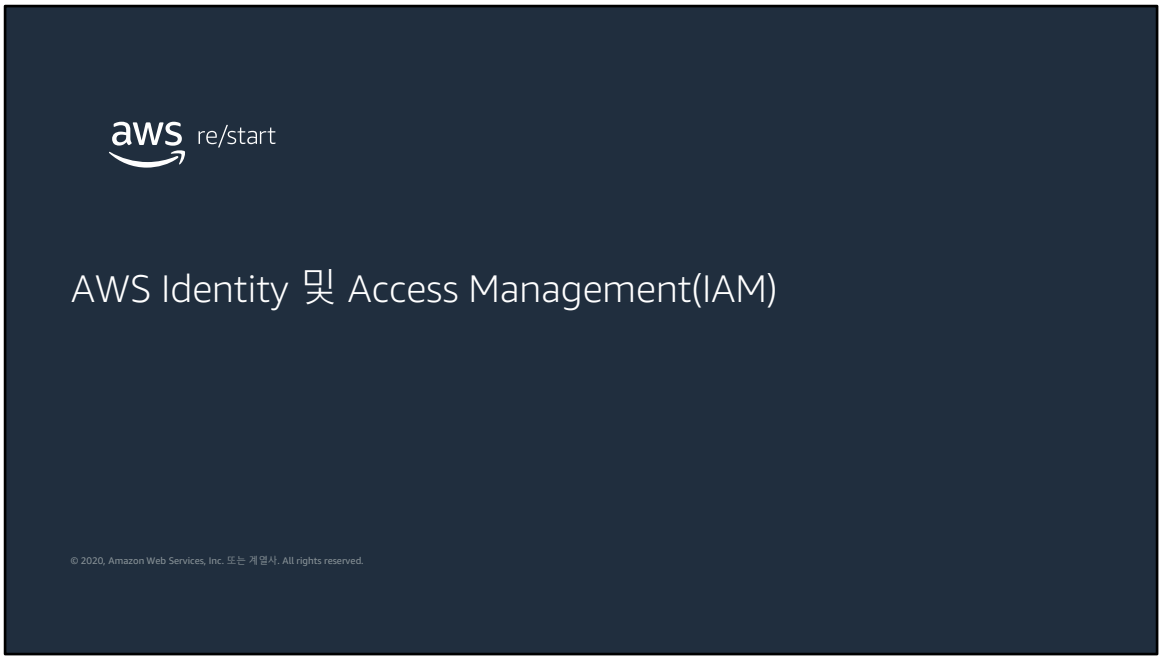


이 모듈에서는 AWS Identity 및 Access Management(IAM)를 소개합니다.

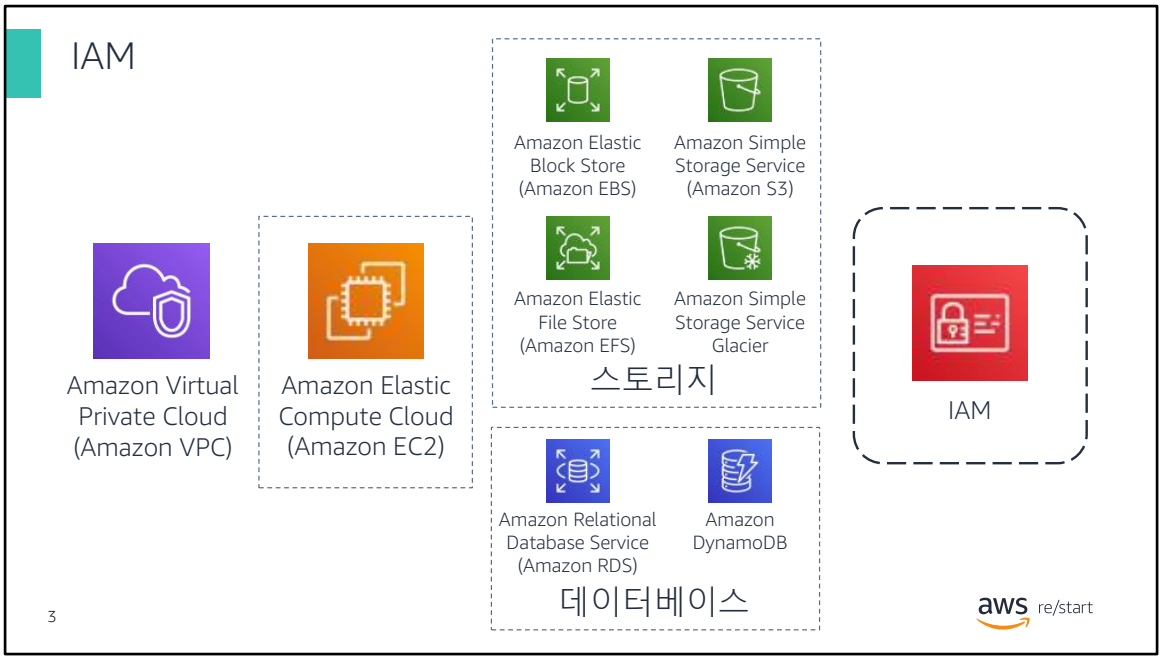
교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- AWS Identity 및 Access Management(IAM) 서비스를 설명합니다.
- IAM에서 지원하는 다양한 보안 인증 정보를 나열합니다.
- 인증 및 권한 부여가 IAM에서 어떻게 구현되는지 설명합니다.

이 모듈에서는 AWS Identity 및 Access Management(IAM) 사용자, 그룹, 역할에 관해 배웁니다. 다양한 유형의 보안 인증 정보에 관해서도 배웁니다.



AWS Identity 및 Access Management(IAM)를 사용하면 AWS 서비스와 리소스에 대한 액세스를 안전하게 관리할 수 있습니다. IAM을 사용하면 인증을 지원하기 위해 AWS 사용자 및 그룹을 생성하고 관리하며, 권한 부여를 지원하기 위해 권한을 사용하여 AWS 리소스에 대한 액세스를 허용 및 차단할 수 있습니다.

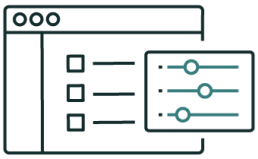
IAM은 사용자, 그룹 및 권한과 같이 여러분이 이미 아는 액세스 제어 개념을 사용하므로, 어떤 사용자가 어떤 서비스에 액세스할 수 있는지 지정할 수 있습니다.

IAM이란?

AWS Identity 및 Access Management(IAM)

인증과 AWS 리소스에 대한 액세스를 중앙에서 관리할 수 있습니다.

- 추가 비용 없이 AWS 계정의 기능으로 제공됩니다.
- **사용자**, **그룹**, **역할** 을 생성합니다.
- 이 엔터티에 **정책**을 적용하여 AWS 리소스에 대한 액세스를 제어합니다.



aws re/start

AWS Identity 및 Access Management(IAM)는 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 해주는 서비스입니다.

인증

IAM을 사용하여 **인증**을 구성하는 일은 AWS 리소스에 액세스할 수 있는 **사람**을 지정하는 일이므로 처음 수행할 단계입니다. IAM은 사용자 인증에 사용되며, 애플리케이션 및 기타 AWS 서비스의 액세스에도 사용됩니다.

권한 부여

IAM은 사용자에 따라 **권한** 부여를 구성하는 데 사용됩니다. 권한 부여는 사용자가 액세스할 수 있는 리소스가 **무엇인지**, 해당 리소스를 가지고 또는 해당 리소스에 **어떤 작업을** 할 수 있는지를 제어합니다. 권한 부여는 정책을 사용하여 정의됩니다. **정책**은 아이덴티티 또는 리소스에 연결될 때 해당 권한을 정의하는 AWS의 객체입니다.

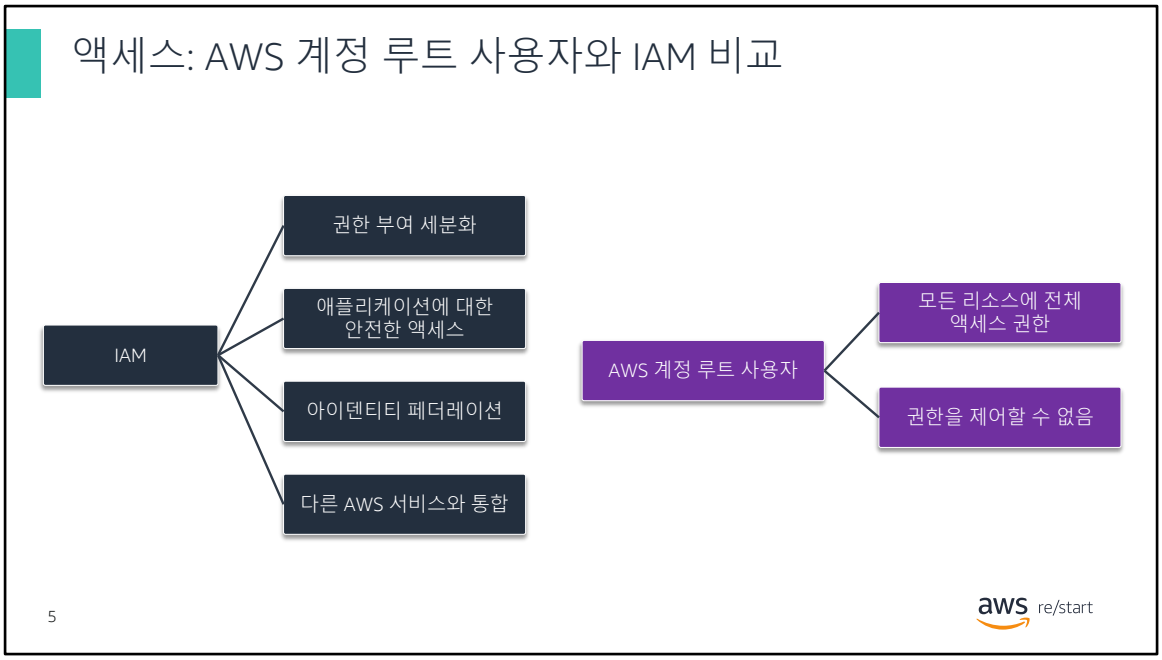
IAM을 사용하면 다른 사람이나 시스템에 액세스 권한을 부여할 때 암호나 액세스 키를 공유할 필요성이 줄어듭니다. 또한 사용자의 액세스를 활성화하거나 비활성화하기가 쉬워집니다.

리소스를 시작, 구성, 관리, 종료할 수 있는 사람과 관련한 액세스를 중앙에서 관리하는 도구로 IAM을 사용하면 됩니다. 또한 다른 AWS 리소스를 프로그래밍 방식으로 호출할 수 있는 애플리케이션이나 사용자 및 시스템에 대한 액세스 권한을 상세하게 제어할 수 있게 해줍니다.

IAM으로 다음 태스크를 수행할 수 있습니다.

- 액세스할 수 있는 리소스와 해당 리소스에 수행할 수 있는 액션을 관리합니다. 예를 들어, Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 영구 종료할 권한이 있는 사람을 결정할 수 있습니다.

- 컨텍스트에 따라 필요한 보안 인증 정보를 정의합니다.
    - 누가 어떤 AWS 서비스에 액세스할 수 있는지
    - 사용자 또는 시스템이 서비스에 어떤 작업을 수행할 수 있는지



AWS 계정 루트 사용자
처음 AWS 계정을 생성할 때 통합 인증 아이덴티티로 시작합니다. 이 엔터티는 해당 계정의 모든 AWS 서비스와 리소스에 대한 완전한 액세스 권한을 가지며, **AWS 계정 루트 사용자**라고 부릅니다. 계정 루트 사용자는 AWS 계정을 만들 때 사용한 이메일 주소 및 암호로 로그인하여 액세스합니다.

AWS 계정 루트 사용자는 계정의 모든 리소스에 대한 모든 액세스 권한을 보유합니다. AWS 계정 루트 사용자 인증 정보의 권한은 제어할 수 없습니다. 그러므로 AWS와의 일상적인 상호 작용에는 계정의 루트 사용자 자격 증명을 사용하지 않는 것이 좋습니다.

IAM
IAM을 사용하여 추가 사용자를 생성하고, 이 사용자에게 최소 권한의 원칙에 따라 권한을 부여하시기 바랍니다. IAM을 사용하면 AWS 서비스 및 리소스에 대한 AWS 계정 사용자의 액세스를 안전하게 제어할 수 있습니다. 예를 들어 관리자 수준의 권한이 필요하다면 이렇게 해볼 수 있습니다.

1. IAM 사용자를 생성합니다.
2. 이 사용자에게 전체 액세스 권한을 부여합니다.
3. 이 보안 인증 정보를 사용하여 AWS와 상호 작용합니다.

이후에 권한을 취소하거나 수정해야 하는 경우, 해당 IAM 사용자에게 연결된 정책을 삭제하거나 수정할 수 있습니다.

또한 AWS 계정에 액세스해야 하는 사용자가 여럿인 경우에는 사용자별로 고유한 보안 인증 정보를 생성하고 누가 어떤 리소스에 대한 액세스 권한이 있는지를 정의하면 됩니다. 다시 말해 보안 인증 정보를 공유할 필요가 없습니다. 예를 들어 AWS 계정의 리소스에 대한 읽기 전용 권한이 있는 IAM 사용자를 생성한 다음, 읽기 액세스가 필요한 사용자에게 해당 보안 인증 정보를 배포할 수 있습니다.

최소 권한의 원칙

모범 실무

- IAM을 통해 최소 권한의 원칙을 따를 수 있습니다.

해야 할 일

- 계정 루트 사용자 액세스 키를 삭제합니다.
- IAM 사용자를 생성합니다.
- 관리자 액세스를 부여합니다.
- 다중 인증(MFA)을 활성화합니다.
- IAM 보안 인증 정보를 사용하여 AWS와 상호 작용합니다.

최소 권한의 원칙은 컴퓨터 보안에서 중요한 개념입니다. 이 원칙을 따르기 위해서는 사용자 및 역할이 무엇을 해야 하는지 결정한 다음 이들이 해당 태스크만을 수행하도록 허용하는 정책을 만듭니다.

IAM 정책을 생성할 때는 최소 권한을 부여하는 표준 보안 관행을 따르시기 바랍니다. 즉, 해당 태스크를 수행하는 데 필요한 권한만 부여하는 것입니다. 최소한의 권한 집합으로 시작하여 필요에 따라 추가 권한을 부여합니다. 너무 폭넓은 권한으로 시작해 이후에 범위를 좁히려고 하는 것보다 이 방법이 훨씬 안전합니다.

보안 인증 정보의 유형

인증 정보의 유형	관련 용례
이메일 주소 및 암호	AWS 계정(루트)과 연결됨
IAM 사용자 이름 및 암호	AWS Management Console에 액세스하는 데 사용됨
액세스 및 비밀 액세스 키	일반적으로 AWS Command Line Interface(AWS CLI) 및 프로그래밍 방식 요청(예: 애플리케이션 프로그래밍 인터페이스(API), 소프트웨어 개발 키트(SDK))에 사용됨
다중 인증(MFA)	추가 보안 계층 AWS 계정 루트 사용자 및 IAM 사용자에 대해 활성화할 수 있음
키 페어	Amazon EC2와 같은 특정 AWS 서비스에만 사용됨

이 테이블에는 다양한 유형의 AWS 보안 인증 정보가 요약되어 있습니다.

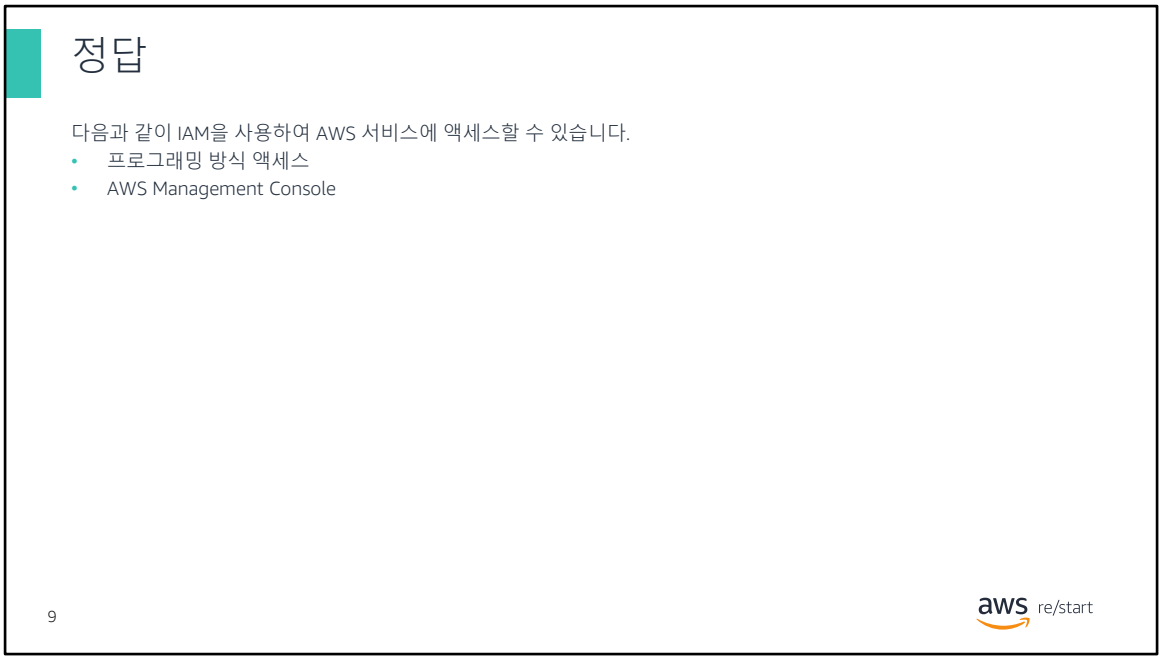
각 AWS 계정에는 할당된 계정 루트 사용자가 있습니다. 이 계정 루트 사용자에게는 계정 복구와 통신을 위해 할당된 이메일 주소가 있습니다. 그러나 일상적인 태스크, 심지어 관리 태스크의 경우에도 계정 루트 사용자를 사용하지 않는 것이 좋습니다. IAM 사용자를 처음 생성할 때만 계정 루트 사용자를 사용하는 모범 실무를 따르는 것이 좋습니다. 그런 다음 계정 루트 사용자 인증 정보를 안전하게 잠급니다. 다른 방법으로는 수행할 수 없는 계정 및 서비스 관리 태스크를 수행할 때만 사용하시기 바랍니다.

이전에 언급한 것처럼, IAM 사용자 이름과 암호 보안 인증 정보는 '콘솔'이라고 부르는 AWS Management Console에 액세스하는 데 사용됩니다. 액세스 키는 사용자에 대해 생성되면 프로그래밍 방식 액세스에 사용할 수 있습니다.

마지막으로, 추가 보안을 위해 AWS에서는 AWS 계정 루트 사용자와 정의된 IAM 사용자에게 다중 인증(MFA)을 적용할 것을 권장합니다.

학습 내용 확인 질문

1. AWS 서비스에 액세스하기 위해 IAM을 사용할 수 있는 두 가지 방법은 무엇입니까?



프로그래밍 방식 액세스와 AWS Management Console 액세스라는 2가지 액세스 유형을 사용자에게 할당할 수 있습니다.

보너스 질문
프로그래밍 방식으로 사용자를 활성화하려면 어떤 키 유형 두 가지가 필요합니까?

정답
AWS 서비스에 대한 액세스 권한을 제공하려면 액세스 키 ID와 비밀 액세스 키가 필요합니다.

IAM: 권한 부여

- 권한을 부여하여 사용자가 AWS 서비스에 액세스할 수 있도록 허용합니다.
- IAM 정책을 생성하여 권한을 할당합니다.
- 권한은 어떤 리소스와 어떤 작업을 사용할 수 있는지 결정합니다.

참고: IAM은 전역에 적용됩니다. 리전별로 적용되지 않고 모든 AWS 리전에 적용됩니다.

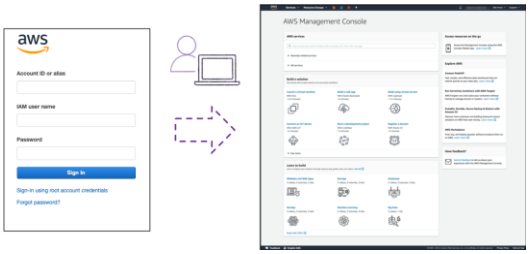
사용자가 인증된 후에는 AWS 서비스에 액세스할 수 있는 권한이 있어야 합니다.

사용자, 그룹, 역할에 권한을 할당하려면 IAM 정책을 만들어야 합니다. 정책은 권한을 명시적으로 나열한 문서입니다. 기본적으로 주어지는 권한은 없습니다. 명시적으로 허용하지 않는 한, 모든 액션은 기본적으로 차단됩니다(암시적 차단). 명시적으로 허용하지 않은 모든 액션은 차단됩니다. 명시적으로 차단한 액션은 언제나 차단됩니다.

IAM은 전역에 적용됩니다. 리전별로 적용되지 않고 모든 AWS 리전에 적용됩니다.

MFA

- **다중 인증(MFA)**은 보안을 강화해 줍니다.
- MFA를 사용하면 AWS 서비스에 액세스하기 위해 사용자 이름과 암호 외에도 고유 인증 코드가 필요합니다.



aws re/start

다음 도구를 사용하여 AWS 서비스 및 리소스에 액세스할 수 있습니다.

- AWS Management Console
- AWS Command Line Interface(AWS CLI)
- 지원되는 다양한 환경의 소프트웨어 개발 키트(SDK) 및 애플리케이션 프로그래밍 인터페이스(API)

보안 강화를 위해 MFA를 활성화하는 것이 좋습니다. MFA를 사용하면 사용자와 시스템은 먼저 인증을 받아야 AWS 서비스 및 리소스에 액세스할 수 있습니다. 인증 디바이스에는 하드웨어 디바이스와 가상 MFA 호환 애플리케이션(Google Authenticator 또는 Authy 2-Factor Authentication)의 두 가지 옵션이 제공됩니다. 단문 메시지 서비스(SMS)는 코드 수신을 위해 SMS 메시지를 받을 수 있는, 모바일 디바이스를 사용하는 또 다른 인증 대안입니다.

AWS Security Token Service(AWS STS)는 IAM 사용자 또는 인증한 사용자에 대한 제한적인 임시 보안 인증 정보도 요청할 수 있는 웹 서비스입니다.

자세한 내용은 AWS Identity 및 Access Management 사용 설명서의 AWS에서 다중 인증(MFA) 사용하기를 참조하십시오.

IAM 사용자

- AWS에 생성하는 엔터티 중 하나입니다.
- AWS와 상호 작용하는 방법을 제공합니다.
- IAM 사용자에 기본적으로 적용되는 보안 인증 정보는 없습니다.
- 사람 또는 애플리케이션을 대표할 수 있습니다.

모범 실무

AWS 계정 루트 사용자를 사용하는 대신 관리 권한이 있는 별도의 IAM 사용자 계정을 생성합니다.

모범 실무

aws re/start

IAM **사용자**는 AWS에 생성하는 엔터티로서, AWS와 상호 작용하는 방법을 제공합니다. IAM 사용자는 기본적으로 개인에게 콘솔에 로그인하고 AWS 서비스에 요청할 때 사용할 수 있는 아이덴티티를 제공합니다.

새롭게 생성된 IAM 사용자에게는 자신을 인증하여 AWS 리소스에 액세스하는 데 사용할 기본 보안 인증 정보가 없습니다. 먼저 인증을 위해 사용자에게 보안 인증 정보를 할당합니다. 그런 다음 사용자에게 AWS 액션을 수행하거나 AWS 리소스에 액세스할 수 있는 권한을 연결합니다. 사용자를 위해 생성하는 보안 인증 정보는 사용자가 AWS에서 자신을 고유하게 식별하는 데 사용됩니다.

IAM 사용자는 권한이 연결된 아이덴티티일 뿐입니다. AWS에 요청을 하기 위해 보안 인증 정보가 반드시 필요한 애플리케이션을 대표할 IAM 사용자를 생성할 수 있습니다. 프로세스가 Microsoft Windows 또는 Linux와 같은 운영 체제에서 자체 아이덴티티와 권한을 갖는 것과 같은 방식으로, 애플리케이션은 여러분의 계정에서 자체 아이덴티티와 자체 권한 집합을 가질 수 있습니다.

계정 루트 사용자 대신 관리 권한이 있는 별도의 IAM 사용자 계정을 생성하는 것이 모범 실무입니다.

IAM 그룹

IAM 그룹은 IAM 사용자의 모음입니다.

- IAM 사용자의 모음입니다.
- 기본 그룹은 없습니다.
- 그룹을 중첩할 수 없습니다.
- 사용자는 여러 그룹에 속할 수 있습니다.

다음을 수행할 수 있습니다.
- 그룹 전체에 대한 권한을 지정합니다.
- IAM 정책을 사용하여 권한을 정의합니다.

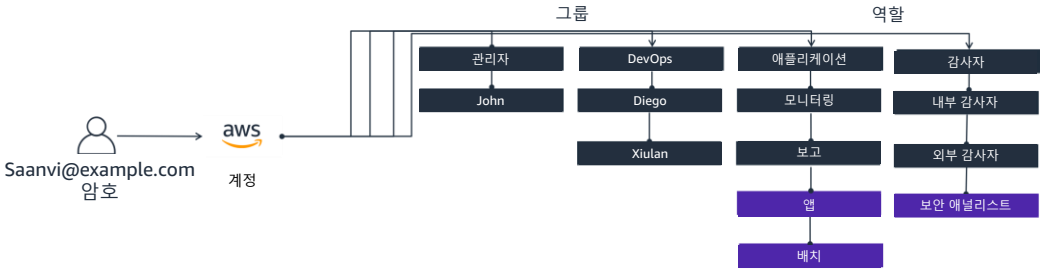
aws re/start

그룹은 IAM 사용자의 모음입니다. 그룹을 사용하면 사용자 모음의 권한을 지정할 수 있으므로, 해당 사용자의 권한을 좀 더 쉽게 관리할 수 있습니다. 예를 들어 **개발자**라는 그룹을 생성하고 개발자에게 일반적으로 필요한 유형의 권한을 해당 그룹에 부여할 수 있습니다. 해당 그룹의 모든 사용자는 그룹에 지정된 권한을 자동으로 보유하게 됩니다. 새로운 사용자가 조직에 들어오고 이 사용자에게 개발자 권한이 있어야 할 경우 해당 사용자를 개발자 그룹에 추가하면 됩니다. 그러면 해당 사용자에게 적절한 권한이 자동으로 부여됩니다. 마찬가지로 조직에서 직무를 변경하는 경우, 해당 사용자의 권한을 편집하는 대신 이전 그룹에서 해당 사용자를 제거하고 새 그룹에 추가할 수 있습니다.

그룹의 주요 특성:
- 그룹은 여러 사용자를 포함할 수 있고, 사용자는 여러 그룹에 속할 수 있습니다.
- 그룹은 중첩될 수 없습니다. 그룹은 사용자만 포함할 수 있고, 다른 그룹은 포함할 수 없습니다.
- AWS 계정의 모든 사용자를 자동으로 포함하는 기본 그룹은 없습니다. 기본 그룹을 원하는 경우, 그룹을 생성하고 새로운 사용자를 각각 그룹에 할당해야 합니다.

IAM 역할

- AWS 리소스에 대한 액세스 권한을 위임하는 데 사용됩니다.
- 임시 액세스를 제공합니다.
- 권한
  - IAM 정책을 사용하여 정의됩니다.
  - IAM 사용자 또는 그룹이 아니라 역할에 연결됩니다.



aws re/start

역할은 AWS 계정의 AWS 리소스에 대한 임시 액세스 권한을 부여하는 도구입니다. 권한은 IAM 사용자 또는 그룹에 연결되지 않습니다. 대신 런타임 시 애플리케이션이나 AWS 서비스가 프로그래밍 방식으로 역할을 수임할 수 있습니다. 역할이 수임되면, AWS는 사용자 또는 애플리케이션이 프로그래밍 방식으로 AWS에 요청할 때 사용할 수 있는 임시 보안 인증 정보를 반환합니다. 따라서 리소스에 액세스해야 하는 엔터티별로 장기적인 보안 인증 정보를 공유할 필요가 없습니다(예: IAM 사용자 생성을 통해).

용례

역할을 사용하는 용례 중 하나는 페더레이션 사용자입니다. 페더레이션 사용자는 IAM 사용자와는 달리 AWS 계정에 영구적인 아이덴티티가 없습니다. 페더레이션 사용자에게 권한을 할당하려면 역할 엔터티를 생성하면 됩니다.

역할 생성

액세스를 허용하려는 리소스가 포함된 AWS 계정에 역할을 생성합니다. 역할을 생성할 때는 두 가지 정책을 지정합니다.

- **신뢰** 정책은 역할을 맡도록 허용된 사람을 지정합니다(신뢰할 수 있는 엔터티 또는 보안 주체).

- **액세스**(또는 **권한**) 정책은 보안 주체가 액세스할 수 있는 리소스와 액션을 정의합니다. 보안 주체는 다음 중 무엇이든 될 수 있습니다.
    - AWS 계정
    - AWS 서비스(예: Amazon Elastic Compute Cloud(Amazon EC2))
    - SAML(Security Assertion Markup Language) 공급자
    - 아이덴티티 공급자(IdP)(예: Login with Amazon, Facebook, Google)

  보안 주체는 IAM 사용자, 그룹 또는 다른 AWS 계정의 역할도 될 수 있습니다(여러분이 소유하지 않은 AWS 계정 포함).

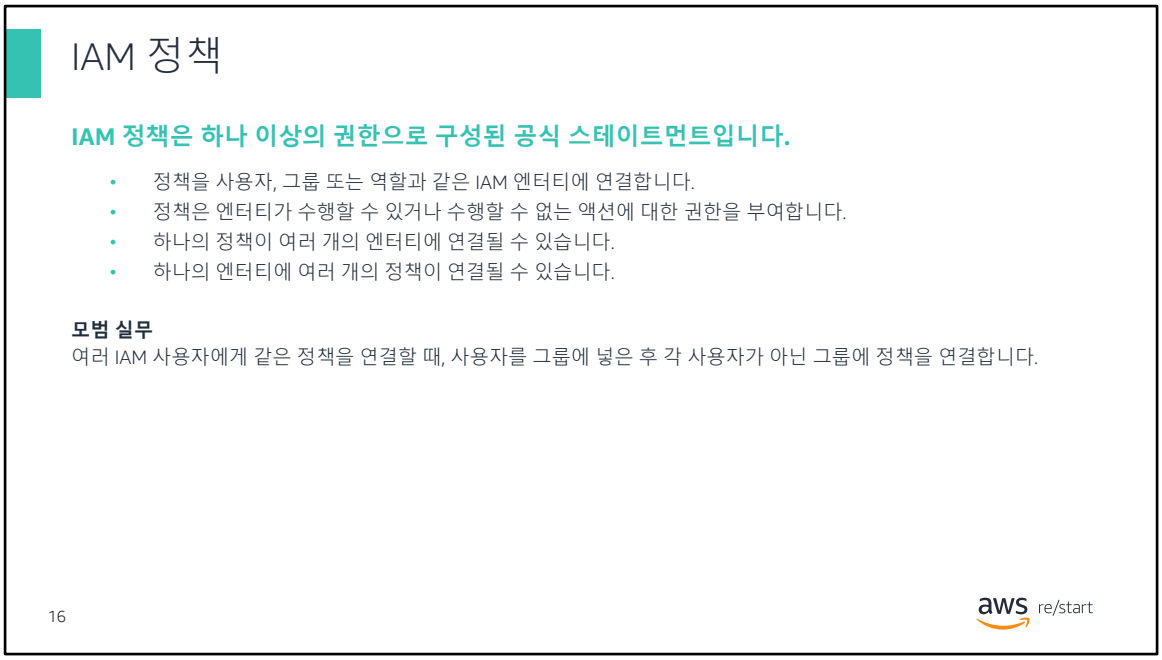
IAM 권한

IAM에서 권한을 결정하는 방법:

aws re/start

정책을 사용하면 IAM 사용자, 그룹, 역할에 부여된 권한을 세밀하게 조정할 수 있습니다. 정책은 JSON(JavaScript Object Notation) 형식으로 저장되므로 버전 제어 시스템에서 사용할 수 있습니다. 각 사용자, 그룹 또는 역할에 대해 최소한의 액세스 권한을 정의하는 것이 모범 실무입니다. 그러면 **권한 부여** 정책을 사용하여 특정 리소스에 대한 액세스를 직접 지정할 수 있습니다.

권한이 허용되었는지 결정할 때, IAM은 먼저 **명시적 차단 정책**을 확인합니다. 명시적 차단 정책이 없는 경우, IAM은 **명시적 허용 정책**을 확인합니다. 명시적 차단 또는 명시적 허용 정책이 없는 경우 IAM은 기본값으로 되돌리는데, 이를 **암시적 차단**이라고 합니다.



IAM 정책은 하나 이상의 권한으로 구성된 공식 스테이트먼트입니다. 정책은 사용자, 그룹, 역할, 리소스 등 IAM 엔터티에 연결될 수 있습니다. 예를 들어 AWS 리소스에 정책을 연결하여 승인된 인터넷 프로토콜(IP) 주소 범위에서 수신되지 않는 모든 요청을 차단할 수 있습니다. 정책은 사용자가 리소스에 대한 액세스를 요청할 때 어떤 액션이 허용되는지, 어떤 리소스에 대한 작업이 허용되는지, 영향이 어떻게 될지 지정합니다.

정책이 평가되는 순서는 평가 결과에 영향을 주지 않습니다. 모든 정책이 평가되며, 결과는 항상 요청 허용 또는 차단입니다. 충돌이 있는 경우, 가장 제한적인 정책이 우선합니다.

IAM 정책의 유형

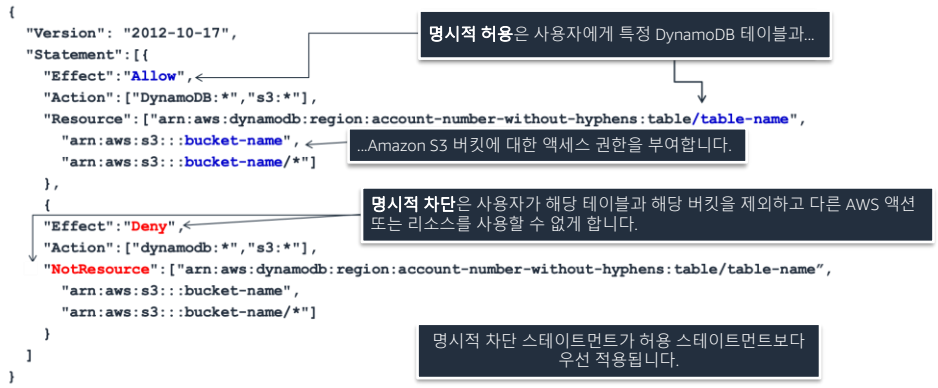
- **아이덴티티 기반 정책**은 IAM 사용자, 역할 또는 그룹과 같은 보안 주체 또는 아이덴티티에 연결할 수 있는 권한 정책입니다. 이러한 정책은 아이덴티티가 수행할 수 있는 액션, 대상 리소스 및 관련 조건을 제어합니다. 아이덴티티 기반 정책은 추가로 다음과 같이 분류될 수 있습니다.
    - 관리형 정책: AWS 계정의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 아이덴티티 기반 정책입니다.
    - 인라인 정책: 여러분이 생성하고 관리하며, 하나의 사용자 그룹 또는 역할에 직접 포함되는 정책입니다.

- **리소스 기반 정책**은 Amazon Simple Storage Service(Amazon S3) 버킷 같은 리소스에 연결할 수 있는 JSON 정책 문서입니다. 이러한 정책은 지정된 보안 주체가 해당 리소스에 대해 수행할 수 있는 액션 및 관련 조건을 제어합니다. 리소스 기반 정책은 인라인 정책이며, 관리형 리소스 기반 정책은 없습니다. 자세한 정보는 **AWS Identity 및 Access Management 사용 설명서**의 IAM의 정책 및 권한을 참조하십시오.

여러 IAM 사용자에게 같은 정책을 연결할 때, 사용자를 그룹에 넣은 후 각 사용자가 아닌 그룹에 정책을 연결합니다. 또한 IAM 정책 시뮬레이터를 사용하여 IAM 및 리소스 기반 정책을 테스트하고 관련 문제를 해결합니다. IAM 정책 시뮬레이터에 관한 자세한 내용은 **AWS Identity 및 Access Management 사용 설명서**의 IAM 정책 시뮬레이터로 IAM 정책 테스트를 참조하십시오.

예: IAM 정책

리소스 기반 정책



aws re/start

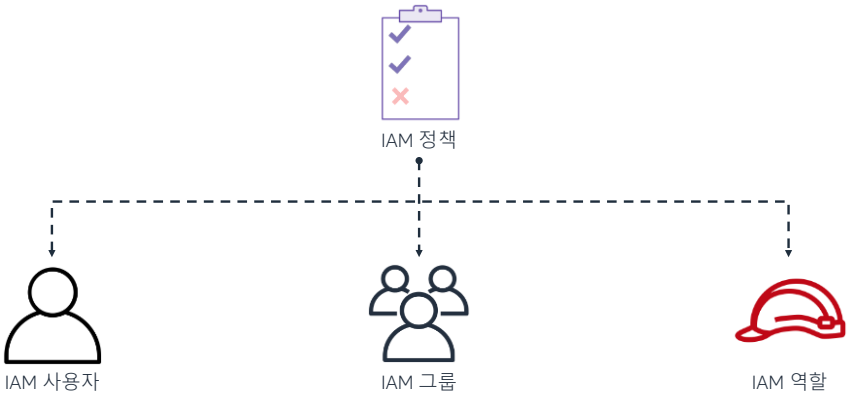
이 정책 예시에서는 다음 리소스에 대한 액세스 권한만 사용자에게 부여합니다.

- 이름이 **table-name**으로 표시되는 Amazon DynamoDB 테이블
- 이름이 **bucket-name**과 버킷에 포함된 모든 객체로 표시되는 AWS 계정의 기업 Amazon S3 버킷

정책에는 명시적 차단("Effect":"Deny") 요소와 **NotResource** 요소가 포함됩니다. 명시적 차단은 다른 정책에서 권한이 부여되었더라도 사용자가 정책에 지정된 AWS 액션과 리소스 외에는 수행 또는 사용할 수 없도록 합니다. 명시적 차단 스테이트먼트가 허용 스테이트먼트보다 우선 적용됩니다.

IAM: 정책 할당

하나의 정책을 IAM 사용자, IAM 그룹, IAM 역할에 할당할 수 있습니다.



aws re/start

같은 정책을 IAM 사용자, IAM 그룹, IAM 역할에 할당할 수 있습니다. 그러면 정책을 재사용할 수 있기 때문에 같은 정책을 각기 다른 아이덴티티를 위해 다시 만들 필요가 없습니다.

IAM 데모

이제 Canvas에 있는 IAM 콘솔 동영상 데모를 살펴봅시다.

핵심 사항

- AWS Identity 및 Access Management(IAM)는 **AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 해주는** 서비스입니다.
- IAM은 다음과 같이 **다양한 유형의 보안 인증 정보**를 제공합니다.
  - 이메일 주소 및 암호
  - IAM 사용자 이름 및 암호
  - 액세스 및 비밀 액세스 키
  - MFA
  - 키 페어
- IAM을 사용하여 **사용자**와 **그룹**을 생성하고 여기에 **역할**을 할당합니다.
- IAM 역할은 특정 리소스에 어떤 액션을 수행할 수 있는지 정의하는 **권한**을 지정합니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- AWS Identity 및 Access Management(IAM)는 AWS 리소스에 대한 액세스를 안전하게 제어할 수 있도록 해주는 서비스입니다.
- IAM은 다음과 같이 다양한 유형의 보안 인증 정보를 제공합니다.
  - 이메일 주소 및 암호
  - IAM 사용자 이름 및 암호
  - 액세스 및 비밀 액세스 키
  - MFA
  - 키 페어
- IAM을 사용하여 사용자와 그룹을 생성하고 여기에 역할을 할당합니다.
- IAM 역할은 특정 리소스에 어떤 액션을 수행할 수 있는지 정의하는 권한을 지정합니다.