IAM 및 S3 버킷 정책 분석을 통한 권한 평가

user01의 액션 허용 여부를 정책 예시로 분석

IAM 유저 user01에게는 다음과 같은 IAM 정책, S3 버킷 정책이 구성되어 있습니다. 유저 user01이 할 수 있는 작업에 대하여 정리하는 보고서입니다.

IAM 정책	"Effect": "Allow", "Action": "s3:*", "Resource": "*"
S3 버킷 정책	"Effect": "Deny", "Principal": "user01", "Action": "s3:PutObject", "Resource": "*"

1. **IAM 정책**
   Effect는 허용 및 거부, Action은 서비스 특정 작업, Resource는 리소스 이름을 나타냅니다. 유저 user01은 S3의 모든 작업, 즉 객체 다운로드 및 업로드가 가능하며 버킷 내 모든 객체에 접근할 수 있습니다.
2. **S3 버킷 정책**
   Principal은 S3 버킷 정책에만 있는 속성이며 보안 주체를 나타냅니다. 유저 user01은 S3의 PutObject 즉, 객체 업로드는 명시적으로 거부되었습니다. AWS 권한 평가 시, 명시적 거부는 허용보다 우선 적용되므로 해당 작업은 IAM 정책에서 허용되더라도 실행할 수 없습니다. 다른 액션들에 대해서는 별도로 거부 항목이 없으므로 IAM 정책에 따라 허용될 수 있습니다.