IAM 정책 및 S3 버킷 정책 분석 보고서

1. 문제 개요

AWS 환경에서 user01에게 특정 권한이 부여된 상태에서, 해당 유저가 어떤 S3 작업을 실제로 수행할 수 있는지 확인해야 합니다.
이를 위해 두 가지 정책이 존재하며, 다음과 같은 조건을 따릅니다:

- **IAM 사용자 정책**: user01에게 부여된 정책 (Identity-based policy)
- **S3 버킷 정책**: 특정 리소스(S3)에 설정된 리소스 기반 정책 (Resource-based policy)

---

2. 정책 상세 내용

부여된 IAM 정책 (Allow)

```
{
   "Effect": "Allow",
   "Action": "s3:*",
   "Resource": "*"
}
```

해석:

- **Effect**: 허용(Allow)
- **Action**: s3:* → S3 서비스의 **모든 작업** 허용
- **Resource**: * → 모든 S3 리소스에 대해 적용됨

이 정책만 보면 user01은:

- S3 버킷 생성(s3:CreateBucket)
- 객체 업로드(s3:PutObject)
- 객체 다운로드(s3:GetObject)
- 버킷 리스트 조회(s3:ListBucket)
- 삭제, 태깅, 권한 수정 등... 모든 S3 작업이 가능

적용된 S3 버킷 정책 (Deny)

```
{
   "Effect": "Deny",
   "Principal": "user01",
   "Action": "s3:PutObject",
   "Resource": "*"
}
```

해석:

- **Effect**: 거부(Deny)
- **Principal**: user01 → 이 정책은 오직 user01에게만 적용됨
- **Action**: s3:PutObject → 객체 업로드 작업만 명시적으로 거부
- **Resource**: * → 모든 S3 버킷/객체에 대해 적용

핵심 요약:

- user01은 **객체 업로드(파일 저장)** 만 불가능함
- 나머지 액션은 이 정책에서 영향을 받지 않음

---

3. 정책 충돌 시 우선순위

정책 종류	정책	결과 설명
IAM 정책	Allow	user01이 모든 S3 작업 가능
S3 버킷 정책	Deny	단, s3:PutObject는 명시적으로 거부됨

정책 충돌 시 Deny가 우선됨
즉, 아무리 IAM 정책이 허용하더라도 S3 버킷 정책에서 명시적 거부가 있으면 **해당 액션은 거부**됩니다.

---

4. user01의 실제 권한 정리

서비스 액션	허용 여부	사유
s3:ListBucket	허용됨	IAM 정책에서 명시적 허용, S3 정책에 거부 없음
s3:GetObject	허용됨	객체 다운로드 허용됨
s3:PutObject	거부됨	S3 버킷 정책에서 명시적 거부
s3:DeleteObject	허용됨	거부 정책 없음
s3:CreateBucket	허용됨	IAM 정책에서 허용
ec2:DescribeInstances	거부됨	IAM 정책에 EC2 관련 권한 없음

---

5. 결론 및 요약

- user01은 IAM 정책에 의해 S3에 대한 모든 권한을 갖지만,
  S3 리소스 자체에서 PutObject를 명시적으로 거부하기 때문에
  객체 업로드는 불가능합니다.
- 다른 S3 작업은 가능하며, EC2 같은 S3 외 서비스는 허용되지 않습니다.
- AWS의 권한 평가 방식에서는 **"Deny가 항상 우선"**이며,
  실제 권한은 IAM 정책과 리소스 정책의 교차 분석을 통해 결정됩니다.