IAM 및 S3 권한 제어 정책 상세 설계 보고서

---

1. 과제 개요

본 보고서는 IAM 사용자 user01에게 EC2 및 S3 자원에 대해 **세분화된 권한을 부여하고 제어**하기 위한 정책 설계 결과를 정리한 것입니다.

요구사항에 따라 다음의 요소를 반영하여 설계하였습니다:

- IAM 정책: EC2 및 S3 작업에 대한 사용자 권한 정의
- S3 리소스 정책: 특정 버킷에 대한 업로드 허용
- 경계 정책(Permissions Boundary): EC2 특정 인스턴스에 한정하여 제어 가능하도록 설정
- AWS 정책 평가 우선순위 및 보안 원칙 고려

---

2. 정책 설계 요구사항 정리

구분	세부 요구사항
EC2	- 모든 EC2 작업 중 정보 조회(읽기), 인스턴스 생성, 삭제, 시작/중지 권한 부여 - 단, **특정 인스턴스에만** start/stop 작업 허용
S3	- 지정된 S3 버킷에만 객체 업로드 가능하게 설정 - 나머지 버킷은 접근 제한
보안 원칙	- 최소 권한 원칙 적용 - 리소스 범위, 조건 기반 제한 설정 - 정책 간 우선순위 명확히 이해

---

3. 정책 구성 및 상세 설명

3.1 IAM 사용자 정책 (user01에 직접 부여)

■ **EC2 및 S3에 대한 일반 권한 부여**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2FullExceptRestricted",
            "Effect": "Allow",
            "Action": [
                "ec2:Describe*",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3LimitedAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::my-project-bucket",
```

```
            "arn:aws:s3:::my-project-bucket/*"
        ]
    }
  ]
}
```

설명:

- **EC2 작업**: 읽기 작업(Describe*)과 인스턴스 생성/시작/중지/종료 작업을 허용
- **S3 작업**: 지정한 버킷(my-project-bucket) 내에서만 객체 업로드/다운로드 가능
- **리소스 범위 제한**을 통해 다른 S3 버킷 접근은 불가
- **IAM 정책만으로는 EC2 전체에 대한 작업이 가능하기 때문에**, 아래에 제시하는 경계 정책을 추가로 활용하여 제어

3.2 EC2 경계 정책 (Permissions Boundary)

■ 특정 인스턴스만 Start/Stop 허용 (태그 기반 제어 포함)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictStartStopToSpecificInstance",
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "arn:aws:ec2:ap-northeast-2:123456789012:instance/i-
0123456789abcdef0"
```

```
    },
    {
      "Sid": "DenyStartStopElsewhere",
      "Effect": "Deny",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:ResourceTag/Owner": "user01"
        }
      }
    }
  ]
}
```

설명:

- 특정 인스턴스(i-0123456789abcdef0)만 제어 가능하도록 허용
- 그 외 인스턴스는 Owner=user01 태그가 없다면 명시적으로 거부됨
- 경계 정책은 IAM 정책과 달리 **최대 권한의 상한선을 설정**하므로, IAM 정책에서 허용해도 이 조건을 넘지 못함
- IAM 사용자에게 이 경계 정책을 적용함으로써 실질적으로 접근 범위를 제한

3.3 S3 리소스 기반 버킷 정책 (해당 S3 버킷에 부착)

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowPutObjectToUser01",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/user01"
         },
         "Action": "s3:PutObject",
         "Resource": "arn:aws:s3:::my-project-bucket/*"
      }
   ]
}
```

설명:

- user01만 해당 버킷에 객체 업로드 가능
- Principal 필드로 특정 사용자에게만 허용
- IAM 정책과 S3 버킷 정책이 **모두 허용**할 때만 권한이 부여됨 (교차 조건 만족)
- 타 사용자는 이 정책에 포함되지 않으므로 업로드 불가

---

4. AWS 권한 평가 흐름 이해

AWS는 IAM 및 리소스 기반 정책을 동시에 평가하며, 다음과 같은 우선순위 원칙을 따릅니다:

순서	평가 원칙
1	명시적 Deny가 존재하면 **무조건 거부**
2	명시적 Allow가 있어야 **허용**
3	정책이 존재하지 않으면 기본적으로 **거부**
4	Permissions Boundary가 설정된 경우, IAM 정책이 허용해도 Boundary를 넘지 못하면 **거부**

---

5. 실무 적용 예시 및 기대 효과

- 사용자는 EC2의 상태 확인, 인스턴스 생성/제어 작업 수행 가능
- 특정 인스턴스에 대해서만 시작/중지 가능 → **운영 인프라 보호**
- S3 버킷도 지정된 버킷에만 객체 업로드 가능 → **데이터 보안 강화**
- IAM 정책과 경계 정책, 리소스 정책을 **조합**함으로써 **정교한 권한 관리 실현**

---

6. 결론

본 보고서는 AWS의 권한 관리 정책을 구성할 때 필요한 세 가지 축(IAM 정책, 경계 정책, 리소스 정책)을 모두 반영하여 user01의 EC2 및 S3 접근을 **최소 권한 원칙에 맞춰 제한적으로 허용**하도록 설계하였습니다.

- EC2에 대해서는 작업별/인스턴스별로 조건 설정
- S3에 대해서는 버킷 단위로 업로드 권한을 제한
- 정책 우선순위 및 조건 기반 필터링을 명확하게 반영

이러한 방식은 실무에서 계정 오용, 과도한 권한, 실수로 인한 서비스 중단을 방지하기 위한 강력한 보안 수단으로 활용됩니다.