8 Kubernetes 보안 강화 방법

03 kube2iam를 활용한 AWS IAM 기반 권한 관리

실습 내용

순서

1. 사전 준비
2. IAM Policy 적용 (접근할 AWS Resource 권한 적용)
3. IRSA 적용 (eksctl)
4. IRSA 적용 검증 (POD 배포 및 awscli 수행)

실습 예제코드 경로

Chapter08 > Ch08_03-kube2iam-irsa

1. 사전 준비

EKS Cluster :

- IRSA 테스트 검증을 위한 Kubernetes 환경, 기존에 사용한 환경과 동일하게 사용

S3 Bucket :

- S3 Bucket 내 파일 목록 조회 및 삭제 검증용으로 Bucket 1개 생성

DynamoDB Table :

- DynamoDB Table 정보 조회 및 삭제 검증용으로 Table 1개 생성

2. IAM Policy 적용 (접근할 AWS Resource 권한 적용)

(1) 접근할 AWS Resource 권한 적용을 위한 IAM Policy 적용 명령어

- Chapter08 > Ch08_03-kube2iam-irsa

```
$ aws iam create-policy \
--policy-name <생성할 IAM Policy명> \
--policy-document file://iam-policy.json
```

3. IRSA 적용 (eksctl)

(1) eksctl를 활용한 IRSA 적용 명령어

```
$ eksctl create iamserviceaccount \
  --name <IRSA명> \
  --namespace <적용할 EKS내 Namespace명> \
  --cluster <EKS 클러스터명> \
  --attach-policy-arn arn:aws:iam::<AWS 12자리 계정 ID>:policy/<2번에서
생성한 접근할 Resource의 IAM Policy명> \
  --approve
```

4. IRSA 적용 검증 (POD 배포 및 awscli 수행) #1

(1) IRSA 적용 검증용 awscli 수행을 위한 POD 배포 명령어

- Chapter08 > Ch08_03-kube2iam-irsa

```
$ kubectl apply -f ./aws-cli-pod.yaml
```

(2) 배포후 POD내 Bash Shell 실행 명령어

```
$ kubectl exec -it aws-cli -- bash
```

(3) Assume Role에 의해 발급된 임시 토큰 권한(STS) 확인 명령어

```
$ aws sts get-caller-identity
```

4. IRSA 적용 검증 (POD 배포 및 awscli 수행) #2

(4) S3 Bucket 내 파일 목록 출력 명령어

```
$ aws s3 ls s3://<S3 Bucket명>
```

(5) S3 Bucket 내 특정 파일 삭제 명령어

```
$ aws s3 rm s3://<S3 Bucket명>/<특정 파일명>
```

4. IRSA 적용 검증 (POD 배포 및 awscli 수행) #3

(6) DynamoDB Table 정보 출력 명령어

```
$ aws dynamodb describe-table --table-name <DynamoDB Table명>
```

(7) DynamoDB Table 삭제 명령어

```
$ aws dynamodb delete-table --table-name <DynamoDB Table명>
```