

AWS Service - Security

Sung-Dong Kim,
School of Computer Engineering,
Hansung University



What to study

- ④ **공동 책임 모델 (Shared Responsibility Model: SRM)**
- ④ **AWS CloudTrail**
- ④ **Other Services**



공동 책임 모델

고객 데이터

고객
책임

플랫폼, 애플리케이션, 자격 증명 및 액세스 관리

운영 체제, 네트워크, 방화벽 구성

클라이언트 측 데이터
암호화 및 데이터
무결성 인증

서버 측 암호화
(파일 시스템 및/또는
데이터)

네트워크 트래픽
보호(암호화, 무결성,
자격 증명)

AWS 기초 서비스

컴퓨팅

스토리지

데이터베이스

네트워킹

AWS의
책임

AWS 글로벌 인프라

리전

가용 영역

엣지 로케이션

☑ AWS의 책임: 클라우드의 보안

- 데이터 센터의 물리적 보안
- 하드웨어 및 소프트웨어 인프라: 스토리지 폐기, 호스트 OS 액세스 로깅 및 감사
- 네트워크 인프라: 침입 탐지
- 가상화 인프라: 인스턴스 격리

```
<html>
<head>
  <title>Example
  <meta http-equiv="Content-Type" content="text/html" />
  <style type="text/css">
    html, body, div, h1, h2, h3 {
      padding: 0;
      font-weight: 100;
    }
    body {
      background: #f0f0f0;
      font-size: 18px;
      color: #555;
    }
  </style>
</head>
```

☑️ 고객의 책임: 클라우드에서의 보안

- EC2 instance 운영 체제: 패치 적용, 유지 관리 등
- 애플리케이션: 암호, 역할 기반 액세스 등
- 보안 그룹 구성
- OS 또는 호스트 기반 방화벽: 침입 탐지 또는 차단 시스템
- 네트워크 구성
- 계정 관리: 각 사용자에게 대한 로그인 및 권한 설정



☑ 서비스 특성 및 보안 책임

- IaaS
 - 고객은 네트워킹 및 스토리지 설정을 보다 유연하게 구성할 수 있음
 - 보안의 더 많은 측면을 고객이 관리해야 함
 - 액세스 제어를 고객이 구성

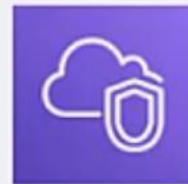
고객이 관리하는 서비스의 예



Amazon
EC2



Amazon Elastic
Block Store
(Amazon EBS)



Amazon Virtual
Private Cloud
(Amazon VPC)

- PaaS
 - 고객이 기본 인프라를 관리할 필요 없음
 - 운영체제, 데이터베이스 패치 적용, 방화벽 구성 및 재해 복구를 AWS가 처리
 - 고객은 코드 또는 데이터 관리에 집중

AWS에서 관리하는 서비스의 예



AWS Lambda



Amazon Relational
Database Service
(Amazon RDS)



AWS Elastic
Beanstalk

- SaaS
 - 소프트웨어가 중앙에서 호스팅 됨
 - 구독 모델 또는 종량 과금제로 라이선스가 부여됨
 - 일반적으로 웹 브라우저, 모바일 앱 또는 API를 통해 액세스 함
 - 고객은 서비스를 지원하는 인프라를 관리할 필요 없음

SaaS의 예



AWS Trusted
Advisor

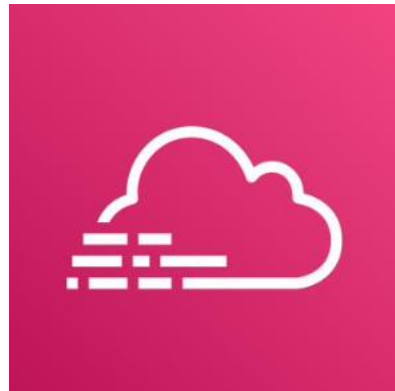


AWS Shield



Amazon Chime

AWS CloudTrail



- ④ AWS 계정의 사용자 활동 및 API 사용 추적
- ④ 지속적으로 사용자 활동을 모니터링하고 API 호출을 기록
- ④ 규정 준수 감사, 보안 분석, 문제 해결에 유용
- ④ 로그 파일은 S3 버킷으로 전송됨

누가?

무엇을?

언제?

어디로?

API 보안 관련 정보

☑ 기본 AWS CloudTrail 이벤트 기록은 기본적으로 활성화 되어 있으며 무료임

- 최근 90일 간의 계정 활동에 대한 모든 관리 이벤트 데이터 포함

☑ CloudTrail 액세스





















- AWS Management Console → CloudTrail 선택
- [Event history (이벤트 기록)]

☑ 90일이 지난 로그 및 이벤트 알림 기능 활성화 → 추적 생성

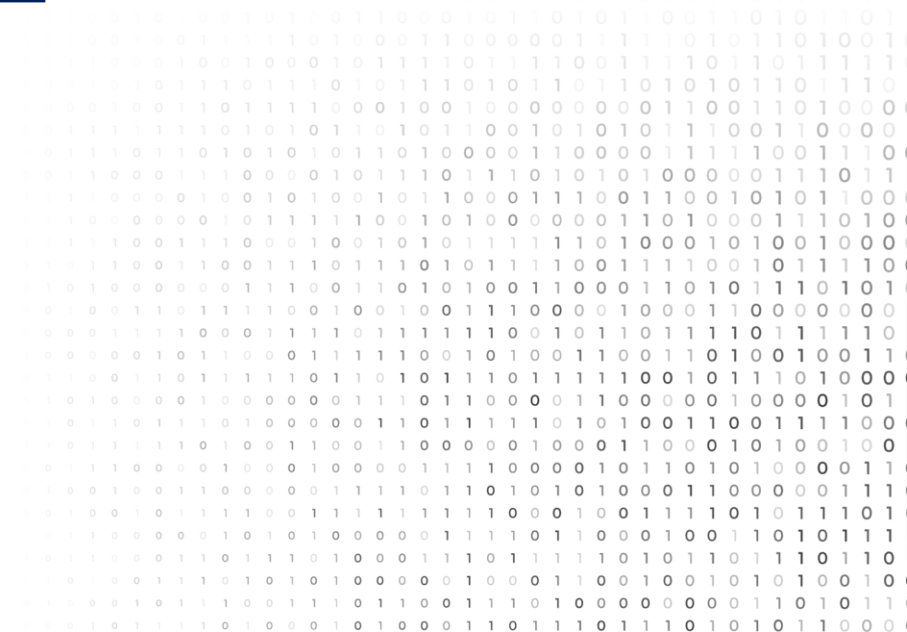
- CloudTrail 콘솔 추적 페이지에서 [Create trail(추적 생성)] 선택
- 이름 지정, 모든 리전 적용, 로그 저장을 위한 새 S3 버킷 생성
- S3 버킷에 대한 액세스 권한 구성

Other Services

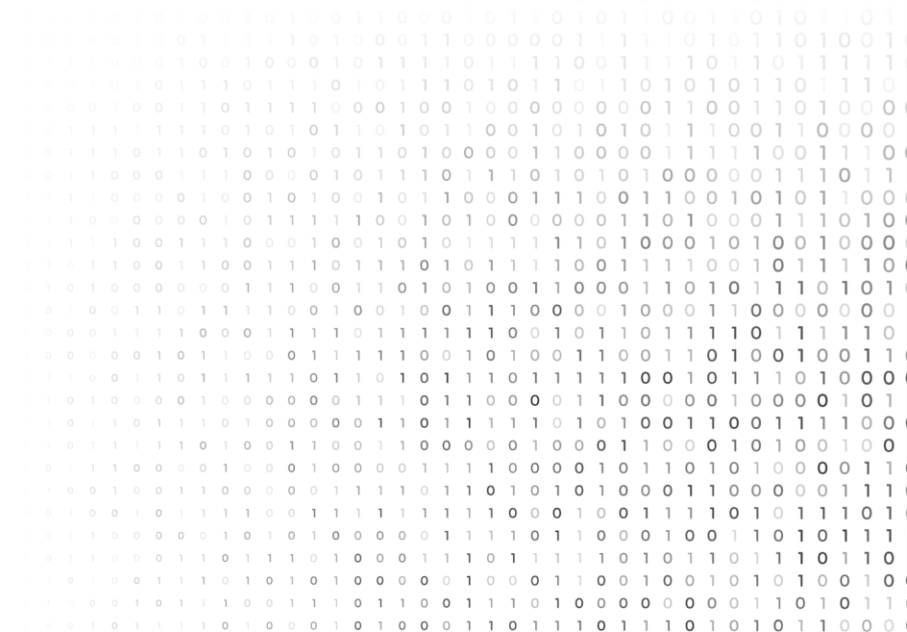
☑ 비용 절감, 성능 개선, 보안 강화에 도움이 되는 지침을 제공하는 서비스

비용 최적화	성능	보안	내결함성 기능	서비스 한도
				
0  9  0 	3  7  0 	2  4  11 	0  15  5 	37  0  1 
7,516.87 USD 잠재적 월별 절감액				

- ④ 암호화 키를 생성하고 관리
- ④ AWS 서비스 및 애플리케이션 전체의 암호화 사용 제어
- ④ AWS CloudTrail과 통합할 경우 모든 키 사용 로깅
- ④ FIPS (Federal Information Processing Standard) 140-2에서
검증한 HSM (하드웨어 보안 모듈)을 사용하여 키 보호



- ④ 웹 및 모바일 애플리케이션에 사용자 가입, 로그인 및 액세스 제어를 추가
- ④ 수백만 명의 사용자까지 확장
- ④ Facebook, Google, Amazon과 같은 소셜 자격 증명 공급자와 SAML (Security Assertion Markup Language) 2.0을 사용한 Microsoft Active Directory와 같은 엔터프라이즈 자격 증명 공급자를 사용한 로그인 지원



- ④ DDoS (분산 서비스 거부 공격) 방어를 위한 관리형
- ④ AWS에서 실행되는 애플리케이션 보호
- ④ AWS Shield Standard는 추가 비용 없이 활성화 됨
- ④ AWS Shield Advanced는 선택형 유료 서비스
- ④ 애플리케이션 다운타임과 지연시간을 최소화 할 수 있음



④ 유휴 데이터 암호화

- 보안 키로 데이터 인코딩
- 보안 키가 있는 사용자만 데이터 디코딩
- AWS KMS에서 보안 키 관리

④ 전송 데이터 암호화

- TLS (전송 계층 보안)
- AWS Certificate Manager: TLS 인증서 배포, 관리 및 갱신 방법 제공
- 보안 HTTP (=HTTPS)은 보안 터널 생성

