AWS 계정 vs IAM

차이점 이해하기

AWS 계정이란?

AWS Account

AWS 서비스를 사용하기 위한 **최상위 컨테이너**

- 고유한 12자리 **계정 ID** (예: 123456789012)
- 이메일 주소로 식별
- 독립적인 **비용 청구** 단위
- 리소스 격리의 기본 단위

IAM이란?

Identity and Access Management

AWS **계정 내**에서 사용자와 권한을 관리하는 서비스

- 계정에 종속됨
- 사용자, 그룹, 역할, 정책 관리
- 세분화된 권한 제어

AWS 계정 vs IAM 비교

구분	AWS 계정	IAM
레벨	최상위	계정 내부
식별	계정 ID (12자리)	사용자명/역할명
비용	청구 단위	비용 발생 안함
격리	완전 격리	권한으로 격리
생성	AWS에서 생성	계정 관리자가 생성

계정 구조

```
AWS 계정 (123456789012)
├── 루트 사용자 (이메일 로그인)
├── IAM 사용자들
│   ├── developer-kim
│   ├── developer-lee
│   └── admin-park
├── IAM 그룹
│   ├── Developers
│   └── Admins
└── IAM 역할
    ├── EC2-S3-Role
    └── Lambda-DynamoDB-Role
```

루트 사용자

Root User

AWS 계정 생성 시 자동으로 만들어지는 **최고 권한** 사용자

- 계정 이메일 + 비밀번호로 로그인
- **모든 권한** 보유 (제한 불가)
- 계정 설정 변경, 계정 삭제 가능

⚠️ 루트 사용자 주의사항

절대 일상 작업에 사용 금지

루트 사용자가 필요한 경우만:

- 최초 IAM 관리자 생성
- 계정 설정 변경 (결제 정보 등)
- 계정 폐쇄

보안 조치

- 강력한 비밀번호 + MFA 필수
- Access Key 생성 금지

IAM 사용자

IAM User

일상적인 AWS 작업을 위한 사용자

- 개인별로 생성
- 필요한 권한만 부여
- 콘솔 로그인 또는 프로그래밍 접근
- 활동 추적 가능 (CloudTrail)

AWS Organizations

여러 AWS 계정을 중앙에서 관리하는 서비스

```
Organization (조직)
├── Management Account (관리 계정)
└── Member Accounts (멤버 계정)
    ├── Development
    ├── Staging
    ├── Production
    └── Security
```

조직 개념

Organization Unit (OU)

계정들을 논리적으로 그룹화

```
Root
├── OU: Workloads
│   ├── OU: Development
│   │   └── dev-account
│   └── OU: Production
│       └── prod-account
└── OU: Security
    └── security-account
```

Service Control Policy (SCP)

조직 수준의 권한 제한

- OU 또는 계정에 적용
- IAM 정책보다 **우선** 적용
- "허용된 것만 가능" 방식

```
{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "ec2:Region": "ap-northeast-2"
    }
  }
}
```

다중 계정 전략

왜 계정을 분리하나요?

목적	설명
환경 분리	개발 실수가 프로덕션에 영향 없음
비용 추적	프로젝트/팀별 비용 명확히 구분
보안 격리	침해 시 영향 범위 최소화
규정 준수	민감 데이터 별도 계정에서 관리

일반적인 계정 구조

계정	용도
Management	Organizations 관리, 통합 결제
Security	보안 로그, 감사
Shared Services	공통 인프라 (CI/CD, VPN)
Development	개발 환경
Staging	테스트 환경
Production	운영 환경

비용 관련 사항

통합 결제 (Consolidated Billing)

- 모든 계정의 비용이 **관리 계정**에 청구
- 볼륨 할인 혜택 공유
- 계정별 비용 리포트 제공

IAM은 무료

- IAM 사용자/그룹/역할/정책 생성: **무료**
- AWS 서비스 사용량만 과금

요약

1. **AWS 계정**은 리소스와 비용의 기본 단위
    - 12자리 고유 ID로 식별
2. **IAM**은 계정 내 사용자/권한 관리
    - 계정에 종속됨
3. **루트 사용자**는 일상 작업에 사용 금지
    - MFA 필수, Access Key 금지
4. **AWS Organizations**로 다중 계정 관리
    - SCP로 조직 수준 권한 제어

다음 세션 예고

MFA 설정 및 모범 사례

다중 인증(MFA) 설정 방법과 보안 강화 방법을 알아봅니다

질문 있으신가요?