8 Kubernetes 보안 강화 방법

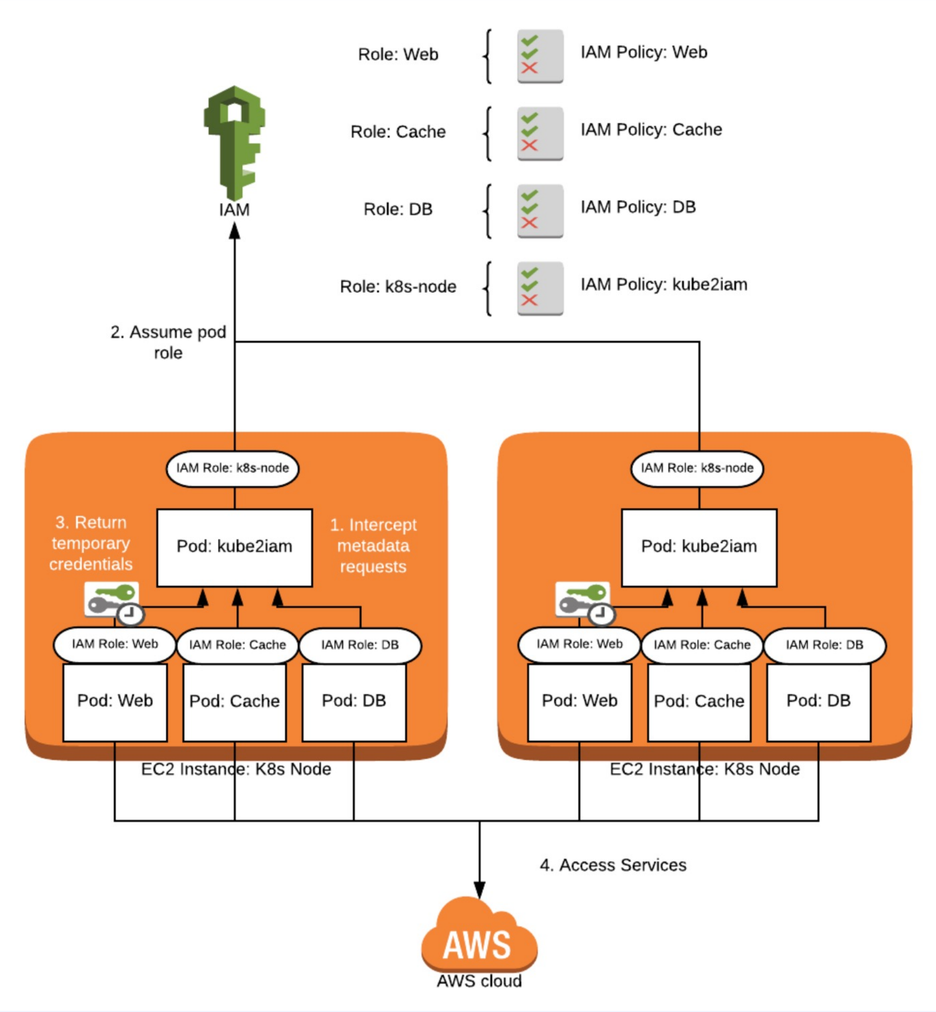
02 kube2iam 소개 및 설치

소개 내용

순서

1. kube2iam 소개
2. kube2iam의 단점 및 대체 방법
3. AWS IRSA 소개
4. AWS IRSA 설치 방법

1. kube2iam 소개



- **Annotation**을 기반으로 Kubernetes 클러스터 내에서 실행되는 컨테이너에 **IAM 자격 증명**을 제공하는 오픈소스 도구
- 각 Kubernetes **POD**가 가질 수 있는 **권한을 제한**
- 트래픽을 **EC2 메타데이터 API**로 Proxy 처리
- AWS 내 Kubernetes에서 실행되는 **애플리케이션**(POD)을 **보호하는 데 도움**이 됨

출처 : https://www.bluematador.com/blog/iam-access-in-kubernetes-kube2iam-vs-kiam

2. kube2iam의 단점 및 대체 방법

단점

- Daemonset 형태로 모든 EKS Worker Node에 POD를 배포해야함
- 이에 모든 EKS Worker Node의 Role에 Assume Role 권한을 부여해야함
- Worker Node마다 Iptables DNAT 설정을 해야함(EC2 메타데이터 API 호출용)

대체 방법

- AWS에서 EKS – IAM 연동 및 자격 증명을 위한 IRSA(IAM Role for Service Account)를 사용

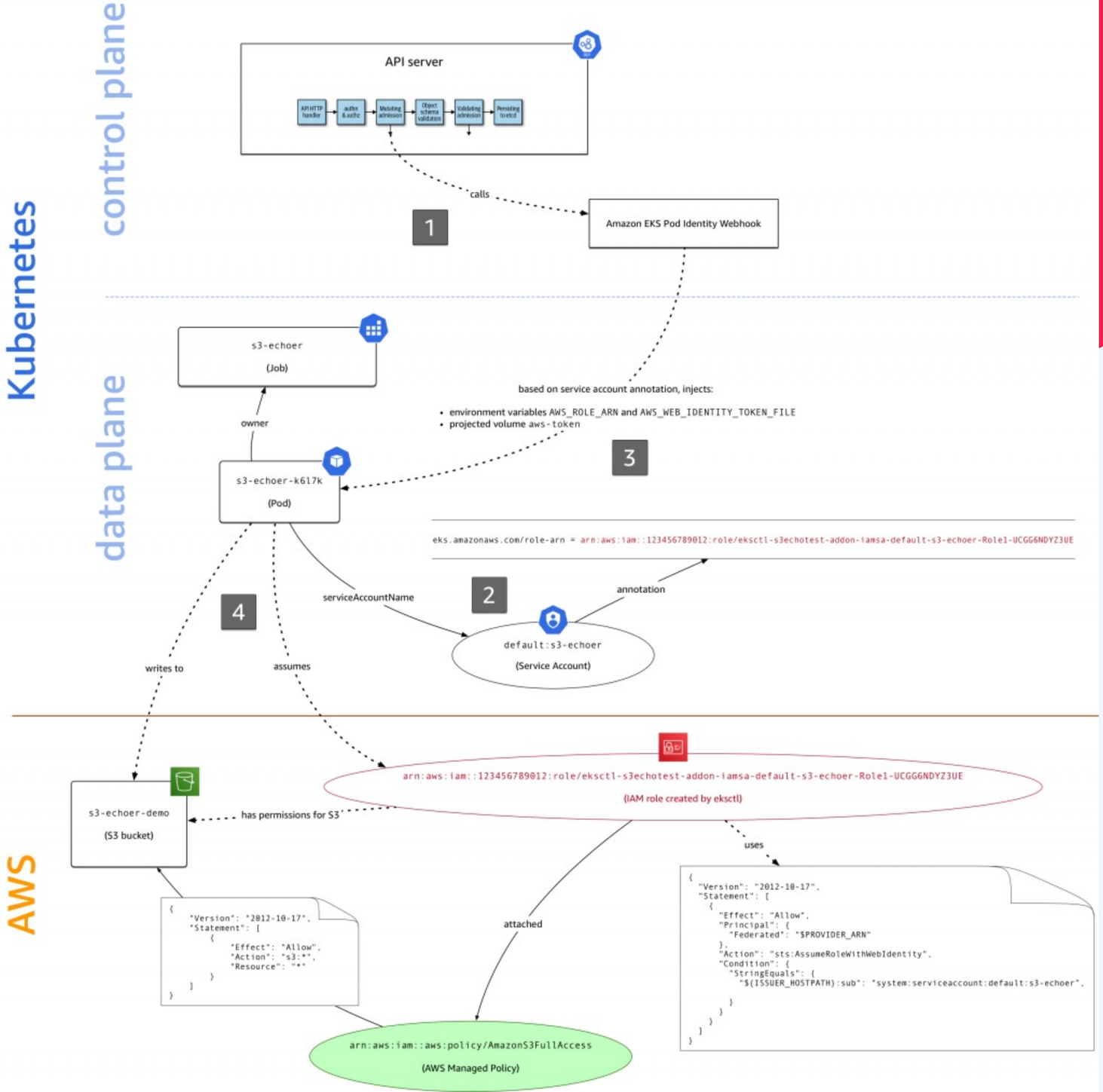
3. AWS IRSA 소개 #1

- IRSA(IAM Role for Service Account , 서비스 어카운트용 IAM 역할)
- OpenID Connect(OIDC) 자격 증명 공급자와 Kubernetes(EKS) Service Account Annotation을 결합하여 POD 수준에서 IAM 역할을 사용할 수 있도록 하는 AWS의 기능
- eksctl 및 awscli를 통해 EKS 및 IAM과 연동하여 구현

3. AWS IRSA 소개 #2

특징	상세내용
최소 권한	• EKS Worker Node가 AWS API 호출 Role에 확장된 권한을 제공할 필요 없음 • IAM 권한의 범위를 Service Account로 지정할 수 있음 • 해당 Service Account를 사용하는 POD만 이 권한에 액세스할 수 있음 • kube2iam, kiam 같은 다른 오픈소스 도구가 필요 없음
자격 증명 격리	• 컨테이너는 컨테이너가 속한 Service Account와 연결된 IAM Role에 대한 자격 증명만 검색할 수 있음 • 컨테이너는 다른 POD에 속한 다른 컨테이너를 위한 자격 증명에는 액세스할 수 없음
감사	• CloudTrail을 통한 액세스 및 이벤트 로깅을 사용하여 이전 감사로그를 검색 및 확인가능

3. AWS IRSA 소개 #3



4. AWS IRSA 설치 방법

(1) IRSA용 OIDC 자격 증명 공급자 생성 명령어

```
$ eksctl utils associate-iam-oidc-provider --cluster <EKS클러스터명> --approve
```

(2) 생성된 IRSA용 OIDC 자격 증명 공급자 URL 확인 명령어

```
$ aws eks describe-cluster --name <EKS클러스터명> --query
"cluster.identity.oidc.issuer" --output text
```

(3) 생성된 IRSA용 OIDC 자격 증명 공급자 ARN 확인 명령어

```
$ aws iam list-open-id-connect-providers | grep <(2)번에서 나온 ID값 입력>
```