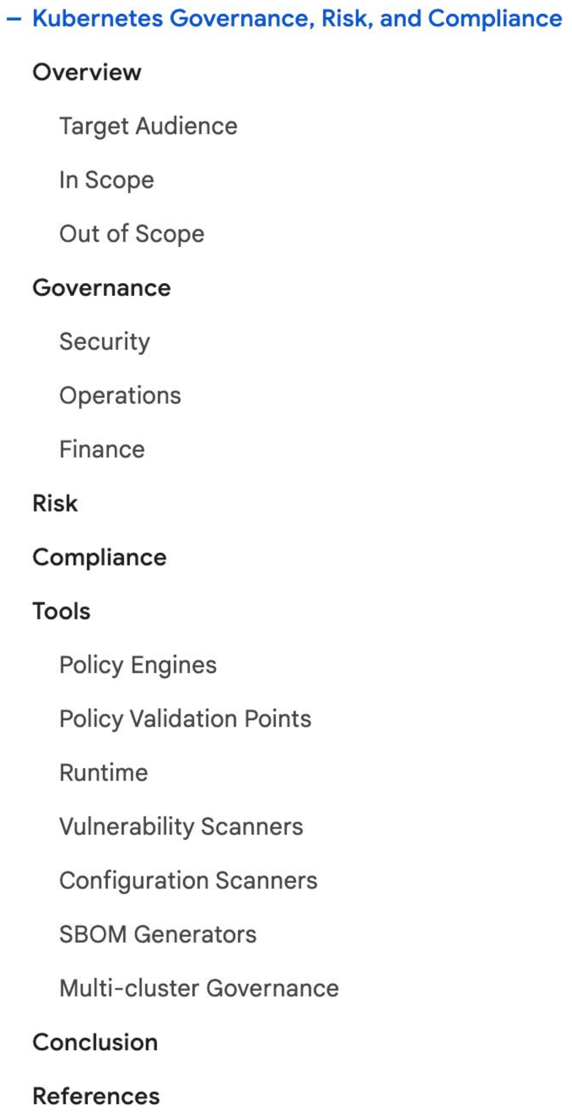
#SIG-SECURITY

Kubernetes Policy Management

WHITE PAPER

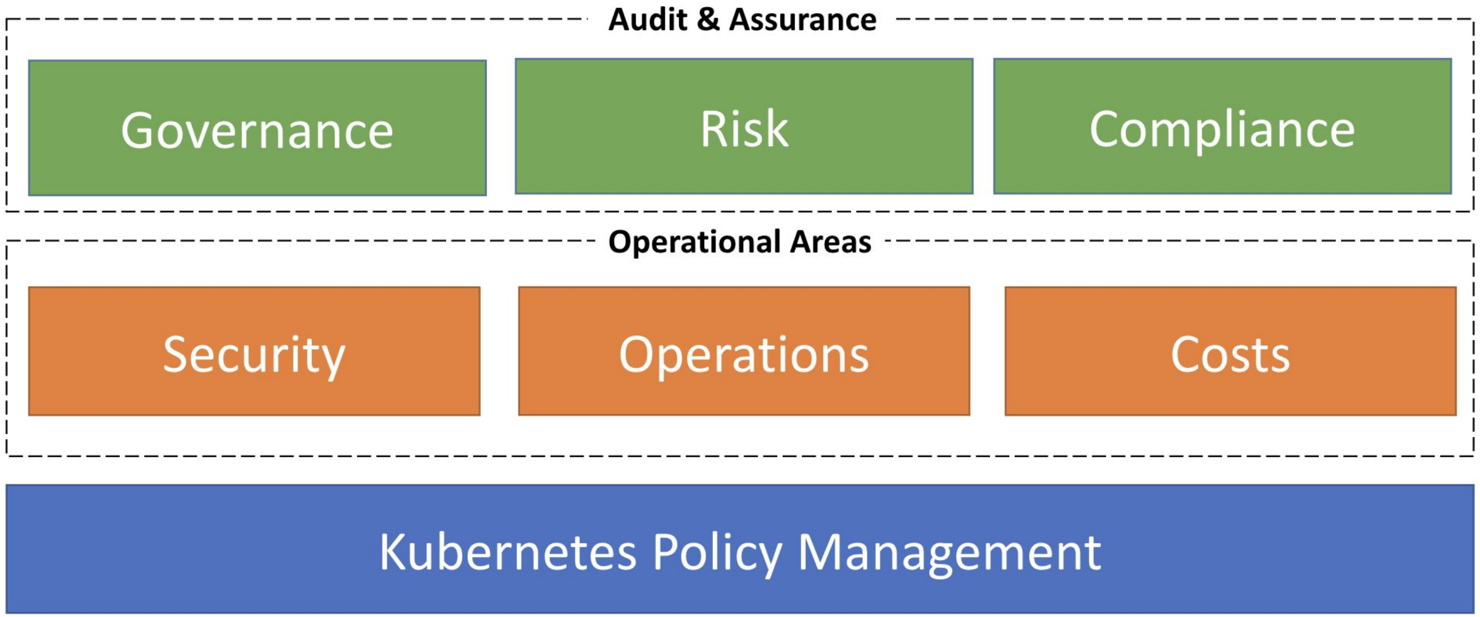
GITHUB.COM/KUBERNETES/SIG-SECURITY

Kubernetes GRC Paper



– Kubernetes Governance, Risk, and Compliance

- Overview
  - Target Audience
  - In Scope
  - Out of Scope
- Governance
  - Security
  - Operations
  - Finance
- Risk
- Compliance
- Tools
  - Policy Engines
  - Policy Validation Points
  - Runtime
  - Vulnerability Scanners
  - Configuration Scanners
  - SBOM Generators
  - Multi-cluster Governance
- Conclusion
- References



Audit & Assurance

Governance

Risk

Compliance

Operational Areas

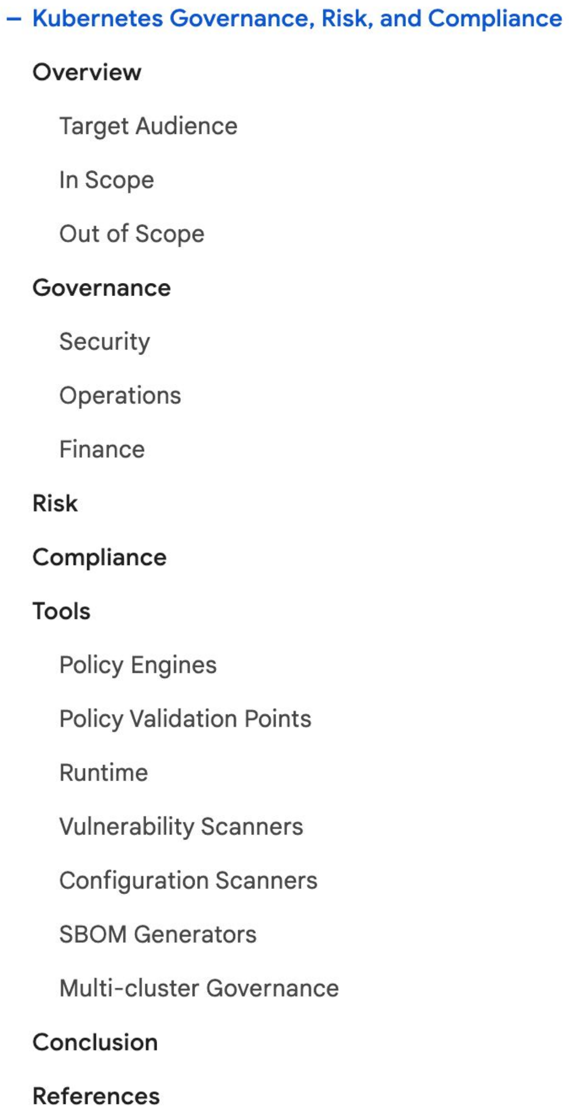
Security

Operations

Costs

Kubernetes Policy Management

Kubernetes GRC Paper

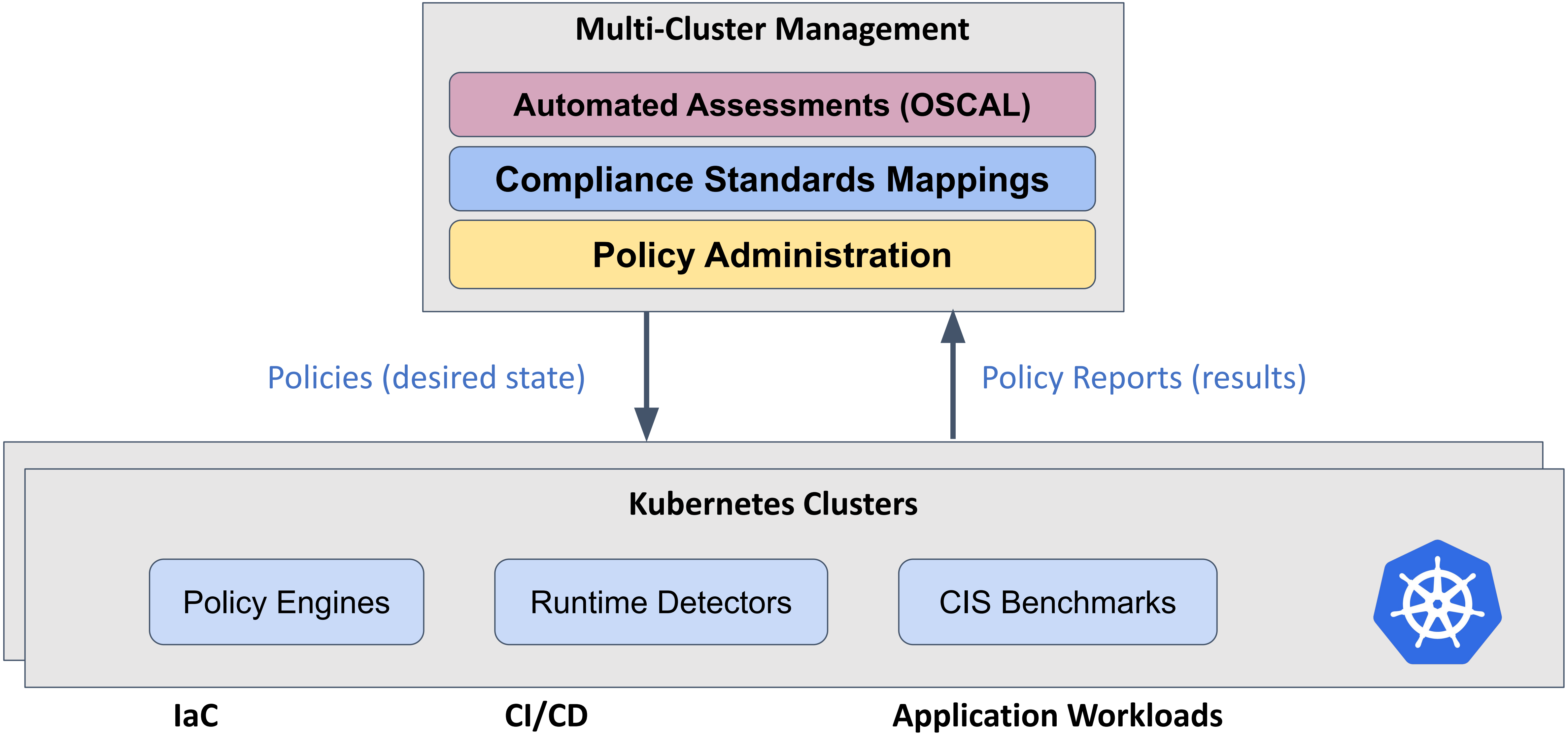


- Kubernetes Governance, Risk, and Compliance
  - Overview
    - Target Audience
    - In Scope
    - Out of Scope
  - Governance
    - Security
    - Operations
    - Finance
  - Risk
  - Compliance
  - Tools
    - Policy Engines
    - Policy Validation Points
    - Runtime
    - Vulnerability Scanners
    - Configuration Scanners
    - SBOM Generators
    - Multi-cluster Governance
  - Conclusion
  - References

Draft Document is Open For Feedback

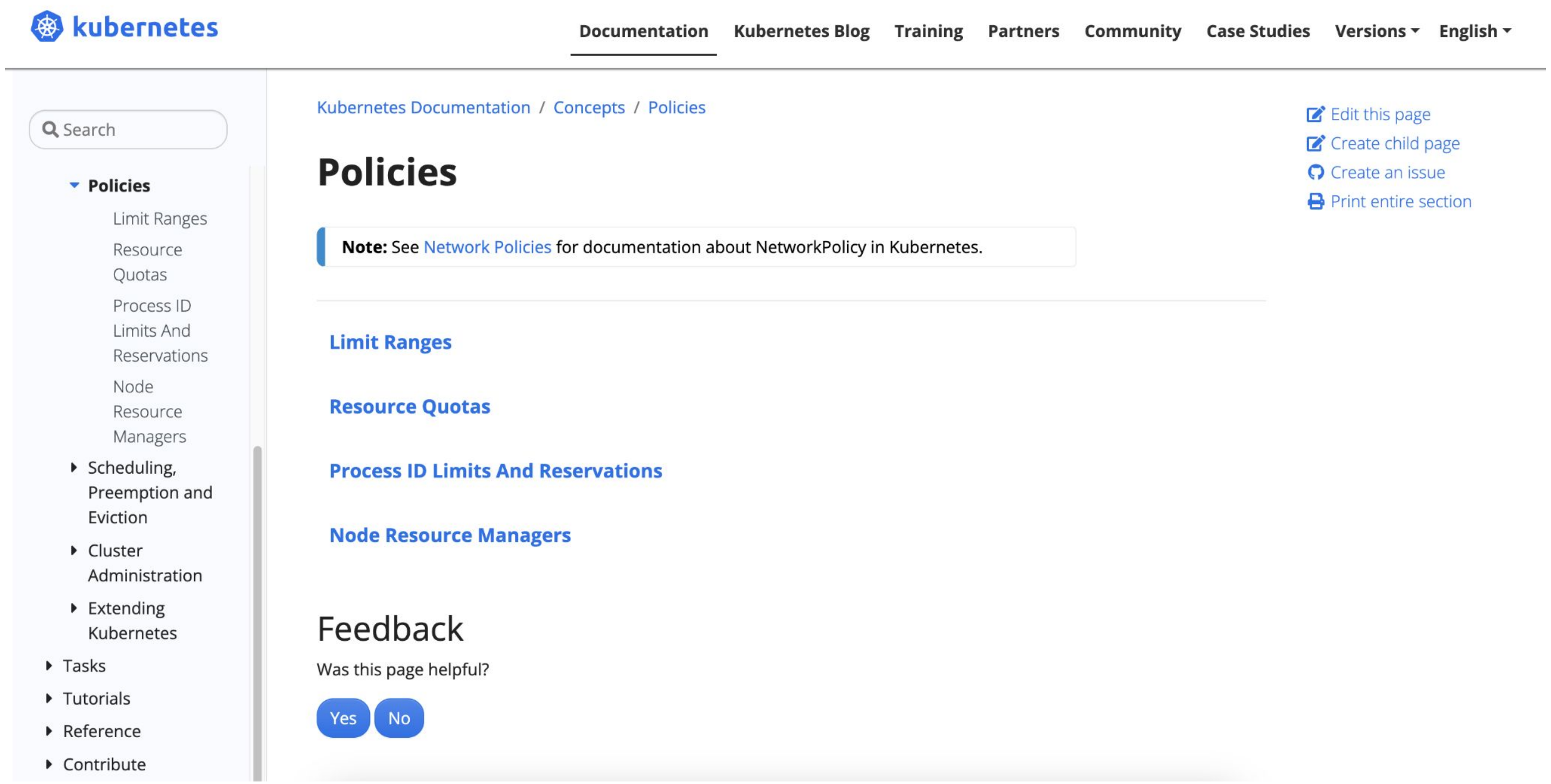
https://docs.google.com/document/d/1pWFBfMloSgupjJBcyq45qg9UHkaPjfAyUQHgmBdTqgQ/edit#heading=h.93cun373c61h

Policy - Compliance Mappings



Kubernetes Documentation Updates

Planning updates to the policies section in the Kubernetes documentation:



Kubernetes Documentation / Concepts / Policies

Policies

Note: See Network Policies for documentation about NetworkPolicy in Kubernetes.

Limit Ranges

Resource Quotas

Process ID Limits And Reservations

Node Resource Managers

Feedback

Was this page helpful?

Yes No

https://kubernetes.io/docs/concepts/policy/

Section Summary

1. Policies are essential for Kubernetes

2. Policies are a key building block for security, compliance, and automating operational workflows

3. The Policy WG has several projects and initiatives around simplifying policy management for Kubernetes

Policy Report API

Deep Dive

Custom Resource Definitions

- Policy Report API provides the `PolicyReport` and `ClusterPolicyReport` CRD

- Both providing `PolicyReportResults` for either namespaced- or cluster scoped resources

- `PolicyReportResults` contain information about the status of a policy validation and optional metadata such as the related resource or rule

Use cases

Depending on the policy engine that creates a `PolicyReport`, there are currently two main use cases

1. They reflect the current validation results of the existing resources compared to the policies applied there.
   - Example Tools
     - Kyverno validation policies
     - Kube Bench Adapter
     - Trivy Operator (Policy Report Adapter)

Use cases

2. Alternatively, `(Cluster)PolicyReports` are used as logs and provide a list of recent violations of various policies

- To avoid infinite growth in this use case, they usually have a configurable limit on results per report

  - Example Tools
    - Falcosidekick PolicyReport output
    - Tracee (Policy Report Adapter)
    - jsPolicy

Use cases

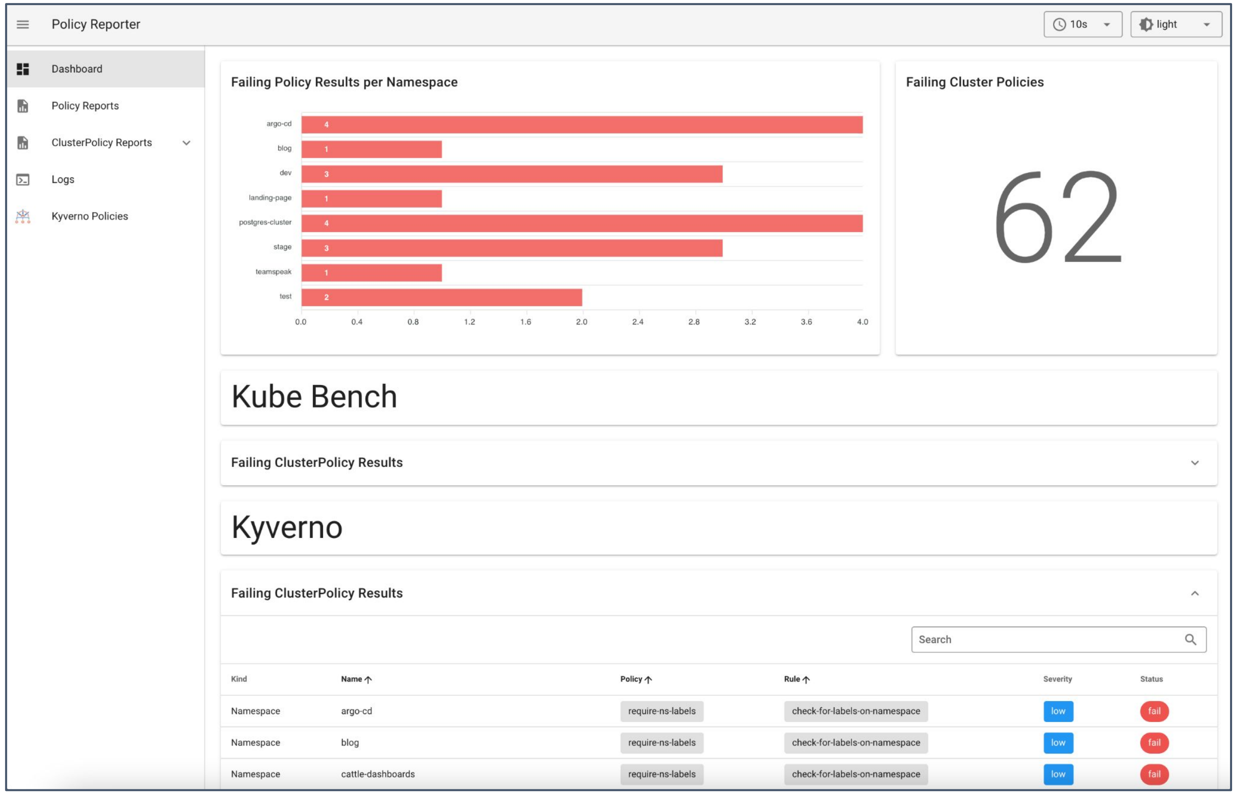
There are also other, more tool specific, use cases.

An example is the use in the Open Cluster Management project, which checks if a required policy in a cluster is violated by checking the corresponding `(Cluster)PolicyReports` for fail results.

Policy Reporter

Introduction

Policy Reporter adds observability and monitoring possibilities to your cluster security based on the `PolicyReport` API.



Failing Policy Results per Namespace

Failing Cluster Policies

62

Kube Bench

Failing ClusterPolicy Results

Kyverno

Failing ClusterPolicy Results

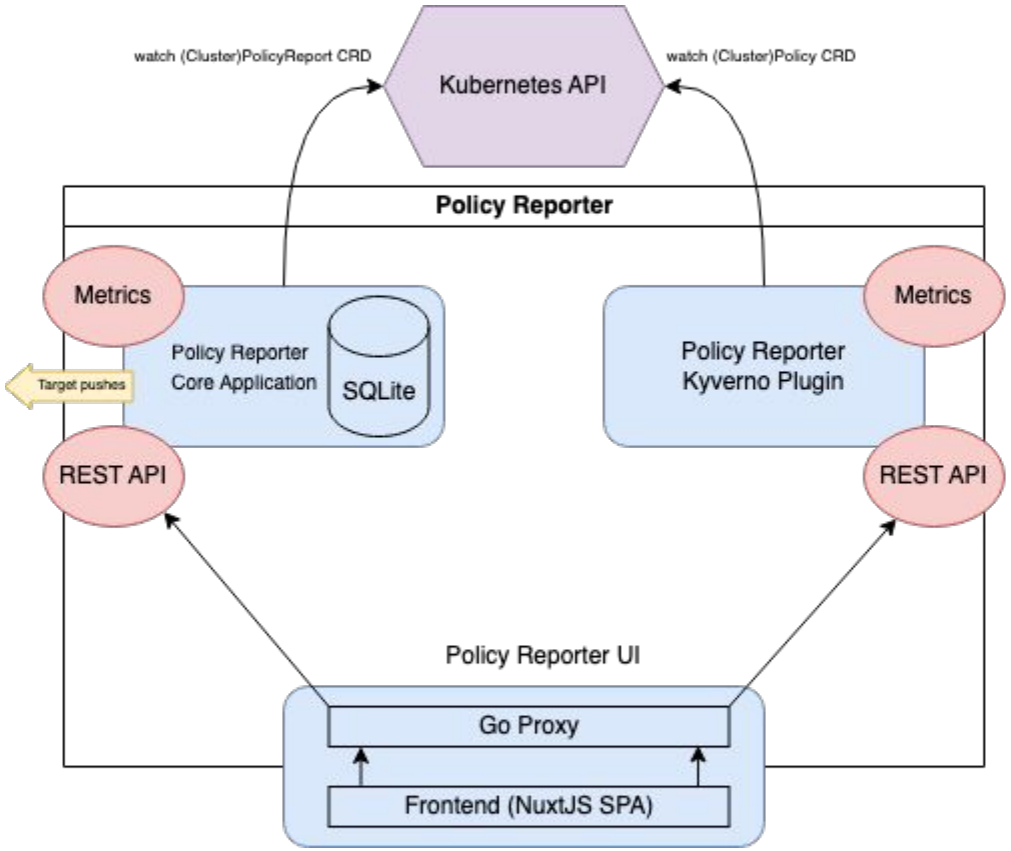
Kind	Name ↑	Policy ↑	Rule ↑	Severity	Status
Namespace	argo-cd	require-ns-labels	check-for-labels-on-namespace	low	fail
Namespace	blog	require-ns-labels	check-for-labels-on-namespace	low	fail
Namespace	cattle-dashboards	require-ns-labels	check-for-labels-on-namespace	low	fail

Feature Examples

- Send new results to tools like Grafana Loki, Slack or AWS S3
- Metrics to observe violations in well known monitoring solutions like Grafana
- Dashboard with detailed information, filter and graphs
- E-Mail Reports on a regular basis about the current status of your cluster security
- Granular configuration and filtering options

Demo

- Monitoring Tools:
  - Prometheus
  - Grafana (Loki)
- Installed Security Tools:
  - Kyverno
  - Trivy Operator
    - Trivy Operator Polr Adapter
- Policy Reporter



https://github.com/fjogeleit/kubecon2023-demo

Policy Reporter UI Demo

Summary

Policy WG

Planned tasks:

1. Promote Policy Report API to a SIG Project
2. Publish Kubernetes GRC Paper
3. Update policy section of the Kubernetes docs
4. Discuss how to define and manage compliance mappings

Policy WG

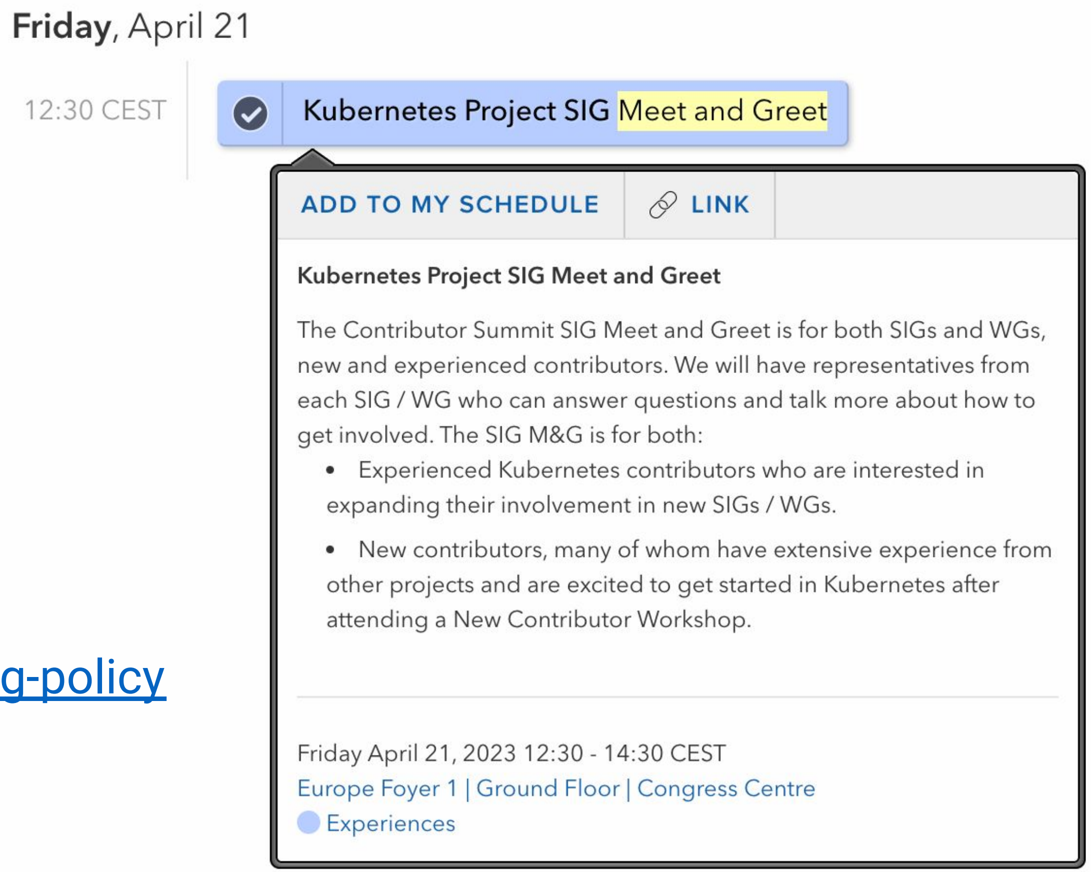
- Mailing list
  kubernetes-wg-policy@googlegroups.com

- Slack
  https://slack.k8s.io/#wg-policy

- GitHub
  https://github.com/kubernetes-sigs/wg-policy-prototypes/

- Community
  https://github.com/kubernetes/community/tree/master/wg-policy

Meetings: Bi-weekly Wed 8:00 AM Pacific



Friday, April 21

12:30 CEST

✓ Kubernetes Project SIG Meet and Greet

Kubernetes Project SIG Meet and Greet

The Contributor Summit SIG Meet and Greet is for both SIGs and WGs, new and experienced contributors. We will have representatives from each SIG / WG who can answer questions and talk more about how to get involved. The SIG M&G is for both:

- Experienced Kubernetes contributors who are interested in expanding their involvement in new SIGs / WGs.
- New contributors, many of whom have extensive experience from other projects and are excited to get started in Kubernetes after attending a New Contributor Workshop.

Friday April 21, 2023 12:30 - 14:30 CEST
Europe Foyer 1 | Ground Floor | Congress Centre
● Experiences

Session Feedback

Thank-You!

KubeCon | CloudNativeCon

Europe 2023