aws re/start

예방: 아이덴티티 관리

Security Fundamentals

보안 수명 주기: 예방 - 아이덴티티 관리를 시작하겠습니다.

교육 내용

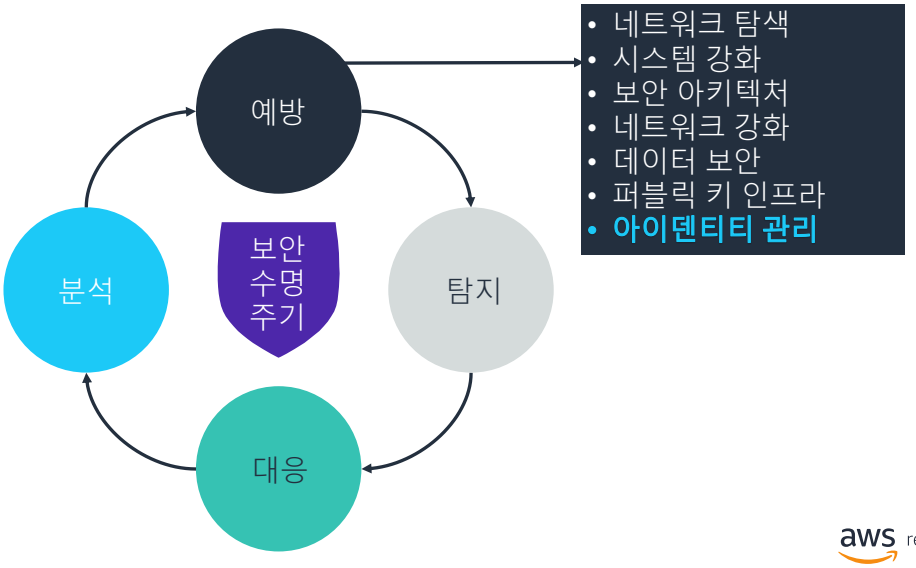
이 강의의 핵심

배울 내용은 다음과 같습니다.

- 아이덴티티 관리의 정의와 다양한 요소를 설명합니다.
- 인증의 원리를 설명합니다.
- 인증 요인의 다양한 유형을 설명합니다.

이 강의에서는 현대적인 IT 보안 솔루션에서 신뢰할 수 있는 인증이 어떻게 핵심적인 구성 요소가 되는지 알아봅니다. 그 원리에 관해서도 알아봅니다.

보안 수명 주기: 예방



aws re/start

복습하자면 보안 수명 주기는 이렇게 구성됩니다.

- **예방** - 첫 번째 방어선입니다.
- **탐지** - 예방이 실패했을 때 수행됩니다.
- **대응** - 보안 위협을 탐지했을 때 취해야 할 조치를 설명합니다.
- **분석** - 향후에 문제가 다시 발생하지 않도록 예방하는 새로운 조치를 구현하면서 주기가 완료됩니다.

이 강의에서는 **아이덴티티 관리의** 개념과 예방 단계에서 사용할 수 있는 방법에 관해 배웁니다.

아이덴티티 관리란?

주체, 객체, 그들의 액세스 권한을 적극적으로 관리합니다.

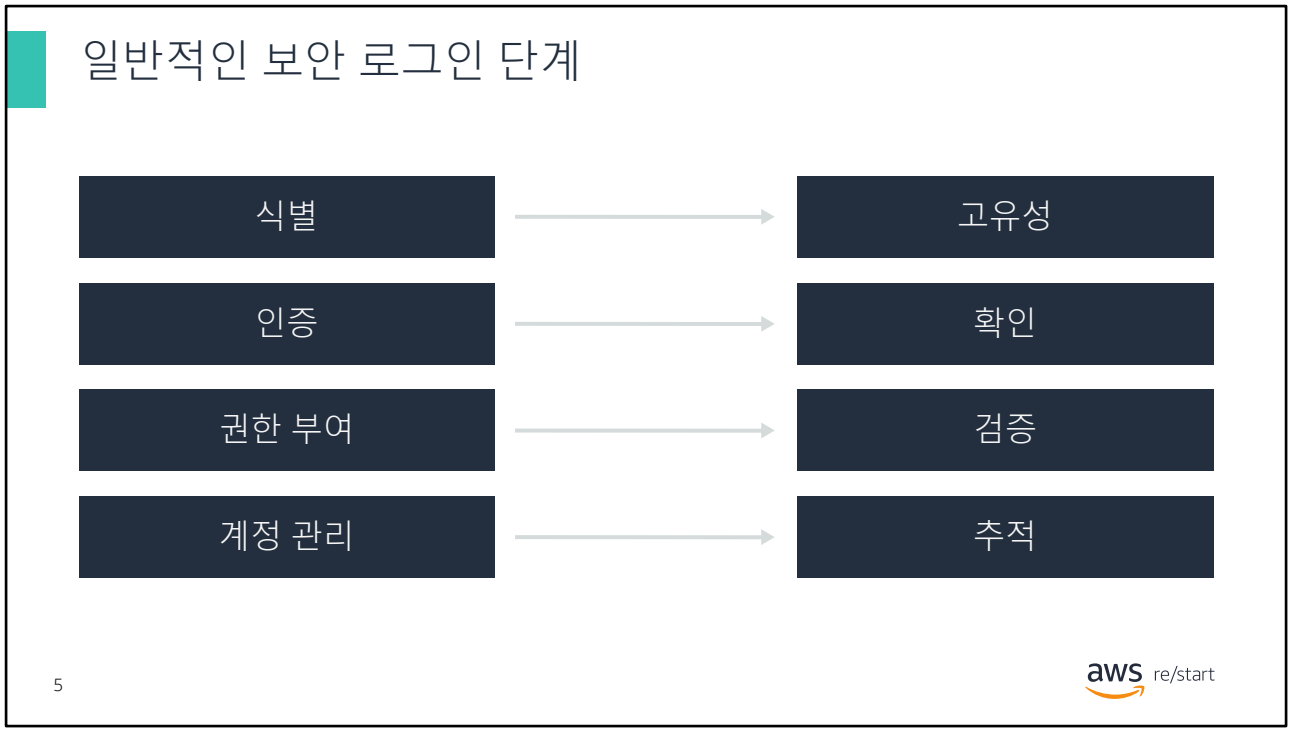
아이덴티티가 리소스에 대한 적절한 액세스를 얻게 합니다.

리소스에 액세스를 부여하는 데 있어 시스템의 확장성을 유지합니다.

aws re/start

아이덴티티 관리는 액세스 권한과 관련하여 주체, 객체, 그리고 그 관계를 적극적으로 관리하는 것입니다.

아이덴티티 관리를 통해 사용자 또는 다른 유형의 아이덴티티는 필요한 리소스에 적합하며 정확한 수준의 액세스 권한을 적절한 시점에 받습니다. 아이덴티티 관리를 구현함으로써 시스템은 리소스에 대한 액세스 권한을 식별 및 부여하는 데 확장성을 유지합니다.



식별, 인증, 권한 부여, 계정 관리는 사용자가 시스템에 로그인할 때 적용되는 일반적인 보안 단계입니다.

비유를 위해 회사의 시설에 물리적인 액세스를 얻고자 하는 방문자의 상황을 예로 들어보겠습니다.

- **식별** - 방문자는 먼저 안내 직원에게 사진이 포함된 신분증을 보여주면서 본인이 맞는지 증명해야 합니다.
- **인증** - 안내 직원은 사진과 앞에 선 사람을 비교하여 방문자의 아이덴티티를 인증합니다.
- **권한 부여** - 방문자를 기다리고 있는 사람이 있으며, 시설에 들어가도록 허용해야 하다는 것을 알리기 위해 안내 직원은 연락 담당자에게 전화하여 방문자에게 액세스를 부여할 것을 요청합니다. 안내 직원은 다음과 같은 행동을 할 수도 있습니다.
    - 방문자에게 배지를 발급해 줍니다.
    - 다른 직원에게 방문자가 권한을 부여받았다는 점을 입증하기 위해 회사의 담당자가 방문자를 시설로 안내하도록 요구합니다.
- **계정 관리** - 방문자에게 방문록에 서명하도록 요구합니다. 방문자가 로그에 다음 정보를 입력합니다.

- 이름
- 도착한 날짜 및 시간과 떠난 날짜 및 시간
- 방문자 배지의 개수
- 연락 담당자의 이름
- 방문 목적

개인 식별 정보(PII)

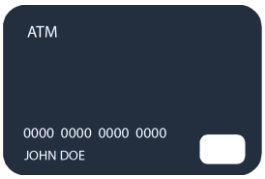
- 엔터티를 고유하게 식별하는 데 사용할 수 있는 데이터
- 예:

aws re/start

개인 식별 정보(PII)는 단독으로 사용하거나 다른 관련 데이터와 함께 사용할 때 개인이 식별되는 데이터 유형입니다. PII에는 개인을 고유하게 식별할 수 있는 여권 정보와 같은 직접 식별자 또는 개인을 식별하는 데 도움이 되는 생일과 같은 간접 식별자가 포함될 수 있습니다.

인증 요소

Pa33wOrd

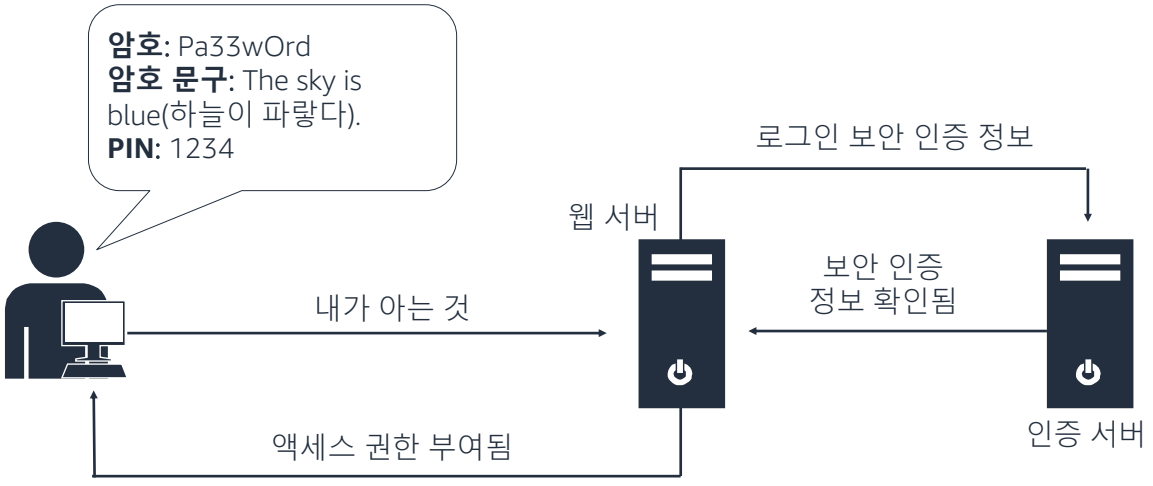


사용자, 프로세스, 디바이스의 아이덴티티를 인증하거나 확인하는 데 여러 요소를 사용하여 액세스를 한층 더 제어할 수 있습니다.

aws re/start

인증 요소의 세 가지 유형은 내가 아는 것, 내가 가지고 있는 것, 내 일부인 것입니다. 모든 인증 도구가 하나 이상의 인증 요소를 포함합니다.

인증 요소: 내가 아는 것



aws re/start

암호, 암호 문구, 개인 식별 번호(PIN)는 인증 요소의 예입니다. 이 요소는 구현하기가 더 간단하지만 가장 보안이 취약하기도 합니다.

인증 요소 - 내가 가지고 있는 것

- 물리적으로 소유하는 것을 사용하여 인증합니다.
- 예:
  - 스마트 카드
  - 인증서
  - 토큰
  - USB 키
  - 키
  - 가상 카드
  - Transaction Authentication Number(TAN)

RSASecureID

USB 키

물리적 키

스마트 카드

aws re/start

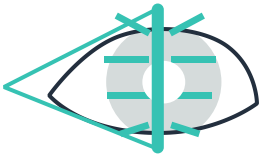
내가 가지고 있는 것을 사용하면 안전하게 인증할 수 있습니다. 이 방법은 내가 아는 것을 제공한 후 두 번째 요소 인증 시스템으로 구현되는 경우가 많습니다.

인증 요소: 내 일부인 것

- 내 일부인 것을 검증하는 데 생체 인식 디바이스가 사용됩니다.
- 생체 인식 디바이스가 사람의 속성을 기반으로 인증합니다.
- 예:
  - 지문 리더
  - 손 모양
  - 망막 스캐너
  - 얼굴 인식
  - 홍채 인식
  - 서명 분석

지문 리더

망막 스캐너



얼굴 인식

지문이나 망막 패턴과 같은 사람의 고유한 속성을 검증하는 인증 메커니즘은 가장 복잡하고 비용이 많이 드는 솔루션입니다. 그러나 잘 구성하면 인증의 신뢰성이 매우 높습니다.

이런 인증 유형에서는 생체 정보의 정확성이 가장 중요한 요소입니다.

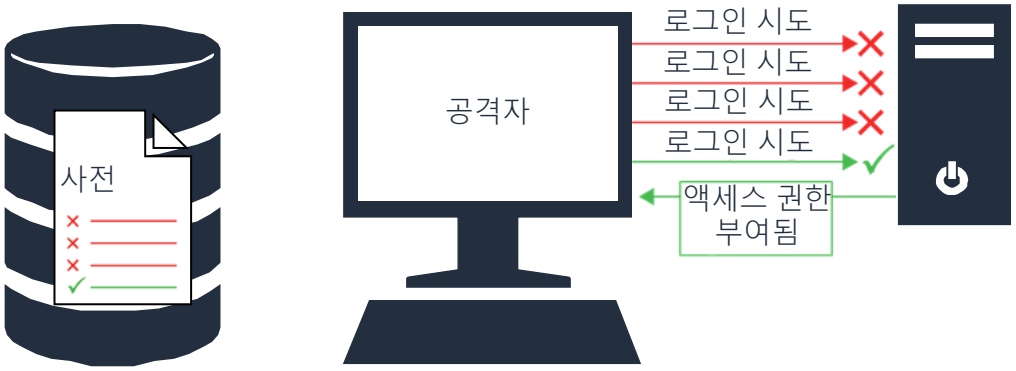
인증: 암호 정책

- 비밀이 생성되는 방법을 정의하는 설정 그룹입니다.
- 다음 파라미터를 포함합니다.
  - 최소 문자 수
  - 암호 복잡성
  - 암호 최대 사용 기간
- 강력한 암호는 시스템이 컴퓨팅하기는 어렵지만 사람이 기억하기는 쉬운 암호입니다.

암호 인증을 사용하면 암호 관리를 제어하는 것이 매우 중요합니다. 암호 인증을 관리하는 가장 기본적인 방법은 암호 파라미터 또는 규칙에 정책을 정의하는 것입니다.

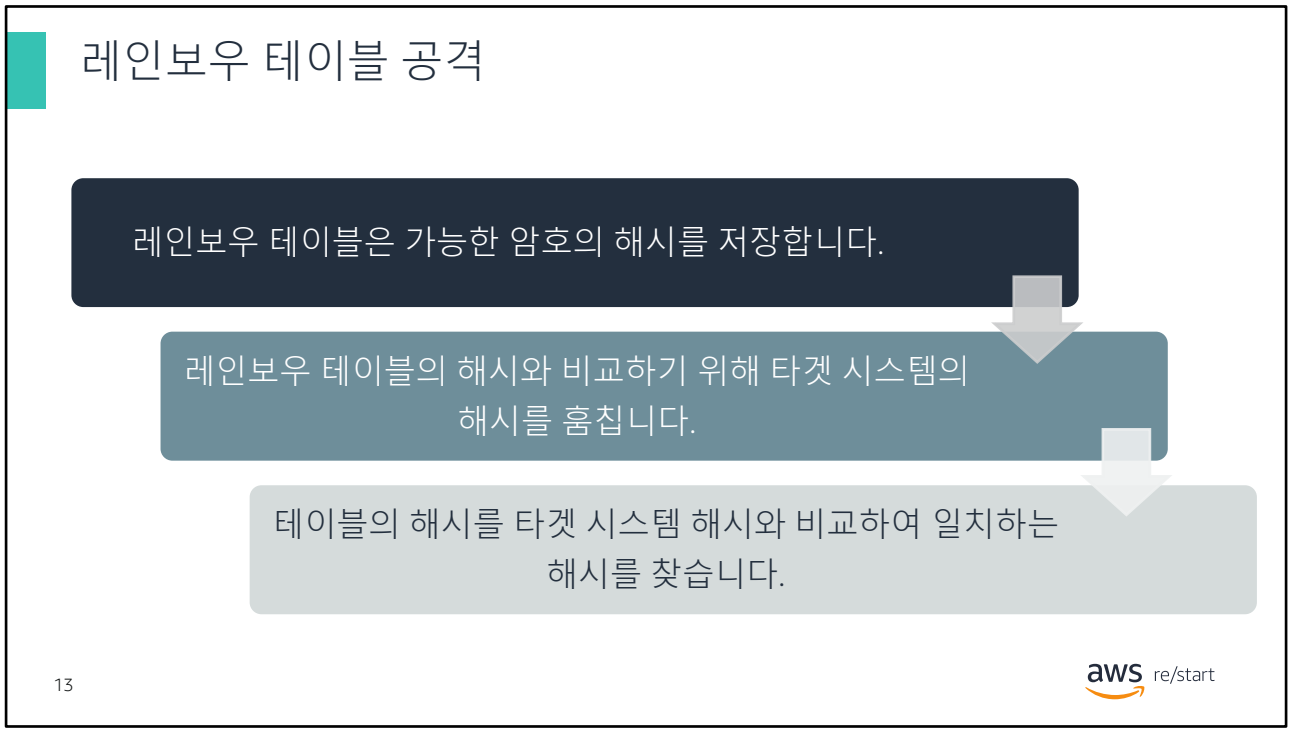
사전 공격

시스템에 로그인하기 위해 사전에 정의된 단어 목록을 암호로 사용합니다.



aws re/start

암호 규칙을 정의할 때는 암호 인증이 당할 수 있는 공격의 유형을 이해해야 합니다. 그런 공격 중 하나는 **사전 공격**입니다. 사전 공격은 일치하는 암호를 찾을 때까지 체계적으로 사전의 각 단어를 암호로 입력합니다. 사전 공격의 대응 조치에는 강력한 암호 정책을 만들고 일정 시도 횟수를 초과하면 액세스를 차단하는 방법이 있습니다.

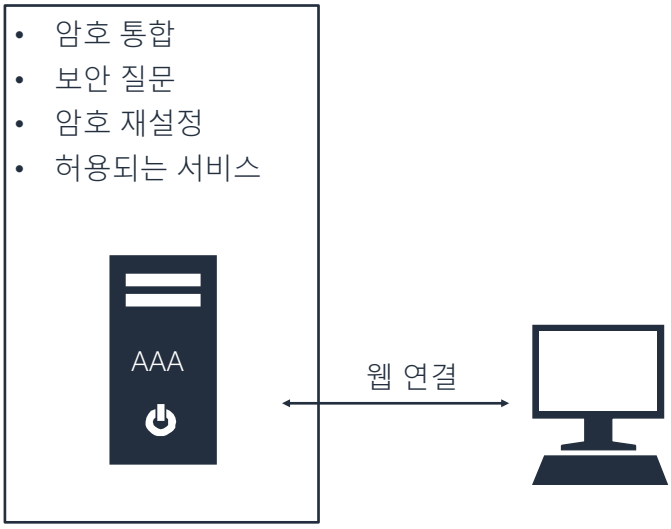


다른 암호 인증 공격 유형으로는 **레인보우 테이블 공격**이 있습니다. 텍스트 암호의 미리 컴퓨팅된 해시를 사용하는 방법입니다. 이 미리 컴퓨팅된 해시를 훔친 해시와 비교하여 해당하는 암호를 찾습니다.

암호 해시는 고유한 암호화 값입니다. 이 암호 해시는 텍스트 암호의 값을 알고리즘을 사용하여 변형해서 생성합니다. 이 알고리즘을 사용하면 특정 입력 값에 항상 같은 해시 값이 생성됩니다. 레인보우 테이블 목록은 특정 해시 알고리즘에 대해 암호화된 암호의 평문 값이기 때문에 일치하는 해시 값을 찾으면 한 암호의 텍스트 암호 값을 쉽게 찾을 수 있습니다.

암호 관리자

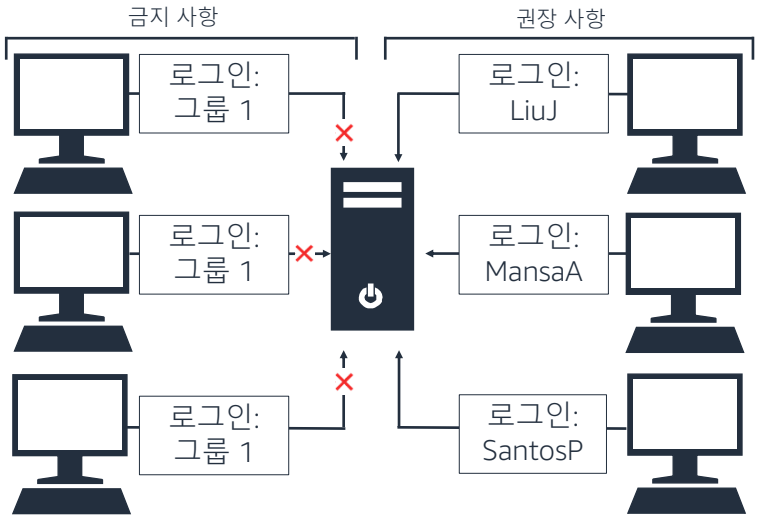
- 중앙화된 인증 시스템을 통해 운영됩니다.
- 추가 로그인 단계를 요구하여 보안을 향상합니다.
- 암호 재설정을 허용합니다.
- 특정 보안 인증 정보를 사용하는 서비스를 관리합니다.
- 로컬 시스템에 개인 암호를 저장합니다.



암호 관리 시스템을 사용하면 좋은 점 중 하나는 사용자에게 보안 인증 정보를 관리하는 데 더 많은 제어권을 준다는 점입니다.

그룹 계정

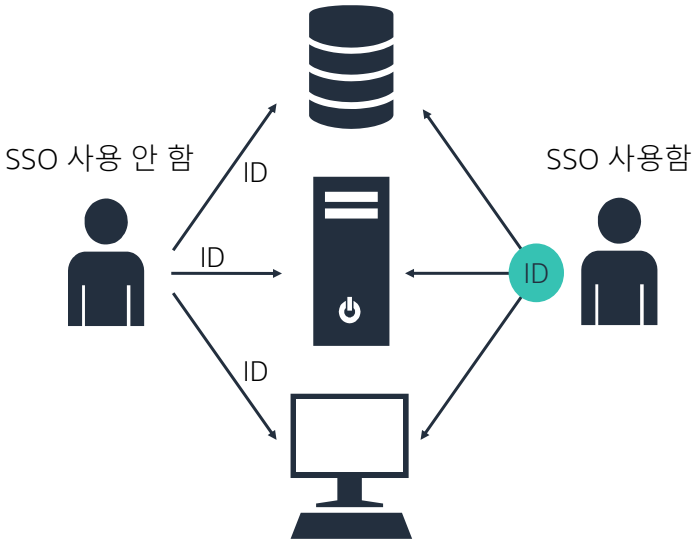
- 그룹 계정을 사용하지 **마십시오**.



인증을 강화하기 위한 모범 실무는 그룹 계정을 사용하지 않는 것입니다. 그룹 계정은 책임을 지지 않기 때문입니다. 그룹 계정은 여러 그룹의 인증을 허용합니다.

통합 인증(SSO)

- 두 개의 독립적인 시스템 간에 암호를 동기화합니다.
- 두 시스템 모두에서 일반적이고 신뢰할 수 있는 로그인 보안 인증 정보를 사용합니다.
- 두 시스템은 독립성을 유지합니다.
- 두 시스템은 신뢰 관계가 아니며 같은 디렉터리 구조에 속하지 않습니다.

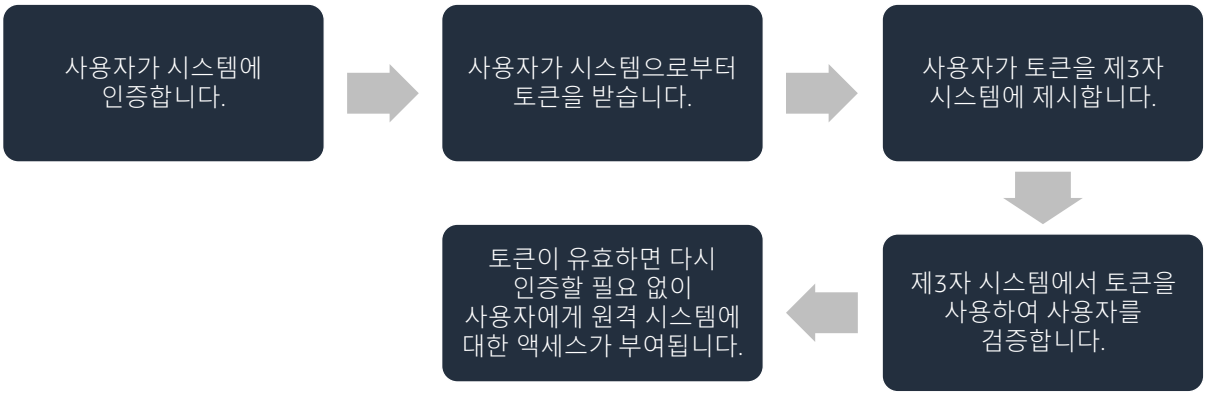


aws re/start

통합 인증(SSO)을 사용하면 사용자는 한 번 로그인한 후 애플리케이션마다 로그인 보안 인증 정보를 다시 입력할 필요 없이 서로 다른 애플리케이션에 대한 액세스 권한을 얻을 수 있습니다.

페더레이션 사용자

- 페더레이션 사용자는 통합 인증(SSO)의 한 형태입니다.
- 하나의 계정을 여러 서비스에 사용합니다.



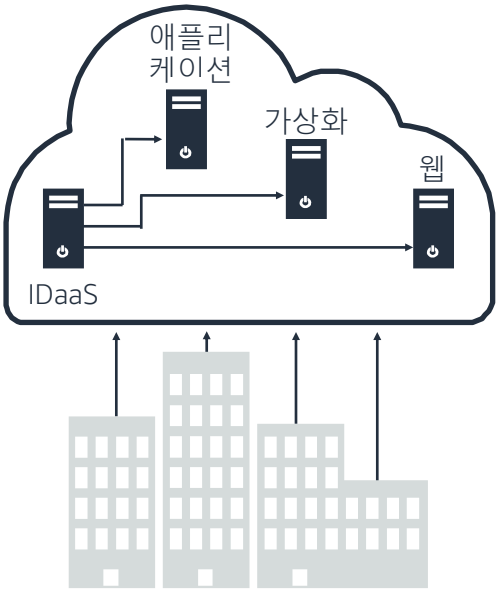
aws re/start

페더레이션 사용자는 통합 인증(SSO) 구현의 한 형태로, 웹 아이덴티티 간에 사용됩니다. 토큰을 사용하여 서로 떨어진 시스템 간에 사용자 아이덴티티를 확인합니다.

SSO를 사용하면 개인은 하나의 그룹 또는 개인 보안 인증 정보를 사용하여 서로 다른 네트워크 또는 서비스에 로그인할 수 있습니다. 예를 들어, SSO를 사용하여 Google 계정 보안 인증 정보로 Facebook에 로그인할 수 있습니다.

아이덴티티 공급자

보안 인증 정보가 클라우드에 저장되며 클라우드 서비스에 사용됩니다.



aws re/start

클라우드에서는 서비스형 아이덴티티 및 액세스 관리(IDaaS)가 사용자의 액세스 수준을 생성하고 제어합니다. 클라우드의 SSO라고 생각하면 됩니다. 제3자 서비스 공급자는 사용자 레코드의 원격 데이터베이스를 사용하여 하나의 로그인 보안 인증 정보 세트를 제공합니다. 이 보안 인증 정보는 플랫폼, 애플리케이션, 네트워크 전체에서 엔터티가 주장하는 신원이 실제와 일치하는지 확인합니다. IT 리소스는 아이덴티티 공급자를 통해 엔터티가 해당 리소스에 액세스해도 되는지, 어느 수준으로 액세스할 수 있는지 확인합니다.

Amazon Cognito는 AWS 클라우드에서 사용할 수 있는 아이덴티티 공급자의 예입니다.

핵심 사항

- 아이덴티티 관리를 통해 사용자는 필요한 리소스에 적합하며 적절한 수준의 액세스 권한을 적절한 시점에 받습니다.
- 인증 요소는 다음과 같이 분류할 수 있습니다.
  - 내가 아는 것. 예: 암호
  - 내가 가지고 있는 것. 예: 스마트 카드
  - 내 일부인 것. 예: 지문
- 효과적인 아이덴티티 관리 솔루션에는 암호 정책을 수립하는 것, 암호 관리자를 사용하는 것, 통합 인증(SSO)과 페더레이션형 ID 관리를 사용하는 것이 있습니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- 아이덴티티 관리를 통해 사용자는 필요한 리소스에 적합하며 적절한 수준의 액세스 권한을 적절한 시점에 받습니다.
- 인증 요소는 다음과 같이 분류할 수 있습니다.
  - 내가 아는 것. 예: 암호
  - 내가 가지고 있는 것. 예: 스마트 카드
  - 내 일부인 것. 예: 지문
- 효과적인 아이덴티티 관리 솔루션에는 암호 정책을 수립하는 것, 암호 관리자를 사용하는 것, 통합 인증(SSO)과 페더레이션형 ID 관리를 적절하게 사용하는 것이 있습니다.