8 Kubernetes 보안 강화 방법

06 OPA Gatekeeper 소개 및 설치

소개 및 실습 내용

순서

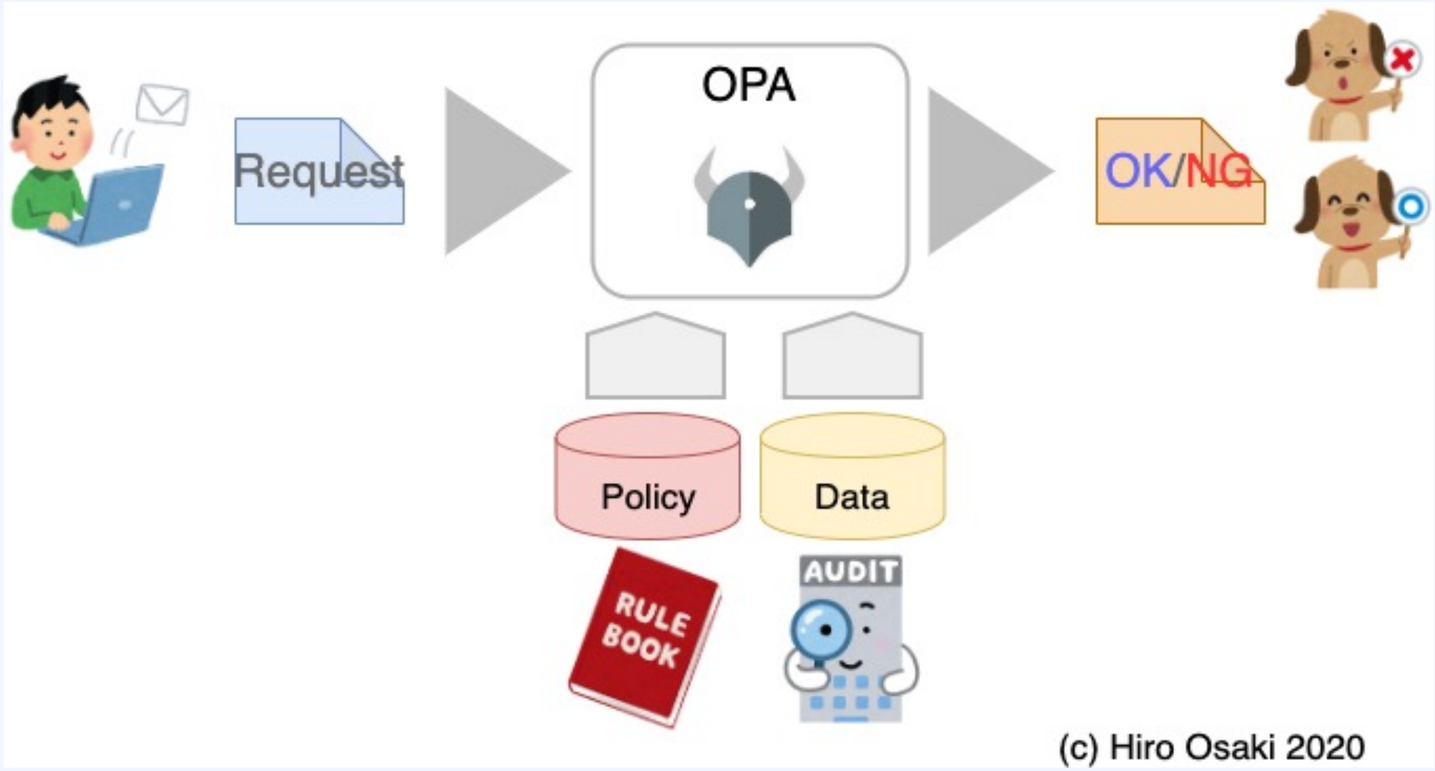
1. OPA 소개
2. OPA Gatekeeper 소개
3. OPA Gatekeeper 설치 (Helm Chart)

실습 예제코드 경로

Chapter08 > Ch08_06-opa-gatekeeper

1. OPA 소개 #1

OPA(Open Policy Agent)는 Kubernetes Object 요청시 주어진 정책을 준수하도록 하는 정책 엔진으로, 정책에 따라 Object의 특정 Action을 허용하거나 거부할 수 있음



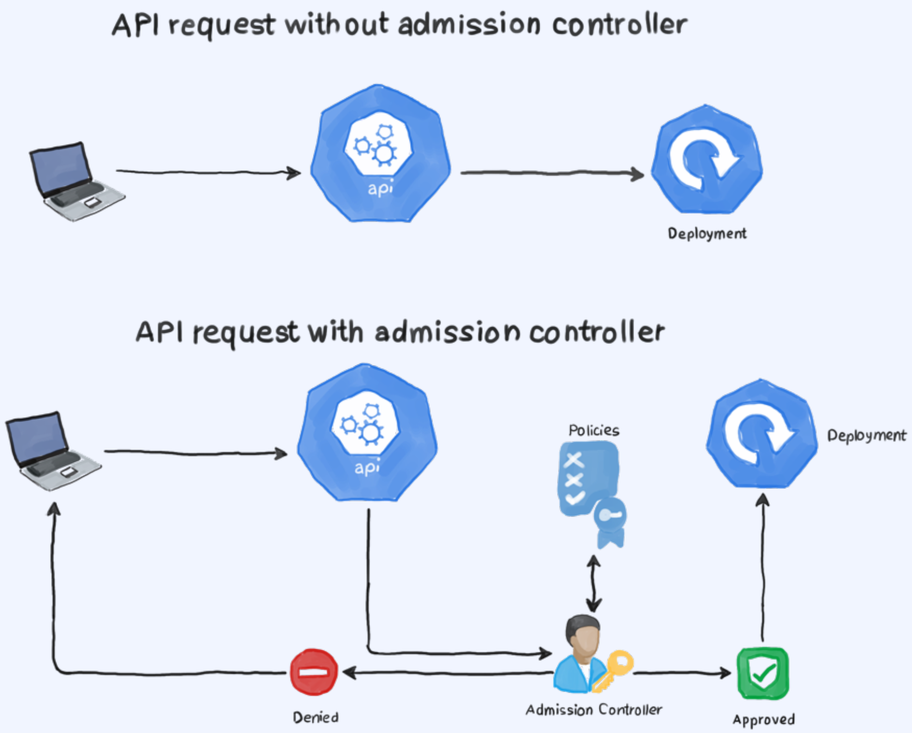
출처 : https://medium.com/@hiroyuki.osaki/illustration-open-policy-agent-aaf05bb0de8f

1. OPA 소개 #2

특징	상세내용
Validation	• Rule을 따르는 요청은 승인 • Rule을 따르지 않는 요청은 거부
Mutation	• Rule을 따르기 위해 요청 내용을 업데이트 가능
Apply tools	• 플랫폼 : Docker, Kubernetes • 도구 : SSH, Terraform, Envoy
Language	• Rego는 JSON과 같은 구조화된 문서 모델을 지원 • Rego 쿼리는 OPA에 저장된 데이터에 대한 쿼리를 명세 할 수 있으며, 이러한 쿼리는 시스템의 원하는 상태를 위반하는 데이터 정책을 정의하는 데 사용 • Rego 소개 - https://www.openpolicyagent.org/docs/latest/policy-language/ • Rego 코드 작성 및 테스트 - https://play.openpolicyagent.org/

2. OPA Gatekeeper 소개 #1

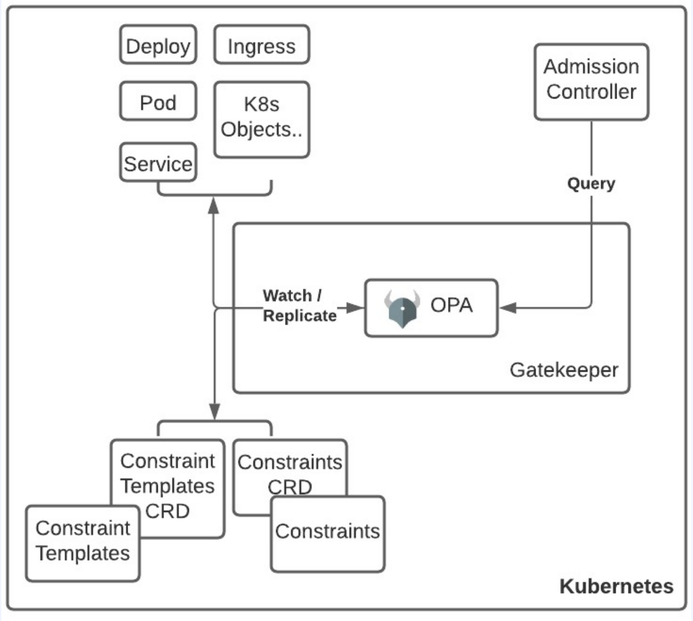
Kubernetes에서는 정책적인 결정을 API 서버와 분리해서 독립적으로 할 수 있도록 하기 위해 Admission Controller Webhook을 제공하며, 하나의 Object가 생성, 업데이트, 삭제될 때 무조건 실행됨



출처 : https://www.magalix.com/blog/integrating-open-policy-agent-opa-with-kubernetes-a-deep-dive-tutorial

2. OPA Gatekeeper 소개 #2

- OPA Gatekeeper는 내부적으로 OPA 엔진을 사용하는 OPA의 K8S Object 및 CRD(Custom Resource Definitions)의 승인/제어를 위해 구현된 오픈소스 도구
- OPA Gatekeeper는 Webhook을 확인하여 OPA 정책 엔진에서 정의한 대로 실행, 정책을 코드로 관리가능하며, 정책을 정의한 대로 Object에 대한 특정 액션을 취해줌



출처 : https://www.infracloud.io/blogs/opa-and-gatekeeper/

2. OPA Gatekeeper 소개 #3

구분	상세 설명
제약조건	• 제약조건을 사용하여 정책을 정의할 수 있음. 제약조건은 Kubernetes에서 배포 동작을 허용하거나 거부하는 조건의 집합임. • ConstraintTemplate을 사용하여 클러스터에 여러 제약조건 정책을 시행할 수 있음.
정책 출시	• 점진적이고 범위가 지정된 방식으로 정책을 시행하여 워크로드가 중단되는 위험을 제한
정책 변경 테스트	• 정책 영향 및 시행 전에 범위를 테스트하기 위한 메커니즘을 제공
기존 정책 감사	• 새로운 워크로드 및 기존 워크로드에 정책 보안 감사 제어 애플리케이션을 적용

3. OPA Gatekeeper 설치 (Helm Chart)

(1) Helm Chart를 이용한 OPA Gatekeeper 설치 명령어

- Chapter08 > Ch08_06-opa-gatekeeper

```
$ helm install ./ --name-template=gatekeeper --namespace
gatekeeper-system --create-namespace
```

(2) Helm Chart 설치 결과 확인 명령어

```
$ helm list -n gatekeeper-system
$ kubectl get all -n gatekeeper-system
```