IAM 실습

IAM(Identity and Access Management)은 클라우드 환경에서 중요한 보안 요소입니다. IAM을 통해 사용자의 접근 권한을 관리하고, 자원에 대한 세부적인 액세스 제어를 설정할 수 있습니다. 아래는 IAM을 활용한 시나리오와 실습 예시입니다.

시나리오 1: 개발팀과 운영팀의 역할 기반 접근 제어 설정

배경:
회사 A는 AWS를 사용하여 애플리케이션을 개발하고 운영합니다. 개발팀과 운영팀이 각각 존재하며, 각 팀은 서로 다른 AWS 자원에 접근할 필요가 있습니다. 회사는 각 팀에 필요한 권한만 부여하여 보안을 강화하고자 합니다.

목표:

- 개발팀은 S3 버킷에만 접근할 수 있고, 새로운 버킷을 생성할 수 있도록 합니다.
- 운영팀은 EC2 인스턴스에만 접근할 수 있으며, 인스턴스를 시작하고 중지할 수 있도록 합니다.

실습:

1. **IAM 사용자 및 그룹 생성**
    - AWS Management Console에 로그인합니다.
    - IAM 서비스로 이동하여 "그룹"을 선택하고, "개발팀"과 "운영팀" 그룹을 생성합니다.
    - 각 그룹에 해당하는 IAM 사용자를 생성합니다. 예를 들어, "dev_user1"과 "ops_user1"을 생성하고, 각각 개발팀과 운영팀 그룹에 추가합니다.
2. **IAM 정책 생성 및 할당**
    - 개발팀용 정책 생성:
        - IAM에서 "정책"을 선택하고, "정책 생성"을 클릭합니다.
        - JSON 탭에서 아래와 같은 정책을 입력합니다:

```
json코드 복사
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

    - 이 정책을 "개발팀 S3 접근"이라는 이름으로 저장하고, 개발팀 그룹에 할당합니다.

- 운영팀용 정책 생성:
    - 같은 방식으로, 아래와 같은 정책을 생성합니다:

```
json코드 복사
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

    - 이 정책을 "운영팀 EC2 접근"이라는 이름으로 저장하고, 운영팀 그룹에 할당합니다.

3. **권한 테스트**
    - "dev_user1"으로 로그인하여 S3 버킷에 접근할 수 있고, 새로운 버킷을 생성할 수 있는지 확인합니다. EC2 인스턴스에 접근하려고 시도해 보지만, 권한이 없다는 메시지가 표시될 것입니다.
    - "ops_user1"으로 로그인하여 EC2 인스턴스를 시작하고 중지할 수 있는지 확인합니다. S3 버킷에 접근하려고 시도해 보지만, 권한이 없다는 메시지가 표시될 것입니다.

시나리오 2: MFA(Multi-Factor Authentication) 활성화

배경:
회사 B는 보안 강화를 위해 IAM 사용자가 로그인할 때 다단계 인증(MFA)을 요구하고자 합니다. 이를 통해 사용자 계정의 보안을 강화합니다.

목표:

- IAM 사용자 "admin_user"에게 MFA를 설정하여, 로그인 시 추가 인증을 요구합니다.

실습:

1. **MFA 장치 설정**
    - AWS Management Console에 로그인하고, IAM 서비스로 이동합니다.
    - "사용자" 메뉴에서 "admin_user"를 선택합니다.
    - "보안 자격 증명" 탭으로 이동하여 "MFA" 섹션에서 "MFA 디바이스 할당"을 클릭합니다.
    - 가상 MFA 장치를 선택하고, Google Authenticator와 같은 MFA 애플리케이션을 사용하여 QR 코드를 스캔합니다.
    - MFA 코드 두 개를 입력하여 설정을 완료합니다.
2. **로그인 시도 및 MFA 확인**
    - "admin_user"로 AWS 콘솔에 다시 로그인합니다.
    - 사용자 이름과 비밀번호를 입력한 후, 추가로 MFA 코드를 입력하도록 요구될 것입니다. MFA 코드를 올바르게 입력하면 로그인할 수 있습니다.

시나리오 3: S3 버킷에 대한 특정 IP 주소에서만 접근 허용

배경:
회사 C는 특정 S3 버킷에 대한 접근을 제한하려고 합니다. 이 버킷은 회사 내부 네트워크에서만 접근할 수 있도록 설정하여 외부에서의 불법 접근을 방지하고자 합니다.

목표:

- 특정 S3 버킷에 대해 회사의 IP 주소(예: `203.0.113.0/24`)에서만 접근 가능하도록 설정합니다.

실습:

1. **S3 버킷 정책 생성**
    - AWS Management Console에서 S3 서비스를 선택하고, 대상 버킷으로 이동합니다.
    - "권한" 탭에서 "버킷 정책"을 추가합니다.
    - 아래와 같은 정책을 추가합니다:

```
json코드 복사
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::example-bucket",
        "arn:aws:s3:::example-bucket/*"
      ],
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        }
      }
    }
  ]
}
```

    - 이 정책은 특정 IP 주소 범위 이외의 모든 접근을 거부합니다.

2. **정책 테스트**
    - 회사 내부 네트워크(해당 IP 범위 내)에서 S3 버킷에 접근해봅니다. 정상적으로 접근할 수 있어야 합니다.
    - 외부 네트워크(예: 모바일 데이터, 다른 네트워크)에서 동일한 S3 버킷에 접근해봅니다. 접근이 거부되어야 합니다.

이러한 시나리오와 실습을 통해 IAM의 다양한 기능을 이해하고, 보안 관리와 권한 설정을 실제로 체험할 수 있습니다. IAM은 매우 강력한 도구이므로, 이러한 실습을 통해 기업 내에서 더 안전하고 효율적으로 사용할 수 있을 것입니다.