aws re/start

AWS 계정 생성을 위한 보안 모범 실무

교육 내용

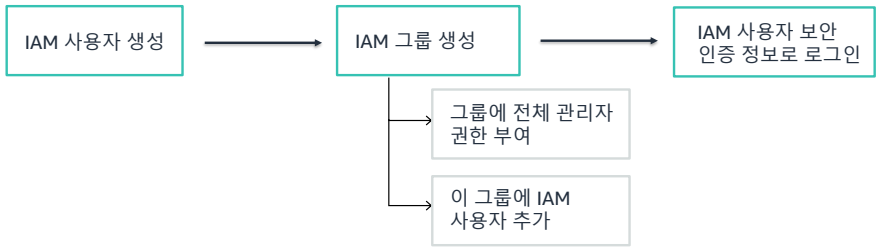
이 강의의 핵심

AWS 계정을 생성할 때 사용할 모범 실무를 설명하는 방법을 배웁니다.

새로운 AWS 계정을 설정하기 위한 모범 실무에는 무엇이 있을까요? 이 강의에서는 보안 모범 실무를 종합적으로 소개하고 모든 계정에서 따라야 하는 1일 차 모범 실무에 대한 인사이트를 제공합니다.

모범 실무(1/4): AWS 사용 1일 차

1. **AWS 계정 루트 사용자의 사용을 가능한 한 빨리 중지합니다.**



3

aws re/start

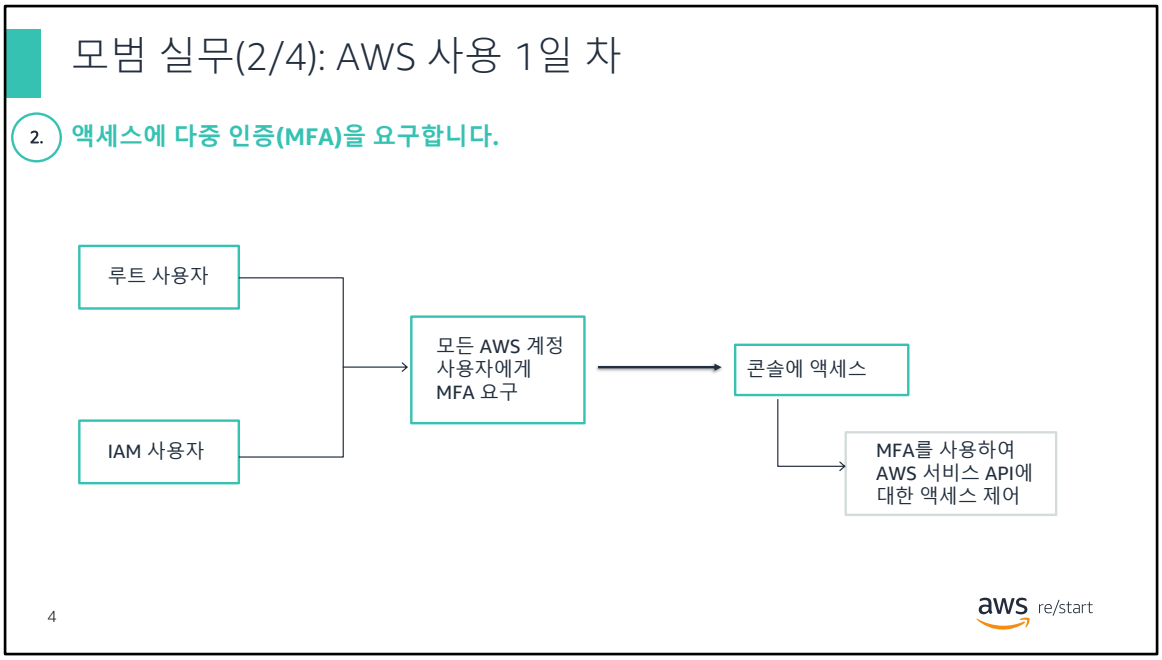
계정 루트 사용자의 액세스 키가 있다면 제거하는 것이 좋습니다. 액세스 키를 제거하기 전에 애플리케이션 내에서 액세스 키가 사용되고 있지 않은지 확인하시기 바랍니다.

AWS 계정 루트 사용자의 사용을 가능한 한 빨리 중지합니다.

계정 루트 사용자의 사용을 중지하려면 다음 단계를 수행합니다.

1. 계정 루트 사용자로 로그인하여 여러분을 위해 AWS Identity 및 Access Management(IAM) 사용자를 생성합니다.
2. IAM 그룹을 생성합니다.
   a) 그룹에 전체 관리자 권한 부여
   b) IAM 사용자를 그룹에 추가
3. IAM 사용자 보안 인증 정보로 로그인합니다.
4. 계정 루트 사용자 보안 인증 정보를 안전한 장소에 저장합니다.
5. 계정 루트 사용자 액세스 키가 있는 경우 비활성화하고 제거합니다
   .

첫 번째 IAM 사용자와 관리자 그룹 설정에 관한 자세한 내용은 **AWS Identity 및 Access Management 사용 설명서**의 첫 번째 IAM 관리 사용자 및 그룹 생성을 참조하십시오.



1. AWS 계정 루트 사용자와 모든 IAM 사용자에게 MFA를 요구합니다.
2. MFA를 사용하여 AWS 서비스 애플리케이션 프로그래밍 인터페이스(API)에 대한 액세스를 제어합니다.

소프트웨어 MFA

AWS Virtual MFA

Google Authenticator

Authy Authenticator(Windows Mobile 앱)

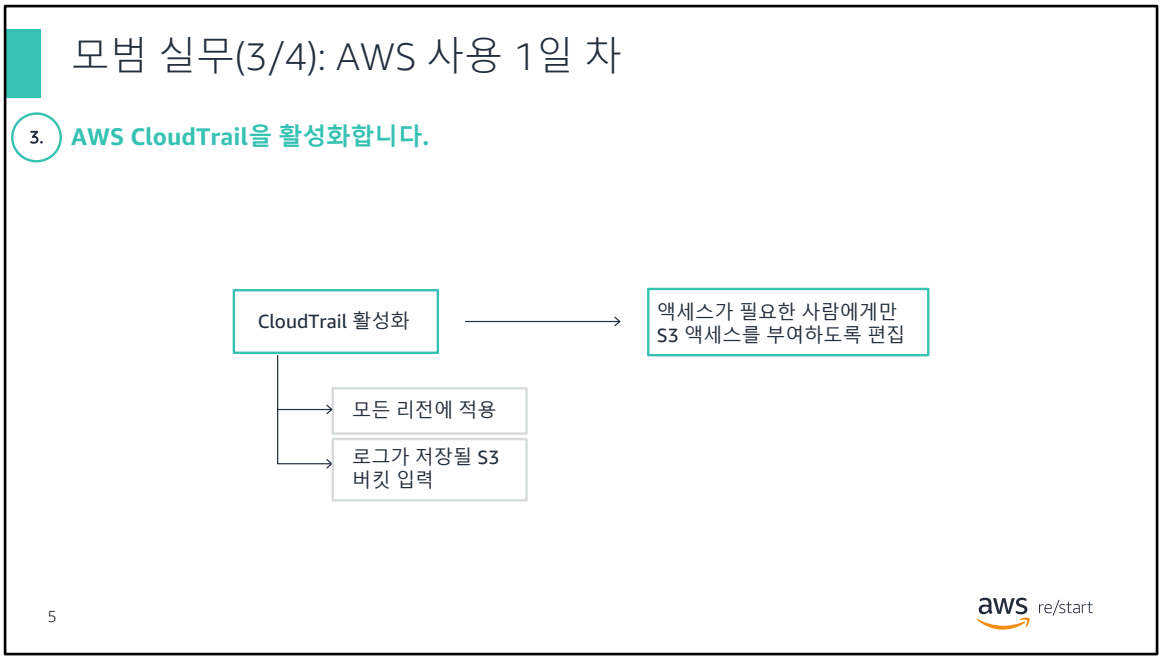
단문 메시지 서비스(SMS) 알림

하드웨어 MFA

Gemalto 전자 열쇠 또는 디스플레이 카드

Gemalto에 관한 자세한 내용은 Thales 웹 사이트의 Multi-Factor

Authentication (MFA)을 참조하십시오.



CloudTrail은 계정의 리소스에 대한 모든 애플리케이션 프로그래밍 인터페이스(API) 요청을 로깅합니다.

AWS CloudTrail을 활성화하는 방법은 다음과 같습니다.

1. 추적을 생성합니다.
    a) 추적 이름 지정
    b) 모든 리전에 추적 적용
    c) 로그가 저장될 새로운 Amazon Simple Storage Service(Amazon S3) 버킷의 이름 입력

2. 관리자와 같이 액세스가 필요한 사용자 외에는 CloudTrail에 사용하는 Amazon S3 버킷에 대한 액세스가 제한되도록 해야 합니다.

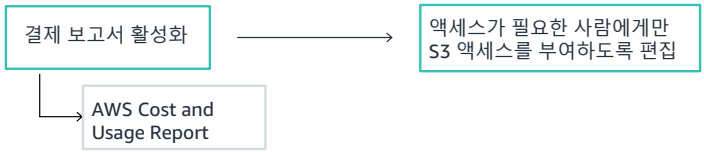
CloudTrail은 이제 모든 사용자에 대해 기본적으로 활성화됩니다. 지난 7일간의 계정 활동에 대한 가시성을 제공하며, 시작하기 위해 서비스에서 추적을 구성할 필요가 없습니다. CloudTrail을 활성화하면 CloudTrail Event History를 통해 계정 활동을 조회, 검색, 다운로드할 수 있습니다.

자세한 내용은 **AWS CloudTrail 사용 설명서**의 '추적 생성 '(http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-

create-a-trail-using-the-console-first-time.html)을 참조하십시오.

모범 실무(4/4): AWS 사용 1일 차

4. **AWS Cost and Usage Report와 같은 결제 보고서를 활성화합니다.**



aws re/start

결제 보고서는 AWS 리소스 사용에 대한 정보와 리소스 사용에 대한 추정 비용을 제공합니다. AWS는 여러분이 지정한 S3 버킷으로 보고서를 전달하며, 최소한 하루에 한 번 보고서를 업데이트합니다.

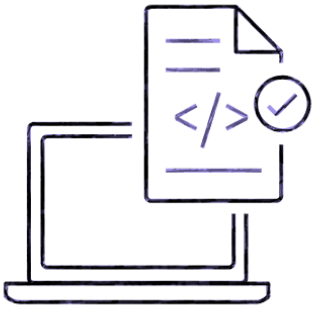
AWS Cost and Usage Report는 AWS 사용 현황을 추적합니다. 이 보고서는 AWS 계정과 관련한 추정 비용을 시간별 또는 일별로 제공합니다.

예를 들어, AWS Cost and Usage Report는 AWS 사용 현황을 추적합니다. 이 보고서는 AWS 계정과 관련한 추정 비용을 시간별 또는 일별로 제공합니다.

자세한 내용은 **Cost and Usage Report 사용 설명서**의 AWS Cost and Usage Report란 무엇입니까?를 참조하십시오.

IAM 모범 실무

- AWS 계정(루트) 액세스 키 삭제
- IAM 사용자
  - 개별 IAM 사용자 생성
  - 불필요한 사용자와 보안 인증 정보 제거
- 그룹을 사용하여 IAM 사용자에게 권한 할당
- IAM 역할
  - Amazon EC2 인스턴스에서 실행되는 애플리케이션에 역할 사용
  - 보안 인증 정보를 공유하지 않고 역할을 사용하여 위임
- 액세스 제어 강화
  - 최소 권한에 따라 액세스 권한 부여
  - 강력한 암호 정책 구성
  - 권한 있는 사용자에 대해 MFA 활성화
  - 보안 강화를 위해 정책 조건 사용
  - 보안 인증 정보 주기적으로 교체
  - AWS 계정 내 활동 모니터링



aws re/start

IAM을 사용할 때 따라야 할 모범 실무가 요약되어 있습니다.

자세한 내용은 **AWS Identity 및 Access Management 사용 설명서**의 IAM 보안 모범 실무를 참조하십시오.

핵심 사항

- **AWS 계정 루트 사용자**는 AWS 계정을 설정할 때 사용하는 이메일 주소입니다. 루트 사용자는 **전체 관리자 액세스 권한을 가집니다.**
  - **루트 사용자 보안 인증 정보를 아무에게도 공유하지 마십시오.**
  - 로그인 후에는 **AWS 계정 루트 사용자의 액세스 키**를 삭제합니다.
- 조직 내의 **개인마다 IAM 사용자**를 만듭니다.
- **항상 MFA로 AWS 계정을 보호합니다.**
- AWS 계정 내에서 **로깅을 위해 AWS CloudTrail**을 활성화하고 **사용 및 비용 정보를 수집하기 위해 결제 보고서**를 활성화합니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- AWS 계정 루트 사용자는 AWS 계정을 설정할 때 사용하는 이메일 주소입니다. 루트 사용자는 전체 관리자 액세스 권한을 가집니다.
  - 루트 사용자 보안 인증 정보를 아무에게도 공유하지 마십시오.
  - 로그인 후에는 AWS 계정 루트 사용자의 액세스 키를 삭제합니다.
- 조직 내의 개인마다 IAM 사용자를 만듭니다.
- 항상 MFA로 AWS 계정을 보호합니다.
- AWS 계정 내에서 로깅을 위해 AWS CloudTrail을 활성화하고 사용 및 비용 정보를 수집하기 위해 결제 보고서를 활성화합니다.