Policy-Based Infrastructure as Code with Kyverno

Kubernetes Community Days Bengaluru

3rd June 2023

Speakers

Kumar Mallikarjuna
Software Engineer
Nirmata

@kr_mallikarjuna
/kumarmallikarjuna
kumar@nirmata.com

Shivam Tyagi
Contributor

@twtyagi
/shivam-tyagi

nirmata

Outline

- Background
  - Policy Management
  - Infrastructure-as-Code (IaC)
- Kyverno
- Crossplane
- Crossplane + Kyverno
- Demo
- Summary
- Q&A

Background: Policy Management

Policy

- Policies define what can and cannot be done on a cluster
- Thus ensuring:
  - Security
  - Compliance
  - Best practices

Policy Engines

- Policy Engines apply policies on the cluster
- Examples:
  - Kyverno
  - OPA
  - jsPolicy

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: disallow-latest-tag
spec:
  validationFailureAction: audit
  background: true
  rules:
  - name: validate-image-tag
    match:
      any:
      - resources:
          kinds:
          - Pod
    validate:
      message: "Using a mutable image tag e.g. 'latest' is not allowed."
      pattern:
        spec:
          containers:
          - image: "!*:latest"
```

Sample Image Verification Policy [1]

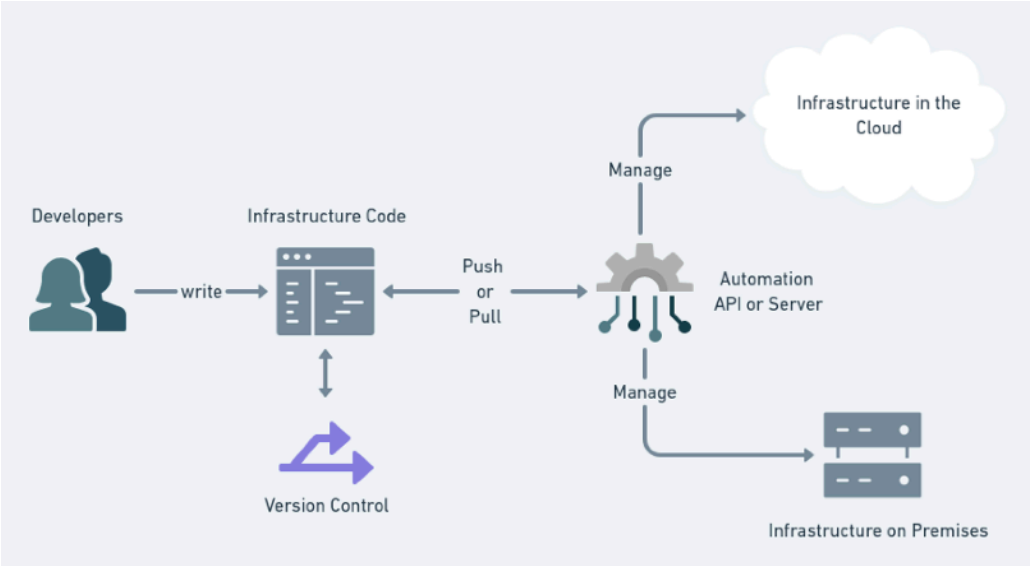
Background: Infrastructure-as-Code (IaC)

What is IaC?

- Managing and provisioning of infrastructure through code instead of through hardware/interactive configuration tools
- Tools:
  - Terraform
  - Crossplane*
  - Pulumi

Advantages

- Cost reduction
- Increase in speed of deployments
- Reduce errors
- Improve infrastructure consistency
- Eliminate configuration drift

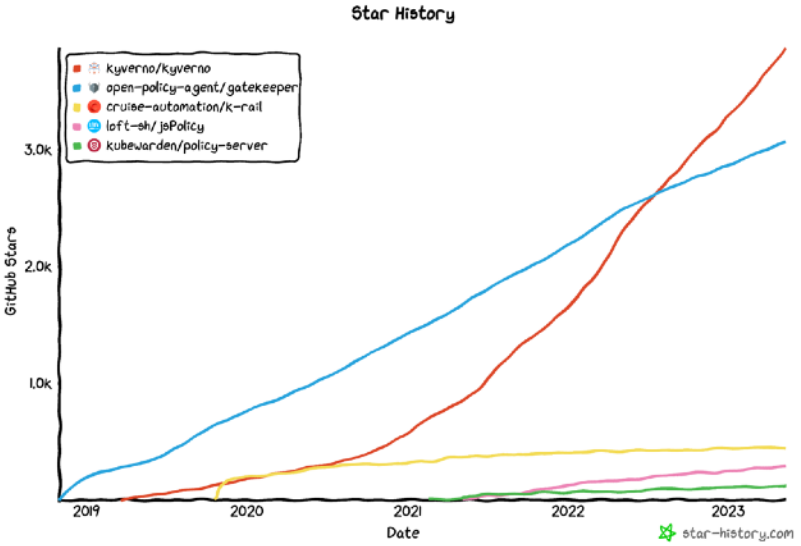


Infrastructure as Code Workflow [2]

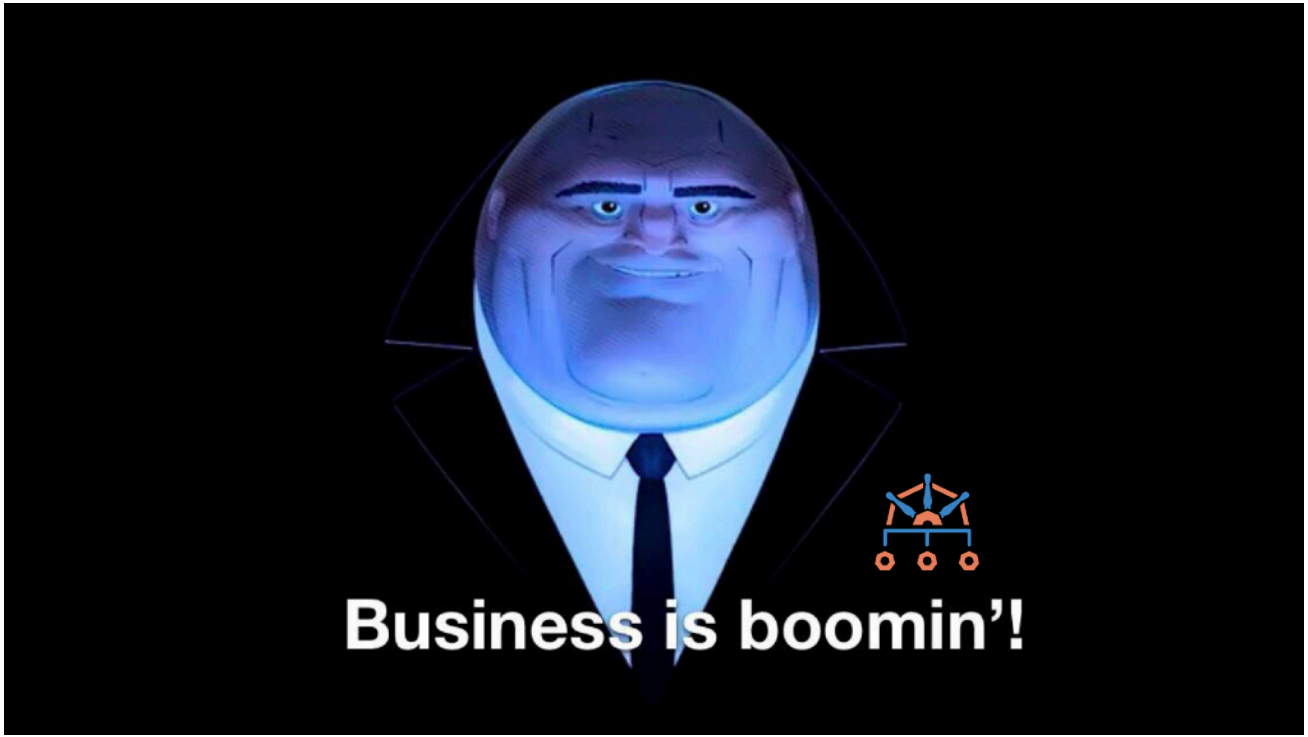
Kyverno

Why Kyverno?

- CNCF Incubating
- YAML-based policies
- Kubernetes-native
- Supports all Kubernetes resources including Custom Resources
- Most starred Kubernetes Policy Engine
- Largest policy library of any engine
- Allows integration into CI/CD pipelines
- Report generation
- Stats:
  - Over 3.9k stars on GitHub
  - More than 1.6 billion image pulls



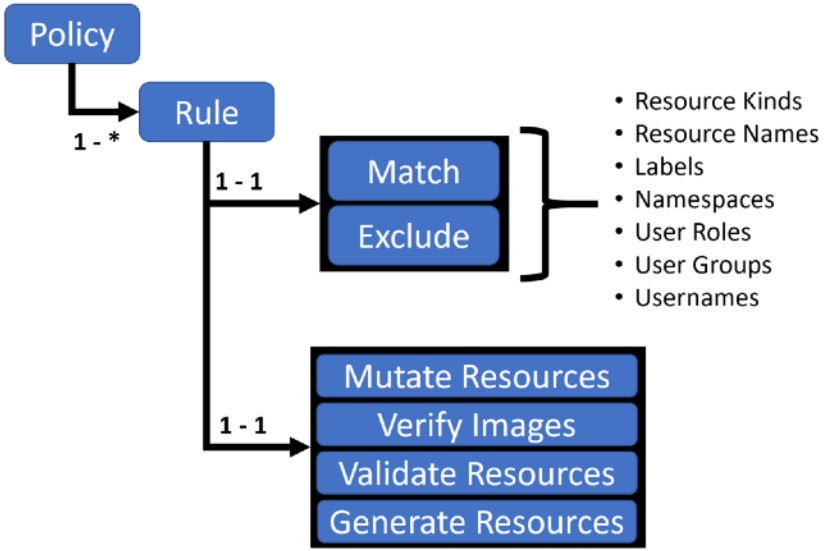
Kyverno Star History [3]



nirmata

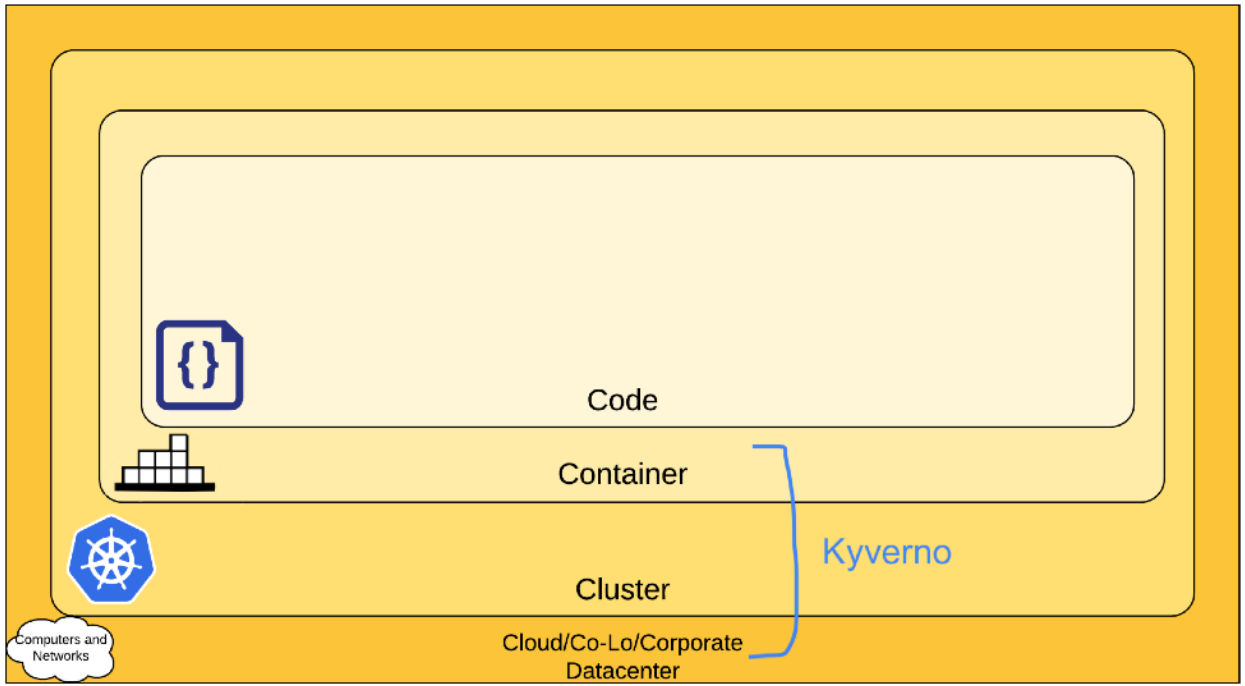
Kyverno: Use Cases

- Pod Security
- Multi-tenancy (Namespace provisioning)
- Supply chain security
- Fine-grained RBAC
- Sidecar injection with mounts, etc.
- And much more… see https://kyverno.io/policies/



Kyverno Policies and Rules [4]

Kyverno: Scope



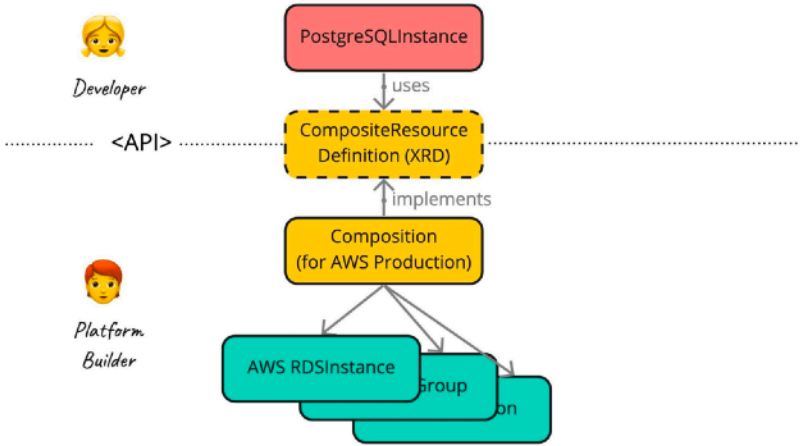
The 4C's of Cloud Native Security [5]

Crossplane

- CNCF Incubating
- YAML-based cloud resource definitions
- Kubernetes-native
- Supports:
  - AWS
  - Azure
  - GCP
  - More…
- Uses Kubernetes controllers to provision and reconcile infrastructure
- Can create new abstractions and APIs
- Allows security and compliance enforcement across resources or clouds, without exposing any complexity to the developers

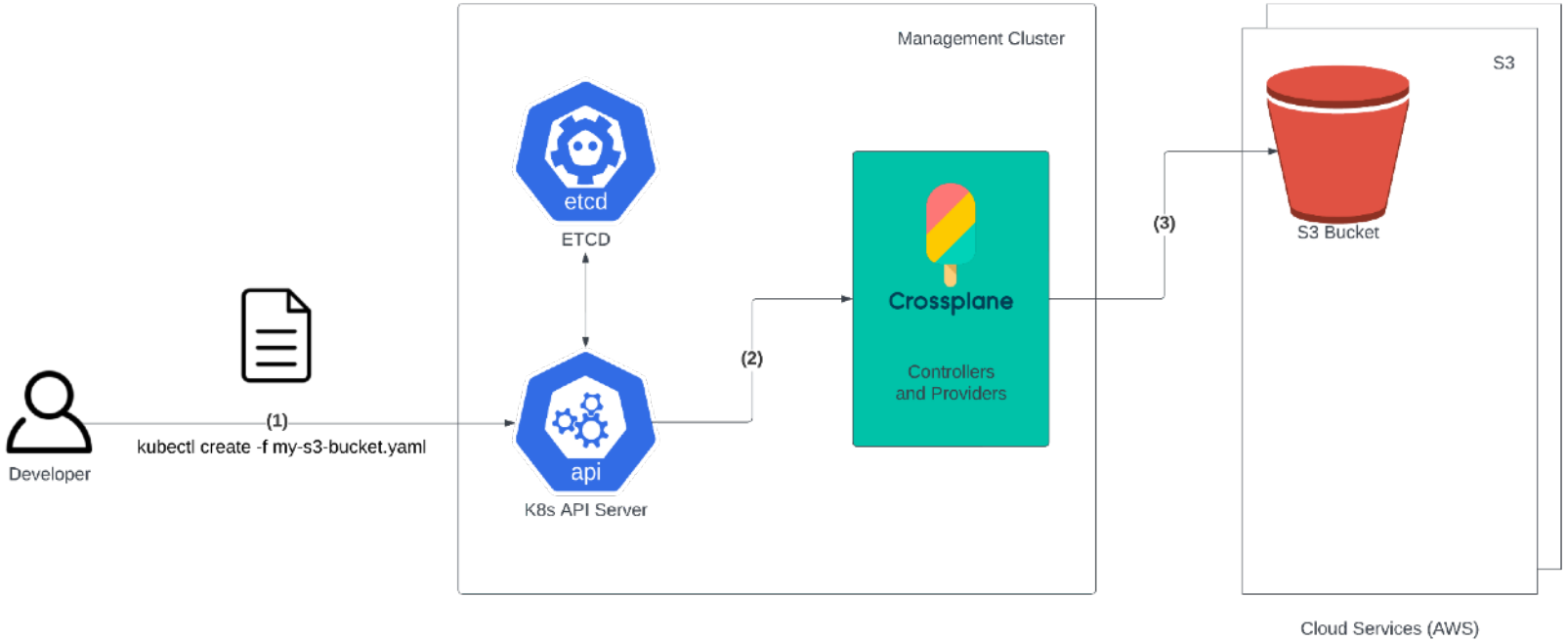
Crossplane: Self-service

- **Compositions** abstract all the infrastructure requirements need to create cloud resources in a self-service model, hiding the infrastructure complexity
- **Example:** When creating a cloud database instance, complexity associated with creating required resources such as virtual private networks, subnets, security groups, can be abstracted.

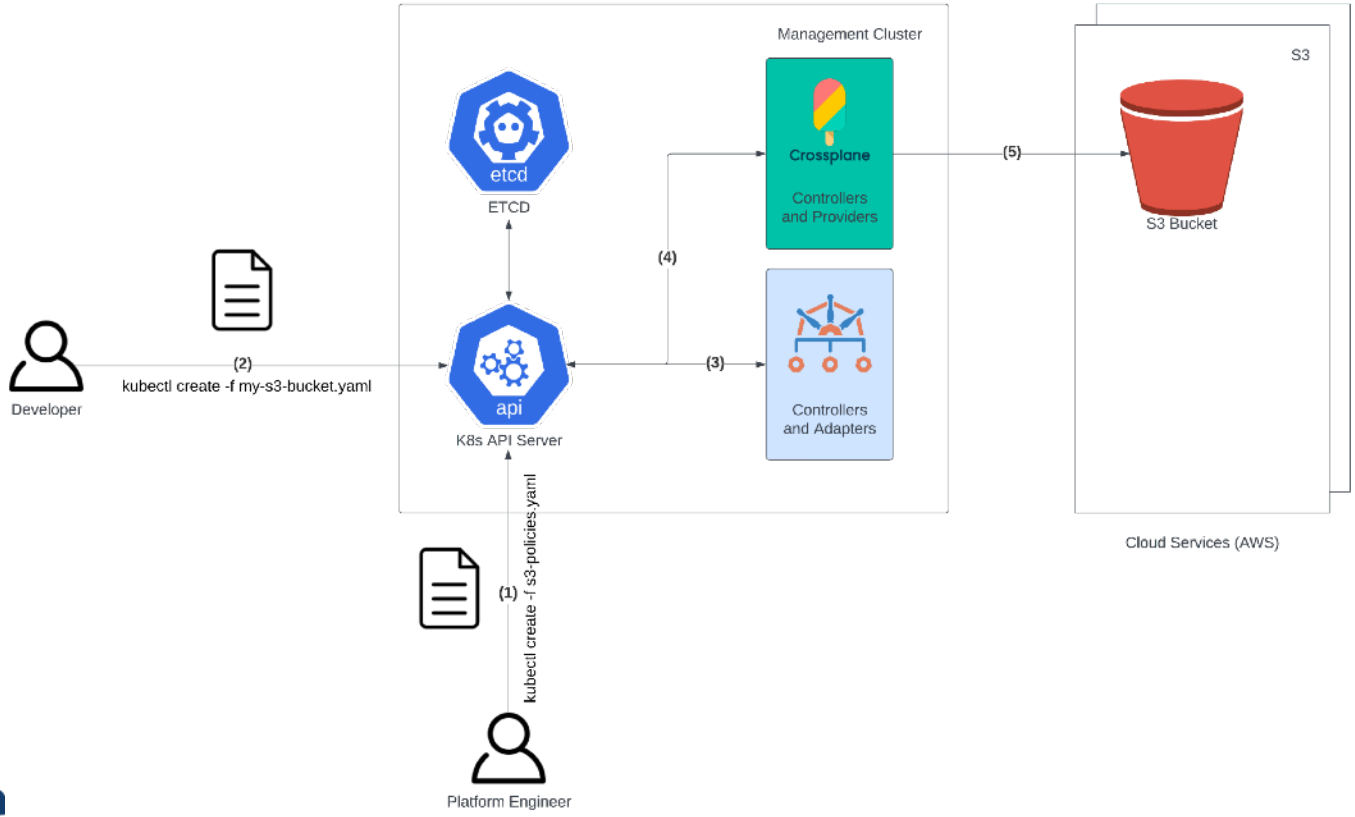


Crossplane Compositions [6]

Crossplane: Self-service



Crossplane + Kyverno



Demo

Summary

- Kubernetes based cloud controllers such as Crossplane can enable developer self-service
- Kubernetes-native policy engines such as Kyverno can provide the necessary policy enforcement
- Proactively enforcing policies prevent misconfigurations, improve security posture and save costs

Join the Community!

Kyverno

- Docs https://kyverno.io
- Policy Library https://kyverno.io/policies
- Playground https://playground.kyverno.io
- Slack https://slack.k8s.io/#kyverno
- Twitter @kyverno

Crossplane

- Docs https://www.crossplane.io
- Slack https://slack.k8s.io/#crossplane
- Twitter @crossplane_io

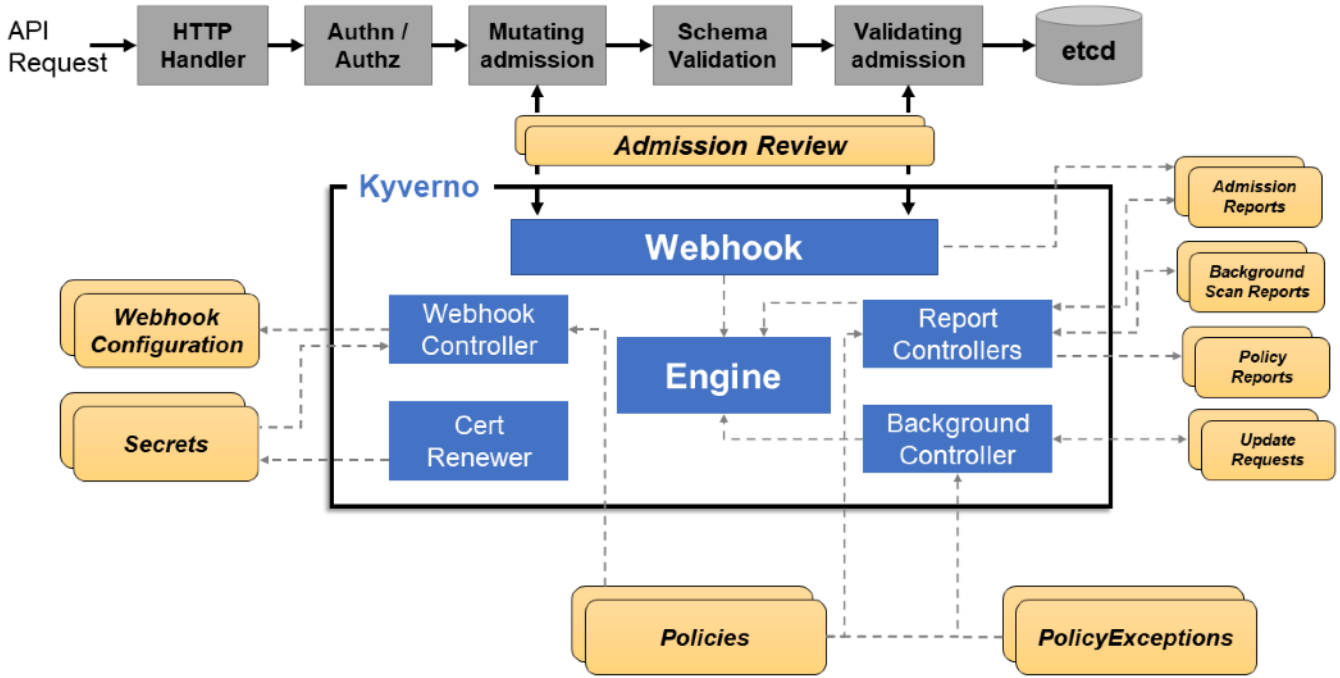
Thank you!

try.nirmata.io

References

1. Kyverno. (2023, January 17). Verify Images. Kyverno. Retrieved May 27, 2023, from https://kyverno.io/docs/writing-policies/verify-images/#verifying-image-signatures
2. Huawei. (2020, February 10). *Kubernetes Cluster Provisioning using Crossplane*. InfraCloud. Retrieved May 28, 2023, from https://www.infracloud.io/blogs/cluster-provisioning-using-crossplane/
3. Start History. (n.d.). *Kyverno Star History*. GitHub Star History. Retrieved May 27, 2023, from https://star-history.com/#kyverno/kyverno&open-policy-agent/gatekeeper&cruise-automation/k-rail&loft-sh/jsPolicy&kubewarden/policy-server&Date
4. Kyverno. (2023, January 17). *Policies and Rules*. Kyverno. Retrieved May 27, 2023, from https://kyverno.io/docs/kyverno-policies/
5. Kubernetes. (2022, September 3). Overview of Cloud Native Security. Kubernetes. Retrieved May 30, 2023, from https://kubernetes.io/docs/concepts/security/overview/
6. Luebken, M. (2021, July 7). Why Crossplane Is so Exciting. The Crossplane Blog. Retrieved May 31, 2023, from https://blog.crossplane.io/why-crossplane-is-so-exciting/
7. Kyverno. (2023, May 12). Introduction. Kyverno. Retrieved June 1, 2023, from https://kyverno.io/docs/introduction/

Appendix



Kyverno Architecture [7]