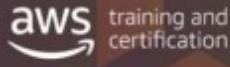




IAM 역할



 역할을 사용하면 사용자 또는 서비스가 필요한 리소스에 액세스하기 위한 권한 집합을 정의할 수 있습니다.

- 권한을 IAM 사용자 또는 그룹에 연결하지 않습니다.
- 권한을 역할에 연결하고 역할을 사용자 또는 서비스에 **위임**합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

역할을 사용하면 사용자 또는 서비스가 필요한 리소스에 액세스하기 위한 권한 집합을 정의할 수 있으며, 이 권한은 IAM 사용자 또는 그룹에 연결되지 않습니다. 권한은 역할에 연결되면 역할은 사용자 또는 서비스에게 위임됩니다.

역할을 사용하면 개별 사용자에게 여러 계정을 생성할 필요가 없어집니다.

사용자가 역할을 수임하면 기존 권한은 일시적으로 무시됩니다. AWS가 사용자 또는 애플리케이션이 AWS에 프로그래밍 방식 요청을 전송하는 데 사용하는 임시 보안 자격 증명을 반환합니다.

그러므로 리소스에 액세스해야 하는 엔터티별로 장기적인 자격 증명을 공유할 필요가 없습니다(예: IAM 사용자 생성을 통해).

Amazon EC2와 같은 서비스에서는, 애플리케이션 또는 AWS 서비스가 런타임 시 프로그래밍 방식으로 역할을 수임할 수 있습니다.

액세스 권한이 필요한 리소스를 포함하는 AWS 계정에서 역할을 생성합니다.
역할을 생성할 때 신뢰 및 액세스 두 개의 정책을 지정합니다.

- **신뢰** 정책은 누가 역할을 맡도록 허용되었는지 지정합니다(신뢰할 수 있는 엔터티 또는 보안 주체).
- **액세스(또는 권한)** 정책은 보안 주체가 사용하도록 허용된 리소스 및 작업을 정의합니다.

이는 조직이 기업 사용자 디렉터리와 같은 자체 자격 증명 시스템을 이미 가지고 있는 경우에 유용합니다. 또 하나의 사용 사례는 AWS 리소스에 액세스해야 하는 모바일 앱 또는 웹 애플리케이션입니다. 자격 증명 공급자를 사용하면 인증이 외부에서 관리됩니다. 그러면 애플리케이션에 장기 보안 자격 증명을 배포하거나 포함할 필요가 없으므로 AWS 계정의 보안에 도움이 됩니다.

자세한 내용은 다음을 참조하십시오.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers.html

보안 주체는 IAM 사용자, 그룹 또는 다른 AWS 계정의 역할이 될 수 있습니다(자신이 소유하지 않은 AWS 계정 포함). 이것은 프로세스 간소화를 약간 과장한 것이지만, 외부 계정 액세스용 역할을 생성하면 제삼자를 위해 사용자 이름 및 암호를 관리할 필요가 없습니다. 수신되는 요청은 역할 요구 사항과 일치해야 합니다. 더 이상 액세스를 원치 않을 경우 역할을 수정/삭제할 수 있습니다. 그러므로 조직 외부 사람을 위한 계정을 생성하고 관리할 필요가 없습니다.

IAM 역할

aws training and certification

사용 사례:

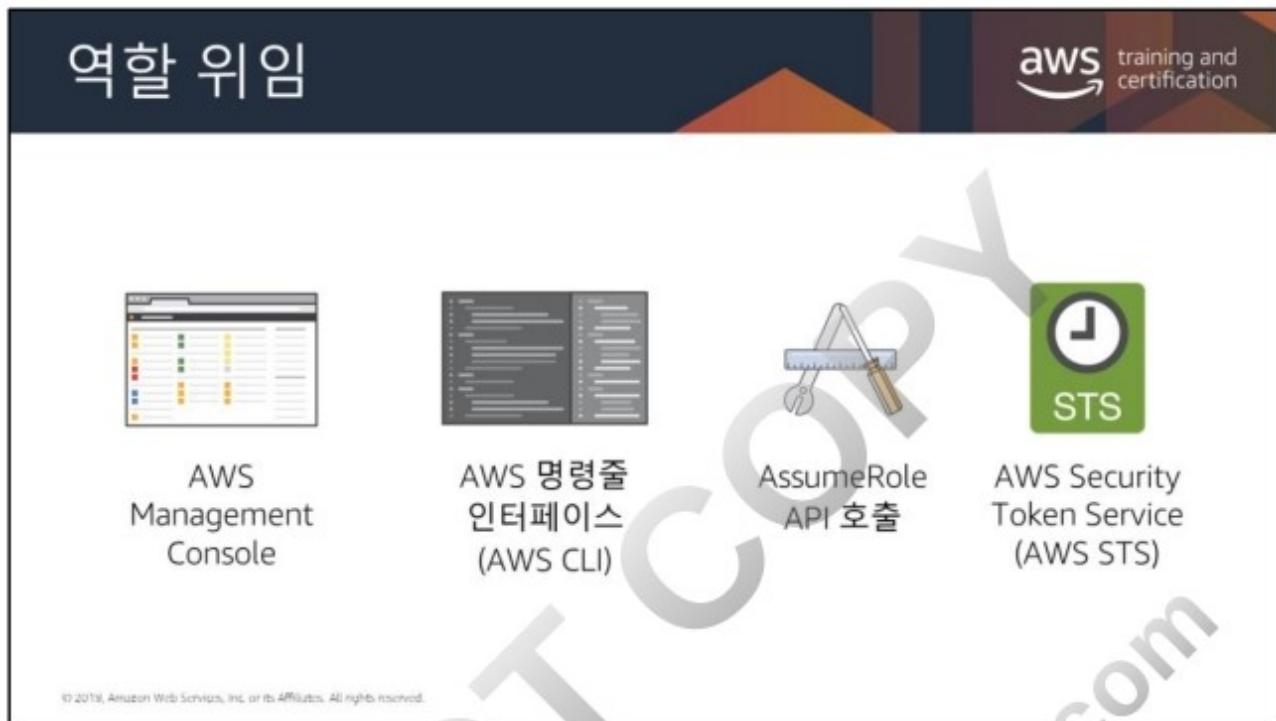
- AWS 리소스에 AWS 서비스에 대한 액세스를 제공합니다.
- 외부 인증 사용자에게 액세스를 제공합니다.
- 타사에게 액세스를 제공합니다.
- 다음 리소스에 액세스하도록 역할을 전환합니다.
 - 자신의 AWS 계정
 - 다른 AWS 계정(교차 계정 액세스)

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

역할을 사용하는 가장 간단한 방법은 자체 AWS 계정 또는 다른 AWS 계정 내에 생성한 역할을 전환할 수 있는 권한을 IAM 사용자에게 부여하는 것입니다. IAM 사용자는 IAM 콘솔을 사용하여 손쉽게 역할을 전환할 수 있습니다. 이렇게 하면 IAM 사용자가 일반적으로는 부여되지 않는 권한을 사용한 후 역할을 끝내면 해당 권한을 포기할 수 있습니다. 이는 실수로 민감한 리소스에 액세스하거나 이를 변경하는 것을 방지하는 데 도움이 됩니다.

연동 사용자는 자격 증명 공급자(IdP)가 제공한 자격 증명을 사용하여 로그인합니다. 그러면 AWS는 이후 AWS 리소스 요청에 추가되도록 사용자에게 전달할 역할과 연결된 임시 자격 증명을 IdP에 제공합니다. 이러한 자격 증명은 할당된 역할에 부여된 권한을 제공합니다. 기업 디렉터리 또는 타사 IdP의 기존 자격 증명을 사용하려는 경우 도움이 될 수 있습니다.

타사에서 조직의 AWS 리소스에 액세스해야 할 때, 역할을 사용하여 리소스에 대한 액세스를 위임할 수 있습니다. 예를 들어 타사에서 AWS 리소스를 관리하는 서비스를 제공할 수 있습니다. IAM 역할을 사용하면 AWS 보안 자격 증명을 공유하지 않고도 타사에 AWS 리소스에 대한 액세스 권한을 부여할 수 있습니다. 대신 타사는 AWS 리소스에 액세스하도록 생성한 역할을 맡을 수 있습니다.



역할은 콘솔, CLI, AssumeRole API 및 AWS Security Token Service (AWS STS)를 사용하여 위임될 수 있습니다. AWS STS는 IAM 사용자 또는 자격 증명 연동으로 인증된 사용자에게 제한적인 임시 권한을 제공하는 웹 서비스입니다.

AssumeRole 작업은 액세스 키 ID, 보안 액세스 키 및 보안 토큰으로 구성된 임시 보 자격 증명 세트를 반환합니다. 일반적으로 AssumeRole은 교차 계정 액세스 또는 자격 증명 연동에 사용됩니다.

AWS STS는 AWS 계정에 대한 AWS 호출을 기록하고 Amazon S3 버킷에 로그 파일을 전송하는 AWS CloudTrail을 지원합니다.

CloudTrail은 IAM 및 AWS STS API에 대한 모든 인증된(자격 증명을 사용해 생성된) API 요청을 기록합니다. 또한 CloudTrail은 AWS STS 작업, AssumeRoleWithSAML 및 AssumeRoleWithWebIdentity에 대한 인증되지 않은 요청을 기록하고 자격 증명 공급자가 제공하는 정보를 기록합니다.

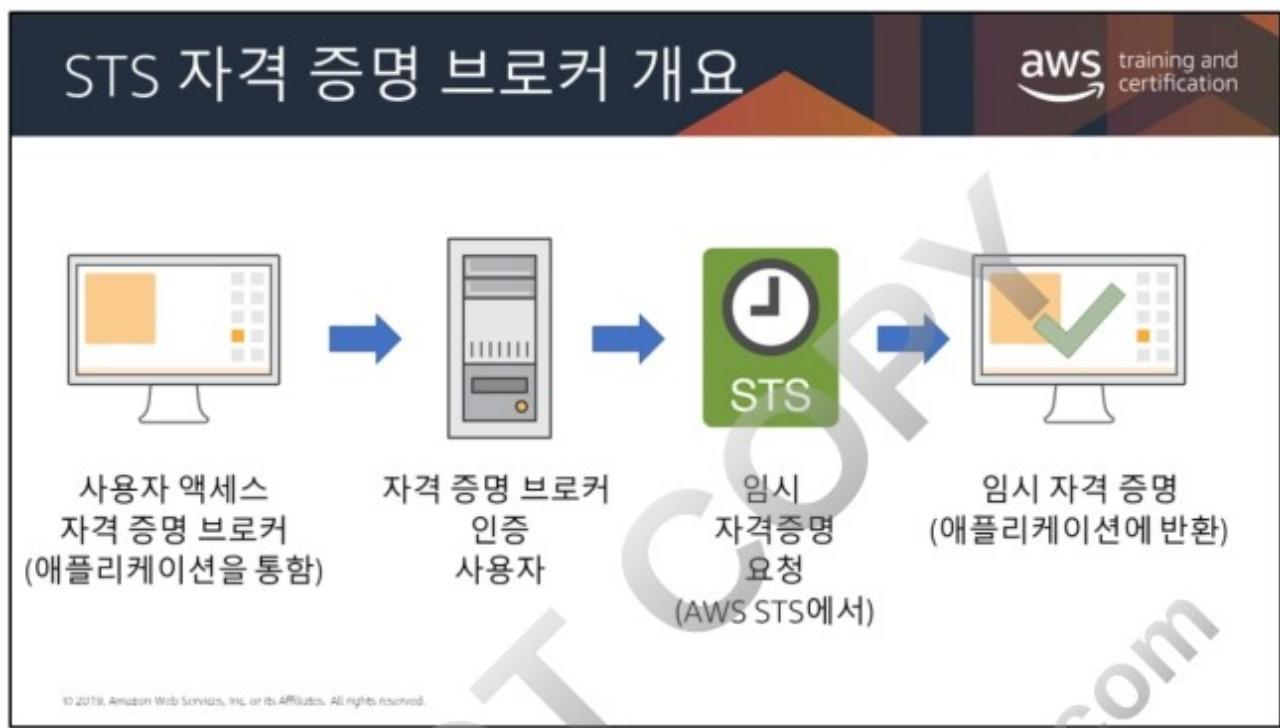
이 정보를 사용하여 위임된 역할을 지닌 연동 사용자의 호출을 외부 연동 호출자에 다시 매핑할 수 있습니다.

AssumeRole의 경우, 호출을 원래 AWS 서비스 또는 원래 사용자의 계정에 다시 매핑할 수 있습니다.

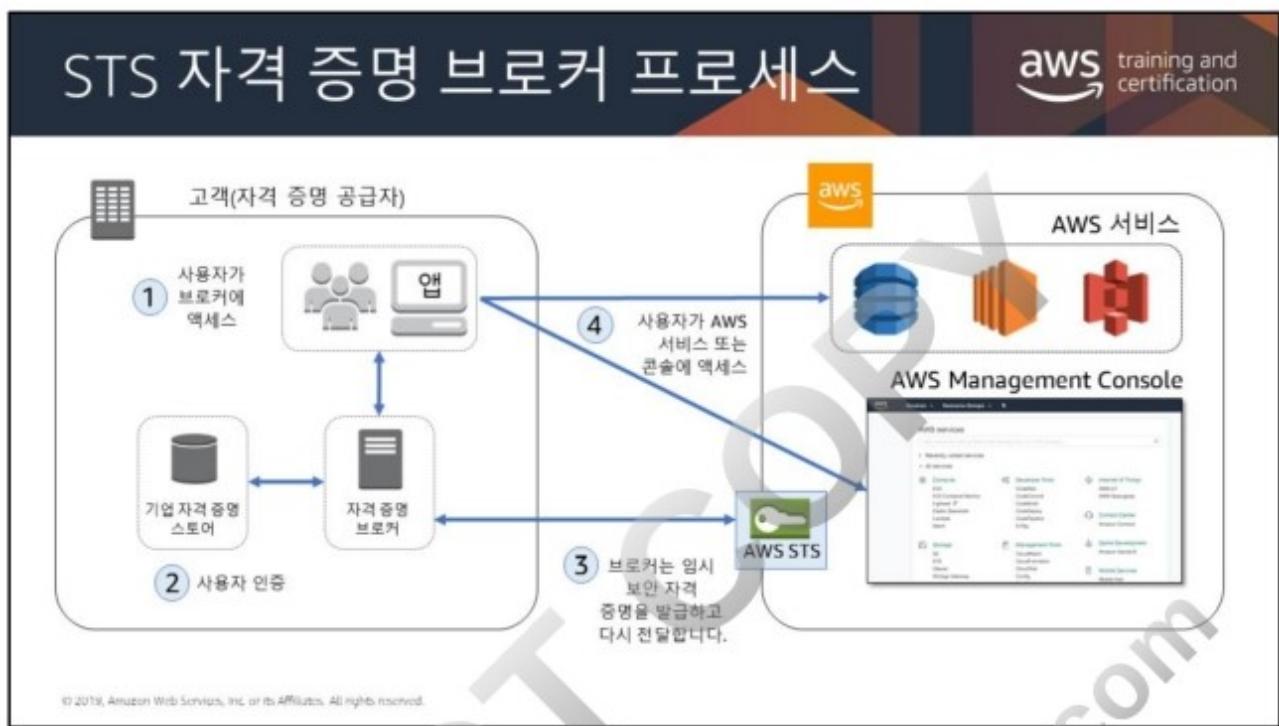
CloudTrail 로그 항목에서 JSON 데이터의 userIdentity 섹션에 AssumeRole 요청을 특정 연동 사용자와 매핑하는 데 필요한 정보가 들어 있습니다.

자세한 내용은 다음을 참조하십시오.

- <https://docs.aws.amazon.com/STS/latest/APIReference>Welcome.html>
- <https://docs.aws.amazon.com/IAM/latest/UserGuide/cloudtrail-integration.html>



AWS STS를 사용해 타사 인증 서비스를 사용하는 애플리케이션에 대한 임시 자격증명을 생성하는 데는 4개의 기본 단계가 있습니다.



위 시나리오에서는,

- 자격 증명 브로커 애플리케이션이 AWS STS API에 액세스하여 임시 보안 자격 증명을 생성할 권리가 있습니다.
- 자격 증명 브로커 애플리케이션은 직원이 기존 인증 시스템 내에서 인증되는지 확인할 수 있습니다.
- 사용자에게 콘솔에 액세스할 수 있는 임시 URL (Single-Sign-On이라고 함)이 제공됩니다.

다른 AWS 계정의 IAM 사용자 그룹:

IAM 역할을 사용하여 교차 계정 액세스를 설정할 수 있습니다. 신뢰하는 계정에서 리소스가 역할을 지원하는 서비스에 위치해야 합니다.

현재 계정 내 IAM 사용자:

IAM 사용자가 자주 사용하지 않는 미션 크리티컬한 권한의 경우, 역할을 사용하여 이러한 권한을 일상적인 권한에서 분리할 수 있습니다. 사용자는 역할을 능동적으로 맡아야 하므로, 실수로 지장을 주는 작업을 수행하는 것을 방지할 수 있습니다.

예를 들어 조직에 매우 중요한 Amazon EC2 인스턴스를 가지고 있을 수 있습니다. 인스턴스를 종료할 수 있는 관리자 권한을 직접 부여하는 대신, 해당 권한이 있는 역할을 생성하고 관리자가 그 역할을 맡도록 할 수 있습니다.

관리자는 이러한 인스턴스를 종료할 권한이 없으며, 종료하려면 먼저 역할을 맡아야 합니다. 역할을 사용하면, 관리자가 조직에 매우 중요한 인스턴스를 종료할 수 있기 전에 역할을 맡는 추가 단계를 거쳐야 합니다.

타사:

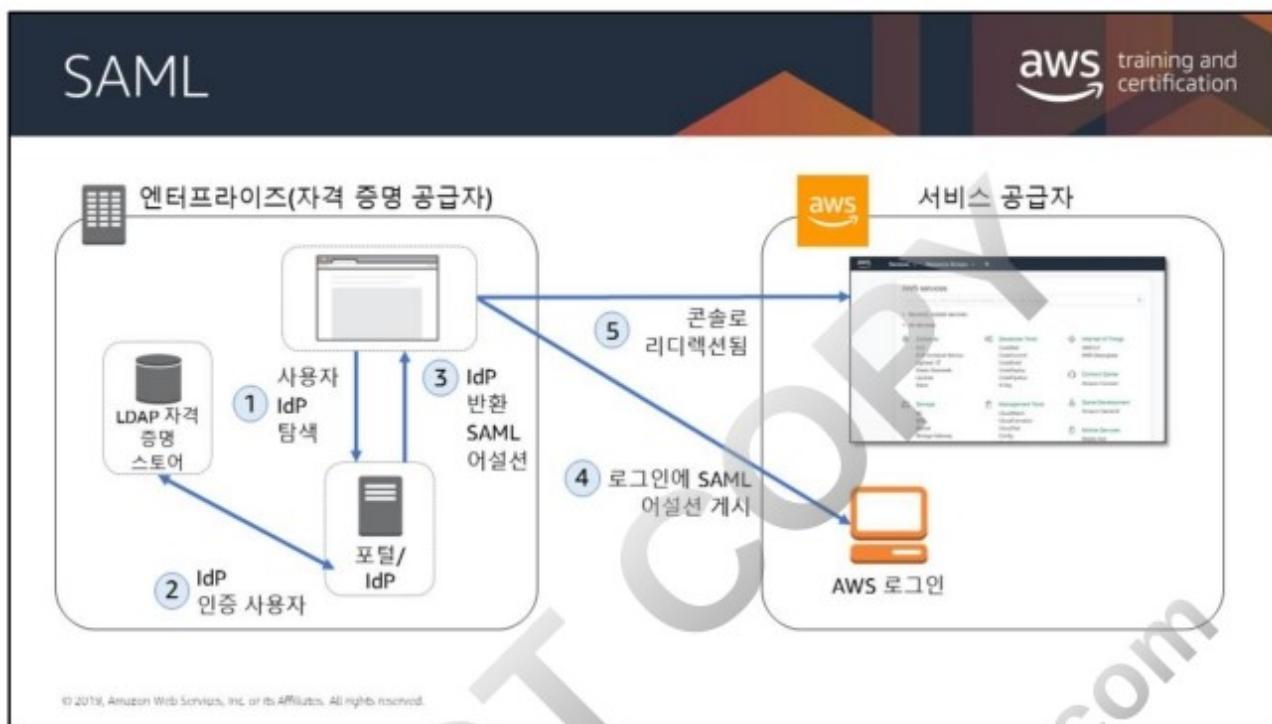
타사에서 조직의 AWS 리소스에 액세스해야 할 때, 역할을 사용하여 리소스에 대한 API 액세스를 위임할 수 있습니다. 예를 들어 타사에서 AWS 리소스를 관리하는 서비스를 제공할 수 있습니다. IAM 역할을 사용하면 AWS 보안 자격 증명을 공유하지 않고도 타사에 AWS 리소스에 대한 액세스 권한을 부여할 수 있습니다. 대신 타사는 AWS 리소스에 액세스하도록 생성한 역할을 맡을 수 있습니다.

여러분이 타사가 맡을 수 있는 역할을 생성할 수 있으려면, 타사는 다음 정보를 제공해야 합니다.

- 타사의 IAM 사용자가 역할을 맡기 위해 사용할 AWS 계정 ID. 여러분이 역할의 신뢰할 수 있는 엔터티를 정의할 때 타사 사용자의 AWS 계정 ID를 지정합니다.
- 타사가 역할과 연결할 수 있는 외부 ID. 여러분이 역할의 신뢰할 수 있는 엔터티를 정의할 때 타사가 제공한 ID를 지정합니다.
- 타사가 AWS 리소스를 사용하는 데 필요한 권한. 역할의 권한 정책을 정의할 때 이러한 권한을 지정합니다. 이 정책은 타사가 수행할 수 있는 작업과 액세스할 수 있는 리소스를 정의합니다.
- 역할을 생성한 후, 역할의 Amazon Resource Name (ARN)을 타사와 공유해야 합니다. 타사가 역할을 맡으려면 역할의 ARN이 필요합니다.

자격 증명 브로커:

- AWS STS를 쿼리하는 데 사용
- 웹 요청에서 사용자를 결정
- AWS 자격 증명(서비스 계정)을 사용하여 AWS 인증
- AWS API에 액세스할 수 있는(AWS STS를 통해) 임시 보안 자격 증명을 발급
- AWS 권한은 자격 증명 브로커의 관리자가 구성
- 구성 가능한 시간 제한: 1~36시간
- 자세한 내용(샘플 IIS authentication 프록시 C# 코드 포함)은 <http://aws.amazon.com/code/1288653099190193>을 참조하십시오.



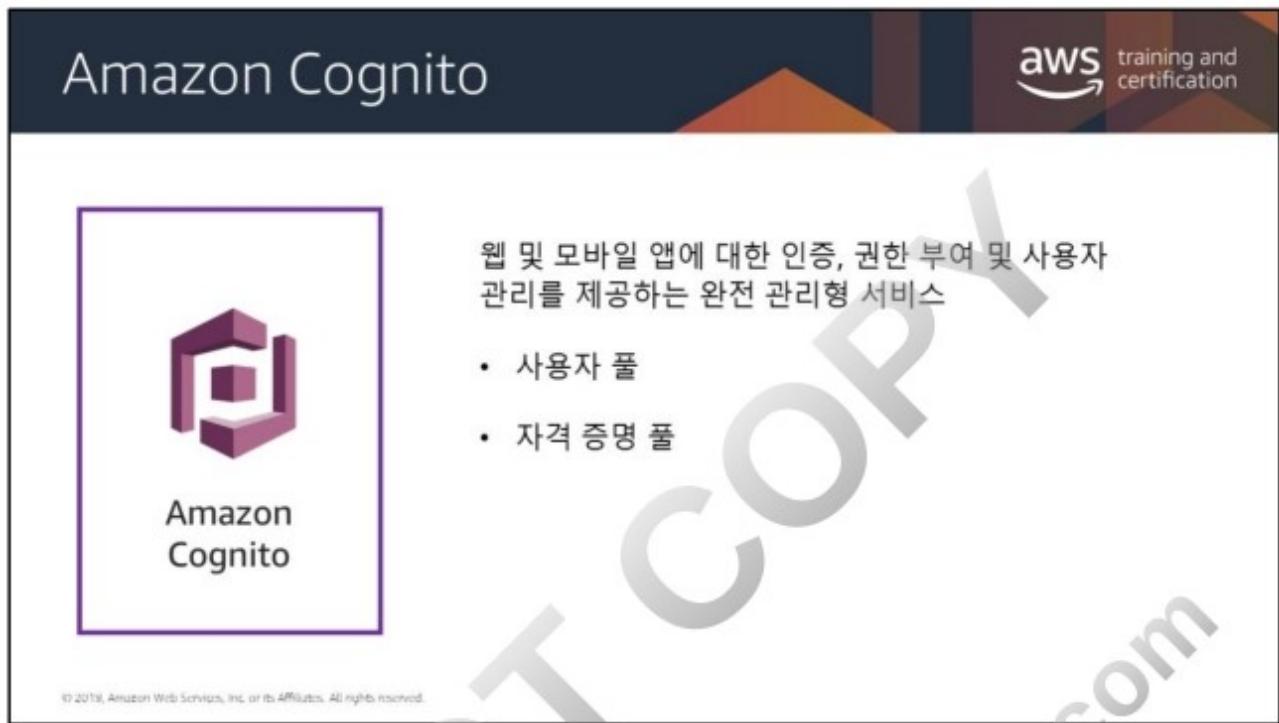
사용자 관점에서는 프로세스가 투명하게 처리됩니다. 사용자는 조직의 내부 포털에서 시작하여 AWS 자격 증명을 제공할 필요 없이 AWS Management Console에 로그인하게 됩니다.

- 1. 사용자가 URL로 이동합니다.** 조직의 사용자가 네트워크의 내부 포털로 찾아갑니다. 포털은 또한 조직과 AWS 간에 SAML 신뢰를 처리하는 IdP로서 기능합니다.
- 2. 사용자가 인증됩니다.** 사용자 자격 증명 공급자(IdP)는 AD와 비교하여 사용자의 자격 증명을 인증합니다.
- 3. 사용자가 인증 응답을 수신합니다.** 클라이언트가 IdP로부터 인증 응답 형식으로 SAML 어설션을 수신합니다.
- 4. 클라이언트가 로그인 통과 AuthN을 게시합니다.** 클라이언트가 새 AWS 로그인 엔드포인트에 SAML 어설션을 게시합니다. 백그라운드에서는 로그인이 AssumeRoleWithSAML API를 사용하여 임시 보안 자격 증명을 요청하고 로그인 URL을 구성합니다.
- 5. 클라이언트는 AWS Management Console로 리디렉션됩니다.** 사용자의 브라우저는 로그인 URL을 수신하고 AWS Management Console로 리디렉션됩니다.

자세한 내용은 다음을 참조하십시오.

- <https://aws.amazon.com/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/>
- <https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/>

DO NOT COPY
zlagusdbs@gmail.com



The screenshot shows the Amazon Cognito landing page. At the top left is the 'Amazon Cognito' logo, which consists of a purple square icon with a white stylized 'A' shape inside, followed by the text 'Amazon Cognito'. At the top right is the 'aws training and certification' logo. The main content area features a large purple 'COPYRIGHTED MATERIAL' watermark. To the left of the watermark is a purple-bordered box containing the Cognito logo and text. To the right of the watermark is a descriptive paragraph and a bulleted list. At the bottom left is a small copyright notice.

Amazon Cognito

aws training and certification

웹 및 모바일 앱에 대한 인증, 권한 부여 및 사용자 관리를 제공하는 완전 관리형 서비스

- 사용자 풀
- 자격 증명 풀

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon Cognito는 웹 및 모바일 앱에 대한 인증, 권한 부여 및 사용자 관리를 제공하는 완전 관리형 서비스입니다. 사용자는 사용자 이름과 암호를 사용하여 직접 로그인하거나 Facebook, Amazon 또는 Google 같은 타사를 통해 로그인할 수 있습니다.

Amazon Cognito의 두 가지 주요 구성 요소는 사용자 풀 및 자격 증명 풀입니다.

- **사용자 풀**은 앱 사용자의 가입 및 로그인 옵션을 제공하는 사용자 디렉터리입니다.
- **자격 증명 풀**을 사용하면 다른 AWS 서비스에 대한 액세스 권한을 사용자에게 부여할 수 있습니다. 자격 증명 풀과 사용자 풀은 별도로 또는 함께 사용할 수 있습니다.

사용자 풀은 Amazon Cognito의 사용자 디렉터리입니다. 사용자 풀을 사용하면 사용자가 Amazon Cognito를 통해, 또는 타사 자격 증명 공급자(IdP)를 통해 연동하여 웹 또는 모바일 앱에 로그인할 수 있습니다.

사용자 풀의 모든 멤버가 디렉터리 프로필을 가지며, SDK를 통해 이 프로필에 액세스할 수 있습니다.

사용자 풀은 다음을 제공합니다.

- 가입 및 로그인 서비스
- 사용자 로그인을 위한 사용자 지정 가능한 내장 웹 UI
- Facebook, Google, Login with Amazon을 통한 소셜 로그인 및 사용자 풀의 SAML 및 OIDC 자격 증명 공급자를 통한 로그인
- 사용자 디렉터리 관리 및 사용자 프로필
- 멀티 팩터 인증(MFA), 자격 증명 손상 여부 확인, 계정 탈취 보호, 전화 및 이메일 확인과 같은 보안 기능
- AWS Lambda 트리거를 통한 사용자 지정 워크플로우 및 사용자 마이그레이션

사용자 풀에 대한 자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/cognito/latest/developerguide/getting-started-with-cognito-user-pools.html>

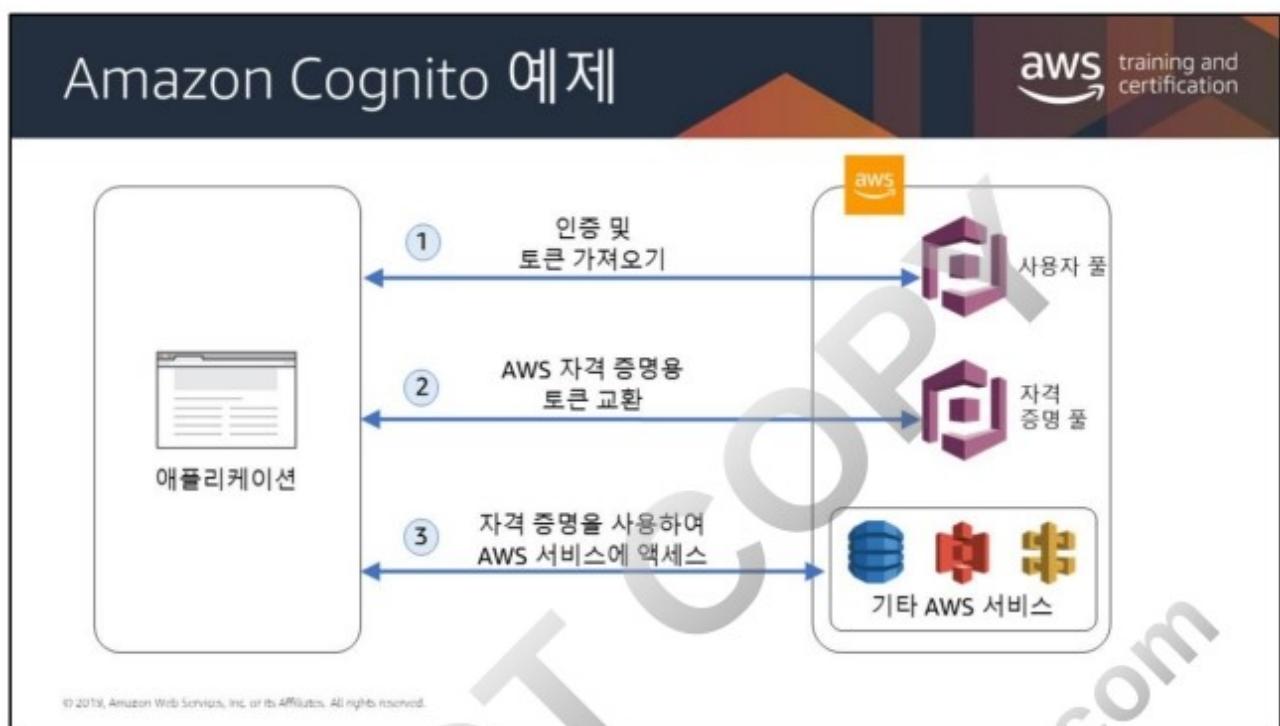
Amazon Cognito 자격 증명 풀은 사용자를 위해 고유한 자격 증명 및 권한 할당을 생성할 수 있게 해줍니다.

자격 증명 풀을 사용하면 사용자가 AWS 서비스에 액세스하거나 Amazon API Gateway를 통해 리소스에 액세스할 수 있는 임시 AWS 자격 증명을 부여받을 수 있습니다.

자격 증명 풀은 게스트(미인증/익명) 사용자와 다음 자격 증명 공급자에게 임시 AWS 자격 증명을 제공합니다.

- Amazon Cognito 사용자 풀
- Facebook, Google, Login with Amazon을 통한 소셜 로그인
- OpenID Connect (OIDC) 공급자
- SAML 자격 증명 공급자
- 개발자 인증 자격 증명

사용자 프로필 정보를 저장하려면 Amazon Cognito 자격 증명 풀이 Amazon Cognito 사용자 풀과 통합되어야 합니다.



이 시나리오는 사용자를 인증한 후 해당 사용자에게 다른 AWS 서비스에 대한 액세스 권한을 부여하는 것이 목표입니다.

- 첫 번째 단계에서는 앱 사용자가 사용자 풀을 통해 로그인하고, 인증 성공 후 사용자 풀 토큰을 부여받습니다.
- 다음 단계에서는 앱이 자격 증명 풀을 통해 사용자 풀 토큰을 AWS 자격 증명과 교환합니다.
- 마지막으로 앱 사용자가 해당 AWS 자격 증명을 사용하여 다른 AWS 서비스에 액세스합니다.

AWS Landing Zone

aws training and certification

AWS 모범 사례에 따라 안전한 다중 계정 AWS 환경을 빠르게 설정할 수 있도록 도와주는 솔루션으로 다음 기능을 갖추고 있습니다.

-  다중 계정 구조
-  Account Vending Machine
-  사용자 액세스
-  알림

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Landing Zone은 AWS 모범 사례에 따라 안전한 다중 계정 AWS 환경을 빠르게 설정할 수 있도록 도와주는 솔루션입니다. 이 솔루션을 사용하면 안전하고 확장 가능한 워크로드 실행을 위한 환경이 자동으로 설정되고 핵심 계정 및 리소스 생성을 통해 초기 보안 기준이 구현되므로 시간을 절약할 수 있습니다. 또한 다중 계정 아키텍처, 자격 증명 및 액세스 관리, 거버넌스, 데이터 보안, 네트워크 설계, 로깅을 시작할 수 있는 기본 환경을 제공합니다.

다중 계정 구조: AWS Landing Zone 솔루션에는 4개의 계정과 Centralized Logging 솔루션, AWS Managed AD, AWS SSO용 Directory Connector와 같이 AWS Service Catalog를 사용하여 배포할 수 있는 추가 제품이 포함되어 있습니다.

Account Vending Machine: Account Vending Machine (AVM)은 AWS Landing Zone의 주요 구성 요소입니다. AVM은 [AWS Service Catalog](#) 제품으로 제공되므로 고객은 계정 보안 기준과 사전 정의된 네트워크로 미리 구성된 조직 단위(OU)에서 새로운 AWS 계정을 생성할 수 있습니다.

사용자 액세스: AWS 계정에 대한 최소 권한 개별 사용자 액세스를 제공하는 것은 AWS 계정 관리에 필수적인 기본 구성 요소입니다. AWS Landing Zone 솔루션은 사용자 및 그룹을 저장할 수 있는 두 가지 옵션을 고객에게 제공합니다.

알림: AWS Landing Zone 솔루션은 [Amazon CloudWatch](#) 경보 및 이벤트를 구성하여 루트 계정 로그인, 콘솔 로그인 실패, API 인증 실패 및 계정 내의 변경 사항(보안 그룹, 네트워크 ACL, Amazon VPC 게이트웨이, 피어링 연결, ClassicLink, Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스 상태, 대규모 Amazon EC2 인스턴스 상태, AWS CloudTrail, AWS Identity and Access Management (IAM) 정책, AWS Config 규칙 준수 상태)에 대한 알림을 전송합니다.

자세한 내용은 <https://aws.amazon.com/solutions/aws-landing-zone/>을 참조하십시오.



“현장”에서의 AWS

aws training and certification

조직에 몇 개의 AWS 계정이 필요합니까?

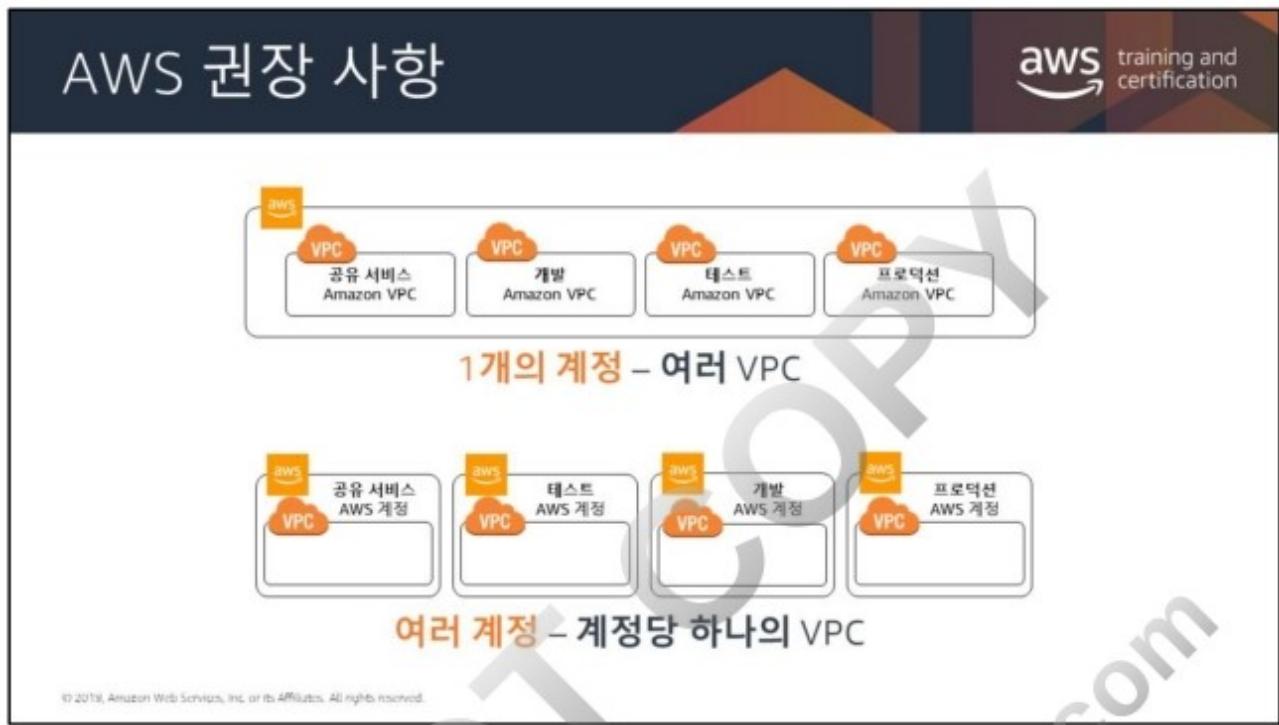
aws
개발

aws
테스트

aws
프로덕션

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.





AWS가 권장하는 두 가지 기본 아키텍처 패턴은 **다중 VPC(단일 AWS 계정 내)**와 **다중 계정**입니다.

다중 계정 시스템에서 각 계정에 단일 VPC가 제공됩니다. 실제로 조직은 (크고 작은) 여러 계정을 생성합니다. 이들 계정은 관리, 유지 및 감사해야 합니다.

여러 AWS 계정

aws training and certification

다음과 같이 **격리**에 활용할 수 있습니다.

- 별도의 사업부, 개발/테스트/프로덕션 환경

다음과 같이 **보안**을 위해 활용할 수 있습니다.

- 규정된 워크로드, 다른 지리적 위치, 다른 계정 관리를 위한 별도의 계정

교차 계정 액세스는 기본적으로 활성화되어 있지 않습니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

많은 AWS 고객은 자신의 조직에 대해 여러 AWS 계정을 생성합니다(예: 다양한 비즈니스 단위에 대한 개별 계정 또는 개발, 테스트 및 프로덕션 리소스에 대한 별도 계정).

고객은 개발 및 프로덕션 리소스에 대해 (일반적으로 통합 결제와 함께) 별도 AWS 계정을 사용하여 다른 유형의 리소스를 완전히 분리할 수 있으며 몇 가지 보안 이점을 제공할 수도 있습니다.

The slide has a dark blue header with the title '여러 AWS 계정을 사용하기 위한 전략' and the AWS logo. Below the header is a large table with four rows. The first row has two columns: '중앙 집중식 보안 관리' and '단일 AWS 계정'. The second row has two columns: '프로덕션, 개발 및 테스트 환경의 분리' and '3개의 AWS 계정'. The third row has two columns: '여러 개의 자율 부서' and '여러 AWS 계정'. The fourth row has two columns: '여러 개의 자율적인 독립 프로젝트가 포함된 중앙 집중식 보안 관리' and '여러 AWS 계정'. A watermark 'DRAFT' is diagonally across the slide.

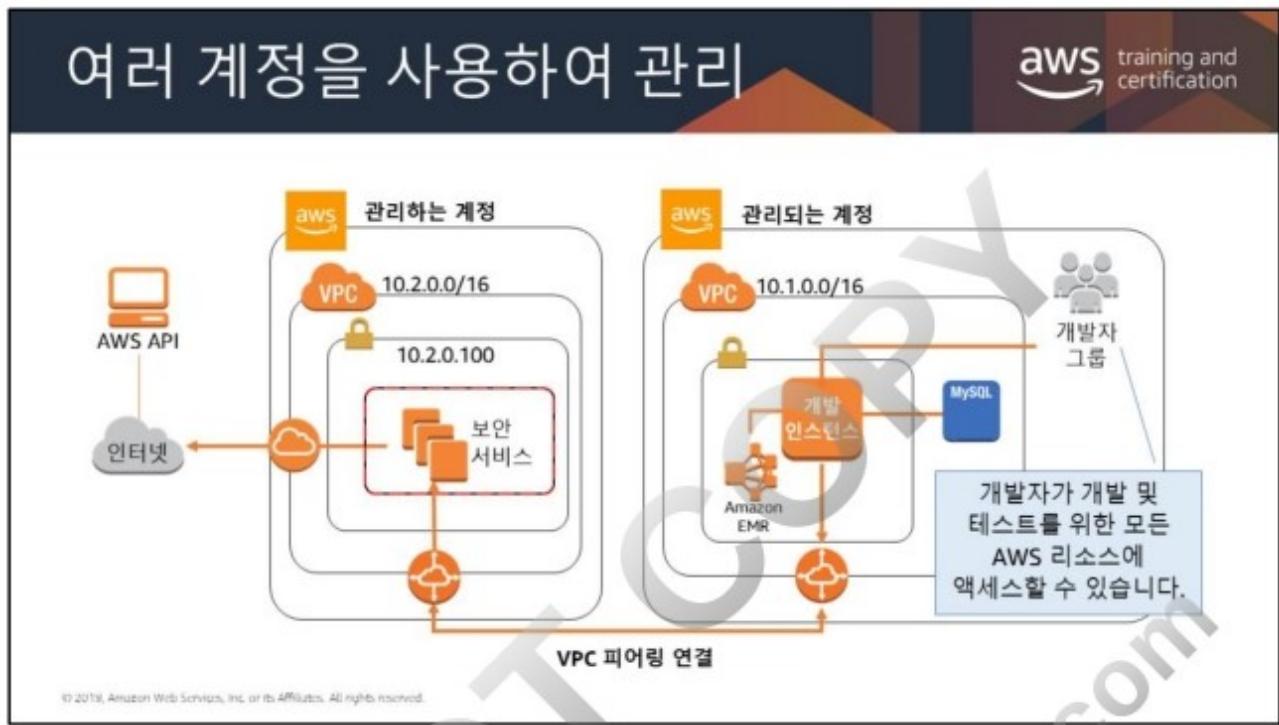
중앙 집중식 보안 관리	단일 AWS 계정
프로덕션, 개발 및 테스트 환경의 분리	3개의 AWS 계정
여러 개의 자율 부서	여러 AWS 계정
여러 개의 자율적인 독립 프로젝트가 포함된 중앙 집중식 보안 관리	여러 AWS 계정

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

보안을 극대화하고 비즈니스 및 거버넌스 요구 사항을 따르는 AWS 계정 전략을 설계할 수 있습니다.

오버헤드를 최소화하는 중앙 집중식 정보 보안 관리를 선호하면 단일 AWS 계정을 선택할 수 있습니다. 또는 회사가 프로덕션, 개발 및 테스트 환경을 별도로 유지하는 경우, 각 환경에 하나씩 세 개의 AWS 계정을 구성할 수 있습니다. 또한 여러 개의 자율 부서가 있는 경우 각 부서마다 별도의 AWS 계정을 만들 수도 있습니다.

여러 계정을 사용하는 경우 보다 효율적인 전략은 공통 프로젝트 리소스(예: DNS 서비스, Active Directory, CMS)를 위한 단일 AWS 계정을 만들고 독립 프로젝트/자율 부서마다 별도 계정을 만드는 것입니다. 그러면 각 부서/프로젝트 계정에 권한 및 정책을 할당하고 계정 간에 리소스에 대한 액세스 권한을 부여할 수 있습니다.



많은 대기업이 보안 및 거버넌스를 위해 다중 계정을 사용합니다. 이 접근 방식에서는 두 개 이상의 AWS 계정이 필요합니다. 하나는 지배하는 계정으로 지정되고, 다른 것들은 지배되는 계정으로 지정됩니다. 이 솔루션은 모든 관리 리소스를 지배 계정의 네트워크로 격리합니다. 지배되는 계정의 모든 인바운드 및 아웃바운드 트래픽은 지배하는 계정의 보안 서비스를 통과합니다. 이를 통해 지배하는 계정에 추가 보안 계층을 구성하여 보안 및 거버넌스를 향상할 수 있습니다.

지배되는 계정 역시 보안 모범 사례를 따라 아키텍처를 설계해야 합니다. 지배하는 계정은 중앙에서 관리할 수 있는 추가 보안 계층을 제공하기 위해 사용됩니다.

이러한 모든 계정을 관리하려면
어떻게 해야 합니까?

aws training and certification



AWS Organizations

중앙 집중식 계정 관리

- 그룹 기반 계정 관리
- AWS 서비스에 대한 정책 기반 액세스
- 자동화된 계정 생성 및 관리
- 통합 결제
- API 기반

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Organizations는 계정 관리를 위한 관리형 서비스입니다. 조직은 모든 AWS 계정을 통합하고, 중앙에서 확인하고, 관리하기 위해 생성하는 엔터티입니다. Organizations에서 조직은 사용자가 설정하는 기능 집합으로 결정되는 다양한 기능을 보유합니다.

여러 AWS 계정에 대한 정책을 중앙에서 관리

Organizations는 여러 AWS 계정에 대한 정책을 관리하도록 지원합니다. 이 서비스를 사용하여 계정 그룹을 생성한 후 정책을 그룹에 연결하여 계정 전체에 올바른 정책이 적용되도록 할 수 있습니다.

Organizations는 사용자 지정 스크립트 및 수동 프로세스 없이 여러 계정에 대해 정책을 중앙에서 관리할 수 있게 해줍니다.

그룹 기반 계정 관리

Organizations를 사용하여 AWS 계정 그룹을 생성할 수 있습니다. 개발 리소스와 프로덕션 리소스에 사용할 계정 그룹을 각각 생성한 후 각 그룹에 서로 다른 정책을 적용할 수 있습니다.

AWS 서비스에 대한 정책 기반 액세스

Organizations를 사용하면 여러 AWS 계정에 대해 AWS 서비스 사용을 중앙에서 제어하는 서비스 제어 정책(SCP)을 생성할 수 있습니다. SCP는 IAM 정책이 IAM 사용자나 역할과 같은 계정의 엔터티에 부여할 수 있는 권한을 제한할 수 있습니다. 엔터티는 계정에 대한 SCP와 IAM 정책 모두가 허용한 서비스만 사용할 수 있습니다. 예를 들어 AWS Direct Connect에 대한 액세스를 제한하려는 경우, IAM 정책이 작동하기 전에 SCP가 액세스를 허용해야 합니다. 정책을 계정 그룹 또는 조직 내 전체 계정에 적용할 수 있습니다.

AWS 계정 생성 및 관리 자동화

Organizations API를 사용하여 새로운 AWS 계정의 생성과 관리를 자동화할 수 있습니다. Organizations API는 프로그래밍 방식으로 새로운 계정을 생성하고 이를 그룹에 추가할 수 있습니다. 그룹에 연결된 정책이 새로운 계정에 자동으로 적용됩니다. 예를 들어 개발자용 샌드박스 계정의 생성을 자동화하고 해당 계정의 엔터티가 필요한 AWS 서비스에만 액세스하도록 권한을 부여할 수 있습니다.

여러 AWS 계정의 결제 통합

Organizations를 사용하면 통합 결제를 통해 조직 내 모든 AWS 계정에 대해 단일 결제 방법을 설정할 수 있습니다. 통합 결제의 경우 모든 계정에서 발생한 비용을 통합해서 볼 수 있습니다. 또한 통합 결제를 사용하면 Amazon EC2와 Amazon S3의 볼륨 할인과 같이 사용량 집계를 통해 요금 혜택을 누릴 수 있습니다.

API 수준에서 AWS 서비스 제어

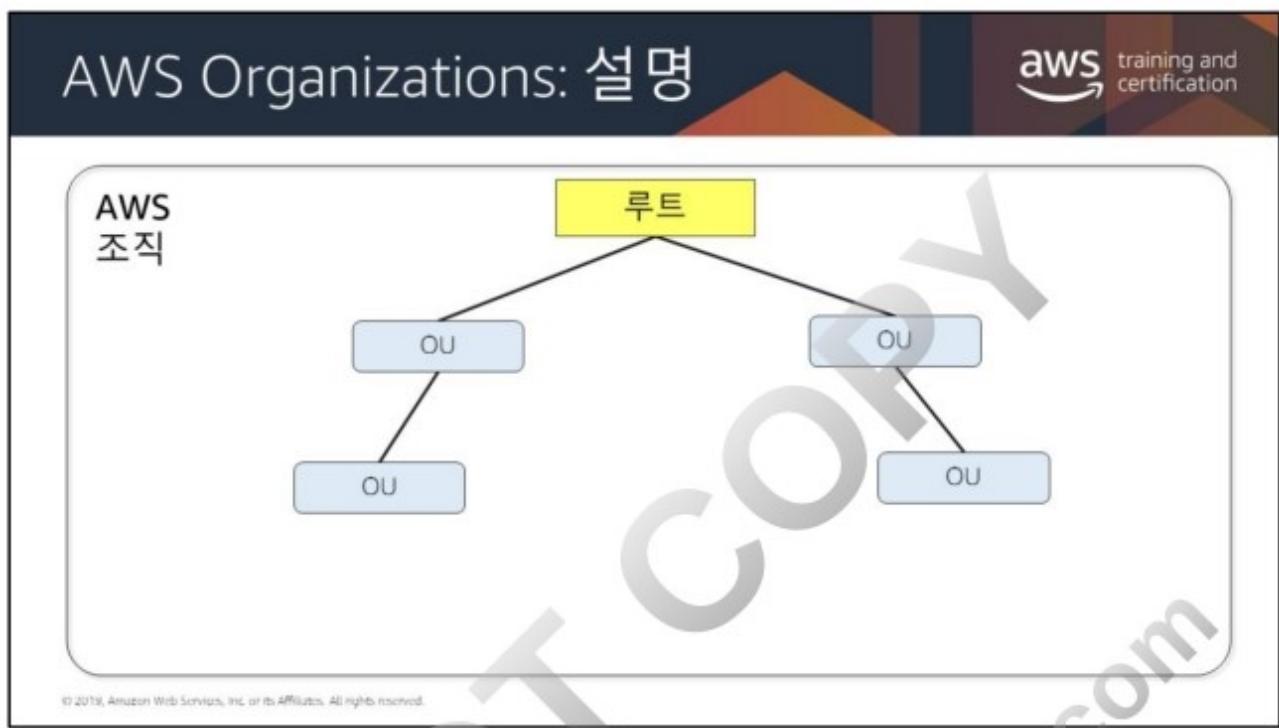
Organizations에서는 SCP를 사용하여 API 수준에서 AWS 서비스 사용을 관리할 수 있습니다. 예를 들어 계정 그룹에 정책을 적용하여 해당 계정의 IAM 사용자만 Amazon S3 버킷에서 데이터를 읽을 있도록 허용할 수 있습니다.

Organizations API를 사용하여 새로운 계정을 생성하고 이를 그룹에 추가할 수 있습니다. 그룹에 연결된 정책이 그룹에 추가된 계정에 자동으로 적용됩니다.

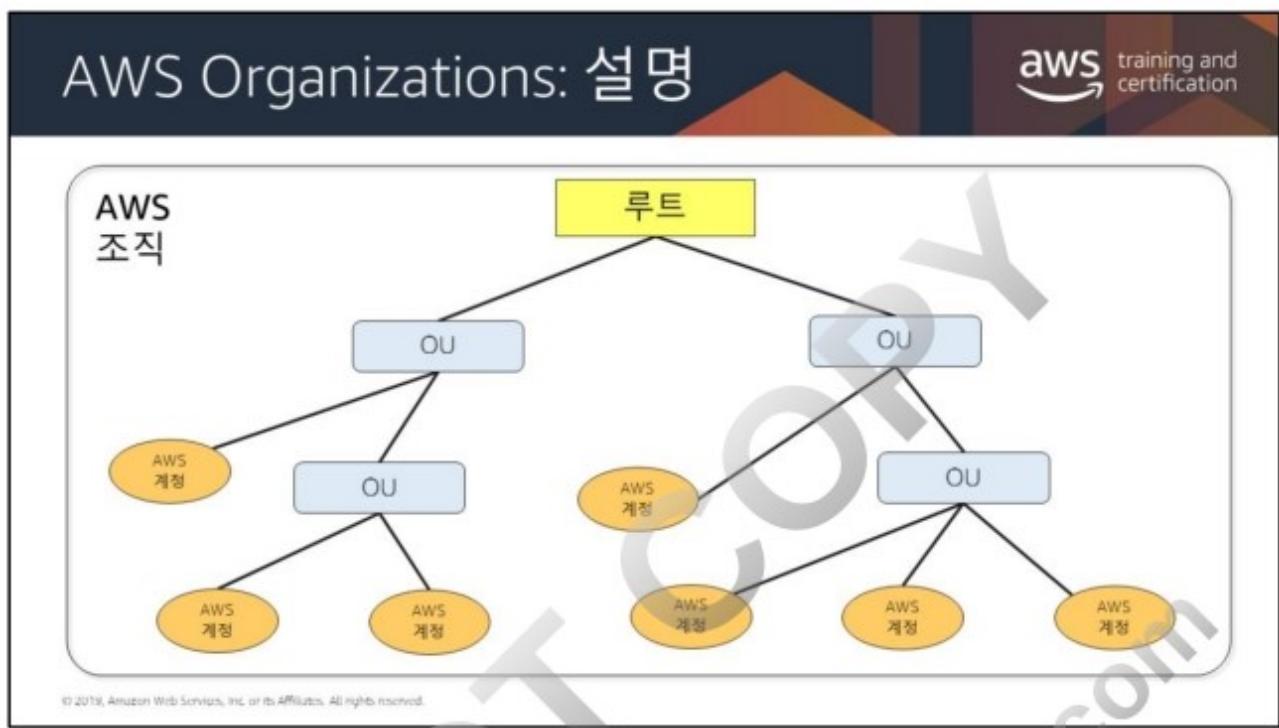




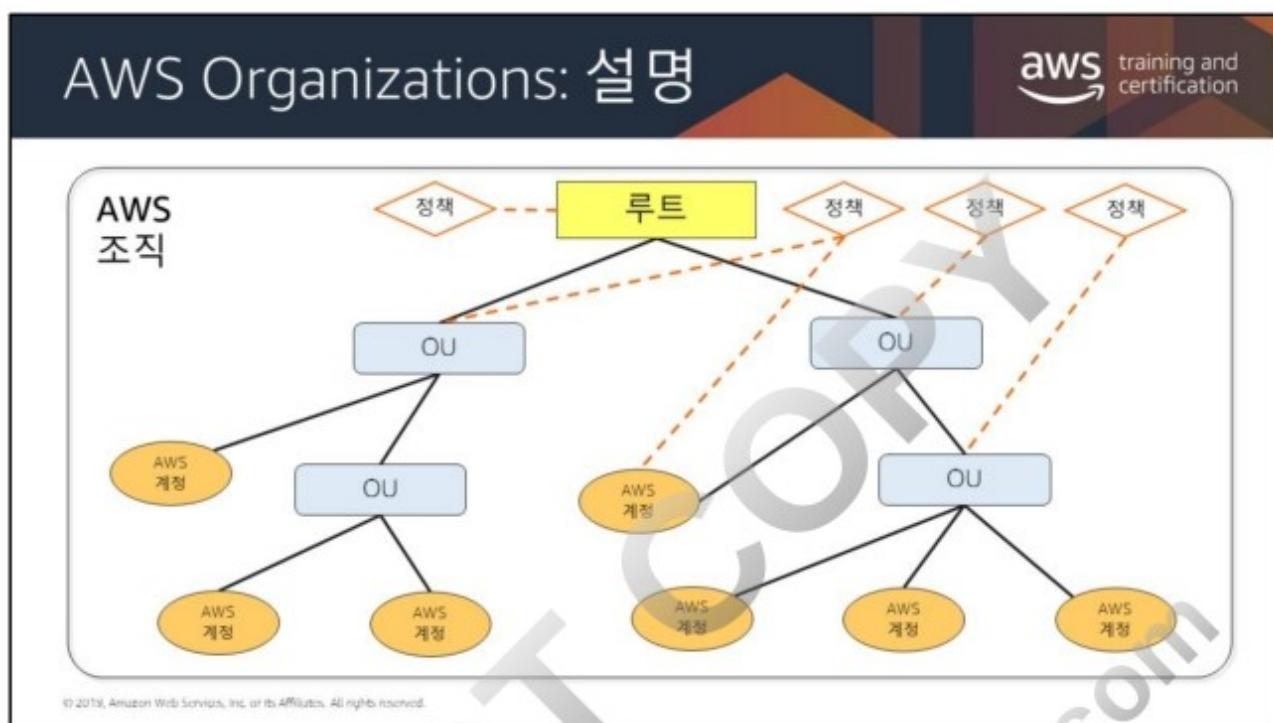
이 예에서 조직에 7개의 계정이 있으며 각 계정은 루트 아래에서 4개의 조직 단위(OU)로 구분되어야 합니다.



이제 조직에 4개의 조직 단위(ou)를 추가했습니다. 2개는 루트 바로 아래에 위치합니다. 그리고 각 기본 ou에 ou가 하나씩 있습니다.



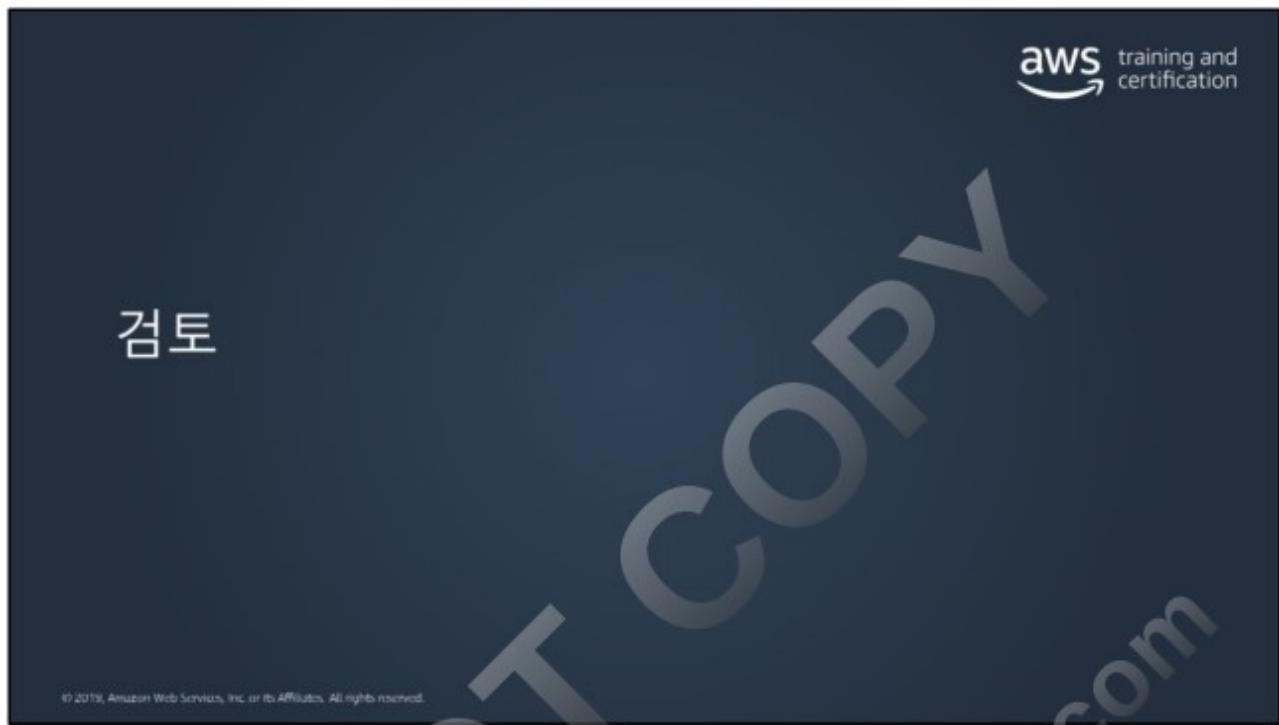
AWS 계정 7개가 모두 조직에 추가되고 적절한 OU에 배치됩니다.



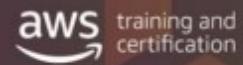
일단 계정이 추가되면 SCP를 조직에 적용할 수 있습니다.

이 예에서는 루트에 SCP가 연결되어 있습니다. 이 정책은 조직의 모든 OU와 계정에 적용됩니다. SCP는 하나 이상의 OU 또는 개별 계정에 적용될 수 있습니다.

AWS Organizations의 서비스 제어 정책은 세분화된 권한 제어를 지원합니다. 자세한 내용은 <https://aws.amazon.com/about-aws/whats-new/2019/03/service-control-policies-enable-fine-grained-permission-controls/>를 참조하십시오.



검토



리소스에 임시 권한을 부여해야 하는 경우
무엇을 사용합니까?

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DO NOT COPY
zlagusdbs@gmail.com

검토

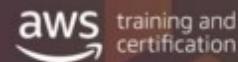
aws training and certification

리소스에 임시 권한을 부여해야 하는 경우
무엇을 사용합니까?

IAM 역할

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

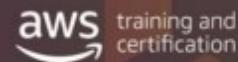
검토



하나의 사용자가 S3 버킷에 액세스할
수 없습니다. 문제의 원인을
파악하려면 무엇을 확인해야 합니까?

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

검토

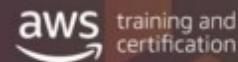


하나의 사용자가 S3 버킷에 액세스할
수 없습니다. 문제의 원인을
파악하려면 무엇을 확인해야 합니까?

사용자와 버킷에 연결된 정책

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

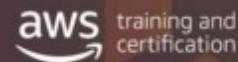
검토



1. DynamoDB를 호출하여 데이터를 가져오는 모바일 애플리케이션을 만들었습니다.
2. 이 애플리케이션은 DynamoDB SDK 및 AWS 계정 루트 사용자 액세스/보안 액세스 키를 사용하여 모바일 앱에서 DynamoDB에 연결합니다.
3. 이 시나리오에서 보안 모범 사례와 관련하여 어떻게 수정해야 합니까?

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

검토

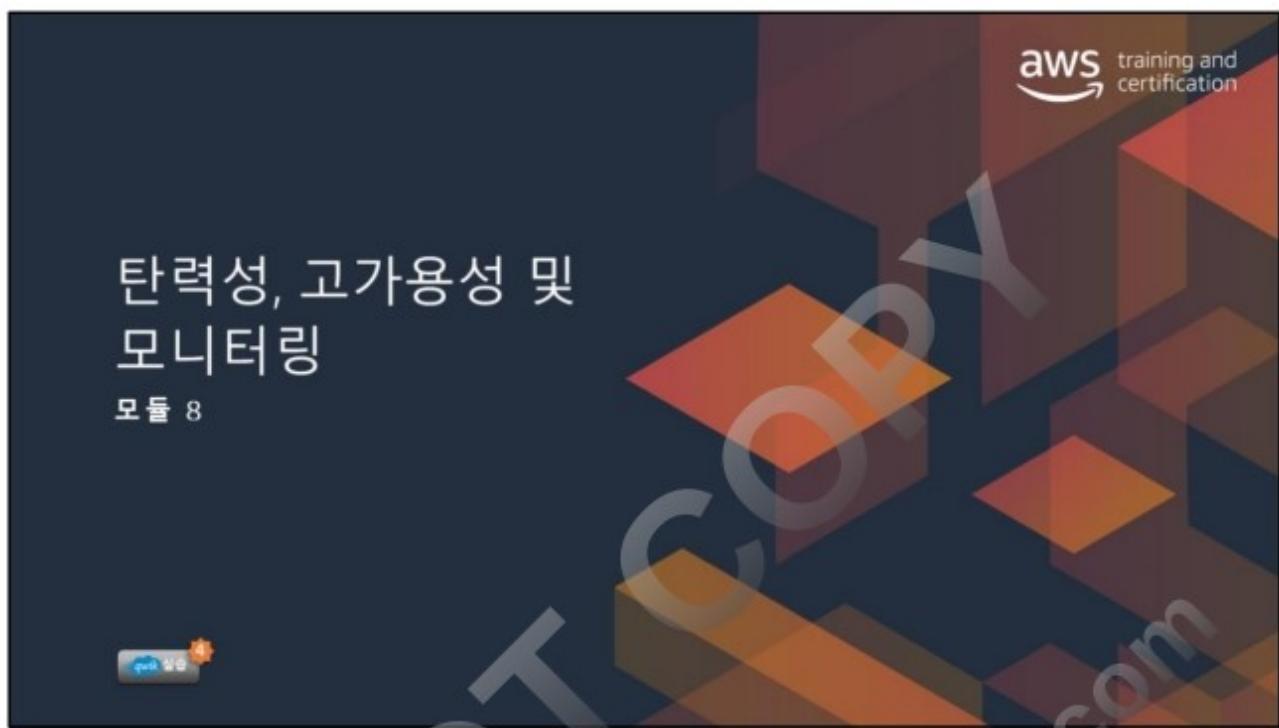


첫째, 프로덕션 환경에서 AWS 계정 루트 사용자 사용을 **중지합니다!**

그런 다음, 가능한 경우 앱이 웹 자격 증명 연동을 통해 IAM 역할을 사용하도록 합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.





모듈 8



아키텍처 측면에서의 필요성

조직에서 급격한 성장(수만 명의 사용자)이 발생하고 있으며 아키텍처에서 용량의 큰 변화를 처리해야 합니다.

모듈 개요

- 탄력성의 이해
- 모니터링
- 규모 조정

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DO NOT COPY
zlagusdbs@gmail.com

고가용성 요소

aws training and certification

내결함성:
애플리케이션 구성 요소의 **내장된 중복성**

확장성:
애플리케이션의 설계 변경 없이 **성장을 수용하는 능력**

복구성:
재해 발생 후 **서비스 복구**와 관련된 프로세스, 정책 및 절차

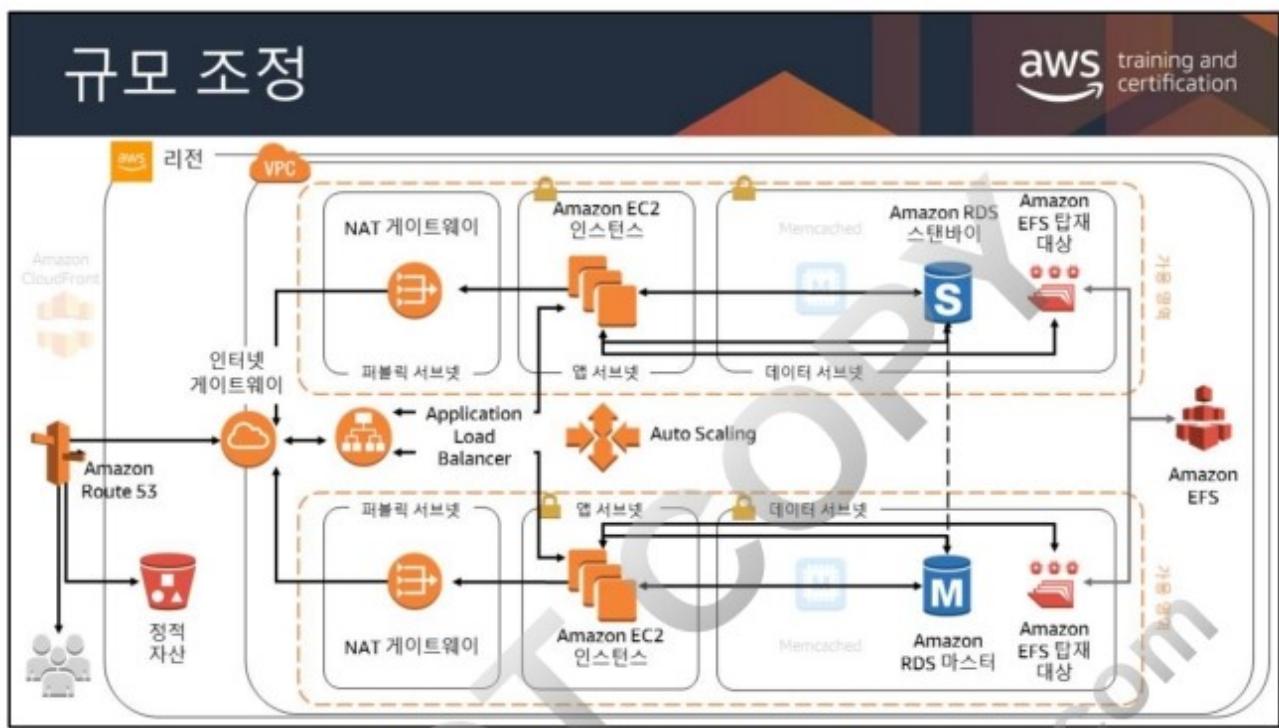
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

애플리케이션의 전반적인 가용성을 결정하는 세 가지 요소는 내결함성, 복구성 및 확장성입니다.

내결함성은 고가용성과 자주 혼동하지만, 내결함성은 애플리케이션 구성 요소의 내장된 중복성을 말합니다. 내결함성이 단일 장애 지점을 방지합니까? 이 모듈에서 나중에 내결함성을 다룹니다.

복구성은 가용성 구성 요소 중 하나로서 간과할 때가 많습니다. 자연재해로 하나 이상의 구성 요소에 장애가 발생하거나 기본 데이터 원본이 손상되었을 때, 데이터 손실 없이 신속하게 서비스를 복원할 수 있습니까? 특정 재해 복구 전략은 이후 모듈에서 다룹니다.

확장성은 필요한 기준 내에서 애플리케이션이 작동하고 사용할 수 있도록, 애플리케이션의 인프라가 증가된 용량 요구에 얼마나 신속하게 대응할 수 있는지 가늠하는 지표입니다. 확장성이 가용성을 보장하진 않지만, 애플리케이션 가용성의 한 부분입니다.



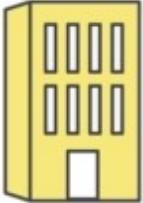
수업이 끝나면 이 아키텍처 디어그램의 모든 구성 요소를 이해할 수 있습니다.
또한 마찬가지로 규모가 크고 강력한 자체 아키텍처 솔루션을 구축할 수
있습니다.



탄력성이 없는 경우 어떤 모습입니까?

aws training and certification

일반적인 데이터 센터



리소스 비용을 선불로 결제하고 해당 리소스가 수요에 적합하길 바람



또는



너무 많은 추가 리소스, 비용 낭비, 전기 소모

ID 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

일반적인 데이터 센터: 일단 배포된 리소스는 일반적으로 필요 여부와 상관없이 실행됩니다. 결과적으로 사용할 필요가 없었던 용량에 대해서도 비용을 지불하게 됩니다. 더 괴로운 것은 촉박하게 더 많은 용량이 필요할 때 용량 추가가 불가능한 것입니다.

수요에 맞춰 확장하거나 축소할 수 있습니다.



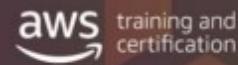
말할 필요도 없이 소매 회사인 Amazon.com은 가장 큰 AWS 고객 중 하나입니다. 보통 수신 트래픽은 예측하기가 쉽습니다. Amazon.com이 인프라를 AWS로 이전까지 전에는 많은 기업이 그렇듯이 전통적인 데이터 센터를 가지고 있었습니다. 피크 로드를 지원하기 위해서는 데이터 센터가 해당 용량을 지원할 수 있는 충분한 하드웨어와 소프트웨어를 제공해야 합니다.



Amazon.com은 11월마다 계절적 피크(미국에서 중요한 쇼핑 이벤트인 블랙 프라이데이)를 경험합니다. 회사는 일년에 한 번인 이 계절적 피크를 지원하기 위해 충분한 리소스를 투자해야 했습니다. 비즈니스가 성장하면서, Amazon.com은 계속해서 추가 하드웨어와 소프트웨어에 투자해야 했습니다. 어느 시점에는 공간이 부족해서 새로운 데이터 센터를 추가해야 했습니다.

온프레미스 솔루션을 사용했으므로 리소스의 76% 가량이 일 년 중 나머지 기간 동안 유휴 상태를 지속하여 리소스가 낭비되었습니다. 그러나 회사가 추가 하드웨어를 투자하지 않았다면 계절적 피크를 지원할 충분한 컴퓨팅 용량을 확보하지 못했을 것입니다. 서버가 중단되었다면 회사는 고객 신뢰를 상실했을 것입니다.

탄력성은 무엇입니까?



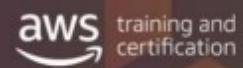
탄력적인 인프라는 용량 요구사항이 변화함에 따라
지능적으로 확장 및 축소될 수 있습니다.

예:

- 트래픽 급증 시 웹 서버 수 증가
- 트래픽이 줄어들 때 데이터베이스의 쓰기 용량 감소
- 아키텍처 전반에 걸친 일상적인 수요 변동 처리

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

세 가지 유형의 탄력성



시간 기반

리소스가 사용되지 않을 때 리소스 끄기
(개발 및 테스트 환경)

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DO NOT COPY
zlagusdbs@gmail.com

세 가지 유형의 탄력성

aws training and certification

 시간 기반	리소스가 사용되지 않을 때 리소스 끄기 (개발 및 테스트 환경)
 볼륨 기반	수요 강도에 맞게 규모 조정 (충분한 컴퓨팅 파워가 있어야 함)
 예측 기반	일일 및 주간 추세를 기반으로 향후 트래픽 예측 (정기적으로 발생하는 스파이크 포함)

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.





환경 모니터링은 아키텍처를 생성할 때 고려해야 할 가장 중요한 요소 중 하나입니다. 리소스 운영 및 작동을 추적할 수 있는 방법이 항상 필요합니다. 모니터링은 “무언가 변화가 필요한가”라는 물음에 대한 첫 번째 힌트를 제공합니다. 다음은 기억해야 할 몇 가지 사항입니다.

- 모니터링은 수요 증가에 따라 확장되고 수요 감소에 따라 축소될 수 있는 대응적 아키텍처를 구축하기 위한 바로 첫 번째 단계입니다. 이 유형의 조정은 비용을 크게 절감하고 여러분과 여러분의 고객에게 더 나은 사용자 경험을 제공합니다.
- 리소스 사용률 및 애플리케이션 성능이 인프라가 수요를 충족하도록 보장하기 위한 중요한 구성 요소입니다. 모니터링을 통해 이 정보를 확보할 수 있습니다.
- 또한 모니터링은 보안 측면에서도 매우 중요합니다. 유효한 파라미터를 사용하면 사용자가 액세스 권한이 없는 AWS 환경에 액세스하는 경우를 파악할 수 있습니다.