사용자 가이드

AWS 설정

AWS 설정: 사용자 가이드

Table of Contents

개요

이 안내서는 최신 보안 모범 사례에 따라 새 AWS 계정 관리자를 생성하고, AWS IAM Identity Center에 첫 번째 관리 사용자를 설정하는 지침을 제공합니다.

AWS 계정은 AWS 서비스에 액세스하기 위해 필요하며, 다음과 같이 두 가지 기본 기능으로 사용됩니다.

- 컨테이너 - AWS 계정은 AWS 고객으로서 생성할 수 있는 모든 AWS 리소스를 담는 컨테이너입니다. Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Relational Database Service(Amazon RDS) 데이터베이스를 생성하여 데이터를 저장하거나, Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 생성하여 데이터를 처리하면, 계정에 리소스가 생성됩니다. 모든 리소스는 리소스를 포함하거나 소유한 계정의 계정 ID가 포함된 Amazon 리소스 이름(ARN)으로 고유하게 식별됩니다.
- 보안 경계 - AWS 계정은 AWS 리소스의 기본 보안 경계입니다. 특정 계정에서 생성한 리소스는 동일한 계정의 자격 증명을 가진 사용자만 사용할 수 있습니다.

  계정에서 생성할 수 있는 주요 리소스에는 IAM 사용자 및 역할 등의 ID, 엔터프라이즈 사용자 디렉터리, 웹 ID 제공업체, IAM Identity Center 디렉터리, 또는 ID 소스에서 제공받은 자격 증명을 사용하여 AWS 서비스에 액세스하는 페더레이션 ID가 있습니다. 이러한 ID에는 누군가가 AWS에 로그인하거나 인증하는 데 사용할 수 있는 자격 증명이 있습니다. 또한 로그인한 사람이 계정의 리소스로 수행할 수 있는 권한을 지정하는 권한 정책이 있습니다.

용어

아마존 웹 서비스 (AWS) 는 일반적인 용어를 사용하여 로그인 프로세스를 설명합니다. 이러한 용어를 숙지하는 것이 좋습니다.

관리자

a라고도 합니다. AWS 계정 관리자 또는 IAM 관리자. 관리자 (일반적으로 정보 기술 (IT) 직원은 다음을 감독하는 개인입니다. AWS 계정. 관리자는 다음에 대해 더 높은 수준의 권한을 가집니다. AWS 계정 해당 조직의 다른 구성원보다 뛰어납니다. 관리자는 다음과 같은 설정을 지정하고 구현합니다. AWS 계정. 또한 IAM ID 센터 사용자를 IAM 생성하기도 합니다. 관리자는 이러한 사용자에게 액세스 자격 증명과 URL 로그인할 수 있는 로그인을 제공합니다. AWS.

계정

표준 AWS 계정 두 가지가 모두 들어 있습니다. AWS 리소스와 해당 리소스에 액세스할 수 있는 ID 계정은 계정 소유자의 이메일 주소 및 암호와 연결됩니다.

보안 인증 정보

액세스 자격 증명 또는 보안 인증 정보라고도 합니다. 자격 증명은 사용자가 제공하는 정보입니다. AWS 로그인하고 액세스 권한 획득하기 AWS 있습니다. 자격 증명에는 이메일 주소, 사용자 이름, 사용자 정의 암호, 계정 ID 또는 별칭, 확인 코드, 일회용 다단계 인증 (MFA) 코드가 포함될 수 있습니다. 인증 및 권한 부여에서 시스템은 보안 인증을 사용하여 호출하는 사용자와 요청된 액세스를 허용할지 여부를 식별합니다. In AWS이러한 자격 증명은 일반적으로 액세스 키 ID와 보안 액세스 키입니다.

자격 증명에 대한 자세한 내용은 자격 증명 이해 및 획득을 참조하십시오. AWS 자격 증명.

> **Note**
>
> 사용자가 제출해야 하는 보안 인증 정보의 유형은 사용자 유형에 따라 다릅니다.

기업 보안 인증

사용자가 회사 네트워크 및 리소스에 액세스할 때 제공하는 보안 인증 정보. 기업 관리자가 다음을 설정할 수 있습니다. AWS 계정 회사 네트워크 및 리소스에 액세스할 때 사용하는 것과 동일한 자격 증명으로 액세스할 수 있도록 합니다. 이러한 보안 인증 정보는 관리자 또는 지원 센터 직원이 제공합니다.

프로필

에 가입할 때 AWS 빌더 ID로 프로필을 생성합니다. 프로필에는 제공한 연락처 정보와 다단계 인증(MFA) 장치 및 활성 세션을 관리할 수 있는 기능이 포함됩니다. 또한 프로필에서의 개인 정보 보호 및 데이터 취급 방법도 알아볼 수 있습니다. 프로필 및 프로필과의 관계에 대한 자세한 내용은 AWS 계정를 참조하십시오. AWS 빌더 ID 및 기타 AWS 자격 증명.

User

사용자란 API 전화를 거는 계정을 보유한 개인 또는 애플리케이션입니다. AWS 제품. 각 사용자는 제품 내에서 고유한 이름을 가집니다. AWS 계정 그리고 다른 사람과 공유되지 않는 보안 자격 증명 세트. 이러한 자격 증명은 보안 자격 증명과 별개입니다. AWS 계정각 사용자는 오직 한 개의 과만 연결됩니다. AWS 계정.

루트 사용자 보안 인증 정보

루트 사용자 자격 증명은 로그인할 때 사용한 자격 증명과 동일합니다. AWS Management Console 루트 사용자로 루트 사용자에 대한 자세한 내용은 루트 사용자를 참조하세요.

확인 코드

인증 코드는 로그인 과정에서 다단계 인증 () 을 사용하여 신원을 확인합니다. MFA 확인 코드의 전달 방법은 다양합니다. 문자 메시지나 이메일을 통해 전송할 수 있습니다. 자세한 내용은 관리자에게 문의하세요.

AWS 사용자 및 자격 증명

다음과 상호 작용할 때 AWS, 다음을 지정합니다. AWS 자신이 누구인지, 요청한 리소스에 액세스할 권한이 있는지 여부를 확인하기 위한 보안 자격 증명. AWS 보안 자격 증명을 사용하여 요청을 인증하고 권한을 부여합니다.

예를 들어, Amazon Simple Storage Service(S3) 버킷에서 보호 파일을 다운로드하려면 보안 인증 정보에서 해당 액세스를 허용해야 합니다. 자격 증명에 파일 다운로드 권한이 없는 것으로 표시되는 경우 AWS 요청을 거부합니다. 하지만 공개적으로 공유되는 Amazon S3 버킷에서 파일을 다운로드하는 데에는 보안 인증 정보가 요구되지 않습니다.

루트 사용자

계정 소유자 또는 계정 루트 사용자라고도 합니다. 루트 사용자는 모든 사용자에 대한 완전한 액세스 권한을 가집니다. AWS 내 서비스 및 리소스 AWS 계정. 처음 만들 때 AWS 계정모든 계정에 완전히 액세스할 수 있는 단일 로그인 ID로 시작합니다. AWS 계정의 서비스 및 리소스. 이 ID는 AWS 계정 루트 사용자. 에 로그인할 수 있습니다. AWS Management Console계정을 만들 때 사용한 이메일 주소와 암호를 사용하여 루트 사용자로 설정합니다. 로그인 방법에 대한 단계별 지침은 로그인을 참조하십시오. AWS Management Console 루트 사용자로.

> **Important**
>
> 를 생성할 때 AWS 계정모든 계정에 완전히 액세스할 수 있는 하나의 로그인 ID로 시작합니다. AWS 서비스 및 계정 내 리소스. 이 ID를 다음과 같이 부릅니다. AWS 계정 루트 사용자는 계정을 만들 때 사용한 이메일 주소와 암호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오. IAM

루트 사용자를 포함한 IAM ID에 대한 자세한 내용은 IAMID (사용자, 사용자 그룹 및 역할) 를 참조하십시오.

IAMID 센터 사용자

IAMID 센터 사용자는 다음을 통해 로그인합니다. AWS 포털에 액세스하세요. 더 AWS 액세스 포털 또는 특정 URL 로그인은 관리자 또는 헬프 데스크 직원이 제공합니다. IAM아이덴티티 센터 사용자를 생성한 경우 AWS 계정 IAMIdentity Center 사용자 가입 초대가 다음 이메일 주소로 발송되었습니다. AWS 계정. 특정 URL 로그인은 이메일 초대장에 포함됩니다. IAM아이덴티티 센터 사용자는 다음을 통해 로그인할 수 없습니다. AWS Management Console. 로그인 방법에 대한 단계별 지침은 로그인을 참조하십시오. AWS 포털에 접속하세요.

> **Note**
>
> 특정 로그인을 URL 북마크에 추가하는 것이 좋습니다. AWS 나중에 빠르게 액세스할 수 있도록 포털에 액세스하세요.

ID 센터에 대한 자세한 내용은 IAM ID 센터란 IAM 무엇입니까? 를 참조하십시오.

페더레이션 자격 증명

페더레이션 ID는 잘 알려진 외부 ID 공급자 (IdP) 를 사용하여 로그인할 수 있는 사용자입니다. 예를 들어 Login with Amazon, 페이스북, 구글 또는 다른 OpenID Connect OIDC () 호환 IdP로 로그인할 수 있습니다. 웹 ID 페더레이션을 사용하면 인증 토큰을 받은 다음 해당 토큰을 임시 보안 자격 증명으로 교환할 수 있습니다. AWS 이는 내 리소스를 사용할 권한이 있는 IAM 역할에 매핑됩니다. AWS 계정. 으로 로그인하지 마십시오. AWS Management Console 또는 AWS 액세스 포털. 대신 사용 중인 외부 ID에 따라 로그인 방법이 결정됩니다.

자세한 내용은 페더레이션 ID로 로그인을 참조하세요.

IAM사용자

IAM사용자는 자신이 만든 엔티티입니다. AWS. 이 사용자는 귀하 내부의 ID입니다. AWS 계정 그러면 특정 사용자 지정 권한이 부여됩니다. IAM사용자 자격 증명은 로그인하는 데 사용되는 이름과 암호로 구성됩니다. AWS Management Console. 로그인 방법에 대한 단계별 지침은 로그인을 참조하십시오. AWS Management Console IAM사용자로.

사용자를 포함한 IAM ID에 대한 자세한 내용은 IAM ID (IAM사용자, 사용자 그룹 및 역할) 를 참조하십시오.

AWS 빌더 ID 사용자

한 사람으로서 AWS 빌더 ID 사용자라면, 특별히 로그인해야 합니다. AWS 액세스하려는 서비스 또는 도구. 원래 요청 ping에 대한 AWS 빌더 ID 사용자는 모든 것을 보완합니다. AWS 계정 이미 생성했거나 만들고 싶습니다. 원래 요청 ping에 대한 AWS 빌더 ID는 사용자를 개인으로 나타내며 이를 사용하여 액세스할 수 있습니다. AWS 보안이 필요 없는 서비스 및 도구 AWS 계정. 또한 정보를 보고 업데이트할 수 있는 프로필도 있습니다. 자세한 내용은 로그인하기를 참조하십시오. AWS 빌더 ID.

사전 조건 및 고려 사항

설정 프로세스를 시작하기 전에, 계정 요구 사항을 검토하고, AWS 계정이 두 개 이상이 필요한지 여부를 고려하고, IAM Identity Center에서 관리 액세스를 위해 계정을 설정하는 데 필요한 요구 사항을 이해해야 합니다.

AWS 계정 요구 사항

AWS 계정에 가입하려면 다음 정보를 제공해야 합니다.

- 계정 이름 - 계정 이름 청구서, Billing and Cost Management 대시보드, AWS Organizations 콘솔 등 다양한 장소에 표시됩니다.

  계정 이름을 쉽게 인식하고 소유할 수 있는 다른 계정과 구분할 수 있도록 계정 이름 지정 표준을 사용하는 것이 좋습니다. 회사 계정인 경우 조직-목적-환경(예: AnyCompany-감사-제품)과 같은 이름 지정 표준을 사용하는 것이 좋습니다. 개인 계정인 경우 이름, 성, 목적 등의 이름 지정 표준을 사용하는 것이 좋습니다(예: \paulo-santos-testaccount).
- 이메일 주소 - 이메일 주소는 계정에서 루트 사용자의 로그인 이름으로 사용되며, 비밀번호를 잊어버리는 등의 계정 복구에 필요합니다. 해당 이메일 주소로 전송된 메시지를 수신할 수 있어야 합니다. 특정 작업을 수행하기 전에 이메일 계정에 액세스할 수 있는지 확인해야 합니다.

  > **Important**
  >
  > 이 계정이 기업용인 경우 회사 배포 목록(예: `it.admins@example.com`)을 사용하는 것을 권장합니다. 개인의 회사 이메일 주소(예: `paulo.santos@example.com`)를 사용하지 마세요. 이렇게 하면 직원이 직위를 변경하거나 퇴사하는 AWS 계정 경우 회사에서 해당 정보에 액세스할 수 있습니다. 이메일 주소를 사용하여 계정의 루트 사용자 자격 증명을 재설정할 수 있습니다. 해동 배포 목록 또는 주소에 대한 액세스를 보호해야 합니다.
- 전화번호 - 이 번호는 계정 소유권을 확인할 때 사용할 수 있습니다. 해당 전화번호에 수신되는 전화를 받을 수 있어야 합니다.

  > **Important**
  >
  > 이 계정이 기업용인 경우 개인 전화번호 대신 회사 전화번호를 사용하는 것이 좋습니다. 이렇게 하면 직원이 직위를 변경하거나 퇴사하는 AWS 계정 경우 회사에서 해당 정보에 액세스할 수 있습니다.

- 다중 인증 디바이스 - AWS 리소스를 보호하려면 루트 사용자 계정에 다중 인증(MFA)을 활성화합니다. 다중 인증(MFA)이 활성화되면 일반 로그인 자격 증명 외에도 추가 보안 계층을 제공하는 보조 인증이 필요합니다. IAM에 대한 자세한 내용은 IAM 사용 설명서의 IAM이란 무엇인가요?를 참조하세요.
- AWS Support플랜 - 계정 생성 과정에서 사용 가능한 플랜 중 하나를 선택하라는 메시지가 표시됩니다. 사용 가능한 요금제에 대한 설명은 AWS Support 플랜 비교를 참조하세요.

IAM Identity Center 관련 고려 사항

다음 주제에서는 특정 환경에 맞춰 IAM Identity Center를 설정하기 위한 지침을 제공합니다. 2부: IAM Identity Center에서 관리자 생성 섹션으로 진행하기 전에 사용자의 환경에 적용되는 지침이 무엇인지 알아보세요.

주제

- Active Directory 또는 외부 ID 제공업체(IdP)
- AWS Organizations
- IAM 역할
- 차세대 방화벽 및 보안 웹 게이트웨이

Active Directory 또는 외부 ID 제공업체(IdP)

Active Directory 또는 외부 ID 제공업체를 통해 사용자 및 그룹을 관리하고 있다면, IAM Identity Center를 활성화하고 ID 소스를 선택할 때 해당 ID 소스를 연결하는 것을 고려해 보는 것이 좋습니다. 기본 Identity Center 디렉터리에 사용자 및 그룹을 생성하기 전에 해당 작업을 수행하면 나중에 ID 소스를 변경할 때 추가 구성 필요해지는 상황을 피할 수 있습니다.

Active Directory를 ID 소스로 사용하려면 구성이 다음과 같은 사전 요구 사항을 충족해야 합니다.

- AWS Managed Microsoft AD를 사용하는 경우 AWS Managed Microsoft AD 디렉터리가 설정된 동일한 AWS 리전에서 IAM Identity Center를 활성화해야 합니다. IAM Identity Center는 디렉터리와 동일한 리전에 할당 데이터를 저장합니다. IAM Identity Center를 관리하려면 IAM Identity Center가 구성된 리전으로 전환해야 합니다. 또한, AWS 액세스 포털은 디렉터리와 동일한 액세스 URL을 사용한다는 점에 유의하세요.
- 관리 계정에 있는 Active Directory를 사용합니다.

기존 AD Connector 또는 AWS Managed Microsoft AD 디렉터리가 AWS Directory Service에 설정되어 있어야 하며, 반드시 AWS Organizations 관리 계정 내에 있어야 합니다. 한 번에 AD Connector 한 개 또는 AWS Managed Microsoft AD 한 개만 연결할 수 있습니다. 여러 도메인이나 포리스트를 지원해야 하는 경우 AWS Managed Microsoft AD를 사용합니다. 자세한 내용은 다음을 참조하세요.

- AWS IAM Identity Center 사용 설명서의 AWS Managed Microsoft AD의 디렉터리를 IAM Identity Center에 연결합니다.
- AWS IAM Identity Center 사용 설명서의 Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결합니다.

- 위임된 관리자 계정에 있는 Active Directory를 사용합니다.

  IAM Identity Center 위임 관리자를 활성화하고 Active Directory를 IAM ID 소스로 사용하려는 경우, 위임된 관리자 계정에 있는 AWS Managed Microsoft AD 디렉터리에 설정된 기존 AD Connector 또는 AWS 디렉터리를 사용할 수 있습니다.

  IAM Identity Center 소스를 다른 소스에서 Active Directory로 변경하거나 Active Directory에서 다른 소스로 변경하려는 경우, 해당 디렉터리는 IAM Identity Center에서 위임한 관리자 계정(있는 경우)에 있어야 하며, 그렇지 않으면 관리 계정에 있어야 합니다.

AWS Organizations

AWS 계정은 반드시 AWS Organizations에서 관리해야 합니다. 조직을 설정하지 않았어도 설정할 필요는 없습니다. IAM Identity Center를 활성화하면, AWS가 조직을 생성할지 여부를 선택하게 됩니다.

AWS Organizations를 이미 설정한 경우, 모든 기능이 활성화되어 있는지 확인합니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직 내 모든 기능 활성화를 참조하세요.

IAM Identity Center를 활성화하려면 AWS Organizations 관리 계정의 자격 증명을 사용하여 AWS Management Console에 로그인해야 합니다. AWS Organizations 회원 계정의 자격 증명으로 로그인한 상태에서는 IAM Identity Center를 활성화할 수 없습니다. 자세한 내용은 AWS Organizations 사용 설명서에서 AWS 조직 생성 및 관리를 참조하세요.

IAM 역할

AWS 계정에서 IAM 역할을 이미 구성한 경우, 계정이 IAM 역할 할당량에 근접하고 있는지 확인하는 것을 권장합니다. 자세한 내용은 IAM 객체 할당량을 참조하세요.

할당량에 근접하고 있으면 할당량 증가를 요청해 보세요. 할당량을 증가시키지 않으면 IAM 역할 할당량을 초과한 계정에 권한 세트를 프로비저닝할 때 IAM Identity Center에 문제가 발생할 수 있습니다.

할당량 증가 요청에 대한 자세한 정보는 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

차세대 방화벽 및 보안 웹 게이트웨이

NGFW 또는 SWG와 같은 웹 콘텐츠 필터링 솔루션을 사용하여 특정 AWS 도메인 또는 URL 엔드포인트에 대한 액세스를 필터링하는 경우, 웹 콘텐츠 필터링 솔루션 허용 목록에 다음 도메인 또는 URL 엔드포인트를 추가해야 합니다.

특정 DNS 도메인

- *.awsapps.com (http://awsapps.com/)
- *.signin.aws

특정 URL 엔드포인트

- https://*[yourdirectory]*.awsapps.com/start
- https://*[yourdirectory]*.awsapps.com/login
- https://*[yourregion]*.signin.aws/platform/login

다수의 AWS 계정 사용

AWS 계정은 AWS의 기초적인 보안 경계 역할을 합니다. 이들은 유용한 수준으로 리소스를 격리하는 컨테이너 역할을 합니다. 리소스와 사용자를 격리하는 기능은 안전하게 관리하는 환경을 구축하기 위한 핵심 요구 사항입니다.

리소스를 별도의 AWS 계정에 분리하면 클라우드 환경에서 다음 원칙을 지원하는 데 도움이 됩니다.

- 보안 제어 - 애플리케이션마다 다른 제어 정책 및 메커니즘을 요구하는 다양한 보안 프로필이 있을 수 있습니다. 예를 들어, 감사자와 상담하여 결제 카드 산업(PCI) 보안 표준이 적용되는 워크로드의 모든 요소를 호스팅하는 단일 AWS 계정 감사자를 가리키는 것이 더 쉽습니다.
- 격리 - AWS 계정는 보안 보호 단위입니다. 잠재적 위험과 보안 위협은 AWS 계정 내로 격리하여 다른 요소에 영향을 미치지 않아야 합니다. 팀이나 보안 프로필이 다르기 때문에 보안 요구 사항이 다를 수 있습니다.
- 다양한 팀 - 팀마다 책임과 리소스 요구 사항이 다릅니다. 각 팀을 별도의 AWS 계정로 분리하여 서로 간섭하는 것을 방지할 수 있습니다.

- 데이터 격리 - 팀을 격리하는 것 외에도 데이터 저장소를 계정별로 격리하는 것도 중요합니다. 이렇게 하면 해당 데이터 저장소에 액세스하고 관리할 수 있는 사람의 수를 제한하는 데 도움이 될 수 있습니다. 이것으로 아주 사적인 데이터의 노출을 억제할 수 있어 유럽 연합의 일반 데이터 보호 규정(GDPR)을 준수하는 데 도움이 될 수 있습니다.
- 비즈니스 프로세스 – 사업부 또는 제품마다 목적 및 프로세스가 완전히 다를 수 있습니다. AWS 계정 여러 개를 사용하면 사업부마다 특정 요구 사항을 지원할 수 있습니다.
- 청구 - 청구 단계에서 계정이 항목을 구분할 수 있는 유일한 방법입니다. 여러 계정을 사용하면 청구 단계에서 사업부, 직무 팀 또는 개별 사용자 간에 항목을 구분할 수 있습니다. 모든 청구서를 단일 결제자(AWS Organizations 사용 및 통합 결제)로 통합할 수 있으며, 항목을 AWS 계정별로 구분할 수도 있습니다.
- 할당량 할당 - AWS 서비스 할당량은 각 AWS 계정 할당량에 대해 개별적으로 적용됩니다. 워크로드를 AWS 계정 여러 개로 분리하여 서로의 할당량을 소비하는 것을 방지할 수 있습니다.

안내서에 설명된 모든 권장 사항 및 절차는 AWS Well-Architected Framework를 준수합니다. 이 프레임워크는 유연하고, 복원력이 뛰어나며, 확장 가능한 클라우드 인프라를 설계하는 데 도움을 주기 위한 것입니다. 소규모로 시작하더라도 프레임워크의 지침을 준수하여 진행하는 것이 좋습니다. 규모가 커져도 현재의 운영에 영향을 주지 않으면서 환경을 안전하게 확장할 수 있습니다.

여러 계정을 추가하기 전에 계정을 관리할 계획을 세우는 것이 좋습니다. 이를 위해서는 무료 AWS 서비스인 AWS Organizations를 사용하여 조직 AWS 계정 내 모든 계정을 관리하는 것을 권장합니다.

또한 AWS는 조직에 AWS 관리형 자동화 계층을 추가하고, 이를 Amazon CloudWatch, AWS CloudTrail, AWS Config, AWS Service Catalog 등의 다른 AWS 서비스와 자동으로 통합하는 AWS Control Tower를 제공합니다. 이러한 서비스에는 추가 비용이 발생할 수 있습니다. 자세한 내용은 AWS Control Tower 요금을 참조하세요.

1부: 새 AWS 계정 설정

이 지침은 AWS 계정를 생성하고 루트 사용자 자격 증명을 보호하는 데 도움이 됩니다. 2부: IAM Identity Center에서 관리자 생성 섹션으로 진행하기 전에 모든 단계를 완료합니다.

주제

1단계: AWS 계정에 등록

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. AWS 계정을 선택합니다.

   > **Note**
   >
   > AWS에 최근에 로그인한 경우 콘솔에 로그인을 선택합니다. AWS 계정 새로 생성 옵션이 보이지 않는 경우 먼저 다른 계정으로 로그인을 선택한 다음 새로 생성을 선택합니다AWS 계정.

3. 계정 정보를 입력한 다음 계속을 선택합니다.

   계정 정보, 특히 이메일 주소를 올바르게 입력해야 합니다. 이메일 주소를 잘못 입력하면 계정에 액세스할 수 없습니다.

4. 개인용 또는 전문가용을 선택합니다.

   이러한 옵션의 차이는 당사가 요청하는 정보에만 있습니다. 두 계정 유형 모두 동일한 특징과 기능을 가지고 있습니다.

5. AWS 계정 요구 사항 섹션에 제공된 지침에 따라 회사 또는 개인 정보를 입력합니다.
6. AWS 고객 동의서를 읽고 수락합니다.
7. 계정 생성 및 계속하기를 선택합니다.

   이제 AWS 계정이 사용할 준비가 되었음을 확인하는 이메일 메시지를 받습니다. 가입 시 입력한 이메일 주소와 암호를 사용하여 새 계정에 로그인할 수 있습니다. 하지만 계정을 활성화할 때까지는 AWS 서비스를 사용할 수 없습니다.

8. 결제 정보 페이지에서 결제 방법 정보를 입력합니다. 계정을 만들 때 사용한 주소와 다른 주소를 사용하려면 새 주소 사용을 선택하고 청구 용도로 사용할 주소를 입력합니다.
9. 확인 및 결제를 선택합니다.

> **Note**
>
> 연락처 주소가 인도에 있는 경우 사용자는 인도의 현지 AWS 판매자인 AISPL과 계약을 체결합니다. 확인 과정의 일환으로 CVV를 제공해야 합니다. 은행에 따라 일회용 비밀번호를 입력해야 할 수도 있습니다. 확인 절차의 일환으로, AISPL에서 카드에 2INR을 부과합니다. 확인을 완료되면 AISPL은 2INR을 환불합니다.

10. 전화번호를 확인하려면 목록에서 국가 또는 지역 코드를 선택하고 몇 분 후에 전화를 받을 수 있는 전화번호를 입력합니다. CAPTCHA 코드를 입력하고 제출합니다.
11. AWS 자동 확인 시스템이 전화를 걸어 PIN을 제공합니다. 휴대폰을 사용하여 PIN을 입력한 다음 계속을 선택합니다.
12. AWS Support 플랜을 선택합니다.

    사용 가능한 요금제에 대한 설명은 AWS Support 플랜 비교를 참조하세요.

    계정이 활성화되고 있음을 나타내는 확인 페이지가 나타납니다. 일반적으로 몇 분이면 되지만 때로는 최대 24시간이 소요될 수 있습니다. 활성화하는 동안 새 AWS 계정에 로그인할 수 있습니다. 활성화가 완료될 때까지 가입 완료 버튼이 표시될 수 있습니다. 이 서명은 무시할 수 있습니다.

    계정 활성화가 완료되면 AWS에서 확인 이메일 메시지를 보냅니다. 이메일 및 스팸 폴더에서 확인 이메일 메시지를 확인하세요. 확인 메시지를 받으면 모든 AWS 서비스에 완전히 액세스할 수 있습니다.

2단계: 루트 사용자로 로그인

처음 만들 때 AWS 계정모든 계정에 완전히 액세스할 수 있는 하나의 로그인 ID로 시작합니다. AWS 서비스 및 계정 내 리소스. 이 ID를 다음과 같이 부릅니다. AWS 계정 루트 사용자는 계정을 만들 때 사용한 이메일 주소와 암호로 로그인하여 액세스할 수 있습니다.

> **Important**
>
> 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용

자로 로그인해야 하는 작업의 전체 목록은 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오. IAM

루트 사용자로 로그인하기

1. 를 여세요. AWS Management Console https://console.aws.amazon.com/에서.

   > **Note**
   >
   > 이전에 이 브라우저에서 루트 사용자로 로그인한 경우 브라우저가 해당 브라우저의 이메일 주소를 기억할 수 있습니다. AWS 계정.
   > 이전에 이 브라우저를 사용하여 사용자로 IAM 로그인한 경우 브라우저에 IAM 사용자 로그인 페이지가 대신 표시될 수 있습니다. 기본 로그인 페이지로 돌아가려면 루트 사용자 이메일을 사용하여 로그인을 선택합니다.

2. 이전에 이 브라우저를 사용하여 로그인하지 않은 경우 기본 로그인 페이지가 나타납니다. 계정 소유자인 경우, 루트 사용자를 선택합니다. 사용자 이름을 입력하세요. AWS 계정 계정과 연결된 이메일 주소를 선택하고 다음을 선택합니다.
3. 보안 검사를 완료하라는 메시지가 표시될 수 있습니다. 보안 검사를 완료하여 다음 단계로 이동합니다. 보안 검사를 완료할 수 없는 경우, 오디오를 듣거나, 새로 고침하여 새로운 문자 집합으로 보안 검사를 진행합니다.
4. 암호를 입력하고 로그인을 선택합니다.

3단계: 나를 MFA 위한 활성화 AWS 계정 루트 사용자

루트 사용자 자격 증명의 보안을 강화하려면 보안 모범 사례에 따라 사용자 자격 증명의 다단계 인증(MFA) 을 활성화하는 것이 좋습니다. AWS 계정. 루트 사용자가 계정에서 민감한 작업을 수행할 수 있으므로 이 추가 인증 계층을 추가하면 계정을 더 안전하게 보호할 수 있습니다. 여러 유형을 사용할 수 MFA 있습니다.

루트 사용자를 MFA 위한 활성화에 대한 지침은 에서 사용자를 위한 MFA 장치 활성화를 참조하십시오. AWS(출처: IAM 사용 설명서).

2부: IAM Identity Center에서 관리자 생성

1부: 새 AWS 계정 설정 섹션을 완료한 후, 다음 단계는 일상적인 작업을 수행하는 데 사용할 관리 사용자에 대한 AWS 계정 액세스를 설정하는 데 도움이 됩니다.

> **Note**
>
> 이 항목에서는 IAM Identity Center에서 AWS 계정의 관리자 액세스를 성공적으로 설정하고, 관리자 사용자를 생성하는 데 필요한 최소 단계를 제공합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 시작하기를 참조하세요.

주제

1단계: IAM Identity Center 활성화

> **Note**
>
> 루트 사용자에 대해 다중 인증(MFA)을 활성화하지 않은 경우, 진행하기 전에 3단계: 나를 MFA 위한 활성화 AWS 계정 루트 사용자 섹션을 완료합니다.

IAM Identity Center 활성화

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.
2. IAM Identity Center 콘솔을 엽니다.
3. IAM Identity Center 활성화에서 활성화를 선택합니다.
4. IAM Identity Center는 AWS Organizations가 필요합니다. 조직을 설정하지 않은 경우, AWS에서 조직을 새로 만들지 여부를 선택해야 합니다. AWS 조직 생성을 선택하여 프로세스를 완료합니다.

AWS Organizations에서 관리 계정과 연결된 주소로 확인 이메일을 자동으로 전송합니다. 확인 이메일을 받기까지 어느 정도 시간이 걸릴 수 있습니다. 24시간 내에 이메일 주소를 확인하세요.

> **Note**
>
> 다중 계정을 사용하는 환경인 경우, 위임 관리를 구성하는 것을 권장합니다. 위임 관리를 사용하면 AWS Organizations의 관리 계정에 액세스해야 하는 사람의 수를 제한할 수 있습니다. 자세한 내용을 알아보려면 AWS IAM Identity Center 사용 설명서의 위임 관리를 참조하세요.

2단계: ID 소스 선택

IAM Identity Center의 ID 소스는 사용자 및 그룹을 관리하는 위치를 정의합니다. 다음 ID 중 하나를 ID 소스로 선택할 수 있습니다.

- IAM Identity Center 디렉터리 - IAM Identity Center를 처음 활성화하는 경우, IAM Identity Center 디렉터리가 기본 ID 소스로 자동으로 구성됩니다. 여기에서 사용자 및 그룹을 생성하고 AWS 계정 및 애플리케이션에 대한 액세스 수준을 할당합니다.
- Active Directory - AWS Directory Service를 사용하는 AWS 관리형 Microsoft AD 디렉터리 또는 Active Directory(AD)의 자체 관리형 디렉터리에서 사용자를 계속 관리하려 할 때 선택하는 옵션입니다.
- 외부 ID 제공업체 - Okta 또는 Azure Active Directory와 같은 외부 ID 제공업체(IdP)를 통해 사용자를 관리하려 할 때 선택하는 옵션입니다.

IAM Identity Center를 활성화한 후에는 ID 소스를 선택해야 합니다. 선택하는 자격 증명 소스에 따라 IAM Identity Center에서 Single Sign-On 액세스가 필요한 사용자 및 그룹을 검색하는 위치가 결정됩니다. ID 소스를 선택한 후, 사용자를 생성하거나 지정하고 AWS 계정에 관리 권한을 할당합니다.

> **Important**
>
> Active Directory 또는 외부 ID 제공업체(IdP)에서 이미 사용자 및 그룹을 관리하고 있다면, IAM Identity Center를 활성화하고 ID 소스를 선택할 때 이 ID 소스를 연결하는 것을 고려해 보는 것이 좋습니다. 기본 Identity Center 디렉터리에 사용자 및 그룹을 생성하고 할당하기 전에 이 작업을 수행해야 합니다. 사용자와 그룹을 한 ID 소스에서 관리하고 있을 때, 다른 ID 소스가 관리하는 것으로 변경하면 IAM Identity Center에서 구성한 모든 사용자 및 그룹 할당이 제거될 수

있습니다. 이런 상황이 발생하면 IAM Identity Center의 관리자를 포함한 모든 사용자는 AWS 계정과 애플리케이션에 대한 Single Sign-On 액세스 권한을 잃게 됩니다.

주제

Active Directory 또는 다른 ID 제공업체를 연결하고 사용자를 지정하세요.

이미 Active Directory 또는 외부 ID 제공업체(IdP)를 사용하고 있다면, 다음 주제가 디렉터리를 IAM Identity Center에 연결하는 데 도움이 될 것입니다.

AWS Managed Microsoft AD 디렉터리, Active Directory의 자체 관리형 디렉터리, 또는 외부 ID 제공업체를 IAM Identity Center를 사용하여 연결할 수 있습니다. AWS Managed Microsoft AD 디렉터리 또는 Active Directory의 자체 관리형 디렉터리를 연결하려는 경우, Active Directory 구성이 Active Directory 또는 외부 ID 제공업체(IdP)의 사전 요구 사항을 충족하는지 확인하세요.

> **Note**
>
> 최상의 보안을 위해 다중 인증을 사용하는 것을 권장합니다. AWS Managed Microsoft AD 디렉터리 또는 Active Directory의 자체 관리형 디렉터리를 연결하면서 AWS Directory Service와 함께 RADIUS MFA를 사용하지 않는 경우, IAM Identity Center에서 MFA를 활성화합니다. 외부 ID 제공업체를 사용할 계획이라면 IAM Identity Center가 아닌 외부 ID 제공업체가 MFA 설정을 관리한다는 점에 유의하세요. IAM Identity Center의 MFA는 외부 ID 제공업체가 사용할 수 없습니다. 자세한 내용을 알아보려면 AWS IAM Identity Center 사용 설명서의 다중 인증(MFA) 활성화를 참조하세요.

AWS Managed Microsoft AD

1. Microsoft Active Directory에 연결 지침을 검토합니다.
2. IAM Identity Center에 AWS Managed Microsoft AD의 디렉터리 연결의 단계를 따르세요.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 정보는 관리 사용자와 IAM Identity Center 동기화를 참조하세요.

Active Directory의 자체 관리형 디렉터리

1. Microsoft Active Directory에 연결 지침을 검토합니다.
2. Active Directory의 자체 관리형 디렉터리를 IAM Identity Center에 연결의 단계를 따르세요.
3. 관리자 권한을 부여하려는 사용자가 IAM Identity Center와 동기화하도록 Active Directory를 구성합니다. 자세한 정보는 관리 사용자와 IAM Identity Center 동기화를 참조하세요.

외부 ID 제공업체(IdP)

1. 외부 ID 제공업체에 연결의 지침을 검토합니다.
2. 외부 ID 제공업체에 연결하는 방법의 단계를 따르세요.
3. 사용자를 IAM Identity Center에 프로비저닝하도록 ID 제공업체를 구성합니다.

> **Note**
>
> IdP의 모든 직원 ID를 IAM Identity Center에 자동으로 그룹 기반으로 프로비저닝하도록 설정하기 전에 관리 권한을 부여하려는 한 명의 사용자를 IAM Identity Center와 동기화하는 것이 좋습니다.

관리 사용자의 IAM Identity Center 동기화

디렉터리를 IAM Identity Center에 연결한 후, 관리 권한을 부여할 사용자를 지정한 다음 디렉터리의 해당 사용자를 IAM Identity Center로 동기화할 수 있습니다.

1. IAM Identity Center 콘솔을 엽니다.
2. 설정을 선택합니다.
3. 설정 페이지에서 ID 소스 탭을 선택하고, 작업을 선택한 다음 동기화 관리를 선택합니다.
4. 동기화 관리 페이지에서 사용자 탭을 선택한 다음 사용자 및 그룹 추가를 선택합니다.
5. 사용자 탭의 사용자에 정확한 사용자 이름을 입력하고 추가를 선택합니다.
6. 추가된 사용자 및 그룹에서 다음 작업을 수행합니다.
   a. 관리 권한을 부여하려는 사용자가 지정되었는지 확인합니다.
   b. 사용자 이름 왼쪽의 확인란을 선택합니다.
   c. 제출을 선택합니다.
7. 동기화 관리 페이지에서 지정한 사용자가 동기화 범위의 사용자 목록에 나타납니다.

8. 탐색 창에서 사용자를 선택합니다.
9. 사용자 페이지에서 지정한 사용자가 목록에 나타나는 데 시간이 다소 걸릴 수 있습니다. 새로 고침 아이콘을 선택하여 사용자 목록을 업데이트합니다.

이때 사용자는 관리 계정에 액세스할 수 없습니다. 관리 권한 세트를 만들고, 해당 권한 세트에 사용자를 할당하여 이 계정에 대한 관리 액세스 권한을 설정합니다.

다음 단계: 3단계: 관리 권한 세트 생성

기본 디렉터리를 사용하고 IAM Identity Center에서 사용자를 생성합니다.

IAM Identity Center를 처음 활성화하면 IAM Identity Center 디렉터리를 사용하여 자동으로 구성됩니다. 다음 단계에 따라 IAM Identity Center에서 사용자를 생성합니다.

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.
2. IAM Identity Center 콘솔을 엽니다.
3. 사용자 추가의 단계에 따라 사용자를 생성합니다.

   사용자 세부 정보를 지정할 때 암호 설정 지침(기본 옵션)이 포함된 이메일을 보내거나 일회용 암호를 생성할 수 있습니다. 이메일을 보내는 경우, 자신이 액세스할 수 있는 이메일 주소를 지정해야 합니다.
4. 사용자를 추가했으면 현재 절차로 다시 돌아옵니다. 암호 설정 지침이 포함된 이메일을 보내는 기본 옵션을 유지한 경우, 다음을 수행합니다.

   a. AWS Single Sign-On 가입 초대라는 제목의 이메일을 받게 됩니다. 해당 이메일을 열고 초대 수락을 선택합니다.
   b. 새 사용자 가입 페이지에서 비밀번호를 입력하고 확인한 다음 새 비밀번호 설정을 선택합니다.

> **Note**
>
> 비밀번호를 저장해 두세요. 잠시 후 5단계: 관리자 자격 증명으로 AWS 액세스 포털에 로그인에 필요합니다.

이때 사용자는 관리 계정에 액세스할 수 없습니다. 관리 권한 세트를 만들고, 해당 권한 세트에 사용자를 할당하여 이 계정에 대한 관리 액세스 권한을 설정합니다.

다음 단계: 3단계: 관리 권한 세트 생성

3단계: 관리 권한 세트 생성

권한 세트는 IAM Identity Center에 저장되며, 사용자 및 그룹이 보유할 수 있는 AWS 계정에 대한 액세스 수준을 정의합니다. 관리자 권한을 부여하는 권한 세트를 생성하려면 다음 단계를 수행합니다.

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.
2. IAM Identity Center 콘솔을 엽니다.
3. IAM Identity Center 탐색 창의 다중 계정 권한에서 권한 세트를 선택합니다.
4. 권한 세트 생성을 선택합니다.
5. 1단계: 권한 세트 유형 선택은 권한 세트 유형 선택 페이지에서 기본 설정을 유지하고 다음을 선택합니다. 기본 설정은 AdministratorAccess의 사전 정의된 권한 세트를 사용하여 AWS의 서비스 및 리소스에 대한 전체 액세스 권한을 부여합니다.

   > **Note**
   >
   > 미리 정의된 AdministratorAccess 권한 세트는 AdministratorAccess AWS 관리형 정책을 사용합니다.

6. 2단계: 권한 세트 세부 정보 지정은 사용 권한 세트 세부 정보 지정 페이지에서 기본 설정을 유지하고 다음을 선택합니다. 기본 설정은 세션을 1시간으로 제한합니다.
7. 3단계: 검토 및 생성은 검토 및 생성 페이지에서 다음을 수행합니다.

   1. 권한 세트 유형을 검토하고 해당 유형이 AdministratorAccess인지 확인합니다.
   2. AWS 관리형 정책을 검토하고 AdministratorAccess인지 확인합니다.
   3. 생성을 선택합니다.

4단계: 관리자의 AWS 계정 액세스 설정

IAM Identity Center에서 관리자의 AWS 계정 액세스 권한을 설정하려면 사용자에게 AdministratorAccess 권한 세트를 할당해야 합니다.

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.

2. IAM Identity Center 콘솔을 엽니다.
3. 탐색 창의 다중 계정 권한에서 AWS 계정을 선택합니다.
4. AWS 계정 페이지에는 조직의 트리 뷰 목록이 표시됩니다. 관리 액세스 권한을 할당하려는 AWS 계정 옆의 확인란을 선택합니다. 조직에 다수의 계정이 있는 경우 관리 계정 옆의 확인란을 선택합니다.
5. 사용자 또는 그룹 할당을 선택합니다.
6. 1단계: 사용자 및 그룹 선택 - "***AWS-account-name***"에 사용자 및 그룹 할당 페이지에서 다음을 수행합니다.
   1. 사용자 탭에서 관리 권한을 부여하려는 사용자를 선택합니다.

      결과를 필터링하려면 검색 상자에 원하는 사용자 이름을 순서대로 입력합니다.
   2. 올바른 사용자가 선택되었는지 확인한 후, 다음을 선택합니다.
7. 2단계: 권한 세트 선택의 경우, "***AWS-account-name***"에 권한 세트 할당 페이지의 권한 세트에서 AdministratorAccess 권한 세트를 선택합니다.
8. 다음을 선택합니다.
9. 3단계: 검토 및 제출의 경우 "***AWS-account-name***"에 대한 할당 검토 및 제출 페이지에서 다음을 수행합니다.
   1. 선택한 사용자 및 권한 세트를 검토합니다.
   2. 올바른 사용자가 AdministratorAccess 권한 세트에 할당되었는지 확인한 후 제출을 선택합니다.

      > **Important**
      >
      > 사용자 할당 프로세스를 완료하는 데 몇 분이 걸릴 수 있습니다. 프로세스가 성공적으로 완료될 때까지 이 페이지를 열어둡니다.
10. 다음 중 하나에 해당하는 경우, 다중 인증(MFA) 활성화의 단계에 따라 IAM Identity Center용 MFA를 활성화합니다.
    - 기본 Identity Center 디렉터리를 ID 소스로 사용하고 있습니다.
    - AWS Managed Microsoft AD 디렉터리 또는 Active Directory의 자체 관리형 디렉터리를 ID 소스로 사용하고, RADIUS MFA를 AWS Directory Service와 함께 사용하지는 않습니다.

> **Note**
>
> 외부 ID 제공업체(IdP)를 사용하는 경우, IAM Identity Center가 아닌 외부 ID 제공업체가 MFA 설정을 관리한다는 점에 유의하세요. IAM Identity Center의 MFA는 외부 ID 제공업체가 사용할 수 없습니다.

관리 사용자에 대한 계정 액세스를 설정하면 IAM Identity Center에서 해당 IAM 역할을 생성합니다. IAM Identity Center에서 제어하는 역할로 관련된 AWS 계정에 생성되며 권한 세트에 지정된 정책이 역할에 연결됩니다.

5단계: 관리자 자격 증명으로 AWS 액세스 포털에 로그인

다음 단계를 완료하여, 관리 사용자의 자격 증명을 사용하여 AWS 액세스 포털에 로그인할 수 있고 AWS 계정에 액세스할 수 있는지 확인합니다.

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.
2. https://console.aws.amazon.com/singlesignon/에서 AWS IAM Identity Center 콘솔을 엽니다.
3. 탐색 창에서 대시보드를 선택합니다.
4. 대시보드 페이지의 설정 요약에서 AWS 액세스 포털 URL을 복사합니다.
5. 별도의 브라우저를 열어 복사한 AWS 액세스 포털 URL을 붙여넣고 Enter 키를 누릅니다.
6. 다음 중 하나를 사용하여 로그인합니다.
   - Active Directory 또는 외부 ID 제공업체(IdP)를 ID 소스로 사용하는 경우, IAM Identity Center에서 AdministratorAccess 권한 세트에 할당한 Active Directory 또는ID 제공업체(IdP) 사용자의 자격 증명을 사용하여 로그인합니다.
   - 기본 IAM Identity Center 디렉터리를 ID 소스로 사용하는 경우, 사용자를 생성할 때 지정한 사용자 이름과 해당 사용자에 지정한 새 암호를 사용하여 로그인합니다.
7. 로그인하면 포털에 AWS 계정 아이콘이 나타납니다.
8. AWS 계정 아이콘을 선택하면, 계정과 연결된 계정 이름, 계정 ID, 이메일 주소가 나타납니다.
9. AdministratorAccess 권한 세트를 표시할 계정 이름을 선택하고, AdministratorAccess 오른쪽에 있는 관리 콘솔 링크를 선택합니다.

로그인하면 사용자에게 할당된 권한 세트의 이름이 AWS 액세스 포털에서 가능한 역할로 표시됩니다. 해당 사용자에게 `AdministratorAccess` 권한 세트를 할당했으므로, 역할이 AWS 액세스 포털에서 `AdministratorAccess/`*`username`*으로 표시됩니다.

10. AWS Management Console로 리디렉션되면, AWS 계정의 관리 액세스 설정을 성공적으로 완료한 것입니다. 10단계로 이동합니다.
11. AWS Management Console에 로그인할 때 사용한 브라우저로 전환하여 IAM Identity Center를 설정한 다음 AWS 계정 루트 사용자에서 로그아웃합니다.

> **Important**
>
> AWS 액세스 포털에 로그인할 때 관리 사용자의 자격 증명을 사용하는 아래 모범 사례를 준수하고, 루트 사용자 자격 증명은 일상적인 작업에 사용하지 않는 것이 좋습니다.

다른 사용자가 계정과 애플리케이션에 액세스하고 IAM Identity Center를 관리하도록 하려면 IAM Identity Center로만 권한 세트를 생성하고 할당합니다.

AWS 계정 생성 문제 해결

여기의 정보를 사용하면 AWS 계정 생성과 관련된 문제를 해결하는 데 도움이 됩니다.

문제

AWS에서 새 계정을 확인하라는 전화가 오지 않음

AWS 계정을 만들 때, SMS 문자 메시지 또는 음성 전화를 받을 수 있는 전화번호를 입력해야 합니다. 전화번호 검증에 사용할 방법을 지정합니다.

메시지나 전화를 받지 못한 경우 다음을 확인합니다.

- 가입 과정에서 올바른 전화번호를 입력하고 올바른 국가 코드를 선택했습니다.
- 휴대폰을 사용하는 경우, SMS 문자 메시지 또는 전화를 받을 수 있는 셀룰러 신호가 있는지 확인합니다.
- 결제 방법으로 입력한 정보가 정확합니다.

SMS 문자 메시지를 받지 못했거나 신원 확인 절차를 완료하라는 전화를 받지 못한 경우, AWS Support AWS 계정를 수동으로 활성화하는 데 도움을 줄 수 있습니다. 다음 단계를 사용합니다.

1. AWS 계정 정보에 입력한 전화번호로 연락할 수 있는지 확인합니다.
2. AWS Support 콘솔을 열고 사례 생성을 선택합니다.
   a. 계정 및 결제 지원을 선택합니다.
   b. 유형에서 계정을 선택합니다.
   c. 카테고리에서 활성화를 선택합니다.
   d. 사례 설명 섹션에 연락을 받을 수 있는 날짜 및 시간을 입력합니다.
   e. 연락처 옵션 섹션에서 연락 방법으로 채팅을 선택합니다.
   f. 제출을 선택합니다.

> **Note**
>
> AWS 계정이 활성화되어 있지 않아도 AWS Support에서 케이스를 생성할 수 있습니다.

전화로 AWS 계정 인증을 시도할 때 "최대 실패 횟수" 관련 오류 발생

AWS Support가 계정을 수동으로 활성화하는 데 도움이 될 수 있습니다. 다음 단계를 따릅니다.

1. 계정을 만들 때 지정한 이메일 주소와 암호를 입력하여 AWS 계정에 로그인합니다.
2. AWS Support 콘솔을 열고 사례 생성을 선택합니다.
3. 계정 및 결제 지원을 선택합니다.
4. 유형에서 계정을 선택합니다.
5. 카테고리에서 활성화를 선택합니다.
6. 사례 설명 섹션에 연락을 받을 수 있는 날짜 및 시간을 입력합니다.
7. 연락처 옵션 섹션에서 연락 방법으로 채팅을 선택합니다.
8. 제출을 선택합니다.

AWS Support에서 사용자에게 연락하여 AWS 계정의 수동 활성화를 시도합니다.

24시간 후에도 계정이 활성화되지 않음

경우에 따라 계정 활성화가 지연될 수 있습니다. 프로세스가 24시간 이상 소요되는 경우 다음을 확인합니다.

- 계정 활성화 프로세스를 완료합니다.

  필요한 정보를 모두 추가하기 전에 가입 프로세스 창을 닫았다면 등록 페이지를 엽니다. 기존 AWS 계정 계정에 로그인을 선택하고, 계정으로 선택한 이메일 주소 및 비밀번호를 사용하여 로그인합니다.
- 결제 방법과 관련된 정보를 확인합니다.

  AWS Billing and Cost Management 콘솔에서 결제 방법에 오류가 있는지 확인합니다.
- 금융 기관에 문의합니다.

금융 기관에서 AWS가 요청한 승인을 거부하는 경우가 있습니다. 결제 방법과 관련된 기관에 연락하여 AWS의 승인 요청을 승인해 달라고 요청합니다. AWS는 금융 기관에서 승인 요청을 승인하는 즉시 승인 요청을 취소하므로, 승인 요청 비용이 청구되지 않습니다. 금융 기관의 명세서에는 승인 요청이 여전히 소액 수수료(보통 1USD)로 표시될 수 있습니다.

- 이메일 및 스팸 폴더에서 추가 정보 요청을 확인합니다.
- 다른 브라우저를 사용해 보세요.
- AWS Support에 문의하세요.

AWS Support에 문의하여 도움을 받으세요. 시도한 문제 해결 단계를 모두 알려주세요.

> **Note**
>
> AWS에 응답 시 신용카드 번호와 같은 민감한 정보를 제공하지 마세요.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.