8 Kubernetes 보안 강화 방법

01 Kubernetes 보안 강화 활용 소개

Kubernetes 보안 강화 방법

1. Kubernetes 보안 강화 활용 소개
2. [실습] kube2iam 소개 및 설치
3. [실습] kube2iam를 활용한 AWS IAM 기반 권한 관리
4. [실습] Falco 소개 및 설치
5. [실습] Falco를 활용한 런타임 보안 강화
6. [실습] OPA Gatekeeper 소개 및 설치
7. [실습] OPA Gatekeeper를 활용한 보안 정책 관리
8. [실습] cert-manager 소개 및 설치
9. [실습] cert-manager를 활용한 TLS 인증서 관리
10. [실습] AWS ACM 활용 TLS 인증서 관리

소개 내용

IAM 기반 권한 관리

런타임 보안 강화

보안 정책 관리

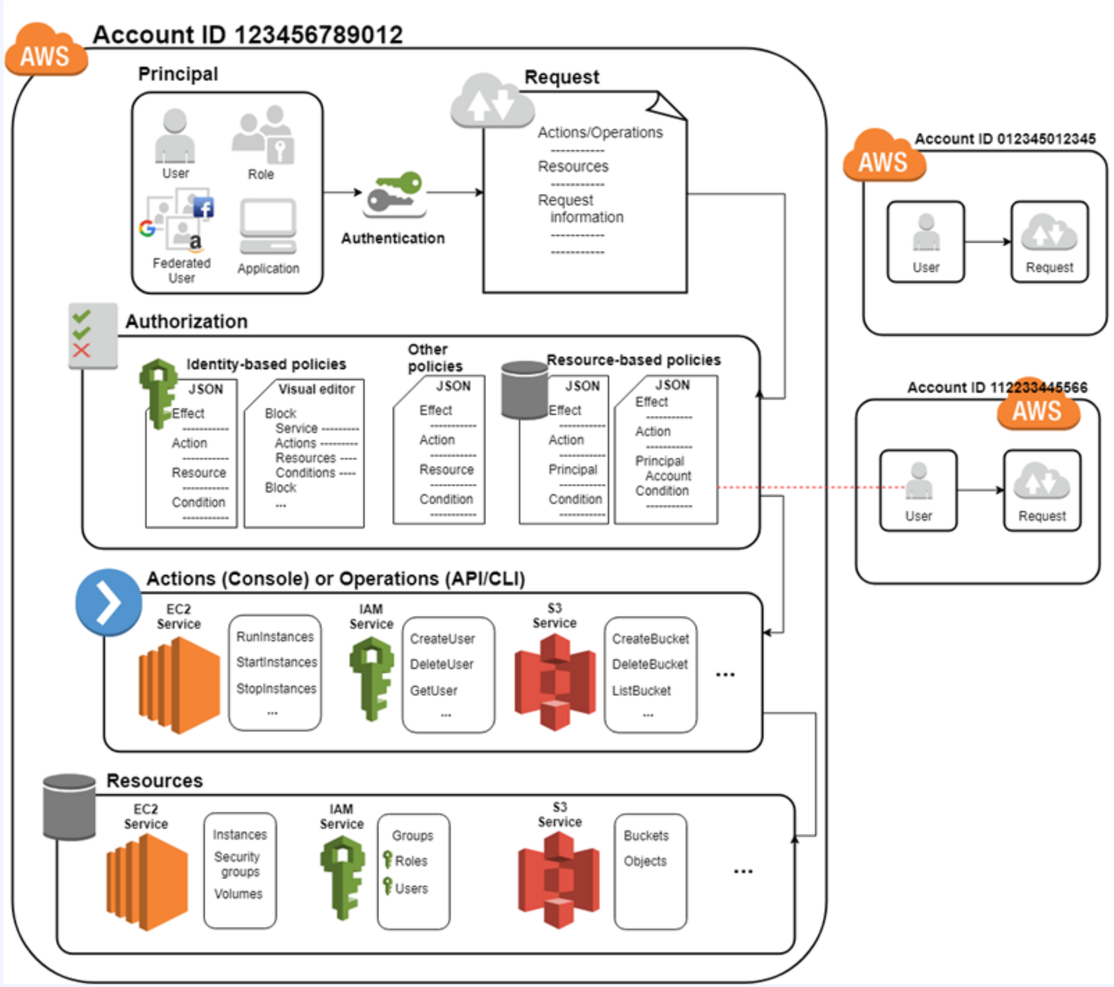
인증서 관리

1. IAM 기반 권한 관리 #1

Identity and Access Management(IAM)는 리소스에 대한 액세스를 안전하게 제어할 수 있는 서비스로, IAM을 사용하여 기본 접근 및 리소스를 사용하도록 권한 부여

구분	상세 설명
User	• IAM User는 플랫폼 내에서 생성하는 사용자로 플랫폼 상호작용하는 사용자 혹은 어플리케이션을 의미
Group	• IAM Group은 IAM User의 집합이고, 그룹을 사용함으로써 다수 사용자에 대하여 동일한 권한을 보다 쉽게 관리 가능
Role	• IAM Role은 특정 권한을 가진 IAM 자격 증명 방식임 • Role을 사용함으로써 특정 사용자 혹은 어플리케이션에 혹은 서비스에 접근 권한을 위임
Policy	• IAM Policy는 접근하는 권한을 정의하는 개체로, IAM 리소스들과 연결하여 사용

1. IAM 기반 권한 관리 #2



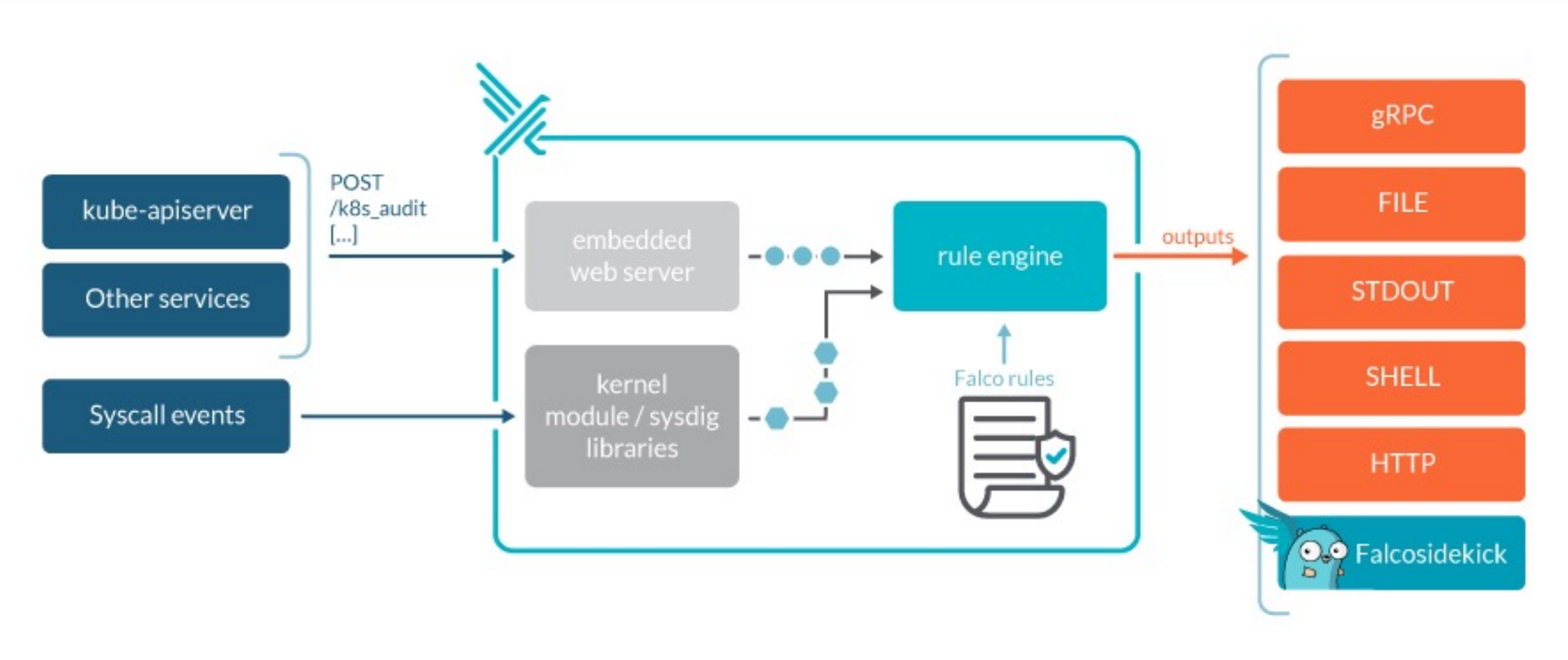
출처 : https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/intro-structure.html

2. 런타임 보안 강화 #1

런타임 보안 강화는 검증된 트래픽만을 허용하는 방법, 서비스 간 최소 권한 아래의 통신을 적용하고 외부 공격으로부터 내부망 이동을 방어하는 방법, 워크로드 자체가 예상 보호 범위 내에서 작동하는지 여부를 검증하는 방법 등을 포함

구분	상세 설명
이미지 스캐닝	• 런타임 취약성 스캐닝을 자동화할 수 있으며, 위험을 줄이고 실행 중인 컨테이너에 사용된 이미지를 보호하기 위한 정책 커스터마이징 지원
워크로드 이상 감지	• 네트워킹 모듈을 표준화하고, 신규 워크로드 설정 시 중요한 문제인 네트워킹 모듈상에 편차가 있는지의 이상을 감지해 보안운영(SecOps) 담당에 리포팅 가능
수신 및 송신 보안	• Kubernetes에 도달하는 외부 소스데이터 수신에 대한 추가 가시성을 보안팀에 제공하고, IP 주소 및 데이터를 기반으로 잘못된 송신 대상으로의 연결을 감지, 차단
위협 탐지	• 오픈 포트를 스캔해 취약성을 확인하고, 진행 중인 내부망 이동 공격이 있는지 확인

2. 런타임 보안 강화 #2



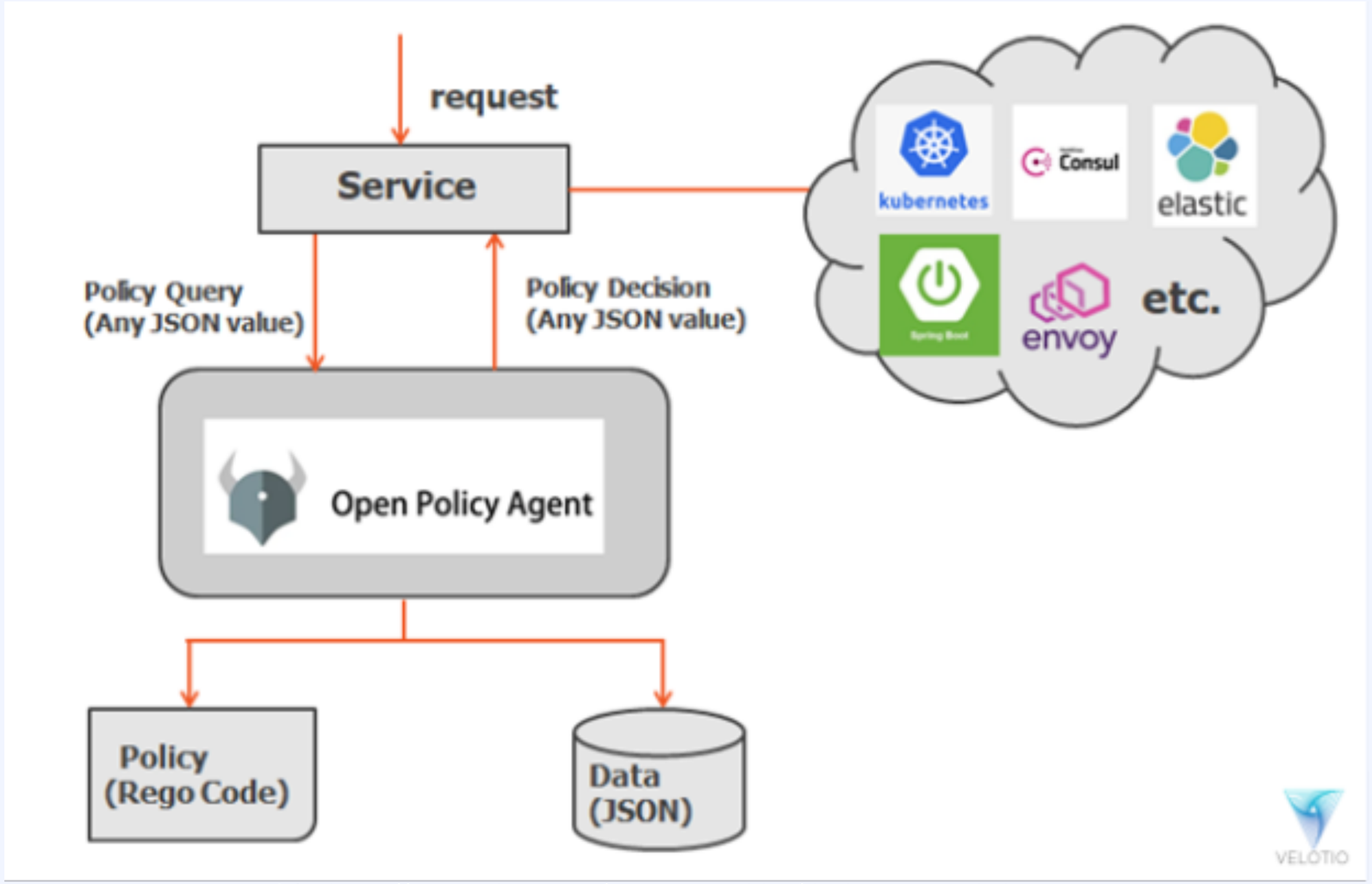
출처 : https://sysdig.com/blog/intro-runtime-security-falco/

3. 보안 정책 관리 #1

보안 정책 관리는 정책 통합하여 적용/관리하는 방식. Kubernetes에 대한 사용자 정의 컴플라이언스 관리 정책의 기술을 제한 없이 구현 가능하도록 제공. 정책을 코드로 관리 할 수 있도록 정책 구현 전용 언어인 Rego라는 선언형 언어를 사용.

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. 보안 정책 관리 #2



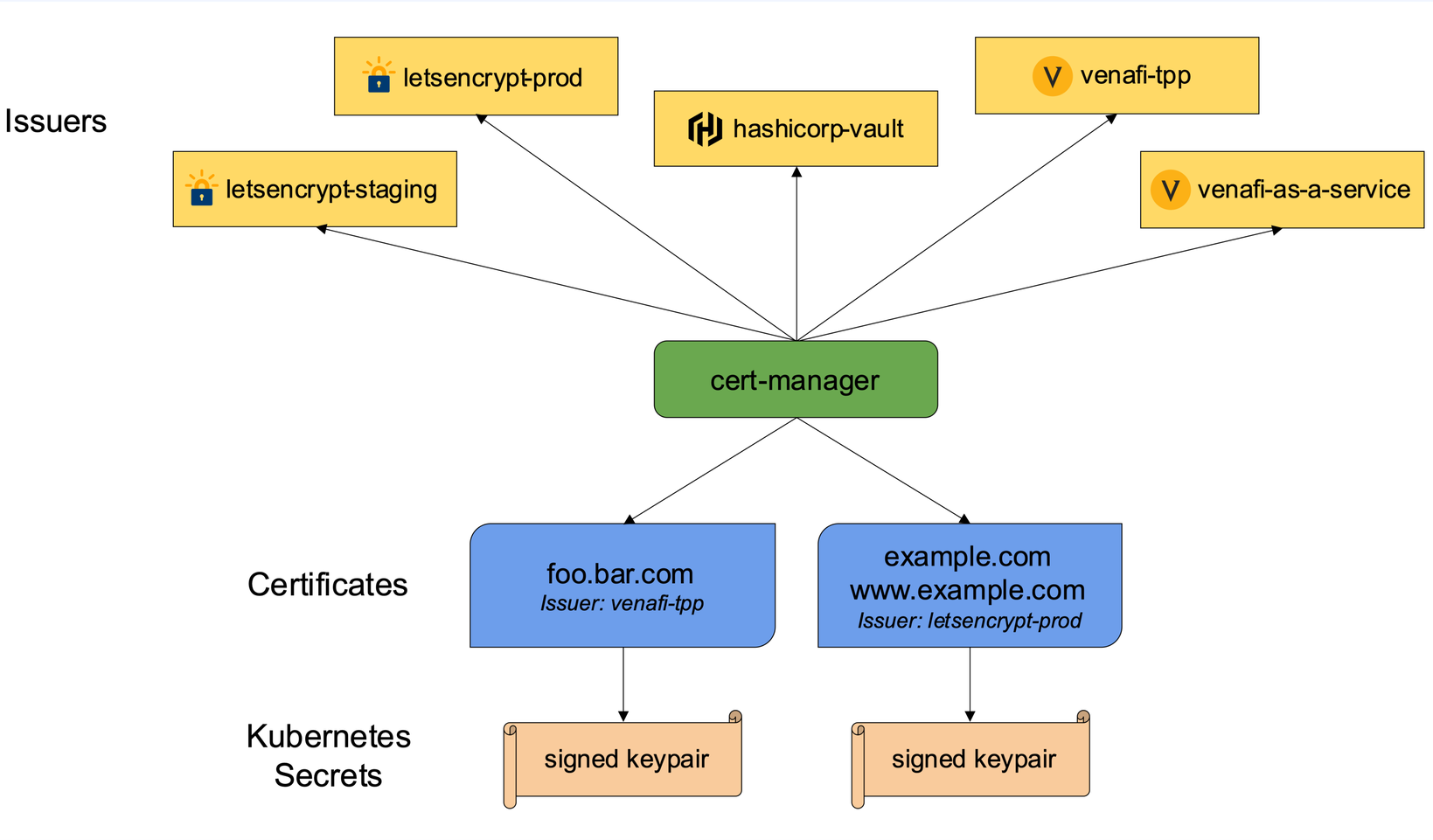
출처 : https://www.velotio.com/engineering-blog/deploy-opa-on-kubernetes

4. 인증서 관리 #1

인증서 관리는 HTTPS 통신을 위한 인증서를 생성하고, 인증서 만료시 자동으로 인증서를 갱신해주는 역할을 하는 관리 방식. 주로 웹 사이트 및 내부 리소스 보안에 사용하며, 공인 및 사설 SSL/TLS 인증서를 손쉽게 프로비저닝, 관리 및 배포할 수 있도록 지원

구분	상세 설명
인증서 적용	• Kubernetes 내에서 외부에 존재하는 Issuers를 활용 • Selfsigned Issuer를 직접 생성해서 생성하여 Certificate를 생성
인증서 검사	• 인증서의 유효성을 검사하고 최신 상태인지를 확인
인증서 갱신	• 생성된 Certificate를 관리하며, 인증서의 만료 시간이 가까워지면 인증서를 자동으로 갱신
다양한 발급자	• Let's Encrypt, HashiCorp Vault, Venafi등 간단한 서명 Keypair 또는 자체 서명과 같은 다양한 발급자로부터 인증서 발급 지원

4. 인증서 관리 #2



출처 : https://cert-manager.io/docs/