8 Kubernetes 보안 강화 방법

10 AWS ACM 활용 TLS 인증서 관리

소개 및 실습 내용

순서

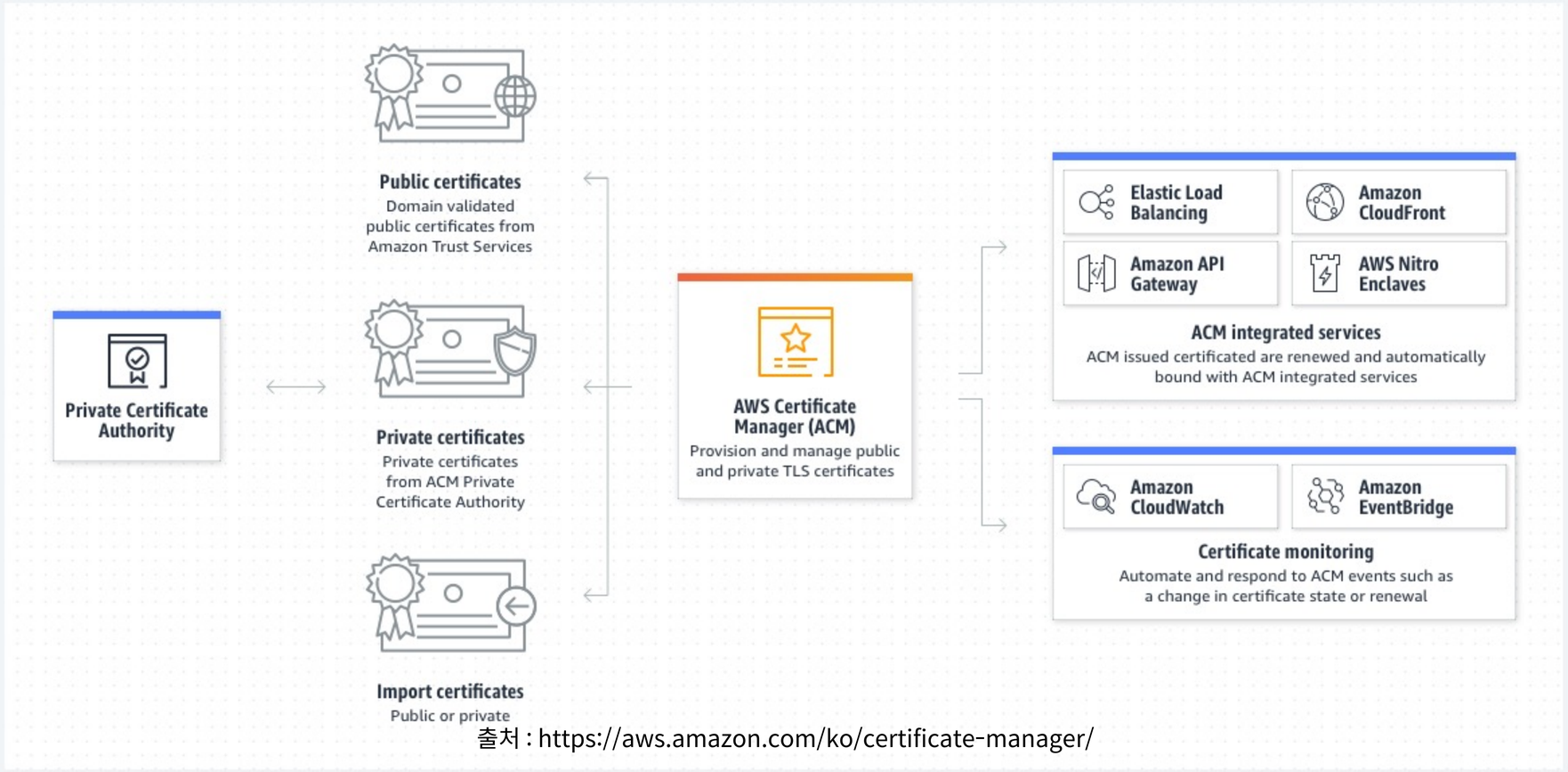
1. AWS ACM 소개
2. 사전 준비사항
3. AWS ACM을 통한 TLS 인증서 발급
4. 테스트용 K8s Object 배포 및 실행
5. Route53 도메인 등록 및 HTTPS 접속 검증

실습 예제코드 경로

Chapter08 > Ch08_10-aws-certificate-manager

1. AWS ACM 소개

AWS ACM(Certificate Manager)는 서비스 및 연결 리소스에 사용할 공인 및 사설 SSL/TLS 인증서를 프로비저닝, 관리 및 배포할 수 있도록 지원하는 서비스



출처 : https://aws.amazon.com/ko/certificate-manager/

2. 사전 준비사항

(1) EKS Cluster

(2) AWS ALB Controller

(3) Domain 주소

- Route53 > 등록된 도메인 > 도메인 등록에서 도메인 준비 (신청후 이메일 인증 1회)
- Domain이 발급 되었다면 다음의 경로에서 도메인을 확인해 사용가능
  - Route53 > 호스팅 영역 > 본인이 등록한 도메인 이름 클릭

3. AWS ACM을 통한 TLS 인증서 발급

(1) AWS Management Console에서 ACM 서비스 접속

- 상단 검색창 > acm(Certificate Manager) > 인증서 요청 버튼 클릭

(2) 퍼블릭 인증서 요청

- 완전히 정규화된 도메인 이름 : <본인이 생성한 Domain 주소> 입력

(3) DNS 검증 수행시 명령어

$ dig +short <DNS 검증 Domain 주소>

4. 테스트용 K8s Object 배포 및 실행

(1) 테스트용 Deployment, Service, Ingress 설치 명령어

- Chapter08 > Ch08_10-aws-certificate-manager

```
$ kubectl apply -f ./
```

(2) 테스트용 K8s Object 배포 및 실행 결과 확인 명령어

```
$ kubectl get all
$ kubectl get ingress
```

5. Route53 도메인 등록 및 HTTPS 접속 검증 #1

(1) AWS Management Console에서 Route53 서비스 접속

- 상단 검색창 > Route53 > **호스팅 영역** > 본인이 생성한 도메인 이름 클릭

(2) Route53 도메인 등록

- 레코드 생성 > 레코드 이름 입력 > 값 – **별칭** 활성화 > 엔드포인트 선택
  > Application/Classic Load Balancer에 대한 별칭 > 리전 선택 [**ap-northeast-2**]
  > 로드 밸런서 선택 > (kubectl get ingress 명령어 출력중 **ADDRESS** 복사후 검색
  > **리소스 선택** > 레코드 생성 버튼 클릭 > 도메인 등록 확인

5. Route53 도메인 등록 및 HTTPS 접속 검증 #2

(3) 등록된 Domain 주소를 웹브라우저에 입력

- 페이지가 안 나올 경우, Domain 주소 앞에 https:// 를 붙임

(4) HTTPS 접속 검증

1. 웹브라우저 주소창 맨앞에 자물쇠 모양 클릭
2. "이 사이트는 보안 연결(HTTPS)이 사용되었습니다." 항목 클릭
3. "인증서가 유효함" 항목 클릭