AWS Academy Cloud Foundations

모듈 4: AWS 클라우드 보안

모듈 개요

주제

- AWS 공동 책임 모델
- AWS Identity and Access Management(IAM)
- 새 AWS 계정 보안
- 계정 보안
- AWS의 데이터 보안
- 규정 준수 보장 작업

활동

- AWS 공동 책임 모델 활동

데모

- 녹화된 IAM 데모

실습

- AWS IAM 소개

지식 확인

모듈 목표

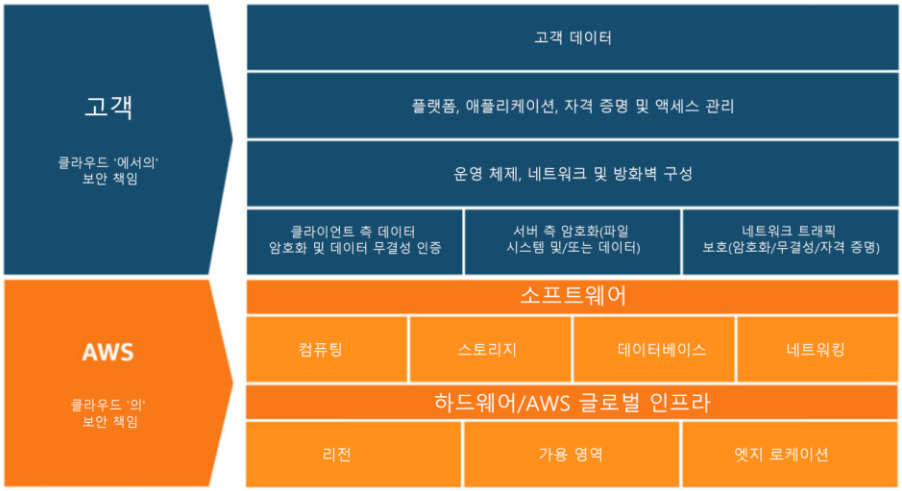
이 모듈을 마치면 다음을 수행할 수 있습니다.

- 공동 책임 모델 이해
- 고객 및 AWS의 책임 확인
- IAM 사용자, 그룹 및 역할 이해
- IAM의 다양한 보안 자격 증명 유형 설명
- 새 AWS 계정 보안을 위한 단계 확인
- IAM 사용자 및 그룹 탐색
- AWS 데이터를 보호하는 방법 이해
- AWS 규정 준수 프로그램 이해

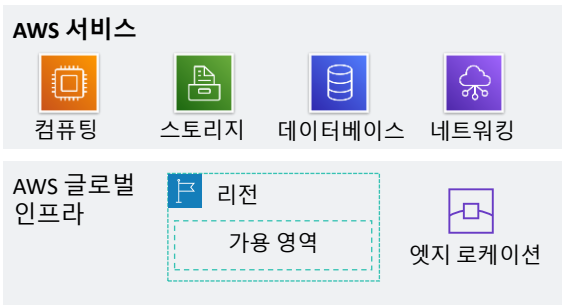
모듈 4: AWS 클라우드 보안

섹션 1: AWS 공동 책임 모델

AWS 공동 책임 모델



AWS의 책임: 클라우드 *의* 보안



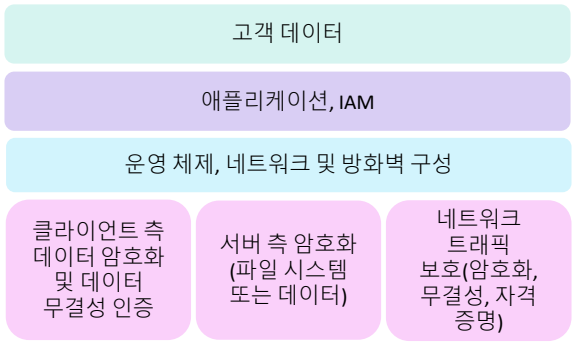
AWS의 책임:

- 데이터 센터의 물리적 보안
  - 필요 기반의 제어된 액세스

- 하드웨어 및 소프트웨어 인프라
  - 스토리지 폐기, 호스트 OS(운영 체제) 액세스 로깅 및 감사
- 네트워크 인프라
  - 침입 탐지

- 가상화 인프라
  - 인스턴스 격리

고객의 책임: 클라우드 *에서*의 보안

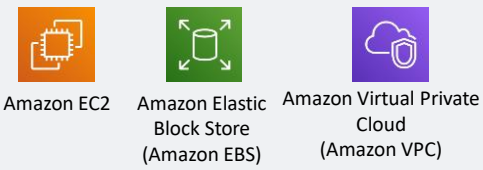


고객의 책임:

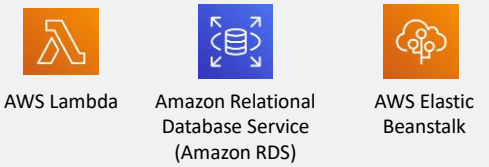
- Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 운영 체제
  - 패치 적용, 유지 관리 등
- 애플리케이션
  - 암호, 역할 기반 액세스 등
- 보안 그룹 구성
- OS 또는 호스트 기반 방화벽
  - 침입 탐지 또는 차단 시스템 등
- 네트워크 구성
- 계정 관리
  - 각 사용자에 대한 로그인 및 권한 설정

서비스 특성 및 보안 책임

고객이 관리하는 서비스의 예



AWS에서 관리하는 서비스의 예



IaaS(서비스형 인프라)

- 고객은 네트워킹 및 스토리지 설정을 보다 유연하게 구성할 수 있음
- 보안의 더 많은 측면을 고객이 관리해야 함
- 액세스 제어를 고객이 구성

PaaS(서비스형 플랫폼)

- 고객이 기본 인프라를 관리할 필요가 없음
- 운영 체제, 데이터베이스 패치 적용, 방화벽 구성 및 재해 복구를 AWS가 처리
- 고객은 코드 또는 데이터 관리에 집중할 수 있음

서비스 특성 및 보안 책임(계속)

SaaS의 예

AWS Trusted Advisor

AWS Shield

Amazon Chime

SaaS(서비스형 소프트웨어)

- 소프트웨어가 중앙에서 호스팅됨
- 구독 모델 또는 종량 과금제로 라이선스가 부여됨
- 일반적으로 웹 브라우저, 모바일 앱 또는 API(애플리케이션 프로그래밍 인터페이스)를 통해 서비스에 액세스함
- 고객은 서비스를 지원하는 인프라를 관리할 필요가 없음

활동: AWS 공동 책임 모델

사진 출처: Pexels의 Pixabay

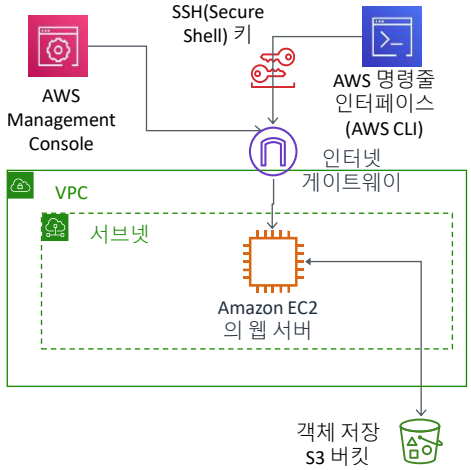
활동: 시나리오 1/2

다음 배포에서 책임은 누구에게 있습니까(AWS 또는 고객)?

1. EC2 인스턴스의 운영 체제에 대한 업그레이드 및 패치
   - **답:** 고객
2. 데이터 센터의 물리적 보안
   - **답:** AWS
3. 가상화 인프라
   - **답:** AWS
4. EC2 보안 그룹 설정
   - **답:** 고객
5. EC2 인스턴스에서 실행되는 애플리케이션의 구성
   - **답:** 고객
6. Oracle 인스턴스가 Amazon RDS 인스턴스로 실행되는 경우 Oracle 업그레이드 또는 패치
   - **답:** AWS
7. Oracle이 EC2 인스턴스에서 실행되는 경우 Oracle 업그레이드 또는 패치
   - **답:** 고객
8. S3 버킷 액세스 구성
   - **답:** 고객

활동: 시나리오 2/2

다음 배포에서 책임은 누구에게 있습니까(AWS 또는 고객)?



1. AWS Management Console에 대한 해킹 차단
   - **답:** AWS
2. 서브넷 구성
   - **답:** 고객
3. VPC 구성
   - **답:** 고객
4. AWS 리전의 네트워크 중단에 대한 보호
   - **답:** AWS
5. SSH 키 보안
   - **답:** 고객
6. AWS 고객 데이터 간의 네트워크 격리 보장
   - **답:** AWS
7. 웹 서버와 S3 버킷 간에 지연 시간이 짧은 네트워크 연결 보장
   - **답:** AWS
8. 모든 사용자 로그인에 대해 Multi-Factor Authentication (다 요소 인증)적용
   - **답:** 고객

섹션 1 핵심 사항

- AWS와 고객은 공동으로 보안을 책임집니다.
  - AWS는 클라우드의 보안을 책임집니다.
  - 고객은 클라우드에서의 보안을 책임집니다.
- **AWS는 AWS 클라우드 서비스를 실행하는 인프라**(하드웨어, 소프트웨어, 네트워킹 및 시설 등)를 보호할 책임이 있습니다.
- IaaS(서비스형 인프라)로 분류되는 서비스의 경우 **고객은 필요한 보안 구성 및 관리 작업을 수행할 책임이 있습니다.**
  - 예: 게스트 OS 업데이트 및 보안 패치, 방화벽, 보안 그룹 구성

모듈 4: AWS 클라우드 보안

섹션 2: AWS Identity and Access Management(IAM)

AWS Identity and Access Management(IAM)

- IAM을 사용하여 AWS 리소스에 대한 액세스 관리 –
  - 리소스는 사용자가 작업을 수행할 수 있는 AWS 계정의 엔터티입니다.
  - 리소스의 예로는 Amazon EC2 인스턴스 또는 Amazon S3 버킷이 있습니다.
- 예 – Amazon EC2 인스턴스를 종료할 수 있는 사용자 제어
- 세분화된 액세스 권한 정의 –
  - 리소스에 액세스할 수 있는 사용자
  - 액세스할 수 있는 리소스와 사용자가 리소스에 수행할 수 있는 작업
  - 리소스에 액세스하는 방법
- IAM은 AWS 계정에 무료로 제공되는 기능입니다.

AWS Identity and Access Management (IAM)

IAM: 필수 구성 요소

AWS 계정으로 인증할 수 있는 사람 또는 애플리케이션입니다.

동일한 권한 부여를 허락 받은 IAM 사용자의 모음입니다.

액세스할 수 있는 리소스와 각 리소스에 대한 액세스 수준을 정의하는 문서입니다.

AWS 서비스 요청을 위한 권한 세트를 부여하는 유용한 메커니즘입니다.

액세스 가능한 IAM 사용자로 인증합니다.

IAM 사용자**를 정의할 때 이 사용자가 사용할 수 있는** 액세스 유형**을 선택합니다.**

프로그래밍 방식 액세스

- 인증 방법:
  - 액세스 키 ID
  - 보안 액세스 키
- AWS CLI 및 AWS SDK 액세스 제공

AWS CLI

AWS 도구 및 SDK

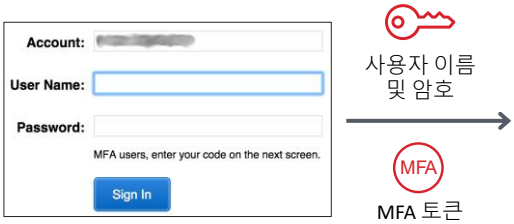
AWS Management Console 액세스

- 인증 방법:
  - 12자리 계정 ID 또는 별칭
  - IAM 사용자 이름
  - IAM 암호
- 활성화하면 **MFA(Multi-Factor Authentication)**에 의해 인증 코드를 입력하라는 메시지가 표시됩니다.

AWS Management Console

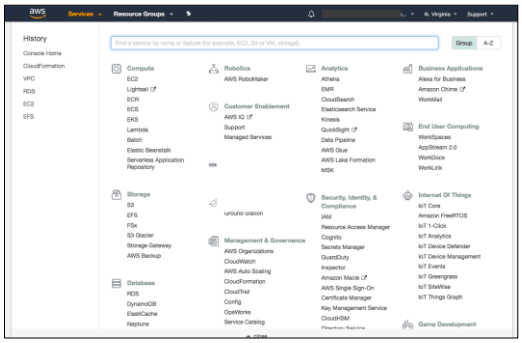
IAM MFA

- MFA는 보안을 향상시킵니다.
- MFA를 사용하는 경우 사용자 이름과 암호에 추가로 고유한 인증 코드를 제공해야 AWS 서비스에 액세스할 수 있습니다.



사용자 이름 및 암호

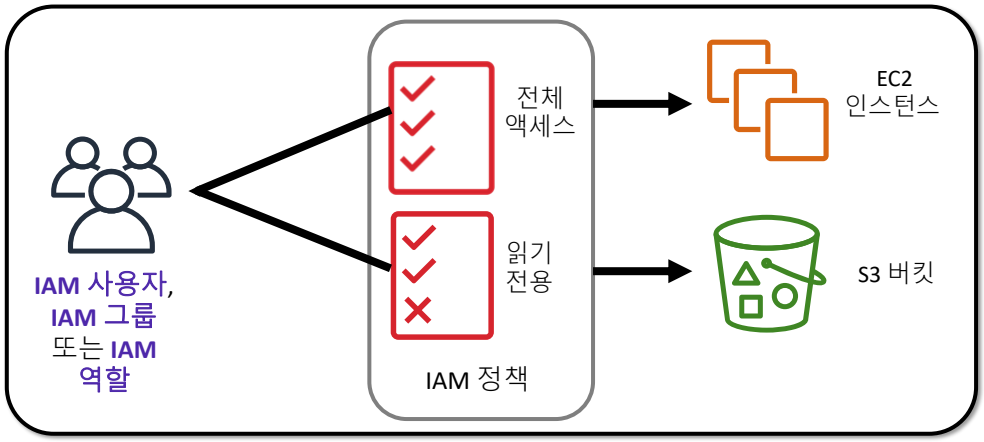
MFA 토큰



AWS Management Console

권한 부여: 허용되는 작업

AWS 계정에 연결한 사용자 또는 애플리케이션에 허용되는 작업은 무엇입니까?



IAM: 권한 부여

- IAM 정책을 생성하여 권한을 할당합니다.
- 권한은 허용되는 **리소스와 작업**을 결정합니다.
  - 기본적으로 모든 권한은 암시적으로 거부됩니다.
  - 명시적으로 거부된 항목은 절대 허용되지 않습니다.

모범 사례: **최소 권한의 원칙**을 따릅니다.

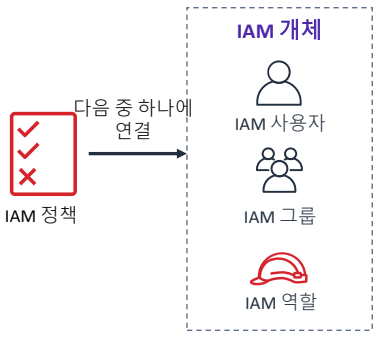
IAM 권한

참고: IAM 서비스 구성의 범위는 **글로벌**입니다. 설정은 모든 AWS 리전에 적용됩니다.

여기부터

IAM 정책

- **IAM** 정책은 권한을 정의하는 문서
  - 세분화된 액세스 제어가 가능함
- 2가지 유형의 정책 - 자격 증명 기반 및 리소스 기반
- 자격 증명 기반 정책 –
  - 정책을 모든 IAM 엔터티에 연결
    - IAM 사용자, IAM 그룹 또는 IAM 역할
  - 정책은 다음을 지정합니다.
    - 엔터티가 **수행할 수 있는** 작업
    - 엔터티가 **수행할 수 없는** 작업
  - 단일 정책을 여러 엔터티에 연결할 수 있음
  - 단일 엔터티에 여러 정책을 연결할 수 있음
- 리소스 기반 정책
  - 리소스(예: S3 버킷)에 연결됨



IAM 정책 예제

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action":["DynamoDB:*","s3:*"],
    "Resource":[
      "arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

명시적 허용은 사용자에게 특정 DynamoDB 테이블과...

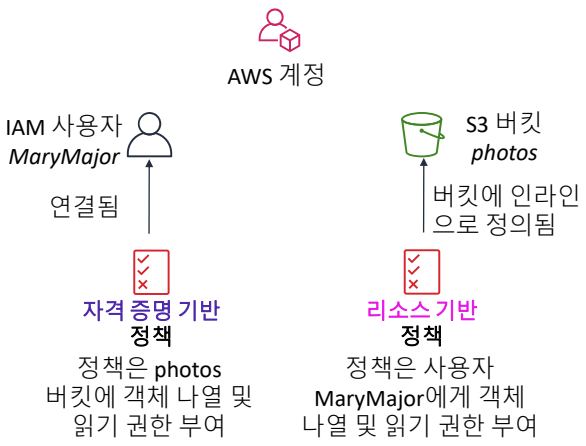
...Amazon S3 버킷에 대한 액세스 권한을 부여합니다.

명시적 거부 는 사용자가 테이블과 해당 버킷을 제외하고 다른 AWS 작업 또는 리소스를 사용할 수 없게 합니다.

명시적 거부문은 허용문보다 **우선** 적용됩니다.

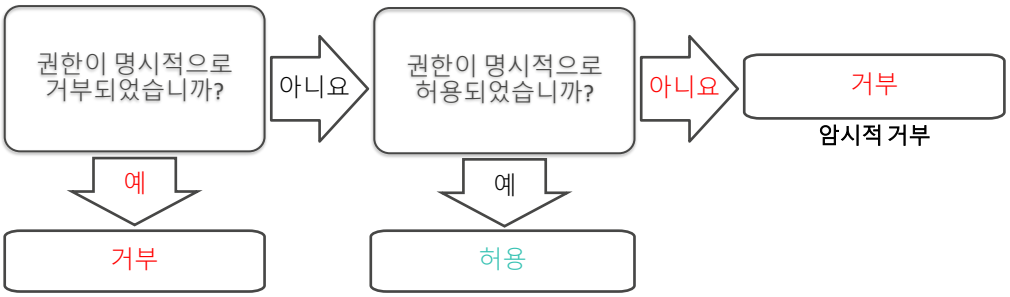
리소스 기반 정책

- 자격 증명 기반 정책은 사용자, 그룹 또는 역할에 연결됨
- 리소스 기반 정책은 리소스에 *연결됨*(사용자, 그룹 또는 역할에 연결되지 않음)
- 리소스 기반 정책의 특성 –
  - 리소스에 액세스할 수 있는 사용자와 해당 사용자가 수행할 수 있는 작업 지정
  - 인라인 전용 정책이며 관리형은 없음
- 리소스 기반 정책은 일부 AWS 서비스에서만 지원됨



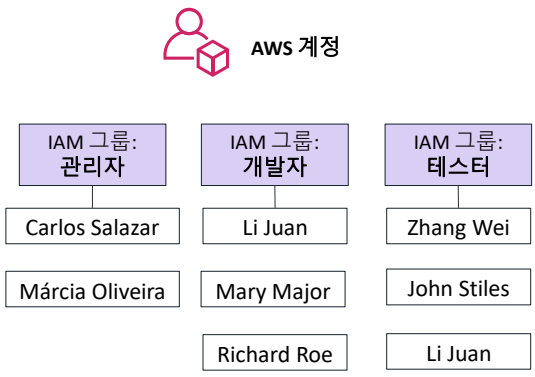
IAM 권한

IAM에서 권한을 결정하는 방법:



IAM 그룹

- IAM 그룹은 **IAM 사용자의 모음**
- 그룹은 여러 사용자에게 동일한 권한을 부여하는 데 사용됨
  - IAM 정책을 그룹에 연결하여 권한을 부여함
- 한 사용자가 여러 그룹에 속할 수 있음
- 기본 그룹은 없음
- 그룹을 중첩할 수 없음



IAM 역할

- IAM 역할은 **특정 권한이 있는 IAM 자격 증명**
- IAM 사용자와 유사함
  - 권한 정책을 IAM 역할에 연결
- IAM 사용자와 다름
  - 한 사람에게 고유하게 연결되지 않음
  - 개인, 애플리케이션 **또는** 서비스**가 역할을** 수임**할 수 있음**
- 역할은 임시 보안 자격 증명을 제공함
- IAM 역할을 사용하여 액세스 권한을 위임하는 방법의 예 –
  - 역할과 동일한 AWS 계정의 IAM 사용자가 사용
  - 역할과 동일한 계정의 AWS 서비스(예: Amazon EC2)에서 사용
  - 역할과 다른 AWS 계정의 IAM 사용자가 사용

IAM 역할

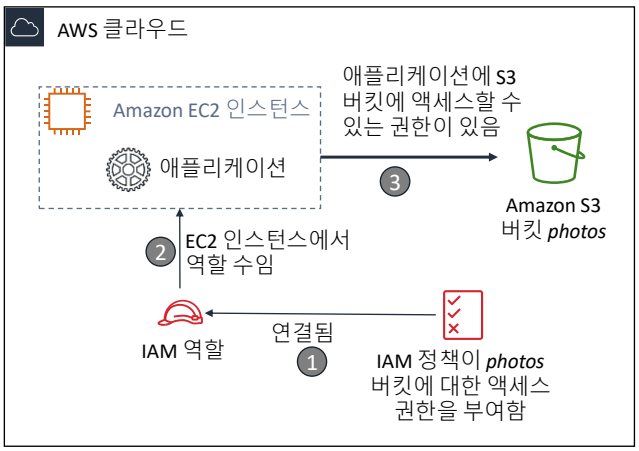
IAM 역할의 사용 예

시나리오:

- EC2 인스턴스에서 실행되는 애플리케이션에 S3 버킷에 대한 액세스 권한이 필요

솔루션:

- S3 버킷에 대한 액세스 권한을 부여하는 IAM 정책 정의
- 정책을 역할에 연결
- EC2 인스턴스가 이 역할을 수임하는 것을 허용



섹션 2 핵심 사항

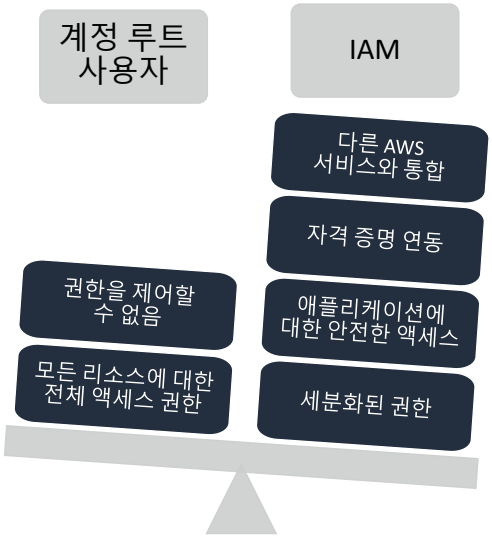
- **IAM 정책**은 JSON(JavaScript Object Notation)으로 작성되며 권한을 정의합니다.
  - IAM 정책은 모든 **IAM 엔터티에** 연결될 수 있습니다.
  - 엔터티는 IAM 사용자, IAM 그룹 및 IAM 역할입니다.
- IAM 사용자**는** 사람, 애플리케이션 또는 서비스에서 AWS에 인증할 수 있는 방법을 제공합니다.
- IAM 그룹**은** 동일한 정책을 여러 사용자에게 연결하는 간단한 방법입니다.
- IAM 역할**에는** 권한 정책이 연결될 수 있으며 사용자 또는 애플리케이션에 임시 액세스 권한을 위임하는 데 사용될 수 있습니다.

녹화된 데모: IAM

모듈 4: AWS 클라우드 보안

섹션 3: 새 AWS 계정 보안

AWS 계정 루트 사용자 액세스와 IAM 액세스 비교



- **모범 사례**: 필요한 경우를 제외하고 AWS 계정 루트 사용자를 사용하지 마십시오.
  - 계정 루트 사용자에 액세스하려면 계정을 생성할 때 사용한 이메일 주소(및 암호)로 로그인해야 합니다.
- 계정 루트 사용자만 수행할 수 있는 작업의 예:
  - 계정 루트 사용자 암호 업데이트
  - AWS Support 플랜 변경
  - IAM 사용자의 권한 복원
  - 계정 설정 변경(예: 연락처 정보, 허용된 리전)

새 AWS 계정 보안: 계정 루트 사용자

1단계: 계정 루트 사용자의 사용을 가능한 빨리 중지합니다.

- 계정 루트 사용자는 모든 리소스에 제한 없이 액세스할 수 있습니다.

- 계정 루트 사용자 사용을 중지하려면:
  1. 계정 루트 사용자로 로그인되어 있는 동안 자신이 사용할 IAM 사용자를 생성합니다. 필요한 경우 액세스 키를 저장합니다.
  2. IAM 그룹을 생성하고 전체 관리자 권한을 이 그룹에 부여한 후 IAM 사용자를 해당 그룹에 추가합니다.
  3. 계정 루트 사용자 액세스 키(있는 경우)를 비활성화하고 제거합니다.
  4. 사용자에 대한 암호 정책을 활성화합니다.
  5. 새로운 IAM 사용자 자격 증명으로 로그인합니다.
  6. 계정 루트 사용자 자격 증명을 안전한 장소에 저장합니다.

새 AWS 계정 보안: MFA

2단계: MFA(Multi-Factor Authentication)를 활성화합니다.

- 계정 루트 사용자와 모든 IAM 사용자에게 MFA를 요구합니다.
- 또한 MFA를 사용하여 AWS 서비스 API에 대한 액세스를 제어할 수 있습니다.

- MFA 토큰 검색 옵션 –
  - 가상 MFA 호환 애플리케이션:
    - Google Authenticator.
    - Authy Authenticator(Windows Phone 앱).
  - U2F 보안 키 디바이스:
    - 예: YubiKey.
  - 하드웨어 MFA 옵션:
    - Gemalto가 제공하는 키 FOB 또는 디스플레이 카드.

MFA 토큰

새 AWS 계정 보안: AWS CloudTrail

aws academy

3단계: AWS CloudTrail을 사용합니다.

- CloudTrail은 계정의 사용자 활동을 추적합니다.
  - 계정에서 지원되는 모든 서비스의 리소스에 대한 모든 API 호출을 로깅합니다.
- 기본 AWS CloudTrail 이벤트 기록은 기본적으로 활성화되어 있으며 무료입니다.
  - 여기에는 최근 90일간의 계정 활동에 대한 모든 관리 이벤트 데이터가 포함됩니다.
- CloudTrail에 액세스하려면 –
  1. AWS Management Console**에 로그인하고** CloudTrail **서비스를 선택합니다.**
  2. [**Event history(이벤트 기록)**]를 클릭하여 지난 90일간의 이벤트를 보고 필터링하고 검색합니다.
- **90일이 지난 로그를 활성화하고 지정된 이벤트 알림 기능을 활성화하려면 추적을 생성합니다.**
  1. CloudTrail 콘솔 추적 페이지에서 [**Create trail(추적 생성)**]을 클릭합니다.
  2. 이름을 지정하고, 모든 리전에 적용한 다음, 로그 저장을 위한 새 Amazon S3 버킷을 생성합니다.
  3. S3 버킷에 대한 액세스 제한을 구성합니다(예: 관리자 사용자만 액세스할 수 있음).

새 AWS 계정 보안: 결제 보고서

aws academy

4단계: 결제 보고서**(예: AWS 비용 및 사용 보고서) 활성화**

- 결제 보고서는 AWS 리소스 사용에 대한 정보와 해당하는 사용에 대한 추정 비용을 제공합니다.
- 보고서는 사용자가 지정한 Amazon S3 버킷으로 전송됩니다.
  - 보고서는 하루에 한 번 이상 업데이트됩니다.
- AWS 비용 및 사용 보고서**는 AWS 사용을 추적하며, AWS 계정과 관련된 시간별 또는 일별 추정 비용을 제공합니다.**

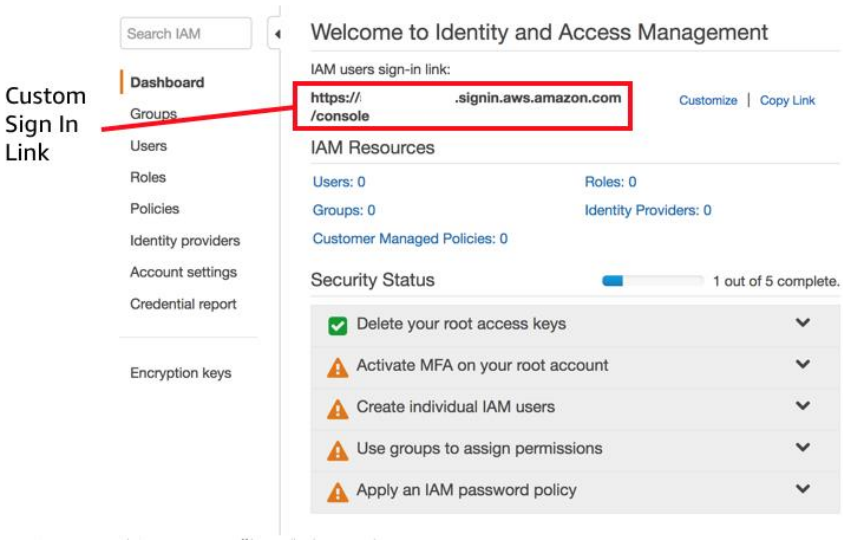
모듈 4: AWS 클라우드 보안

선택 사항: 새 AWS 계정 보안 – 전체 시연

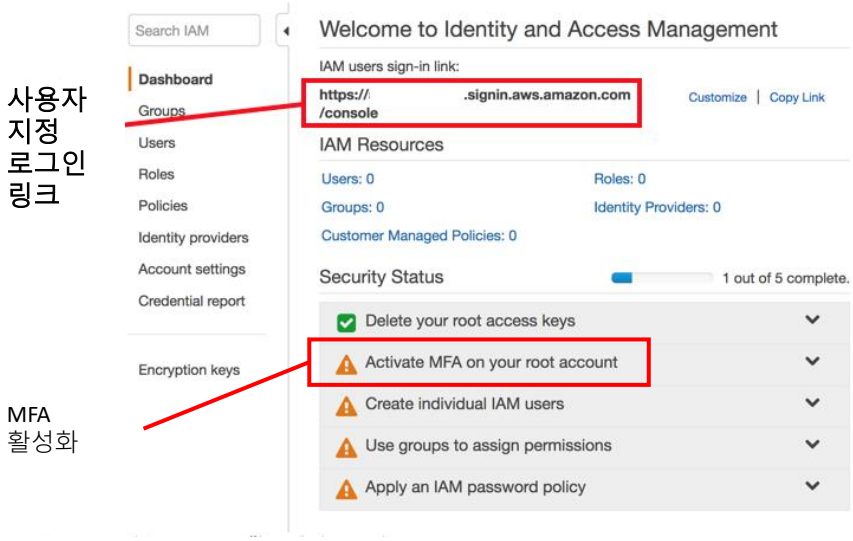
aws academy

IAM 보안 상태 검토

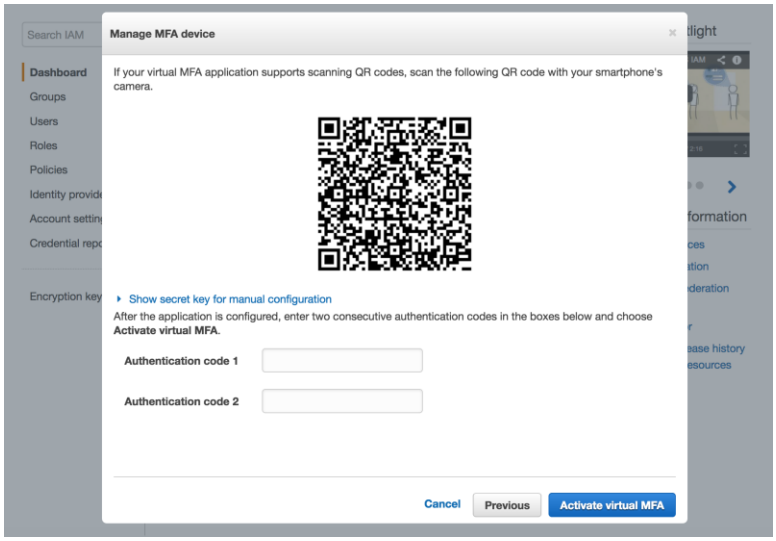
aws academy



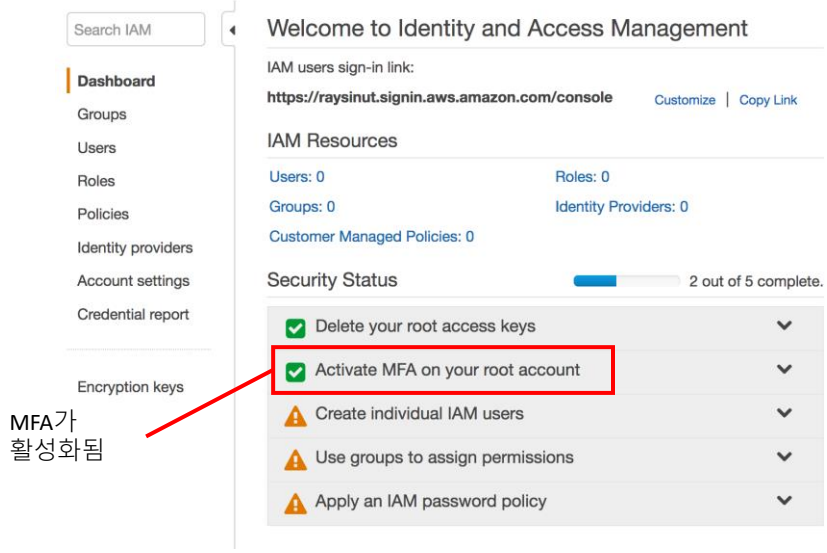
계정 루트 사용자에 대해 MFA 활성화



계정 루트 사용자에 대해 MFA 활성화

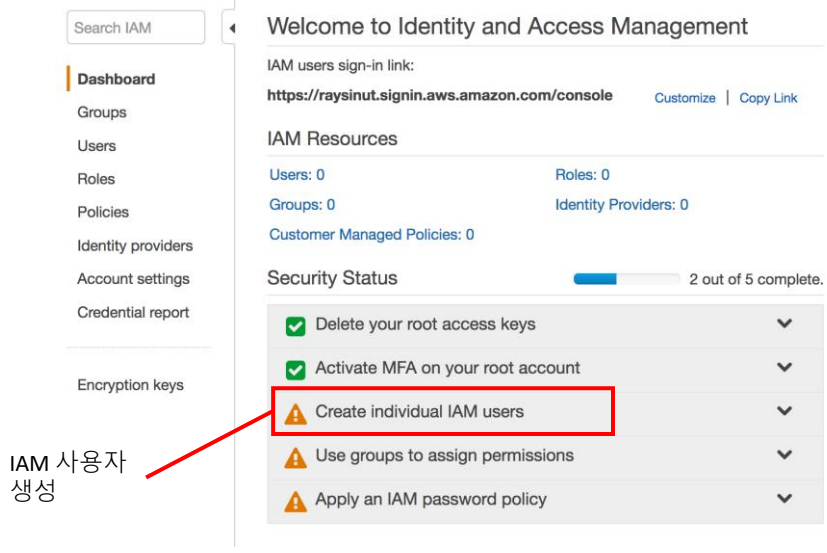


계정 루트 사용자에 대한 MFA가 활성화됨



MFA가 활성화됨

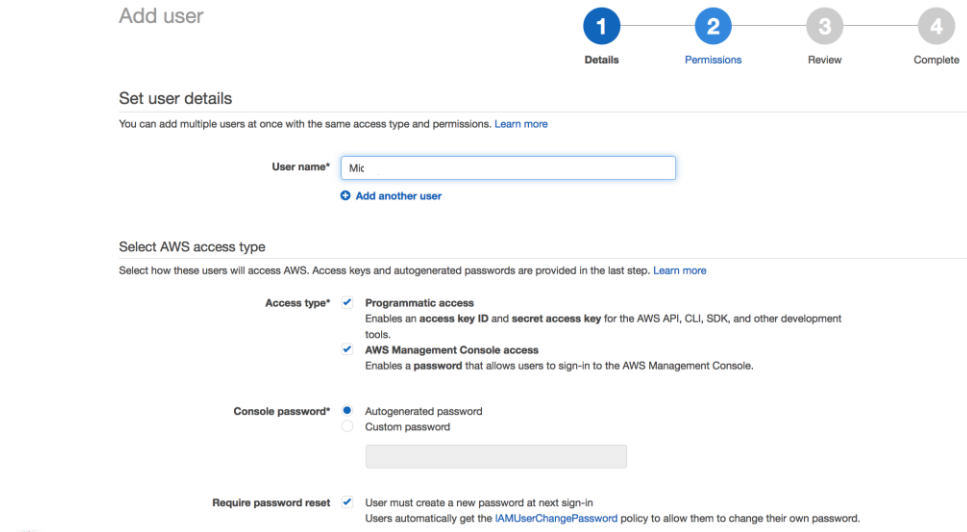
개별 IAM 사용자 생성(1)



IAM 사용자 생성

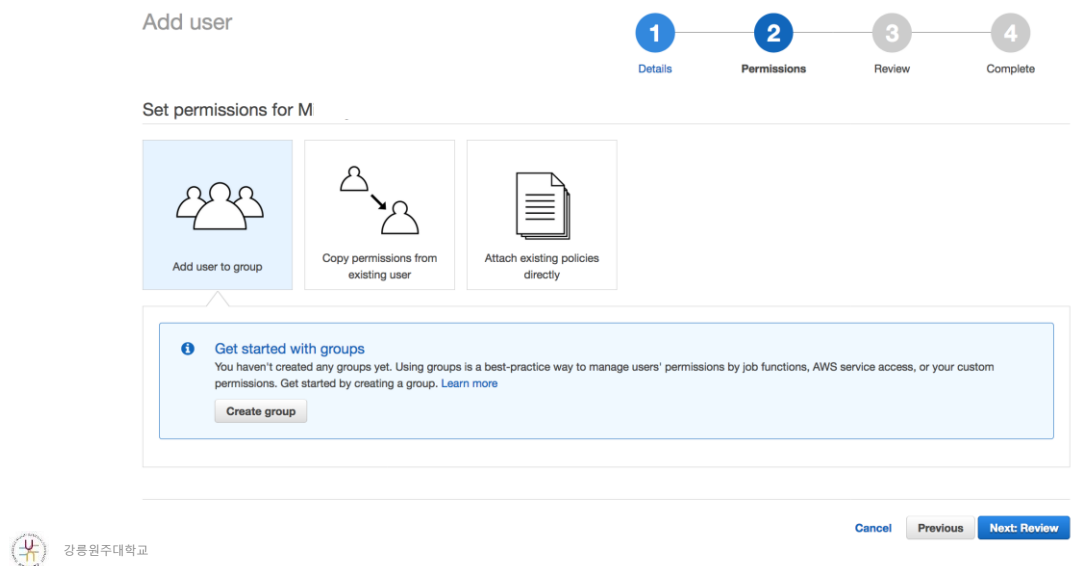
개별 IAM 사용자 생성(2)

aws academy

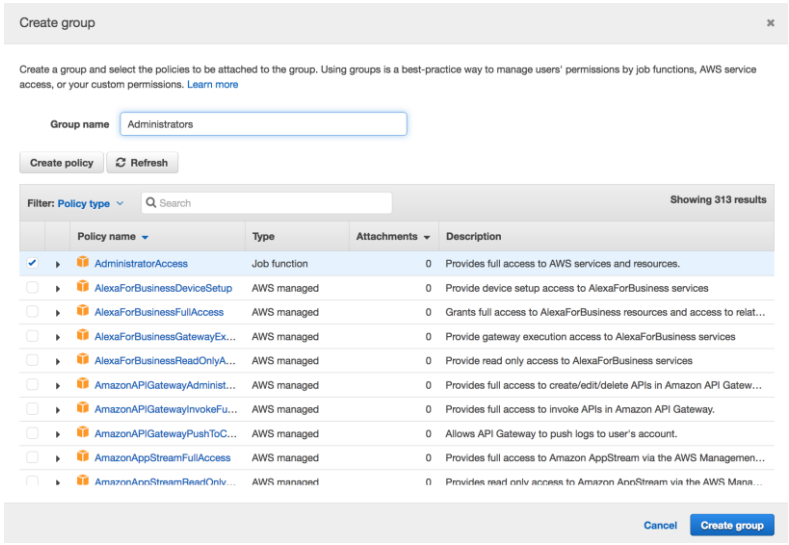


개별 IAM 사용자 생성(3)

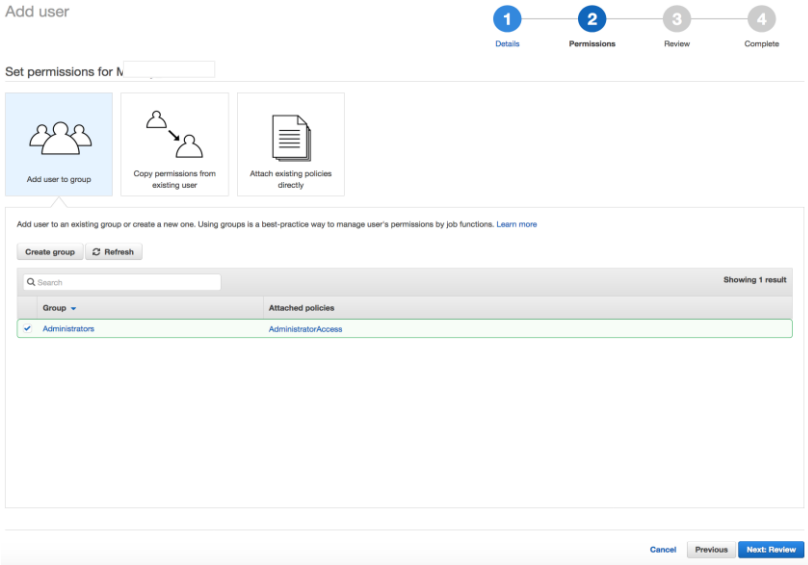
aws academy



개별 IAM 사용자 생성(4)

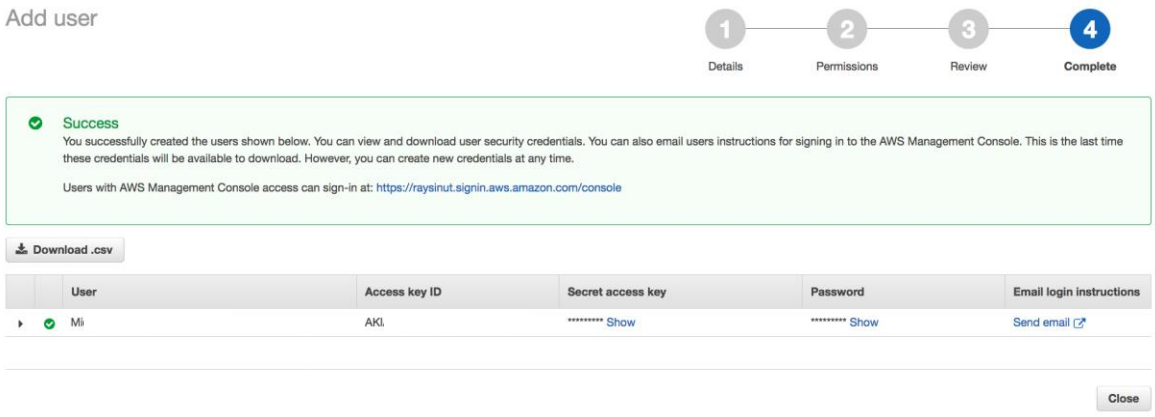


개별 IAM 사용자 생성(5)



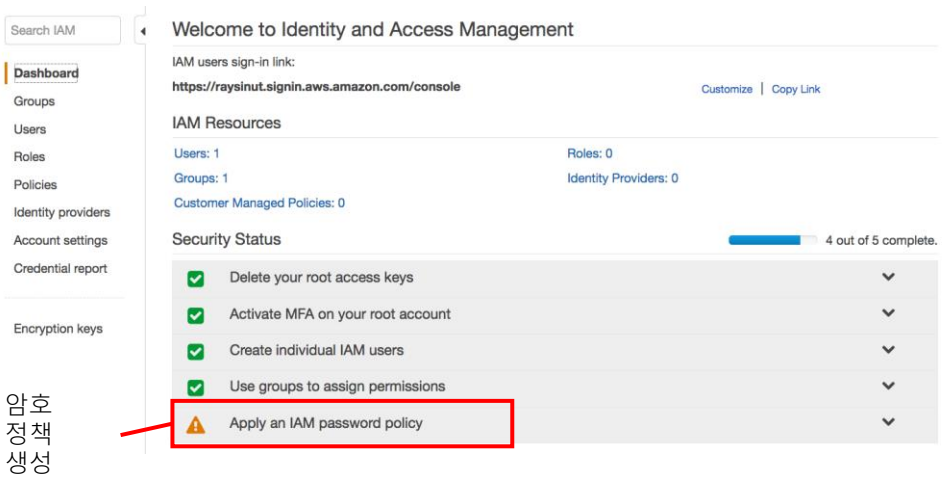
IAM 사용자 생성 성공

aws academy



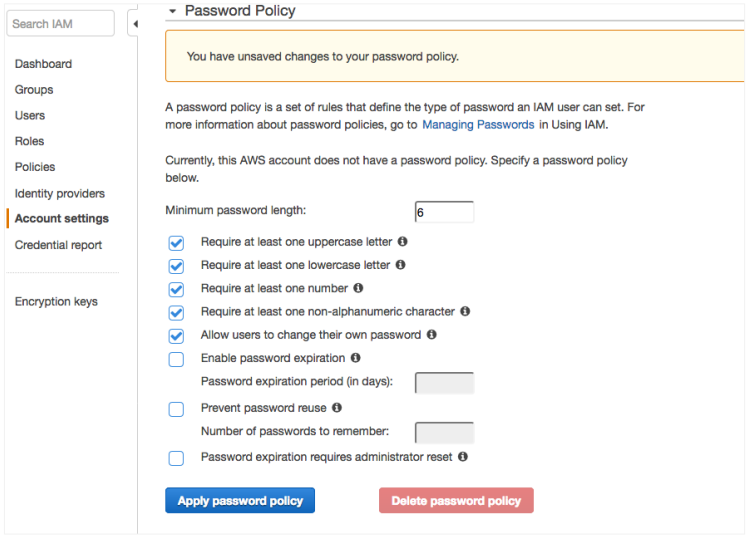
IAM 대시보드 보안 상태

aws academy

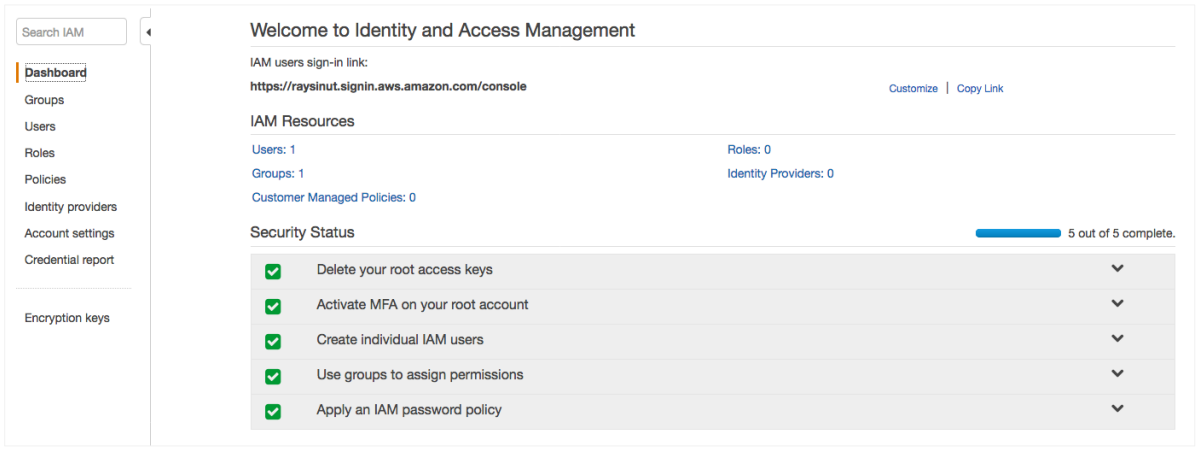


암호 정책 생성

IAM 암호 정책 설정



보안 상태 확인 완료



섹션 3 핵심 사항

aws academy

AWS 계정 보안을 위한 모범 사례:

- **MFA(Multi-Factor Authentication)를 사용하여 로그인을** 보호합니다.
- **계정 루트 사용자** 액세스 키를 삭제합니다.
- **개별** IAM 사용자를 생성하고 최소 권한의 원칙에 따라 권한을 부여합니다.
- **그룹을 사용**하여 IAM 사용자에게 권한을 할당합니다.
- **강력한 암호 정책**을 구성합니다.
- **자격 증명을 공유하는 대신** 역할을 사용하여 위임합니다.
- **AWS CloudTrail을 사용하여 계정 활동을** 모니터링합니다.

실습 1: IAM 소개

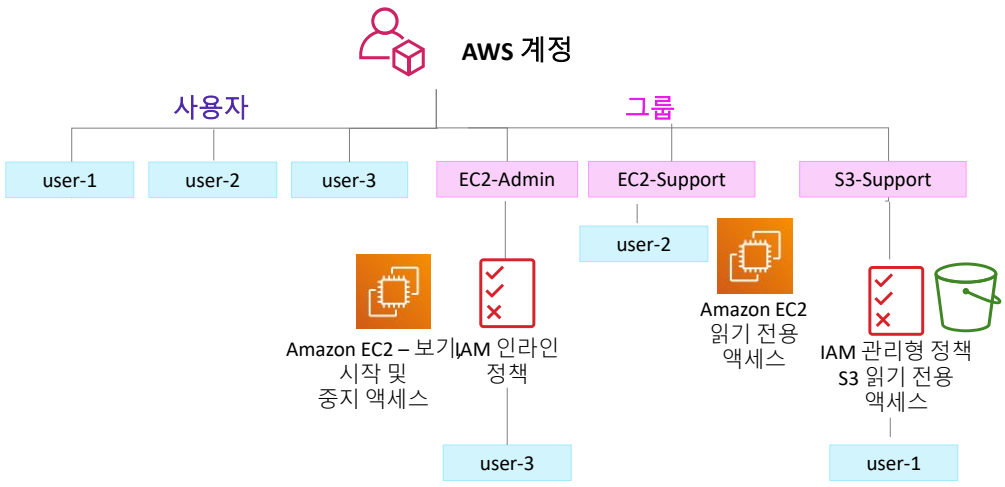
aws academy

실습 1: 과제

- 과제 1: 사용자 및 그룹 살펴보기
- 과제 2: 사용자를 그룹에 추가
- 과제 3: 로그인 및 사용자 테스트

AWS Identity and Access Management (IAM)

실습 1: 최종 제품



약 40분

실습 1:
AWS IAM 소개 시작

실습 개요:
핵심 사항

모듈 4: AWS 클라우드 보안

섹션 4: 계정 보안

AWS Organizations

- **AWS Organizations**를 사용하면 여러 AWS 계정을 통합하여 중앙에서 관리할 수 있습니다.

AWS Organizations

- AWS Organizations의 보안 기능:
  - **계정을 OU(조직 단위)로 그룹화**하고 각 OU에 다른 액세스 정책을 연결합니다.
  - **IAM에 대한 통합 및 지원**
    - 사용자에 대한 권한은 AWS Organizations를 통해 허용되는 권한과 해당 계정의 IAM을 통해 부여되는 권한의 교차점입니다.
  - **서비스 제어 정책을 사용**하여 각 AWS 계정이 액세스할 수 있는 AWS 서비스 및 API 작업에 대한 제어를 설정할 수 있습니다.

AWS Organizations: 서비스 제어 정책

- **SCP(서비스 제어 정책)**는 계정에 대한 중앙 집중식 제어를 제공합니다.
  - 조직에 포함된 계정에서 사용할 수 있는 권한을 제한합니다.
- 계정이 액세스 제어 지침을 준수하는지 확인합니다.
- SCP는 IAM 권한 정책과 *유사*합니다.
  - 비슷한 구문을 사용합니다.
  - 그러나 SCP는 권한을 부여하지는 않습니다.
  - 대신 SCP는 조직의 최대 권한을 지정합니다.

AWS Key Management Service(AWS KMS)

AWS Key Management Service(AWS KMS) 기능:

- 암호화 키를 생성하고 관리**할 수 있습니다.**
- AWS 서비스 및 애플리케이션 전체의 암호화 사용을 제어할 수 있습니다.
- AWS CloudTrail과 통합할 경우 모든 키 사용을 로깅합니다.
- FIPS(Federal Information Processing Standards) 140-2에서 검증한 HSM(하드웨어 보안 모듈)을 사용하여 키를 보호합니다.

AWS Key Management Service(AWS KMS)

Amazon Cognito

Amazon Cognito 기능

- 웹 및 모바일 애플리케이션에 사용자 가입, 로그인 및 액세스 제어를 추가합니다.
- 수백만 명의 사용자까지 확장됩니다.
- Facebook, Google 및 Amazon과 같은 소셜 자격 증명 공급자와 SAML(Security Assertion Markup Language) 2.0을 사용한 Microsoft Active Directory와 같은 엔터프라이즈 자격 증명 공급자를 사용한 로그인을 지원합니다.

Amazon Cognito

AWS Shield

- **AWS Shield** 기능:
  - DDoS(분산 서비스 거부 공격) 방어를 위한 관리형 서비스
  - AWS에서 실행되는 애플리케이션 보호
  - 상시 탐지 및 자동 인라인 완화 제공
  - AWS Shield Standard는 추가 비용 없이 활성화됩니다. AWS Shield Advanced는 선택형 유료 서비스입니다.
- 이 서비스를 사용하면 애플리케이션 다운타임과 지연 시간을 최소화할 수 있습니다.

AWS Shield

모듈 4: AWS 클라우드 보안

섹션 5: AWS의 데이터 보안

유휴 *데이터 암호화*

- **암호화**는 읽을 수 없는 보안 키로 데이터를 인코딩합니다.
  - 보안 키가 있는 사용자만 데이터를 디코딩할 수 있습니다.
  - AWS KMS에서 보안 키를 관리할 수 있습니다.

- AWS는 **유휴 데이터의 암호화를 지원합니다.**
  - 유휴 데이터 = 디스크 또는 테이프에 물리적으로 저장된 데이터
  - 다음을 포함하여 AWS KMS가 지원하는 모든 서비스에 저장된 데이터를 암호화할 수 있습니다.
    - Amazon S3
    - Amazon EBS
    - Amazon Elastic File System(Amazon EFS)
    - Amazon RDS 관리형 데이터베이스

전송 중 *데이터의 암호화*

- 전송 중 데이터**(네트워크에서 이동하는 데이터)의 암호화**
  - **TLS(전송 계층 보안)**(이전의 SSL)는 개방형 표준 프로토콜입니다.
  - **AWS Certificate Manager**는 TLS 또는 SSL 인증서를 관리, 배포 및 갱신하는 방법을 제공합니다.
- 보안 HTTP(HTTPS)는 보안 터널을 생성합니다.
  - 양방향 데이터 교환에는 TLS 또는 SSL이 사용됩니다.
- **AWS 서비스는 전송 중 데이터 암호화를 지원합니다.**
  - 2가지 예:

Amazon S3 버킷 및 객체 보안

- 새로 생성된 S3 버킷과 객체는 기본적으로 비공개이며 보호됩니다.
- Amazon S3의 데이터 객체를 공유해야 하는 사용 사례의 경우 –
  - 데이터 액세스를 관리하고 제어하는 것이 필수적입니다.
  - 최소 권한 원칙을 준수하는 권한을 따르고 Amazon S3 암호화 사용을 고려하십시오.
- S3 데이터 액세스 제어를 위한 도구 및 옵션 –
  - Amazon S3 Block Public Access 기능: 사용이 간단합니다.
  - IAM 정책: 사용자가 IAM을 사용하여 인증할 수 있는 경우에 좋은 옵션입니다.
  - 버킷 정책
  - ACL(액세스 제어 목록): 레거시 액세스 제어 메커니즘입니다.
  - AWS Trusted Advisor 버킷 권한 확인: 무료로 제공되는 기능입니다.

모듈 4: AWS 클라우드 보안

섹션 6: 규정 준수 보장 작업

AWS 규정 준수 프로그램

- 고객에게 적용되는 보안 및 규제 준수와 요건은 매우 다양합니다.
- **AWS는 인증 기관 및 독립 감사자와 협력하여 AWS가 설정하고 운영하는 정책, 프로세스 및 제어에 대한 상세한 정보를 제공합니다.**

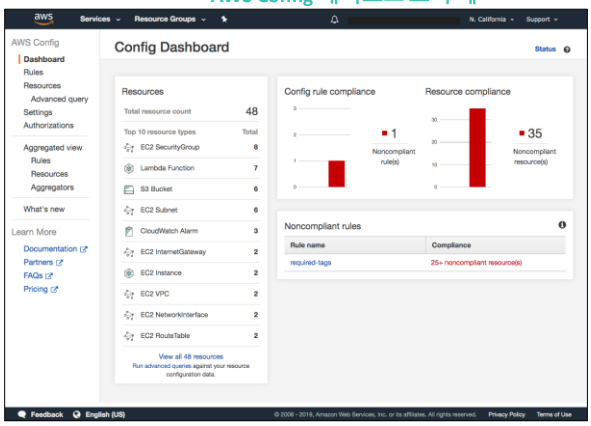
- 규정 준수 프로그램은 넓은 범위로 다음과 같이 분류될 수 있습니다.
  - **인증 및 인가**
    - 독립적인 외부 감사자가 평가
    - 예: ISO 27001, 27017, 27018 및 ISO/IEC 9001
  - **법률, 규정 및 개인 정보**
    - AWS는 보안 기능 및 법적 계약을 제공하여 규정 준수를 지원합니다.
    - 예: EU GDPR(General Data Protection Regulation), HIPAA
  - **준수 및 프레임워크**
    - 산업별 또는 기능별 보안 또는 규정 준수 요구 사항
    - 예: CIS(Center for Internet Security), EU-미국 프라이버시 실드 인증



AWS Config

AWS Config

AWS Config 대시보드 보기 예



- **AWS** 리소스의 구성을 측정, 감사 및 평가합니다.
- 구성을 지속적으로 모니터링하는 데 사용됩니다.
- 기록된 구성과 원하는 구성을 자동으로 비교하여 평가합니다.
- 구성 변경을 검토합니다.
- 세부 구성 기록을 봅니다.
- 규정 준수 감사 및 보안 분석을 간소화합니다.

AWS Artifact

AWS Artifact

- 규정 준수 관련 정보를 위한 리소스입니다.
- 보안 및 규정 준수 보고서에 액세스하고 온라인 계약을 선택할 수 있습니다.
- 예제 다운로드에 액세스할 수 있습니다.
  - AWS ISO 인증
  - PCI(Payment Card Industry) 및 SOC(Service Organization Control) 보고서
- AWS Management Console에서 직접 AWS Artifact에 액세스할 수 있습니다.
  - **[Security, Identify & Compliance(보안, 자격 증명 및 규정 준수)]**에서 **[Artifact]**를 클릭합니다.

섹션 6 핵심 사항

- **AWS 보안 규정 준수 프로그램**은 AWS가 설정하고 운영하는 정책, 프로세스 및 제어에 대한 정보를 제공합니다.
- **AWS Config**는 AWS 리소스의 구성을 측정, 감사 및 평가하는 데 사용됩니다.
- **AWS Artifact**는 보안 및 규정 준수 보고서에 대한 액세스를 제공합니다.

모듈 4: AWS 클라우드 보안

섹션 7: 추가 보안 서비스 및 리소스

AWS Service Catalog

AWS Service Catalog

- 조직에서 승인한 IT 서비스의 카탈로그를 생성하고 관리
  - 직원이 *승인된* IT 서비스를 찾고 배포하는 데 도움이 됨
  - IT 서비스에는 하나 이상의 AWS 리소스가 포함될 수 있음
  - 예:
    - EC2 인스턴스, 스토리지 볼륨, 데이터베이스 및 네트워킹 구성 요소
- 제약 조건을 지정하여 AWS 서비스 사용을 제어
  - 제약 조건의 예:
    - 제품을 시작할 수 있는 AWS 리전
    - 허용되는 IP 주소 범위
- 중앙에서 IT 서비스 수명 주기 관리
- 규정 준수 요구 사항을 충족하는 데 도움이 됨

선택형 추가 보안 서비스

Amazon Macie

사전 예방적으로 **PII(개인 식별 정보)를 보호**하고 이러한 정보의 이동에 대해 파악할 수 있습니다.

Amazon Inspector

애플리케이션에 대한 표준 및 모범 사례를 정의하고 이러한 **표준**을 **준수하는지 확인**합니다.

Amazon GuardDuty

지능형 **위협 탐지** 및 지속적인 모니터링을 통해 AWS 계정과 워크로드를 보호합니다.

모듈 4: AWS 클라우드 보안

모듈 요약

aws academy

모듈 요약

aws academy

이 모듈에서 학습한 내용은 다음과 같습니다.

- 공동 책임 모델 이해
- 고객 및 AWS의 책임 확인
- IAM 사용자, 그룹 및 역할 이해
- IAM의 다양한 보안 자격 증명 유형 설명
- 새 AWS 계정 보안을 위한 단계 확인
- IAM 사용자 및 그룹 탐색
- AWS 데이터를 보호하는 방법 이해
- AWS 규정 준수 프로그램 이해

지식 확인 완료

샘플 시험 문항

AWS 공동 책임 모델에서 다음 중 AWS의 책임은 무엇입니까?

A. 타사 애플리케이션 구성
B. 물리적 하드웨어 유지 관리
C. 애플리케이션 액세스 및 데이터 보호
D. 사용자 지정 Amazon Machine Image(AMI) 관리

추가 리소스

- AWS 클라우드 보안 홈 페이지
- AWS 보안 리소스
- AWS 보안 블로그
- 보안 공지
- 취약성 및 침투 테스트
- AWS Well-Architected 프레임워크 – 보안 원칙
- AWS 설명서 – IAM 모범 사례

감사합니다.