**IAM 및 S3 권한 설정을 통한 세분화된 접근 제어**

EC2 작업과 S3 업로드 권한을 조건에 맞게 정책으로 구현하고 경계 정책으로 제한 설정

IAM 유저 user01에게 식별된 권한의 내용대로 IAM 정책 및 버킷 정책을 생성하는 보고서입니다.

1. **IAM 정책**  
   EC2에 대한 작업 중 EC2의 모든 작업을 허가하도록 설정합니다.

|  |  |
| --- | --- |
| IAM 정책 구문 | "Effect": "Allow",  "Action": "ec2:\*",  "Resource": "\*" |

1. **S3 버킷 정책**  
   파일 업로드를 가능하게 하도록 권한을 설정합니다.

|  |  |
| --- | --- |
| S3 버킷 정책 구문 | "Effect": "Allow",  "Principal": "user01",  "Action": "s3:PutObject",  "Resource": "\*" |

1. **권한 경계 정책**  
   특정 EC2의 Stop/Start만 허용하도록 권한 경계를 설정합니다. 권한 경계는 IAM 주체가 수행할 수 있는 작업의 최대 허용 범위를 정의하며 명시적 허용 조건으로만 구성되어야 합니다.

|  |  |
| --- | --- |
| 권한 경계 정책 구문 | "Effect": "Allow",  "Action": [  "ec2:StartInstances",  "ec2:StopInstances"  ],  "Resource": "\*",  "Condition": {  "StringEquals": {  "ec2:ResourceTag/Name": "allowed-instance"  }  } |