



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.

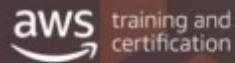
목차

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.

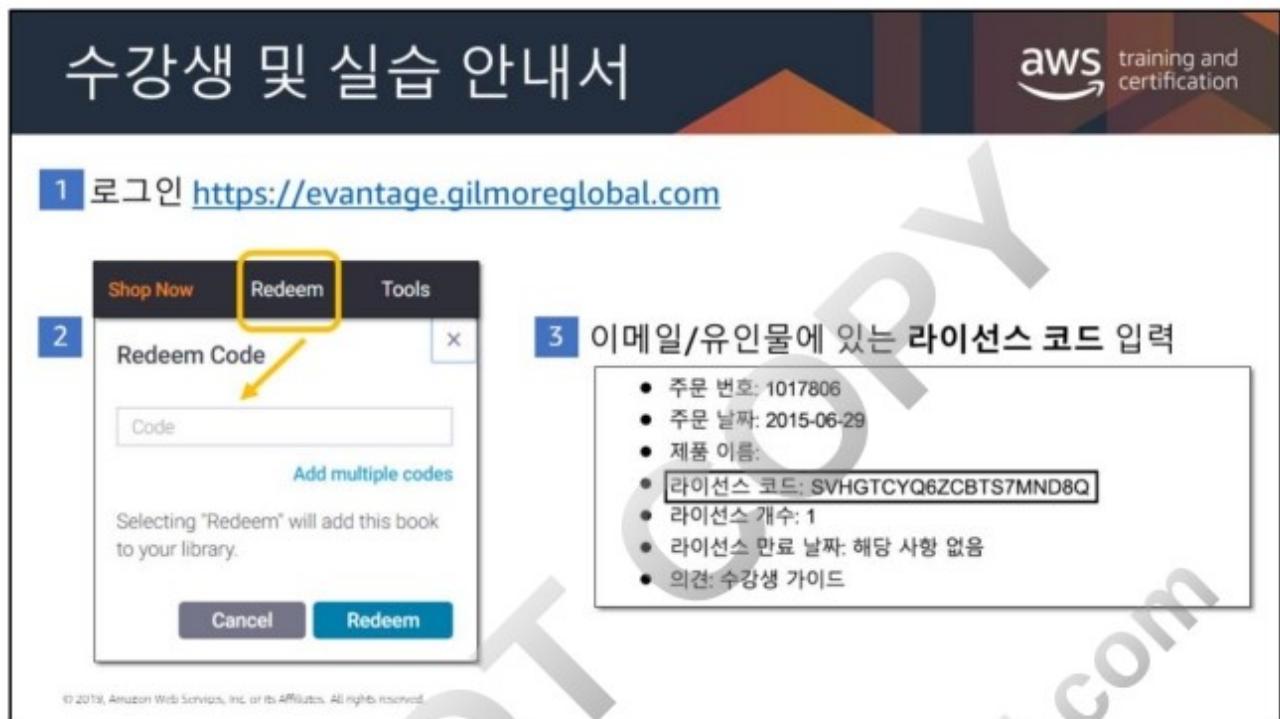
안내 사항



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

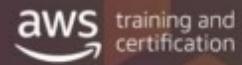
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DO NOT COPY
zlagusdbs@gmail.com



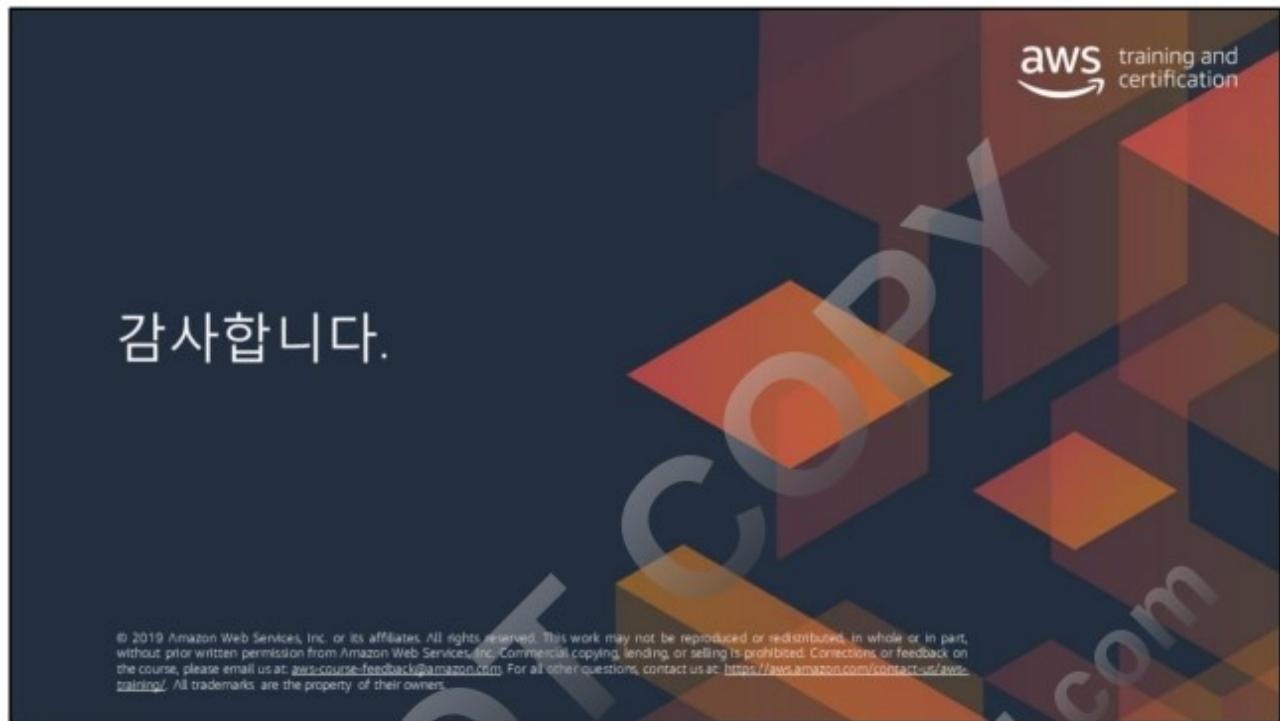
로그인해 수강생 및 실습 안내서에 액세스하려면 <http://online.vitalsource.com>을
참조하십시오.

본인 소개

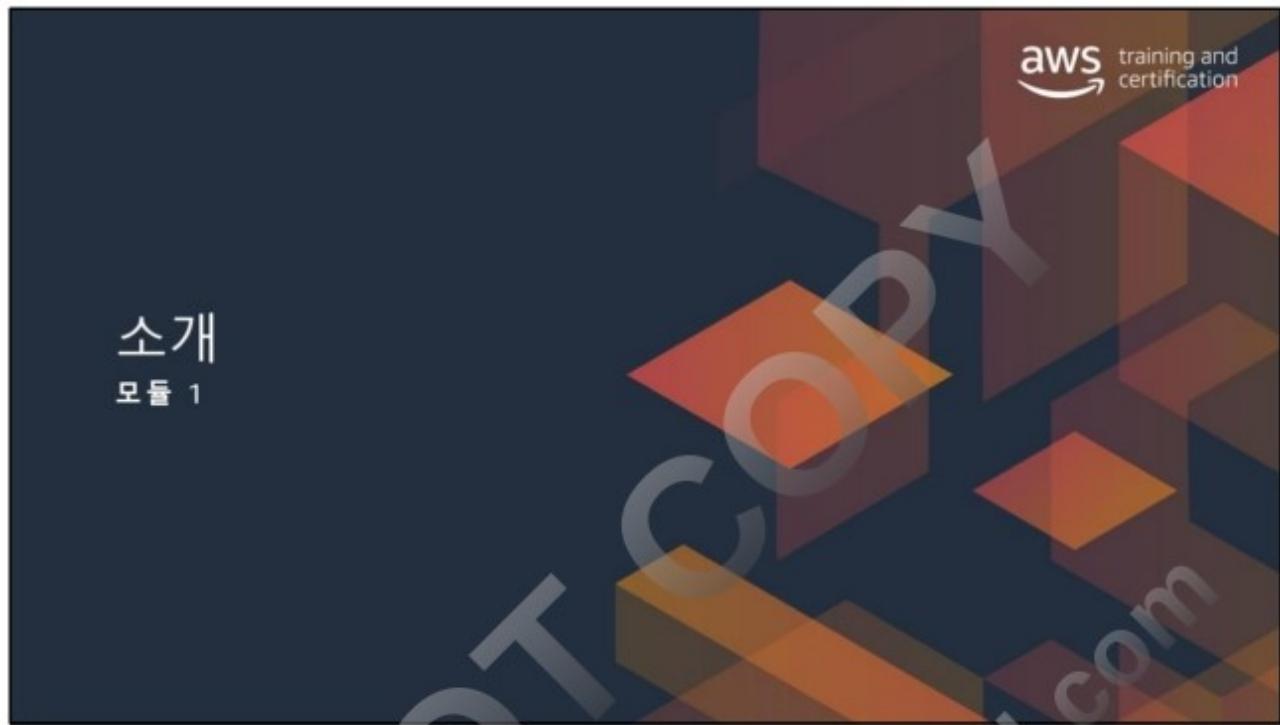


- 이름
- 소속 조직
- 역할
- 기대치
- AWS 경험 수준

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



DO NOT COPY
zlagusdbs@gmail.com



DO NOT COPY
zlagusdbs@gmail.com

미리 보기



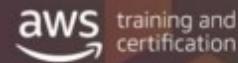
간단한 복습:

- 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.



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.



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

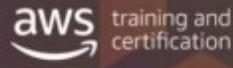
- 애플리케이션 및 아키텍처가 적절한 계획 없이 구축된 것입니다.
- 서비스는 서로 구분되어야 했습니다.

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

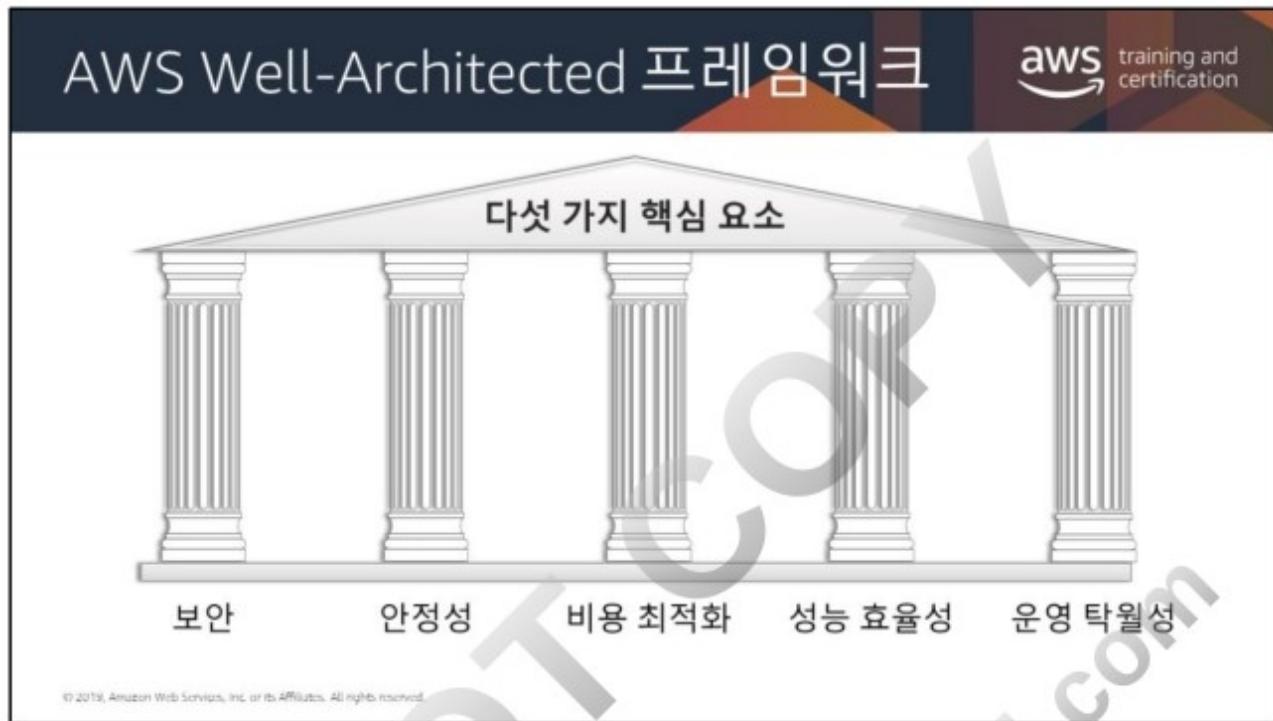
-  자본 비용을 가변 비용으로 대체
-  규모의 경제로 얻게 되는 이점
-  용량 추정 불필요
-  속도 및 민첩성 개선
-  중요한 문제에 집중
-  몇 분 만에 전 세계에 배포

© 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.

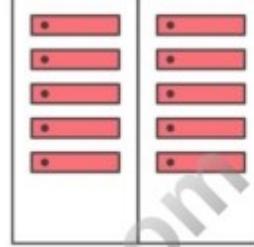
<https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf>

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.

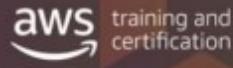
설계 또는 아키텍처를 생성할 때 이들이 배포, 업데이트 및 운영될 방식을 고려합니다. 결함 축소 및 안전한 수정을 위해 노력하고 로깅 계측을 사용한 관찰을 활성화하는 것이 반드시 필요합니다.

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>

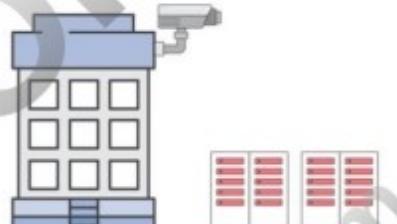


AWS 데이터 센터

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.



ID 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 지연 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 지연 시간을 줄일 수 있는 리전에서 애플리케이션과 워크로드를 실행할 수 있습니다.



최종 사용자에게 더 짧은 지역 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.

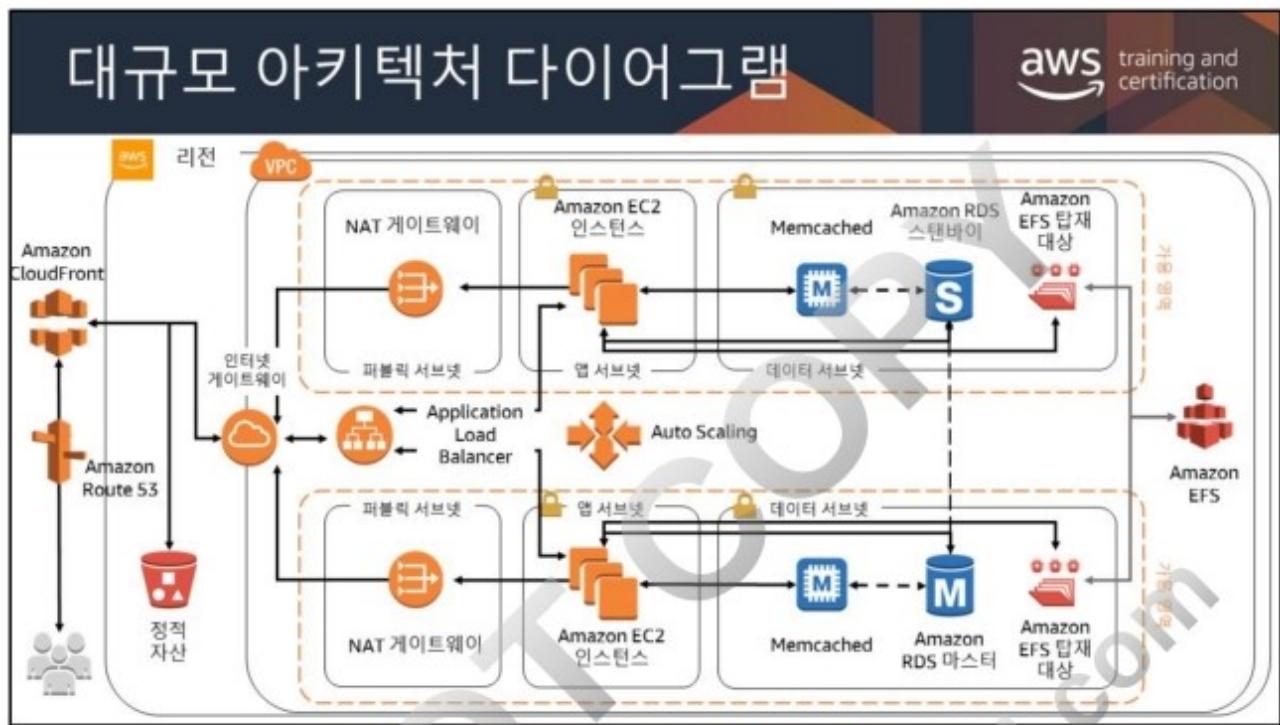
리전 엣지 캐시

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.

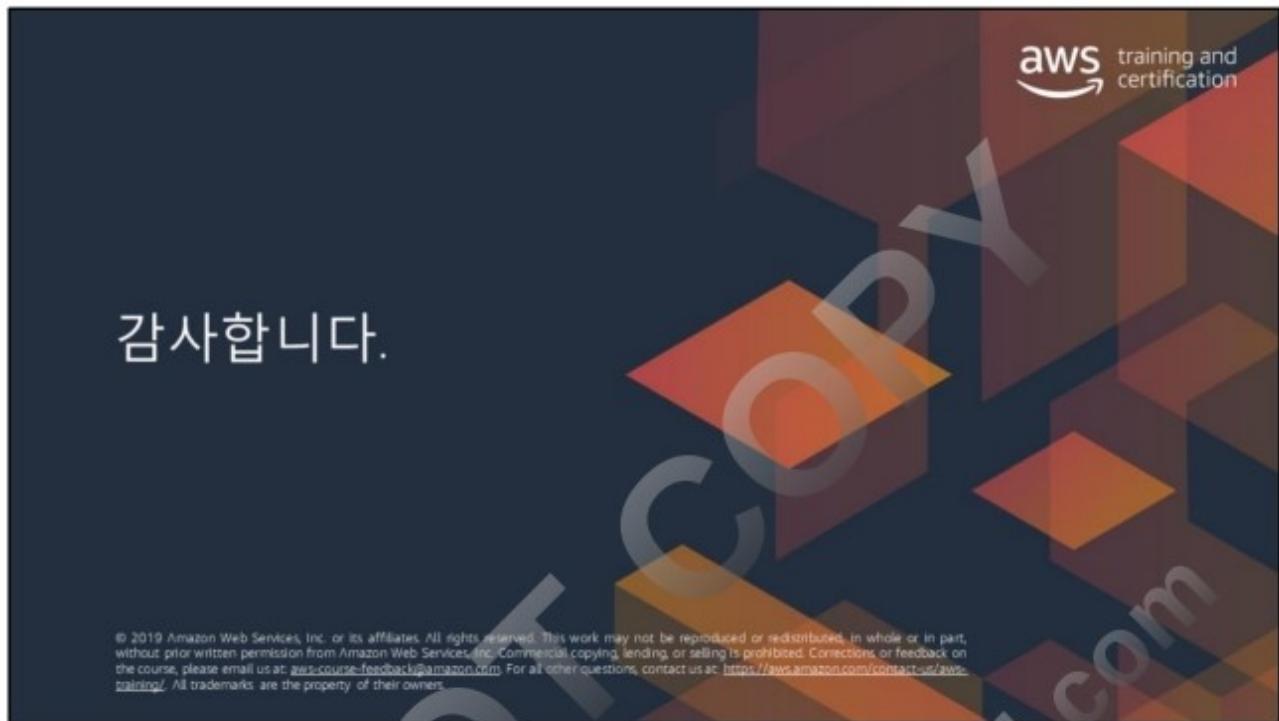
자세한 내용은 <https://aws.amazon.com/cloudfront/features/>를 참조하십시오.



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.

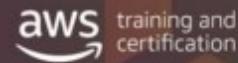






수업이 끝나면 이 아키텍처 디아그램의 모든 구성 요소를 이해할 수 있습니다. 또한 마찬가지로 규모가 크고 강력한 자체 아키텍처 솔루션을 구축할 수 있습니다.

모듈 2



아키텍처 측면에서의 필요성

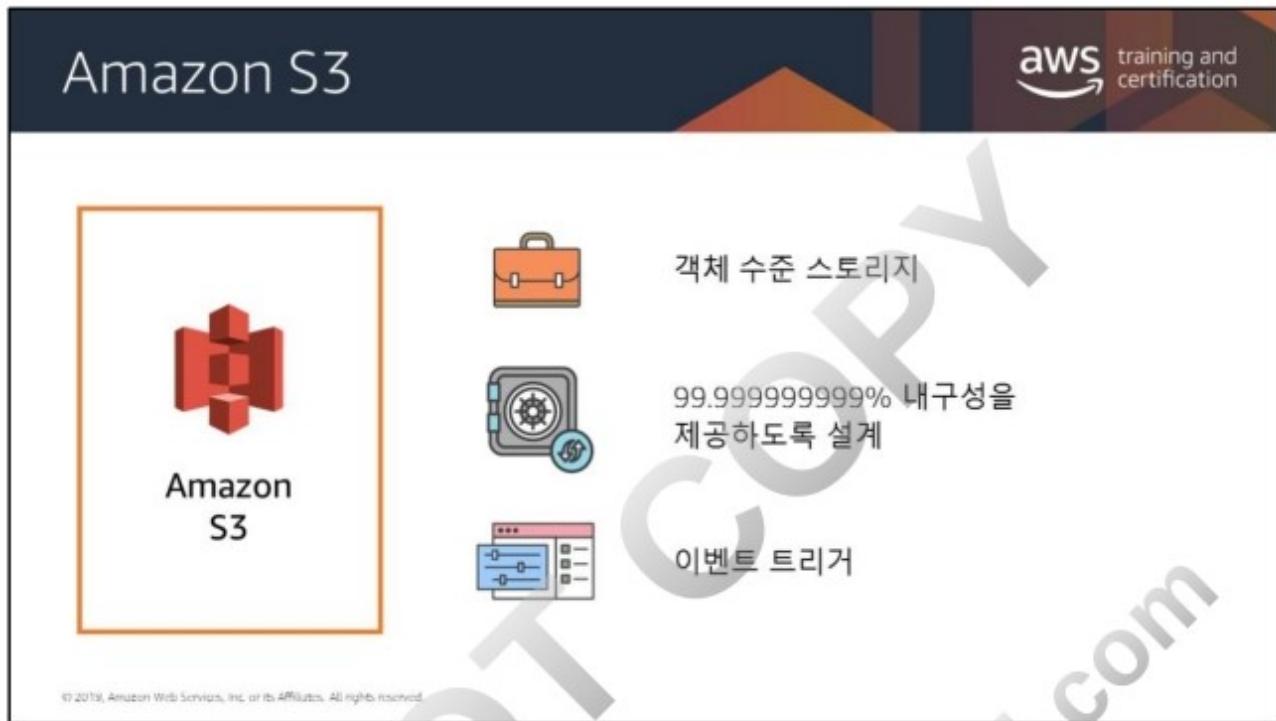
이제 막 창업한 기업으로서 클라우드에서 안정적으로 데이터를 배포, 저장, 분석하는 간편한 방법이 필요합니다.

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.

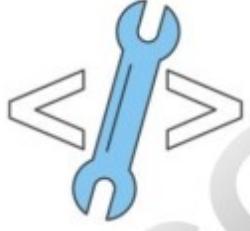
Amazon S3는 웹 기반 AWS Management Console, API 및 SDK를 통한 프로그래밍 방식 또는 타사 솔루션(API/SDK를 사용)을 통해 액세스할 수 있습니다.

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

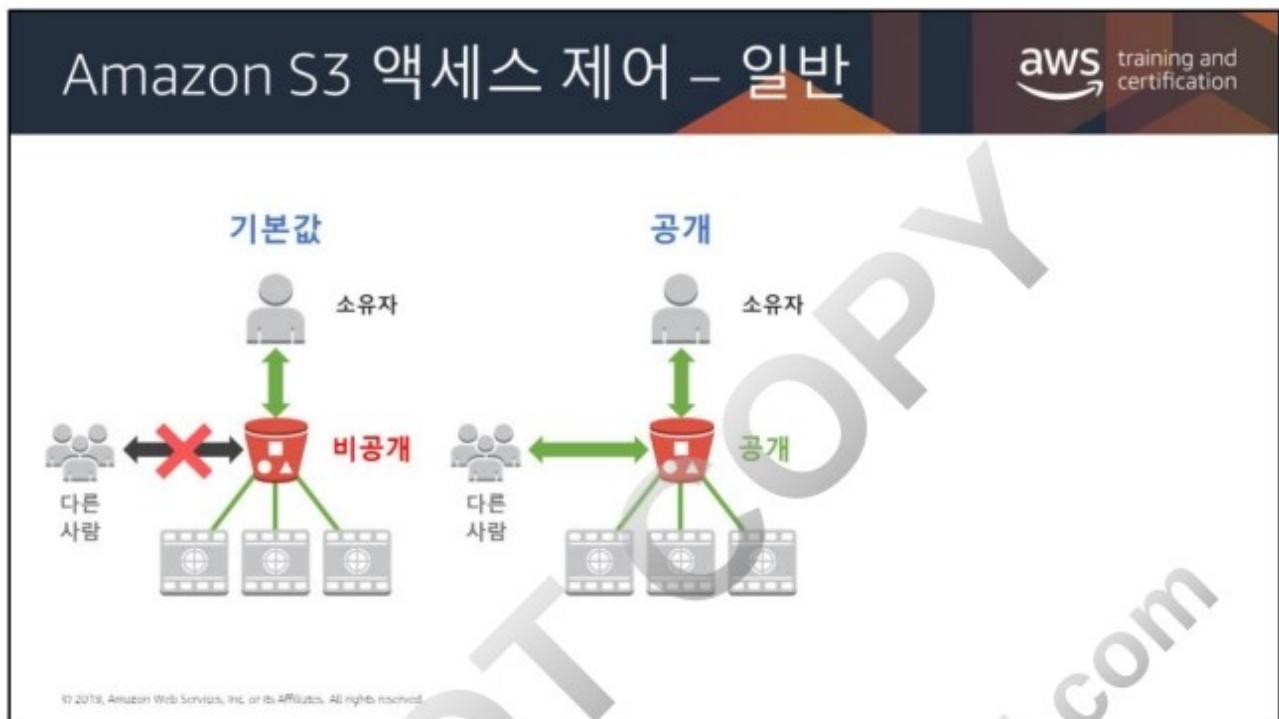
<https://aws.amazon.com/blogs/aws/amazon-s3-block-public-access-another-layer-of-protection-for-your-accounts-and-buckets/>

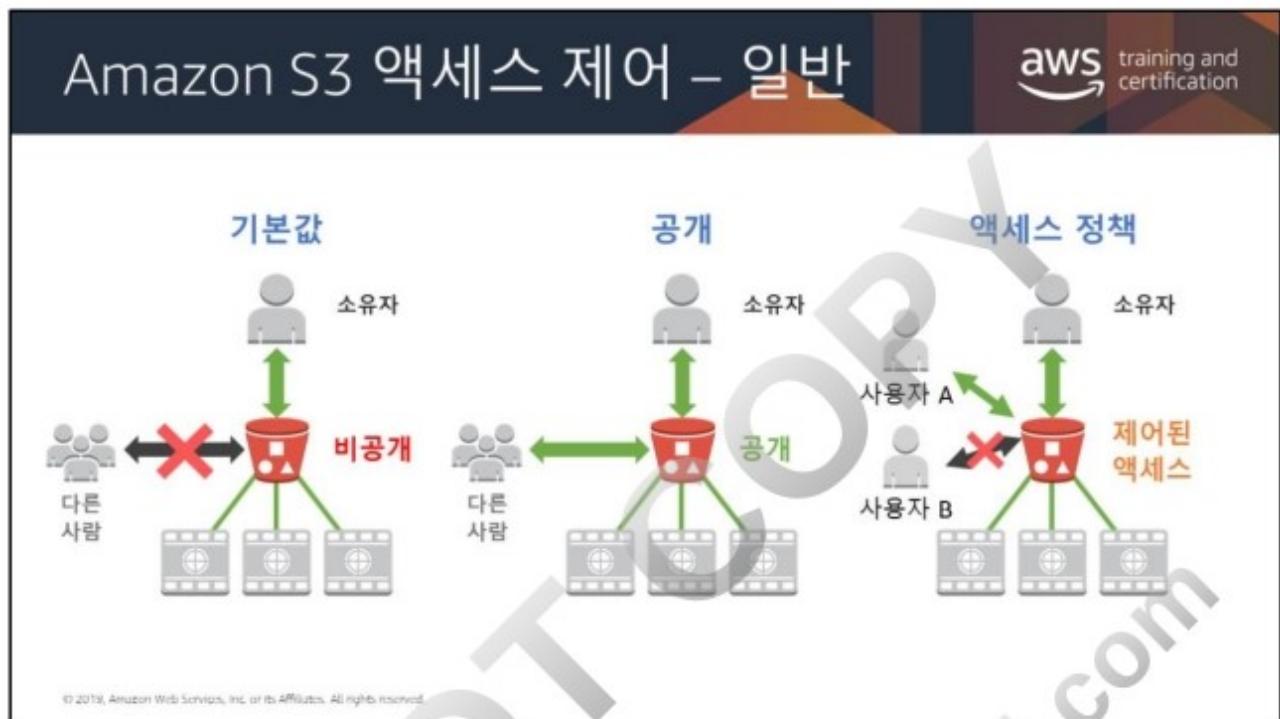
S3 개발자 안내서: Amazon S3 퍼블릭 액세스 차단 사용

<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 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, there is a dashed line connecting the "AWS Policy Generator" text to the JSON document. A watermark "DO NOT COPY" and "zlagusdbs@gmail.com" is diagonally across the page.

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

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

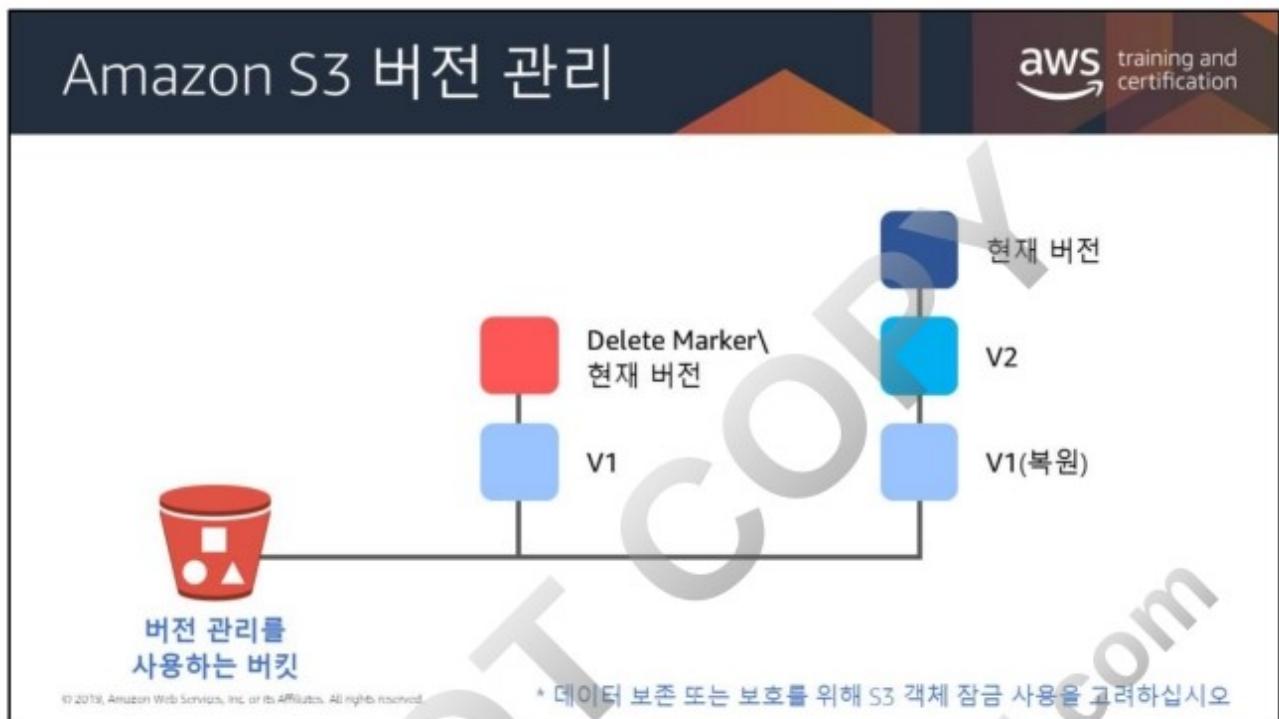
aws training and certification

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>