Hewlett Packard
Enterprise

Cray Systems Management (CSM) Security Policy Engine

Srinivasa Rao (Vasu) Yarlagadda and Jeremy Duckworth

May 2023

Background

Introduction to Kyverno

Integration into CSM

DevSecOps Policy Shaping

Future Work

Implement Container Image Signature Validation

Replace PSPs

Background

Introduction to Kyverno

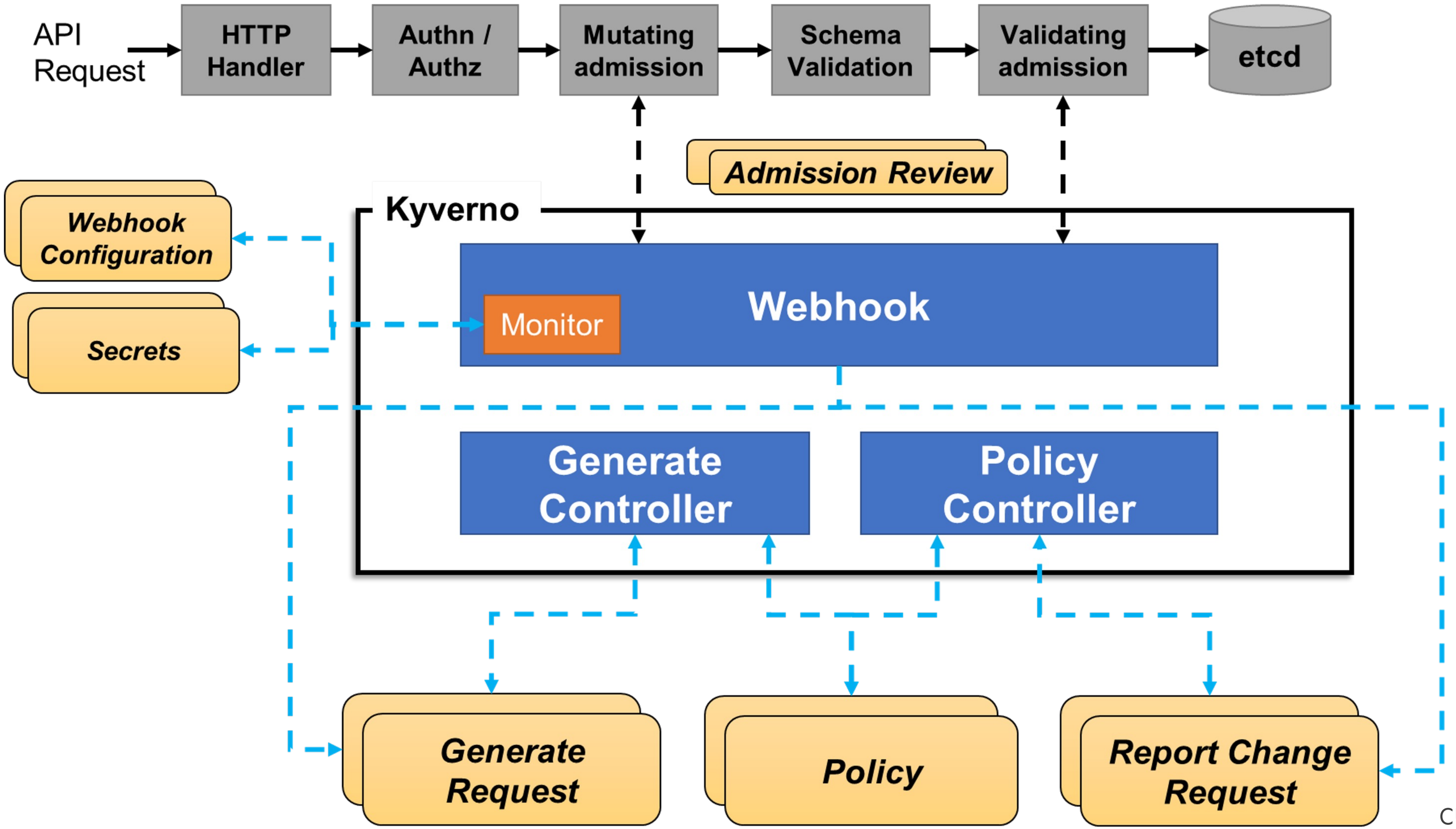
What is Kyverno?

Overview

- Kyverno is a Kubernetes-native policy engine.
- Kyverno uses the Kubernetes admission webhook to validate, mutate, and generate Kubernetes resources, and verify images.
- A CLI is available to test and validate policy behavior against resources prior to adding them into a cluster.
- Using Kyverno, a central platform team can define policies and ensure the configurations are compliant with their security and best practices standards.
- Kyverno does not require learning a new programming language to define policies – it uses declarative manifests like Kubernetes.

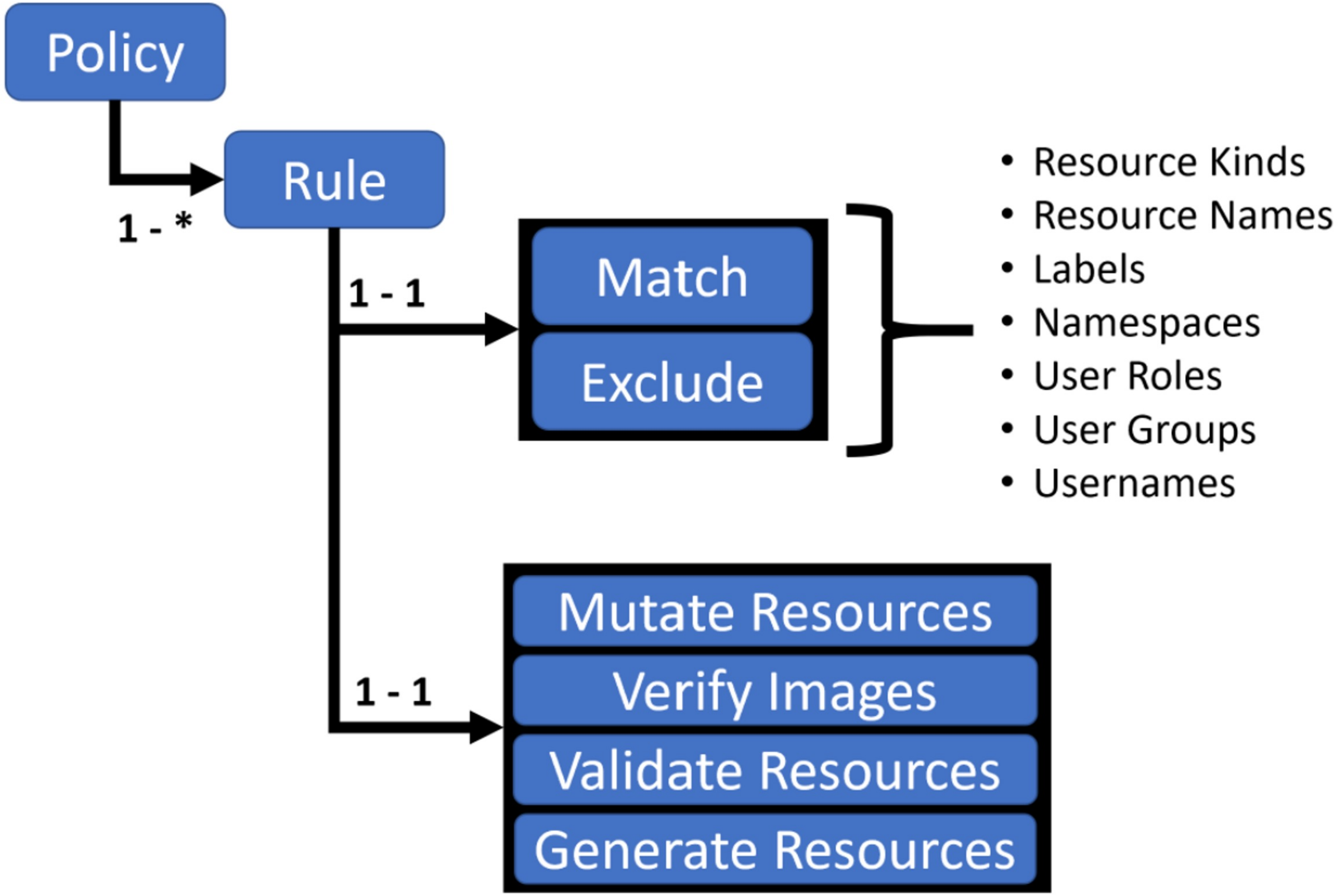
What is Kyverno?

Architecture



What is Kyverno?

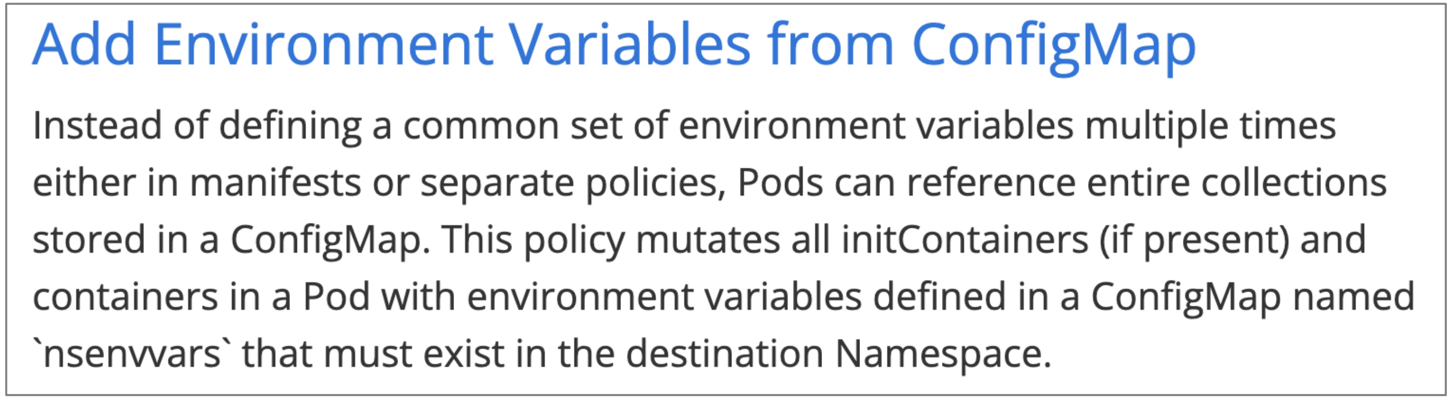
Policy Grammar



What is Kyverno?

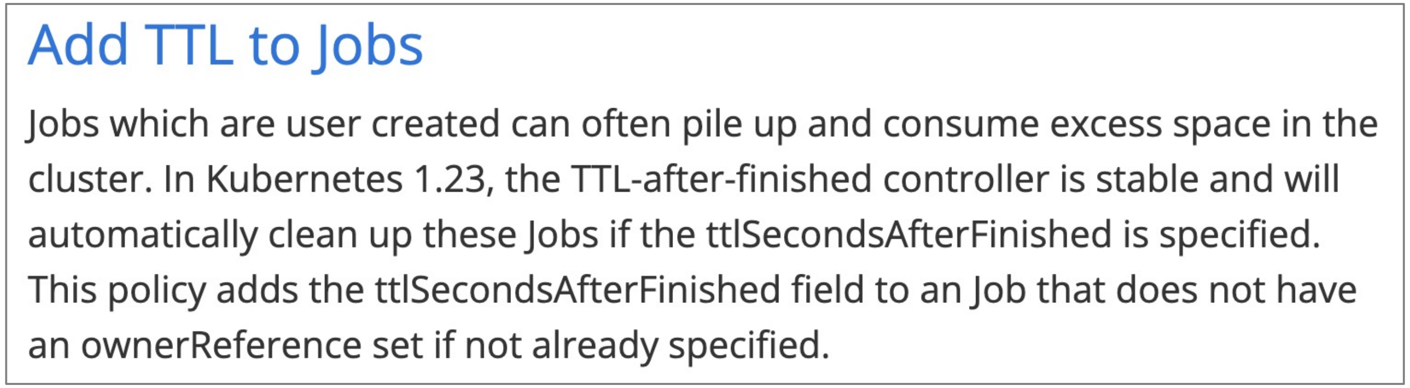
Use Cases Transcend Security

- Kyverno Policy Library: https://kyverno.io/policies/



Add Environment Variables from ConfigMap

Instead of defining a common set of environment variables multiple times either in manifests or separate policies, Pods can reference entire collections stored in a ConfigMap. This policy mutates all initContainers (if present) and containers in a Pod with environment variables defined in a ConfigMap named `nsenvvars` that must exist in the destination Namespace.



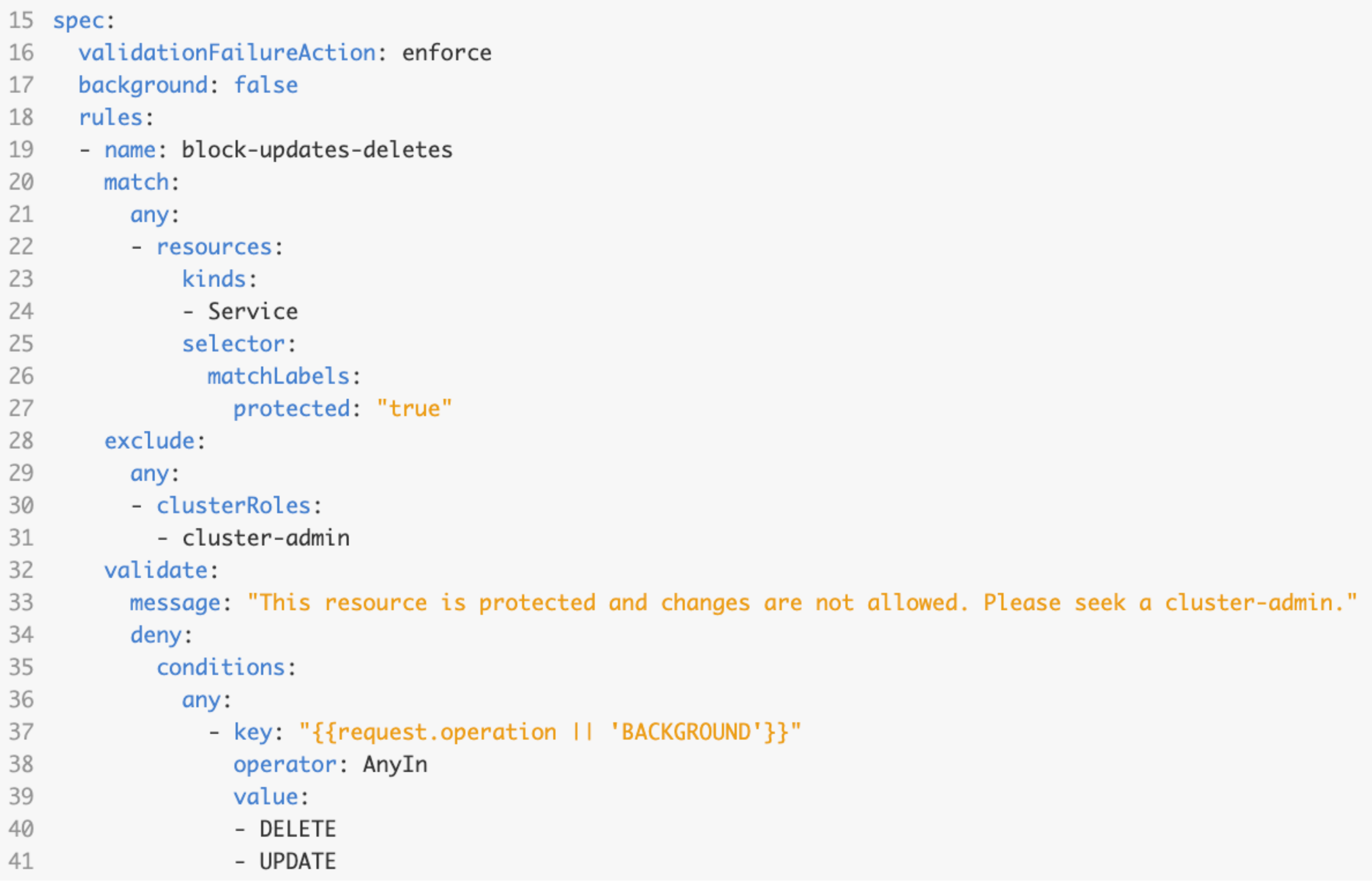
Add TTL to Jobs

Jobs which are user created can often pile up and consume excess space in the cluster. In Kubernetes 1.23, the TTL-after-finished controller is stable and will automatically clean up these Jobs if the ttlSecondsAfterFinished is specified. This policy adds the ttlSecondsAfterFinished field to an Job that does not have an ownerReference set if not already specified.

What is Kyverno?

Sample Validation Policy (1)

https://kyverno.io/policies/other/block_updates_deletes/block_updates_deletes/

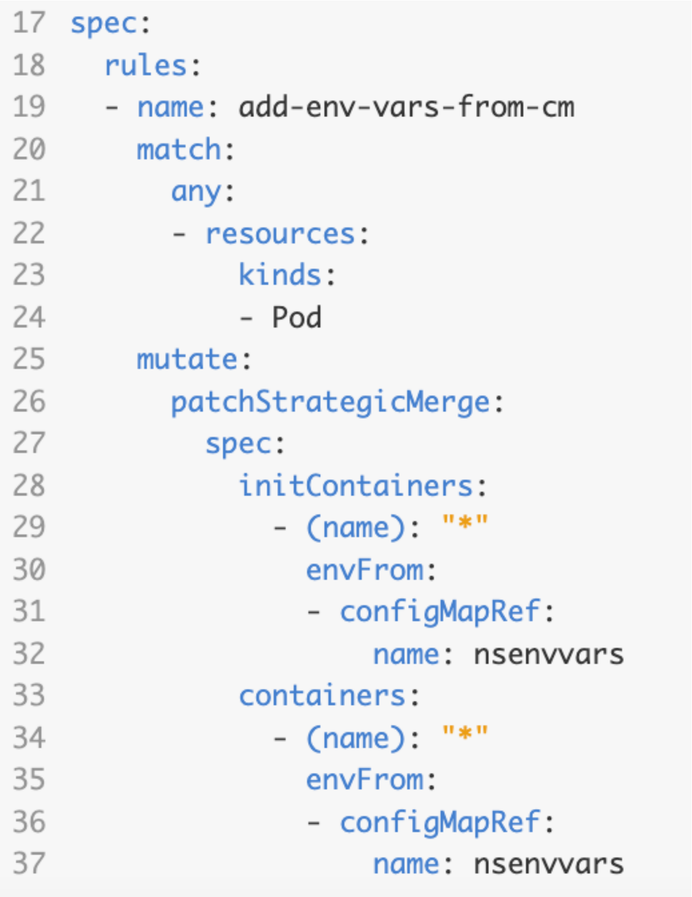


```yaml
spec:
  validationFailureAction: enforce
  background: false
  rules:
  - name: block-updates-deletes
    match:
      any:
      - resources:
          kinds:
          - Service
          selector:
            matchLabels:
              protected: "true"
    exclude:
      any:
      - clusterRoles:
        - cluster-admin
    validate:
      message: "This resource is protected and changes are not allowed. Please seek a cluster-admin."
      deny:
        conditions:
          any:
            - key: "{{request.operation || 'BACKGROUND'}}"
              operator: AnyIn
              value:
              - DELETE
              - UPDATE
```

What is Kyverno?

Sample Mutate Policy

https://kyverno.io/policies/other/add_env_vars_from_cm/add-env-vars-from-cm/

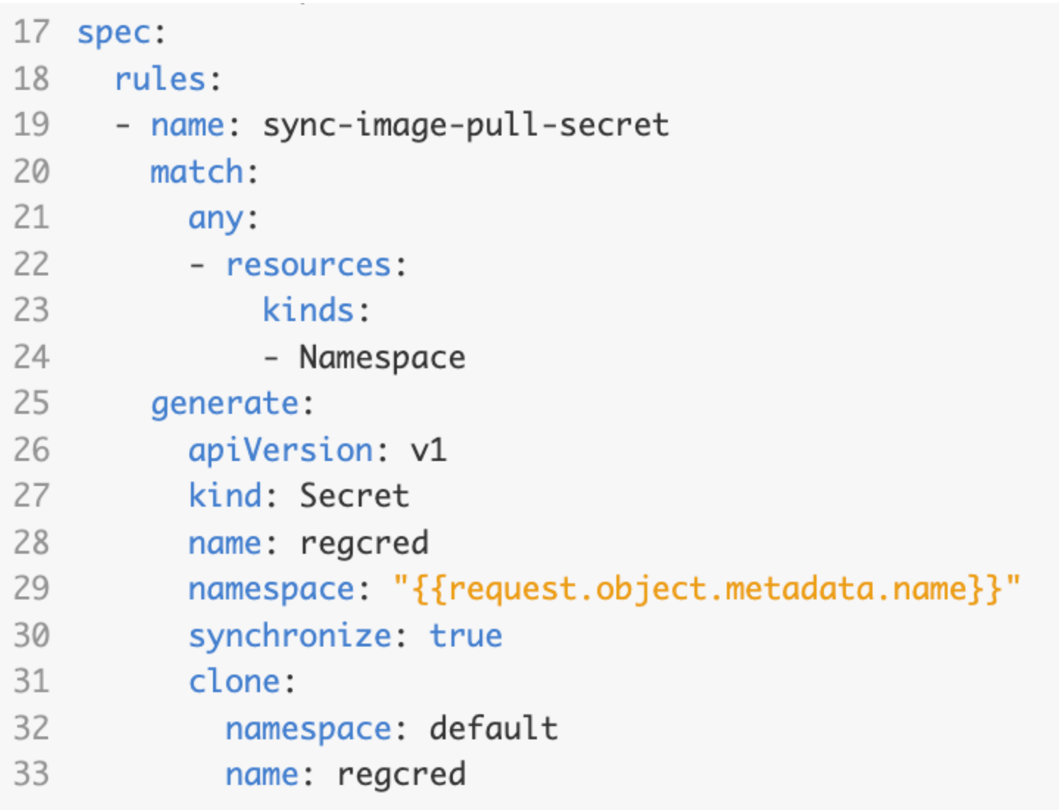


```yaml
spec:
  rules:
  - name: add-env-vars-from-cm
    match:
      any:
      - resources:
          kinds:
          - Pod
    mutate:
      patchStrategicMerge:
        spec:
          initContainers:
            - (name): "*"
              envFrom:
              - configMapRef:
                  name: nsenvvars
          containers:
            - (name): "*"
              envFrom:
              - configMapRef:
                  name: nsenvvars
```

What is Kyverno?

Sample Generate Policy

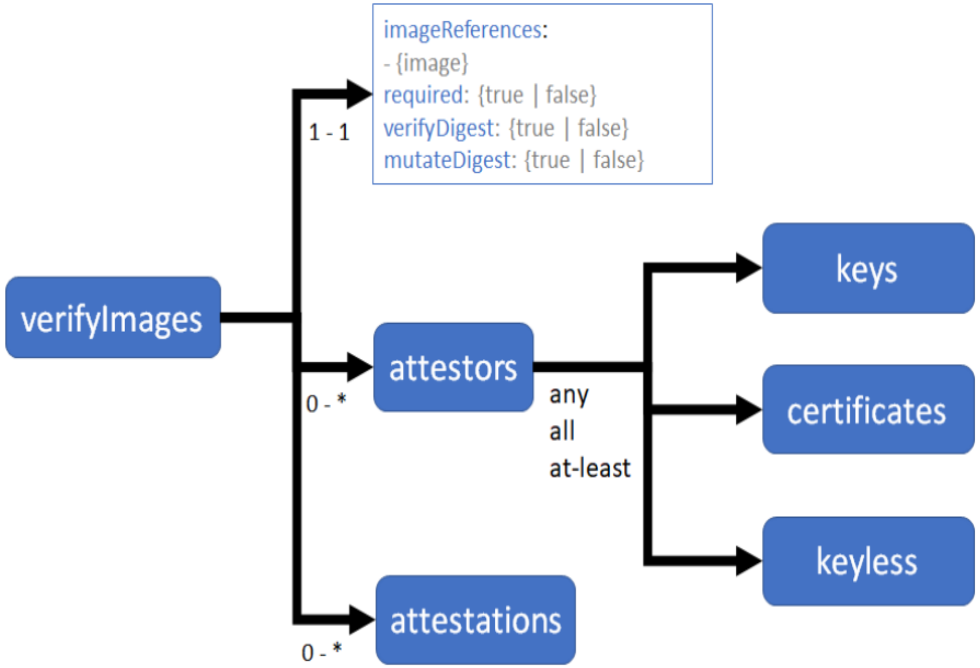
https://kyverno.io/policies/other/sync_secrets/sync_secrets/



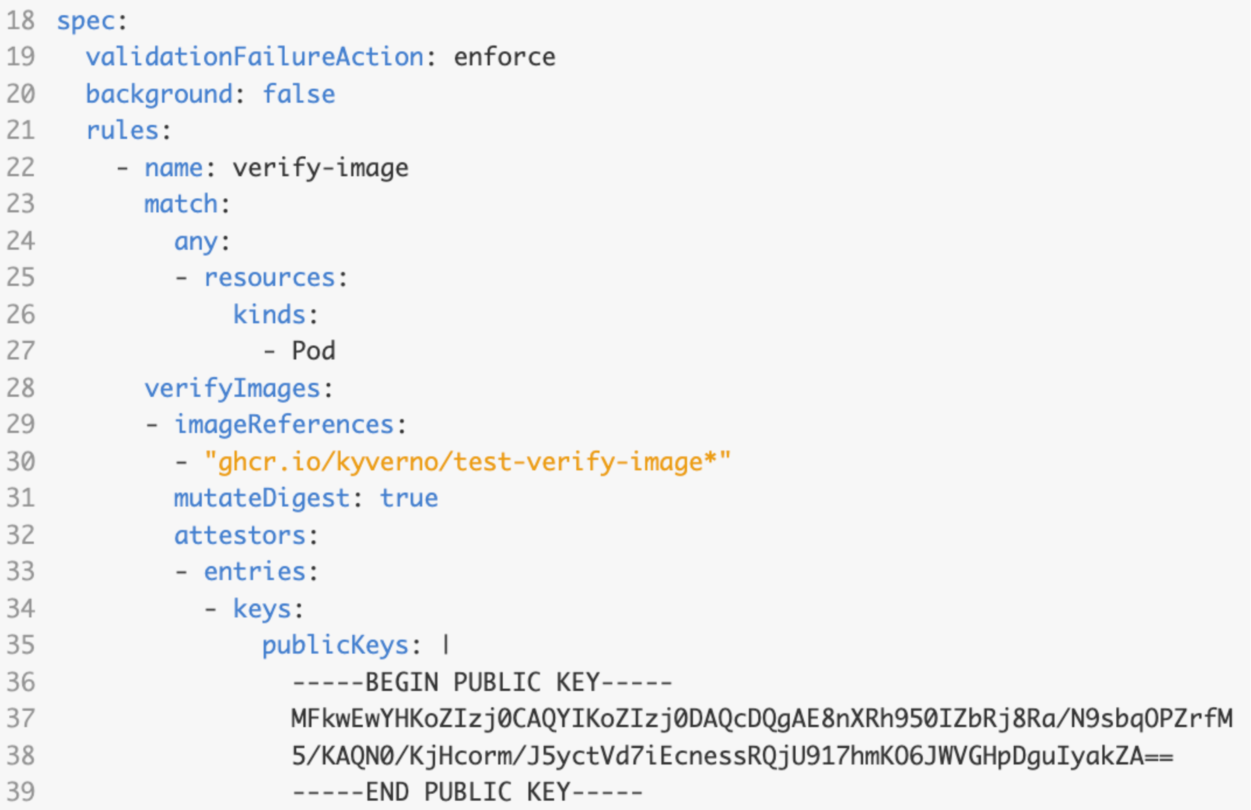
```yaml
spec:
  rules:
  - name: sync-image-pull-secret
    match:
      any:
      - resources:
          kinds:
          - Namespace
    generate:
      apiVersion: v1
      kind: Secret
      name: regcred
      namespace: "{{request.object.metadata.name}}"
      synchronize: true
      clone:
        namespace: default
        name: regcred
```

What is Kyverno?

Sample VerifyImages Policy



https://kyverno.io/policies/other/verify_image/



```
spec:
  validationFailureAction: enforce
  background: false
  rules:
    - name: verify-image
      match:
        any:
        - resources:
            kinds:
              - Pod
      verifyImages:
      - imageReferences:
        - "ghcr.io/kyverno/test-verify-image*"
        mutateDigest: true
        attestors:
        - entries:
          - keys:
              publicKeys: |
                -----BEGIN PUBLIC KEY-----
                MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE8nXRh950IZbRj8Ra/N9sbqOPZrfM
                5/KAQN0/KjHcorm/J5yctVd7iEcnessRQjU917hmKO6JWVGHpDguIyakZA==
                -----END PUBLIC KEY-----
```

Integration into CSM

DevSecOps Policy Shaping

Integration into CSM

Feature by Version

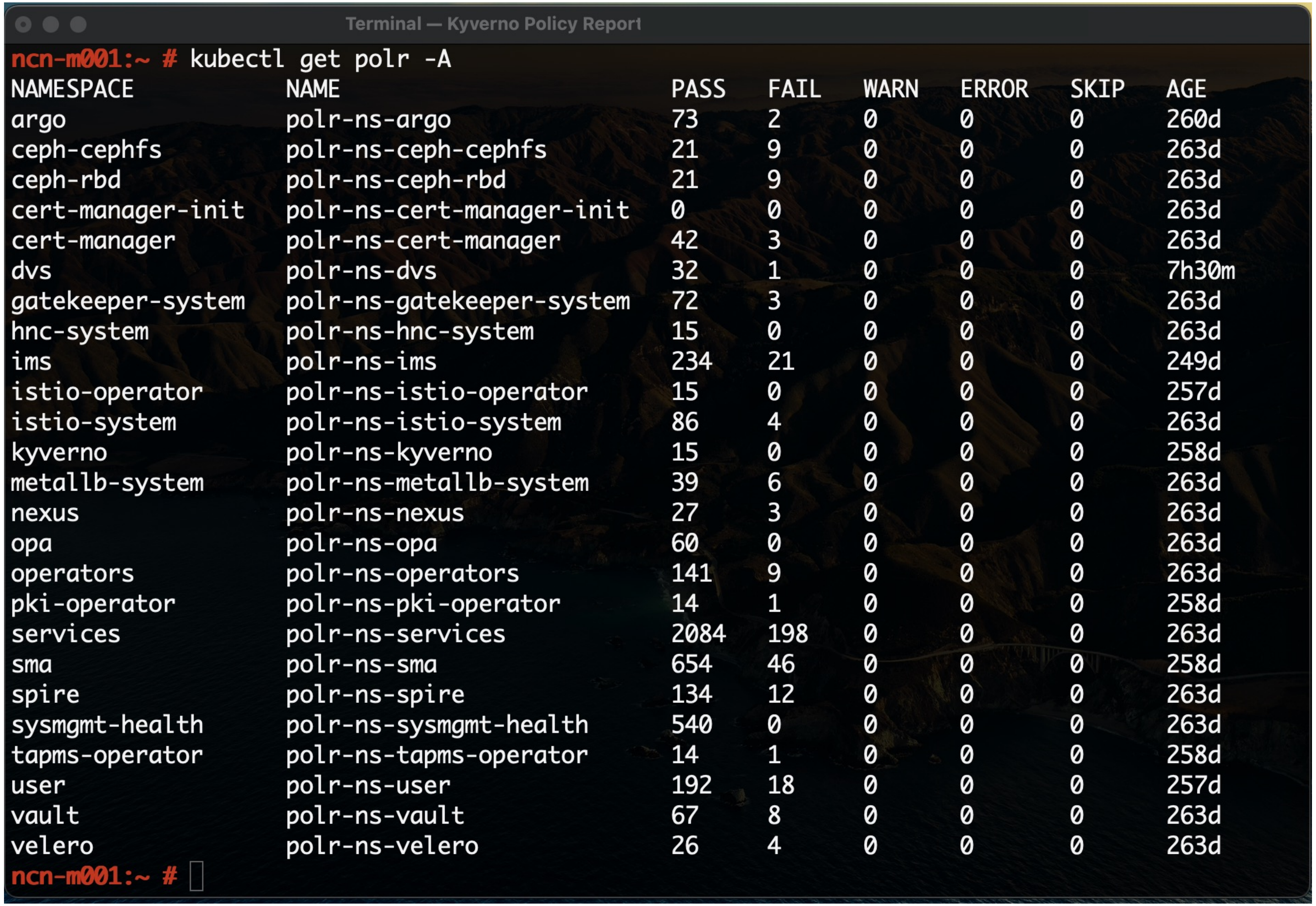
- Kyverno was added to CSM Distribution in 1.3, along with set of custom mutation policies to harden CSM micro-services that were exposed to network ingress.

- In CSM 1.4, OPA Gatekeeper is removed from the CSM Distribution to consolidate policy engine use, using Kyverno. Upstream Kyverno polices for auditing Kubernetes Pod Security Policies (PSS) were also introduced as the first step towards replacing PSPs, and also established a refreshed observability baseline for NIST 800-190 alignement.

- Prometheus and Grafana integration for Kyverno observability was also introduced in CSM 1.4, along with an operational mutation policy to shape job TTLs to alleviate storage pressure on Kubernetes nodes.

Integration into CSM

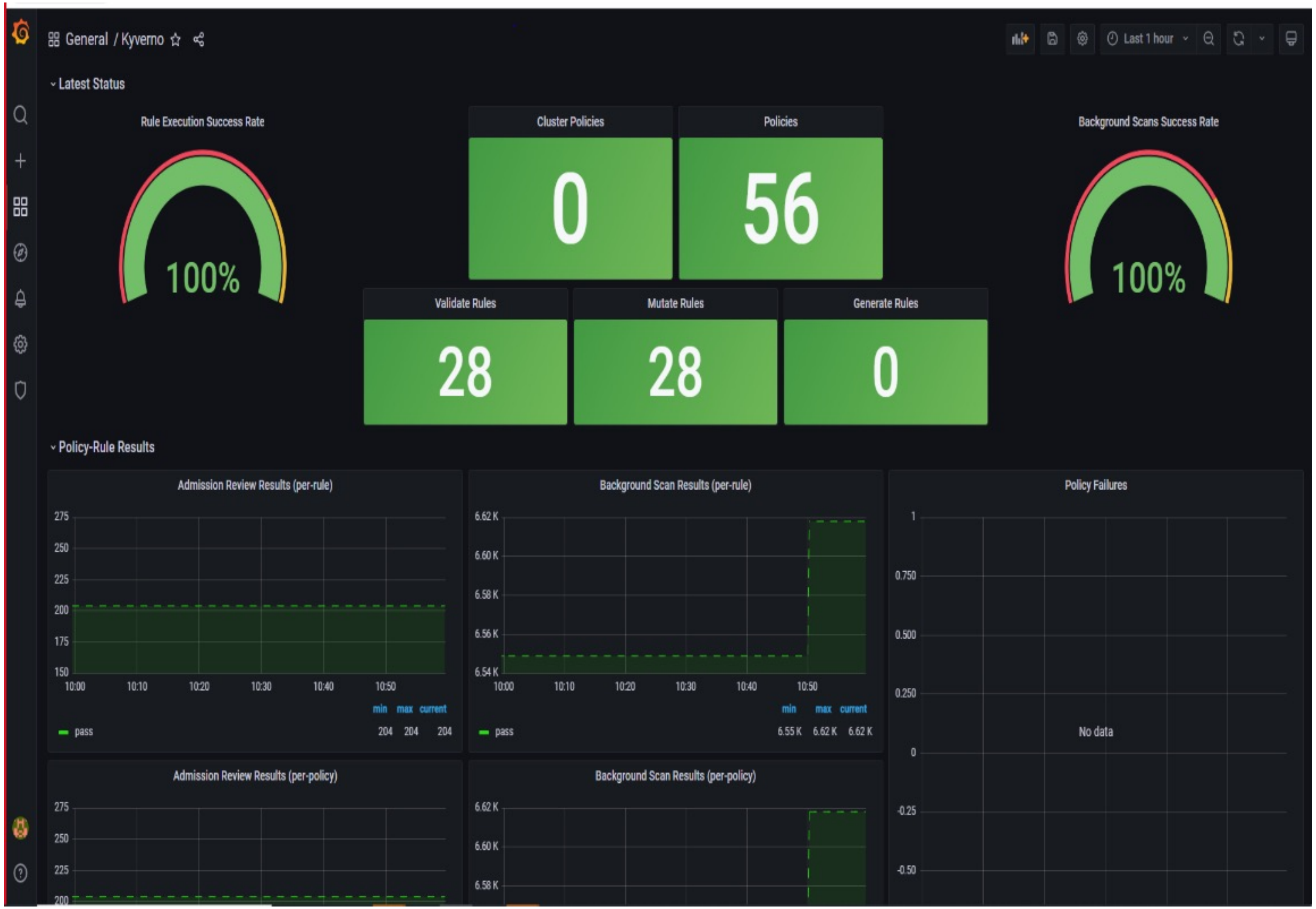
Policy Reporting



```
ncn-m001:~ # kubectl get polr -A
NAMESPACE           NAME                        PASS   FAIL   WARN   ERROR   SKIP   AGE
argo                polr-ns-argo                73     2      0      0       0      260d
ceph-cephfs         polr-ns-ceph-cephfs         21     9      0      0       0      263d
ceph-rbd            polr-ns-ceph-rbd            21     9      0      0       0      263d
cert-manager-init   polr-ns-cert-manager-init   0      0      0      0       0      263d
cert-manager        polr-ns-cert-manager        42     3      0      0       0      263d
dvs                 polr-ns-dvs                 32     1      0      0       0      7h30m
gatekeeper-system   polr-ns-gatekeeper-system   72     3      0      0       0      263d
hnc-system          polr-ns-hnc-system          15     0      0      0       0      263d
ims                 polr-ns-ims                 234    21     0      0       0      249d
istio-operator      polr-ns-istio-operator      15     0      0      0       0      257d
istio-system        polr-ns-istio-system        86     4      0      0       0      263d
kyverno             polr-ns-kyverno             15     0      0      0       0      258d
metallb-system      polr-ns-metallb-system      39     6      0      0       0      263d
nexus               polr-ns-nexus               27     3      0      0       0      263d
opa                 polr-ns-opa                 60     0      0      0       0      263d
operators           polr-ns-operators           141    9      0      0       0      263d
pki-operator        polr-ns-pki-operator        14     1      0      0       0      258d
services            polr-ns-services            2084   198    0      0       0      263d
sma                 polr-ns-sma                 654    46     0      0       0      258d
spire               polr-ns-spire               134    12     0      0       0      263d
sysmgmt-health      polr-ns-sysmgmt-health      540    0      0      0       0      263d
tapms-operator      polr-ns-tapms-operator      14     1      0      0       0      258d
user                polr-ns-user                192    18     0      0       0      257d
vault               polr-ns-vault               67     8      0      0       0      263d
velero              polr-ns-velero              26     4      0      0       0      263d
ncn-m001:~ #
```

Integration into CSM

Prometheus and Grafana Integration



Future Work

Implement container image signature validation; Replace PSPs

Future Work

Focused Initiatives

- To improve supply chain security, distribute signatures as OCI artifacts (to Nexus), and enable signature validation in Kyverno. Policy must be flexible to allow customers to run their own containers (e.g., add keys, exclude certain resources from the policy, etc)
- Replace PSPs with PSSs implemented as Kyverno Policy
- Establish an improved governance and observability model for developer alignment with NIST 800-190 and related security baseline guidance

Questions?