04. IAM 및 AWS CLI

👋 IAM
    역할1. 권한 부여
        최소 권한 원칙
        Root 보다는 IAM User를 사용하자
    역할2. 정책 관리
        정책 구조
    역할3. 보안
        방어 메커니즘
🗝️ AWS 접근하기
    액세스 키
    AWS CLI
        AWS CloudShell
👮‍♂️ IAM Role
🔐 IAM 보안 도구
    IAM 자격 증명 보고서
    IAM 액세스 관리자
🎩 IAM 모범 사례

👋 IAM

Identity and Access Management

글로벌 서비스 : 리전을 선택하지 않음

- **Root 계정** : 가입 시 기본 생성 공유X
- **사용자** : 그룹으로 묶을 수 있음
- **그룹** : 사용자만 배치 가능 (그룹 in 그룹 불가)

역할1. 권한 부여

사용자 or 그룹에 IAM 정책(`JSON`)으로 권한을 부여할 수 있다.

최소 권한 원칙

- 한 사용자가 너무 많은 서비스를 실행하여 큰 비용이 발생시키면 안되니까
- 사용자가 꼭 필요로 하는 것 이상의 권한을 주지 않는다.

Root 보다는 IAM User를 사용하자

역할2. 정책 관리

- 그룹마다 다른 정책을 만들어 관리할 수 있다.
- 사용자에게만 연결이 가능한 인라인 정책 생성 가능
- 그룹 여부에 상관없이 사용자에게 인라인 정책 사용 가능

정책 구조

- **Version**: Y-M-D
- **Id**: (선택)
- **Statement**: List 형태
  - **Sid**: 식별자(선택)
  - **Effect**: 접근 허용/거부 여부
  - **Principal**: 역할이 적용될 사용자 또는 역할
  - **Action**: Effect에 의해 허용/거부되는 API 목록
  - **Resource**: 적용될 Action의 리소스 목록
  - **Condition**: Statement가 언제 적용될 지 결정 (선택)

역할3. 보안

사용자와 그룹이 손상되지 않도록 보호한다.

방어 메커니즘

- 비밀번호 정책 정의
  - 비밀번호가 강력할수록 계정 보안 강화
  - 다양한 옵션으로 비밀번호 정책 설정 가능
    - 최소 비밀번호 길이, 문자 유형, 만료 기간, 재사용 방지 등
- **MFA**
  - 비밀번호 + 보안 장치 조합
  - 비밀번호를 도난당했거나 잃어버려도 괜찮 !

🗝️ AWS 접근하기

1. AWS Management Console
2. AWS CLI
3. AWS SDK

액세스 키

- CLI, SDK 사용을 위해 필요
- 관리 콘솔에서 생성 가능
- 사용자들이 액세스 키 직접 관리 (=비밀번호, 공유 금지)
- `Access key ID` + `Secret Access Key`

AWS CLI

CLI 권한은 IAM에서 얻는 권한과 완전히 같다.

- aws configure
- AWS access key ID 입력
- Secret access key 입력
- 기본 리전 입력

AWS CloudShell

터미널을 통해 명령을 내리는 것 대신 사용할 수 있는 대안

CloudShell 사용할 수 있는 리전이 따로 있음

장점

- 저장소 기능
  - 파일 생성 가능
  - 재접속 시에도 유지
- 구성 가능
  - 글씨 크기, 테마, 안전한 붙여넣기 등
- 파일 업로드/다운로드 가능
- 탭으로 동시에 여러 개 터미널 생성 가능

👮🏻 IAM Role

사용자와 같지만 AWS 서비스에 의해 사용되도록 만들어짐

ex) EC2 인스턴스가 AWS에 있는 다른 서비스에 접근하려는 경우

🔐 IAM 보안 도구

IAM 자격 증명 보고서

- 계정 수준에서 가능
- 계정에 있는 사용자와 자격 증명 상태 조회 가능

IAM 액세스 관리자

- 사용자 수준에서 가능
- 사용자에게 부여된 서비스 권한, 해당 서비스에 마지막으로 액세스한 시간 조회
- 최소 권한 원칙에 적합

🎩 IAM 모범 사례

- AWS 계정을 설정할 때를 제외하고 루트 계정을 사용하지 않는다.
- 한 명의 AWS 사용자는 한 명의 물리적 사용자와 매핑한다.
- 사용자를 그룹에 할당하고 그룹에 권한을 할당하여 보안이 그룹 수준에서 관리되도록 한다.
- 강력한 비밀번호 정책을 만든다.
- 다중 인증 또는 MFA를 사용한다.
- AWS 서비스에 권한을 부여할 때 역할을 생성하고 사용한다.
- 계정의 권한을 감사하기 위해 IAM 자격 증명 보고서나 IAM 액세스 관리자 기능을 사용한다.

- IAM 사용자와 액세스 키를 공유하지 않는다.