

* Cloudtrail 이란?

- AWS 계정 내에서 이루어지는 모든 작업과 활동에 대해 기록하는 서비스
- 계정 내에서 이루어지는 API 호출도 모두 기록함
- AWS 계정 생성시 자동으로 활성화되며 최대 90 일간의 기록을 볼 수 있음
- 최근 이벤트를 확인할 수 있는 이벤트 기록, '추적' 기능, Insight 이벤트로 이루어짐

* 추적

- '추적'을 활성화하면 모든 리전 혹은 선택한 리전에 대하여 활동기록을 기록하고 S3 Bucket 에 보관할 수 있음
- Organization 와 연동하여 사용가능하며 자신의 '조직'을 선택하면 조직 내 모든 계정을 추적할 수 있음
- Insight 이벤트는 write API 호출에 관련된 비정상적인 호출을 탐지함