



training and
certification

Architecting on AWS (KO)

Student Guide

버전 6.5.3

100-ARCHIT-65-KO-SG

인쇄는 오로지 개인의 사적 용도를 위한 것입니다. 이 책의 어떠한 부분도 출판업체의 사전 허가 없이 복제 또는 전송될 수 없습니다. 이를 위반할 경우 처벌을 받게 됩니다.

© 2019 Amazon Web Services, Inc. 및 자회사. All rights reserved.

본 내용은 Amazon Web Services, Inc.의 사전 서면 허가 없이 전체 또는 일부를
복제하거나 재배포할 수 없습니다. 상업적인 복제, 임대 또는 판매는 금지됩니다.

본 과정에 대한 수정 사항이나 피드백이 있으면 다음으로 이메일을 보내주십시오.

aws-course-feedback@amazon.com.

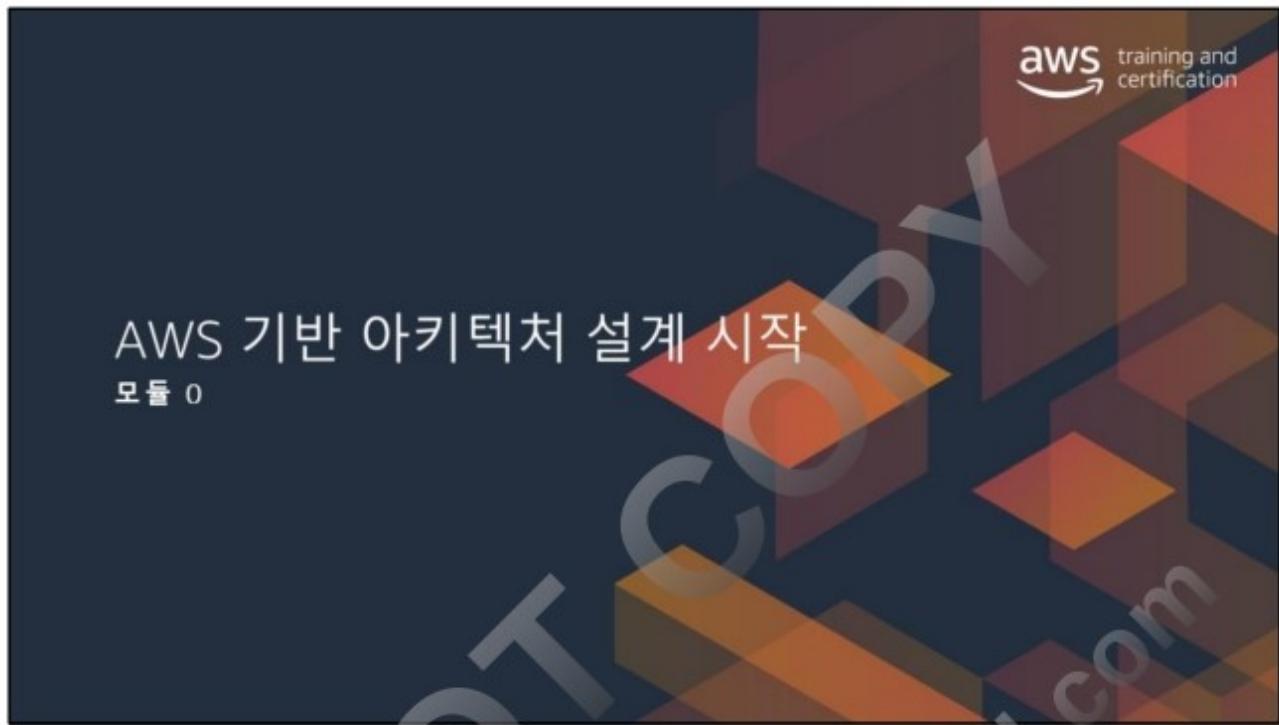
기타 모든 문의사항은

<https://aws.amazon.com/contact-us/aws-training/>을 통해 연락해 주십시오.

모든 상표는 해당 소유자의 자산입니다.

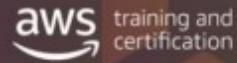
목차

모듈 0: AWS 기반 아키텍처 설계 시작	4
모듈 1: 소개	10
모듈 2: 가장 간단한 아키텍처	34
모듈 3: 컴퓨팅 계층 추가	83
모듈 4: 데이터베이스 계층 추가	153
모듈 5: AWS에서의 네트워킹 1부	210
모듈 6: AWS 기반 네트워킹 2부	264
모듈 7: AWS Identity and Access Management(IAM)	325
모듈 8: 탄력성, 고가용성 및 모니터링	388
모듈 9: 자동화	448
모듈 10: 캐싱	488
모듈 11: 결합 해제된 아키텍처 구축	535
모듈 12: 마이크로 서비스 및 서비스 아키텍처	570
모듈 13: RTO/RPO 및 백업 복구 설정	626
모듈 14: 최적화 및 검토	680
모듈 15: 과정 마무리	707
모듈: 부록	711



DO NOT COPY
zlagusdbs@gmail.com

과정 결과



- AWS 아키텍처의 각 측면과 어떻게 이들이 결합되어 복잡한 시스템을 구축하는지 설명할 수 있습니다.
- AWS 서비스를 활용하여 다양한 시나리오를 위한 아키텍처를 구축하는 과정을 체험합니다.
- AWS 클라우드 모범 사례 및 설계 패턴을 따라 최적의 IT 솔루션을 설계할 수 있습니다.

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

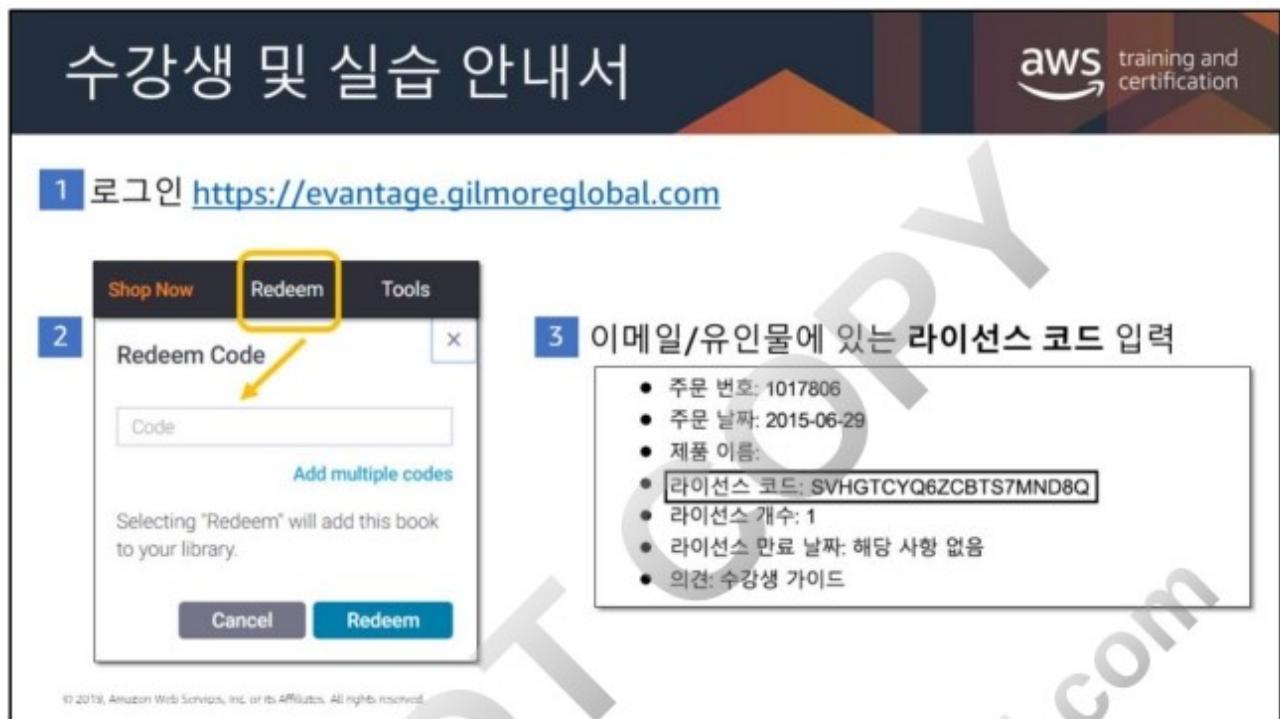
안내 사항



- 주차
- 시설:
 - 비상구
 - 화재 경보 프로토콜
 - 보안
- 휴식 및 점심 시간
- 음식
- 휴대폰
- 수강생 매뉴얼: Gilmore

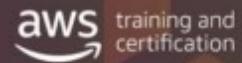
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DO NOT COPY
zlagusdbs@gmail.com



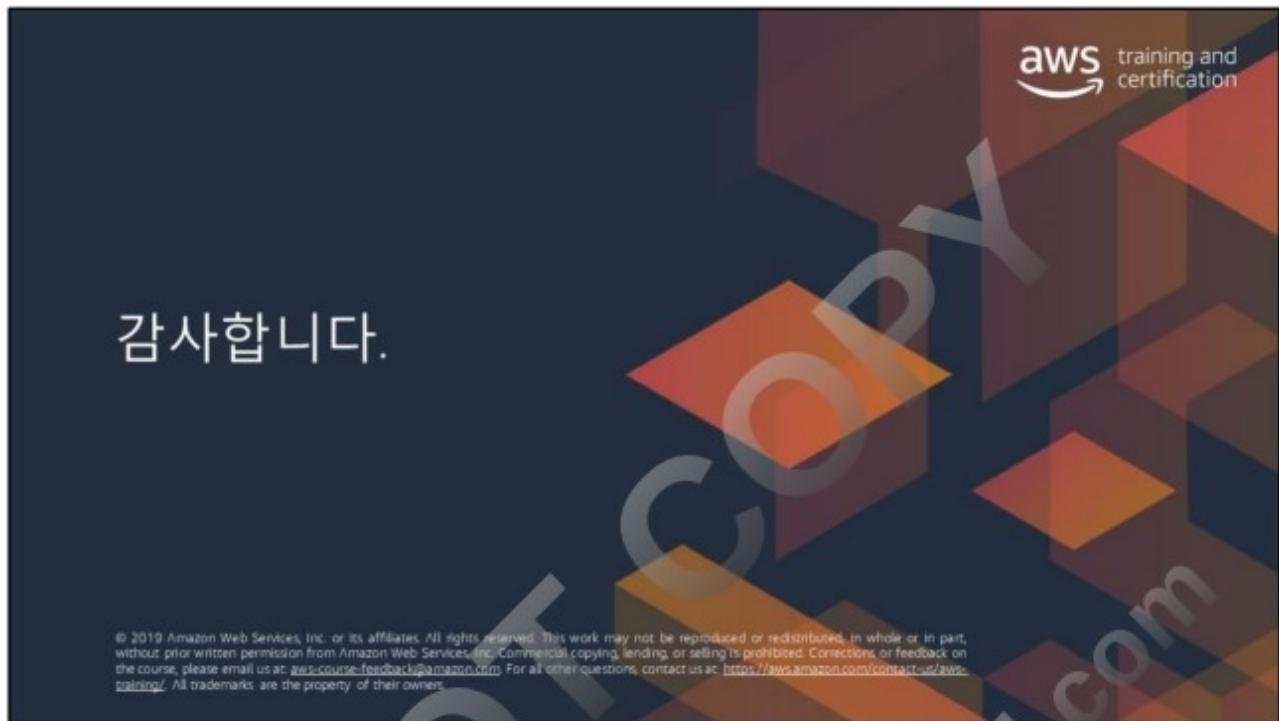
로그인해 수강생 및 실습 안내서에 액세스하려면 <http://online.vitalsource.com>을
참조하십시오.

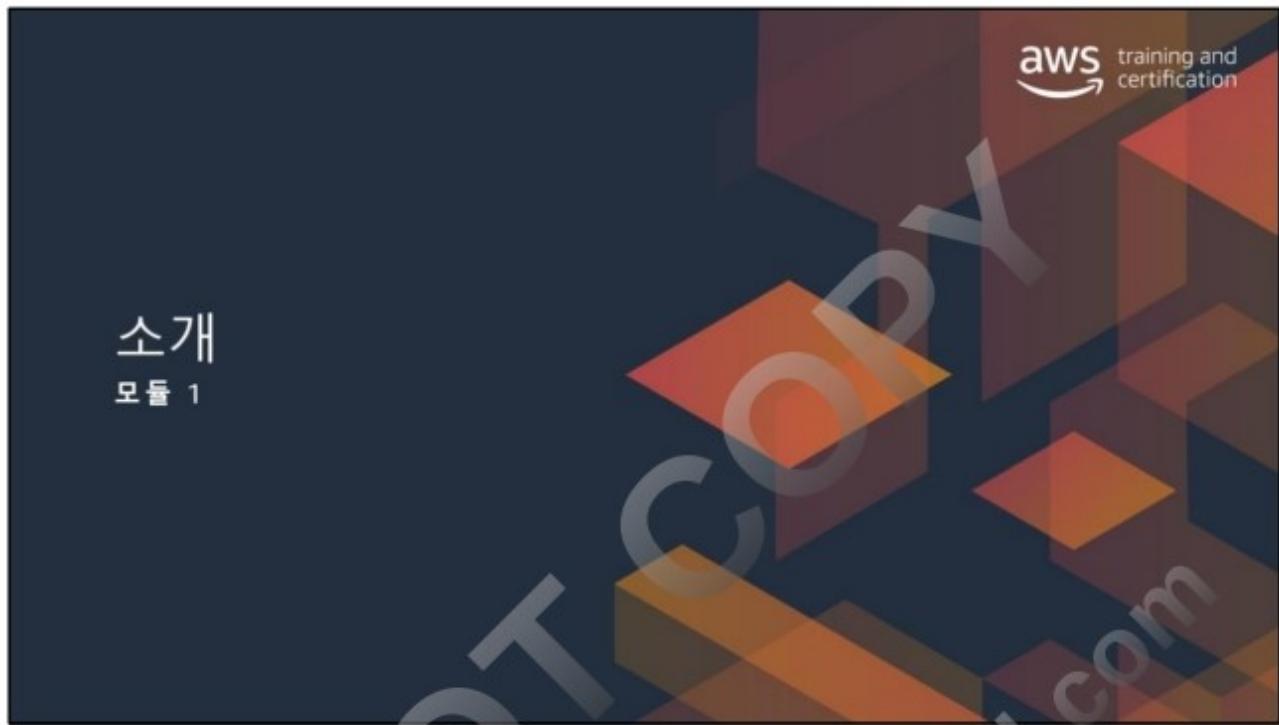
본인 소개



- 이름
- 소속 조직
- 역할
- 기대치
- AWS 경험 수준

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





DO NOT COPY
zlagusdbs@gmail.com

미리 보기



간단한 복습:

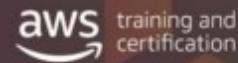
- 클라우드란 무엇입니까? AWS란 무엇입니까?
- 클라우드 설계 지침
- Well-Architected 프레임워크
- AWS 글로벌 인프라
- 대규모 아키텍처 설계

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

DO NOT COPY
zlagusdbs@gmail.com



모듈 1



아키텍처 측면에서의 필요성

때는 2000년, Amazon.com의 새로운 쇼핑 웹 사이트 서비스가 고가용성을 확보하고 효율적으로 확장하기 위해 애쓰고 있었습니다.

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



AWS training and certification

Amazon.com의 전자 상거래 도구는 “뒤죽박죽” 섞여 있었습니다.

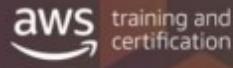
- 애플리케이션 및 아키텍처가 적절한 계획 없이 구축된 것입니다.
- 서비스는 서로 구분되어야 했습니다.

해결책: 도구가 잘 문서화된 일련의 API로 정비되어 Amazon에서 서비스 개발을 위한 표준이 되었습니다.

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

<https://techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/>

문제 지속



여전히 Amazon.com은 신속하게 애플리케이션을 구축하는 데 어려움을 겪었습니다.

- 데이터베이스, 컴퓨팅 및 스토리지 구성 요소는 구축하는 데 **3개월**이 걸렸습니다.
- 각 팀이 **규모 또는 재사용에 대한 계획 없이** 자체 리소스를 구축했습니다.

해결책: 인프라 상에 고가용성, 확장성, 신뢰성이 뛰어난 아키텍처를 생성하기 위한 내부 서비스를 구축했습니다. 2006년, 이들 서비스를 AWS로 판매하기 시작했습니다.

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

클라우드란 무엇입니까? AWS란 무엇입니까?

aws training and certification

프로그래밍 가능한 리소스 동적 기능 종량 과금제

클라우드가 제공하는 다른 이점은 무엇입니까?

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

클라우드는 그 고유한 파워를 활용할 수 있는 사람에게 막대한 이점을 제공합니다. 프로그래밍 가능한 리소스로 IT 자산을 사용하면 기존의 접근 방식으로는 가능하지 않은 방식으로 빠르게 인프라를 구축하고 해체할 수 있습니다.

이러한 리소스에 액세스하여 매우 역동적으로 혁신을 추진할 수 있습니다. 마우스 클릭 몇 번으로 데이터베이스 처리량 또는 컴퓨팅 파워를 늘릴 수 있습니다. 이는 실제로 비즈니스에서 상당한 차이를 만들 수 있는 민첩성과 유연성을 제공합니다.

또한 클라우드 컴퓨팅의 가장 큰 장점 중 하나는 사용량에 따라 비용을 지불하는 것입니다. 본격적인 약정 없이 시스템을 테스트하고 활용할 수 있습니다. 이러한 서비스는 언제든지 사용을 중지할 수 있으며 필요에 따라 전술을 변경할 수 있습니다.

AWS를 사용한 클라우드 컴퓨팅의 여섯 가지 장점을 살펴보겠습니다. 자세한 내용은 <https://aws.amazon.com/what-is-cloud-computing>을 참조하십시오.

클라우드 컴퓨팅의 여섯 가지 장점

aws training and certification

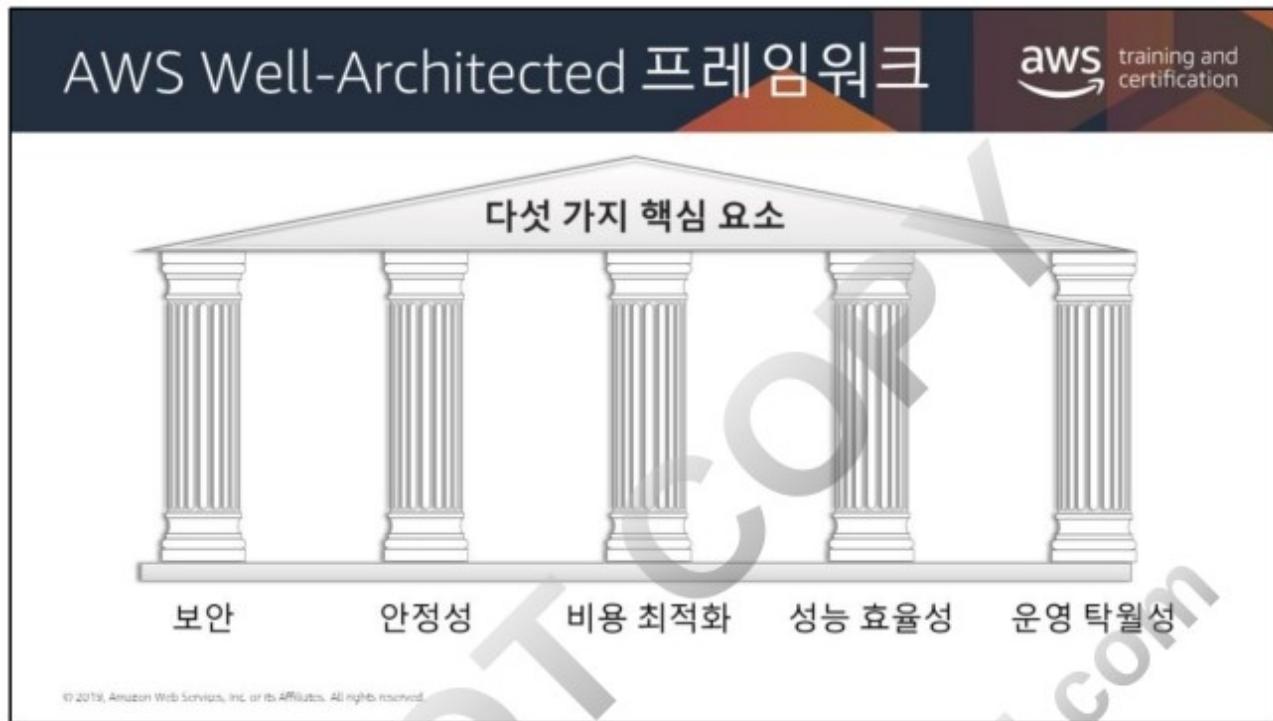
-  자본 비용을 가변 비용으로 대체
-  규모의 경제로 얻게 되는 이점
-  용량 추정 불필요
-  속도 및 민첩성 개선
-  중요한 문제에 집중
-  몇 분 만에 전 세계에 배포

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

AWS를 사용한 클라우드 컴퓨팅의 여섯 가지 주요 이점에 대한 자세한 내용은 다음을 참조하십시오.

https://www.youtube.com/watch?v=yMJ75k9X5_8





먼저 Well-Architected 프레임워크 설계 원칙의 목표 일부를 살펴보겠습니다.

잘 설계된 아키텍처에 대한 몇 가지 도움을 받고 싶은 경우:

AWS Well-Architected Tool은 최신 AWS 모범 사례에 대한 온디맨드 액세스를 제공하는 셀프 서비스 도구입니다. 아키텍트 및 관리자가 AWS 솔루션스 아키텍트 없이도 언제든지 AWS 워크로드를 검토할 수 있도록 도와줍니다. 이 서비스는 클라우드 아키텍트가 안전하고, 성능이 뛰어나며, 복원력을 갖춘 효율적인 애플리케이션 인프라를 구축할 수 있도록 개발된 AWS Well-Architected 프레임워크를 기반으로 합니다. 이 서비스를 사용하면 워크로드의 상태를 검토하고 최신 AWS 아키텍처 모범 사례와 비교할 수 있습니다.

보안

aws training and certification

The slide illustrates the AWS Security Pillar with four main components:

- 자격 증명 기반** (Identity): Represented by a green 'i' icon.
- 추적 가능성 활성화** (Compliance): Represented by a wrench and screwdriver icon.
- 모든 계층에서의 보안** (Security): Represented by a stack of layered clouds.
- 위험 평가 및 완화 전략** (Risk Management): Represented by an orange briefcase icon.

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

보안이 다루는 것은 정보 보호와 가능한 손해의 완화입니다. 고객의 아키텍처는 강력한 자격 증명 기반, 추적 가능성 활성화, 모든 계층에서 보안 적용, 보안 모범 사례 자동화, 전송 및 저장 시 데이터 암호화 등의 몇몇 기본적인 보안 조치를 구현하여 보다 강력한 보안 태세를 갖추게 됩니다.

자세한 내용은 다음을 참조하십시오.

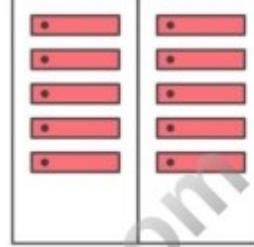
<https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>

안정성

aws training and certification

- 컴퓨팅 리소스를 동적으로 확보하여 수요를 충족
- 인프라 또는 서비스 장애로부터 신속하게 복구
- 다음과 같은 중단을 완화
 - 구성 오류
 - 일시적인 네트워크 문제

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



기존 환경에서는 안정성을 보장하기가 어려울 수 있습니다. 단일 장애 지점, 자동화 미비, 탄력성 부족에서 문제가 발생합니다. 안정성 핵심 요소의 아이디어를 적용하면 이러한 문제를 다수 방지할 수 있습니다. 고가용성, 내결함성, 전반적 중복성 측면에서 아키텍처를 적절히 설계하면 여러분과 여러분의 고객에게 도움이 될 수 있습니다.

자세한 내용은 다음을 참조하십시오.

<https://d1.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf>

비용 최적화

aws training and certification

- 효율성 측정
- 불필요한 비용 제거
- 관리형 서비스 사용을 고려



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

비용 최적화는 모든 우수한 아키텍처 설계에서 항상 요구되는 사항입니다. 이 프로세스는 반복적이며 프로덕션 수명 내내 정교화되고 개선되어야 합니다. 현재 아키텍처가 목표를 기준으로 얼마나 효율적인지 이해하는 것이 불필요한 비용을 제거함으로써 궁극적으로 도움이 됩니다. 관리형 서비스는 클라우드 규모에서 운영되고 트랜잭션 또는 서비스당 더 저렴한 비용을 제공할 수 있으므로 이러한 서비스의 사용을 고려합니다.

자세한 내용은 다음을 참조하십시오.

<https://d1.awsstatic.com/whitepapers/architecture/AWS-Cost-Optimization-Pillar.pdf>

운영 탁월성

aws training and certification

- 시스템을 실행 및 모니터링하는 기능
- 지원 프로세스 및 절차를 지속적으로 개선하기 위해

배포됨

업데이트됨

운영됨

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

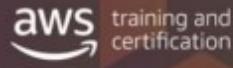
설계 또는 아키텍처를 생성할 때 이들이 배포, 업데이트 및 운영될 방식을 고려합니다. 결함 축소 및 안전한 수정을 위해 노력하고 로깅 계측을 사용한 관찰을 활성화하는 것이 반드시 필요합니다.

AWS에서는 전체 워크로드(애플리케이션, 인프라, 정책, 거버넌스 및 운영)를 코드로 볼 수 있습니다. 모든 것이 코드를 사용하여 정의되고 업데이트될 수 있습니다. 이는 애플리케이션 코드에 사용하는 동일한 엔지니어링 원칙을 스택의 모든 요소에 적용할 수 있다는 의미입니다.

자세한 내용은 다음을 참조하십시오.

<https://d1.awsstatic.com/whitepapers/architecture/AWS-Operational-Excellence-Pillar.pdf>

성능 효율성



aws training and certification

- 효율적인 리소스를 선택하고 수요 변화에 맞춰 효율성을 유지
- 고급 기술을 대중화
- Mechanical sympathy

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

성능을 고려할 때, 고객은 컴퓨팅 리소스를 효율적으로 사용하고 수요가 변동해도 이 효율을 유지하여 성능을 최대화하기를 원할 것입니다.

또한 고급 기술을 대중화하는 것도 중요합니다. 기술을 직접 구현하기 어려운 상황에서는 벤더를 이용하는 것을 고려하십시오. 벤더는 고객을 위해 기술을 구현하면서 복잡성과 지식을 떠맡아 고객 내부 팀이 보다 가치 부가적인 업무에 집중할 수 있게 해줍니다.

Mechanical sympathy: 달성하려는 목표에 가장 적합한 기술 접근 방식을 사용합니다. 예를 들어, 데이터베이스 또는 스토리지 접근 방식을 선택할 때 데이터 액세스 패턴을 고려합니다.

자세한 내용은 다음을 참조하십시오.

<https://d1.awsstatic.com/whitepapers/architecture/AWS-Performance-Efficiency-Pillar.pdf>

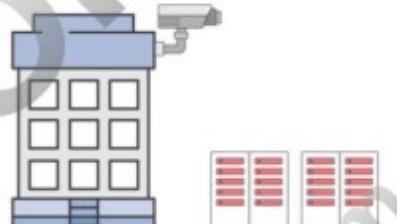


AWS 데이터 센터

aws training and certification

- 보통 단일 데이터 센터에서 수만 개의 서버를 운영
- 모든 데이터 센터는 “콜드 연결”이 아니라 온라인으로 연결됨
- AWS 사용자 정의 네트워크 장비:
 - 다양한 ODM 사용
 - 사용자 지정 네트워크 프로토콜 스택

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



AWS 데이터 센터는 전 세계 여러 리전에 클러스터 형태로 구축됩니다. 대규모의 데이터 센터는 바람직하지 않습니다. 모든 데이터 센터는 온라인 방식이며 고객에게 서비스를 제공합니다. 어떤 데이터 센터도 “콜드” 방식이 아닙니다. 장애 시 자동화된 프로세스는 고객 데이터 트래픽을 장애 지역에서 먼 곳으로 이동합니다. 핵심 애플리케이션이 N+1 구성으로 구현되므로, 데이터 센터에 장애가 발생할 경우에도 나머지 사이트로 트래픽을 균형 있게 분산시킬 수 있는 충분한 용량을 갖추고 있습니다.

원천 설계 제조업자, 즉 "ODM"은 제2회사의 사양에 따라 제품을 설계하고 제조합니다. 제2회사는 이 제품을 자신의 브랜드로 판매합니다.

자세한 내용은 <https://aws.amazon.com/compliance/data-center/>를 참조하십시오.

AWS 가용 영역

각 가용 영역은

- 하나 이상의 데이터 센터로 구성됩니다.
- 내결합성을 갖도록 설계됩니다.
- 프라이빗 링크를 통해 다른 가용 영역과 상호 연결됩니다.
- 가용 영역은 사용자가 선택할 수 있습니다.
- AWS는 복원성을 위해 가용 영역 간 복제를 권장합니다.

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

AWS 데이터 센터는 가용 영역 내에 편성됩니다. 각 가용 영역은 하나 이상의 데이터 센터로 구성되며, 일부 가용 영역은 최대 6개의 데이터 센터로 구성되기도 합니다. 하지만 하나의 데이터 센터가 2개의 가용 영역에 포함될 수는 없습니다.

각 가용 영역은 독립된 장애 영역으로 설계되었습니다. 즉, 가용 영역은 일반적인 대도시 리전 내에서 물리적으로 격리되어 있으며, 홍수 위험성이 낮은 지대에 위치합니다(자세한 홍수 지대 분류는 리전에 따라 차이가 있음). 또한, 별도의 무정전 전원 공급 장치와 현장 백업 발전 시설 외에도 독립적인 유틸리티의 서로 다른 그리드를 통해 전력을 공급받음으로써 단일 장애 지점이 더욱 줄어듭니다. 가용 영역은 여러 티어1 전송 서비스 제공자에게 모두 중복으로 연결됩니다.

사용자는 시스템이 상주할 가용 영역을 선택해야 합니다. 시스템은 여러 가용 영역에 걸쳐 확장할 수 있습니다. 재해가 발생하는 경우, 임시 또는 장기 가용 영역 장애를 극복할 수 있도록 시스템을 설계해야 합니다. 여러 개의 가용 영역에 애플리케이션을 분산하면 자연 재해나 시스템 장애 등 대부분의 장애 상황에서도 복원력을 유지할 수 있습니다.

AWS 리전

각 AWS 리전은 두 개 이상의 가용 영역으로 이루어져 있습니다.

- AWS는 전 세계에 21개의 리전을 보유하고 있습니다.
- 사용자는 리전 간 데이터 복제를 활성화하고 제어할 수 있습니다.
- 리전 간 통신은 AWS 백본 네트워크 인프라를 사용합니다.

The diagram illustrates three distinct regions, each represented by a blue horizontal bar at the bottom. Above each bar are two stylized building icons. The top bar has one large building and one smaller building. The middle bar has two medium-sized buildings. The bottom bar has one large building and one smaller building. The entire diagram is enclosed in a light gray rounded rectangle with the text 'AWS 리전' (AWS Region) written above it in orange.

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

가용 영역은 다시 AWS 리전으로 그룹화됩니다. 각 리전은 2개 이상의 가용 영역을 포함합니다.

애플리케이션을 여러 가용 영역으로 분산할 때는 EU 개인 정보 보호 지침과 같은 위치별 개인 정보 및 규정 준수 요구 사항을 주의하십시오. 특정 리전에 데이터를 저장하는 경우, 해당 리전 내에서만 데이터가 복제됩니다. 고객이 데이터를 저장한 리전 외부로 AWS가 데이터를 이동하는 일은 없습니다. 비즈니스 요구 사항에 따라 필요할 경우 리전 간 데이터 복제는 사용자의 책임입니다. AWS에서는 각 리전이 위치한 국가 및 주(해당하는 경우)에 대한 정보를 제공하며, 규정 준수와 네트워크 지역 시간 요구 사항에 따라 데이터를 저장할 리전을 선택하는 것은 사용자의 책임입니다.

AWS 리전은 여러 인터넷 서비스 공급자(ISP), 그리고 퍼블릭 인터넷에 비해 비용이 더 저렴하고 리전 간 네트워크 지연 시간이 더 일관적인 프라이빗 글로벌 네트워크 백본에 연결되어 있습니다.

자세한 내용은 <https://aws.amazon.com/about-aws/global-infrastructure/#reglink-pr>을 참조하십시오.



AWS는 지정한 리전에만 데이터가 보관되도록 하고 지역 시간을 줄이고 처리량은 늘리려는 고객을 돋기 위해 꾸준히 글로벌 인프라를 확장하고 있습니다. AWS는 귀하를 비롯한 모든 고객의 비즈니스가 성장함에 따라 고객의 글로벌 요구에 맞는 인프라를 지속적으로 제공할 것입니다.

AWS GovCloud(미국)는 특정 규제 및 규정 준수 요구 사항을 준수함으로써 미국 정부 기관과 고객들이 민감한 워크로드를 클라우드로 이전할 수 있도록 설계된 격리 리전입니다.

사용 가능한 AWS 제품과 서비스는 리전에 따라 달라지므로 모든 서비스를 모든 리전에서 사용할 수 있는 것은 아닙니다.

선결제 비용, 장기 약정, 글로벌 인프라 유지 관리와 운영에 따른 확장 문제를 방지하면서 최종 사용자의 지역 시간을 줄일 수 있는 리전에서 애플리케이션과 워크로드를 실행할 수 있습니다.



최종 사용자에게 더 짧은 지연 시간으로 콘텐츠를 전송하기 위해 Amazon CloudFront는 현재 30개국 69개 도시에서 187개 PoP(엣지 로케이션 176개, 리전 엣지 캐시 11개)의 글로벌 네트워크를 사용하고 있습니다.

엣지 로케이션은 북미, 유럽, 아시아, 오스트레일리아 및 남아메리카에 위치해 있으며, Amazon Route 53 및 Amazon CloudFront와 같은 AWS 서비스를 지원합니다.

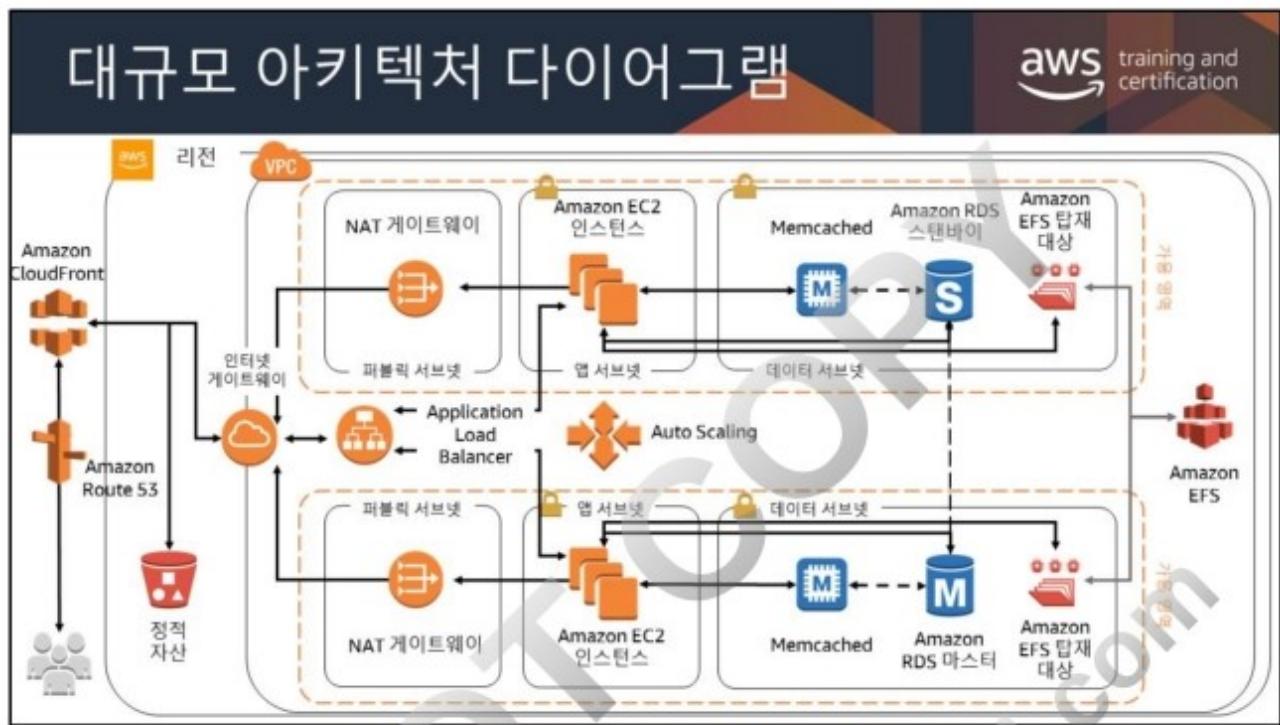
리전 엣지 캐시

Amazon CloudFront에서 기본적으로 사용되는 리전 엣지 캐시는 엣지 로케이션에 유지할 정도로 자주 액세스하지 않는 콘텐츠가 있을 때 활용됩니다. 리전 엣지 캐시가 이 콘텐츠를 흡수하여 오리진 서버에서 해당 콘텐츠를 가져오지 않아도 되는 대안을 제공합니다.

자세한 내용은 <https://aws.amazon.com/cloudfront/features/>를 참조하십시오.



DO NOT COPY
zlagusdbs@gmail.com



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

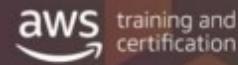






수업이 끝나면 이 아키텍처 디아그램의 모든 구성 요소를 이해할 수 있습니다. 또한 마찬가지로 규모가 크고 강력한 자체 아키텍처 솔루션을 구축할 수 있습니다.

모듈 2



아키텍처 측면에서의 필요성

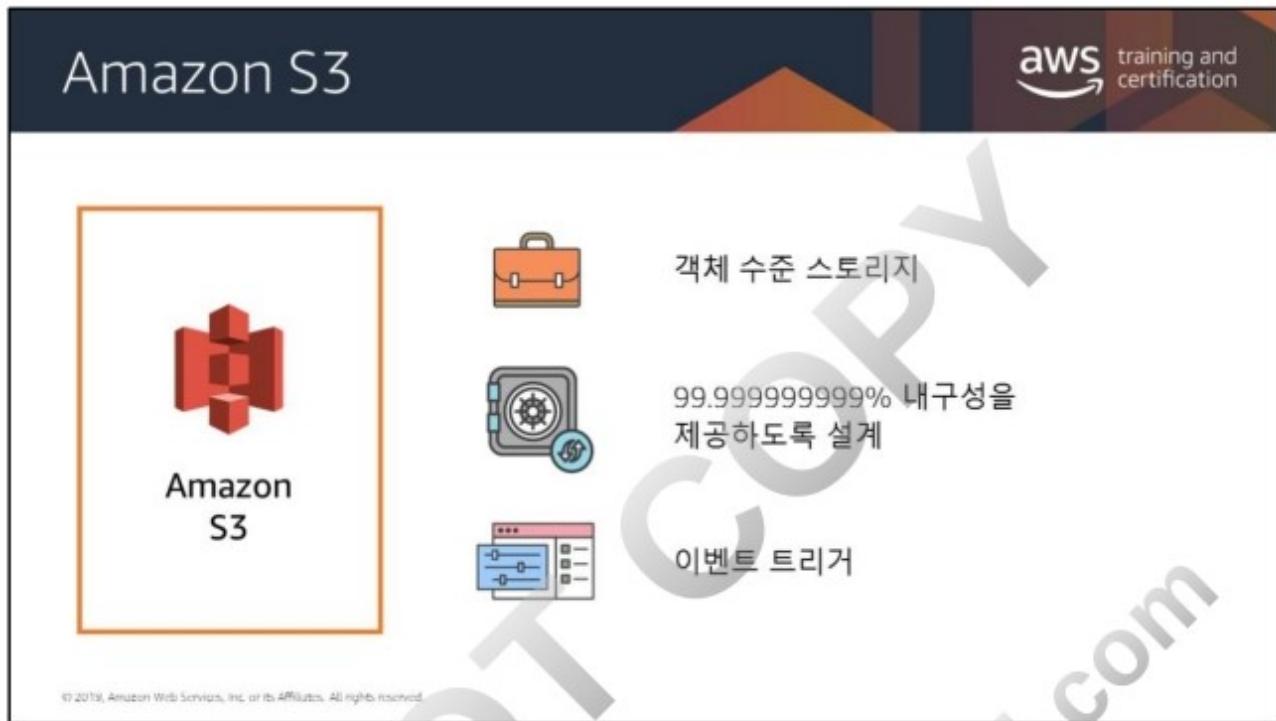
이제 막 창업한 기업으로서 클라우드에서 안정적으로 데이터를 배포, 저장, 분석하는 간편한 방법이 필요합니다.

모듈 개요

- Amazon Simple Storage Service (Amazon S3)가 해결할 수 있는 문제
- 콘텐츠를 효율적으로 저장
- Amazon Glacier가 해결할 수 있는 문제
- 리전 선택

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





Amazon S3는 객체 수준 스토리지입니다. 즉, 파일 일부를 변경하려면, 파일을 변경한 다음 변경된 파일 전체를 다시 업로드해야 합니다.

Amazon S3를 사용하면 원하는 만큼 데이터를 저장할 수 있습니다. 개별 객체는 5TB를 넘을 수 없지만, 총 데이터는 필요한 만큼 저장할 수 있습니다.

기본적으로 Amazon S3의 데이터는 여러 시설과 각 시설의 여러 디바이스에 중복 저장됩니다.

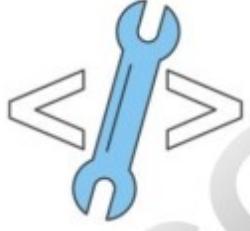
Amazon S3는 웹 기반 AWS Management Console, API 및 SDK를 통한 프로그래밍 방식 또는 타사 솔루션(API/SDK를 사용)을 통해 액세스할 수 있습니다.

Amazon S3에는 이벤트 알림 기능이 포함되어 있습니다. 이 기능을 사용하면 특정 버킷으로 객체가 업로드되거나 삭제되는 등 특정 이벤트가 발생할 때 자동 알림을 보내도록 설정할 수 있습니다. 이러한 알림은 사용자에게 전송되거나, AWS Lambda 스크립트와 같은 다른 프로세스를 트리거하는 데 사용될 수도 있습니다.

스토리지 클래스 분석을 이용하면 스토리지 액세스 패턴을 분석해 올바른 데이터를 올바른 스토리지 클래스로 이전할 수 있습니다. 이 새로운 S3 Analytics 기능은 액세스 빈도가 낮은 스토리지를 Amazon S3 Standard-Infrequent Access (Standard - IA)로 이전할 최적의 수명 주기 정책을 자동으로 식별합니다. 전체 버킷, 접두사 또는 객체 태그를 모니터링하도록 스토리지 클래스 분석 정책을 구성할 수 있습니다. 빈도가 낮은 액세스 패턴이 관찰되면 해당 결과를 바탕으로 손쉽게 새로운 수명 주기 정책을 생성할 수 있습니다. 또한 스토리지 클래스 분석은 AWS Management Console에서 일별 스토리지 사용량을 시각적으로 확인할 수 있습니다. 이 정보를 S3 버킷에 저장하여 Amazon QuickSight와 같은 비즈니스 인텔리전스 도구를 사용해 분석할 수 있습니다.

Amazon S3

aws training and certification



이것이 어떤 문제를 해결하는
데 도움이 되었습니까?

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

그렇다면 이러한 Amazon S3 기능을 사용하여 어떻게 요구 사항을 해결할 수 있을까요?

Amazon S3 사용 사례 1

aws training and certification

정적 웹 콘텐츠와 미디어 저장 및 배포

 [https://\[bucket name\].s3.amazonaws.com](https://[bucket name].s3.amazonaws.com)

 [https://\[bucket name\].s3.amazonaws.com/Video.mp4](https://[bucket name].s3.amazonaws.com/Video.mp4)



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

먼저, Amazon S3를 사용하여 정적 웹 콘텐츠 또는 미디어를 저장하고 배포할 수 있습니다. 이러한 파일은 각 객체가 고유한 HTTP URL에 연결되므로 Amazon S3에서 직접 전송할 수 있습니다. Amazon S3는 콘텐츠 전송 네트워크(예: Amazon CloudFront)의 오리진으로 사용할 수도 있습니다. Amazon S3는 뛰어난 탄력성이 요구되는 빠르게 성장하는 웹 사이트에 효과적입니다. 그 예로는 동영상 또는 사진 공유와 같이 대량의 사용자 생성 콘텐츠가 포함된 워크로드가 있습니다.

Amazon S3 액세스 제어 – 일반

aws training and certification

기본값

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

기본적으로 모든 Amazon S3 리소스, 즉 버킷, 객체 및 관련 하위 리소스(예: 수명 주기 구성 및 웹 사이트 구성)는 비공개입니다. 리소스를 생성한 AWS 계정의 리소스 소유자만 해당 리소스에 액세스할 수 있습니다. 리소스 소유자는 액세스 정책을 작성하여 다른 사람에게 액세스 권한을 부여할 수 있습니다.

모듈 7에서는 AWS Identity and Access Management (IAM)와 액세스 제어 목록(ACL) 및 버킷 정책을 비교합니다. Amazon S3에서의 액세스 제어에 대한 자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-overview.html>

중요

정적 컨텐트를 갖는 S3의 정적 웹 사이트 사용 사례는 AWS 아키텍처를 빠르게 설정할 수 있는 좋은 예이지만, Amazon S3에 대한 퍼블릭 액세스는 일반적인 사용 사례가 아닙니다. **대부분의 사용 사례는 퍼블릭 액세스가 필요하지 않습니다.** 다른 애플리케이션의 데이터를 Amazon S3에 저장하는 경우가 더 많습니다. 이러한 유형의 버킷에는 퍼블릭 액세스를 사용해서는 안 됩니다.

Amazon S3 버킷은 **기본적으로 보호됩니다**. 새로 생성되고 수정되지 않은 버킷에 액세스할 수 있는 것은 계정 관리자와 루트 사용자뿐입니다. 버킷 정책을 수정하면 추가 액세스를 활성화할 수 있으며, AWS는 개발자가 다양한 워크로드용 버킷을 구성할 수 있는 다양한 도구를 제공합니다. Amazon S3에는 실수로 인한 고객 데이터 노출을 방지하기 위해 추가 보호 계층 역할을 하는 “퍼블릭 액세스 차단” 기능이 포함됩니다.

버킷에 대한 퍼블릭 액세스 설정에서 고객은 다음 네 가지 옵션을 지정할 수 있습니다. 기본적으로 모든 옵션이 활성화되어 있습니다.

- 새 퍼블릭 ACL 및 퍼블릭 객체 업로드 차단
- 퍼블릭 ACL을 통해 부여된 퍼블릭 액세스 권한 제거
- 새 퍼블릭 버킷 정책 차단
- 퍼블릭 정책이 있는 버킷에 대한 퍼블릭 액세스 및 교차 계정 액세스 차단

퍼블릭 액세스 설정

정적 퍼블릭 웹 사이트와 같이 퍼블릭 액세스가 필요한 경우에는 이러한 설정을 수동으로 비활성화해야 합니다.

<https://aws.amazon.com/blogs/aws/amazon-s3-block-public-access-another-layer-of-protection-for-your-accounts-and-buckets/>

퍼블릭 및 프라이빗 액세스에 대한 자세한 내용은

<https://youtu.be/x25FSsXrBqU?t=989>(16:29에 시작)를 참조하십시오.

다음 글도 읽어보십시오.

2018년 11월 Jeff Barr의 블로그 게시물

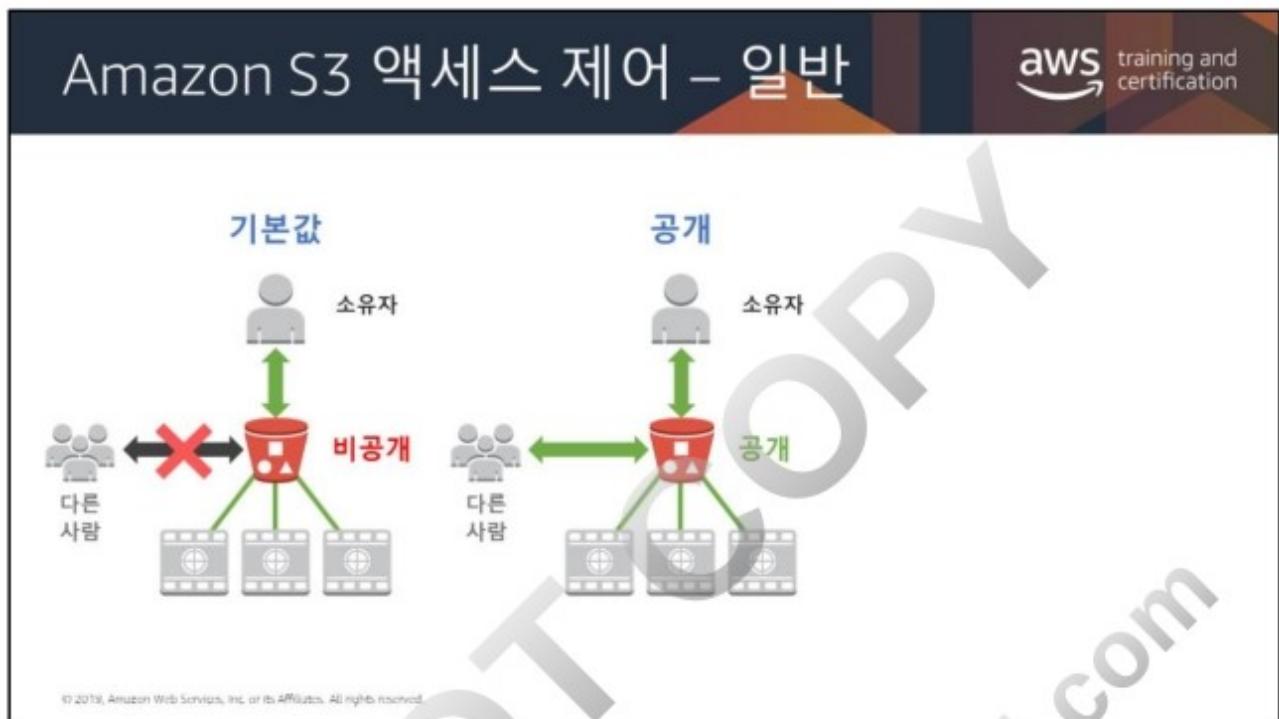
<https://aws.amazon.com/blogs/aws/amazon-s3-block-public-access-another-layer-of-protection-for-your-accounts-and-buckets/>

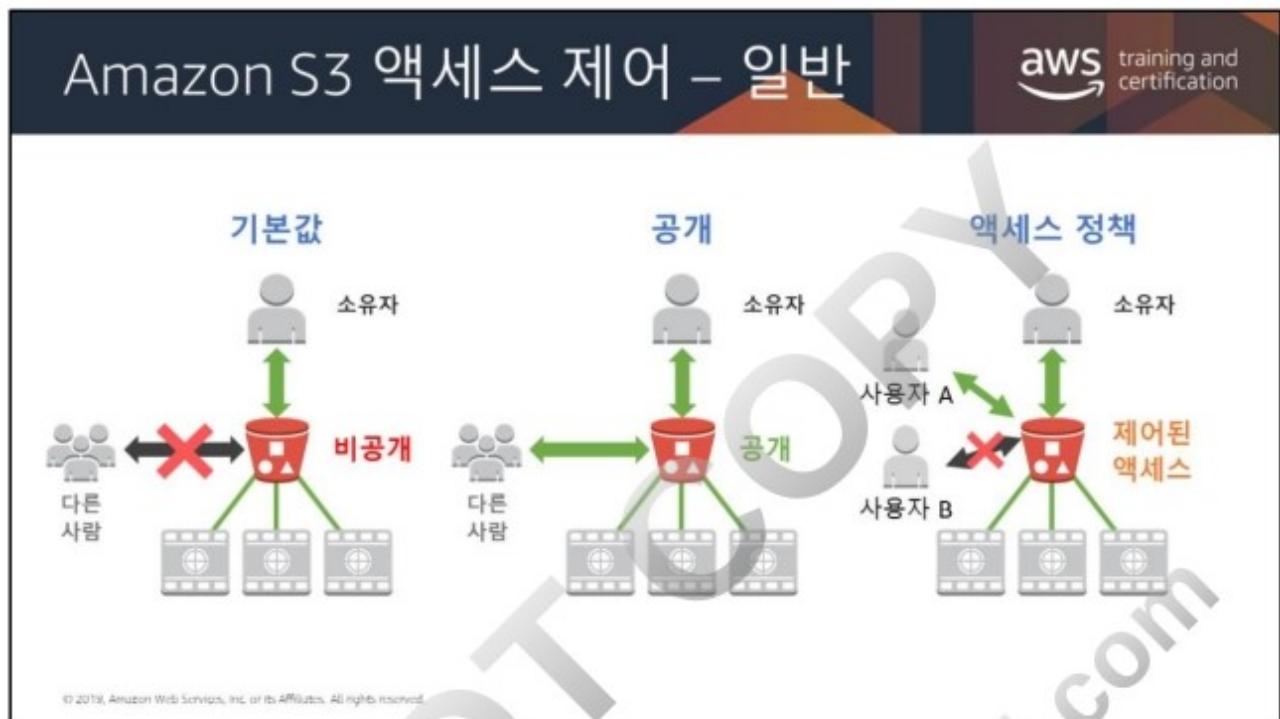
S3 개발자 안내서: Amazon S3 퍼블릭 액세스 차단 사용

<https://docs.aws.amazon.com/AmazonS3/latest/dev/access-control-block-public-access.html>

S3 콘솔 사용 설명서: S3 버킷에 대한 퍼블릭 액세스를 어떻게 차단합니까?

<https://docs.aws.amazon.com/AmazonS3/latest/user-guide/block-public-access.html>





Amazon S3 액세스 제어 – 버킷 정책

The screenshot shows the AWS Policy Generator interface. On the left, there is a red bucket icon with the text "버킷 정책". In the center, a large JSON policy document is displayed:

```
{  
    "Statement": [  
        {  
            "Sid": "Access-to-specific-bucket-only",  
            "Principal": "*",  
            "Action": [  
                "s3:GetObject",  
                "s3:PutObject"  
            ],  
            "Effect": "Allow",  
            "Resource": ["arn:aws:s3:::my_secure_bucket",  
                        "arn:aws:s3:::my_secure_bucket/*"]  
        }  
    ]  
}
```

On the right, the AWS logo and "training and certification" text are visible. A large watermark "DO NOT COPY" and "zlagusdbs@gmail.com" are diagonally across the page.

S3 버킷에서 정책을 추가하여 다른 AWS 계정 또는 사용자에게 그 안에 저장된 객체에 액세스하도록 허용할 수 있습니다. 버킷 정책은 ACL 액세스 정책을 보완하며, 경우에 따라 이를 대체할 수 있습니다.

버킷 정책은 크기가 20KB로 제한됩니다.

Amazon S3 사용 사례 2

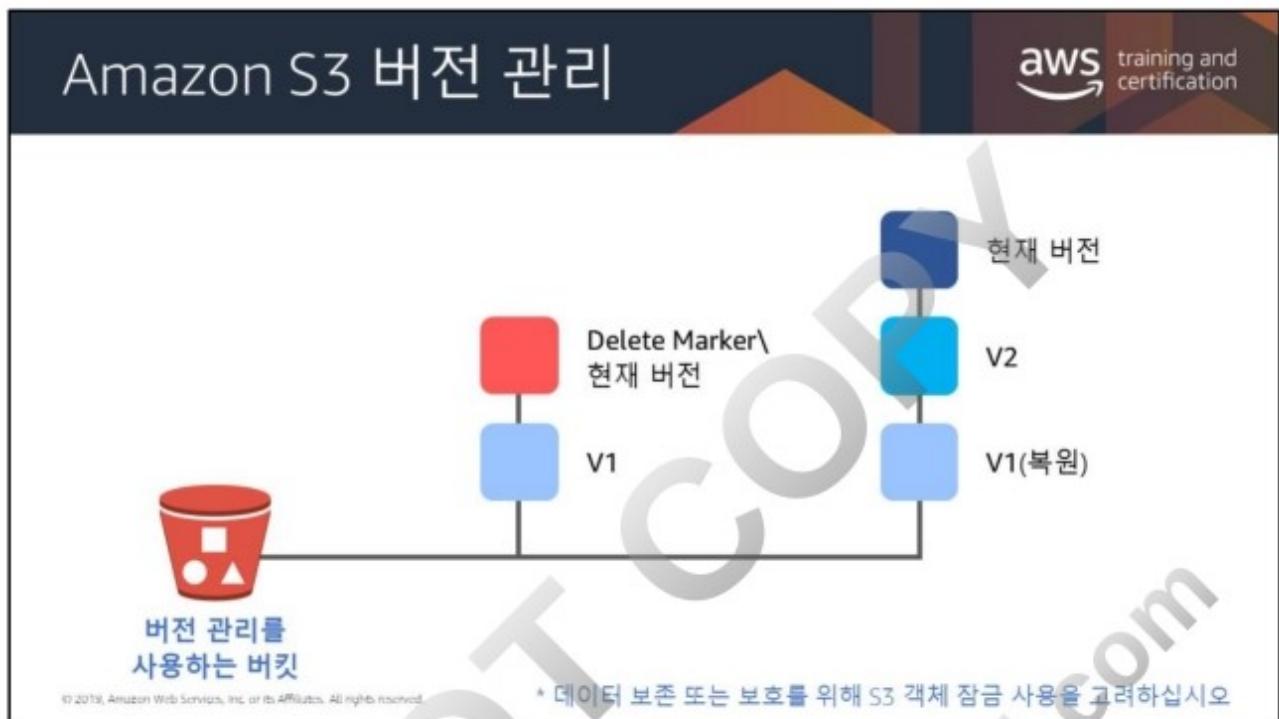
aws training and certification

전체 정적 웹 사이트 호스팅

HTML 파일, 이미지, 동영상 및 클라이언트 측 스크립트

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

Amazon S3를 사용하여 정적 웹 사이트 전체를 호스팅할 수 있습니다. Amazon S3는 정적 HTML 파일, 이미지, 동영상, 클라이언트 측 스크립트(예: JavaScript 형식)를 위한 스토리지를 비롯해 저렴하고 고가용성이며 확장 가능한 솔루션을 제공합니다.



버전 관리 기능의 버킷을 사용하면 실수로 삭제하거나 덮어쓴 객체를 복구할 수 있습니다. 예:

- 객체를 영구적으로 제거하지 않고 삭제하는 경우, Amazon S3는 삭제 마커를 삽입하는데 이것이 객체의 현재 버전이 됩니다. 언제나 이전 버전을 복원할 수 있습니다.
- 객체를 덮어쓴 경우 버킷에 새 객체 버전이 생깁니다. 언제나 이전 버전을 복원할 수 있습니다.

버전 관리에 대한 자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html>

데이터 보존 또는 보호를 위해 S3 객체 잠금을 사용할 수 있습니다. WORM (Write-Once-Read-Many) 모델을 사용하면 S3 스토리지 내에서 실수로 덮어쓰거나 삭제하는 일을 방지할 수 있습니다.

객체를 일정 기간 동안 잠그려면 보존 기간을 사용하고 명시적으로 제거할 때까지 잠그려면 법적 보존을 사용하십시오.

이 기능은 개별 객체 버전에 보존 기간 및 법적 보존이 적용된 버전 관리 버킷에만 적용되며 Amazon S3는 해당 객체 버전에 대한 메타데이터 내에 잠금 정보를 저장합니다. 이 기능이 새 버전 생성을 방지하지는 않습니다. 객체 잠금 기능은 **SEC 17a-4, CTCC, FINRA** 준수에 도움이 됩니다.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lock.html>

DO NOT COPY
zlagusdbs@gmail.com

Amazon S3 액세스 제어 – CORS

```
<CORSConfiguration>
<CORSRule>
<AllowedOrigin>http://www.example.com</AllowedOrigin>
<AllowedMethod>PUT</AllowedMethod>
<AllowedMethod>POST</AllowedMethod>
<AllowedMethod>DELETE</AllowedMethod>
<AllowedHeader>*</AllowedHeader>
<MaxAgeSeconds>3000</MaxAgeSeconds>
<ExposeHeader>x-amz-server-side-encryption</ExposeHeader>
<ExposeHeader>x-amz-request-id</ExposeHeader>
<ExposeHeader>x-amz-id-2</ExposeHeader>
</CORSRule>
</CORSConfiguration>
```

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

CORS (Cross Origin Resource Sharing)는 한 도메인에서 로드되어 있는 클라이언트 웹 애플리케이션이 다른 도메인에 있는 리소스와 상호 작용하는 방법을 정의합니다. CORS 지원을 통해 Amazon S3로 다양한 기능의 클라이언트 측 웹 애플리케이션을 구축하고 개별적으로 Amazon S3 리소스에 대한 교차 오리진 액세스를 허용할 수 있습니다.

버킷을 구성하여 교차 오리진 요청을 허용하려면 CORS 구성, 즉 다음을 식별하는 규칙을 포함하는 XML 문서를 생성합니다.

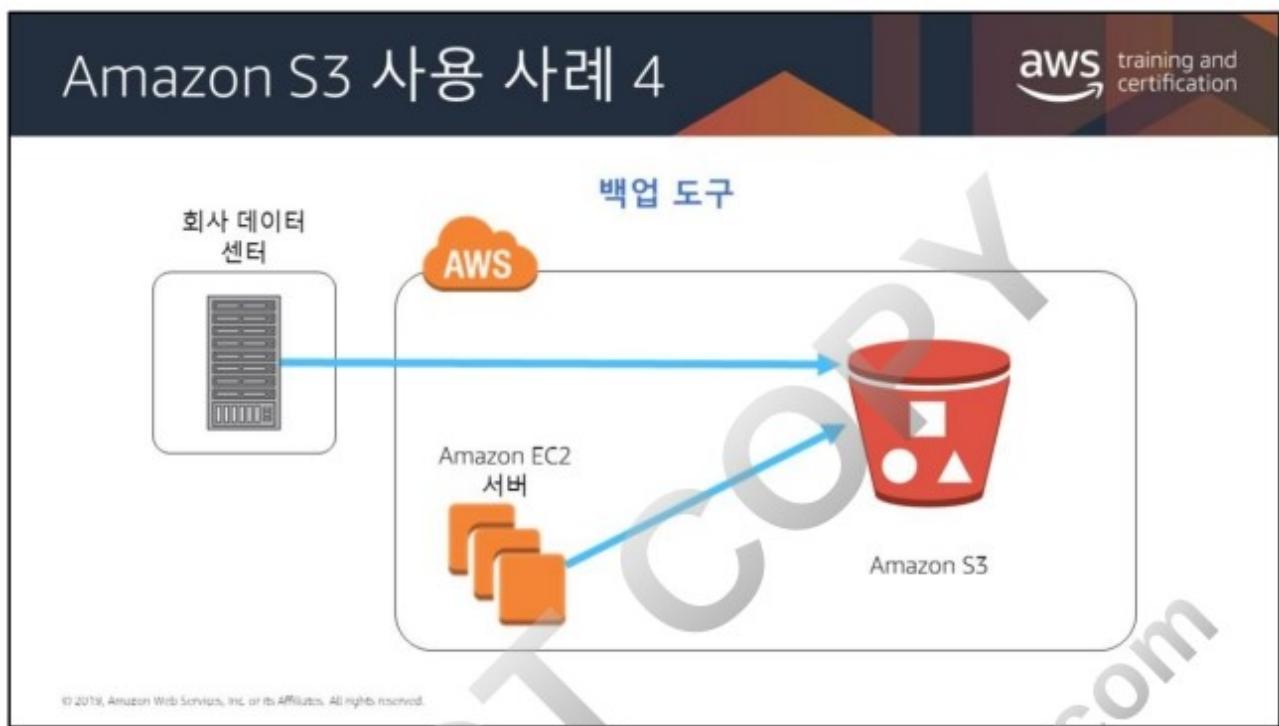
- 버킷에 액세스하도록 허용할 오리진
- 각 오리진에 대해 지원할 작업(HTTP 메서드)
- 기타 작업별 정보

CORS에 대한 자세한 내용은 다음을 참조하십시오.

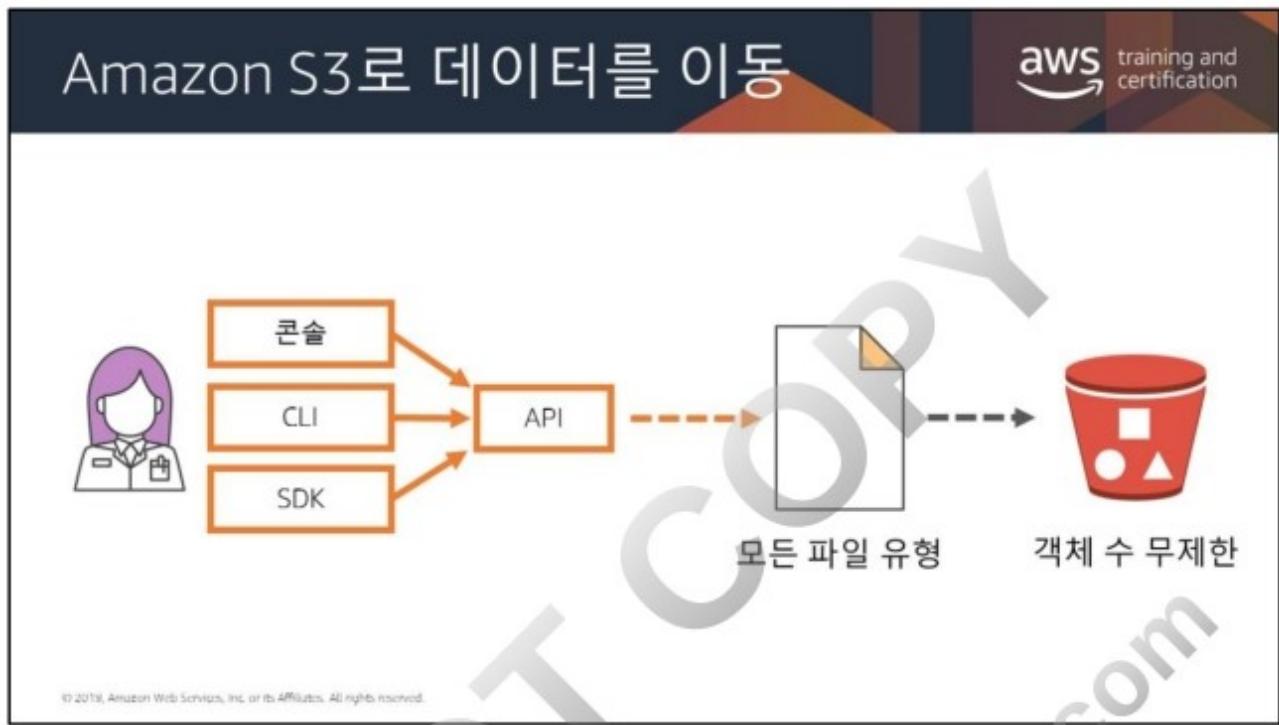
<https://docs.aws.amazon.com/AmazonS3/latest/dev/cors.html>



또한 Amazon S3를 금융 거래 분석, 클릭스트림 분석, 미디어 트랜스코딩 같은 연산 또는 대규모 분석을 위한 데이터 스토어로 사용할 수도 있습니다. 수평 확장성 덕분에 손쉽게 다수의 동시 트랜잭션이 가능하므로 Amazon S3가 이러한 워크로드를 지원할 수 있습니다.



Amazon S3는 뛰어난 내구성 및 확장성을 갖춰 백업 및 아카이브 도구로도 유용합니다. 이밖에도 수명 주기 정책을 사용하여 장기 데이터를 Amazon Glacier로 이전할 수 있습니다. 더 높은 수준의 내구성이 필요할 경우, 교차 리전 복제를 사용하여 객체를 다른 리전에 있는 다른 Amazon S3 버킷에 자동으로 복사할 수 있습니다.



Amazon S3에 업로드한 파일은 S3 객체로 저장됩니다. 객체는 파일 데이터 및 그 객체를 설명하는 메타데이터로 구성됩니다. 한 버킷에 저장할 수 있는 객체 수에는 제한이 없습니다.

몇 가지 방법으로 데이터를 Amazon S3로 이동할 수 있습니다.

- **콘솔, AWS 명령줄 인터페이스(AWS CLI) 또는 API**를 사용하여 전송합니다. 데이터가 소량이거나 이미 AWS 네트워크 내에 있는 경우 콘솔, CLI 또는 API를 사용하여 손쉽게 Amazon S3로 데이터를 전송할 수 있습니다.
- **S3 버킷에 업로드합니다.** 이미지, 백업, 데이터, 동영상 등 모든 파일 형식을 S3 버킷으로 업로드할 수 있습니다. Amazon S3 콘솔을 사용하여 업로드할 수 있는 파일의 최대 크기는 160GB입니다. CLI 또는 API를 사용하면 더 많은 파일을 이동할 수 있습니다.
- **AWS DataSync**는 온프레미스 스토리지와 Amazon S3 또는 Amazon Elastic File System (Amazon EFS) 간의 데이터 이동을 쉽게 자동화할 수 있는 데이터 전송 서비스입니다.
- **AWS Transfer for SFTP**는 완전 관리형 고가용성의 보안 파일 전송 프로토콜인 SFTP 서비스로, 애플리케이션이 SFTP를 통해 Amazon S3로 직접 파일을 전송할 수 있도록 합니다.

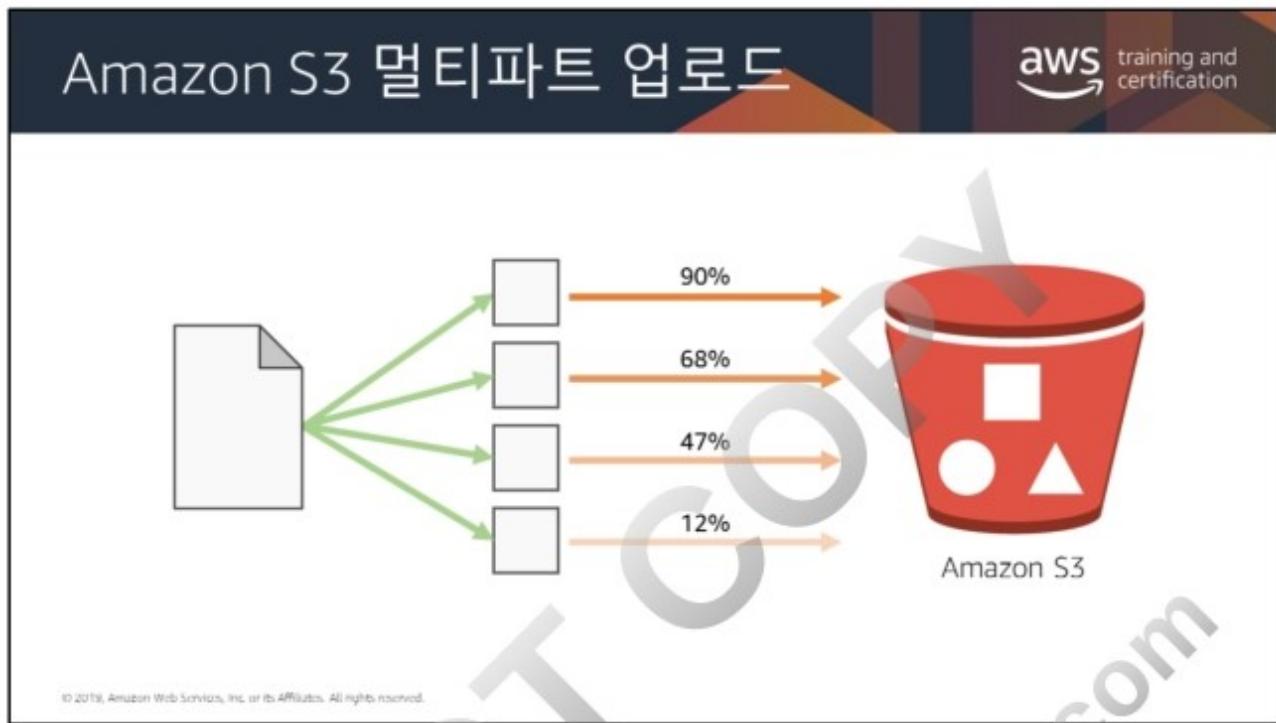
DataSync를 사용하면 오픈 소스 도구보다 최대 10배 빠르게 데이터를 전송할 수 있습니다. 또한 DataSync는 자체 인스턴스 실행, 암호화 처리, 스크립트 관리, 네트워크 최적화, 데이터 무결성 검증 등 마이그레이션 속도를 자연시킬 수 있는 여러 작업을 자동으로 처리합니다.

DataSync는 NFS 프로토콜을 사용한 온프레미스 소프트웨어를 사용하여 기존 스토리지 또는 파일 시스템에 연결하므로 복사한 데이터에 대해서만 비용을 지불하면 됩니다.

<https://aws.amazon.com/datasync/>

AWS Transfer for SFTP는 완전 관리형 고가용성의 보안 파일 전송 프로토콜인 SFTP 서비스로, 애플리케이션이 SFTP를 통해 Amazon S3로 직접 파일을 전송할 수 있도록 합니다. 서버를 생성하고 사용자 계정을 설정하여 하나 이상의 Amazon S3 버킷에 서버를 연결할 수 있습니다. 고객과 파트너는 기존 워크플로의 변경 없이 평소처럼 연결 및 전송할 수 있습니다. 또 다른 장점으로 사용자 자격 증명과 권한 및 키에 대한 제어 기능, 기존 DNS 이름과 SSH 퍼블릭 키를 사용한 AWS Transfer for SFTP로의 마이그레이션, 파일 처리 및 쿼리를 위한 "지능형" FTP 사이트를 구축하는 AWS Lambda 함수 작성 등이 있습니다.

<https://aws.amazon.com/blogs/aws/new-aws-transfer-for-sftp-fully-managed-sftp-service-for-amazon-s3/>



멀티파트 업로드를 사용하면 대용량 객체를 관리 가능한 파트로 분할하여 일관되게 업로드할 수 있습니다. 이 프로세스는 세 단계로 이루어집니다.

- 업로드 시작
- 객체 파트 업로드
- 멀티파트 업로드 완료

멀티파트 업로드 요청이 완료되면, Amazon S3가 개별 조각으로부터 전체 객체를 다시 생성합니다.

이 방법의 이점은 다음과 같습니다.

개선된 처리량: 파트를 병렬로 업로드하여 처리량을 개선할 수 있습니다.

네트워크 문제로부터 빠른 복구: 더 작은 파트 크기가 네트워크 오류로 인해 실패한 업로드의 재시작 시 영향을 최소화합니다.

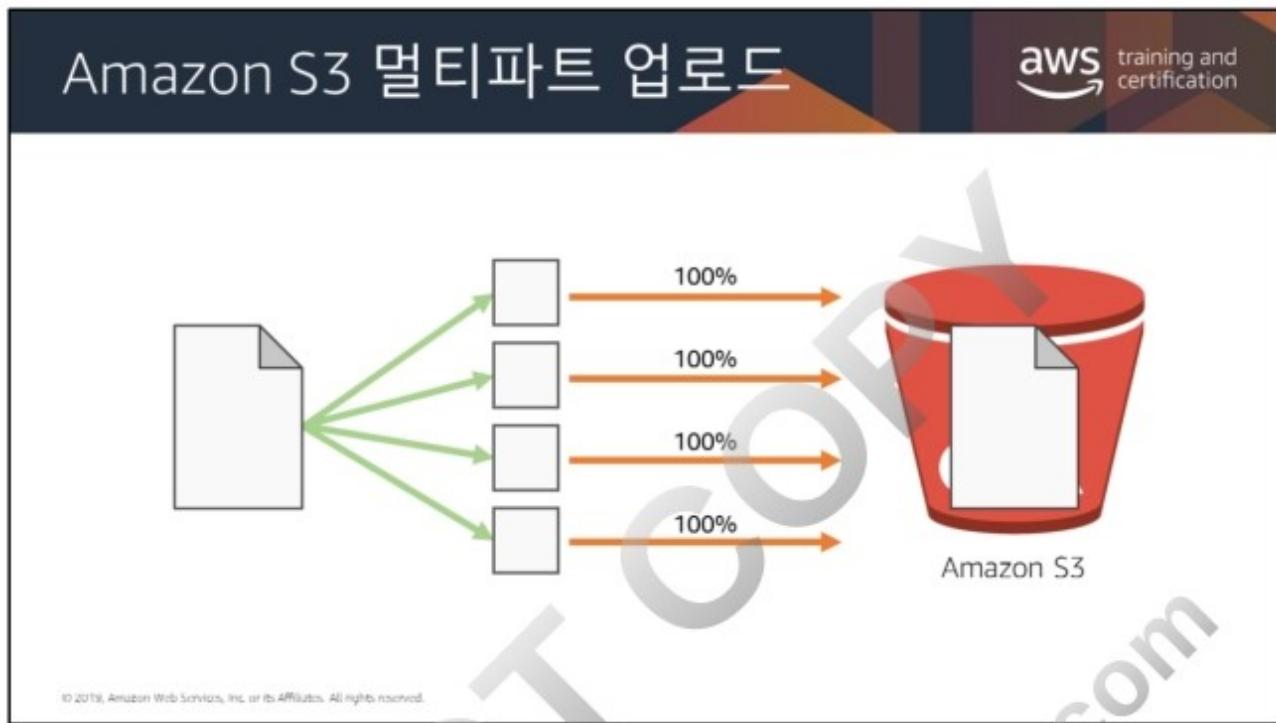
객체 업로드 일시 중지 및 재개: 객체 파트를 장시간에 걸쳐 업로드할 수 있습니다. 일단 멀티파트 업로드가 시작되면 제한 시간이 없습니다. 멀티파트 업로드를 명시적으로 완료하거나 중단해야 합니다.

최종 객체 크기를 알기 전에 업로드를 시작: 객체를 생성하는 동안 업로드할 수 있습니다.

대용량 객체를 업로드: 멀티파트 업로드 API를 사용하여 최대 5TB의 대용량 객체를 업로드할 수 있습니다.

멀티파트 업로드에 대한 자세한 내용은

<https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html>를
참조하십시오.



멀티파트 업로드를 사용하면 대용량 객체를 관리 가능한 파트로 분할하여 일관되게 업로드할 수 있습니다. 이 프로세스는 세 단계로 이루어집니다. 즉, 업로드를 시작하고, 객체 파트를 업로드하고, 모든 파트를 업로드한 후 멀티파트 업로드를 완료합니다. 멀티파트 업로드 요청이 완료되면, Amazon S3가 개별 조각으로 부터 전체 객체를 다시 생성합니다.

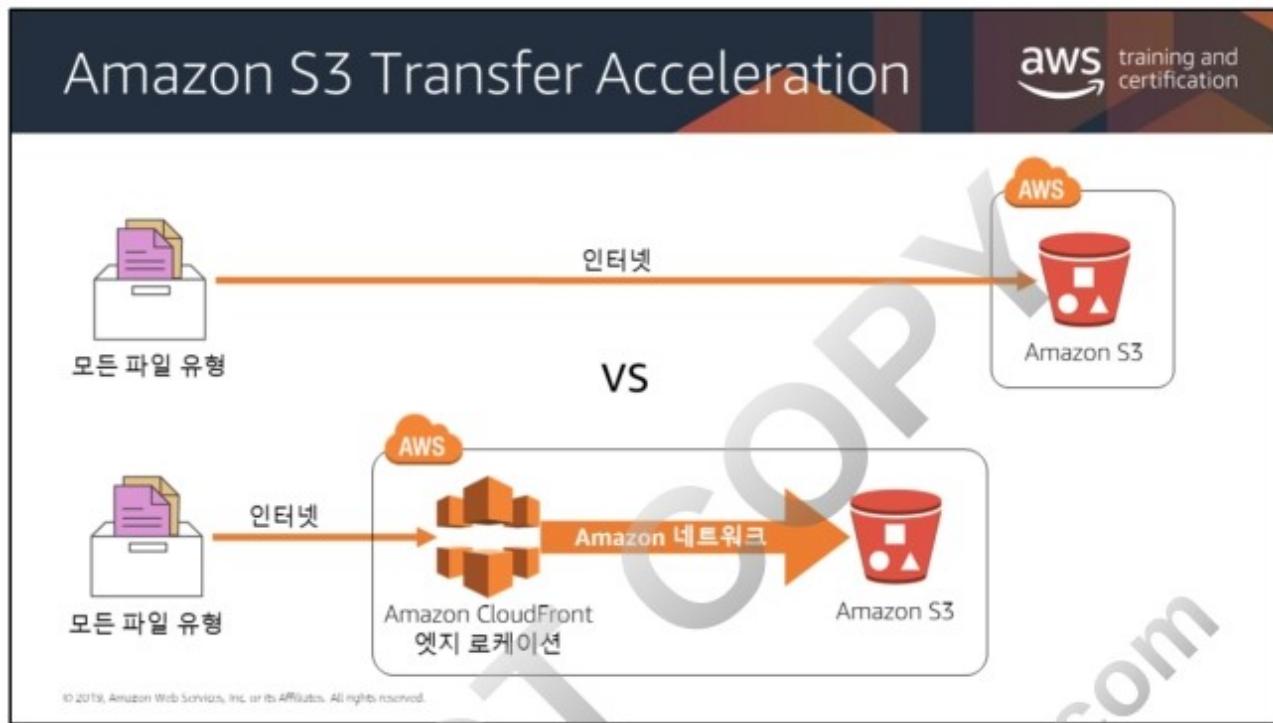
개선된 처리량 - 파트를 병렬로 업로드하여 처리량을 개선할 수 있습니다.
네트워크 문제로부터 빠른 복구 - 더 작은 파트 크기가 네트워크 오류로 인해 실패한 업로드의 재시작 시 영향을 최소화합니다.

객체 업로드 일시 중지 및 재개 - 객체 파트를 장시간에 걸쳐 업로드할 수 있습니다. 일단 멀티파트 업로드가 시작되면 제한 시간이 없습니다.
멀티파트 업로드를 명시적으로 완료하거나 중단해야 합니다.

최종 객체 크기를 알기 전에 업로드를 시작 - 객체를 생성하는 동안 업로드할 수 있습니다.

멀티파트 업로드 API를 사용하여 최대 5TB의 대용량 객체를 업로드할 수 있습니다.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/mpuoverview.html>



Amazon S3 Transfer Acceleration은 전 세계에 분산된 Amazon CloudFront의 엣지 로케이션을 통해 S3 버킷으로 빠르고 간편하게 데이터를 전송할 수 있도록 해줍니다. 이 데이터는 최적화된 네트워크 경로를 통해 Amazon S3로 라우팅됩니다.

다음과 같은 경우 Transfer Acceleration을 사용합니다.

- 전 세계 각지에서 중앙의 버킷으로 업로드하는 고객이 있는 경우
- 전 세계에서 정기적으로 기가바이트 또는 테라바이트 규모의 데이터를 전송하는 경우
- 인터넷을 통해 Amazon S3로 업로드할 때 사용 가능한 대역폭을 충분히 활용하지 못하는 경우

Amazon S3로 데이터를 이동

aws training and certification

AWS Snowball

페타바이트 규모의 데이터 전송



AWS Snowmobile

엑사바이트 규모의 데이터 전송



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

AWS Snowball은 데이터 전송을 위해 코드를 작성하거나 하드웨어를 구매할 필요가 없는 페타바이트 규모의 데이터 전송 옵션입니다. AWS Management Console에서 작업을 생성하기만 하면 Snowball 어플라이언스가 고객에게 배송됩니다. 어플라이언스를 로컬 네트워크에 연결하고 파일을 어플라이언스로 직접 전송합니다. 작업이 완료되면 전자 잉크 배송 레이블이 자동으로 업데이트되어 Amazon Simple Notification Service (Amazon SNS) 또는 콘솔을 통해 추적될 수 있습니다. 그런 다음 Snowball이 안전한 Amazon 시설로 회수되어 네트워크로 전송됩니다.

AWS Snowball Edge Optimized는 원격의 외진 환경 또는 네트워크 연결이 끊기거나 열악한 환경에서 추가 컴퓨팅 파워가 필요한 엣지 처리 사용 사례에 적합합니다. 이 서비스는 52개의 vCPU, 208GB의 메모리, 7.68TB의 NVMe SSD, 42TB의 S3 호환 스토리지를 제공합니다. 연결이 끊긴 환경에서 고급 기계 학습 및 풀 모션 비디오 분석을 하는 경우 흔히 사용됩니다.

Snowball에 대한 자세한 내용은 <https://aws.amazon.com/snowball/>을 참조하십시오.

<https://aws.amazon.com/snowball-edge/>

AWS Snowmobile은 엑사바이트 규모에서 사용하는 훨씬 대규모의 데이터 전송 옵션입니다. 이 서비스는 막대한 양의 데이터를 AWS로 이전할 때만 사용해야 합니다. Snowmobile은 세미 트레일러 트럭으로 견인되는 45피트 길이의 견고한 운반 컨테이너입니다. Snowmobile 1개로 100PB를 운반할 수 있습니다.

Snowmobile은 운반 중에 보안 전담 인력, GPS 추적, 경보 모니터링, 24/7 비디오 감시, 경호 차량(선택 사항) 등 데이터 보호를 위해 설계된 다중 보안 계층을 사용합니다. 모든 데이터는 AWS Key Management Service(AWS KMS)를 통해 관리되고 데이터 보안 및 완전한 연계보관성(chain of custody)을 보장하도록 설계된 256비트 암호화 키로 암호화됩니다.

Snowmobile에 대한 자세한 내용은 <https://aws.amazon.com/snowmobile/> 단원을 참조하십시오.

Amazon S3는 언제 사용해야 합니까?

aws training and certification



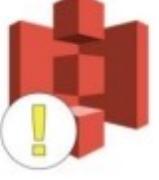
모범 사용 사례

- 한 번 쓰고 여러 번 읽어야 하는 경우
- 데이터 액세스가 일시적으로 급증
- 사용자가 매우 많고 콘텐츠 양이 다양
- 데이터 세트가 계속 증가

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

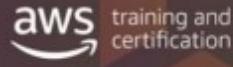
Amazon S3는 언제 사용해야 합니까?

aws training and certification

모범 사용 사례	이상적인 사용 사례가 아닌 경우
 한 번 쓰고 여러 번 읽어야 하는 경우 데이터 액세스가 일시적으로 급증 사용자가 매우 많고 콘텐츠 양이 다양 데이터 세트가 계속 증가	 블록 스토리지 요구 사항 자주 바뀌는 데이터 장기 아카이브 스토리지

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

Amazon S3 비용



다음에 대해 사용한 만큼만
지불

월별 GB

다른 리전 또는 인터넷으로
전송

PUT, COPY, POST, LIST 및 GET
요청



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

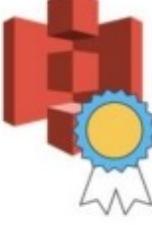
세부적인 비용은 리전과 수행된 특정 요청에 따라 달라질 수 있습니다.
일반적으로 리전 경계를 넘어가는 전송에 대한 비용만 지불합니다. 다시 말해
같은 리전 내에 있는 Amazon CloudFront 엣지 로케이션으로 전송된 데이터에는
비용이 부과되지 않습니다.

Amazon S3 비용

aws training and certification

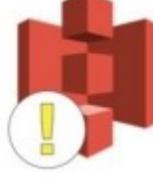
**다음에 대해 사용한 만큼만
지불**

월별 GB
다른 리전 또는 인터넷으로
전송
PUT, COPY, POST, LIST 및 GET
요청

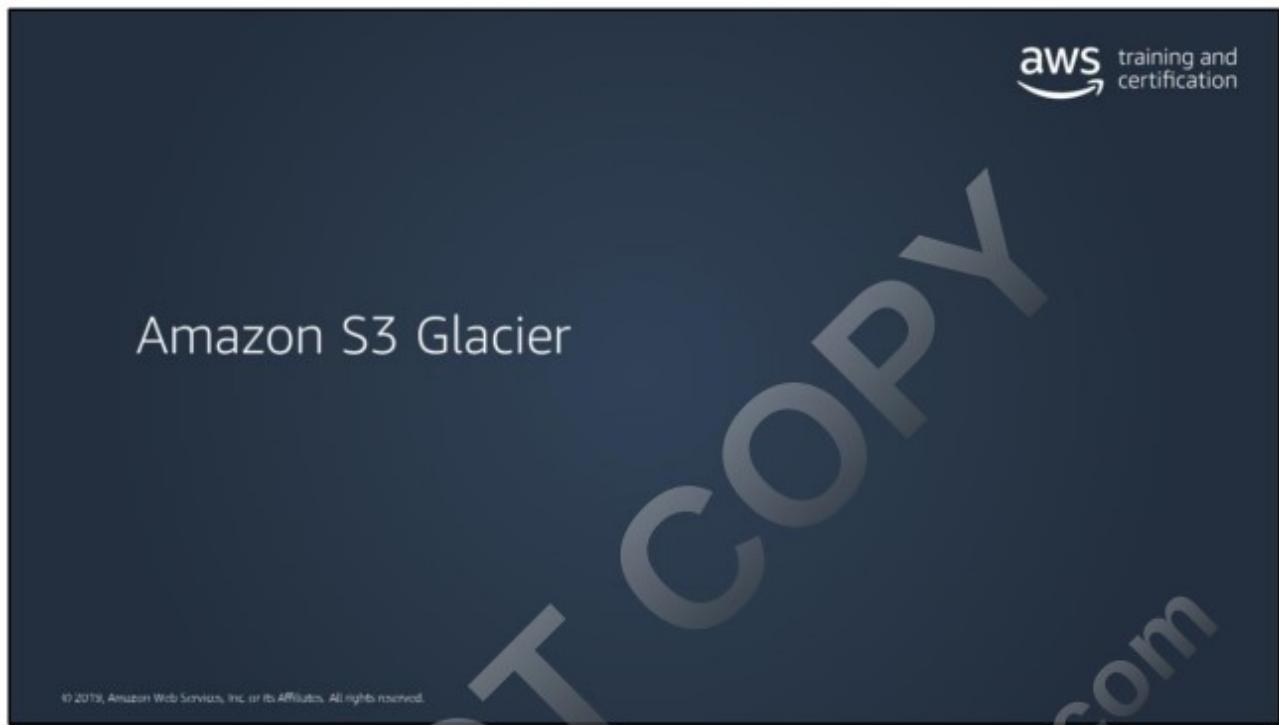


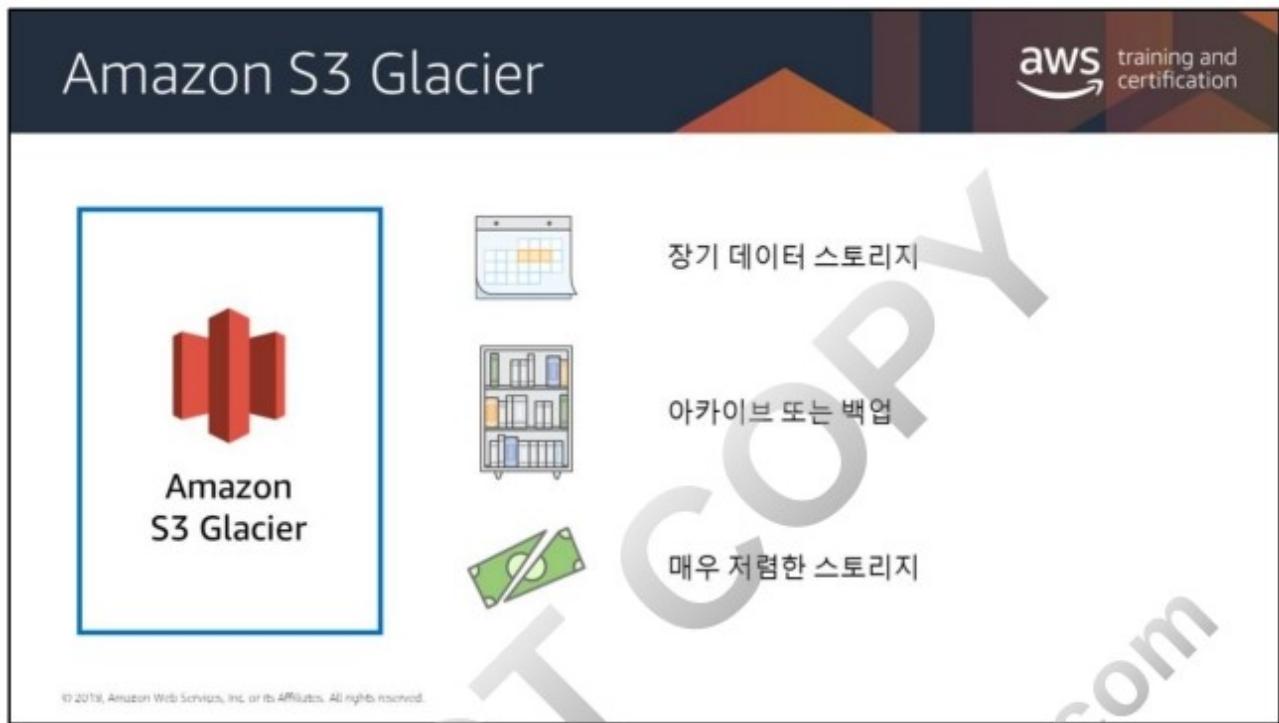
**다음에 대해서는
비용을 지불할 필요가 없음**

Amazon S3로 수신
동일한 리전 내 Amazon EC2로
또는 CloudFront로 전송



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





Amazon S3 Glacier는 저렴한 스토리지 비용이 가장 중요하고, 데이터를 검색하는 일이 거의 없으며, 몇 시간 정도의 검색 지연 시간이 허용될 때 선택할 수 있는 훌륭한 스토리지입니다. 애플리케이션에 빠르거나 빈번한 데이터 액세스가 필요하다면 Amazon S3를 사용하는 것이 좋습니다.

Amazon S3 Glacier의 데이터 아카이브를 사용하면 매우 저렴한 비용(Amazon S3와 비교해서도 매우 저렴)으로 데이터를 저장할 수 있지만, 필요할 때 데이터를 즉시 검색할 수는 없습니다. Amazon S3 Glacier에 저장된 데이터는 검색하는 데 몇 시간이 걸리며, 이 점이 바로 보관에 적합한 이유입니다.

다양한 액세스 시간과 비용으로 데이터를 검색할 수 있는 3가지 옵션이 제공됩니다.

- **신속** 검색은 보통 1~5분 이내에 완료됩니다.
- **표준** 검색은 보통 3~5시간 이내에 완료됩니다.
- **대량** 검색은 보통 5~12시간 이내에 완료됩니다.

몇 가지 추가 세부 정보:

- Amazon Glacier는 **보안, 내구성 및 매우 저렴한 비용**을 제공하도록 설계된 **데이터 아카이브 서비스**입니다.
- 99.99999999%의 객체 내구성을 제공하도록 설계되었습니다.
- 전송 시 데이터 및 저장 시 데이터의 SSL/TLS 암호화를 지원합니다.
- 저장소 잠금 기능은 잠금 가능한 정책을 통해 규정 준수를 강화합니다.
- 매우 저렴한 비용의 설계는 장기 아카이브에 적합합니다.



아카이브는 사진, 동영상, 문서 등 저장소에 저장한 모든 객체입니다. 또한 Amazon S3 Glacier 내 스토리지의 기본 단위입니다. 각 아카이브는 고유 ID가 있으며 선택 사항으로 설명을 추가할 수 있습니다. 아카이브를 업로드하면 Amazon S3 Glacier가 아카이브 ID가 포함된 응답을 반환합니다. 이 아카이브 ID는 아카이브가 저장된 리전에서 고유합니다.

Amazon S3 Glacier는 관리 콘솔을 제공합니다. 이 콘솔에서 저장소를 생성하거나 삭제할 수 있습니다. 하지만 다른 모든 Amazon S3 Glacier 작업에서는 CLI를 사용하거나 코드를 작성해야 합니다. 예를 들어 사진, 동영상 및 기타 문서 같은 데이터를 업로드하려면 AWS CLI를 사용하거나, 혹은 REST API를 직접 사용하거나 AWS SDK를 사용하여 요청 코드를 작성해야 합니다.

저장소는 아카이브를 저장할 수 있는 컨테이너입니다. 저장소를 생성할 때 저장소 이름과 저장소를 생성할 AWS 리전을 지정해야 합니다.

저장소 잠금 기능은 잠금 가능한 정책을 통해 규정 준수를 강화합니다.

The diagram shows three categories of search types:

- 신속 검색** (Fast Search): Represented by a large yellow box.
- 표준 검색** (Standard Search): Represented by a smaller grey filing cabinet.
- 대량 검색** (Large Volume Search): Represented by a larger grey filing cabinet.

A large watermark reading "COPY" is overlaid across the center of the diagram.

검색 옵션을 사용하여 필요한 모든 아카이브에 필요한 시점에 간편하고 저렴한 가격으로 액세스할 수 있습니다.

- **신속 검색**을 사용하여 1GB당 0.03 USD의 고정 요율로 1~5분 이내에 데이터에 액세스할 수 있습니다. 신속 검색을 사용하면 아카이브 하위 집합을 긴급하게 사용해야 하는 경우 데이터에 신속하게 액세스할 수 있습니다.
 - 페타바이트 규모의 대용량 데이터를 검색해야 할 경우, **대량 검색**을 사용하여 1GB당 0.0025 USD의 저렴한 고정 요율로 약 5~12시간 이내에 데이터에 액세스할 수 있습니다. 대량 검색을 사용하면 효과적인 비용으로 빅 데이터 분석, 미디어 트랜스코딩 같은 작업을 위한 막대한 양의 데이터에 액세스할 수 있습니다.



다음은 Amazon S3 스토리지 클래스 비교를 위한 설명입니다.

범용: Amazon S3 Standard

가용성 요구 사항이 더 높은 경우: 교차 리전 복제를 사용

액세스 빈도가 낮은 데이터: Amazon S3 Standard - Infrequent Access

저장된 GB당 비용이 저렴

PUT, COPY, POST 또는 GET 요청당 비용이 높음

최소 30일 스토리지

자주는 아니지만 빠른 액세스: Amazon S3 One Zone-Infrequent Access

단일 가용 영역

S3 Standard – Infrequent Access보다 20% 저렴

스토리지 클래스 분석

표준 데이터와 같이 즉시 액세스할 수 있어야 하지만 자주 요청되지 않을 것으로 예상하는 데이터를 저장할 수 있도록 AWS에서는 Amazon S3 Standard – IA (Infrequent Access)를 제공합니다.

Amazon S3 Standard – IA는 안정성, 가용성, 보안을 비롯한 Amazon S3의 모든 이점을 제공하며, 사용자의 오래된 디지털 이미지나 오래된 로그 파일과 같이 자주 액세스하지 않는 데이터 저장을 위한 다른 비용 모델의 솔루션을 제공합니다.

Amazon S3 One Zone-IA는 액세스 빈도가 낮지만 필요할 때 빠르게 액세스해야 하는 중요하지 않은 데이터를 위한 Amazon S3 스토리지 클래스입니다. 최소 3개의 가용 영역에 데이터를 저장하는 다른 Amazon 객체 스토리지 클래스와는 달리 S3 One Zone-IA는 단일 가용 영역에 데이터를 저장합니다. 따라서 S3 One Zone-IA에서 데이터를 저장하는 비용은 S3 Standard – IA를 사용한 데이터 저장보다 20% 저렴합니다.

Amazon S3 분석 스토리지 클래스 분석을 이용하면 스토리지 액세스 패턴을 분석해 올바른 데이터를 올바른 스토리지 클래스로 옮길 시간을 결정할 수 있습니다. 이 새로운 Amazon S3 분석 기능은 데이터 액세스 패턴을 관찰해 자주 액세스하지 않는 STANDARD 스토리지를 STANDARD_IA(IA는 자주 액세스하지 않는다는 의미) 스토리지 클래스로 옮길 시점을 알려줍니다.

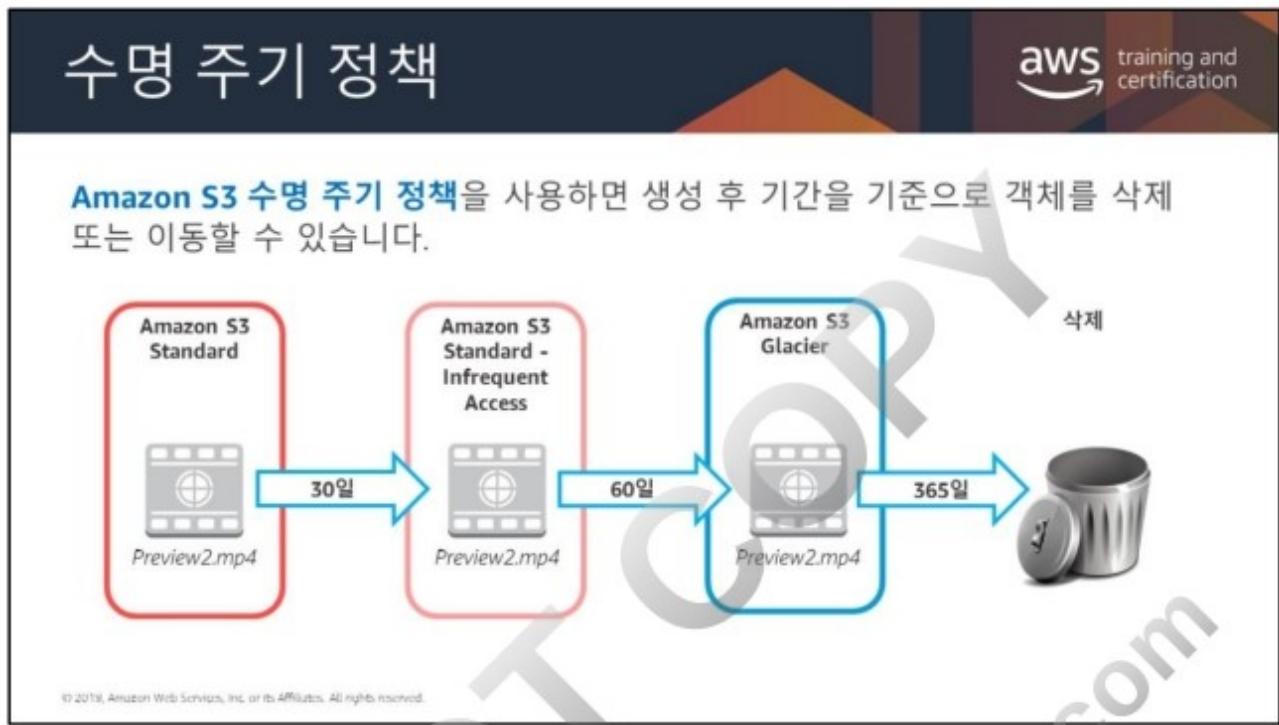
Amazon S3 스토리지 클래스에 대한 자세한 내용은 <https://aws.amazon.com/s3/storage-classes/>를 참조하십시오.

Amazon S3 인텔리전트 티어링은 액세스 패턴이 변경되면 두 개의 스토리지 액세스 티어 간에 객체를 자동으로 이동하여 스토리지 비용을 최적화할 수 있는 Amazon Simple Storage Service(Amazon S3)를 위한 스토리지 클래스입니다. Amazon S3 인텔리전트 티어링은 알 수 없거나 변화하는 액세스 패턴이 한 달 이상 유지되는 액세스 스토리지에 이상적입니다. 예를 들어 새로 시작한 애플리케이션 및 데이터 레이크의 경우, 스토리지의 하위 집합마다 액세스 패턴이 다를 수 있습니다.

Amazon S3 인텔리전트 티어링은 객체가 저장된 S3 티어에 상관없이 동일한 밀리초 단위의 지연 시간 및 99% 가용성 SLA를 제공합니다. Amazon S3 인텔리전트 티어링은 자동으로 스토리지 비용을 최적화하기 때문에 액세스 빈도가 낮은 스토리지의 비용을 절감하기 위해 스토리지 액세스 패턴을 분석 또는 감사할 필요가 없습니다.

S3 Glacier Deep Archive는 데이터의 내구성과 장기 보존을 위한 사용자에게 적합한 가장 저렴한 스토리지 티어입니다. 이러한 스토리지 유형은 거의 또는 전혀 액세스할 필요가 없는 데이터의 내구성 높은 사본을 보관해야 하는 고객에게 적합합니다. 또한 고객이 온프레미스 테이프 라이브러리를 만들 필요가 없어집니다. 12시간 이내에 검색할 수 있습니다.

<https://aws.amazon.com/about-aws/whats-new/2018/11/s3-glacier-deep-archive/>



Amazon S3에 저장된 데이터의 수명 주기를 자동화해야 합니다. 수명 주기 정책을 사용하면 다양한 Amazon S3 스토리지 유형 간에 데이터가 주기적으로 순환되도록 할 수 있습니다.

이를 통해 시간이 지나면서 데이터의 중요도가 감소하면 비용을 더 적게 지불함으로써 전체 비용을 줄일 수 있습니다.

객체별로 수명 주기 규칙을 설정할 수 있을 뿐 아니라 버킷별로 수명 주기 규칙을 설정할 수도 있습니다.

자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html>



리전 선택

aws training and certification

데이터 주권 및 규정 준수

관련된 지역 데이터
프라이버시 법률이
있습니까?

고객 데이터를
해외에 저장할 수
있습니까?

거버넌스 의무를
준수할 수 있습니까?

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

데이터는 데이터가 저장되는 국가 및 지역 법의 적용을 받습니다. 또한 일부 법에서는 해당 관할권에서 사업을 운영하는 경우, 다른 곳에 데이터를 저장하지 못하도록 규정하고 있습니다. 마찬가지로 규정 준수 표준(미국 건강 보험 양도 및 책임에 관한 법(HIPAA) 등)은 데이터를 어디에 어떻게 저장해야 하는지에 대한 엄격한 지침을 제시합니다. 또한 AWS는 2011년에 첫 번째 탄소 중립 리전을 공개했고, 현재 5개의 탄소 중립 리전을 제공하고 있습니다.

환경을 배치할 장소를 평가할 때는 이 모든 것을 고려해야 합니다.

탄소 중립 옵션에 대한 자세한 내용은 다음을 참조하십시오.
<https://aws.amazon.com/about-aws/sustainability/>

리전 선택

aws training and certification

사용자와 데이터 간 근접성

지연 시간의 작은 차이가 고객 경험에 영향을 미칠 수 있습니다.

사용자에게 가장 가까운 리전을 선택하십시오.

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

근접성은 리전을 선택할 때 고려해야 할 중대한 요소입니다. 특히 지연 시간이 매우 중요한 경우에는 더욱 그렇습니다. 대부분의 경우, 가장 가까운 리전과 가장 먼 리전 간의 지연 시간의 차이는 상대적으로 작습니다. 하지만 지연 시간의 작은 차이가 고객 경험에 영향을 줄 수 있습니다. 고객은 즉각적으로 응답하는 환경을 기대하며, 시간이 지나고 기술이 더 강력해질수록 그러한 기대도 함께 상승합니다.

리전 선택

aws training and certification

서비스 및 기능 가용성

일부 서비스는 아직 모든 리전에서 제공되지는 않습니다.

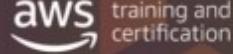
일부 서비스는 교차 리전으로 사용할 수 있지만 지역 시간이 증가합니다.

정기적으로 서비스를 새 리전으로 확장하고 있습니다.

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

AWS에서는 모든 리전에서 서비스와 기능을 제공하기 위해 최선을 다하지만, 글로벌 접근성을 제공함에 따라 발생하는 복잡한 문제는 이러한 목표 달성을 매우 어렵게 합니다. AWS는 서비스를 모든 리전에서 제공할 수 있을 때까지 기다렸다가 출시하지 않고, 서비스가 준비되면 먼저 릴리스하고 가능한 한 빠르게 제공 리전을 확장합니다.

리전 선택



비용 효율성

- 비용은 리전별로 다릅니다.
- Amazon S3와 같은 일부 서비스는 데이터를 외부로 전송할 때 비용이 발생합니다.
- 전체 환경을 다른 리전으로 복제하는 비용 효율성을 고려하십시오.



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

서비스 비용은 서비스가 사용되는 리전에 따라 달라질 수 있습니다. 예를 들어 US-East 1의 Amazon EC2 인스턴스 비용과 EU-West 1에서 실행되는 인스턴스의 비용이 다를 수 있습니다. 일반적으로 비용 차이는 다른 3가지 고려 사항을 대신할 만큼 크지 않을 수 있습니다. 하지만 리전 간의 자연 시간/규정 준수/서비스 가용성 차이가 미미한 경우, 더 저렴한 리전을 환경에 사용함으로써 비용을 절감할 수도 있습니다.

고객이 전 세계 여러 곳에 있는 경우, 고객에게 가까운 여러 리전에 환경을 복제함으로써 고객 경험을 최적화하는 방법을 고려해보십시오. 그러면 여러 환경에 로드를 분산하게 되므로, 인프라를 추가함에 따라 각 환경의 구성 요소 비용이 낮아질 수 있습니다. 예를 들어 두 번째 애플리케이션 환경을 추가하면 각 환경의 처리 및 스토리지 용량 요구 사항을 절반으로 줄일 수 있습니다. AWS는 사용자에게 이러한 유연성을 제공하도록 설계되었고, 사용자는 사용한 만큼만 비용을 지불하므로, 다른 환경을 추가하는 비용을 경감하는 방법으로 기존 환경을 손쉽게 축소할 수 있습니다.

이러한 접근 방식의 단점은 이제 2개의 환경을 관리해야 하고, 새로운 구성 요소 비용을 모두 경감하기에 충분할 만큼 기존 구성 요소를 모두 축소할 수는 없다는 것입니다. 또한, 한 리전에 "진짜 원본"이 있는 단일 스토리지(예: 마스터 RDS 인스턴스)를 유지해야 하고, 두 번째 리전은 이와 통신해야 하기 때문에 이 과정에서 자연 시간 및 비용이 증가할 수 있습니다.

DO NOT COPY
zlagusdbs@gmail.com



실습 1: 정적 웹 사이트 호스팅



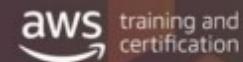
"가용성이 뛰어난 정적 웹 사이트를 만들고 싶습니다"

사용된 기술:

- Amazon S3

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

실습 1: 정적 웹 사이트 호스팅



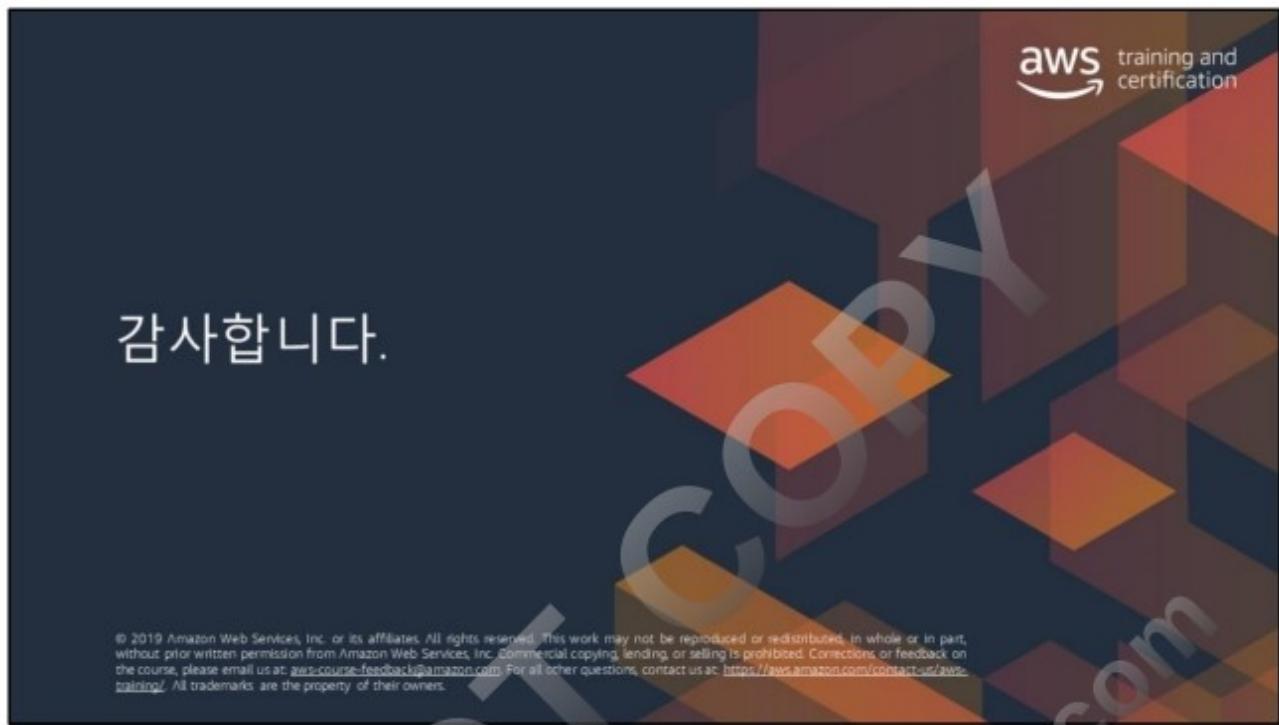
다음을 수행합니다.

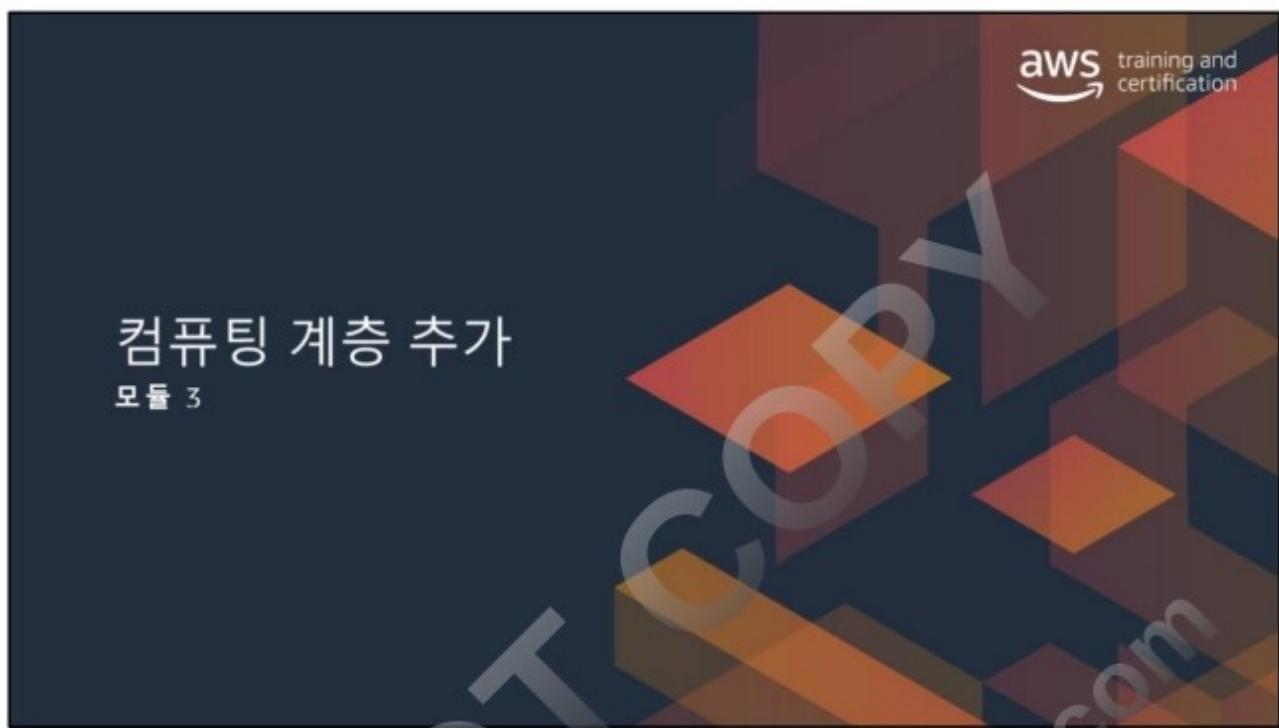
- S3 버킷 생성
- 웹 사이트 배포
- 공개적으로 사용 가능한 사이트 구축



소요 시간: 20분

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







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

모듈 3

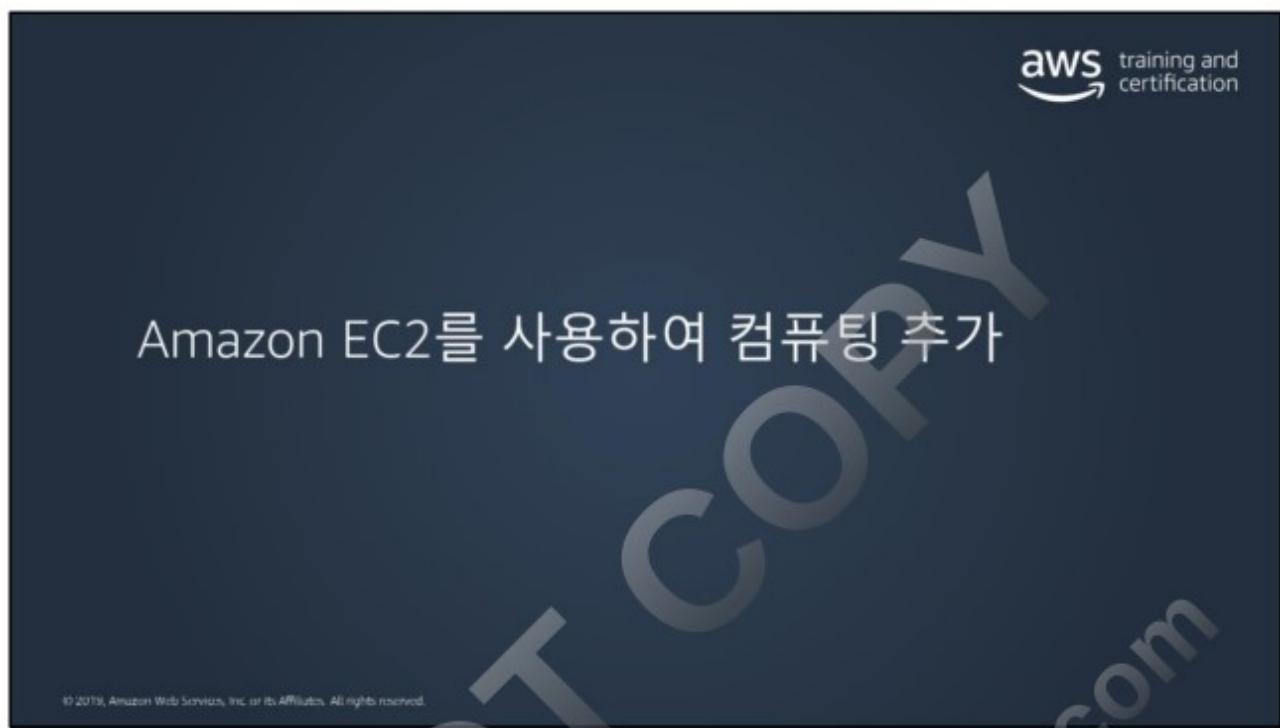
아키텍처 측면에서의 필요성

작은 수의 일관된 사용자가 사용할 애플리케이션을 실행해야 합니다.

모듈 개요

- Amazon Elastic Compute Cloud (EC2)
- 인스턴스 유형 및 패밀리
- Amazon Elastic Block Store (Amazon EBS) 볼륨
- 규정 준수 옵션

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



Amazon EC2는 어떤 필요를 해결할 수 있습니까?



The slide features the Amazon EC2 logo, which consists of three orange 3D cubes stacked vertically, enclosed in a thin orange square border. Below the logo, the text "Amazon EC2" is written in a black sans-serif font.

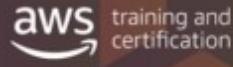
aws training and certification

- 웹 호스팅
- 데이터베이스
- 인증
- 서버가 처리할 수 있는 모든 것

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

Amazon EC2는 기존의 온프레미스 서버와 똑같지만 클라우드에서 사용할 수 있습니다. 웹 호스팅, 애플리케이션, 데이터베이스, 인증 서비스를 비롯해 서버가 수행할 수 있는 모든 워크로드를 지원할 수 있습니다.

가상 머신과 물리적 서버

 aws training and certification

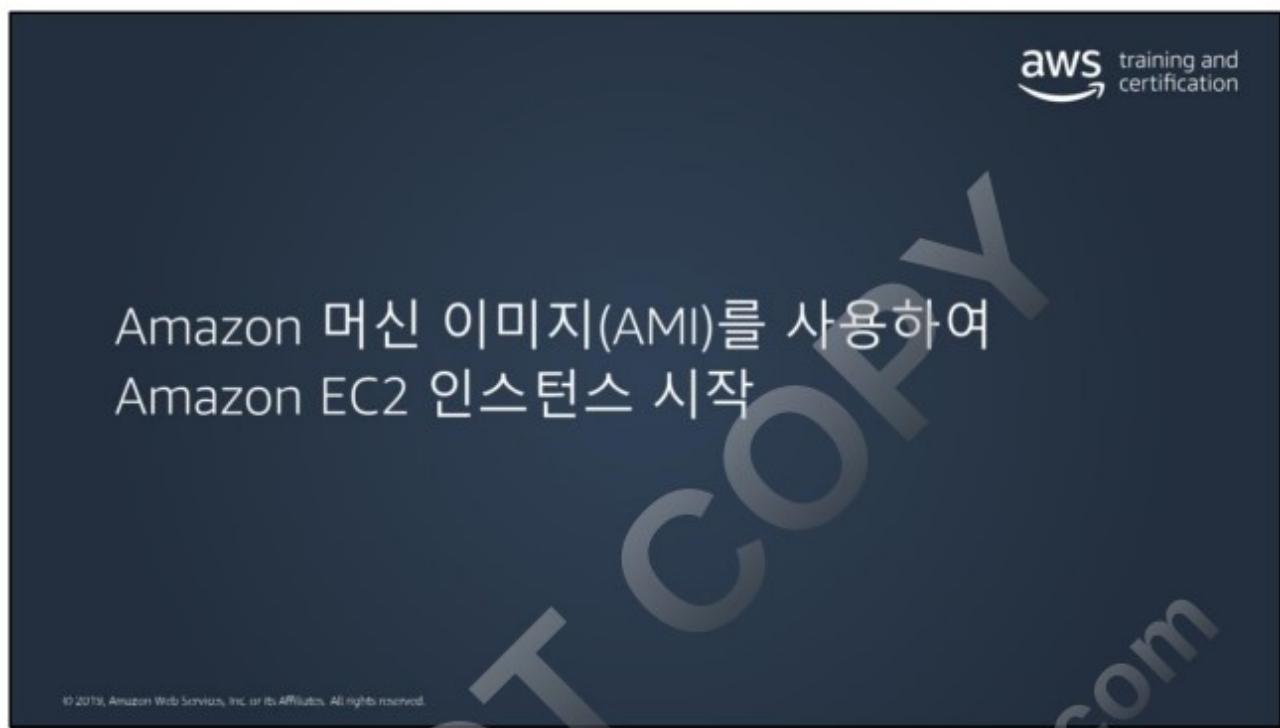
 Amazon EC2는 온프레미스 서버로 해결하기 어려운 몇몇 문제를 해결할 수 있습니다.

일회용 리소스를 사용하는 경우

 데이터 기반 의사 결정	 빠른 반복	 자유로운 실수
---	--	--

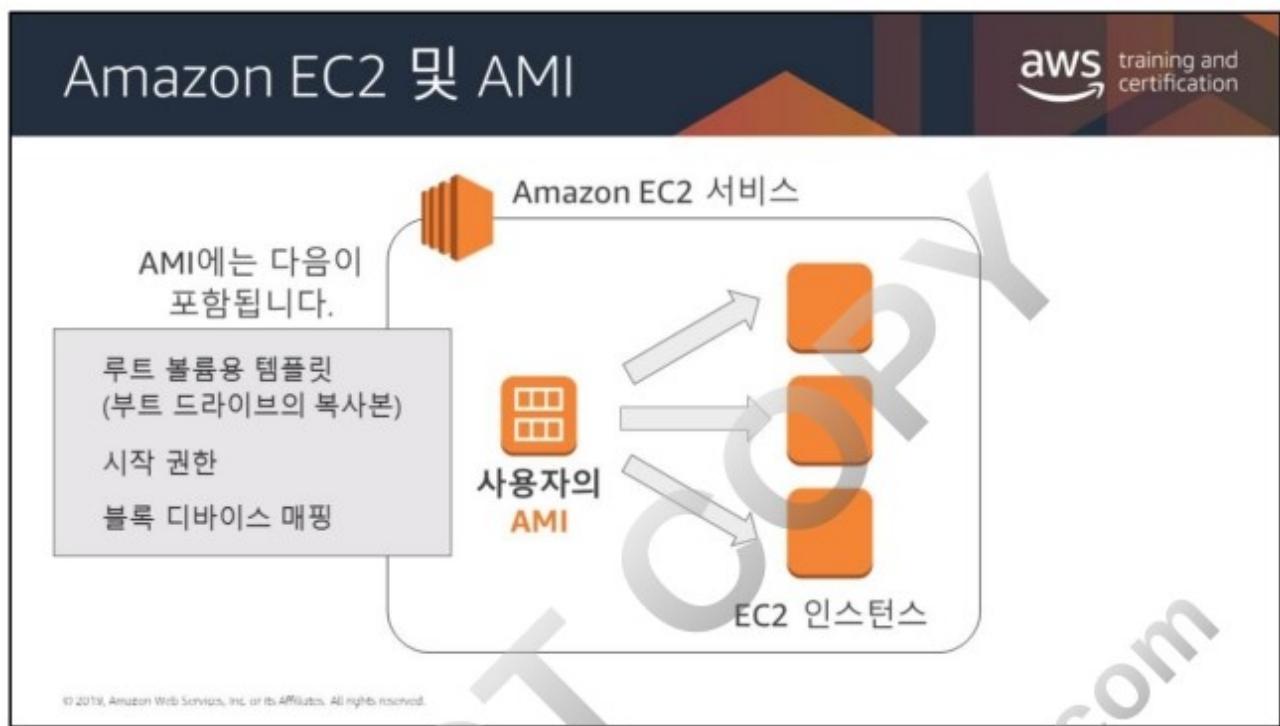
ID 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS에서는 서버, 데이터베이스, 스토리지 및 상위 애플리케이션 구성 요소를 몇 초 이내에 인스턴스화할 수 있습니다. 이들을 임시 또는 일회용 리소스로 취급할 수 있으므로 고정적이고 유한한 IT 인프라의 경직성과 제약에서 자유로울 수 있습니다. 이는 변화 관리, 테스트, 안정성 및 용량 계획에 접근하는 방식으로 다시 정의합니다.





Amazon 머신 이미지(AMI)는 클라우드의 가상 서버인 인스턴스를 시작하는데 필요한 정보를 제공합니다. 인스턴스를 시작할 때 소스 AMI를 지정해야 합니다. 동일한 구성의 인스턴스가 여러 개 필요할 때는 한 AMI에서 여러 인스턴스를 시작할 수 있습니다. 예를 들어, 단일 AMI를 사용해 일단의 (IP 주소만 제외하고 동일한) 인스턴스를 시작하고 하나의 로드 밸런서 뒤에 배치할 수 있습니다. 또한 여러 AMI를 사용하여 다양한 유형의 인스턴스를 시작할 수도 있습니다. 예를 들어, 아키텍처에서 한 AMI를 사용해 웹 서버 인스턴스를 구현하고 다른 AMI를 사용해 애플리케이션 서버 인스턴스를 구현할 수 있습니다.



AMI는 다음을 포함합니다.

- EC2 인스턴스 루트 볼륨용 템플릿. 루트 볼륨은 일반적으로 전체 운영 체제(OS) 및 해당 OS에 설치된 모든 구성 요소(애플리케이션, 라이브러리, 유틸리티 등)를 포함합니다. EC2 서비스는 템플릿을 새 EC2 인스턴스의 루트 볼륨에 복사하고 인스턴스를 시작합니다.
- AMI를 사용하여 인스턴스를 시작할 수 있는 AWS 계정을 제어하는 시작 권한
- 시작될 때 인스턴스(있는 경우)에 연결할 볼륨을 지정하는 블록 디바이스 매핑

AMI에 대한 자세한 내용은

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>를
참조하십시오.



사전 구축: Amazon은 인스턴스를 시작할 수 있는 다수의 미리 빌드된 AMI를 제공합니다. 이러한 AMI에는 Linux 및 Windows 옵션이 포함되며, 설정을 사용자 지정할 수 있는 다양한 하위 옵션이 제공됩니다.

AWS Marketplace: AWS Marketplace는 수천 개의 소프트웨어 솔루션이 나열된 디지털 카탈로그를 제공합니다. 이러한 AMI는 빠르게 시작하는 데 도움이 되는 특정 사용 사례를 제공합니다.

자체 생성: AMI는 단지 "도너 머신" 또는 "골든 인스턴스", 즉 사용자가 AMI에 배치하려는 특정 OS 및 애플리케이션 콘텐츠로 구성한 가상 머신(VM)의 익명화된 블록 수준 복사본입니다. AMI를 생성할 때 Amazon EC2는 인스턴스를 중지하고, 루트 볼륨 스냅샷을 생성하고, 마지막으로 이 스냅샷을 AMI로 등록합니다.

또한 전 세계의 사람들이 생성한 **커뮤니티 AMI**도 있습니다. 이러한 AMI는 AWS가 점검하지 않으며 사용자가 그 사용에 따른 위험을 부담합니다. 이러한 AMI는 다양한 문제에 대한 다양한 해결책을 제공할 수 있지만, 각별히 주의하여 사용해야 합니다. 어떤 프로덕션/기업 환경에서도 사용하지 마십시오.

AMI에 대한 자세한 내용은

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>를
참조하십시오.

DO NOT COPY
zlagusdbs@gmail.com

AMI는 어떠한 도움을 줍니까?

aws training and certification



반복성

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

AMI를 사용하여 모든 문제를 해결할 수 있습니다. 먼저, 반복성: 동일한 AMI에서 시작된 인스턴스는 서로 똑같은 복제본입니다. 그러므로 유사한 인스턴스의 클러스터를 구축하거나 컴퓨팅 환경을 재생성하기가 훨씬 쉬워집니다.

AMI는 어떠한 도움을 줍니까?

aws training and certification

-  반복성
-  재사용성

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

재사용 가능성: AMI는 EC2 인스턴스의 전체 구성 및 콘텐츠를 패키징하므로 효율적이고 정확하게 인스턴스를 계속 다시 사용할 수 있습니다.

AMI는 어떠한 도움을 줍니까?

aws training and certification

-  반복성
-  재사용성
-  복구성

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

복구성: AMI는 장애가 발생한 시스템을 동일한 AMI에서 생성된 새 인스턴스로 교체하는 데 이상적입니다.

AMI는 어떠한 도움을 줍니까?

aws training and certification

-  반복성
-  재사용성
-  복구성
-  Marketplace 솔루션

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

AWS Marketplace: 특정 공급자의 소프트웨어 솔루션을 찾고 있다면 아마도 EC2 인스턴스에서 실행하여 해당 솔루션을 구현할 수 있는 AMI가 Marketplace에 있을 것입니다. 또한 개인 소프트웨어 공급자가 AMI를 생성하여 Marketplace에서 판매할 수도 있습니다.

AMI는 어떠한 도움을 줍니까?

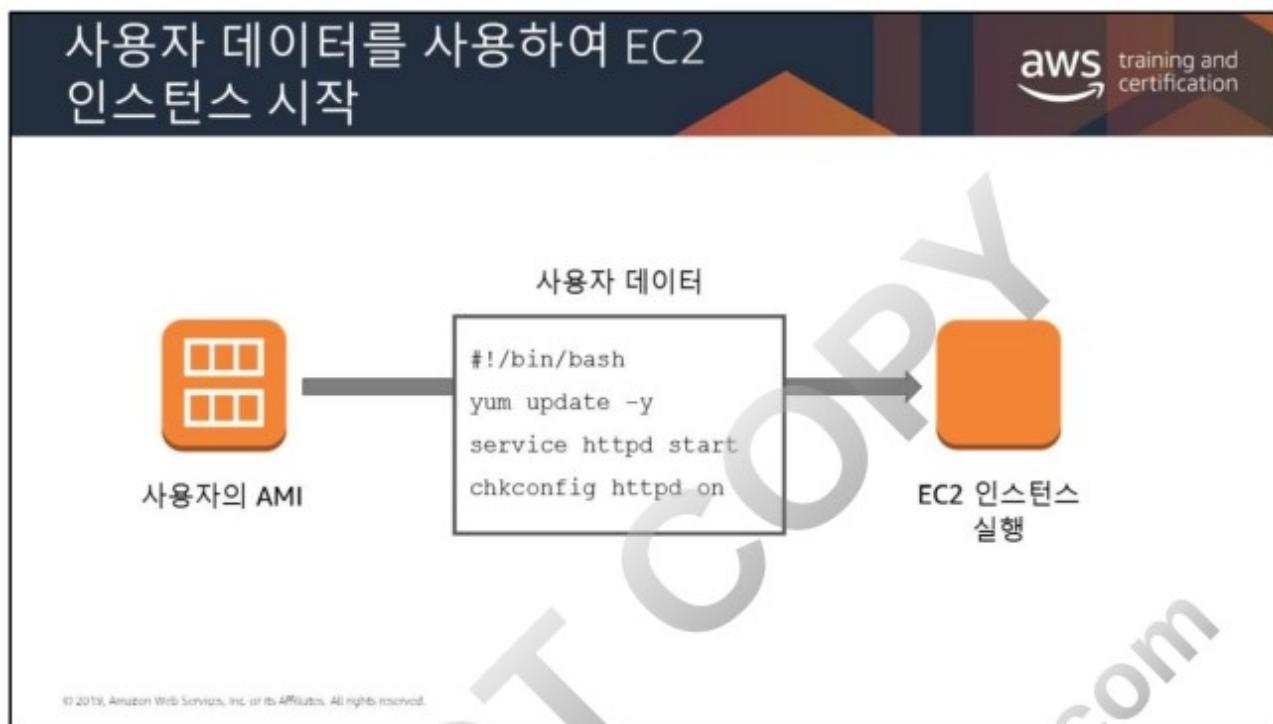
aws training and certification

-  반복성
-  재사용성
-  복구성
-  Marketplace 솔루션
-  백업

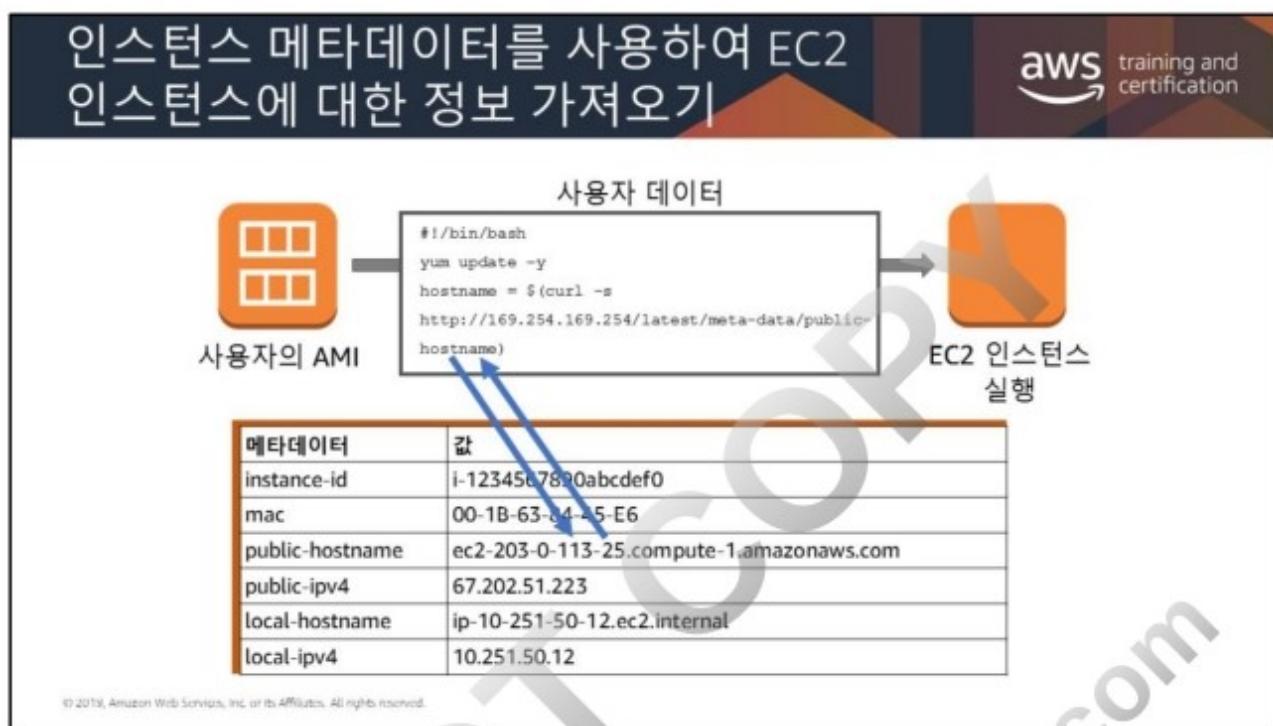
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

백업: AMI는 전체 EC2 인스턴스 구성을 백업하는 뛰어난 방법을 제공하여, 장애 발생 시 대체 인스턴스를 시작하는 데 사용할 수 있습니다.



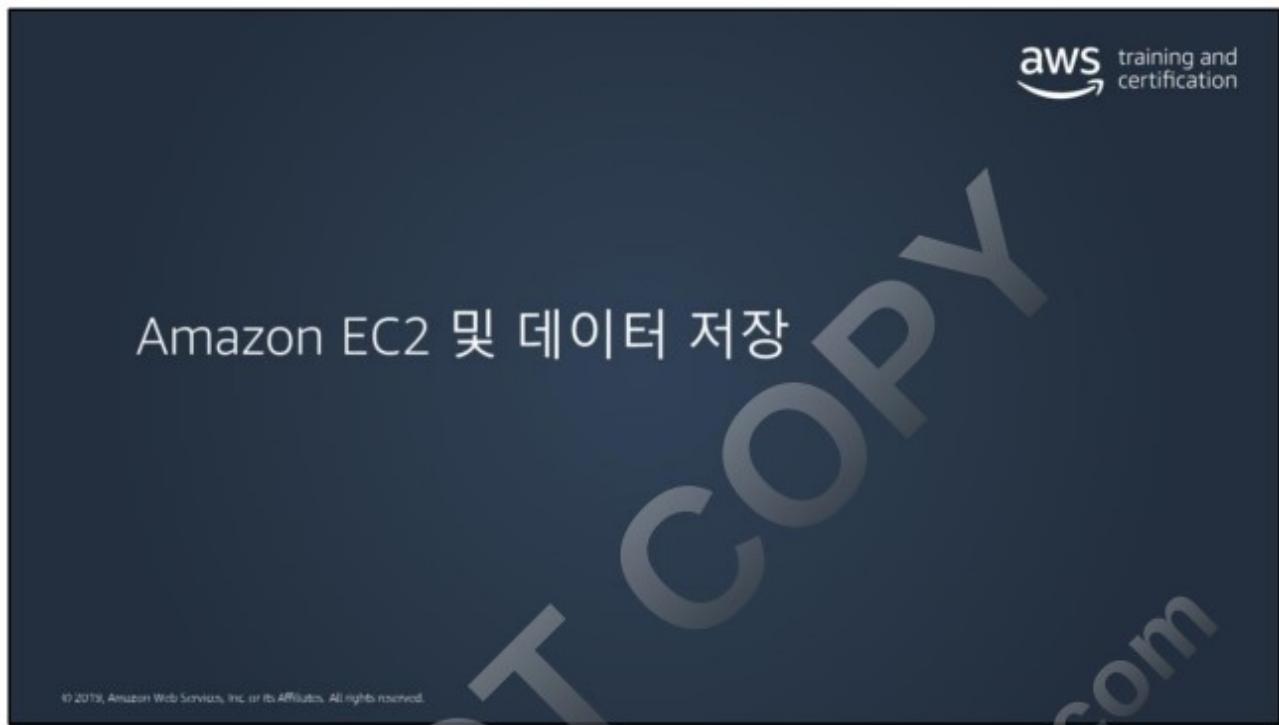


EC2 인스턴스를 생성할 때 사용자 데이터를 인스턴스에 전달할 수 있는 옵션이 있습니다. 사용자 데이터는 인스턴스 시작 완료를 자동화할 수 있습니다. 예를 들어 인스턴스 AMI를 패치 및 업데이트하거나, 소프트웨어 라이선스 키를 가져와 설치하거나 또는, 추가 소프트웨어를 설치할 수 있습니다. 사용자 데이터는 shell 스크립트 또는 cloud-init 명령으로 구현됩니다. 이 명령은 인스턴스가 시작한 후 네트워크 액세스가 가능하기 전에 루트 또는 관리자 권한으로 실행됩니다.



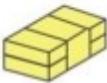
사용자 데이터가 새 EC2 인스턴스 시작을 완료하려면 인스턴스 자체에 대한 정보를 조회해야 합니다. 예를 들어 시작을 완료할 새 인스턴스의 퍼블릭 IP 주소, 호스트 이름 또는 mac 주소를 식별하고 공유해야 합니다. Instance Metadata Service에서 해당 정보를 제공할 수 있습니다.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>



Amazon Elastic Block Store (Amazon EBS)는 어떤 문제를 해결합니까?

aws training and certification

 애플리케이션에는 블록 수준 스토리지가 필요합니다.

 종료 후에도 데이터가 지속되어야 합니다.

 인스턴스 스토어는 휘발성입니다.

 데이터 볼륨을 백업할 수 있어야 합니다.

유의 사항: 동일한 인스턴스에 여러 Amazon EBS 볼륨이 있을 수 있지만 각 볼륨은 한 번에 하나의 인스턴스에만 연결할 수 있습니다.

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

Amazon EBS 볼륨은 Amazon EC2 인스턴스를 위해 안정적이고 분리 가능한 블록 수준 스토리지(외부 하드 드라이브처럼)를 제공합니다. 볼륨이 인스턴스에 직접 연결되어 있으므로, 데이터가 저장된 위치와 인스턴스에서 사용되는 위치 간에 매우 짧은 지연 시간을 제공할 수 있습니다. 이러한 이유로 Amazon EBS 볼륨은 Amazon EC2 인스턴스를 사용해 데이터베이스를 실행하는데 사용할 수 있습니다. Amazon EBS 볼륨은 인스턴스를 AMI로 백업하는데 사용할 수 있으며, AMI는 Amazon S3에 저장되고 이후에 새로운 Amazon EC2 인스턴스를 생성하는데 재사용될 수 있습니다.

인스턴스 스토어는 인스턴스에 블록 수준의 임시 스토리지를 제공합니다. 이 스토리지는 호스트 컴퓨터에 물리적으로 연결된 디스크에 위치합니다. 인스턴스 스토어는 버퍼, 캐시, 스크래치 데이터 및 기타 임시 콘텐츠와 같이 자주 변경되는 정보의 임시 스토리지나 로드 밸런싱된 웹 서버 풀과 같이 인스턴스 플릿에서 복제되는 데이터에 가장 적합합니다.

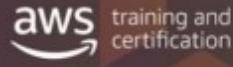
EBS에 대한 자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

인스턴스 스토리지에 대한 자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/InstanceStorage.html>

Amazon EBS 볼륨 유형



SSD 기반

볼륨 유형	범용 SSD	프로비저닝된 IOPS SSD
설명	다양한 워크로드에 사용할 수 있으며 가격 대비 성능이 우수한 범용 SSD 볼륨	지연 시간이 짧거나 처리량이 많은 미션 크리티컬 워크로드에 적합한 고성능 SSD 볼륨
사용 사례	<ul style="list-style-type: none">대부분의 워크로드에 추천	<ul style="list-style-type: none">IOPS 성능을 유지해야 하는 크리티컬 비즈니스 애플리케이션대규모 데이터베이스 워크로드

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

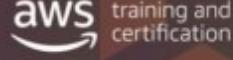
SSD 기반 볼륨은 I/O 크기가 작은 읽기/쓰기 작업을 자주 처리하는 트랜잭션 워크로드에 최적화되어 있으며, 기준 성능 측정은 IOPS입니다.

HDD 기반 볼륨: 대용량 스트리밍 워크로드에 최적화되어 있으며, IOPS보다는 처리량(MiB/s로 측정)이 더 정확한 성능 측정 기준.

Amazon EBS 볼륨 유형에 대한 자세한 내용은

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>을
참조하십시오.

Amazon EBS 볼륨 유형

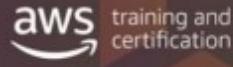


하드 디스크 기반

볼륨 유형	처리량 최적화 HDD	클드 HDD
설명	자주 액세스하고 처리량 집약적인 워크로드에 적합한 저렴한 HDD 볼륨	자주 액세스하지 않는 워크로드에 적합한 최저 비용 HDD 볼륨
사용 사례	<ul style="list-style-type: none">스트리밍 워크로드빅 데이터데이터 웨어하우스로그 처리부트 볼륨이 될 수 없음	<ul style="list-style-type: none">자주 액세스하지 않는 대용량 데이터를 위한 처리량 중심의 스토리지스토리지 비용이 최대한 낮아야 하는 시나리오부트 볼륨이 될 수 없음

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

Amazon EBS 최적화 인스턴스



EBS 최적화 인스턴스

- 최적화된 구성 스택
- Amazon EBS I/O를 위한 추가 전용 용량
- Amazon EBS와 기타 트래픽 간 경합을 최소화
- 425Mbps ~ 14,000Mbps 범위의 옵션

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

Amazon EBS 최적화 인스턴스는 최적화된 구성 스택을 사용하고 Amazon EBS I/O를 위한 추가 전용 용량을 제공합니다. 이러한 최적화를 통해 Amazon EBS I/O와 인스턴스의 다른 트래픽 간의 경합이 최소화되어 EBS 볼륨의 성능이 극대화됩니다.

EBS 최적화 인스턴스는 Amazon EBS에 전용 대역폭을 제공하며, 사용하는 인스턴스 유형에 따라 425Mbps에서 14,000Mbps 사이에서 대역폭을 선택할 수 있습니다.

자세한 내용은

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html>를
참조하십시오.

EBS 기반 EC2 인스턴스에는 EC2 최대 절전 모드를 사용할 수 있습니다. 이 기능은 나중에 동일한 시점에서 인스턴스를 다시 시작할 수 있도록 인스턴스의 인 메모리 스토리지와 프라이빗 IP, 탄력적 IP를 저장합니다. 현재는 Linux1 EC2 인스턴스에서만 활성화할 수 있습니다. Linux2는 곧 지원할 예정입니다.
인스턴스가 최대 절전 모드에 들어가면 연결된 EBS 볼륨과 탄력적 IP에 대해서만 비용을 지불합니다.

<https://aws.amazon.com/blogs/aws/new-hibernate-your-ec2-instances/>

공유 파일 시스템

여러 인스턴스가 동일한 스토리지를 사용해야 하는 경우 어떻게 합니까?



Amazon EBS는 하나의 인스턴스에만 연결됩니다.



Amazon S3가 하나의 옵션이지만 이상적인 것은 아닙니다.

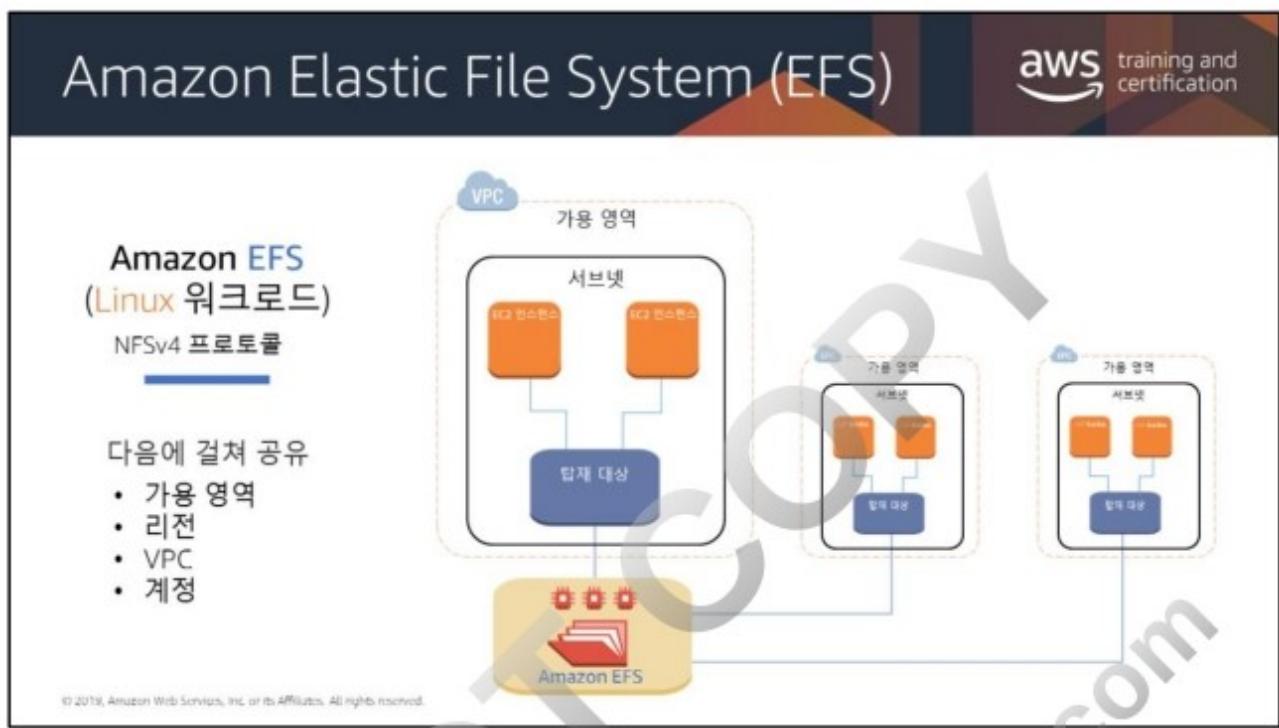


이런 작업에는 Amazon EFS 및 Amazon FSx가 적합합니다.

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

문제: 여러 인스턴스에서 실행되는 애플리케이션이 동일한 파일 시스템을 사용해야 하는 경우 어떻게 처리합니까? Amazon S3가 하나의 옵션지만, 네트워크 파일 시스템의 성능 및 읽기-쓰기 일관성이 필요할 경우 어떻게 해야 할까요? Amazon Elastic File System (Amazon EFS)가 최선의 옵션일 것입니다.

S3는 블록 스토어가 아니라 객체 스토어 시스템이므로 변경 사항이 파일 내 문자 블록이 아니라 전체 파일을 덮어씁니다. 다양한 크기의 파일을 높은 처리량으로 변경하려면 파일 시스템이 이러한 변경을 처리하는 데 객체 스토어 시스템보다 우수합니다.



Amazon Elastic File System (Amazon EFS)은 AWS 클라우드 서비스와 온프레미스 리소스에서 사용할 수 있는 간단하고 확장 가능하며 탄력적인 Linux 기반 워크로드용 파일 시스템을 제공합니다. AWS Direct Connect 또는 AWS VPN을 통해 수천 개의 EC2 인스턴스와 온프레미스 서버 간에 파일을 공유하면서 여러 가용 영역과 AWS 리전, VPC에 걸쳐 파일 시스템에 액세스할 수 있습니다. 파일 시스템을 생성하여 Amazon EC2 인스턴스에 탑재한 다음, 해당 파일 시스템에서 데이터를 읽고 쓸 수 있습니다. Amazon EFS 파일 시스템을 Network File System 버전 4.0 및 4.1 (NFSv4) 프로토콜을 통해 VPC에 탑재할 수 있습니다.

Amazon VPC의 여러 Amazon EC2 인스턴스들이 동시에 Amazon EFS 파일 시스템에 액세스할 수 있으므로 단일 연결을 넘어 확장되는 애플리케이션이 파일 시스템에 액세스할 수 있습니다. 같은 리전의 여러 가용 영역에서 실행되는 Amazon EC2 인스턴스가 이 파일 시스템에 액세스할 수 있으므로 많은 사용자가 공통 데이터 소스를 액세스하거나 공유할 수 있습니다.

계정 및 VPC 간 액세스에 대한 자세한 내용은 다음을 참조하십시오. [이제 Amazon EFS가 계정 및 VPC 간 액세스 지원](#)

VPC 피어링에 대한 자세한 내용은 다음을 참조하십시오. [다른 계정 또는 VPC에서 EFS 파일 시스템 탑재](#)

이 프로토콜을 지원하는 Amazon EC2 Linux Amazon 머신 이미지(AMI)의 목록은 [NFS 지원](#)을 참조하십시오. Amazon Linux AMI와 Ubuntu AMI에 포함된 것과 같은, 최신 버전의 Linux NFSv4.1 클라이언트를 사용하는 것을 권장합니다. 일부 AMI의 경우, Amazon EC2 인스턴스에 파일 시스템을 탑재하려면 NFS 클라이언트를 설치해야 합니다. 지침은 [NFS 클라이언트 설치](#)를 참조하십시오.

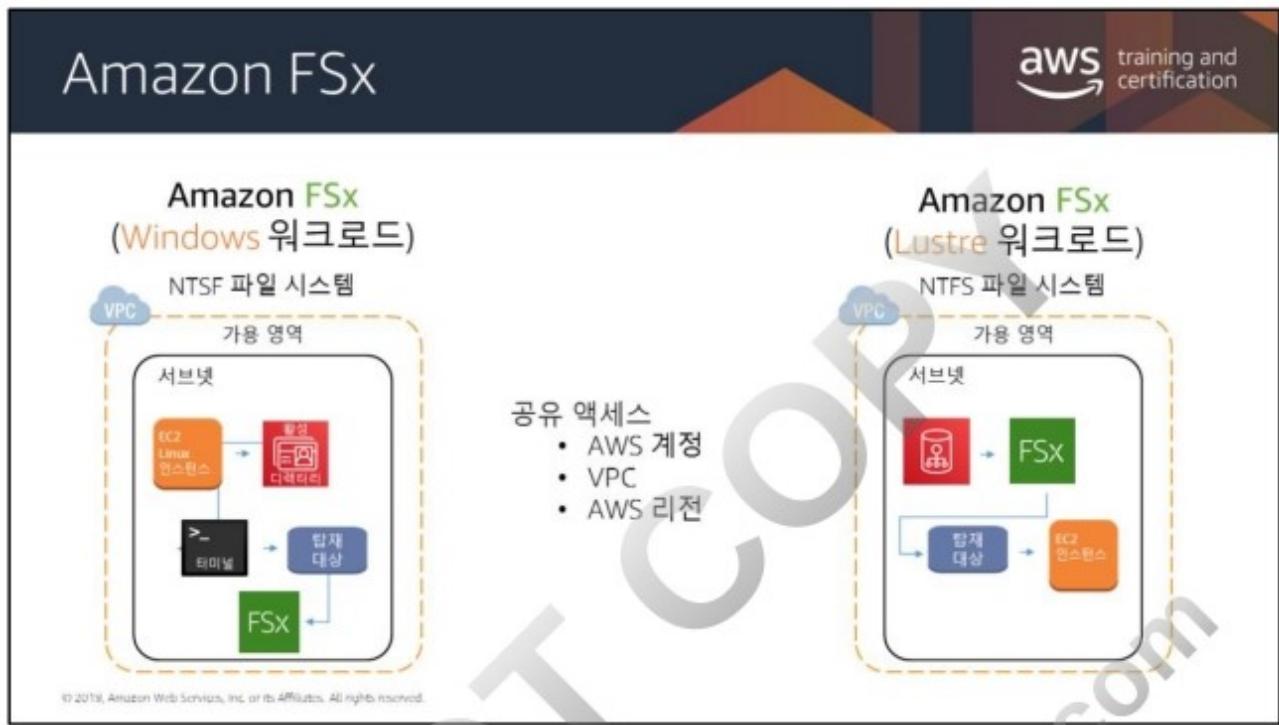
다음과 같은 제한 사항이 있습니다.

- Amazon EFS 파일 시스템은 한 번에 하나의 VPC에 있는 인스턴스에만 탑재할 수 있습니다.
- 파일 시스템과 VPC는 동일한 AWS 리전에 위치해 있어야 합니다.

파일 스토리지는 어떻게 다릅니까?

객체 스토리지 솔루션은 파일을 객체로 저장할 수 있도록 해주지만, 기존 애플리케이션이 객체를 액세스하려면 새로운 코드와 API를 사용해야 하고 이름 지정 시맨틱에 대한 직접적인 지식이 있어야 합니다. 기존 파일 시스템 시맨틱 및 권한 모델을 지원하는 파일 스토리지 솔루션은 공유 파일 스토리지와 연동하도록 손쉽게 구성되는 애플리케이션과 통합하기 위해 새로운 코드를 작성할 필요가 없다는 점에서 고유한 장점을 지닙니다.

블록 스토리지는 자체 관리형 파일 스토리지 솔루션의 기본 스토리지 구성 요소로 사용될 수 있습니다. 하지만 호스트와 볼륨 간에 일대일 관계가 필요하므로 완전 관리형 파일 스토리지 솔루션의 확장성, 가용성 및 저렴한 비용은 제공하기 힘들고, 지원을 위한 추가 예산과 관리 리소스가 필요합니다. 완전 관리형 클라우드 파일 스토리지 솔루션을 사용하면 복잡성을 제거하고, 비용을 절감하고, 관리를 간소화할 수 있습니다.



Amazon FSx는 Windows 기반 애플리케이션을 위한 Amazon FSx for Windows File Server와 컴퓨팅 집약적 워크로드를 위한 Amazon FSx for Lustre라는 두 가지 파일 시스템을 제공합니다.

Amazon FSx for Windows File Server는 엔터프라이즈 애플리케이션용으로 설계되었으며, 네이티브 Windows 파일 시스템을 지원하는 완전 관리형 서비스입니다. 이 서비스를 사용하면 엔터프라이즈 애플리케이션을 손쉽게 Amazon Web Services로 이전할 수 있습니다. SSD 스토리지 기반인 Amazon FSx for Windows File Server는 CRM, ERP, .NET 애플리케이션 및 사용자 홈 디렉토리 등 공유 스토리지가 필요한 Windows 워크로드 지원에 적합합니다. 수천 개의 컴퓨팅 인스턴스가 단일 Amazon FSx 파일 시스템에 동시에 액세스할 수 있으므로, Amazon FSx는 AWS Direct Connect 또는 AWS VPN을 통한 온프레미스 액세스를 제공합니다. 또한 VPC 피어링 또는 AWS Transit Gateway를 사용하여 여러 VPC, 계정, 리전에서 액세스할 수 있습니다. Amazon FSx for Windows File Server는 Windows Amazon EC2 인스턴스에 높은 처리량과 1밀리초 미만의 지연 시간을 보장하는 공유 파일 스토리지 시스템을 제공합니다. Amazon FSx for Windows File Server는 다음을 지원합니다.

- SMB 프로토콜
- Windows NTFS
- Active Directory (AD) 통합
- 분산 파일 시스템(DFS)

Amazon FSx for Windows File Server는 Amazon EC2 Linux 인스턴스에도 탑재할 수 있습니다. 자세한 방법은 [Microsoft Windows 파일 공유 사용](#)을 참조하십시오.

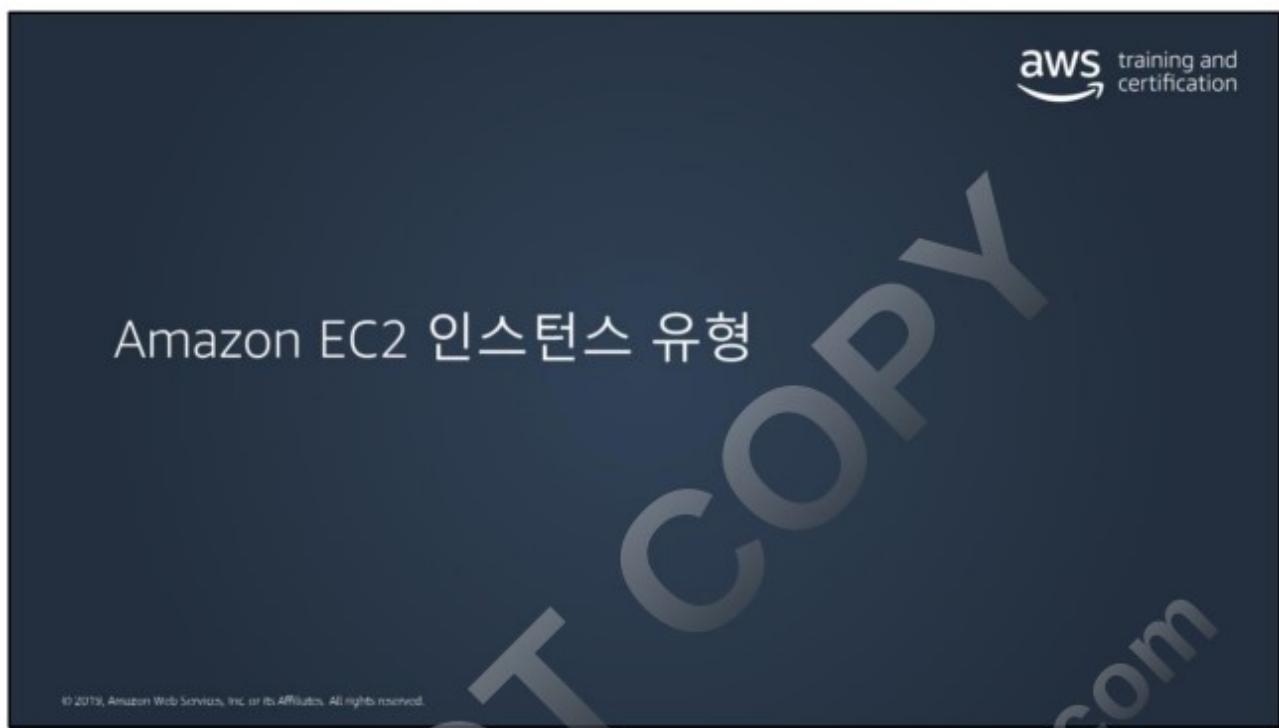
Amazon FSx for Lustre

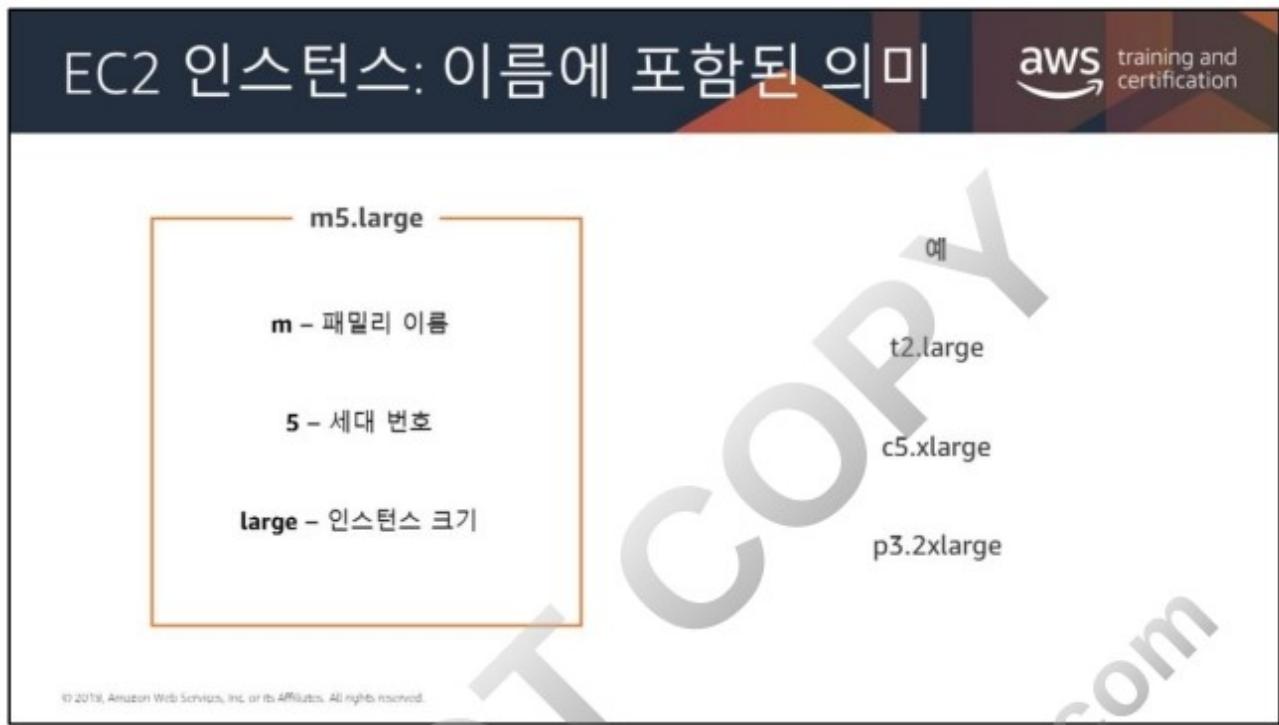
Amazon FSx for Lustre는 고성능 컴퓨팅(HPC), 기계 학습, 미디어 처리 워크플로에 최적화된 완전 관리형 파일 시스템을 제공합니다. 하나의 Amazon FSx for Lustre 파일 시스템은 방대한 데이터를 1밀리초 미만의 지연 시간과 초당 수백 기가바이트(GB)의 처리량으로 처리할 수 있습니다. Amazon FSx for Lustre는 Amazon S3와 통합할 수 있으므로 고성능 파일 시스템으로 장기간의 데이터를 처리할 수 있습니다. 데이터는 Amazon FSx for Lustre 파일 시스템과 Amazon S3 사이에서 자동으로 복사할 수 있습니다.

Amazon FSx for Lustre는 POSIX와 호환되므로 아무런 변경 없이도 현재의 Linux 기반 애플리케이션을 사용할 수 있습니다. FSx for Lustre는 네이티브 파일 시스템 인터페이스를 제공하며, Linux 운영 체제의 파일 시스템처럼 작동합니다. 또한 쓰기 후 읽기 일관성을 제공하고 파일 잠금을 지원합니다. FSx for Lustre 파일 시스템에 대한 액세스는 POSIX 권한 및 Amazon Virtual Private Cloud (VPC) 권한으로 제어할 수 있습니다.

Amazon FSx for Lustre는 Amazon EC2 인스턴스에도 탑재할 수 있습니다. 자세한 내용은 [Amazon EC2 인스턴스에서 탑재](#)를 참조하십시오.

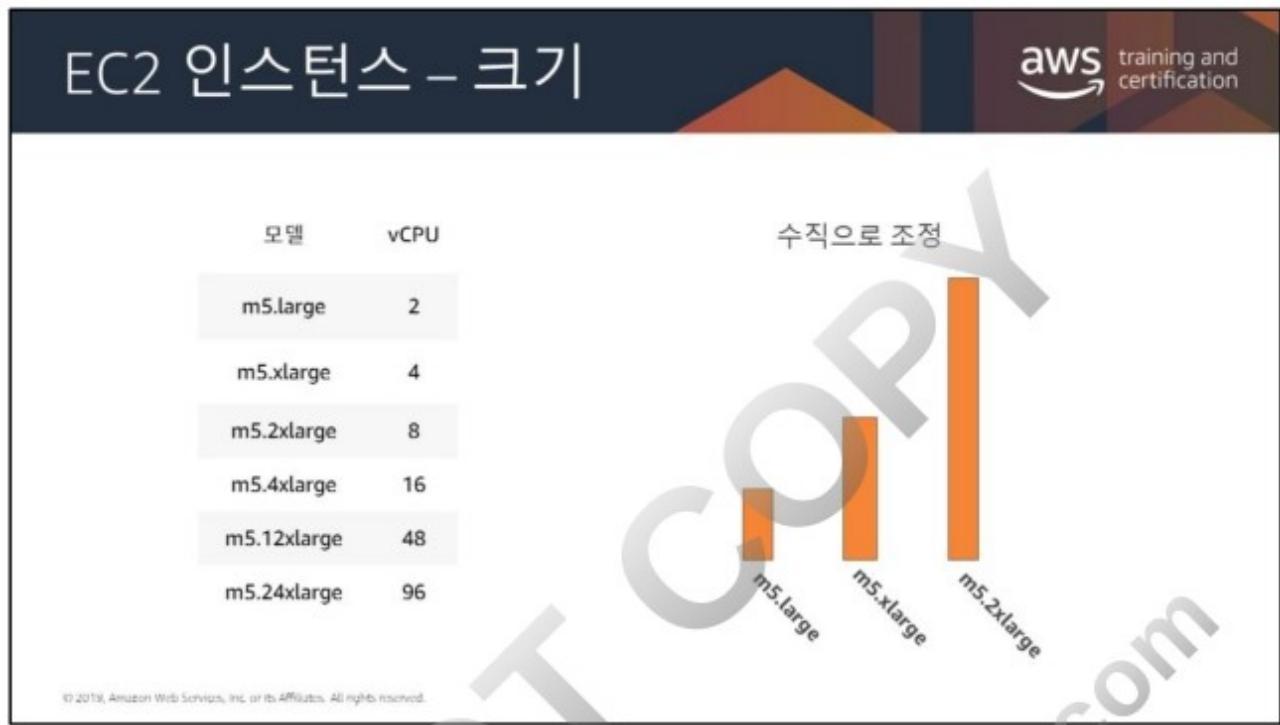
두 가지 Amazon FSx 솔루션 모두 AWS Direct Connect나 VPN 연결을 통한 온프레미스 워크로드 연결을 지원합니다. 두 솔루션 모두 사용한 리소스에 대해서만 비용을 지불합니다.





인스턴스 유형을 보면 모델 이름이 몇 개의 부분으로 구성된 것을 알 수 있습니다. M 유형을 예로 들어 보겠습니다.

M은 패밀리 이름이고 그 뒤에 숫자가 나옵니다. 여기서는 5입니다. 이 숫자는 해당 유형의 세대 번호입니다. 따라서 M5 인스턴스는 M 패밀리의 5세대입니다. 일반적으로 세대가 높을수록 인스턴스가 더 강력하고 더 우수한 가격 대비 가치를 제공합니다.



이름의 다음 부분은 인스턴스의 크기입니다. 크기를 비교할 때는 크기 범주의 계수 부분을 확인하는 것이 중요합니다.

예를 들어 m5.2xlarge는 크기가 m5.xlarge의 두 배입니다. 이 m5.xlarge는 m5.large의 두 배입니다.

나중에 나오는 차트를 보면 m5.12xlarge가 있습니다. 이 인스턴스는 m5.xlarge보다 12배 강력합니다.

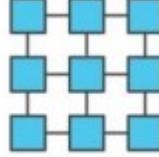
또한 네트워크 대역폭이 EC2 인스턴스의 크기와 연계되는 것도 알아야 합니다. 고도의 네트워크 집약적 작업을 수행하는 경우 이러한 요구를 충족하기 위해 인스턴스 사양을 높여야 할 수 있습니다.

EC2 인스턴스 - 유형

aws training and certification

다음을 위해 올바른 유형을 선택하는 것은 매우 중요합니다.

효율적인 인스턴스 사용률



불필요한 비용을 절감



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

불필요한 비용을 줄이고 인스턴스 사용률을 높이려면 올바른 인스턴스 유형을 선택하는 것이 매우 중요합니다.

각 인스턴스 패밀리는 고유한 장점이 있으며, 솔루션 아키텍처를 설계할 때 이를 고려해야 합니다.

모든 인스턴스 패밀리를 살펴보면서 권장 워크로드에 대해 알아보겠습니다.

EC2 인스턴스 - 유형

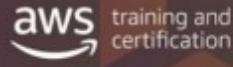


The infographic provides a comparison of various AWS Lambda instance types across five categories:

범용	일곱 가지 선택지
컴퓨팅 최적화	세 가지 선택지
메모리 최적화	일곱 가지 선택지
가속화된 컴퓨팅	네 가지 선택지
스토리지 최적화	네 가지 선택지

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

EC2 - 범용 예제



웹 사이트 및 웹 애플리케이션 같은 일시적으로 폭증할 수 있는 워크로드에 적합

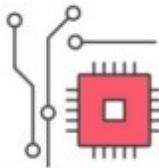
모델	vCPU	시간당 CPU 크레딧	메모리(GiB)	스토리지
t3.nano	2	6	0.5	EBS 전용
t3.micro	2	12	1	EBS 전용
t3.small	2	24	2	EBS 전용
t3.medium	2	24	4	EBS 전용
t3.large	2	36	8	EBS 전용
t3.xlarge	4	96	16	EBS 전용
t3.2xlarge	8	192	32	EBS 전용

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

T2 인스턴스는 기본 수준의 CPU 성능에 기본 수준 이상의 순간 성능을 제공하는 성능 순간 확장 가능 인스턴스입니다.

이 인스턴스 유형의 사용 사례에는 웹 사이트 및 웹 애플리케이션, 개발 환경, 빌드 서버, 코드 리포지토리, 마이크로서비스, 테스트 및 스테이징 환경, LOB (line of business) 애플리케이션이 포함됩니다.

EC2 - 컴퓨팅 최적화 예제



컴퓨팅 집약적 워크로드에 최적화

모델	vCPU	메모리(GiB)	스토리지	EBS 대역폭(Mbps)
c5.large	2	4	EBS 전용	최대 2,250
c5.xlarge	4	8	EBS 전용	최대 2,250
c5.2xlarge	8	16	EBS 전용	최대 2,250
c5.4xlarge	16	32	EBS 전용	2,250
c5.9xlarge	36	72	EBS 전용	4,500
c5.18xlarge	72	144	EBS 전용	9,000

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

C5 인스턴스는 컴퓨팅 집약적 워크로드에 최적화되었으며, 컴퓨팅 속도당 가격 비율이 저렴하고 매우 비용 효율적이며 높은 성능을 제공합니다.

사용 사례에는 고성능 웹 서버, 과학 모델링, 배치 처리, 분산 분석, 고성능 컴퓨팅(HPC), 기계 학습/딥 러닝 추론, 광고 서비스, 확장성이 높은 멀티플레이어 게임, 동영상 인코딩이 포함됩니다.

HPC 워크로드에는 Elastic Fabric Adapter 사용을 고려해

보십시오. <https://aws.amazon.com/about-aws/whats-new/2018/11/introducing-elastic-fabric-adapter/>

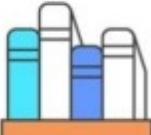
Elastic Fabric Adapter(EFA)는 AWS가 제공하는 탄력성과 확장성을 통해 온프레미스 HPC 클러스터의 성능을 제공하는 Amazon EC2 인스턴스용 네트워크 어댑터입니다. 전산 유체 역학, 날씨 모델링, 저장 장치 시뮬레이션과 같이 높은 수준의 인스턴스 간 통신이 필요한 HPC 애플리케이션을 실행할 수 있습니다. 또한 HPC 애플리케이션은 수천 개의 CPU 코어로 확장할 수 있는 메시지 전달 인터페이스(MPI)와 같은 인기 있는 HPC 기술을 사용합니다. EFA는 업계 표준 libfabric API를 지원하므로 지원되는 MPI 라이브러리를 사용하는 애플리케이션을 거의 또는 전혀 수정하지 않고 AWS로 마이그레이션할 수 있습니다.

(참고: EFA는 C5n.9xI, C5n.18xI, P3dn.24xI 인스턴스에서 활성화할 수 있는 선택적 EC2 네트워킹 기능으로 제공됩니다. 몇 개월 안에 추가 인스턴스 유형을 지원할 계획입니다.)

DO NOT COPY
zlagusdbs@gmail.com

EC2 - 메모리 최적화 예제

aws training and certification



메모리 집약적 애플리케이션
또는 CPU보다 RAM이 더
필요한 경우

모델	vCPU	메모리(GiB)	스토리지(GiB)	전용 EBS 대역폭(Mbps)	네트워킹 성능(Gbps)
r5.large	2	16	EBS 전용	최대 3,500	최대 10
r5.xlarge	4	32	EBS 전용	최대 3,500	최대 10
r5.2xlarge	8	64	EBS 전용	최대 3,500	최대 10
r5.4xlarge	16	128	EBS 전용	3,500	최대 10
r5.12xlarge	48	384	EBS 전용	7,000	10
r5.24xlarge	96	768	EBS 전용	14,000	25

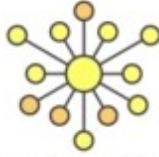
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

R4 인스턴스는 메모리 집약적 애플리케이션에 최적화되어 있습니다.

사용 사례에는 고성능 데이터베이스, 데이터 마이닝 및 분석, 인 메모리 데이터베이스, 분산형 웹 스케일 인 메모리 캐시, 구조화되지 않은 빅 데이터를 실시간으로 처리하는 애플리케이션, 하둡/Spark 클러스터 및 기타 엔터프라이즈 애플리케이션이 포함됩니다.

EC2 – 가속화된 컴퓨팅 예제

aws training and certification



고성능 GPU 기반 인스턴스
일반적으로 기계 학습/딥 러닝에 사용

모델	GPU	vCPU	메모리(GiB)	GPU 메모리(GiB)	GPU P2P
p3.2xlarge	1	8	61	16	-
p3.8xlarge	4	32	244	64	NVLink
p3.16xlarge	8	64	488	128	NVLink
p3.dn24x	12	96	768	256	NVLink

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

P3 인스턴스는 범용 GPU 컴퓨팅 애플리케이션에 사용됩니다.

사용 사례에는 기계 학습, 딥 러닝, 고성능 컴퓨팅, 전산 유체 역학(CFD), 계산 금융, 지진 분석, 음성 인식, 자율 주행 차량, 신약 개발이 포함됩니다.

EC2 – 스토리지 최적화 예제



높은 디스크 처리량을 갖는
최대 16TB의 HDD 기반 로컬
스토리지

모델	vCPU	메모리 (GiB)	네트워킹 성능	인스턴스 스토리지(GB)
h1.2xlarge	8	32	최대 10기가비트	1 x 2,000 HDD
h1.4xlarge	16	64	최대 10기가비트	2 x 2,000 HDD
h1.8xlarge	32	128	10기가비트	4 x 2,000 HDD
h1.16xlarge	64	256	25기가비트	8 x 2,000 HDD

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

H1 인스턴스는 최대 16TB의 HDD 기반 로컬 스토리지, 높은 디스크 처리량 및 컴퓨팅과 메모리의 균형을 제공합니다.

사용 사례에는 Amazon EMR 기반 워크로드, HDFS 및 MapR-FS와 같은 분산 파일 시스템, 네트워크 파일 시스템, Apache Kafka와 같은 로그 또는 데이터 처리 애플리케이션, 빅 데이터 워크플로 클러스터가 포함됩니다.

인텔® 제온 CPU 및 EC2 인스턴스

aws training and certification

현재 모든 EC2 인스턴스 유형은 다음을 포함합니다.

- 인텔 AES-NI: 암호화로 인한 성능 저하 감소
- 인텔 AVX (AVX2, AVX-512): 부동 소수점 성능을 개선합니다. HVM 배포에서만 사용할 수 있습니다.

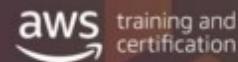
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

인텔 프로세서를 사용하는 현재의 모든 EC2 인스턴스 유형은 인텔의 AES-NI(Advanced Encryption Standard New Instructions)를 포함하고 있으며, 이는 암호화 활성화 시 높아지는 프로세서의 성능 저하를 줄여줍니다.

또한 모든 인스턴스 유형에는 부동 소수점 집약적 워크로드를 위해 인텔이 커스텀 제작한 명령인 AVX(Advanced Vector Extension)의 일부 형식이 포함되어 있습니다. AVX2는 AVX보다 두 배 뛰어난 부동 소수점 성능을 제공하며, 새로운 인텔 제온 확장형 프로세서 CPU 제품군에서만 제공되는 AVX-512는 AVX2의 성능을 두 배로 높입니다.

인텔 TSX (Transactional Synchronization Extensions): 필요에 따라 멀티스레드와 단일 스레드를 전환하여 애플리케이션별로 워크로드에 최적화된 성능을 제공합니다.

인텔® 제온 CPU 및 EC2 인스턴스



일부 EC2 인스턴스 유형은 다음을 포함합니다.

- **인텔 Turbo Boost**: 필요할 때 기본 클럭 속도보다 빠르게 코어 실행
- **인텔 TSX**: 필요에 따라 멀티 스레드 또는 단일 스레드 사용
- **P State 및 C State 제어**: 각 코어의 성능 및 절전 상태 미세 조정

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

일부 인스턴스 유형에는 인텔 Turbo Boost, 인텔 TSX, P State 및 C State 제어 기능도 포함됩니다.

인텔 Turbo Boost는 필요에 따라 코어의 클럭 속도를 지능적으로 높입니다.

인텔 TSX (Transactional Synchronization Extensions): 필요에 따라 멀티스레드와 단일 스레드를 전환하여 애플리케이션별로 워크로드에 최적화된 성능을 제공합니다.

P State 및 C State 제어를 통해 각 코어의 성능 및 절전 상태를 필요에 맞게 조정할 수 있습니다.

현재 이러한 옵션을 지원하는 인스턴스 유형을 확인하려면 AWS 인스턴스 유형 페이지(<https://aws.amazon.com/ec2/instance-types/>)를 참조하십시오.



다양한 워크로드에 적합한 여러 인텔 프로세서가 있습니다.

- 인텔® AVX 512:** 과학 시뮬레이션, 금융 분석, 인공 지능(AI)/딥 러닝, 3D 모델링 및 분석, 이미지 및 오디오/비디오 처리, 암호화 및 데이터 압축에 최적화.
- 인텔® AES-NI:** 인텔® AES-NI는 보다 빠른 데이터 보호와 강력한 보안을 제공하여, 이전에는 불가능했던 분야에도 적용되는 광범위한 암호화를 실현합니다.
- 인텔® TSX:** 인텔® TSX(Transactional Synchronization Extensions)는 프로세서가 잠금 보호된 중요 섹션을 통해 스레드를 동적으로 직렬화할지 여부를 결정하고, 필요시에만 직렬화를 수행합니다. 비즈니스 애플리케이션의 컴퓨팅 성능을 동적으로 최적화
- 인텔® Turbo Boost:** 인텔® Turbo Boost Technology 2.0은 최대 로딩을 위한 프로세서 및 그래픽 성능을 가속화하므로 전력, 전류 및 온도의 사양 한계 미만으로 작동하는 경우 프로세서 코어를 자동으로 정격 작동 주파수보다 빠르게 실행될 수 있도록 합니다.

The slide has a dark blue header with the text "인텔® 제온 확장형 프로세서" and the AWS logo "aws training and certification". The main content area has a light gray background with a large diagonal watermark reading "zlaguabschaff.com".

최신 인텔 제온 프로세서

최대:

- CPU당 28개 코어
- 6개의 메모리 채널
- 대역폭/처리량의 PCIe 레인 48개
- 100Gbps 네트워크 대역폭(C5n.16xlarge)

인텔 AVX-512:

- AVX2 부동 소수점 성능의 2배
- 512비트 명령(AVX/AVX2는 256비트)

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

최신 인텔 제온 프로세서는 인텔 제온 확장형 프로세서 제품군입니다. 이 제품군은 코어당 성능이 향상된 최대 28개의 코어, 대폭 증가한 메모리 대역폭(6개의 메모리 채널)과 I/O 대역폭 및 처리량(48개의 PCIe 레인)으로 이전 세대보다 성능이 크게 향상되어, 인 메모리 데이터베이스 및 고성능 컴퓨팅과 같이 데이터가 많이 필요하고 자연 시간에 민감한 애플리케이션은 고밀도 컴퓨팅 및 대규모 데이터 볼륨 액세스 속도 향상을 통해 눈에 띄게 성능이 개선됩니다.

이 제품군에는 AVX2를 사용하여 프로세서의 부동 소수점 성능을 두 배로 높여 주는 최신 버전의 인텔 AVX 명령도 포함되어 있습니다.

인텔® 제온 제품군 및 EC2 인스턴스

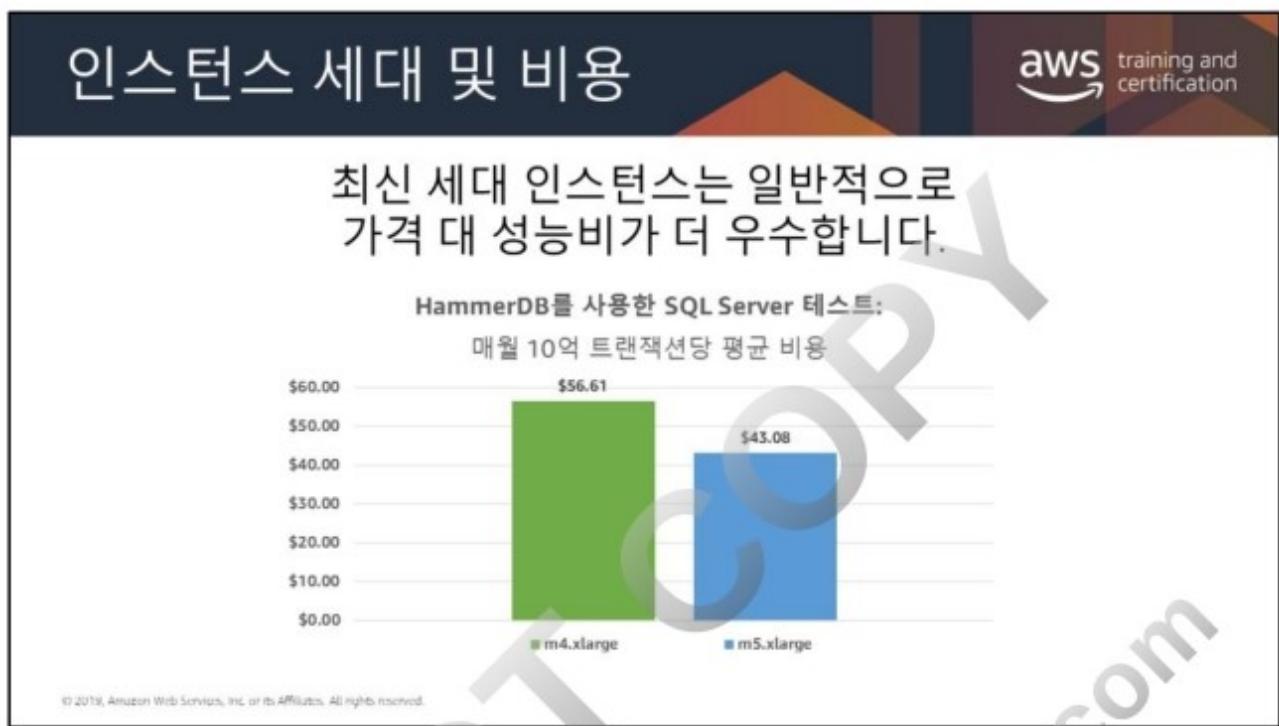
aws training and certification

인텔 제온 확장형 프로세서 제품군	인텔 제온 E5 프로세서 제품군	인텔 제온 E7 프로세서 제품군
<ul style="list-style-type: none">고용량 메모리z1dC5/C5nM5R5T3	<ul style="list-style-type: none">M4R4P2/P3G3F1H1I3D2	<ul style="list-style-type: none">X1/X1e

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

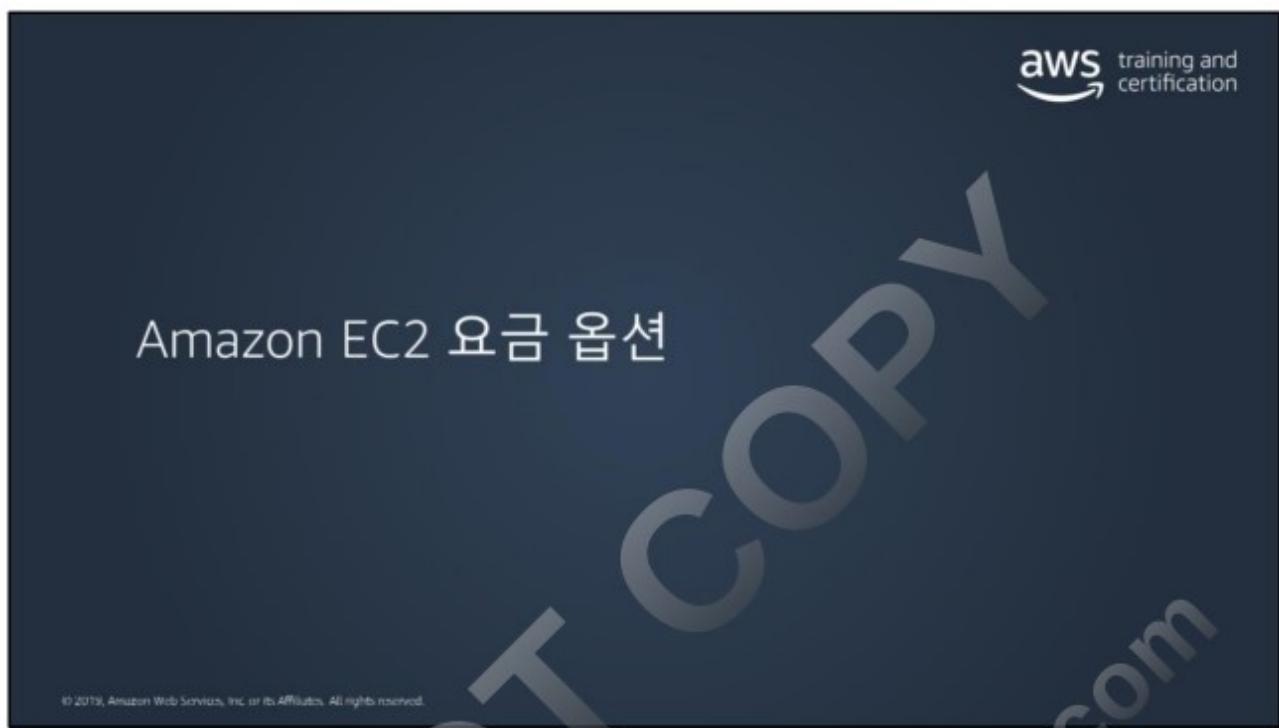
다음은 2019년 3월 기준 최신 EC2 인스턴스 유형 및 관련 프로세서 제품군입니다.
EC2 인스턴스 유형의 최신 목록은 AWS 인스턴스 유형 정보 페이지를
참조하십시오.

<https://aws.amazon.com/ec2/instance-types/>



최신 세대 인스턴스가 이전 세대 인스턴스보다 시간당 비용이 더 많이 들지만, 가격 대 성능 비율은 최신 인스턴스가 일반적으로 이전 세대보다 높습니다. 다음은 m4.xlarge 및 m5.xlarge 인스턴스에 배포된 여러 SQL Server에서 HammerDB를 사용하여 수행한 테스트의 예입니다. 이 테스트에서는 일정 수의 사용자(3~233명)를 기준으로 각 인스턴스에 의해 수행될 수 있는 트랜잭션의 수와 인스턴스 운영 비용을 월별로 비교하고 각 인스턴스 유형별 전체 결과의 평균을 구했습니다. 전체 세부 정보는 아래에 제공된 링크에서 읽을 수 있습니다.

출처: <https://www.dbbest.com/blog/validating-aws-ec2-sql-server-deployments-using-benchmark-tools/>



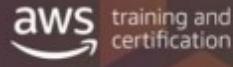


AWS 프리 티어의 일환으로 신규 AWS 고객은 가입 후 최대 1년 동안 무료로 제공되는 Amazon EC2 t2.micro 인스턴스, S3 버킷 용량 및 기타 여러 AWS 서비스를 사용하여 시작할 수 있습니다. 프리 티어에서 제공되는 내용은 서비스마다 다릅니다. 자세한 내용은 <https://aws.amazon.com/free/>를 참조하십시오.

온디맨드, 예약, 스팟 인스턴스로 시작한 Amazon Linux 및 Ubuntu 기반 인스턴스의 Amazon EC2 사용량은 최소 기간 60초 이후 초 단위로 요금이 부과됩니다. 다른 모든 운영 체제는 1시간 단위로 요금이 부과되며, 1시간을 전부 사용하는지 여부에 상관없이 해당 시간이 시작될 때 1시간으로 계산되어 청구됩니다. 예약 인스턴스는 청구서가 처리될 때까지 온디맨드 인스턴스로 실행되며 온디맨드 인스턴스와 구별할 수 없다는 점을 유의하십시오.

AWS 요금제 적용 방식에 대한 자세한 내용은 https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf를 참조하십시오.

온디맨드 인스턴스

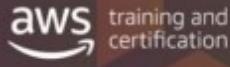


즉시 필요한 컴퓨팅 파워를 해결

• 컴퓨팅 파워에 대한 초당(Amazon Linux 및 Ubuntu) 또는 시간당(다른 모든 OS) 비용을 지불
• 장기 약정 필요 없음
• 선결제 금액 없음
• 애플리케이션의 수요에 따라 컴퓨팅 파워를 확장 또는 축소

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

예약 인스턴스



아키텍처에 대해 상당한 할인을 제공할 수 있음

- 용량에 대한 비용을 미리 지불
- 스탠다드 RI, 컨버터블 RI, 예약 RI
- 3가지 선결제 방법
- 여러 계정(결제 패밀리 내) 사이에서 공유 가능

미리 용량을 예약하여 비용을 절감할 수 있음

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

예약 인스턴스(RI)는 아키텍처의 비용을 줄일 수 있는 뛰어난 도구입니다. EC2 인스턴스 사용량의 기본 수준을 알고 있다면 RI가 상당한 할인을 제공할 수 있습니다.

RI는 여러 방법으로 설정할 수 있습니다.

- 스탠다드 RI: 가장 큰 할인 혜택(온디맨드 가격 대비 최대 75% 할인)을 제공하며 준비 상태 사용에 가장 적합합니다.
- 컨버터블 RI: 할인 혜택(최대 54% 할인 온디맨드 가격)을 제공하며 RI의 속성을 변경할 수 있습니다. 단, 변경한 결과 동일한 가치 이상의 RI가 생성되어야 합니다.
- 예약 RI: 이 RI는 사용자가 선택한 기간에 시작되므로 용량 요구 사항을 충족할 수 있습니다.

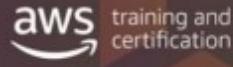
약정 기간: AWS는 스탠다드 RI를 1년 또는 3년 약정으로 제공합니다. 예약 인스턴스 Marketplace 판매자도 RI를 제공하며 약정 기간은 더 짧습니다. AWS는 컨버터블 RI를 1년 또는 3년 약정으로 제공합니다.

결제 옵션: 전체 선결제, 부분 선결제, 선결제 없음의 세 가지 결제 옵션 중 선택할 수 있습니다. 일부 또는 선결제 없음 결제 옵션을 선택한 경우 기간이 지남에 따라 매월 일정 금액씩 잔액을 지불하게 됩니다.

자세한 내용은 <https://docs.aws.amazon.com/aws-technical-content/latest/cost-optimization-reservation-models/introduction.html>를 참조하십시오.

DO NOT COPY
zlagusdbs@gmail.com

스팟 인스턴스

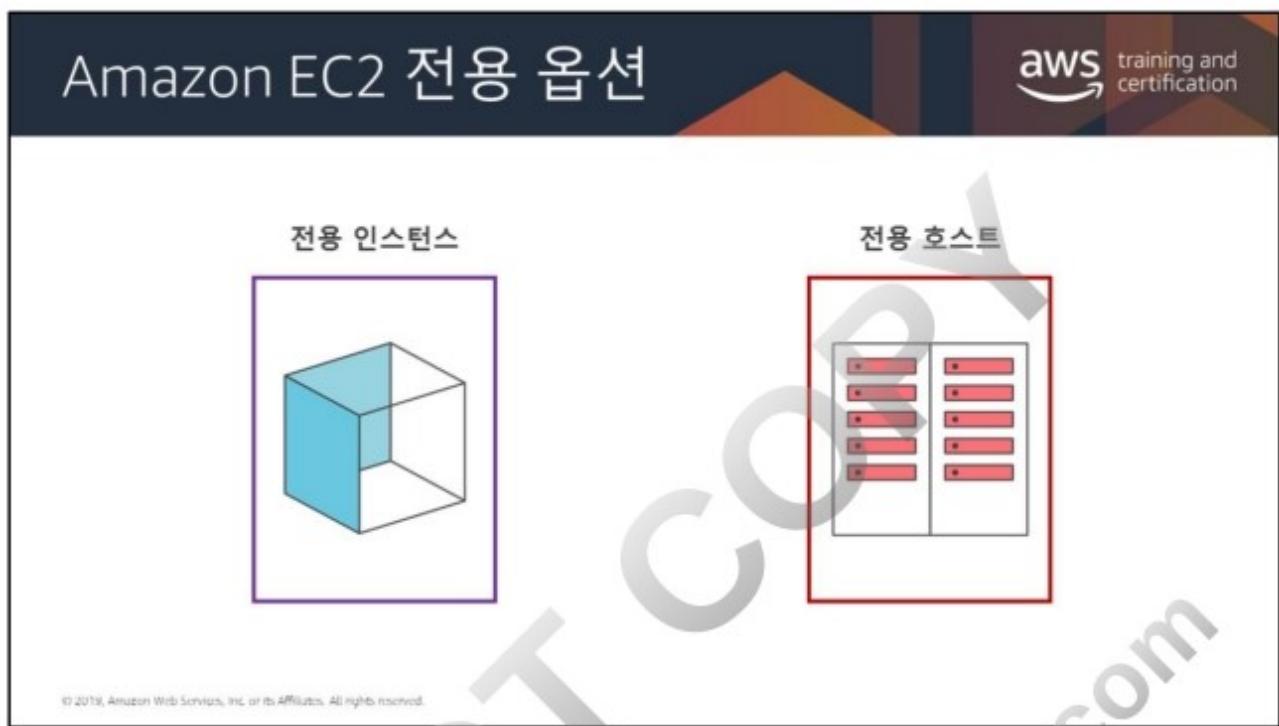


워크로드의 시작 및 중지를 수용할 수 있는 한 최고의 할인 제공 가능

미사용 Amazon EC2 용량 구매
가격은 수요와 공급을 기반으로 AWS에서 제어
종료 2분 전에 종료 공지를 제공
스팟 블록: 1~6시간의 지속 시간을 지닌 스팟 인스턴스 시작

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

Amazon EC2 스팟 인스턴스의 경우, 새 요금 모델에서는 스팟 인스턴스에 대해 입찰할 필요가 없고, 시작한 인스턴스에 대해 현재 적용되는 스팟 가격을 지불하기만 하면 됩니다. 시장 가격을 분석하거나 최대 입찰 가격을 설정하느라 시간을 들일 필요 없이 온디맨드 용량 요청과 똑같은 방법으로 스팟 용량을 요청할 수 있습니다.

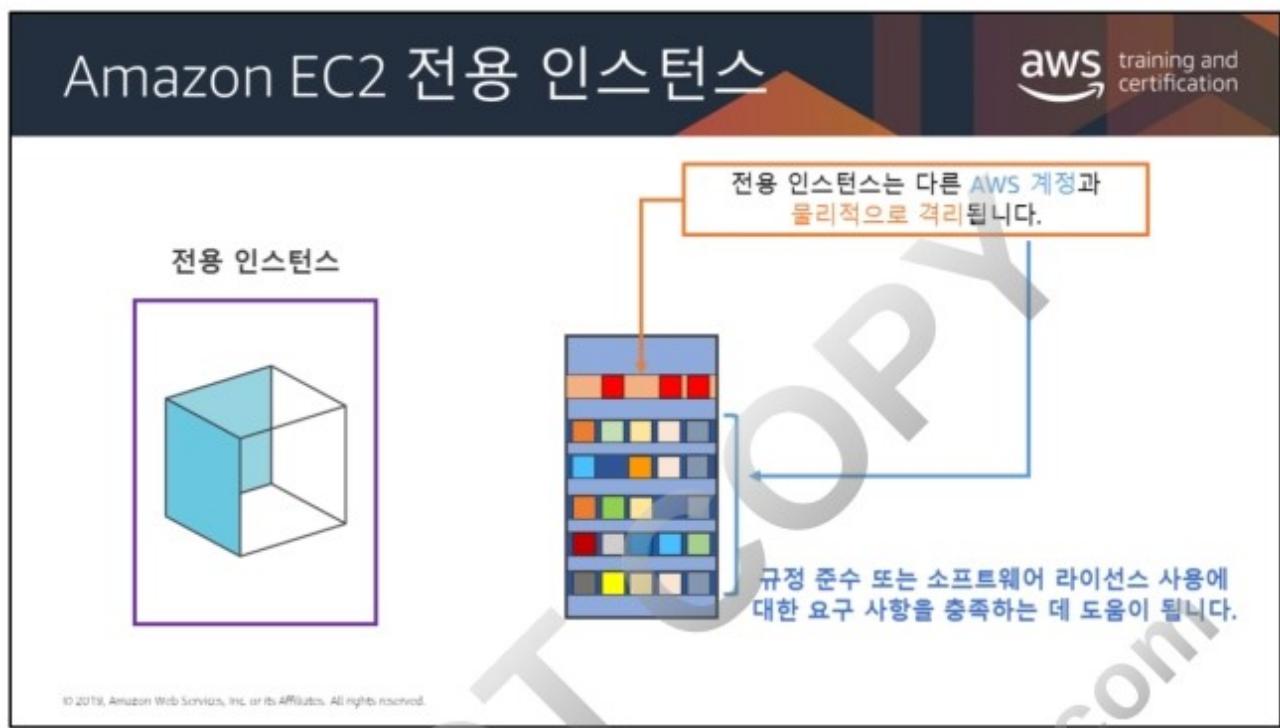


이러한 전용 옵션 외에도 라이선스 요구 사항에 따라 AWS License Manager를 고려할 수도 있습니다.

AWS License Manager를 사용하면 AWS 및 온프레미스 서버에서 다양한 소프트웨어 공급업체(Microsoft, SAP, Oracle 등)의 라이선스를 더 쉽게 관리할 수 있습니다. 이를 통해 관리자는 EC2 인스턴스를 시작할 때 사용자 지정 라이선스 규칙을 생성하고 이러한 규칙을 사용하여 허용 범위 이상의 라이선스를 사용해 라이선스를 위반하지 않도록 제한하거나 다른 서버에 단기적으로 라이선스를 재할당할 수 있습니다.

관리자는 AWS License Manager 대시보드에서 라이선스를 검토하고 관리할 수 있습니다.

<https://aws.amazon.com/about-aws/whats-new/2018/11/announcing-aws-license-manager/>



전용 인스턴스는 단일 고객을 위한 전용 하드웨어의 VPC에서 실행되는 Amazon EC2 인스턴스입니다. 전용 인스턴스는 다른 AWS 계정에 속하는 인스턴스로부터 호스트 하드웨어 수준에서 물리적으로 격리됩니다. 전용 인스턴스 요금은 두 부분으로 구성됩니다.

- 시간당 인스턴스 사용 요금
- 리전당 전용 요금(실행 중인 전용 인스턴스 수와 상관없이 시간당 결제된다는 점에 유의)

Amazon EC2 전용 호스트

전용 호스트는 고객 전용의 EC2 인스턴스 용량을 갖춘 물리적 서버입니다.

전용 호스트는 고객 전용의 EC2 인스턴스 용량을 갖춘 물리적 서버입니다.

호스트
ID: h-039725dyhc980010

규정 준수 또는 소프트웨어 라이선스 사용에 대한 엄격한 요구 사항을 충족하는 데 도움이 됩니다.

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



전용 호스트는 고객 전용의 인스턴스 용량을 제공하는 물리적 EC2 서버입니다. 전용 호스트를 사용하면 Windows Server, SQL Server 및 SUSE Linux Enterprise Server(라이선스 약관에 따름)를 비롯한 기존 서버에 한정된 소프트웨어 라이선스를 사용할 수 있으므로, 규정 준수 요구 사항을 해결하면서 비용도 절감할 수 있습니다. 전용 호스트는 온디맨드(시간당)로 구입할 수 있습니다. 예약은 온디맨드 요금과 비교하여 최대 70%의 할인을 제공할 수 있습니다.

전용 호스트 이점:

- 라이선스 비용 절감:** 전용 호스트를 사용하면 Amazon EC2에서 자체 소켓당 또는 코어당 소프트웨어 라이선스를 사용함으로써 비용을 절약할 수 있습니다.
- 규정 준수 및 규제 요구 사항 충족 지원:** 전용 호스트를 사용하면 특정 물리적 서버의 VPC에서 인스턴스를 시작할 수 있습니다. 이를 통해 기업 규정 준수 및 규제 요구 사항을 충족하는 구성을 사용하여 인스턴스를 배포할 수 있습니다.

전용 호스트에 대한 자세한 내용은 <https://aws.amazon.com/ec2/dedicated-hosts/>를 참조하십시오.

Amazon EC2 테넌시

aws training and certification

	하드웨어를 자신의 계정만 사용합니까?	설명
기본값	아니요	인스턴스가 공유된 하드웨어에서 실행됩니다.
전용 인스턴스	예	비 특정 하드웨어에서 실행됩니다.
전용 호스트	예	고객이 선택한 특정 하드웨어에서 실행되어 고객이 보다 세밀하게 제어할 수 있습니다.

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

인스턴스를 시작한 이후에는 테넌시를 변경하는 데 몇 가지 제한이 있습니다.

- 인스턴스를 시작한 후 인스턴스 테넌시를 기본에서 전용 또는 호스트로 변경할 수 없습니다.
- 인스턴스를 시작한 후 인스턴스 테넌시를 전용 또는 호스트에서 기본으로 변경할 수 없습니다.
- 인스턴스를 시작한 후 인스턴스 테넌시를 전용에서 호스트로 또는 호스트에서 전용으로 변경할 수 있습니다.

자세한 내용은 [인스턴스 테넌시 변경](#)을 참조하십시오.

사용자의 인스턴스 추적

aws training and certification

다음 작업에 도움이 되도록 AWS 리소스에 메타데이터 **태그**를 할당합니다.

관리 검색 필터링

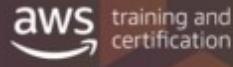
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS 고객은 AWS 리소스에 태그 형태의 메타데이터를 지정할 수 있습니다. 각 태그는 고객이 정의한 키와 보다 간편하게 리소스를 관리, 검색 및 필터링할 수 있는 값(선택 사항)으로 구성되는 간단한 레이블입니다.

태그의 고유한 유형은 없지만 고객은 태그를 사용해 리소스를 용도, 소유자, 환경 등의 기준으로 범주화할 수 있습니다. 이 웹 페이지에서는 AWS 고객이 일관되고 효과적인 태깅 전략을 구현하는 데 도움이 되도록 일반적으로 사용되는 태깅 범주 및 전략을 설명합니다. 다음 단원에서는 AWS 리소스, 태그 지정, 세부 결제 및 IAM에 대한 기본 지식이 있는 것으로 가정합니다.

AWS 태깅 전략에 대한 자세한 내용은 <https://aws.amazon.com/answers/account-management/aws-tagging-strategies/> 단원을 참조하십시오.

태그 지정 모범 사례



</>

- 태그에 대한 표준화된 대/소문자 구분 형식
- 리소스 태그를 관리하는 데 도움이 되는 자동화된 도구를 구현합니다.
- 태그는 너무 적게 사용하는 것보다 너무 많이 사용하는 것이 낫습니다.
- 태그는 수정하기 쉽습니다.
- 예: 앱 버전, ENV, DNS 이름, 앱 스택 식별자

리소스가 어떤 기능을 수행하고 비용에 미치는 영향은 무엇인지 이해하는 데 도움이 됩니다.

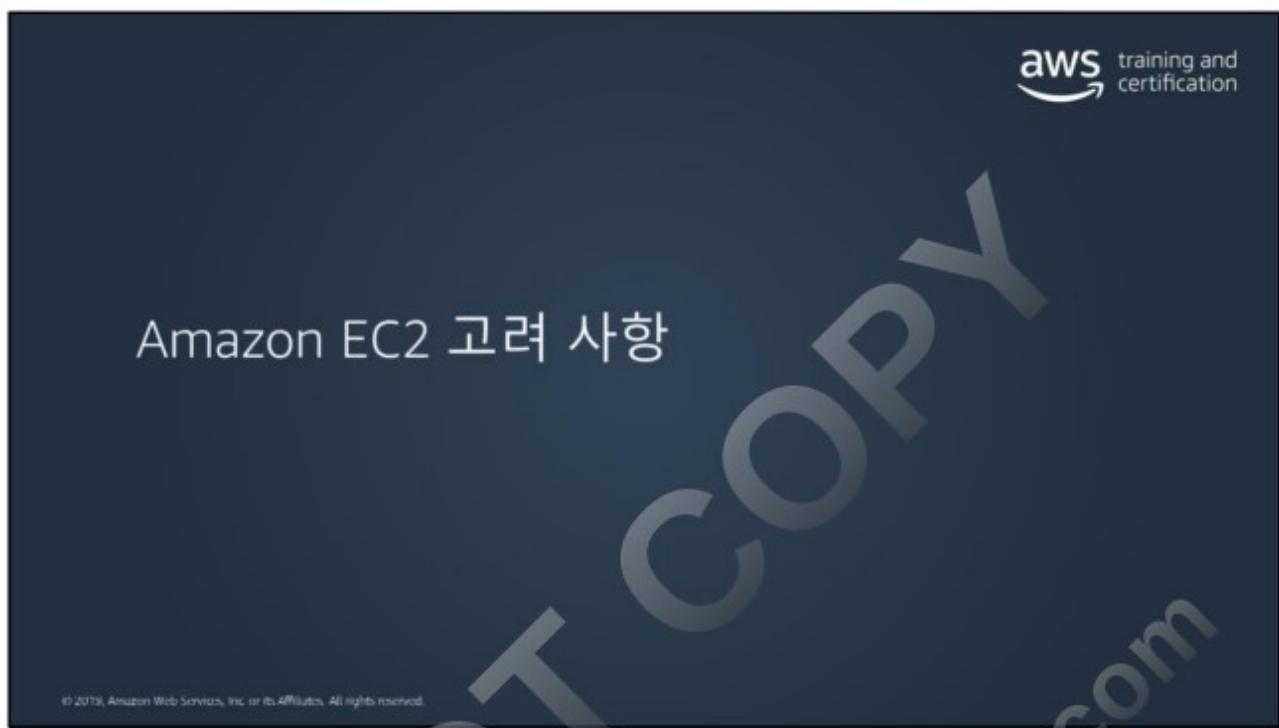
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

항상 표준화된 대/소문자 구분 형식의 태그를 사용하고 모든 리소스 유형에 일관적으로 태그를 구현합니다.
액세스 제어, 비용 추적, 자동화 및 조직을 관리하는 기능을 지원하는 태그 차원을 고려합니다.

리소스 태그를 관리하는 데 도움이 되는 자동화된 도구를 구현합니다. [Resource Groups Tagging API](#)를 사용하면 프로그래밍 방식으로 태그를 제어할 수 있어 자동으로 태그 및 리소스를 관리, 검색 및 필터링하기가 더 쉬워집니다. 또한 AWS 리전당 한 번의 API 호출을 사용하여 모든 지원 대상 서비스에 대한 태그 데이터 백업을 간소화합니다.

너무 많은 태그를 사용하는 것이 너무 적은 태그를 사용하는 것보다 낫습니다.

참고로 변화하는 비즈니스 요구 사항을 수용하기 위해 태그를 수정하는 것은 간단합니다. 하지만 향후의, 특히 태그 기반 액세스 제어, 자동화 또는 업스트림 결제 보고서와 관련한 변경의 영향을 고려해야 합니다.

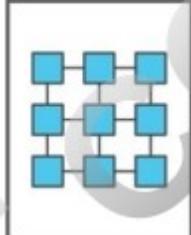


아키텍처 고려 사항 1

aws training and certification

컴퓨팅 계층이 가능한 한 가장 짧은 지연 시간 및 가장 높은 초당 패킷 네트워크 성능을 요구합니까?

클러스터 배치 그룹



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

클러스터 배치 그룹은 단일 가용 영역 내에 있는 인스턴스의 논리적 그룹입니다. 이 그룹은 가장 짧은 지연 시간과 가장 높은 초당 패킷 네트워크 성능을 제공합니다.

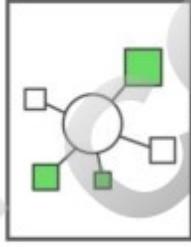
이 그룹에 필요한 모든 인스턴스를 동시에 시작하는 것이 좋습니다. 나중에 더 많은 인스턴스를 그룹에 추가하려할 경우 용량 부족 오류가 나타날 가능성이 커집니다.

아키텍처 고려 사항 2

aws training and certification

애플리케이션에 서로 분리되어야 하는 소수의 크리티컬 인스턴스가 있습니까?

분산형 배치 그룹



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

분산형 배치 그룹은 의도적으로 다른 기본 하드웨어에 배치되는 인스턴스의 그룹입니다. 이 그룹은 인스턴스가 기본 하드웨어를 공유할 경우 발생할 수 있는 동시 장애의 위험을 줄여 줍니다.

이 유형의 그룹은 여러 가용 영역을 포괄할 수 있으며, 그룹 별로 가용 영역당 최대 7개의 인스턴스가 가능합니다.

아키텍처 고려 사항 3

HDFS, HBase, Cassandra 같은 대규모의 분산 및 복제 워크로드가 EC2에서 실행되고 있습니까?

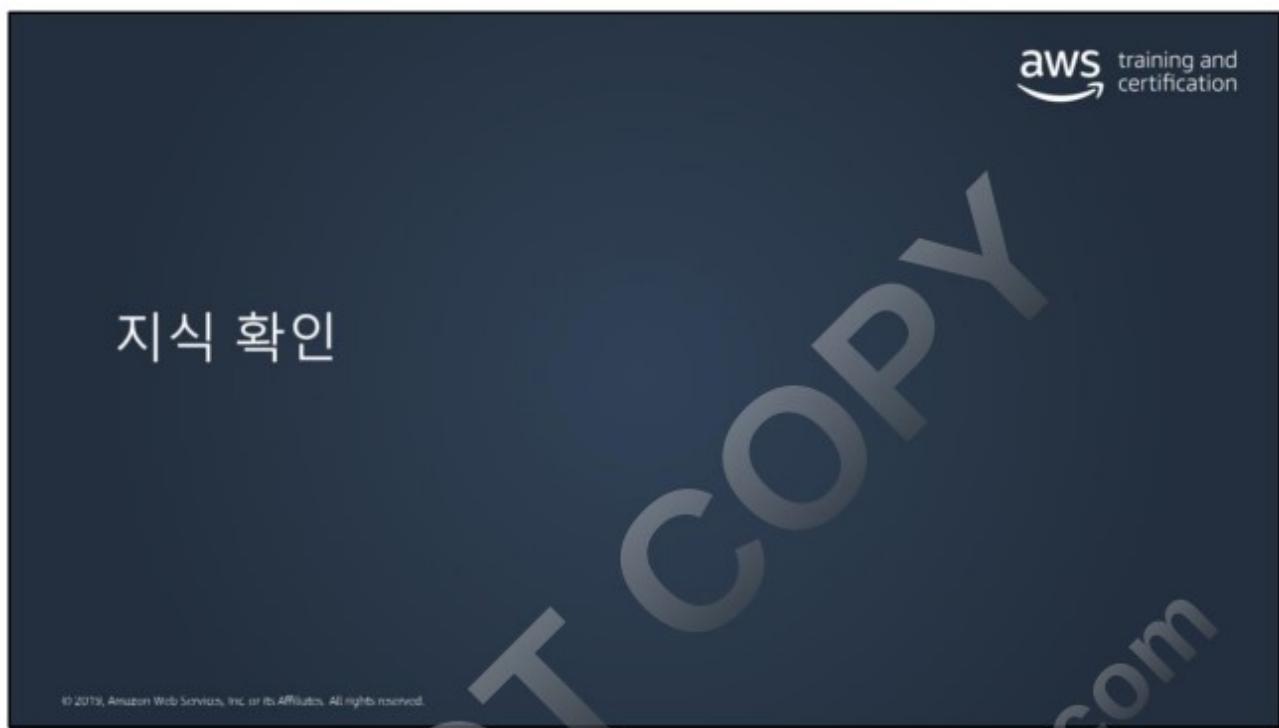
파티션 배치 그룹



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

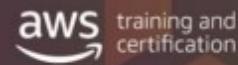
파티션 배치 그룹은 EC2 인스턴스를 논리적 파티션에 분산하여 서로 다른 파티션의 인스턴스가 동일한 기본 하드웨어를 공유하지 않도록 함으로써 하드웨어 장애의 영향을 단일 파티션으로 억제합니다.

또한 파티션 배치 그룹은 파티션에 대한 가시성을 제공하고 토플로지 인식 애플리케이션이 이 정보를 사용하여 지능형 데이터 복제 결정을 내릴 수 있도록 함으로써 데이터 가용성 및 내구성을 높입니다.



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

지식 확인 4



AMI란 무엇입니까?



1. AMI는 로컬 호스트 이름, 인스턴스 ID, 퍼블릭 IP 주소 등 인스턴스에 대한 데이터를 저장하는 객체입니다.
2. AMI는 인스턴스 종료 시 사라지는 블록 수준 스토리지를 제공합니다.
3. AMI는 새로운 EC2 인스턴스를 생성할 때 사용되며 루트 볼륨에 대한 템플릿을 포함합니다.
4. Amazon S3용 스토리지 버킷의 한 유형입니다.

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

지식 확인 4: 정답



AMI란 무엇입니까?



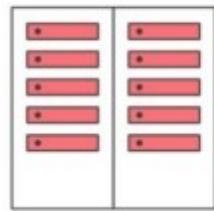
1. AMI는 로컬 호스트 이름, 인스턴스 ID, 퍼블릭 IP 주소 등 인스턴스에 대한 데이터를 저장하는 객체입니다.
2. AMI는 인스턴스 종료 시 사라지는 블록 수준 스토리지를 제공합니다.
3. AMI는 새로운 EC2 인스턴스를 생성할 때 사용되며 루트 볼륨에 대한 템플릿을 포함합니다.
4. Amazon S3용 스토리지 버킷의 한 유형입니다.

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

지식 확인 5



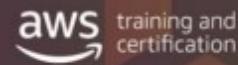
인스턴스가 실행될 호스트를 선택하는 경우, 어떤 옵션을 사용해야 합니까?



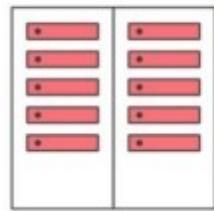
1. 기본값
2. 전용 인스턴스
3. 전용 호스트

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

지식 확인 5: 정답



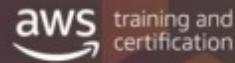
인스턴스가 실행될 호스트를 선택하는 경우, 어떤 옵션을 사용해야 합니까?



1. 기본값
2. 전용 인스턴스
3. **전용 호스트**

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

지식 확인 6



Amazon EBS란 무엇입니까?



- 수요 및 스토리지 요구 사항을 충족하기 위해 놀라운 크기로 확장될 수 있는 객체 스토리지 솔루션입니다.
- 동시에 여러 개의 인스턴스에 연결될 수 있는 블록 스토리지 디바이스입니다.
- 동시에 여러 개의 인스턴스에 연결될 수 있는 파일 스토리지 시스템입니다.
- 한 번에 한 개의 인스턴스에 연결되는 블록 스토리지 디바이스. Amazon S3에 백업할 수 있습니다.

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

지식 확인 6: 정답



Amazon EBS란 무엇입니까?



- 수요 및 스토리지 요구 사항을 충족하기 위해 놀라운 크기로 확장될 수 있는 객체 스토리지 솔루션입니다.
- 동시에 여러 개의 인스턴스에 연결될 수 있는 블록 스토리지 디바이스입니다.
- 동시에 여러 개의 인스턴스에 연결될 수 있는 파일 스토리지 시스템입니다.
- 한 번에 한 개의 인스턴스에 연결되는 블록 스토리지 디바이스. Amazon S3에 백업할 수 있습니다.

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

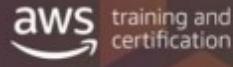






수업이 끝나면 이 아키텍처 디어그램의 모든 구성 요소를 이해할 수 있습니다.
또한 마찬가지로 규모가 크고 강력한 자체 아키텍처 솔루션을 구축할 수 있습니다.

모듈 4



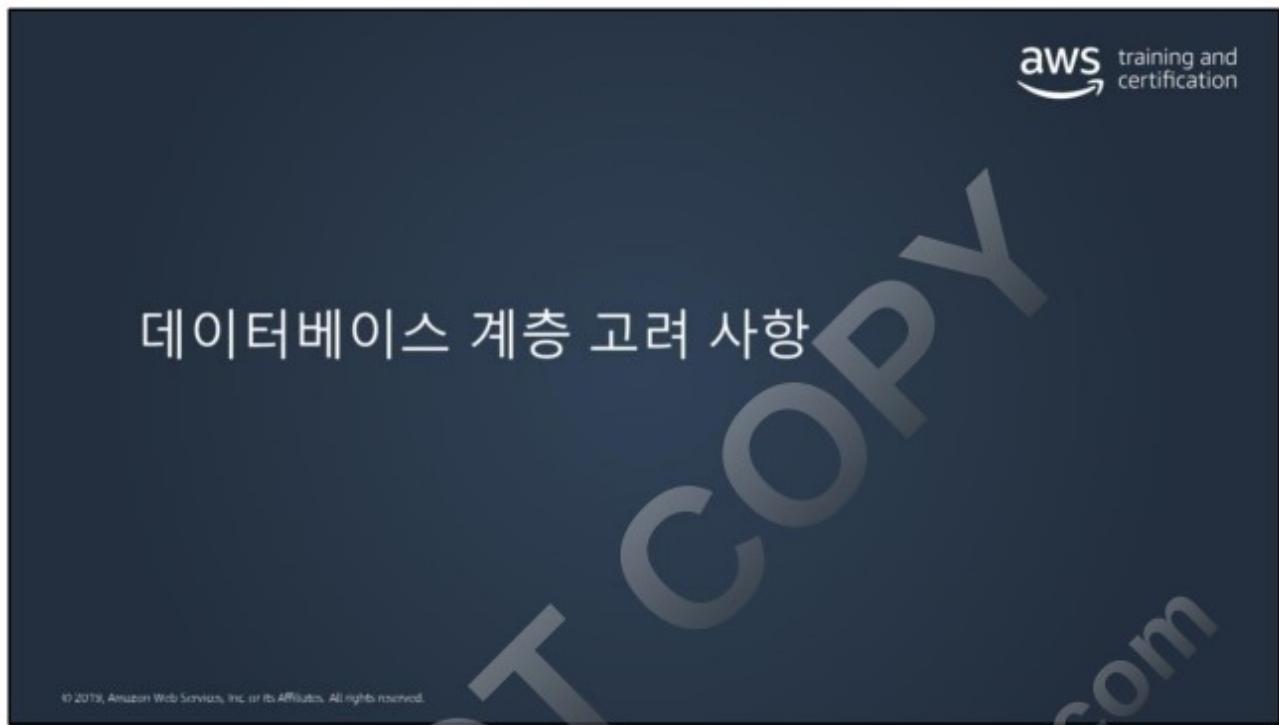
아키텍처 측면에서의 필요성

고가용성이고 확장이 용이하며 애플리케이션 서버와 분리된 데이터베이스가 필요합니다.

모듈 개요

- 데이터베이스 유형 비교
- 관리형 서비스와 비관리형 서비스
- Amazon Relational Database Service (Amazon RDS) 및 Amazon DynamoDB

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



고려할 사항

aws training and certification

The diagram illustrates factors to consider when scaling a database system. On the left, four icons represent different aspects: a double-headed arrow for '확장성' (Scalability), a briefcase for '총 스토리지 요구 사항' (Total storage requirements), a bar chart for '객체 크기 및 유형' (Object size and type), and a stack of coins with a lock for '내구성' (Durability). To the right, a large blue double-headed arrow indicates the need to consider both increasing (upward) and decreasing (downward) data volumes, along with the question: '얼마나 많은 처리량이 필요한가? 선택한 솔루션이 필요할 경우 나중에 확장이 가능한가?' (How much processing power is needed? Is the chosen solution scalable for future needs?).

확장성

총 스토리지 요구 사항

객체 크기 및 유형

내구성

얼마나 많은 처리량이 필요한가?
선택한 솔루션이 필요할 경우 나중에
확장이 가능한가?

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

고려할 사항

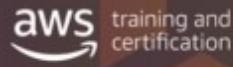
aws training and certification

- 확장성
- 총 스토리지 요구 사항
- 객체 크기 및 유형
- 내구성

데이터베이스가 얼마나 커야 하는가?
데이터가 GB, TB 또는 PB 규모인가?

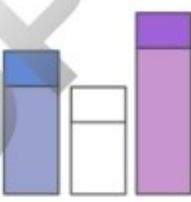
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

고려할 사항



확장성
총 스토리지 요구 사항
객체 크기 및 유형
내구성

단순 데이터 구조, 대용량 데이터 객체, 또는 모두를 저장해야 하는가?



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

고려할 사항

aws training and certification

확장성

총 스토리지 요구 사항

객체 크기 및 유형

내구성

어떤 수준의 데이터 내구성, 데이터 가용성 및
복구성이 필요한가?
관련 규제 의무가 있는가?

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

데이터베이스 유형

aws training and certification

아키텍처에 대해 두 가지 유형의 데이터베이스 옵션을 사용할 수 있습니다.

관계형

기존 예:

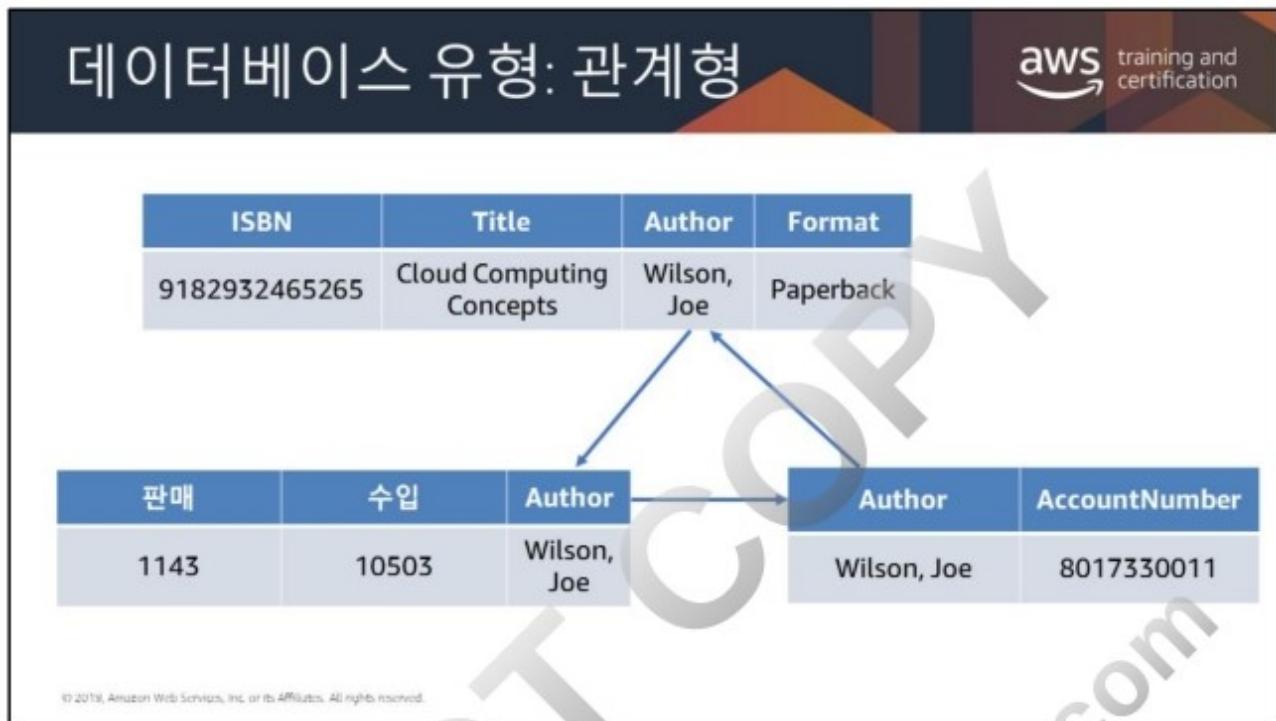
Microsoft SQL Server
Oracle Database,
MySQL

비관계형

기존 예:

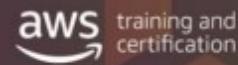
MongoDB
Cassandra
Redis

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



SQL 데이터베이스는 데이터를 행과 열에 저장합니다. 행은 하나의 항목에 대한 모든 정보를 포함하고, 열은 데이터 요소를 분리하는 속성을 포함합니다. SQL 데이터베이스 스키마는 고정되어 있으며, 열은 데이터 입력 전에 잠겨 있어야 합니다. 데이터베이스가 전체적으로 변경되고 오프라인인 경우, 스키마를 수정할 수 있습니다. SQL 데이터베이스의 데이터는 복잡한 쿼리가 가능한 SQL (Structure Query Language)을 사용하여 쿼리합니다. SQL 데이터베이스는 하드웨어 성능을 높이는 방법으로 수직적으로 확장합니다.

데이터베이스 유형: 관계형



관계형 데이터베이스를 선택해야 할 경우:

- 엄격한 스키마 규칙 및 데이터 품질 적용이 필요
- 데이터베이스가 과도한 읽기/쓰기 용량을 필요로 하지 않음
- 최상의 성능을 필요로 하지 않는 관계형 데이터베이스의 경우 RDBMS가 자원 소비가 적은 최고의 솔루션이 될 수 있습니다.

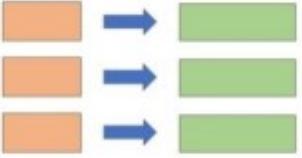
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

데이터베이스 유형: 비관계형

aws training and certification

키-값

문서



```
{  
    ISBN: 9182932465265,  
    Title: "Cloud Computing Concepts",  
    Author: "Wilson, Joe",  
    Format: "Paperback"  
}
```

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

NoSQL 데이터베이스는 키 값 페어, 문서 및 그래프를 비롯한 다양한 스토리지 모델 중 하나를 사용하여 데이터를 저장합니다. NoSQL 스키마는 동적입니다. 각 행은 각 열에 대한 데이터를 포함할 필요가 없습니다. NoSQL 데이터베이스의 데이터는 문서 수집에 집중하여 쿼리합니다. NoSQL 데이터베이스는 서버를 추가하는 방법으로 수평적으로 확장합니다.

데이터베이스 유형: 비관계형



비관계형 데이터베이스를 선택해야 할 경우:

- 데이터베이스를 수평적으로 확장해야 함
- 데이터가 기존 스키마에 적합하지 않음
- 읽기/쓰기 속도가 기존 SQL DB에서 경제적으로 지원할 수 있는 범위를 초과

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



비관리형 데이터베이스

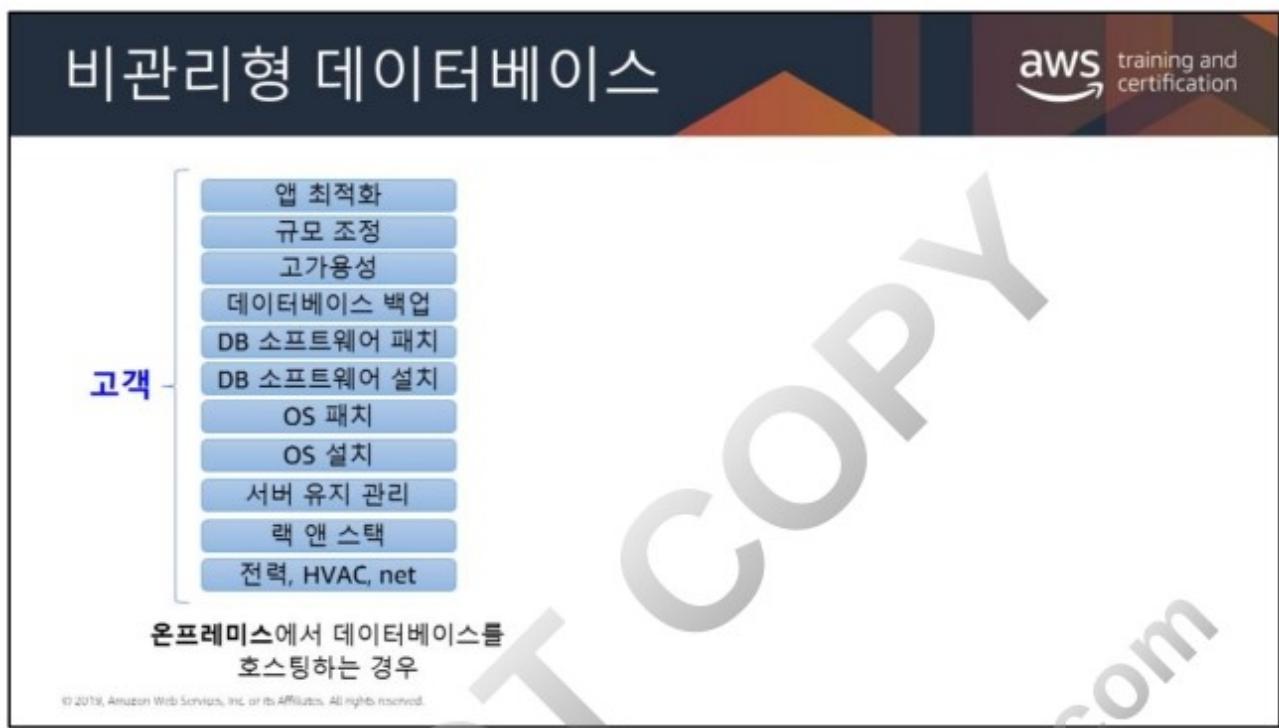
aws training and certification

고객

- 앱 최적화
- 규모 조정
- 고가용성
- 데이터베이스 백업
- DB 소프트웨어 패치
- DB 소프트웨어 설치
- OS 패치
- OS 설치
- 서버 유지 관리
- 랙 앤 스택
- 전력, HVAC, net

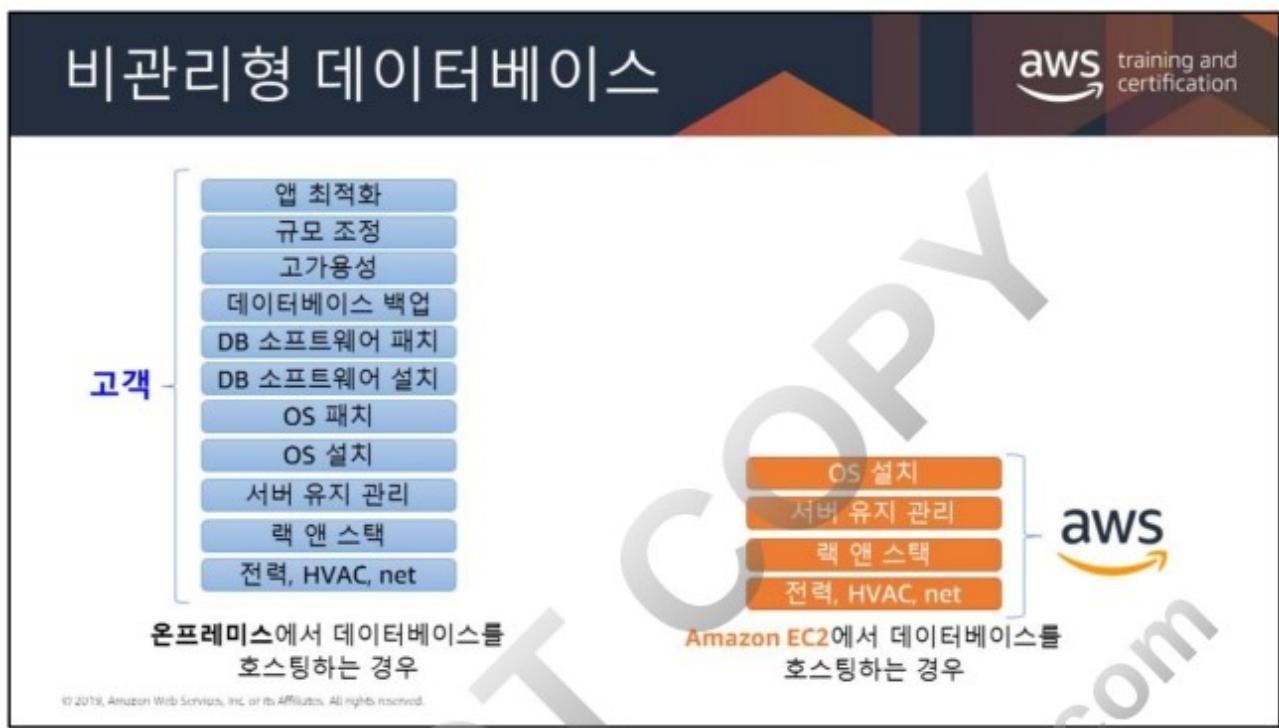
온프레미스에서 데이터베이스를
호스팅하는 경우

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

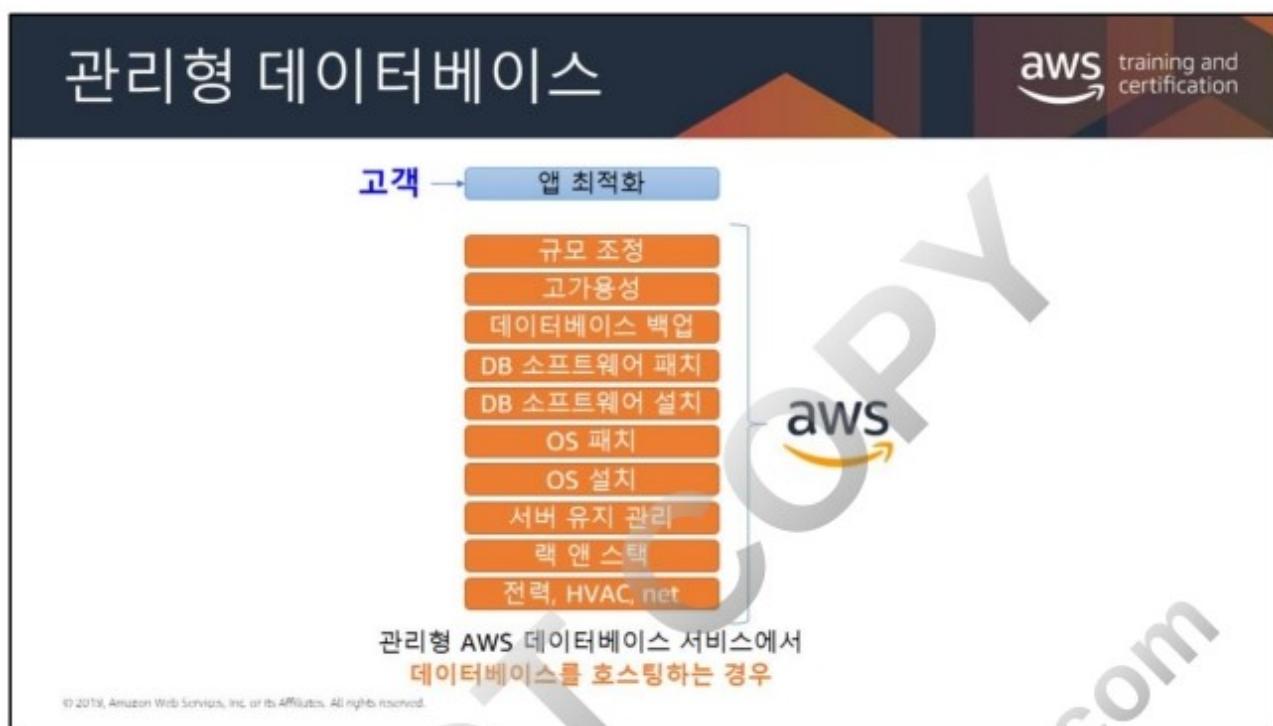


일반적으로, 사용자가 모든 보안 백업, DB 튜닝 및 복제를 책임집니다.

규정 준수 의무에 따라 애플리케이션에 대해 자체 관리형 DB 솔루션을 생성해야 할 수도 있습니다.







AWS 관리형 데이터베이스

이것들은 시스템에 고가용성, 확장성 그리고 백업을 제공합니다. 패키지들을 선택하실 수 있습니다. 사용할 것들을 선택하십시오.

규모조정, 고가용성, 데이터베이스 백업, 데이터베이스 소프트웨어 패치, 데이터베이스 소프트웨어 설치, OS 패치

반복적 업무 부담을 경감

OS 설치, 서버 유지 관리, 랙 앤 스택, 전력, HVAC, 네트워크

일반적으로 사용자는 “데이터베이스 계층이 애플리케이션과 최대한 잘 연동하도록” 앱 최적화만 책임집니다.



Amazon 데이터베이스 옵션

aws training and certification

관계형 데이터베이스


Amazon RDS


Amazon Redshift


Amazon Aurora

비관계형 데이터베이스


Amazon DynamoDB


Amazon ElastiCache


Amazon Neptune

이것은 일반적인 예일 뿐 더 많은 데이터베이스가 있습니다.

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

Amazon Relational Database Service(RDS) for Oracle은 Active Data Guard로 읽기 전용 복제본을 지원합니다. Amazon RDS for Oracle을 사용하면 Active Data Guard 구성을 완벽하게 관리하고 기본 DB 인스턴스와 해당 복제본 간에 보안 네트워크 연결을 유지 관리하여 기본 DB 인스턴스와 동일한 AWS 리전에 복제본을 손쉽게 생성할 수 있습니다.

자세한 내용은 <https://aws.amazon.com/rds/oracle/>을 참조하십시오.



Amazon RDS



관계형

Amazon RDS

완전 관리형 관계형 데이터베이스 서비스

몇 분이면 새 인스턴스를 프로비저닝

몇 번의 마우스 클릭으로 수직으로 조정

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

Amazon RDS 개요

aws training and certification

관계형



Amazon RDS

다음과 같은 애플리케이션에 적합:

-  보다 복잡한 데이터를 사용
-  데이터 세트를 결합하고 연결해야 함
-  구문 규칙을 적용해야 함

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

실수에 의한 데이터 삭제를 방지하기 위해 Amazon Relational Database Service (RDS)는 데이터베이스 삭제 후 자동 백업 보존을 지원합니다. 실수로 데이터 손실이 발생하는 상황에서는 보존된 백업에 정의된 특정 시점으로 Amazon RDS 인스턴스를 복원할 수 있습니다. 보존된 자동 백업은 삭제된 데이터베이스에 지정된 수명 주기 정책을 준수합니다. 자동 백업은 지정된 보존 기간이 지나면 삭제되기 때문에 오래된 백업을 수동으로 삭제할 필요가 없습니다. 이 기능은 MySQL, MariaDB, PostgreSQL, Oracle 및 Microsoft SQL Server 데이터베이스 엔진에서 사용할 수 있습니다.

Amazon RDS 및 Amazon Aurora

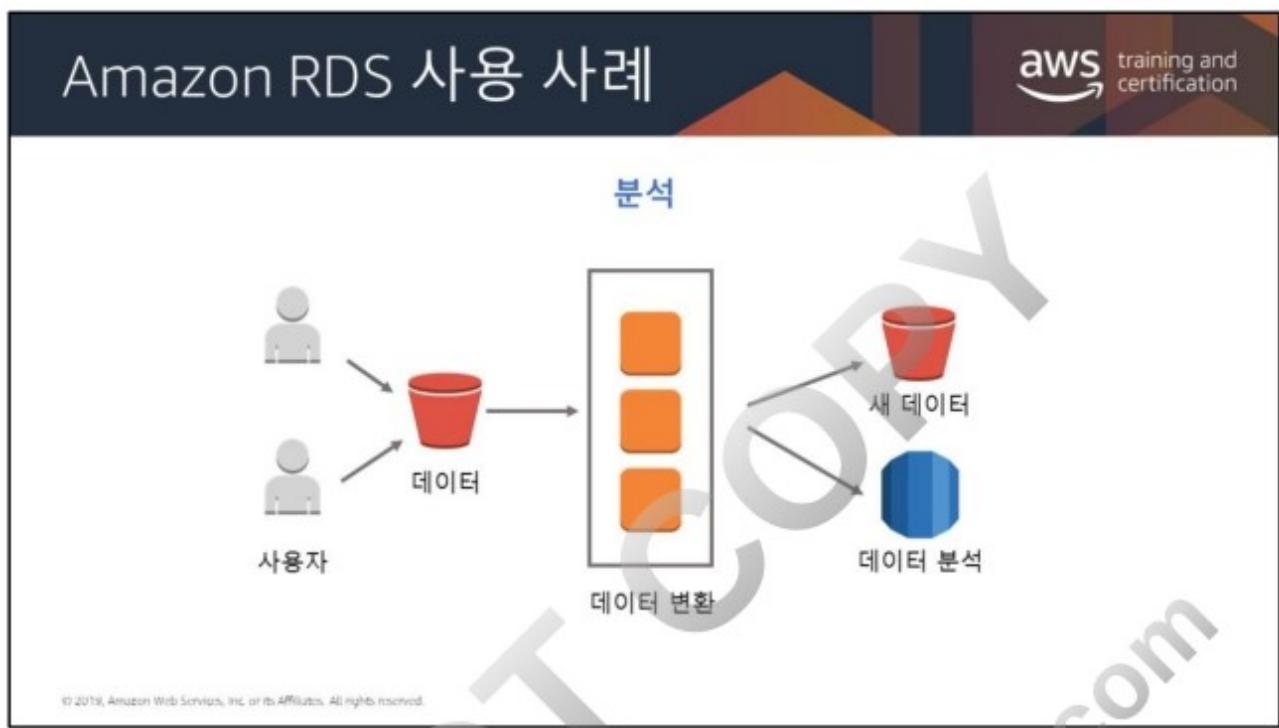


Amazon Aurora는 MySQL 및 PostgreSQL과 호환되는 완전 관리형 관계형 데이터베이스 엔진입니다.

- MySQL 처리량의 최대 5배
- PostgreSQL의 처리량의 최대 3배
- 3개의 가용 영역에 6가지 방법으로 데이터를 복제
- 기존 애플리케이션을 최소한으로 변경

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

DO NOT COPY
zlagusdbs@gmail.com



Amazon DynamoDB

aws training and certification



비관계형
Amazon
DynamoDB

완전 관리형 비관계형 데이터베이스 서비스

이벤트 중심 프로그래밍(서비스 컴퓨팅)

최상의 수평 확장 기능

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

Amazon DynamoDB는 속도가 빠른 NoSQL 데이터베이스로, 간단하고 비용 효율적인 방법으로 데이터를 저장합니다. Amazon DynamoDB의 처리량과 10밀리초 미만의 지연 시간은 게임, 광고 기술, 모바일 및 기타 다양한 애플리케이션에 매우 적합합니다. DynamoDB는 API와 사용이 쉬운 관리 콘솔을 통해 원활한 처리량과 스토리지 확장 기능을 제공하므로, 사용자의 요구에 맞게 쉽게 확장하거나 축소할 수 있습니다. 많은 AWS 고객들은 버튼 클릭 한번으로 단 몇 분 만에 DynamoDB 배포를 만들고 연간 수조 개의 데이터베이스 요청을 처리할 수 있습니다.

DynamoDB 테이블은 스키마가 고정되어 있지 않으며 각 항목마다 속성 수가 서로 다를 수 있습니다. 보조 인덱스를 추가하여 성능에 영향을 미치지 않고 수행할 수 있는 쿼리의 유연성을 높일 수 있습니다. SSD (Solid Storage Drive) 스토리지 자동 3방향 복제 기능으로 성능, 안정성 및 보안이 기본 제공됩니다. DynamoDB는 검증된 암호화 방법을 사용하여 안전하게 사용자를 인증하고 데이터에 대한 무단 액세스를 차단합니다.

Amazon DynamoDB 트랜잭션은 테이블 내, 외에서 여러 항목을 한번에 모두 수행하거나 아무것도 수행하지 않도록 조정하여 개발자 경험을 간소화합니다. 트랜잭션은 DynamoDB에서 원자성, 일관성, 격리 및 내구성(ACID)을 제공하여 애플리케이션에서 데이터의 정확성을 보다 쉽게 유지할 수 있습니다.

DynamoDB 트랜잭션 읽기 및 쓰기 API를 사용하면 여러 항목을 추가, 업데이트 또는 삭제해야 하는 복잡한 비즈니스 워크플로를 한 번에 모두 수행하거나 아무것도 수행하지 않도록 관리할 수 있습니다. 자세한 내용은 <https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/transactions.html>을 참조하십시오.

Amazon DynamoDB

aws training and certification

비관계형



Amazon
DynamoDB

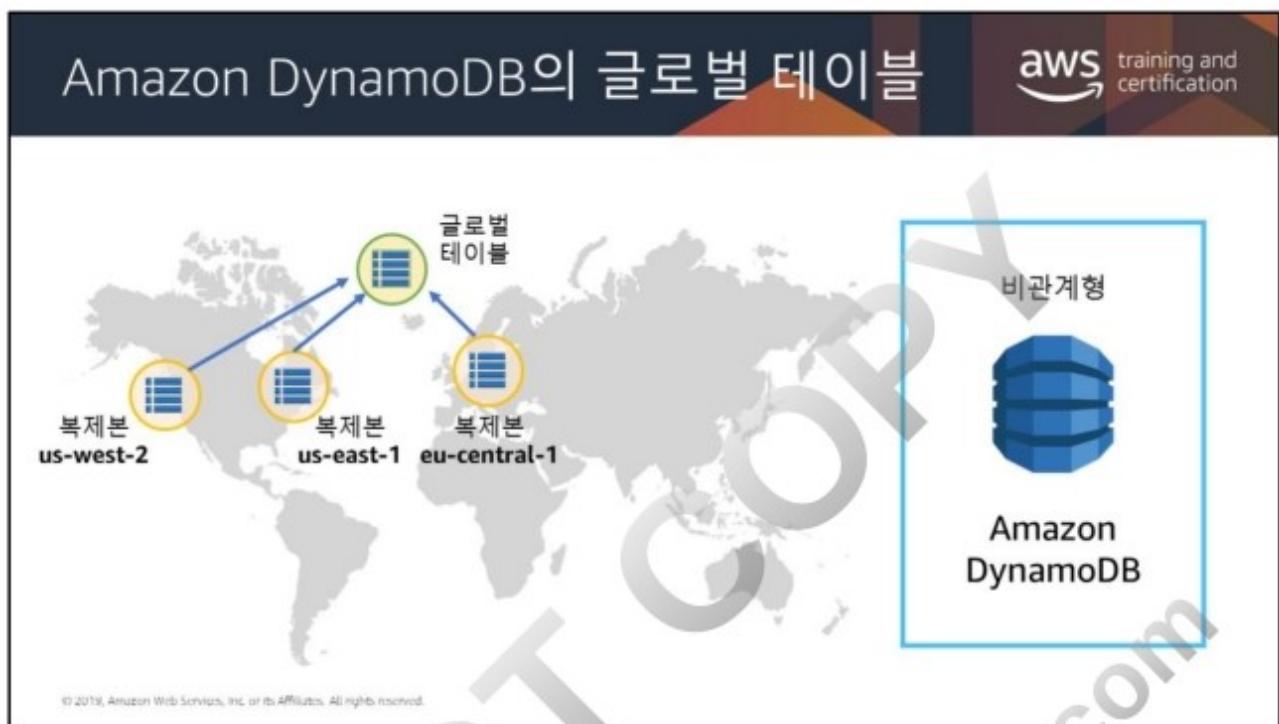
다음과 같은 애플리케이션에 적합:

-  대용량의 단순 데이터를 보유
-  신속하고 간편하게 확장해야 함
-  복잡한 조인이 필요하지 않음

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

DynamoDB 트랜잭션은 단일 AWS 계정 및 리전 내에 있는 하나 이상의 테이블에서 ACID를 제공합니다. 여러 항목에 대한 삽입, 삭제, 업데이트를 조정해야 하는 애플리케이션에 사용할 수 있습니다.

<https://aws.amazon.com/blogs/aws/new-amazon-dynamodb-transactions/>



글로벌 테이블은 단일 AWS 계정이 소유하고 복제본 테이블로 식별되는 한 개 이상의 DynamoDB 테이블의 모음입니다. 복제본 테이블(줄여서 복제본이라고도 함)은 글로벌 테이블의 일부로 기능하는 단일 DynamoDB 테이블입니다. 각 복제본에는 동일한 집합의 데이터 항목이 저장됩니다. 글로벌 테이블은 리전당 한 개의 복제본 테이블을 가질 수 있습니다. 모든 복제본은 동일한 테이블 이름과 동일한 기본 키 스키마를 갖습니다.

Amazon DynamoDB 글로벌 테이블은 복제 솔루션을 직접 구축하여 관리하지 않고도 다중 리전의 다중 마스터 데이터베이스를 만들 수 있는 종합 관리형 솔루션을 제공합니다. 글로벌 테이블을 만들 때, 테이블을 사용하기 원하는 AWS 리전을 지정해야 합니다. DynamoDB는 이러한 리전에 동일한 테이블을 만들고, 이들 모든 테이블에 대한 데이터 변경을 지속적으로 전파하기 위해 필요한 모든 작업을 수행합니다.

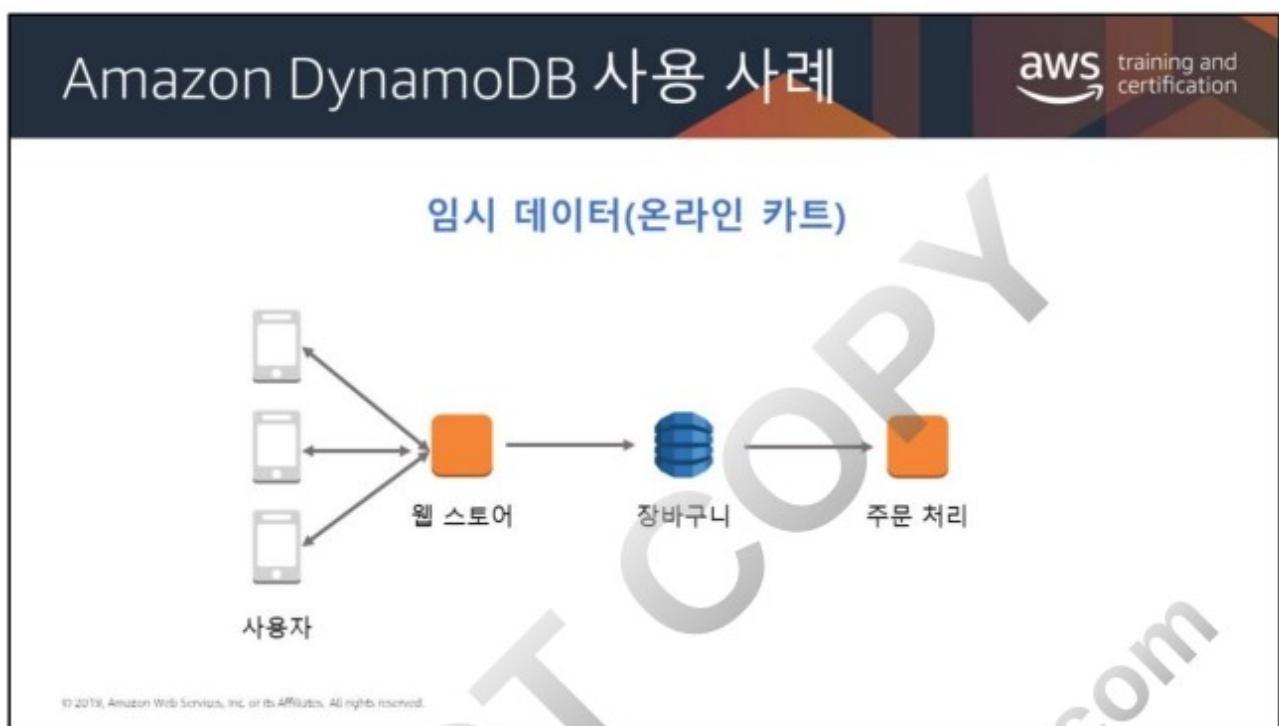
Amazon DynamoDB 사용 사례

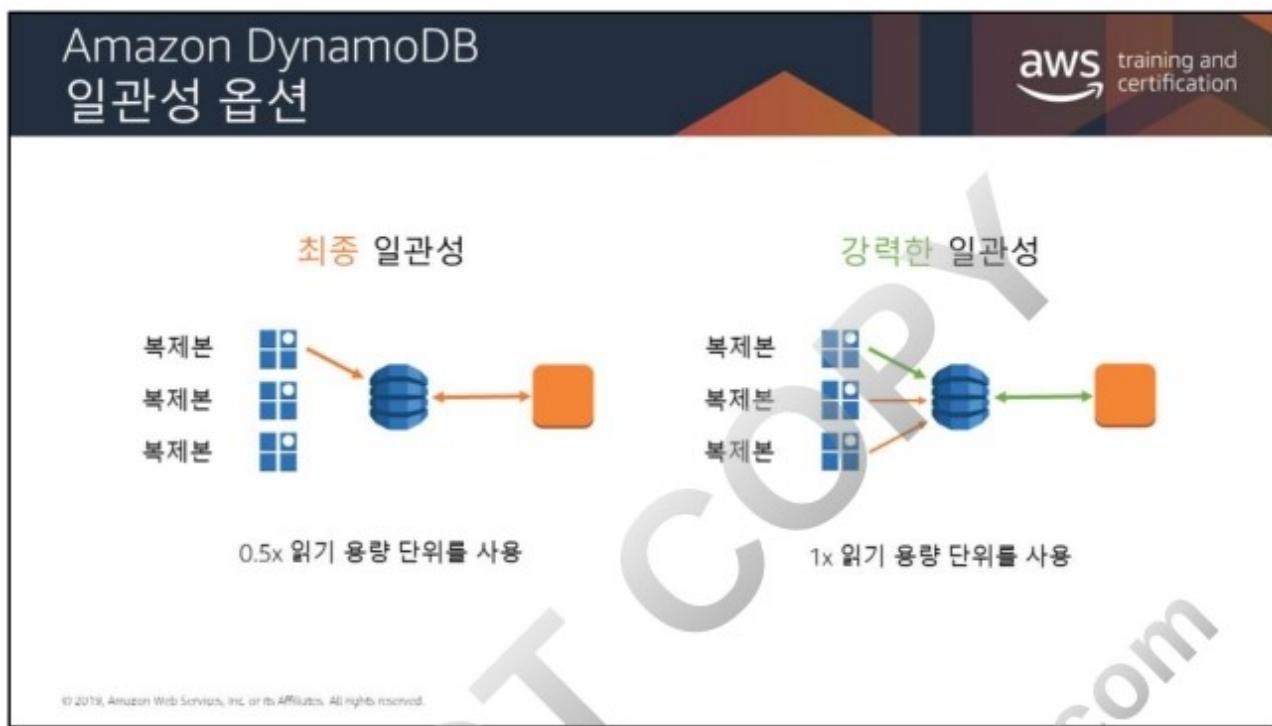
순위표 및 점수 매기기

The diagram illustrates a three-tier architecture for managing game scores. On the left, a player icon points to a stack of three orange squares representing the game server. From the game server, a double-headed arrow connects to a blue database cylinder icon labeled '순위표' (Leaderboard). To the right, a sample table titled 'GameScores' is shown, listing user IDs, game titles, top scores, and timestamps.

UserId	GameTitle	TopScore	TopScoreDateTime	승	패
"101"	"Galaxy Invaders"	5642	"2015-09-15:17:24:31"	21	72
"101"	"Meteor Blasters"	1000	"2015-10-22:23:18:01"	12	3
"101"	"Starship X"	24	"2015-08-31:13:14:21"	4	9
"102"	"Alien Adventure"	192	"2015-07-12:11:07:56"	32	192
"102"	"Galaxy Invaders"	0	"2015-09-18:07:33:42"	0	5
"103"	"Attack Ships"	3	"2015-10-19:01:13:24"	1	6
"103"	"Galaxy Invaders"	2317	"2015-09-11:06:53:00"	40	3
"103"	"Meteor Blasters"	723	"2015-10-19:01:13:24"	22	12
"103"	"Starship X"	42	"2015-07-11:06:53:00"	4	19

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





읽기 일관성은 성공적인 쓰기 또는 데이터 항목의 업데이트가 동일 항목에 대한 다음 읽기 작업에 반영되는 방법과 시기를 의미합니다. Amazon DynamoDB가 제공하는 논리에 따라 애플리케이션에서 사용자가 원하는 대로 각 읽기 요청의 일관성 특징을 지정할 수 있습니다.

최종적 일관된 읽기(Eventually Consistent Read)

DynamoDB 테이블의 데이터를 읽을 때, 응답은 최근 완료된 쓰기 작업의 결과를 반영하지 않을 수 있습니다. 응답에는 변경 전 데이터가 일부 포함될 수 있습니다. 잠시 후 읽기 요청을 반복하면 응답이 최신 데이터를 반환합니다.

강력한 일관된 읽기(Strongly Consistent Read)

강력한 일관된 읽기를 요청하면 DynamoDB는 성공한 모든 이전 쓰기 작업의 업데이트를 반영하여 가장 최신 데이터로 응답을 반환합니다. 강력한 일관된 읽기는 네트워크 지연 또는 중단이 발생한 경우에 사용이 어려울 수 있습니다.

별도로 지정하지 않는 한 DynamoDB는 최종적 일관된 읽기를 사용합니다. 읽기 작업(예: GetItem, Query, Scan)은 ConsistentRead 파라미터를 제공합니다. 이 파라미터를 true로 설정하면 DynamoDB는 작업 중에 강력한 일관된 읽기를 사용합니다.



Amazon RDS 보안 제어

aws training and certification

몇 가지 고려할 사항:

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



Amazon RDS 보안 제어

aws training and certification

몇 가지 고려할 사항:

DB 자체에 대한 액세스 – 누가 가시성을 보유하고 데이터베이스에 대한 작업을 실행할 수 있는가?

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

액세스 제어

Amazon RDS 내에서 DB 인스턴스를 처음 생성할 때, 마스터 사용자 계정을 생성합니다. 이 계정은 DB 인스턴스에 대한 액세스를 제어하기 위해 Amazon RDS 컨텍스트에서만 사용하게 됩니다. 마스터 사용자 계정은 모든 데이터베이스 권한으로 DB 인스턴스에 로그인할 수 있도록 해주는 기본 데이터베이스 사용자 계정입니다. DB 인스턴스를 만들 때 각 DB 인스턴스에 연결할 마스터 사용자 이름과 암호를 지정할 수 있습니다. DB 인스턴스를 만든 후, 마스터 사용자 자격 증명을 사용하여 데이터베이스에 연결할 수 있습니다. 나중에 추가 사용자 계정을 만들어 DB 인스턴스에 액세스할 수 있는 사용자를 제한할 수도 있습니다.

DB 보안 그룹을 통해 Amazon RDS 인스턴스에 대한 액세스를 제어할 수 있습니다. 이 보안 그룹은 Amazon EC2 보안 그룹과 유사하지만 서로 호환되지는 않습니다. DB 보안 그룹은 DB 인스턴스에 대한 네트워크 액세스를 제어하는 방화벽처럼 작동합니다. 데이터베이스 보안 그룹 기본값은 "모두 거부" 액세스 모드입니다. 따라서 고객이 네트워크 수신을 명시적으로 승인해야만 합니다. 이를 위한 두 가지 방법은 일정한 네트워크 IP 범위를 승인하거나 기존 Amazon EC2 보안 그룹을 승인하는 것입니다. DB 보안 그룹은 데이터베이스 서버 포트에 대한 액세스만을 허용하고(다른 모든 것은 차단), Amazon RDS DB 인스턴스를 다시

시작하지 않고도 업데이트될 수 있습니다. 이로써 고객은 데이터베이스에 대한 액세스를 원활하게 제어할 수 있습니다. AWS IAM을 이용해 RDS DB 인스턴스에 대한 액세스를 추가로 통제할 수 있습니다. AWS IAM을 사용하면 개별 AWS IAM 사용자가 호출할 권한이 있는 RDS 작업을 제어할 수 있습니다.

DO NOT COPY
zlagusdbs@gmail.com

Amazon RDS 보안 제어

aws training and certification

몇 가지 고려할 사항:

DB 자체에 대한 액세스 – 누가 가시성을 보유하고 데이터베이스에 대한 작업을 실행할 수 있는가?

저장 시 암호화 – 저장 시 암호화되는 데이터에는 DB 인스턴스에 대한 기본 스토리지, 자동 백업, 읽기 전용 복제본, 스냅샷이 포함됩니다.

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

저장 시 암호화

저장된 Amazon RDS DB 인스턴스 및 스냅샷을 암호화할 수 있습니다. 암호화가 활성화되면, 인스턴스의 자동 백업, 읽기 전용 복제본 및 스냅샷이 AES-256을 사용해 암호화됩니다. 그런 다음 Amazon RDS는 데이터베이스 클라이언트 애플리케이션을 변경할 필요 없이 성능에 대한 영향을 최소화하여 해당 데이터에 대한 액세스 및 복호화 인증을 처리합니다. 이러한 암호화는 MySQL, PostgreSQL, Oracle 및 SQL Server용 Amazon RDS DB 인스턴스에서 제공되며, AWS GovCloud (us-gov-west-1) 리전에 있는 DB 인스턴스에서는 제공되지 않습니다.

Amazon RDS 보안 제어

aws training and certification

몇 가지 고려할 사항:

DB 자체에 대한 액세스 – 누가 가시성을 보유하고 데이터베이스에 대한 작업을 실행할 수 있는가?

저장 시 암호화 – 저장 시 암호화되는 데이터에는 DB 인스턴스에 대한 기본 스토리지, 자동 백업, 읽기 전용 복제본, 스냅샷이 포함됩니다.

전송 중 암호화 – 전송 중 암호화는 SSL을 사용하여 수행할 수 있습니다.

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

전송 중 암호화

SSL을 사용하여 애플리케이션과 DB 인스턴스 사이의 연결을 암호화할 수 있습니다. MySQL 및 SQL Server의 경우, RDS는 SSL 인증서를 생성하고 이 인증서를 인스턴스가 프로비저닝되면 DB 인스턴스에 설치합니다. MySQL의 경우, 연결을 암호화하기 위해 --ssl_ca 파라미터를 사용해 MySQL 클라이언트를 시작하고 퍼블릭 키를 참조합니다. SQL 서버의 경우, 퍼블릭 키를 다운로드하고 인증서를 Windows 운영 체제로 가져옵니다. Oracle RDS는 DB 인스턴스에 Oracle 기본 네트워크 암호화를 사용합니다. 기본 네트워크 암호화 옵션을 옵션 그룹에 추가한 다음, 해당 옵션 그룹을 DB 인스턴스와 연결하기만 하면 됩니다.

암호화된 연결이 설정되면, DB 인스턴스와 애플리케이션 간에 전송되는 데이터는 전송 중에 암호화됩니다. 암호화된 연결만 허용하도록 DB 인스턴스를 구성할 수 있습니다. Amazon RDS에서의 SSL 지원은 애플리케이션과 DB 인스턴스 간의 연결을 암호화하는 데 사용됩니다. 따라서 이 지원을 통해 DB 인스턴스 자체를 인증할 수 없습니다. SSL은 보안상 장점이 있지만, SSL 암호화는 컴퓨팅 집약적 작업이며 데이터베이스 연결의 지연 시간을 늘린다는 점에 유의해야 합니다.

Amazon RDS 보안 제어

aws training and certification

몇 가지 고려할 사항:

- DB 자체에 대한 액세스** – 누가 가시성을 보유하고 데이터베이스에 대한 작업을 실행할 수 있는가?
- 저장 시 암호화** – 저장 시 암호화되는 데이터에는 DB 인스턴스에 대한 기본 스토리지, 자동 백업, 읽기 전용 복제본, 스냅샷이 포함됩니다.
- 전송 중 암호화** – 전송 중 암호화는 SSL을 사용하여 수행할 수 있습니다.
- 이벤트 알림** – Amazon RDS 인스턴스에서 발생할 수 있는 다양한 중요 이벤트에 대한 알림을 받을 수 있습니다.

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

이벤트 알림

RDS 인스턴스에서 발생할 수 있는 다양한 중요 이벤트의 알림을 수신할 수 있습니다. 이벤트의 예로 인스턴스가 종료되었는지, 백업이 시작되었는지, 장애 조치가 수행되었는지, 보안 그룹이 변경되었는지 또는 스토리지 공간에 여유가 없는지 등을 들 수 있습니다. Amazon RDS는 구독 가능한 범주로 이벤트를 그룹화합니다. 따라서 해당 범주의 이벤트가 발생했을 때 이에 대한 알림을 받을 수 있습니다. 구독 가능한 이벤트 범주로는 DB 인스턴스, DB 스냅샷, DB 보안 그룹 또는 DB 파라미터 그룹 등이 있습니다. Amazon RDS 이벤트는 Amazon SNS를 통해 게시되며, 이메일이나 텍스트 메시지로 전송됩니다.

DynamoDB 보안 제어

aws training and certification

몇 가지 고려할 사항:

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

DO NOT COPY
zlagusdbs@gmail.com

DynamoDB 보안 제어

aws training and certification

몇 가지 고려할 사항:

정의 가능한 액세스 권한 – DynamoDB에서는 데이터베이스의 테이블에서 항목, 심지어 속성까지 모든 것에 대해 액세스 권한을 부여할 수 있습니다.

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

DynamoDB 보안 제어

aws training and certification

몇 가지 고려할 사항:

정의 가능한 액세스 권한 – DynamoDB에서는 데이터베이스의 테이블에서 항목, 심지어 속성까지 모든 것에 대해 액세스 권한을 부여할 수 있습니다.

저장 시 암호화 – DynamoDB는 완전 관리형 저장 암호화 기능을 제공합니다.

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

DynamoDB 보안 제어

aws training and certification

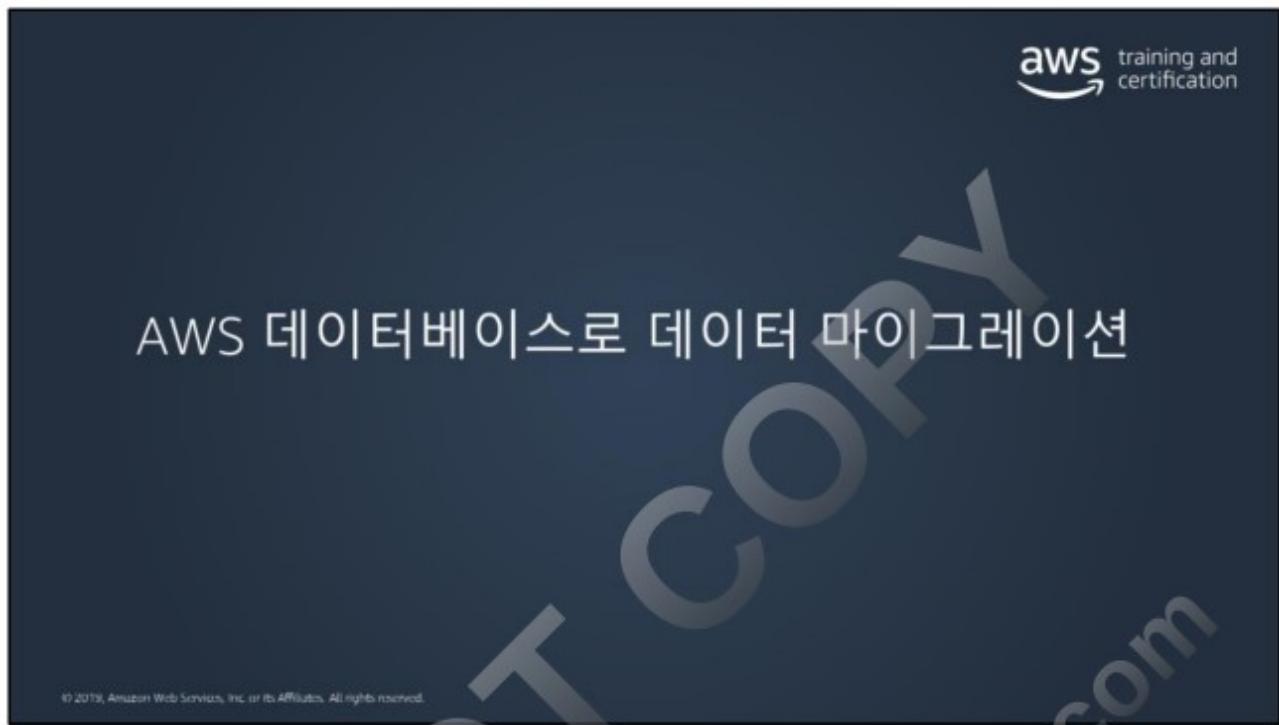
몇 가지 고려할 사항:

정의 가능한 액세스 권한 – DynamoDB에서는 데이터베이스의 테이블에서 항목, 심지어 속성까지 모든 것에 대해 액세스 권한을 부여할 수 있습니다.

저장 시 암호화 – DynamoDB는 완전 관리형 저장 암호화 기능을 제공합니다.

SSL/TLS – 기본적으로 DynamoDB와의 통신은 SSL/TLS 암호화를 사용하여 네트워크 트래픽을 보호하는 HTTPS 프로토콜을 사용합니다.

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



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

The screenshot shows the AWS DMS landing page. At the top left is the title "AWS Database Migration Service (AWS DMS)". To the right is the "aws training and certification" logo. Below the title is a large blue icon of a database migration symbol (two interlocking gears). To the right of the icon is the text "대부분의 상용 및 오픈 소스 데이터베이스와의 마이그레이션을 지원합니다." (Supports migration to most commercial and open-source databases). Further down is another section with the text "Amazon EC2, Amazon RDS, Amazon S3 및 온프레미스의 데이터베이스 간 마이그레이션에 사용할 수 있습니다." (Can be used for migration between databases in Amazon EC2, Amazon RDS, Amazon S3, and on-premises). A watermark "zlagu.com" is diagonally across the page.

AWS Database Migration Service (AWS DMS)

aws training and certification

대부분의 상용 및 오픈 소스 데이터베이스와의
마이그레이션을 지원합니다.

Amazon EC2, Amazon RDS, Amazon S3 및
온프레미스의 데이터베이스 간 마이그레이션에
사용할 수 있습니다.

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

Amazon DMS는 가장 광범위하게 사용되는 데이터베이스(Oracle, PostgreSQL, Microsoft SQL Server, Amazon Redshift, Amazon Aurora, MariaDB 및 MySQL) 간 마이그레이션을 지원합니다. 또한 동종(동일한 엔진) 및 이종(서로 다른 엔진) 마이그레이션을 지원합니다.

이 서비스는 Amazon EC2, Amazon RDS 및 온프레미스의 데이터베이스 간 마이그레이션에 사용할 수 있습니다.

- 여기에는 Amazon EC2 또는 RDS 데이터베이스로부터 온프레미스로의 마이그레이션이 포함됩니다.
- 대상 또는 원본 데이터베이스 중 하나가 Amazon EC2에 있어야 합니다(두 개의 온프레미스 데이터베이스 간 마이그레이션은 지원 안 됨).

대상 데이터베이스에서 사용할 수 있도록 원본 데이터의 형식을 자동으로 처리합니다.

스키마나 코드는 변환하지 않습니다.

- 동종 마이그레이션의 경우 기본 도구를 사용하여 이러한 변환을 수행할 수 있습니다.
- 이종 마이그레이션의 경우 **AWS Schema Conversion Tool**을 사용할 수 있습니다.

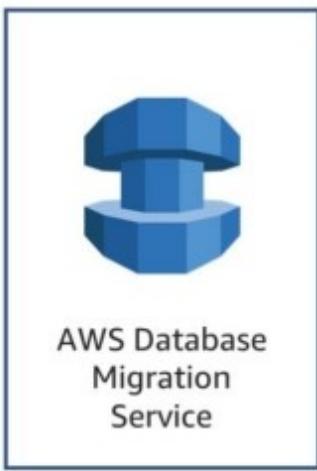
자세한 내용은 다음을 참조하십시오.

<http://docs.aws.amazon.com/dms/latest/userguide>Welcome.html>.

DO NOT COPY
zlagusdbs@gmail.com



AWS Snowball Edge 및 AWS DMS를 사용



AWS Database Migration Service

데이터 마이그레이션이 힘든 경우:

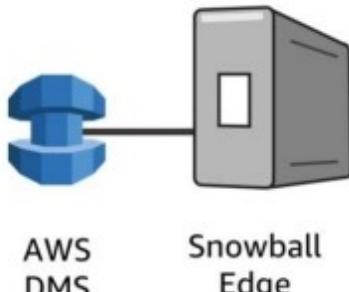
- 데이터베이스가 너무 큼
- 연결이 너무 느림
- 개인정보 보호 및 보안 문제

AWS Snowball Edge를 권장



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

AWS Snowball Edge 및 AWS DMS를 사용



The diagram illustrates the integration between AWS DMS and AWS Snowball Edge. On the left, a blue hexagonal icon represents AWS DMS, connected by a line to a grey rectangular icon representing the Snowball Edge device. Below the icons, the text 'AWS DMS' and 'Snowball Edge' is written respectively.

AWS DMS에는 Snowball Edge 통합 포인트가 있습니다.

Snowball Edge 디바이스를 사용하여 하나 이상의 데이터베이스를 마이그레이션할 수 있습니다.

- 멀티 테라바이트 스토리지
- 인터넷 또는 DX 대역폭을 사용하지 않음

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

외부에서 포트를 여는 것이 아니라 데이터 센터 내부에서 직접 안전하고 견고한 디바이스를 물리적으로 연결할 수 있습니다.

이제 매우 큰 데이터베이스를 온프레미스에서 AWS 클라우드로 이전할 수 있습니다.

이 통합은 "pull" 모델이 아니라 "push" 모델을 통한 데이터베이스를 마이그레이션합니다.

네트워크 인프라를 업그레이드하고 전용 대역폭을 사용할 필요 없이 동일한 AWS Snowball Edge 디바이스를 사용하여 하나 이상의 데이터베이스를 마이그레이션할 수 있습니다.

이러한 멀티 테라바이트 또는 멀티 페타바이트 데이터베이스를 AWS로 마이그레이션하는 동안 온프레미스 데이터베이스가 온라인 상태로 유지됩니다. AWS Snowball Edge 어플라이언스가 AWS로 반송되어 자동으로 대상 Amazon RDS 또는 Amazon EC2 기반 데이터베이스로 로드되면 온프레미스 데이터베이스를 폐기할 수 있습니다.

기존 데이터를 마이그레이션하거나(일회성) 선택적으로 대상 데이터베이스로 지속적 데이터 복제를 수행할 수 있습니다.

AWS Snowball Edge 및 AWS DMS 작업에 대한 몇 가지 참고 사항:

- AWS DMS를 통합하는 데 필요한 AWS Snowball의 버전은 [AWS Snowball Edge](#)입니다.
- 현재, AWS DMS Snowball 에이전트를 실행하려면 Linux 호스트가 필요합니다.
- AWS Snowball Edge가 원본 데이터베이스와 동일한 네트워크에 있어야 합니다.

DO NOT COPY
zlagusdbs@gmail.com

AWS Schema Conversion Tool

aws training and certification

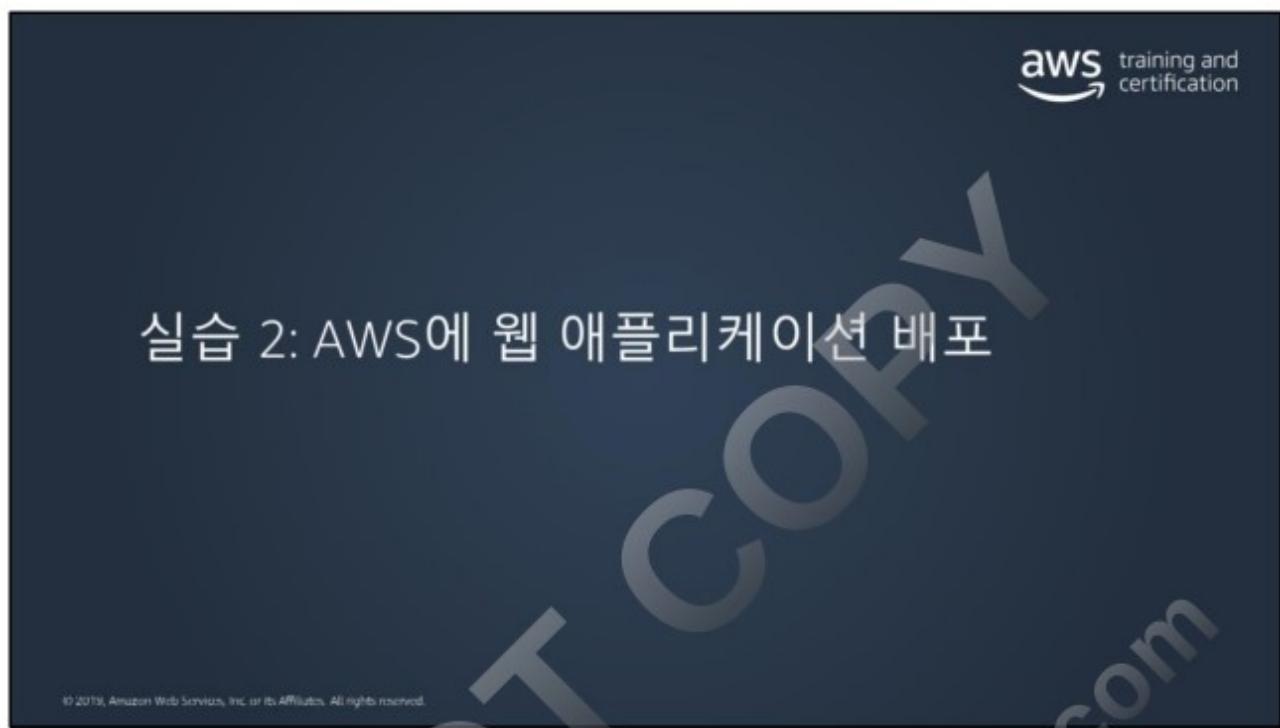
사용자가 기존 데이터베이스 스키마를 한 데이터베이스 엔진에서 다른 데이터베이스 엔진으로 변환하도록 해주는 독립형 애플리케이션입니다.

원본 데이터베이스	대상 데이터베이스
Microsoft SQL Server	Amazon Aurora, MySQL, PostgreSQL
MySQL	PostgreSQL
Oracle	Amazon Aurora, MySQL, PostgreSQL
Oracle 데이터 웨어하우스	Amazon Redshift
PostgreSQL	Amazon Aurora, MySQL
Teradata	Amazon Redshift

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

AWS Schema Conversion Tool에 대한 자세한 내용은

<http://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/Welcome.html>
을 참조하십시오.



실습 2: AWS에 웹 애플리케이션 배포



"웹 애플리케이션과 데이터베이스를 호스팅하려고 합니다."

사용된 기술:

- Amazon EC2
- Amazon RDS
- 보안 그룹

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

실습 2: AWS에 웹 애플리케이션 배포

aws training and certification

실습 시작 시 제공됨:

- 2개의 가용영역에 걸친 VPC
- 2개의 퍼블릭 서브넷
- 2개의 프라이빗 서브넷

The diagram illustrates a Lab VPC structure. At the top, a cloud icon labeled "VPC" contains two separate sections, each representing an "Availability Zone". Each zone contains a "Public Subnet" (10.0.0.0/24) and a "Private Subnet" (10.0.2.0/23 and 10.0.4.0/23). Each subnet is enclosed in a dashed orange border and features a small padlock icon at the bottom right corner, indicating it is locked or private. The entire VPC is labeled "Lab VPC" at the bottom center.

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

실습 2: AWS에 웹 애플리케이션 배포



보안 구성

- 앱 보안 그룹: 인터넷에서 액세스하도록 허용
- DB 보안 그룹: 앱 보안 그룹에서 액세스하도록 허용



"울타리를 치고 리소스를 그 안에 배치합니다."

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

실습 2: AWS에 웹 애플리케이션 배포

aws training and certification

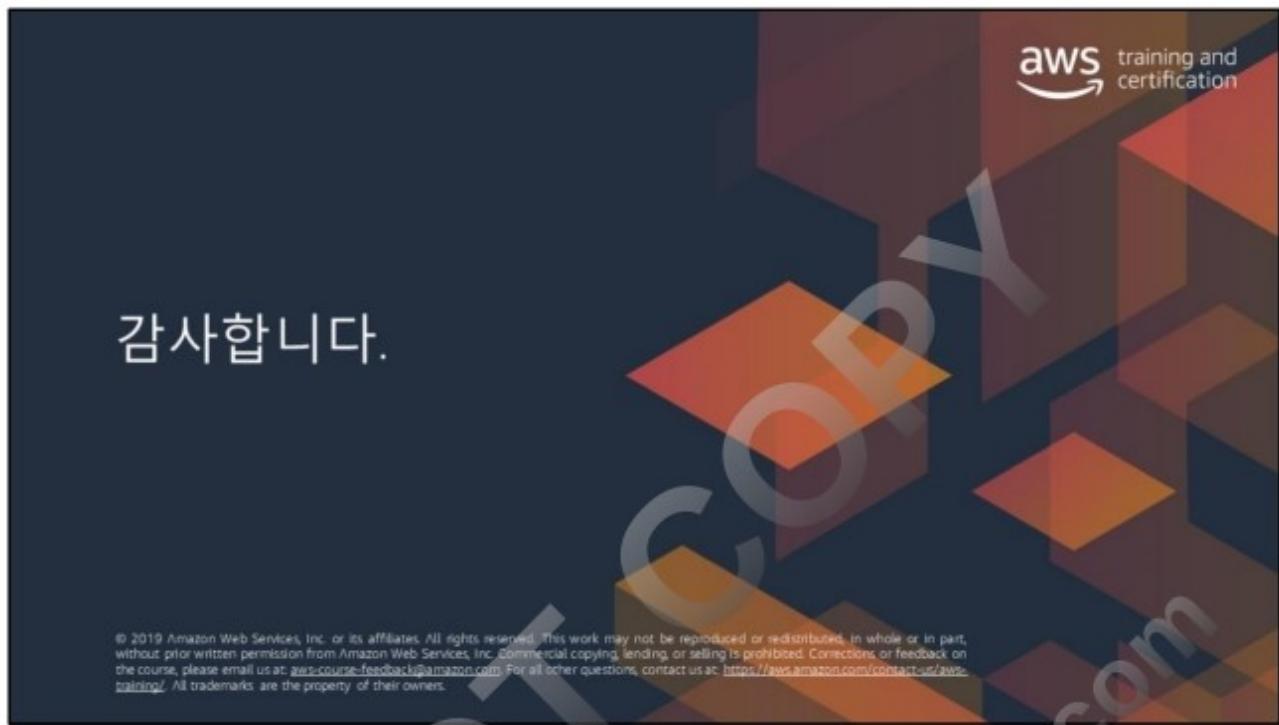
이 실습에서는

- 데이터베이스 서버를 배포합니다.
- 애플리케이션 서버를 배포합니다.
- 애플리케이션을 테스트합니다.

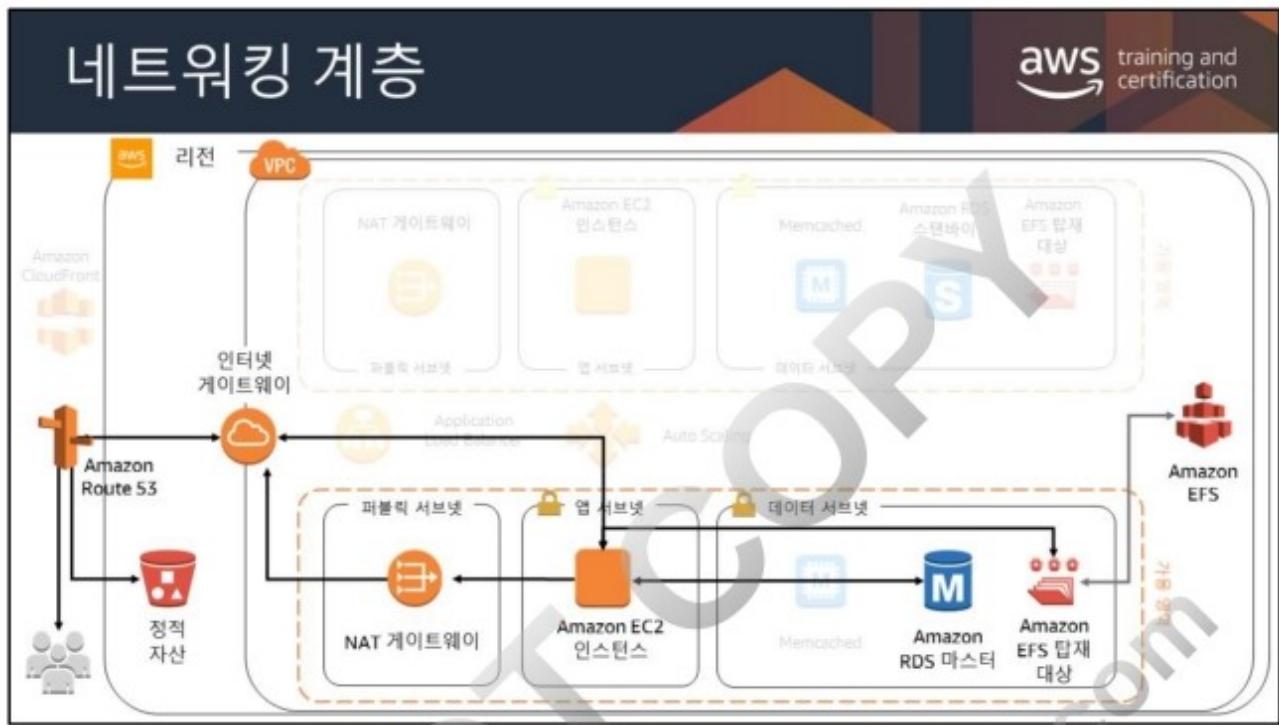
시간: 30분

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

The diagram illustrates a VPC (Virtual Private Cloud) network structure. At the top, a cloud icon labeled "VPC" contains two separate sections, each represented by a dashed-line box. The left section, labeled "Lab VPC", contains two subnets: "퍼블릭 서브넷 1" (IP range 10.0.0.0/24) and "퍼블릭 서브넷 2" (IP range 10.0.1.0/24). The right section contains two subnets: "프라이빗 서브넷 1" (IP range 10.0.2.0/23) and "프라이빗 서브넷 2" (IP range 10.0.4.0/23). Within these subnets, there are various AWS services and instances: an "App Server" (orange square icon), an "Amazon RDS DB Instance" (MySQL icon), and two "MySQL" databases. Each service is accompanied by its specific IP range and subnet name. Below the subnets, the text "가용 영역" (Available Region) is repeated twice.

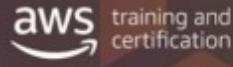






수업이 끝나면 이 아키텍처 디어그램의 모든 구성 요소를 이해할 수 있습니다.
또한 마찬가지로 규모가 크고 강력한 자체 아키텍처 솔루션을 구축할 수 있습니다.

모듈 5



아키텍처 측면에서의 필요성

워크로드 격리를 제공하는 네트워크 환경에서 AWS 리소스를 배포하고 관리해야 합니다.

모듈 개요

- Amazon Virtual Private Cloud (VPC)
- 서브넷
- 게이트웨이
- 네트워크 보안

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



VPC란 무엇입니까?

VPC

AWS Cloud의 프라이빗 네트워크 공간

개발 테스트

워크로드에 대한 논리적 격리를 제공합니다.

리소스에 대한 사용자 지정 액세스 제어 및 보안 설정을 허용합니다.

aws training and certification

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

Amazon VPC 세부 사항

VPC는 AWS 계정 전용 가상 네트워크입니다.

IPv4 또는 IPv6 주소 범위에 존재합니다.

점유 리소스에 대한 특정 CIDR 범위를 생성할 수 있습니다.

인바운드 및 아웃바운드 트래픽에 대한 엄격한 액세스 규칙을 제공합니다.

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

Amazon VPC (Amazon Virtual Private Cloud)는 클라우드의 네트워크 환경입니다. Amazon VPC는 AWS 리소스를 사용자가 정의한 가상 네트워크안에서 시작할 수 있게 합니다.

Amazon VPC는 사용자 본인의 IP 주소 범위 선택, 서브넷 작성, 라우팅 테이블 및 네트워크 게이트웨이 구성을 포함해 사용자의 환경과 리소스를 상호 격리할 때 이를 보다 효과적으로 제어할 수 있도록 설계되었습니다. VPC에서 IPv4와 IPv6을 모두 사용하여 리소스와 애플리케이션을 안전하고 쉽게 액세스할 수 있습니다. Virtual Private Cloud (VPC)는 사용자의 AWS 계정 전용 가상 네트워크입니다.

참고: 기본적으로 Amazon EC2와 Amazon VPC는 IPv4 주소 지정 프로토콜을 사용합니다. 인터넷을 통해 프라이빗 IPv4 주소에 연결할 수는 없지만, 전역적으로 고유한 퍼블릭 IPv4 주소를 인스턴스에 할당할 수는 있습니다. IPv6 CIDR 블록을 VPC와 서브넷에 연결하고 해당 블록의 IPv6 주소를 VPC의 리소스에 할당할 수도 있습니다. IPv6 주소는 퍼블릭이며 인터넷을 통해 연결할 수 있습니다.

VPC에서의 IP 주소 지정에 대한 자세한 내용은

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html>을

참조하십시오.

DO NOT COPY
zlagusdbs@gmail.com

VPC 배포

VPC는 22개의 AWS 리전 중 1개 리전에 배포됩니다.

VPC 리전 내 모든 가용 영역의 리소스를 호스팅할 수 있습니다.

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

하나의 VPC 사용

aws training and certification

하나의 VPC가 적절한 사용 사례는 **제한적입니다**.

- 한 명 또는 매우 작은 팀이 관리하는 소규모 단일 애플리케이션
- 고성능 컴퓨팅
- 자격 증명 관리

대부분의 사용 사례에서는 인프라를 구성하는 데 2개의 기본 패턴을 사용합니다.

다중 VPC 및 복수 계정

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

단일 VPC 환경이 여러 VPC에 걸쳐 분산된 환경보다 자연 시간이 짧으므로 고성능 컴퓨팅 환경(예: 물리 시뮬레이션)은 단일 VPC 내에서 가장 잘 작동할 수 있습니다.

자격 증명 관리 환경은 최적의 보안을 위해 하나의 VPC로 제한되는 것이 좋을 수 있습니다.

작은 팀이 지원하는 소규모 애플리케이션은 하나의 VPC를 사용하는 것이 가장 간편할 수 있습니다.

다중 VPC 패턴

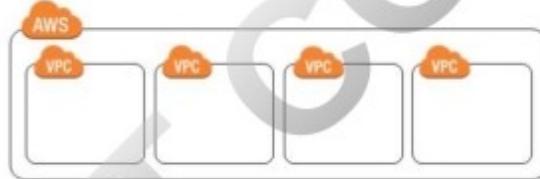


다음에 가장 적합:

- 단일 팀 또는 단일 조직(예: 관리형 서비스 공급자)
- 더 쉽게 표준 상태를 유지하고 액세스를 관리할 수 있는 제한된 팀

예외:

- 거버넌스 및 규정 준수 표준은 조직의 복잡성과 관계없이 워크로드 격리를 요구할 수 있습니다.



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

다중 VPC 패턴은 각 애플리케이션 환경의 모든 리소스 프로비저닝 및 관리를 완전히 제어하는 단일 팀 또는 조직에 적합합니다. 예를 들어, 대규모 전자 상거래 애플리케이션을 개발하는 단일 팀은 개발자가 개발/프로덕션 환경에 대한 전체 액세스 권한이 있을 때 이 패턴을 사용할 수 있습니다. 또한 테스트/프로덕션의 모든 리소스를 관리하는 관리형 서비스 공급자(MSP)의 경우, 이 패턴이 매우 일반적입니다.

복수 계정 패턴

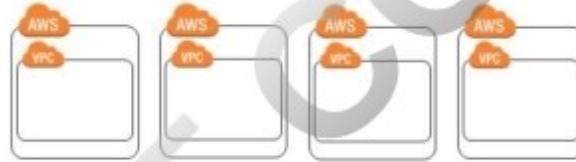


다음에 가장 적합:

- 대규모 조직 및 여러 IT 팀이 있는 조직
- 빠른 성장이 예상되는 중간 규모의 조직

그 이유는 무엇일까요?

- 액세스 및 표준 관리는 조직이 복잡할수록 더 어려울 수 있습니다.



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

다중 계정 패턴은 여러 팀에서 관리하는 애플리케이션을 배포하는 엔터프라이즈 고객 또는 조직에 가장 적합합니다. 예를 들어, 2개 이상의 팀을 지원하는 조직은 이 패턴을 사용하여, 개발 환경 리소스에는 전체 액세스 권한이 있지만, 프로덕션 환경 리소스에는 제한된 액세스 또는 전혀 액세스 권한이 없는 개발자를 지원할 수 있습니다.

VPC 제한

동일한 리전 또는 다른 리전에 여러 VPC를 보유할 수 있습니다.

The diagram illustrates VPC limits across two regions: eu-west-1 and us-east-2. In the eu-west-1 region, there are five VPC icons represented by orange clouds with the word 'VPC' inside. In the us-east-2 region, there are two VPC icons. A large watermark reading 'DO NOT COPY' diagonally across the slide also contains the text 'zlagusdbs@gmail.com'.

eu-west-1

us-east-2

서비스 제한: 계정당 리전당 VPC 5개

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

동일한 리전 또는 다른 리전, 동일한 계정 또는 다른 계정에서 여러 VPC를 생성할 수 있습니다. 계정당 지원 가능한 VPC의 수는 한도가 있으므로 VPC의 서비스 제한을 숙지해야 합니다.

VPC 및 IP 주소 지정



- 각 VPC는 사용자가 지정하는 프라이빗 IP 주소의 범위를 예약합니다.
- 이러한 프라이빗 IP 주소는 해당 VPC에 배포된 리소스에서 사용할 수 있습니다.
- IP 범위는 CIDR (Classless Inter-Domain Routing) 표기법을 사용하여 정의됩니다.
- 고유 IP 주소 가져오기(BYOLP-Bring Your Own IP) 접두사 지원

예: 10.0.0.0/16 = 10.0.0.0에서 10.0.255.255까지의 모든 IP

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

Amazon VPC는 AWS 클라우드 내의 분리된 안전한 사설 공간입니다. 사용자는 자신이 정의한 이 가상 네트워크 공간안에서 AWS 리소스들을 시작할 수 있습니다. VPC를 생성하면 사용자는 VPC의 인스턴스가 사용할 사설 IP 주소를 직접 제공할 수 있습니다.

VPC는 듀얼 스택 모드로 작동할 수 있습니다 : 리소스는 IPv4, IPv6 또는 이들 두 가지 IP 모두를 통해 통신할 수 있습니다. IPv4 주소와 IPv6 주소는 서로 독립적입니다. VPC에서는 IPv4와 IPv6에 대해 별도로 라우팅 및 보안을 구성해야 합니다.

Amazon Virtual Private Cloud(VPC)에서는 고객이 자신의 퍼블릭 IP 주소 접두사를 AWS로 가져와서 사용할 수 있습니다. 고객 IP를 탄력적 IP 주소로 가져온 다음 동일한 방식으로 사용할 수 있습니다. 예를 들어 고객 IP를 Amazon EC2 인스턴스, 네트워크 로드 밸런서 및 NAT 게이트웨이에 연결할 수 있습니다. AWS를 통해 IP 주소 범위를 알리면 서비스의 다운타임을 최소화할 수 있으므로, 이는 특히 마이그레이션에 유용합니다.

또한 개별 IP 주소 또는 접두사를 화이트리스트에 추가할 필요가 있는 파트너와 고객이 사용하는 신뢰할 수 있는 IP 주소를 유지하는 데에도 유용합니다. 예를 들어 상업용 이메일은 IP 주소 평판에 의존합니다. BYOIP(Bring Your Own IP)를 사용하면 고객은 이미 신뢰할 수 있는 이메일 애플리케이션을 기준 전송 평판을 잃지 않고 AWS로 마이그레이션할 수 있습니다.

BYOIP 사용은 무료입니다. 탄력적 IP 주소와 달리 고객은 BYOIP로 가져온 연결되지 않은 IP 주소에 비용을 지불할 필요가 없습니다. BYOIP에 대한 자세한 내용은 다음을 참조하십시오. <https://aws.amazon.com/about-aws/whats-new/2018/10/announcing-the-general-availability-of-bring-your-own-ip-for-amazon-virtual-private-cloud/>.

CIDR 예

CIDR	총 IP
/28	16
...	...
/20	4,096
/19	8,192
/18	16,384
/17	32,768
/16	65,536

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

이 주소 집합을 CIDR (Classless Inter-Domain Routing) 블록 형태로 지정합니다(예. 10.0.0.0/16). 이것은 VPC의 기본 CIDR 블록입니다. 또한, /28 (16 IP 주소)과 /16 (65,536 IP 주소) 사이에서 네트워크의 블록 크기를 지정할 수도 있습니다.

Amazon VPC는 IPv4 및 IPv6 주소 지정을 지원하며, 이들 IP에 대해 상이한 CIDR 블록 크기 제한이 있습니다. 기본적으로 모든 VPC와 서브넷에는 IPv4 CIDR 블록이 있어야 합니다. 이러한 동작은 변경할 수 없습니다. IPv6 CIDR 블록을 VPC에 선택적으로 연결할 수 있습니다.

서브넷을 사용하여 VPC 분리

aws training and certification

서브넷은 리소스 그룹을 격리할 수 있는 VPC IP 주소 범위의 세그먼트 또는 파티션입니다.

예:

CIDR /22인 VPC는 총 1,024개의 IP를 포함합니다.

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

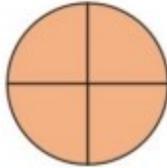
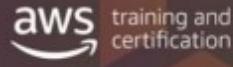
Amazon VPC를 사용하면 고객들이 가상 네트워크를 생성하고 이를 서브넷으로 분할할 수 있습니다. VPC 서브넷은 특정 가용 영역에 매핑됩니다. 따라서 서브넷 배치는 EC2 인스턴스를 여러 위치에 올바르게 분산할 수 있도록 보장하는 하나의 메커니즘입니다.

서브넷을 생성할 때는 VPC CIDR 블록의 하위 집합에 속하는 CIDR 블록을 해당 서브넷에 대해 지정합니다. 각 서브넷은 하나의 가용 영역 내에 모두 상주해야 하며, 다른 영역으로 확장할 수 없습니다.

이전에 설명한 대로 IPv6 CIDR 블록을 VPC에 할당하고 IPv6 CIDR 블록을 서브넷에 할당할 수도 있습니다.

VPC에서 IP 주소 지정에 관한 자세한 내용은 아래의 사이트를 각각 참조하십시오.
<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html>
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#vpc-sizing-ipv6

서브넷: 키 속성



- 서브넷은 VPC CIDR 블록의 하위 집합입니다.
- 서브넷 CIDR 블록은 중첩될 수 없습니다.
- 각 서브넷은 하나의 가용 영역 내에서만 존재합니다
- 가용 영역에 서브넷이 여러 개 포함될 수 있습니다.

AWS는 각 서브넷에서 5개의 IP 주소를 예약합니다.

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

AWS는 각 서브넷의 CIDR 블록에서 첫 IP 주소 4개와 마지막 IP 주소를 예약합니다.

AWS 설명서에서:

예를 들어, CIDR 블록이 10.0.0.0/24인 서브넷에서는 다음과 같은 5개의 IP 주소가 예약되어 있습니다.

- 10.0.0.0: 네트워크 주소
- 10.0.0.1: AWS에서 VPC 라우터용으로 예약
- 10.0.0.2: AWS에 의해 예약됨. DNS 서버의 IP 주소는 항상 VPC 네트워크 범위 +2에 위치합니다. 다만 우리는 각 서브넷 범위 +2의 위치도 예약합니다. 여러 개의 CIDR 블록이 있는 VPC의 경우, DNS 서버의 IP 주소는 기본 CIDR에 위치합니다. 자세한 내용은

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#AmazonDNS를 참조하십시오.

- 10.0.0.3: 차후 사용을 위해 AWS에서 예약
- 10.0.0.255: 네트워크 브로드캐스트 주소. AWS는 VPC에서 브로드캐스트를 지원하지 않으므로 이 주소를 예약합니다.

라우팅 테이블: VPC 리소스 간에 트래픽 보내기

aws training and certification

라우팅 테이블:

- VPC 리소스 간에 트래픽을 연결하는 데 필요합니다.
- 각 VPC에는 주요(기본) 라우팅 테이블이 있습니다.
- 사용자 지정 라우팅 테이블을 생성할 수 있습니다.
- 모든 서브넷에는 연결된 라우팅 테이블이 있어야 합니다.

모범 사례: 각 서브넷에 대해 사용자 지정 라우팅 테이블 사용

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

라우팅 테이블은 네트워크 트래픽이 향하는 방향을 결정하는 데 사용되는 경로라고 부르는 규칙 세트를 포함합니다.

VPC를 생성하면, 자동으로 기본 라우팅 테이블이 생성됩니다. 처음에는 기본 라우팅 테이블(및 VPC의 모든 라우팅 테이블)에 단일 경로 즉, VPC 내 모든 리소스에 대하여 통신을 허용하는 로컬 경로만 포함되어 있습니다. 라우팅 테이블의 로컬 경로는 수정할 수 없습니다. VPC에서 인스턴스를 시작할 때마다 로컬 경로는 해당 인스턴스에 자동으로 적용됩니다. 라우팅 테이블에 새 인스턴스를 추가할 필요가 없습니다. VPC에 대한 사용자 정의 라우팅 테이블을 추가로 생성할 수 있습니다.

VPC에 있는 각 서브넷은 라우팅 테이블에 연결되어 있어야 합니다. 이 테이블이 서브넷에 대한 라우팅을 제어합니다. 서브넷을 특정 라우팅 테이블과 명시적으로 연결하지 않는 경우, 서브넷은 암시적으로 기본 라우팅 테이블과 연결되어 이를 사용합니다. 서브넷은 한 번에 하나의 라우팅 테이블에만 연결할 수 있지만, 여러 서브넷을 같은 라우팅 테이블에 연결할 수 있습니다.

각 서브넷에 대한 사용자 지정 라우팅 테이블을 사용하여 대상에 대해 세부적인 라우팅을 활성화합니다.

서브넷을 통해 허용되는 다양한 수준의 네트워크 격리

aws training and certification

퍼블릭 서브넷

서브넷을 사용하여 인터넷 액세스 접근성을 정의합니다.

퍼블릭 서브넷

- 퍼블릭 인터넷에 대한 인바운드/아웃바운드 액세스를 지원하도록 인터넷 게이트웨이에 대한 라우팅 테이블 항목을 포함합니다.

프라이빗 서브넷

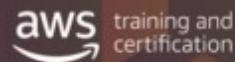
- 인터넷 게이트웨이에 대한 라우팅 테이블 항목이 없습니다.
- 퍼블릭 인터넷에서 직접 액세스할 수 없습니다.
- 일반적으로 제한된 아웃 바운드 퍼블릭 인터넷 액세스를 지원하기 위해 NAT 게이트웨이를 사용합니다.

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

애플리케이션 또는 기능 티어(웹/앱/데이터 등)를 기준으로 서브넷을 정의하기보다는, 인터넷 접근성을 기준으로 서브넷을 구성해야 합니다. 이를 통해 퍼블릭 리소스와 프라이빗 리소스 간에 명확한 서브넷 수준의 격리를 정의할 수 있습니다.

참고: PCI 규정 준수 등 특정 상황에서 매우 민감한 데이터는 인터넷에 직접 또는 간접적으로 연결될 수 없는 경우, 이러한 서브넷을 "보호된" 서브넷이라고 부릅니다.

퍼블릭 서브넷에 인터넷 연결



인터넷 게이트웨이

- VPC의 인스턴스와 인터넷 간에 통신을 허용합니다.
- 기본적으로 가용성이 뛰어나고, 중복적이며, 수평적으로 확장됩니다.
- 인터넷으로 라우팅 가능한 트래픽에 대한 서브넷 라우팅 테이블에 대상을 제공합니다.

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

인터넷 게이트웨이는 수평적 확장으로 이중화를 지원하는 고가용성 VPC 구성 요소로서 VPC의 인스턴스와 인터넷 간 통신이 가능한 이유도 인터넷 게이트웨이가 있기 때문입니다. 따라서 네트워크 트래픽에 가용성 위험이나 대역폭 제약이 발생하지 않습니다.

인터넷 게이트웨이를 사용하는 2가지 목적은 인터넷 라우팅 트래픽에 대한 VPC 라우팅 테이블의 대상을 제공하고 퍼블릭 IPv4 주소가 할당된 인스턴스에 대해 네트워크 주소 변환(NAT)을 수행하는 데 있습니다.

인터넷 게이트웨이는 IPv4 및 IPv6 트래픽을 지원합니다.

퍼블릭 서브넷에 인터넷 연결

인터넷 게이트웨이

- VPC의 인스턴스와 인터넷 간에 통신을 허용합니다.
- 기본적으로 가용성이 뛰어나고, 중복적이며, 수평적으로 확장됩니다.
- 인터넷으로 라우팅 가능한 트래픽에 대한 서브넷 라우팅 테이블에 대상을 제공합니다.

인터넷 게이트웨이

VPC 10.0.0.0/16

인터넷 게이트웨이

사용자

인터넷 게이트웨이

10.0.0.0/16

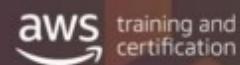
퍼블릭 라우팅 테이블

목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	<igw-id>

인스턴스 A
(퍼블릭 IP 보유)
10.0.10.0/24
퍼블릭 서브넷

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

프라이빗 서브넷에 인터넷 연결



NAT 게이트웨이

- 프라이빗 서브넷의 인스턴스가 인터넷 또는 다른 AWS 서비스로의 아웃바운드 트래픽을 시작하도록 활성화합니다.
- 프라이빗 인스턴스가 인터넷에서 인바운드 트래픽을 수신하는 것을 차단합니다.

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

프라이빗 서브넷에 인터넷 연결

NAT 게이트웨이

- 프라이빗 서브넷의 인스턴스가 인터넷 또는 다른 AWS 서비스로의 아웃바운드 트래픽을 시작하도록 활성화합니다.
- 프라이빗 인스턴스가 인터넷에서 인바운드 트래픽을 수신하는 것을 차단합니다.

퍼블릭 라우팅 테이블

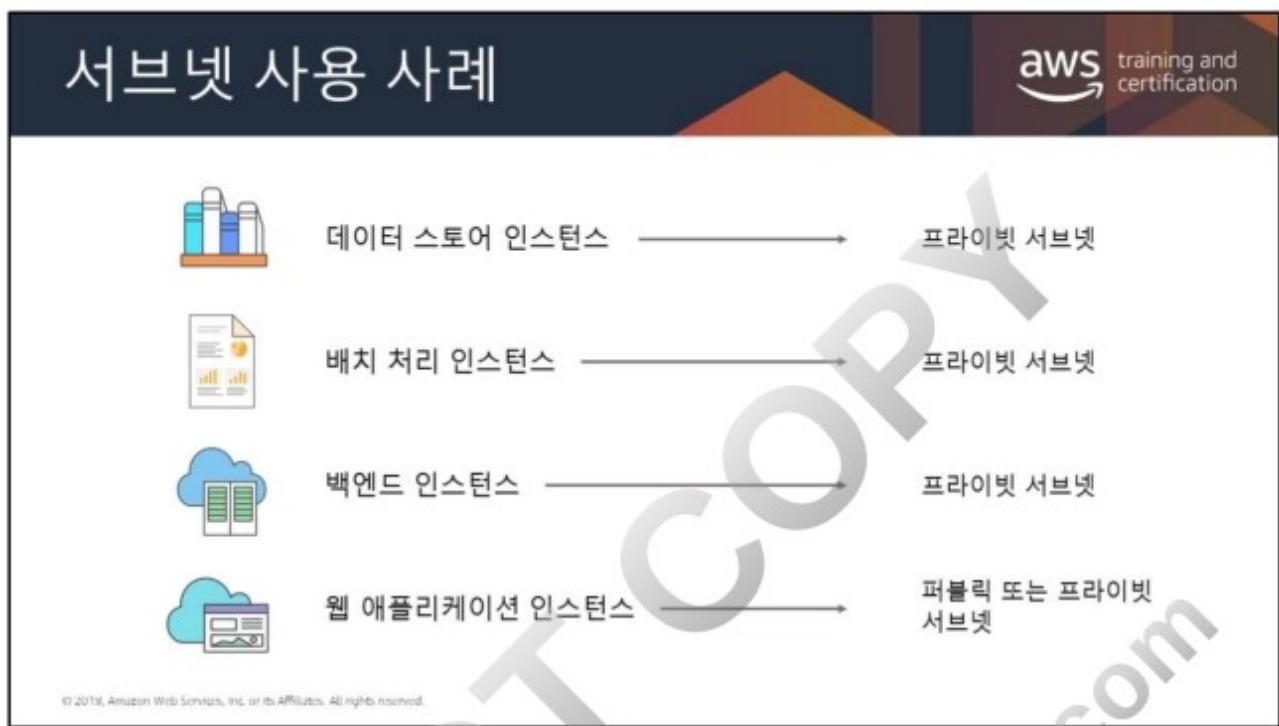
목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	<igw-id>

프라이빗 라우팅 테이블

목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	<nat-id>

VPC 사용자 인터넷 게이트웨이 10.0.0.0/16 VPC NAT 게이트웨이 10.0.10.0/24 사용자 프라이빗 인스턴스 (프라이빗 IP 보유) 10.0.20.0/24 프라이빗 서브넷

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



웹 티어 인스턴스를 퍼블릭 서브넷에 넣을 수 있지만 AWS는 퍼블릭 서브넷에 배치된 로드 밸런서 뒷쪽의 프라이빗 서브넷 내부에 이 인스턴스를 배치할 것을 권장합니다. 일부 환경에서는 웹 애플리케이션 인스턴스를 탄력적 IP에 직접 연결해야 하며(탄력적 IP를 로드 밸런서에 연결할 수 있더라도), 그런 경우 웹 애플리케이션 인스턴스는 퍼블릭 서브넷에 있어야 합니다. 로드 밸런서는 이후 모듈에서 자세히 다루기로 하겠습니다.

서브넷 권장 사항

작은 크기보다는 더 큰 크기의 서브넷을 고려합니다(/24 이상).

워크로드 배치 간소화:

- 워크로드를 10개의 작은 서브넷 중 어디에 배치할지 선택하는 것이 1개의 큰 서브넷보다 더 복잡합니다.

IP를 낭비하거나 IP가 부족할 확률이 낮음:

- 서브넷에서 사용 가능한 IP가 부족한 경우, 해당 서브넷에 IP를 추가할 수 없습니다.

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

기본 서브넷 구성

aws training and certification

서브넷을 설정하기 위한 가장 좋은 방법을 잘 모르는 경우:

가용 영역당 1개의 퍼블릭 서브넷과 1개의 프라이빗 서브넷으로 시작합니다.

VPC 10.0.0.0/21 (10.0.0.0-10.0.7.255)

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

Auto Scaling 시 충분한 IP 주소 용량을 제공하기 위해 가용 영역당 퍼블릭 서브넷과 프라이빗 서브넷을 하나씩 사용할 것을 고려하십시오.

서브넷은 인터넷 접근성을 정의하는 데 사용되어야 하므로 가용 영역당 1개의 퍼블릭 서브넷과 1개의 프라이빗 서브넷보다 더 많은 서브넷을 구성할 이유는 없습니다. 이러한 환경에서는 인터넷에 직접 액세스해야 하는 모든 리소스(퍼블릭 로드 밸런서, NAT 인스턴스, 배스천 호스트 등)는 퍼블릭 서브넷으로 가고, 모든 다른 인스턴스는 프라이빗 서브넷으로 갑니다(예외: 직접적 또는 간접적으로 인터넷에 대한 액세스가 전혀 필요 없는 리소스는 별도의 프라이빗 서브넷으로 갑니다).

일부 환경에서는 리소스 "티어" 간에 분리 계층을 생성하는데 서브넷을 사용하려고 시도합니다(예: 백엔드 애플리케이션 인스턴스와 데이터 소스를 개별 프라이빗 서브넷에 추가). 이러한 사례에서는 각 서브넷에 필요한 호스트 수를 좀 더 정확히 예측해야 하므로, IP가 빠르게 고갈되거나, 다른데 사용할 수 있었을 미사용 IP가 너무 많이 남을 가능성이 높습니다.

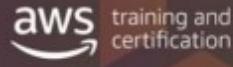
서브넷은 네트워크 ACL 규칙을 사용하여 리소스 간에 매우 기본적인 분리 요소를 제공할 수 있습니다. 반면에 보안 그룹은 인프라를 너무 복잡하게 만들고, IP를 낭비하거나 IP가 부족할 위험 없이 리소스 간에 좀 더 정교한 수준의 트래픽 제어를 제공할 수 있습니다. 이 접근 방식에서는 VPC에서 필요한 퍼블릭 IP와 프라이빗 IP 수만 예측하고 서브넷 내 리소스 간에 분리는 다른 리소스를 사용하여 생성하면 됩니다.

DO NOT COPY
zlagusdbs@gmail.com



AWS의 리소스 대부분은 프라이빗 서브넷에서 호스팅할 수 있으며, 필요에 따라 인터넷에 대한 제어된 액세스를 위해 퍼블릭 서브넷을 사용할 수 있습니다. 때문에 퍼블릭 서브넷과 비교하여 프라이빗 서브넷에 훨씬 더 많은 IP를 제공하도록 서브넷을 계획해야 합니다. 아키텍처를 계획할 때, VPC에서 필요한 호스트 수가 몇 개인지와 그중 몇 개를 프라이빗 서브넷에 배치할 수 있는지를 예측하는 것이 중요합니다. 프라이빗 서브넷에 퍼블릭 리소스를 배치하는 데 대한 전략을 뒤에서 좀 더 상세히 다루기로 하겠습니다.

탄력적 네트워크 인터페이스



**탄력적 네트워크 인터페이스는
가상 네트워크 인터페이스입니다.**
동일한 가용영역 안에서 EC2 인스턴스
간에 이동할 수 있습니다.

새 인스턴스로 이동하면 네트워크 인터페이스는
다음을 유지합니다.

- 프라이빗 IP 주소
- 탄력적 IP 주소
- MAC 주소

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

탄력적 네트워크 인터페이스는 VPC에서 인스턴스에 장착할 수 있는 가상 네트워크 인터페이스입니다. 네트워크 인터페이스를 만들고 인스턴스에 연결하는 것은 물론, 인스턴스에서 분리한 후 다른 인스턴스에 연결할 수도 있습니다. 프라이빗 IP 주소, 탄력적 IP 주소 및 MAC 주소를 포함한 네트워크 인터페이스의 속성은 네트워크 인터페이스를 따르는데, 그 이유는 이 인터페이스가 인스턴스에 연결되거나 혹은 인스턴스에서 분리되었다가 다른 인스턴스에 다시 연결되기 때문입니다. 네트워크 인터페이스를 인스턴스 간에 이동하면 네트워크 트래픽이 새 인스턴스로 리디렉션됩니다. VPC의 각 인스턴스에는 사용자 VPC의 IP 주소 범위에서 프라이빗 IP 주소가 할당된 기본 네트워크 인터페이스(primary network interface)가 있습니다. 인스턴스의 기본 네트워크 인터페이스는 분리할 수 없습니다. 추가 네트워크 인터페이스를 생성하고 연결할 수는 있습니다.

다음 작업을 수행하려는 경우, 여러 네트워크 인터페이스를 하나의 인스턴스에 연결하면 유용합니다.

- 관리 네트워크 생성
- VPC에서 네트워크 및 보안 어플라이언스 사용
- 별도의 서브넷에 있는 워크로드/역할로 이중 홈 인스턴스 생성
- 저예산 고가용성 솔루션 생성

한 서브넷의 네트워크 인터페이스를 동일 VPC에 있는 다른 서브넷의 인스턴스에 연결할 수 있지만, 네트워크 인터페이스와 인스턴스가 둘 다 동일 가용 영역 안에 상주해야 합니다. 이는 트래픽을 다른 가용 영역으로 리디렉션하려는 일부 DR 시나리오에서 사용이 제한됩니다. 그래도 이것은 동일한 서브넷 또는 가용 영역의 대기 VM으로 장애 조치를 수행할 필요가 있는 비교적 덜 파국적인 시나리오에서 유용합니다.

DO NOT COPY
zlagusdbs@gmail.com

탄력적 네트워크 인터페이스

aws training and certification

인스턴스에 네트워크 인터페이스가 두 개 이상 있는 이유는 무엇입니까?

요구 사항:

- 관리 네트워크 생성
- VPC에서 네트워크 및 보안 어플라이언스 사용
- 별도의 서브넷에 있는 워크로드/역할로 이중 홈 인스턴스 생성

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

다음 작업을 수행하려는 경우, 여러 네트워크 인터페이스를 하나의 인스턴스에 연결하면 유용합니다.

- 관리 네트워크 생성
- VPC에서 네트워크 및 보안 어플라이언스 사용
- 별도의 서브넷에 있는 워크로드/역할로 이중 홈 인스턴스 생성
- 저예산 고가용성 솔루션 생성



네트워크 인터페이스를 사용하여 관리 네트워크를 생성할 수 있습니다. 이 시나리오에서는 인스턴스의 기본 네트워크 인터페이스(eth0)가 퍼블릭 트래픽을 처리하고, 보조 네트워크 인터페이스(eth1)는 백엔드 관리 트래픽을 처리하며 VPC에서 액세스 제어가 더욱 제한되는 별도의 서브넷에 연결됩니다.

로드 밸런서 뒤에 있거나 없을 수 있는 퍼블릭 인터페이스에는 인터넷에서 서버에 액세스할 수 있도록 허용(예: 0.0.0.0/0 또는 로드 밸런서에서 TCP 포트 80 및 443을 허용)하는 보안 그룹이 연결되어 있는 반면, 프라이빗 인터페이스에는 VPC 내 또는 인터넷에서 허용된 IP 주소 범위, VPC 내 프라이빗 서브넷 또는 가상 프라이빗 게이트웨이에서만 SSH 액세스를 허용하는 보안 그룹이 연결되어 있습니다.

탄력적 IP 주소



- 인스턴스 또는 네트워크 인터페이스에 연결할 수 있습니다.
- 즉시 트래픽을 재연결하고 전송할 수 있습니다.
- AWS 리전당 5개가 허용됩니다.
- BYOIP (Bring Your Own IP) 주소를 생성할 수 있습니다.

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

탄력적 IP 주소(EIP)는 동적 클라우드 컴퓨팅을 위해 설계된 고정 퍼블릭 IPv4 주소입니다. 계정의 어떤 VPC에 대해서든 탄력적 IP 주소를 인스턴스 또는 네트워크 인터페이스와 연결할 수 있습니다. 탄력적 IP 주소로 주소를 VPC의 다른 인스턴스에 신속하게 다시 매핑하여 인스턴스의 장애를 숨길 수 있습니다. 탄력적 IP 주소를 인스턴스와 직접 연결하는 대신 네트워크 인터페이스에 연결하면 네트워크 인터페이스의 모든 속성을 한 번에 한 인스턴스에서 다른 인스턴스로 이동할 수 있다는 이점이 있습니다.

하나의 인스턴스에서 다른 인스턴스로 탄력적 IP 주소를 이동할 수 있습니다. 인스턴스는 동일한 VPC 또는 다른 VPC에 위치할 수 있습니다. 탄력적 IP 주소는 VPC의 인터넷 게이트웨이를 통해 액세스할 수 있습니다. VPC와 네트워크 간에 VPN 연결을 설정한 경우, VPN 트래픽은 인터넷 게이트웨이가 아닌 가상 프라이빗 게이트웨이를 통과하기 때문에 탄력적 IP 주소에 액세스할 수 없습니다.

탄력적 IP 주소는 5개로 제한되며, 이를 절약하기 위해 NAT 디바이스를 사용할 수 있습니다. 인스턴스 장애 시, 주소를 다른 인스턴스로 매핑하고 다른 모든 노드와의 통신에서 DNS 호스트 이름을 사용하려면 기본적으로 탄력적 IP 주소를 사용할 것을 적극 권장합니다.

BYOIP (Bring Your Own IP) 주소 접두사에서 탄력적 IP 주소를 생성하여 EC2 인스턴스, Network Load Balancer 및 NAT Gateway와 같은 AWS 리소스에 사용할 수 있습니다. BYOIP 주소 접두사에서 생성하는 탄력적 IP 주소는 Amazon에서 가져오는 탄력적 IP 주소와 정확히 동일하게 작동합니다.

인스턴스를 중지해도 탄력적 IP 주소는 인스턴스와 연결된 상태를 유지합니다. IPv6에 대한 탄력적 IP 주소는 현재 지원되지 않습니다.

DO NOT COPY
zlagusdbs@gmail.com

탄력적 IP 주소

aws training and certification



- 인스턴스 또는 네트워크 인터페이스에 연결할 수 있습니다.
- 즉시 트래픽을 재연결하고 전송할 수 있습니다.
- AWS 리전당 5개가 허용됩니다.



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



DO NOT COPY
zlagusdbs@gmail.com

보안 그룹



- AWS 리소스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 **가상 방화벽**
- 트래픽은 모든 IP 프로토콜, 포트 또는 IP 주소로 **제한**될 수 있습니다.
- 규칙은 **상태 저장**입니다.

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

Amazon VPC는 인스턴스의 송수신 트래픽을 모두 필터링할 수 있는 완전한 방화벽 솔루션을 지원합니다. 기본 그룹은 동일한 그룹 내의 다른 구성원으로부터의 인바운드 통신과 모든 대상에 대한 아웃바운드 통신을 허용합니다. 트래픽은 모든 IP 프로토콜, 서비스 포트, 원본/대상 IP 주소(개별 IP 또는 Classless Inter-Domain Routing (CIDR) 블록)에 의해 제한될 수 있습니다.

상태 저장 규칙 관련: 예를 들어 집 컴퓨터에서 인스턴스에 대한 ICMP 펑 명령을 시작하고, 인바운드 보안 그룹 규칙이 ICMP 트래픽을 허용한 경우, 연결에 대한 정보(포트 정보 포함)가 추적됩니다. 펑 명령에 대한 인스턴스의 응답 트래픽은 새로운 요청으로 추적되지 않고 대신 설정된 연결로 처리되므로 아웃바운드 보안 그룹 규칙이 아웃바운드 ICMP 트래픽을 제한하는 경우에도 인스턴스 외부로의 트래픽 흐름이 허용됩니다.

모든 트래픽 흐름이 추적되지는 않습니다. 보안 그룹 규칙이 모든 트래픽(0.0.0.0/0)에 대한 TCP 또는 UDP 흐름을 허용하고, 반대 방향에 이에 상응하는 규칙이 응답 트래픽을 허용하는 경우, 해당 트래픽 흐름은 추적되지 않습니다. 따라서 응답 트래픽은 응답 트래픽을 허용하는 인바운드 또는 아웃바운드 규칙을 기준으로 흐름이 허용되며, 추적 정보에 포함되지 않습니다.

보안 그룹: 기본 설정

aws training and certification

새 보안 그룹:

모든 인바운드
트래픽 차단

모든 아웃바운드
트래픽 허용

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

기본적으로 보안 그룹은 모든 아웃바운드 트래픽을 허용하는 아웃바운드 규칙을 포함합니다. 규칙을 제거하고 특정 아웃바운드 트래픽만 허용하는 아웃바운드 규칙을 추가할 수 있습니다. 보안 그룹에 아웃바운드 규칙이 없는 경우, 인스턴스에서 시작하는 아웃바운드 트래픽은 허용되지 않습니다.

트래픽은 프로토콜, 서비스 포트 및 소스 IP 주소(개별 IP 또는 CIDR 블록) 또는 보안 그룹에 의해 제한 될 수 있습니다.

보안 그룹은 다른 클래스의 인스턴스에 대해 서로 다른 규칙을 설정하도록 구성할 수 있습니다. 기존의 3계층 웹 애플리케이션을 예로 들어 보겠습니다. 웹 서버 그룹에는 인터넷에 개방된 80번 포트(HTTP) 및/또는 443번 포트(HTTPS)가 있을 수 있습니다. 애플리케이션 서버 그룹에는 웹 서버 그룹에만 액세스할 수 있는 8000번 포트(애플리케이션별)가 있을 수 있습니다. 데이터베이스 서버 그룹에는 애플리케이션 서버 그룹에만 개방된 3306번 포트(MySQL)가 있을 수 있습니다. 세 그룹 모두 포트 22 (SSH)에 대한 관리 액세스는 허용되나, 고객의 기업 네트워크에서만 가능합니다. 이 메커니즘을 이용하면 매우 안전한 애플리케이션을 배포할 수 있습니다.

보안 그룹: 트래픽 제어

aws training and certification

대부분 조직은 각 기능 티어에 대한 인바운드 규칙으로 보안 그룹을 생성합니다.

The diagram illustrates a security group rule. It shows two security groups: 'App Layer security group' and 'Database Layer security group'. An arrow points from the 'App Layer security group' to the 'Database Layer security group', indicating that traffic is allowed from the former to the latter. Both security groups are enclosed within a larger box labeled '프라이빗 서브넷' (Private Subnet). A lock icon is positioned at the top left of this box.

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



이 슬라이드는 보안 그룹 체인의 예입니다. 트래픽이 상위 티어에서 하위 티어로만 흐른 후 다시 반대로 흐르도록 인바운드와 아웃바운드 규칙이 설정됩니다. 보안 그룹은 한 티어에서 발생한 보안 위반으로 손상된 클라이언트에 서브넷 전체의 모든 리소스에 대한 액세스가 자동으로 제공되는 것을 방지하는 방화벽 역할을 합니다.

네트워크 ACL(액세스 제어 목록)

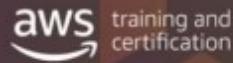


- 서브넷 경계의 방화벽
- 기본적으로 모든 인바운드 및 아웃바운드 트래픽을 허용합니다.
- 상태 비저장으로 인바운드 및 아웃바운드 트래픽 모두에 대한 명시적인 규칙이 필요합니다.

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

DO NOT COPY
zlagusdbs@gmail.com

네트워크 ACL(액세스 제어 목록)



특정 네트워크 보안
요구 사항에서 권장됩니다.

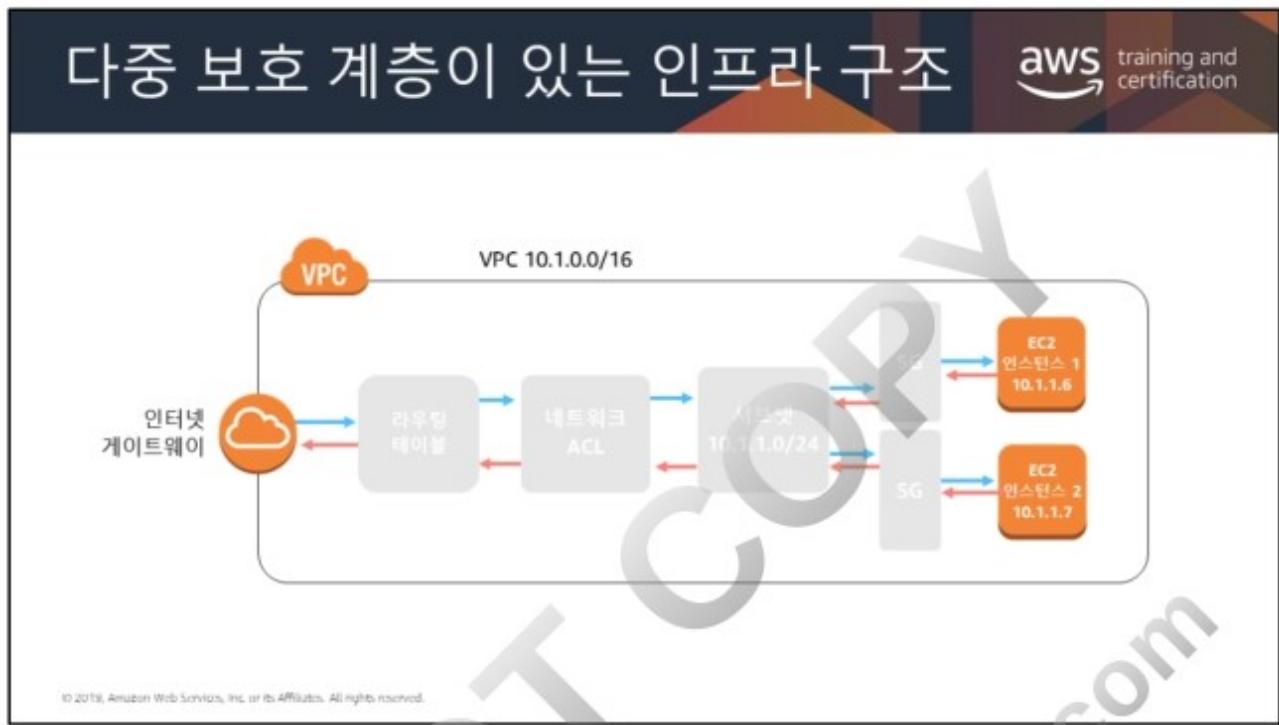
- 서브넷 경계의 방화벽
- 모든 인바운드 및 아웃바운드 트래픽을 허용합니다 (VPC의 기본 NACL)
- 상태 비저장이므로 인바운드 및 아웃바운드 트래픽 모두에 대한 명시적인 규칙이 필요합니다.



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

사용자 지정 네트워크 ACL을 생성하여 서브넷과 연결할 수 있습니다. 기본적으로 각 사용자 지정 네트워크 ACL은 규칙을 추가하기 전에는 모든 인바운드 및 아웃바운드 트래픽을 거부합니다.

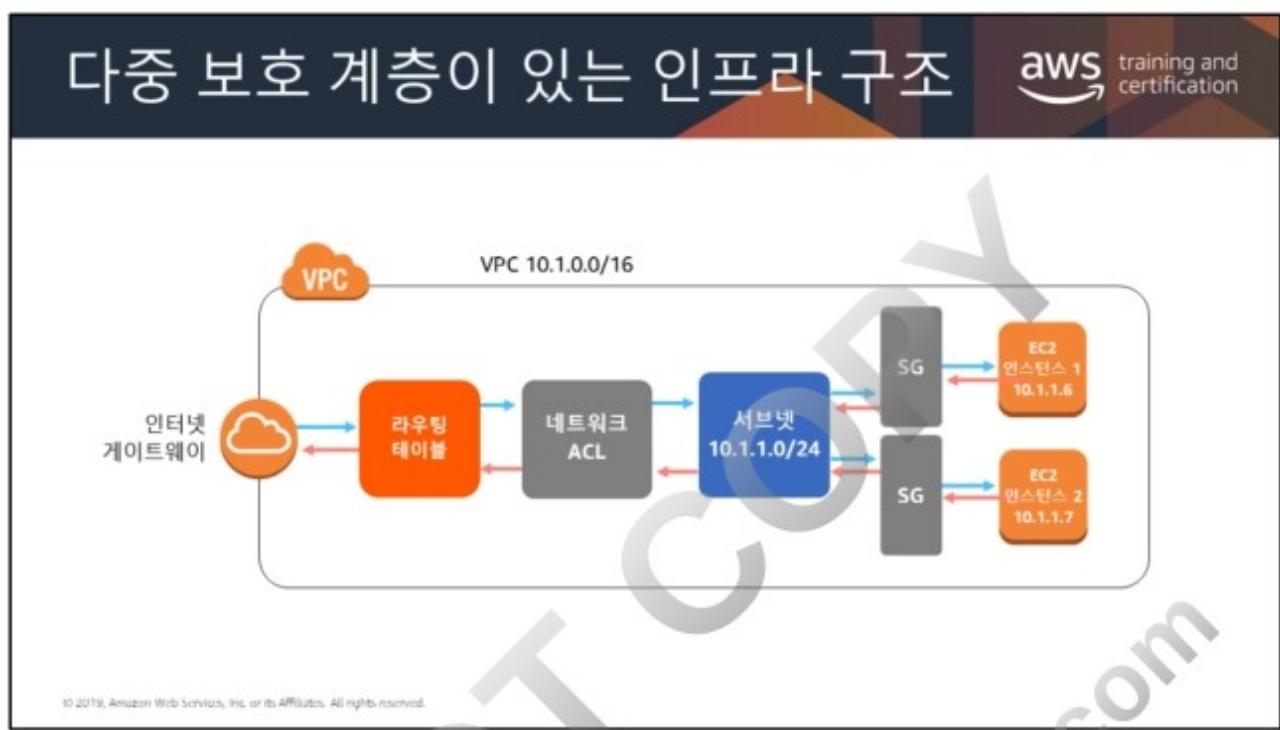




모범 사례는 다중 방어 계층으로 인프라를 보호하는 것입니다. VPC에서 인프라를 실행함으로써 어떤 인스턴스를 인터넷에 먼저 노출할지 제어할 수 있으며, 보안 그룹과 네트워크 ACL을 지정하여 인프라 및 서브넷 수준에서 인프라의 보호를 강화할 수 있습니다. 또한 운영 시스템의 수준에서 방화벽으로 인스턴스를 보호해야 하며, 다른 보안 모범 사례를 따라야 합니다.

AWS 고객은 일반적으로 보안 그룹을 네트워크 패킷 필터링의 기본적인 방법으로 활용합니다. 그 이유는 상태 저장 패킷 필터링을 수행하고 다른 보안 그룹을 참조하는 규칙을 사용할 수 있는 기능을 통해 보안 그룹을 네트워크 ACL 보다 더 다양한 용도로 활용할 수 있기 때문입니다. 그러나 네트워크 ACL은 트래픽의 특정 하위 집합을 거부하거나 서브넷에 대한 고급 수준의 가드 레일을 제공할 때 효과적인 보조 컨트롤로 활용할 수 있습니다.

네트워크 ACL과 보안 그룹을 모두 심층 방어 수단으로 구현하면 이러한 컨트롤 중 한 가지를 잘못 구성하더라도 호스트가 예기치 못한 트래픽에 노출되지 않습니다.



VPC로 트래픽 보내기

aws training and certification

VPC 서브넷의 인스턴스에 대해 인터넷 액세스를 활성화하려면 다음을 수행해야 합니다.

인터넷 게이트웨이를 VPC에 연결합니다.

라우팅 테이블을 인터넷 게이트웨이에 연결합니다.

목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	<igw-id>

인스턴스에 퍼블릭 IP 또는 탄력적인 IP 주소가 있는지 확인합니다.

네트워크 ACL과 SG가 관련 트래픽 흐름을 허용하는지 확인합니다.

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

지식 확인 1



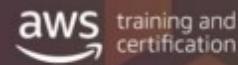
VPC는 어디에 배포됩니까?

- 리전
- 가용 영역
- 서브넷
- CIDR 블록

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

DO NOT COPY
zlagusdbs@gmail.com

지식 확인 1



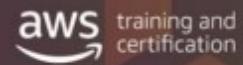
VPC는 어디에 배포됩니까?

- 리전
- 가용 영역
- 서브넷
- CIDR 블록

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

DO NOT COPY
zlagusdbs@gmail.com

지식 확인 2

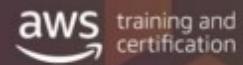


기본적으로 보안 그룹은 모든 수신 트래픽을 허용합니다. 원치 않는 트래픽을 차단하도록 규칙을 설정해야 합니다.

- 참
- 거짓

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

지식 확인 2



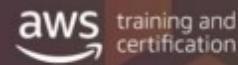
기본적으로 보안 그룹은 모든 수신 트래픽을 허용합니다. 원치 않는 트래픽을 차단하도록 규칙을 설정해야 합니다.

- 참
- 거짓

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



실습 3: Virtual Private Cloud 생성



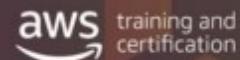
"클라우드에 프라이빗 네트워크가 필요합니다."

사용된 기술:

- Amazon VPC
- VPC 피어링
- 테스트에 Amazon EC2 및 Amazon RDS가 사용됩니다.

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

실습 3: Virtual Private Cloud 생성



다음을 사용하여 VPC를 생성합니다.

- 인터넷 게이트웨이
- 퍼블릭 서브넷
- 프라이빗 서브넷
- 각 서브넷에 대한 라우팅 테이블

그런 다음 앱 서버를 실행하고 연결하여 퍼블릭 서브넷을 테스트합니다.



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

실습 3: Virtual Private Cloud 생성

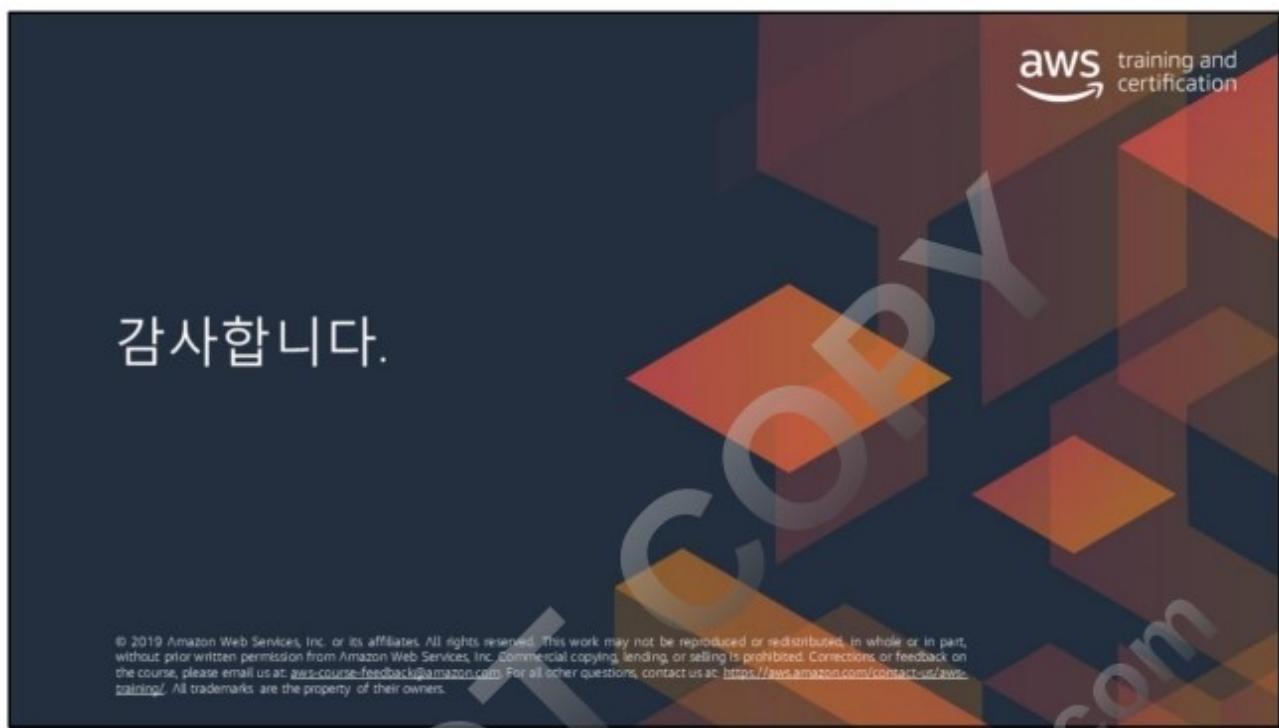
aws training and certification

선택 과제:

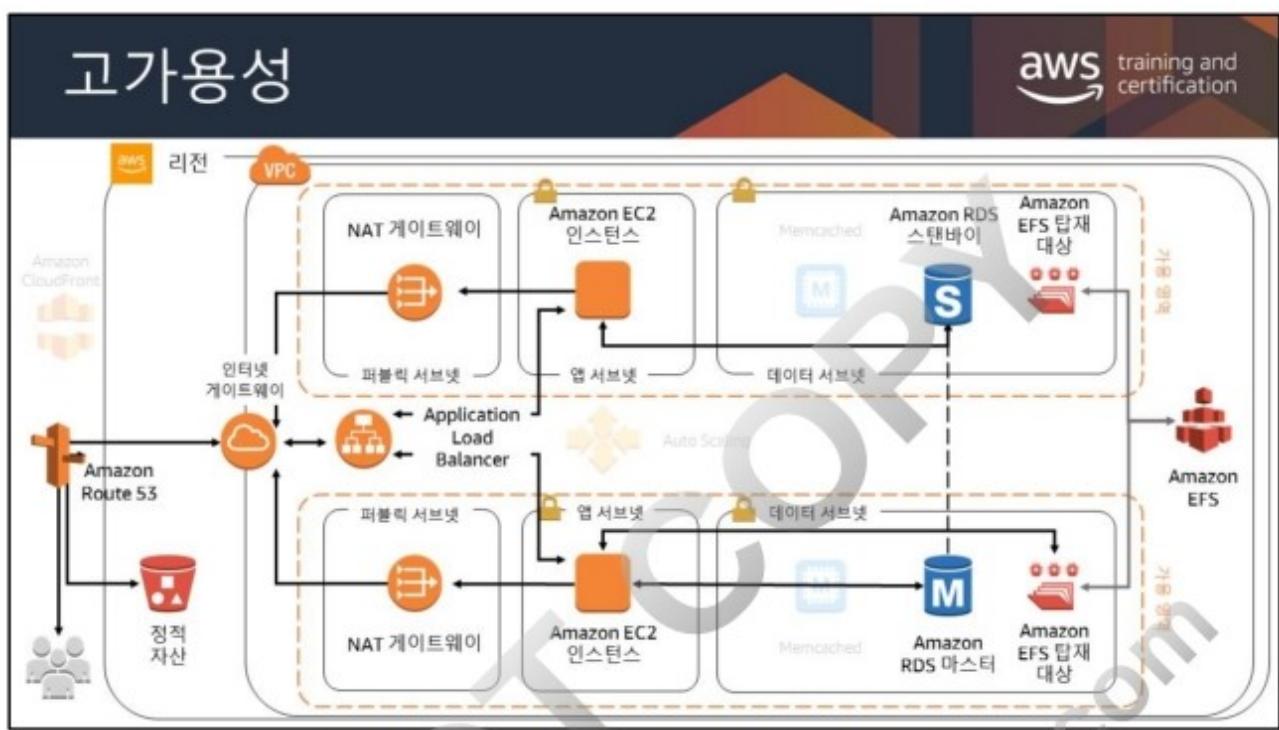
- VPC 피어링 연결 생성
- 라우팅 테이블 구성
- 애플리케이션을 데이터베이스에 연결하여 테스트

시간: 30분

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







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

모듈 6



아키텍처 측면에서의 필요성

애플리케이션은 훨씬 더 큰 사용자 기반 및 변동 로드를 지원해야 하며 가용 영역 수준의 장애를 처리해야 합니다.

모듈 개요

- 네트워크 연결
- VPC 엔드포인트
- 로드 밸런싱
- 고가용성

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



가상 프라이빗 게이트웨이(VGW)



Amazon VPC와 다른 네트워크 사이에 프라이빗 연결(VPN)을 설정할 수 있습니다.

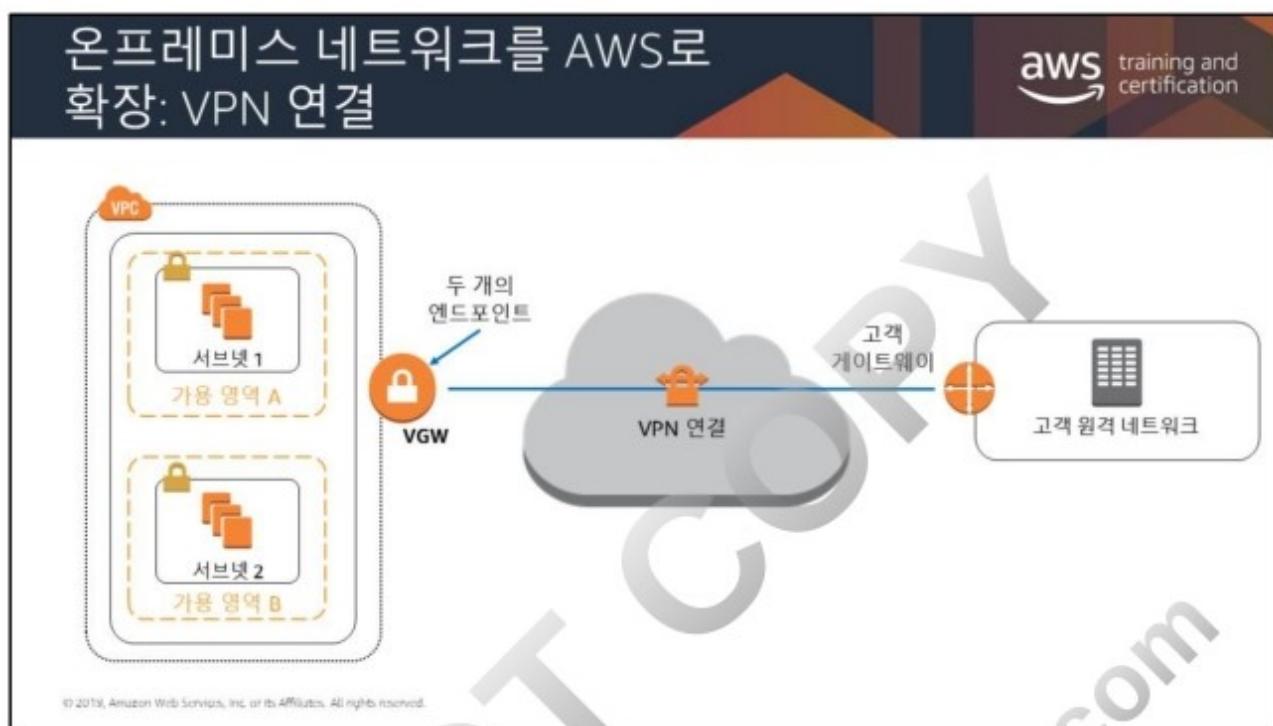
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

기본적으로 Amazon VPC에서 시작하는 인스턴스는 고객의(원격) 네트워크와 통신할 수 없습니다. VPC에 가상 프라이빗 게이트웨이(VGW)를 연결하고, 사용자 지정 라우팅 테이블을 생성하고, 보안 그룹 규칙을 업데이트하고, AWS 관리형 VPN 연결을 생성하여 VPC에서 원격 네트워크에 액세스하도록 할 수 있습니다.

VPN 연결이라는 용어는 일반적인 용어지만, Amazon VPC 설명서에서 VPN 연결은 VPC와 고객 네트워크 사이의 연결을 의미합니다. AWS는 인터넷 프로토콜 보안(IPsec) VPN 연결을 지원합니다.

VGW는 VPN 연결의 Amazon 측 VPN 집선장치입니다. VGW를 만든 후 VPN 연결을 생성할 VPC에 연결합니다.

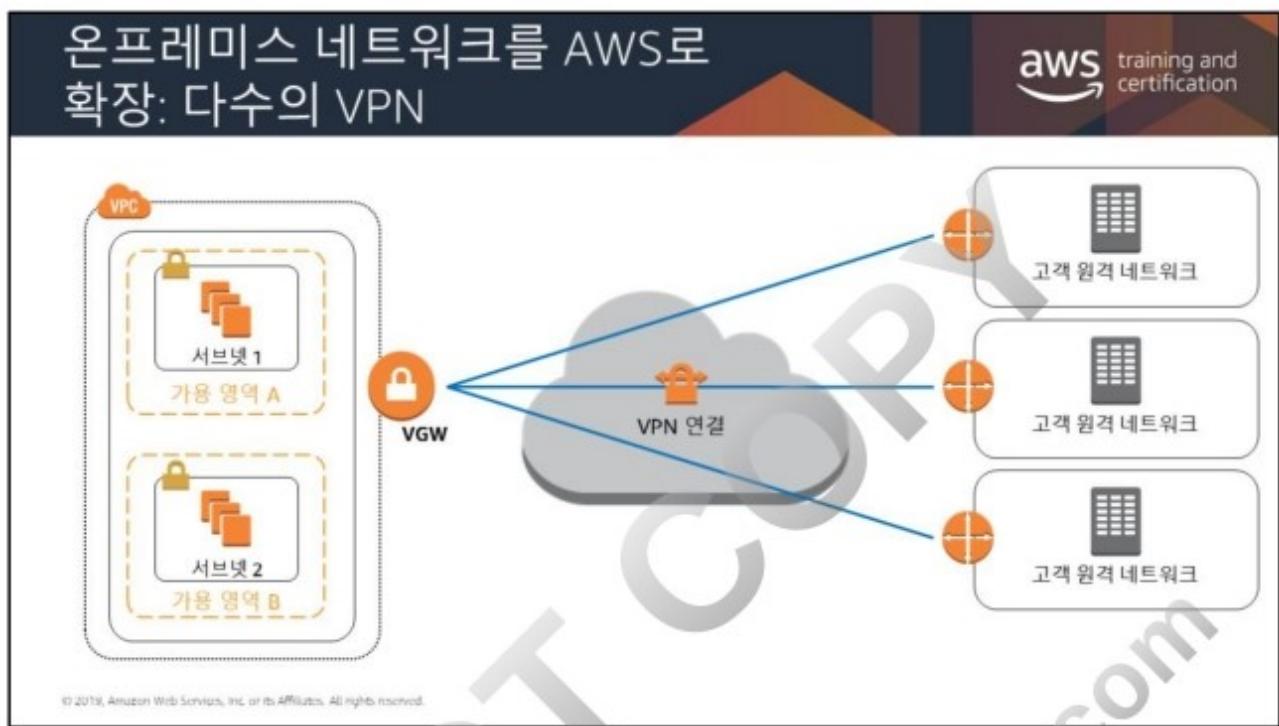
VGW를 생성할 때 Amazon 측 게이트웨이의 프라이빗 ASN(자율 시스템 번호)을 지정할 수 있습니다. ASN을 지정하지 않는 경우 VGW는 기본 ASN(64512)으로 생성됩니다. VGW를 생성한 후에는 ASN을 변경할 수 없습니다.



한 가지 방법은 VPC의 가상 게이트웨이와 데이터 센터 간에 VPN 연결을 사용하는 것입니다. AWS 하드웨어 VPN에서는 기본적인 자동 장애 조치를 지원할 수 있도록 2개의 VPN 엔드포인트가 제공됩니다. AWS 하드웨어 VPN 생성에 대한 자세한 내용은

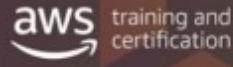
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html을 참조하십시오.

소프트웨어 VPN 어플라이언스를 실행하는 VPC의 Amazon EC2 인스턴스를 사용하여 원격 네트워크에 대한 VPN 연결을 생성할 수도 있습니다. AWS에서는 소프트웨어 VPN 어플라이언스를 제공하거나 유지 관리하지 않지만, AWS Marketplace에서 파트너 및 오픈 소스 커뮤니티가 제공하는 다양한 제품을 선택할 수 있습니다.



이 슬라이드에서 보는 것처럼 고객이 VPN 연결의 고객 측 중복성과 장애 조치를 구현할 수 있도록, AWS의 VGW는 다수의 고객 게이트웨이 연결을 지원 및 권장합니다. 라우팅 구성 시 고객에게 유연성을 제공하도록 동적 및 정적 라우팅 옵션 둘 다 제공됩니다. 동적 라우팅은 BGP 피어링을 사용하여 AWS와 해당 원격 엔드포인트 간에 라우팅 정보를 교환합니다. 또한, 동적 라우팅을 사용하면 고객이 BGP 광고의 가중치(지표), 라우팅 속성 및 정책을 지정하고 네트워크와 AWS 간의 네트워크 경로에 영향을 줄 수 있습니다.

AWS Direct Connect (DX)



AWS Direct Connect (DX)는 1 또는 10Gbps의 전용 프라이빗 네트워크 연결을 제공합니다.



AWS Direct Connect



데이터 전송 비용 감소

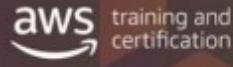


예측 가능한 지표로 애플리케이션 성능 향상

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

AWS Direct Connect(DX)는 인터넷을 통한 단순한 연결을 넘어, 중요한 애플리케이션을 위해 AWS 네트워크에 규모, 속도 및 일관성을 가지고 액세스할 수 있는 고유한 솔루션입니다. DX에는 인터넷이 필요하지 않습니다. 대신 사용자의 온프레미스 솔루션과 AWS 간에 프라이빗 네트워크 연결을 사용합니다.

DX 사용 사례



AWS Direct Connect

- 하이브리드 클라우드 아키텍처
- 지속적인 대용량 데이터 세트 전송
- 네트워크 성능 예측 가능성
- 보안 및 규정 준수

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

서비스 이점

DX는 다양한 시나리오에서 유용합니다. 아래에 몇 가지 시나리오가 나와 있습니다.

대용량 데이터 세트 전송

AWS 클라우드와 데이터 센터 간에 전송해야 하는 대용량 데이터 세트에서 작동하는 HPC 애플리케이션을 예로 들어보겠습니다. 이러한 애플리케이션의 경우, DX를 사용해 AWS 클라우드에 연결하는 것이 좋은 해결책이 됩니다. 데이터 센터나 사무실 위치에서 네트워크 전송의 인터넷 대역폭을 두고 경쟁할 필요가 없습니다.

고대역폭 연결은 잠재적 네트워크 혼잡과 애플리케이션 성능 저하를 줄여줍니다.

네트워크 전송 비용 절감

대용량 데이터 세트 전송에 DX를 사용함으로써, 애플리케이션이 사용하는 인터넷 대역폭을 제한할 수 있습니다. 이를 통해 인터넷 서비스 공급자(ISP)에게 지불하는 네트워크 비용을 절감하고 인터넷 대역폭 증가 약정 또는 새로운 계약에 비용을 지불할 필요가 없습니다.

또한, DX를 통해 전송되는 모든 데이터는 인터넷 데이터 전송 요금이 아닌 저렴한 DX 데이터 전송 요금으로 부과되어 네트워크 비용을 크게 절약할 수 있습니다.

애플리케이션 성능 향상

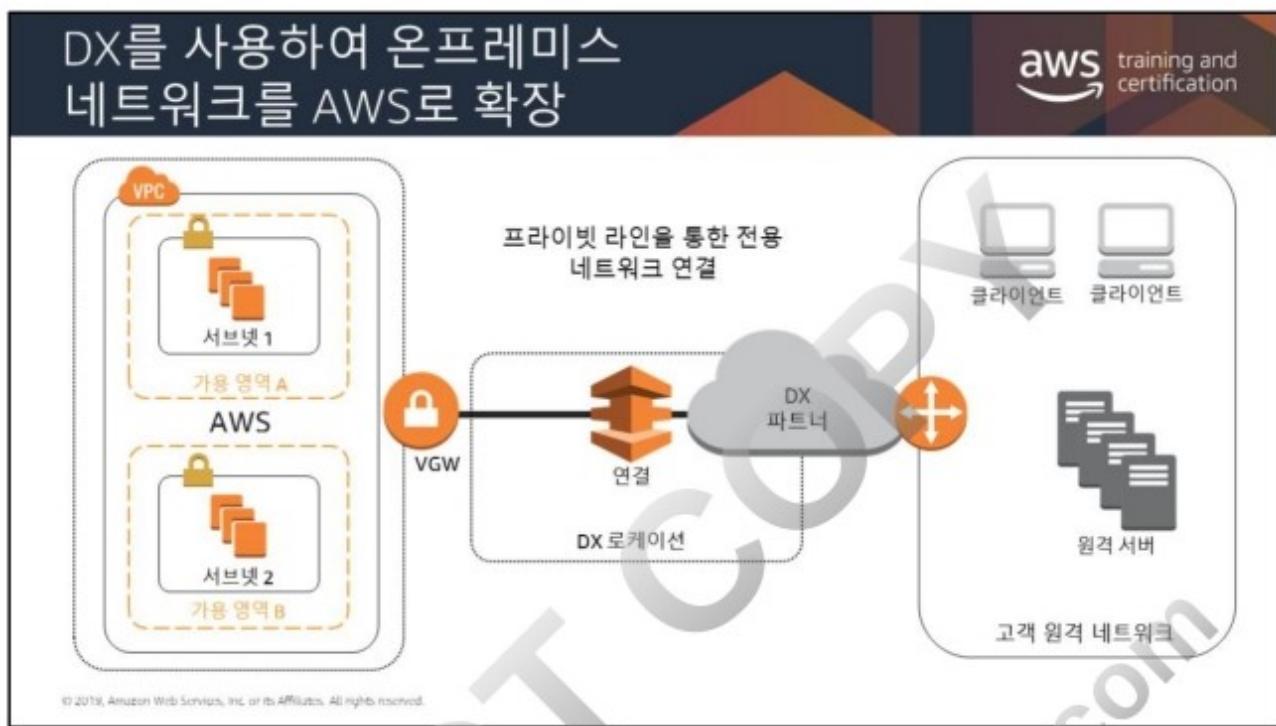
예측 가능한 네트워크 성능이 필요한 애플리케이션도 DX를 활용할 수 있습니다. 오디오 또는 동영상 스트림과 같은 실시간 데이터 피드에서 운영되는 애플리케이션이 그 예입니다. 이러한 경우, 전용 네트워크 연결이 표준 인터넷 연결보다 더 일관된 네트워크 성능을 제공할 수 있습니다.

보안 및 규정 준수

엔터프라이즈 보안 또는 규제 정책에 따라 AWS 클라우드에 호스팅된 애플리케이션이 프라이빗 네트워크 회로로만 액세스되도록 해야 할 경우가 있습니다. DX에서는 데이터 센터와 애플리케이션 간의 트래픽이 전용 프라이빗 네트워크 연결을 통해서만 전송되므로 이러한 요구 사항을 기본적으로 충족합니다.

하이브리드 클라우드 아키텍처

고객이 소유한 기존 데이터 센터 장비에 액세스해야 하는 애플리케이션도 DX를 활용할 수 있습니다. 다음 섹션에서는 이러한 사용 사례를 다루고, DX에서 지원할 수 있는 다른 시나리오도 소개합니다.



이점:

- 예측 가능한 네트워크 성능
- 대역폭 비용 감소
- 1Gbps 또는 10Gbps 프로비저닝된 연결
- BGP 피어링과 라우팅 정책 지원

AWS에서는 Equinix, Coresite, Eircom, TelecityGroup 및 Terramark와의 긴밀한 협력을 통해 전 세계 모든 AWS 리전에 대한 글로벌 DX 액세스를 구축했습니다. 일부 로케이션에서는(LA, 뉴욕 및 런던), 이 서비스의 기능을 확장하여 추가적인 IT 핫 스팟에 대한 액세스도 제공합니다.

제한 사항:

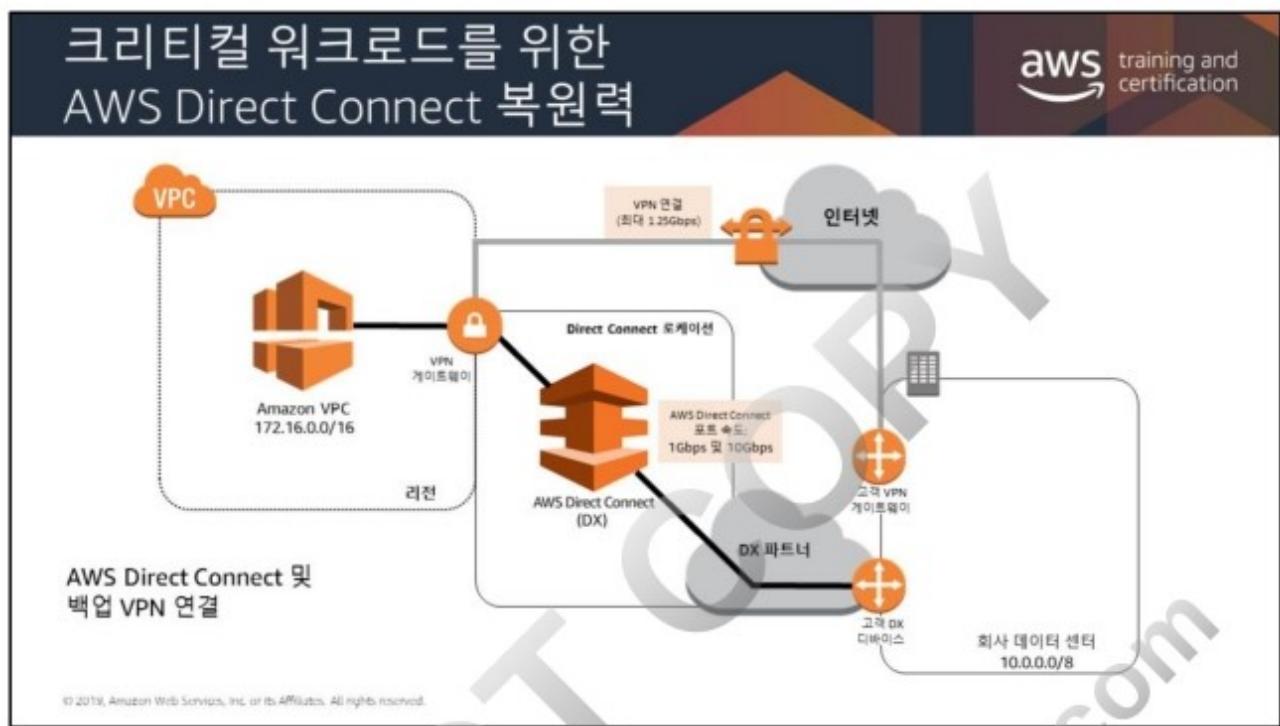
통신 및 호스팅 제공업체가 추가로 필요하거나 새로운 네트워크 회로를 프로비저닝해야 할 수도 있습니다.

DX를 사용하면 온프레미스에서 Amazon VPC로 전용 네트워크 연결을 손쉽게 구축할 수 있습니다. 고객은 DX를 사용해 AWS와 고객의 데이터 센터, 사무실 또는 코로케이션 환경 간에 프라이빗 연결을 설정할 수 있습니다. 이 프라이빗 연결은 네트워크 비용을 줄이고, 대역폭 처리량을 높이며, 인터넷 기반 연결보다 더 일관된 네트워크 환경을 제공합니다.

DX를 사용하면 고객은 DX 로케이션 중 하나와 AWS 네트워크 간에 1Gbps 또는 10Gbps 전용 네트워크 연결(또는 다수의 연결)을 구축하고, 산업 표준 VLAN을 사용하여 프라이빗 IP 주소를 사용하는 VPC 내에서 실행되는 Amazon EC2 인스턴스에 액세스할 수 있습니다. 고객은 DX 로케이션에 있는 DX 엔드포인트를 원격 네트워크와 통합하기 위해 WAN 서비스 공급자의 에코시스템을 선택할 수도 있습니다.

현재 AWS DX 로케이션의 목록은 <http://aws.amazon.com/directconnect/details/>를 참조하십시오.

크리티컬 워크로드를 위한 높은 복원력의 AWS Direct Connect 사용 방법에 대한 정보는 <https://aws.amazon.com/directconnect/resiliency-recommendation/>을 참조하십시오.



AWS 고객은 더 저렴한 백업 연결과 결합하여 하나 이상의 AWS Direct Connect(DX) 연결을 AWS에 대한 기본 연결에 사용할 수 있습니다. 이 목표를 달성하기 위해 위 다이어그램에 표시된 대로 VPN 백업을 사용하여 DX 연결을 설정할 수 있습니다.

이 예의 구성은 2개의 동적 라우팅 연결로 구성됩니다. 2개의 고객 디바이스로부터 하나는 DX 연결을 사용하고 다른 하나는 VPN 연결을 사용합니다. AWS는 DX 및 동적 라우팅 VPN 연결을 설정하는 데 도움이 되는 라우터 구성 예를 제공합니다. 기본적으로 AWS는 사용자의 DX 연결을 통해 트래픽을 전송하는 것을 항상 선호합니다. 따라서 기본 및 백업 연결을 정의하기 위한 추가 AWS 관련 구성이 필요하지 않습니다. 하지만 고객은 내부 시스템이 올바른 경로를 선택하도록 DX와 VPN 전용 내부 라우팅 전파를 구성해야 합니다. 다중 데이터 센터 HA 네트워크 연결 솔루션 개요에 이 시나리오를 위한 라우팅 조작 옵션이 자세히 설명되어 있습니다. 하지만 단일 데이터 센터에서 AWS로 연결하는 대부분의 고객은 일반적으로 기본 구성이면 충분합니다.

AWS Direct Connect는 단일 모드 광섬유를 통해 다음 포트 속도를 지원합니다.
1Gbps: 1000BASE-LX(1310nm) 및 10 Gbps: 10GBASE-LR(1310nm).

AWS 관리형 VPN은 VPN 터널 당 최대 1.25Gbps의 처리량을 지원하며 동일한 VGW에 종료되는 AWS 관리형 VPN 터널이 여러 개인 경우 외부 데이터 경로에 대해 ECMP(Equal Cost Multi Path)를 지원하지 않습니다.

이 접근 방식을 통해 AWS 트래픽의 기본 네트워크 경로 및 네트워크 공급자를 선택할 수 있으며, 백업 VPN 연결에 대해 다른 공급자를 사용할 수도 있습니다. 조직의 위험 허용도, 예산 및 데이터 센터 연결 정책에 부합하는 네트워크 공급자와 AWS Direct Connect 로케이션을 선택하십시오. 예를 들어, 네트워크 공급자 가동 중단과 관련된 위험이 우려된다면 AWS Direct Connect 및 인터넷 연결에 서로 다른 네트워크 공급자를 사용할 것을 고려할 수 있습니다. 하지만 이 설계는 단일 고객 위치로부터 AWS 연결을 제공하므로 중복 네트워크 공급자 구성을 사용하더라도 모든 위치 관련 중단(예: 정전 또는 시설 외부 케이블 절단)이 여전히 AWS 연결에 영향을 미칠 수 있습니다. 또한, VPN 연결이 애플리케이션의 지연 시간 및 대역폭 요구 사항을 지원하는 데 충분한 백업이 되고 있는지 AWS Direct Connect 사용률을 모니터링해야 합니다.

VPC 연결

aws training and certification

- 일반적으로 일부 워크로드를 격리하는 것이 좋습니다.
- 그러나 둘 이상의 VPC 간에 데이터를 전송해야 할 수도 있습니다.

The diagram illustrates three separate Virtual Private Clouds (VPCs) represented by orange cloud icons. Below each icon is a white rectangular box containing the Korean word for the environment: '개발' (Development), '테스트' (Test), and '프로덕션' (Production). The clouds are arranged horizontally, separated by thin lines.

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

비즈니스 또는 아키텍처 규모가 충분히 커지게 되면 보안 또는 아키텍처 측면의 필요를 위해 또는 단지 단순성을 위해 별도의 논리적 요소가 필요할 것입니다.

VPC 연결 - VPC 피어링

인스턴스는 피어링 연결을 통해 동일한 네트워크에 있는 것처럼 통신할 수 있습니다.

- 프라이빗 IP 주소 사용
- 내부 및 리전 간 지원
- IP 공간은 중복될 수 없음
- 두 VPC 간 하나의 피어링 리소스만 해당
- 전이적 피어링 관계는 지원되지 않음
- 서로 다른 AWS 계정 간에 설정 가능

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

다이어그램에서 Dev VPC와 Test VPC는 피어링되어 있습니다. 그러나 이는 Prod가 Dev와 통신할 수 있다는 것을 의미하지는 않습니다. 기본적으로 VPC 피어링에서는 명시적으로 피어로 설정되어 있지 않으면 Prod가 Dev에 연결하도록 허용하지 않습니다. 따라서 어떤 VPC가 서로 통신할 수 있는지 제어할 수 있습니다.

VPC 피어링 연결을 설정하려면, 요청자 VPC(또는 로컬 VPC)의 소유자가 피어 VPC의 소유자에게 요청을 전송하여 VPC 피어링 연결을 생성합니다. 피어 VPC는 여러분이나 다른 AWS 계정에서 소유할 수 있으며, CIDR 블록이 요청자 VPC의 CIDR 블록과 중복되어서는 안 됩니다. 피어 VPC의 소유자가 VPC 피어링 연결 요청을 수락해야 VPC 피어링 연결이 활성화됩니다. 프라이빗 IP 주소를 사용하여 피어 VPC 간에 트래픽이 전송되도록 하려면, VPC의 라우팅 테이블에 피어 VPC의 IP 주소 범위를 가리키는 하나 이상의 경로를 추가합니다. 피어 VPC의 소유자는 자신의 VPC 라우팅 테이블에 여러분의 VPC IP 주소 범위를 가리키는 하나 이상의 경로를 추가합니다. 또한, 인스턴스와 연결된 보안 그룹 규칙을 업데이트하여 피어 VPC로 송수신되는 트래픽이 제한되지 않도록 해야 할 수 있습니다.

VPC 피어링 연결은 두 VPC 간에 일대일 관계입니다. 소유한 각 VPC에 대해 여러 개의 VPC 피어링 연결을 생성할 수 있지만, 전이적 피어링 관계는 지원되지 않습니다. VPC는 직접 피어링되지 않은 VPC와는 피어링 관계를 갖지 않습니다. 자신의 VPC 사이에서, 또는 단일 리전 내에 있는 다른 AWS 계정의 VPC 사이에서 VPC 피어링 연결을 만들 수도 있습니다.

이제 서로 다른 리전에 있는 VPC 사이에서도 피어링 관계를 설정할 수 있습니다. 리전 간 VPC 피어링을 통해 서로 다른 리전에서 실행되는 Amazon EC2 인스턴스, Amazon RDS 데이터베이스, Lambda 함수 같은 VPC 리소스가 게이트웨이, VPN 연결 또는 별도의 네트워크 어플라이언스 없이 프라이빗 IP 주소를 사용하여 서로 통신할 수 있습니다. 리전 간 VPC 피어링 연결을 통해 전송되는 데이터에는 표준 리전 간 데이터 전송 요금이 부과됩니다.

VPC 피어링

aws training and certification

- 인터넷 게이트웨이 또는 가상 게이트웨이가 필요 없음
- 고가용성 연결, 단일 장애 지점 없음
- 대역폭 병목 현상 없음
- 트래픽은 항상 글로벌 AWS 백본에서 유지됨

The diagram shows two VPCs, VPC A and VPC B, connected via a central VPC Peering connection labeled 'PCX-1'. VPC A has an IP range of 10.2.0.0/16 and VPC B has an IP range of 10.1.0.0/16. Each VPC contains an orange cloud icon labeled 'VPC'. Between them are two tables labeled '라우팅 테이블' (Routing Table) with the following entries:

라우팅 테이블	
목적지	대상
10.1.0.0/16	로컬
10.2.0.0/16	PCX-1

라우팅 테이블	
목적지	대상
10.1.0.0/16	로컬
10.2.0.0/16	PCX-1

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

다른 VPC와 VPC 피어링 연결을 생성하려면, 다음 제한과 규칙을 이해해야 합니다.

- VPC당 생성할 수 있는 활성 및 보류 VPC 피어링 연결의 수에는 제한이 있습니다.
- VPC 피어링은 전이적 피어링 관계를 지원하지 않습니다. VPC 피어링 연결에서 VPC는 피어 VPC가 피어링되어 있는 다른 VPC에 액세스할 권한이 없습니다. 이는 모든 것이 자신의 AWS 계정 내에 설정되어 있는 VPC 피어링 연결에도 적용됩니다.
- 동일한 2개의 VPC 간에 동시에 두 개 이상의 VPC 피어링 연결을 생성할 수 없습니다.
- VPC 피어링 연결에서 MTU(최대 전송 단위)는 1,500바이트입니다.
- 배치 그룹은 피어링된 여러 VPC를 포괄할 수 있지만, 피어링된 VPC의 인스턴스 간에는 양방향 대역폭이 제공되지 않습니다.
- VPC 피어링 연결에서는 유니캐스트 역경로 전달은 지원되지 않습니다.
- 피어링된 VPC에서 인스턴스 간에 프라이빗 DNS 값을 확인할 수 없습니다.
- 리전 간 VPC 피어링을 사용하는 트래픽은 전 세계의 AWS 백본에 항상 머무르며 퍼블릭 인터넷을 통과하지 않으므로 일반적인 도용 및 DDoS 공격 같은 위협 벡터를 줄입니다.

이제 인바운드 및 아웃바운드 규칙 모두에서 피어링된 VPC의 보안 그룹을 참조할 수 있습니다. 이 기능은 교차 계정으로 지원되므로 두 VPC가 계정이 서로 다를 수 있습니다. 피어링된 VPC 내 보안 그룹 참조에 대한 지원은 CIDR 범위 대신 보안 그룹 멤버십을 통해 피어링 트래픽을 제어하여 VPC 구성의 간소화를 줍니다. 콘솔, AWS CLI 및 SDK를 사용하여 피어링된 VPC에서 보안 그룹을 참조할 수 있습니다.

DO NOT COPY
zlagusdbs@gmail.com

여러 VPC 피어링

aws training and certification

일반 모범 사례

다음과 같이 여러 VPC를 연결할 때 고려해야 할 몇 가지 범용 네트워크 설계 원칙이 있습니다.

목적지	대상
10.1.0.0/16	로컬
10.2.0.0/16	VPC-1

중복되는 CIDR
블록 없음

VPC

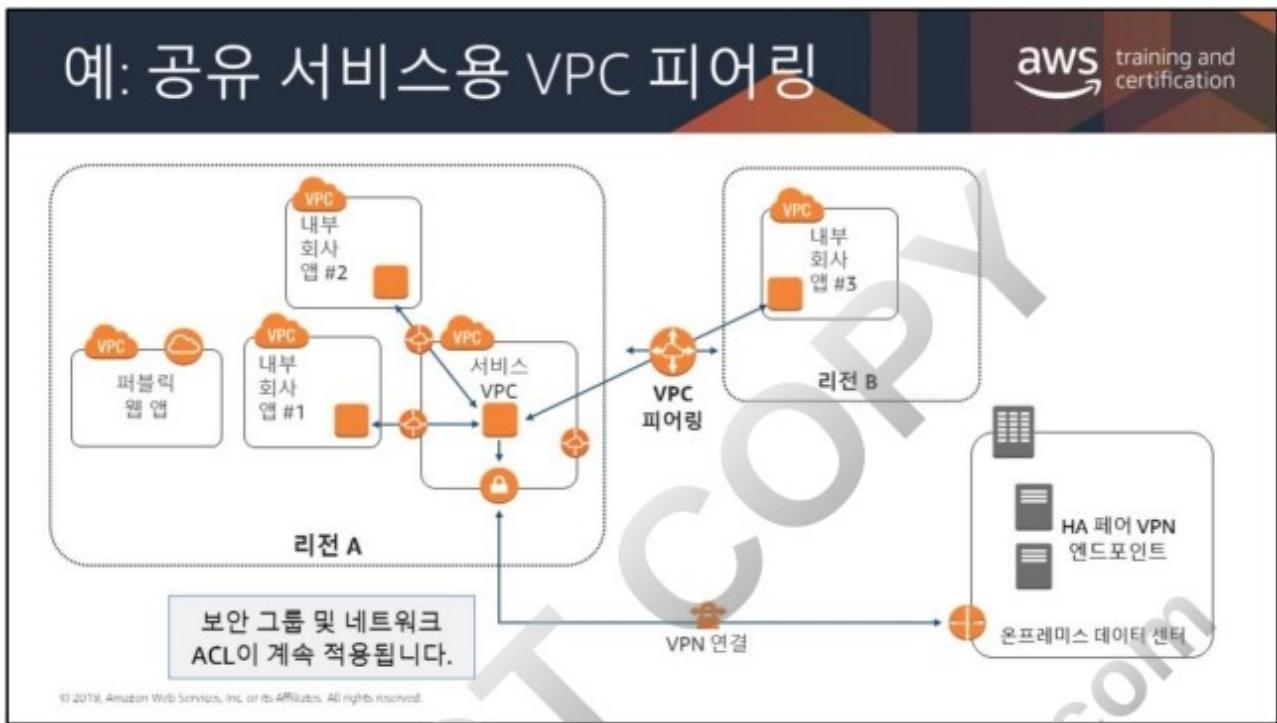
필수 VPC만 연결

솔루션을 확장할 수
있어야 함

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

단일 AWS 리전의 여러 VPC를 연결할 때 고려해야 할 몇 가지 범용 네트워크 설계 원칙이 있습니다.

- VPC 네트워크 범위(CIDR 블록)가 중복되지 않아야 합니다.
- 선택한 솔루션이 현재 및 미래의 VPC 연결 수요에 따라 확장이 가능한지 확인해야 합니다.
- 단일 장애 지점이 없는 고가용성(HA) 설계를 구현해야 합니다.
- 솔루션 선택에 영향을 미치므로 데이터 전송 요구를 고려해야 합니다. 데이터 전송량을 기준으로 어떤 솔루션은 다른 솔루션보다 비용이 높을 수 있습니다.
- 반드시 서로 통신해야 하는 VPC들만 연결해야 합니다.



이 예에서는, 맙은 책임을 이행하기 위해, 기업 IT 및 기업 정보 보안 그룹이 각 부서에서 피어링할 수 있는 "서비스 VPC"를 제공합니다. 이 VPC는 Active Directory 연결, 보안 검사 도구, 모니터링/로깅 도구 및 다양한 기타 기능을 포함하고 있습니다. 부서 VPC가 일부 온프레미스 리소스에 액세스하는 데 사용할 수 있는 프록시도 제공합니다.

VPC 피어링:

- **1 - 1 Peer** = 다른 VPC의 다른 앱으로부터 회사 앱을 분리하지만, 항상 dev/qa와 prod 사이에 임시 연결을 생성하여, 데이터를 전송하고, 연결을 제거할 수 있습니다.
- 보안 그룹 및 네트워크 ACL이 계속 적용됩니다.

다른 리전의 VPC와의 피어링 연결이 존재한다는 점을 유의하십시오. 이제 서로 다른 AWS 리전의 VPC 사이에 피어링 관계를 설정할 수 있습니다. 리전 간 VPC 피어링을 통해 서로 다른 AWS 리전에서 실행되는 EC2 인스턴스, Amazon RDS, Lambda 함수 같은 VPC 리소스가 게이트웨이, VPN 연결 또는 별도의 물리적 하드웨어 없이 프라이빗 IP 주소를 사용하여 서로 통신할 수 있습니다.

VPC 연결 - Transit Gateway



AWS Transit
Gateway

단일 게이트웨이로 최대 5,000개의 VPC와
온프레미스 환경 연결

네트워크 사이를 이동하는 모든 트래픽의 허브
역할 담당

가용성이 뛰어나고 유연한 완전 관리형 라우팅
서비스

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

17

Transit Gateway 실행 - 연결

aws training and certification

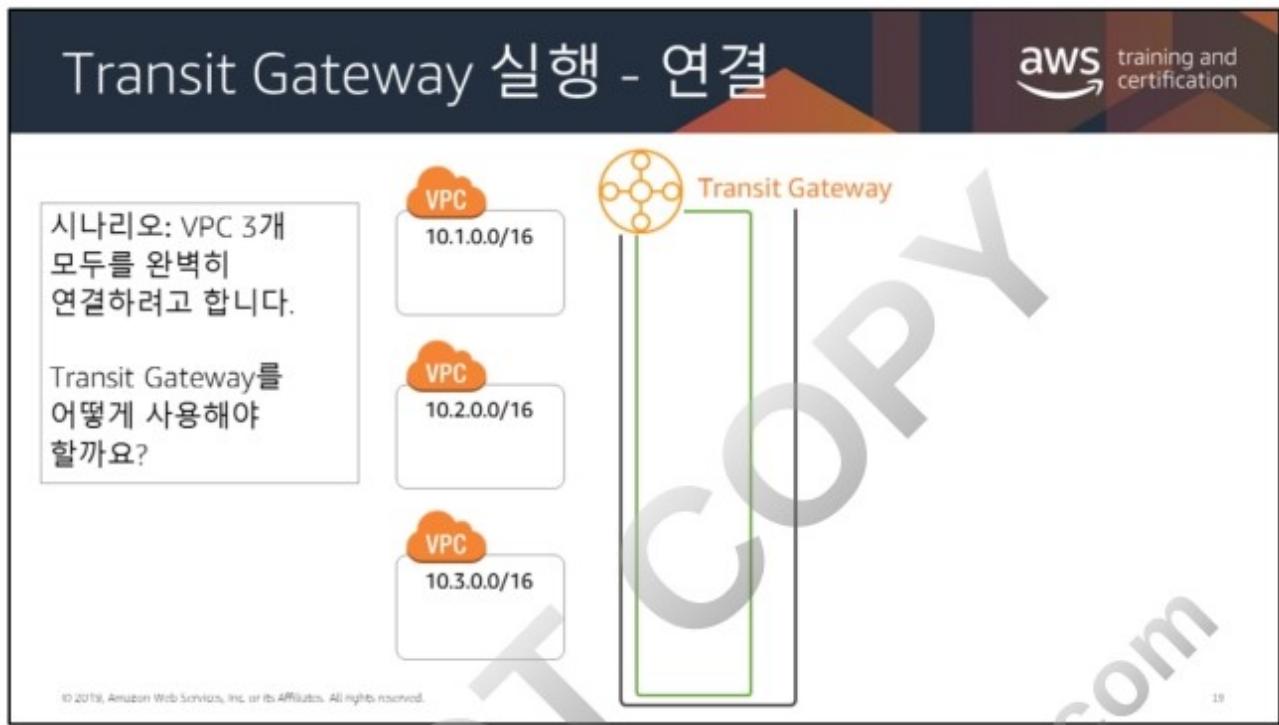
시나리오: VPC 3개 모두를 완벽히 연결하려고 합니다.

Transit Gateway를 어떻게 사용해야 할까요?

VPC 10.1.0.0/16
VPC 10.2.0.0/16
VPC 10.3.0.0/16

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved. 18

여러 VPC를 연결하는 것이 매우 바람직한 경우가 많습니다. 대규모 그룹에서 VPC 피어링 연결을 관리하는 것은 어렵고 짜증나는 일입니다. 시간 경과에 따른 환경 확장, 조정 방법, VPC 관리 방법을 염두에 두어야 합니다.



이 연결을 생성하는 첫 번째 단계는 transit gateway를 설정하는 것입니다. Amazon EC2 대시보드를 통해 이를 수행할 수 있습니다. transit gateway 사용 요금은 다양합니다. 아키텍처와 예산이 이를 지원하는지 확인하십시오.

Transit Gateway 실행 - 연결

aws training and certification

시나리오: VPC 3개 모두를 완벽히 연결하려고 합니다.

Transit Gateway를 어떻게 사용해야 할까요?

The diagram illustrates a network architecture where three separate Virtual Private Clouds (VPCs) are interconnected through a central Transit Gateway. Each VPC is represented by a cloud icon containing two orange circular icons, likely representing interfaces or endpoints. A green vertical line connects each VPC to a central green box labeled 'Transit Gateway'. The top VPC has an IP range of 10.1.0.0/16, the middle one has 10.2.0.0/16, and the bottom one has 10.3.0.0/16. This visualizes how multiple VPCs can be integrated into a single logical network via the Transit Gateway.

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

20

Transit Gateway는 서브넷에 배포된 네트워크 인터페이스를 통해 작동합니다.
Transit Gateway를 효과적으로 사용하려면 대상 VPC가 있는 가용 영역마다
하나의 attachment를 배포해야 합니다.

Transit Gateway 실행 - 연결

aws training and certification

시나리오: VPC 3개 모두를 완벽히 연결하려고 합니다.

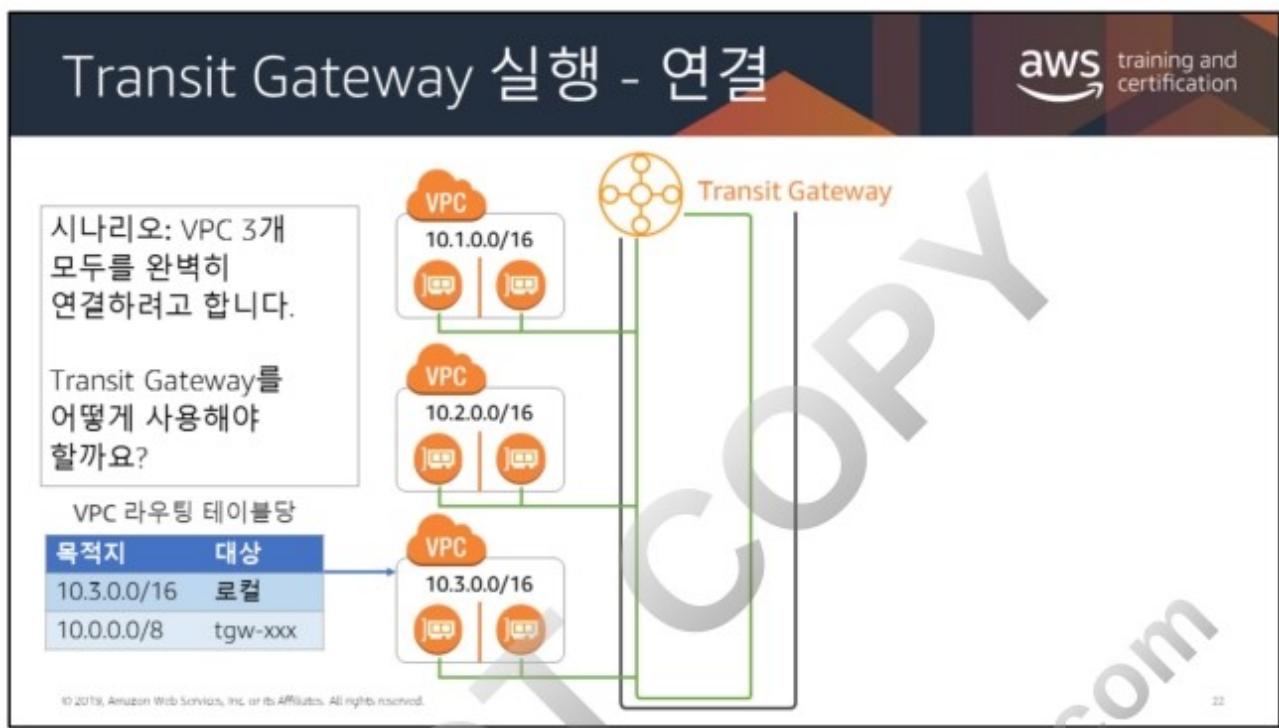
Transit Gateway를 어떻게 사용해야 할까요?

VPC 라우팅 테이블당

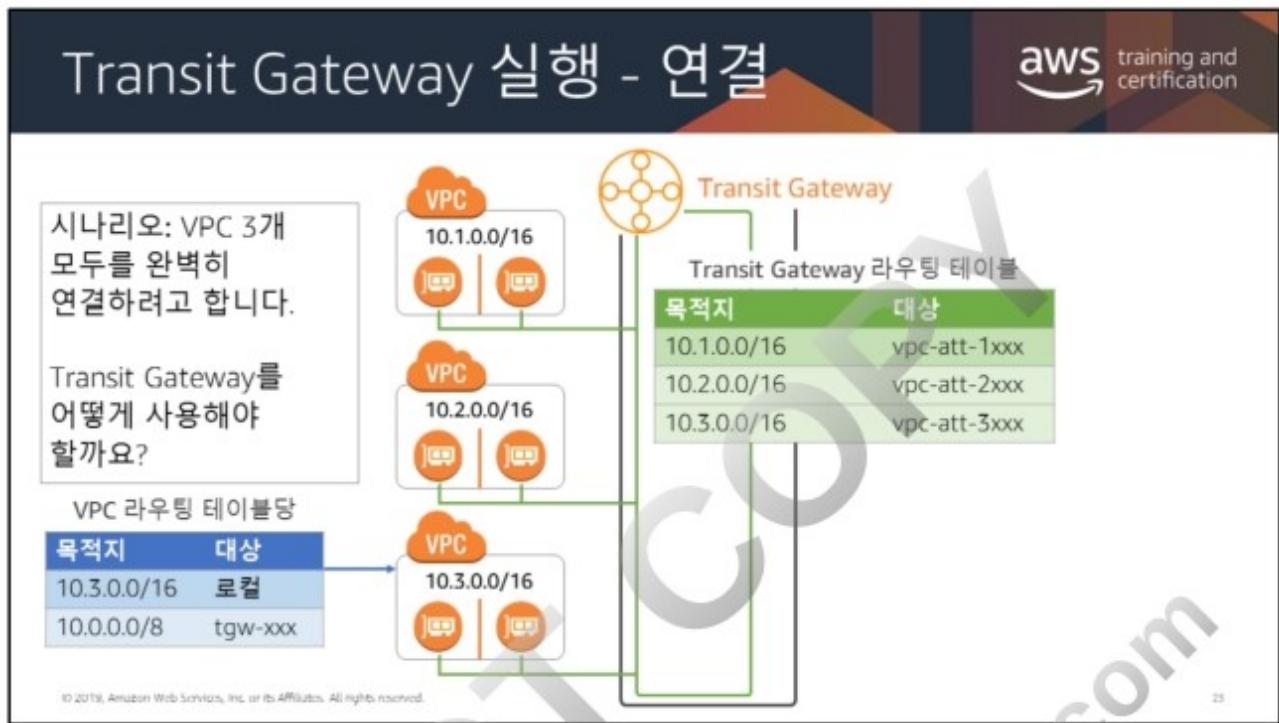
목적지	대상
10.3.0.0/16	로컬
10.0.0.0/8	tgw-xxx

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

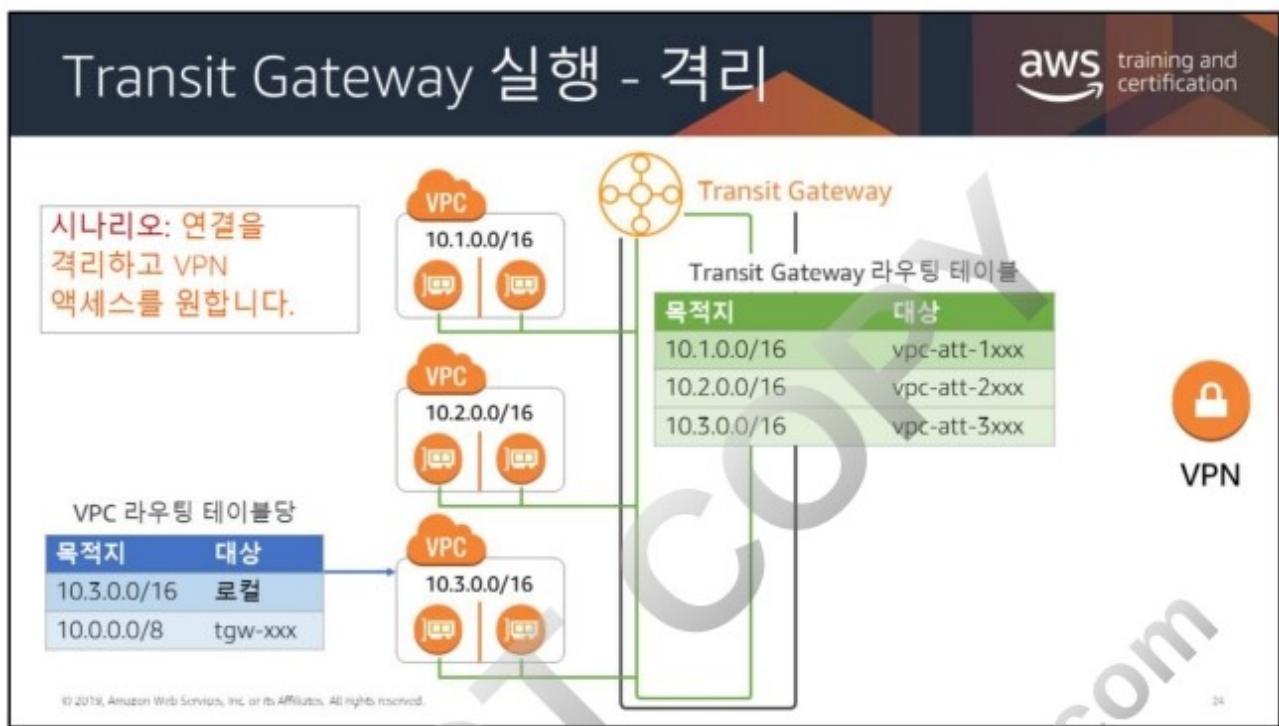
VPC의 각 라우팅 테이블에서 트래픽이 Transit Gateway attachment를 향해 외부로 라우팅되는지 확인하십시오.



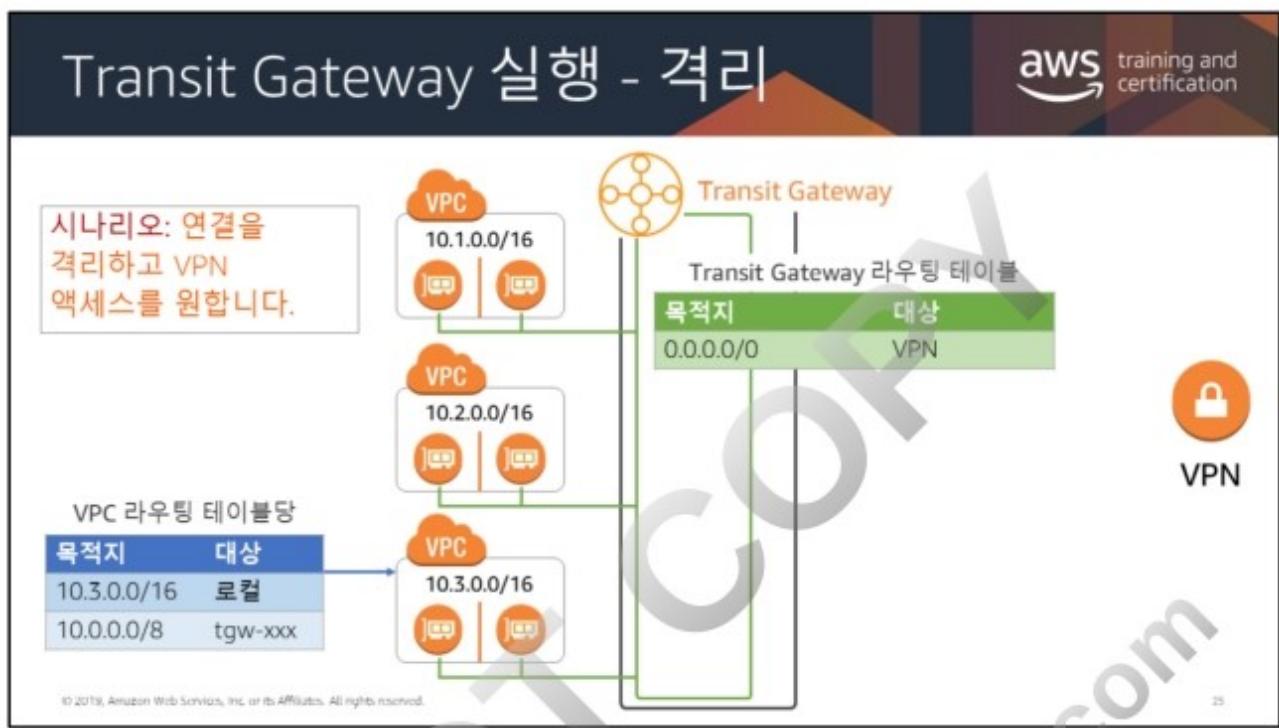
이러한 attachment는 Transit Gateway에 연결됩니다.



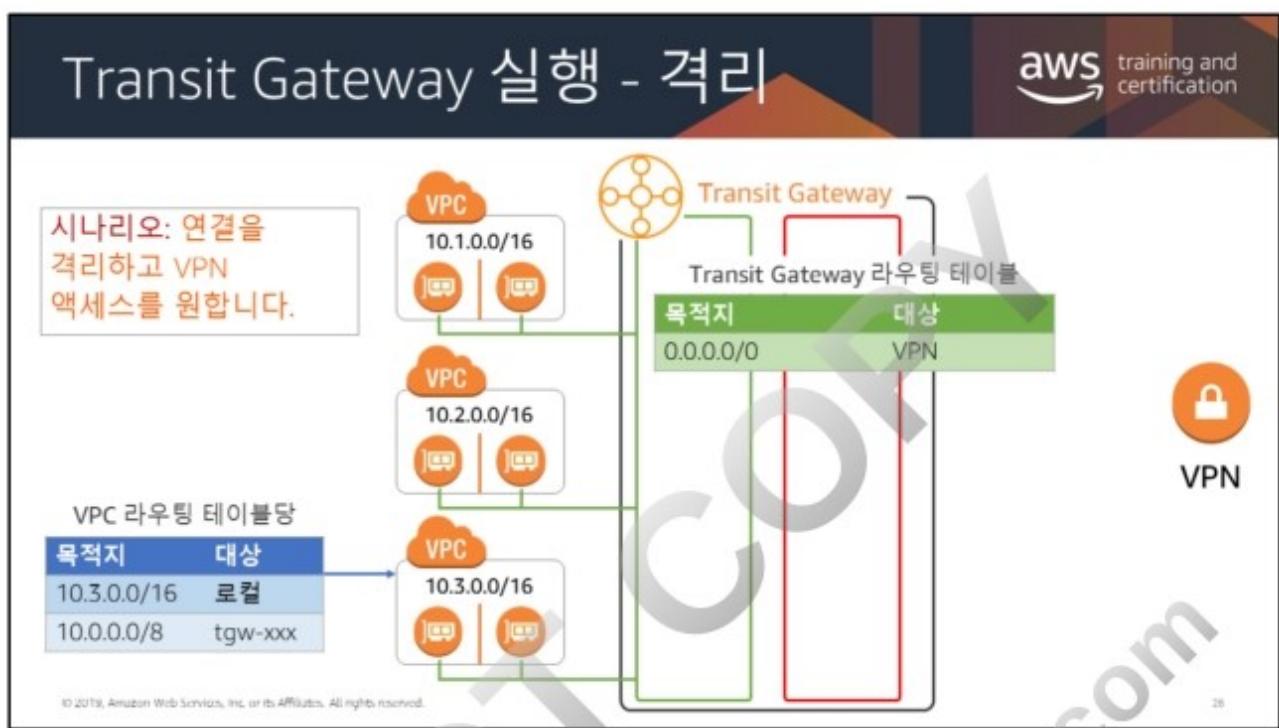
Transit Gateway 내부에서 라우팅 테이블을 생성하여 적절하게 트래픽을 전달할 수 있습니다. 매우 구체적으로 상호 작용하는 라우팅 테이블이 여러 개 있을 수 있습니다. 여기서는 하나의 라우팅 테이블로 전체 연결을 허용합니다.



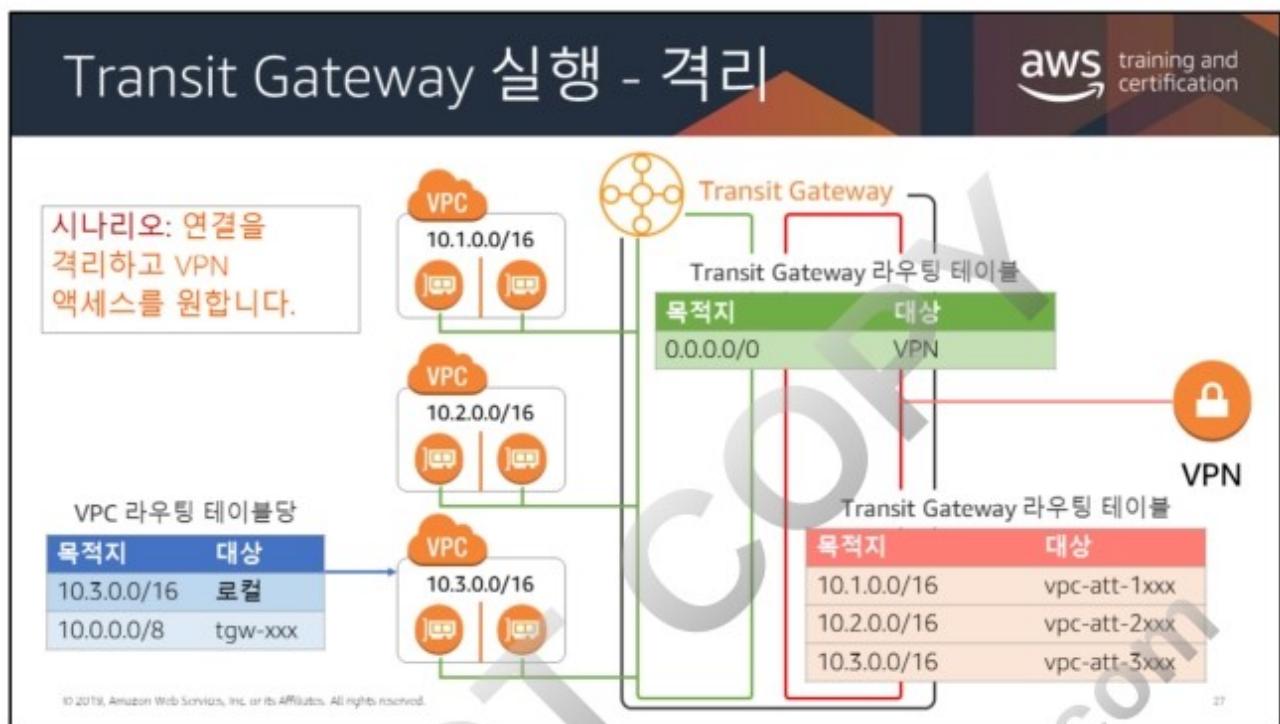
일반적인 아키텍처는 VPN 소스에서 환경에 대한 전체 액세스 권한을 갖는 것입니다. 이 시나리오에서는 또한 VPC가 서로 통신하지 않게 할 것입니다.



먼저 초기 테이블의 경로를 수정하여 VPN 연결을 향하도록 합니다. 그러면 VPC 간 통신이 중지되고 아웃바운드 액세스를 제공합니다.



이제 VPN에만 연결된 격리된 환경을 생성합니다. Transit Gateway 내에 다른 라우팅 테이블을 추가합니다.



VPN에서 대상 VPC를 향하도록 이 라우팅 테이블을 설정합니다. 이제 교차 통신이 없는 격리되고 안전한 VPN 액세스를 얻었습니다.

VPC 엔드포인트

AWS를 벗어나지 않고 EC2 인스턴스를 VPC 외부 서비스와 프라이빗하게 연결합니다.

인터넷 게이트웨이, VPN, NAT (Network Address Translation) 디바이스 또는 방화벽 프록시를 사용할 필요가 없습니다.



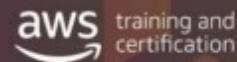
- 인터넷을 통해 통과할 필요가 없습니다.
- 동일한 리전에 있어야 합니다.
- 가용성이 뛰어나고, 중복적이며, 수평적으로 확장됩니다.

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

Amazon VPC 엔드포인트는 AWS 네트워크를 벗어나지 않고 VPC와 다른 AWS 서비스 간에 프라이빗 연결이 가능하게 합니다. 엔드포인트를 사용하면 Amazon EC2 인스턴스가 프라이빗 IP 주소로 동일한 리전의 AWS 서비스와 통신할 수 있습니다. 인터넷에서 우회하거나 NAT 인스턴스, VPN 연결 또는 DX를 통과할 필요가 없습니다. 또한 VPC 엔드포인트는 특정 VPC에서 액세스할 수 있는 Amazon S3 버킷을 제어하거나 S3 버킷을 특정 VPC로 잠그는 정책을 추가하는 등의 추가 보안 기능도 제공합니다. 현재, AWS에서는 Amazon S3 및 Amazon DynamoDB와 연결을 위한 VPC 엔드포인트만 지원합니다.

엔드포인트는 가상 디바이스입니다. 수평 확장되고 가용성이 높은 중복 VPC 구성 요소로서 가용성 위험이나 네트워크 트래픽에 대한 대역폭 제약 없이 VPC의 인스턴스와 서비스 간에 통신할 수 있습니다.

두 가지 유형의 엔드포인트



인터페이스 엔드포인트

- Amazon CloudWatch Logs
- AWS CodeBuild
- Amazon EC2 API
- Elastic Load Balancing API
- AWS Key Management Service (AWS KMS)
- Amazon Kinesis Data Streams
- AWS Service Catalog
- Amazon Simple Notification Service (Amazon SNS)
- AWS Systems Manager
- 다른 AWS 계정에서 호스팅하는 엔드포인트 서비스
- 그 외 다수

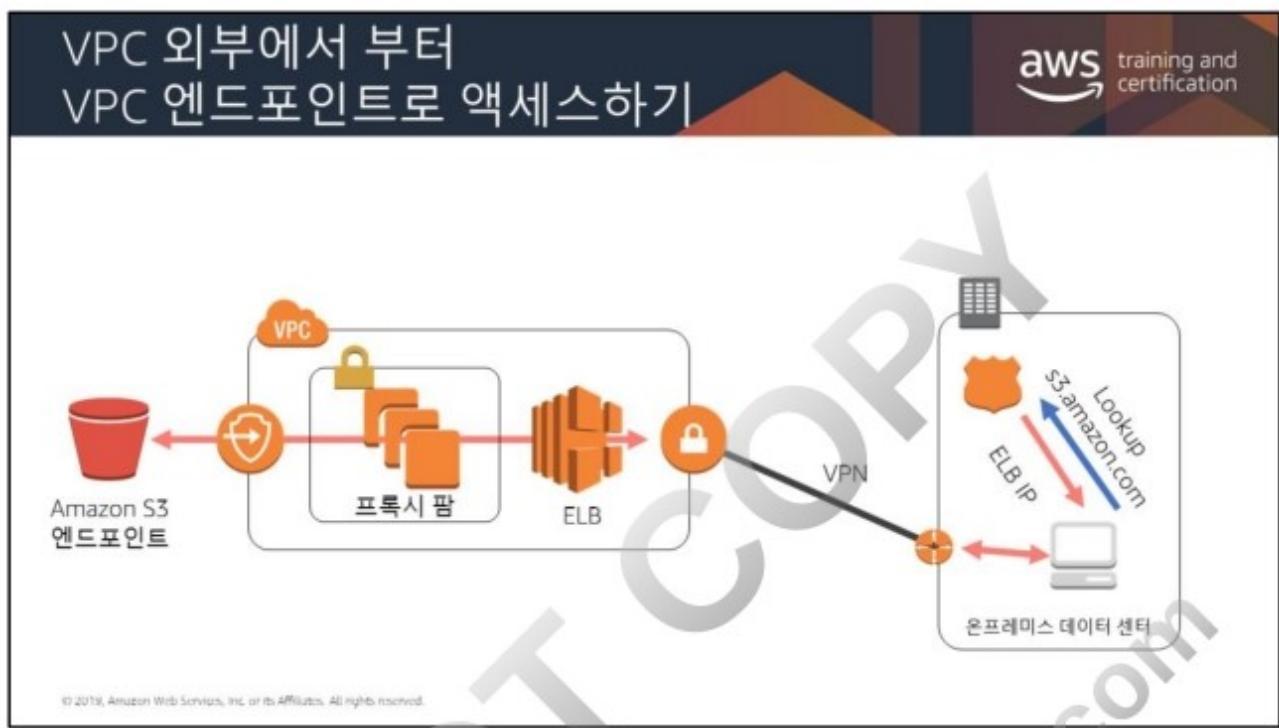
게이트웨이 엔드포인트

- Amazon Simple Storage Service(Amazon S3)
- Amazon DynamoDB

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

인터페이스 엔드포인트는 지원되는 서비스로 향하는 트래픽의 진입점 역할을 하는 프라이빗 IP 주소가 할당된 탄력적 네트워크 인터페이스입니다.

게이트웨이 엔드포인트는 라우팅 테이블의 지정된 라우팅의 대상인 게이트웨이로, 지원되는 AWS 서비스의 트래픽에 사용됩니다.



기업 도메인 이름 서비스(DNS)

원격 네트워크에서 VPC 엔드포인트를 사용하는 첫 번째 단계는 엔드포인트를 통해 리디렉션 할 트래픽을 식별하는 것입니다. 이 솔루션은 기업 DNS 서버를 사용해 VPC 엔드포인트 전용 트래픽에 대한 DNS 확인을 무시합니다. 위 예제에서 DNS 서버는 `s3.amazonaws.com`을 내부 ELB 로드 밸런서로 확인하도록 구성되어 있습니다. 이 로드 밸런서는 미국 표준 S3 버킷으로 향하는 트래픽을 VPC 엔드포인트로 리디렉션합니다. 그러면 기업 네트워크에서 S3 버킷으로 가는 Amazon S3 요청이 인터넷을 경유하지 않고 프라이빗 VPN 또는 DX 연결을 통해 전송됩니다.

Elastic Load Balancing (ELB)

ELB는 수신되는 Amazon S3 TCP, UDP 연결을 여러 Amazon EC2 프록시 인스턴스로 자동 분산시킵니다. 그러므로 S3 트래픽을 여러 프록시 서버로 분산하는 데 필요한 로드 밸런싱 용량을 원활하게 제공함으로써 프록시 팝의 내결합성 수준을 개선할 수 있습니다. 또한 ELB 로드 밸런서가 여러 가용 영역을 사용하여 내결합성을 최대화하도록 구성하십시오.

프록시 팜

프록시 팜은 Amazon S3 트래픽을 VPC 엔드포인트로 프록시합니다. 프록시 팜은 ACL(액세스 제어 목록)을 사용하여 VPC 엔드포인트 트래픽에 대한 추가 제어를 제공할 수 있습니다. ACL은 솔루션을 사용할 권한이 부여될 원격 사용자 또는 네트워크를 지정할 수 있으며, 클라이언트가 액세스할 수 있는 VPC 엔드포인트 또는 대상 도메인을 추가로 제한할 수 있습니다. Auto Scaling 그룹이 프록시 서비스를 관리하고 프록시 서버 로드에 따라 자동으로 필요한 인스턴스 수를 확장 또는 축소하도록 구성하십시오.

DO NOT COPY
zlagusdbs@gmail.com



Elastic Load Balancing (ELB)

수신되는 애플리케이션 트래픽을 여러 Amazon EC2 인스턴스, 컨테이너 및 IP 주소에 걸쳐 분산하는 관리형 로드 밸런싱 서비스.

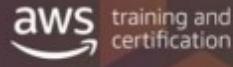
The diagram shows a user icon with a blue arrow pointing to an orange rectangular icon labeled 'ELB'. From the ELB icon, three blue arrows branch out to three separate orange square icons, each containing the Korean character '앱' (App).

Elastic Load
Balancing

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

웹 계층의 기반은 아키텍처에서 ELB의 사용을 포함합니다. 이러한 로드 밸런서는 EC2 인스턴스로 트래픽을 전송할 뿐만 아니라, AWS가 제공하는 관리형 모니터링 서비스인 Amazon CloudWatch로 지표를 전송할 수 있습니다. Amazon EC2 및 ELB의 지표는 트리거의 역할을 할 수 있습니다. 따라서 자연 시간이 유난히 길거나 AWS 서버 사용률이 지나치게 높아지고 있음을 알게 되는 경우, Auto Scaling을 활용하여 AWS 웹 서버 집합에 용량을 추가할 수 있습니다.

ELB: 기능



Elastic Load Balancing

- HTTP, HTTPS, TCP, UDP 및 SSL(보안 TCP, UDP) 프로토콜을 사용합니다.
- 외부 또는 내부에 위치할 수 있습니다.
- 각 로드 밸런서에 DNS 이름이 부여됩니다.
- 비정상 인스턴스를 인식하고 이에 대응합니다.

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

ELB는 수신되는 애플리케이션 트래픽을 Amazon EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상으로 자동 분산시킵니다. 단일 가용 영역 또는 여러 가용 영역에서 애플리케이션 트래픽의 다양한 로드를 처리할 수 있습니다. ELB가 제공하는 세 가지 로드 밸런서는 모두 애플리케이션의 내결함성에 필요한 고가용성, 자동 확장/축소, 강력한 보안을 갖추고 있습니다.

ELB: 옵션

The slide features a large watermark 'NOT COPY' diagonally across the center. In the top right corner is the AWS logo with the text 'training and certification'. The main content area has a blue header 'Application Load Balancer' containing a circular icon with 'HTTP' and 'HTTPS' text. Below this is a bulleted list:

- 유연한 애플리케이션 관리
- HTTP 및 HTTPS 트래픽의 고급 로드 밸런싱
- 요청수준(계층 7)에서 운영됨
- (계층 7)

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

ELB는 Application Load Balancer, Network Load Balancer, Classic Load Balancer 등 세 가지 유형의 로드 밸런서를 지원합니다. 애플리케이션 요구 사항에 따라 로드 밸런서를 선택할 수 있습니다.

애플리케이션 로드 밸런서는 개방형 시스템 간 상호 연결(OSI) 모델의 일곱 번째 계층인 애플리케이션 계층에서 작동합니다. Application Load Balancer는 콘텐츠 기반 라우팅을 지원하고 컨테이너에서 실행되는 애플리케이션을 지원합니다. 이들은 HTTP 또는 HTTPS를 통해 그리고 HTTPS 리스너를 사용하는 HTTP/2를 통해 기본 Web Socket을 지원합니다. 또한 대상이 EC2 인스턴스이든 컨테이너이든 관계없이 그 상태를 확인합니다. EC2 인스턴스 또는 컨테이너에서 실행되는 웹 사이트 및 모바일 앱은 Application Load Balancer를 사용하는 이점을 누릴 수 있습니다.

Network Load Balancer는 사용자가 아무런 조치를 하지 않아도 높은 처리량과 매우 짧은 지연 시간을 유지하면서 초당 수천만 개의 요청을 처리하도록 설계되었습니다. 클라이언트로부터 수신되는 트래픽을 수락하고 이 트래픽을 **동일한** 가용 영역 내 대상 전체로 분산합니다. Network Load Balancer는 연결 수준(계층 4)에서 작동하며 IP 프로토콜 데이터에 따라 연결을 대상, 즉 Amazon EC2 인스턴스, 컨테이너 및 IP 주소로 라우팅합니다. Network Load Balancer는 완전 프로그래밍 방식의 대상 그룹 및 대상 제어를 포함해 Application Load Balancer와 API 호환이 가능합니다.

Network Load Balancer는 TCP, UDP 트래픽을 로드 밸런싱하는 데 적합합니다.
Network Load Balancer는 가용 영역당 하나의 정적 IP 주소를 사용하면서
갑작스럽고 변동이 심한 트래픽 패턴을 처리하는 데 최적화되어 있습니다.

Classic Load Balancer는 여러 가용 영역의 EC2 인스턴스 사이에서 기본적인 로드
밸런싱을 제공하며, OSI의 요청 수준 및 연결 수준 모두에서 작동합니다.

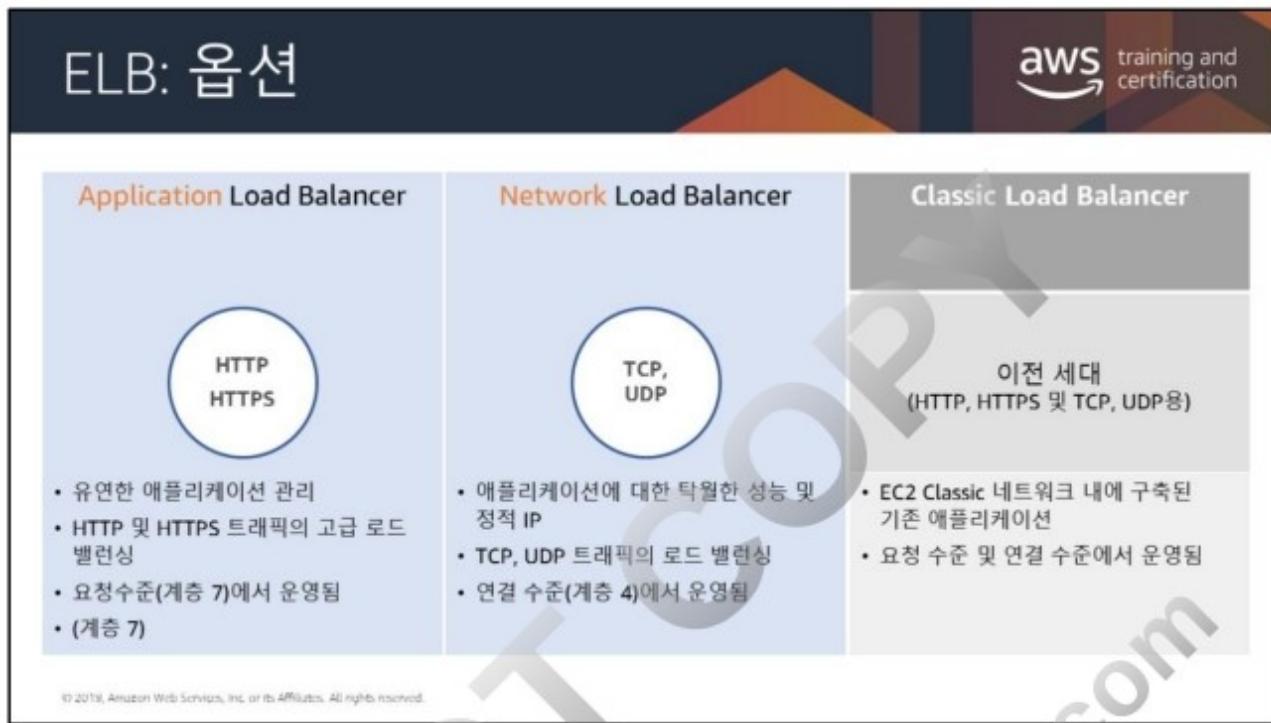
DO NOT COPY
zlagusdbs@gmail.com

ELB: 옵션

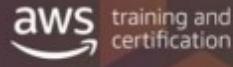
The diagram compares two types of AWS Load Balancers:

- Application Load Balancer:** Handles **HTTP** and **HTTPS** traffic. It manages application-level requests and can route them to multiple back-end servers. It is typically used at the Application Layer (Layer 7) of the OSI model.
- Network Load Balancer:** Handles **TCP** and **UDP** traffic. It performs load balancing at the transport layer (Layer 4) without understanding the content of individual application requests.

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



ELB를 사용해야 하는 이유



The slide features four icons with corresponding Korean labels below them:

- 고가용성 (High Availability): Represented by a stack of three green squares.
- 상태 확인 (Health Check): Represented by a white medical kit with a red cross.
- 보안 기능 (Security Features): Represented by a person icon holding a shield.
- TLS 종료 (TLS Termination): Represented by a blue wallet with a gear and a circular arrow icon.

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

고가용성

ELB는 트래픽을 단일 가용 영역 또는 여러 가용 영역에 있는 여러 대상(Amazon EC2 인스턴스, 컨테이너, IP 주소)에 자동으로 분산합니다.

상태 확인

Amazon EC2 인스턴스의 가용성을 확인하기 위해 로드 밸런서는 주기적으로 핑을 보내거나, 연결을 시도하거나, 요청을 전송하여 Amazon EC2 인스턴스를 테스트합니다. 이러한 테스트를 상태 확인이라고 부릅니다. 등록된 각 Amazon EC2 인스턴스가 상태 확인의 대상에 HTTP 상태 코드 200으로 응답해야 로드 밸런서가 인스턴스를 정상으로 간주합니다.

보안 기능

Amazon VPC 내에 프로비저닝된 ELB 로드 밸런서는 보안 그룹과 같은 네트워크 보안 그룹을 활용할 수 있습니다.

전송 계층 보안 종료

ELB는 통합 인증 관리 및 SSL 복호화를 지원하여 사용자가 로드 밸런서의 SSL 설정을 중앙 집중식으로 관리하고 애플리케이션으로부터 CPU 집약적 작업을 오프로드할 수 있는 유연성을 제공합니다.

계층 4 또는 계층 7 로드 밸런싱

계층 7 전용 기능에 대해 HTTP/HTTPS 애플리케이션을 로드 밸런싱하거나 TCP, UDP 프로토콜에만 의존하는 애플리케이션에 대해 엄격한 계층 4 로드 밸런싱을 사용할 수 있습니다.

일목요연한 기능 비교는

<https://aws.amazon.com/elasticloadbalancing/details/#compare>를 참조하십시오.

등록 취소 지연

프로덕션 플릿에서 인스턴스를 제거해야 하지만 사용자에게 영향을 미치지 않으려는 경우:

영향을 받는 백엔드 인스턴스는 등록 취소 전에 진행 중인 요청을 완료합니다.

The diagram illustrates the flow of user traffic from a user icon to an Application Load Balancer (ELB) icon. Three arrows point from the ELB to three separate orange boxes labeled 'App'. Below the ELB is the text '등록 취소 지연 활성화' (Registration Delay Enabled). A callout box on the left states: '영향을 받는 백엔드 인스턴스는 등록 취소 전에 진행 중인 요청을 완료합니다.' (Affected backend instances complete pending requests before deregistration).

등록 취소 지연 활성화

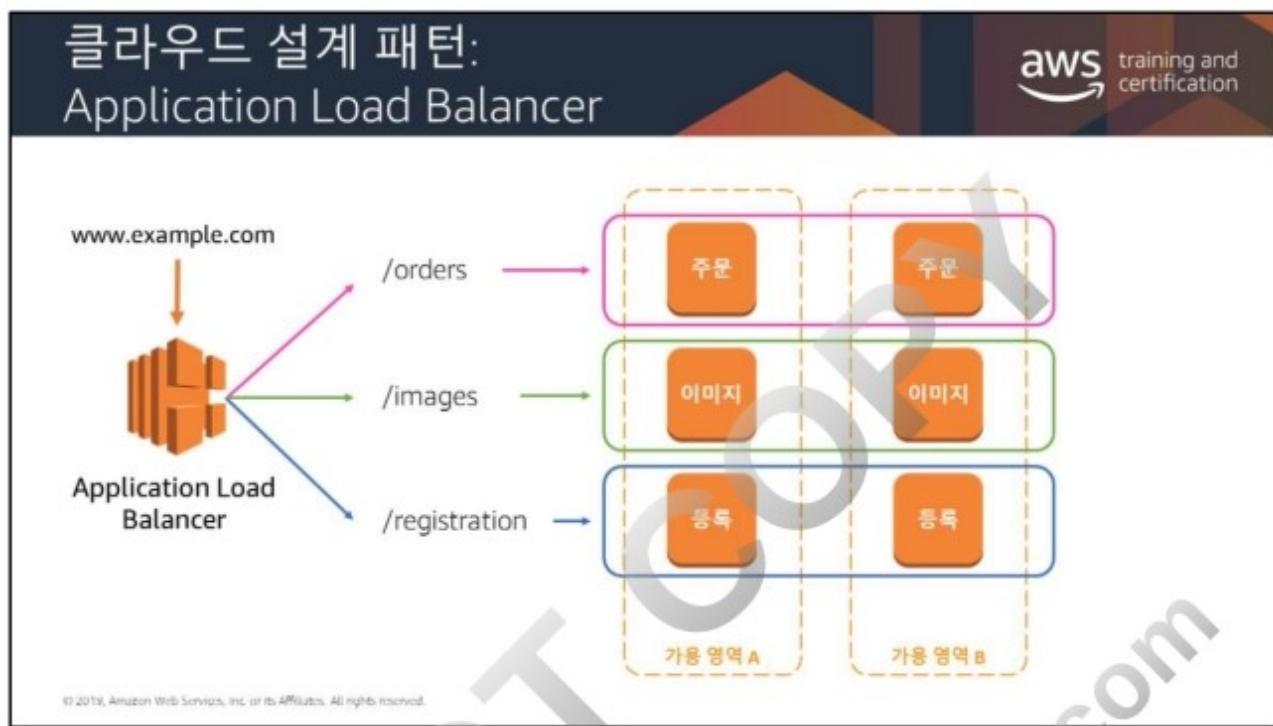
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

로드 밸런서에서 등록 취소 지연을 활성화하면, 등록이 취소될 백엔드 인스턴스는 등록 취소 전에 진행 중인 요청을 먼저 완료합니다. 마찬가지로 백엔드 인스턴스가 상태 확인에 실패할 경우, 로드 밸런서는 비정상 인스턴스에 새 요청을 보내지 않습니다. 이를 통해 진행 중인 요청을 계속 처리하면서 기존 요청을 완료할 수 있습니다. 즉, 고객 경험에 영향을 주지 않고 소프트웨어 업그레이드 배포 또는 백엔드 인스턴스 교체와 같은 유지 관리 작업을 수행할 수 있습니다.

등록 취소 지연은 또한 Auto Scaling과 통합되므로 로드 밸런서 뒤에서 용량을 훨씬 쉽게 관리할 수 있습니다. 등록 취소 지연이 활성화되면 Auto Scaling은 처리 중인 요청이 완료되길 기다렸다가 인스턴스를 종료합니다.

자세한 내용은

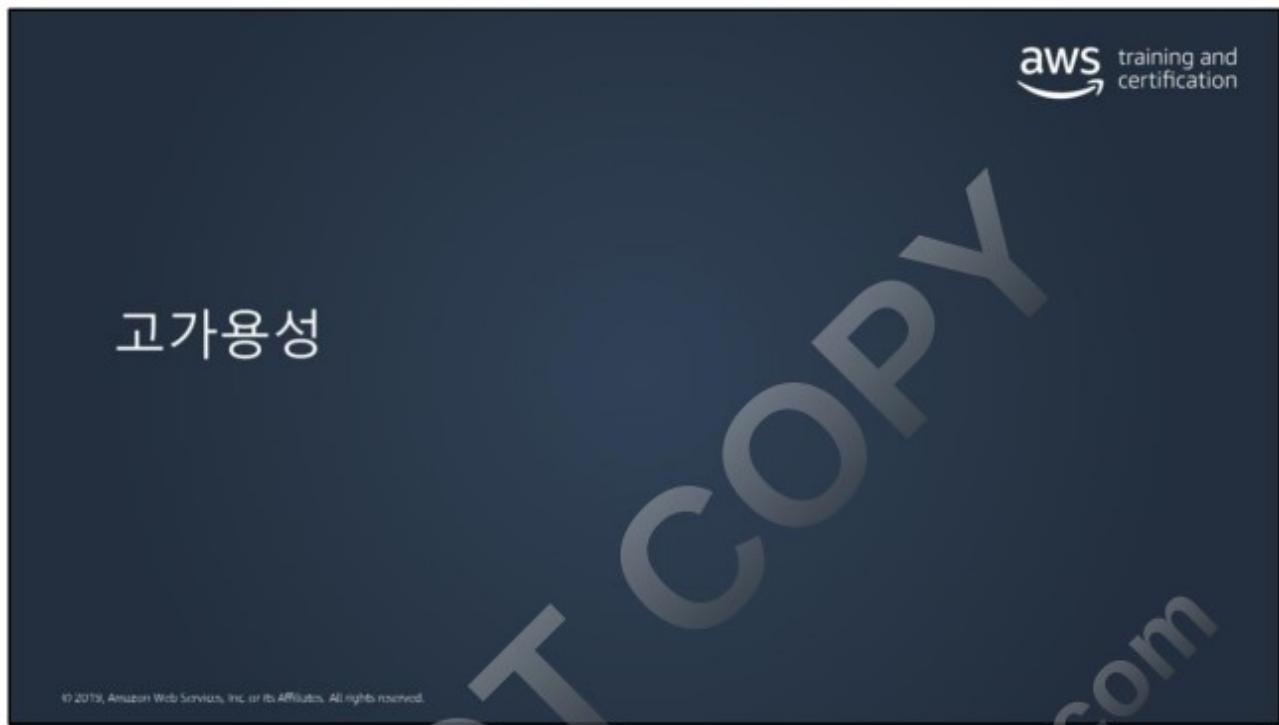
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#deregistration-delay>를 참조하십시오(내용 아래 등록 취소 지연 클릭).



자세한 내용은 다음을 참조하십시오.

<https://aws.amazon.com/blogs/devops/introducing-application-load-balancer-unlocking-and-optimizing-architectures/>

이제 Application Load Balancer가 고급 요청 라우팅 기능을 지원합니다. 다음을 참조하십시오. <https://aws.amazon.com/about-aws/whats-new/2019/03/application-load-balancers-now-support-advanced-request-routing/>



고가용성이란 무엇일까요?

애플리케이션은 허용되는 성능 저하 시간 내에 장애로부터 복구하거나 보조 소스로 이동할 수 있습니다.

가동률	연간 최대 가동 중간 시간	일일 기준 가동 중단 시간
90%	36.5일	2.4시간
99%	3.65일	14분
99.9%	8.76시간	86초
99.99%	52.6분	8.6초
99.999%	5.25분	0.86초

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

고가용성 예제

aws training and certification

모든 기능은 장애가 발생한다는 가정하에 역방향으로 설계합니다.

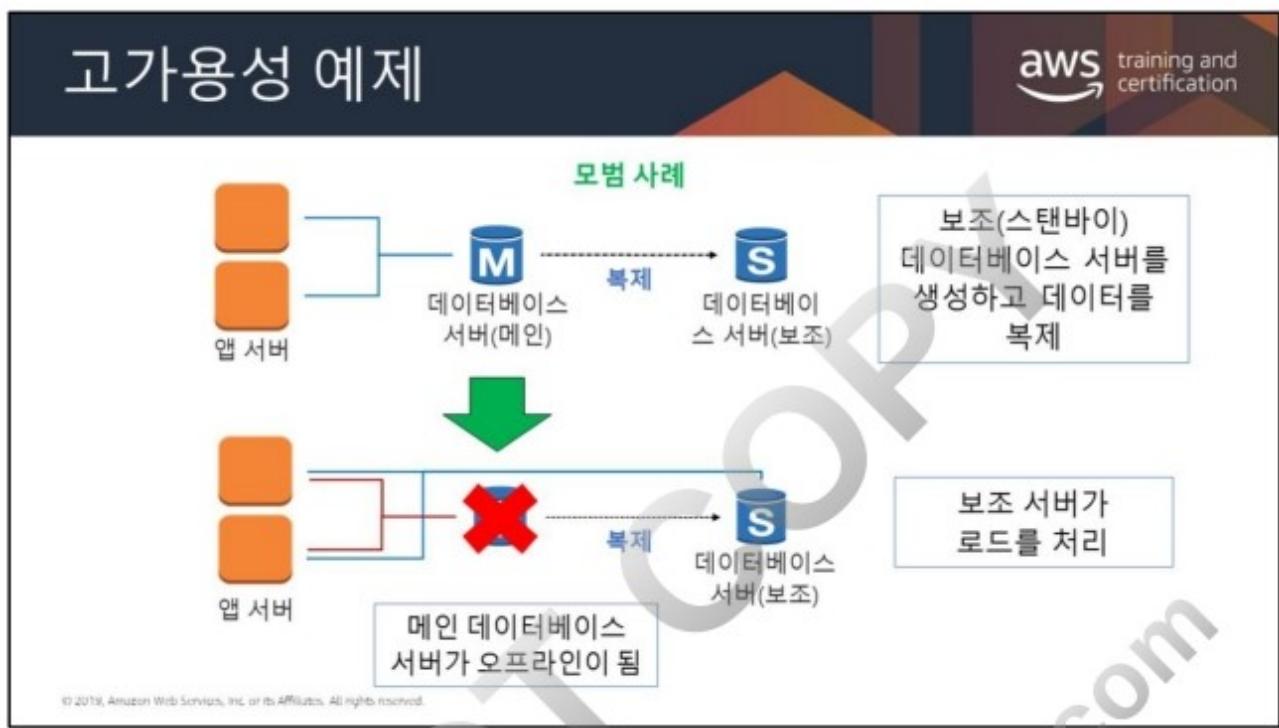
가능한 모든 지점에서 중복성을 구현하여, 단일 장애로 인해 전체 시스템이 중단되지 않도록 합니다.

애플리케이션 서버 (App Server) → 데이터베이스 서버 (Database Server)

안티 패턴

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

```
graph LR; A[애플리케이션 서버] --- B[데이터베이스 서버]; style A fill:#f0f0ff,stroke:#333,stroke-width:1px; style B fill:#f0f0ff,stroke:#333,stroke-width:1px;
```



얼마나 많은 가용 영역을 사용해야 합니까?

aws training and certification

AWS 리전당 2개의 가용 영역을 시작합니다.

한 가용 영역의 리소스에 접근할 수 없더라도 애플리케이션에 장애가 발생해서는 안 됩니다.

The diagram illustrates a VPC (Virtual Private Cloud) represented by a dashed orange rectangle. Inside the VPC, there are two orange boxes labeled 'EC2'. Below these boxes, the text '가용 영역 A' and '가용 영역 B' indicates two separate availability zones within the VPC. Above the VPC, a grey cloud icon represents the '인터넷 게이트웨이' (Internet Gateway), which is connected to the VPC. This setup ensures that even if one availability zone fails, traffic can still be directed through the other.

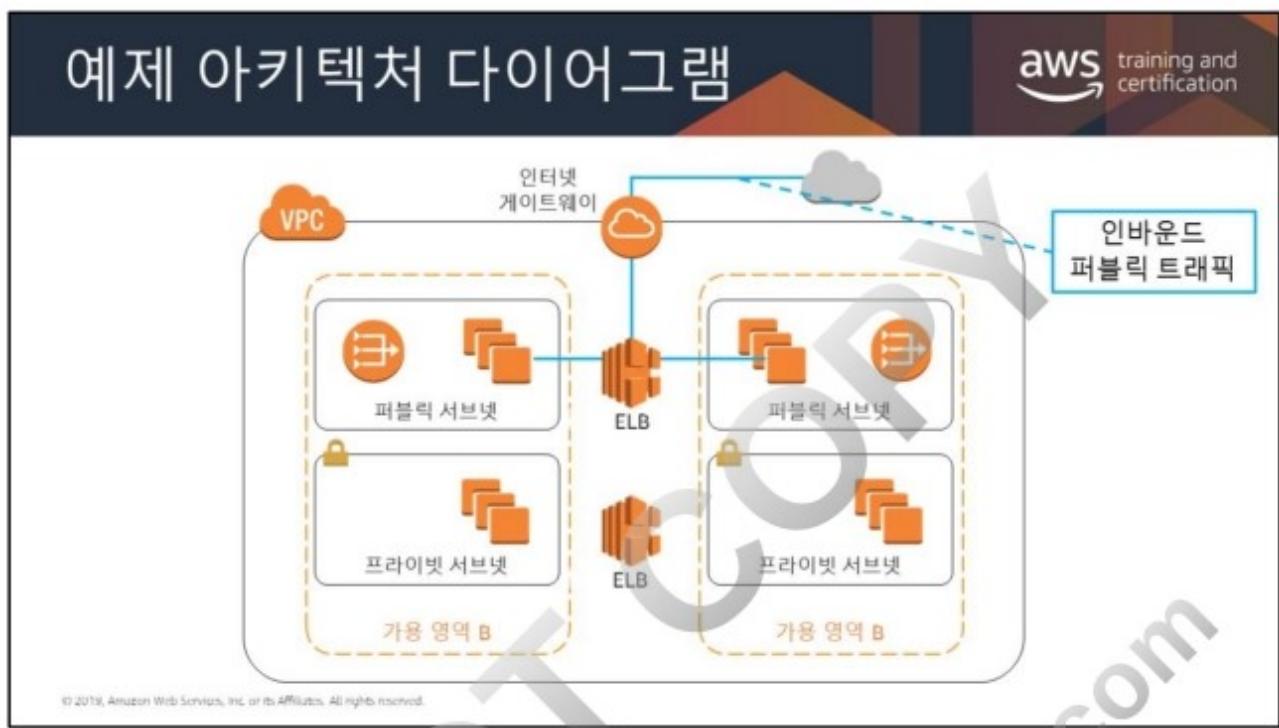
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

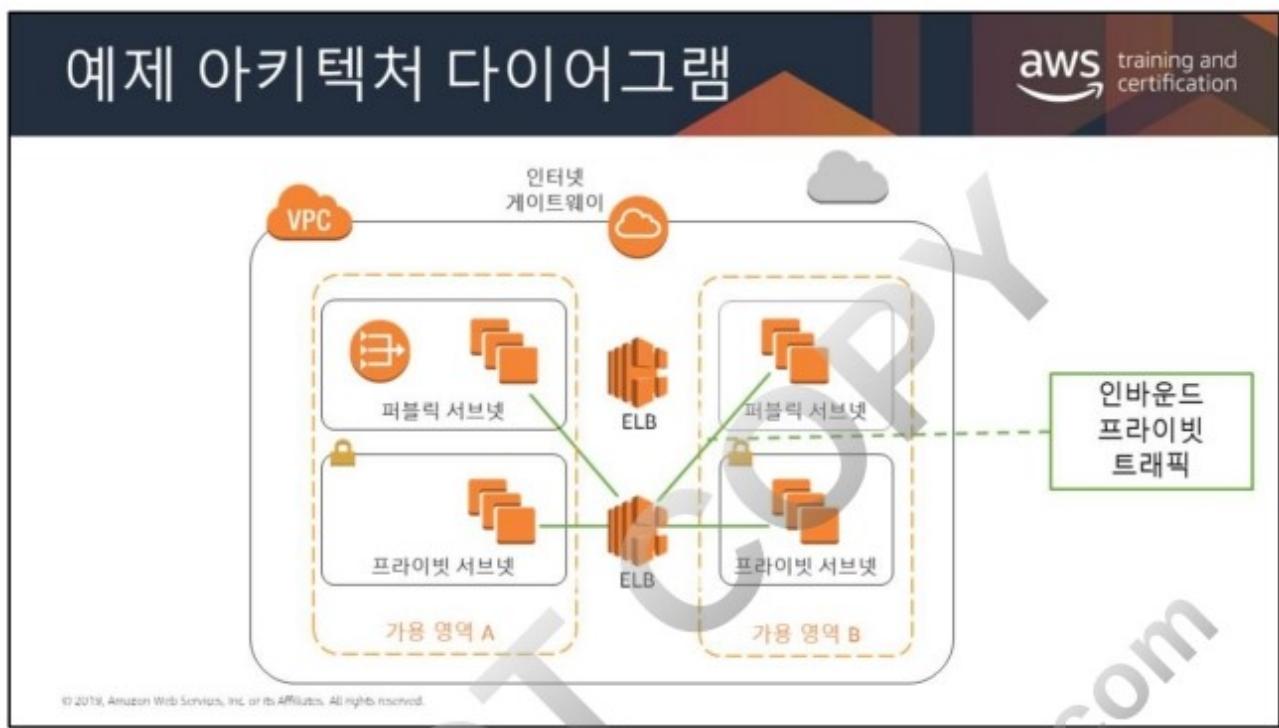
대부분의 애플리케이션은 두 개의 가용 영역을 지원하도록 설계할 수 있습니다. 기본/보조 장애 조치만 지원하는 데이터 소스를 사용할 경우 이보다 많은 가용 영역을 사용하더라도 도움이 되지 않을 수 있습니다. 가용 영역은 물리적으로 분산되어 있으므로 한 AWS 리전에서 3개 이상의 가용 영역에 리소스를 복제할 때 누릴 수 있는 이점은 별로 없습니다.

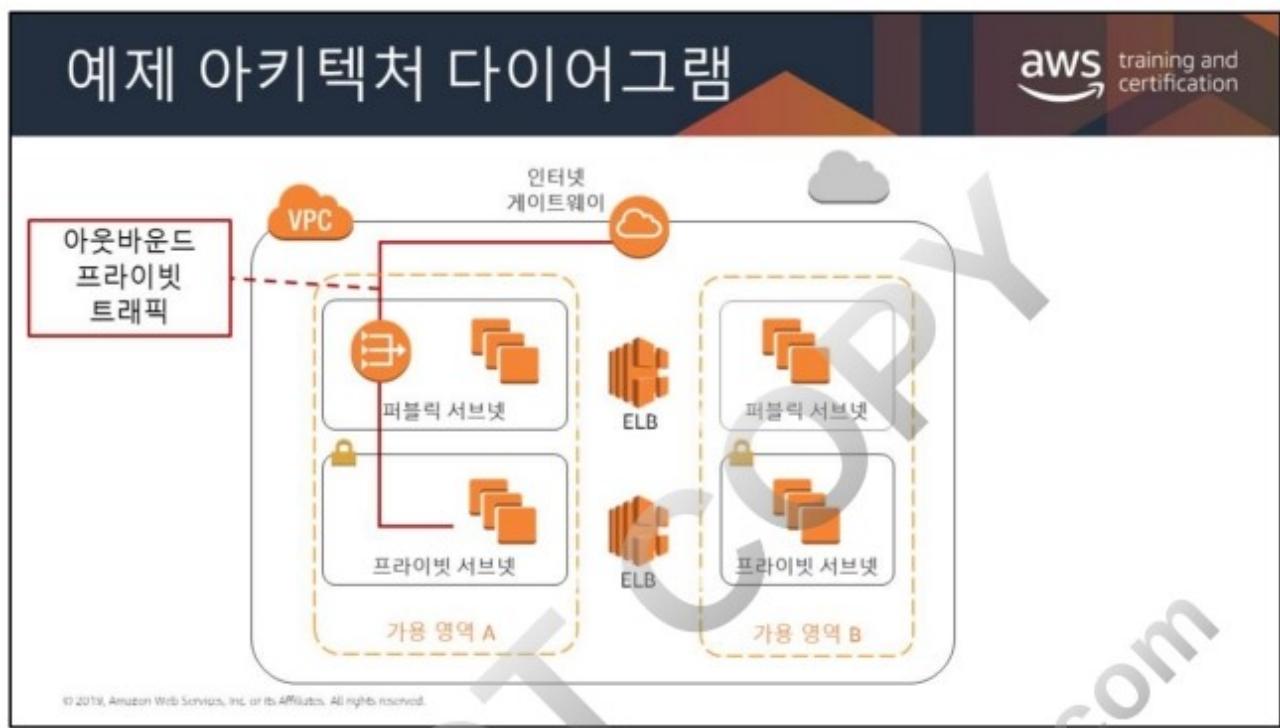
Amazon EC2 스팟 인스턴스 사용량이 많거나 Amazon DynamoDB와 같이 액티브/패시브를 넘어서는 데이터 소스의 경우, 2개를 초과하는 가용 영역을 사용하는 이점이 있을 수 있습니다.

이 기본 패턴에서는 2개의 웹 서버(Amazon EC2)가 ELB 로드 밸런서 뒤에 위치하며, 이 로드 밸런서가 서버 간에 트래픽을 분산합니다. 서버 중 하나에 장애가 발생하면, 로드 밸런서가 이를 인식합니다. 로드 밸런서는 비정상 인스턴스로 트래픽을 분산하는 작업을 중단합니다. 이렇게 하면 구성 요소가 상주하는 가용 영역 중 하나에 문제가 발생하더라도 애플리케이션을 계속 사용할 수 있습니다.

다른 방법을 사용해 인프라의 가용성을 더 높일 수도 있습니다. 이러한 방법은 이후 모듈에서 다룹니다.









Amazon Route 53

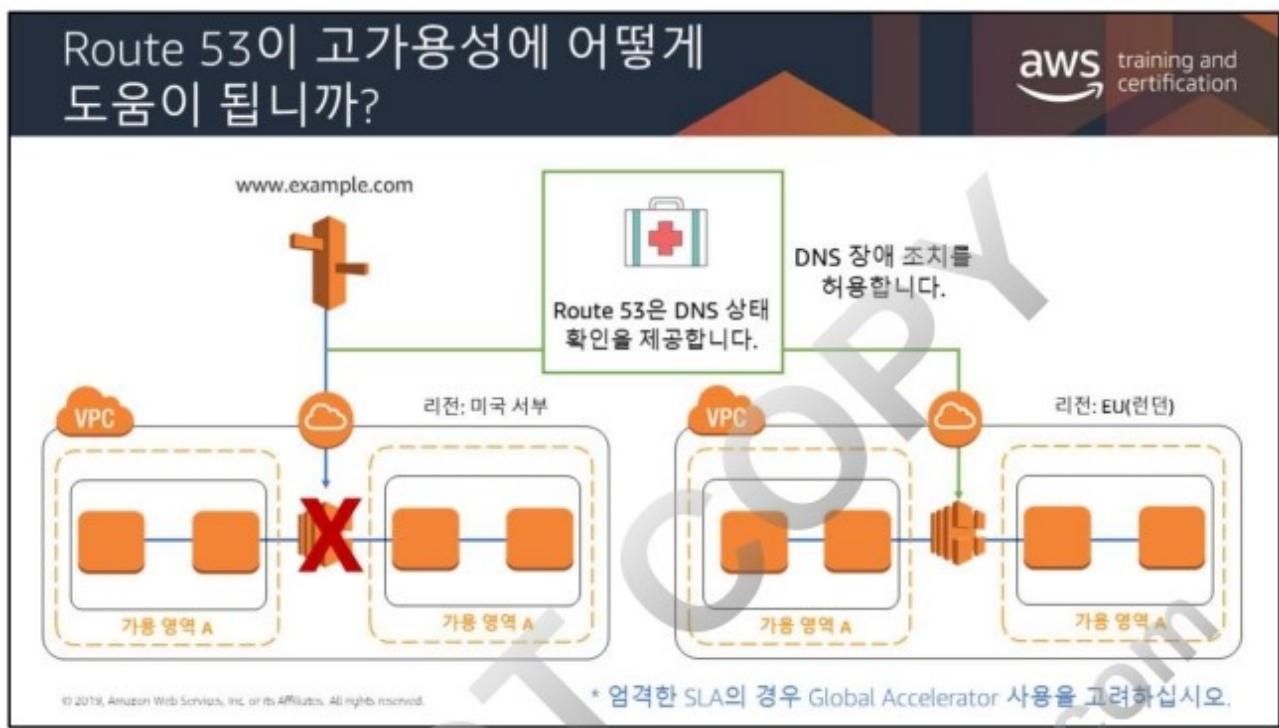


Route 53은 가용성과 확장성이 뛰어난 클라우드 Domain Name System (DNS) 서비스입니다.

- DNS는 도메인 이름을 IP 주소로 변환합니다.
- 도메인 이름을 구입하여 관리하고 DNS 설정을 자동으로 구성할 수 있습니다.
- AWS에서 유연한 고성능, 고가용성 아키텍처를 위한 도구를 제공합니다.
- 멀티플 라우팅 옵션

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

Amazon Route 53은 도메인 이름 시스템(DNS), 도메인 이름 등록 및 웹 서비스 상태 확인을 제공합니다. 이 서비스는 최종 사용자를 인터넷 애플리케이션으로 라우팅할 수 있는 안정적이고 비용 효율적인 방법을 개발자와 기업에 제공하기 위해 설계되었습니다. 이 서비스는 *example.com*과 같은 이름을 192.0.2.1과 같이 컴퓨터 간 연결에 사용되는 IP 주소로 변환합니다. DNS를 상태 확인 서비스와 결합하여 정상적인 엔드포인트로 트래픽을 라우팅하거나 개별적으로 엔드포인트에 대한 모니터링 또는 경보를 설정할 수 있습니다. *example.com*과 같은 도메인 이름을 구매 및 관리하고 도메인에 대한 DNS 설정을 자동으로 구성할 수도 있습니다. Route 53은 사용자 요청을 Amazon EC2 인스턴스, ELB 로드 밸런서 또는 Amazon S3 버킷처럼 AWS에서 실행되는 인프라에 효과적으로 연결하며, 사용자를 AWS 외부의 인프라로 라우팅하는 데에도 사용할 수 있습니다.



SLA가 엄격하거나 애플리케이션에 최대한 빠른 장애 조치가 필요한 경우, 아키텍처에 Global Accelerator를 추가하는 것을 고려하십시오.

Global Accelerator는 장애 조치에서 DNS의 역할을 제거하여 네트워크의 복원력을 높입니다. 또한 사용자와 애플리케이션을 캐싱 문제에서 보호하고 거의 즉각적으로 트래픽을 정상적인 엔드포인트로 리디렉션 할 수 있습니다. 또한 아키텍처에 추가하는 새 엔드포인트는 DNS 전파를 기다리지 않고 즉시 트래픽을 수신할 수 있습니다.

Anycast부터 AWS 엣지 로케이션까지 정적 IP 주소를 사용하는 Global Accelerator는 고정 진입점 주소를 제공하여 사용자와 가장 가까운 엣지 로케이션에서 트래픽을 수신하도록 합니다.

Route 53 라우팅 옵션

aws training and certification

- 간단한 라운드 로빈
- 가중치 기반 라운드 로빈
- 지연 시간 기반 라우팅
- 상태 확인 및 DNS 장애 조치
- 지리 위치 라우팅
- 트래픽 바이어스를 통한 지리 근접 라우팅
- 다중 값 응답

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

단순 라우팅(라운드 로빈)은 다수의 요청을 모든 참여 서버로 최대한 균일하게 분산합니다.

가중치 기반 라운드 로빈에서는 각 응답이 처리되는 빈도를 지정하기 위해 리소스 레코드 세트에 가중치를 할당할 수 있습니다. 이 기능을 사용하면 소프트웨어를 변경한 서버로 소규모 트래픽을 전송하여 A/B 테스트를 수행할 수 있습니다. 예를 들어 하나의 DNS 이름과 연결된 두 개의 레코드 세트가 있다고 가정해 보겠습니다. 하나에는 가중치 3, 다른 하나에는 가중치 1을 부여합니다. 이 경우, Amazon Route 53이 75%까지 가중치 3 레코드 세트를 반환하고 25%는 가중치 1 레코드 세트를 반환합니다. 가중치는 0부터 255 사이의 숫자로 지정할 수 있습니다.

지연 시간 기반 라우팅(LBR)을 사용하면 전 세계 사용자를 대상으로 애플리케이션의 성능을 향상할 수 있습니다. LBR은 애플리케이션이 실행되고 있는 여러 AWS 리전의 실제 성능 측정치를 기준으로 가장 빠른 환경을 제공하는 AWS 엔드포인트(예: Amazon EC2 인스턴스, 탄력적 IP 주소 또는 로드 밸런서)로 고객을 라우팅합니다.

Amazon Route 53 상태 확인은 웹 애플리케이션, 웹 서버 및 기타 리소스의 상태와 성능을 모니터링합니다. 상태 확인을 각각 생성하여 다음 중 하나를 모니터링할 수 있습니다.

- 지정한 리소스(예: 웹 서버)의 상태
- 다른 상태 확인의 상태
- Amazon CloudWatch 경보의 상태

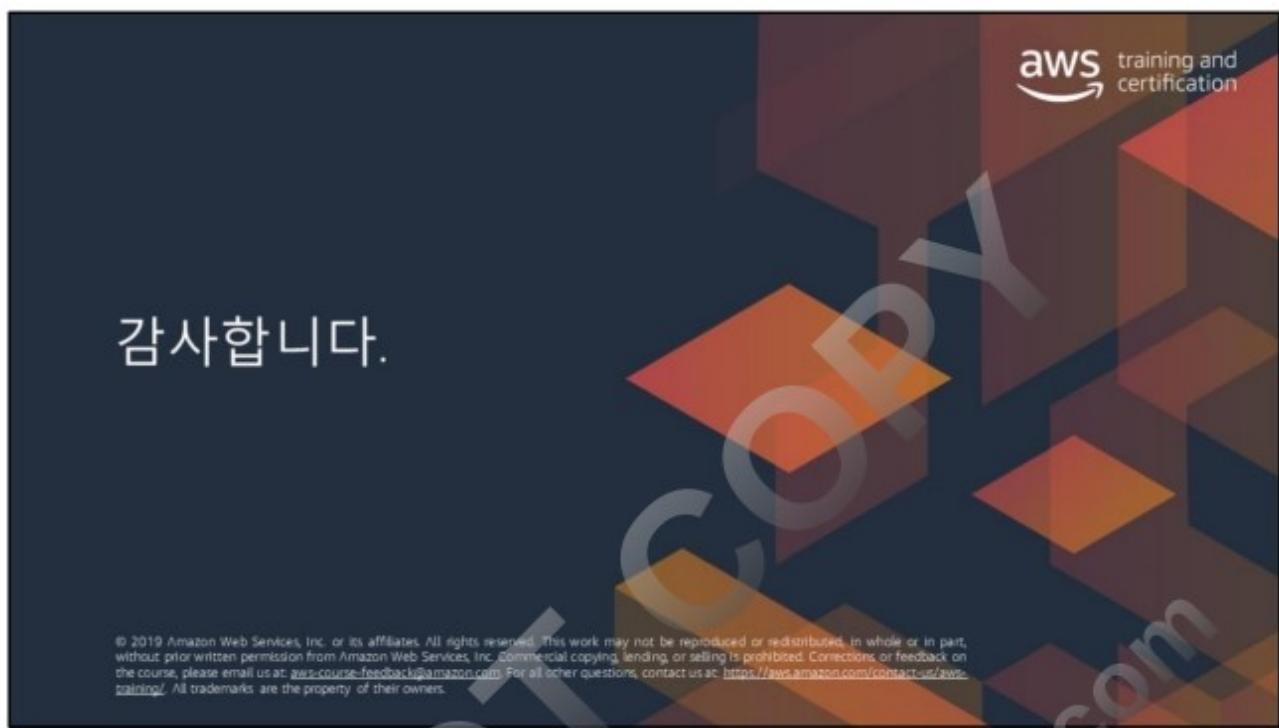
상태 확인을 생성하면 상태 확인의 상태를 받고, 상태가 변경될 때 알림을 받으며, DNS 장애 조치를 구성할 수 있습니다.

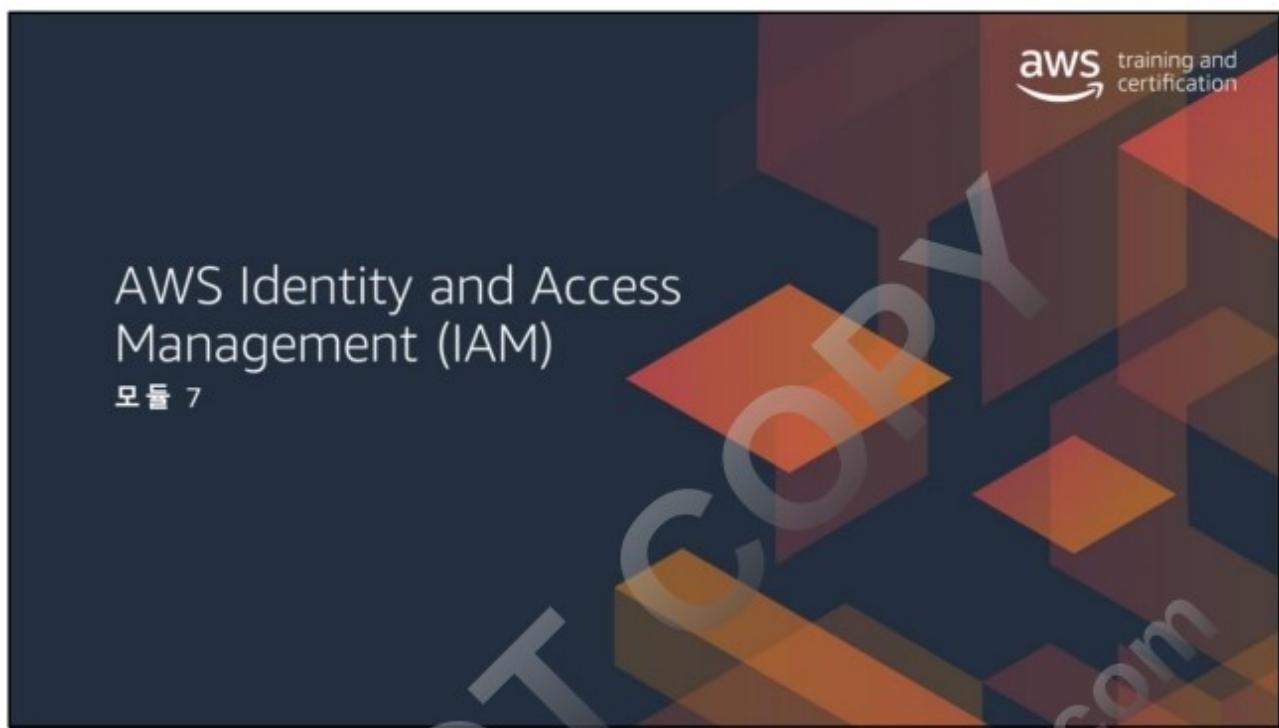
지리 위치 라우팅을 사용하면 사용자의 지리적 위치(DNS 쿼리의 오리진)에 따라 트래픽을 지원할 리소스를 선택할 수 있습니다. 지리 위치 라우팅을 사용할 때 콘텐츠를 현지화하고 웹 사이트의 일부 또는 전체를 사용자의 언어로 표시할 수 있습니다. 또한, 지리 위치 라우팅을 사용하여 배포 권한이 있는 위치에만 콘텐츠를 배포하도록 제한할 수 있습니다. 또한 예측 가능하고 관리가 쉬운 방법으로 엔드포인트 간에 로드를 분산함으로써, 각 최종 사용자 위치를 일관되게 동일한 엔드포인트로 라우팅할 수 있습니다.

DNS 장애 조치의 경우, Amazon Route 53은 웹 사이트의 가동 중단을 탐지하고 최종 사용자를 애플리케이션이 제대로 작동하는 대체 위치로 리디렉션할 수 있습니다. 이 기능을 활성화하면, Amazon Route 53 상태 확인 에이전트가 가용성을 확인하기 위해 애플리케이션의 각 위치/엔드포인트를 모니터링합니다. 이 기능을 활용하여 고객 사용 애플리케이션의 가용성을 높일 수 있습니다.

지리 근접 라우팅은 Route 53 트래픽 흐름을 사용할 경우 사용자와 리소스 사이의 물리적 거리를 기반으로 트래픽을 라우팅할 수 있게 해줍니다. 또한 양 또는 음의 바이어스를 지정하여 각 리소스로 라우팅되는 트래픽을 증감할 수도 있습니다. 트래픽 흐름 정책을 생성할 때 AWS 리전(AWS 리소스를 사용하는 경우) 또는 각 엔드포인트의 위도 및 경도를 지정할 수 있습니다.

다중 값 응답을 사용하면, 트래픽을 거의 무작위적으로 웹 서버 같은 다수의 리소스로 라우팅하려는 경우 각 리소스마다 하나씩 다중 값 응답 레코드를 생성하고, 선택적으로 Amazon Route 53 상태 확인을 각 레코드에 연결할 수 있습니다. 예를 들어, 각각 자체 IP 주소를 갖는 12개의 웹 서버로 HTTP 웹 서비스를 관리하는 경우를 생각해보겠습니다. 어떤 웹 서버도 단독으로 모든 트래픽을 처리할 수는 없습니다. 하지만 다중 값 응답 레코드를 생성할 경우, Amazon Route 53이 최대 8개의 정상 레코드로 각 DNS 쿼리에 응답합니다. Amazon Route 53은 DNS 해석기마다 다른 응답을 제공합니다. 해석기가 응답을 캐시한 후 한 웹 서버가 사용 불가능해질 경우 클라이언트 소프트웨어는 응답에 포함된 다른 IP 주소를 시도할 수 있습니다.





모듈 7



아키텍처 측면에서의 필요성

팀원이 전문적인 역할을 맡고 있을 만큼 충분히 큰 규모의 조직입니다. 필수 권한을 통한 보호 및 액세스 제어 기능이 필요합니다.

모듈 개요

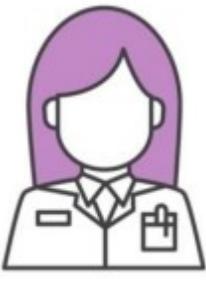
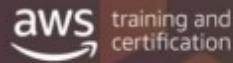
- IAM 사용자, 그룹 및 역할
- 연동 자격 증명 관리
- Amazon Cognito
- AWS Organizations

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

- 어떤 사용자는 AWS Management Console에 액세스해야 하고, 또 어떤 사용자는 AWS 명령줄 인터페이스(AWS CLI)를 사용해야 합니다.
- 각 환경(개발/테스트/프로덕션)은 액세스 요구 사항이 서로 다릅니다.
- 온프레미스 인증은 SSO 자격 증명 연동을 통해 관리됩니다.
- 보안 운영 팀은 AWS 클라우드에서 누가 데이터에 손을 대는지 확인할 수 있어야 합니다.
- 외부 감사자는 로그에만 액세스해야 하며 다른 어떤 것도 액세스할 수 없어야 합니다.
- 모바일 앱은 수천 명의 사용자를 인증해야 합니다.



AWS 계정 루트 사용자



이 계정은 **모든** AWS 서비스 및 리소스에 대한 **전체 액세스 권한**을 갖습니다.

- 결제 정보
- 개인 데이터
- 전체 아키텍처 및 해당 구성 요소

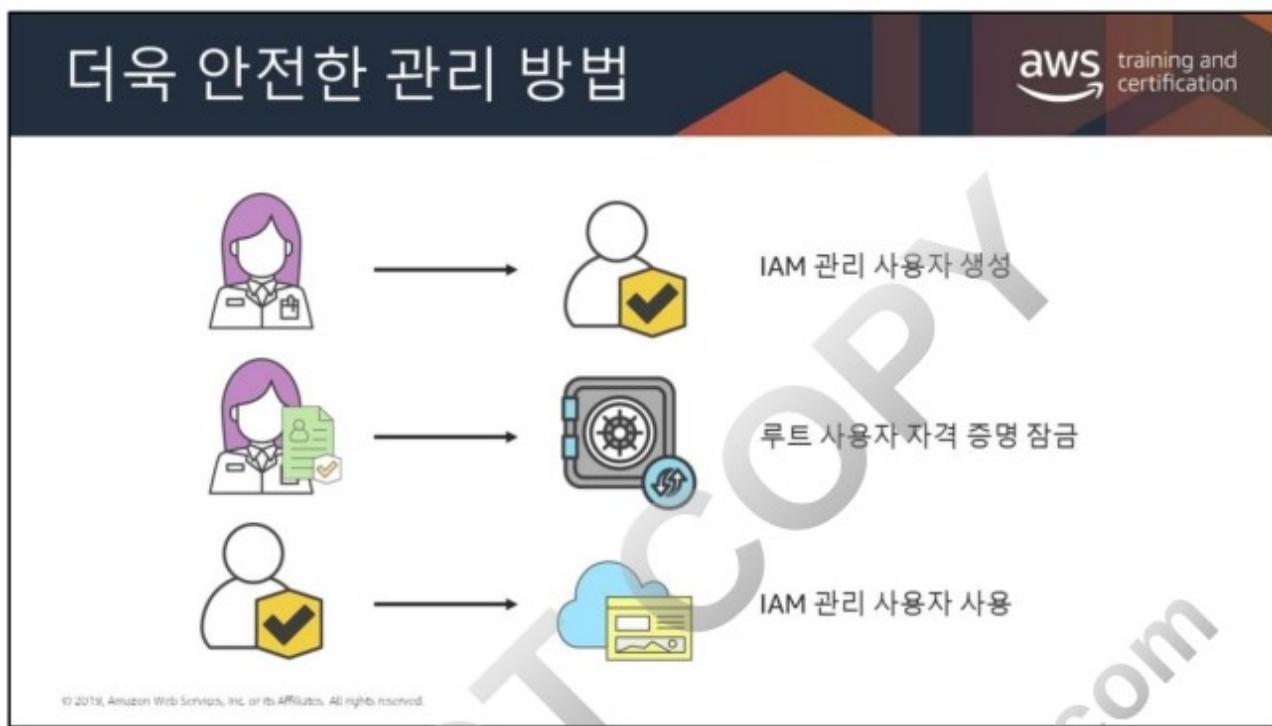
AWS 계정 루트 사용자는 강력한 권한을 가지며 제한을 받지 않습니다.

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

AWS 계정을 처음 생성할 때 루트 사용자로 시작합니다. 이 사용자는 계정의 모든 AWS 서비스 및 리소스에 대한 전체 액세스 권한을 가집니다. 이 자격증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 제공한 이메일 주소 및 암호로 로그인하여 액세스합니다.

AWS 계정 루트 사용자에 대한 자세한 내용은

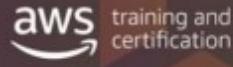
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html를
참조하십시오.



AWS 계정 루트 사용자는 계정의 모든 리소스에 대한 전체 액세스 권한을 가지며, 사용자는 루트 계정 자격 증명의 권한을 제어할 수 없습니다.

AWS와의 일상적인 상호 작용에는 루트 계정 자격 증명을 사용하지 않는 것이 좋습니다. IAM 사용자는 비교적 쉽게 관리될 수 있으며 감사될 수 있습니다. IAM 계정 보안 주체(나중에 설명)에 더 많은 권한이 필요할 경우 권한을 추가할 수 있습니다. 마찬가지로 권한을 제거 또는 취소해야 할 경우, 환경에 미치는 영향을 최소화하며 해당 작업을 수행할 수 있습니다.

IAM을 사용하여 추가 사용자를 생성하고, 이러한 사용자에게 권한을 지정하여, 최소한의 권한 원칙을 적용하십시오.

전체 제어 권한은 모든 사람이 원합니다. 

문제: 액세스 권한을 세분화하여 제어할 수 있어야 합니다.

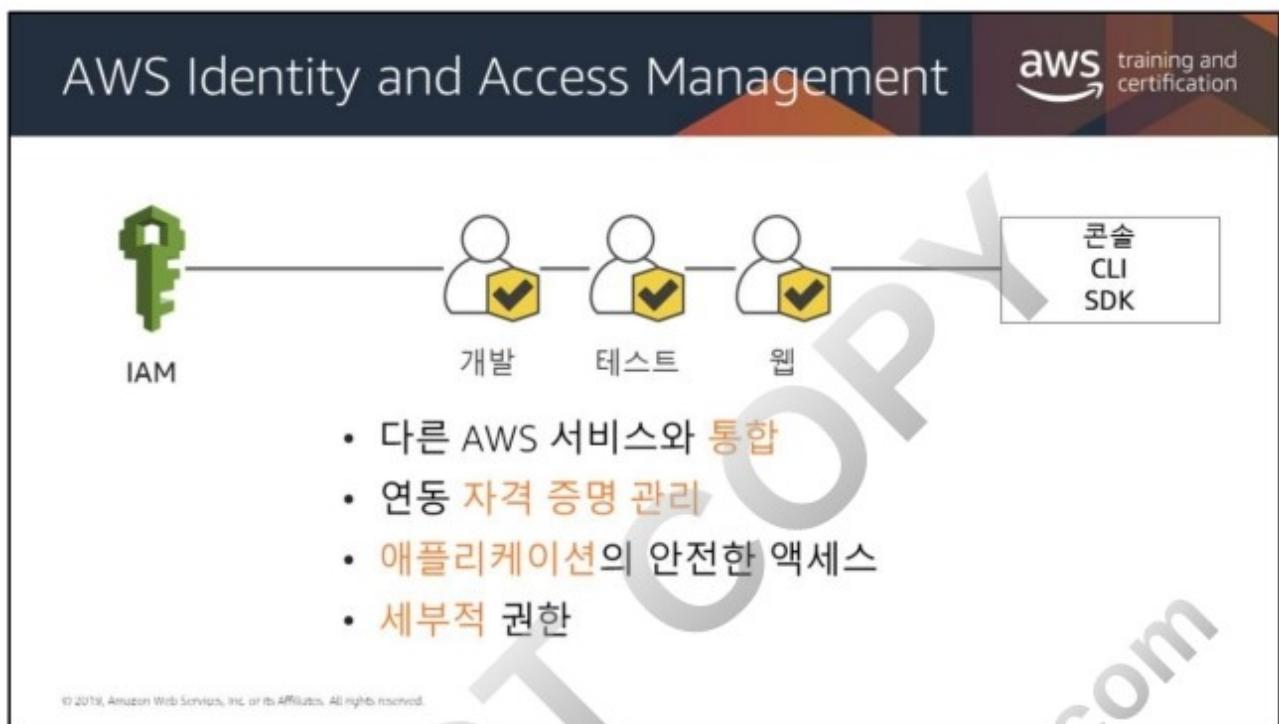


© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

이제 AWS 프로파일에서 가장 중요한 계정을 보호하고 관리자 계정을 생성했으므로 간편한 액세스 및 보안을 위해 추가 계정을 생성합니다. 최소 권한 부여가 표준이 되어야 합니다.

AWS 계정 루트 사용자와 비슷한 권한을 갖는 계정을 생성할 수 있지만 필요한 기능만 제어하는 관리자 계정을 생성하는 것이 더 좋습니다. DBA가 EC2 인스턴스를 프로비저닝할 수 있어야 합니까? 그렇지 않다면 계정을 적절히 프로비저닝합니다.

다양한 계정 유형으로 다양한 계정을 보유하는 것이 유용할 수 있습니다. 권한은 필요에 따라 추가 또는 제거할 수 있습니다.



AWS 자격 증명 관리 시스템에서 사용자를 생성하거나, 사용자에게 개별 보안 자격 증명(예: 액세스 키, 암호, 멀티 팩터 인증(MFA) 디바이스)을 할당하거나, AWS 서비스 및 리소스에 대한 액세스를 제공할 수 있도록 임시 보안 자격 증명을 요청할 수 있습니다. 사용자가 수행할 수 있는 작업을 제어하는 권한을 지정할 수 있습니다.

연합 ID 관리의 경우, 기업 디렉터리에 의해 관리되는 사용자를 위해 만기 구성이 가능한 보안 자격 증명을 요청할 수 있습니다. 이는 직원 및 애플리케이션에게 보안 액세스를 제공합니다. 그러므로 직원 및 애플리케이션을 위해 IAM 사용자 계정을 생성하지 않아도 이들이 AWS 계정 내 리소스에 액세스할 수 있습니다. 이 보안 자격 증명에 권한을 지정하여 사용자가 수행할 수 있는 작업을 제어합니다.

IAM은 AWS 리소스에 대한 액세스를 제어할 수 있게 해주는 서비스입니다. IAM을 사용하면 다양한 수준의 계정 권한 및 권한 부여로 사용자 계정 및 자격 증명을 생성할 수 있습니다.

IAM은 콘솔, AWS CLI, AWS SDK 및 보안 API 엔드포인트에서 액세스할 수 있습니다.



보안 주체란 AWS 리소스에 대해 작업을 수행할 수 있는 엔터티입니다. 시간이 지나면서 사용자 및 서비스가 역할을 맡도록 허용할 수 있습니다. 연동 사용자를 지원하거나 애플리케이션이 AWS 계정에 액세스하도록 허용하는 프로그래밍 방식 액세스를 지원할 수 있습니다. 사용자, 역할, 연동 사용자 및 애플리케이션은 모두 AWS 보안 주체입니다.

보안 주체는 AWS IAM 사용자나 AWS 서비스(예: Amazon EC2, SAML 공급자 또는 자격 증명 공급자(IdP))일 수 있습니다.

AWS 계정에서 IAM 사용자를 생성하는 대신 IdP를 사용할 수 있습니다. IdP를 사용하면 AWS 외부의 사용자 자격 증명을 관리하고(예: Login with Amazon, Google 및 Facebook) 이러한 외부 사용자 자격 증명에 계정의 AWS 리소스를 사용할 권한을 제공할 수 있습니다.

이미지 출처:

Login with Amazon - <https://login.amazon.com/button-guide>

Continue with Facebook - <https://developers.facebook.com/docs/facebook-login/web/login-button>

Sign in with Google - <https://developers.google.com/identity/sign-in/web/build-button>

IAM 사용자

IAM 사용자는 별도의 AWS 계정이 아니라 계정 내 사용자입니다.

각 사용자는 자체 자격 증명을 갖습니다.

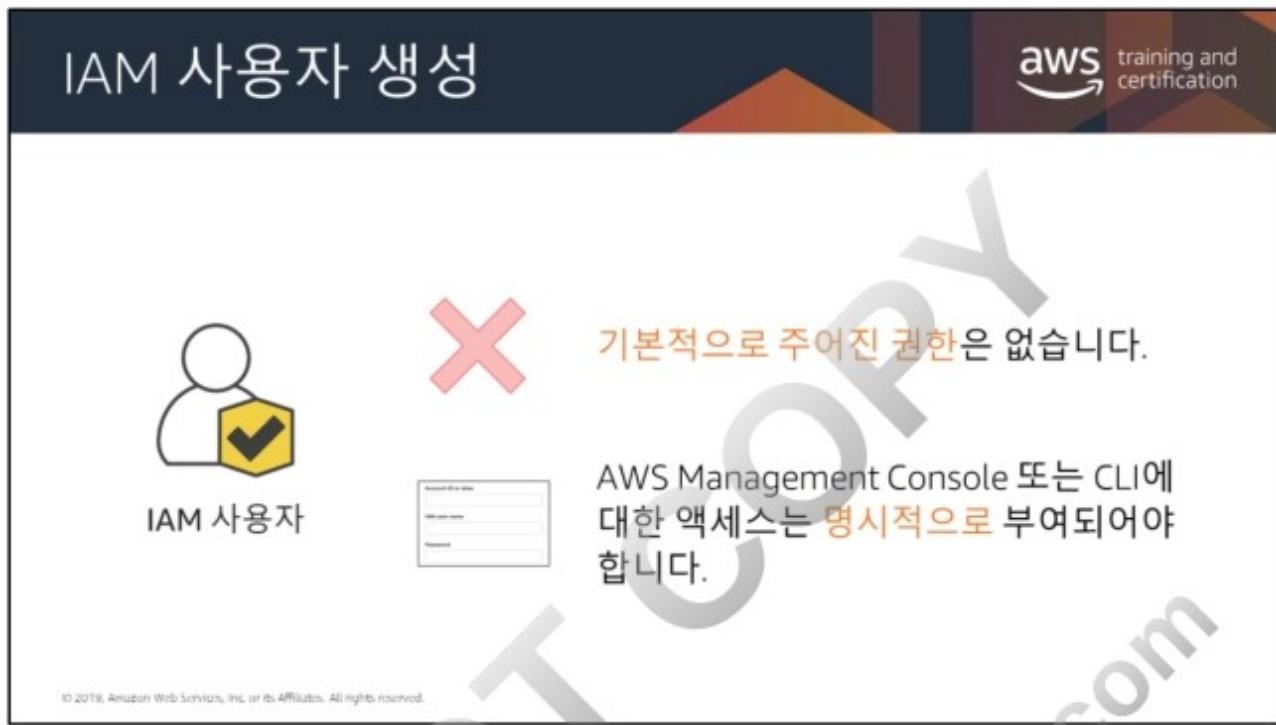
IAM 사용자는 부여된 권한을 기준으로 특정 AWS 작업을 수행할 권리가 있습니다.

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

IAM 사용자는 별도의 AWS 계정이 아니라 계정 안의 보안 주체입니다. 각 IAM 사용자는 콘솔에 액세스하기 위한 고유의 암호를 가집니다. 또한 사용자가 계정 내 리소스에 대한 작업을 프로그래밍 방식으로 요청할 수 있도록 각 사용자마다 개별 액세스 키를 생성할 수도 있습니다. CLI 액세스 권한이 없어도 콘솔에 액세스할 수 있습니다. 반대의 경우도 마찬가지입니다. 콘솔 액세스 권한이 없어도 CLI에 액세스할 수 있습니다.

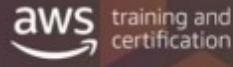
새롭게 생성된 IAM 사용자에게는 자신을 인증하고 AWS 리소스에 액세스하는 데 사용할 기본 자격 증명이 없습니다. 먼저 IAM 사용자에게 인증을 위한 보안 자격 증명을 지정한 다음, AWS 작업을 수행하거나 AWS 리소스에 액세스할 수 있는 권한을 부여해야 합니다. 사용자를 위해 생성하는 자격 증명은 사용자가 AWS에서 자신을 고유하게 식별하는 데 사용됩니다.

AWS 계정에서 IAM 사용자를 생성하는 대신 IAM IdP를 사용할 수 있습니다. IdP를 사용하면 AWS 외부의 사용자 자격 증명을 관리하고(예: Amazon.com, Google 및 Facebook) 이러한 외부 사용자 자격 증명에 계정의 AWS 리소스를 사용할 권한을 제공할 수 있습니다.



IAM 보안 주체에는 기본 권한이 없습니다. 모든 사용자에게 관리자 권한을 부여하는 것은 권장하지 않습니다. 최소 권한 원칙을 따르는 것이 중요합니다.

권한 부여



정책

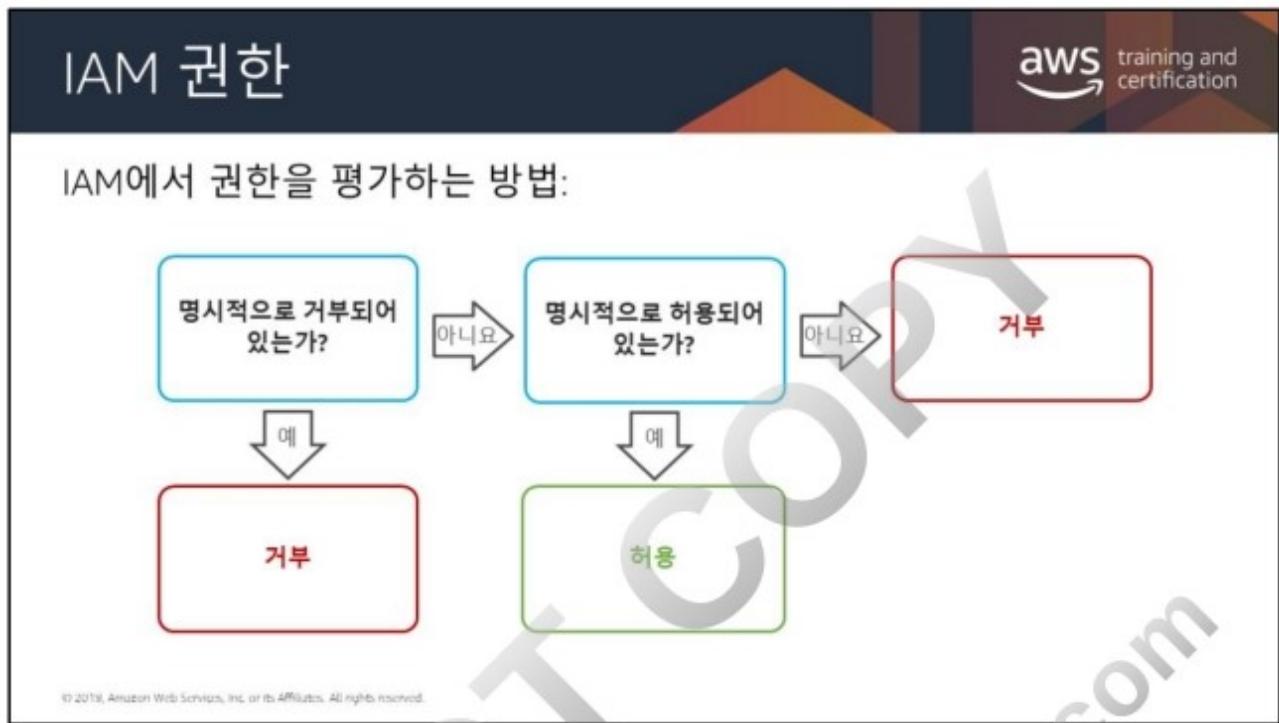
- 하나 이상의 권한에 대한 형식 선언
- 요청 시에 평가됨
- IAM 정책은 AWS 서비스에 대한 액세스만 제어합니다.
- IAM에는 하이퍼바이저에 대한 가시성이 없습니다.

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

정책은 자격 증명 또는 리소스에 연결될 때 해당 권한을 정의하는 AWS의 개체입니다. AWS는 사용자와 같은 보안 주체가 요청할 때 이러한 정책을 평가합니다.

IAM 정책은 AWS 서비스에 대한 액세스만 제어합니다. IAM은 하이퍼바이저 계층 이상으로는 가시성이 없으며 AWS를 벗어날 수 없습니다.

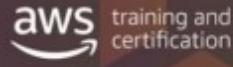
OS 지원을 원할 경우 LDAP, SAML 또는 기타 자격 증명 관리 시스템을 사용합니다.



정책을 통해 IAM 사용자, 그룹, 역할에 부여된 권한을 세부적으로 조정할 수 있습니다. 정책은 JSON 형식으로 저장되므로, 버전 관리 시스템과 함께 사용할 수 있습니다. 각 사용자, 그룹 또는 역할에 대해 최소한의 액세스 권한을 정의하는 것이 좋습니다. 그런 다음 권한 부여 정책을 사용하여 특정 리소스에 대한 액세스를 사용자 정의할 수 있습니다.

권한이 허용되었는지 결정할 때, IAM은 먼저 명시적 거부 정책을 확인합니다. 명시적 거부 정책이 없는 경우, IAM은 다음으로 명시적 허용 정책을 확인합니다. 명시적 거부 정책이나 명시적 허용 정책이 둘 다 없는 경우, 기본 설정인 암시적 거부로 되돌아갑니다.

권한 부여



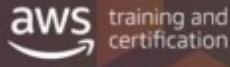
정책

- 리소스 기반 – 연결된 AWS 리소스
- 자격 증명 기반 – 연결된 IAM 보안 주체

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

정책 권한은 요청이 허용되는지 또는 거부되는지 결정합니다. 정책은 JSON 문서로 AWS에 저장되며 자격 증명 기반 정책으로 보안 주체에 연결되거나 리소스 기반 정책으로 리소스에 연결된 됩니다.

자격 증명 기반 정책



연결 대상:

- 사용자
- 그룹
- 역할

제어:

- 수행 작업
- 리소스 대상
- 필요한 조건

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

자격 증명 기반 정책

자격 증명 기반 정책은 IAM 사용자, 역할 또는 그룹과 같은 보안 주체(또는 자격 증명)에 연결할 수 있는 권한 정책입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 관련 조건을 제어합니다.

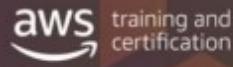
자격 증명 기반 정책을 추가로 분류할 수 있습니다.

관리형 정책은 AWS 계정의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 자격 증명 기반 정책입니다. 두 가지 유형의 관리형 정책을 사용할 수 있습니다.

- **AWS 관리형 정책**은 AWS에서 생성하고 관리하는 관리형 정책입니다. 정책 사용이 처음이라면 AWS 관리형 정책을 사용하여 시작하는 것이 좋습니다.
- **고객 관리형 정책**은 고객이 AWS 계정에서 생성하고 관리하는 관리형 정책입니다. 고객 관리형 정책은 AWS 관리형 정책이 아닌 정책을 보다 정밀하게 제어합니다. IAM 정책은 시각적 편집기를 사용하여 또는 JSON 정책 문서를 직접 생성하여 생성 및 편집할 수 있습니다.

인라인 정책은 사용자가 생성하고 관리하며, 단일 사용자, 그룹 또는 역할에 직접 포함되는 정책입니다.

리소스 기반 정책



연결 대상:

- AWS 리소스(예: Amazon S3, Amazon Glacier 및 AWS KMS)


리소스 기반
정책

제어:

- 특정 보안 주체가 허용한 작업
- 필요한 조건
- 항상 인라인 정책임
- AWS 관리형 리소스 기반 정책이 없음

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

리소스 기반 정책은 Amazon S3 버킷과 같은 리소스에 연결되는 JSON 정책 문서입니다.

이러한 정책은 지정된 보안 주체가 해당 리소스에 대해 수행할 수 있는 작업 및 관련 조건을 제어합니다. 리소스 기반 정책은 인라인 정책이며, 관리형 리소스 기반 정책은 없습니다.

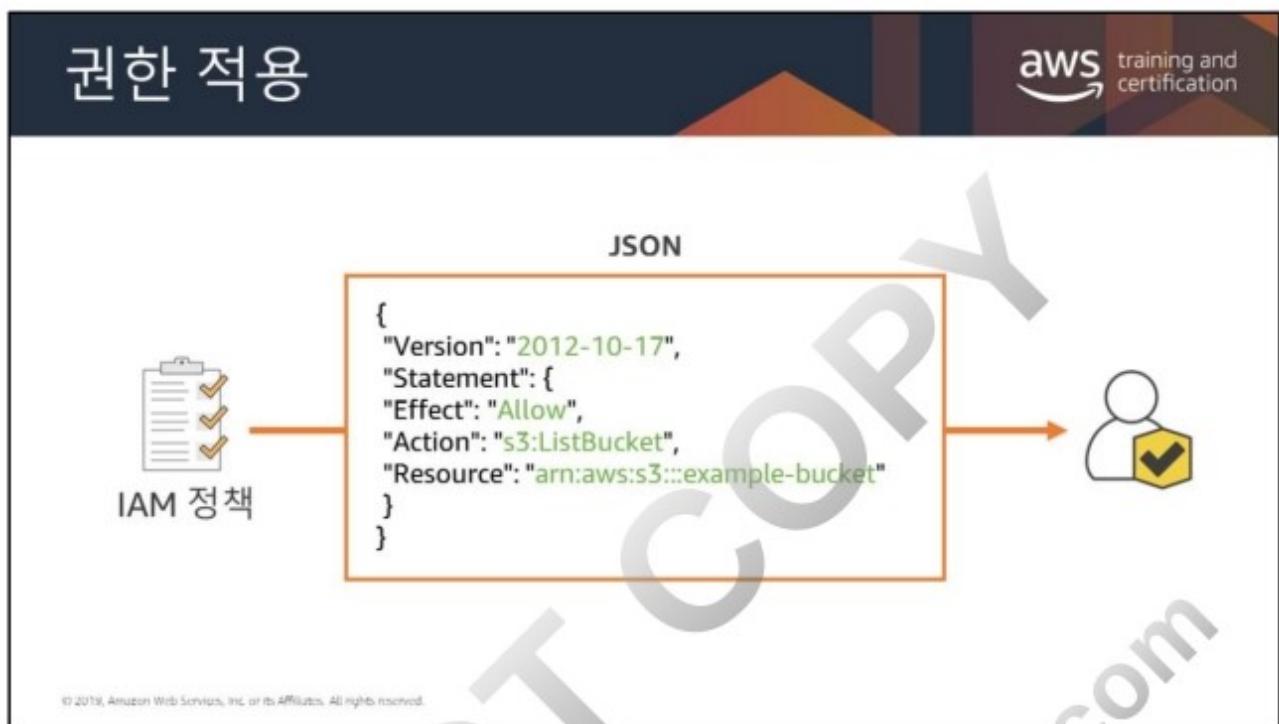
IAM 자격 증명이 기술적으로는 AWS 리소스이지만 리소스 기반 정책을 IAM 자격 증명에 연결할 수는 없습니다.



IAM 사용자는 권한이 연결된 자격 증명(보안 주체)일 뿐입니다.

AWS에 요청을 하기 위해서는 자격 증명이 반드시 필요한 애플리케이션에 사용할 IAM 사용자를 생성할 수 있습니다.

애플리케이션은 계정 내에서 고유한 자격 증명과 AWS 서비스에 액세스할 수 있는 고유한 권한 세트를 가질 수 있습니다. 이는 현대 운영 체제에서 프로세스가 고유한 자격 증명과 권한을 갖는 것과 비슷합니다. 애플리케이션 또는 심지어 EC2 인스턴스가 s3 버킷과 같은 리소스에 액세스할 권리가 있는 경우에는 코드에 자격 증명을 포함할 필요가 없습니다.



IAM 정책은 하나 이상의 권한으로 구성된 공식 문입니다.

- 어떤 IAM 엔터티에도 정책을 연결할 수 있습니다.
- 정책은 엔터티가 수행할 수 있거나 수행할 수 없는 작업에 대한 권한을 부여합니다.
- 단일 정책이 여러 개의 엔터티에 연결될 수 있습니다.
- 단일 엔터티에 여러 개의 정책이 연결될 수 있습니다.

IAM 정책 예

The screenshot shows a sample IAM policy document with annotations:

```
{  
    "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/*"]  
        }  
    ]  
}
```

Annotations in Korean:

- 사용자에게 액세스 권한 부여(특정 DynamoDB 테이블과...)
- ... 특정 Amazon S3 버킷 및 해당 콘텐츠
- 명시적 거부 문은 보안 주체가 지정된 테이블 및 버킷이 아닌 AWS 작업 또는 리소스를 사용할 수 없도록 합니다.
- 명시적 거부 문은 허용문보다 우선 적용됩니다.

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

중요: 버전 구문을 편집하지 마십시오. 이것은 IAM 정책을 처리하는 엔진을 참조합니다.

작업 섹션의 별표는 와일드카드입니다. 이 경우, DynamoDB 및 Amazon S3 서비스에 대한 모든 작업이 허용됩니다. 와일드 카드를 포함하는 이름을 사용할 수도 있습니다. 예를 들어 s3>List*는 ListAllMyBuckets, ListBucket, ListBucketByTags, ListBucketMultipartUploads, ListBucketVersions, ListMultipartUploadParts와 일치합니다.

거부 섹션에서 NotResource는 이전에 본 적이 없다면 혼동을 줄 수 있습니다. NotResource는 지정된 목록의 리소스를 제외한 모든 리소스와 명시적으로 일치하는 고급 정책 요소입니다.

여기에서 NotResource는 여기에 나열된 것 이외의 모든 작업을 명시적으로 거부하는 것을 의미합니다. 정책의 전반부를 변경하는 경우 거부 문도 적절히 변경해야 합니다.

묵시적 거부가 있는데 이렇게 하는 이유는 무엇일까요? 누군가에게는 의도치 않은 권한 부여를 방지하기 위해 액세스를 잠그는 것이 중요합니다. (악의적 사용자를 상정하기 쉽지만 선의를 가졌지만 제대로 이해하지 못한 사용자도 있을 수 있습니다.) 이로 인해 복잡성이 추가된다는 점을 주의하십시오. 이것이 반드시 나쁜 것은 아니지만 복잡성은 추가 작업을 요구하는 것으로 보일 수 있습니다.

NotResource를 사용하면 일치하는 리소스를 길게 나열하는 대신 일치하면 안 되는 몇 개의 리소스만 나열하면 되므로 정책이 짧아집니다. NotResource를 사용할 때는 이 요소에 지정된 리소스들이 제한되는 유일한 리소스라는 점을 유의해야 합니다.

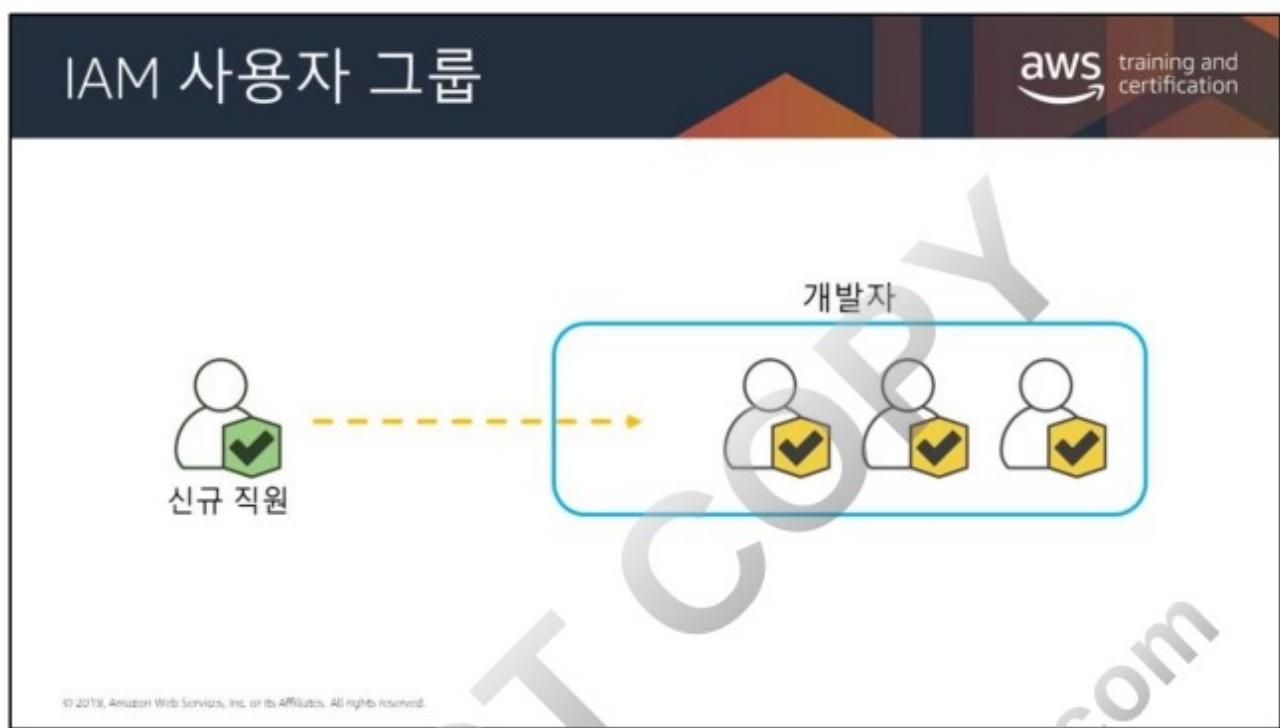


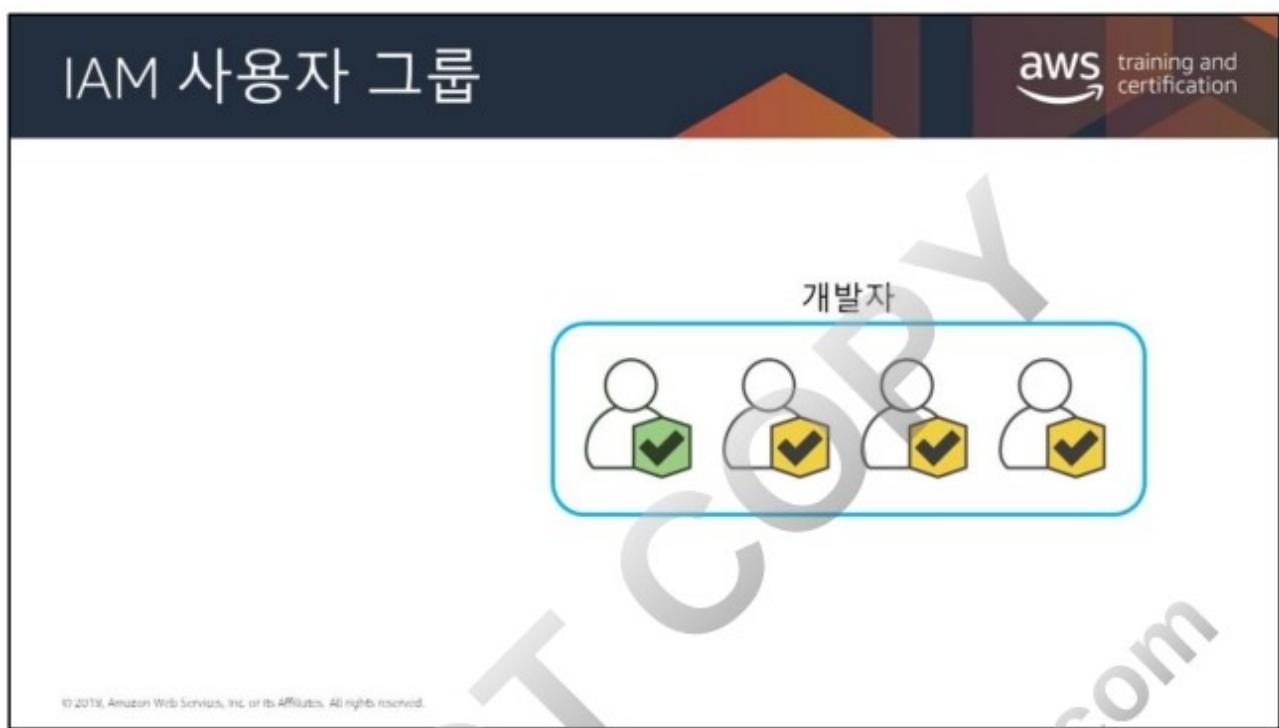
사용자 구성

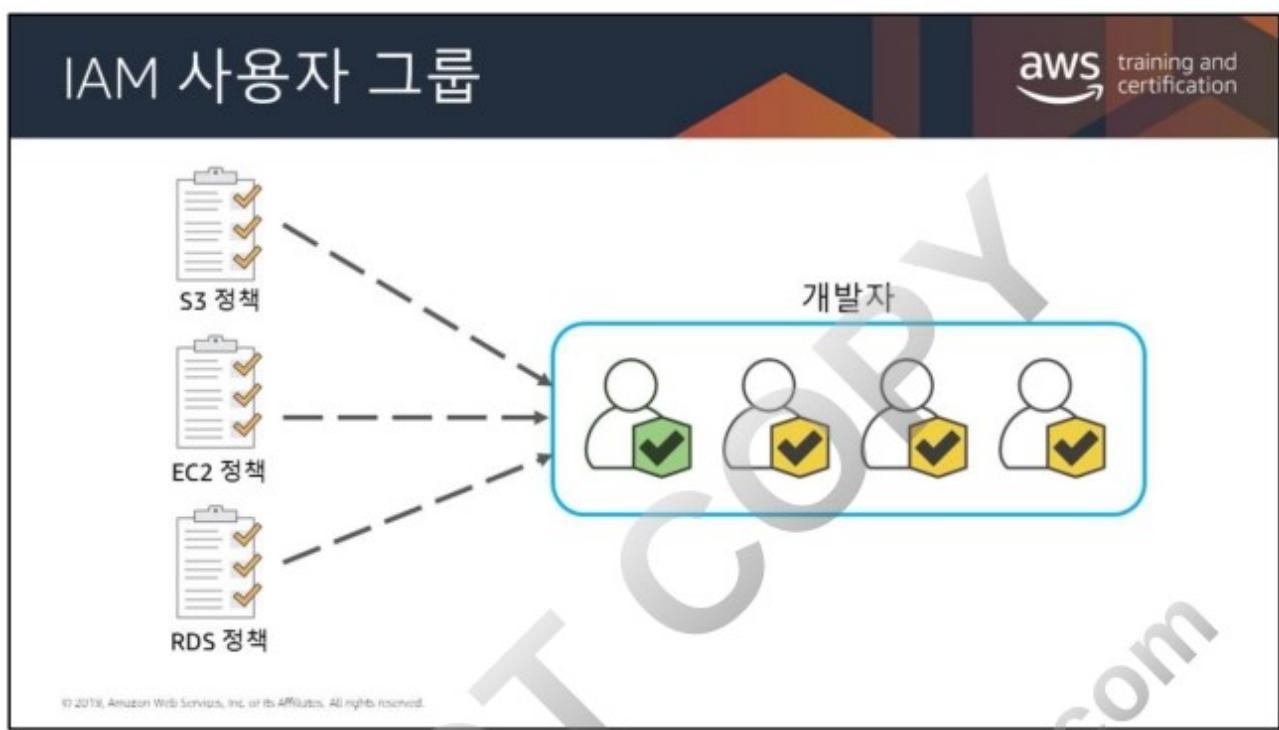
aws training and certification

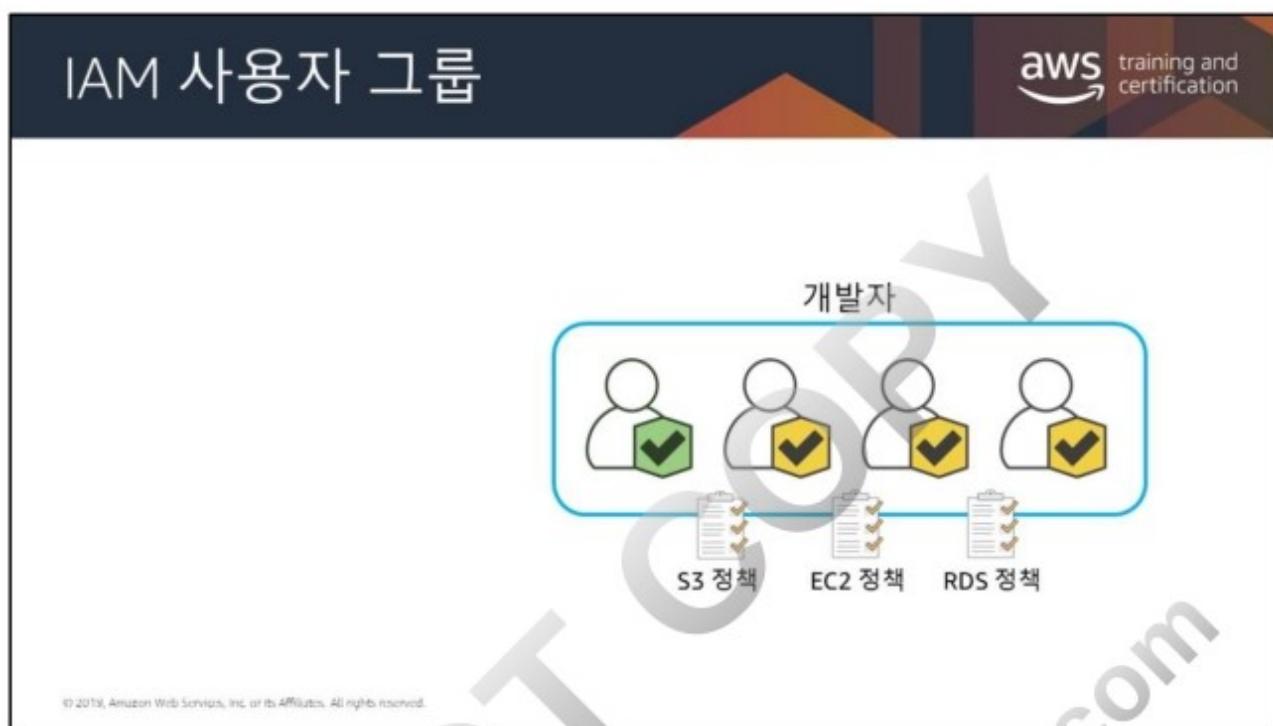
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

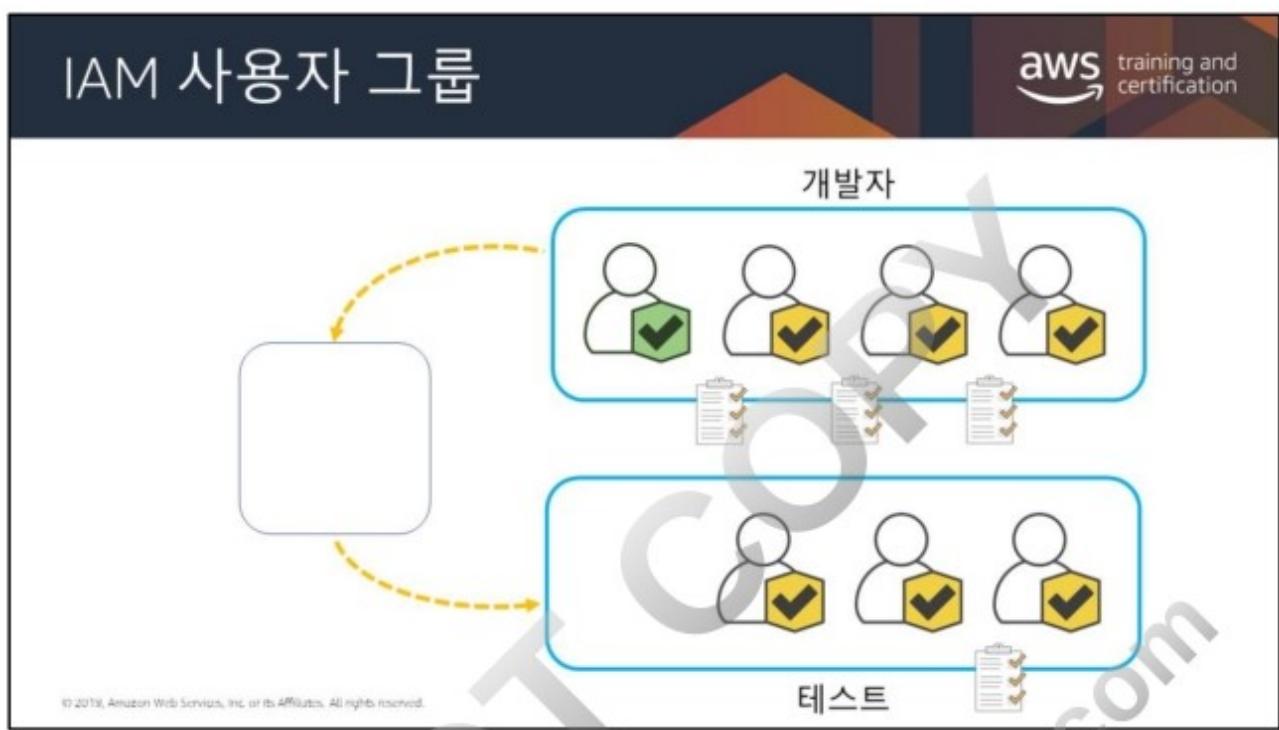
DO NOT COPY
zlagusdbs@gmail.com



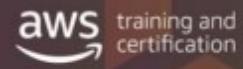








사용자가 하루만 테스트해야 하는
경우에는 어떻게 합니까?



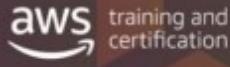
다른 그룹 간에 사용자를 계속 푸시/풀링하지 않으려는
경우 어떻게 합니까?

다른 대상에게 영구 자격 증명을 부여하고 싶지 않으면
어떻게 합니까?

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



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.

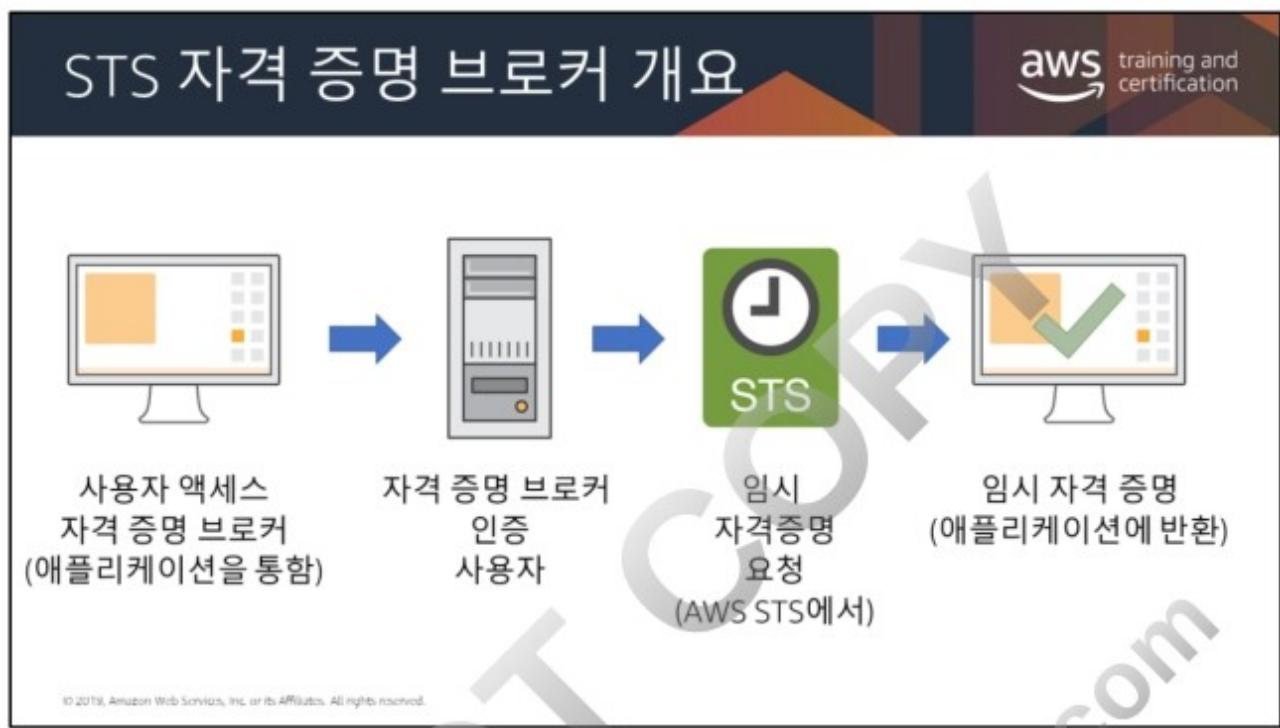
이 정보를 사용하여 위임된 역할을 지닌 연동 사용자의 호출을 외부 연동 호출자에 다시 매핑할 수 있습니다.

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

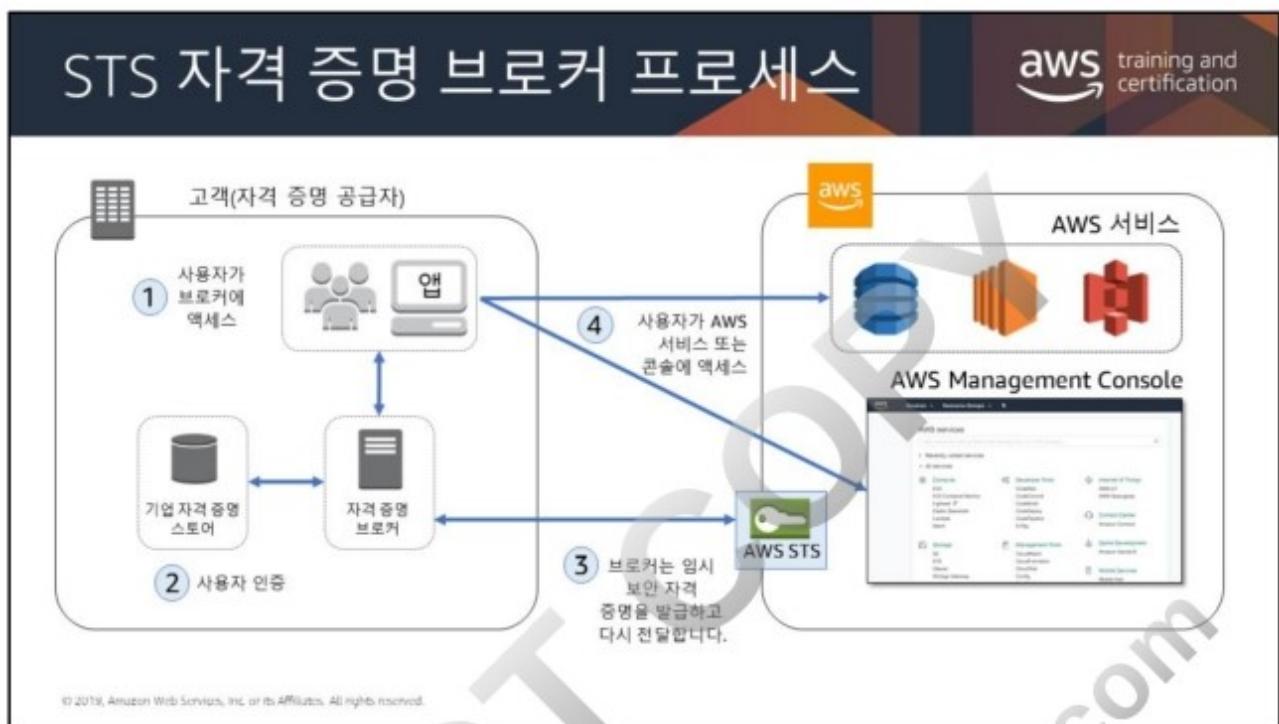
CloudTrail 로그 항목에서 JSON 데이터의 userIdentity 섹션에 AssumeRole 요청을 특정 연동 사용자와 매핑하는 데 필요한 정보가 들어 있습니다.

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:

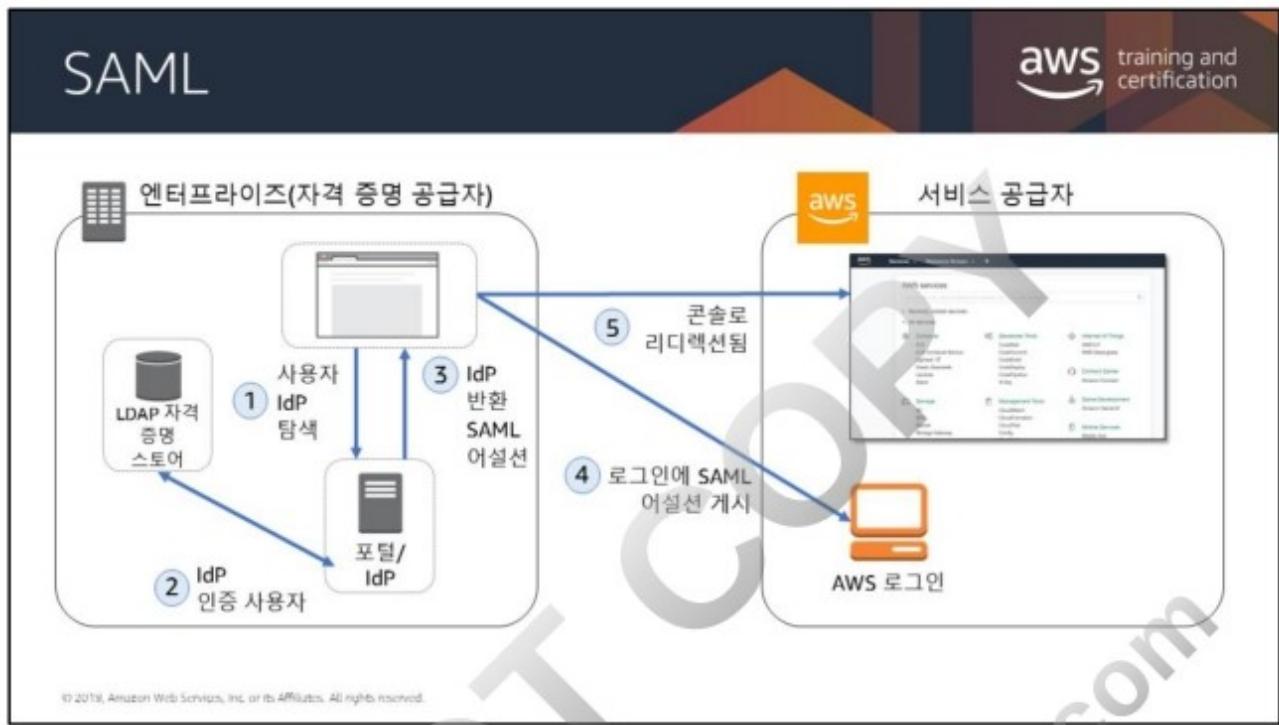
타사에서 조직의 AWS 리소스에 액세스해야 할 때, 역할을 사용하여 리소스에 대한 API 액세스를 위임할 수 있습니다. 예를 들어 타사에서 AWS 리소스를 관리하는 서비스를 제공할 수 있습니다. IAM 역할을 사용하면 AWS 보안 자격 증명을 공유하지 않고도 타사에 AWS 리소스에 대한 액세스 권한을 부여할 수 있습니다. 대신 타사는 AWS 리소스에 액세스하도록 생성한 역할을 맡을 수 있습니다.

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.



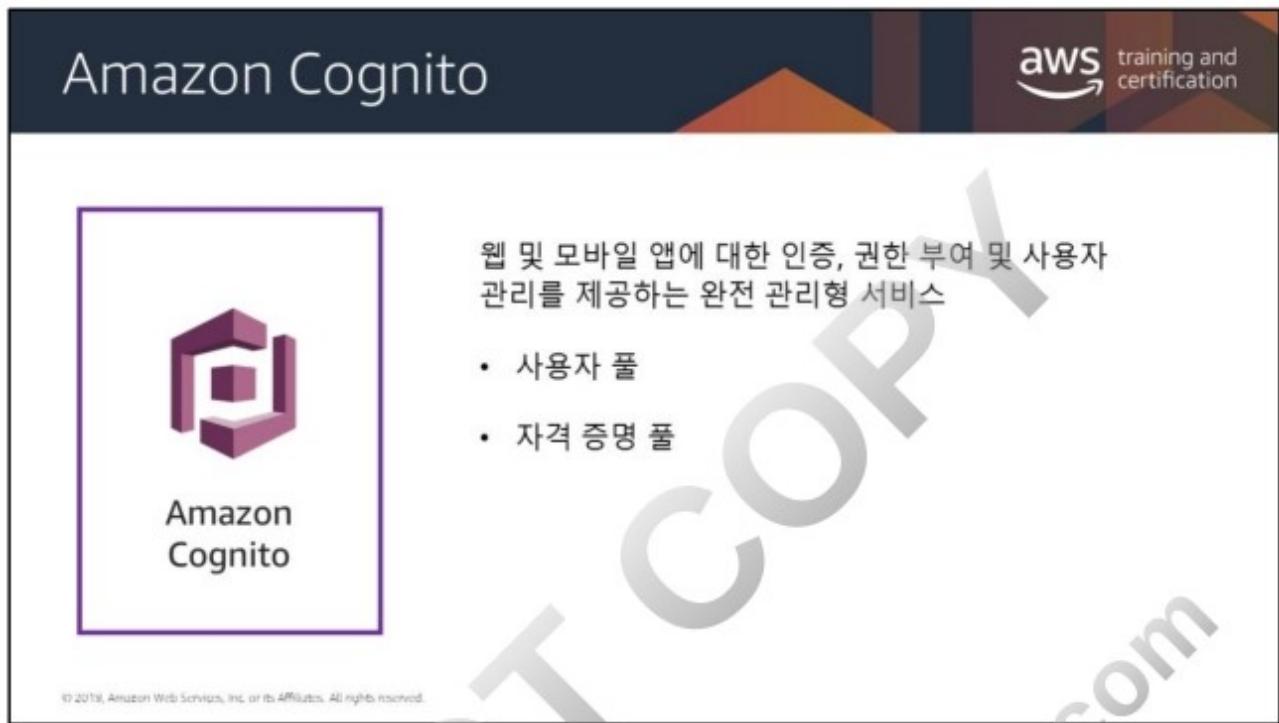
사용자 관점에서는 프로세스가 투명하게 처리됩니다. 사용자는 조직의 내부 포털에서 시작하여 AWS 자격 증명을 제공할 필요 없이 AWS Management Console에 로그인하게 됩니다.

- 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>

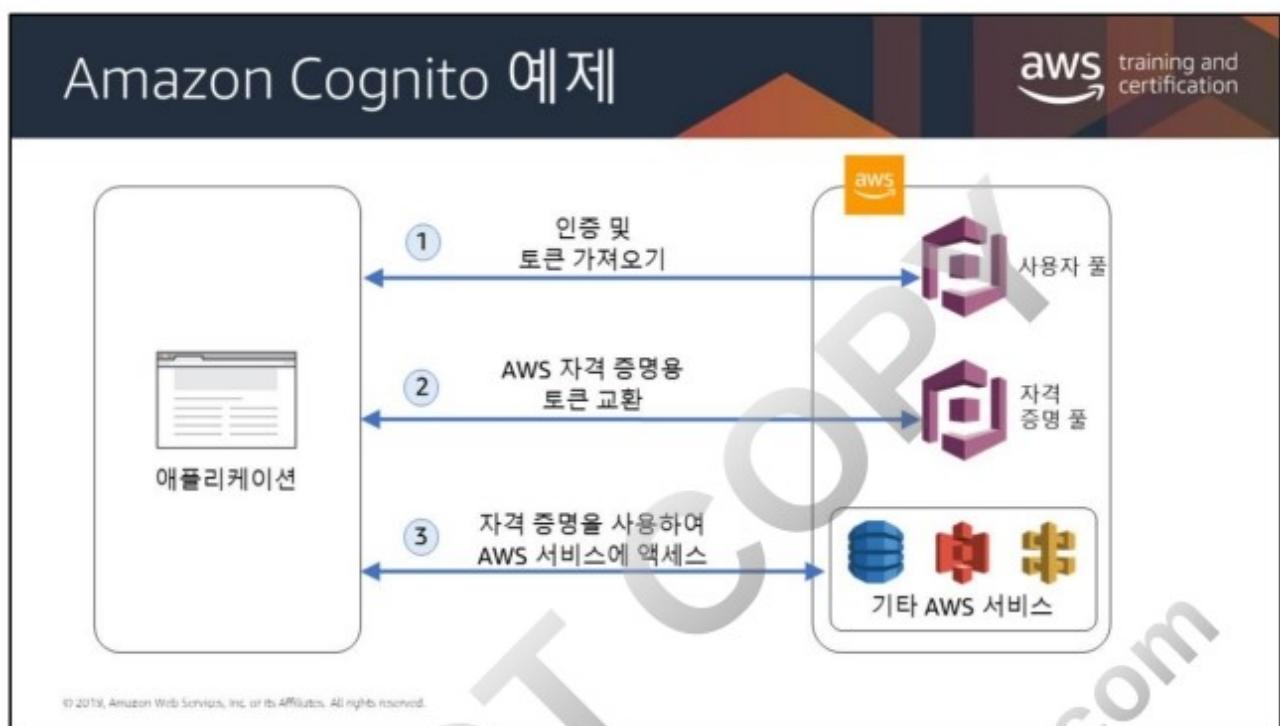
Amazon Cognito 자격 증명 풀은 사용자를 위해 고유한 자격 증명 및 권한 할당을 생성할 수 있게 해줍니다.

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.

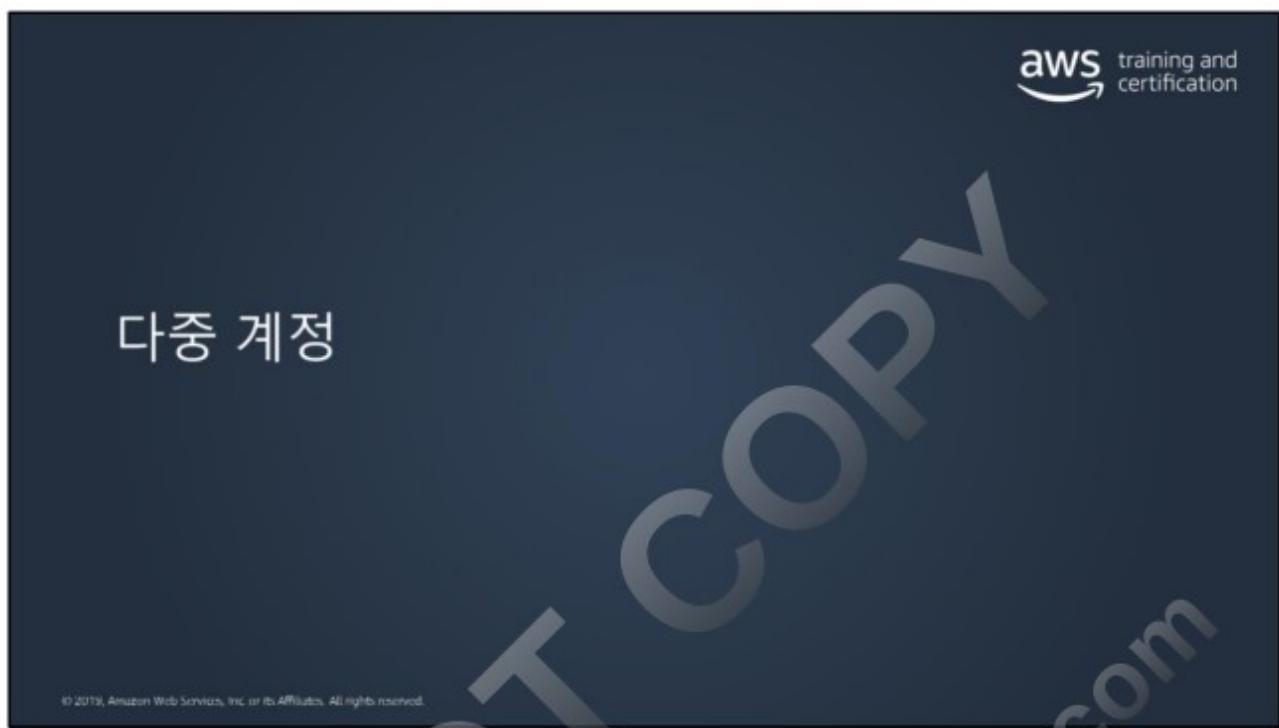
다중 계정 구조: AWS Landing Zone 솔루션에는 4개의 계정과 Centralized Logging 솔루션, AWS Managed AD, AWS SSO용 Directory Connector와 같이 AWS Service Catalog를 사용하여 배포할 수 있는 추가 제품이 포함되어 있습니다.

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?

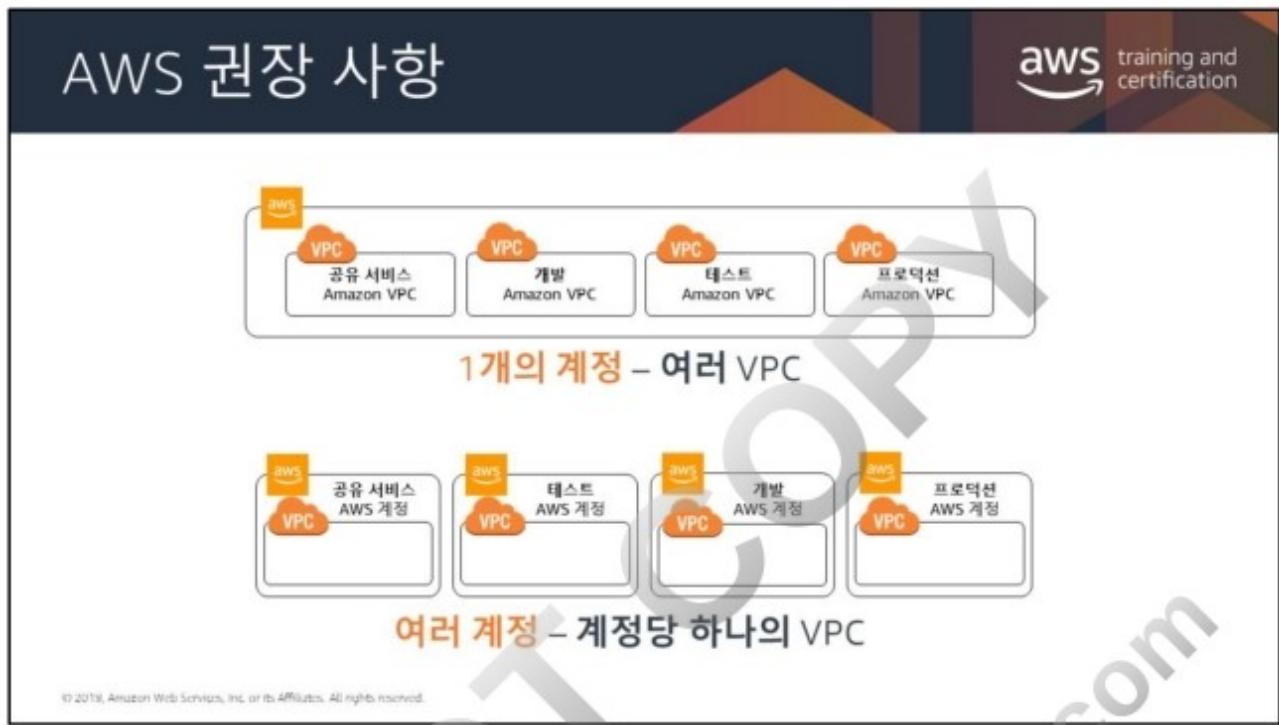
aws
개발

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.

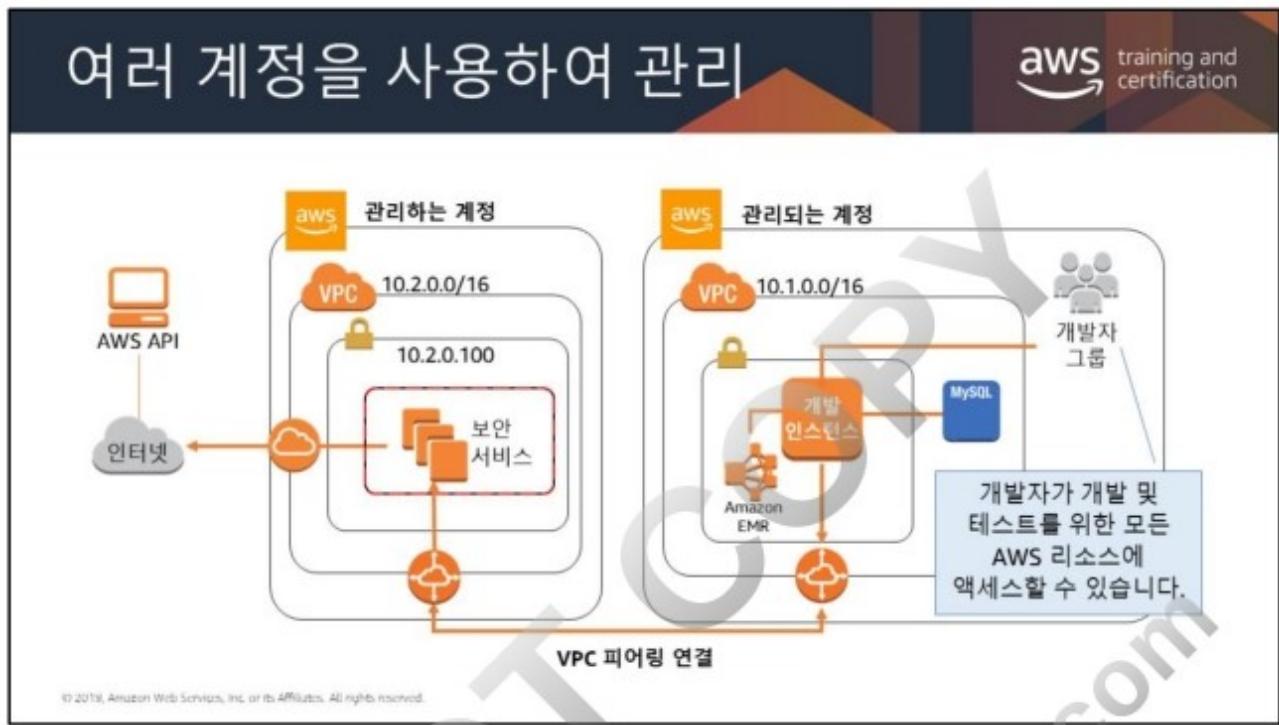
중앙 집중식 보안 관리	단일 AWS 계정
프로덕션, 개발 및 테스트 환경의 분리	3개의 AWS 계정
여러 개의 자율 부서	여러 AWS 계정
여러 개의 자율적인 독립 프로젝트가 포함된 중앙 집중식 보안 관리	여러 AWS 계정

© 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

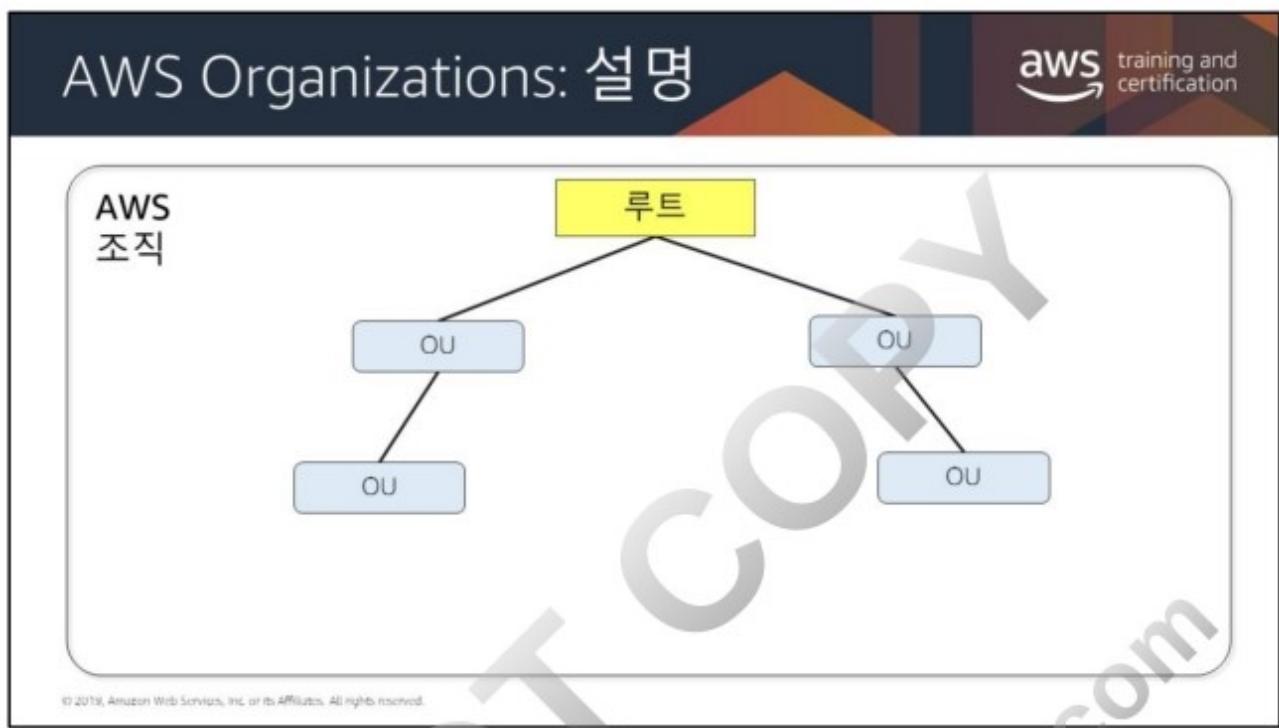
Organizations에서는 SCP를 사용하여 API 수준에서 AWS 서비스 사용을 관리할 수 있습니다. 예를 들어 계정 그룹에 정책을 적용하여 해당 계정의 IAM 사용자만 Amazon S3 버킷에서 데이터를 읽을 있도록 허용할 수 있습니다.

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

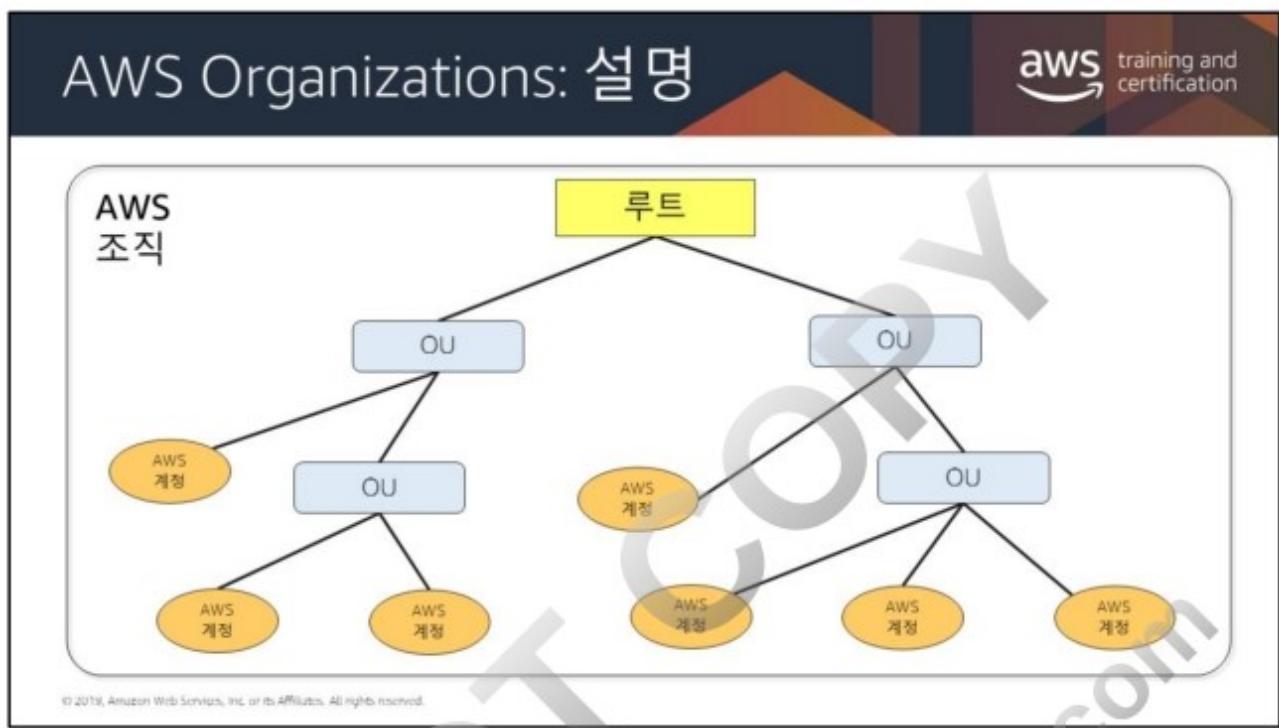




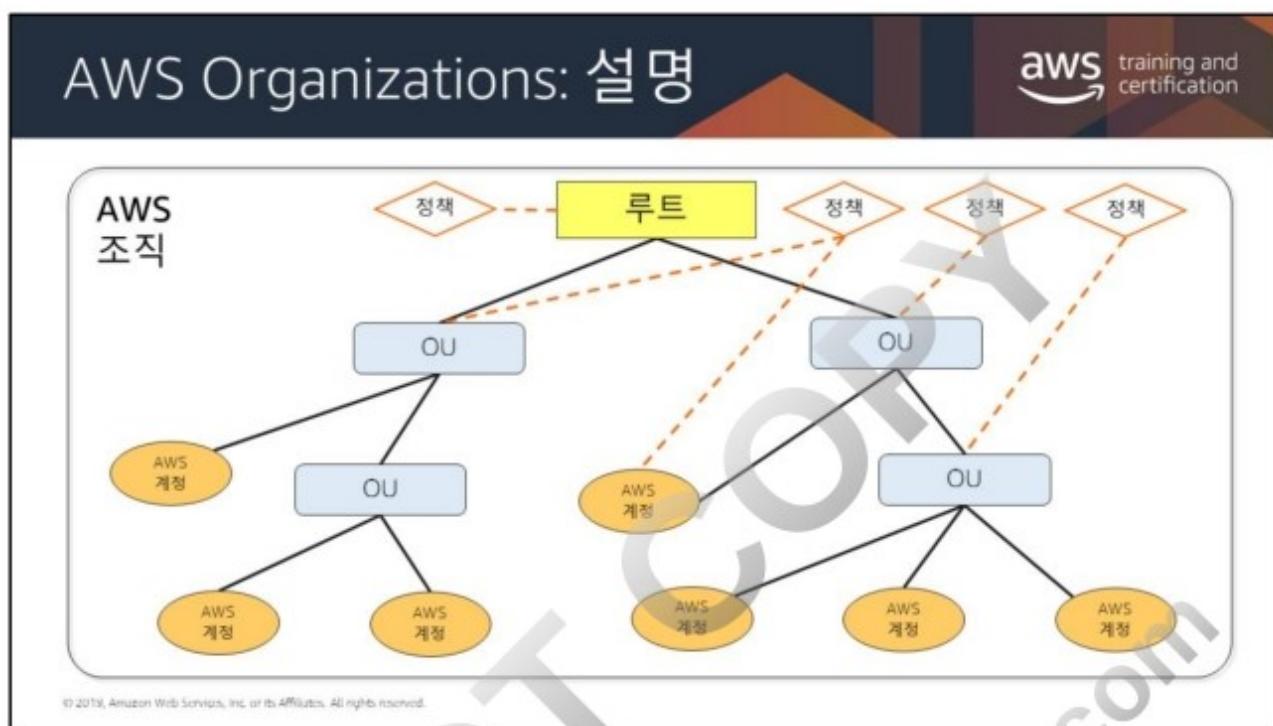
이 예에서 조직에 7개의 계정이 있으며 각 계정은 루트 아래에서 4개의 조직 단위(OU)로 구분되어야 합니다.



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

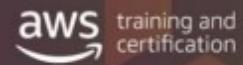
aws training and certification

리소스에 임시 권한을 부여해야 하는 경우
무엇을 사용합니까?

IAM 역할

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

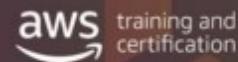
검토



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

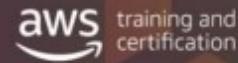


하나의 사용자가 S3 버킷에 액세스할
수 없습니다. 문제의 원인을
파악하려면 무엇을 확인해야 합니까?

사용자와 버킷에 연결된 정책

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

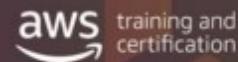
검토



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

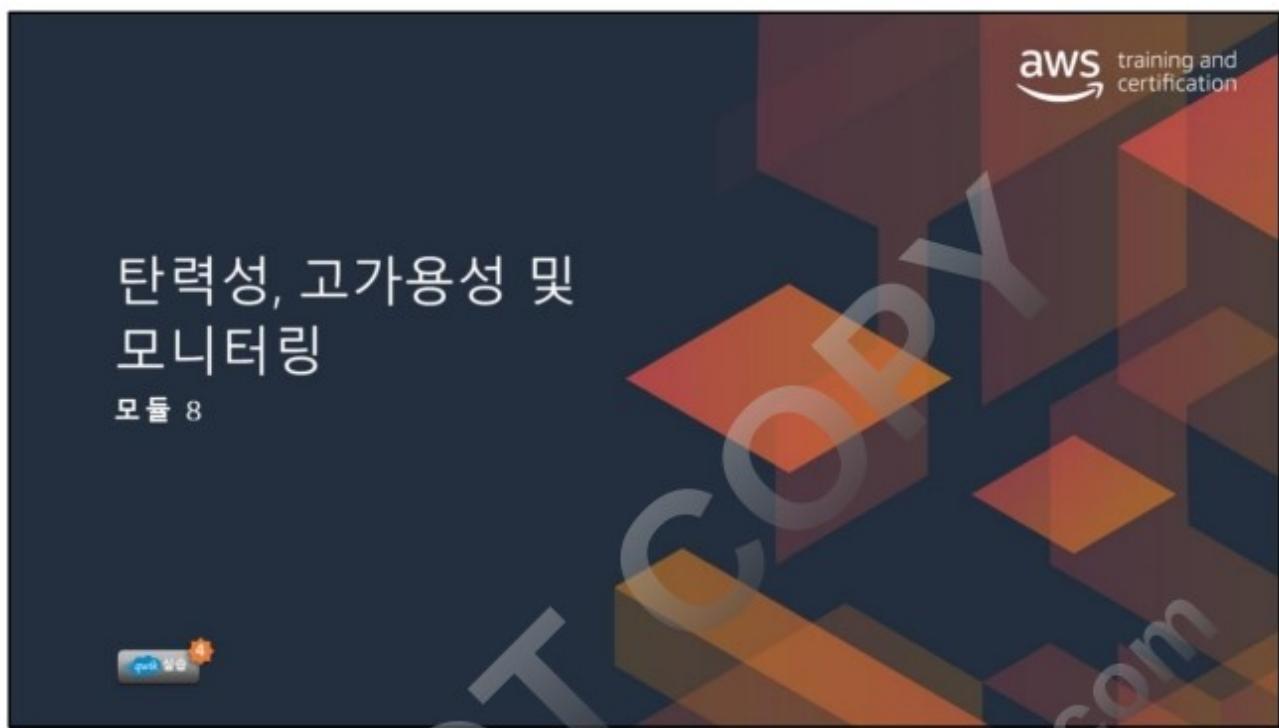


첫째, 프로덕션 환경에서 AWS 계정 루트 사용자 사용을 **중지합니다!**

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.

The slide has a dark blue header bar with the AWS logo and 'training and certification' text. The main title '고가용성 요소' is in large white font. Below it, there are three sections with descriptions:

- 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

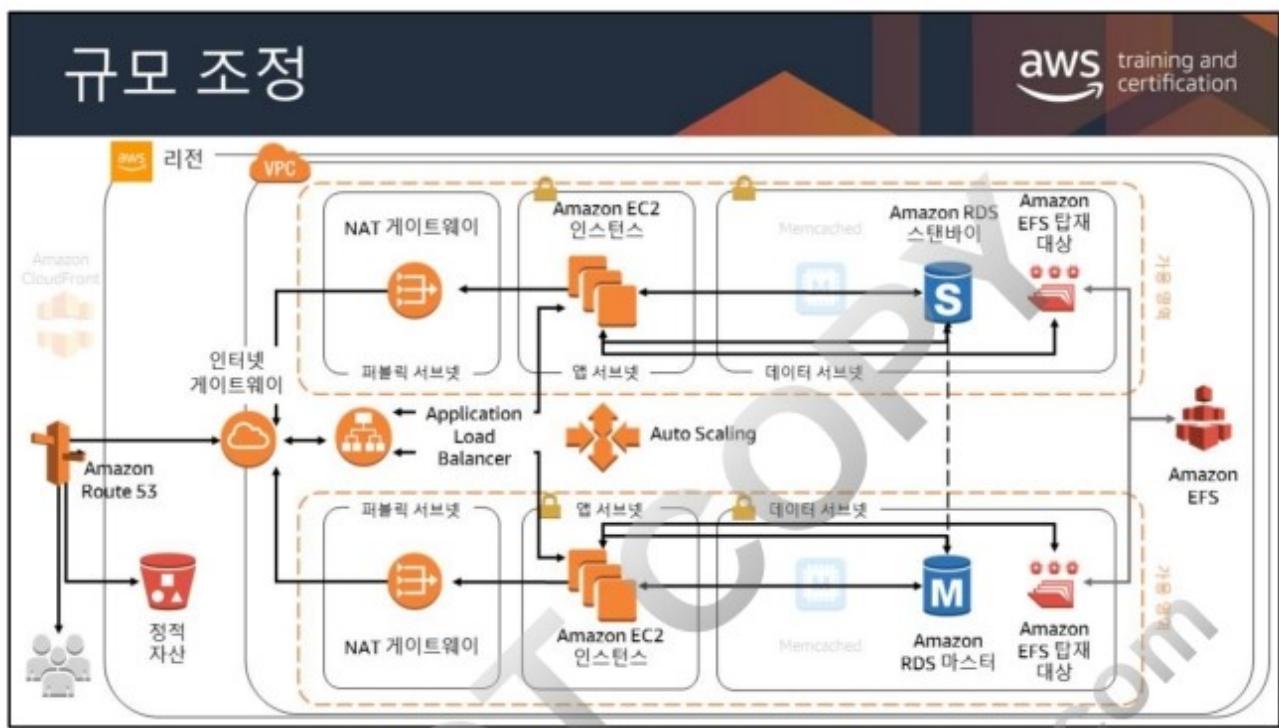
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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.



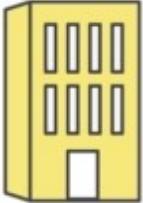
수업이 끝나면 이 아키텍처 디어그램의 모든 구성 요소를 이해할 수 있습니다.
또한 마찬가지로 규모가 크고 강력한 자체 아키텍처 솔루션을 구축할 수 있습니다.



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.

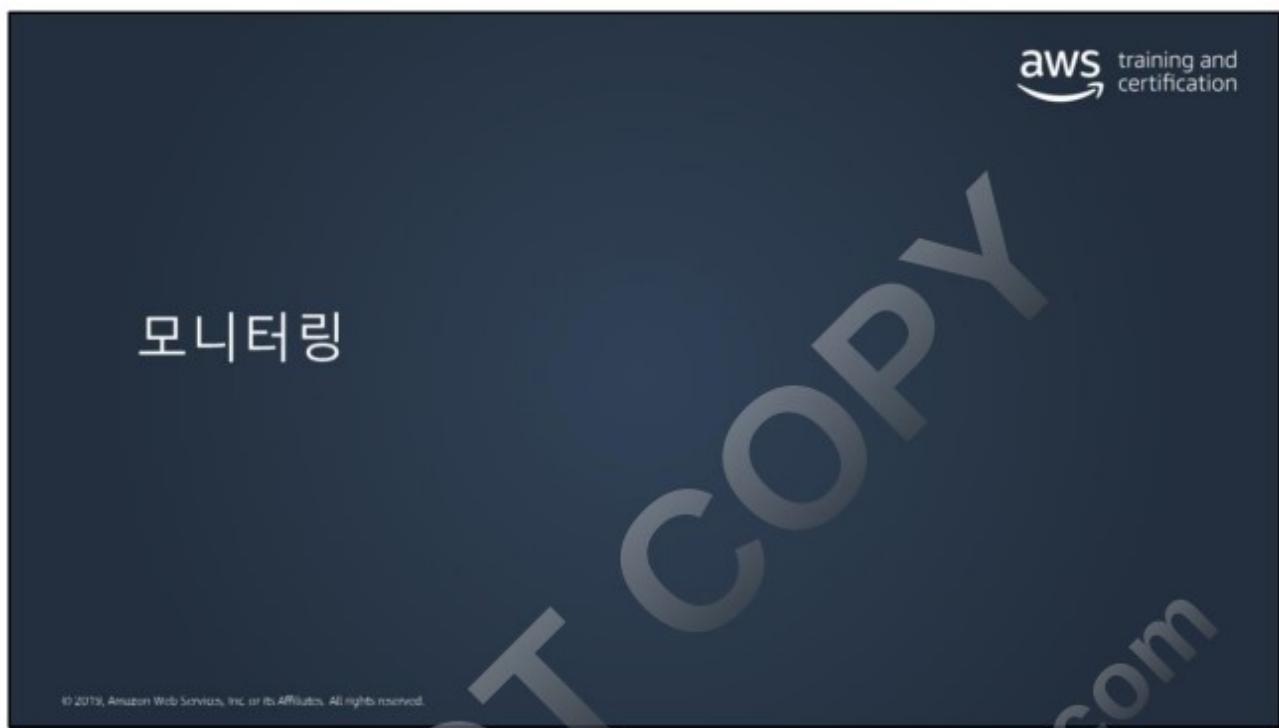
DO NOT COPY
zlagusdbs@gmail.com

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.

비용을 이해하기 위한 모니터링

aws training and certification

보다 유연하고 탄력적인 아키텍처를 만들려면
어디에서 비용을 지출하고 있는지 알아야 합니다.

AWS Cost Explorer

-  보고서를 생성합니다.
-  13개월 데이터
-  예측을 제공합니다.
-  지출 패턴을 참조합니다.

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

Cost Optimization Monitor – 서비스 사용량 및 비용 분석 정보를 제공하는 보고서를 생성할 수 있습니다. 기간, 계정, 리소스 또는 태그를 기준으로 분류할 수 있는 예상 비용을 제공합니다.

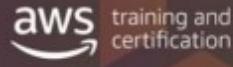
AWS Cost Explorer – 지난 13개월까지 데이터를 볼 수 있으므로 시간 흐름에 따른 AWS 리소스 소비 패턴을 확인할 수 있습니다.

AWS Cost Explorer를 사용한 예측 – 예측은 과거 사용량을 기반으로 사용자가 선택한 예측 기간 동안 AWS 서비스 사용량을 예측하는 것입니다. 보고서의 미래 시간 범위를 선택하여 예측을 생성합니다. 예측을 통해 AWS 청구 금액을 예상하고 사용할 것으로 예측되는 금액에 대해서 경보와 예산을 적용할 수 있습니다. 예측은 예상이므로 예상 청구 금액은 추정치이며 각 청구서 기간의 실제 요금과 다를 수 있습니다.

정확도 범위에 따라 신뢰 구간이 다릅니다. 신뢰 구간이 높을수록 예측이 정확할 가능성이 높습니다. AWS Cost Explorer 예측의 신뢰 구간은 80%입니다. AWS에 80% 신뢰 구간 내로 예측하는 데 충분한 데이터가 없는 경우, AWS Cost Explorer는 예측을 표시하지 않습니다.

<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/ce-modify.html#ce-timerange>

Amazon CloudWatch를 사용하여 인프라 모니터링



Amazon CloudWatch

• 리소스에 대한 지표를 수집하고 추적합니다.

• 경보를 생성하고 알림을 전송할 수 있습니다.

• 설정한 규칙에 따라 리소스의 용량 변화를 트리거할 수 있습니다.

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

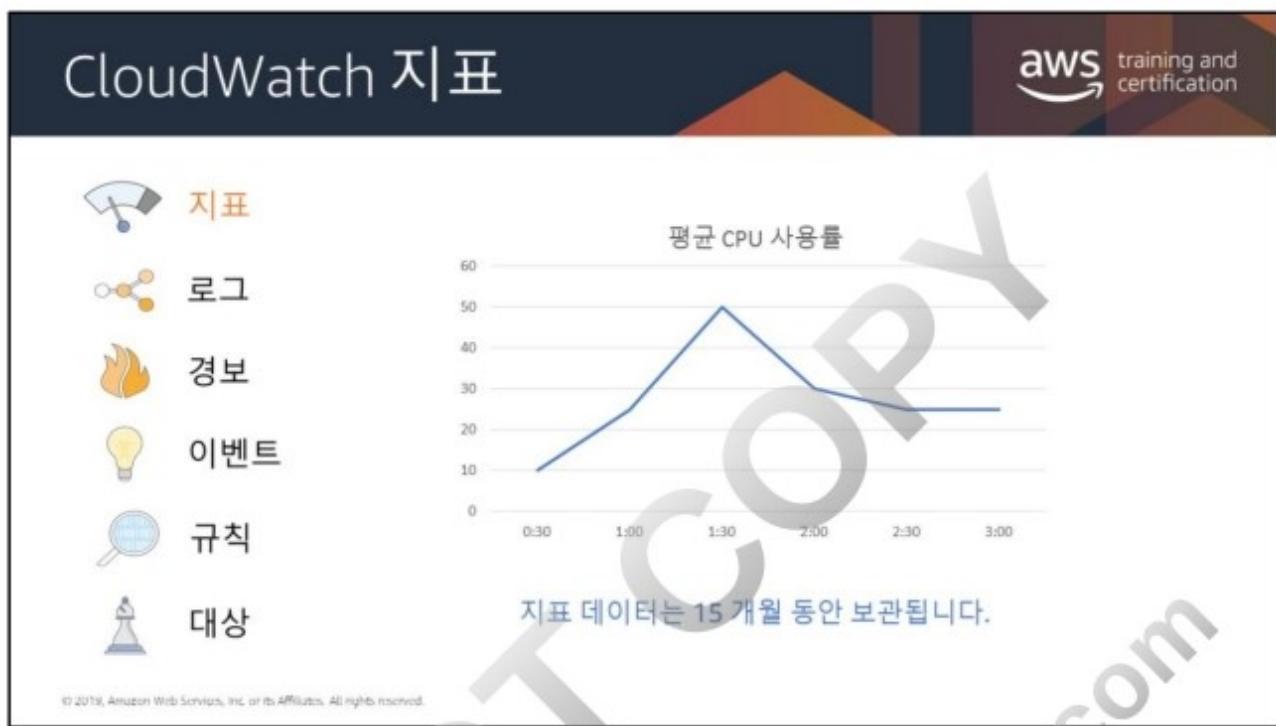
탄력적 아키텍처를 생성하는 여정의 첫 단계는 Amazon CloudWatch를 살펴보는 것입니다. CloudWatch는 AWS 리소스 및 애플리케이션에 대한 가시성을 확대하는 데 도움이 됩니다.

CloudWatch를 사용하여 리소스 및 애플리케이션에 대해 측정할 수 있는 변수인 지표를 수집하고 추적할 수 있습니다. CloudWatch 경보는 알림을 보내거나 정의한 규칙을 기준으로 모니터링하는 리소스를 자동으로 변경합니다. 예를 들어 Amazon EC2 인스턴스의 CPU 사용량과 디스크 읽기 및 쓰기를 모니터링한 다음, 이러한 데이터를 사용하여 증가된 로드를 처리하기 위해 추가 인스턴스를 시작해야 할지 결정할 수 있습니다. 또한 이러한 데이터를 사용하여 사용률이 낮은 인스턴스를 중지하고 비용을 절감할 수도 있습니다. AWS에서 기본으로 제공하는 지표 이외에도 사용자 지정 지표를 모니터링할 수 있습니다. CloudWatch를 사용하면 시스템 전체의 리소스 사용률, 애플리케이션 성능 및 운영 상태를 파악할 수 있습니다.

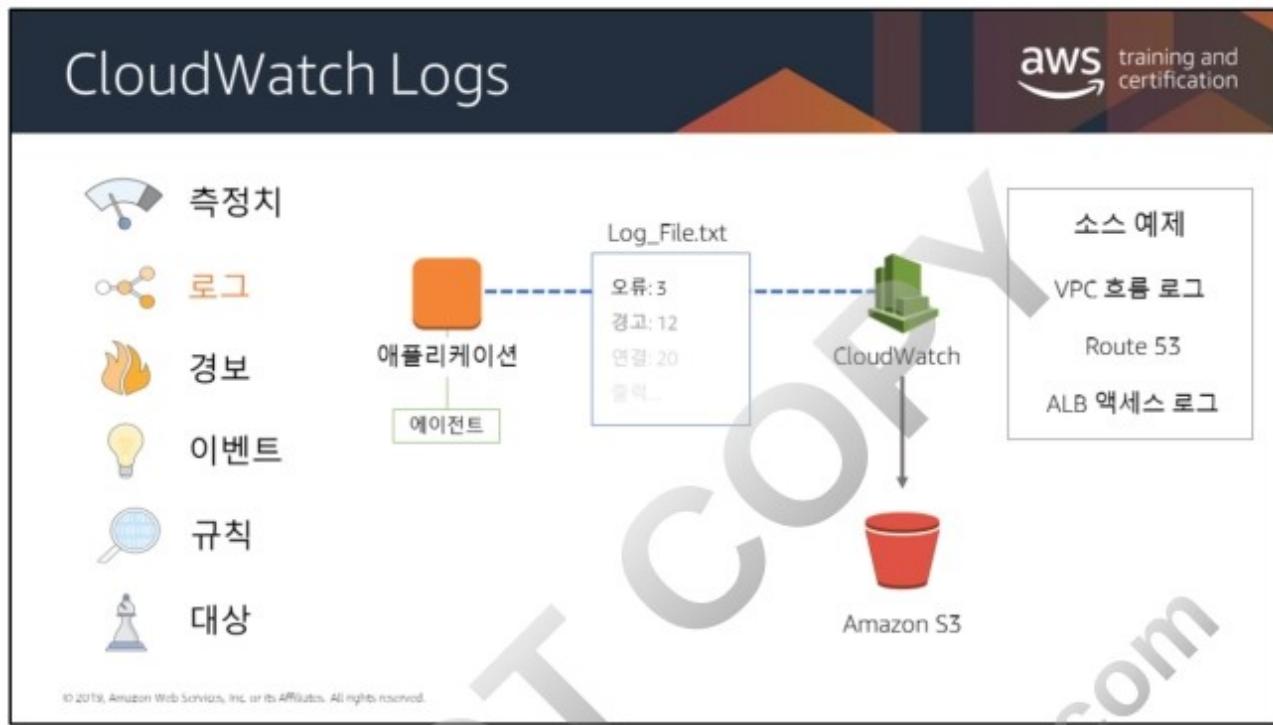
자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html>.





지표는 시스템 성능에 대한 데이터입니다. 많은 AWS 서비스가 리소스에 대한 지표를 기본적으로 제공합니다(예: Amazon EC2 인스턴스, Amazon EBS 볼륨, Amazon RDS DB 인스턴스). 또한 Amazon EC2 인스턴스 같은 일부 리소스에 대해 세부 모니터링을 활성화하거나 자체 애플리케이션 지표를 게시할 수도 있습니다. Amazon CloudWatch는 검색, 그래프 처리 및 경보를 위해 계정에 모든 지표(AWS 리소스 지표 및 사용자가 제공한 애플리케이션 지표 모두)를 로드할 수 있습니다.



CloudWatch Logs를 사용하면 소스(예: EC2 인스턴스, Amazon Route 53, AWS CloudTrail 및 기타 AWS 서비스)의 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다.

예를 들어 Amazon EC2 인스턴스의 로그를 실시간으로 모니터링할 수 있습니다. 애플리케이션 로그에서 오류 발생 횟수를 추적하고 해당 비율이 사전에 정의된 수준을 초과할 경우 알림을 보낼 수 있습니다.

CloudWatch Logs는 로그 데이터 자체를 모니터링하기 때문에 코드 변경이 필요하지 않습니다.

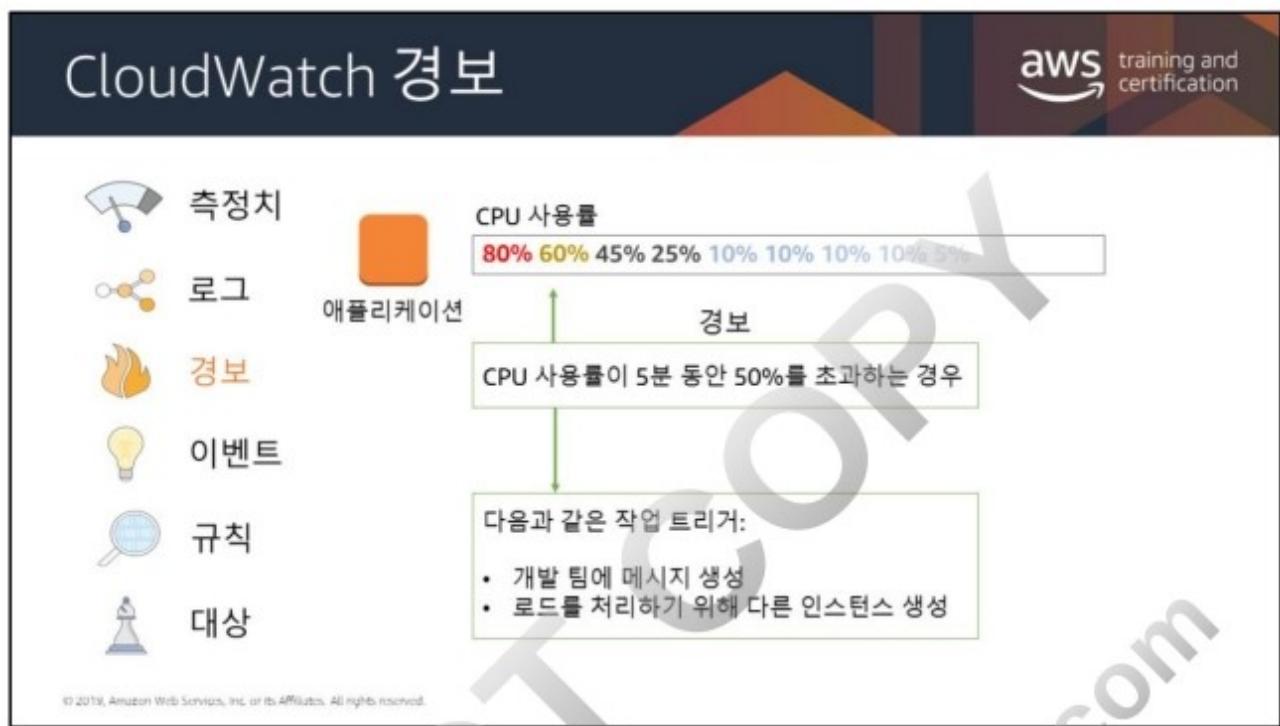
또한 CloudWatch Logs Insights를 사용하여 몇 초 만에 로그를 분석하면 빠른 대화형 쿼리 및 시각화를 얻을 수 있습니다. 선 또는 누적 영역형 차트를 사용하여 쿼리 결과를 시각화할 수 있으며, CloudWatch 대시보드에서 해당 쿼리를 추가할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html>

<https://aws.amazon.com/blogs/aws/new-amazon-cloudwatch-logs-insights-fast-interactive-log-analytics/>

DO NOT COPY
zlagusdbs@gmail.com



경보를 사용하여 작업을 자동으로 시작할 수 있습니다. 경보는 지정한 기간에 단일 지표를 감시하고 시간에 따른 임계값 대비 지표 값을 기준으로 지정된 작업을 하나 이상 수행합니다. 작업이란 Amazon SNS 주제 또는 Auto Scaling 정책으로 전송되는 알림을 말합니다. 대시보드에 경보를 추가할 수도 있습니다.

경보는 지속되는 상태 변경에 대해서만 작업을 호출합니다. CloudWatch 경보는 특정 상태가 되었다고 해서 작업을 호출하지는 않습니다. 상태가 변경되어야 하고 지정된 기간 동안 변경된 상태가 유지되어야 합니다.

이 예에서는 경보가 트리거되면 Auto Scaling 정책 실행, 알림 전송(인스턴스에 대한 알림을 운영팀에 전송) 등 다른 작업이 시작됩니다.

또한, 작업은 경보가 트리거되지 않아도 실행될 수 있습니다.



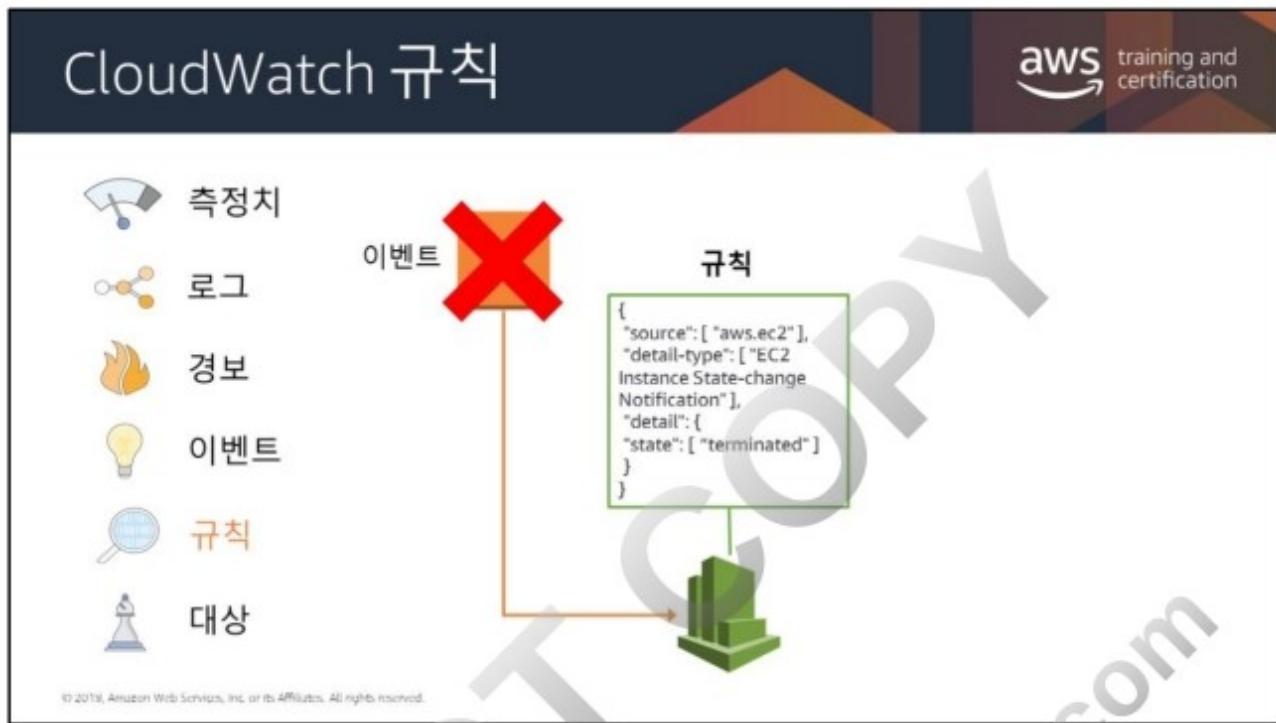
Amazon CloudWatch Events는 AWS 리소스의 변경 사항을 설명하는 시스템
이벤트의 스트림을 거의 실시간으로 제공합니다.

AWS 리소스는 상태 변경 시 이벤트를 생성할 수 있습니다. 예를 들어, Amazon EC2는 EC2 인스턴스의 상태가 보류에서 실행으로 변경될 때 이벤트를 생성하며, Amazon EC2 Auto Scaling은 인스턴스가 시작 또는 종료될 때 이벤트를 생성합니다.

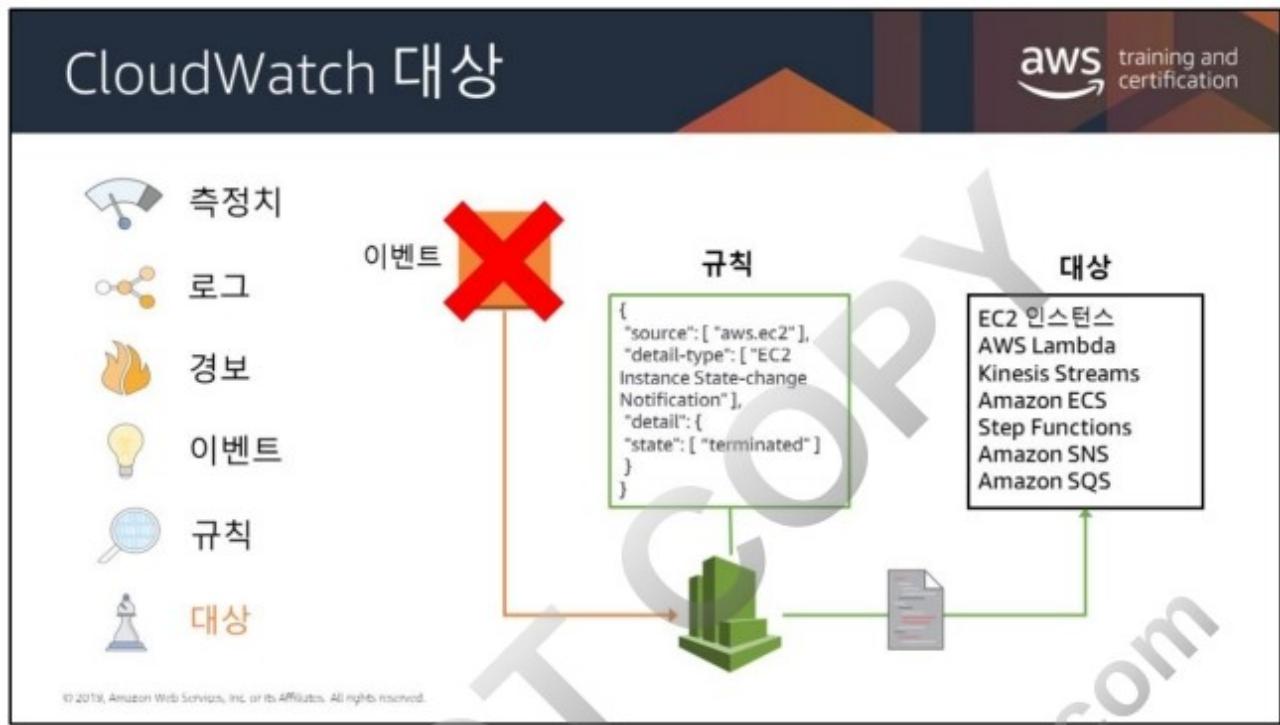
신속하게 설정할 수 있는 단순 규칙을 사용하여 일치하는 이벤트를 검색하고
하나 이상의 대상 함수 또는 스트림으로 이를 라우팅할 수 있습니다.

CloudWatch Events는 운영 변경 시 이를 알아차립니다. CloudWatch Events는
환경에 응답하기 위한 메시지를 전송하고, 함수를 활성화하고, 변경을 수행하고,
상태 정보를 기록하는 등 이러한 운영 변경에 응답하고 필요에 따라 교정 조치를
취합니다.

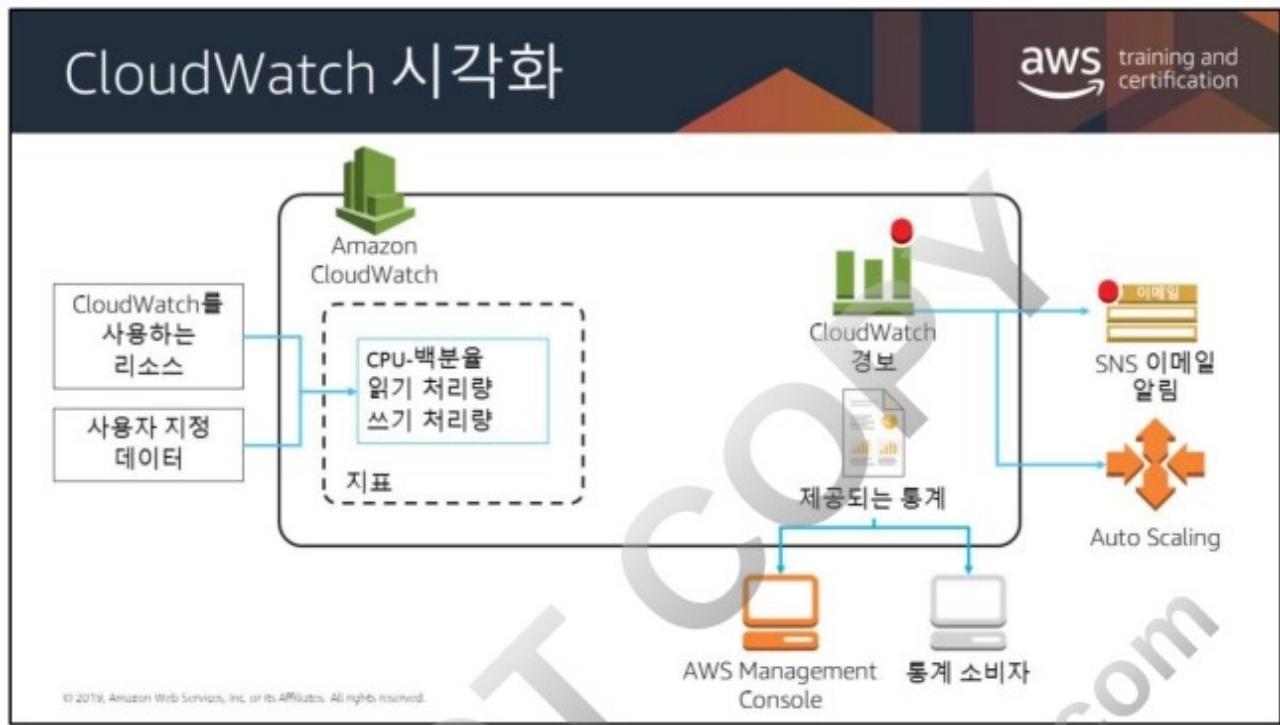
또한 CloudWatch Events를 사용하여 cron 또는 rate 표현식을 통해 특정 시간에
자체 트리거되는 자동 작업을 예약할 수 있습니다.



규칙은 들어오는 이벤트에서 일치하는 것을 찾아서 대상으로 라우팅하여 처리합니다. 단일 규칙으로 여러 개의 대상으로 라우팅을 할 수 있으며, 이들은 모두 병렬 처리됩니다. 규칙이 처리되는 특정한 순서는 없습니다. 따라서 한 조직의 서로 다른 파트들이 자신이 관심 있는 이벤트를 찾아서 처리할 수 있습니다. 규칙은 특정 부분만 전달하거나 상수로 덮어쓰기를 해서 대상에 전송되는 JSON을 사용자 지정할 수 있습니다.



대상은 이벤트를 처리합니다. 대상에는 Amazon EC2 인스턴스, AWS Lambda 함수, Kinesis 스트림, Amazon ECS 작업, Step Functions 상태 시스템, Amazon SNS 주제, Amazon SQS 대기열 및 기본 제공 대상이 포함될 수 있습니다. 대상은 JSON 형식으로 이벤트를 수신합니다.



Amazon CloudWatch는 기본적으로 지표 리포지토리입니다. AWS 서비스(예: Amazon EC2)는 지표를 리포지토리에 저장하므로 이러한 지표를 기반으로 통계를 검색할 수 있습니다. 사용자 지정 지표를 리포지토리에 저장하면 해당 지표에 대한 통계도 검색할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_architecture.html



AWS CloudTrail은 계정에 대한 AWS API 호출을 기록하고 로그 파일을 사용자에게 전달하는 웹 서비스입니다. API 호출자 자격 증명, API 호출 시간, API 호출자의 원본 IP 주소, 요청 파라미터 및 AWS 서비스가 반환한 응답 요소와 같은 정보가 기록됩니다.

CloudTrail에서는 AWS 관리 콘솔, AWS SDK, 명령줄 도구, 상위 수준 AWS 서비스(예: AWS CloudFormation)를 통해 이루어진 API 호출을 비롯하여 계정에 대한 AWS API 호출 내역을 확인할 수 있습니다. CloudTrail에서 작성되는 AWS API 호출 내역을 통해 보안 분석, 리소스 변경 사항 추적 및 규정 준수 감사를 수행할 수 있습니다.

CloudTrail은 리전 단위로 활성화됩니다. 여러 리전을 사용하는 경우, 리전별로 로그 파일이 전송될 장소를 선택할 수 있습니다. 예를 들어 리전별로 별도의 Amazon S3 버킷을 사용하거나 모든 리전의 로그 파일을 하나의 Amazon S3 버킷에 집계할 수 있습니다.

CloudTrail에서 지원하는 AWS 서비스 목록은

<http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-supported-services.html>를 참조하십시오.

CloudTrail APN 파트너에 대한 자세한 내용은 다음을 참조하십시오.

- Splunk: <http://aws.amazon.com/cloudtrail/partners/splunk/>
- AlertLogic: <https://aws.amazon.com/cloudtrail/partners/alert-logic/>
- SumoLogic: <https://aws.amazon.com/cloudtrail/partners/sumo-logic/>

네트워크 모니터링 VPC 흐름 로그

VPC Flow Logs

- VPC의 **트래픽 흐름 세부 정보**를 캡처합니다.
- 허용, 거부 또는 모든 트래픽
- **VPC, 서브넷** 및 **ENI**에 대해 활성화될 수 있습니다.
- 로그는 **CloudWatch Logs**로 게시됩니다.
- 로그는 **Amazon S3**로 게시됩니다.

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

VPC Flow Logs는 VPC의 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 캡처할 수 있게 해주는 기능입니다. 흐름 로그 데이터는 Amazon CloudWatch Logs를 통해 저장됩니다. 흐름 로그를 생성하고 난 후에는 Amazon CloudWatch Logs의 데이터를 확인하고 가져올 수 있습니다.

흐름 로그는 특정 트래픽이 인스턴스에 도달하지 않는 문제를 해결하는 등 다양한 작업에 도움을 주므로 과도하게 제한적인 보안 그룹 규칙을 진단할 수 있게 도와줍니다. 또한, 흐름 로그를 보안 도구로 사용하여 인스턴스에 도달하는 트래픽을 모니터링할 수 있습니다.

사용 사례:

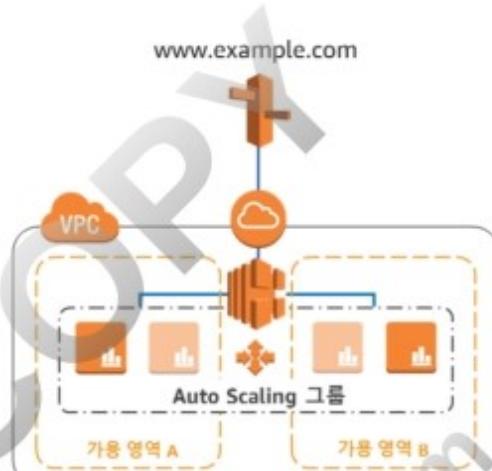
- 연결 문제 해결
- 네트워크 액세스 규칙 테스트
- 트래픽 모니터링
- 보안 인시던트 탐지 및 조사



Auto Scaling을 사용하여 탄력성 제공

 Amazon EC2 Auto Scaling

- 지정된 조건에 따라 인스턴스를 시작 또는 종료합니다.
- 지정된 경우, 새 인스턴스를 로드 밸런서에 자동으로 등록합니다.
- 여러 가용 영역에 걸쳐 시작할 수 있습니다.



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

조정 정책을 지정했다면, Auto Scaling에서는 애플리케이션의 늘어나거나 줄어드는 수요에 따라 인스턴스를 시작하거나 종료할 수 있습니다. Auto Scaling은 ELB와 통합되어 기존 Auto Scaling 그룹에 하나 이상의 로드 밸런서를 추가할 수 있습니다. 로드 밸런서를 연결한 후에는 로드 밸런서가 자동으로 인스턴스를 그룹에 등록하고 인스턴스 간에 수신 트래픽을 분산합니다.

하나의 가용 영역이 비정상 또는 사용 불가 상태가 되었을 때, Auto Scaling에서는 영향을 받지 않은 가용 영역에서 새 인스턴스를 시작합니다. 비정상 가용 영역이 정상 상태로 복귀하는 경우 Auto Scaling 그룹의 모든 가용 영역에 걸쳐 애플리케이션 인스턴스가 자동으로 고르게 재분배됩니다. 이는 최소의 인스턴스로 가용 영역에서 새 인스턴스를 시작하려고 하는 방식으로 Auto Scaling에 의해 수행됩니다. 하지만 시도가 실패하는 경우 성공할 때까지 Auto Scaling은 다른 가용 영역에서 시작을 계속 시도합니다.

자동 조정 방법

aws training and certification

예약

예측 가능한 워크로드에 적합

 시간 또는 날짜를 기준으로 조정

사용 사례: 야간에 개발 및 테스트 인스턴스 종료

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

일정 기반 조정을 사용하면 알려진 부하 변경에 앞서 애플리케이션을 조정할 수 있습니다. 예를 들어 매주 수요일에 웹 애플리케이션 트래픽이 증가하고 목요일까지 높은 상태로 유지되다가 금요일에 줄어들기 시작합니다. 웹 애플리케이션의 예측 가능한 트래픽 패턴에 따라 조정 활동을 계획할 수 있습니다.

자동 조정 방법

aws training and certification

예약	동적
예측 가능한 워크로드에 적합	일반적 조정에 탁월
 시간 또는 날짜를 기준으로 조정	 대상 추적 지원
사용 사례: 야간에 개발 및 테스트 인스턴스 종료	사용 사례: CPU 사용률에 따라 조정

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





Amazon EC2 Auto Scaling은 동일한 Auto Scaling 그룹(ASG) 내에서 여러 구매 옵션을 지원합니다. 단일 ASG 내에 스팟, 온디맨드 및 예약 인스턴스(RI)(청구서가 처리될 때까지는 온디맨드 인스턴스)를 포함할 수 있으므로 컴퓨팅 비용을 최대 90%까지 절감할 수 있습니다.

Amazon EC2 Fleet을 사용하면 원하는 ASG 용량을 구성하는 EC2 인스턴스 유형의 조합을 정의할 수 있습니다. 이 조합은 구매 옵션 중 각 유형의 비율로 정의됩니다. EC2 Auto Scaling은 ASG가 축소 또는 확장함에 따라 원하는 비용 최적화를 유지합니다. 혼합 플릿으로 구성된 ASG도 단일 플릿 ASG와 동일한 수명 주기 후크, 인스턴스 상태 확인, 예약 조정을 지원합니다.

인스턴스 유형 및 구매 모델을 혼합하여 ASG를 정의할 때 구성할 수 있는 옵션은 다음과 같습니다.

최고 스팟 가격: ASG 인스턴스의 최고 스팟 가격을 설정합니다.

스팟 할당 전략: 가용 영역 다양성에 따라 구성합니다. 단일 가용 영역에서 특정 인스턴스 유형에 대한 수요가 높을 때 특히 유용합니다.

(선택 사항) 온디맨드 기본: 초기 용량을 온디맨드 인스턴스로 구성합니다. 전체 용량을 구성하는 온디맨드 인스턴스 비율과 구분됩니다.

기본을 초과하는 온디맨드 비율: 초기 그룹에 추가하는 온디맨드 인스턴스 비율을 제어합니다.

혼합 플릿 구성은 RAM 및 vCPU 용량이 다른 다양한 EC2 인스턴스 유형과 조합할 수 있습니다. EC2 Auto Scaling은 원하는 용량에 맞춰 가장 낮은 가격의 조합을 자동으로 프로비저닝합니다.

DO NOT COPY
zlagusdbs@gmail.com

Auto Scaling 최소 용량

aws training and certification

Auto Scaling 그룹에서 다음을 정의:

- 원하는 용량
- 최소 용량
- 최대 용량

설정하기에 적절한 **최소** 용량은 어떻게 됩니까?

설정하기에 적절한 **최대** 용량은 어떻게 됩니까?

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



Auto Scaling 고려 사항

aws training and certification

- 여러 유형의 autoscaling을 결합해야 할 수 있음
- 단계 조정을 사용하여 아키텍처를 조정하려면 더 많은 작업이 필요할 수 있음
- 일부 아키텍처의 경우 둘 이상의 지표를 사용하여 조정해야 함(예: CPU 외의 추가 지표 사용)
- 조기에 빠르게 확장하고 시간이 지남에 따라 천천히 축소
- 수명 주기 후크 사용

Auto Scaling이 인스턴스를 시작 또는 종료할 때 사용자 지정 작업 수행

주의: 인스턴스가 시작 후 완전히 사용 가능한 상태가 되려면 몇 분 정도 걸릴 수 있습니다.

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



읽기 전용 복제본으로 수평적 규모조정: Amazon RDS

The diagram illustrates the architecture of Amazon RDS Read Replicas. It shows a central orange square at the top connected to five blue cylinders below it, labeled 'R' (Read) four times and 'M' (Master) once. A red arrow labeled '읽기' (Read) points from the left towards the top, while a green arrow labeled '쓰기' (Write) points from the bottom towards the right. This visualizes how reads are handled by multiple replicas while writes are directed to the master database.

- 읽기 중심의 워크로드 처리를 위해 수평적으로 확장
- 보고서 오프로드
- 주의 사항:
 - 복제는 비동기식
 - 현재 Amazon Aurora, MySQL, MariaDB, PostgreSQL, Oracle에서 사용 가능

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

PostgreSQL 읽기 전용 복제본에는 특정 요구 사항이 있습니다. 자세한 내용은 다음을 참조하십시오.

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html#USER_ReadRepl.PostgreSQL

Oracle은 Dataguard로 읽기 전용 복제본을 지원합니다. 자세한 내용은 다음을 참조하십시오. <https://aws.amazon.com/about-aws/whats-new/2019/03/Amazon-RDS-for-Oracle-Now-Supports-In-region-Read-Replicas-with-Active-Data-Guard-for-Read-Scalability-and-Availability/>

Amazon RDS 규모조정: 버튼을 눌러 조정

aws training and certification

- 노드를 수직적으로 확장 또는 축소
- micro부터 24xlarge에 이르는 모든 크기 지원
- 종종 다운타임 없이 수직적으로 조정

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

Amazon RDS API를 사용하거나 콘솔에서 몇 번의 클릭만으로 컴퓨팅 및 메모리 리소스를 조정해 배포를 확장하거나 축소할 수 있습니다. 조정 작업은 일반적으로 몇 분 내에 완료됩니다. *일반적인 RDS는 조정 시 1~2분의 짧은 다운타임이 필요하지만 Aurora Serverless는 다운타임 없이 조정할 수 있습니다.

스토리지 요구 사항이 증가함에 따라 다운타임 없이 즉시 추가 스토리지를 프로비저닝할 수 있습니다. 또한 RDS의 PIOPS를 사용하면(SQL Server용 Amazon RDS 제외) IOPS 속도를 1,000 IOPS 단위로 1,000 IOPS에서 30,000 IOPS까지 지정하고 스토리지를 100GB에서 3TB까지 지정하여 DB 인스턴스의 처리량을 확장할 수 있습니다.

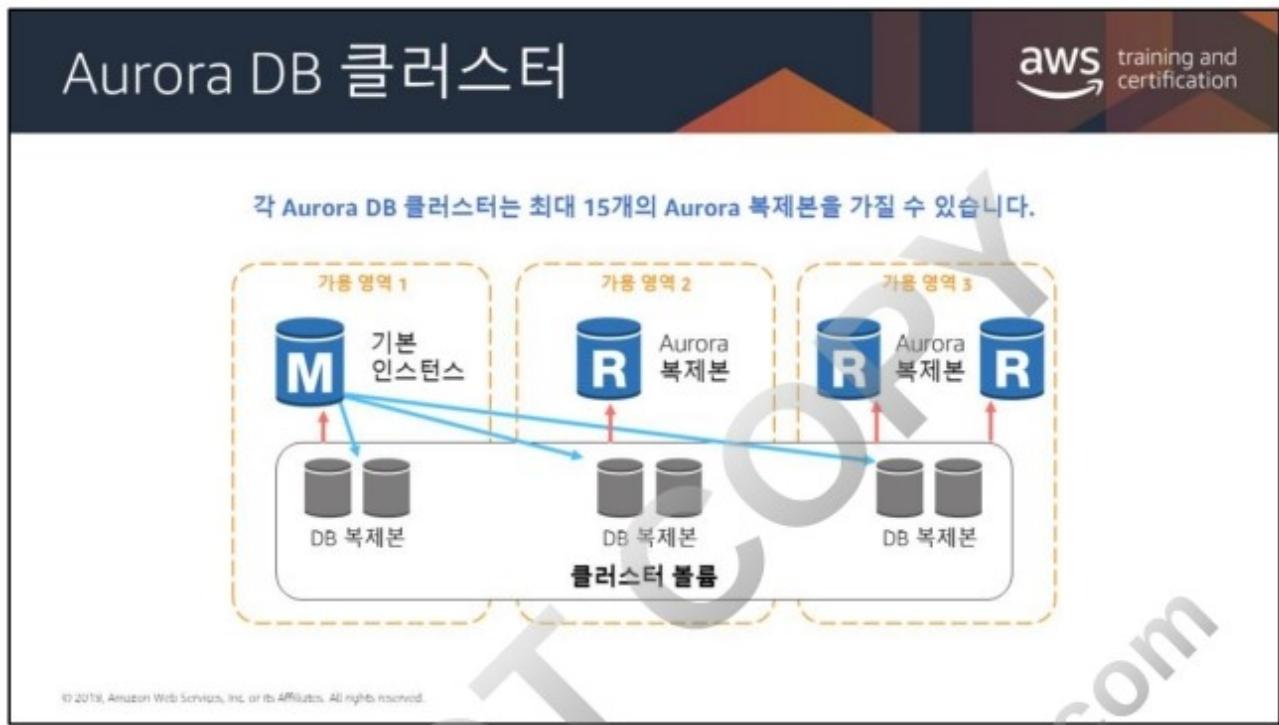
다운타임 없이 스토리지를 늘릴 수 있습니다. 그러나 인스턴스 유형을 변경하려면 다운타임이 필요합니다. 다음을 참조하십시오.

<https://aws.amazon.com/blogs/database/scaling-your-amazon-rds-instance-vertically-and-horizontally>

현재 SQL Server용 Amazon RDS에서는 기존 SQL Server DB 인스턴스의 스토리지 또는 IOPS 확장을 지원하지 않습니다.

대기 데이터베이스가 먼저 업그레이드된 다음 새로 크기가 조정된 데이터베이스로 장애 조치가 이루어지기 때문에 다중 가용 영역 환경에서 확장할 때 가동 중지 시간이 최소화됩니다. 단일 가용 영역 인스턴스의 경우 조정 작업 동안에는 인스턴스를 사용할 수 없습니다. DB 인스턴스 변경으로 인한 가동 중단 시간을 설명하는 표를 보려면

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.DBInstance.Modifying.html#USER_ModifyInstance.Settings을 참조하십시오.



기본 인스턴스 – 읽기 및 쓰기 작업을 지원하고, 클러스터 볼륨의 모든 데이터 변경을 실행합니다. 각 Aurora DB 클러스터마다 기본 인스턴스가 하나씩 있습니다.

Aurora 복제본 – 읽기 작업만 지원합니다. 각 Aurora DB 클러스터마다 기본 인스턴스 이외에 최대 15개의 Aurora 복제본을 가질 수 있습니다. 다수의 Aurora 복제본이 읽기 워크로드를 분산시키면 Aurora 복제본을 별도의 가용 영역으로 이동시켜 데이터베이스 가용성을 높이는 것도 가능합니다.

읽기 전용 복제본은 마스터와 동일한 리전에 있을 수 있습니다.

Aurora Serverless

애플리케이션에 자동으로 응답합니다.

- 용량 조정
- 종료
- 시작

사용한 ACU 수에 따라 비용 지불

갑작스럽거나 예측할 수 없는 단기 워크로드에 적합합니다.

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

Amazon Aurora Serverless는 관계형 데이터베이스인 Amazon Aurora를 위한 온디맨드 Auto Scaling 구성입니다. Aurora Serverless DB Cluster는 데이터베이스 서버 인프라를 관리할 필요 없이 애플리케이션의 필요에 따라 자동으로 시작 및 종료하고 용량을 축소 또는 확장하는 DB 클러스터입니다.

Aurora Serverless는 사용 빈도가 낮거나 간헐적이거나 예측할 수 없는 워크로드를 위한 상대적으로 간단하고 비용 효율적인 옵션을 제공합니다. 자동으로 시작하고, 애플리케이션의 사용량에 맞춰 용량을 조정하고, 사용하지 않는 경우 종료되기 때문에 이러한 옵션을 제공할 수 있습니다. 최대 및 최소 Aurora 용량 단위(ACU)를 정의하고 사용한 ACU 수에 대해서만 지불합니다.

데이터베이스 샤딩으로 Amazon RDS 쓰기 조정

샤딩이 없으면 모든 데이터가 **하나의 파티션**에 상주합니다.

- 예: 하나의 데이터베이스에서 성이 A~Z에 속하는 사용자

샤딩은 데이터를 **큰 청크(샤드)**로 분할합니다.

- 예: 하나의 데이터베이스에서 성이 A~M에 속하는 사용자, 다른 데이터베이스에서 N~Z에 속하는 사용자
- 사용자

대부분의 경우에 샤딩은 **뛰어난 성능과 높은 운영 효율성**을 제공합니다.

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

샤딩은 데이터베이스 서버를 여러 대 사용하여 쓰기 성능을 개선하는 기술입니다. 기본적으로 동일한 구조를 가진 데이터베이스는 쓰기 프로세스를 분산할 수 있도록 적절한 테이블 열을 키로 사용하여 준비되고 분할됩니다. AWS 클라우드에서 제공하는 RDBMS 서비스를 사용하면 이러한 샤딩을 수행하여 가용성과 운영 효율성을 높일 수 있습니다.

샤딩 백엔드 데이터베이스로 Amazon RDS를 사용할 수 있습니다. MySQL Server와 같은 샤딩 소프트웨어를 Spider Storage Engine과 결합하여 Amazon EC2 인스턴스에 설치합니다. 여러 RDS를 준비하고 이를 샤딩 백엔드 데이터베이스로 사용합니다. RDS를 여러 리전에 배포할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

http://en.clouddesigntpattern.org/index.php/CDP:Sharding_Write_Pattern.

DynamoDB - 두 가지 조정

aws training and certification

Auto Scaling

모든 새 테이블의 기본값



상한 및 하한 지정

사용 사례: 일반 조정, 대부분의 애플리케이션에 적합한 솔루션.

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

콘솔을 사용하여 새 DynamoDB 테이블을 생성하는 경우, 테이블에 Auto Scaling이 기본적으로 활성화됩니다. DynamoDB Auto Scaling은 동적으로 변동하는 요청 볼륨에 대응하여 가동 중단 없이 읽기 및 쓰기 처리량 용량을 자동으로 조정합니다. DynamoDB Auto Scaling을 사용하면 사용자가 원하는 처리량 사용률 목표, 최소 및 최대 한도만 설정하면 Auto Scaling이 나머지를 자동으로 처리합니다.

DynamoDB Auto Scaling은 Amazon CloudWatch와 연동하여 지속적으로 실제 처리량 사용을 모니터링하다가 실제 사용률이 목표에서 벗어날 경우 자동으로 용량을 확장 또는 축소합니다. Auto Scaling은 신규 테이블, 기존 테이블 및 글로벌 보조 인덱스에 대해 활성화할 수 있습니다. 콘솔에서 몇 번의 클릭으로 Auto Scaling을 활성화할 수 있으며, 콘솔을 통해 모든 조정 활동을 확인할 수 있습니다. 또한 AWS 명령줄 인터페이스 및 AWS 소프트웨어 개발 키트를 사용해 프로그래밍 방식으로 DynamoDB Auto Scaling을 관리할 수도 있습니다.

DynamoDB Auto Scaling을 사용하는 데는 DynamoDB 및 CloudWatch 경보에 대해 이미 지불하고 있는 비용 외에 추가 비용이 들지 않습니다. DynamoDB Auto Scaling은 모든 AWS 리전에서 사용할 수 있으며, 즉시 적용됩니다.

DynamoDB - 두 가지 조정

aws training and certification

Auto Scaling

모든 새 테이블의 기본값



상한 및 하한 지정

사용 사례: 일반 조정, 대부분의 애플리케이션에 적합한 솔루션.

온디맨드

요청당 지불



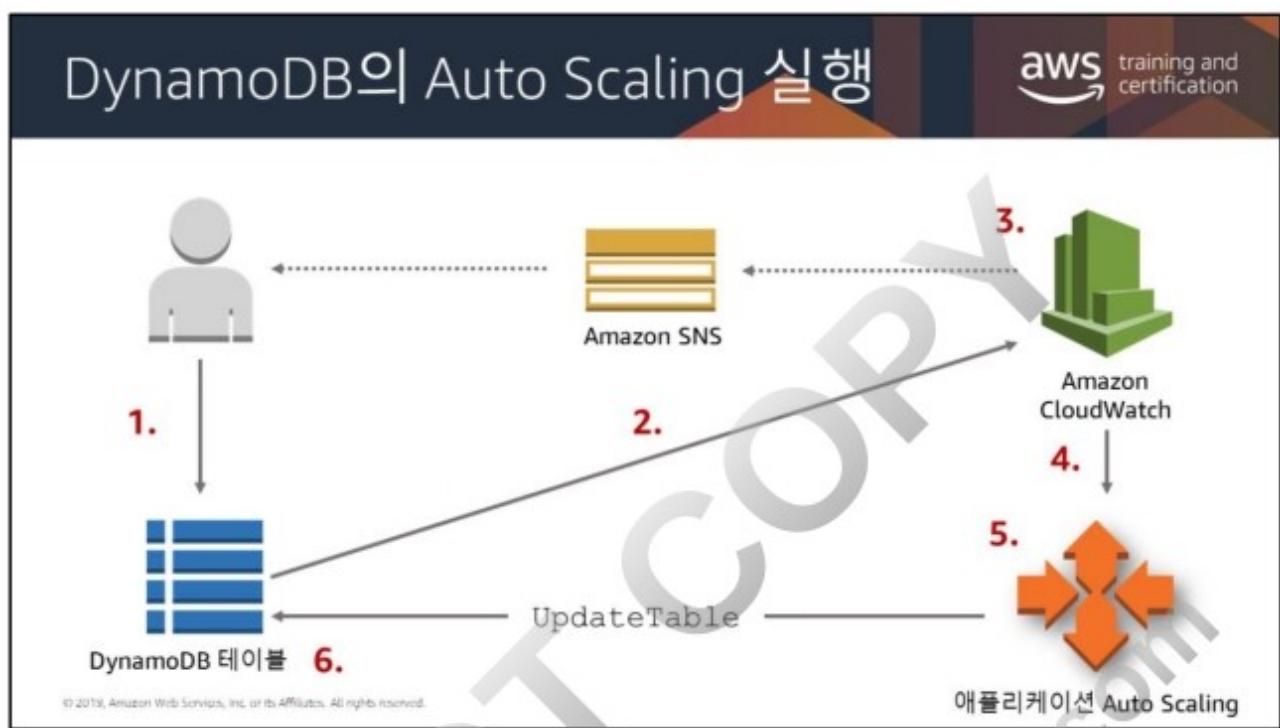
프로비저닝 없음

사용 사례: 갑작스럽고 예측할 수 없는 워크로드, 빠르게 용량이 필요한 경우.

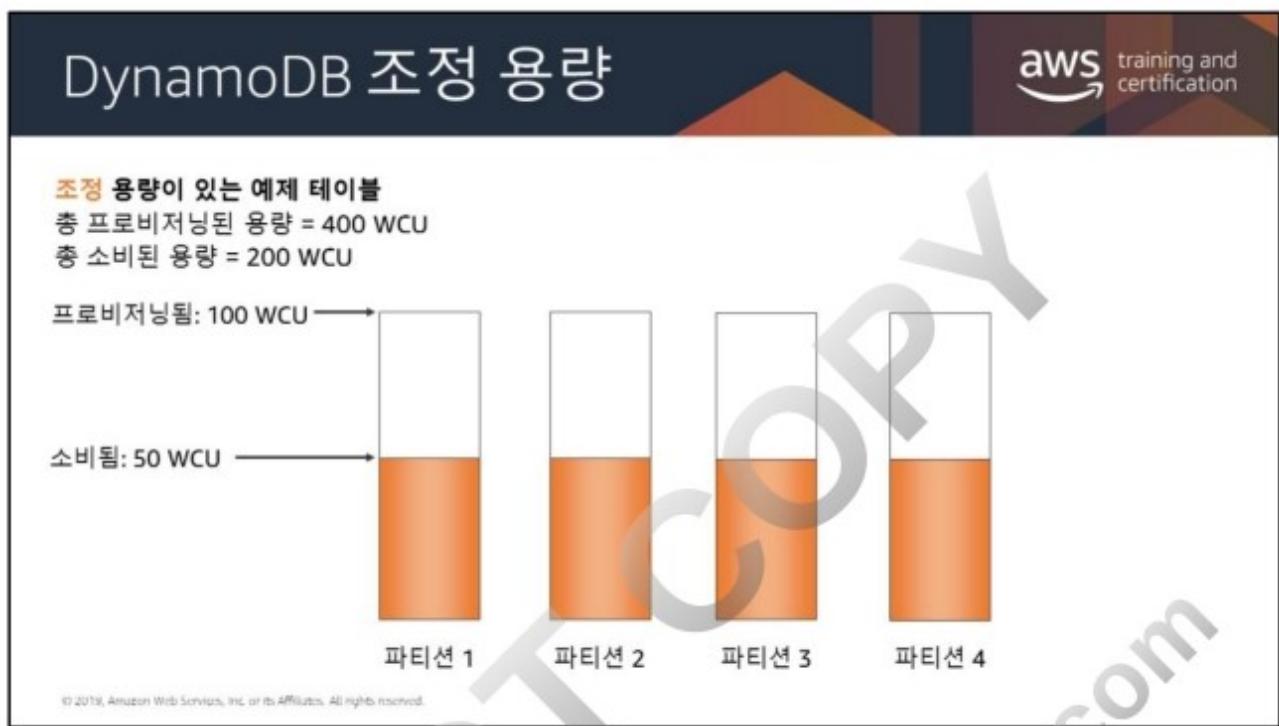
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon DynamoDB On-Demand는 용량 계획 없이 초당 수천 건의 요청을 처리할 수 있는 DynamoDB의 유연한 결제 옵션입니다. 프로비저닝 요금 모델 대신 요청당 요금으로 전환합니다. DynamoDB On-Demand는 모든 트래픽 수준의 증가 또는 조정을 관찰할 수 있습니다. 트래픽 수준이 새로운 피크에 도달하는 경우, DynamoDB는 워크로드에 맞춰 신속하게 조정됩니다. 워크로드 예측이 어렵거나 짧은 시간 동안 대규모 스파이크가 있는 경우에 적합합니다. 하루에 한 번 프로비저닝 용량에서 온디맨드로 테이블을 변경할 수 있습니다. 온디맨드 용량에서 프로비저닝 용량으로는 자유롭게 변경할 수 있습니다.

<https://aws.amazon.com/blogs/aws/amazon-dynamodb-on-demand-no-capacity-planning-and-pay-per-request-pricing/>



1. DynamoDB 테이블의 애플리케이션 Auto Scaling 정책을 생성합니다.
2. DynamoDB가 사용 용량 지표를 Amazon CloudWatch에 게시합니다.
3. 테이블에서 사용한 용량이 특정 기간 동안의 목표 사용률을 초과하는 경우(또는 목표에 미달하는 경우), Amazon CloudWatch가 경보를 트리거합니다. 콘솔에서 경보를 보고 Amazon SNS를 사용하여 알림을 수신할 수 있습니다.
4. CloudWatch 경보가 애플리케이션 Auto Scaling을 호출하여 조정 정책을 평가합니다.
5. 애플리케이션 Auto Scaling이 UpdateTable 요청을 생성하여 테이블의 프로비저닝된 처리량을 조정합니다.
6. DynamoDB는 UpdateTable 요청을 처리하고 해당 테이블의 할당된 처리 용량을 동적으로 늘리거나 줄임으로써 목표 사용률에 근접하게 합니다.



항상 읽기와 및 쓰기 작업을 골고루 배포할 수 있는 것은 아닙니다. 데이터 액세스가 불균형할 때, “핫” 파티션은 다른 파티션보다 볼륨이 많은 읽기 및 쓰기 트래픽을 받을 수 있습니다. 극단적인 상황에서는 단일 파티션이 3,000 RCU나 1,000 WCU 이상을 수신하는 경우 조절이 발생할 수도 있습니다.

고르지 못한 액세스 패턴을 더 효과적으로 수용하기 위해 DynamoDB 조정 용량을 사용하면, 애플리케이션은 트래픽이 테이블의 프로비저닝된 용량이나 파티션 최대 용량을 초과하지 않을 경우 조절 없이 핫 파티션에 계속 읽기 및 쓰기 작업을 수행할 수 있습니다. 조정 용량은 더 많은 트래픽을 받는 파티션의 처리량 용량을 자동으로 증가시킵니다.

모든 DynamoDB 테이블에서 자동으로 조정 용량이 활성화되어 있기 때문에, 이를 명시적으로 활성화하거나 비활성화할 필요가 없습니다.

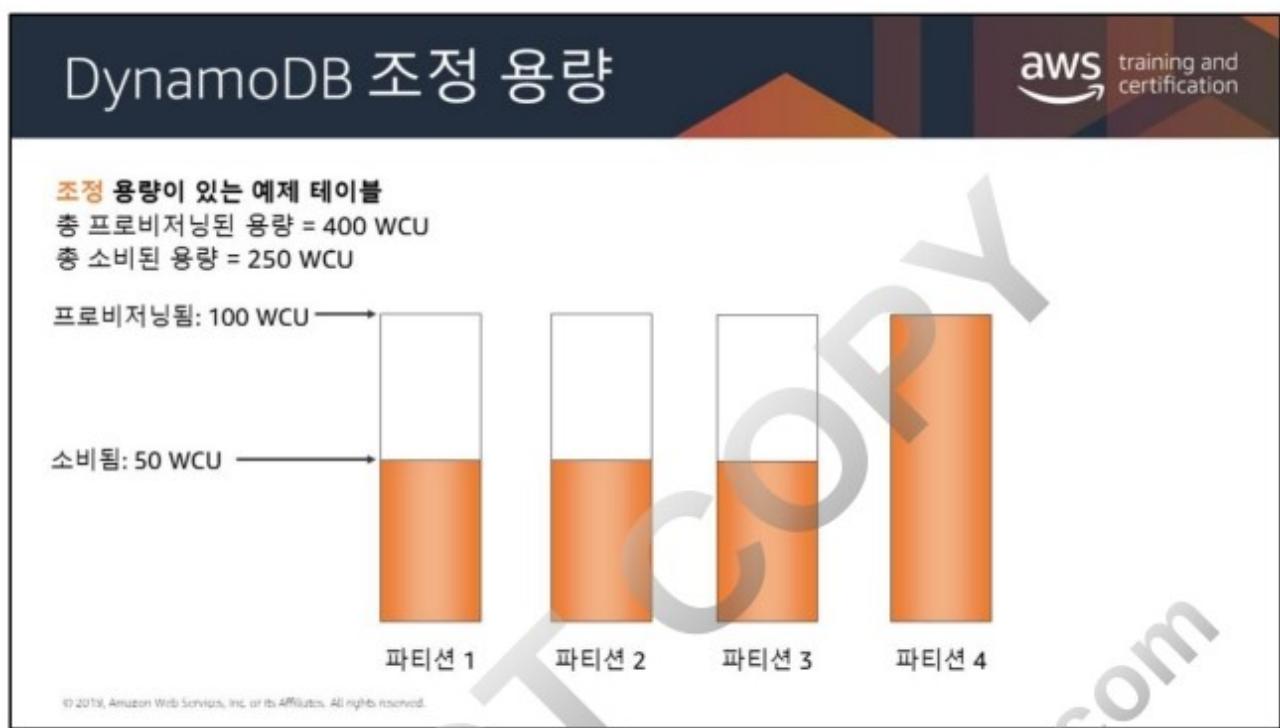
다음 다이어그램에는 조정 용량 작동 방식이 나와 있습니다. 예제 테이블은 4개의 파티션에 균일하게 공유된 400 WCU(쓰기 용량 단위)로 프로비저닝되어 있어 각 파티션은 초당 최대 100 WCU를 유지할 수 있습니다. 파티션 1, 2, 3은 각각 50 WCU/초의 쓰기 트래픽을 수신하는 반면, 파티션 4는 150 WCU/초를 수신합니다. 이 핫 파티션은 미사용 버스트 용량이 있는 동안 쓰기 트래픽을 수락할 수 있지만, 결국 100 WCU/초를 초과하는 트래픽을 제한합니다.

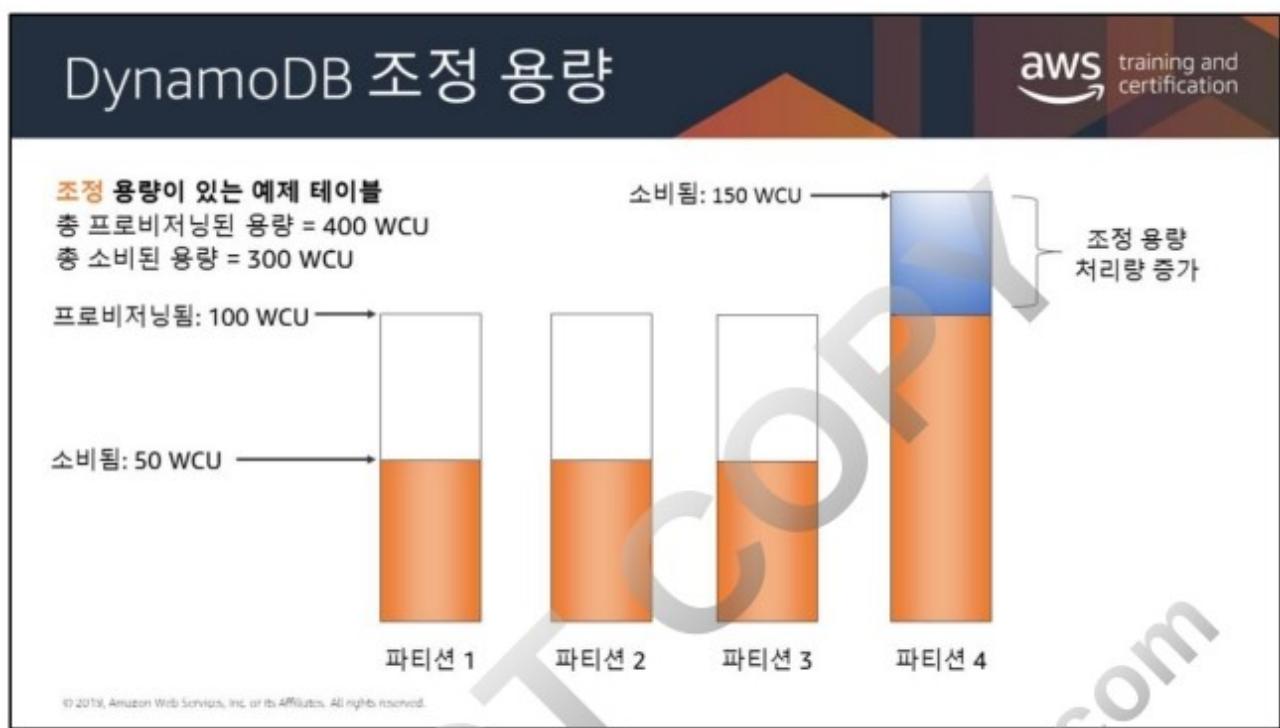
DynamoDB 조정 용량은 파티션 4의 용량을 늘리는 것으로 대응하므로 해당 파티션이 제한되지 않고 150 WCU/초의 높은 워크로드를 유지할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-partition-key-design.html>.

DO NOT COPY
zlagusdbs@gmail.com





파티션 키 값	균등성
사용자 ID(애플리케이션에 사용자가 많은 경우)	좋음
상태 코드(상태 코드가 단 몇 개만 가능한 경우)	나쁨
항목 생성 날짜, 가장 가까운 시간으로 반올림(예: 일, 시 또는 분)	나쁨
디바이스 ID(각 디바이스가 비교적 유사한 간격으로 데이터를 액세스하는 경우)	좋음
디바이스 ID(많은 디바이스가 추적되고 있긴 하지만, 하나만 사용량이 매우 많은 경우)	나쁨

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

테이블 기본 키의 파티션 키 부분은 테이블의 데이터가 저장되는 논리적 파티션을 결정합니다. 이는 기본 물리적 파티션에 영향을 줍니다. 테이블의 프로비저닝된 I/O 용량은 이 물리적 파티션으로 고르게 분배됩니다. 따라서 I/O 요청을 고르게 분산시키지 않는 파티션 키 설계는 "핫" 파티션을 발생시킬 수 있으며, 이는 조절과 프로비저닝된 I/O 용량을 비효율적으로 사용하게 되는 문제를 초래합니다.

테이블의 프로비저닝된 처리량의 최적 사용량은 개별 항목의 워크로드 패턴과 파티션-키 설계가 결정합니다. 이것이 모든 파티션 키 값에 액세스하여 효율적인 처리량 수준을 달성해야 한다는 의미는 아닙니다. 또한 액세스된 파티션 키 값의 백분율이 높아야 한다는 의미는 더더욱 아닙니다. 그 의미는 워크로드가 액세스하는 고유 파티션 키 값이 많을 수록 요청이 여러 파티션 공간으로 더 많이 분산된다는 것입니다. 일반적으로 총 파티션 키 값 중 액세스한 파티션 키 값의 비율이 증가할수록 처리량을 보다 효율적으로 활용할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/bp-partition-key-uniform-load.html>



실습 4: 고가용성 환경 생성

aws training and certification

"복원력이 뛰어난 인프라를 원합니다."

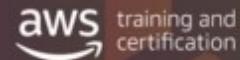
사용된 기술:

- Amazon VPC
- Application Load Balancer
- Amazon EC2 Auto Scaling 그룹
- Amazon RDS

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

DO NOT COPY
zlagusdbs@gmail.com

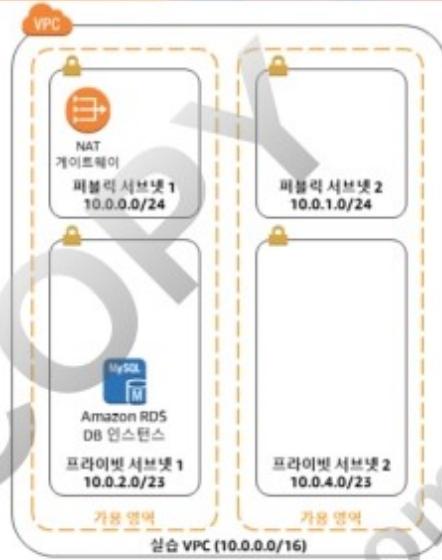
실습 4: 고가용성 환경 생성



실습 시작 시 제공됨:

- 2개의 가용영역에 걸친 VPC
- 2개의 퍼블릭 서브넷
- 2개의 프라이빗 서브넷
- 1개의 NAT 게이트웨이
- Amazon RDS DB 인스턴스

고가용성을 얻을 수 있습니다!



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

실습 4: 고가용성 환경 생성

aws training and certification

요청을 여러 서버에 분산하려면 다음을 사용합니다.

- Amazon EC2 Auto Scaling 그룹
- 로드 밸런서



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

실습 4: 고가용성 환경 생성

aws training and certification

로드 밸런서는 **퍼블릭 서브넷**에 분산됩니다.

애플리케이션 서버는 **프라이빗 서브넷**에 있습니다.



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

실습 4: 고가용성 환경 생성

aws training and certification

3티어 아키텍처를 생성합니다.

보안 그룹은 각 계층 간에 추가 보안을 제공합니다.

```
graph LR; Internet[인터넷] -- "HTTP + HTTPS 트래픽 허용" --> ALB[애플리케이션 로드 밸런서]; ALB -- "HTTP 트래픽 허용" --> AS[앱 서버]; AS -- "MySQL 트래픽 허용" --> RDS[Amazon RDS MySQL DB 인스턴스];
```

인터넷 → HTTP + HTTPS 트래픽 허용 → 애플리케이션 로드 밸런서 보안 그룹 → HTTP 트래픽 허용 → 앱 서버 보안 그룹 → MySQL 트래픽 허용 → 데이터베이스 보안 그룹

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

실습 4: 고가용성 환경 생성

aws training and certification

최종 구성:

- 로드 밸런서
- 여러 애플리케이션 서버
- 다중 가용 영역 데이터베이스
- 각 가용 영역의 NAT 게이트웨이

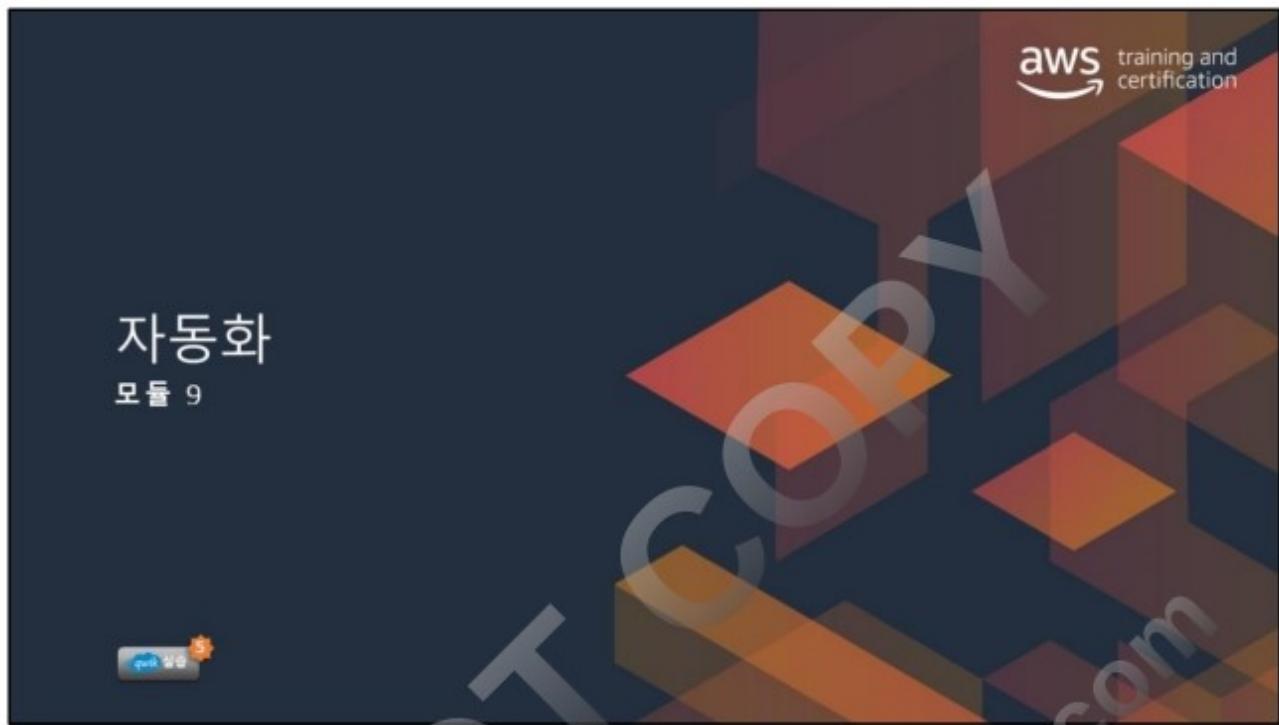
확장성, 안정성, 고가용성!

시간: 40분

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

The diagram illustrates a highly available environment within a VPC. It shows two availability zones (AZ1 and AZ2), each containing a NAT gateway, an application load balancer, and an Auto Scaling group with two EC2 instances. MySQL DB instances are connected to RDS DB instances in each AZ. The VPC has two public subnets (10.0.0.0/24 and 10.0.1.0/24) and two private subnets (10.0.2.0/23 and 10.0.4.0/23). A central VPC (10.0.0.0/16) connects them.





모듈 9



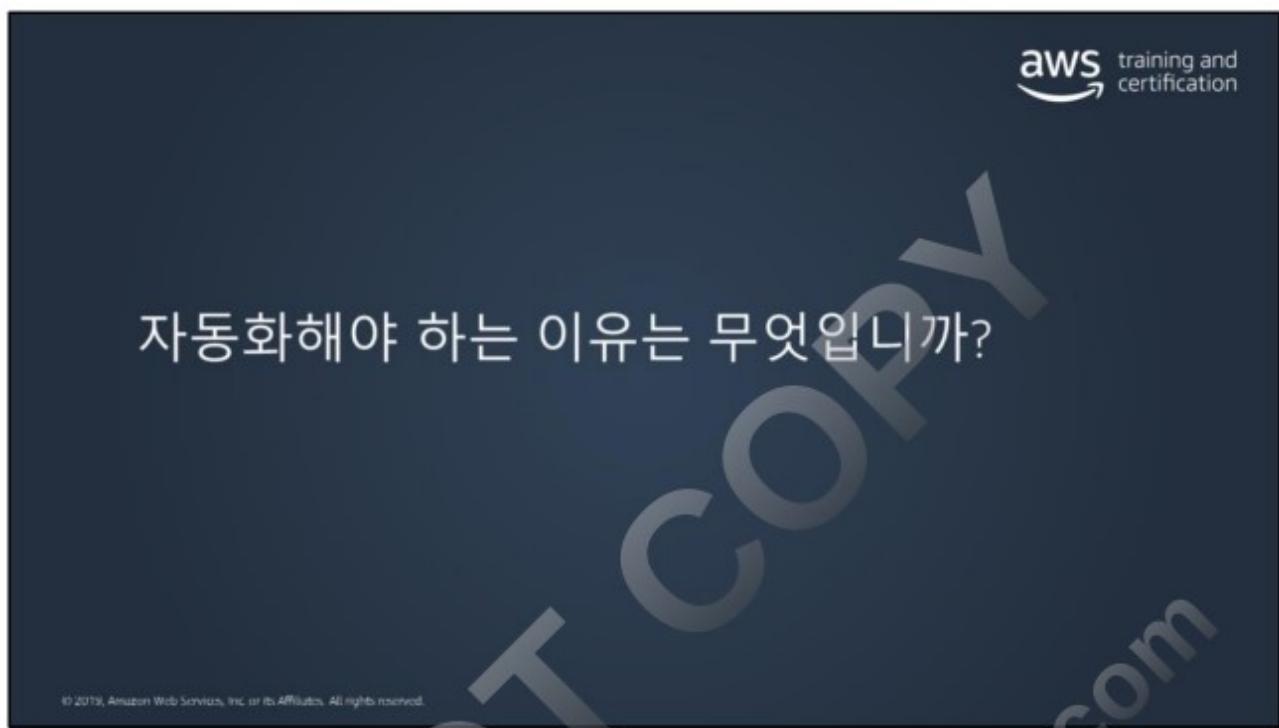
아키텍처 측면에서의 필요성

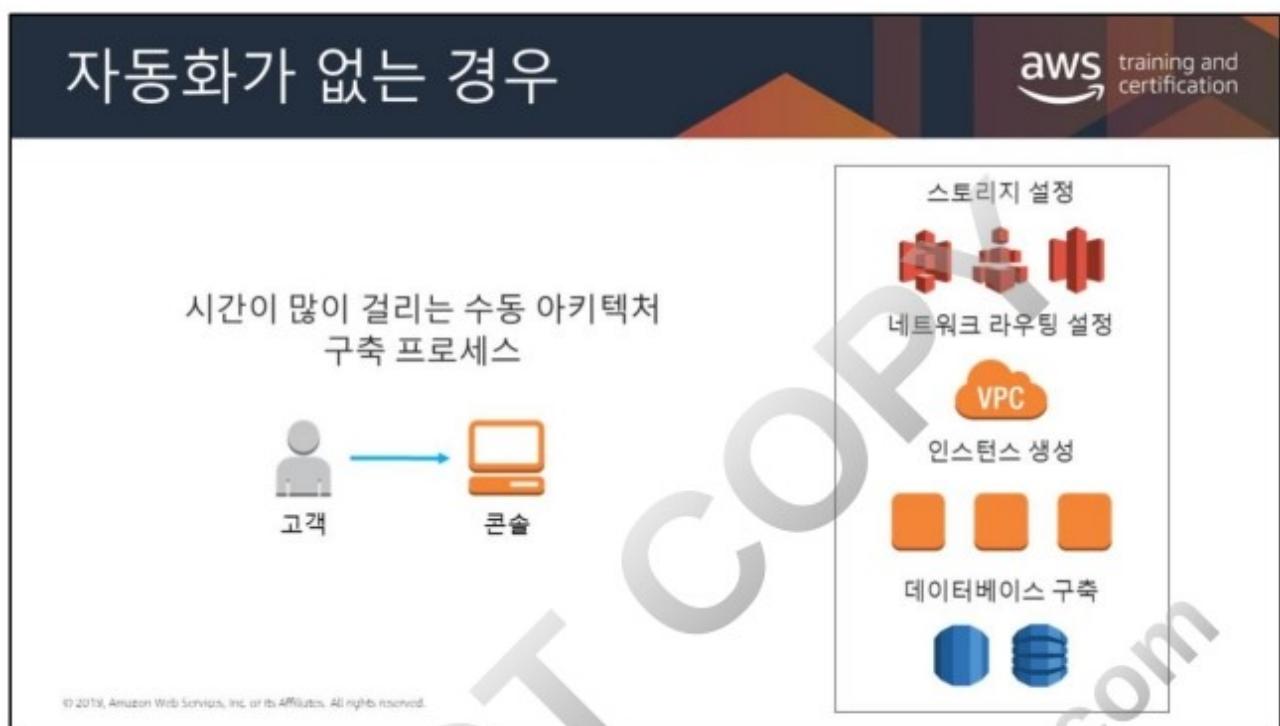
지속적 성장을 위해서는 자동화를 시작해야 합니다. 조직에 있는 다양한 아키텍처를 일관되게 배포, 관리, 업데이트할 방법이 필요합니다.

모듈 개요

- 자동화가 필요한 이유
- 인프라 자동화
- 배포 자동화

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





대규모 컴퓨팅 환경을 구축하려면 상당한 시간과 에너지가 필요합니다. 다음과 같은 몇 가지 사항을 고려해야 합니다.

- 설계 또는 구현, 어디에 노력을 투입할 것인가? 또한 수동 구현의 위험은 무엇인가?
- 어떻게 프로덕션 서버를 업데이트할 것인가? 어떻게 배포를 여러 지리적 리전에 둘아웃할 것인가? 장애가 발생할 경우 어떻게 롤백을 관리할 것인가?
- 배포에 대한 디버깅은 어떻게 할 것인가? 어떻게 오류를 발견하고 수정하며 수정을 확인할 것인가?
- 어떻게 다양한 시스템과 및 하위 시스템에 대한 종속성을 관리할 것인가?
- 마지막으로, 이 모든 작업을 수동으로 할 수 있는가?



수동으로 개별 구성 요소를 생성하여 환경에 추가할 경우 확장이 불가능합니다.
여러분이 대규모 기업 애플리케이션을 담당하고 있는 경우 수동으로 이러한 작업을 처리할 인력은 충분하지 않습니다.

아키텍처 및 애플리케이션을 처음부터 생성하면 내재된 버전 관리가 없습니다. 비상시, 프로덕션 스택을 이전 버전으로 롤백하는 것이 유용하지만, 수동으로 환경을 생성할 경우 이것이 불가능합니다.

감사 추적 기능은 많은 규정 준수 및 보안 상황에서 매우 중요합니다. 사람들이 수동으로 환경을 제어하고 편집하도록 허용하는 것은 위험합니다.

마지막으로, 위험을 최소화하려면 일관성이 매우 중요합니다. 자동화는 일관성을 유지할 수 있게 해줍니다.

일반적으로



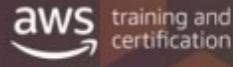
프로덕션 환경에서 뭔가를 **수동으로**
변경해야 하는 경우,
위험이 따릅니다.

수동 프로세스는 보상 없는 **위험**입니다.

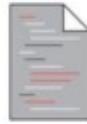
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



인프라 자동화




AWS
CloudFormation

 AWS 인프라를 설명하는 공통 언어를 제공합니다

 설명된 리소스를
자동화된 방식으로 생성하고 구축합니다

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS CloudFormation은 리소스를 안전하고 반복 가능한 방식으로 프로비저닝하므로, 수동 작업을 수행하거나 사용자 지정 스크립트를 작성할 필요 없이 인프라와 애플리케이션을 구축 및 재구축할 수 있습니다.

AWS CloudFormation을 사용하면 인프라를 코드로 취급할 수 있습니다. 원하는 코드 편집기를 사용하여 코드를 작성하고, GitHub 또는 AWS CodeCommit과 같은 버전 관리 시스템에 체크인하고, 적절한 환경에 배포하기 전에 팀원들과 파일을 검토할 수 있습니다.

어떻게 작동합니까?

AWS CloudFormation 템플릿

- 생성할 리소스를 설명하는 **JSON/YAML** 형식 파일
- 소스 코드로 취급**: 리포지토리에 저장

```
graph LR; CodeEditor[코드 편집기] --- JSONBox[JSON]; CodeEditor --- YAMLBox[YAML]
```

JSON

```
{ "Resources" : { "HelloBucket" : { "Type" : "AWS::S3::Bucket" } } }
```

YAML

```
Resources: HelloBucket: Type: AWS::S3::Bucket
```

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

AWS CloudFormation 템플릿에 대한 추가 설명:

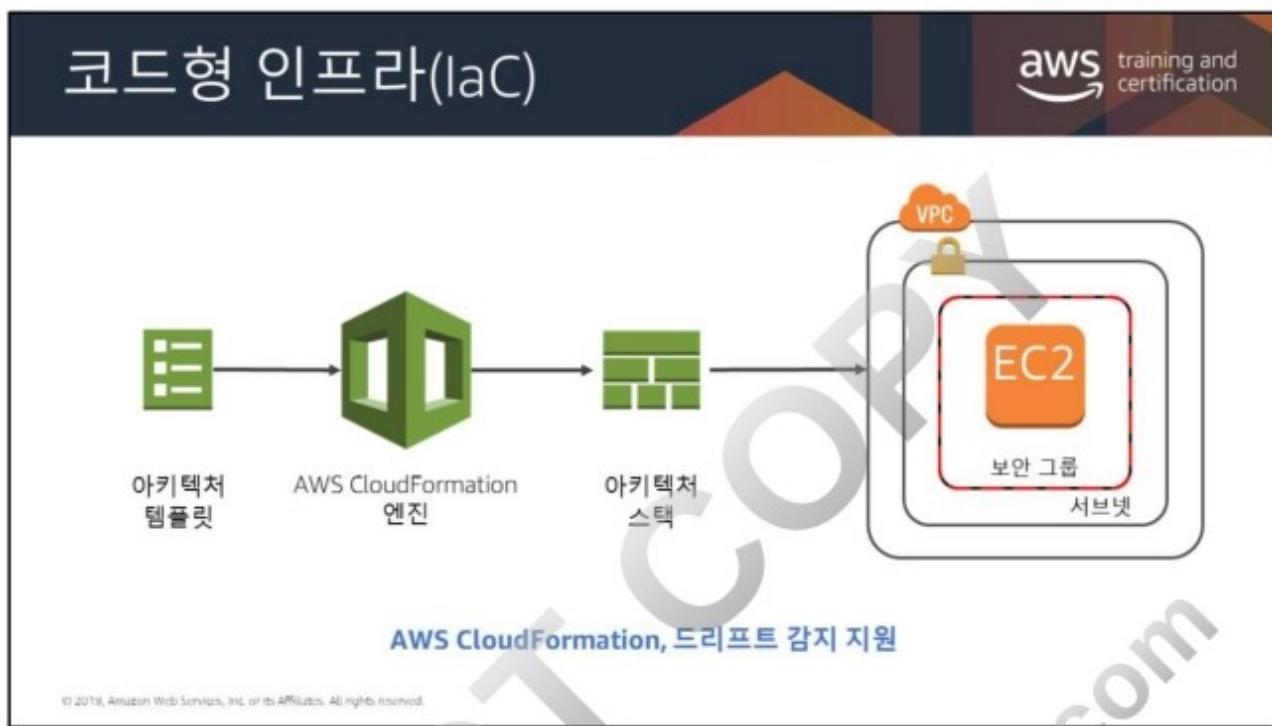
- 템플릿을 코드로 취급하고, 원하는 버전 제어 방법(예: Git, SVN 등)으로 이를 관리합니다.
- JSON 템플릿 파일 내에 전체 애플리케이션 스택(고객 애플리케이션에 필요한 모든 리소스)을 정의합니다.
- 템플릿에 대한 런타임 파라미터를 정의합니다(Amazon EC2 인스턴스 크기, Amazon EC2 키 페어 등).

이제 YAML 형식 템플릿을 생성하여 AWS CloudFormation에서 AWS 리소스 및 속성을 설명할 수 있습니다. 이제, YAML 형식 템플릿 또는 JSON 형식 템플릿을 사용해 AWS 인프라를 모델링하고 설명할 수 있는 옵션이 있습니다. YAML 형식의 AWS CloudFormation 템플릿은 기존의 JSON 형식 템플릿과 동일한 구조를 따르고 동일한 기능을 모두 지원합니다.

또한 한 스택의 출력을 다른 스택과 공유할 수 있는 교차 스택 참조를 만들 수도 있습니다. 이렇게 하면 IAM 역할, VPC 정보, 보안 그룹 등을 공유할 수 있습니다. 이전에는 이렇게 하려면 AWS CloudFormation 사용자 지정 리소스를 사용해야 했습니다. 이제 새로운 ImportValue 내장 함수를 사용해 간단히 한 스택에서 값을 내보내고 다른 스택에서 값을 가져올 수 있습니다.

교차 스택 참조는 AWS 인프라를 스택(예: 네트워크 스택, 애플리케이션 스택 등) 기준으로 그룹화된 논리적 구성 요소로 분리하는 고객, 그리고 중첩 스택의 대안으로 스택을 느슨하게 결합해야 하는 고객에게 유용합니다.

DO NOT COPY
zlagusdbs@gmail.com



AWS CloudFormation을 사용하면 Amazon Web Services (AWS) 리소스 세트를 템플릿을 제출하는 것만큼 간단하게 배포할 수 있습니다.

템플릿은 특정 환경에 배포될 리소스를 설명 및 정의하는 텍스트 파일입니다.

AWS CloudFormation은 템플릿을 처리하는 엔진입니다. AWS CloudFormation의 출력은 스택이라고 합니다.

스택은 그룹으로 함께 배포되는 AWS 리소스의 모음입니다.

AWS CloudFormation 템플릿에 대한 추가 설명:

- 이를 코드로 취급하고 버전 관리 시스템을 사용하여 관리할 수 있습니다.
- JSON 또는 YAML 템플릿 파일 내에 전체 애플리케이션 스택(고객 애플리케이션에 필요한 모든 리소스)을 정의합니다.
- 템플릿의 런타임 파라미터를 정의합니다(Amazon EC2 인스턴스 크기, Amazon EC2 키 페어 등).

AWS CloudFormation이 지원하는 리소스 목록은

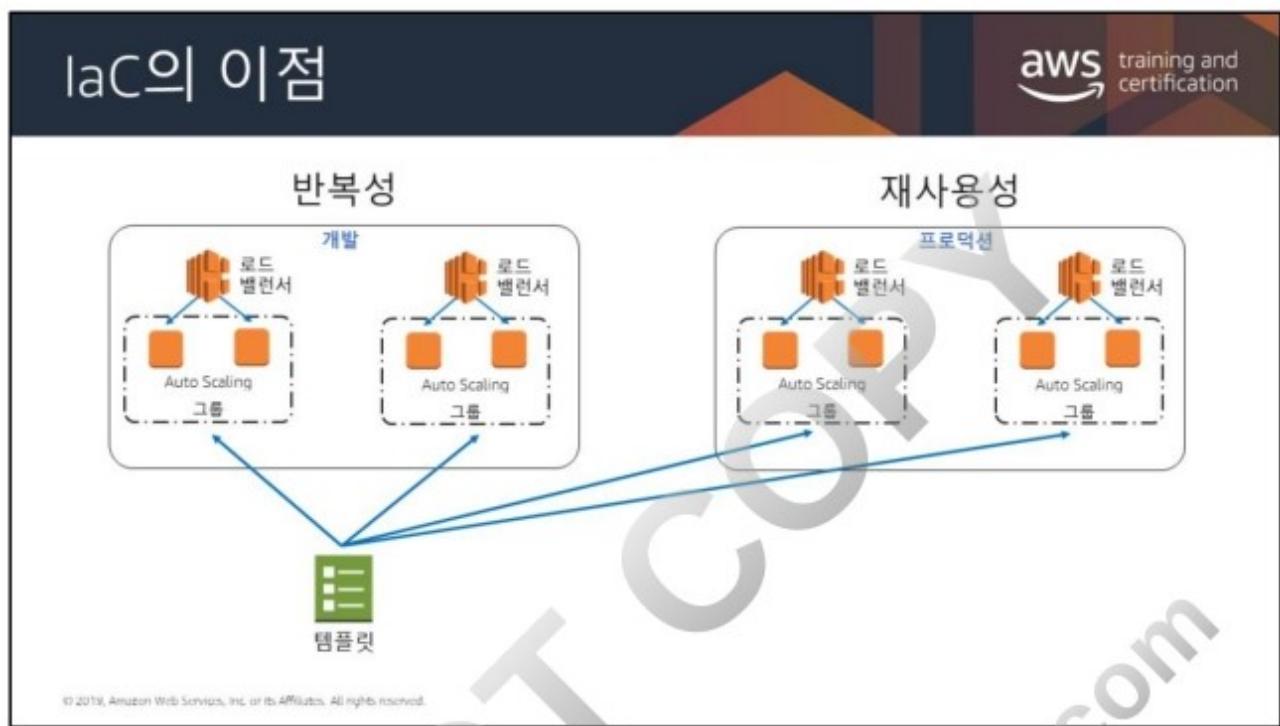
<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-template-resource-type-ref.html>을 참조하십시오.

샘플 템플릿은

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-sample-templates.html>을 참조하십시오.

스택에서 드리프트 감지 작업을 수행하면 스택이 소기의(기존) 템플릿 구성에서 드리프트되었는지 확인하고, 드리프트 감지를 지원하는 스택에 있는 각 리소스의 드리프트 상태 관련 세부 정보를 반환합니다. "현재 스택의 드리프트 감지" 대화 상자를 클릭하면 스택에서 드리프트 감지를 활성화할 수 있습니다. 대화 상자를 닫고 드리프트 세부 정보를 나중에 검토하는 경우에도 드리프트 감지 프로세스가 계속됩니다. 자세한 내용은 다음 사이트를 참조하십시오.

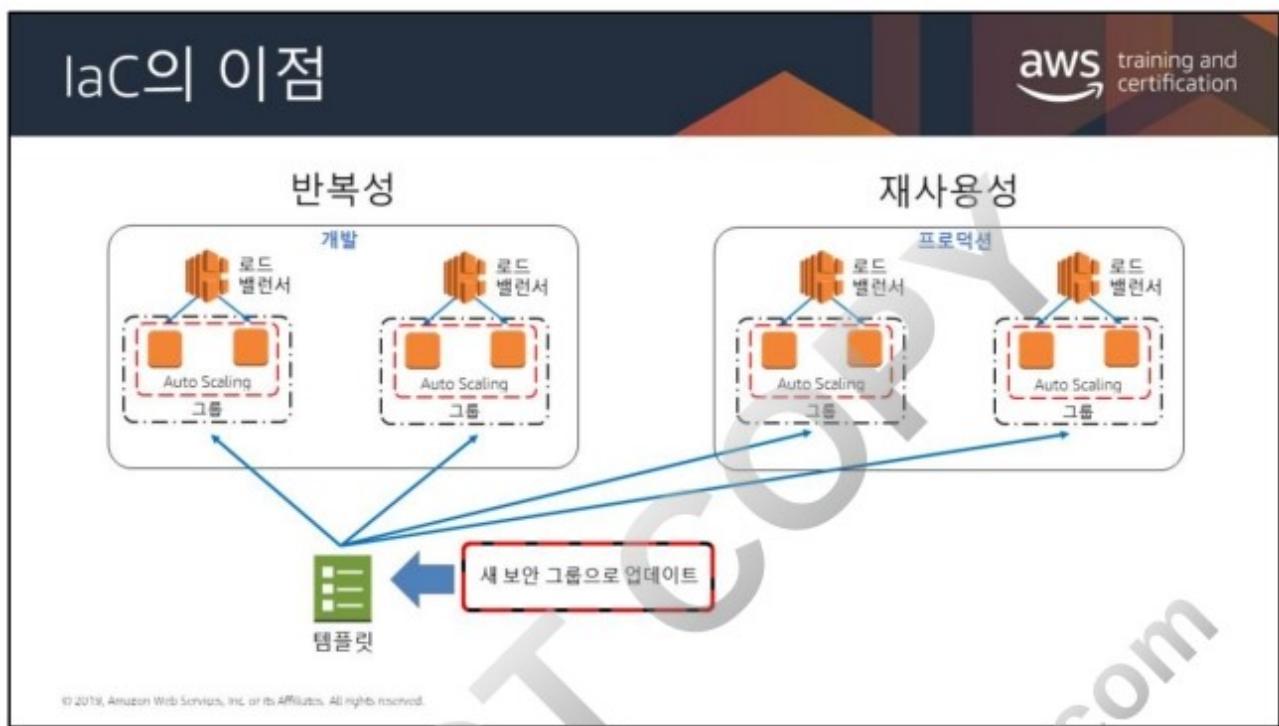
- <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/detect-drift-stack.html>
- <https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html>



인프라를 코드형으로 구축하는 경우, 환경을 구축하면서 반복성과 재사용성의 이점을 활용할 수 있습니다.

템플릿 하나(또는 템플릿의 조합)로 복잡한 동일 환경을 반복해서 구축할 수 있습니다.

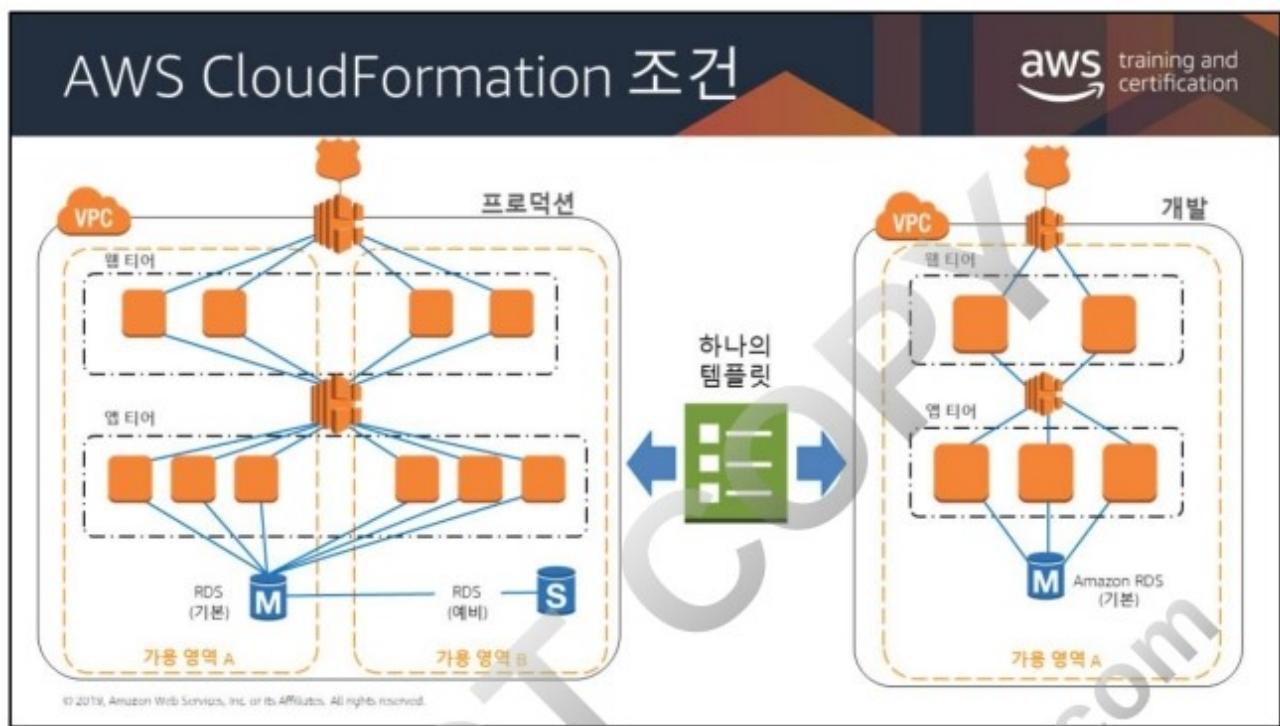
AWS에서 이를 사용하는 경우, 조건에 따라 다른 환경을 생성할 수도 있습니다. 즉 생성했던 환경의 컨텍스트에 맞게 환경이 구축되도록 할 수 있습니다. 예를 들어 템플릿이 개발 환경 또는 프로덕션 환경에서 시작되었는지에 따라 서로 다른 AMI가 사용되도록 템플릿을 설계할 수 있습니다.



이 시나리오에서는 인스턴스 스택에 새로운 보안 그룹을 추가하도록 템플릿이 업데이트되었습니다.

이러한 환경을 시작하는 데 사용된 템플릿을 하나만 변경하면, 모든 네 개의 환경에 새로운 보안 그룹 리소스가 추가됩니다.

이 기능은 리소스의 간편한 유지 관리성뿐만 아니라 뛰어난 일관성과 병렬화를 통한 필요한 작업 감소라는 이점을 제공합니다.



프로덕션 환경과 개발 환경을 동일한 스택에서 구축해야 합니다. 이렇게 해야 애플리케이션이 프로덕션에서도 설계 및 개발된 방식대로 작동합니다.

또한 개발 환경과 테스트 환경에서 동일한 스택을 사용해야 합니다. 모든 환경이 동일한 애플리케이션 및 구성을 갖게 됩니다.

기능 테스트, 사용자 승인 테스트 및 로드 테스트를 위해 여러 테스트 환경이 필요할 수 있습니다. 이러한 환경을 수동으로 생성하면 큰 위험이 수반됩니다.

AWS CloudFormation 템플릿에서 조건 문을 사용해 개발, 테스트 및 프로덕션이 크기 및 범위는 다르지만 나머지는 동일하게 구성되도록 할 수 있습니다.



스택을 업데이트하는 한 가지 방법은 기존 템플릿을 편집한 후 다시 실행하는 것입니다.

그러나 사용자가 AWS CloudFormation이 스택을 업데이트할 때 수행할 변경에 대한 추가 통찰이 필요할 경우 변경 세트를 사용할 수 있습니다.

변경 세트를 사용하면 업데이트가 진행되기 전에 변경 사항을 미리 보고 변경 사항이 예상과 일치하는지 확인한 후 업데이트를 승인할 수 있습니다.

다음은 변경 세트를 사용하는 기본 워크플로우입니다.

1. 업데이트하려는 스택의 변경 사항을 제출하여 변경 세트를 생성합니다.
2. 변경 집합을 보고 어떤 스택 설정과 리소스가 변경될지 확인합니다.
3. 어떻게 변경할지 결정하기 전에 다른 변경 사항을 고려하려면 추가 변경 집합을 만듭니다.
4. 변경 집합을 실행합니다. AWS CloudFormation이 이러한 변경 사항을 사용하여 스택을 업데이트합니다.

자세한 내용은

<http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-updating-stacks-changesets.html>를 참조하십시오.

DO NOT COPY
zlagusdbs@gmail.com

설계 예

계층화된 아키텍처

프런트 엔드	CRM 웹 인터페이스, 관리자 인터페이스, 분석 대시보드
백엔드	고객, 캠페인, 제품, 마케팅 자료, 분석
공유	CRM DB, 일반 모니터링/경보, 서브넷, 보안 그룹
기본 네트워크	VPC, 인터넷 게이트웨이, VPN, NAT
자격 증명	IAM 사용자, 그룹, 역할

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

AWS Quick Start

aws training and certification

표준화된 템플릿

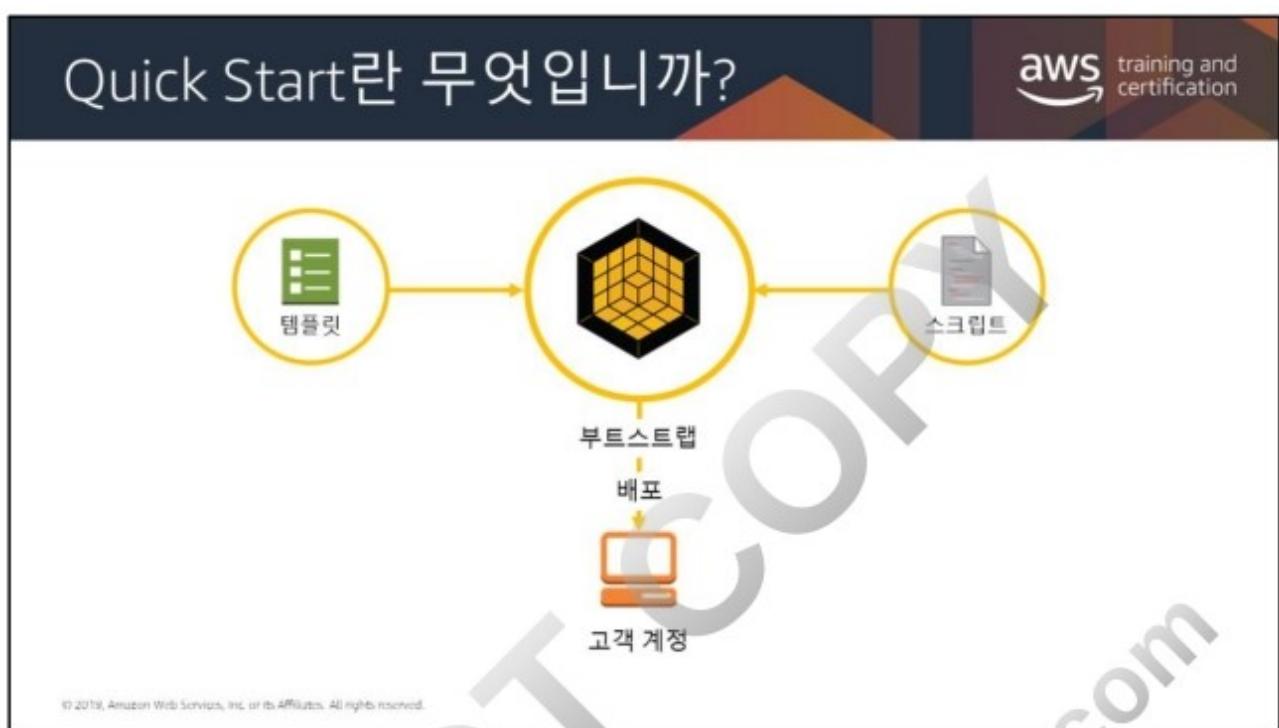


- AWS 클라우드에서의 모범 표준 배포
- AWS 보안 및 고가용성 모범 사례에 기초
- 클릭 한 번으로 1시간 내에 전체 아키텍처 생성
- 실험 및 간편한 구축에 적합

AWS 솔루션스 아키텍트가 구축한
AWS CloudFormation 템플릿

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

Quick Start는 고객이 AWS에서 인기 있는 솔루션을 배포하는 데 활용할 수 있도록 AWS 솔루션스 아키텍트 및 파트너가 보안 및 고가용성 관련 AWS 모범 사례를 기반으로 구축합니다. 이러한 참조 배포는 AWS 클라우드에서 자동으로 주요 기술을 구현하는데, 흔히 한 번의 클릭으로 한 시간이 채 걸리지 않습니다. 몇 단계를 통해 테스트 또는 프로덕션 환경을 구축하여 즉시 사용을 시작할 수 있습니다.

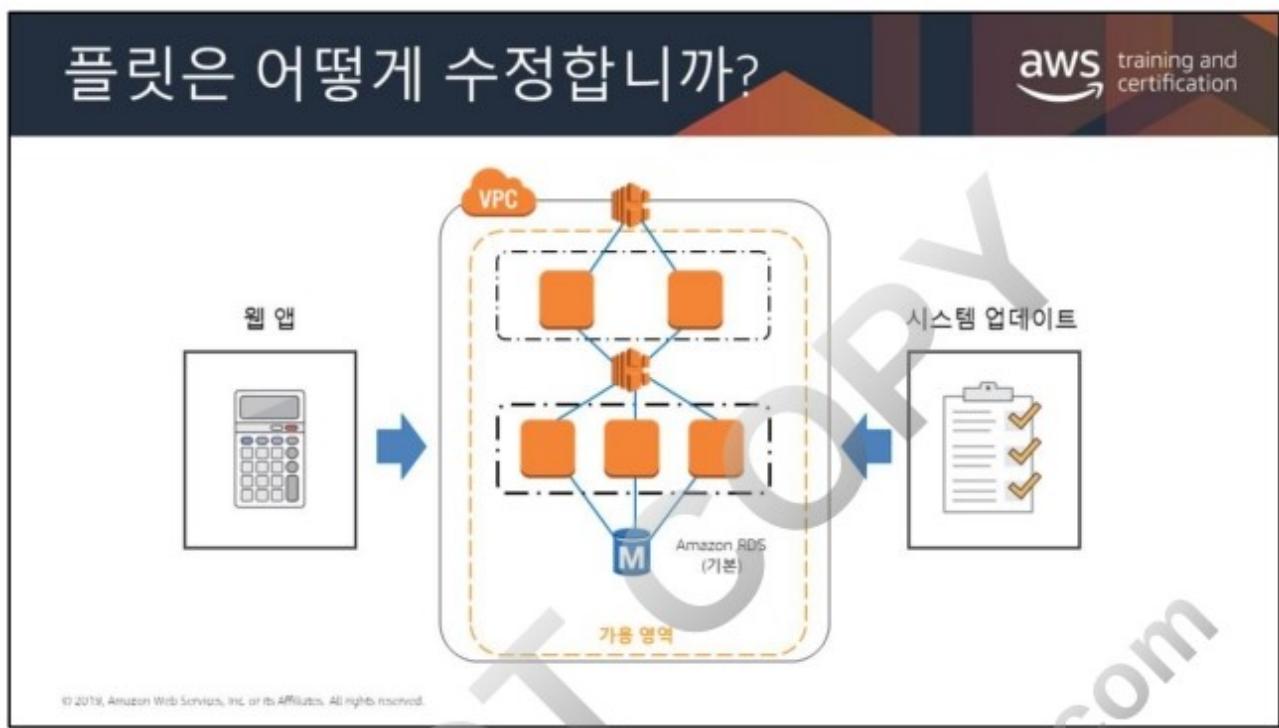


이 Quick Start는 AWS 계정에서 환경을 생성하기 위한 AWS CloudFormation 템플릿 및 관련 스크립트로 구성됩니다. 모든 부트스트래핑 및 배포를 사용자 대신 처리합니다. 또한 모든 구성 요소가 어떻게 생성되었는지 보여주는 배포 안내서가 제공됩니다.

이 환경을 생성 및 실행하는 데 사용된 리소스의 요금이 부과됩니다.

자세한 내용은 다음을 참조하십시오. <https://aws.amazon.com/quickstart/>





AWS CloudFormation을 사용하여 전체 인프라를 자동으로 생성할 수 있습니다.
하지만 여전히 몇 가지 중요한 고려 사항이 있습니다.

어떻게 Amazon EC2 인스턴스를 업데이트할 것인가? 각 상자에 로그인하여 직접 명령을 업데이트 해야 하는가? 최신 버전의 웹 앱을 다운로드하는가? 오류가 발생할 경우 어떻게 변경 사항을 되돌리는가? 3가지 앱을 실행하는 서버가 100개라면 어떻게 할 것인가?

이러한 시나리오에 도움이 될 수 있는 기존의 도구들이 있지만, 즉시 사용 가능한 솔루션이 더 편리할 것입니다.

Systems Manager

aws training and certification



자동화된 구성 및 대규모 시스템의 지속적 관리가 가능한 기능의 집합

- 모든 Windows 및 Linux 워크로드
- Amazon EC2 또는 온프레미스에서 실행

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

AWS Systems Manager는 소프트웨어 인벤토리 수집, OS 패치 적용, 시스템 이미지 생성, Windows 및 Linux 운영 체제 구성 등 자동으로 수행할 수 있는 관리형 서비스입니다. 이러한 기능을 활용해 시스템 구성은 정의 및 추적하고, 드리프트를 방지하고, Amazon EC2 및 온프레미스 구성의 소프트웨어 규정 준수를 유지할 수 있습니다. AWS Systems Manager는 클라우드의 규모 및 민첩성을 고려하여 설계되었지만 온프레미스 데이터 센터로 확장되는 관리 접근 방식을 제공하므로, 기존 인프라를 AWS와 더 쉽고 완벽하게 연결할 수 있습니다.

AWS Systems Manager는 Amazon EC2 콘솔에서 열 수 있습니다. 관리할 인스턴스를 선택한 후 수행할 관리 작업을 정의합니다. AWS Systems Manager는 무료로 제공되며, Amazon EC2 리소스와 온프레미스 리소스를 모두 관리할 수 있습니다.

무엇을 할 수 있습니까?

The diagram illustrates four key features of AWS Systems Manager:

- 명령 실행 (Command): Represented by a green icon of a terminal window.
- 유지 관리 기간 (Patch Manager): Represented by a green icon of a gear with a 'L' on it.
- 패치 관리 (Session Manager): Represented by a green icon of a tree.
- 상태 관리자 (Inventory): Represented by a green icon of a building.
- 세션 관리자 (Session Manager): Represented by a green icon of a person at a computer.
- 인벤토리 (Inventory): Represented by a green icon of a warehouse.

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

Systems Manager Run Command를 사용하여 대규모 관리형 인스턴스의 구성을 원격으로 안전하게 관리합니다. Run Command를 사용하여 수십 또는 수백 개의 대상 인스턴스 집합에서 애플리케이션 업데이트 또는 Linux 셸 스크립트 및 Windows PowerShell 명령 실행과 같은 온디맨드 변경을 수행합니다.

자세한 내용은 다음을 참조하십시오. <https://docs.aws.amazon.com/systems-manager/latest/userguide/execute-remote-commands.html>

Patch Manager를 사용하여 관리형 인스턴스의 패치 적용 프로세스를 자동화합니다. 이 기능을 사용하면 인스턴스를 스캔하여 패치 누락 여부를 확인하고 누락된 패치를 개별적으로 적용하거나 Amazon EC2 태그를 사용하여 대규모 인스턴스 그룹에 적용할 수 있습니다. 보안 패치의 경우, Patch Manager가 승인 및 거부된 패치 목록뿐 아니라 릴리스 후 며칠 이내에 패치를 자동 승인하는 규칙을 포함하는 패치 기준선을 사용합니다. 보안 패치는 해당 인스턴스에 대해 구성된 패치 기본 리포지토리로부터 설치됩니다. Systems Manager 유지 관리 기간 작업으로 실행되도록 패치 적용을 예약하여 보안 패치를 정기적으로 설치할 수 있습니다. Linux 운영 체제의 경우 사용자가 패치 기준선의 일부로 패치 적용 작업에 사용할 리포지토리를 정의할 수 있습니다.

따라서 인스턴스에서 어떤 리포지토리가 구성되어 있는지 상관없이 업데이트가 신뢰할 수 있는 리포지토리로부터만 설치되도록 할 수 있습니다. Linux의 경우, 운영 체제 보안 업데이트로 분류된 업데이트뿐 아니라 인스턴스의 모든 패키지를 업데이트할 수도 있습니다.

자세한 내용은 다음을 참조하십시오. <https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html>

Maintenance Windows를 사용해 관리형 인스턴스가 비즈니스 크리티컬 작업을 중단하지 않고 패치 및 업데이트 설치와 같은 반복적 관리 작업을 실행하는 일정을 설정합니다.

자세한 내용은 다음을 참조하십시오. <https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-maintenance.html>

Systems Manager 상태 관리자를 사용하여 관리형 인스턴스를 정의된 상태로 유지하는 프로세스를 자동화합니다. 상태 관리자를 사용하여 시작 시 인스턴스가 특정 소프트웨어로 부트스트랩되거나 Windows 도메인에 조인되거나(Windows 인스턴스만 해당) 특정 소프트웨어 업데이트로 패치되도록 할 수 있습니다.

자세한 내용은 다음을 참조하십시오. <https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-state.html>

세션 관리자를 사용하여 대화형 원클릭 브라우저 기반 셀 또는 AWS CLI를 통해 Amazon EC2 인스턴스를 관리합니다. 세션 관리자는 인바운드 포트를 열거나 접속 호스트를 유지하거나 SSH 키를 관리할 필요 없이 안전하고 감사 가능한 인스턴스 관리를 제공합니다. 또한 세션 관리자를 사용하면 인스턴스 액세스 제어, 엄격한 보안 관행, 인스턴스 액세스 세부 정보가 포함된 전면 감사가 가능한 로그를 요구하는 기업 정책을 쉽게 준수하면서 최종 사용자에게 Amazon EC2 인스턴스에 대한 원클릭 교차 플랫폼 액세스를 제공할 수 있습니다.

자세한 내용은 다음을 참조하십시오. <https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>

인벤토리를 사용하면 Amazon EC2 및 온프레미스 컴퓨팅 환경에 대한 가시성을 확보할 수 있습니다. 인벤토리를 사용하여 관리형 인스턴스에서 메타데이터를 수집할 수 있습니다.

자세한 내용은 다음을 참조하십시오. <https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-inventory.html>

www.flaticon.com의 [smalllikeart](#)가 만든 세션 관리자 아이콘
www.flaticon.com의 [wanicon](#)이 만든 인벤토리 아이콘

DO NOT COPY
zlagusdbs@gmail.com

인프라 및 배포 자동화를 위한 AWS OpsWorks

aws training and certification



AWS OpsWorks

구성 관리 서비스

- AWS OpsWorks Stacks
- AWS OpsWorks for Chef Automate
- AWS OpsWorks for Puppet Enterprise



CHEF



puppet

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

AWS OpsWorks Stacks는 Chef를 사용하여 모든 형태와 규모의 애플리케이션을 구성하고 운영하도록 지원하는 구성 관리 서비스입니다. 애플리케이션의 아키텍처 및 각 구성 요소의 사양을 정의할 수 있습니다. 구성 요소에는 패키지 설치, 소프트웨어 구성 및 리소스(예: 스토리지)가 포함됩니다. 애플리케이션 서버 및 데이터베이스 같은 일반적인 기술을 위한 템플릿에서 시작할 수도 있고, 스크립팅 가능한 작업을 수행하도록 자체적으로 구축할 수도 있습니다. AWS OpsWorks Stacks에는 시간 또는 부하를 기반으로 애플리케이션을 조정하는 자동화 기능과 환경이 조정됨에 따라 변경 사항을 조정하는 동적 구성이 포함되어 있습니다.

AWS OpsWorks for Chef Automate는 완전 관리형 Chef Automate 서버뿐 아니라 지속적 배포를 위한 워크플로 자동화, 규정 준수 및 보안을 위한 자동 테스트, 노드와 노드 상태를 볼 수 있는 사용자 인터페이스를 제공하는 자동화 도구 세트를 제공합니다. Chef Automate 플랫폼은 소프트웨어 및 운영 체제 구성, 지속적 규정 준수, 패키지 설치, 데이터베이스 설정 등의 운영 작업을 처리하여 전체 스택 자동화를 제공합니다. Chef 서버는 중앙에서 구성 작업을 저장하고, 노드 몇 개부터 수천 개까지 규모에 상관없이 컴퓨팅 환경에 있는 각 노드에 이러한 작업을 제공합니다. OpsWorks for Chef Automate는 Chef 커뮤니티의 도구 및 툴과 완벽히 호환되며, Chef 서버에 새로운 노드를 자동으로 등록합니다.

AWS OpsWorks for Puppet Enterprise는 관리형 Puppet Enterprise 서버뿐 아니라 조정을 위한 워크플로 자동화, 자동 프로비저닝, 추적 가능성을 위한 시각화를 제공하는 자동화 도구 세트를 제공합니다. Puppet Enterprise 서버는 소프트웨어 및 운영 체제 구성, 패키지 설치, 데이터베이스 설정 등의 운영 작업을 처리하여 풀 스택 자동화를 제공합니다. Puppet 마스터는 중앙에서 구성 작업을 저장하고, 노드 몇 개부터 수천 개까지 규모에 상관없이 컴퓨팅 환경에 있는 각 노드에 이러한 작업을 제공합니다.

DO NOT COPY
zlagusdbs@gmail.com

OpsWorks Stacks에는 수명 주기 이벤트가 있습니다.

aws training and certification

다음 트리거에서 스크립트를 실행할 수 있습니다.

Setup은 새 인스턴스가 성공적으로 부팅된 후 새 인스턴스에서 발생합니다.

Configure는 인스턴스가 온라인 상태에 진입하거나 온라인 상태에서 나갈 때 스택의 모든 인스턴스에서 발생합니다.

Deploy는 앱을 배포할 때 발생합니다.

Undeploy는 앱을 삭제할 때 발생합니다.

Shutdown은 인스턴스를 중지할 때 발생합니다.

AWS OpsWorks Stacks

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

DO NOT
zlagusdbs@gmail.com

AWS CloudFormation과 함께 AWS OpsWorks Stacks 사용하기

AWS CloudFormation을 사용하여 인프라(VPC, IAM 역할)를 구축하고, AWS OpsWorks Stacks를 사용하여 애플리케이션 계층을 배포합니다.

PHP 애플리케이션 스택

- 로드 밸런싱 계층
- 확장 가능한 PHP 앱 계층
- Amazon RDS 계층

경보

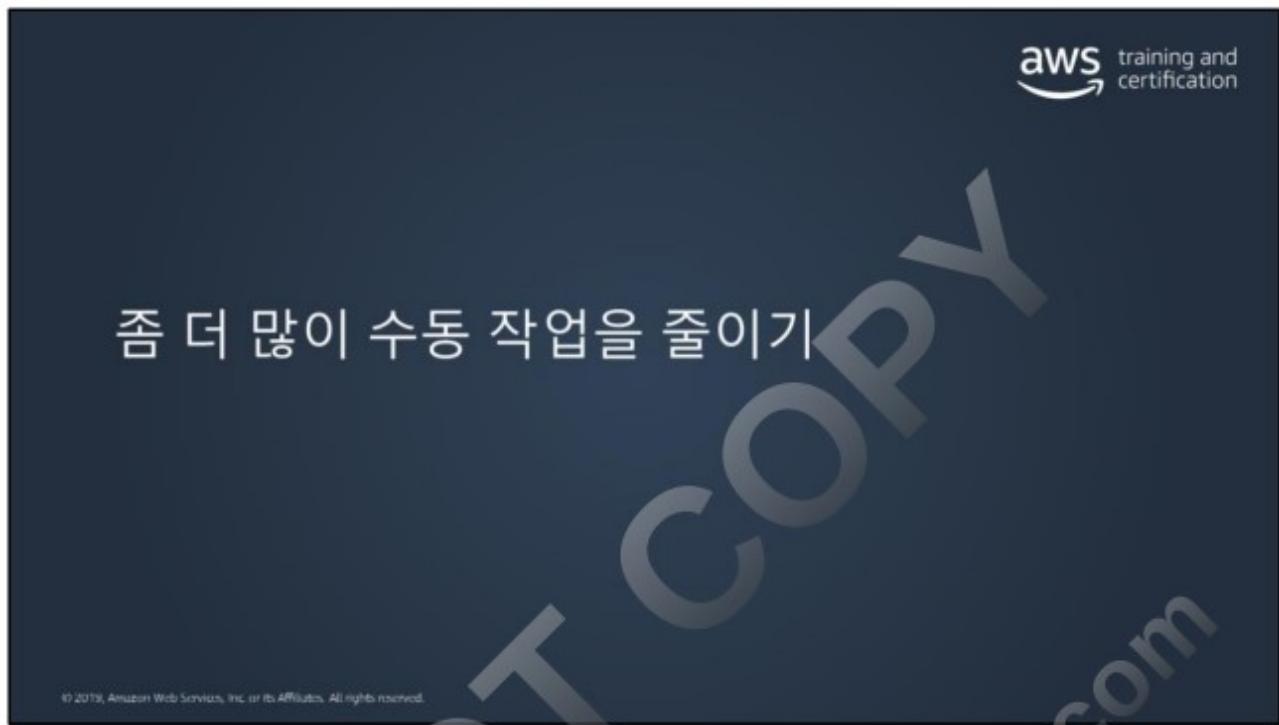
로그

Amazon VPC

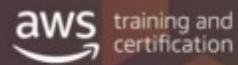
IAM 권한

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

AWS OpsWorks Stacks는 AWS CloudFormation을 통해 생성할 수 있으므로 두 기술을 동시에 사용할 수 있습니다. 계층화된 AWS CloudFormation 템플릿 세트를 사용할 수 있습니다. 즉, 한 템플릿으로 환경의 인프라를 생성하고(예: Amazon VPC, IAM 역할, 외부 애플리케이션과의 통신용 Amazon SQS 대기열), 별도의 AWS CloudFormation 템플릿을 사용하여 해당 인프라 내에 배포되는 AWS OpsWorks Stacks 스택을 생성합니다.



일반적 문제



- 앱 배포에 관련된 인프라 관리는 어려울 수 있습니다
- 서버 관리와 구성에 많은 시간이 걸릴 수 있습니다
- 여러 프로젝트나 애플리케이션에서 일관성 부족

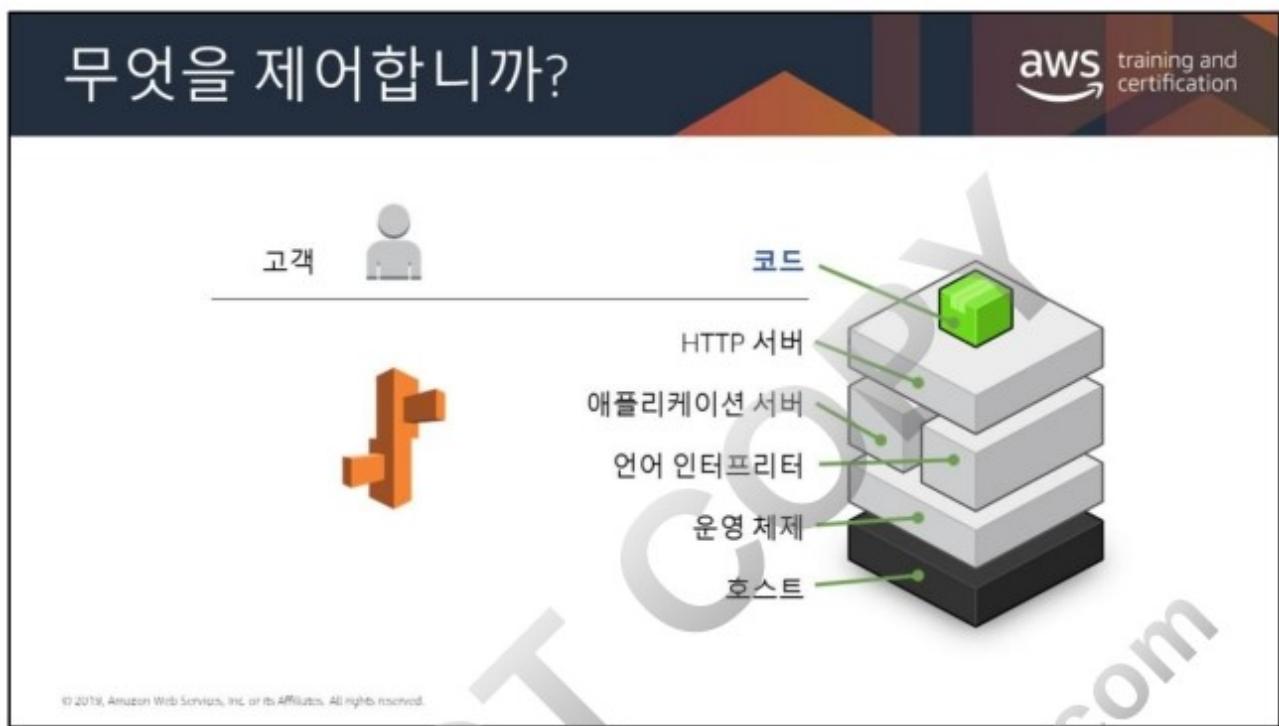
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



The image shows the AWS Elastic Beanstalk landing page. At the top left is the title "AWS Elastic Beanstalk". To the right is the "aws training and certification" logo. On the left side, there is a large orange square containing the AWS logo (a stylized orange 'F'). Below the logo, the text "AWS Elastic Beanstalk" is displayed. To the right of the logo, there are three bullet points in Korean:

- 인프라를 프로비저닝 및 운영하고 사용자를 위해 애플리케이션 스택을 관리
- 완전한 투명성 - 생성되는 모든 것을 확인할 수 있습니다
- 적절한 규모를 유지합니다. 애플리케이션의 크기를 자동으로 늘리거나 줄입니다

At the bottom left, there is a small copyright notice: "© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved."



AWS Elastic Beanstalk의 목표는 개발자가 기본 인프라에 대해 걱정할 필요 없이 클라우드에 확장 가능한 웹 애플리케이션 및 서비스를 배포하고 유지 관리하도록 돋는 것입니다. Elastic Beanstalk은 환경 내 각 EC2 인스턴스를 선택된 플랫폼에서 애플리케이션을 실행하는 데 필요한 구성 요소로 구성합니다. 애플리케이션 스택을 설치 및 구성하기 위해 인스턴스에 로깅하는 것에 대해 걱정할 필요가 없습니다.

Elastic Beanstalk - 환경

Elastic Beanstalk는 필요한 인프라 리소스를 프로비저닝합니다

Elastic Beanstalk는 애플리케이션 환경에 고유한 도메인 이름을 제공합니다(예: [http://\[your app\].elasticbeanstalk.com](http://[your app].elasticbeanstalk.com))

- Route 53을 사용하여 사용자 고유의 도메인 이름을 이 도메인 이름으로 확인할 수 있습니다

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

AWS Elastic Beanstalk으로 작업 시 두 가지 유형의 환경을 선택할 수 있습니다. 단일 인스턴스 환경은 단일 EC2 인스턴스를 시작할 수 있지만 로드 밸런싱 또는 Auto Scaling이 포함되지 않습니다. 다른 유형의 환경은 여러 EC2 인스턴스를 시작할 수 있지만 로드 밸런싱 및 Auto Scaling 구성이 포함됩니다.

Elastic Beanstalk은 ELB, Auto Scaling 그룹, 보안 그룹, 데이터베이스(선택 사항) 등과 같이 필요한 인프라 리소스를 프로비저닝합니다.



자주 하는 질문 중 하나가 애플리케이션 관리를 제공하는 다양한 서비스와 이러한 서비스를 구분하는 것에 관한 것입니다. 고객이 필요한 간편성 및 제어의 수준에 따라 달라집니다.

AWS Elastic Beanstalk는 널리 사용되는 컨테이너인 Java, PHP, Node.js, Python, Ruby 및 Docker로 웹 애플리케이션을 구축할 수 있는 사용이 간편한 애플리케이션 서비스입니다. 코드를 업로드하길 원하고, 환경을 사용자 정의할 필요가 없다면, Elastic Beanstalk가 적합합니다.

AWS OpsWorks를 사용하면 애플리케이션을 시작하고 애플리케이션의 아키텍처 및 각 구성 요소의 사양을 정의할 수 있습니다. 구성 요소에는 패키지 설치, 소프트웨어 구성 및 리소스(예: 스토리지)가 포함됩니다. 앱 서버, 데이터베이스 등과 같은 일반 기술용 템플릿을 사용하거나 자체 템플릿을 작성할 수 있습니다.



실습 5: 인프라 배포 자동화



"일관되고 반복 가능한 방식으로 인프라를 배포하고 싶습니다."

사용된 기술:

- AWS CloudFormation

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

실습 5: 인프라 배포 자동화



계층에 인프라를 배포합니다.

- 네트워크 계층
- 애플리케이션 계층

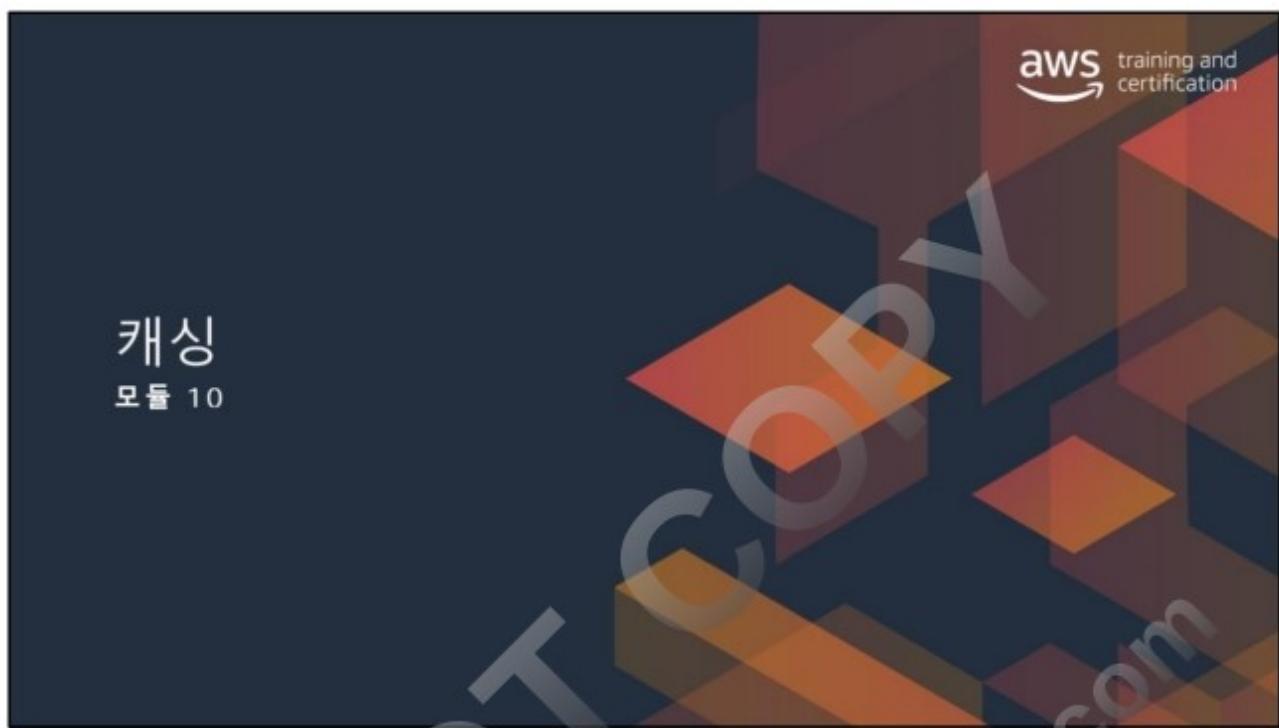
추가 작업:

- 스택 업데이트
- 삭제 정책이 있는 스택 삭제

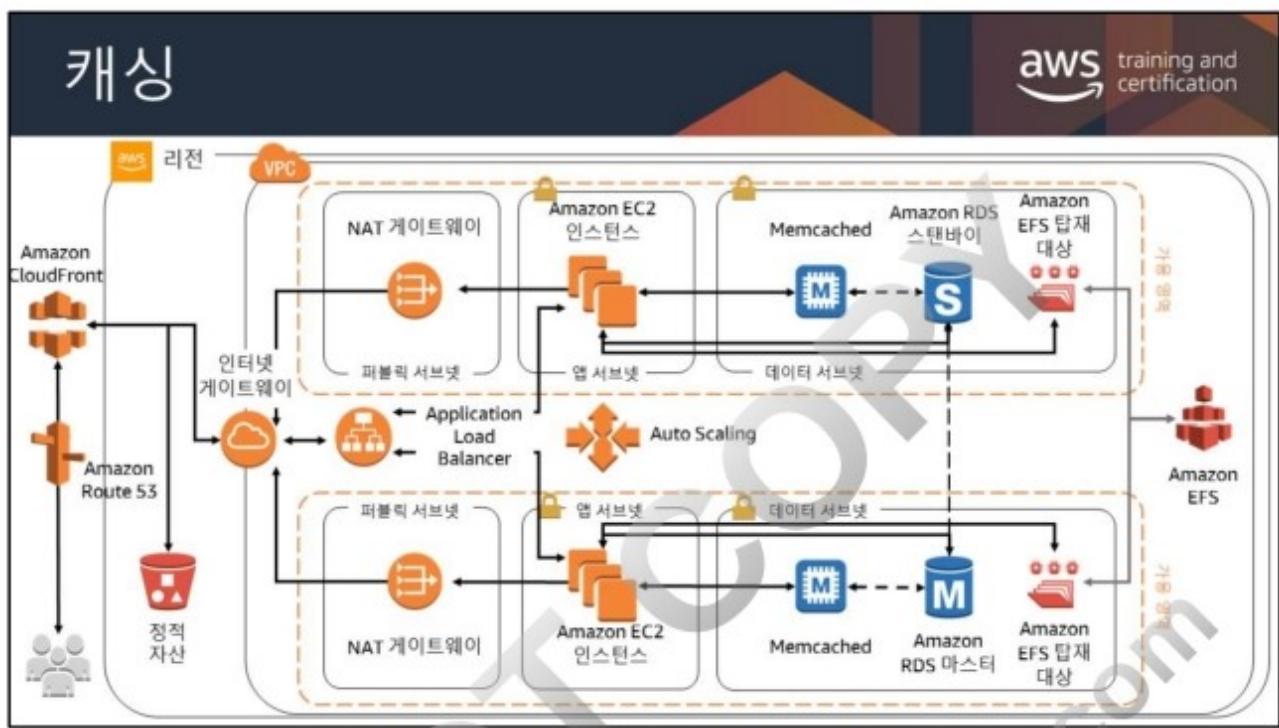
시간: 30분

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





DO NOT COPY
zlagusdbs@gmail.com



수업이 끝나면 이 아키텍처 디어그램의 모든 구성 요소를 이해할 수 있습니다.
또한 규모가 크고 견고한 자체 아키텍처 솔루션을 구성할 수도 있습니다.

모듈 10



아키텍처 측면에서의 필요성

동일한 요청으로 인프라 용량이 지속적으로 과부하됩니다. 이는 비효율적으로 비용 및 지연 시간을 늘립니다.

모듈 개요

- 캐싱 개요
- 엣지 캐싱
- 데이터베이스 캐싱

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





캐시가 어떻게 성능을 향상시키는지를 설명하기 위해 철물점으로 이동하는 것을 고려해 보시기 바랍니다.

철물점이 수 마일 떨어져 있다면 뭔가 필요할 때마다 그 곳에 가기 위해 상당한 노력을 기울일 것입니다.



그 대신 공구 창고(캐시)가 가까운 곳에 있다면 여러분이 필요한 소모품으로 공구 창고를 채우면 됩니다. 그렇다면 이제 뭔가 필요할 때 철물점으로 이동하는 대신, 그냥 여러분의 공구 창고로 가면 됩니다.

그러나 저장한 내용물(stockpile)을 새로운 것으로 바꿔야 할 때, 철물점은 항상 옵션에 있습니다.

무엇을 캐시해야 합니까?

aws training and certification

-  수집하려면 느리고 비싼 쿼리가 필요한 데이터
-  비교적 정적이고 자주 액세스하는 데이터(예: 소셜 미디어 웹 사이트의 프로필)
-  공개 거래되는 주식 가격처럼 일정 기간 동안 변화가 없을 수 있는 정보

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

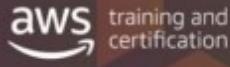
속도 및 비용 – 데이터베이스에서 데이터를 획득하는 것은 캐시에 비해 언제나 더 많은 시간과 비용이 듭니다. 일부 데이터베이스 쿼리는 본래부터 다른 데이터베이스 쿼리에 비해 더 많은 시간과 비용이 듦니다. 예를 들면, 여러 테이블에서 조인을 수행하는 쿼리는 단순한 단일 테이블 쿼리보다 훨씬 더 많은 시간과 비용이 듦니다. 관심이 있는 데이터를 획득하기 위해 시간과 비용이 많이 드는 쿼리가 필요할 경우, 이러한 쿼리는 캐싱 후보에 속합니다. 데이터를 획득하기 위해 비교적 빠르고 간단한 쿼리가 필요할 경우, 이러한 쿼리는 그 밖의 요인에 따라 여전히 캐싱 후보가 될 수 있습니다.

데이터 및 액세스 패턴 – 캐싱할 항목을 결정할 때에도 데이터 그 자체와 데이터의 액세스 패턴을 이해해야 합니다. 예를 들면, 변화 속도가 빠르거나 액세스가 거의 없는 데이터는 캐싱할 필요가 없습니다. 캐싱을 통해 유의미한 이점을 얻으려면 소셜 미디어 사이트의 개인 프로필과 같이 비교적 정적이면서도 액세스빈도가 높은 데이터가 있어야 합니다. 이와는 반대로, 캐싱을 해도 속도나 비용 면에서 이득이 없다면 데이터를 캐싱할 필요가 없습니다. 예를 들면, 검색 결과를 반환하는 웹 페이지를 굳이 캐싱할 필요는 없습니다. 그 이유는 그러한 쿼리 및 결과가 거의 항상 고유한 것이기 때문입니다.

기한 경과 – 기본적으로 캐싱된 데이터는 기한이 지난 데이터입니다. 이러한 데이터는 특정 상황에서 기한이 경과하지 않을 경우에도 항상 기한이 경과한 것으로 간주 및 취급해야 합니다. 사용 중인 데이터가 캐싱 후보인지 여부를 결정할 때 기한이 경과한 데이터에 대한 애플리케이션의 내결함성을 결정해야 합니다. 사용 중인 애플리케이션의 경우, 하나의 컨텍스트에서 기한이 경과한 데이터를 허용할 수 있더라도 다른 컨텍스트에서는 그럴 수 없습니다.

예를 들면, 공개적으로 거래되는 주식의 가격 정보를 웹 사이트 상에서 제공하는 경우, 가격 공개는 최대 n 분까지 지연될 수 있다는 면책 요건을 전제로 하여 기한 경과를 허용할 수 있습니다. 그러나 주식을 매매하는 중개인(브로커)에게 동일한 주식에 대한 가격 정보를 제공할 때에는 실시간 데이터가 필요합니다.

캐싱의 이점



The slide features three icons illustrating the benefits of caching:

- 애플리케이션 속도 향상**: Represented by a blue cloud icon containing a computer monitor displaying a chart.
- 시간이 많이 걸리는 DB 쿼리의 부담 완화**: Represented by a purple gear icon with a green triangle in the center.
- 응답 지연 시간 감소**: Represented by a hand pointing at a yellow button with a light effect around it.

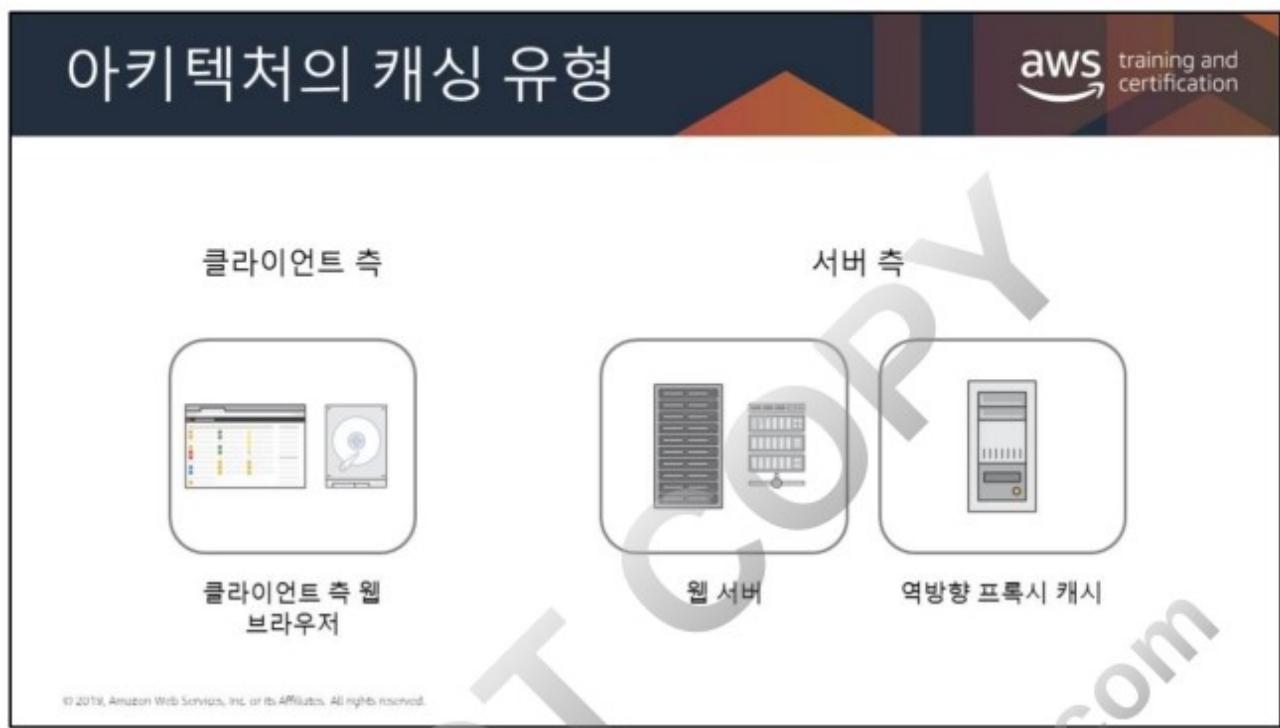
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

캐시는 메모리에 데이터를 저장하여 흔히 액세스하는 애플리케이션 데이터에 대해 높은 처리량, 지연 시간이 짧은 액세스를 제공합니다. 캐싱은 애플리케이션의 속도를 높일 수 있습니다. 캐싱은 애플리케이션 사용자가 경험하는 응답 지연 시간을 줄입니다. 시간 소모적인 데이터베이스 쿼리와 복잡한 쿼리는 애플리케이션에 병목 현상을 일으키는 경우가 많습니다. 읽기 집약적인 애플리케이션에서 캐싱은 애플리케이션 처리 시간과 데이터베이스 액세스 시간을 줄임으로써 유의한 수준의 성능 향상을 제공합니다.

쓰기 집약적인 애플리케이션은 대체로 캐싱에서 큰 효과를 보지 못합니다. 하지만 쓰기 집약적인 애플리케이션도 보통 읽기/쓰기 비율이 1보다 큽니다. 즉, 읽기 캐싱은 여전히 유용하다는 것을 나타냅니다.

데이터 캐싱을 고려해야 할 경우를 열거하면 다음과 같습니다.

- 캐시 검색에 비해 데이터 획득에 더 많은 시간과 비용이 드는 경우
- 충분한 빈도로 데이터에 액세스하는 경우
- 데이터가 비교적 정적인 경우 또는 신속한 변화와 기한 경과가 큰 문제에 속하지 않는 경우



컴퓨팅에서 캐시는 대체로 일시적인 성격의 데이터 하위 집합을 저장하는 고속 데이터 스토리지 계층에 속하기 때문에 향후 그러한 데이터에 대한 요청은 해당 데이터의 기본 스토리지 위치를 액세스할 때보다 더 신속하게 처리됩니다. 캐싱을 이용하면 이전에 검색하거나 계산된 데이터를 효과적으로 재사용할 수 있습니다.

웹 캐싱은 오리진 서버보다는 오히려 캐시로부터 향후 요청을 이행하기 위해 캐시에서 HTTP 응답 및 웹 리소스를 보관함으로써 진행됩니다.

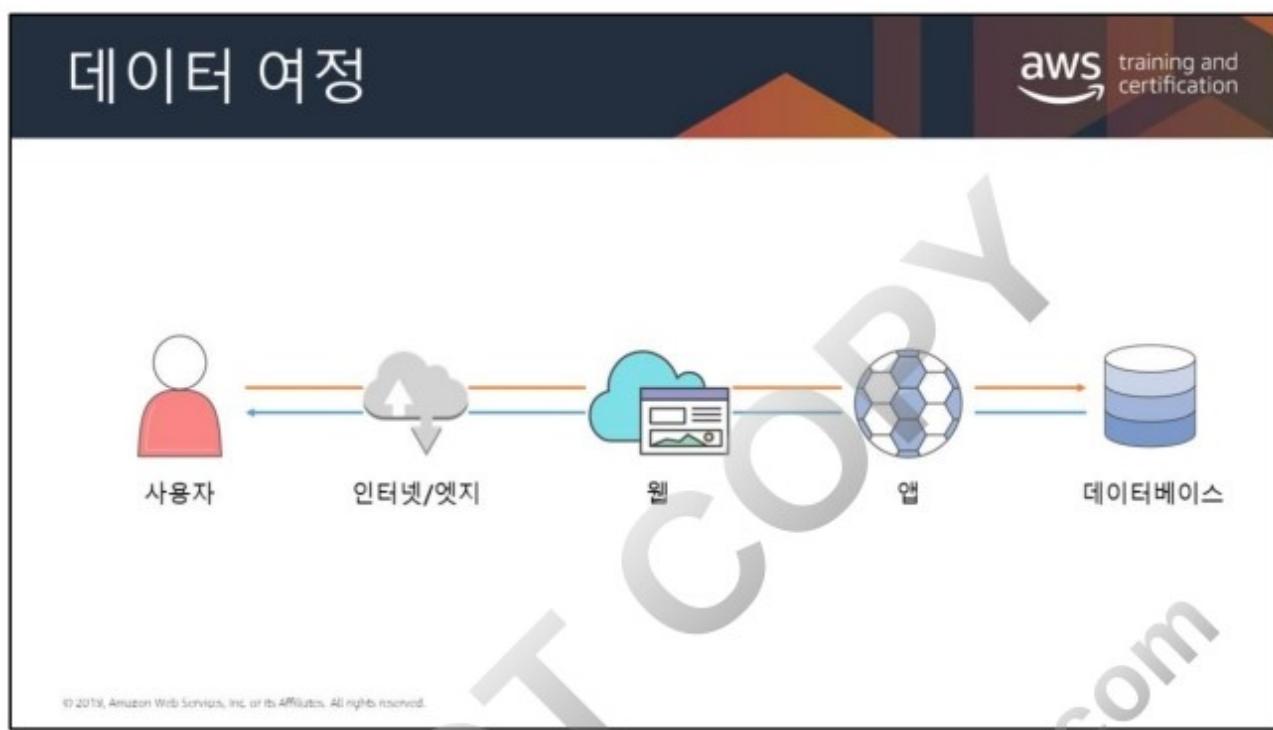
웹 캐시는 다양한 기술에서 효과적으로 활용할 수 있습니다. 가장 기본적인 레벨은 클라이언트 측 웹 캐싱입니다. 데이터는 반복된 쿼리를 웹 서버에 전달하기보다는 오히려 브라우저 내에 저장됩니다. HTTP 캐시 헤더는 저장된 웹 콘텐츠에 대한 캐시로부터 향후 응답을 브라우저가 얼마나 오랫동안 이행할 수 있는지에 관한 세부 정보를 제공합니다.

서버 측에서는 다양한 웹 캐싱 기법을 활용해 웹 사이트 성능을 향상시킬 수 있습니다.

역방향 프록시 캐시 또는 웹 애플리케이션 액셀러레이터는 캐시된 버전의 HTTP 응답을 보관된 상태에서 제공하기 위해 애플리케이션 및 웹 서버의 앞쪽에 배치할 수 있습니다. 이러한 캐시들은 사이트 관리자가 구현하며, 브라우저와 오리진 서버 간의 중개자 역할을 담당합니다. 또한 이러한 캐시들은 흔히 HTTP 캐시 지시문을 기반으로 합니다.

DO NOT COPY
zlagusdbs@gmail.com









웹 트래픽이 지리적으로 분산된 경우, 전체 인프라를 전 세계에 복제하는 것은 때때로 불가능할 수도 있습니다(그리고 꼭 비용 효율적이지만은 않습니다). CDN에서는 웹 콘텐츠(예: 비디오, 웹 페이지, 이미지 등)의 캐시된 사본을 고객에게 제공하기 위해 엣지 로케이션의 글로벌 네트워크를 사용할 수 있습니다. 응답 시간을 줄이기 위해 CDN은 고객 또는 발신 요청 위치에 가장 가까운 엣지 로케이션을 사용합니다. 웹 자산이 캐시에서 제공되면 처리량은 크게 증가합니다. 동적 데이터의 경우, 오리진 서버에서 데이터를 검색하도록 많은 CDN을 구성할 수 있습니다.

Amazon CloudFront



Amazon의 글로벌 CDN(콘텐츠 전송 네트워크)

기본적인 멀티 티어 캐시와 광범위한 유연성으로 모든 전송 사례에 최적화

아키텍처에 추가적인 보안 계층 제공

WebSocket 프로토콜 지원

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

Amazon CloudFront는 웹 사이트, API, 동영상 콘텐츠 또는 기타 웹 자산의 전송을 가속화하는 글로벌 CDN 서비스입니다. 다른 AWS 제품과 통합하여 사용하면 개발자와 기업이 최소 사용 약정 없이도 최종 사용자에게 쉽고 빠르게 콘텐츠를 전송할 수 있습니다.

Amazon CloudFront는 지연 시간 및 처리량을 위한 네트워크 계층 최적화와 함께 캐시 동작 최적화를 위한 강력한 유연성을 제공하는 데 최적화되어 있습니다.

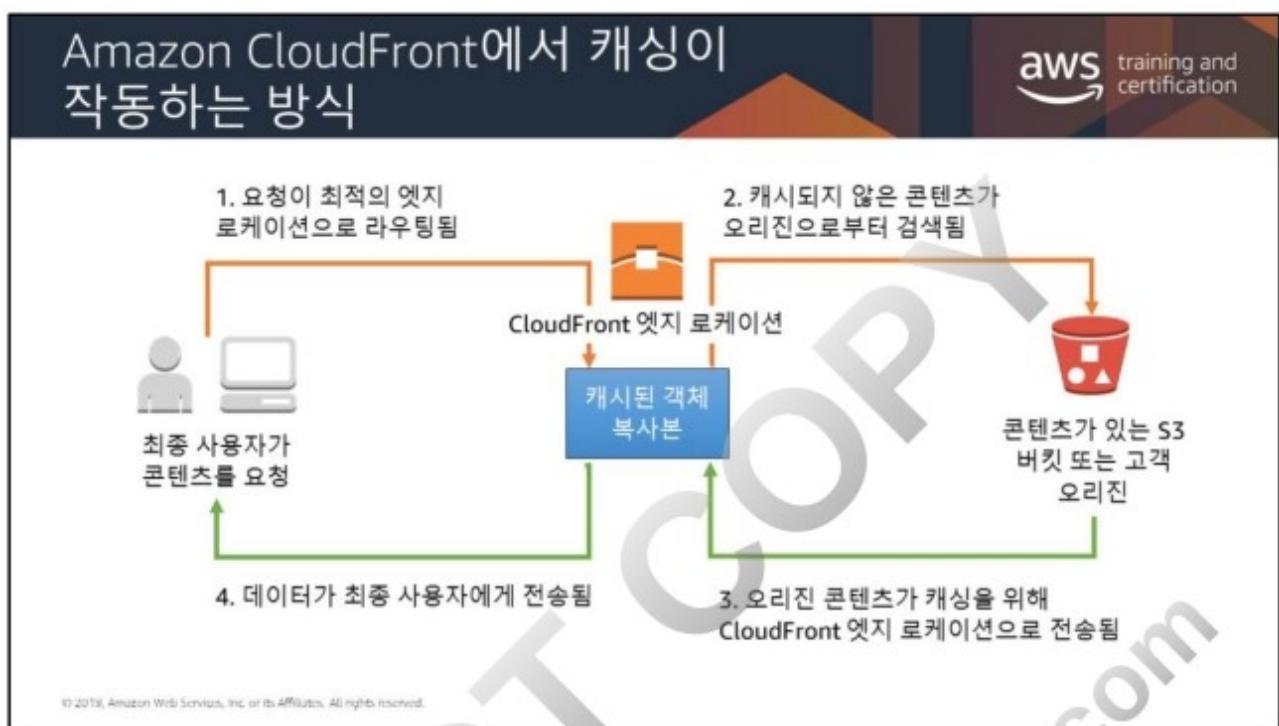
콘텐츠 전송 네트워크(CDN)는 멀티 티어 캐시를 기본적으로 제공하며, 이와 더불어 객체가 아직 엣지에 캐시되지 않았을 때 오리진 서버의 지연 시간을 개선하고 부하를 줄여주는 리전 엣지 캐시도 함께 제공합니다.

CloudFront는 짧은 지연 시간과 빠른 데이터 전송 속도로 콘텐츠를 쉽게 배포할 수 있는 비용 효율적인 방법을 제공합니다. 모든 AWS 인프라 서비스와 마찬가지로 CloudFront는 장기 약정 또는 최소 요금이 필요하지 않은 종량 과금제 서비스입니다. CloudFront를 사용하면 엣지 로케이션의 글로벌 네트워크를 사용해 최종 사용자에게 파일이 전송됩니다.

Amazon CloudFront는 WebSocket 프로토콜을 통한 실시간 양방향 통신을 지원합니다. 이 영구 연결을 통해 클라이언트와 서버가 반복적인 연결로 인한 오버헤드 없이 서로 실시간 데이터를 전송할 수 있습니다. 이는 특히 채팅, 공동 작업, 게임, 금융 거래 같은 통신 애플리케이션에 유용합니다.

CloudFront의 WebSocket 지원으로 고객은 다른 동적 및 정적 콘텐츠와 동일한 경로를 통해 WebSocket 트래픽을 관리할 수 있습니다. CloudFront의 엣지 로케이션 글로벌 네트워크로 트래픽이 사용자에 더 가까워지고, 응답성 및 안정성이 개선되며, 고객은 AWS Shield 및 AWS WAF에 기본 통합된 CloudFront를 통한 DDoS 보호를 이용할 수 있습니다.

WebSocket 프로토콜은 클라이언트가 업데이트된 데이터를 수신하거나 새로운 정보를 보내려 할 때마다 계속 새 연결을 열 필요가 없기 때문에 일반적 TCP 연결의 오버헤드를 제거합니다. WebSocket 연결은 클라이언트 또는 서버에서 닫을 때까지 계속 열려 있으며, 연결이 열려 있는 동안 데이터를 주고받을 수 있습니다.



CloudFront를 통해 서비스하는 콘텐츠를 최종 사용자가 요청하면 자연 시간(시간 지연)이 가장 짧은 엣지 로케이션으로 사용자가 라우팅되므로 가능한 최고의 성능으로 콘텐츠가 제공됩니다. 콘텐츠가 이미 자연 시간이 가장 짧은 엣지 로케이션에 있는 경우, CloudFront가 콘텐츠를 즉시 제공합니다. 콘텐츠가 현재 해당 엣지 로케이션에 없는 경우, CloudFront에서는 콘텐츠의 최종 버전에 대한 원본으로 식별한 Amazon S3 버킷 또는 HTTP 서버(예: 웹 서버)에서 콘텐츠를 검색합니다.

상기의 예에서 콘텐츠가 캐시되지 않은 경우, 요청된 객체는 오리진으로부터 검색됩니다. 사용자가 요청한 데이터를 검색하여 반환하기 위해 단계 1, 2, 3 및 4가 진행됩니다.

콘텐츠가 캐시된 경우, 캐시된 객체 요청은 최적의 엣지 로케이션으로 라우팅되고 캐시된 객체는 단계 1과 4에서처럼 검색됩니다.



CloudFront의 캐싱 및 가속화 기술을 통해 AWS는 정적 이미지에서 사용자 입력 콘텐츠까지 모든 콘텐츠를 제공할 수 있습니다.

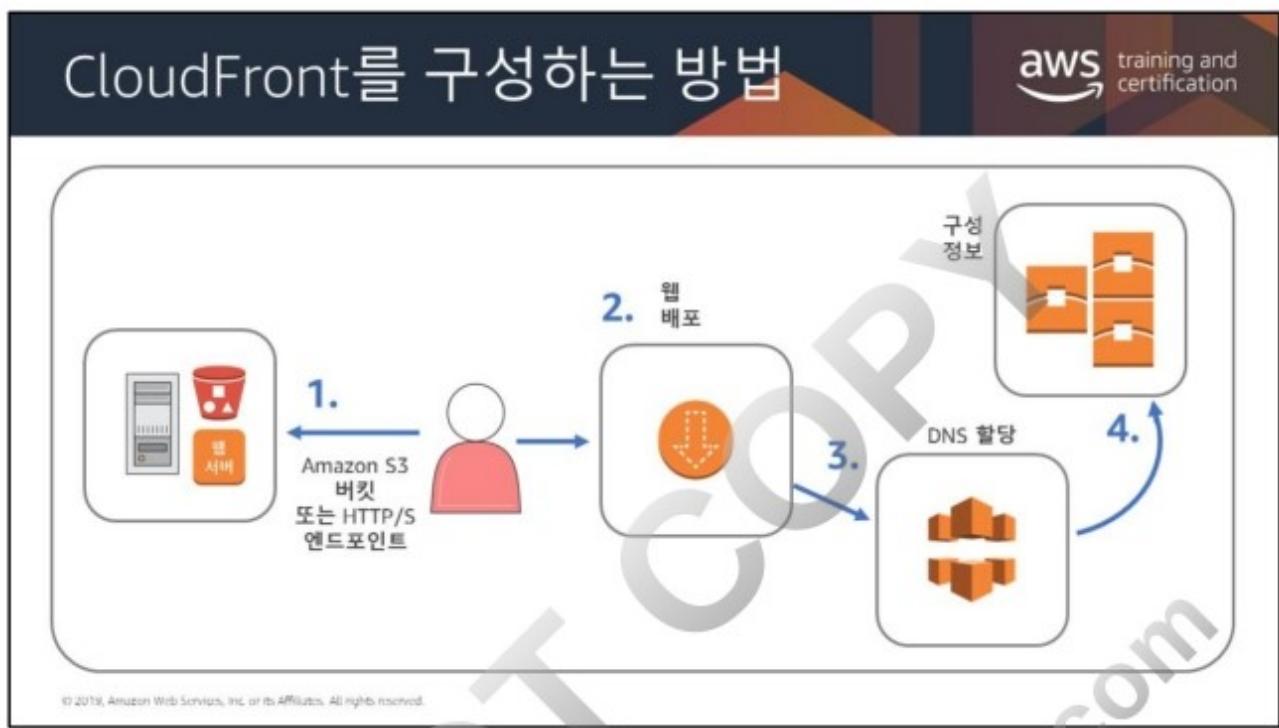
정적: TTL (Time-To-Live)이 높은 이미지, js, html 등

동영상: rtmp 및 http 스트리밍 지원

동적: 사용자 정의 콘텐츠 및 캐싱할 수 없는 콘텐츠

사용자 입력: http 작업 지원(Put/Post 등 포함)

보안: SSL (HTTPS)을 통해 콘텐츠를 안전하게 제공



1. CloudFront가 사용자의 파일을 가져오는 출처에 해당하는 Amazon S3 버킷 또는 사용자의 HTTP 서버와 같은 오리진 서버를 지정합니다. 이들 서버는 전 세계의 CloudFront 엣지 로케이션에서 배포됩니다.

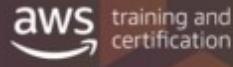
오리진 서버는 객체의 최종 원본 버전을 저장합니다. HTTP를 통해 콘텐츠를 서비스하는 경우, 오리진 서버는 Amazon S3 버킷 또는 HTTP 서버(예: 웹 서버)입니다. HTTP 서버는 Amazon EC2 (Amazon Elastic Compute Cloud) 인스턴스 또는 사용자가 관리하는 온프레미스 서버에서 실행할 수 있습니다. 이들 서버를 일컬어 사용자 지정 오리진이라고도 합니다.

2. 사용자가 웹 사이트나 애플리케이션을 통해 파일을 요청할 경우, 어떤 오리진 서버에서 파일을 가져올지를 CloudFront에 알려주는 CloudFront 배포를 만듭니다. 동시에 CloudFront에서 모든 요청을 기록할지 여부 및 배포를 만들자마자 활성화할지 여부와 같은 세부 사항을 지정합니다.

3. CloudFront는 새 배포에 도메인 이름을 할당합니다.

4. CloudFront는 콘텐츠를 제외한 배포의 구성을 모든 엣지 로케이션에 전달합니다. 엣지 로케이션은 지리적으로 분산된 여러 데이터 센터의 서버들로 이루어진 집합체이며, 여기서 CloudFront는 객체의 사본을 캐시합니다.

콘텐츠 만료 방법



Time To Live (TTL)

- 기간 고정(만료 기간)
- 고객이 설정
- CloudFront에서 오리진으로의 GET 요청에 **If-Modified-Since header**를 사용

객체 이름 변경

- Header-v1.jpg를 Header-v2.jpg로 변경
- 새 이름이 생기면 새로 고침이 수행됨

객체 무효화

- 마지막 수단: 매우 비효율적이고 비용이 많이 들

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

캐시된 콘텐츠를 만료하는 방법은 3가지가 있는데, 처음 2가지 방법을 사용하는 것이 좋습니다. 즉시 교체할 필요가 없다면 TTL이 가장 간편합니다. (자세한 내용은

<http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/RequestAndResponseBehaviorS3Origin.html>을 참조하십시오.)

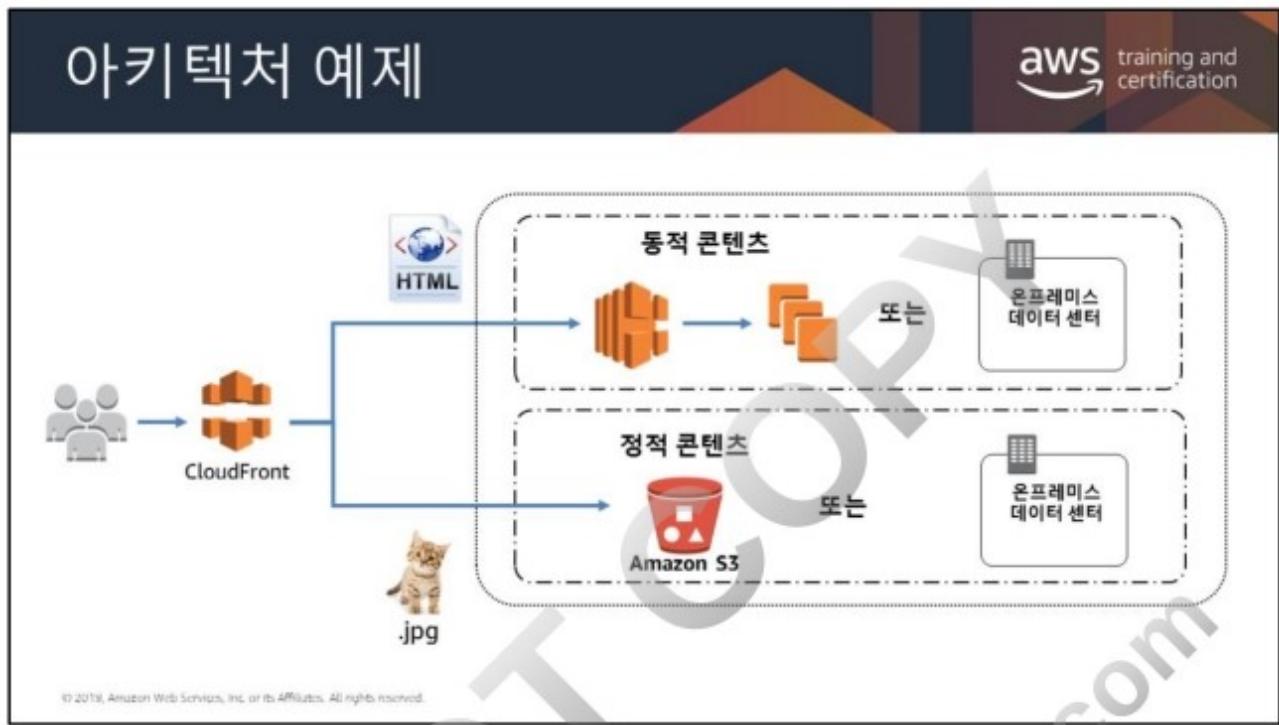
특정 오리진에 대한 TTL을 0으로 설정하더라도 CloudFront는 해당 오리진에서 콘텐츠를 계속 캐시합니다. 그런 다음, If-Modified-Since 헤더를 포함한 GET 요청을 전달함으로써 오리진에서 콘텐츠가 변경되지 않았다면 CloudFront가 캐시된 콘텐츠를 계속 사용할 수 있는지를 오리진이 알려주도록 합니다.

두 번째 방법은 약간의 노력이 더 필요하지만 즉각적입니다(일부 CMS 시스템에서 이 방법을 어느 정도 지원할 수 있음). 고객이 CloudFront 배포에서 기존 객체를 업데이트하고 같은 객체 이름을 사용할 수는 있지만 이는 권장되지는 않습니다. CloudFront는 사용자가 새로운 객체 또는 업데이트된 객체를 오리진에 저장했을 때가 아니라, 해당 객체가 요청되었을 때에만 객체를 엣지 로케이션에 배포합니다. 오리진에 있는 기존 객체를 같은 이름의 최신 버전으로 업데이트하는 경우, 엣지 로케이션은 두 개의 나열된 이벤트가 모두

발생해야 오리진에서 새로운 버전을 가져옵니다.

세 번째 방법은 개별 객체에 대해 매우 드문 경우에만 사용해야 합니다. 이는 결코 좋은 솔루션이 아닙니다(시스템이 모든 엣지 로케이션과 강제로 상호 작용해야 하기 때문).

DO NOT COPY
zlagusdbs@gmail.com



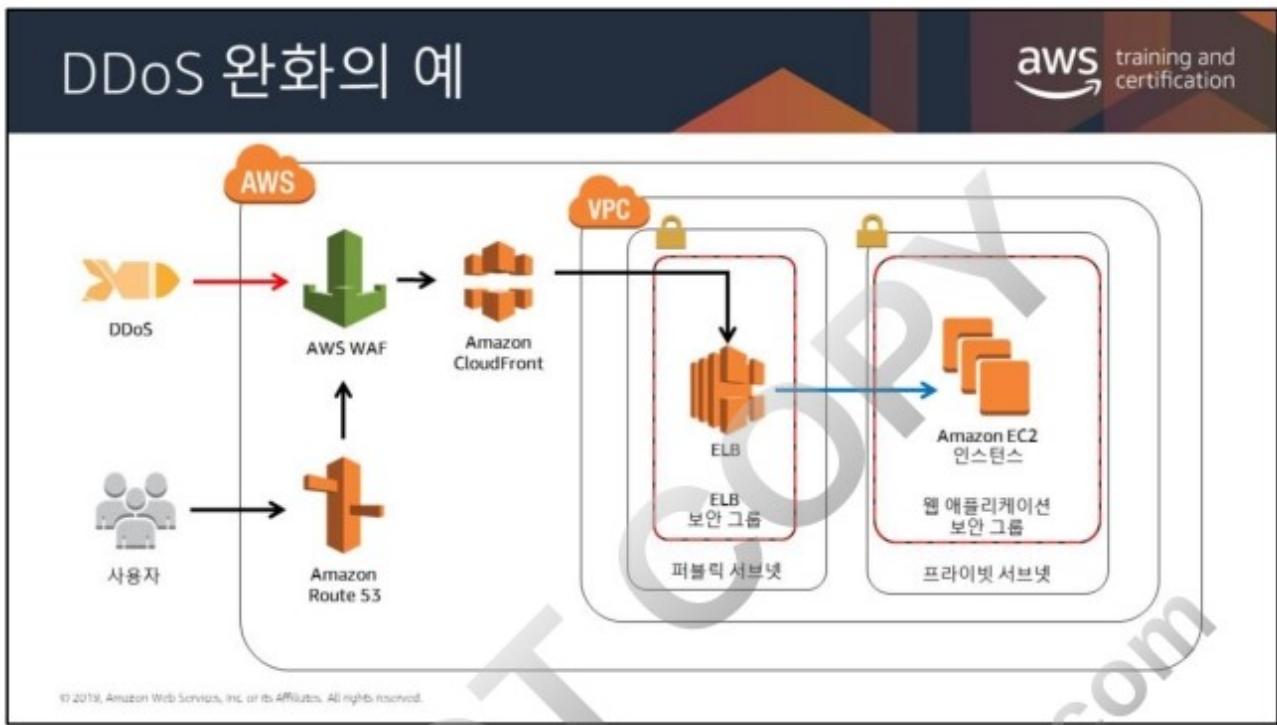
사용자는 대체로 정적 콘텐츠만 캐시합니다. 다만 동적이거나 또는 고유한 콘텐츠는 애플리케이션의 성능에 영향을 미칩니다. 수요에 따라 차이는 있겠지만, Amazon S3에서 동적 콘텐츠 또는 고유한 콘텐츠를 캐싱하면 성능 향상에 도움이 될 수 있습니다.

정적 콘텐츠 오프로딩:

- 정적 자산에 대해 상대 URL 참조 대신, 절대 URL 참조를 생성합니다.
- 정적 자산을 Amazon S3에 저장합니다.
- "WORM (Write Once Read Many)"에 대해 최적화합니다.

또한 콘텐츠를 지리적으로 제한할 수 있습니다. 지리적 차단이라고도 하는 지리적 제한을 사용하면 특정 지리적 위치에 있는 사용자가 CloudFront 웹 배포를 통해 배포한 콘텐츠에 액세스하는 것을 차단할 수 있습니다. 지리적 제한은 다음의 두 가지 방법 중 하나를 선택하여 사용하면 됩니다.

- CloudFront 지리적 제한 기능을 사용하면 배포와 연결된 파일 전체에 대한 액세스를 제한하고 국가 수준에서 액세스를 제한할 수 있습니다.
- 타사 지리적 위치 서비스를 사용하면 배포와 연결된 파일의 하위 집합에 대한 액세스를 제한하거나 국가 수준보다 더 세분화된 범위에서 액세스를 제한할 수 있습니다.



이것은 DDoS 공격을 방지 또는 완화하는 데 도움이 될 수 있는 복원력이 뛰어난 아키텍처의 예에 속합니다.

공격 노출 영역을 최소화하기 위한 전략은 (a) 필요한 인터넷 접속 지점의 수를 축소하고, (b) 중요하지 않은 인터넷 접속 지점을 제거하며, (c) 관리 트래픽에서 최종 사용자 트래픽을 분리하고, (d) 신뢰할 수 없는 최종 사용자가 액세스할 수 없도록 필요한 인터넷 접속 지점을 난독화하며, (e) 공격의 영향을 최소화하기 위해 인터넷 접속 지점의 결합을 해제하는 것입니다. Amazon Virtual Private Cloud (VPC)로 이 전략을 달성할 수 있습니다.

AWS를 사용하면 2가지 형태의 확장, 즉 수평 확장 및 수직 확장을 활용할 수 있습니다. DDoS의 측면에서 볼 때, AWS의 확장을 활용할 수 있는 방법은 3가지가 있습니다. 즉, (1) 사용자의 애플리케이션에 적절한 인스턴스 유형을 선택하고, (2) 자동 확장을 위한 Elastic Load Balancing 및 Auto Scaling 등의 서비스를 구성하며, (3) Amazon CloudFront와 Amazon Route 53과 같은 AWS 글로벌 서비스에 내재화된 확장 기능을 사용하는 것입니다.

ELB는 유효한 TCP 요청만을 지원하기 때문에 UDP 및 SYN 플러드와 같은 DDoS 공격은 인스턴스에 도달할 수 없습니다.

네트워크 트래픽이 높을 때(DDoS 공격의 전형적인 결과) Auto Scaling 그룹에 새 인스턴스를 점진적으로 추가하는 조건을 설정할 수 있습니다.

Elastic Load Balancing 및 Amazon EC2와 같이 AWS 리전에서 제공하는 서비스를 사용하면 DDoS 복원력을 구축할 수 있으며 확장을 통해 특정 리전 내에서 예상치 못한 트래픽 양을 처리할 수 있습니다. Amazon CloudFront, AWS WAF, Amazon Route 53 및 Amazon API Gateway와 같이 AWS 엣지 로케이션에서 제공하는 서비스를 이용하면 애플리케이션에 더 큰 내결함성을 제공하고 더 많은 양의 트래픽을 관리하기 위한 확장성을 증진할 수 있는 엣지 로케이션의 글로벌 네트워크를 활용할 수 있습니다.

이러한 각각의 서비스를 사용하여 인프라 계층 및 애플리케이션 계층에 대한 복원력을 구축하는 데 따른 이점들은 이후 섹션에서 설명하고 있습니다.

Amazon CloudFront에는 유효한 TCP 연결 및 HTTP 요청만 실행하고 유효하지 않은 요청은 폐기할 수 있는 필터링 기능도 포함하고 있습니다.

WAF(웹 애플리케이션 방화벽)는 IP 주소, HTTP 헤더, HTTP 본문 또는 URI 문자열과 같은 데이터를 기반으로 하여 웹 요청을 필터링하기 위해 HTTP 트래픽에 규칙 세트를 적용하는 도구입니다. 불법적인 트래픽을 오프로드하여 DDoS 공격을 완화하는 데 도움을 줄 수 있습니다.

현재 AWS는 관리형 WAF 서비스를 제공하고 있습니다. AWS WAF에 대한 자세한 내용은 <http://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html>을 참조하십시오.

백서: AWS Best Practices for DDoS Resiliency:

https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf





세션 관리

aws training and certification

Elastic Load Balancing



고정 세션

사용자 세션을 관리하는 특정 서버로 요청을 라우팅할 수 있습니다

- 클라이언트 측 쿠키
- 비용 효율성
- 세션 검색 속도 증가

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

세션 관리가 캐싱과 관련이 없는 것처럼 보이지 않을 수도 있지만 실제로는 관련이 있습니다.

기본적으로 웹 세션은 동일한 사용자가 환경으로 보내는 일련의 HTTP 트랜잭션입니다. HTTP는 문서를 전송할 수 있도록 설계되었습니다. 이는 상태를 관리하지 않습니다. 모든 요청은 이전 트랜잭션과 무관합니다. 서버에 전달된 모든 요청에 대한 자격 증명을 사용자들이 전송할 필요가 정말로 있다고 생각하십니까? 귀사의 서버는 사용자들과 그들의 요구 사항이 증가함에 따라 확장하는 데 필요한 네트워크 및 컴퓨팅 파워를 보유하고 있습니까?

세션 관리는 인증 및 액세스 제어를 의미합니다. 상태 관리에 대한 일반적인 접근 방식은 고정 세션 또는 분산 캐시의 사용을 포함합니다.

고정 세션(세션 선호도라고도 함)을 사용하면 사용자의 세션을 관리하는 특정 서버로 요청을 라우팅 할 수 있습니다. 세션의 유효성은 로드 밸런서에서 설정된 클라이언트 측 쿠키 또는 파라미터 등 여러 가지 방법으로 결정할 수 있습니다.

사용자는 애플리케이션을 실행하는 웹 서버에 세션을 저장하기 때문에 고정 세션은 비용 효율적입니다. 이는 네트워크 지연 시간을 없애고 해당 세션의 검색 속도를 높입니다. 그러나 장애가 발생할 경우, 하나의 노드에 저장된 여러 세션이 손실될 가능성이 있습니다.

확장 시 활성 세션은 늘어난 용량에 대한 트래픽 라우팅을 차단하기 때문에 트래픽이 여러 서버에 걸쳐 불균일하게 분산될 가능성이 있습니다.

DO NOT COPY
zlagusdbs@gmail.com

상태 정보를 위해 DynamoDB를 사용하는 경우

aws training and certification

사용 사례: 온라인 게임 사이트
문제: 더 빠른 세션 검색

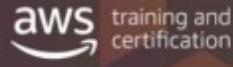
The diagram illustrates a system architecture for an online game site. A user icon sends a request to a CloudFront icon. This request is then processed by a Web Server icon, which finally reaches a Game Server icon. Above this flow, a blue cylinder labeled '세션 상태' (Session State) has a downward arrow pointing to the connection between the CloudFront and Web Server icons, indicating that session state information is passed through the web layer.

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





데이터베이스 캐싱은 언제 시작해야 합니까?



The slide features three icons illustrating scenarios where database caching might be beneficial:

- Icon 1:** A tablet and a smartphone. **Text:** 고객에 대한 응답 시간이 우려되는 경우 (When there is concern about response time to customers).
- Icon 2:** A computer monitor displaying a pie chart. **Text:** 부하가 큰 대용량 요청으로 데이터베이스가 넘치는 것을 알게 되는 경우 (When it becomes known that the database is overflowing due to high-volume, high-load requests).
- Icon 3:** A briefcase containing a green folder and a blue profile icon. **Text:** 데이터베이스 비용을 줄이고 싶을 때 (When you want to reduce database costs).

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

상태 정보를 위해 DynamoDB를 사용하는 경우

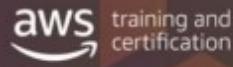
aws training and certification

사용 사례: 온라인 게임 사이트
문제: 더 빠른 DB 응답 필요

The diagram illustrates a client request flow. A user icon sends a request to a CloudFront icon, which then forwards it to a Web Server icon. The Web Server icon then connects to a Game Server icon. Above this flow, a blue cylinder icon labeled '세션 상태' (Session State) has a blue arrow pointing down to the Web Server icon. A red circle with a white exclamation mark is positioned next to the arrow, with the text '밀리초 단위의 응답 시간' (Response time in milliseconds) written below it, indicating the need for faster response times.

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

Amazon DynamoDB Accelerator





Amazon
DynamoDB
Accelerator

- 탁월한 성능
- 높은 확장성
- 완전관리형
- DynamoDB와 API 호환
- 보안

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

탁월한 성능

DynamoDB는 10밀리초 미만의 일관된 지연 시간을 제공합니다. DynamoDB plus DAX는 읽기 중심의 워크로드에 대한 초당 수백만 건의 요청에서 마이크로초 단위의 응답 시간을 제공합니다.

뛰어난 확장성

DAX는 온디맨드 조정 기능이 있습니다. 3노드의 DAX 클러스터로 시작하여 최대 10노드의 클러스터에 이르기까지 필요에 따라 용량을 늘릴 수 있습니다.

완전 관리형

DynamoDB와 마찬가지로 DAX는 완전관리형 서비스입니다. DAX는 프로비저닝, 설정 및 구성, 소프트웨어 패치 그리고 조정 작업 중 노드를 통한 데이터 복제 등 다양한 관리 작업을 처리합니다. DAX는 장애 탐지, 장애 복구, 소프트웨어 패치와 같은 일반적인 관리 작업들을 자동으로 실행합니다.

DynamoDB와 API 호환

DAX는 DynamoDB와 API 호환이 되기 때문에 작동 중인 애플리케이션 코드를 변경할 필요가 없습니다. DAX 클러스터를 프로비저닝하고 DAX 클라이언트 SDK를 사용하여 DAX 클러스터에서 기존 DynamoDB API 호출을 가리키면, DAX가 나머지 모든 작업을 처리합니다.

유연성

여러 DynamoDB 테이블에 대해 하나의 DAX 클러스터를 프로비저닝하거나 하나의 DynamoDB 테이블에 대해 여러 DAX 클러스터를 프로비저닝하거나 혹은 앞서 언급한 2가지 방법을 조합하여 프로비저닝할 수 있습니다.

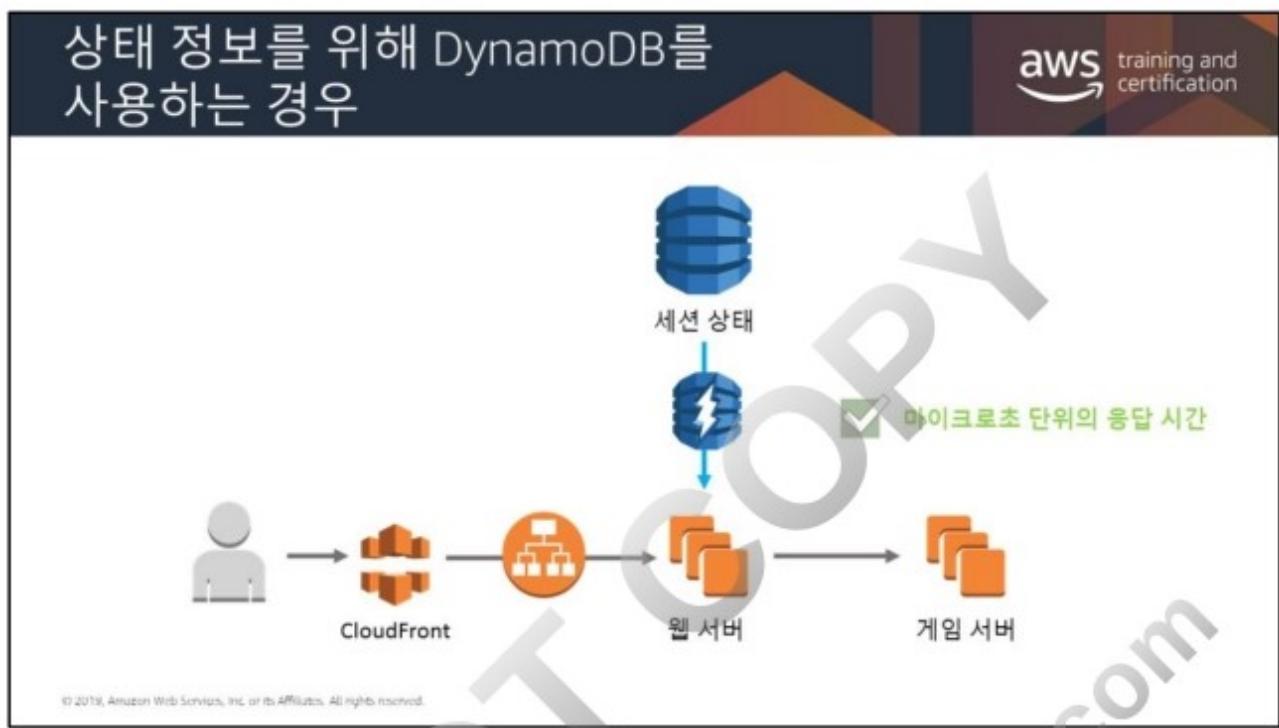
보안

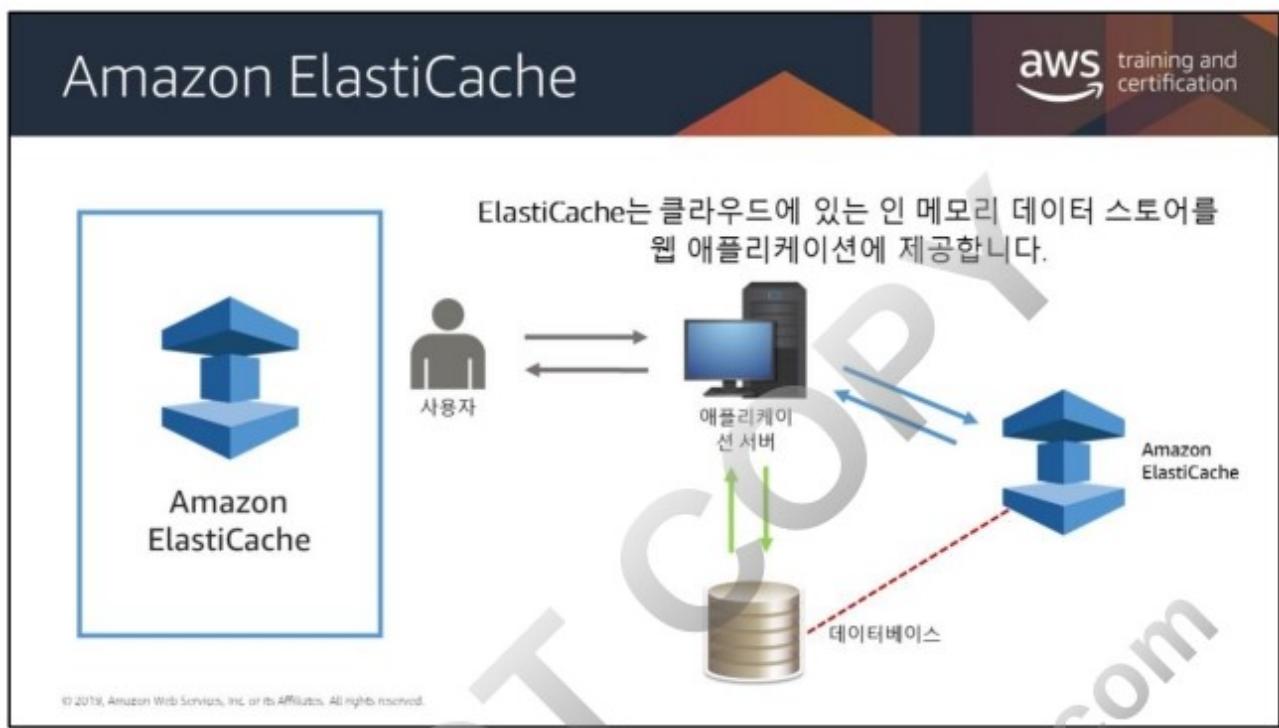
DAX는 AWS 서비스와 완벽하게 통합되어 보안을 강화합니다. AWS Identity and Access Management (IAM)를 사용하면 각 사용자에게 고유한 보안 자격 증명을 할당하고 서비스 및 리소스에 대한 각 사용자의 액세스를 제어할 수 있습니다. Amazon CloudWatch를 사용하면 시스템 전체의 리소스 사용률, 애플리케이션 성능 및 운영 상태를 파악할 수 있습니다. AWS CloudTrail과 통합하면 클러스터 구성의 변경 사항을 손쉽게 기록하고 감사할 수 있습니다. DAX는 기존 애플리케이션에서 안전하고 간편하게 액세스할 수 있도록 Amazon Virtual Private Cloud (VPC)를 지원합니다. 태깅은 DAX 클러스터를 관리하는 데 도움이 되는 가시성을 추가로 제공합니다.

캐시된 데이터를 검색하면 기존 DynamoDB 테이블에서 읽기 부하가 줄어듭니다. 따라서 프로비저닝된 읽기 용량을 줄이면서 전체 운영 비용을 절감할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

<https://aws.amazon.com/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>





Amazon ElastiCache는 클라우드에서 인 메모리 캐시를 배포, 운영, 조정하는 데 사용되는 웹 서비스입니다. ElastiCache는 비교적 느린 디스크 기반 데이터베이스에 전적으로 의존하기보다는 빠른 관리형 인 메모리 데이터 스토어에서 정보를 검색할 수 있는 기능을 지원함으로써 웹 애플리케이션의 성능을 향상합니다. 가능하다면 애플리케이션은 ElastiCache에서 데이터를 검색하고 캐시에서 데이터를 찾을 수 없을 때에는 데이터베이스를 참조하게 됩니다.

어떻게 작동합니까?

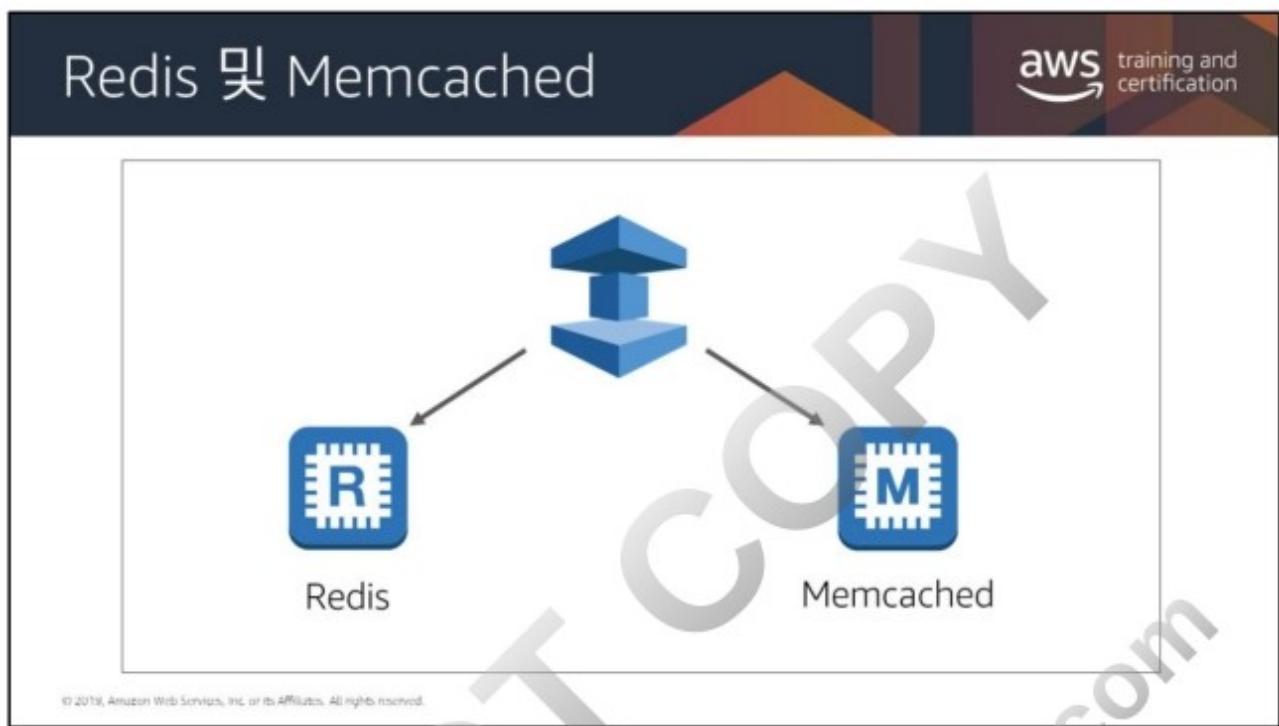
The diagram illustrates the architecture of an Amazon ElastiCache cluster. On the left, a blue 3D cube icon represents 'Amazon ElastiCache'. A line connects it to a rectangular box labeled '클러스터' (Cluster). Inside the cluster box is a 3x5 grid of blue squares, each labeled 'CACHE'. The bottom row of these squares is labeled '캐시 노드' (Cache Node). To the right of the cluster box is a bulleted list:

- 노드는 ElastiCache 배포에서 가장 작은 블록입니다.
- 각 노드에는 고유한 DNS (Domain Name Service) 이름 및 포트가 있습니다
- 완전관리형 서비스

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

캐시 노드는 ElastiCache 배포에서 가장 작은 빌딩 블록입니다. 이것은 다른 노드와 분리되어 존재하거나 혹은 다른 노드와의 일부 관계(클러스터라고도 함)에서도 존재할 수 있습니다.

Amazon ElastiCache는 완전 관리형 서비스이기 때문에 사용하지 않는 캐시 노드를 계속 실행할 필요가 없습니다. 더 많은 용량이 필요할 경우, 그러한 요구를 수용할 수 있도록 클러스터를 확장할 수 있습니다.

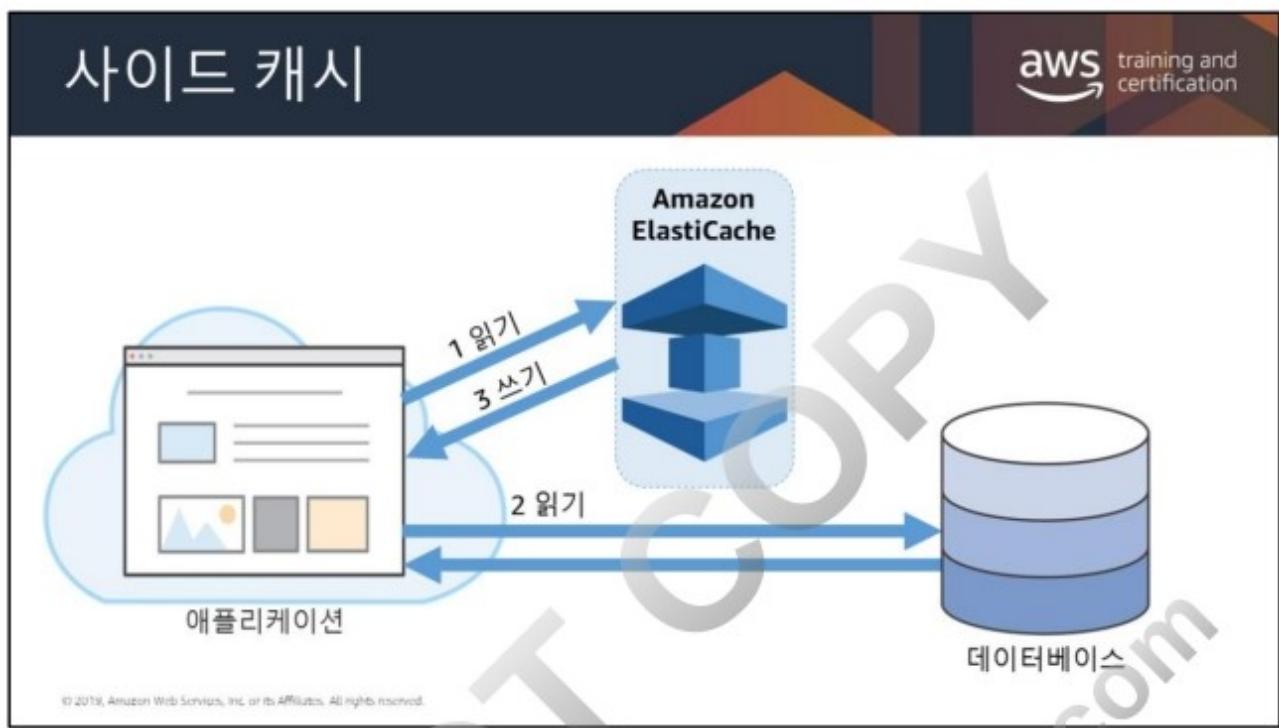


Memcached 사용 ElastiCache는 클러스터당 최대 20개의 노드까지 확장할 수 있으며, Redis용 ElastiCache는 데이터 액세스 성능 향상을 위해 최대 90개의 노드까지 확장할 수 있습니다. ElastiCache는 Amazon VPC를 지원하므로 사용 중인 노드에 대해 선택한 IP 범위로 클러스터를 격리할 수 있습니다.

ElastiCache는 다른 AWS 서비스에서 사용하는 것과 동일한 고안정성 인프라에서 실행됩니다. Redis 워크로드의 경우, ElastiCache는 자동 장애 조치가 적용된 다중 AZ를 통해 고가용성을 지원합니다. Memcached 워크로드의 경우, 데이터가 클러스터의 모든 노드에 분할되므로 수요가 증가할 때 더 많은 데이터를 더 잘 처리하도록 확장할 수 있습니다. ElastiCache를 사용하면 하드웨어 프로비저닝, 소프트웨어 패치, 모니터링, 장애 복구 및 백업과 같은 관리 작업을 더 이상 수행할 필요가 없습니다. ElastiCache는 워크로드를 계속 실행하기 위해 클러스터를 지속적으로 모니터링하기 때문에 사용자는 애플리케이션 개발에 집중할 수 있습니다.

비교	Memcached	Redis
DB 부하를 오프로드하는 단순 캐시	예	예
쓰기/스토리지를 위해 수평적으로 확장할 수 있는 기능	예	아니요
다중 스레드 성능	예	아니요
고급 데이터 유형	아니요	예
데이터 세트 정렬/순위 지정	아니요	예
Pub/Sub 기능	아니요	예
자동 장애 조치가 있는 다중 가용 영역	아니요	예
지속성	아니요	예

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



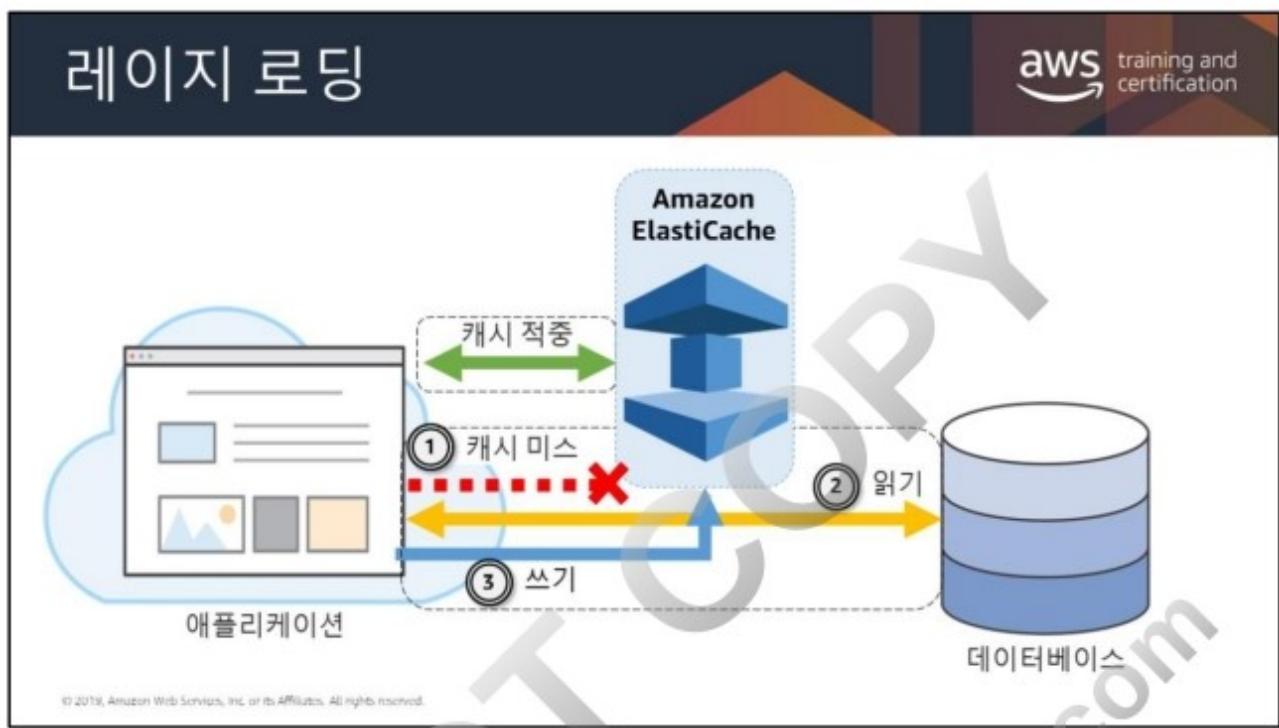
백엔드 데이터 스토어에 캐시를 사용하는 경우, 사이드 캐시가 가장 일반적으로 알려진 접근 방식일 것입니다. 정식 예에는 Redis와 Memcached가 모두 포함됩니다. 이러한 캐시는 기본 데이터 스토어와 분리된 범용 캐시이며, 워크로드 및 내구성 요구 사항에 따라 읽기 및 쓰기 처리량에 도움이 될 수 있습니다.

읽기 중심의 워크로드의 경우, 사이드 캐시는 일반적으로 다음과 같이 사용됩니다.

1. 지정된 키-값 쌍의 경우, 애플리케이션이 먼저 캐시에서 데이터 읽기를 시도합니다. 캐시가 데이터로 채워진 경우(캐시 적중), 해당 값이 반환됩니다. 그렇지 않은 경우, 2단계로 이동합니다.
2. 원하는 키-값 쌍을 캐시에서 찾을 수 없는 경우, 애플리케이션이 기본 데이터 스토어에서 데이터를 가져옵니다.
3. 애플리케이션이 데이터를 다시 가져와야 할 경우, 데이터가 존재하도록 2단계의 키-값 쌍이 캐시에 기록됩니다.

자세한 내용은 다음을 참조하십시오.

<https://aws.amazon.com/blogs/database/amazon-dynamodb-accelerator-dax-a-read-throughwrite-through-cache-for-dynamodb/>

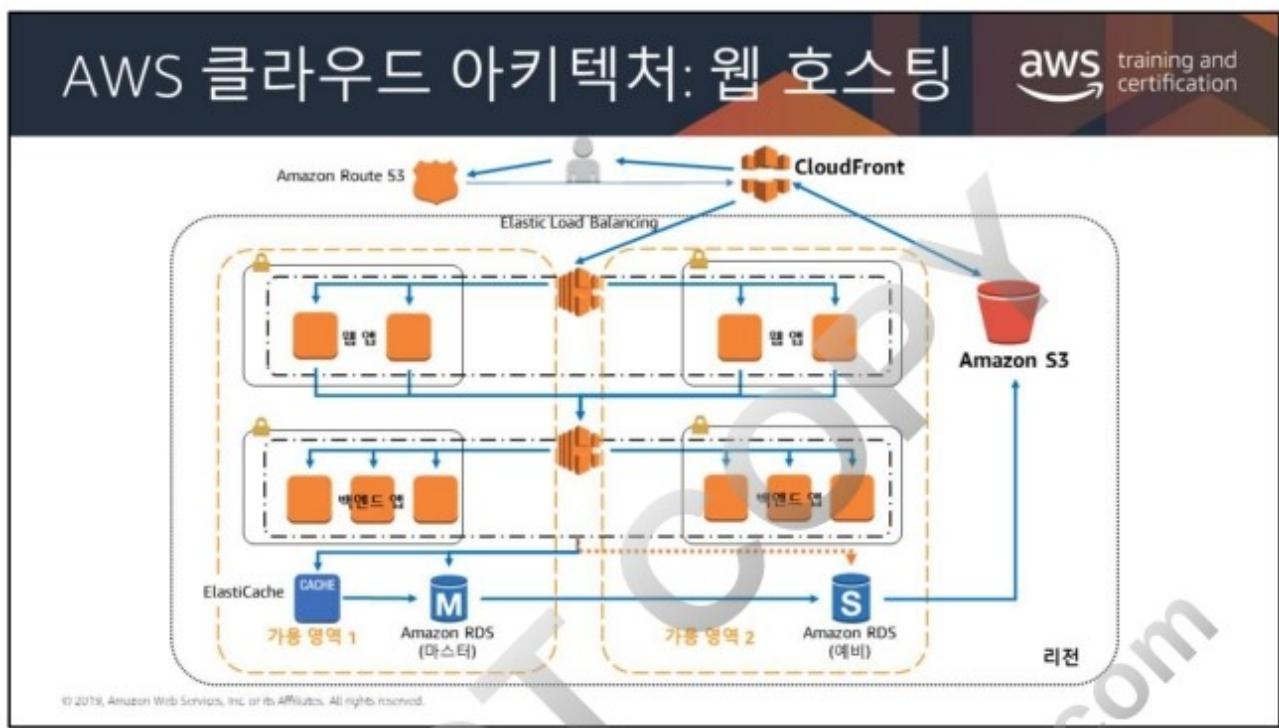


레이저 로딩은 필요할 때만 데이터를 캐시로 로드하는 캐싱 전략입니다. 이 배포에서 ElastiCache는 사용자의 애플리케이션과 액세스 대상의 데이터 스토어 또는 데이터베이스 사이에 위치합니다. 애플리케이션은 데이터를 요청할 때마다 먼저 ElastiCache 캐시로 요청을 보냅니다. 데이터가 캐시에 존재하며 최신일 경우, 캐시 적중이 발생하며 ElastiCache는 데이터를 애플리케이션으로 반환합니다. 그렇지 않으면 애플리케이션은 데이터를 애플리케이션에 반환하는 데이터 스토어에 데이터를 요청합니다. 이에 애플리케이션은 스토어에서 받은 데이터를 캐시에 작성합니다. 따라서 다음 번에 데이터 요청이 있을 때 해당 데이터를 좀 더 신속하게 검색할 수 있습니다.

레이저 로딩을 이용하면 요청된 데이터만 캐시됩니다. 한 번도 요청되지 데이터가 대부분이므로 레이저 로딩은 불필요한 데이터로 캐시를 채우는 상황을 방지할 수 있습니다. 다만 캐시 미스 페널티가 있습니다. 각각의 캐시 미스는 3회의 이동으로 나타납니다. 이로 인해 애플리케이션으로 데이터를 가져오는 작업이 눈에 띄게 지연될 수 있습니다. 또한 캐시 미스가 있을 때에만 데이터가 캐시에 작성될 경우, 데이터베이스에서 데이터가 변경될 때 캐시를 업데이트하지 않으므로 캐시의 데이터는 오래된 데이터가 될 수 있습니다. 이러한 문제를 해결하는 연속 쓰기 및 TTL 추가 전략에 대한 설명은 다음 시간에 다루기로 하겠습니다.



레이저 로딩은 기한 경과 데이터에 대해 허용되는 반면, 연속 쓰기는 데이터를 항상 최신 상태로 유지하며 다만 불필요한 데이터로 캐시를 채울 수 있습니다. TTL (Time To Live) 값을 각각의 쓰기에 추가하면 각 전략을 활용할 수 있으며 캐시를 데이터로 채우는 것을 대체로 방지할 수 있습니다. TTL은 키가 만료될 때까지 인 메모리 엔진에 따라 수 초 또는 수 밀리초의 수를 지정하는 정수값 또는 키입니다. 애플리케이션이 만료된 키를 읽으려고 시도할 때 이러한 시도는 캐시에서 데이터를 찾을 수 없는 것처럼 처리됩니다. 즉, 데이터베이스는 쿼리되며 캐시는 업데이트됩니다. 이렇게 하면 데이터를 기한 내에 업데이트할 수 있으며, 캐시의 값은 때때로 데이터베이스에서 새로 고쳐야 합니다.



기존 웹 호스팅 아키텍처는 아키텍처를 표시 계층, 애플리케이션 계층 및 지속성 계층으로 나눈 일반 3티어 웹 애플리케이션 모델을 구현합니다. 표시 계층, 애플리케이션 계층 또는 지속성 계층에서 호스트를 추가하면 확장성이 제공됩니다.

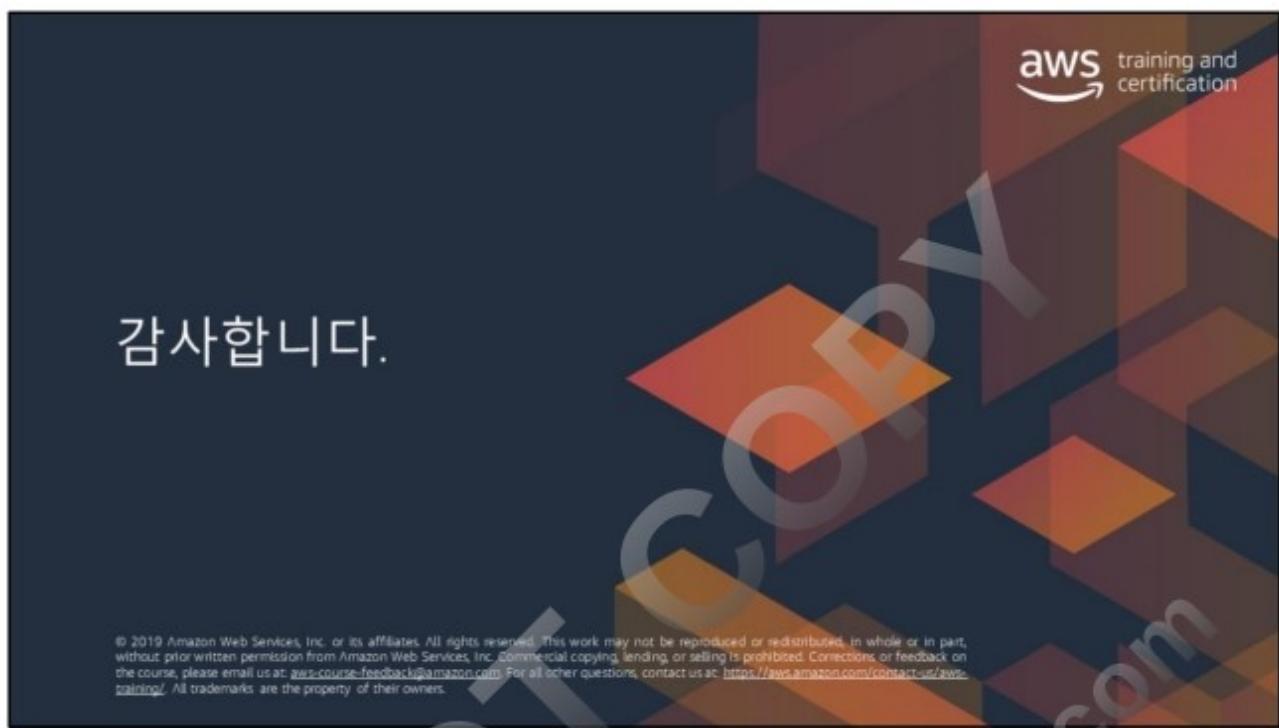
AWS 클라우드에서 웹 애플리케이션 호스팅

기존 웹 호스팅 아키텍처는 약간의 수정만 거쳐도 AWS 제품에서 제공되는 클라우드 서비스로 손쉽게 이식할 수 있습니다. 하지만 여기서 제기해야 할 첫 번째 문제는 기존 웹 애플리케이션 호스팅 솔루션을 AWS 클라우드로 옮겼을 때 어떤 가치가 있으느냐 하는 것입니다. 클라우드가 적합한 솔루션이라고 판단될 경우, 적절한 아키텍처가 필요합니다.

- *Amazon Route 53*은 도메인 관리 및 Zone APEX 지원을 간소화하기 위한 DNS 서비스를 제공합니다.
- *Amazon CloudFront*는 대용량 콘텐츠를 위한 엣지 캐싱을 제공합니다.
- *Elastic Load Balancing*은 이 디아이그램의 웹 서버 Auto Scaling 그룹으로 트래픽을 분산시킵니다.
- 외부 방화벽은 보안 그룹을 통해 모든 웹 서버 인스턴스로 이동되었습니다.

- 백엔드 방화벽은 모든 백엔드 인스턴스로 이동되었습니다.
- Amazon EC2 인스턴스의 앱 서버 로드 밸런서는 앱 서버 클러스터 전반에 걸쳐 트래픽을 분산시킵니다.
- *Amazon ElastiCache*는 앱에 대한 캐싱 서비스를 제공하여 데이터베이스 티어에서 부하를 제거합니다.

DO NOT COPY
zlagusdbs@gmail.com





모듈 11



아키텍처 측면에서의 필요성

이제 아키텍처는 수십만 명의 사용자들을 지원하지만 일부가 실패하면 전체 애플리케이션이 실패합니다. 종속성을 제거해야 합니다.

모듈 개요

- 결합 해제된 아키텍처
- Amazon SQS 및 Amazon SNS를 사용하여 결합 해제된 아키텍처 구축

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



“밀결합”이라는 용어가 의미하는 것은 무엇입니까?

www.example.com

웹 티어

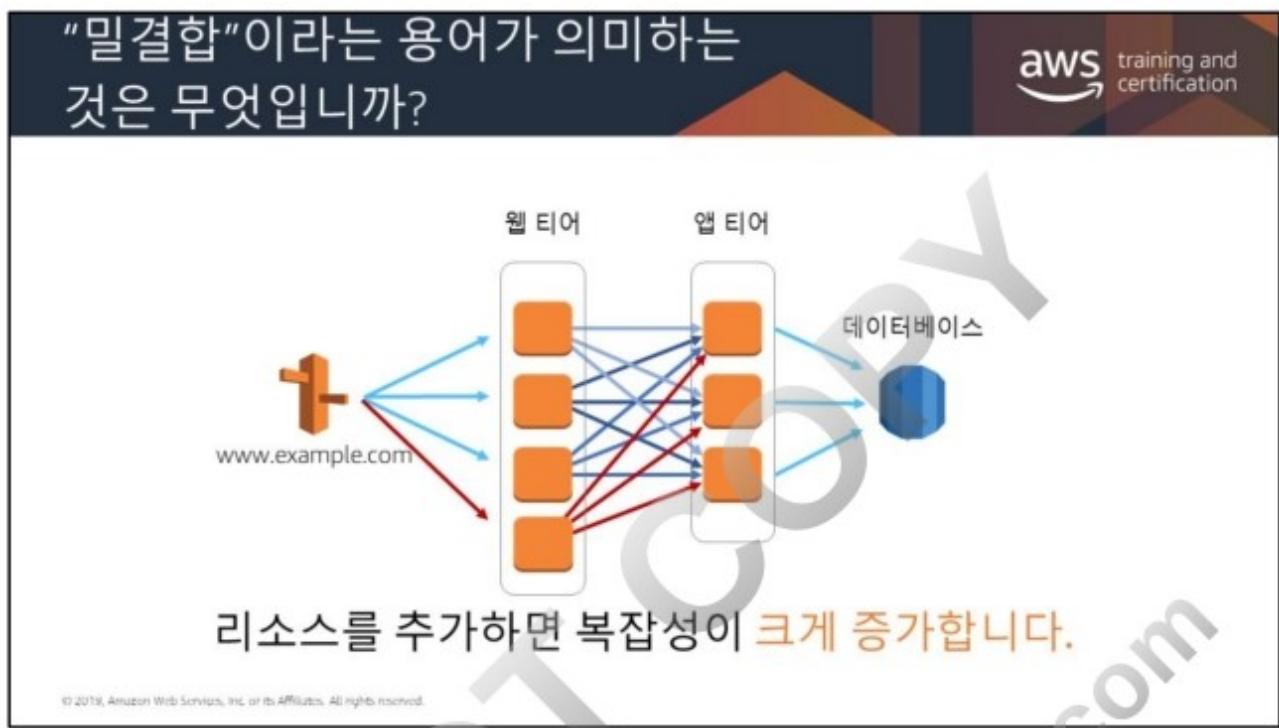
앱 티어

데이터베이스

구성 요소들은 서로 **강력하게 결합**되어 있습니다.

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

기존 인프라는 강력하게 통합된 서버 체인을 중심으로 움직이며 각 서버는 특정 목적을 가지고 있습니다. 이러한 구성 요소/계층의 하나에 장애가 발생하면 시스템에 치명적인 영향을 줄 수 있습니다. 또한, 이 때문에 규모 조정이 지연될 수 있습니다. 한 계층에 서버를 추가하거나 제거하는 경우, 연결된 모든 계층의 모든 서버가 적절하게 연결되어야 합니다.



구성 요소 하나의 변경이나 장애가 다른 구성 요소에 영향을 주지 않도록 상호 종속성을 줄여야 합니다. 느슨하게 결합된 경우, 관리형 솔루션을 시스템 계층 간의 중간자로 활용할 수 있습니다. 이렇게 하면 중간자가 구성 요소 또는 계층의 장애 및 규모 조정을 자동으로 처리합니다.

“밀결합”이라는 용어가 의미하는 것은 무엇입니까?

aws training and certification

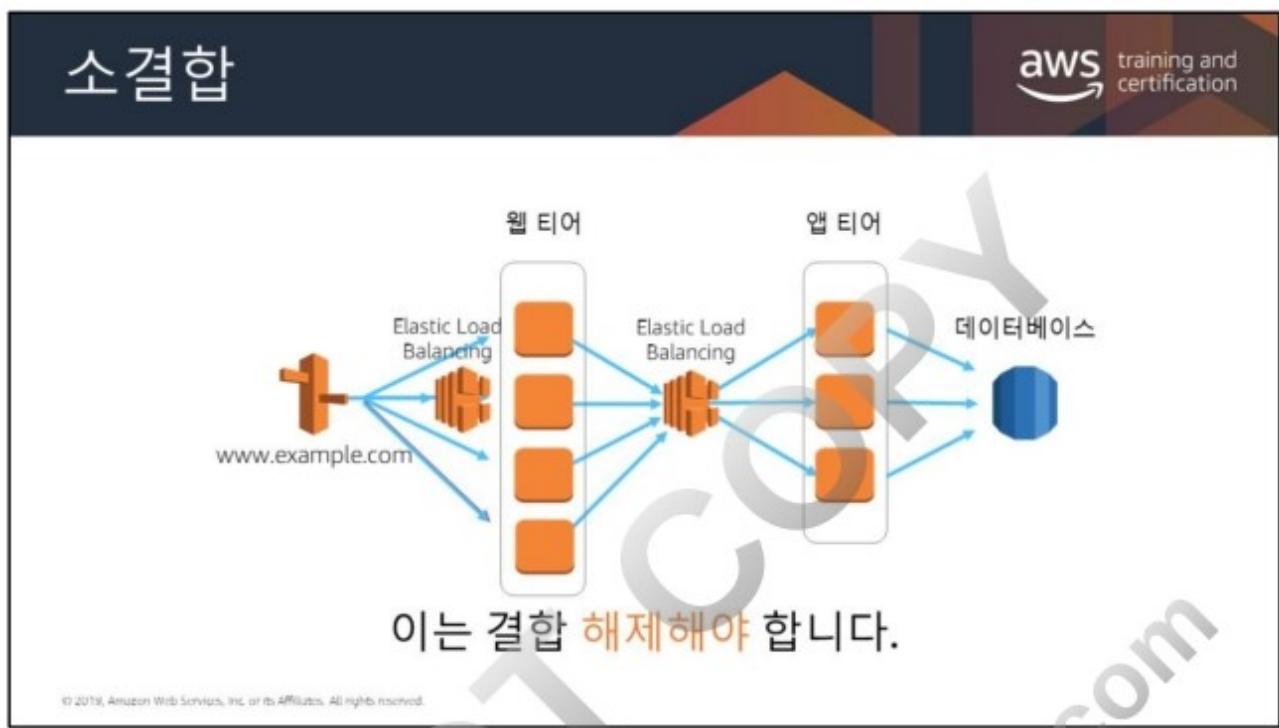
웹 티어 앱 티어

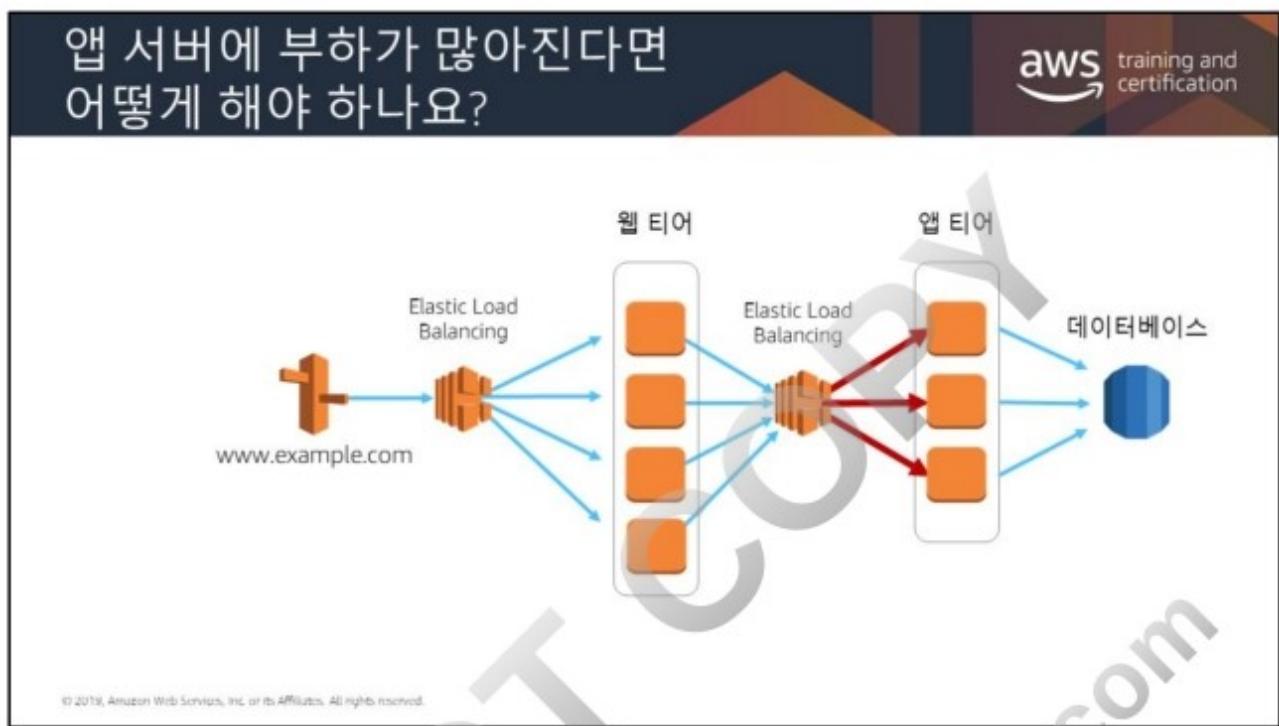
www.example.com

데이터베이스

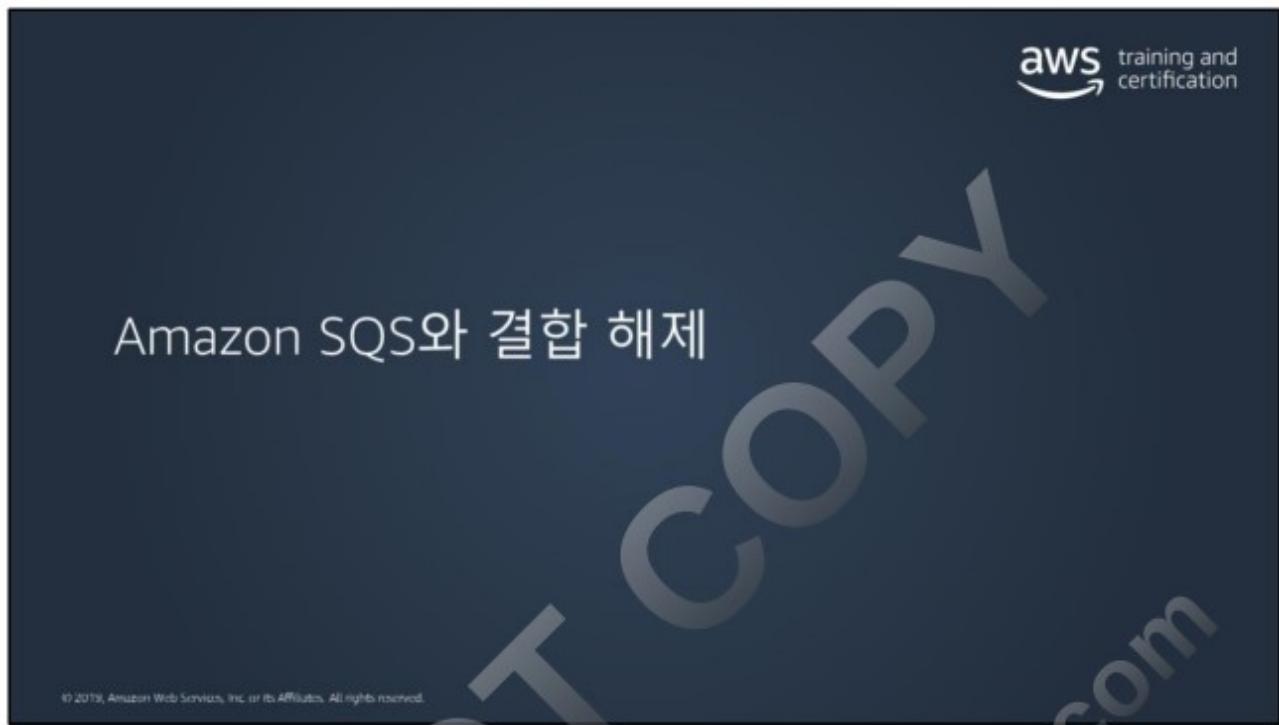
이는 결합 해제해야 합니다.

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





고객 주문을 처리하는 웹 애플리케이션을 고려합니다. 주문 처리 워크플로우의 한 가지 잠재적인 취약점은 해당 주문을 데이터베이스에 저장하는 데 있습니다. 기업은 모든 주문이 데이터베이스에 계속 유지되는 것을 새로운 요구 사항으로 기대합니다. 그러나 잠재적 교착, 경합 조건 또는 네트워크 문제가 발생할 경우, 해당 주문을 계속 유지할 수 없게 됩니다. 결국 해당 주문은 복원을 위한 어떤 수단도 없이 손실됩니다.



Amazon Simple Queue Service (Amazon SQS)



aws training and certification

완전 관리형 메시지 대기열 서비스

메시지는 처리 및 삭제될 때까지 저장됩니다.

발신자와 수신자 간 버퍼 역할을 담당

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

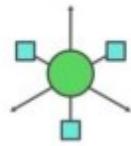
Amazon SQS는 관리 부담이 없으며 최소한의 구성으로도 바로 사용할 수 있는 완전 관리형 서비스입니다. 이 서비스는 방대한 규모로 작동하므로 하루에 수십억 건의 메시지를 처리할 수 있습니다. 컴퓨터, 네트워크 또는 가용 영역의 장애가 발생하더라도 메시지를 액세스할 수 있도록, 다수의 중복 가용 영역이 있는 고가용성의 단일 AWS 리전 내에 모든 메시지 대기열과 메시지를 저장합니다. 메시지는 동시에 전송하고 읽을 수 있습니다.

개발자는 Amazon SQS 대기열을 익명으로 또는 특정 AWS 계정과 안전하게 공유할 수 있습니다. IP 주소와 특정 시간으로 대기열 공유를 제한할 수도 있습니다. 서버 측 암호화(SSE)는 AWS Key Management Service (AWS KMS)에서 관리하는 키를 사용하여 Amazon SQS 대기열의 메시지 콘텐츠를 보호합니다. SSE는 Amazon SQS가 메시지를 수신하는 즉시 이를 암호화합니다. 이 메시지는 암호화된 형태로 저장되며 Amazon SQS는 권한이 있는 사용자에게 전송할 메시지만 복호화합니다.

소결합 실현(Amazon SQS 사용)



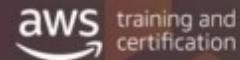
SQS 대기열을 사용하면 다음 사항들을 수행할 수 있습니다.



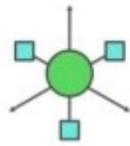
비동기식 처리를
사용하여 각 단계에서
신속하게 응답

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

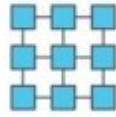
소결합 실현(Amazon SQS 사용)



SQS 대기열을 사용하면 다음 사항들을 수행할 수 있습니다.



비동기식 처리를
사용하여 각 단계에서
신속하게 응답

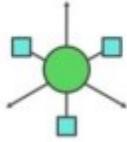
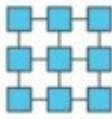
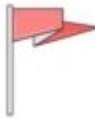


작업 인스턴스의 수를
늘려 성능 및 서비스 요구
사항 처리

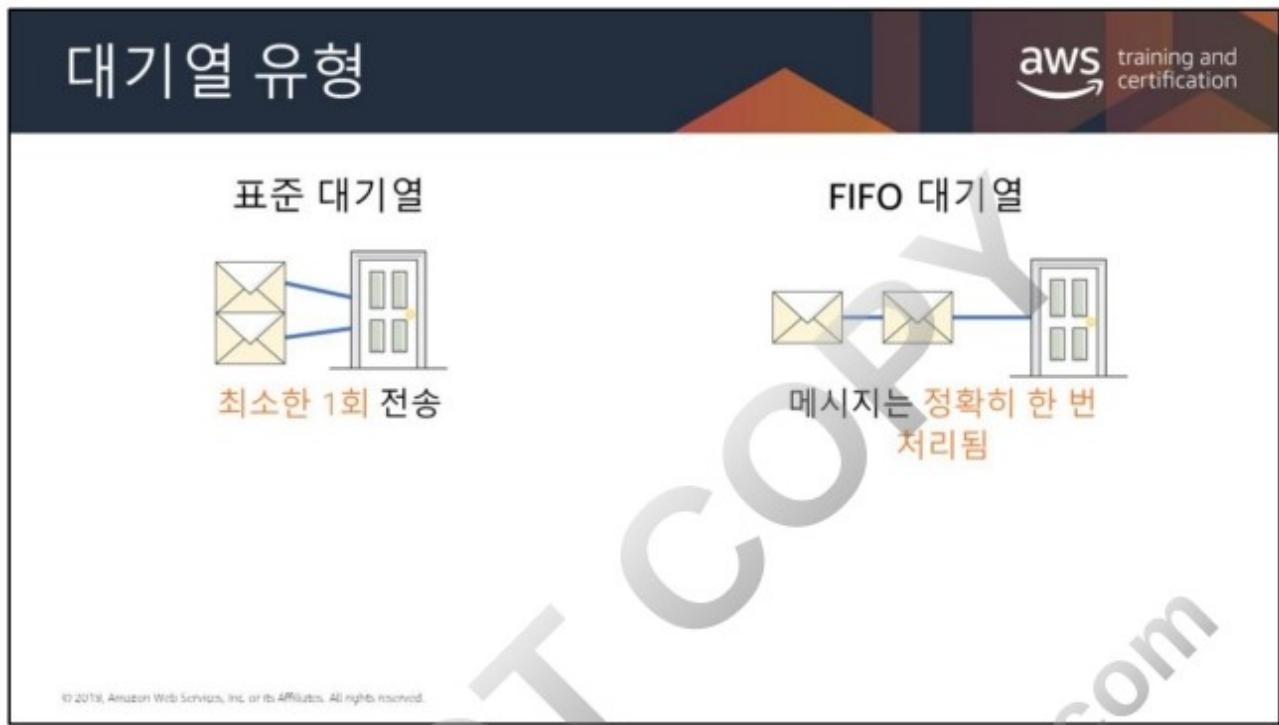
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

소결합 실현(Amazon SQS 사용)

SQS 대기열을 사용하면 다음 사항들을 수행할 수 있습니다.

- 비동기식 처리를 사용하여 각 단계에서 신속하게 응답
- 작업 인스턴스의 수를 늘려 성능 및 서비스 요구 사항 처리
- 메시지가 대기열에 남아 있기 때문에 실패한 단계에서 쉽게 복구

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



SQS 대기열은 2가지 유형 즉, 표준 대기열과 FIFO 대기열로 구분됩니다.

표준 대기열은 최소 1회 전송 및 최선의 정렬을 제공합니다.

최소 1회 전송이란 때때로 메시지 사본이 2개 이상 전송되는 것을 의미합니다.

최선의 정렬은 때때로 메시지가 전송된 순서와는 다르게 전송될 수 있음을 의미합니다.

FIFO(선입선출) 대기열은 메시지가 전송된 순서대로 정확히 한 번 처리될 수 있도록 설계되어 있습니다.

대기열 유형

aws training and certification

표준 대기열

최소한 1회 전송

API 작업당 거의 무한한 수의
초당 트랜잭션(TPS).

FIFO 대기열

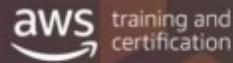
메시지는 정확히 한 번
처리됨

초당 300건의 메시지까지 지원

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

다만 표준 대기열은 최대 처리량을 제공하는 반면, FIFO 대기열은 초당 최대 300건의 메시지(초당 300건의 전송, 수신 또는 삭제 작업)를 지원합니다. 작업당 최대 10건의 메시지를 일괄 처리할 경우, FIFO 대기열은 초당 최대 3,000건의 메시지를 지원할 수 있습니다.

SQS 일반 사용 사례



The slide illustrates four common use cases for SQS:

- 작업 대기열**: Represented by a stack of three white squares on a green base.
- 버퍼 배치 작업**: Represented by a grid of colored squares (blue, magenta, yellow) with arrows indicating movement between them.
- 요청 오프로딩**: Represented by a circular icon with two overlapping arrows forming a cycle.
- 조정 트리거**: Represented by a bar chart with a pie chart on top, showing growth or distribution.

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

SQS 대기열을 사용하는 방법은 여러 가지가 있습니다.

작업 대기열: 동일한 양의 작업 일부를 동시에 처리하지 못할 수 있는 분산 애플리케이션의 구성 요소를 분리합니다.

배치 작업 버퍼링: 아키텍처에 확장성과 안정성을 더하고, 메시지를 손실하거나 지연 시간을 늘리지 않고 일시적인 볼륨 스파이크를 원활하게 처리합니다.

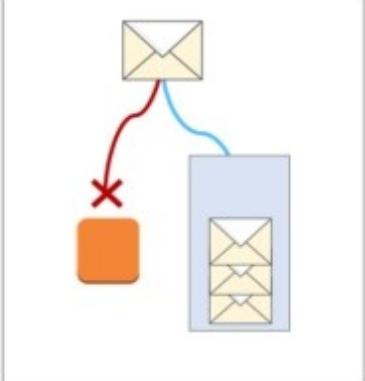
요청 오프로딩: 요청을 전송하여 대화식 요청 경로에서 속도가 느린 작업을 제거합니다.

Auto Scaling: Amazon SQS 대기열을 사용하면 애플리케이션의 로드를 결정하는데 도움이 됩니다. 또한 Auto Scaling과 결합 시 트래픽 볼륨에 따라 Amazon EC2 인스턴스의 수를 확장 또는 축소할 수 있습니다.

Amazon SQS 기능

aws training and certification

배달 못한 편지 대기열 지원



The diagram illustrates the concept of a Dead Letter Queue (DLQ). A blue rectangular box represents an Amazon SQS queue. An orange square icon with a red 'X' symbol is positioned below it, indicating a failed message. A red curved arrow points from the failed message to the queue, representing the message being rejected and placed into the DLQ.

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

배달 못한 편지 대기열(DLQ)은 처리되지 못한 메시지 대기열입니다. DLQ는 최대 처리 시도 수가 도달한 후에 메시지를 수신합니다. DLQ는 다른 Amazon SQS 대기열과 같습니다. 다른 SQS 대기열과 마찬가지로 DLQ로 메시지를 보내고 받을 수 있습니다. SQS API 및 SQS 콘솔에서 DLQ를 만들 수 있습니다.

Amazon SQS 기능

aws training and certification

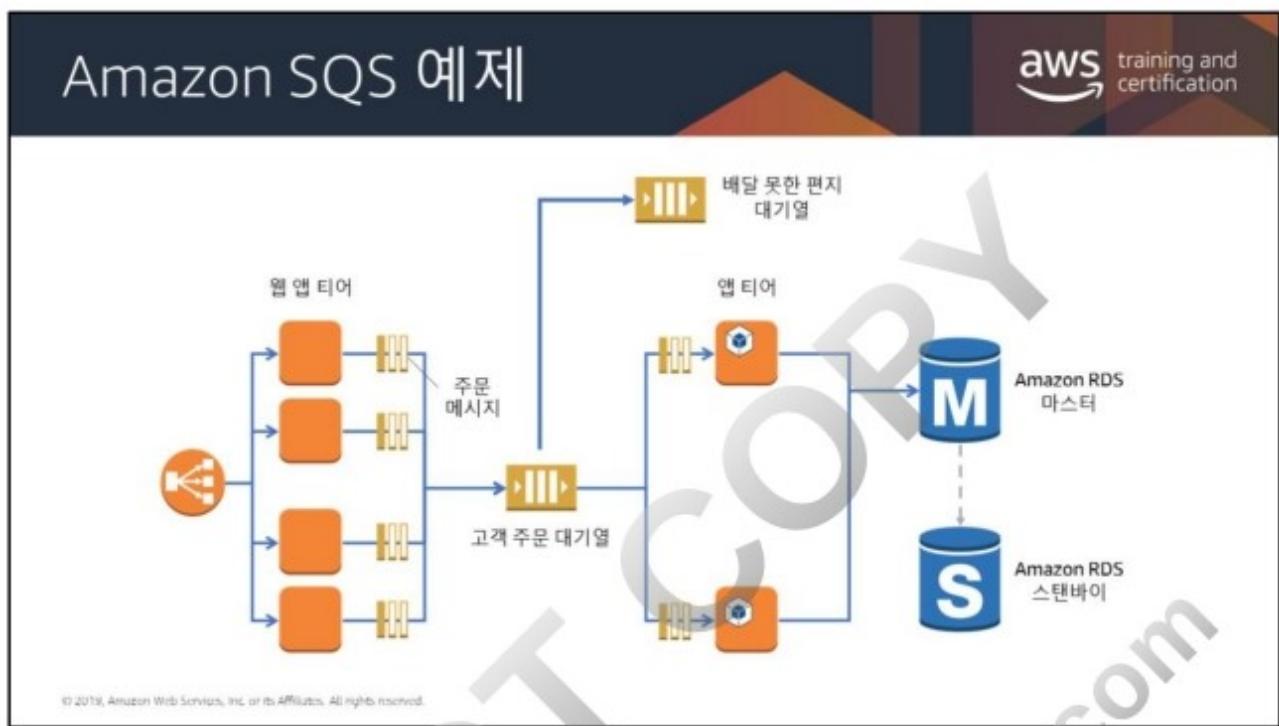
배달 못한 편지 대기열 지원 가시성 제한 시간

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

가시성 제한 시간이란 애플리케이션 구성 요소가 대기열에서 메시지를 가져온 후 해당 메시지가 다른 애플리케이션에는 보이지 않는 시간 간격을 가리킵니다. 메시지를 수신한 구성 요소는 일반적으로 이 가시성 제한 시간 동안 메시지를 처리한 다음, 이를 대기열에서 삭제합니다. 가시성 제한 시간은 여러 구성 요소가 같은 메시지를 처리하는 것을 방지합니다. 애플리케이션이 처리하는 데 시간이 더 필요한 경우, "보이지 않는" 제한 시간을 수정할 수 있습니다.



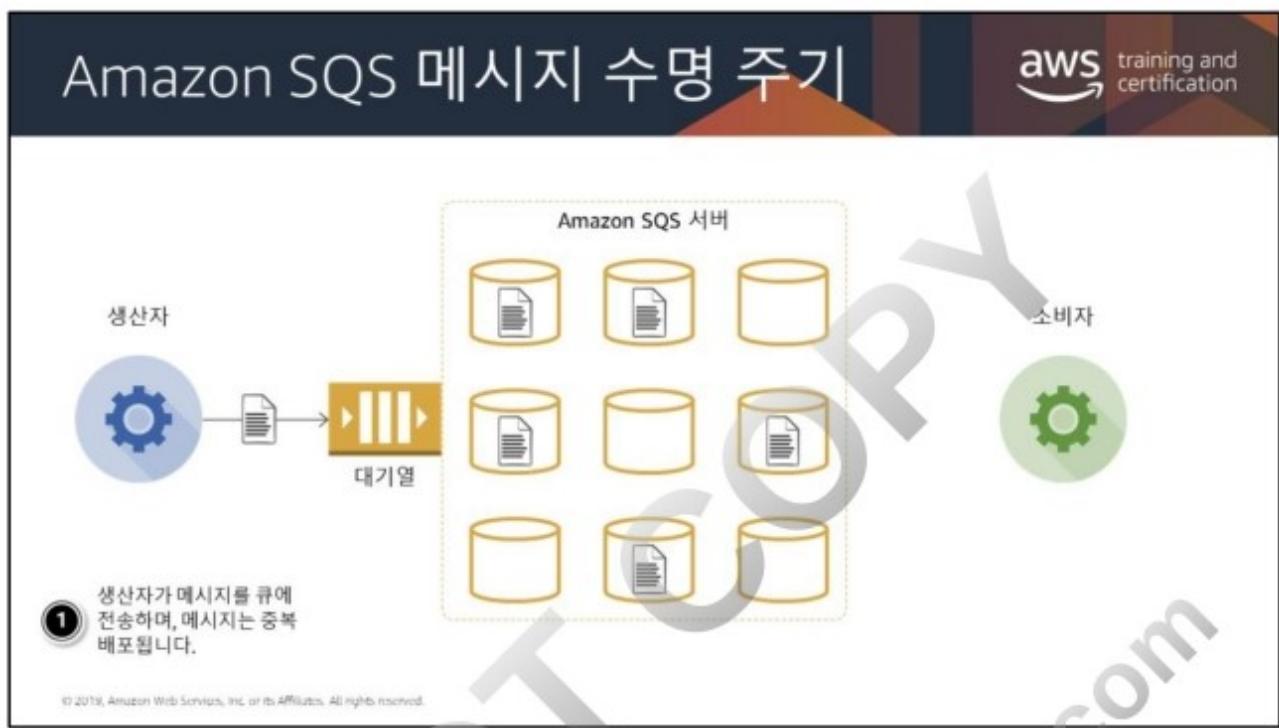
긴 폴링은 Amazon SQS 대기열에서 메시지를 검색하는 방법입니다. 짧은 폴링의 기본값은 폴링 중인 메시지 대기열이 비어 있더라도 즉시 반환됩니다. 다만 긴 폴링은 메시지가 메시지 대기열에 도달하거나 긴 폴링 제한 시간이 초과할 때까지 응답을 반환하지 않습니다. 긴 폴링을 사용하면 Amazon SQS 대기열에서 메시지가 제공되는 즉시 저렴한 방법으로 메시지를 검색할 수 있습니다.



SQS 대기열을 도입하여 주문 애플리케이션을 개선하는 방법을 알아봅니다. 대기열을 사용하면 처리 로직을 자체 구성 요소로 분리된 후, 웹 애플리케이션과 별도로 구분된 프로세스에서 실행할 수 있습니다. 이를 통해 시스템은 트래픽 급증에 보다 탄력적으로 대처할 수 있으며 비용 관리를 위해 필요한 만큼 신속하게 작업을 수행할 수 있습니다. 또한 주문을 메시지로 유지(임시 데이터베이스로 작동하는 대기열을 가지고)하기 위한 메커니즘을 갖추게 되었으며, 데이터베이스와의 트랜잭션의 범위를 스택 아래로 이동할 수 있습니다. 애플리케이션 예외 또는 트랜잭션 장애가 발생하면 SQS 대기열은 주문 처리를 중단하거나 Amazon SQS DLQ (Dead Letter Queue)로 리디렉션하여 나중에 다시 처리할 수 있습니다.

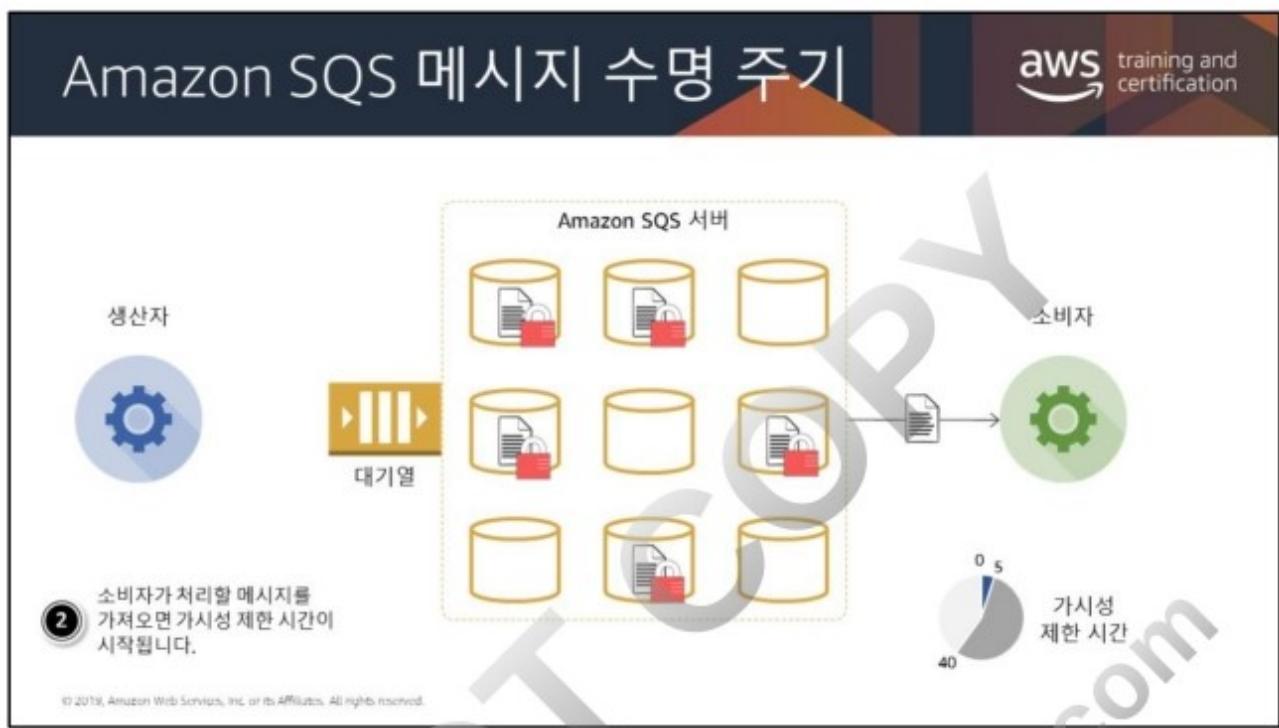
이 사용 사례에 관한 자세한 내용은

<https://aws.amazon.com/blogs/compute/building-loosely-coupled-scalable-c-applications-with-amazon-sqs-and-amazon-sns/>를 참조하십시오.



Amazon SQS (Amazon Simple Queue Service)는 웹 애플리케이션의 한 구성 요소가 생성하여 또 다른 구성 요소가 사용할 메시지를 웹 애플리케이션이 대기열에 넣을 수 있도록 허용하는 분산 대기열 시스템입니다. 대기열은 처리 대기 중인 메시지들의 임시 리포지토리이며 1~14 일간 메시지를 보관합니다(기본 설정된 보관 기간은 4일). Amazon SQS를 사용하면 애플리케이션의 구성 요소들을 분리하여 독립적으로 실행할 수 있습니다. 메시지는 형식에 관계없이 최대 256KB의 텍스트로 작성할 수 있습니다. Amazon SQS는 여러 생산자와 소비자가 같은 대기열에서 상호 작용하도록 지원합니다. Amazon SQS는 Amazon EC2, Amazon S3, Amazon ECS, AWS Lambda 및 Amazon DynamoDB 등 여러 AWS 서비스와 함께 사용할 수 있습니다.

Amazon SQS에서는 2가지 종류의 메시지 대기열을 제공합니다. 표준 대기열은 최대 처리량, 최선의 정렬 및 최소 1회 전송을 제공합니다. Amazon SQS FIFO 대기열은 메시지가 전송된 순서대로 정확히 한 번 제한된 처리량에 따라 처리될 수 있도록 설계되어 있습니다. 다음 시나리오는 생성에서 삭제까지 대기열에 있는 Amazon SQS 메시지의 수명 주기를 설명합니다. 여기서 생산자는 대기열에 메시지를 보내며 해당 메시지는 Amazon SQS 서버에 중복 배포됩니다.



소비자가 메시지를 처리할 준비가 완료되면 대기열에서 메시지를 검색합니다. 메시지는 처리하는 동안 대기열에 그대로 유지됩니다. 다른 소비자가 해당 메시지를 다시 처리하지 못하도록 Amazon SQS는 가시성 제한 시간을 설정합니다. 이는 Amazon SQS가 다른 소비자들이 해당 메시지를 수신하고 처리하는 것을 제한하는 시간을 의미합니다. 메시지의 가시성 제한 시간은 30초로 기본 설정됩니다. 이 사례에서는 제한 시간을 40초로 설정했습니다. 제한 시간은 최대 12시간입니다. 가시성 제한 시간이 만료되기 전에 소비자가 메시지를 삭제하지 않을 경우, 다른 소비자가 메시지를 볼 수 있게 되며 해당 메시지는 다시 처리될 수 있습니다. 일반적으로 가시성 제한 시간은 애플리케이션이 대기열에서 메시지를 처리하고 삭제하는 데 걸리는 최대 시간으로 설정해야 합니다.



Amazon SQS는 메시지를 자동으로 삭제하지 않습니다. Amazon SQS는 분산 시스템이므로 소비자가 메시지를 실제로 수신하는 것을 보장할 수 없습니다(예를 들면, 연결 문제가 있거나 소비자 애플리케이션의 문제가 있을 경우). 따라서 소비자는 수신하고 처리한 메시지를 대기열에서 삭제해야 합니다.

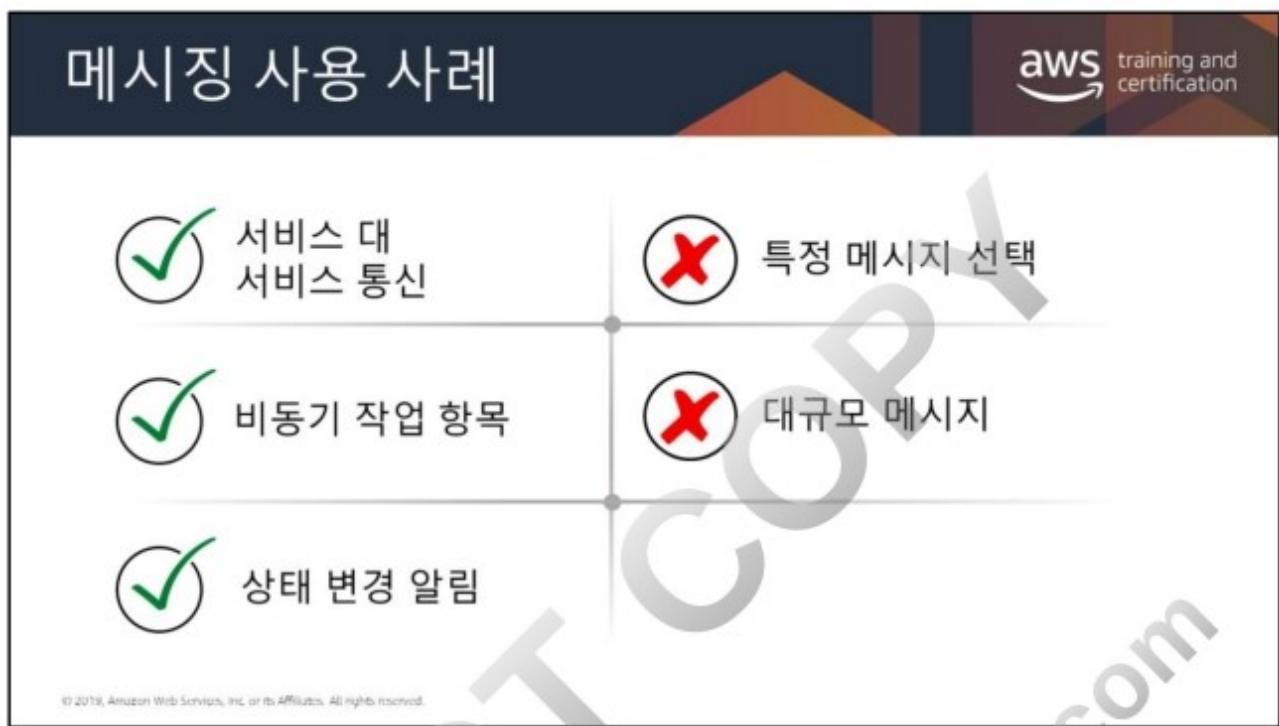
메시징 사용 사례

aws training and certification

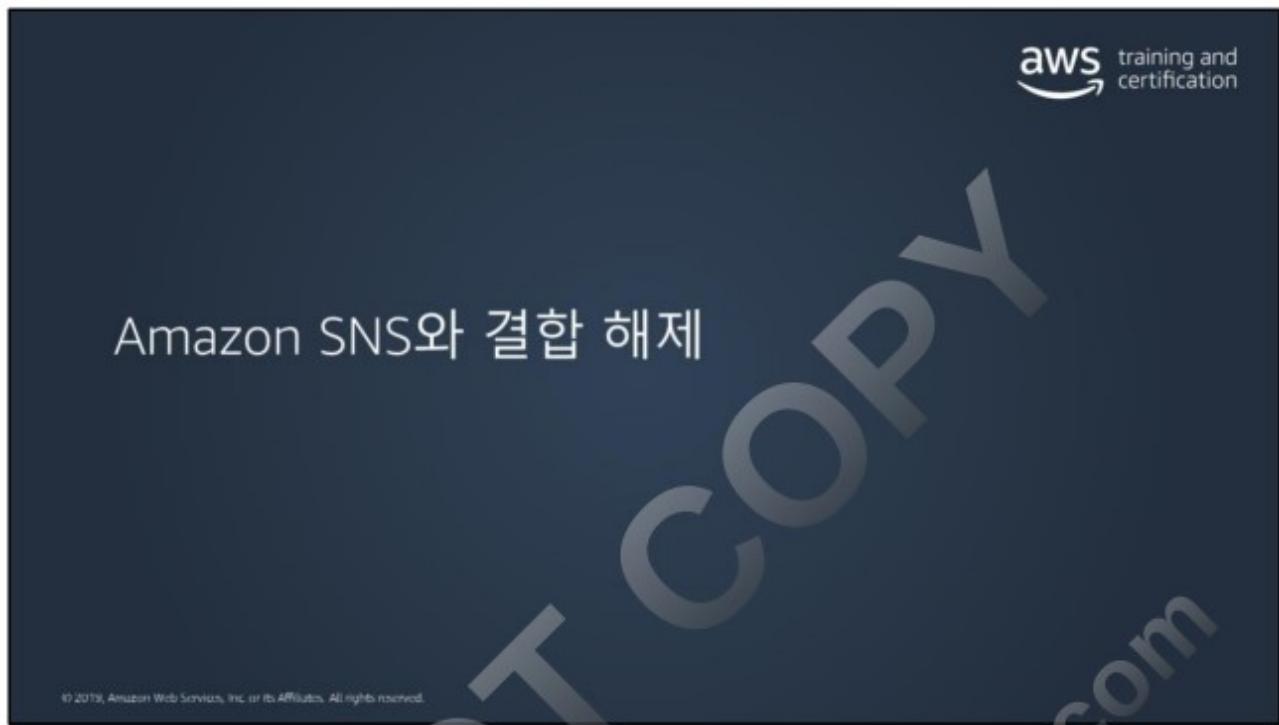
- 서비스 대
서비스 통신
- 비동기 작업 항목
- 상태 변경 알림

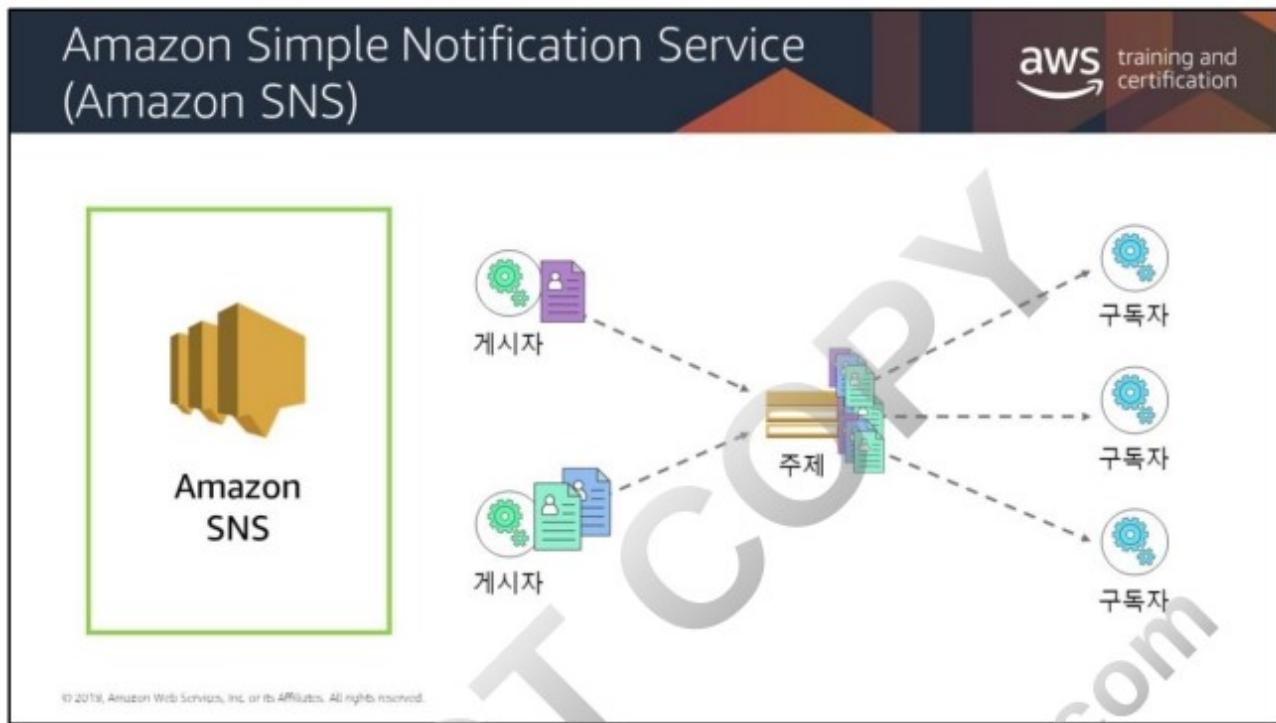
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

메시징 서비스가 매우 적합한 몇 가지 일반적인 사용 사례가 있습니다. 서로 통신해야 하는 2개의 서비스 또는 시스템이 있는 경우가 그렇습니다. 웹 사이트(프런트 엔드)가 고객 관계 관리(CRM)시스템(백엔드)의 고객 배송 주소를 업데이트해야 한다고 생각해 보십시오. 그 대신 대기열을 설정해 프런트 엔드 웹 사이트 코드가 대기열에 메시지를 전송하도록 하고, 백엔드 CRM 서비스가 메시지를 소비하도록 할 수도 있습니다. 또는 호텔 예약 시스템이 예약을 취소해야 하는데 이 프로세스에 시간이 많이 소요된다고 가정해 보겠습니다. 그 대신 대기열에 메시지를 넣고 일부 호텔 예약 시스템이 해당 대기열에서 메시지를 소비하고 비동기 취소를 수행하도록 할 수 있습니다. 메시징 서비스는 변경 알림에도 적합합니다. 일부 리소스를 관리하는 서비스와 이러한 리소스의 변경에 대한 업데이트를 수신하는 그 밖의 서비스가 있습니다. 예를 들어 인벤토리 시스템은 일부 품목이 부족해 주문이 필요할 때 알림을 게시할 수 있습니다.



특정 기술이 사용 사례에 적합하지 않은 경우를 아는 것도 중요합니다. 메시징에는 일반적으로 보게 되는 고유한 안티 패턴이 있습니다. 특정 속성 집합과 일치하거나 심지어 애드혹 논리적 쿼리와 일치하는 메시지를 대기열에서 선택적으로 수신하는 기능이 아쉬울 수 있습니다. 예를 들어 서비스는 특정 속성이 있는 메시지를 요청하는데, 서비스가 전송한 다른 메시지에 대한 응답이 포함되어 있기 때문입니다. 이로 인해 아무도 폴링하지 않고 결코 소비되지 않는 메시지가 대기열에 있는 시나리오가 발생할 수 있습니다. 대부분의 메시징 프로토콜과 구현은 메시지의 크기가 적절할 때(수십 또는 수백 KB) 가장 효과적입니다. 메시지 크기가 커진다면, Amazon S3와 같은 전용 스토리지 시스템을 사용하고 해당 스토어에 있는 객체에 대한 참조를 메시지 자체에 넣어 전달하는 것이 가장 좋습니다.





Amazon Simple Notification Service (Amazon SNS)는 클라우드에서 손쉽게 알림 기능을 설정, 작동 및 전송할 수 있는 웹 서비스입니다. 이 서비스는 "게시-구독"(pub-sub) 메시징 패러다임을 따르며 "푸시" 메커니즘을 사용하여 클라이언트에 알림을 전달합니다.

사용자는 주제를 생성하고 어떤 게시자 및 구독자가 주제와 통신할 수 있는지를 결정하는 정책을 정의함으로써 주제에 대한 액세스를 제어합니다. 게시자는 자신이 생성한 주제 또는 게시할 권한이 있는 주제로 메시지를 보냅니다.

게시자는 각 메시지에 특정 대상 주소를 포함하는 대신 메시지를 해당 주제로 전송할 수 있습니다. Amazon SNS는 주제와 해당 주제를 구독하는 구독자 목록을 일치시켜 각각의 구독자에게 메시지를 전송합니다.

각 주제는 Amazon SNS 엔드포인트를 식별하는 고유한 이름을 가지므로, 게시자는 메시지를 게시하고 구독자는 알림을 받도록 등록할 수 있습니다. 구독자는 구독하는 주제에 게시된 모든 메시지를 수신하며, 특정 주제를 구독하는 모든 구독자는 동일한 메시지를 수신합니다.

Amazon SNS는 암호화된 주제를 지원합니다. 암호화된 주제에 메시지를 게시할 때 Amazon SNS는 메시지를 암호화하기 위해 AWS KMS (<https://aws.amazon.com/kms/>)에서 제공하는 고객 마스터 키(CMK)를 사용합니다.

Amazon SNS는 고객이 관리하는 CMK와 AWS가 관리하는 CMK를 지원합니다. Amazon SNS가 메시지를 수신하는 즉시 서버에서 256비트 AES-GCM 알고리즘을 사용한 암호화가 진행됩니다. 메시지는 내구성을 위해 여러 가용 영역(AZ)에 암호화된 형식으로 저장되며, Amazon Simple Queue Service (Amazon SQS) 대기열, AWS Lambda 함수, HTTP 및 HTTPS 웹후크 등 구독 중인 엔드포인트에 전달되기 직전에 해독됩니다.

<https://aws.amazon.com/blogs/compute/encrypting-messages-published-to-amazon-sns-with-aws-kms/>

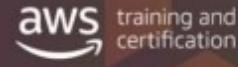
Amazon SNS 구독 유형



Amazon SNS

- 이메일
- HTTP/HTTPS
- SMS(문자 서비스) 클라이언트
- Amazon SQS 대기열
- AWS Lambda 함수

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



고객은 구독 요청 시 다음 전송 중 하나를 선택할 수 있습니다.

"Email" 또는 "Email-JSON" – 등록된 주소로 이메일 메시지가 전송됩니다.
Email-JSON은 알림을 JSON 객체로 전송하고, Email은 텍스트 기반
이메일로 전송합니다.

"HTTP" 또는 "HTTPS" – 구독자가 구독 등록 시 URL을 지정합니다. 알림은
HTTP POST를 통해 지정된 URL로 전송됩니다.

"SMS" – 등록된 전화번호로 SMS 문자 메시지가 전송됩니다.

"SQS" – 사용자는 SQS 표준 대기열을 엔드포인트로 지정할 수 있습니다.
Amazon SNS는 지정된 대기열에 알림 메시지를 추가합니다. 현재 FIFO
대기열은 지원되지 않습니다.

또한 메시지 사용자 지정을 처리하기 위해 AWS Lambda 함수에 메시지를 전송할
수 있으며, 메시지 지속성을 제공하거나 기타 AWS 서비스와 통신할 수도
있습니다.



Amazon SNS 알림을 사용하는 방법은 여러 가지가 있습니다.

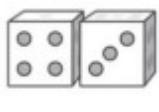
- 예를 들어, AWS Auto Scaling 그룹에 특정 변경 사항이 발생하는 등의 이벤트가 있을 경우, 사용자는 즉시 알림을 받을 수 있습니다.
- Amazon SNS를 사용하면 구독자에게 이메일 또는 SMS로 특정 뉴스 헤드라인을 푸시할 수 있습니다. 수신한 이메일 또는 SMS 문자에 흥미를 느낀 사람은 자세한 내용을 확인하기 위해 웹사이트를 방문하거나 애플리케이션을 시작할 수 있습니다.
- 업데이트가 가능함을 나타내는 알림을 앱으로 전송할 수 있습니다. 알림 메시지는 업데이트를 다운로드 및 설치하기 위한 링크를 포함할 수 있습니다.

Amazon SNS의 특성



aws training and certification

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

	하나의 게시된 메시지
	리콜 옵션이 없음
	HTTP/HTTPS 재시도
	주문 및 전달을 보장할 수 없음

모든 알림 메시지에는 게시 메시지가 하나만 포함됩니다.

Amazon SNS는 게시자가 주제에 게시한 메시지를 그 순서 그대로 전송하려고 시도합니다. 하지만 네트워크 문제로 인해 구독자에게 순서가 바뀌어 전송될 가능성도 없진 않습니다.

메시지가 성공적으로 전송되면, 이를 회수할 방법은 없습니다.

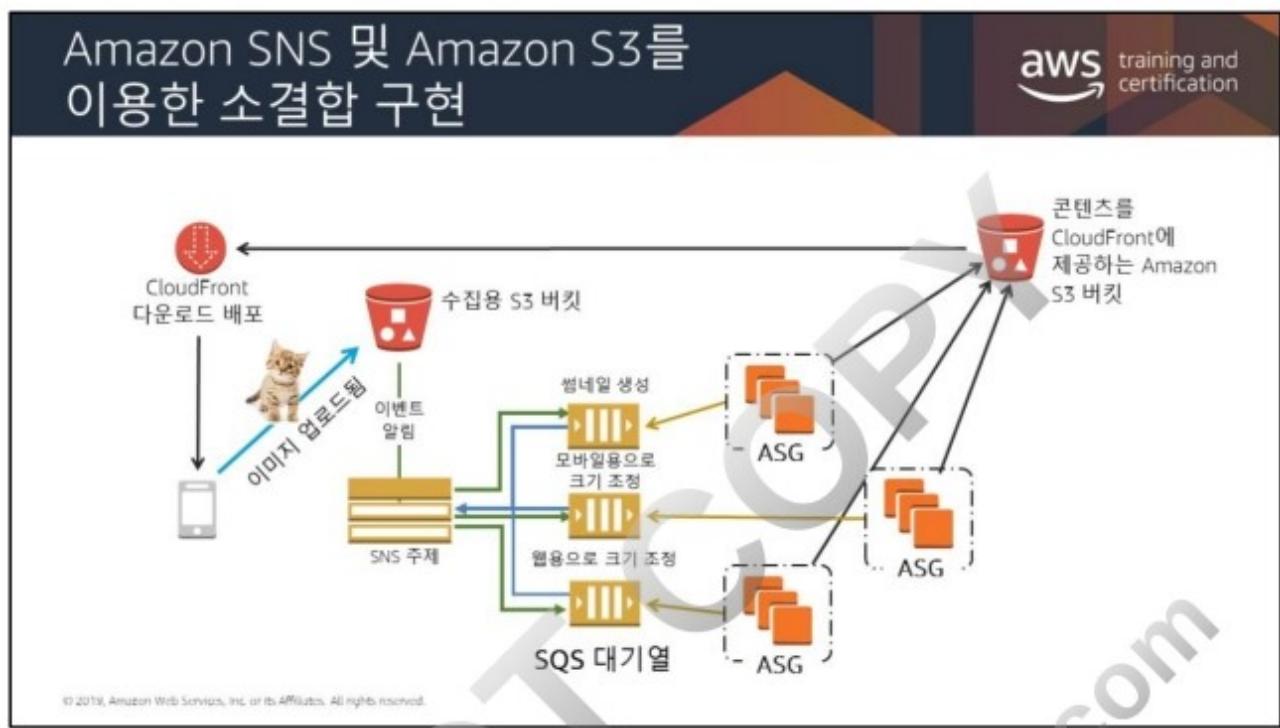
Amazon SNS 전송 정책을 사용해 재시도 패턴(선형, 기하학, 지수 백오프), 최대/최소 재시도 지연 및 기타 파라미터를 제어할 수 있습니다.

메시지가 유실되지 않도록 Amazon SNS에 게시된 모든 메시지는 여러 서버와 데이터 센터에 걸쳐 중복 저장됩니다.

Amazon SNS는 가장 크고 수요가 가장 많은 애플리케이션의 요구 사항에 부합하도록 설계되어, 애플리케이션이 언제든 무제한의 메시지를 게시할 수 있습니다.

Amazon SNS를 이용하면 서로 다른 디바이스의 애플리케이션과 최종 사용자가 모바일 푸시 알림(Apple, Google 및 Kindle Fire 디바이스), HTTP/HTTPS, Email/Email-JSON, SMS 또는 Amazon Simple Queue Service (SQS) 대기열, AWS Lambda 함수 등을 통해 알림을 수신할 수 있습니다.

Amazon SNS는 액세스 제어 메커니즘을 갖추고 있어 주제와 메시지가 무단 액세스로부터 확실하게 보호됩니다. 주제의 소유자가 주제 별로 일정한 정책을 수립해 주제를 게시하거나 구독할 수 있는 대상을 제한할 수 있습니다. 또한 전송 메커니즘을 HTTPS로 지정하여 알림을 암호화할 수도 있습니다.



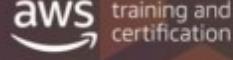
SNS에서는 주제를 사용하여 메시지 게시자를 구독자로부터 분리하고 여러 수신자에 대한 메시지를 동시에 팬아웃하며 애플리케이션에서 폴링을 제거할 수 있습니다.

SNS를 사용하면 단일 계정 내에서 메시지를 전송하거나 상이한 계정 내 리소스로 메시지를 전송하여 관리 경리를 생성할 수 있습니다.

Amazon EC2, Amazon S3 및 Amazon CloudWatch와 같은 AWS 서비스는 사용자의 SNS 주제로 메시지를 게시하여 이벤트 중심의 컴퓨팅 및 워크플로우를 트리거할 수 있습니다.

이 대체 시나리오에서는 Amazon S3에 이미지를 업로드하면 이벤트 알림이 트리거되고, 자동으로 메시지가 SNS 주제에 전송됩니다.

Amazon SNS는 Amazon SQS와 어떻게 다릅니까?



	Amazon SNS (게시자/구독자)	Amazon SQS (생산자/소비자)
메시지 지속성	아니요	예
전송 메커니즘	푸시(수동적)	풀링(능동적)
생산자/소비자	게시/구독	송신/수신
배포 모델	일대다	일대일

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

- Amazon SNS를 사용하면 애플리케이션에서 푸시 메커니즘을 통해 타임 크리티컬 메시지를 여러 구독자에게 전송할 수 있습니다.
- Amazon SQS는 풀링 모델을 통해 메시지를 교환합니다. 즉 전송 및 수신 구성 요소가 결합 해제됩니다.
- Amazon SQS는 애플리케이션의 분산 구성 요소를 위한 유연성을 제공하므로 각 구성 요소를 동시에 사용하지 않고도 메시지를 송신 및 수신할 수 있습니다.





모듈 12

aws training and certification

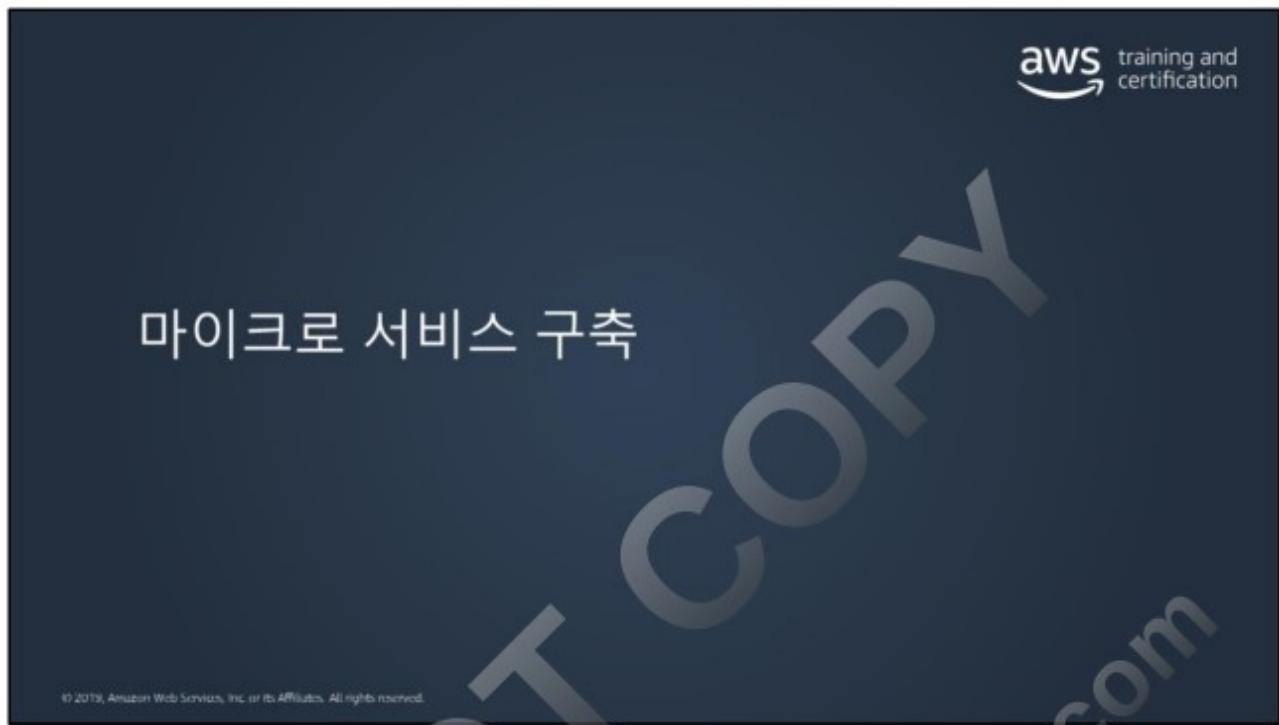
아키텍처 관련 문제

모놀리식 아키텍처가 분리되면 개별 구성 요소가 별도의 팀에서 관리되며, 이에 따라 한 팀에서 구성 요소를 변경하는 경우 충돌이 발생할 수 있습니다.

모듈 개요

- 마이크로 서비스 구축
- 컨테이너 서비스
- 서비스 환경 구현

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

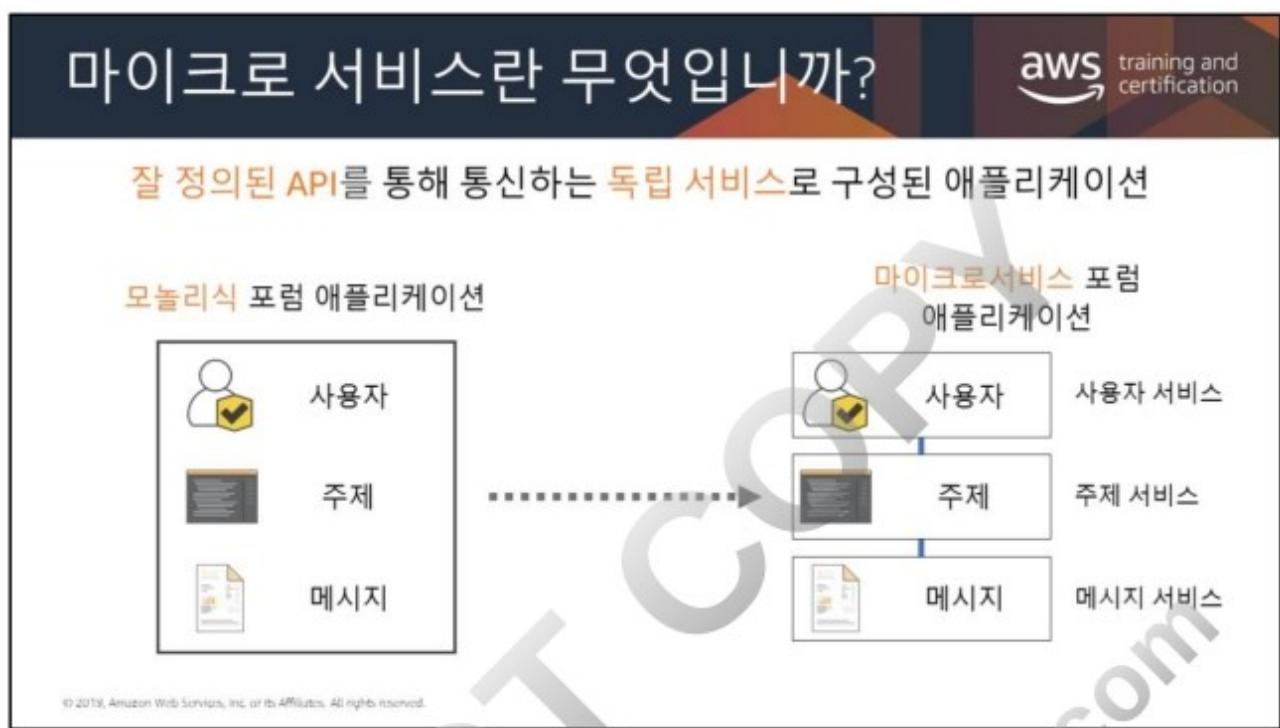


The screenshot shows a slide titled "마이크로 서비스란 무엇입니까?" (What is a microservice?). It features the AWS logo and the text "training and certification". Below the title, it says "잘 정의된 API를 통해 통신하는 독립 서비스로 구성된 애플리케이션" (Application composed of independent services communicating via well-defined APIs). A large watermark "NOT COPY" is diagonally across the slide. At the bottom left, there is a small copyright notice: "© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved."

재래식 모놀리식 애플리케이션에는 서로 긴밀히 결합된 모든 이동 및 작동 요소가 포함되어 있습니다. 한 요소에 장애가 발생할 경우 전체 애플리케이션이 중단됩니다. 수요가 급증할 경우 전체 아키텍처를 확장해야 합니다. 모놀리식 애플리케이션에 기능을 추가하는 과정은 시간이 흐를수록 복잡해집니다. 코드 베이스의 각 요소는 서로 잘 조화되어야 제대로 동기화됩니다.

마이크로서비스 아키텍처에서는 애플리케이션이 각 애플리케이션 프로세스를 서비스로 실행하는 독립적 구성 요소로 구축됩니다. 이러한 서비스는 경량 API를 사용하여 잘 정의된 인터페이스를 통해 통신합니다. 서비스는 비즈니스 기능을 위해 구축되고, 각 서비스는 단일 기능을 수행합니다. 서비스가 독립적으로 실행되므로 각 서비스를 업데이트, 배포 및 조정하며 애플리케이션의 특정 기능의 수요를 충족할 수 있습니다.

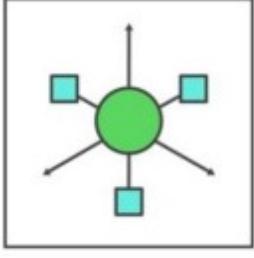
AWS 기반 마이크로서비스 아키텍처에 대한 자세한 내용은 다음을 참조하십시오.
<https://aws.amazon.com/microservices/>



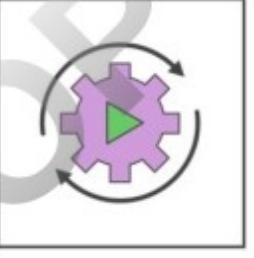
마이크로서비스의 특성

aws training and certification

자율적



전문적



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

자율적

마이크로서비스 아키텍처의 각 구성 요소 서비스는 다른 서비스의 기능에 영향을 미치지 않고 개발, 배포, 운용 및 조정할 수 있습니다. 서비스가 다른 서비스와 어떤 코드 또는 구현도 공유할 필요가 없습니다. 개별 구성 요소 사이의 모든 통신은 잘 정의된 API를 통해 이루어집니다.

전문적

각 서비스는 일련의 기능을 제공하도록 설계되었으며 집중적으로 특정 문제를 해결합니다. 시간이 흐르면서 개발자가 서비스에 더 많은 코드를 기여하고 서비스가 복잡해지면 이를 더 작은 서비스로 분할할 수 있습니다.



컨테이너 솔루션을 생성하는 데 도움이 필요한 경우, AWS Container Competency 프로그램을 고려하십시오.

AWS 컨테이너 컴피던시는 AWS 컨테이너에서 워크로드를 실행하는 고객의 능력을 개선할 수 있도록 AWS와 통합되는 제품 또는 솔루션이 있는 APN 기술 파트너를 인정합니다. 이를 통해 사용자는 컨테이너의 모니터링, 로깅, 보안뿐 아니라 컨테이너에서 오케스트레이션 및 일정 예약, 인프라, 애플리케이션 빌드/테스트, 배포를 최적화할 수 있습니다.

APN 파트너가 AWS 컴피던시를 획득하려면 산업별 기술과 관련된 엄격한 기술적 검증을 거쳐야 합니다. 이러한 검증 덕에 고객은 AWS 파트너 네트워크 내 수십만 개의 APN 파트너 솔루션을 자신 있게 선택할 수 있습니다.

컨테이너에 대해 알아보겠습니다.

aws training and certification

The infographic features three icons: a yellow network-like icon labeled '반복 가능' (Replicable), an orange briefcase icon labeled '독립형 실행 환경' (Independent execution environment), and a yellow alarm clock icon labeled 'VM보다 더 빠른 처리 속도' (Faster processing speed than VM). A large diagonal watermark 'DO NOT COPY' and 'zlagusdbs.com' is overlaid across the slide.

반복 가능

독립형 실행 환경

VM보다 더 빠른 처리 속도

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

마이크로서비스 지향 아키텍처의 이점은 강의가 진행되는 이 시점에도 여전히 실행 환경으로 가상 머신을 사용하고 있는 인프라 수준까지 확산되어야 합니다. 클라우드에서 VM을 실행하면 동적이고 탄력적인 환경을 구현할 수 있지만 마찰을 더 줄여야 할 수 있습니다. 클라우드에서 VM을 실행하면 동적이고 탄력적인 환경을 구현할 수 있지만 마찰을 더 줄여야 할 수 있습니다.

컨테이너란 무엇입니까?

aws training and certification

컨테이너

The diagram illustrates the components of a container. It shows a yellow rectangular box labeled "컨테이너" (Container) containing four items: "애플리케이션" (Application), "Dockerfile" (represented by a blue icon with code), "구성" (Configuration), and "OS에 연결" (Connect to OS) (represented by a brown icon).

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

컨테이너는 리소스 격리 프로세스에서 애플리케이션과 종속 항목을 실행하게 해주는 운영 시스템 가상화 방법입니다. 컨테이너를 사용함으로써 애플리케이션의 코드, 구성 및 종속 항목을 사용이 간편한 빌딩 블록으로 손쉽게 패키징할 수 있으며 환경 일관성, 운영 효율성, 개발자 생산성, 버전 제어를 제공합니다.

컨테이너 이미지는 컨테이너가 사용할 수 있는 파일 시스템의 스냅샷입니다. 예를 들어, Debian 운영 체제를 컨테이너 이미지로 보유할 수 있습니다. 그러한 컨테이너를 실행하면 컨테이너에서 유효하게 Debian 운영 체제를 사용하게 되는 것입니다. 또한 모든 코드 종속성을 컨테이너 이미지에 패키징하고 이를 코드 아티팩트로 사용할 수도 있습니다. 일반적으로 컨테이너 이미지는 공간 측면에서 가상 머신보다 훨씬 작습니다. 컨테이너 실행은 수백 밀리초밖에 걸리지 않습니다.

따라서 컨테이너를 사용하면 고속이고 휴대 가능하며 인프라에 구애받지 않는 실행 환경을 사용할 수 있습니다.

컨테이너는 어떤 문제를 해결할 수 있습니까?

aws training and certification

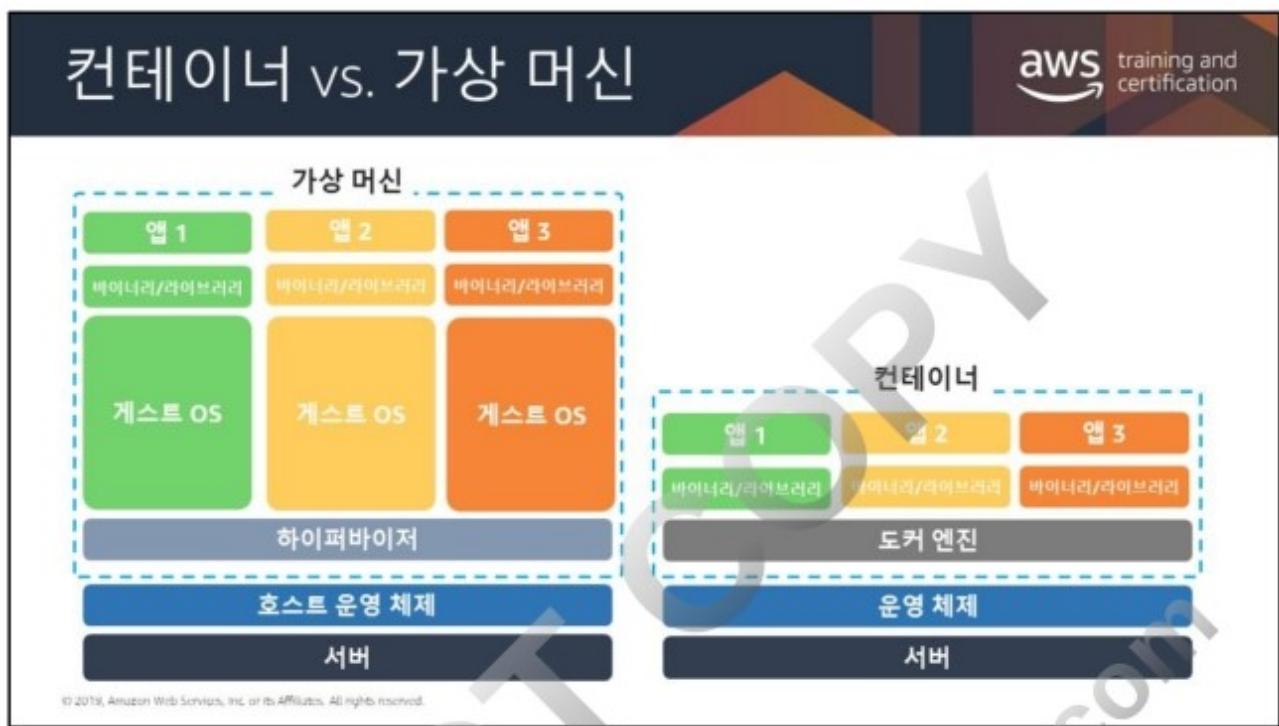
다양한 환경에서 소프트웨어를 안정적으로 실행

개발자 워크스테이션 프로덕션 테스트 환경

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

컨테이너는 애플리케이션을 배포 환경에 관계없이 빠르고 안정적으로 일관되게 배포할 수 있도록 해줍니다. 컨테이너는 리소스에 대한 좀 더 세분화된 제어가 가능하여 인프라의 효율성을 개선합니다.

사전 제작된 컨테이너 솔루션을 찾고 있다면, Amazon ECS 콘솔 또는 AWS Marketplace를 통해 AWS Marketplace for Containers에 방문해 개별 소프트웨어 판매자의 컨테이너 제품을 찾아 구매합니다. 이 제품들은 Amazon ECS, AWS Fargate, Amazon EKS 등 Docker와 호환되는 AWS 컨테이너 서비스에서 실행되는 검증된 상용 지원 제품입니다. 고성능 컴퓨팅, 보안 및 개발자 도구 등 카테고리별로 제품을 선택할 수 있습니다. 또한 컨테이너 애플리케이션을 관리, 분석 또는 보호하는 SaaS 제품도 있습니다. 자세한 내용은 <https://aws.amazon.com/marketplace/features/containers>를 참조하십시오.



컨테이너의 기능을 들으면 직관적으로 가상 머신과 비슷하다고 생각할 수 있습니다. 하지만 세부적인 부분이 다릅니다. 가장 큰 차이점은 하이퍼바이저가 필요 없다는 것입니다. 컨테이너는 적절한 Kernel 기능이 지원되고 도커 데몬이 있는 어떤 Linux 시스템에서나 실행할 수 있습니다. 이러한 특성으로 컨테이너는 휴대성이 매우 뛰어납니다. 노트북, VM, EC2 인스턴스 및 베어 메탈 서버 어디에든 호스팅할 수 있습니다.

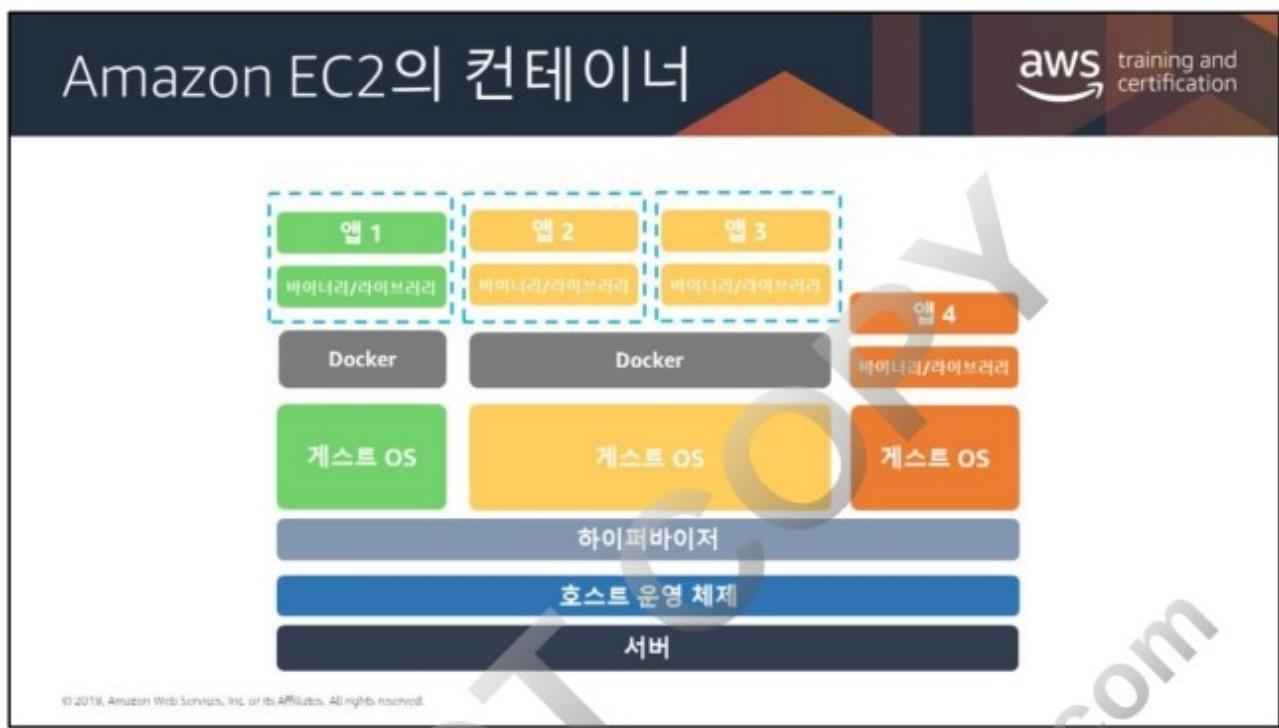
또한, 하이퍼바이저가 필요 없다는 것은 성능 오버헤드가 거의 발생하지 않는다는 뜻입니다. 프로세스가 Kernel과 직접 통신하며, 대체로 컨테이너 사일로에 대해서는 인식하지 못합니다. 대부분의 컨테이너는 몇 초 만에 부팅됩니다.

엔터프라이즈 내에는 컨테이너 및 가상 머신의 사용 사례와 그 차이점에 대한 많은 질문이 있습니다. 또한 AWS 내에서 컨테이너는 이제 Elastic Container Services, Docker, Elastic Beanstalk의 유ти리티를 통해 인프라의 핵심 부분이 되고 있습니다. 다음은 VM을 포함하여 Docker와 컨테이너의 차이점에 대한 간략한 개요입니다.

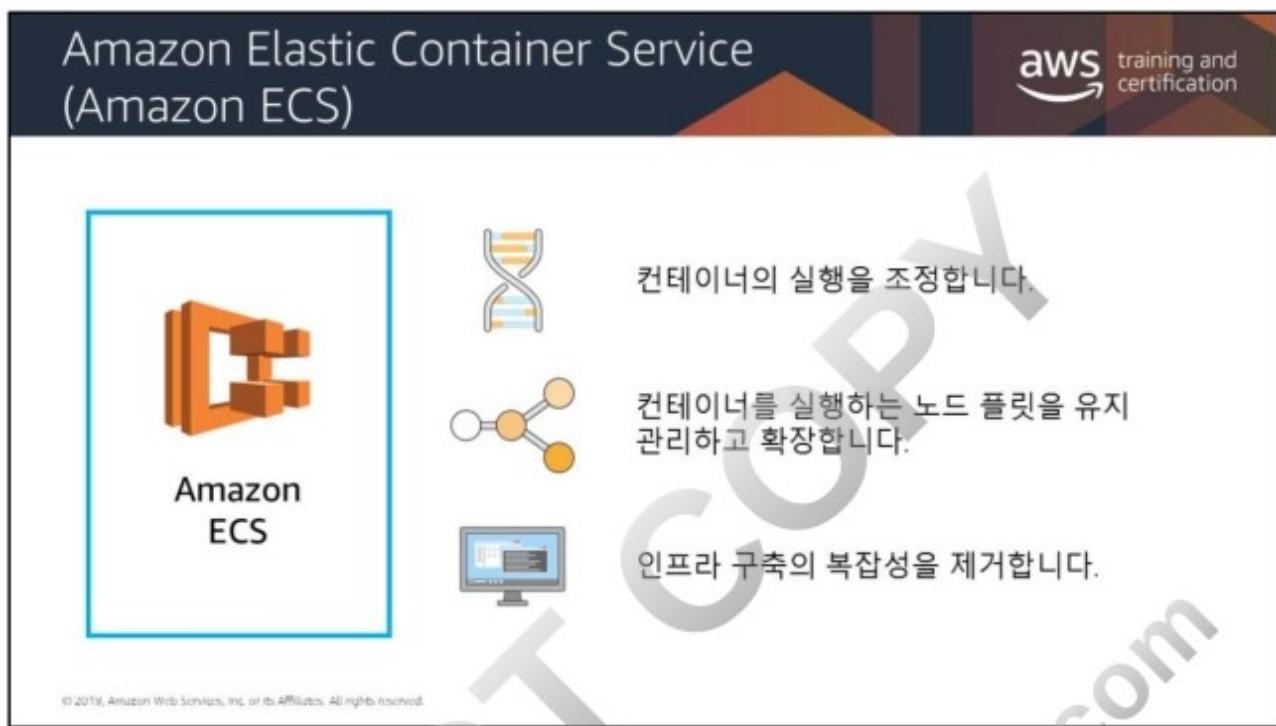
Docker, 컨테이너, VM, ECS의 개요는 다음을 참조하십시오.

<http://crmtrilogix.com/Cloud-Blog/AWS/Docker-Containers-VMs-and-ECS---an-overview/219>

DO NOT COPY
zlagusdbs@gmail.com



가상 머신 내 Amazon EC2의 컨테이너.



Amazon EC2 Container Service (Amazon ECS)는 도커 컨테이너를 지원하는 확장성과 성능이 뛰어난 컨테이너 관리 서비스로서, 서비스를 사용하여 Amazon EC2 인스턴스의 관리형 클러스터에서 애플리케이션을 손쉽게 실행할 수 있습니다.

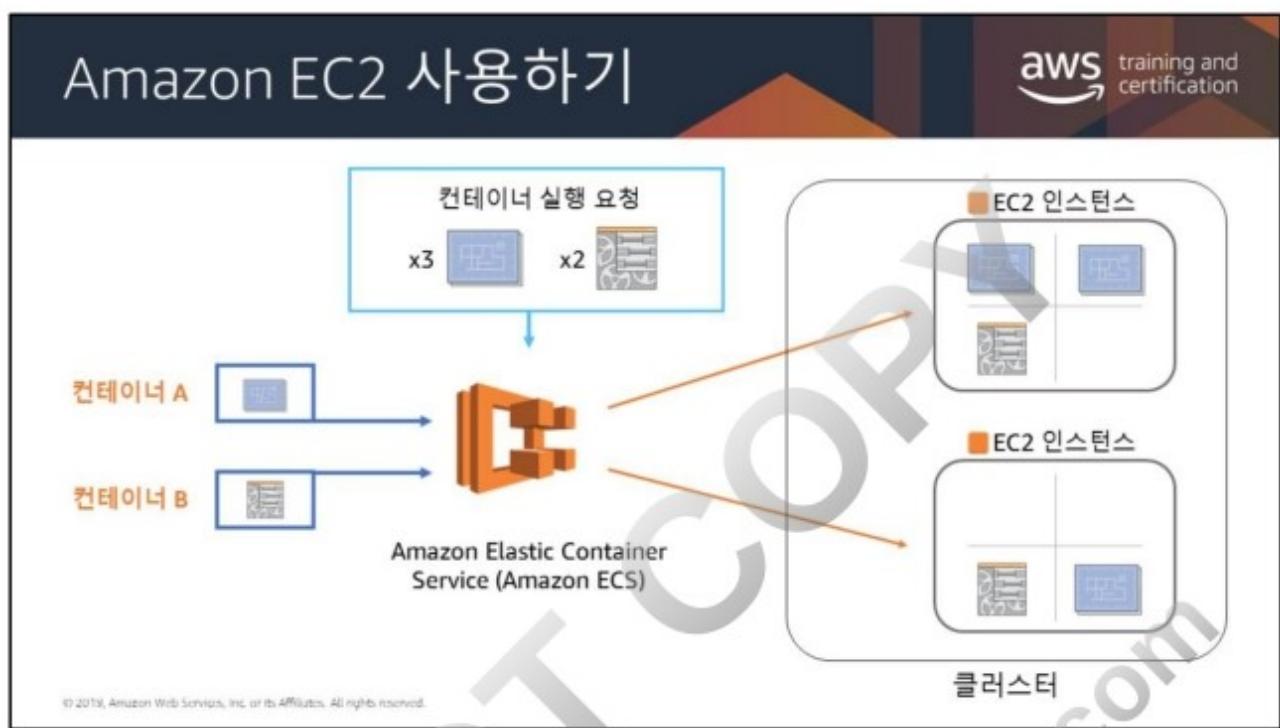
Amazon ECS는 컨테이너를 호스팅하기 위한 확장성이 뛰어난 클러스터 서비스로 다음과 같은 기능을 제공합니다.

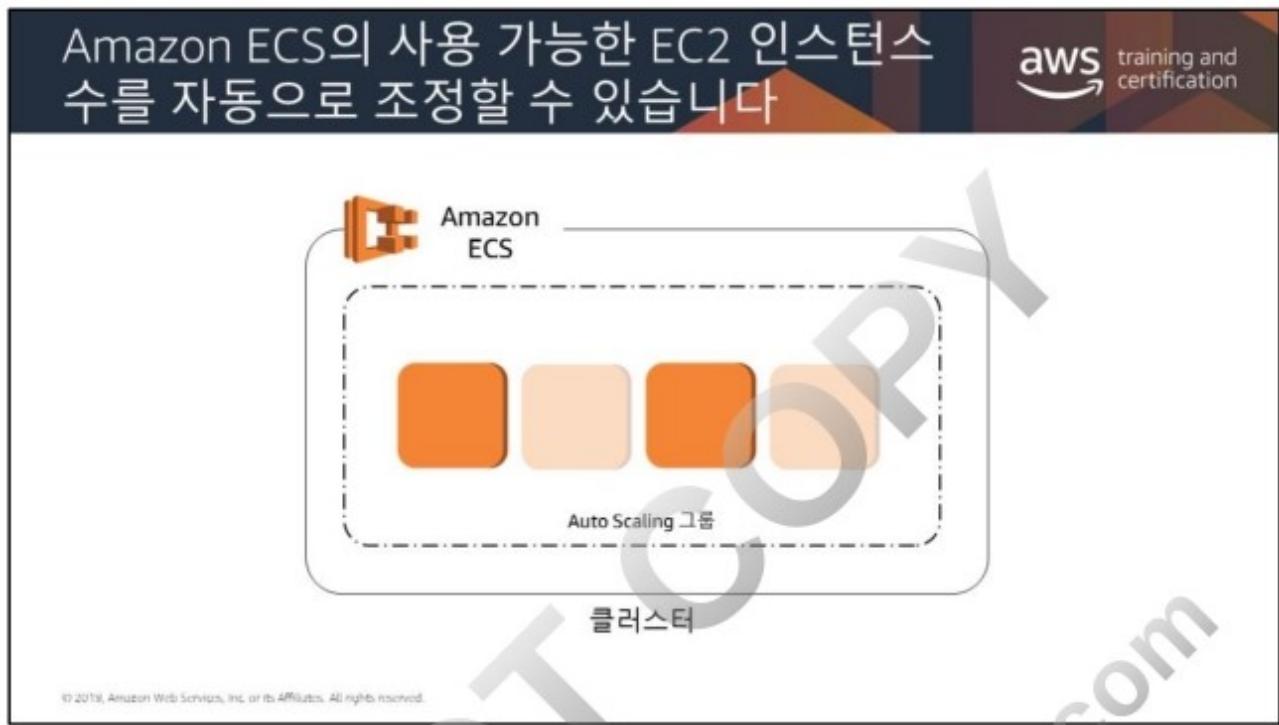
- 최대 수천 개의 인스턴스까지 확장할 수 있습니다.
- 컨테이너 배포를 모니터링합니다.
- 클러스터의 전체 상태를 관리합니다.
- 내장 스케줄러 또는 타사 스케줄러(예: Apache Mesos, Blox)를 사용하여 컨테이너 일정을 예약합니다.
- API를 사용하여 확장 가능합니다.
- Fargate 또는 EC2 시작 유형으로 시작 가능

클러스터는 스팟 인스턴스와 예약 인스턴스를 활용할 수 있습니다.

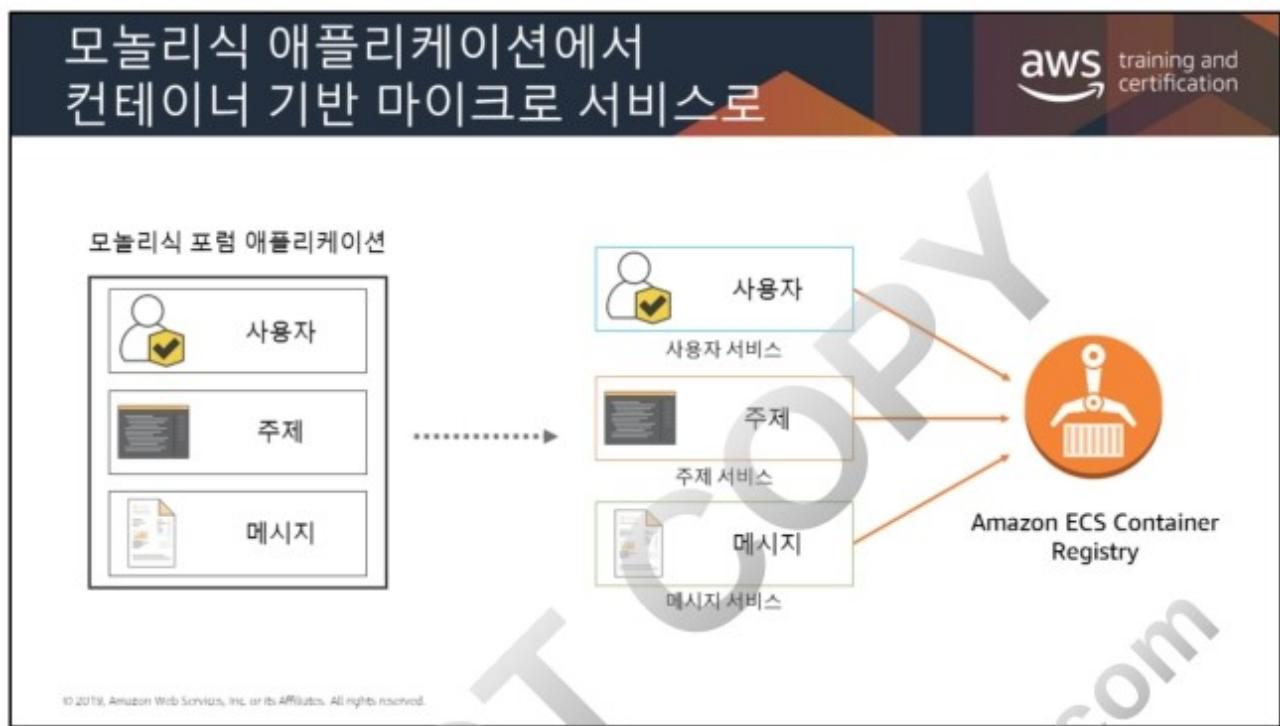
시작 유형에 대한 자세한 내용은 다음을 참조하십시오.

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/launch_types.html

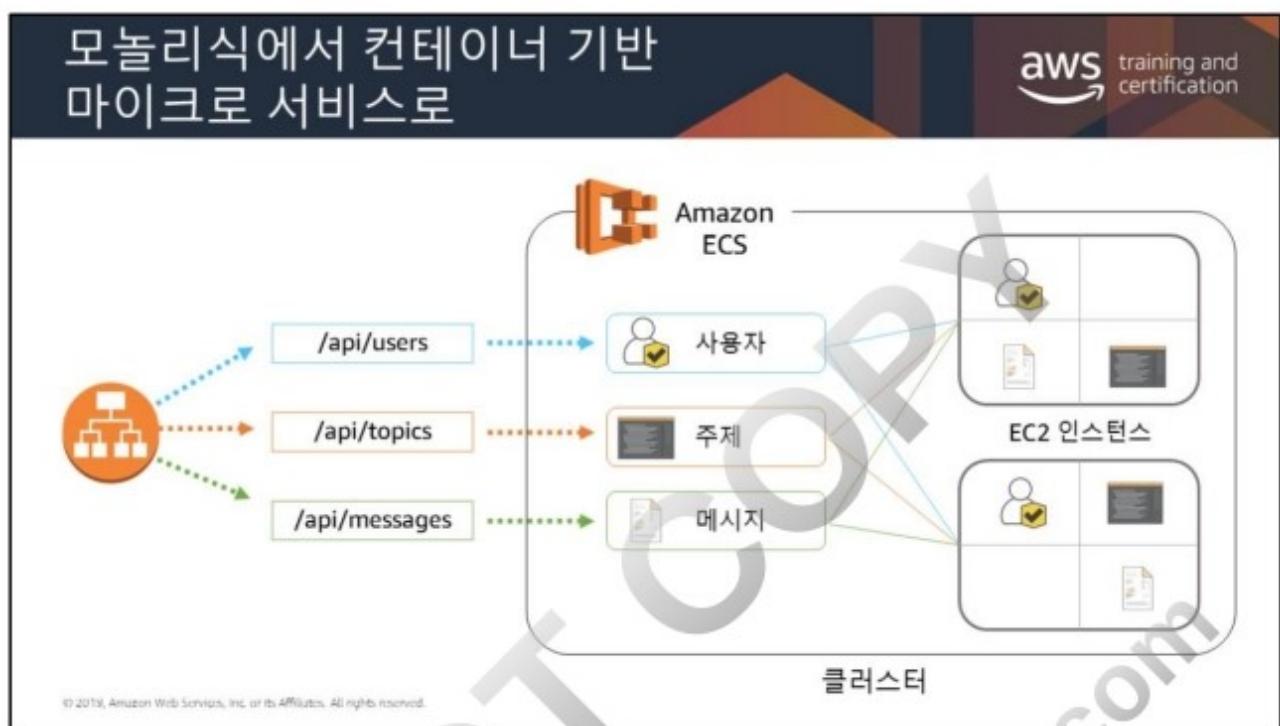




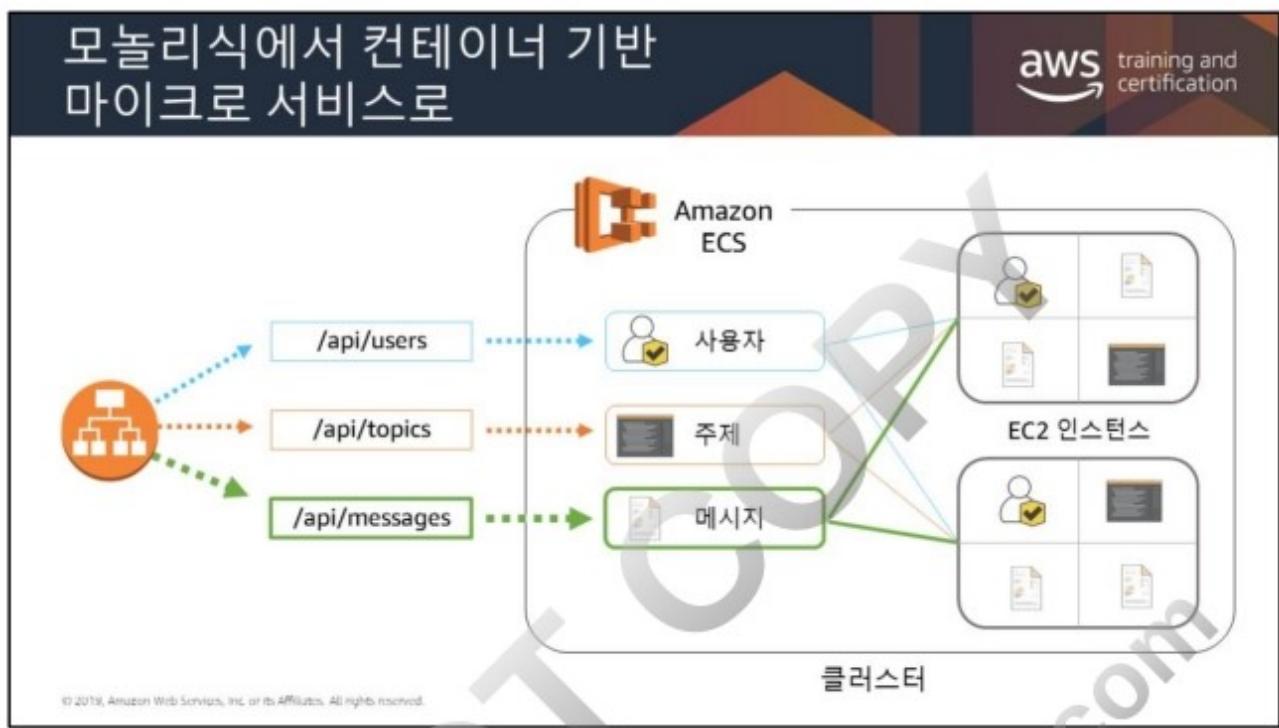
컨테이너 인스턴스를 제거하도록 Auto Scaling 그룹을 구성할 경우 제거된 컨테이너 인스턴스에서 실행되는 모든 작업이 중지됩니다. 작업이 서비스의 일부로 실행되는 경우 필요한 리소스(CPU, 메모리, 포트)가 사용 가능하면 Amazon ECS가 다른 인스턴스에서 해당 작업을 다시 시작합니다. 하지만 수동으로 시작한 작업은 자동으로 다시 시작되지 않습니다.



이 모놀리식 포럼 애플리케이션을 마이크로 서비스 접근 방식으로 전환하려면 코드를 캡슐화된 개별 서비스로 분할할 수 있습니다. 각 서비스가 제 기능을 완벽하게 수행하는지 확인한 다음, 이들 서비스를 Amazon ECS Container Registry에 등록합니다.



다음에는 Amazon ECS 내부에서 원래 애플리케이션의 이러한 요소 각각에 대해 서비스를 생성합니다. 그런 다음 이러한 서비스를 위한 대상 그룹 인스턴스를 등록합니다. 마지막으로 Amazon ECS 앱 서비스를 가리키는 대상 그룹을 포함하는 Application Load Balancer를 생성합니다.



AWS Cloud Map과 AWS App Mesh는 아키텍처 구축 및 문제 해결에 도움이 될 수 있습니다.

AWS Cloud Map은 완전 관리형 서비스로서, 모든 애플리케이션 리소스(예: 데이터베이스, 대기열, 마이크로서비스 및 기타 클라우드 리소스)를 사용자 지정 네임스페이스를 사용해 등록할 수 있습니다. 그러면 AWS Cloud Map은 리소스를 추가 및 등록할 때 수작업 매핑을 최소화하도록 리소스의 위치가 최신인지 확인하기 위해 상태를 지속적으로 확인합니다. AWS Cloud Map은 마이크로서비스와 애플리케이션의 서비스 검색, 지속적 통합, 상태 모니터링을 지원합니다. 자세한 내용은 다음을 참조하십시오.

- <https://aws.amazon.com/blogs/aws/aws-cloud-map-easily-create-and-maintain-custom-maps-of-your-applications/>
- <https://aws.amazon.com/cloud-map/>
- <https://www.youtube.com/watch?v=qTE1PbdY3hY>

AWS App Mesh은 모든 마이크로서비스에서 Amazon CloudWatch, AWS X-Ray 및 호환되는 AWS 파트너 및 커뮤니티 모니터링 및 추적 도구로 내보낼 수 있는 지표, 로그, 추적을 캡처합니다. 또한 마이크로서비스 간 트래픽 라우팅에 대한 사용자 지정 제어를 제공하여 애플리케이션의 배포, 장애 또는 조정을 지원합니다.

App Mesh는 애플리케이션 내에서 코드를 요구하거나 로드 밸런서를 사용하지 않고도 프록시를 통해 마이크로서비스를 서로 직접 연결하여 구성할 수 있습니다. App Mesh는 마이크로서비스 컨테이너와 함께 배포되는 오픈 소스 서비스 메시 프록시인 Envoy를 사용합니다. 자세한 내용은 다음을 참조하십시오.

- <https://aws.amazon.com/app-mesh/features/>
- <https://www.youtube.com/watch?v=qTE1PbdY3hY>

DO NOT COPY
zlagusdbs@gmail.com

AWS Fargate

aws training and certification

완전 관리형 컨테이너 서비스

- 클러스터 프로비저닝 및 관리
- 실행 시간 환경 관리
- 규모 조정

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

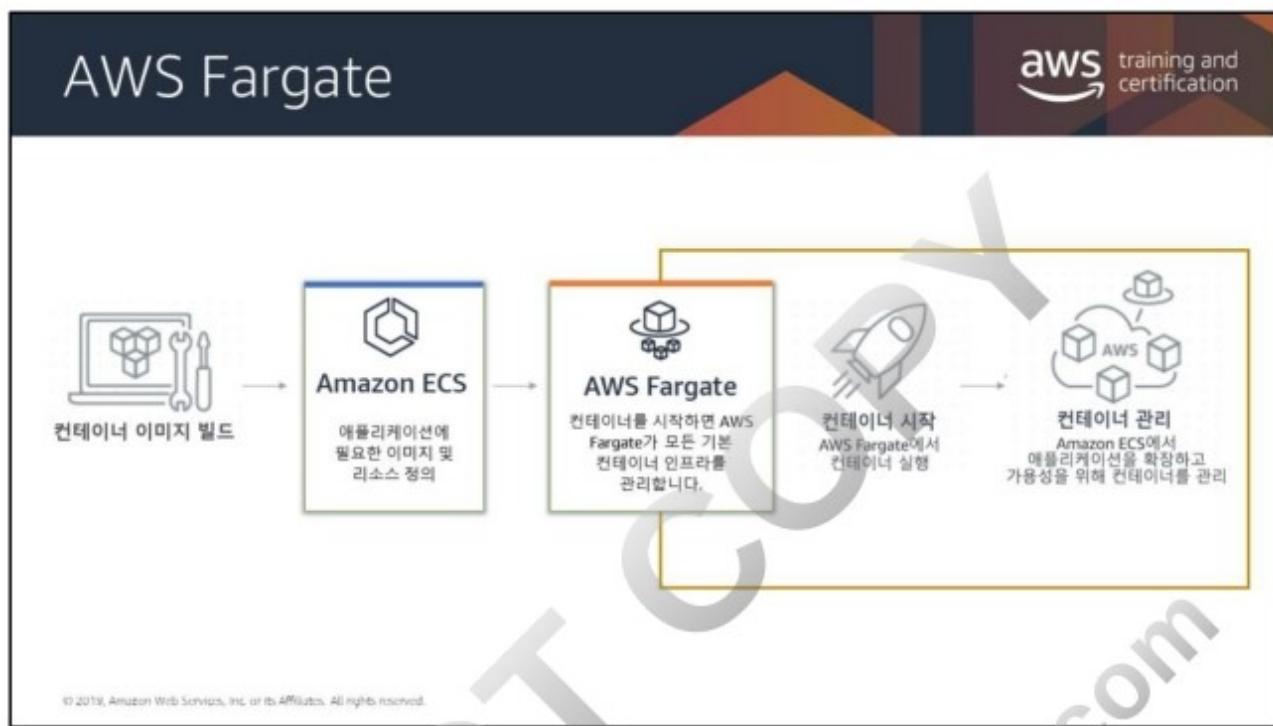
AWS Fargate는 서버 또는 클러스터를 관리할 필요 없이 [컨테이너](#)를 실행할 수 있게 해주는 Amazon ECS 및 Amazon Elastic Container Service for Kubernetes (Amazon EKS) 용 기술입니다. AWS Fargate를 사용하면 더 이상 컨테이너를 실행하기 위해 가상 머신을 프로비저닝, 구성 및 조정할 필요가 없습니다. 따라서 서버 유형을 선택하거나, 클러스터를 조정할 시점을 결정하거나, 클러스터 패킹을 최적화할 필요가 없습니다. AWS Fargate에서는 서버 또는 클러스터에 대해 고민하거나 상호 작용할 필요가 없습니다. Fargate를 사용하면 애플리케이션을 실행하는 인프라의 관리 대신 애플리케이션 설계 및 구축에 집중할 수 있습니다.

이 서비스는 Amazon ECS를 지원합니다.
AWS Fargate에 대한 자세한 내용은 다음을 참조하십시오.

<https://aws.amazon.com/fargate/>

Amazon EKS와의 통합에 대한 자세한 내용은 다음을 참조하십시오.

<https://aws.amazon.com/about-aws/whats-new/2018/11/aws-fargate-and-amazon-ecs-now-integrate-with-aws-cloud-map/>



Amazon ECS에는 Fargate 시작 유형과 EC2 시작 유형이라는 두 가지 모드가 있습니다. Fargate 시작 유형의 경우, 애플리케이션을 컨테이너로 패키징하고, CPU 및 메모리 요구 사항을 지정하고, 네트워킹 및 IAM 정책을 정의한 후 애플리케이션을 시작하기만 하면 됩니다. EC2 시작 유형의 경우, 컨테이너 애플리케이션을 실행하는 인프라에 대해 서버 수준의 좀 더 세분화된 제어를 할 수 있습니다. EC2 시작 유형에서는 Amazon ECS를 사용하여 서버 클러스터를 관리하고 서버에 컨테이너를 배치하는 일정을 예약할 수 있습니다. Amazon ECS는 클러스터 내 모든 CPU, 메모리 및 기타 리소스를 계속 추적하고, 지정한 리소스 요구 사항에 따라 컨테이너를 실행하기에 가장 적합한 서버를 찾습니다.



아키텍처가 효율적입니까?

하나의 기능만 수행하는 서비스를 지원하기 위해 전체 인스턴스를 사용하고 있습니까?

www API 간단한 앱

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

아키텍처가 효율적입니까?

aws training and certification

하나의 기능만 수행하는 서비스를 지원하기 위해 전체 인스턴스를 사용하고 있습니까?

www API 간단한 앱

다른 서비스를 활용하여 관리:

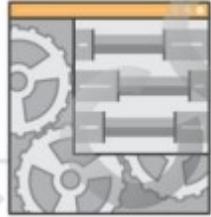
HA 및 FT 플랫 상태 모니터링 용량

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

서비스 컴퓨팅이란 무엇입니까?

aws training and certification

서버를 관리하지 않고 앱과 서비스를 구축하고 실행



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

서비스 컴퓨팅이란 무엇입니까?

서비스 컴퓨팅을 사용하면 서버를 생각하지 않고 애플리케이션과 서비스를 구축하고 실행할 수 있습니다. 서비스 애플리케이션에서는 사용자가 서버를 프로비저닝, 확장, 관리할 필요가 없습니다. 거의 모든 유형의 애플리케이션 또는 백엔드 서비스를 위해 서비스 애플리케이션을 구축할 수 있으며, 애플리케이션을 고가용성으로 실행하고 확장하는 데 필요한 모든 것이 자동으로 처리됩니다.

서비스 컴퓨팅은 왜 사용합니까?

서비스 애플리케이션 구축은 개발자가 클라우드든 온프레미스든 서버 또는 런타임의 관리 및 운영에 신경을 쓰는 대신 핵심 제품에 집중할 수 있다는 것을 의미합니다. 이렇게 오버헤드가 줄어들면 개발자는 확장성과 안정성을 갖춘 훌륭한 제품을 개발하는 데 시간과 에너지를 쓸 수 있습니다.

자세한 내용은 다음을 참조하십시오. <https://aws.amazon.com/serverless/>

AWS Lambda



AWS Lambda

- 완전 관리형 컴퓨팅 서비스
- 상태 비저장 코드 실행
- Node.js, Java, Python, C#, Go, Ruby 지원
- 일정에서 또는 이벤트에 대한 응답으로 코드 실행
(예: Amazon S3 버킷 또는 Amazon DynamoDB 테이블의 데이터 변경)
- 엣지에서 실행 가능

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

AWS Lambda를 사용하면 서버를 프로비저닝하거나 관리할 필요 없이 코드를 실행할 수 있습니다. 이 서비스는 고가용성 컴퓨팅 인프라에서 코드를 실행하고 서버 및 운영 체제 유지 관리, 용량 프로비저닝 및 자동 조정, 코드 모니터링 및 로깅 등 모든 컴퓨팅 리소스 관리를 수행합니다. 사용자는 AWS Lambda가 지원하는 언어(현재 Node.js, Java, C#, Python, Ruby) 중 하나로 코드를 제공하기만 하면 됩니다.

Lambda@Edge는 Amazon CloudFront CDN에서 생성된 이벤트에 대한 응답으로 Lambda 함수를 실행하고 고가용성을 유지한 채로 최종 사용자에게 가장 가까운 AWS 엣지 로케이션에서 코드를 확장할 수 있습니다. Lambda 함수를 사용하여 다음 지점에서 CloudFront 요청 및 응답을 변경할 수 있습니다.

- 최종 사용자 요청
- 오리진 요청
- 오리진 응답
- 최종 사용자 응답

이를 통해 웹 사이트 보안 및 개인 정보 보호 강화, 엣지에 동적 애플리케이션 구축, SEO, 실시간 이미지 변환, 사용자 인증 및 권한 부여, 사용자 추적 및 분석, 기타 사용 사례가 가능합니다.

Lambda@Edge는 Node.js만 지원합니다

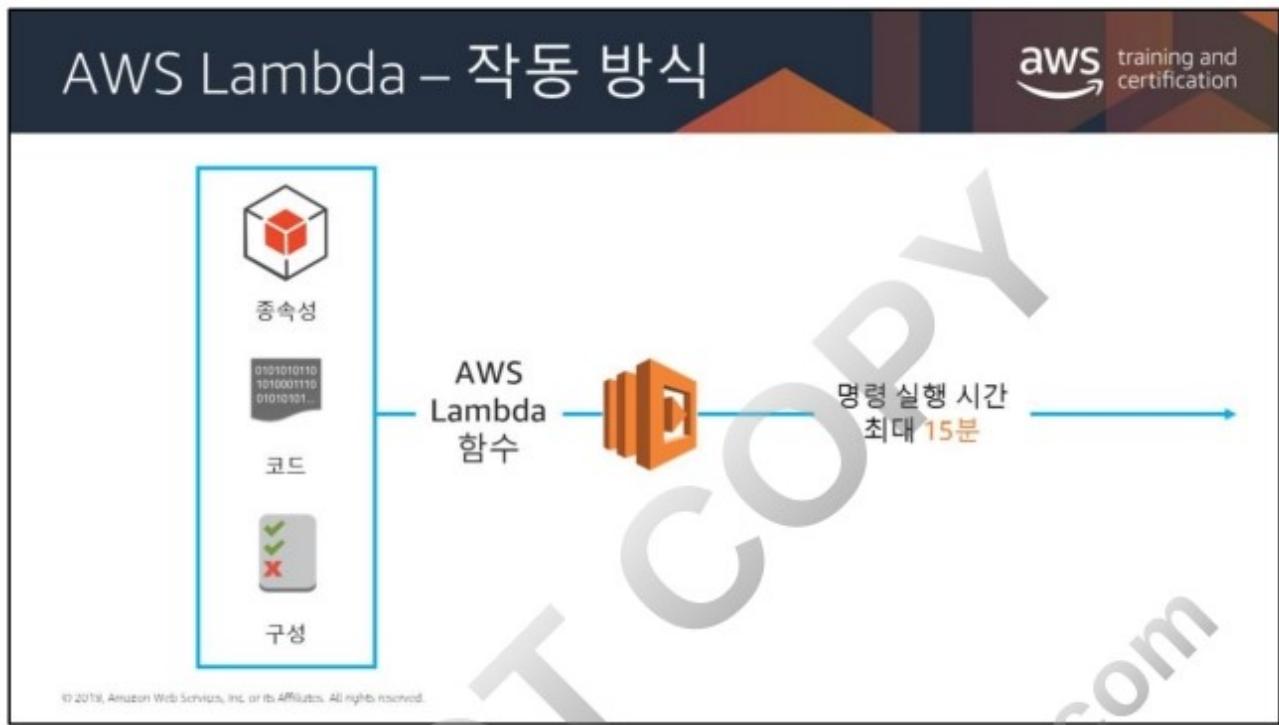
자세한 내용은 다음을 참조하십시오.

- <https://aws.amazon.com/lambda/edge/>
<https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html>
- <https://aws.amazon.com/blogs/networking-and-content-delivery/adding-http-security-headers-using-lambdaedge-and-amazon-cloudfront/>

.NET Core 2.1 런타임을 사용하여 PowerShell Core 6.0에서 AWS Lambda 함수를 개발할 수도 있습니다. PowerShell 개발자는 AWS Lambda를 사용하여 PowerShell 환경 내에서 AWS 리소스를 관리하고 풍부한 자동화 스크립트를 작성할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- <https://aws.amazon.com/about-aws/whats-new/2018/09/aws-lambda-supports-powershell-core/>



AWS Lambda의 핵심 구성 요소는 이벤트 소스와 *Lambda* 함수입니다. 이벤트 소스는 이벤트를 게시하고, *Lambda* 함수는 이벤트를 처리하도록 사용자가 작성하는 사용자 지정 코드입니다. *Lambda*는 사용자 대신 *Lambda* 함수를 실행합니다.

Lambda 함수는 코드, 관련 종속성 및 구성으로 이루어집니다. 구성에는 이벤트를 수신하는 핸들러, 사용자 대신 *Lambda* 함수를 실행하기 위해 *AWS Lambda*가 맡을 수 있는 IAM 역할, 할당할 컴퓨팅 리소스, 실행 제한 시간 등의 정보가 포함됩니다.

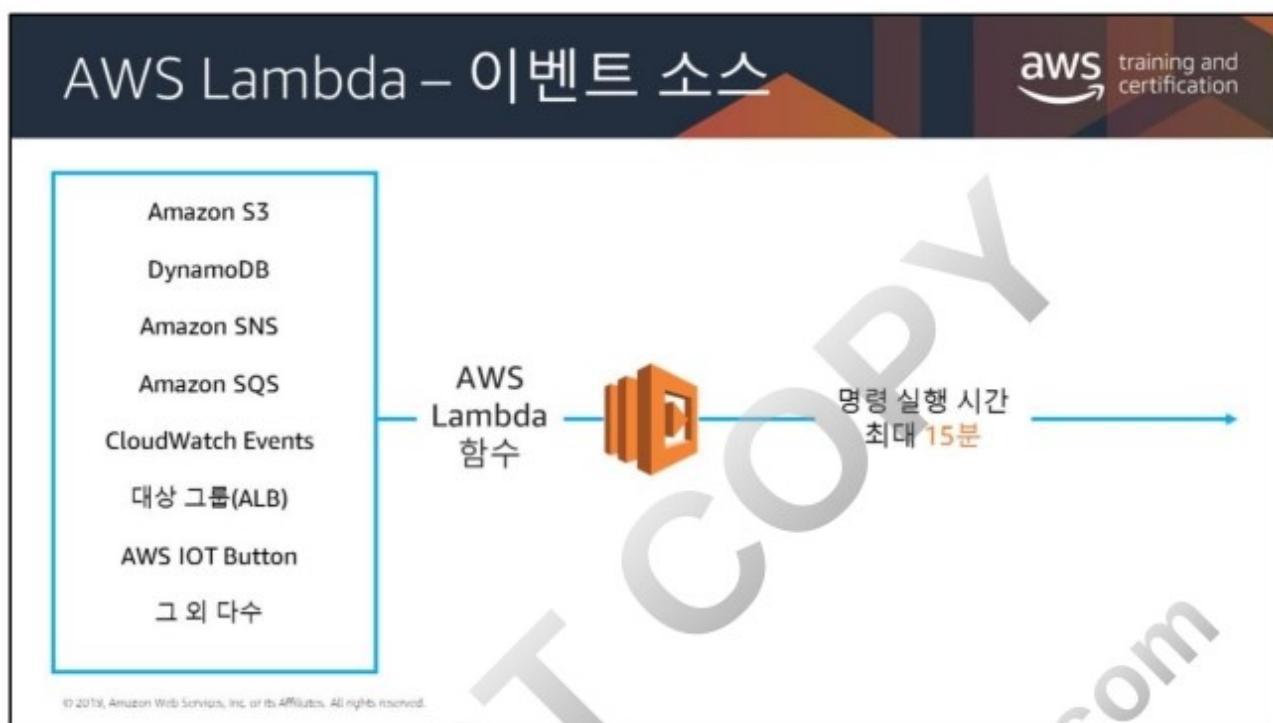
계층을 사용하면 *AWS Lambda* 함수 개발자가 패키지, 바이너리, 런타임 및 *Lambda* 함수에 필요한 그 밖의 파일을 함수 코드와 별개의 구성 요소로 유지할 수 있습니다. *Lambda* 함수를 생성할 때 함수의 실행 환경에 포함될 하나 이상의 계층을 지정할 수 있습니다. 이렇게 하면 여러 *Lambda* 함수에 분산된 동일한 파일의 사본을 유지할 필요가 없습니다. 예를 들어 Python으로 작성된 서비스 애플리케이션은 PyMySQL 같은 패키지를 사용하여 Amazon RDS MySQL 데이터베이스를 쿼리할 수 있습니다. 계층이 있는 경우 PyMySQL 패키지의 단일 사본만 유지하면 애플리케이션 내 모든 함수가 이를 사용할 수 있습니다.

Lambda 계층 제한:

- 단일 함수는 한 번에 최대 5개의 계층을 소비할 수 있습니다.
- 압축되지 않은 함수의 총 크기(계층 포함)는 압축되지 않은 배포 패키지 크기 제한인 250MB를 초과할 수 없습니다.

Lambda 계층은 리소스 수준 권한을 지원하며, 특정 AWS 계정, AWS Organizations 또는 모든 계정에서 공유할 수 있습니다. 계층은 함수 생성 도중이나 이후에 추가할 수 있으며, 필요한 경우 업데이트도 가능합니다. AWS Serverless Application Model (SAM)도 함수 전반의 계층 관리를 지원합니다.

함수 버전과 마찬가지로 계층은 개별 버전 및 해당 권한을 지원합니다. 게시된 계층 버전은 업데이트할 수 없습니다(버전 권한 변경 제외). 계층을 업데이트하려면 새 버전을 게시해야 합니다. 이렇게 하면 여러 함수에서 새 계층의 룰아웃을 제어할 수 있습니다.



ALB를 사용하여 HTTP/HTTPS를 통해 Lambda 함수에 트래픽을 전송할 수 있습니다. ALB가 콘텐츠 기반 라우팅이므로 ALB로 들어오는 요청의 호스트 또는 호스트 및 URL 경로를 기반으로 다른 Lambda 함수에 트래픽을 전송할 수도 있습니다. ALB 대상으로 Lambda 함수를 등록하면 로드 밸런서가 JSON 형식으로 Lambda 함수에 콘텐츠를 전달합니다. 기본적으로 Lambda 유형의 대상 그룹에 대한 상태 확인은 비활성화되어 있습니다.

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/lambda-functions.html>

서비스 컴퓨팅의 이점

aws training and certification

구성이 아니라 애플리케이션에 집중함

요청 시에만 컴퓨팅 리소스 사용

마이크로 서비스 아키텍처 구축

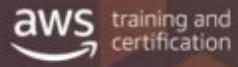
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



이 예에서 시뮬레이션된 슬롯 머신 브라우저 기반 게임은 슬롯을 당길 때마다 무작위 결과를 생성하는 Lambda 함수를 호출하고, 결과를 표시하는데 사용되는 이미지의 파일 이름으로 해당 결과를 반환합니다. 이미지는 애플리케이션 경험을 제공하는데 필요한 HTML, CSS 및 기타 자산의 정적 웹 호스트로 가능하도록 구성된 Amazon S3 버킷에 저장됩니다.

자세한 내용은 다음을 참조하십시오. <https://docs.aws.amazon.com/sdk-for-javascript/v2/developer-guide/lambda-examples.html>

AWS Lambda



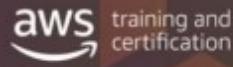
AWS Lambda가 처리하는 작업:

- 서버
- 용량 요구
- 배포
- 조정 및 내결합성
- OS 또는 언어 업데이트
- 지표 및 로깅

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

DO NOT COPY
zlagusdbs@gmail.com

AWS Lambda



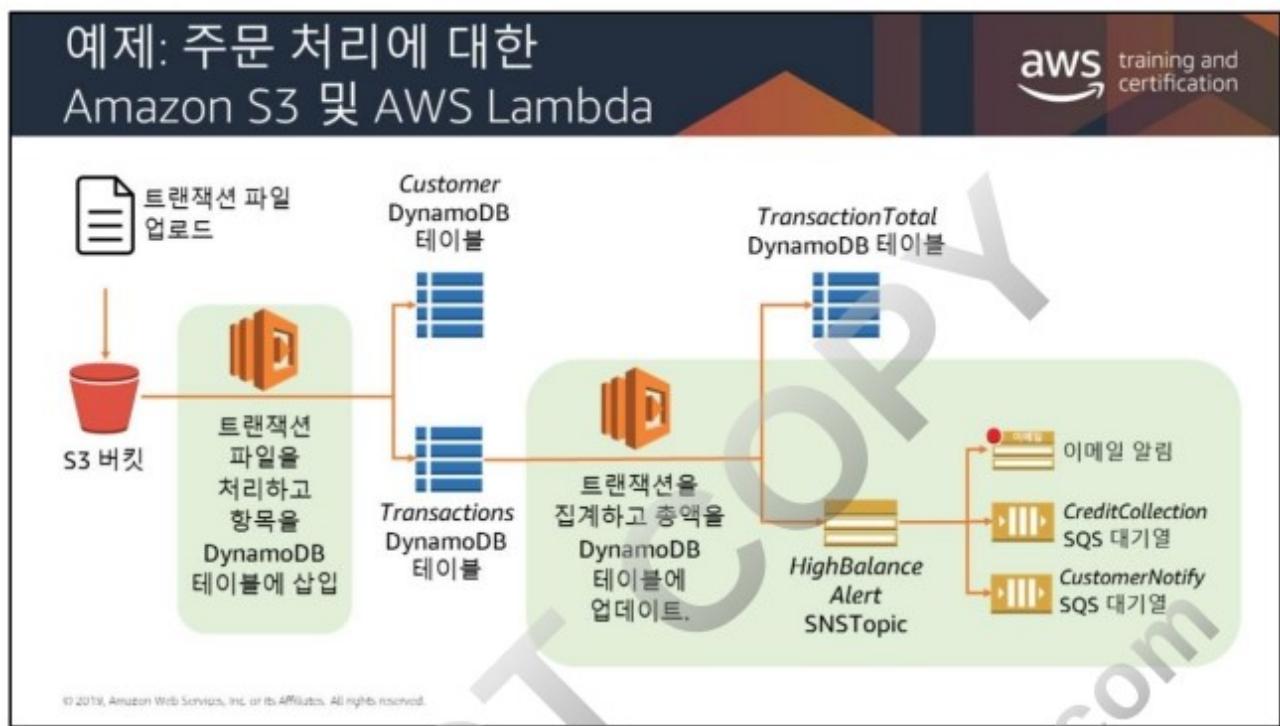
AWS Lambda가 처리하는 작업:

- 서버
- 용량 요구
- 배포
- 조정 및 내결함성
- OS 또는 언어 업데이트
- 지표 및 로깅

AWS Lambda를 사용하면 할 수 있는 작업:

- 자체 코드 사용 가능(네이티브 라이브러리 포함)
- 코드를 병렬로 실행
- 백엔드, 이벤트 핸들러 및 데이터 처리 시스템 생성
- 유동 리소스에 대해 비용을 지불할 필요가 없음!

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



Amazon API Gateway



애플리케이션의 "현관" 역할을 하는 API를 생성할 수 있습니다.

최대 수십만 건의 동시 API 호출을 처리합니다.

다음에서 실행되는 워크로드를 처리할 수 있습니다.

- Amazon EC2
- AWS Lambda
- 모든 웹 애플리케이션

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



API Gateway

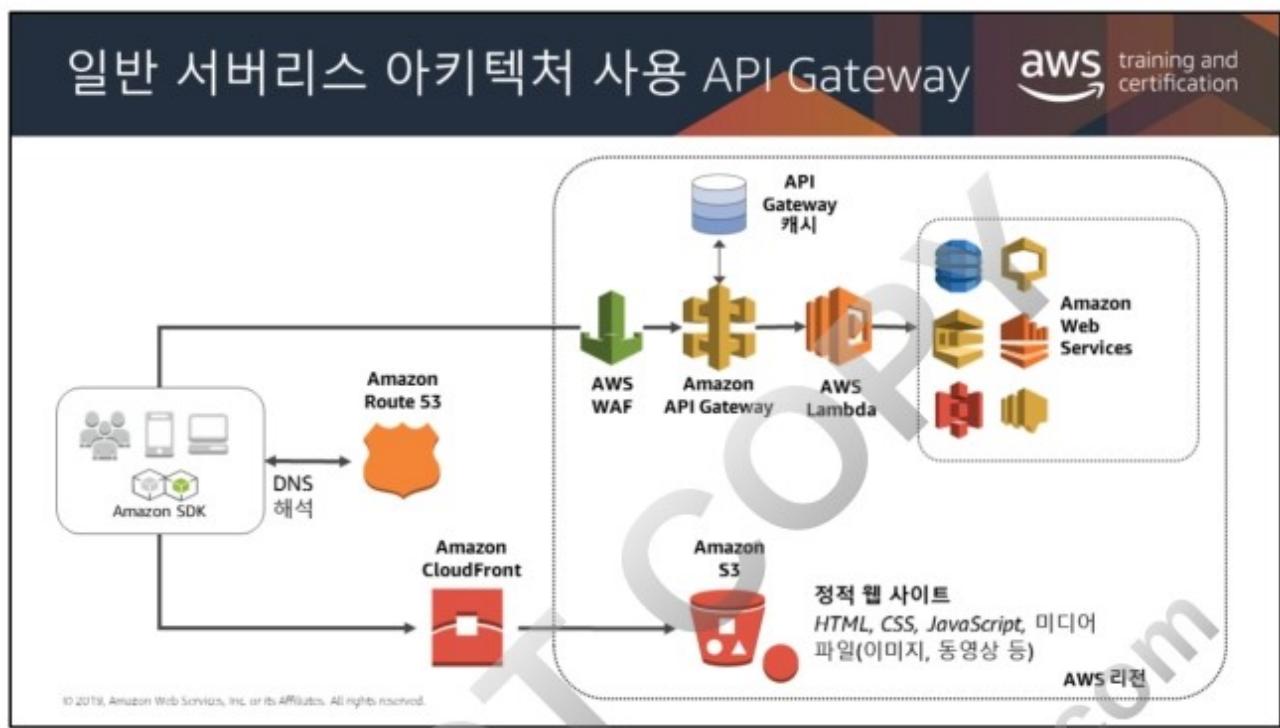


The API Gateway logo icon consists of a yellow square containing a stylized golden symbol resembling a cross or a series of interconnected lines forming a cube-like structure.

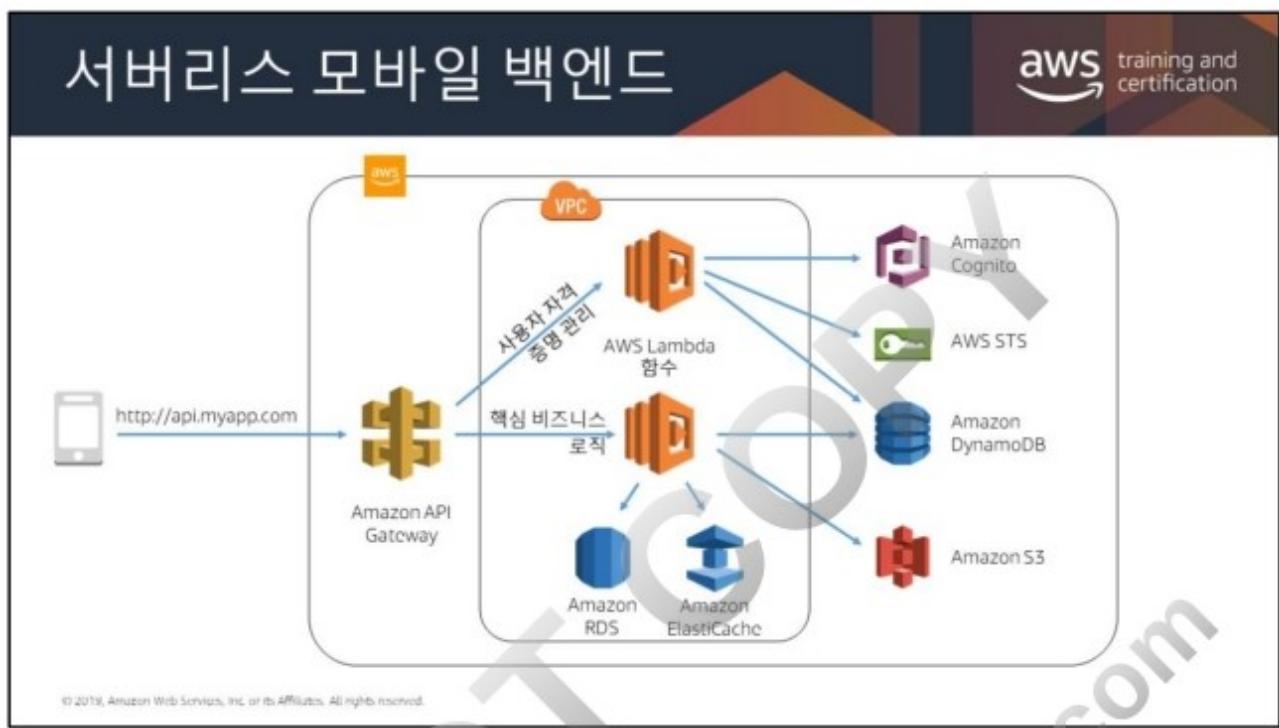
API
Gateway

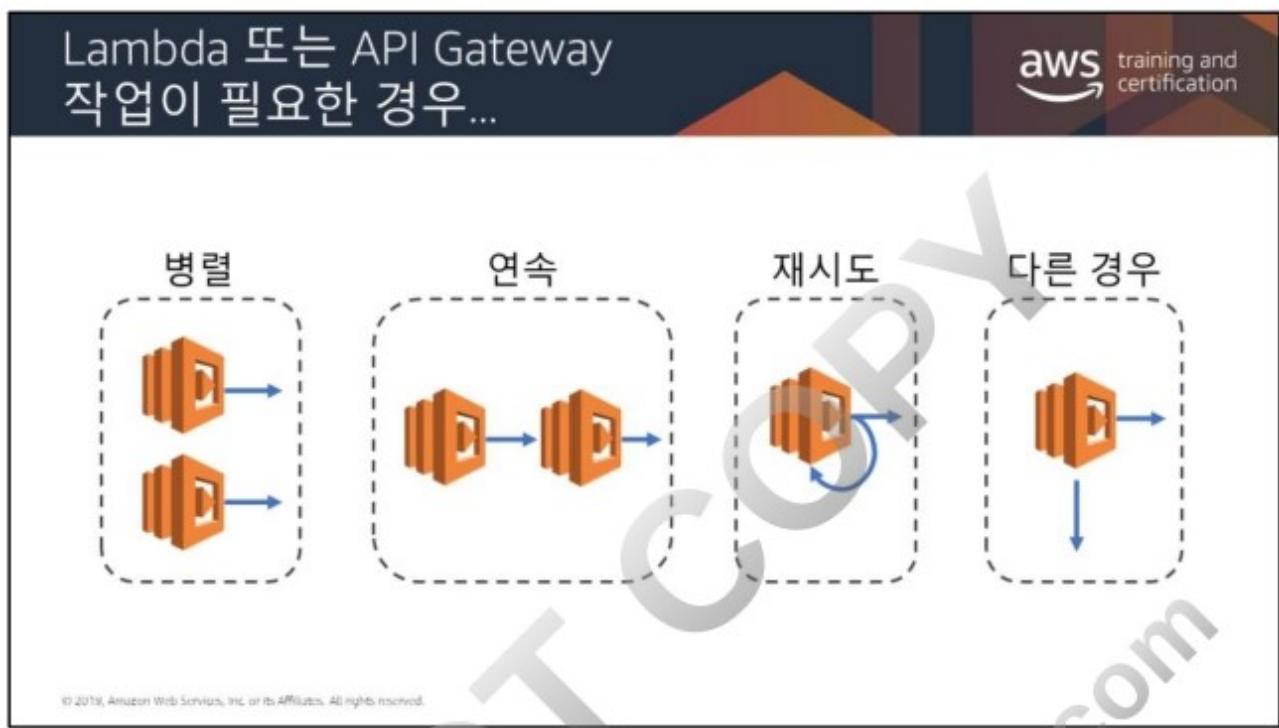
- 다양한 버전과 단계의 API를 호스팅 및 사용
- 개발자에게 API 키를 생성하여 배포
- 서명 버전 4를 활용하여 API에 대한 액세스를 승인
- AWS Lambda와 긴밀하게 통합됨
- 프라이빗 VPC와의 엔드포인트 통합

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



컨테이너는 소프트웨어 제공의 새로운 패러다임을 소개합니다. Amazon ECS/Fargate를 사용하면 컨테이너를 손쉽게 관리할 수 있지만 여전히 인프라를 유지하고 리소스를 사용해야 합니다.





AWS Step Functions



AWS Step Functions

- 시각적 워크플로를 사용한 마이크로 서비스 조정
- 애플리케이션 기능을 단계별로 실행할 수 있습니다.
- 각 단계를 자동으로 트리거하고 추적합니다.
- 단계가 실패한 경우 단순 오류를 파악하여 로깅을 제공합니다.

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

Step Functions는 상태 시스템입니다.

```
graph TD; A[자동판매기] --> B[트랜잭션 대기 중]; B --> C[탄산음료 선택]; C --> D[탄산음료 판매]
```

상태 시스템은 출력을 결정하기 위해 이전 조건에 의존하는 일련의 작동 조건을 가진 객체입니다.

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

상태 시스템은 출력을 결정하기 위해 이전 조건에 의존하는 일련의 작동 조건을 가진 객체입니다.

상태 시스템의 일반적인 예 하나는 탄산음료 자판기입니다. 자판기는 운영 상태에서 시작하여(거래를 대기) 동전 또는 지폐가 투입되면 탄산음료 선택으로 전환합니다. 그러면 판매 상태가 시작되어 탄산음료가 고객에게 제공됩니다. 완료 후 다시 운영 상태로 돌아갑니다.

AWS Step Functions를 사용하면 AWS 환경에서 사용자 고유의 상태 시스템을 자동화할 수 있습니다. 이를 위해 다양한 상태, 작업, 선택, 오류 처리 등으로 구성된 구조를 포함하는 JSON 기반 Amazon States 언어가 사용됩니다.

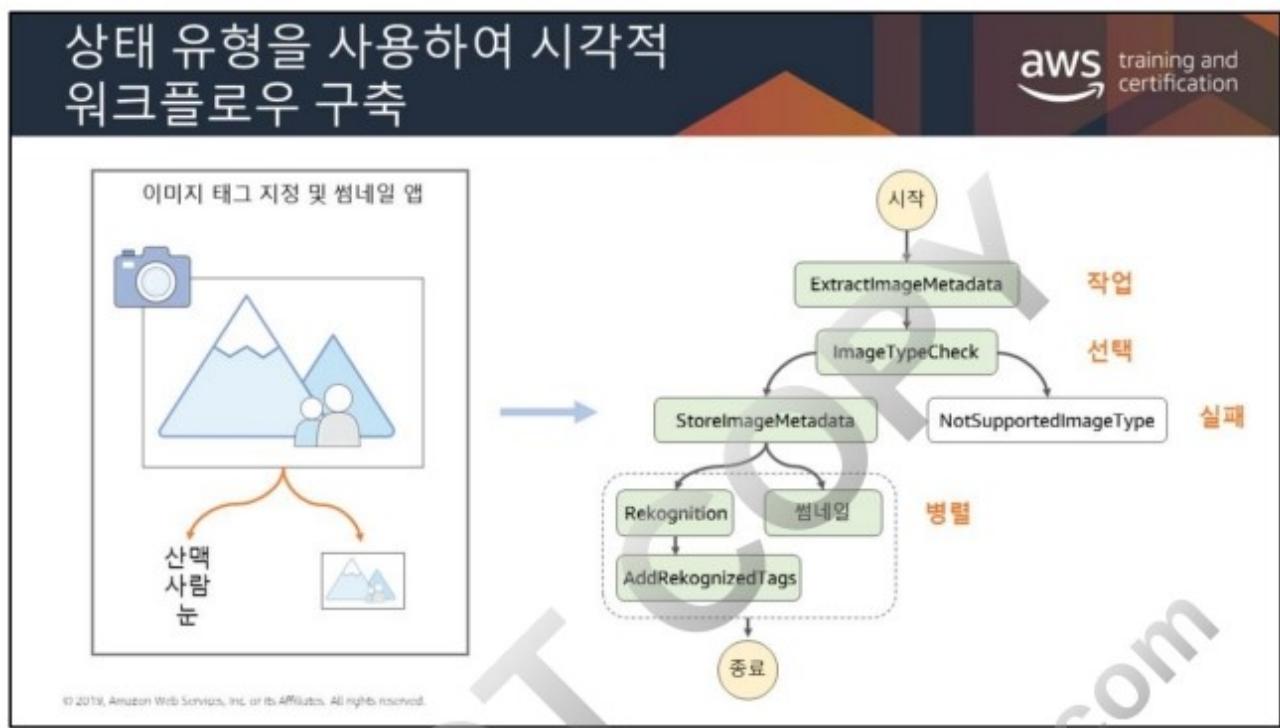
Amazon 상태 언어

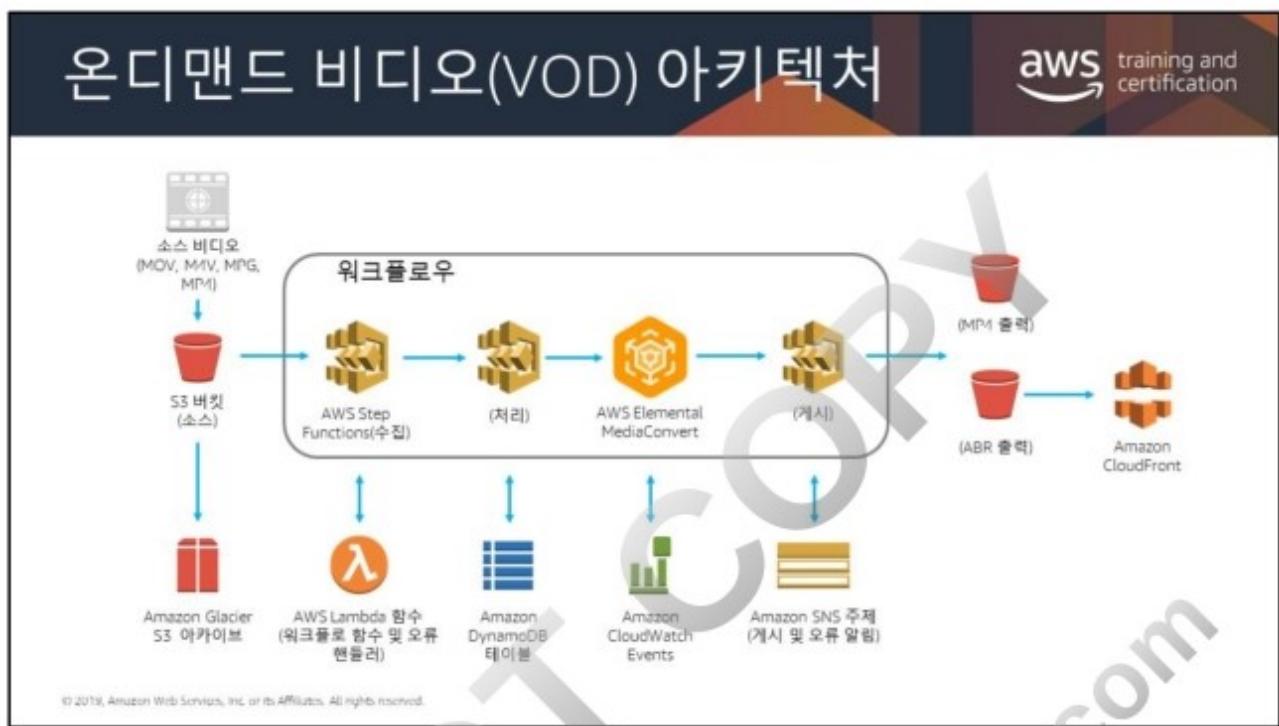
```
graph TD; 시작((시작)) --> StartState[StartState]; StartState --> 종료((종료)); 종료 --> 최종함수((최종 함수));
```

```
{
  "Comment": "An example of the ASL.",
  "StartAt": "StartState",
  "States": {
    "StartState": {
      "Type": "Task",
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:myLambda",
      "Next": "FinalState"
    },
    "FinalState": {
      "Type": "Task",
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:myLambda",
      "End": true
    }
  }
}
```

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

Amazon States 언어는 작업을 수행하거나(작업 상태), 다음으로 전환할 상태를 결정하거나(선택 상태), 오류를 표시하며 실행을 중지하거나(실패 상태) 할 수 있는 [상태](#)의 모음인 상태 시스템을 정의하는 데 사용되는 JSON 기반의 구조화된 언어입니다. 자세한 내용은 [Amazon States 언어 사양](#) 및 Amazon States 언어 코드를 검증하는 도구인 [Statelint](#)를 참조하십시오.

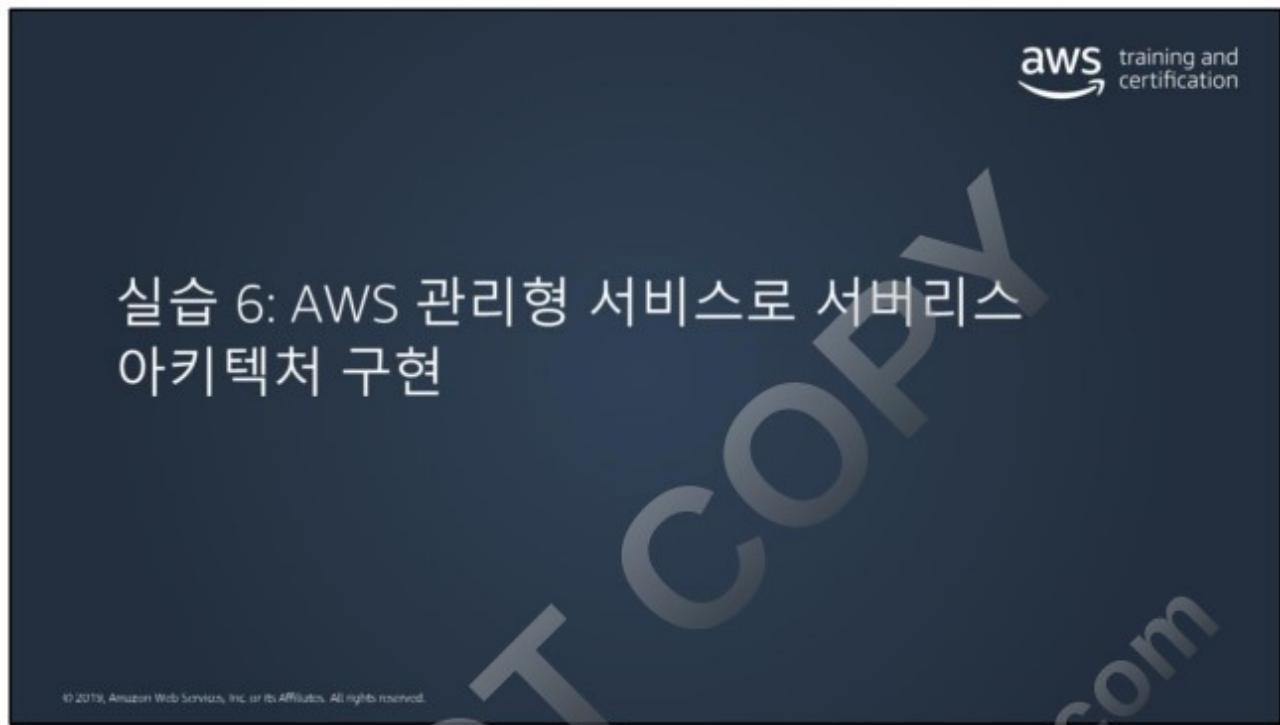




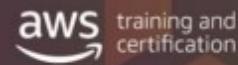
AWS는 소스 동영상을 수집하고, 광범위한 디바이스에서 재생할 수 있도록 동영상을 처리하고, Amazon CloudFront를 통해 최종 사용자에게 주문형으로 제공할 트랜스코딩된 미디어 파일을 저장하는 솔루션을 제공합니다. 자세한 내용은 다음을 참조하십시오.

<https://docs.aws.amazon.com/solutions/latest/video-on-demand/architecture.html>

Amazon Elastic Transcoder를 인코딩에 사용하기 원하는 고객을 위해 이 주문형 동영상 솔루션에는 Elastic Transcoder를 사용하여 동일한 워크플로를 배포하는 다른 AWS CloudFormation 템플릿이 포함되어 있습니다. 자세한 내용은 다음을 참조하십시오. <https://docs.aws.amazon.com/solutions/latest/video-on-demand/appendix-e.html>



실습 6: 서비스 아키텍처 구현



"클라우드를 위해 구축된 안정적이고 확장 가능하며 저렴한
애플리케이션을 원합니다."

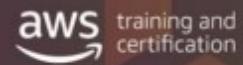
사용된 기술:

- AWS Lambda
- Amazon SNS
- Amazon DynamoDB
- Amazon S3
- Amazon Cognito

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

DO NOT COPY
zlagusdbs@gmail.com

실습 6: 서비스 아키텍처 구현



시나리오

- 재고 내역 파일을 업로드하고 저장합니다.
- 대시보드를 통해 재고 수준을 모니터링합니다.
- 재고가 없을 때 재고 관리자에게 알립니다.

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

실습 6: 서비스 아키텍처 구현

aws training and certification

CSV 재고 내역 파일이 Amazon S3에 업로드됩니다.

재고 내역 파일 업로드

Amazon S3 버킷

store	item	count
Berlin	Echo Dot	12
Berlin	Echo (2nd Gen)	19
Berlin	Echo Show	18
Berlin	Echo Plus	0
Berlin	Echo Look	10
Berlin	Amazon Tap	15

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

실습 6: 서비스 아키텍처 구현

AWS Lambda 함수는 DynamoDB 테이블에 파일 콘텐츠를 로드합니다.

```
graph TD; A["재고 내역 파일 업로드"] --> B["Amazon S3 버킷"]; B --> C["AWS Lambda  
함수는 재고 내역  
파일을 읽고 항목을  
DynamoDB  
테이블에  
삽입합니다."]; C --> D["Amazon DynamoDB 테이블"];
```

The diagram illustrates a serverless architecture. It starts with a document icon labeled "재고 내역 파일 업로드" (Upload inventory file). An arrow points from this icon to a red bucket icon labeled "Amazon S3 버킷" (Amazon S3 Bucket). Another arrow points from the bucket to an orange lambda function icon labeled "AWS Lambda". Below the lambda icon is a box containing the text: "함수는 재고 내역 파일을 읽고 항목을 DynamoDB 테이블에 삽입합니다." (The function reads the inventory file and inserts items into the DynamoDB table). A final arrow points from the lambda function to a blue grid icon labeled "Amazon DynamoDB 테이블" (Amazon DynamoDB Table).

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

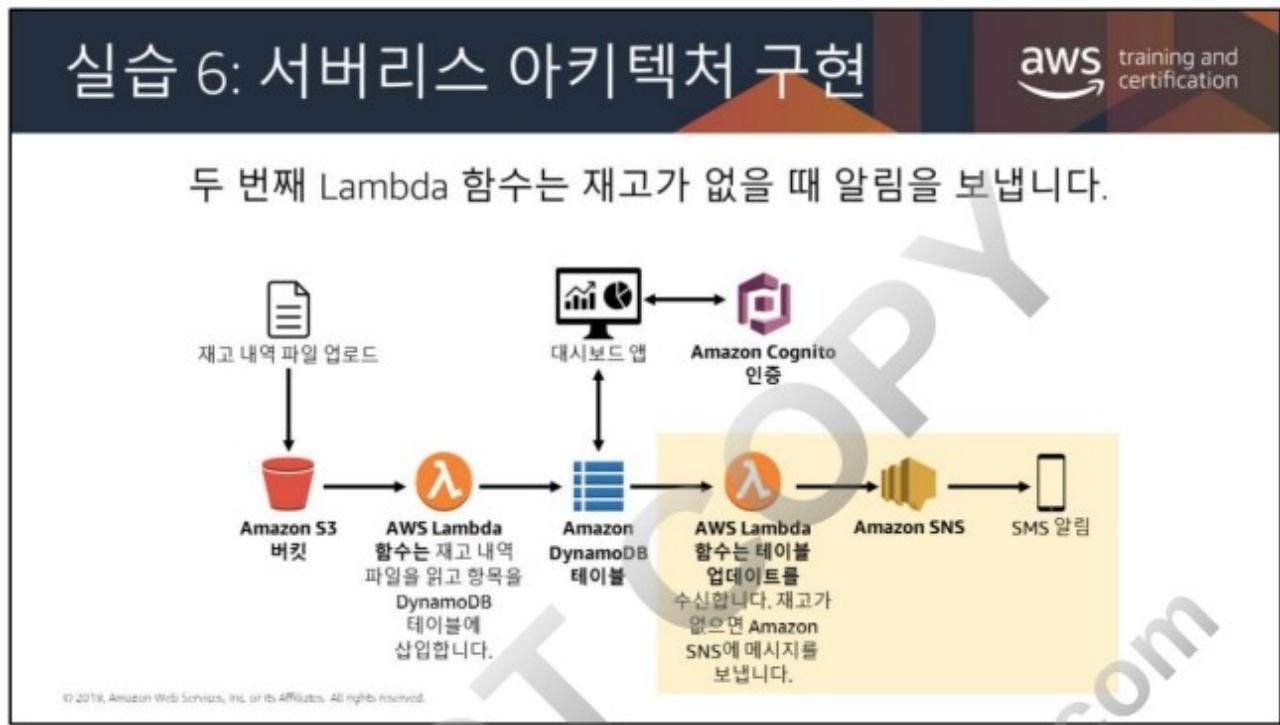
실습 6: 서비스 아키텍처 구현

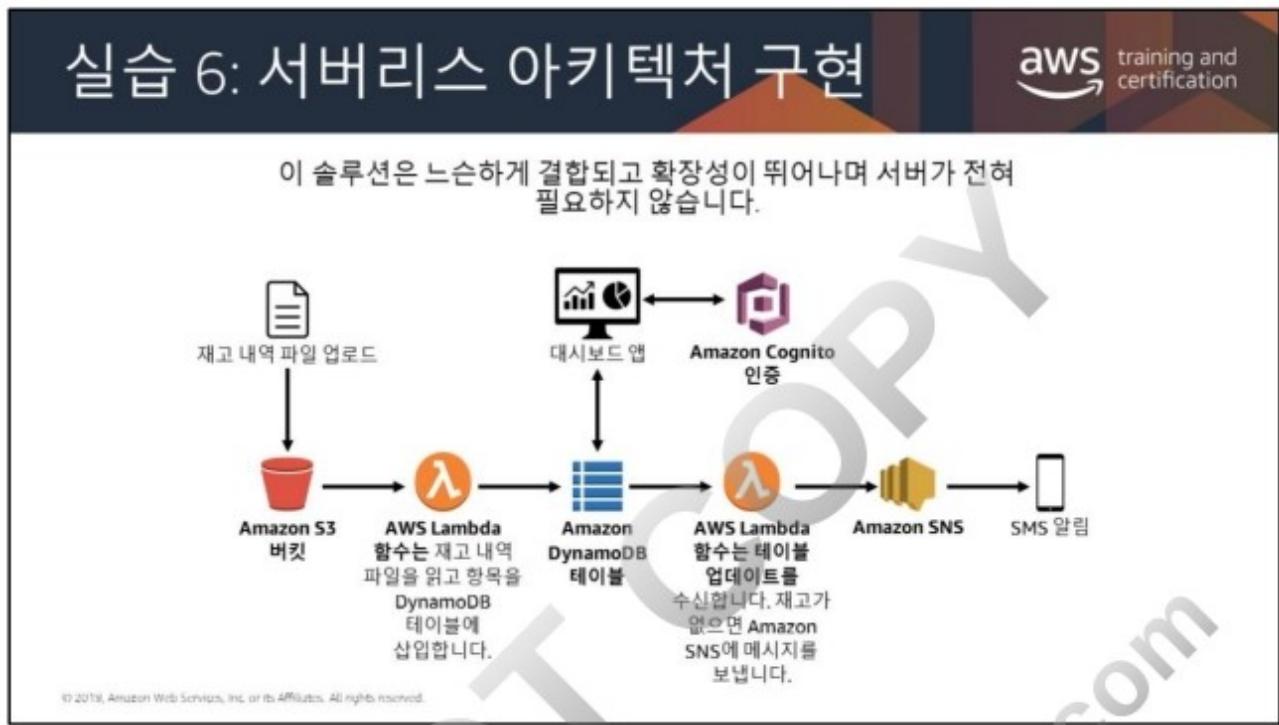
aws training and certification

재고 내역은 서비스 대시보드 앱을 통해 모니터링할 수 있습니다.

The diagram illustrates a serverless architecture. It starts with a file upload icon labeled "재고 내역 파일 업로드" (Inventory file upload) pointing to an "Amazon S3 버킷" (Bucket). An arrow points from the bucket to an "AWS Lambda" function icon. Below the Lambda icon, the text reads: "함수는 재고 내역 파일을 읽고 항목을 DynamoDB 테이블에 삽입합니다." (The function reads the inventory file and inserts items into the DynamoDB table). An arrow points from the Lambda function to an "Amazon DynamoDB 테이블" (Table) icon. From the DynamoDB table, an arrow points up to a "대시보드 앱" (Dashboard app) icon, which is connected to an "Amazon Cognito 인증" (Authentication) icon. The text "대시보드 앱" is also present next to the dashboard icon.

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









모듈 13



아키텍처 측면에서의 필요성

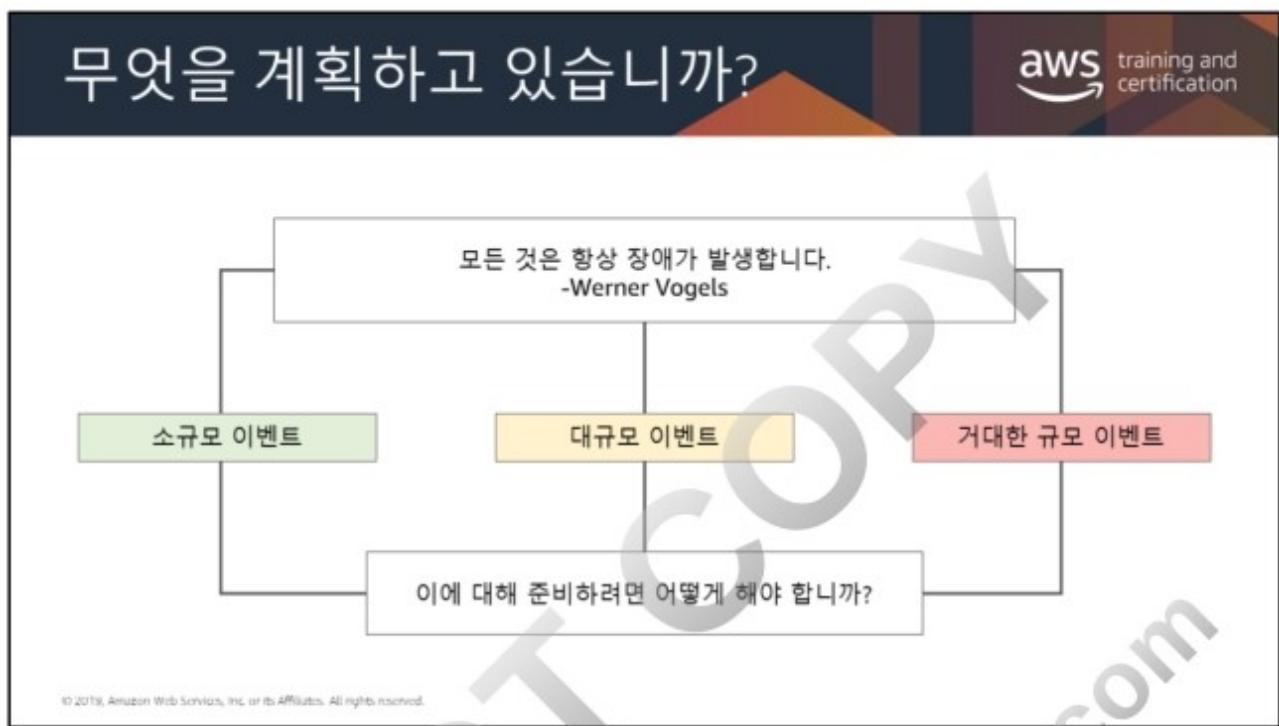
인프라를 사용할 수 없는 경우 적절한 시간 내에 적절한 비용으로 애플리케이션을 다시 실행할 수 있어야 합니다.

모듈 개요

- 재해 복구 계획
- 복구 옵션

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





어떤 종류의 재해에 대비할 계획입니까?

- 복원 및 백업을 가져오기만 하면 되는 소규모 이벤트인가요?
- 여러 리소스가 영향을 받는 비교적 큰 규모의 이벤트인가요?
- 여러 사용자와 리소스가 영향을 받는 거대한 규모의 이벤트인가요?

DR(재해 복구)은 재해 대비 및 복구에 대한 것입니다. 한 기업의 비즈니스 연속성 또는 재무 상태에 부정적인 영향을 미치는 모든 이벤트를 재해라고 할 수 있습니다. 여기에는 하드웨어/소프트웨어 장애, 네트워크 중단, 정전, 화재나 수해 등 건물의 물리적인 손상, 인간의 실수, 그 외 일부 중대한 이벤트가 포함됩니다.

재해의 영향을 최소화하기 위해 기업들은 계획 및 준비, 직원 교육, 프로세스의 문서화 및 업데이트에 많은 시간과 자원을 투자합니다. 특정 시스템에서 재해 복구(DR) 계획에 대한 투자 규모는 잠재적인 중단으로 인한 손실에 따라 현저하게 달라질 수 있습니다.

기존의 물리적 환경을 가진 기업들은 재해 발생시 대체로 예비 용량을 사용할 수 있도록 인프라를 복제해야 합니다. 이러한 인프라는 예상되는 용량 요구 사항을 언제든지 지원할 수 있도록 조달, 설치 및 유지 관리해야 합니다. 인프라는 정상적인 운영 중에 대체로 사용률이 낮거나 과도하게 프로비저닝됩니다.

AWS를 사용하면 귀사에서 필요한 만큼 및 사용량에 따라 인프라를 확장할 수 있습니다. 따라서 Amazon에서 자체 글로벌 웹 사이트 네트워크를 운영할 때 사용하는 것과 동일한 수준의 높은 보안성과 안정성을 갖춘 신속한 인프라를 활용할 수 있습니다. 또한 AWS는 재해 복구(DR) 이벤트 중에 리소스를 신속하게 변경하고 최적화할 수 있는 유연성도 제공하며, 결과적으로 비용을 크게 절감할 수 있습니다.

DO NOT COPY
zlagusdbs@gmail.com

가용성 개념

aws training and certification

고가용성

- 애플리케이션의 가동 중단 시간 최소화

백업

- 데이터를 안전하게 유지합니다.

재해 복구

- 주요 재해 발생 후 애플리케이션 및 데이터 백업을 가져옵니다.

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

프로덕션 시스템은 대체로 가동 시간의 측면에서 정의되었거나 암묵적인 목표를 갖고 있습니다. 시스템은 개별 또는 다수의 구성 요소(예: 하드 디스크, 서버, 네트워크 링크 등)에서 발생하는 장애를 견딜 수 있을 때 **가용성이 높습니다**.

높은 가용성은 중복성 및 내결함성을 제공합니다. 그 목적은 장애가 발생한 경우에도 이러한 서비스를 계속 사용할 수 있도록 하는 데 있습니다.

백업은 데이터를 보호하고 비즈니스 지속성을 유지하는 데 있어 중요합니다. 그와 동시에, 백업을 제대로 구현하는 것은 까다로운 문제가 될 수 있습니다. 데이터가 생성되는 속도는 기하급수적으로 증가하고 있습니다. 그러나 로컬 디스크의 밀도 및 내구성은 데이터만큼 빠른 속도로 증가하지 않고 있습니다. 엔터프라이즈 백업은 그 자체가 하나의 산업이 되었습니다.

데이터는 수많은 엔드포인트, 노트북, 데스크톱, 서버, 가상 머신 및 모바일 디바이스에서 생성되고 있습니다. 즉, 백업 문제는 그 속성상 분산된 상태입니다. 현재 백업 소프트웨어는 중앙 집중적인 특성이 매우 강합니다. 즉, 여러 디바이스에서 데이터를 수집한 후 이를 단일한 곳에 저장하는 것이 일반화되고 있습니다. 때때로 저장된 데이터의 사본은 테이프로 전송되기도 합니다. 중앙 집중식 접근 방식은 재해 복구 중 백업 대상을 압도함으로써 복구 SLA가 손상되는 결과를 초래할 우려가 있습니다.

과거의 엔터프라이즈 백업 시나리오에서는 고성능 데이터 액세스가 필요한 경우, 디스크를 사용해야 했습니다. 비용 효율적인 아카이브 스토리지가 필요한 경우에는 테이프를 사용해야 했습니다. 데이터를 오프사이트에 보관하려면 아카이브 테이프를 물리적으로 다른 위치에 전달해야 했습니다. 테이프에서 뭔가 필요한 것이 없는 한, 로컬 디스크에서 충분히 복구할 수 있었지만 그러한 테이프가 사이트에 없는 경우에는 복구하는 데 꽤 많은 시간이 걸렸을 것입니다.

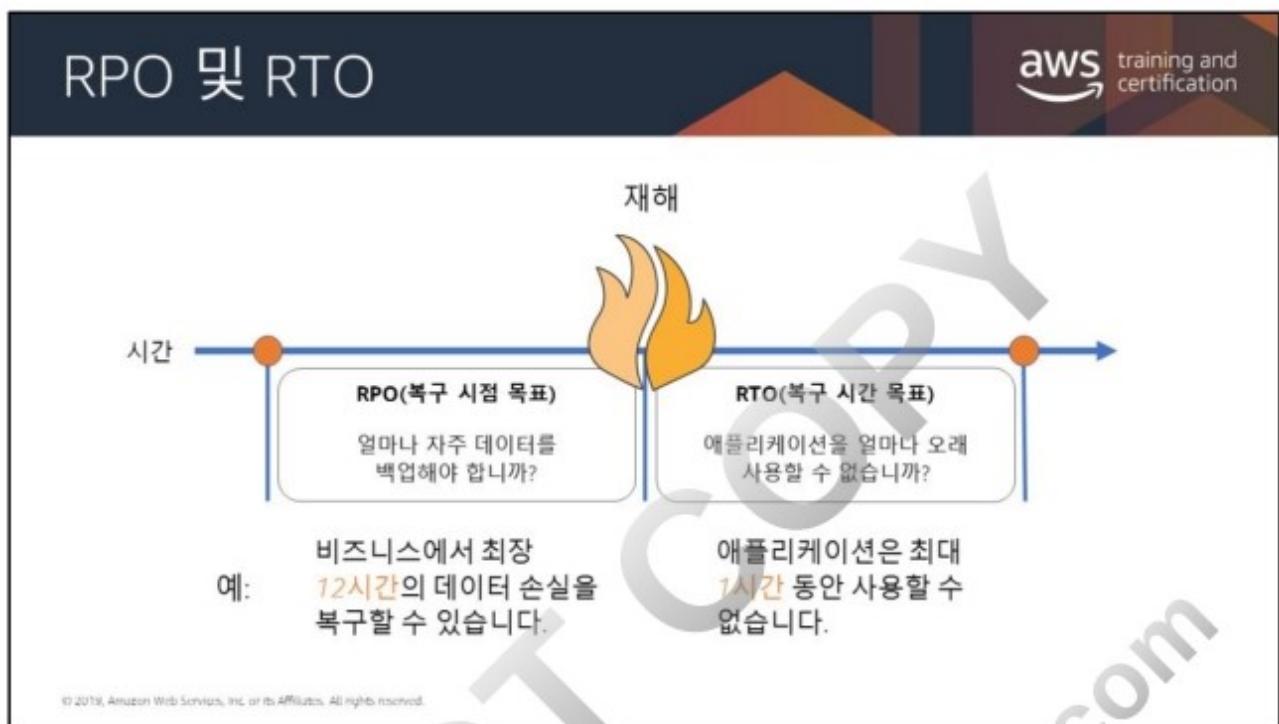
클라우드는 이러한 관행에 변화를 가져왔습니다. 백업 소프트웨어는 그 자체를 변경하지 않고도 클라우드에 작성할 수 있습니다. (이에 대해서는 나중에 설명하기로 하겠습니다.)

재해 복구(DR)은 재해 대비 및 복구에 대해 다룹니다. 재해란 한 기업의 비즈니스 지속성 또는 재무 상태에 부정적인 영향을 미치는 모든 이벤트를 의미하며, 여기에는 하드웨어/소프트웨어 장애, 네트워크 중단, 정전, 건물의 물리적인 손상(화재나 수해 등), 인간의 실수 또는 그 외 일부 중대한 이벤트가 포함됩니다.

재해의 영향을 최소화하기 위해 기업들은 계획 및 준비, 직원 교육, 프로세스의 문서화 및 업데이트에 많은 시간과 자원을 투자합니다. 특정 시스템에서 재해 복구(DR) 계획에 대한 투자 규모는 잠재적인 중단으로 인한 손실에 따라 현저하게 달라질 수 있습니다. 기존의 물리적 환경을 가진 기업들은 재해 발생시 대체로 예비 용량을 사용할 수 있도록 인프라를 복제해야 합니다. 이러한 인프라는 예상되는 용량 요구 사항을 언제든지 지원할 수 있도록 조달, 설치 및 유지 관리해야 합니다. 인프라는 정상적인 운영 중에 대체로 사용률이 낮거나 과도하게 프로비저닝됩니다.



복구 시점 목표(RPO)는 수용 가능한 데이터 손실량을 시간으로 측정한 값입니다. 예를 들면, 어떤 재해가 낮 12시(정오)에 발생하고 RPO가 1시간이라면 시스템은 오전 11시 이전에 시스템에 있던 모든 데이터를 복구해야 합니다. 데이터 손실 구간은 오전 11시부터 낮 12시(정오)까지 1시간에 불과합니다.



복구 시간 목표(RTO)란 운영 수준 계약(OLA)에서 정의한 바와 같이 중단 후 비즈니스 프로세스를 서비스 수준으로 복원하기까지 걸리는 시간을 의미합니다. 예를 들어, 어떤 재해가 낮 12시(정오)에 발생하고 RTO가 8시간이라면 재해 복구(DR) 프로세스는 비즈니스 프로세스를 오후 8시까지 허용 가능한 서비스 수준으로 복원해야 합니다.

일반적으로 회사는 시스템을 가동할 수 없을 때 기업에 미칠 재정적 영향에 근거하여 허용 가능한 RPO 및 RTO를 결정합니다. 회사는 가동 중지 시간 및 시스템 가용성 부족으로 인한 사업 손실 및 회사 평판 손상 등 여러 가지 요인들을 고려하여 재정적 영향을 평가합니다.

그런 다음, IT 조직은 RTO에 따라 수립된 일정 및 서비스 수준의 범위 내에서 RPO에 근거하여 비용 효율적인 시스템 복구를 제공할 수 있는 솔루션을 계획합니다.



AWS는 전 세계 여러 지역에서 사용이 가능하므로, 시스템이 완전히 배포된 사이트 외에도 재해 복구(DR) 사이트 또한 가장 적합한 위치를 선택할 수 있습니다.

리전을 이용할 수 없는 경우는 매우 희박합니다. 그러나 매우 큰 규모의 이벤트(예: 유성 충돌)가 어떤 지역에 영향을 미칠 경우, 실제로 리전을 이용할 수 없습니다.

AWS는 리전별로 제공되는 현재 서비스(리전별 제품 및 서비스)를 목록으로 나열한 페이지를 유지 관리합니다. AWS는 한 리전의 어떤 대규모 이벤트가 다른 리전에 영향을 미치지 않도록 엄격한 리전 격리 정책을 유지합니다. 당사는 고객들이 다중 리전 전략에 대해 유사한 접근 방식을 취할 것을 권장합니다. 각 리전은 다른 리전에 영향을 미치지 않고 오프라인으로 전환할 수 있어야 합니다.

미국 내 AWS 리전과 연결되는 AWS Direct Connect (DX) 회선을 보유하고 있는 경우, 퍼블릭 인터넷을 통한 트래픽 이동 없이 AWS GovCloud (US)를 포함한 미국 내 모든 리전에 액세스할 수 있습니다.

또한 애플리케이션이 배포되는 방법도 고려하십시오. 각 리전에 개별적으로 애플리케이션을 배포할 경우, 재해 발생 시 해당 리전을 격리하고 모든 트래픽을 다른 리전으로 이전할 수 있습니다.

새로운 애플리케이션과 인프라를 신속하게 배포하는 경우, 액티브-액티브 리전이 필요할 수 있습니다. 어떤 리전의 애플리케이션이 사용 불능 상태가 되거나 오작동하는 문제를 야기하는 뭔가를 귀사에서 배포한다고 가정해 보겠습니다. Route 53의 활성 레코드 세트에서 해당 리전을 제거하고 근본 원인을 확인한 다음, 변경 사항을 롤백한 후에 해당 리전을 다시 활성화할 수 있습니다.

DO NOT COPY
zlagusdbs@gmail.com



재해 복구에 대한 다양한 접근법을 논의하기에 앞서 재해 복구와 가장 관련이 있는 AWS 서비스 및 기능들을 검토하는 것이 중요합니다. 이 섹션은 이러한 내용을 요약하고 있습니다.

재해 복구(DR)를 계획할 경우, 데이터 마이그레이션과 영구 스토리지를 지원하는 서비스 및 기능의 사용을 고려하는 것이 중요합니다. 그 이유는 재해가 닥쳤을 때 AWS에 백업한 데이터를 바로 그러한 서비스 및 기능을 통해 복구할 수 있기 때문입니다. AWS에서 시스템의 규모 축소 또는 최대 확장이 수반되는 일부 시나리오의 경우, 컴퓨팅 리소스가 필요한 경우도 있습니다.

재해 발생 중에는 새로운 리소스를 가동하거나 사전 구성된 기존 리소스에 대해 장애 조치를 진행할 필요가 있습니다. 이러한 리소스는 코드 및 콘텐츠뿐만 아니라 DNS 항목, 네트워크 방화벽 규칙 및 가상 머신/인스턴스와 같은 다른 부분들도 포함합니다.



AWS는 데이터를 저장할 수 있는 다양한 방법을 제공합니다. 서비스마다 기능이 다르기 때문에 각 시스템의 요구에 맞는 적절한 서비스를 찾을 수 있습니다.

Amazon S3는 미션 크리티컬 및 기본 데이터 스토리지에 적합하게 설계된, 내구성이 뛰어난 스토리지 인프라를 제공합니다. 객체는 하나의 리전 내에서 99.999999999%(119s)의 내구성을 제공하도록 설계된 여러 시설의 여러 장치에 중복 저장됩니다. AWS는 Amazon S3, AWS MFA, 버킷 정책 및 AWS IAM의 버전 관리를 통해 데이터 보존 및 보관에 대한 추가 보호 기능을 제공합니다. 교차 리전 복제는 버킷 수준의 구성에 속하며, 이러한 구성을 통해 서로 다른 AWS 리전에 있는 여러 버킷에서 객체를 비동기적으로 자동 복사할 수 있습니다. 이러한 버킷을 일컬어 원본 버킷 및 대상 버킷이라고 하며, 이들은 상이한 AWS 계정에서 소유할 수 있습니다.

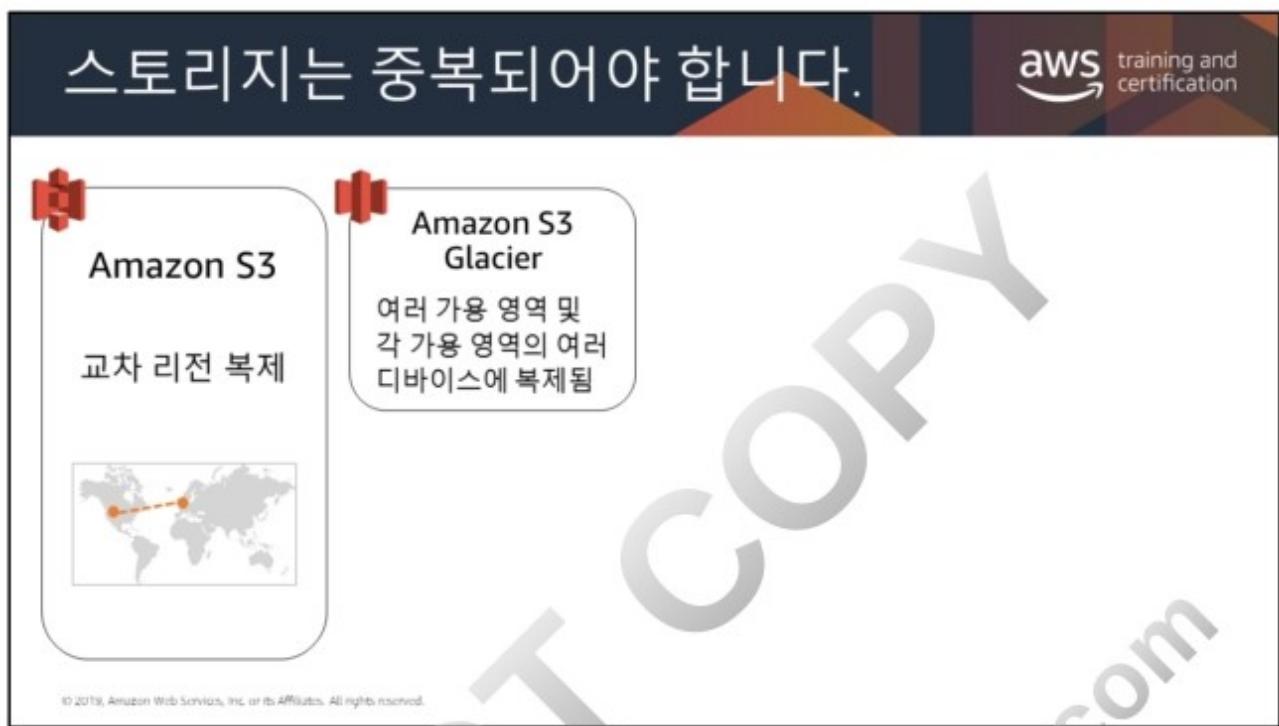
이 기능을 활성화하려면 Amazon S3에게 구성에 따라 객체를 복제하도록 지시하는 복제 구성을 원본 버킷에 추가합니다.

스토리지는 중복되어야 합니다.

Amazon S3
교차 리전 복제

Amazon S3 Glacier
여러 가용 영역 및
각 가용 영역의 여러
디바이스에 복제됨

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



Amazon S3 Glacier는 데이터 보관 및 백업을 위한 스토리지를 매우 저렴한 비용으로 제공합니다. 객체(또는 Amazon S3 Glacier에서 아카이브)는 몇 시간 정도의 검색 시간이면 충분한 수준의 빈번하지 않은 액세스에 최적화되어 있습니다. Amazon S3 Glacier는 Amazon S3와 동일한 내구성을 구현하도록 설계되었습니다. Amazon S3 Glacier에 업로드하는 데이터의 자체 인덱스는 사용자가 유지해야 하지만 재해 복구 또는 비정기적인 조정 작업을 위해 각 저장소에 있는 모든 아카이브의 인벤토리가 유지 관리됩니다. 저장소 인벤토리는 대략 하루에 한 번 업데이트됩니다. 저장소 인벤토리는 JSON 또는 CSV 파일 형태로 요청할 수 있으며 크기, 생성 날짜 및 아카이브 설명(업로드 시 제공한 경우)을 비롯하여 저장소에 포함된 아카이브에 대한 세부 정보를 포함합니다. 인벤토리는 가장 최근에 인벤토리 업데이트가 이루어진 시점의 저장소 상태를 표시합니다.

Amazon S3와 마찬가지로 Amazon S3 Glacier도 교차 리전 복제가 가능합니다.

스토리지는 중복되어야 합니다.

aws training and certification

Amazon S3
교차 리전 복제



Amazon S3 Glacier
여러 가용 영역 및 각 가용 영역의 여러 디바이스에 복제됨

Amazon EBS

- 특정 시점 볼륨 스냅샷 생성
- 리전 및 계정 간의 스냅샷 복사

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

Amazon EBS는 데이터 볼륨의 특정 시점 스냅샷을 생성하는 기능을 제공합니다. 이 스냅샷은 새로운 Amazon EBS 볼륨의 시작 지점으로 사용할 수 있으며, 사용자의 데이터는 장기간 내구성을 위해 보호할 수 있는데 그 이유는 스냅샷이 Amazon S3에 저장되기 때문입니다. 볼륨이 생성되면 실행 중인 Amazon EC2 인스턴스에 연결할 수 있습니다. Amazon EBS 볼륨은 인스턴스의 수명에 관계없이 지속되는 오프 인스턴스 스토리지를 제공하는데, 이 스토리지는 가용 영역의 여러 서버에 걸쳐 복제되기 때문에 단일 구성 요소의 장애로 인해 데이터가 손실되는 것을 방지합니다. 하나의 스냅샷을 생성해 이를 Amazon S3에 복사했다면(스냅샷 상태가 완료된 경우) 한 AWS 리전에서 다른 리전 또는 동일한 리전 내에서 해당 스냅샷을 복사할 수 있습니다. Amazon S3 서버 측 암호화(256비트 AES)는 복사 작업을 진행하는 동안 스냅샷의 전송 중 데이터를 보호합니다. 스냅샷 복사본은 원본 스냅샷의 ID와는 다른 ID를 받습니다.

스토리지는 중복되어야 합니다.

aws training and certification

Amazon S3
교차 리전 복제



Amazon S3 Glacier
여러 가용 영역 및 각 가용 영역의 여러 디바이스에 복제됨

Amazon EBS

- 특정 시점 볼륨 스냅샷 생성
- 리전 및 계정 간의 스냅샷 복사

AWS Snowball
고속 인터넷보다 대용량(10TB 초과) 데이터를 더 빨리 전송합니다.



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

AWS Snowball은 물리적 전송 시 보안을 유지하도록 설계된 스토리지 디바이스를 사용해 AWS에서 테라바이트(TB) ~ 페타바이트(PB) 규모의 데이터 송수신을 가속화할 수 있는 데이터 전송 솔루션입니다. Snowball을 사용하면 고속 네트워크 비용, 오랜 전송 시간, 보안 문제 등 대규모 데이터 전송과 관련해 발생할 수 있는 문제들을 없애는데 도움이 됩니다. Amazon S3에 저장되어 있는 많은 양의 데이터를 빠르게 검색해야 할 경우, Snowball 디바이스는 고속 인터넷보다 훨씬 더 빠르게 데이터를 검색하는 데 도움을 줄 수 있습니다.

스토리지는 중복되어야 합니다.

aws training and certification

Amazon S3
교차 리전 복제

Amazon S3 Glacier
여러 가용 영역 및 각 가용 영역의 여러 디바이스에 복제됨

AWS Snowball
고속 인터넷보다 대용량(10TB 초과) 데이터를 더 빨리 전송합니다.

Amazon EBS

- 특정 시점 볼륨 스냅샷 생성
- 리전 및 계정 간의 스냅샷 복사

AWS DataSync

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

Amazon DataSync를 사용하면 오픈 소스 도구보다 최대 10배 빠른 속도로 온프레미스 파일 시스템 또는 클라우드 내 파일 시스템에서 Amazon EFS(Amazon Elastic File System)로 효율적이면서도 안전하게 파일을 동기화할 수 있습니다. AWS DataSync는 인터넷 또는 DX 연결을 통해 파일을 안전하면서도 효율적으로 복사합니다.

자세한 내용은 다음을 참조하십시오. <https://aws.amazon.com/datasync/>

컴퓨팅 백업 조정은 쉬워야 합니다.

aws training and certification

새로운 서버 인스턴스 또는 컨테이너를 몇 분 내에 확보하고 부팅합니다.

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

사용자가 제어하는 가상 머신을 신속하게 생성할 수 있는 기능은 재해 복구(DR) 상황에서 매우 중요합니다. 별도의 가용 영역에서 인스턴스를 시작함으로써 단일 위치에서 장애가 발생할 경우 애플리케이션을 보호할 수 있습니다.

기본 하드웨어의 시스템 상태 검사가 실패할 경우, EC2 인스턴스의 자동 복구를 준비할 수 있습니다. 인스턴스는 (필요하다면 새 하드웨어에서) 재부팅되지만 해당 인스턴스 ID, IP 주소, 탄력적 IP 주소, EBS 볼륨 연결 및 그 밖의 구성 세부 정보는 그대로 유지됩니다. 복구가 완료되려면 초기화 프로세스의 일환에서 인스턴스가 어떤 서비스 또는 애플리케이션을 자동으로 시작하는지 여부를 확인해야 합니다.

Amazon 머신 이미지(AMI)는 운영 체제에 맞춰 사전 구성되며, 일부 사전 구성된 AMI에는 애플리케이션 스택이 포함될 수도 있습니다. 또한 나만의 AMI를 구성할 수도 있습니다. 재해 복구(DR)의 측면에서 AWS는 사용자가 나만의 AMI를 구성하고 식별한 후 복구 절차의 일환으로 이러한 AMI를 실행할 것을 적극 권장하고 있습니다. 이러한 AMI는 귀하가 선택한 운영 체제 및 적절한 애플리케이션 스택으로 사전 구성해야 합니다.

네트워킹 재해 복구 옵션

aws training and certification

Amazon Route 53

- 트래픽 분산
- 장애 조치

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

재해를 처리하는 경우, 사용 중인 시스템이 다른 장소에서 장애 조치를 진행할 때 네트워크 설정을 수정해야 할 가능성이 큽니다. AWS는 Amazon Route 53, ELB, Amazon VPC 및 DX와 같은 네트워크 설정을 관리하고 수정할 수 있도록 여러 가지 서비스 및 기능을 제공합니다.

Amazon Route 53은 (DNS 엔드포인트 상태 검사와 같은 DR 시나리오를 처리할 때 효과적일 수 있는) 수많은 글로벌 로드 밸런싱 기능들은 물론, 다수의 엔드포인트와 심지어는 Amazon S3에서 호스팅되는 정적 웹 사이트 간에 장애 조치를 실행하는 기능도 포함하고 있습니다.

네트워킹 재해 복구 옵션

aws training and certification

Amazon Route 53

- 트래픽 분산
- 장애 조치

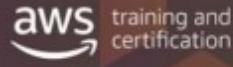
Elastic Load Balancing

- 로드 밸런싱
- 상태 확인 및 장애 조치

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

ELB는 수신되는 애플리케이션 트래픽을 여러 Amazon EC2 인스턴스에 자동으로 분산합니다. 따라서 수신되는 애플리케이션 트래픽에 응답하는데 필요한 로드 밸런싱 용량을 원활하게 제공함으로써 애플리케이션의 내결함성을 훨씬 더 크게 높일 수 있습니다. Elastic IP 주소를 사전 할당하는 것과 마찬가지로, 로드 밸런서를 사전 할당하면 DNS 이름을 미리 알 수 있어 재해 복구 계획을 간단히 실행할 수 있습니다.

네트워킹 재해 복구 옵션



Amazon Route 53

- 트래픽 분산
- 장애 조치

Elastic Load Balancing

- 로드 밸런싱
- 상태 확인 및 장애 조치

Amazon VPC

기존 온프레미스 네트워크 토플로지를 클라우드로 확장합니다.

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

DR의 맥락에서 **Amazon VPC**를 사용하면 기존 네트워크 토플로지를 클라우드로 확장할 수 있습니다. 이는 대체로 내부 네트워크에 위치한 엔터프라이즈 애플리케이션을 복구할 때 매우 적합할 수 있습니다.

네트워킹 재해 복구 옵션

aws training and certification

Amazon Route 53

- 트래픽 분산
- 장애 조치

Elastic Load Balancing

- 로드 밸런싱
- 상태 확인 및 장애 조치

Amazon VPC

기존 온프레미스 네트워크 토플로지를 클라우드로 확장합니다.

AWS Direct Connect

클라우드로 대규모 온프레미스 환경의 빠르고 일관적인 복제/백업

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

Amazon Direct Connect (DX)를 사용해 온프레미스에서 AWS로 전용 네트워크 연결을 간편하게 설정할 수 있습니다. 대개의 경우, 이 서비스는 네트워크 비용을 줄이고 대역폭 처리량을 높이며 인터넷 기반 연결보다 더 일관된 네트워크 환경을 제공할 수 있습니다.

크리티컬 워크로드를 위한 높은 복원력의 AWS Direct Connect 사용 방법에 대한 정보는 <https://aws.amazon.com/directconnect/resiliency-recommendation/> 단원을 참조하십시오.

The slide has a dark blue header with white text: "데이터베이스는 백업 및 중복되어야 합니다." In the top right corner is the "aws training and certification" logo. A large, diagonal watermark reading "NOT COPY" is overlaid across the slide. The main content area has a white background with a blue rounded rectangle containing the title "Amazon RDS". Below it is a bulleted list:

- 스냅샷 데이터를 별도의 리전에 저장합니다.
- 읽기 전용 복제본을 다중 AZ와 결합하여 복원력이 뛰어난 재해 복구 전략을 수립합니다.
- 자동 백업

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

다양한 데이터베이스 요구 사항을 위해 Amazon RDS, Amazon DynamoDB 및 Amazon Redshift와 같은 AWS 서비스의 사용을 고려하십시오.

Amazon RDS를 이미 실행 중인 데이터베이스에 있는 중요 데이터를 보존할 목적으로 재해 복구(DR) 준비 단계에서 사용하거나 혹은 프로덕션 데이터베이스를 실행하기 위해 복구 단계에서 사용할 수도 있습니다. 여러 리전에서 보고 싶을 때 Amazon RDS는 한 리전에서 다른 리전으로 데이터를 스냅샷하고 다른 리전에서 읽기 복제본을 실행하는 기능을 제공합니다. Amazon RDS를 사용하면 수동 DB 스냅샷 또는 DB 클러스터 스냅샷을 공유할 수 있습니다. 최대 20개의 다른 AWS 계정과 수동 스냅샷을 공유할 수 있습니다. 암호화되지 않은 수동 스냅샷을 퍼블릭으로 공유할 수도 있습니다. 이렇게 하면 모든 AWS 계정에서 해당 스냅샷을 사용할 수 있습니다. 스냅샷을 퍼블릭으로 공유할 경우 사용자의 프라이빗 정보가 퍼블릭 스냅샷에 포함되지 않도록 주의하십시오.

MySQL 및 MariaDB용 Amazon RDS 읽기 전용 복제본은 다중 AZ 배포를 지원합니다. 읽기 전용 복제본을 다중 AZ와 결합하면 탄력적인 재해 복구 전략을 수립하고 데이터베이스 엔진 업그레이드 프로세스를 간소화할 수 있습니다. Amazon RDS 읽기 전용 복제본을 사용하면 동일한 AWS 리전 또는 상이한 AWS 리전에서 데이터베이스 인스턴스에 대해 하나 이상의 읽기 전용 사본을 생성할 수 있습니다. 원본 데이터베이스에 적용된 업데이트는 읽기 전용 복제본에 비동기적으로 적용됩니다. 읽기 전용 복제본은 읽기 작업이 많은 워크로드에 대한 확장성을 제공할 뿐만 아니라 필요 시 독립실행형 데이터베이스로 승격될 수 있습니다.

데이터베이스는 백업 및 중복되어야 합니다.

Amazon RDS

- 데이터 스냅샷을 생성해 별도의 리전에 저장합니다.
- 읽기 전용 복제본을 다중 AZ와 결합하여 복원력이 뛰어난 재해 복구 전략을 수립합니다.
- 자동 백업 보존

Amazon DynamoDB

- 전체 테이블을 몇 초 안에 백업합니다.
- 특정 시점 복구를 사용하여 최대 35일 동안 지속적으로 테이블을 백업합니다.
- 콘솔에서 한 번 클릭하거나 단일 API 호출로 백업을 시작합니다.
- 전역 테이블로 전 세계에 분산된 앱의 빠른 로컬 성능을 위한 다중 리전, 다중 마스터 테이블 생성

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

준비 단계에서 **Amazon DynamoDB**를 사용하면 다른 리전의 DynamoDB 또는 Amazon S3에 데이터를 복사할 수 있습니다. DR의 복구 단계에서는 단 한 번의 마우스 클릭이나 API 호출로 몇 분 만에 원활하게 확장할 수 있습니다.

전역 테이블은 DynamoDB의 글로벌 풋프린트를 기반으로 구축되어 있어 완전관리형의 다중 리전 멀티 마스터 데이터베이스를 제공하는데, 이 데이터베이스는 대규모로 확장된 글로벌 애플리케이션에 대해 신속한 로컬 읽기 및 쓰기 성능을 제공합니다. 전역 테이블은 사용자가 선택한 AWS 리전에 걸쳐 Amazon DynamoDB 테이블을 자동으로 복제합니다.

전역 테이블을 사용하면 리전 간에 데이터를 복제하고 업데이트 충돌을 해결해야 하는 어려운 작업을 수행할 필요가 없기 때문에 애플리케이션의 비즈니스 로직에 집중할 수 있습니다. 또한 전역 테이블을 사용하면 좀처럼 볼 수 없는 전체 리전의 격리 또는 성능 저하가 발생할 경우에도 애플리케이션의 가용성을 높은 수준으로 유지할 수 있습니다.

자동화를 사용하여 신속하게 복구합니다. 

 AWS
CloudFormation

템플릿을 사용하여 필요에 따라 리소스 모음을 신속하게 배포합니다.

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

zlagu COPY.com

AWS CloudFormation을 사용하면 텍스트 파일로 전체 인프라를 모델링할 수 있습니다. 이 템플릿은 인프라의 단일 정보 소스가 됩니다. 그러면 조직 전체에서 사용되는 인프라 구성 요소를 표준화하여 구성 규정을 준수하고 문제를 더 빠르게 해결할 수 있습니다.

AWS CloudFormation은 리소스를 안전하고 반복 가능한 방식으로 프로비저닝하므로 수작업을 수행하거나 사용자 지정 스크립트를 작성할 필요 없이 인프라와 애플리케이션을 구축 및 재구축 할 수 있습니다. AWS CloudFormation에서는 스택을 관리할 때 수행해야 할 적절한 작업을 결정하고, 오류가 탐지되면 변경 사항을 자동으로 롤백합니다.

자동화를 사용하여 신속하게 복구합니다. 

AWS CloudFormation
템플릿을 사용하여 필요에 따라 리소스 모음을 신속하게 배포합니다.

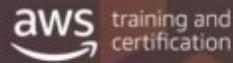
AWS Elastic Beanstalk
단 몇 번의 클릭으로 전체 스택을 빠르게 재배포합니다.

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

AWS Elastic Beanstalk을 사용하여 업데이트된 원본 번들을 업로드한 후 AWS Elastic Beanstalk 환경에 배포하거나 이전에 업로드한 버전을 다시 배포할 수 있습니다.

이전에 업로드한 애플리케이션 버전을 환경에 배포할 수 있습니다.

자동화를 사용하여 신속하게 복구합니다.



AWS CloudFormation
템플릿을 사용하여 필요에 따라 리소스 모음을 신속하게 배포합니다.

AWS Elastic Beanstalk
단 몇 번의 클릭으로 전체 스택을 빠르게 재배포합니다.

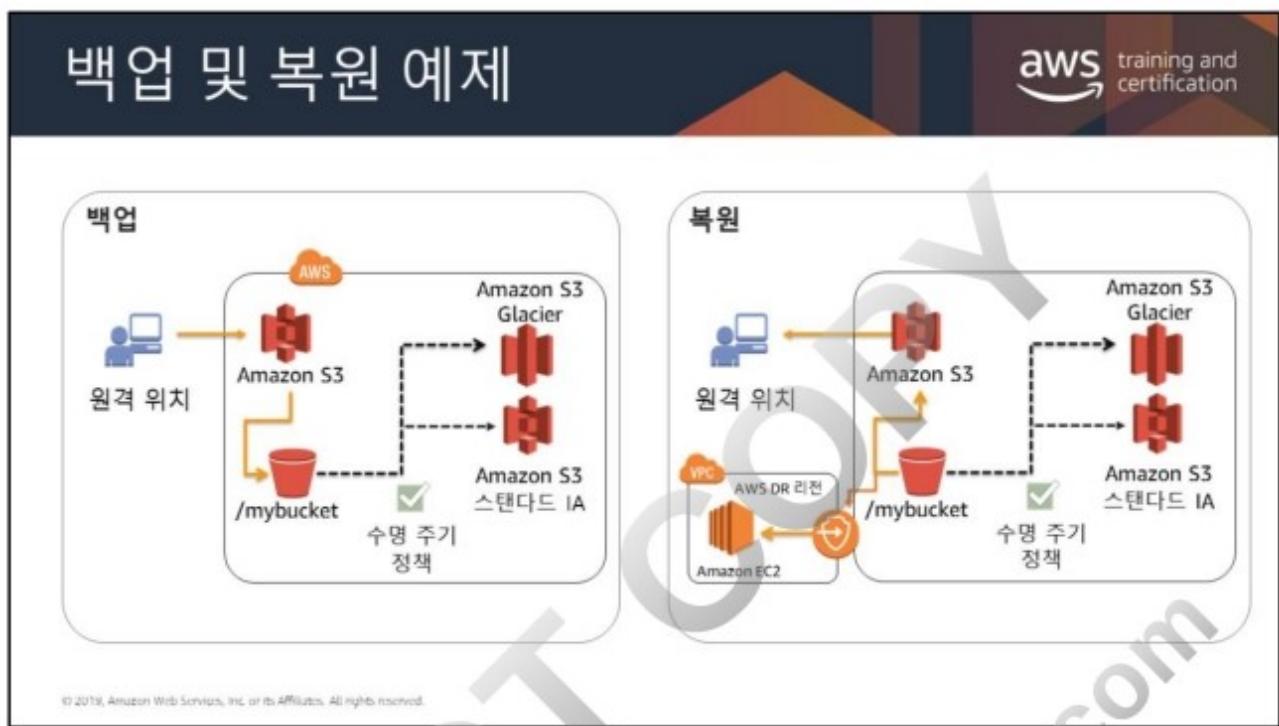
AWS OpsWorks

- 자동 호스트 교체
- 복구 단계에서 AWS CloudFormation과 결합합니다.
- 정의된 RTO를 지원하는 새로운 스택을 제공합니다.

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS OpsWorks는 모든 유형과 규모의 애플리케이션을 간편하게 배포하고 운영할 수 있는 애플리케이션 관리 서비스입니다. 사용자의 환경은 일련의 계층으로서 정의할 수 있으며, 각 계층은 애플리케이션 티어로 구성할 수 있습니다. AWS OpsWorks는 자동 호스트 교체를 포함하고 있기 때문에 인스턴스 장애가 발생하면 자동으로 교체됩니다. 준비 단계에서 AWS OpsWorks를 사용하면 환경을 템플릿으로 만들 수 있으며, 복구 단계에서 AWS CloudFormation과 결합할 수 있습니다. 정의된 RTO를 지원하는 저장된 구성에서 새 스택을 신속하게 프로비저닝할 수 있습니다.

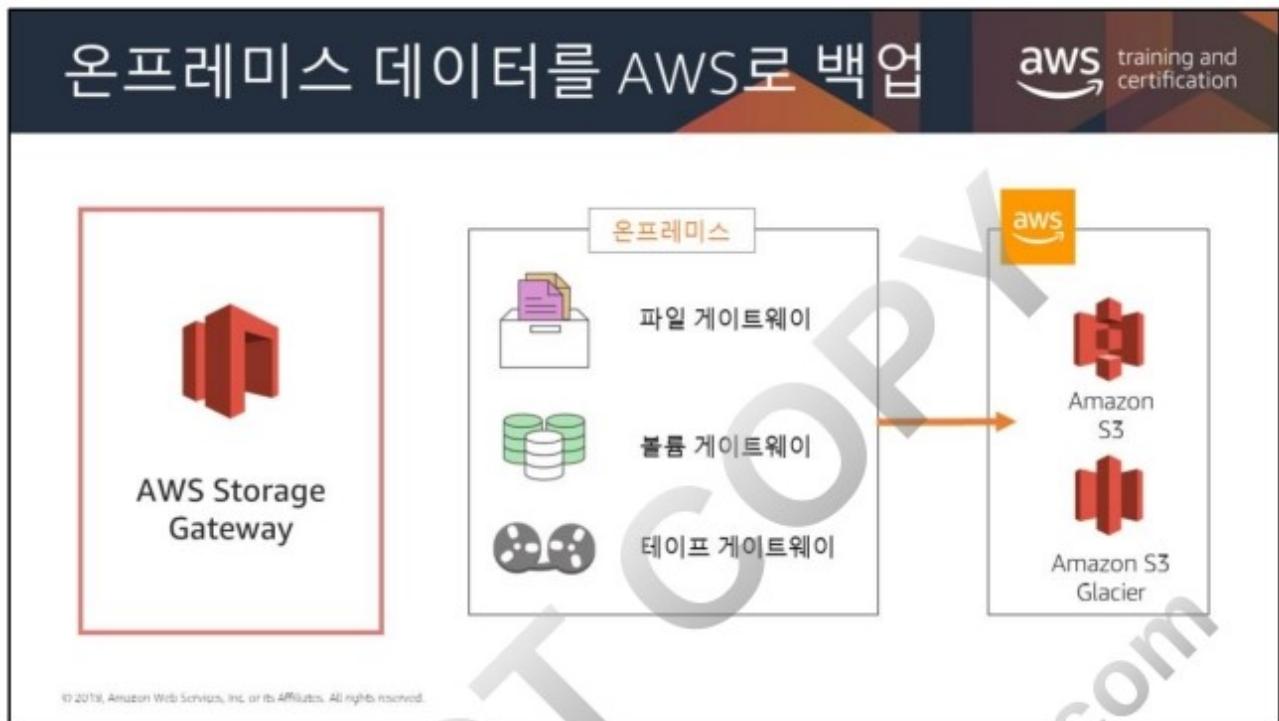




대부분의 기존 환경에서는 데이터를 테이프에 백업하여 정기적으로 오프사이트로 전송합니다. 이 방법을 사용할 경우, 가동 중단 또는 재해 발생 시 시스템을 복원하는 데 많은 시간이 걸릴 수 있습니다.

Amazon S3는 복원을 수행하기 위해 급하게 필요할 수 있는 백업 데이터를 위한 이상적인 대상입니다. Amazon S3와 데이터를 주고 받는 과정은 주로 네트워크를 통해 이루어지므로 어떤 위치에서든 액세스가 가능합니다. Amazon S3와 통합되는 다양한 상용 및 오픈 소스 백업 솔루션이 있습니다. 예:

- AWS Snowball을 사용하면 스토리지 디바이스를 AWS에 직접 연결하여 대규모의 데이터 세트를 전송할 수 있습니다.
- 몇 시간의 검색 시간으로 충분한 장기간 데이터 저장의 경우, Amazon S3와 동일한 내구성 모델을 가진 Amazon S3 Glacier가 있습니다. Amazon S3 Glacier 및 Amazon S3를 함께 사용하면 계층화된 백업 솔루션을 생성할 수 있습니다.



AWS Storage Gateway는 온프레미스 소프트웨어 어플라이언스를 클라우드 기반 스토리지와 연결하여 온프레미스 IT 환경과 AWS 스토리지 인프라 간에 원활하면서도 매우 안전한 통합을 제공합니다. 이 서비스를 사용하면 확장 가능하고 비용 효율적인 스토리지인 AWS 클라우드에 데이터를 안전하게 저장할 수 있습니다. Storage Gateway는 기존 애플리케이션과 연동하는 업계 표준 스토리지 프로토콜을 지원하는 동시에 Amazon S3 또는 Amazon S3 Glacier에서 암호화된 모든 데이터를 안전하게 저장합니다.

AWS Storage Gateway를 사용하면 AWS 관리 서비스를 로컬로 확장할 수 있습니다. 이 서비스는 Amazon CloudWatch, AWS CloudTrail, AWS KMS, AWS IAM 등과도 통합됩니다.

AWS Storage Gateway는 파일, 볼륨 및 테이프라는 3가지 스토리지 인터페이스를 지원합니다. 각 게이트웨이에서는 1가지 유형의 인터페이스를 제공할 수 있습니다.

파일 게이트웨이를 사용하면 NFS 및 SMB 파일 프로토콜을 사용하여 Amazon S3에서 객체를 저장 및 검색할 수 있습니다. 파일 게이트웨이를 통해 작성된 객체는 S3에서 직접 액세스할 수 있습니다.

볼륨 게이트웨이는 iSCSI 프로토콜을 사용하여 애플리케이션에 블록 스토리지를 제공합니다. 볼륨의 데이터는 Amazon S3에 저장됩니다. AWS에서 iSCSI 볼륨에 액세스하려면 EBS 볼륨을 생성하는 데 사용될 수 있는 EBS 스냅샷을 작성할 수 있습니다.

테이프 게이트웨이는 백업 애플리케이션에 가상 미디어 체인저 및 가상 테이프 드라이브로 구성된 iSCSI 가상 테이프 라이브러리(VTL) 인터페이스를 제공합니다. 가상 테이프 데이터는 Amazon S3에 저장되거나 Amazon S3 Glacier에 보관할 수 있습니다.

AWS 클라우드에 온프레미스 데이터를 백업하려면 다음의 두 가지 일반적인 방식 중 한 가지를 선택하면 됩니다.

- AWS 서비스에 API 호출을 실행하여 Amazon S3에 백업 데이터를 직접 작성합니다.
- 인터넷에서 안전한 HTTP PUT 및 GET 요청을 통해 백업 데이터를 직접 작성하거나 검색합니다. 여기서 엔드포인트가 Amazon S3에 직접 연결되어 데이터를 작성 및 검색합니다.

게이트웨이 가상 테이프 라이브러리(VTL)

가상 테이프 컬렉션을 무제한으로 보유할 수 있습니다.

각 가상 테이프는 Amazon S3에서 지원하는 가상 테이프 라이브러리에 저장하거나 혹은 Amazon S3 Glacier에서 지원하는 가상 테이프 선반에 저장할 수 있습니다.

게이트웨이 캐싱 볼륨

기본 데이터는 Amazon S3에 저장하고 자주 액세스하는 데이터는 로컬에 보관할 수 있습니다. 게이트웨이 캐싱 볼륨은 기본 스토리지에서 상당한 비용 절감을 제공하며 온프레미스로 스토리지를 확장할 필요성을 최소화하고 자주 액세스하는 데이터에 대해 액세스 지연 시간을 짧게 유지합니다.

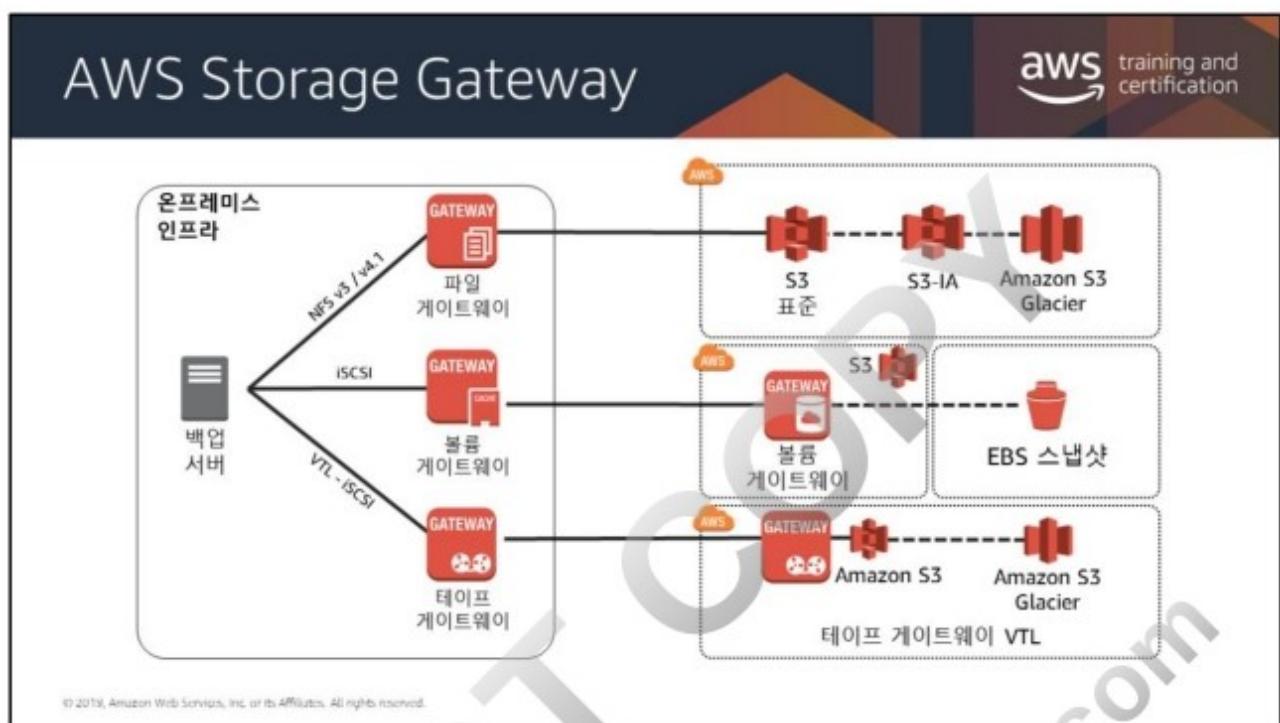
게이트웨이 저장 볼륨

전체 데이터 세트에 액세스 시 지연 시간이 짧아야 하는 경우 기본 데이터를 로컬에 저장하도록 온프레미스 데이터 게이트웨이를 구성하고 이 데이터의 특정 시점 스냅샷을 비동기적으로 Amazon S3에 백업할 수 있습니다.

AWS Storage Gateway 하드웨어 어플라이언스

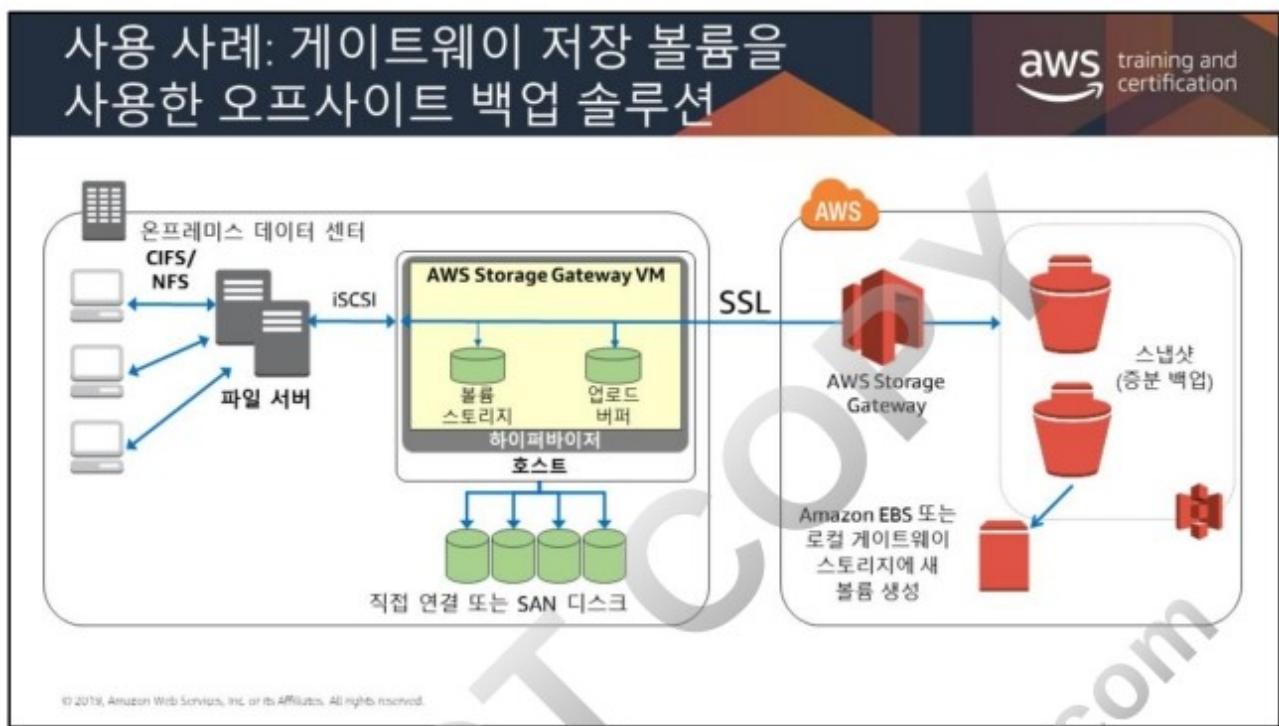
AWS Storage Gateway 하드웨어 어플라이언스는 온프레미스에 설치할 수 있는 타사 서버에 미리 설치된 AWS Storage Gateway 소프트웨어를 제공하는 하드웨어 어플라이언스입니다. AWS Storage Gateway 하드웨어 어플라이언스는 AWS Management Console의 하드웨어 페이지에서 관리할 수 있습니다.

<https://docs.aws.amazon.com/storagegateway/latest/userguide/HardwareAppliance.html>



NFS v3 및 v4.1 프로토콜 외에 AWS Storage Gateway 서비스는 파일 게이트웨이에 SMB(서버 메시지 블록) 프로토콜을 추가했습니다. 이 프로토콜은 Microsoft Windows용으로 개발된 파일 기반 애플리케이션에서 손쉽게 Amazon Simple Storage Service (S3)에 객체를 저장하고 해당 객체에 액세스할 수 있도록 지원합니다. 자세한 내용은 다음을 참조하십시오.

<https://aws.amazon.com/about-aws/whats-new/2018/06/aws-storage-gateway-adds-smb-support-to-store-objects-in-amazon-s3/>



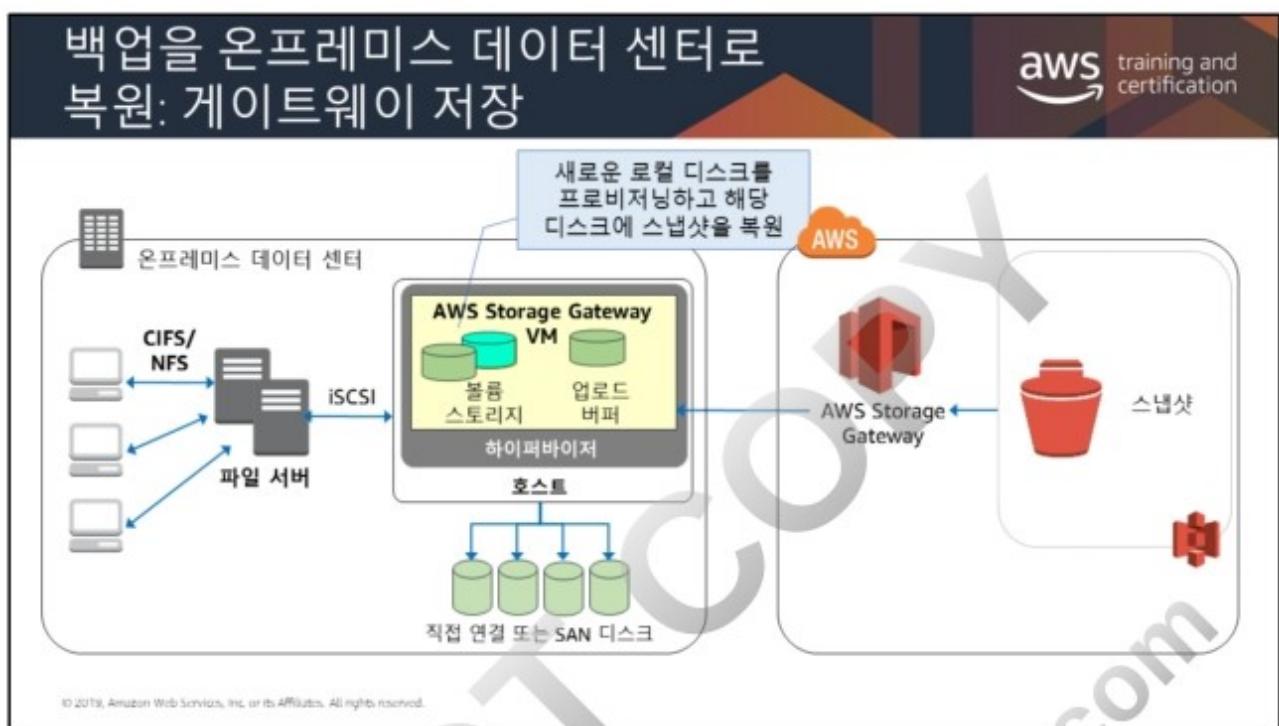
AWS Storage Gateway 소프트웨어 어플라이언스(가상 머신)를 데이터 센터의 호스트에 설치하고 활성화하면 게이트웨이 스토리지 볼륨을 생성하여 온프레미스 Direct Attached Storage (DAS) 또는 Storage Area Network (SAN) 디스크에 매핑할 수 있습니다. 새 디스크로 진행해도 되고, 데이터를 이미 저장하고 있는 디스크로 진행해도 됩니다. 그리고 나서 이러한 스토리지 볼륨을 온프레미스 애플리케이션 서버에 iSCSI 디바이스로서 마운트할 수 있습니다. 온프레미스 애플리케이션이 데이터를 게이트웨이 저장 볼륨에서 쓰고 읽으면 이 데이터는 볼륨에 할당된 디스크에 저장되고 검색됩니다.

Amazon S3로의 업로드를 준비하기 위해 게이트웨이는 업로드 버퍼라고 불리는 스테이징 영역에도 수신 데이터를 저장합니다. 온프레미스 DAS 또는 SAN 디스크를 작업 스토리지로 사용할 수 있습니다. 게이트웨이는 업로드 버퍼의 데이터를 암호화된 Secure Sockets Layer (SSL) 연결을 통해 AWS 클라우드에서 실행되는 AWS Storage Gateway 서비스로 업로드합니다. 이때 서비스는 Amazon S3에 데이터를 암호화하여 저장합니다.

스냅샷이라고 불리는 저장 볼륨에 대한 증분 백업을 실행할 수 있습니다. 게이트웨이는 Amazon S3의 이러한 스냅샷을 Amazon EBS로 저장합니다. 새 스냅샷을 만들 때 마지막 스냅샷 이후에 변경된 데이터만 저장됩니다. 스냅샷은 예정된 시간에 또는 일회성으로 시작할 수 있습니다. 스냅샷을 삭제할 때는 다른 스냅샷에 필요하지 않은 데이터만 제거됩니다.

데이터의 백업을 복원해야 할 경우, Amazon EBS 스냅샷을 온프레미스 게이트웨이 스토리지 볼륨에 복원할 수 있습니다. 또한 스냅샷을 새 Amazon EBS 볼륨의 기반으로 사용한 다음, Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스에 연결할 수 있습니다.

DO NOT COPY
zlagusdbs@gmail.com

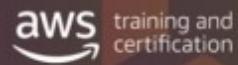


게이트웨이 저장 볼륨의 경우, 볼륨 데이터가 온프레미스에 저장됩니다. 이 경우, 스냅샷이 Amazon S3에 지속적인 오프사이트 백업을 제공합니다. 예를 들어, 스토리지 볼륨으로 할당된 로컬 디스크가 손상된 경우 새로운 로컬 디스크를 프로비저닝하고 볼륨 생성 과정 중에 스냅샷으로 복원할 수 있습니다. (이 방법에 대한 자세한 내용은

<http://docs.aws.amazon.com/storagegateway/latest/userguide/ApplicationStorageVolumesStored-Adding.html>에서 Adding a Storage Volume을 참조하십시오).

게이트웨이 저장 볼륨으로의 스냅샷 복원을 시작하고 나면 백그라운드에 스냅샷 데이터가 다운로드됩니다. 이 기능으로 스냅샷에서 볼륨을 생성한 후 Amazon S3에서 볼륨으로 모든 데이터가 전송될 때까지 기다리지 않아도 애플리케이션에서 볼륨과 모든 데이터에 액세스할 수 있습니다. 애플리케이션에서 아직 로드되지 않은 데이터에 액세스하는 경우, 게이트웨이는 요청된 데이터를 즉시 Amazon S3에서 다운로드하며, 백그라운드에서 볼륨의 나머지 데이터 로드를 진행합니다.

백업 및 복원

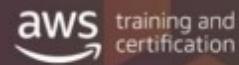


준비 단계

- 현재 시스템을 백업합니다.
- Amazon S3에 백업을 저장합니다.
- AWS의 백업으로부터 복원하는 절차를 기술합니다.
 - 사용할 AMI(필요하면 자체 AMI를 구성)
 - 백업으로부터 시스템을 복원하는 방법
 - 새로운 시스템으로 전환하는 방법
 - 배포를 구성하는 방법

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

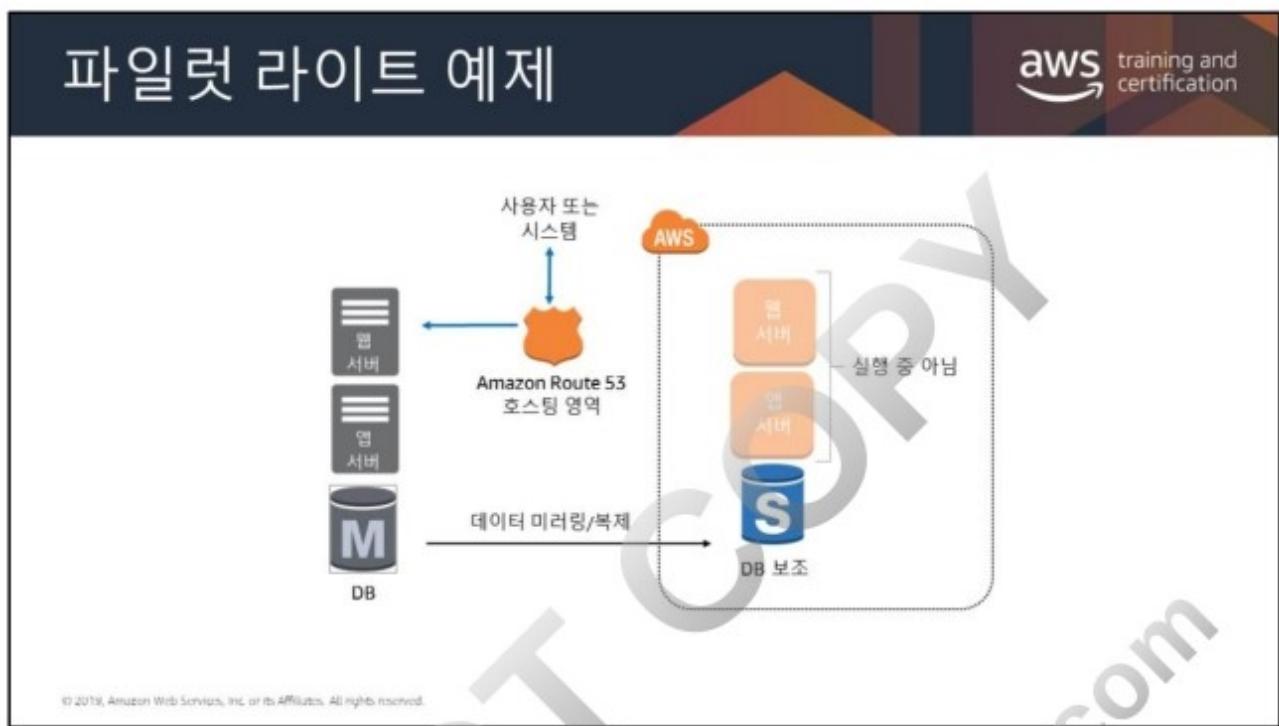
백업 및 복원



재해 발생 시:

- Amazon S3로부터 백업을 검색합니다.
- 필요한 인프라를 준비합니다.
 - 준비된 AMI, ELB 등이 있는 Amazon EC2 인스턴스.
 - AWS CloudFormation을 사용해 주요 네트워킹 배포를 자동화합니다.
- 백업으로부터 시스템을 복원합니다.
- 새로운 시스템으로 전환합니다.
 - AWS를 가리키도록 DNS 레코드를 조정합니다.

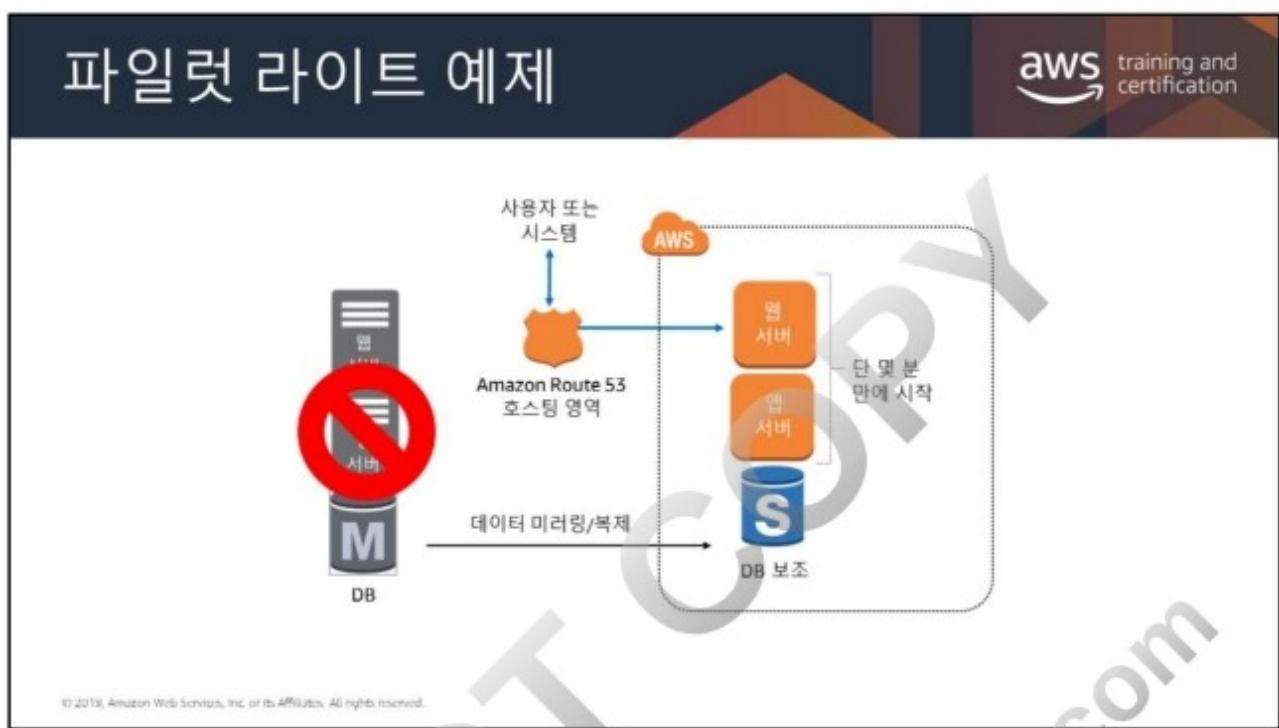
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



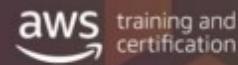
이 패턴은 비교적 저렴하게 구현할 수 있습니다. 재해 복구 준비 단계에서는 데이터 마이그레이션과 영구 스토리지를 지원하는 서비스 및 기능의 사용을 고려하는 것이 중요한데, 이로써 재해가 닥쳤을 때 AWS에 백업한 데이터를 복구할 수 있기 때문입니다. AWS에서 시스템의 규모 축소 또는 최대 확장이 수반되는 일부 시나리오의 경우, 컴퓨팅 리소스가 필요한 경우도 있습니다.

재해에 대처할 때, AWS에서 시스템을 실행할 수 있도록 신속하게 컴퓨팅 리소스를 공급하거나 AWS에서 이미 실행 중인 리소스에 장애 조치를 취하는 것이 관건입니다. 필수적인 인프라에는 DNS, 네트워킹 기능 및 다양한 Amazon EC2 기능들이 포함됩니다.

준비 단계에서는 복구 단계 시, 전체 환경이 시작되는 작은 코어인 파일럿 라이트에 정기적으로 변경되는 데이터를 복제해야 합니다. 운영 체제 및 애플리케이션과 같이 업데이트 빈도가 비교적 적은 데이터는 정기적으로 업데이트하고 AMI로 저장할 수 있습니다.



파일럿 라이트(Pilot Light)



이점

- 매우 비용 효율적(더 적은 24/7 리소스 사용)

준비 단계

- 데이터를 복제 또는 미러링하도록 Amazon EC2 인스턴스를 설정합니다.
- AWS에 모든 사용자 정의 지원 소프트웨어 패키지가 있는지 확인합니다.
- 빠른 복구가 필요한 핵심 서버의 Amazon 머신 이미지(AMI)를 생성 및 관리합니다.
- 이 서버를 정기적으로 실행하고, 테스트하고, 소프트웨어 업데이트 및 구성 변경 사항을 적용합니다.
- AWS 리소스의 프로비저닝을 자동화할 것인지 고려합니다.

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

파일럿 라이트(Pilot Light)



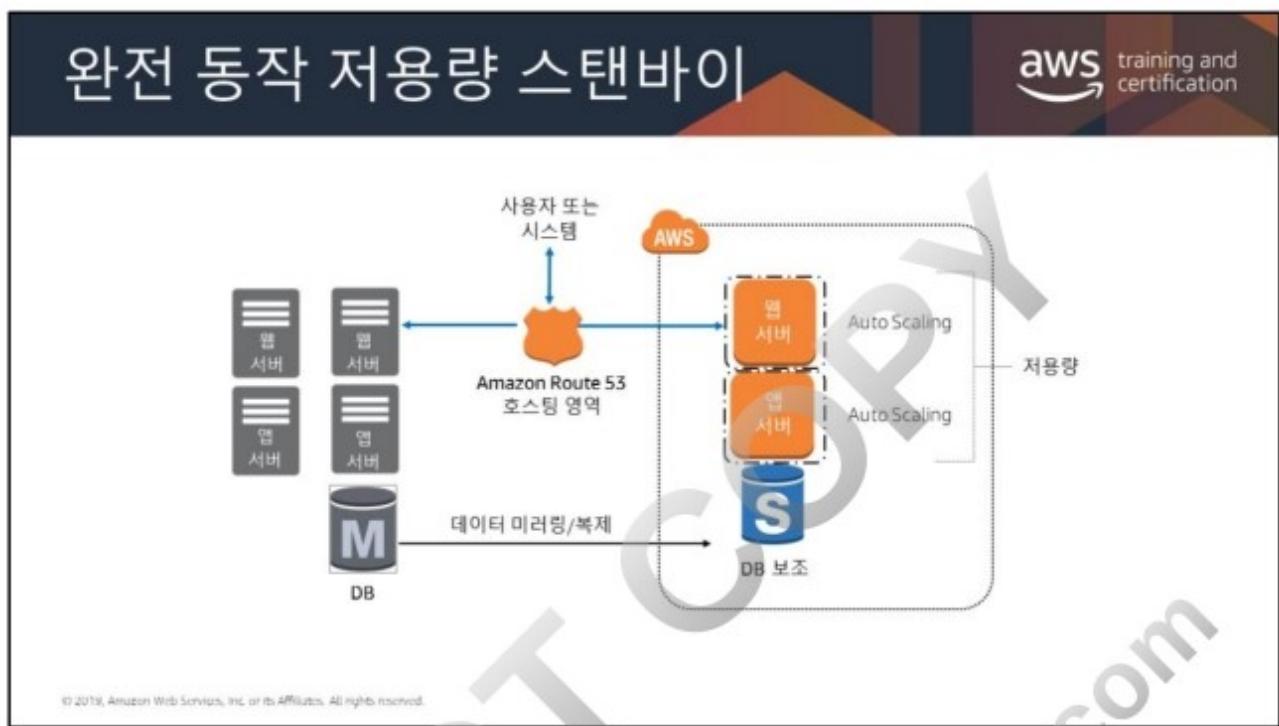
재해 발생 시

- 복제된 핵심 데이터 세트 주위의 리소스를 자동으로 준비합니다.
- 필요에 따라 시스템을 확장하여 현재 프로덕션 트래픽을 처리합니다.
- 새로운 시스템으로 전환합니다.
 - AWS를 가리키도록 DNS 레코드를 조정합니다.

목표

- RTO: DR 필요성을 감지하고 자동으로 대체 시스템을 확장하는데 소요되는 시간
- RPO: 복제 유형에 따라 다름

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



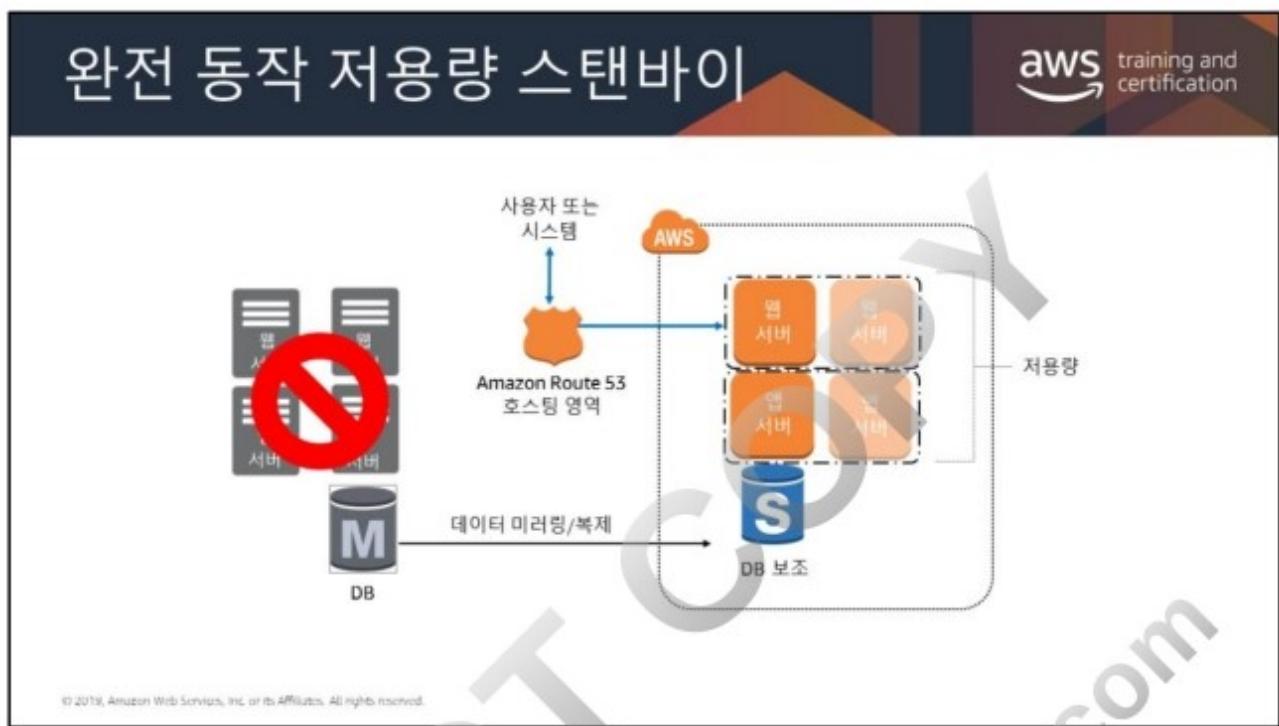
저용량 스탠바이는 파일럿 라이트의 다음 수준과 유사합니다. 웜 대기(*warm standby*)라는 용어는 완전한 기능 환경의 축소 버전이 항상 클라우드에서 실행되는 DR 시나리오를 설명하는데 사용됩니다. 웜 대기 솔루션은 파일럿 라이트 요소와 준비 과정을 확장합니다. 일부 서비스는 항상 실행 중이므로 이 솔루션을 사용하면 복구 시간을 더욱 단축할 수 있습니다. 비즈니스 크리티컬한 시스템을 확인한 후 AWS상에 이러한 시스템을 모두 복제하고 상시 접속되도록 합니다.

이러한 서버는 규모가 제일 작은 Amazon EC2 인스턴스에서 실행할 수 있습니다. 이 솔루션은 최대 프로덕션 부하를 처리할 정도로 규모가 확장되지는 않지만 기능은 온전하게 작동합니다. 이 솔루션은 테스트, 품질 보장 및 내부 사용 등 프로덕션 이외의 작업에 사용할 수 있습니다.

재해 시, 이 시스템은 프로덕션 부하를 처리할 수 있도록 신속하게 규모를 확장합니다. AWS에서는 로드 밸런서에 더 많은 인스턴스를 추가하거나 작은 용량의 서버가 더 큰 Amazon EC2 인스턴스 유형에서 실행되도록 크기를 조정함으로써 규모를 확장할 수 있습니다. 이전 단원에서 설명한 것처럼 수평적 확장은 수직 확장보다 우선적으로 적용됩니다.

상기의 다이어그램에서는 주 시스템과 AWS에서 실행되는 저용량 시스템이라는 두 개의 시스템이 실행됩니다. Amazon Route 53을 사용하여 주 시스템과 클라우드 시스템 간에 요청을 분산합니다.

DO NOT COPY
zlagusdbs@gmail.com



기본 환경을 사용할 수 없는 경우, Amazon Route 53은 보조 환경으로 전환됩니다. 보조 시스템은 기본 시스템으로부터 장애 조치가 실행될 경우 용량을 자동으로 확장하도록 설계되어 있습니다.

완전 동작 저용량 스탠바이

aws training and certification

이점

- 언제라도 서비스 트래픽 일부를 처리할 수 있음
- 비용 절감(완전 DR 대비 IT 리소스가 적음)

준비

- 파일럿 라이트와 유사
- 모든 필수 구성 요소가 24/7 실행되지만, 서비스 트래픽에 맞게 확장되지는 않음
- 모범 사례: 지속적인 테스트
 - 서비스 트래픽의 통계적 하위 집합을 DR 사이트로 "드문드문" 보냄

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

이 패턴에서는 활성 시스템이 실행되므로 비용이 더 많이 듭니다.

완전 동작 저용량 스탠바이



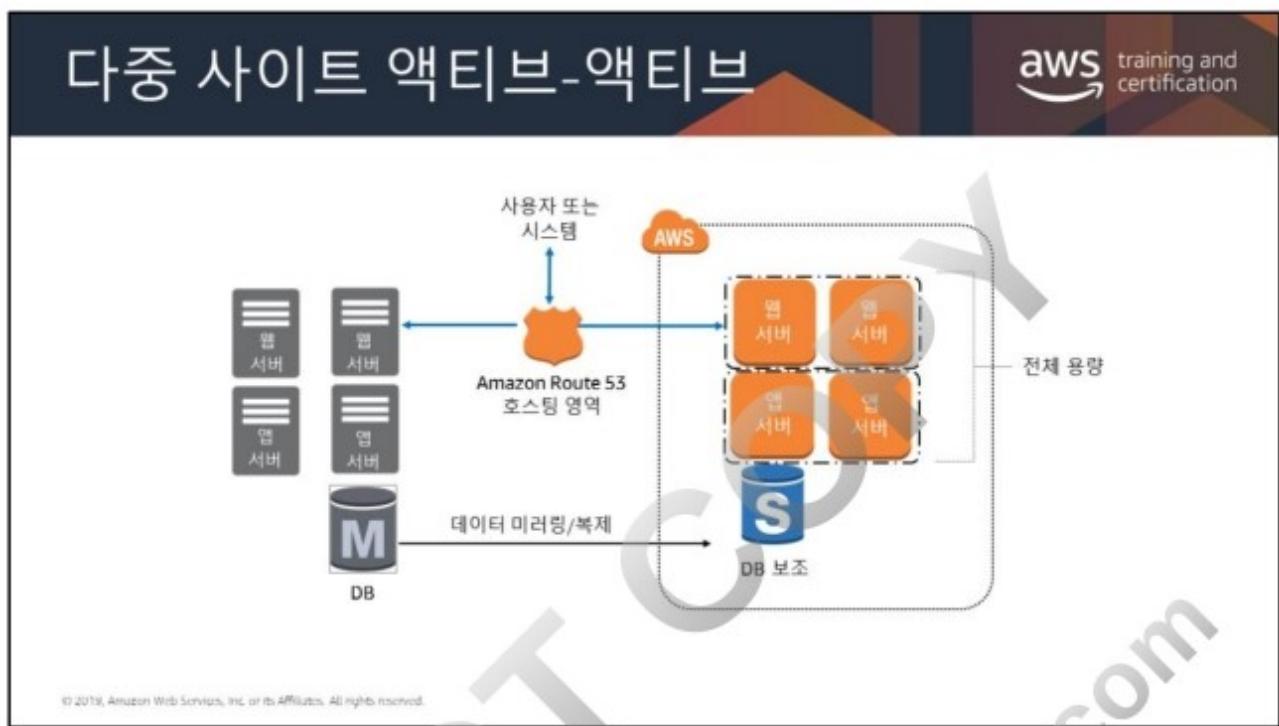
재해 발생 시

- 가장 중요한 서비스 부하에 대해 즉시 장애 조치
 - DNS 레코드가 AWS를 가리키도록 DNS 레코드를 조정
 - 모든 서비스 부하를 처리하도록 시스템을 자동 확장

목표

- RTO: 중요 로드의 경우는 장애 조치를 취하는 데 소요되는 시간, 나머지 로드의 경우는 추가 확장에 소요되는 시간
- RPO: 복제 유형에 따라 다름

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



다음 수준의 재해 복구는 온프레미스 시스템과 동시에 AWS에서 완벽하게 작동하는 시스템을 실행하는 것입니다.

다중 사이트 솔루션은 액티브-액티브 구성으로 기존의 현장 인프라뿐 아니라 AWS에서도 실행됩니다. 사용하는 데이터 복제 방법은 선택한 복구 시점에 의해 결정됩니다.

Amazon Route 53과 같은 가중치 기반 라우팅을 지원하는 DNS 서비스를 사용하면 프로덕션 트래픽을 동일한 애플리케이션이나 서비스를 제공하는 다른 사이트로 라우팅할 수 있습니다. 일정량의 트래픽은 AWS의 인프라로 전송되며, 나머지는 현장 인프라로 전송됩니다.

현장 재해 시, DNS 가중치를 조정하여 모든 트래픽을 AWS 서버로 보낼 수도 있습니다. 최대 프로덕션 부하량을 처리할 수 있도록 AWS 서비스 용량을 신속하게 증가시킬 수 있습니다. Amazon EC2 Auto Scaling을 사용하면 이 프로세스를 자동으로 실행할 수 있습니다. 기본 데이터베이스 서비스의 장애를 감지하고 AWS에서 실행되는 병렬 데이터베이스 서비스로 이관되기 위해 몇 가지 애플리케이션 로직이 필요할 수 있습니다.

이 시나리오의 비용은 정상 운영 중 AWS가 처리하는 프로덕션 트래픽의 양에 따라 결정됩니다. 복구 단계에서는 전체 재해 복구 환경이 필요한 기간 동안 트래픽을 실제로 사용한 만큼만 비용을 지불하면 됩니다. "항시 작동하는" AWS 서버에 대해 Amazon EC2 예약 인스턴스를 구입하면 비용을 더욱 줄일 수 있습니다.

DO NOT COPY
zlagusdbs@gmail.com

다중 사이트 액티브-액티브



이점

- 언제라도 모든 프로덕션 로드를 처리할 수 있습니다.

준비

- 저용량 스탠바이와 유사합니다.
- 프로덕션 로드에 따라 완전히 확장/축소

재해 발생 시

- 모든 프로덕션 로드에 대해 즉시 장애 조치

목표

- RTO: 장애 조치에 소요되는 시간
- RPO: 복제 유형에 따라 다름

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

이 패턴은 모든 패턴 중에서 잠재적으로 가동 중단 시간이 가장 짧습니다. 더 많은 시스템이 실행되므로 비용도 더 많이 듭니다.



애플리케이션은 복잡성의 스펙트럼에 배치할 수 있습니다. 심각한 재해가 발생하더라도 비즈니스 연속성을 통해 중요한 비즈니스 기능이 계속 빠르게 작동하거나 복구됩니다.

다음 슬라이드에서는 AWS의 사용을 강조하고 AWS와 기존 DR 방법 (RTO/RPO가 가장 높은 순위에서 가장 낮은 순위로 정렬됨)을 비교하는 4가지 DR 시나리오에 대해 간략히 설명합니다.

- 백업 및 복원
- 파일럿 라이트
- 완전 동작 저용량 스탠바이
- 다중 사이트 액티브-액티브

위 그림은 DR 이벤트가 발생한 후 얼마나 빨리 사용자에게 시스템을 사용 가능한 상태로 다시 제공할 수 있는지에 따라 4가지 시나리오로 분류한 스펙트럼입니다.

AWS를 사용하면 이러한 DR 전략 각각을 저렴한 비용으로 운영할 수 있습니다. 위의 예는 단편적인 예일 뿐이며, 이러한 예를 변형하거나 서로 조합하여 사용하는 것도 가능합니다. 애플리케이션을 이미 AWS에서 실행 중인 경우, 여러 리전을 적용할 수 있으며 동일한 DR 전략도 계속 적용할 수 있습니다.



단순하게 시작하여 차차 보강

- 첫 번째 단계로 AWS에 백업
- RTO/RPO를 점진적으로 개선하기 위해 지속적으로 노력

소프트웨어 라이선스 문제가 있는지 확인

DR 솔루션에 대한 연습

- “게임 데이” 시나리오를 연습. 이 시나리오에서는 크리티컬한 시스템을 오프라인 또는 전체 리전에 걸쳐 테스트합니다. 전체 인스턴스 집합에 충돌이 발생할 경우 어떻게 해야 하나요?
- 백업, 스냅샷, AMI 등이 작동하는지 확인
- 모니터링 시스템을 모니터링

한 가지 추가 사항은..



귀하의 의견은 매우 중요합니다!

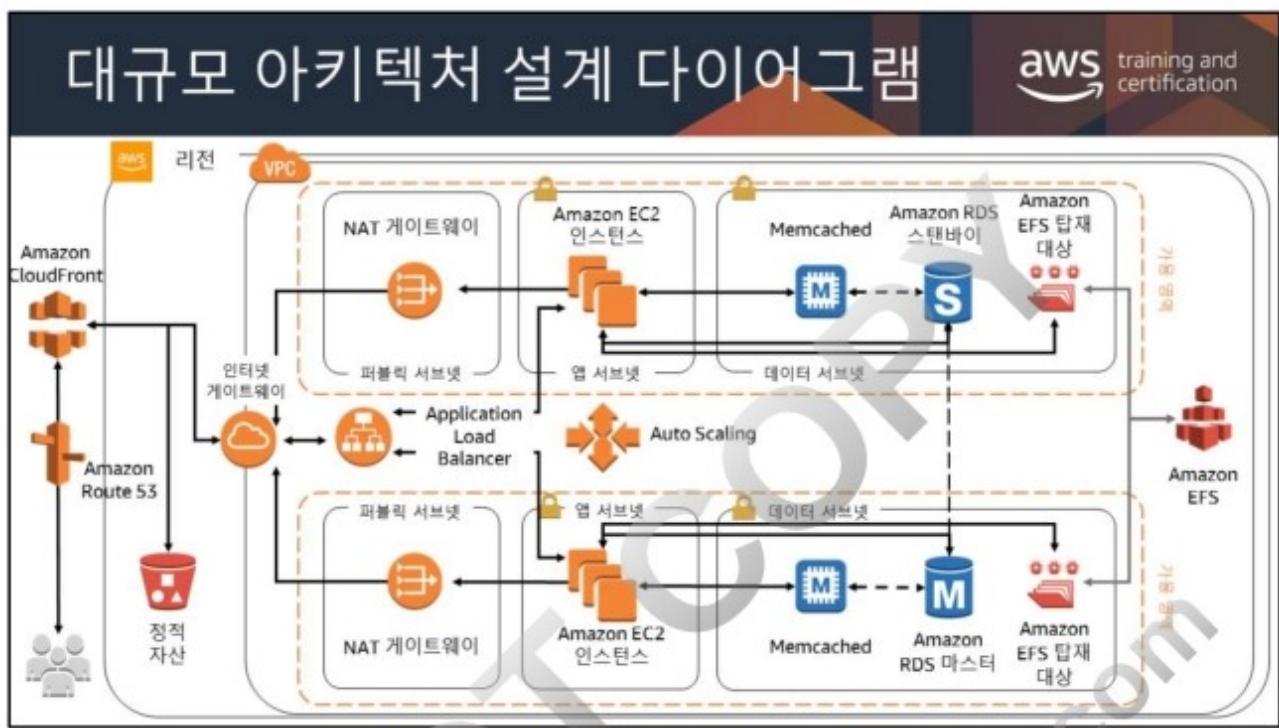
- <https://aws.training>에 로그인합니다.
- My Transcript(내 스크립트)를 선택한 다음 Archived(아카이브) 탭을 클릭합니다.
- AWS 기반 아키텍처 완료 교육을 찾은 다음 Evaluate(평가)를 클릭합니다.

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

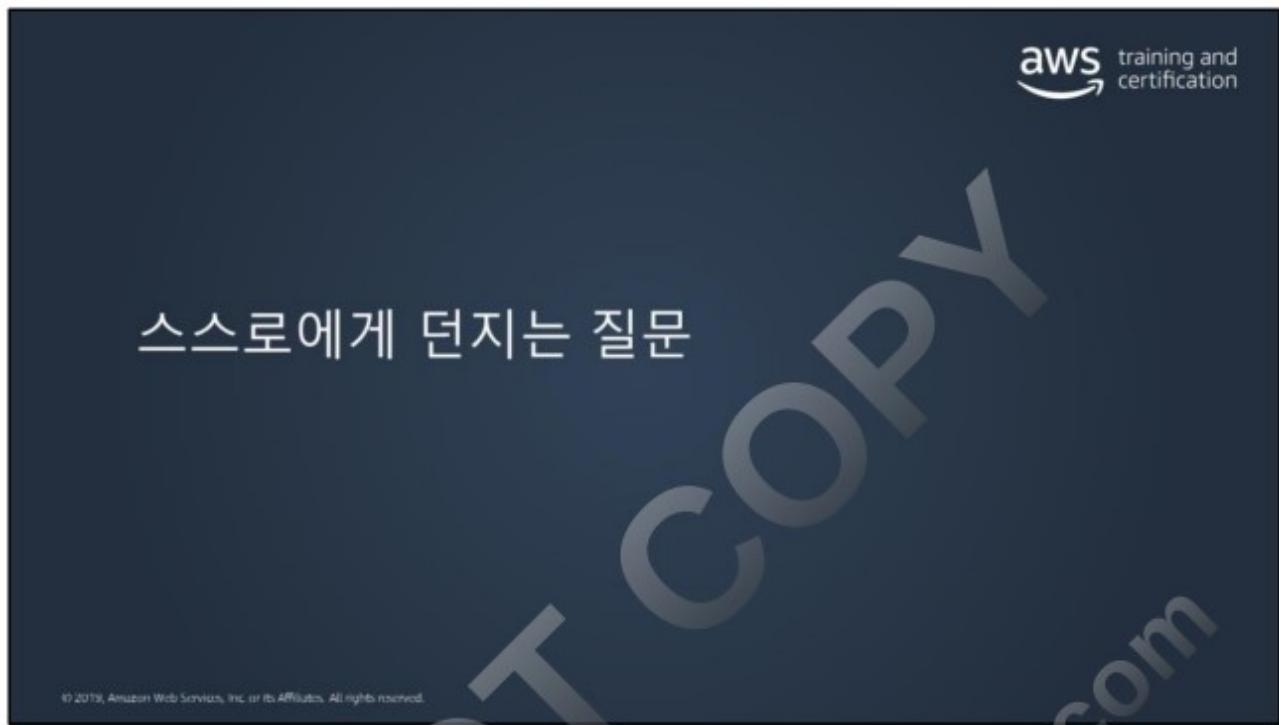




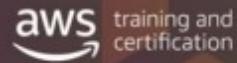
DO NOT COPY
zlagusdbs@gmail.com



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



Q1



이 아키텍처가 해결 중인 문제에 대해 **가장 적합한 리소스를 사용하고 있습니까?**

- 더 적합한 **인스턴스 유형**이 있습니까?
- 관리형 서비스를 사용해야 합니까?

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

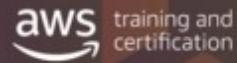
조직이 데이터 센터에 배치할 하드웨어를 구매할 때 흔히 예산이 책정되어 있으며 미래 지향적으로 구매를 결정합니다. 오늘 최고 성능을 자랑하는 하드웨어도 대략 18개월이면 쓸모가 없어질 것입니다. 그러므로 한 번의 구매로 미래의 요구 사항까지 대비하기 위해 당장 필요한 것보다 상향하여 구매할 수 밖에 없습니다.

따라서 데이터 센터 구축을 고려할 때 "지금 당장 필요한 것이 무엇인가?"를 물어야 합니다. 규모를 늘리거나 줄여야 한다면 그럴 수 있습니다.

또 하나의 방법은 "실제로 사용하지 않는 용량에 비용을 지불할 여력이 있는가?"를 묻는 것입니다.

Amazon RDS 같은 관리형 서비스는 모든 요구 사항을 미리 따져보지 않아도 AWS에서 리소스를 구축할 수 있게 해줍니다. 예를 들어 개발자가 Microsoft SQL Server 데이터베이스를 요청했는데 여러분이 이 소프트웨어를 설치해본 적이 없다고 한다면 상당한 시간과 노력이 필요할 것입니다. 그 대신, 어떤 종류의 데이터베이스가 필요한지 파악하여 AWS가 대신 구축하게 하십시오. 데이터베이스, 데이터, 액세스 권한은 여러분이 완벽하게 제어합니다. AWS가 하는 모든 것은 여러분이 설계나 구현 같은 창의적인 작업에만 집중할 수 있게 하는 것입니다.

Q2



이 아키텍처는 **복원력**이 있습니까?

- 단일 장애 지점이 존재합니까?
- 장애에서 **복구**할 수 있습니까?
- 자체 **복구 기능**이 있습니까?

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

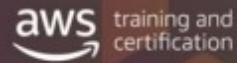
Amazon에서 모범 사례 중 하나는 프로세스의 끝에서 시작하여 그 과정을 되짚어보는 것입니다. 우리는 스스로 묻습니다. 어디에서 장애가 발생할 것인가? 장애가 발생한다면 어떻게 될 것인가?

예, 여러분이 해결할 수 있습니다. 하지만 반드시 여러분이 해결해야 합니까? 대신, 잘못된 비트를 삭제하고 새로운 비트를 캐시시오. 여러분은 재해에 대한 사후 보고를 할 수 있고 또 해야 합니다. 하지만 인스턴스, 컨테이너 또는 유사한 구성 요소가 가동 중지되었다면 먼저 교체한 다음 원인을 파악하십시오.

AWS를 사용하면 프로덕션 환경에 영향을 주지 않고 전체재해 대응 연습을 실시할 수 있습니다. 예, 비용은 몇 달러에 불과하니까 두 번째 데이터 센터를 구축하는 것과는 비교할 수 없습니다.

여러분은 창의적인 작업을 수행하기 위해 채용된 것입니다. 그런데 자동화할 수 있는 작업을 수동으로 처리하는 라 시간을 소비할 이유가 있을까요? AWS를 사용하면 스스로 모니터링하고, 필요에 따라 장애가 발생한 요소를 삭제한 후 사용자에게 무엇이 발생했는지 보고할 수 있는 환경을 구축할 수 있습니다.

Q3



이 아키텍처에서 구성 요소 간 긴밀한 종속성을 제거할 수 있습니까?

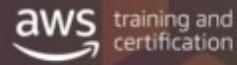
- 마이크로 서비스
- 결합 해제

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

마이크로 서비스는 아키텍처의 안정성과 가용성을 높이기 위한 최선의 방법 중 하나입니다. 이 접근 방식을 사용하면 애플리케이션 구성 요소 간 종속성을 축소하여 혁신 속도를 개선할 수 있습니다. IT 팀이 비동기식으로 작업하여 전체 시스템에 영향을 미치지 않고 기능 업데이트를 제공할 수 있습니다.

이러한 종류의 접근 방식을 선택하기 위해서는 시스템 작동 방식에 대한 새로운 사고 방식이 필요할 수 있습니다. 모놀리식 시스템은 상당한 매몰 비용이 발생하지만, 시간을 들여 각 구성 요소를 분리한 후 어떻게 작동하는지 살펴본다면 클라우드에서는 이러한 비용을 방지할 수 있습니다.

Q4



이 아키텍처를 효과적으로 확장할 수 있습니까?
(100명의 사용자 -> 100만 명의 사용자)

- 최소 인프라
- Auto Scaling

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

여러분은 가능한 한 규모가 크고 속도가 빠르며 성능이 강력한 시스템을 원할 수 있겠지만, 여러분이 시스템을 최대 성능까지 사용하지 않는다면 낭비일 뿐입니다.

구체적인 수치를 파악하는 데 충분한 데이터 포인트를 수집하는 데 약 3개월이 걸립니다. 따라서 실제로 얼마의 용량이 필요한지 파악하려면 먼저 필요한 것보다 큰 용량의 시스템에서 시작하십시오. 그런 다음 실제 시스템 사용량을 보면서 환경의 "적정 크기"를 판단할 수 있습니다.

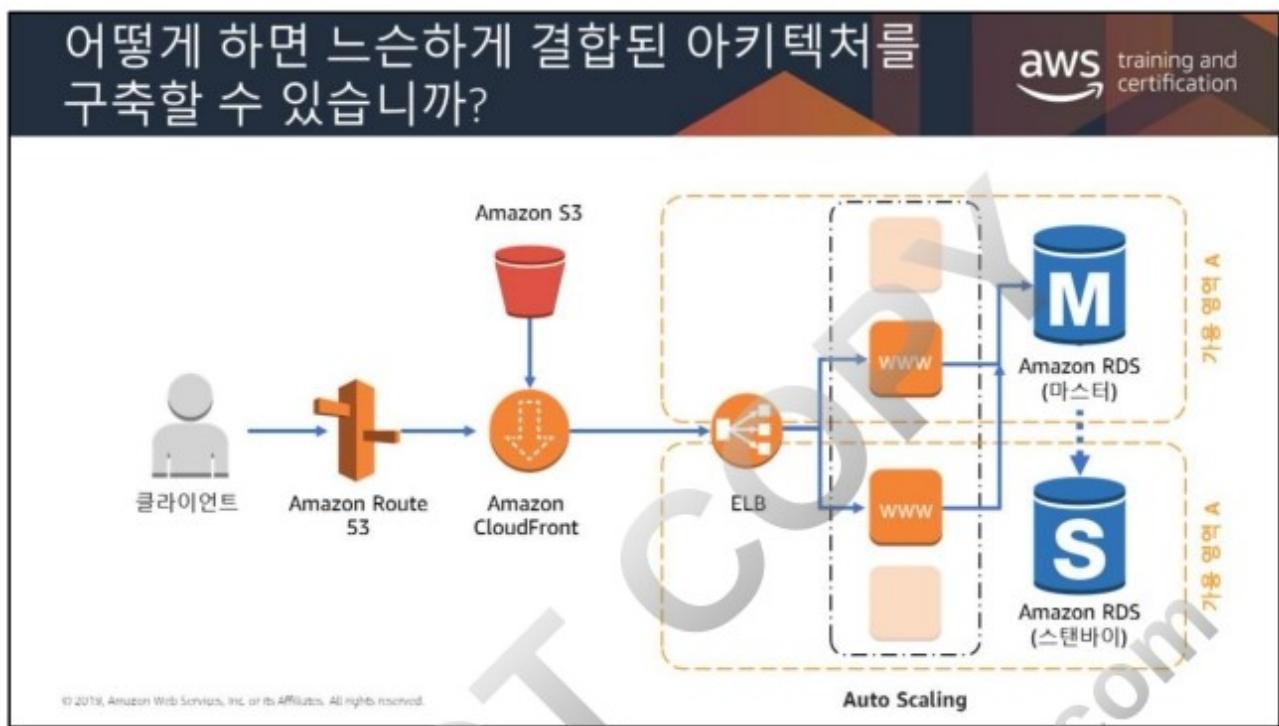
온프레미스 데이터 센터를 운영 중이라면 새로운 리소스 가동은 데이터 센터 자체와 관련된 모든 라인 항목에 의해 흡수됩니다. AWS에서 새로운 워크로드를 실행할 경우 이와 관련된 비용이 발생합니다. 다행히 AWS에서 비용은 투명합니다. 여러분은 새 인스턴스를 시작하는 것이 물리적 서버를 구축하는 것보다 훨씬 저렴하다는 것을 알 수 있을 것입니다.

IT 세계에서는 두 가지 유형의 장애가 있습니다.

- 여러분이 하드웨어 또는 소프트웨어에 지정된 한계를 벗어난 무언가를 요청했기 때문에 어딘가에서 장애가 발생합니다.
- 여러분의 제품이 너무 성공적이어서 사용자의 요청이 하드웨어 및 소프트웨어의 지정된 한계를 초과합니다.

Auto Scaling은 비용을 수반합니다. 하지만 이 기능이 없다면 소프트웨어가 로드를 처리하지 못하고 다운될 것입니다. 소프트웨어를 계속 실행하기 위해 충분한 투자 가치가 있습니다.

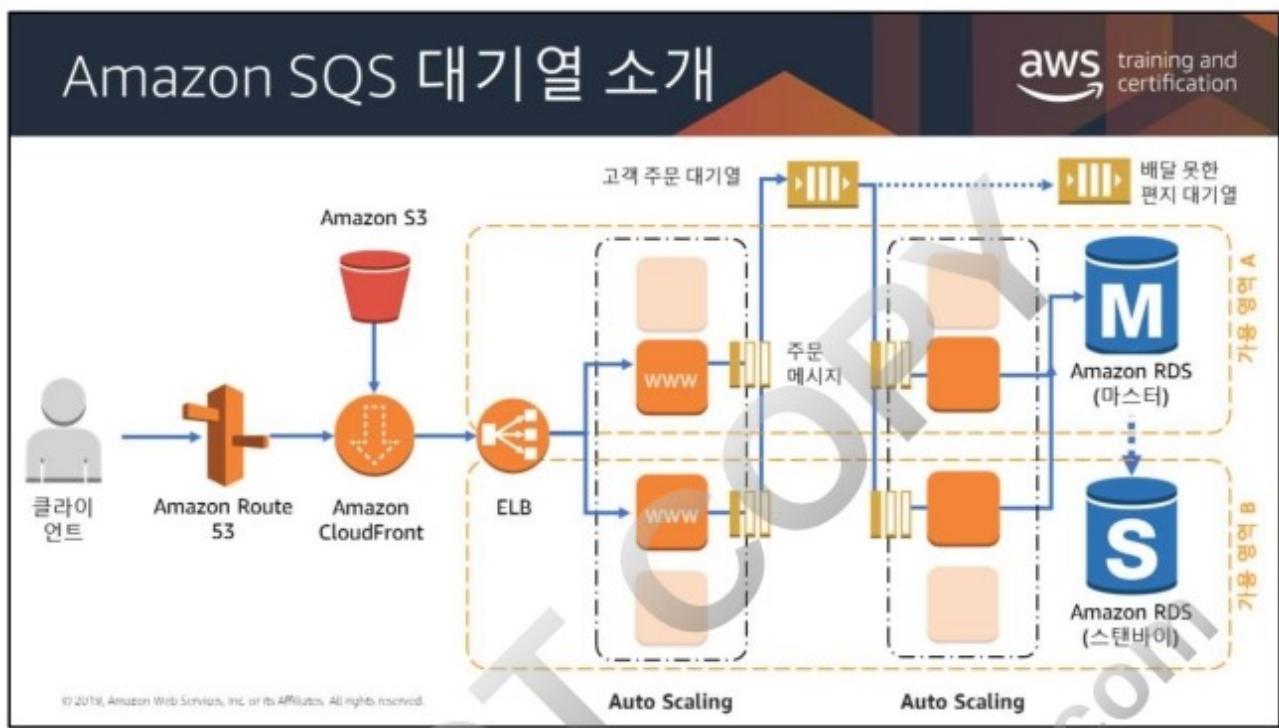




이 예제에서는 애플리케이션이 주문 데이터를 처리 및 유지해야 하고 인기 아이템에 대한 트래픽 증가도 처리해야 합니다.

주문 처리 워크플로우의 한 가지 잠재적인 취약점은 해당 주문을 데이터베이스에 저장하는 데 있습니다. 기업은 모든 주문이 데이터베이스에 계속 유지되는 것으로 기대합니다. 그러나 잠재적 교착, 경합 조건 또는 네트워크 문제가 발생할 경우, 해당 주문을 계속 유지할 수 없게 됩니다. 결국 해당 주문은 복원을 위한 어떤 수단도 없이 손실됩니다.

우수한 로깅 기능을 사용한다면 언제 오류가 발생했는지, 어떤 고객의 주문에 장애가 발생했는지 식별할 수 있을 것입니다. 그렇다고 거래를 "복원"할 수 있는 것은 아닙니다. 이 정도면 그 고객은 더 이상 여러분의 고객이 아닐 것입니다.



이 시나리오에서 어떻게 비용을 절감할 수 있습니까?

aws training and certification

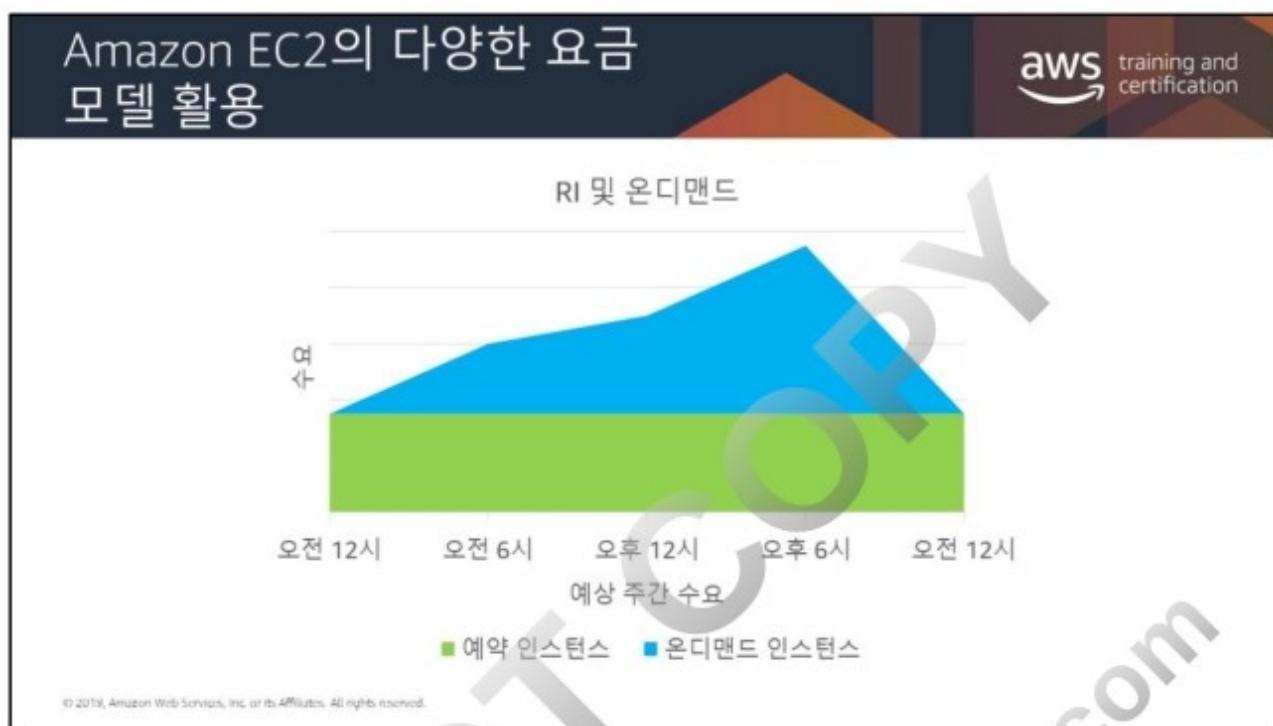
클라이언트 트래픽 볼륨:

- 근무 시간 중 트래픽 급증
- 항상 일관된 기본 수준 트래픽
- 온디맨드 인스턴스 사용

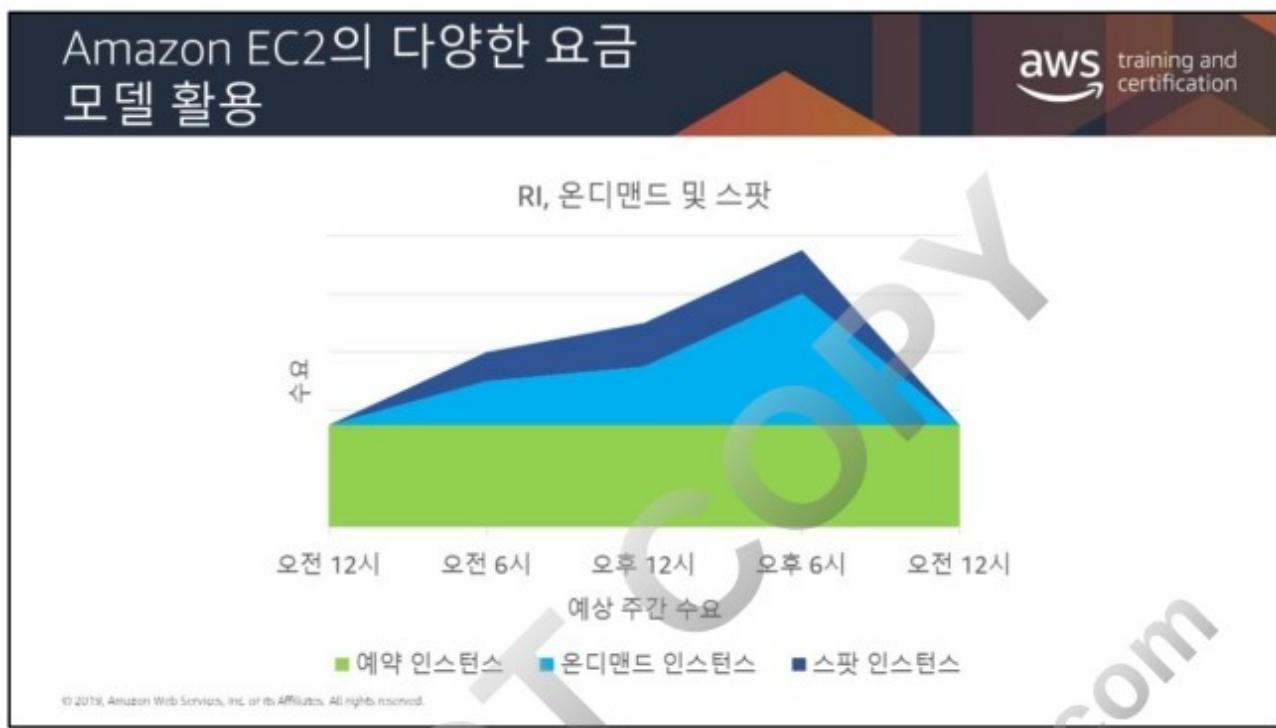
예상 주간 수요

■ 온디맨드 인스턴스

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



이 차트는 예약 인스턴스와 온디맨드 인스턴스를 함께 사용하여 시간이 지나면서 변동하는 수요를 수용하는 매우 기본적인 방법을 보여줍니다. 이 예제에서는 여러 예약 인스턴스를 구매하여 실행하고 있습니다. 하지만 시간이 지나면서 수요가 증가함에 따라 인스턴스 추가에 대한 요구도 증가합니다. 이 고객은 저녁이 되어 필요 없어지면 종료할 수 있는 온디맨드 인스턴스로 용량을 보충합니다.



두 번째 차트에서는 이 고객이 좀 더 복잡한 접근 방식을 택하여 3가지 요금 모델을 모두 활용하려고 시도합니다. 이 경우에는 일부 인스턴스를 먼저 온디맨드로 보충하고, 추가로 필요한 용량은 스팟 인스턴스로 채웁니다. 이렇게 하면 온디맨드 대신 스팟을 사용하여 비용을 절감할 수 있지만, 입찰에 실패하면 해당 인스턴스를 잃게 되므로 예상치 못한 인스턴스 종료가 발생할 수 있습니다. 이는 고객의 데이터 손실 또는 용량 부족으로 이어질 수 있습니다. 즉, 이러한 모델은 갑작스러운 인스턴스 종료가 허용되고 적절하게 처리될 수 있는 상황에서만 구현해야 합니다.

2017년에 도입된 새로운 요금 모델에서는 스팟 인스턴스에 대한 입찰이 더 이상 필요하지 않습니다. 시작된 인스턴스에 대해 현재 시간에 적용되는 스팟 가격을 지불하면 됩니다. 스팟 가격은 예측 가능하고, 자주 업데이트되지 않으며, Amazon EC2 예비 용량의 공급과 수요에 따라 결정됩니다. 또한 중단의 영향을 줄이고 스팟 인스턴스를 최적화하려면 여러 용량 풀에서 애플리케이션을 다양화하고 실행합니다. 모든 리전의 각 가용 영역에 있는 각 인스턴스 패밀리와 각 인스턴스 크기는 별도의 스팟 풀입니다. RequestSpotFleet API를 사용하여 자동으로 수천 개의 스팟 인스턴스를 시작하고 리소스를 다양화할 수 있습니다.

중단의 영향을 더욱 줄이기 위해서는 용량을 더 이상 사용할 수 없을 때 인스턴스를 종료하는 대신 중지하거나 최대 절전 모드로 전환하여 중단 알림에 대응하도록 스팟 인스턴스와 스팟 플릿을 설정할 수도 있습니다.

스팟 인스턴스 사용에 대한 자세한 내용은 다음을 참조하십시오.

<https://aws.amazon.com/ec2/spot/getting-started/>

스팟 요금에 대한 자세한 내용은 다음을 참조하십시오.

<https://aws.amazon.com/blogs/compute/new-amazon-ec2-spot-pricing/>

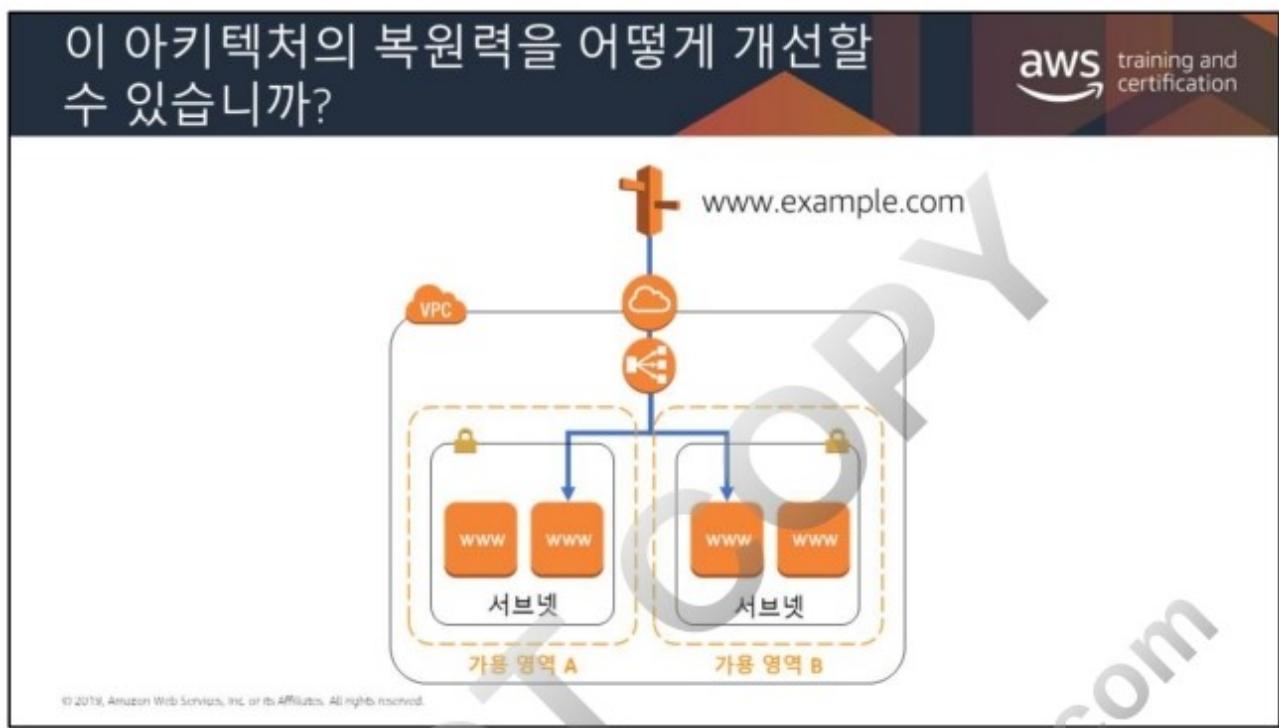
3가지 모델을 모두 함께 활용한 AWS 고객 중 하나가 Pinterest입니다. 자세한 내용은 <http://www.allthingsdistributed.com/2012/08/tco-and-return-on-agility.html>을 참조하십시오.

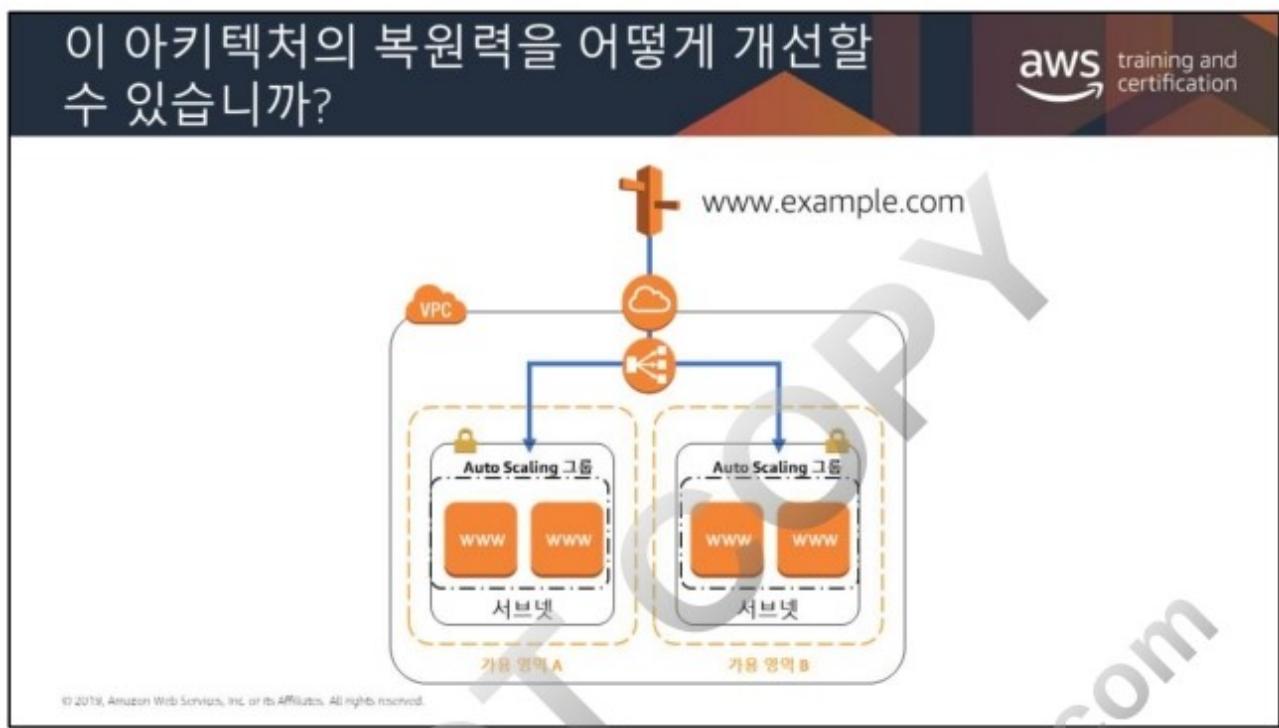
이 아키텍처의 복원력을 어떻게 개선할 수 있습니까?

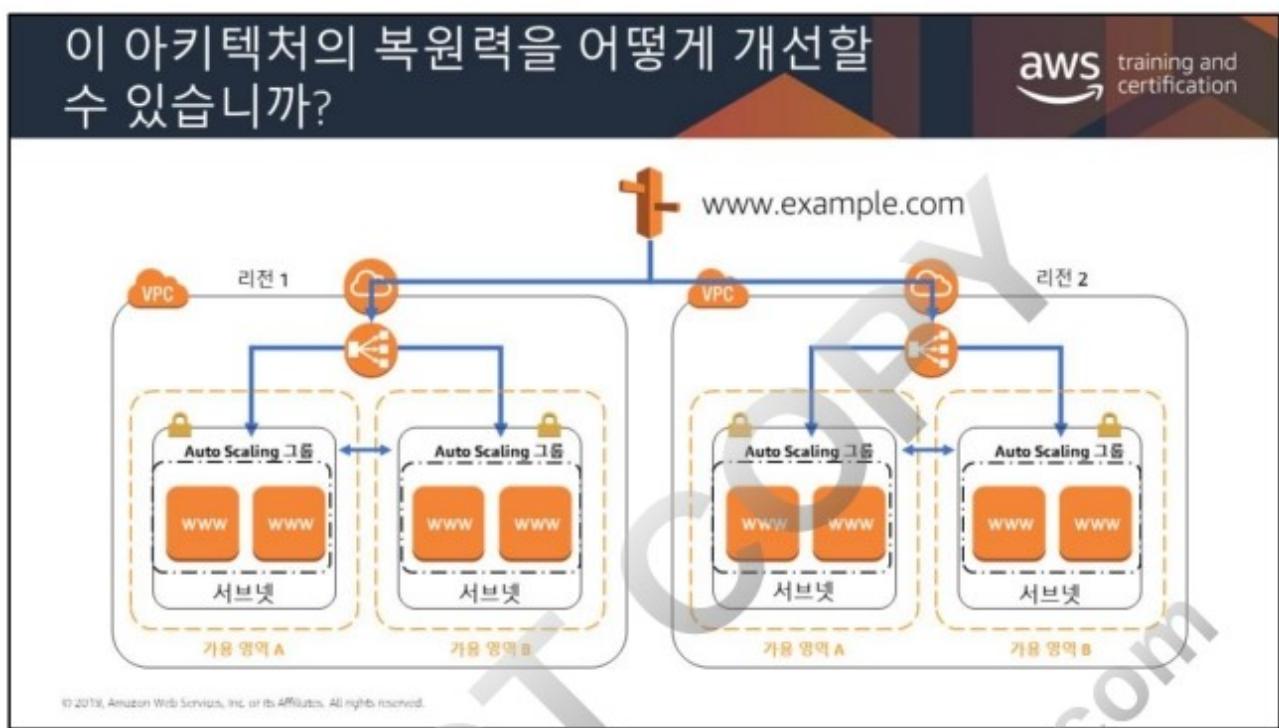
aws training and certification

The diagram illustrates a network architecture within a Virtual Private Cloud (VPC). At the top, a URL 'www.example.com' is connected to an orange cloud icon representing an Application Load Balancer (ALB). This ALB is connected to an orange VPC icon. Below the VPC icon is a network icon (routers and switches). A dashed orange box labeled '서브넷' (Subnet) contains two orange boxes labeled 'www'. Arrows point from the network icon down to the subnet, and from the subnet to the 'www' boxes. A yellow banner at the bottom of the subnet area reads '가용 영역 A' (Availability Zone A). A large watermark 'DO NOT COPY' and an email address 'zlagusdbs@gmail.com' are diagonally overlaid across the slide.

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







참고: Auto Scaling 그룹은 여러 가용 영역에 걸쳐 있을 수 있습니다.

인스턴스 유형은 무엇입니까?



클라이언트에 기계 학습을 사용하여 사용자가 제출한 이미지에 상표 등록된 로고가 포함되어 있는지 여부를 확인하는 웹 애플리케이션이 있습니다.

웹 서버로 어떤 유형의 인스턴스를 추천하시겠습니까?

백엔드 기계 학습을 위해 어떤 유형의 인스턴스를 추천하시겠습니까?

<https://aws.amazon.com/ec2/instance-types/>를 자유롭게 사용

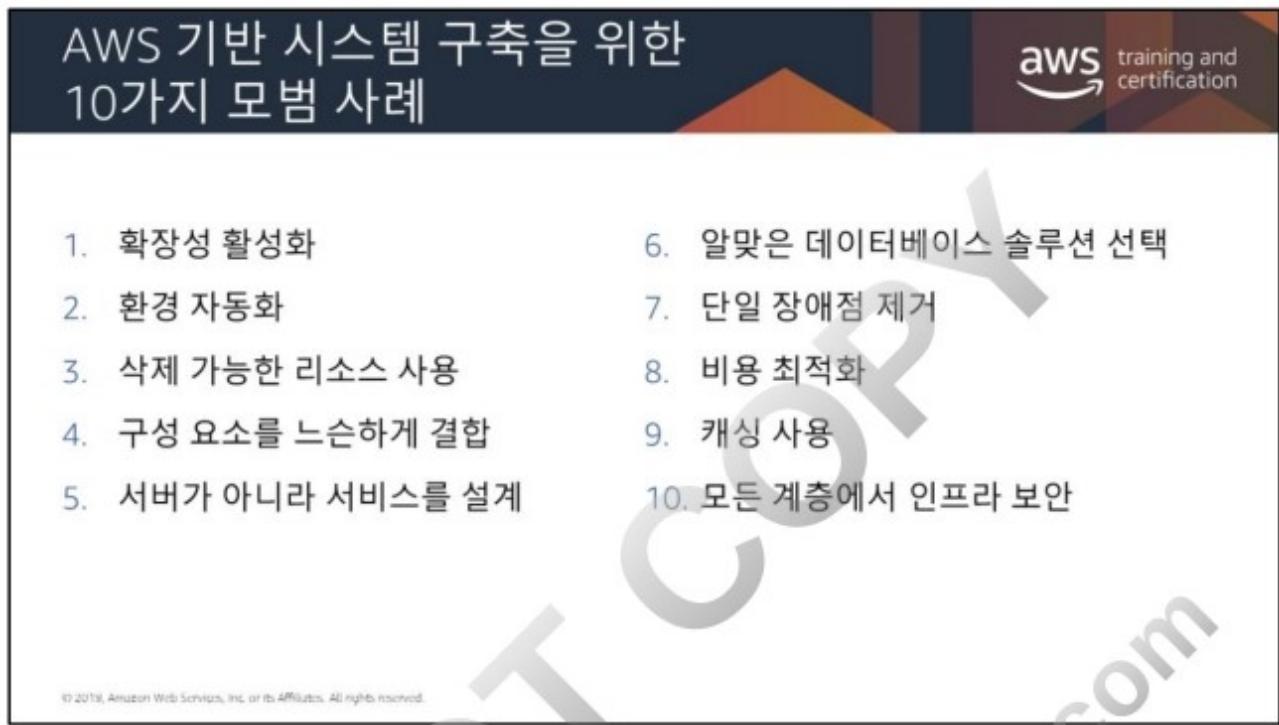
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

인스턴스 유형에 대한 자세한 내용은 <https://aws.amazon.com/ec2/instance-types/>를 참조하십시오.



AWS Well Architected Tool은 사용자가 콘솔에서 최신 AWS 아키텍처 모범 사례를 사용자의 워크로드와 비교하고 검토할 수 있는 무료 도구입니다. 이는 AWS Well-Architected Framework를 기반으로 합니다. AWS 솔루션 아키텍처 팀이 수만 개의 워크로드를 검토하는 데 사용했습니다.

<https://aws.amazon.com/well-architected-tool/>



AWS 기반 시스템 구축을 위한
10가지 모범 사례

aws training and certification

1. 확장성 활성화
2. 환경 자동화
3. 삭제 가능한 리소스 사용
4. 구성 요소를 느슨하게 결합
5. 서버가 아니라 서비스를 설계
6. 알맞은 데이터베이스 솔루션 선택
7. 단일 장애점 제거
8. 비용 최적화
9. 캐싱 사용
10. 모든 계층에서 인프라 보안

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



두 개의 진실, 두 개의 거짓



그룹으로, 강의에서 다룬 자료를 통해 선택한 주제에 관한 진실인 설명과 거짓인 설명을 두 개씩 제시합니다.

- 도전 과제를 생성할 때 리소스로 수강생 안내서를 자유롭게 사용할 수 있습니다.
- 모든 사람이 준비가 되면, 작성한 주제를 학급과 공유하여 진실 여부를 판단하도록 합니다.

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



종이 위에 아키텍처 설계

aws training and certification

그룹으로, 할당된 문제를 해결하는 간단한 아키텍처를 설계합니다.

- 아키텍처를 작성할 때 리소스로 수강생 안내서를 자유롭게 사용할 수 있습니다.
- 아키텍처가 고가용성이고 장애에 대한 복원력이 뛰어나야 합니다.
- 비용 효율성도 고려해야 합니다.
- 선택한 아키텍처를 설명할 준비를 하십시오.

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

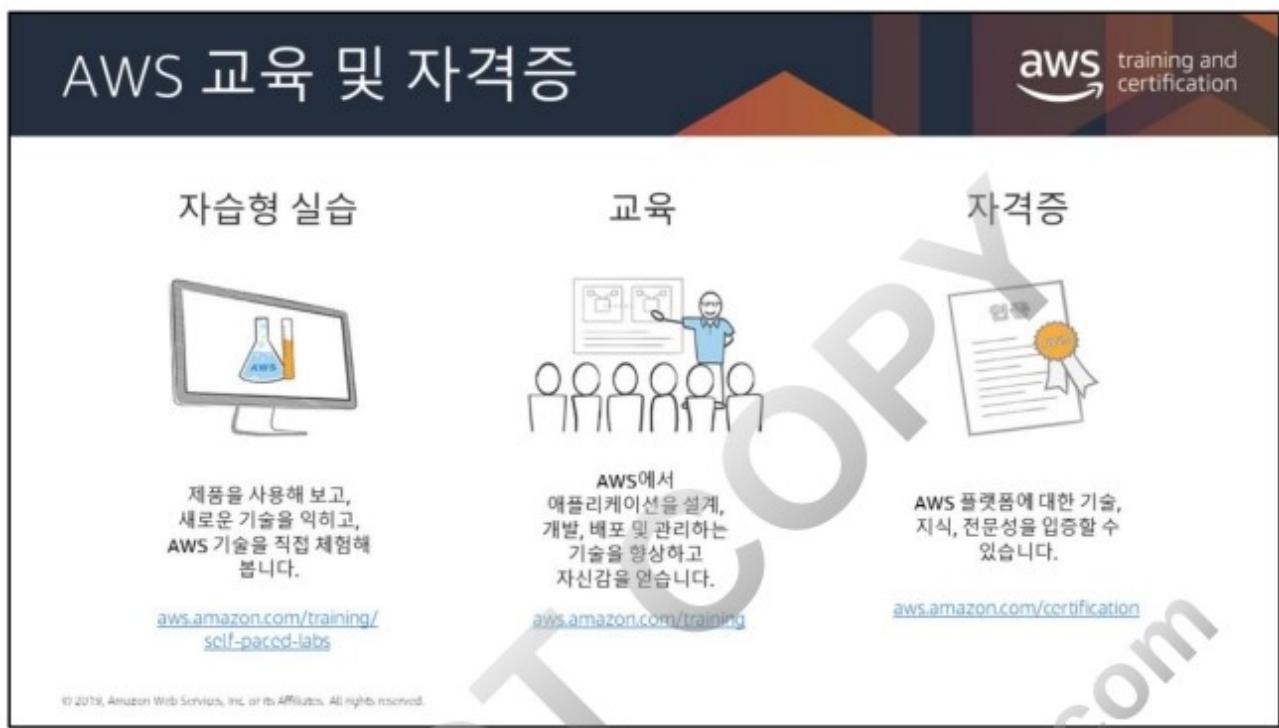
문제 샘플:

- 온라인 이미지 크기 조정 앱
- 주문 처리 기능이 있는 간단한 온라인 스토어
- 주문형 동영상 스트리밍
- 계정 로그인(Facebook/Google/Amazon)을 사용하는 이미지 공유 웹 사이트
- 온라인 가상 데스크톱
- 이 연습에 여러분의 아키텍처 도전 과제를 자유롭게 추가할 수 있습니다.





AWS 교육 및 자격증



The page features three main sections: '자습형 실습' (Self-paced Labs) with a computer monitor icon, '교육' (Education) with a teacher and students icon, and '자격증' (Certification) with a certificate icon. Each section includes a brief description and a link to the AWS website.

자습형 실습



제품을 사용해 보고,
새로운 기술을 익히고,
AWS 기술을 직접 체험해
봅니다.

[aws.amazon.com/training/
self-paced-labs](https://aws.amazon.com/training/self-paced-labs)

교육



AWS에서
애플리케이션을 설계,
개발, 배포 및 관리하는
기술을 향상하고
자신감을 얻습니다.

aws.amazon.com/training

자격증

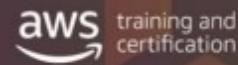


AWS 플랫폼에 대한 기술,
지식, 전문성을 입증할 수
있습니다.

aws.amazon.com/certification

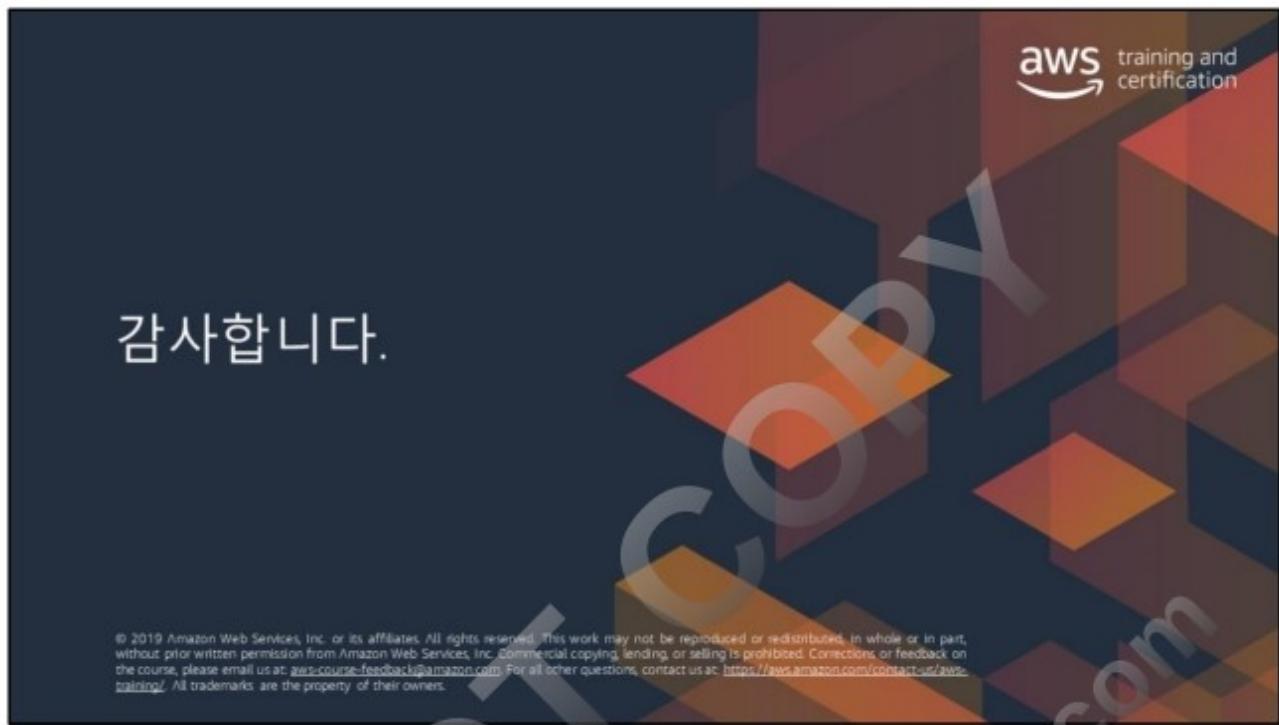
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

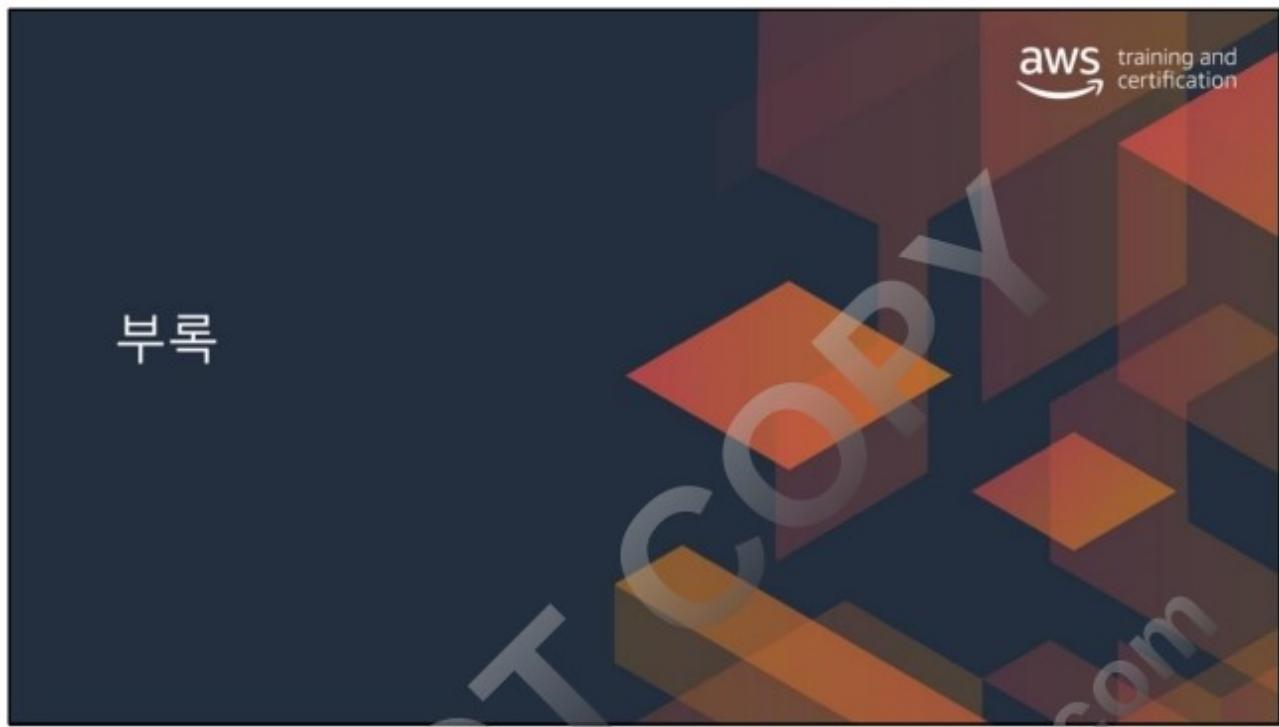
귀하의 의견은 매우 중요합니다!



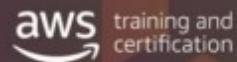
- <https://aws.training>에 로그인합니다.
- “My Transcript(내 트랜스크립트)”를 선택한 다음 “Archived(보관됨)” 탭을 클릭합니다.
- AWS 기반 아키텍처 설계 완료 교육을 찾은 다음 “Evaluate(평가)”를 클릭합니다.

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



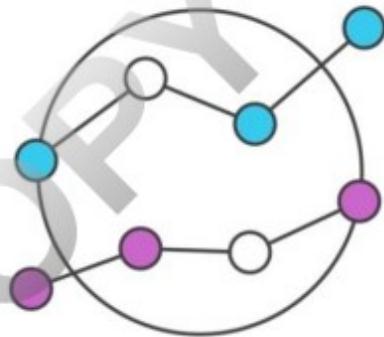


비용의 장점



하드웨어 구매 또는 데이터 센터 구축
불필요

- 리소스를 사용하는 만큼 비용 지불
- 초기 자본 비용 절감

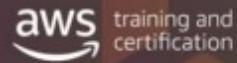


© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

사용 방법이 결정되기도 전에 데이터 센터와 서버에 대규모의 투자를 하는 대신 컴퓨팅 리소스를 사용할 때만, 그리고 사용한 만큼의 리소스에 대해서만 비용을 지불할 수 있습니다.

이러한 이점은 특히 스타트업 또는 선결제 예산에 제약이 있는 프로젝트에 적합합니다. 기술의 첨단에 선다는 것은 위험이 따를 수 있습니다. 온프레미스 인프라를 직접 구축할 경우 비용의 제약을 받을 수 있으며, 테스트, 실험 및 혁신이 자연될 수 있습니다. 비용 이점을 통해 신속하게 준비하고 실행할 수 있으면서도 사용한 만큼만 비용을 지불합니다.

규모의 장점



큰 규모의 경제를 활용

- 자체 보유보다 저렴한 비용
 - 전문화된 하드웨어 및 소프트웨어
 - 대용량 하드웨어 구입



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

클라우드 컴퓨팅을 사용하면, 인프라를 소유할 때보다 가변 비용이 낮습니다. 수많은 고객의 사용량이 클라우드에 집계되므로, AWS와 같은 공급자는 더 높은 규모의 경제를 달성할 수 있으며, 따라서 사용량에 따라 지불하는 방식의 요금이 더 낮아집니다.

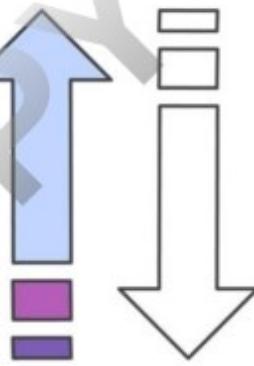
AWS는 대규모 클라우드에 최적화된 독자적인 하드웨어 및 소프트웨어를 개발했습니다. 이러한 제품을 대량으로 구매할 경우 AWS가 대부분의 온프레미스 데이터 센터보다 낮은 비용과 높은 효율을 지원할 수 있습니다. 이러한 절감은 가격을 인하하고 고객 경험을 개선하는데 충당될 수 있습니다.

용량의 장점

aws training and certification

용량 추정 불필요

- 필요에 따라 확장 및 축소
- 오버프로비저닝 불필요



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

필요한 인프라 용량을 추정할 필요가 없습니다. AWS를 사용하면 컴퓨팅 리소스를 사용할 때만 그리고 사용한 만큼에 대해서만 비용을 지불합니다. 필요한 만큼의 리소스에 액세스하고 필요에 따라 몇 분 만에 수평적 및 수직적으로 확장 또는 축소할 수 있습니다.

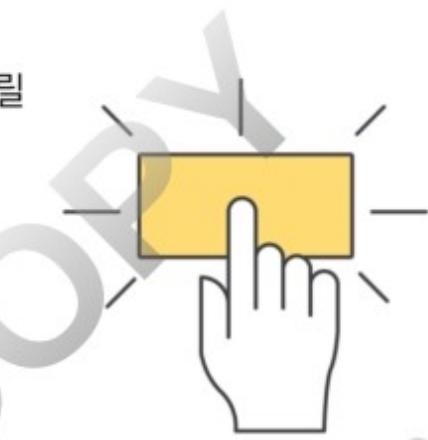
예를 들어 새로운 제품 또는 서비스를 출시하는 경우, 아직 고객의 반응을 알지 못하는 상황이라면 용량을 추정하기란 매우 힘듭니다. 수요 변동 및 급증에 따른 인프라 조정은 대부분의 경우 정적인 온프레미스 솔루션에 비해 엄청난 이점을 제공합니다.

속도의 장점

aws training and certification

하드웨어를 설치 및 설정할 때까지 기다릴 필요가 없음

- 한 번의 클릭으로 새 IT 리소스 확보
- 리소스 개발 시간 단축



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

클라우드 컴퓨팅 환경에서는 새 IT 리소스를 클릭 한 번으로 확보할 수 있습니다. 개발자에게 리소스를 몇 주가 아니라 몇 분 만에 제공할 수 있습니다. 이에 따라 실험 및 개발에 드는 비용이 상당히 절감되고 시간이 단축되므로, 조직의 민첩성이 크게 향상됩니다.

온프레미스 환경에서 서버 한 대를 프로비저닝하려면 6~20주가 걸릴 수 있습니다. 이 기간은 진정으로 혁신을 억제합니다. AWS에서는 수백 개 또는 수천 개의 서비스를 몇 분 만에 전적으로 사용자가 직접 프로비저닝할 수 있습니다. 그러므로 신속하게 실험하고 생성할 수 있습니다.

집중의 장점

aws training and certification

인프라가 아니라 애플리케이션에 집중

- 리소스를 확보하여 새 프로젝트에 투자
- 데이터 센터 운영 및 유지 관리에 비용 투자 불필요
- 일회용 리소스를 통해 신속한 실험 가능

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

인프라가 아니라 비즈니스를 차별화하는 프로젝트에 집중할 수 있습니다.
클라우드 컴퓨팅을 사용하면 수많은 서버를 관리하느라 시간을 허비하지 않고
고객에게 더욱 집중할 수 있습니다.

클라우드는 여러분의 과중한 업무 부담을 이미 상당히 제거했습니다. 대부분의 기업에서 가장 희소한 리소스는 소프트웨어 개발 엔지니어입니다. 엔지니어링 팀이 완수해야 할 작업들이 우선 순위에 따라 길게 늘어 있습니다. 기본 인프라에 대한 작업을 수행하는 대신 미션을 추진하는 프로젝트에 해당 리소스를 집중할 수 있는 것은 상당한 이점입니다.

글로벌의 장점



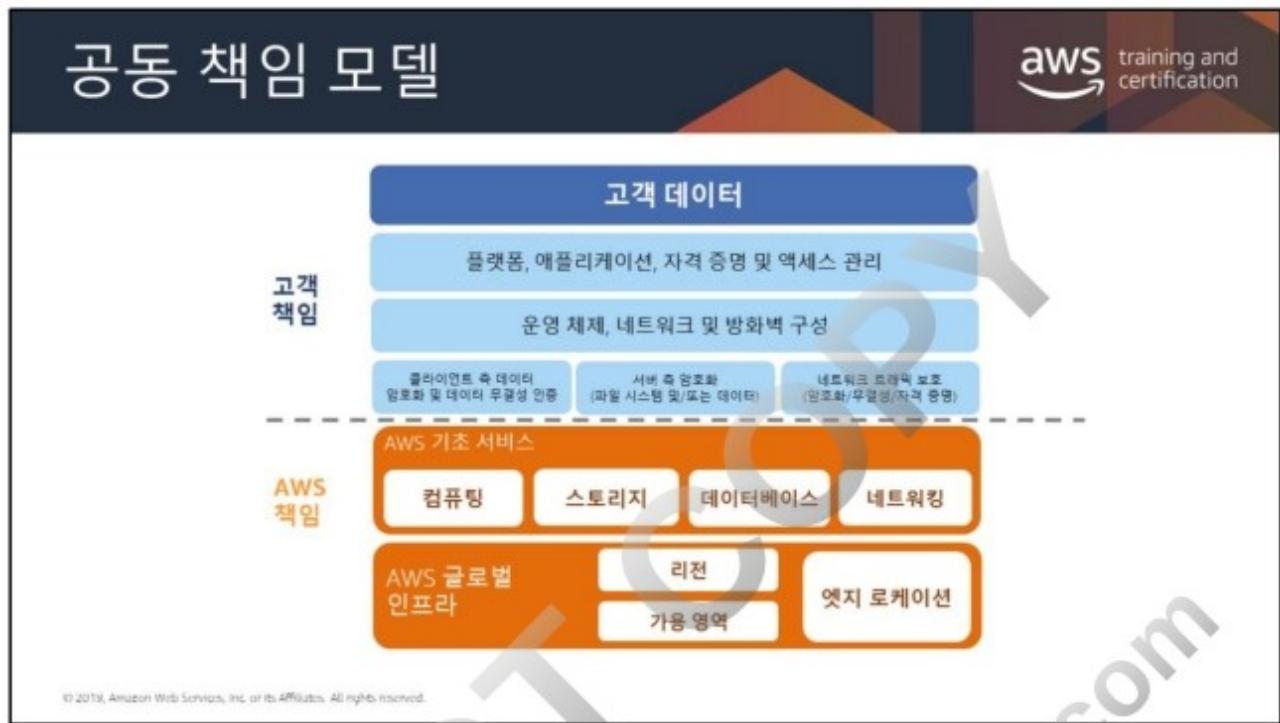
몇 분 만에 전 세계에 배포

- 전 세계에 분포된 여러 AWS 리전
- 애플리케이션을 사용자와 가까이 유지
- 고가용성 및 재해 복구 측면



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

몇 번의 클릭이면 전 세계 여러 리전에 애플리케이션을 배포할 수 있습니다.
그러므로 최소한의 비용으로 간단하게 지역 시간을 단축하고 고객 경험을
개선할 수 있습니다.



Amazon Web Services에서는 기업이 지난 수십 년간 사용해 온 익숙한 보안 접근 방식을 제공합니다. 중요한 것은 이와 더불어 클라우드 컴퓨팅의 유연성과 저렴한 비용도 제공한다는 것입니다. 온디맨드 인프라를 제공하면서 동시에 기업이 기존의 자체 소유 환경에서 기대하는 보안 격리도 제공하는 데는 아무런 문제가 없습니다.

정상적인 동작 이해

AWS Shield는 다음과 같은 공격을 비롯해 모든 유형의 DDoS 공격으로부터 웹 사이트를 보호할 수 있게 해줍니다.

- 인프라 계층 공격(UDP flood 등).
- 상태 고갈 공격(TCP SYN flood 등).
- 애플리케이션 계층 공격(HTTP GET 또는 POST flood 등).

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

AWS에서는 DDoS 공격으로부터 보호를 위해 AWS Shield Standard 및 AWS Shield Advanced를 제공합니다. AWS Shield Standard는 AWS WAF 및 기타 AWS 서비스에 대해 이미 지불한 비용 외에 다른 추가 비용 없이 자동으로 포함됩니다. AWS는 AWS DDoS 공격에 대한 추가적인 보호를 위해 AWS Shield Advanced를 제공합니다. AWS Shield Advanced는 DDoS 공격으로부터 보호를 Amazon EC2 인스턴스, Elastic Load Balancing 로드 밸런서, CloudFront 배포 및 Amazon Route 53 호스팅 영역까지 확장 적용합니다.

일반적으로 AWS Shield가 탐지하는 인프라 계층 공격의 99%가 Amazon CloudFront 및 Amazon Route 53에 대한 공격의 경우 1초 이내에, 그리고 Elastic Load Balancing에 대한 공격의 경우 5분 이내에 완화됩니다. 나머지 1%의 인프라 공격은 일반적으로 20분 이내에 완화됩니다. 애플리케이션 계층 공격은 AWS WAF에 규칙을 작성함으로써 완화할 수 있습니다. 공격은 수신 트래픽과 함께 검사되고 완화됩니다.

AWS Shield Standard는 AWS에서 실행되는 웹 애플리케이션을 가장 일반적이고 빈번히 발생하는 인프라 계층 공격(예: UDP flood)과 상태 고갈 공격(예: TCP SYN flood)으로부터 자동으로 보호합니다. 또한 고객은 AWS WAF를 사용하여 HTTP POST 또는 GET 플러드와 같은 애플리케이션 계층 공격으로부터 보호할 수 있습니다.

AWS Shield Advanced는 계층 3 및 계층 4 DDoS 공격 완화를 관리합니다. 즉, 사용자가 지정한 웹 애플리케이션을 UDP flood 또는 TCP SYN flood와 같은 공격으로부터 보호합니다. 또한, 애플리케이션 계층(계층 7) 공격의 경우 AWS WAF를 사용하여 자체 완화 기능을 적용하거나, 고객을 대신하여 계층 7 DDoS 공격을 완화하는 규칙을 작성할 수 있는 24X7 AWS DDoS Response Team (DRT)을 이용할 수도 있습니다.

AWS Key Management Service(KMS)

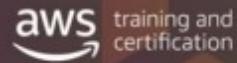
AWS training and certification

- 봉투 암호화를 사용한 2계층 키 구조
- 고유한 데이터 키로 고객 데이터를 암호화
- AWS KMS 마스터 키가 데이터 키를 암호화

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

애플리케이션의 데이터를 암호화해야 하는 개발자라면, AWS KMS를 지원하는 AWS SDK를 사용하여 암호화 키를 쉽게 사용하고 보호할 수 있습니다. 개발자와 증가하는 여러 애플리케이션을 지원하기 위해 확장 가능한 키 관리 인프라를 찾고 있는 IT 관리자라면, AWS KMS를 사용하여 라이선스 비용과 운영 부담을 덜 수 있습니다. 규제 또는 규정 준수를 목적으로 데이터 보안을 제공할 책임이 있는 담당자라면, AWS KMS를 사용하여 데이터가 사용되고 저장되는 애플리케이션 전체에서 지속적으로 데이터가 암호화되는지 확인해야 합니다.

AWS KMS: 이점

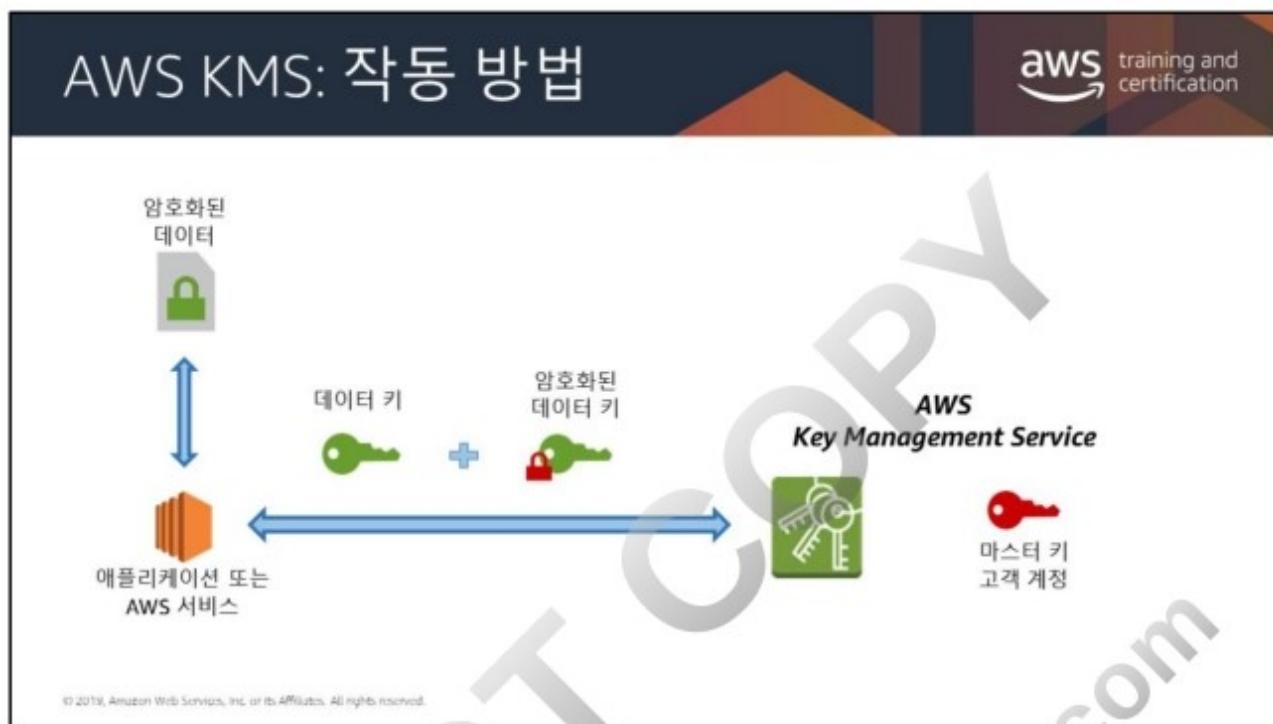


- 마스터 키에는 절대 접근할 수 없습니다.
- 고객은 데이터 키를 직접 사용할 수 있으며, 이 데이터 키는 암호화된 객체마다 고유한 값을 갖습니다.
 - 키 하나가 손상되더라도 해당 키로 다른 객체의 암호화를 해제할 수는 없습니다.
- 손상된 데이터 키로 인한 위험은 매우 적습니다.
- 대용량 데이터에 대한 암호화 성능이 향상되었습니다.
- 수백만 개의 데이터 키보다 소수의 마스터 키를 관리하기가 쉽습니다.

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

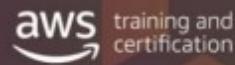
AWS KMS에서 다음과 같은 키 관리 기능을 수행할 수 있습니다.

- 고유한 별칭과 설명으로 키 생성
- 키를 관리할 수 있는 IAM 사용자와 역할을 정의
- 데이터를 암호화 및 암호화 해제할 키를 사용할 수 있는 IAM 사용자와 역할을 정의
- AWS KMS에서 일 년마다 자동으로 키를 교체하도록 설정
- 아무도 사용할 수 없도록 임시로 키 비활성화
- 비활성화된 키를 다시 활성화
- AWS CloudTrail의 로그를 점검하여 키 사용을 감사



1. 애플리케이션 또는 AWS 서비스 클라이언트에서 데이터를 암호화하기 위해 암호화 키를 요청하고 레퍼런스를 해당 계정의 마스터 키로 전달합니다.
2. 클라이언트의 요청은 해당 요청이 마스터 키 사용에 대한 액세스 권한이 있는지에 따라 인증됩니다.
3. 새로운 데이터 암호화 키가 생성되고, 키 사본이 마스터 키로 암호화됩니다.
4. 데이터 키와 암호화된 데이터 키가 모두 고객에게 반환됩니다. 데이터 키는 고객 데이터를 암호화하는 데 사용되고 그런 다음 가능한 한 빠르게 삭제됩니다.
5. 암호화된 데이터 키는 향후 사용을 위해 저장되고 소스 데이터의 암호화를 해제해야 할 때 AWS KMS로 다시 전송됩니다.

WAF를 사용해 계층 7을 보호



WAF는 애플리케이션 계층 트래픽을 검사하고 필터를 적용(HTTP 및 HTTPS)

- 중요한 기능:
 - OWASP 상위 10
 - 속도 제한
 - 화이트리스트 또는 블랙리스트(사용자 지정 가능 규칙)
 - WAF Sandwich로 네이티브 자동 조정
 - 학습 엔진

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

트래픽 속도를 제한하는 방법의 좋은 예는 웹 애플리케이션 방화벽입니다. WAF는 본래 방화벽으로 HTTP 및 HTTPS 트래픽에 특정 규칙을 적용한 것입니다(즉, 포트 80 및 443). AWS에서 이는 소프트웨어 방화벽으로 웹 트래픽을 검사하고 예상 동작의 기준을 준수하는지 확인합니다. 이를 수행하기 위해 WAF를 사용하는 기능은 OWASP (Open Web Application Security Project) 상위 10을 준수합니다. 상위 10 프로젝트의 목적은 조직들이 직면하고 있는 가장 위험한 위험을 확인함으로써 애플리케이션 보안에 관한 인식을 높이는 것입니다. 상위 10 프로젝트는 MITRE, PCI DSS, DISA, FTC 등 많은 표준, 서적, 도구, 조직에 의해 참조되고 있습니다.

앞서 언급한 대로, 속도 제한은 서비스로 보내는 요청의 양 또는 유형을 보고 사용자, 세션 또는 IP 주소당 요청할 수 있는 건수를 제한하는 임계값을 정의하는 능력입니다. 다시 말해, 이는 알 수 없는 공격자로부터 방어막을 제공하기 때문에 ACL에 대한 우수한 보안책입니다.

화이트리스트와 블랙리스트는 사용자를 명시적으로 허용하거나 차단할 수 있어 네트워크 ACL과 유사하지만 WAF 계층에서는 세션 및 프로토콜 설정이 보다 세분화되어 있습니다.

