



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

Advanced Kyverno Patterns

Automating Platform Security & Operations



Speaker



Frank Jogleit
Senior Software Engineer, Nirmata



Johannes Sonner
Platform Engineering Lead, Deutsche Telekom

Agenda



KubeCon

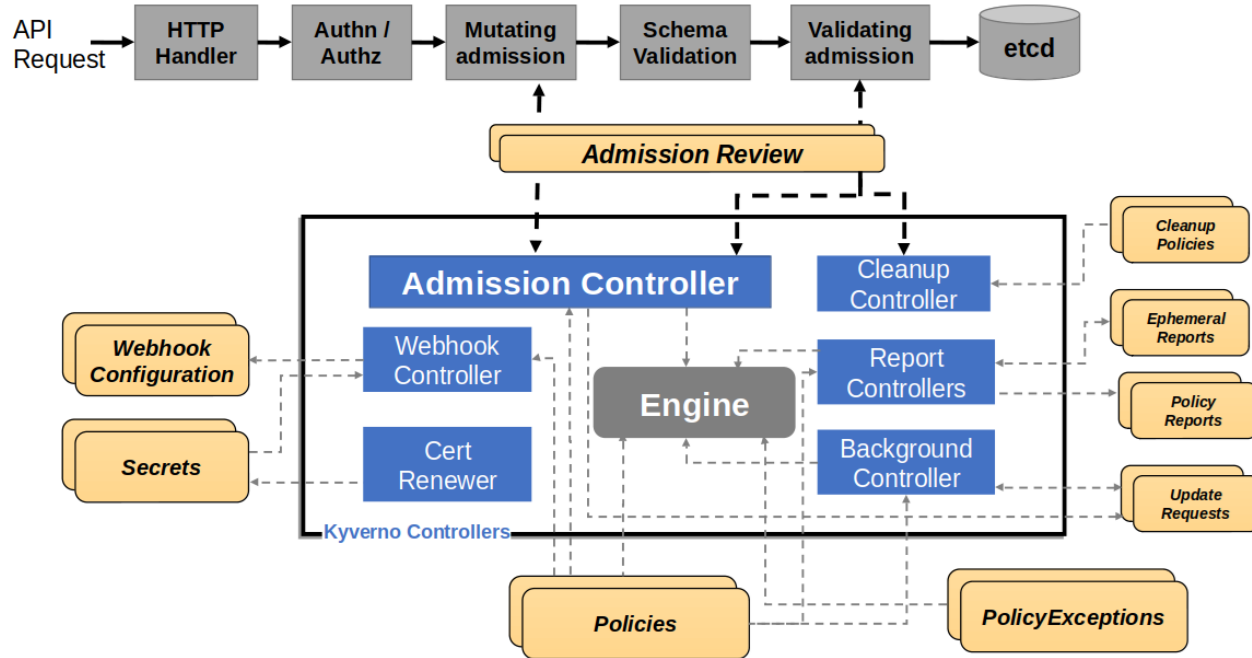


CloudNativeCon

Europe 2026

- **Kyverno Introduction & Kyverno Benefits**
- **The Mission:** Build a frictionless, secure IDP
- **The Execution (Patterns):**
 - *Self-Service:* Automating the "First Mile" (RBAC).
 - *Integration:* Closing the "Infrastructure Gap" (Crossplane/ACM).
 - *Optimization:* Enhancing 3rd party tools (Pulumi).
 - *Reporting:* Guardrails & Compliance
- **The Verdict:** What we learned.
- **Kyverno Roadmap**
- **Q&A**

Kyverno Introduction



Why Kyverno

1. Declarative YAML/CEL based Policy as Code
2. Full Resource Lifecycle Management
3. Integrated Reporting (OpenReports)
4. Fine-Grained Exceptions
5. Built for Kubernetes, now runs everywhere

Complete Resource Lifecycle Management

1. ValidatingPolicy
2. ImageValidatingPolicy
3. MutatingPolicy
4. GeneratingPolicy
5. DeletingPolicy

Kyverno vs Built-In Policies

Features	Kyverno	Kubernetes (VAP/MAP)
Low-code policies as resources	Y	Y
Admission Controls	Y	Y
Non-K8s resources (Terraform, Dockerfiles, etc.)	Y	N
Complex logic	Y	N
Background scans	Y	N
Shift-Left (CI/CD)	Y	N
Resource Validation	Y	Y
Resource Mutation	Y	Admission Only
Resource Generation	Y	N
Resource Cleanup	Y	N
Fine-Grained Policy Exceptions	Y	N
OpenReports	Y	N
OCI Image & Attestation Verification	Y	N

The Mission

260M
customers in
50 countries

IDP for B2C
Germany (15M
daily users)

500
microservices
by 40 teams



**Requires a strong digital foundation to build, deploy and run
microservices fast, secure and reliably.**

Automating The First Mile (RBAC)

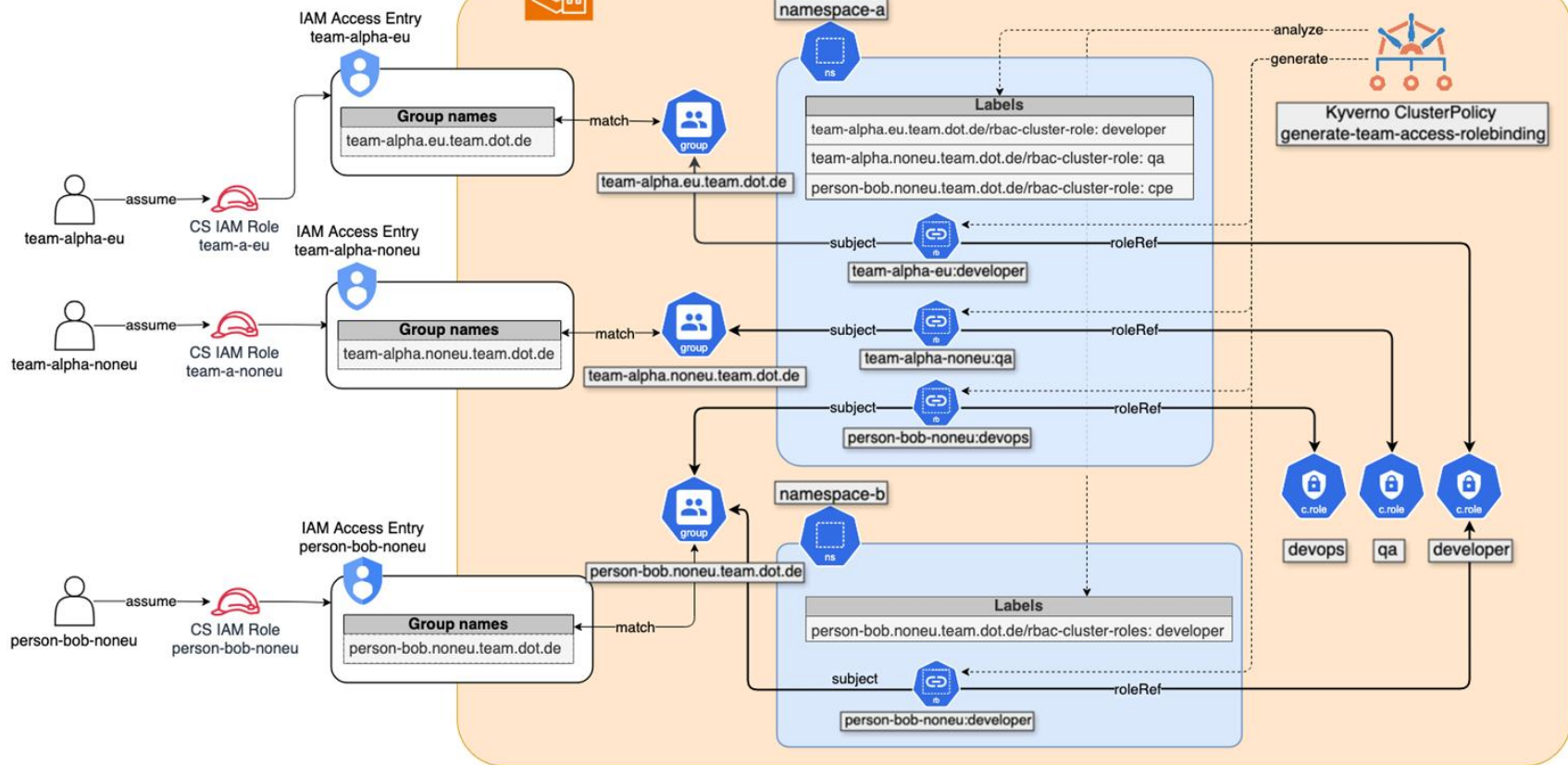
Goal

Self-service ephemeral namespaces with dynamic access

Implementation

- Dynamic RBAC based on namespace labels
- Users set labels for RBAC groups/Role combinations
- Kyverno creates RoleBindings

EKS Cluster



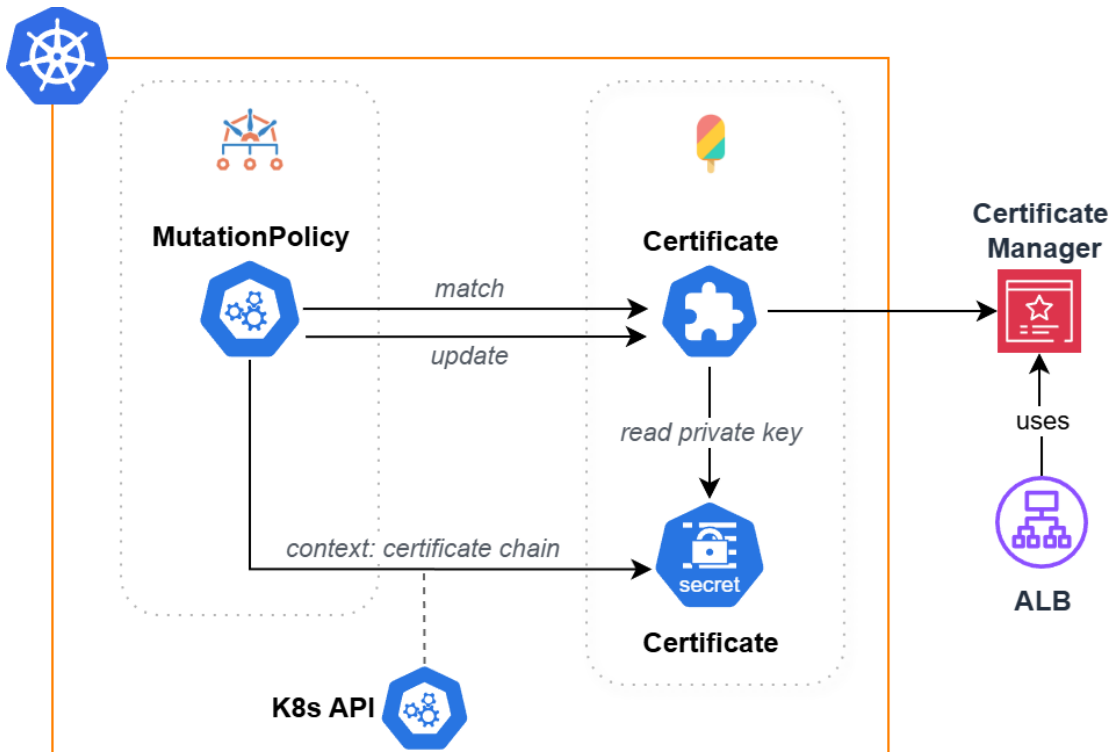
Closing Infrastructure Provider Gaps

Problem

Missing Field: Certificate Chain (Secret)

Implementation

- Leverage Mutate Policy to update Certificate
- `apiCall`: read secret data from Certificate



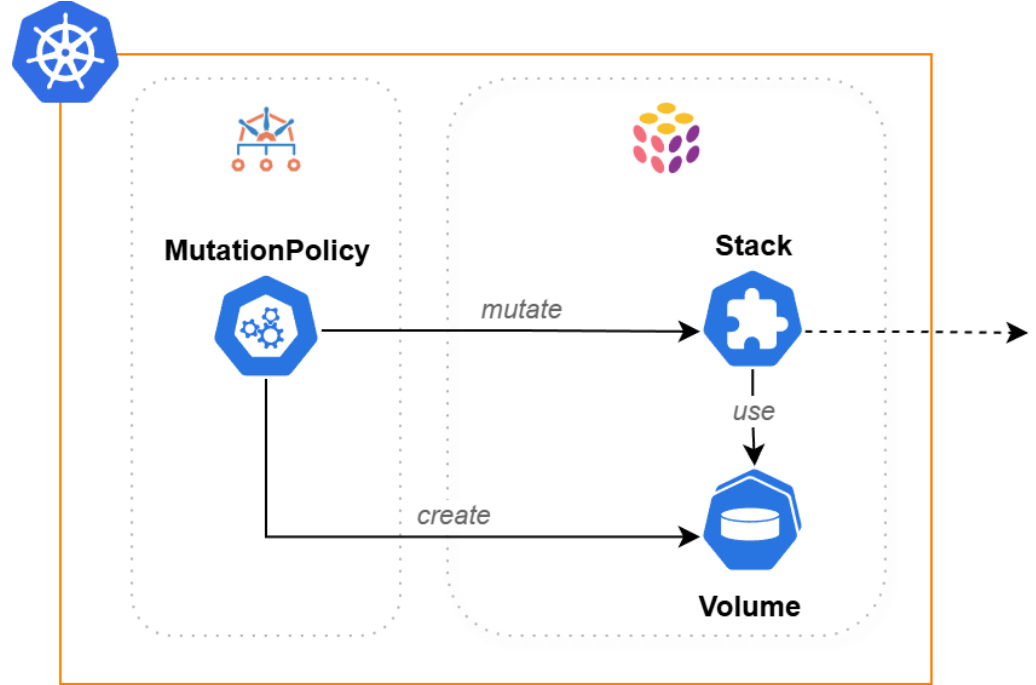
Closing Infrastructure Provider Gaps

Problem

Default configurations & Performance issues

Implementation

- Policies: Create volumes for caching
- Mutate: use volumes & shared config



KubeCon



CloudNativeCon

Europe 2026

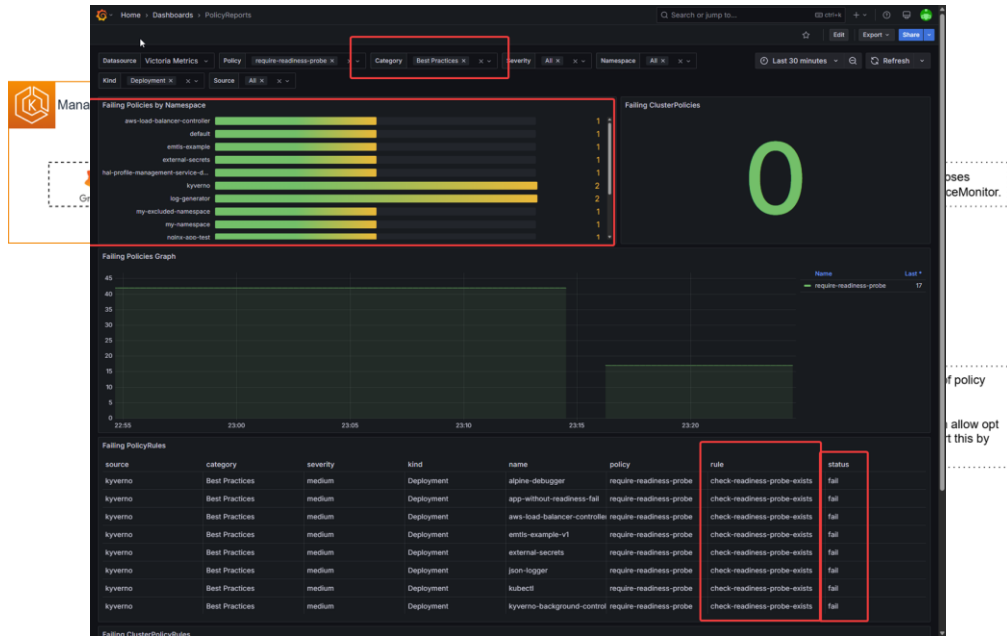
Guardrails & Compliance Reporting

Problem

- Identify compliance and configuration best-practices across many workloads

Implementation

- Policy reporter exposes metrics by ServiceMonitor
- Policies are clustered into different categories (reliability, security, etc.)
- Policies can be opted-out by label
- Visualization in Grafana



What we learned

1. Look at Kyverno as a holistic automation tool.
2. Visibility (reporting) is just as important as Enforcement.
3. Prefer a little bit of "duct tape" to custom controller implementations.

Upcoming

- **ClusterPolicy** and **CleanupPolicy** marked for deprecation in release v1.17.0; planned removal in v1.20.0
- Unified CLI and Playground for all payloads and policy types
- Extended Kyverno SDK / API development for easier implementation of the Kyverno Engine in all kinds of projects
- Kyverno AuthZ Server GA
- Migration of PolicyReporter, reports-server, Backstage Plugin to [OpenReports.io](https://openreports.io)



KubeCon



CloudNativeCon

Europe 2026

Q&A

