04. IAM 및 AWS CLI

날짜 @2024년 8월 25일

IAM

Identity and Access Management

사용자와 그룹

- 사용자 생성 후 그룹에 배치
- 사용자는 여러 그룹에 들어갈 수 있음
- 그룹에는 사용자만 배치 가능
- 그룹에 그룹을 배치할 수 없음

❓ 사용자와 그룹을 생성하는 이유는 무엇일까?
: 계정 사용을 허용하고 권한을 부여하기 위해서

IAM 정책

- JSON 형식
- 그룹과 사용자에게 각각 권한 부여 가능
  - 인라인 정책: 사용자에게만 주는 권한
  - 여러 그룹에 포함되어 있는 사용자라면 포함된 모든 그룹의 권한을 상속 받음
- 구성 요소
  - Version
    - 버전
  - Id
    - 정책 식별자
  - Statement
    - 문장
    - Sid: 문장 Id 옵션
    - Effect: 특정 api 허용 여부
    - Principal: 특정 정책이 적용될 사용자, 계정, 역할
  - Action

        - Effect에 기반하여 허용 및 거부되는 api 호출 목록
    - Resource
        - 적용될 Action의 Resource 목록
    - Condition
        - Statement가 언제 적용될지

비밀번호 정책

- 사용자 별로 비밀번호 정책 정의 가능
- 최소 길이
- 특정 문자 요형 요구
    - 대소문자, 숫자, 특수 문자
- 비밀번호 만료 기간 설정
- 사용자가 사용하고 있는 혹은 이미 사용했던 비밀번호 제한

MFA

- 방어 메커니즘
- AWS에서는 필수로 사용해야 함
- 비밀번호와 소유한 보안 장치의 조합
- 보안 장치
    - 가상 MFA 장치
    - 물리적인 장치
        - 유니버셜 세컨트 팩터 UTF
        - 젬알토: 하드웨어 보안 토큰 장치
        - SurePassId: 미국 정부 클라우드 AWS GovCloud

AWS Access

Access Key

- 관리 콘솔에서 생성 가능
- 사용자들이 각자 관리
- 비밀번호처럼 암호이기 때문에 잘 관리해야 함
- access key id = username
- secret access key = password

CLI

- 명령줄 인터페이스
- shell에서 명령어를 입력하면 명령어를 사용하여 AWS 서비스와 상호작용 할 수 있도록 해주는 도구
- AWS 서비스의 공용 api로 직접 Access 가능
- 오픈 소스

SDK

- 소프트웨어 개발 키트
- 특정 언어로 된 라이브러리의 집합
- 프로그래밍 언어에 따라 개별 sdk가 존재함
- 코딩을 통해 애플리케이션 내에 심어야 함

Cloud Shell

- AWS에서 무료로 제공하는 터미널
- UI custom 가능
- 특정 리전에서만 사용 가능

IAM Role

- AWS 서비스에 대한 권한
- 사용자 권한과 비슷하지만 실제 사람이 사용하도록 만든 것이 아닌 AWS 서비스에 사용되도록 만듦
- ec2 인스턴스는 ASW에서 특정한 작업 수행을 시도할 거고, 해당 작업을 수행하기 위해서는 ec2 인스턴스에 권한을 부여해야 함 → 이때 사용하는 것이 Role

IAM 보안 도구

- 자격 증명 보고서
- account-level
- 확인 가능한 것
  - 계정에 있는 사용자
  - 다양한 자격 증명

IAM Access 관리자

- user-level
- 확인 가능한 것
  - 사용자에게 부여된 권한
  - 마지막으로 access한 시간(= 어떤 권한이 사용되지 않는지 알 수 있음)
- 사용자의 권한을 줄여 최소 권한의 원칙을 지킬 수 있음

IAM 모범 사례

- AWS 계정을 설정할 때를 제외하고는 루트 계정 사용하지 않기
- 한 명의 AWS 사용자는 한 명의 물리적 사용자와 동일
- 자격 증명 정보 공유하지 말고 유저 생성
- 사용자를 그룹에 할당하고 그룹에 권한을 할당하여 보안이 그룹 수준에서 관리되도록 하기
- 강력한 비밀번호 정책 만들기
- 다중 인증이나 MFA 사용하기
- AWS 서비스에 권할을 부여할 때 역할을 생성하고 사용하기
- CLI 또는 일부 SDK에서 access key 필요
  - access key = password
- 계정 권한 감시는 IAM 자격 증명 보고서나 IAM 액세스 관리자 기능 사용