* IAM(Identity and Access Management)이란?
- AWS 리소스에 대한 액세스를 안전하게 제어할 수 있는 서비스, IAM을 사용하여 리소스를 사용하도록 인증 및 권한 부여된 대상을 제어
- 주요 기능
    - AWS 계정에 대한 공유 액세스
    - 서비스별 세분화된 권한 제공 가능
    - EC2에서 실행되는 앱을 위한 AWS 리소스 액세스 권한 제공
    - 멀티 팩터 인증(MFA)
    - 자격 증명 연동
- AWS 서비스들은 IAM Role을 할당받아 권한을 부여받을 수 있음
- Access Key와 Secret Access Key를 직접 입력하지 않고 권한 부여 가능
- IAM 사용자 계정을 만들어 사용자에게 적절한 권한을 부여하고 사용 가능한 서비스를 제한할 수 있음

* 정책(Policy)
- User, Group, Role이 사용할 수 있는 권한의 범위를 지정한 것
- S3FullAccess, Administrator Access 등 다양한 액세스 권한이 이미 정의되어 있으며 이를 'AWS 관리형 정책'이라 함
- 사용자 정의 정책 생성
    - JSON 형식 또는 직접 선택을 통해 사용자 정의 정책 선택 가능
- JSON 형식의 정책 구성요소
    - Effect : Allow 또는 Deny를 사용하여 허용 / 거부 여부 표시
    - Principal : 접근을 허용 혹은 차단할 대상
    - Action : 작업을 허용 혹은 차단할 접근 타입(Get, Put 등)
    - Resource : 작업이 적용되는 리소스 목록
    - Condition : 권한이 부여되는 상황(조건)

* 역할(Role)
- 특정 권한을 가진 계정에 생성할 수 있는 IAM 자격증명
- 역할에는 다음과 같은 주체가 있음
    - AWS 계정의 IAM 사용자
    - AWS의 서비스(EC2, RDS, ELB 등)
    - 외부 자격 증명 공급자 서비스에 의해 인증된 외부 사용자
- 역할 생성시 IAM 사용자, 서비스, 외부 사용자 등 주체를 정해야 함
- 하나의 역할에는 다수의 정책을 연결할 수 있음
- 생성된 역할을 서비스 혹은 IAM 사용자 등에 연결
- Region에 국한되지 않고 사용 가능
- 신규 유저 생성시 최초에는 아무런 권한이 없으며 Access Key와 Secret Access Key가 할당됨
- 각 키는 최초 생성시에만 볼 수 있으며 즉시 보관해야 함

* 그룹 & 사용자
- 사용자는 IAM 사용자를 의미하여 관리자 계정에 의해 부여받은 권한에 한해 제한된 서비스에 접근할 수 있는 계정을 의미함
- 콘솔 로그인과 프로그래밍 액세스 가능 여부를 선택하여 생성 가능
- 콘솔 로그인이 승인된 경우, 별도의 링크를 통해 콘솔에 로그인 할 수 있음
- 각 사용자마다 정책을 부여할 수 있음
- 사용자 모두에게 일일이 부여하기 힘들거나 그룹단위로 통제하고 싶은 경우, 'Group'을 사용할 수 있음
- 그룹은 이미 생성된 사용자와 권한을 설정할 수 있으며 그룹 내 모든 사용자는 그룹의 권한을 적용받음