Kyverno en K8S

+

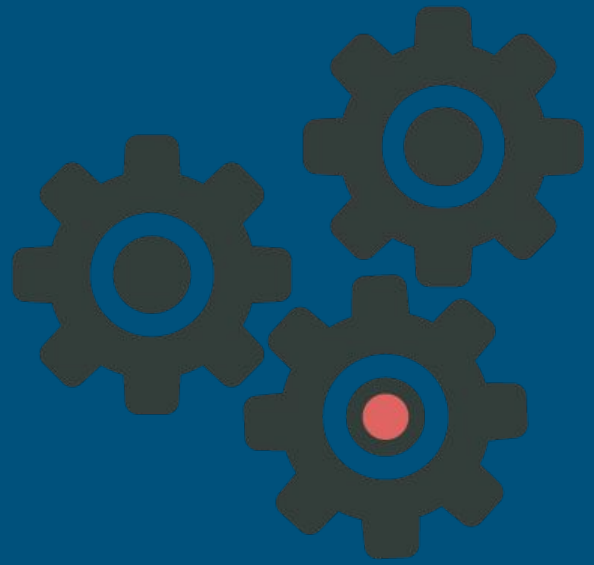
ÍNDICE

¿ Qué es Kyverno ?

¿ Qué es Kyverno ?

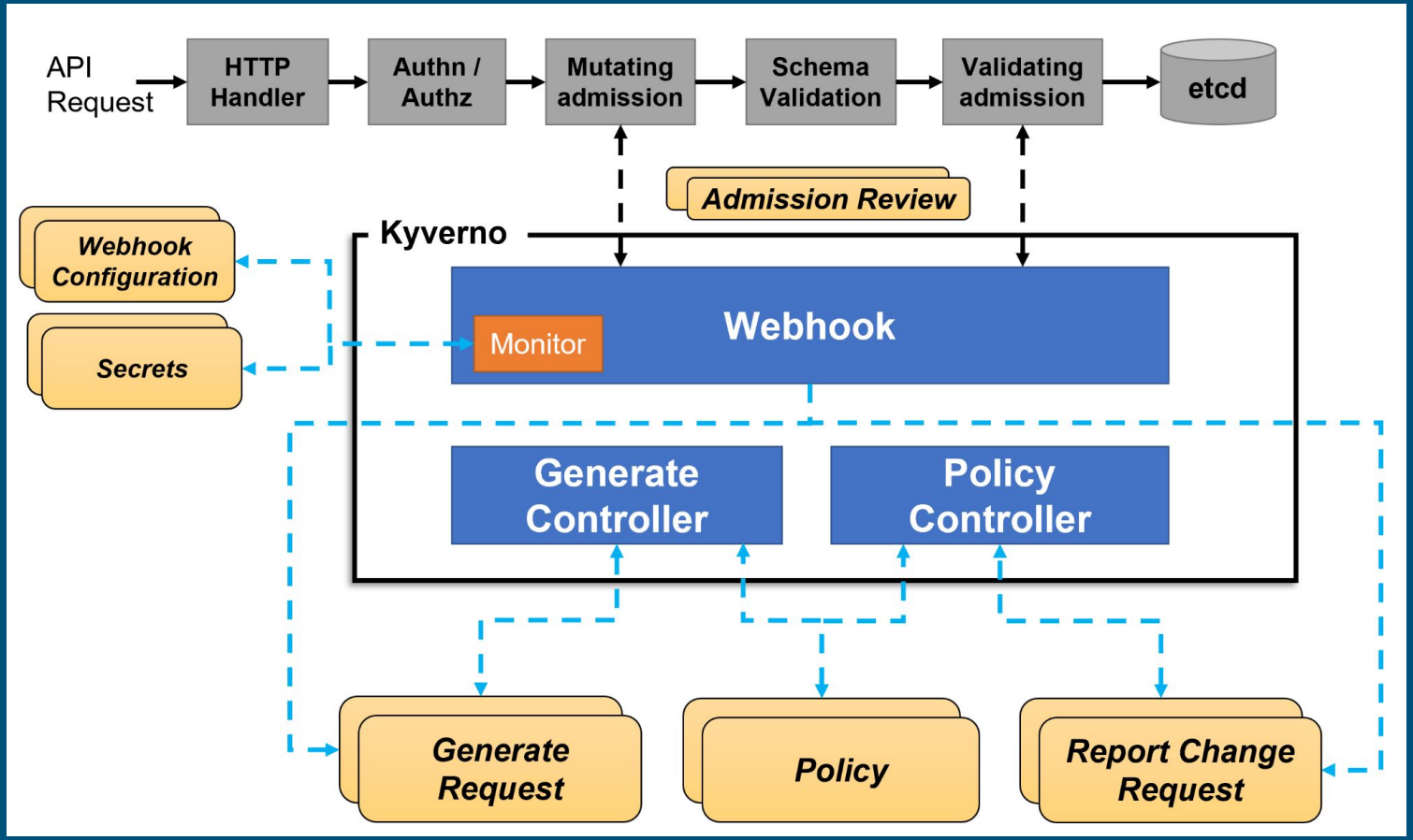
Kyverno es un motor de políticas diseñado para Kubernetes. Las políticas pueden validar, mutar o generar recursos de Kubernetes y se escriben en lenguaje YAML. Se puede utilizar Kyverno CLI para testear políticas o validar recursos como parte de un Pipeline de un CI/CD.

Funcionamiento de Kyverno



Funcionamiento de Kyverno

Kyverno recibe las respuestas HTTP del webhook configurado (validación,mutación o generación) desde la API de Kubernetes y si la respuesta coincide con alguna política, automáticamente se aplica la política y se procede a admitir o rechazar la petición de Kubernetes.


API Request
HTTP Handler
Authn / Authz
Mutating admission
Schema Validation
Validating admission
etcd
Admission Review
Kyverno
Webhook Configuration
Secrets
Monitor
Webhook
Generate Controller
Policy Controller
Generate Request
Policy
Report Change Request

Políticas y Reglas

Validación

Las reglas de validación son probablemente los tipos de reglas más comunes y prácticos con los que se trabaja, y el principal tipo de uso para los controladores de admisión como Kyverno. En una regla de validación, se definen las propiedades obligatorias con las que debe crearse un recurso.

Cuando un usuario o proceso crea un recurso, Kyverno comprueba las propiedades del recurso con la regla de validación. Si esas propiedades se validan, es decir, si hay coinciden y se realiza el acuerdo entre Kyverno y la petición, se permite la creación del recurso. Si esas propiedades son diferentes, la creación se bloquea.

Ejemplo regla validación ✓

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: requiere-ns-etiqueta-dept
spec:
  validationFailureAction: enforce
  rules:
  - name: requiere-ns-etiqueta-dept
    match:
      any:
      - resources:
          kinds:
          - Namespace
    validate:
      message: "Necesitas la etiqueta `departamento` con el valor `produccion` en los nuevos namespaces
que vayas a crear."
      pattern:
        metadata:
          labels:
              departamento: produccion
```

Mutación

Una regla de mutación puede utilizarse para modificar los recursos que coincidan con la regla y se utiliza cuando un objeto necesita ser modificado de una manera determinada.

La mutación de recursos se produce antes de la validación, por lo que las reglas de validación no deben contradecir los cambios realizados por las reglas de mutación.

Ejemplo regla mutación

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: cambiar-image-pull-policy
spec:
  rules:
    - name: cambiar-image-pull-policy
      match:
        any:
        - resources:
            kinds:
            - Pod
      mutate:
        patchStrategicMerge:
          spec:
            containers:
              # Busca coincidencias de recursos que utilicen una imagen con etiqueta latest
              - (image): "*:latest"
                # Establece el valor del parámetro imagePullPolicy a "IfNotPresent"
                imagePullPolicy: "IfNotPresent"
```

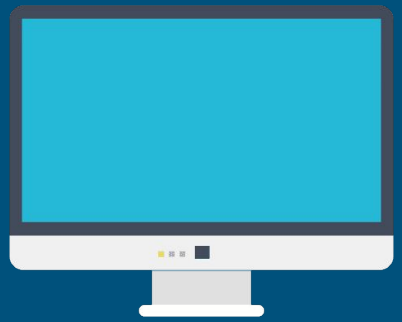
Generación

Las reglas de generación se utilizan para crear un recurso o recursos adicionales cuando se crea un recurso o se modifica se definición (por ejemplo modificar el fichero de definición .yaml de recurso).

Por lo tanto, el trigger desencadenante del uso de la política consiste en la generación de recursos, es decir, cuando se genere un recurso y coincida con la política, la aplicará.

```yaml
apiVersion: kyverno.io/v1
kind: ClusterPolicy
metadata:
  name: quota-ns
spec:
  rules:
  - name: generar-resourcequota
    match:
      resources:
        kinds:
        - Namespace
    generate:
      kind: ResourceQuota
      name: resourcequota-default
      synchronize: true
      namespace: "{{request.object.metadata.name}}"
      data:
        spec:
          hard:
            requests.cpu: '4'
            requests.memory: '16Gi'
            limits.cpu: '4'
            limits.memory: '16Gi'
  - name: generar-limitrange
    match:
      resources:
        kinds:
        - Namespace
    generate:
      kind: LimitRange
      name: limitrange-default
      synchronize: true
      namespace: "{{request.object.metadata.name}}"
      data:
        spec:
          limits:
          - default:
              cpu: 500m
              memory: 1Gi
            defaultRequest:
              cpu: 200m
              memory: 256Mi
            type: Container
```

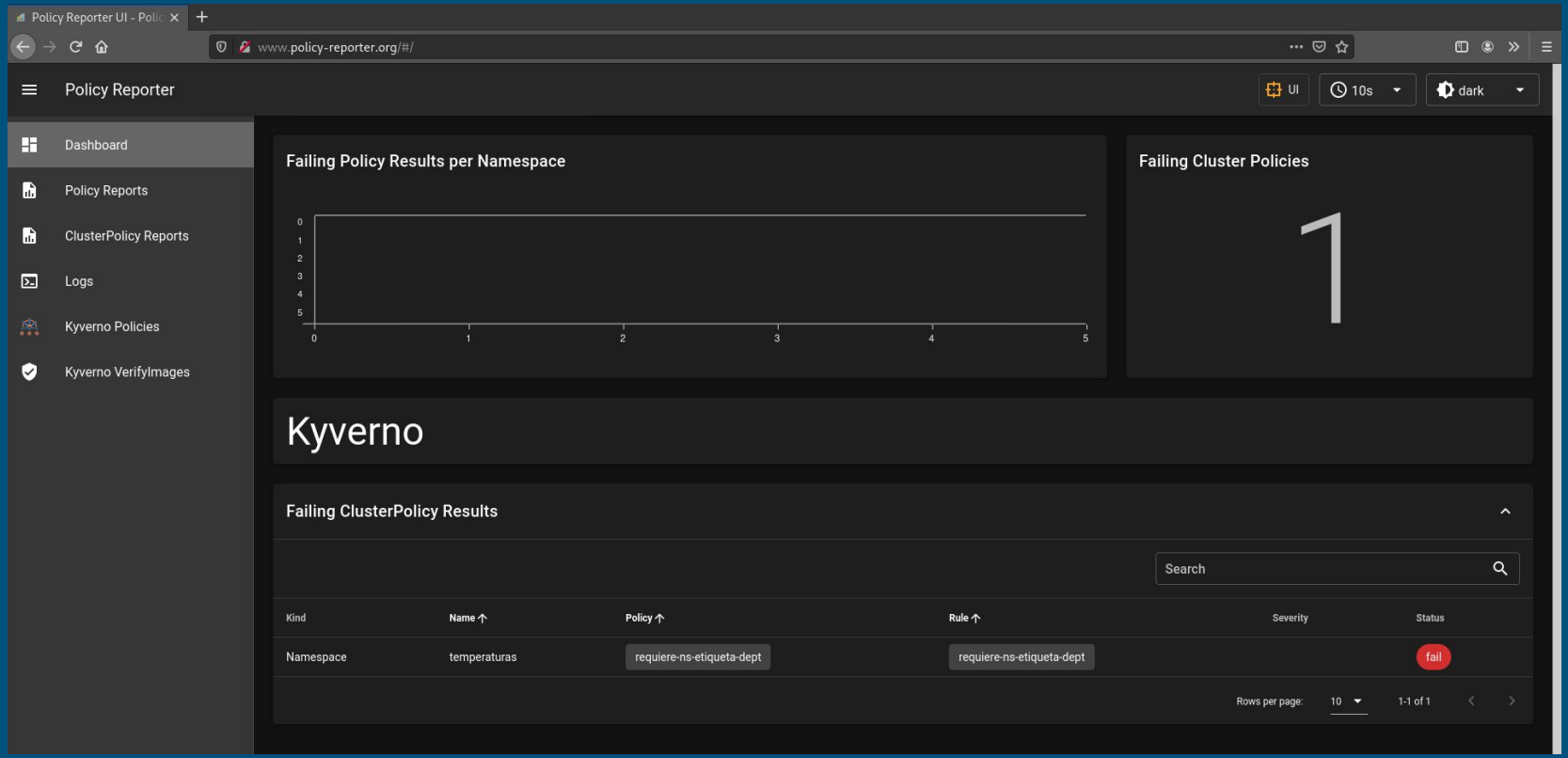
Policy Reporter UI



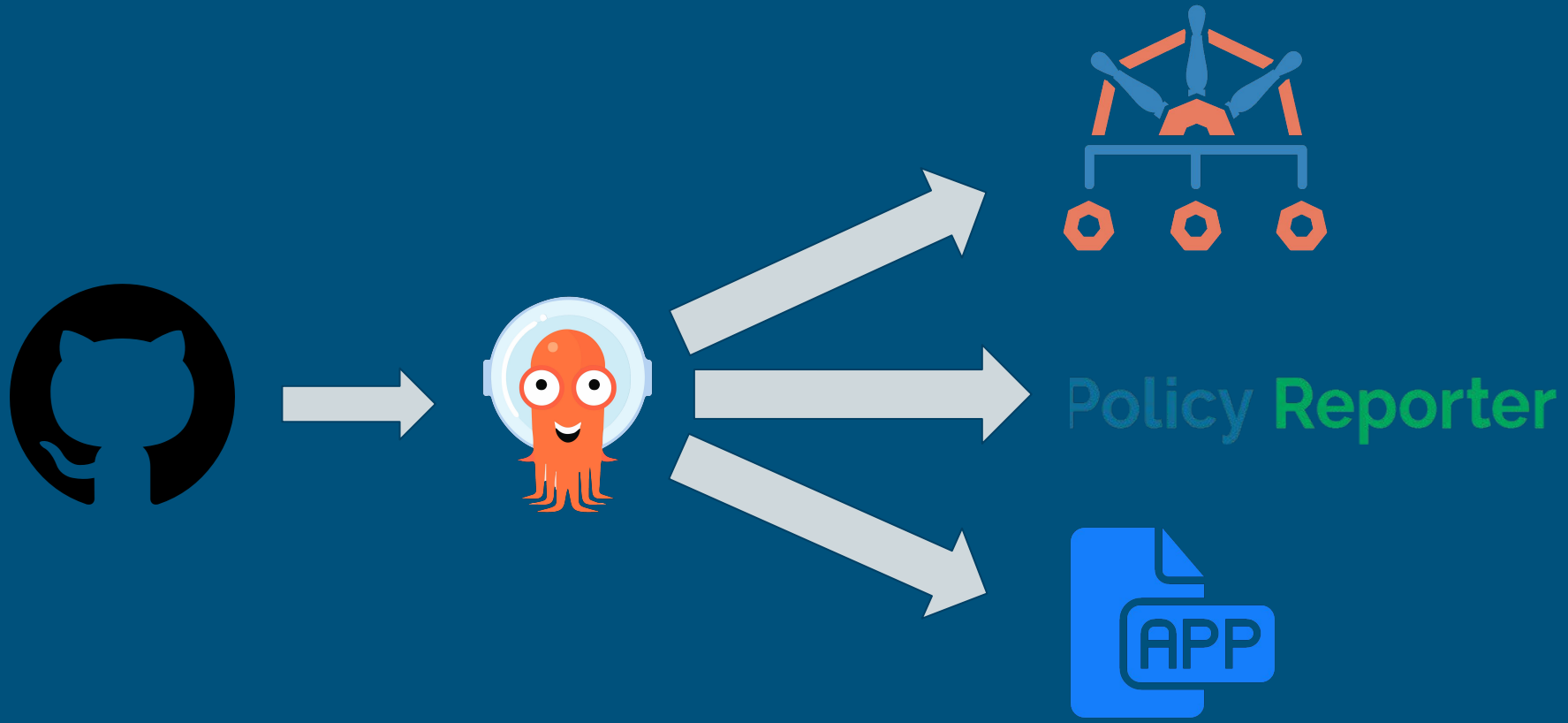
¿ Qué es Policy Reporter UI ?

Policy Reporter UI es una herramienta gráfica que nos permite ver de una forma más visual y atractiva las reglas de validación de Kyverno.

Con Policy Reporter UI podemos observar qué recursos de nuestro cluster cumplen la reglas que tenemos definidas y qué recursos no las cumplen, de tal manera que podremos detectar errores más rápidamente. En principio, Policy Reporter funciona sin necesidad de tener Kyverno instalado ya que mira los PolicyReports de los ClusterPolicies de K8S.


Policy Reporter UI - Polic
www.policy-reporter.org/#/
Policy Reporter
UI
10s
dark
Dashboard
Policy Reports
ClusterPolicy Reports
Logs
Kyverno Policies
Kyverno VerifyImages
Failing Policy Results per Namespace
0
1
2
3
4
5
Failing Cluster Policies
1
Kyverno
Failing ClusterPolicy Results
Search
Kind
Name
Policy
Rule
Severity
Status
Namespace
temperaturas
requiere-ns-etiqueta-dept
requiere-ns-etiqueta-dept
fail
Rows per page:
10
1-1 of 1

Escenario Final


Policy Reporter
APP