

**RESILIENCE**  
**REALIZED**



**KubeCon**



**CloudNativeCon**

North America 2021



KubeCon



CloudNativeCon

North America 2021

RESILIENCE

REALIZED

# Policy Matters!

*The Why, What, and How of Kubernetes Policy Management*

Aradhna Chetal, TIAA

Jayashree Ramanathan, Red Hat

Jim Bugwadia, Nirmata

Robert Ficcaglia, SunStone Secure

# The Panelists



**Aradhna Chetal**

Senior Director Executive  
Cloud Security Services,  
TIAA



**Jayashree Ramanathan**

Distinguished Engineer  
Chief Security and  
Governance Architect  
Red Hat



**Jim Bugwadia**

Co-founder and CEO  
Nirmata



**Robert Ficcaglia**

CTO  
SunStone Secure

# Kubernetes Policy 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 operators and users a universal view of policy architecture in Kubernetes.*

## Current Projects

1. Policy Report Custom Resource Definition
2. Kubernetes Policy Management Paper

## Meetings

Wed 8:00 AM Pacific  
Every two weeks

## Slack:

<https://slack.k8s.io/#wg-policy>

## GitHub:

[kubernetes-sigs/wg-policy-prototypes](https://github.com/kubernetes-sigs/wg-policy-prototypes)

# Policy Report CRD

Engine / Tool	Area	Status
Kyverno	Configuration Security	Completed
Policy Reporter	UI / Reporting / Notifications	Completed
kube-bench	CIS Kubernetes Benchmarks (Control plane, worker nodes)	Completed
Falco	Runtime Security	In progress
Trivy	Vulnerability scanning	In progress
KubeArmor	Runtime Security	Scheduled

# Kubernetes Policy Management

<b>Introduction</b>	<b>2</b>
Policy Management	2
Target Audience	2
In Scope	3
Out of Scope	3
Policy Engines and Tools	4
<b>Policy Architecture</b>	<b>4</b>
Policy Administration Point (PAP)	5
Policy Enforcement Point (PEP)	6
Admission Controls	8
Runtime enforcement	9
Policy Decision Point (PDP)	10
Policy Information Point (PIP)	11

<b>Lifecycle Phases</b>	<b>12</b>
Develop	12
Distribute	13
Deploy	13
Runtime	14
<b>Security Assurance</b>	<b>14</b>
Threat Modelling	14
Security across delivery pipelines	15
Supply Chain Security	15
Operations and Runtime Security	15
Incident Response	16
<b>Compliance</b>	<b>17</b>
<b>Conclusion</b>	<b>19</b>
<b>Acknowledgements</b>	<b>19</b>