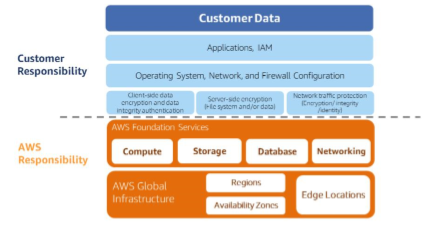
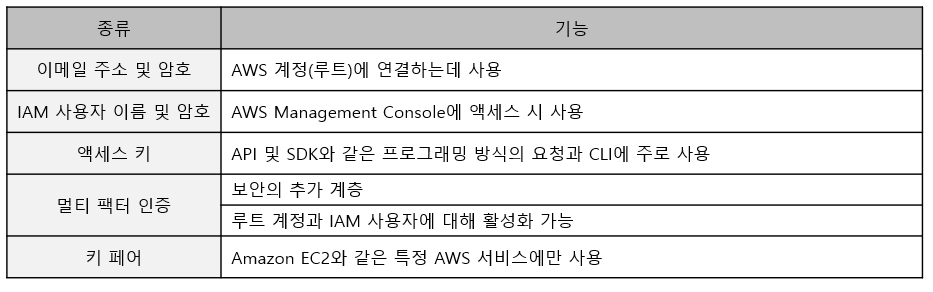
1. 파트 1: AWS 공유 책임 모델(사진 출처: 강의 자료)

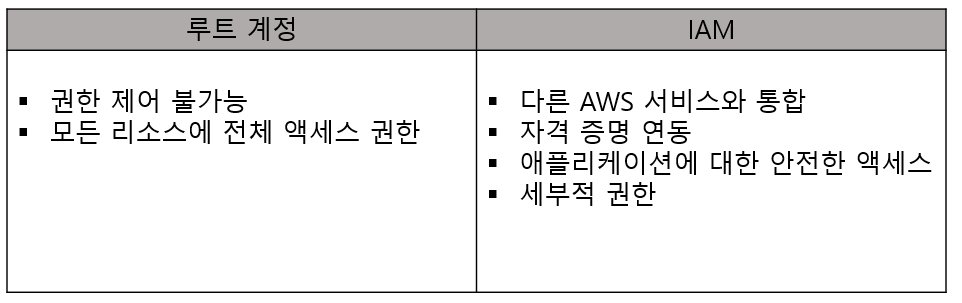


* 1. 요약
     1. AWS와 고객은 보안의 책임 분담함
     2. 고객은 구축하려고 하는 보안 조치를 완전히 제어 가능
     3. 고객은 AWS 서비스 카탈로그를 사용하여 IT 서비스의 카탈로그를 관리 가능
     4. 인프라스트럭처 서비스의 보안 구성은 완벽히 고객의 통제 아래 있음.

1. 파트 2: AWS Identity and Access Management (IAM)
   1. 소개
      1. AWS 리소스에 대한 사용자의 **액세스 및 인증을 중앙에서 관리**
      2. 추가비용 없이 AWS 계정의 기능으로 제공
      3. **사용자, 그룹, 역할**을 생성하고 **정책** 적용하여 AWS 리소스에 대한 액세스 제어
      4. 맥락에 따라 필요한 자격 증명 정의  
         (예: **누가 어떤 서비스**에 액세스하고 있으며 **무슨 작업**을 수행하고자 하는가?)
   2. 보안 자격 증명의 유형



* 1. 루트 계정 액세스와 IAM 액세스의 비교
     1. IAM을 사용하면 **최소한의 권한** 원칙 적용
     2. 루트 계정 vs IAM



* 1. 인증
     1. 프로그래밍 방식 액세스
        + 액세스 키 ID와 보안 액세스키 인증
        + API, CLI, SDK 그리고 다른 개발 도구에 액세스 권한 제공
     2. 콘솔 액세스
        + 계정 ID 또는 별칭, IAM 사용자 이름과 패스워드 사용
        + MFA를 활성화할 경우, MFA 인증 코드 추가 입력
  2. 권한 부여
     1. 권한을 부여해 사용자가 AWS 서비스의 액세스 허용
     2. 권한: 어떤 리소스와 어떤 작업을 사용할 수 있을 지 결정
        + 기본 설정에서 모든 권한은 암시적으로 거부되어 있음.
        + 명시적으로 거부된 사항은 절대 허용될 수 없음.
     3. 모범 사례
        + 최소한의 권한 원칙 적용  
          주의: IAM은 글로벌임. 리전 별로 별도로 관리하지 않고 전 리전에 적용됨.
  3. 사용자
     1. 정의 및 특성
        + 사용자가 AWS에 생성한 엔티티
        + AWS와 상호작용하는 방법 제공
        + IAM 사용자에 대한 시본 보안 자격 증명 없음  
          자격 증명은 개벽적으로 지정해애 함
        + IAM 사용자는 사람이 아닐 수 있음.
     2. 모범 사례
        + 루트 계정 사용자를 위해 관리 권한이 있는 별도의 IAM 사용자 계성 생성
  4. 그룹
     1. 정의
        + IAM 사용자의 모음
     2. 특성
        + 전체 그룹에 대한 권한 지정
        + 기본 그룹은 없음
        + 그룹 중첩 불가능
        + 한 사용자가 여러 그룹에 속할 수 있음
        + 권한은 IAM 정책을 사용하여 정의
  5. **역할(\*시험에 잘 나옴\*)**
     1. AWS 리소스에 대한 액세스 권한을 위임하는데 사용
     2. 여기서 권한은…
        + IAM 정책을 사용하여 정의됨.
        + IAM 사용자 또는 그룹이 아니라 역할에 연결됨.
     3. 다시 한번 정리하면
        + IAM 정책에 의해 권한을 결정
        + 계정 정보나 인증키를 프로그램에 내장할 필요 없이 ARN id 기반으로 인증
        + 앱이 또다른 앱에 접근하면 IAM에게 물어보고 App의 ARN id를 보고 인증
        + 키 페어: 마스터 키를 AMI에 넣고, 개인키를 match시켜 인증
  6. 정책
     1. 정의 및 특성
        + 하나 이상의 권한으로 구성된 공식 문
        + 정책을 IAM(사용자, 그룹 또는 역할)에 연결
        + 정책은 엔티티가 수행할 수 있거나 수행할 수 없는 작업에 대한 권한 부여
        + 단일 정책이 여러 개의 엔티티에 연결 가능
        + 단일 엔티티에 여러 개의 정책 연결 가능
     2. 모범 사례
        + 여러 IAM 사용자에게 같은 정책을 연결할 때, 사용자를 그룹에 넣은 후 사용자가 아닌 그룹에 정책 연결

1. 파트 3: AWS Trusted Advisor
   1. AWS Trusted Advisor는 다섯 가지 영역에서 모범 사례(검사)를 제공
      1. 비용 최적화
      2. 성능
      3. 보안
      4. 내결함성
      5. 서비스 한도
   2. 모범 사례를 바탕으로 만들어진 app
   3. 각 사항에 대한 제안 사항을 알려줌
2. 파트 4: AWS CloudTrail
   1. AWS CloudTrail: API 호출에 대한 로그를 저장
   2. AWS CloudTrail의 이점 🡺 감사, 추적
      1. 사용자 및 리소스 활동
      2. 규정 준수 간소화
      3. 상시 가동
      4. 보안 자동화
      5. 분석과 문제 해결