Samsung Cloud Platform

Management

IAM(Identity and Access Management)

엔터프라이즈 레벨의 자격증명 및 접근권한 관리 서비스

IAM은 Samsung Cloud Platform에 등록된 사용자의 본인 여부 확인 및 접근권한 부여를 통해 Account 내에서 서비스 및 자원에 접근 가능한 범위를 제어하는 서비스 입니다. Account 관리자는 IAM을 통해 사용자, 사용자 그룹, 정책, 역할 항목을 상세히 관리할 수 있으며, 대시보드를 통해 Account내의 권한 부여 현황을 한눈에 파악하고 제어할 수 있습니다.

강력한 사용자 인증

콘솔 및 API 접근 시 사용자는 다중인증(MFA; Multi-Factor Authentication) 및 인증키 인증을 반드시 수행해야 합니다. 또한, 접근 가능한 IP 대역을 통해서만 Account에 접근이 가능하도록 허가함으로써 권한 없는 사용자의 미인가 접근을 원천 차단합니다.

손쉬운 권한 관리

Account 관리자(Root 사용자)는 사용자 및 사용자 그룹, 정책, 역할을 손쉽게 생성하여 관리할 수 있습니다. 업무 목적에 따라 사용자(IAM 사용자)를 그룹 및 역할에 매핑하여 사용자의 접근 권한을 업무에 필요한 부분으로 한정합니다.

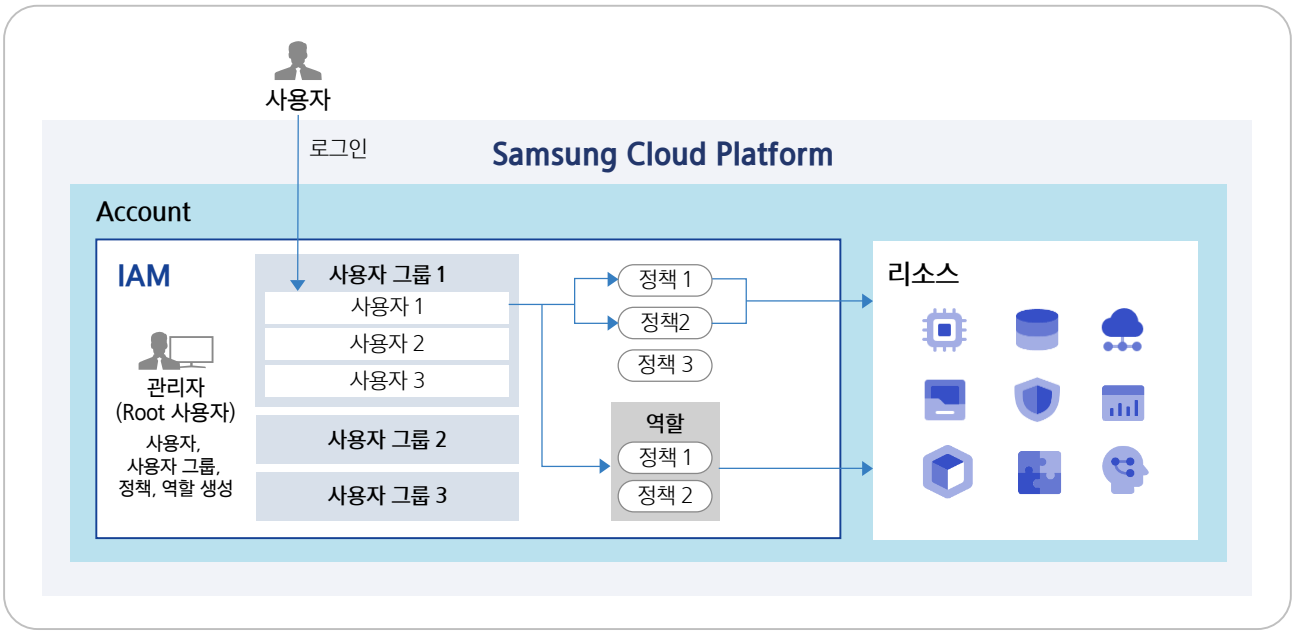
최적화된 접근제어 정책 운용

Account내의 서비스별로 세밀한 수준에서 제어/액션/자원유형 및 인증방식/IP에 대한 접근제어 정책을 만듭니다. 이를 통해 클라우드 자원에 대한 접근 권한 부여시 최소 권한 정책을 적용하여 사용자에 따른 적절한 접근 제어가 가능합니다.

임시 자격증명을 통한 접근 통제

Account 관리자는 임시 자격증명을 통한 역할을 생성하여 필요에 따라 최소한의 권한만 부여할 수 있습니다. 임시 자격증명을 통해 제한된 시간 동안 필요한 권한만을 제공함으로써, 다수의 사용자에 대해 높은 수준의 중앙 집중식 관리가 가능합니다.

서비스 구성도



주요 기능

- **회원가입 및 보안자격 증명**
  - 추가 인증을 통한 가입 및 로그인 시 MFA 적용
  - 인증키 및 IP 접근제어 기반 미인가자 접근 시도 차단
- **사용자 그룹별 권한 관리**
  - Account 기반 사용자 그룹 설정 및 정책 부여
  - 사용자 그룹별 사용자 및 정책 매핑을 통한 간편한 관리
- **접근제어 정책**
  - 서비스별 작업 유형, 개별 자원별 접근 권한에 대한 상세한 관리
  - 정책 기반 접근 IP제어, 인증방식 적용을 통한 접근 제어
- **역할 생성 및 전환**
  - Account 및 SRN(SCP Resource Number) 대상 역할 주체 설정
  - 역할 전환을 통한 임시 자격증명 부여로 보안 강화

SAMSUNG SDS

www.samsungsds.com / cloud.samsungsds.com
contact.sds@samsung.com / scp_sales@samsung.com
youtube.com/samsungsds