Kubernetes automation in multi-tenant environments with Kyverno

Chip Zoller

Hello

- Chip Zoller
- Work @ Dell Technologies
- Background as consultant, engineer focused on automation and cloud native apps
- Member of the Kyverno project
- Focus on everything that’s not Golang
- Blog at neonmirrors.net

Multi-tenancy in Kubernetes

- Tenancy: Segregation of workloads by some boundary (customer, business unit, environment)
  - Hard vs Soft
- Hard
  - “Hard” multi-tenancy enabled via separate clusters
  - Strict isolation
  - For hostile workloads (ex., Coke vs Pepsi)
  - Better controls blast radius
- Soft
  - “Soft” multi-tenancy enabled primarily via **namespaces**
  - Relaxed isolation
  - More “friendly” workloads (ex., devA vs devB)

What is Kyverno

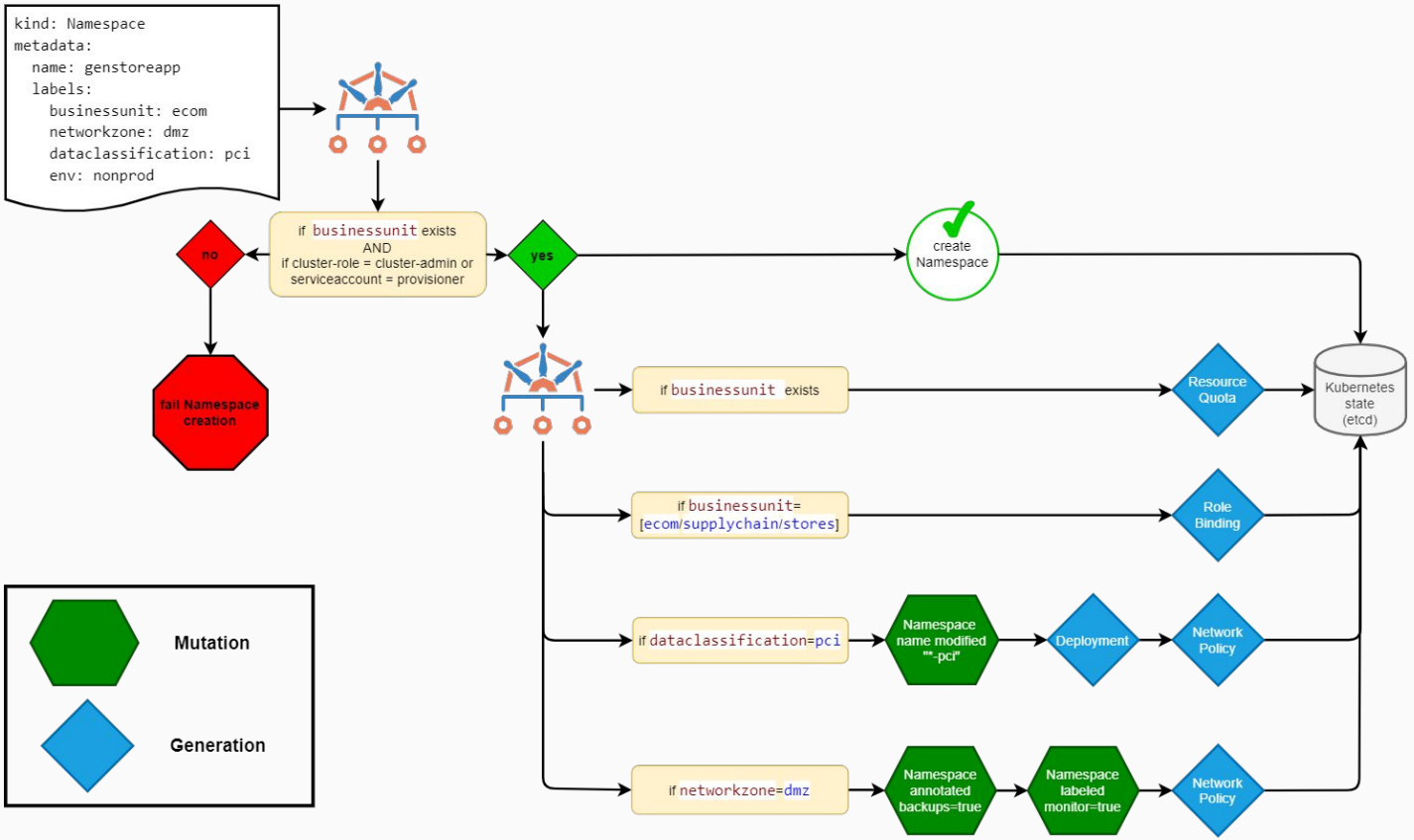
- CNCF policy engine written specifically for Kubernetes
- Policy == security guardrails for your cluster
- Has validation, mutation, and **generation** abilities
- No new language to learn!
- Operates as a webhook controller
- Becomes an automation engine rather than a yes/no doer
- Policy as K8s CRs; scoped to whole cluster or namespace
- PSP deprecation in 1.21 (i.e., now), replace w/ Kyverno

Sample Kyverno Policy

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: require-labels
spec:
  validationFailureAction: enforce
  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: "?*"
```

Demo

Demo Workflow



Wrapping Up

- More on Kyverno
  - Kyverno.io
  - Extensive sample policy library (50+) at https://kyverno.io/policies/
  - Community on Kubernetes Slack at #kyverno
- Blog resources
  - https://neonmirrors.net/post/2020-11/exploring-kyverno-intro/
  - https://neonmirrors.net/post/2021-01/kyverno-the-swiss-army-knife-of-kubernetes/
  - https://neonmirrors.net/post/2021-02/kubernetes-policy-comparison-opa-gatekeeper-vs-kyverno/

Questions?

Thank you!

Chip Zoller
@chipzoller
neonmirrors.net