


## AWS 기반 시스템 구축을 위한 10가지 모범 사례

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

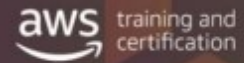
9. 캐싱 사용

10. 모든 계층에서 인프라 보안

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



## 두 개의 진실, 두 개의 거짓



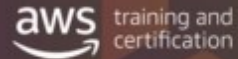
그룹으로, 강의에서 다룬 자료를 통해 선택한 주제에 관한 진실인 설명과 거짓인 설명을 두 개씩 제시합니다.

- 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



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


## 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](https://aws.amazon.com/training)

## 자격증



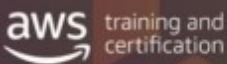
AWS 플랫폼에 대한 기술,  
지식, 전문성을 입증할 수  
있습니다.

[aws.amazon.com/certification](https://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.



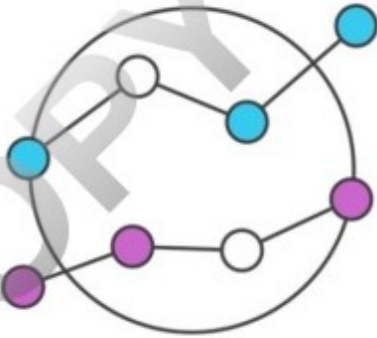


# 비용의 장점

training and certification

## 하드웨어 구매 또는 데이터 센터 구축 불필요

- 리소스를 사용하는 만큼 비용 지불
- 초기 자본 비용 절감

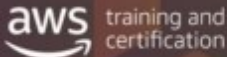


© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

사용 방법이 결정되기도 전에 데이터 센터와 서버에 대규모의 투자를 하는 대신 컴퓨팅 리소스를 사용할 때만, 그리고 사용한 만큼의 리소스에 대해서만 비용을 지불할 수 있습니다.

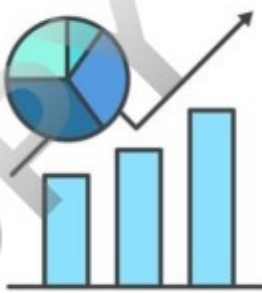
이러한 이점은 특히 스타트업 또는 선결제 예산에 제약이 있는 프로젝트에 적합합니다. 기술의 첨단에 선다는 것은 위험이 따를 수 있습니다. 온프레미스 인프라를 직접 구축할 경우 비용의 제약을 받을 수 있으며, 테스트, 실험 및 혁신이 지연될 수 있습니다. 비용 이점을 통해 신속하게 준비하고 실행할 수 있으면서도 사용한 만큼만 비용을 지불합니다.

# 규모의 장점



## 큰 규모의 경제를 활용

- 자체 보유보다 저렴한 비용
  - 전문화된 하드웨어 및 소프트웨어
  - 대용량 하드웨어 구입



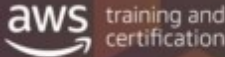
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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 개선하는 데 총당될 수 있습니다.

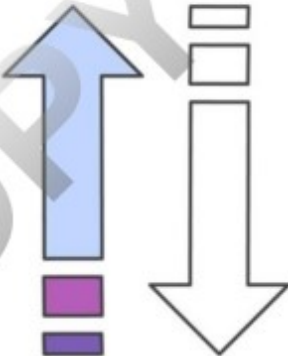


# 용량의 장점



## 용량 추정 불필요

- 필요에 따라 확장 및 축소
- 오버프로비저닝 불필요

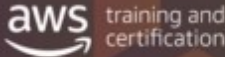


© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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.

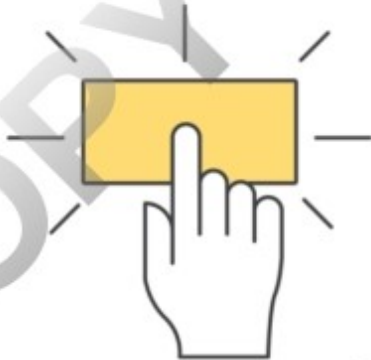
예를 들어 새로운 제품 또는 서비스를 출시하는 경우, 아직 고객의 반응을 알지 못하는 상황이라면 용량을 추정하기란 매우 힘듭니다. 수요 변동 및 급증에 따른 인프라 조정은 대부분의 경우 정적인 온프레미스 솔루션에 비해 엄청난 이점을 제공합니다.

## 속도의 장점



하드웨어를 설치 및 설정할 때까지 기다릴 필요가 없음

- 한 번의 클릭으로 새 IT 리소스 확보
- 리소스 개발 시간 단축



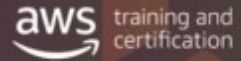
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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



### 인프라가 아니라 애플리케이션에 집중

- 리소스를 확보하여 새 프로젝트에 투자
- 데이터 센터 운영 및 유지 관리에 비용 투자 불필요
- 일회용 리소스를 통해 신속한 실험 가능

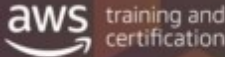


© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

인프라가 아니라 비즈니스를 차별화하는 프로젝트에 집중할 수 있습니다. 클라우드 컴퓨팅을 사용하면 수많은 서버를 관리하느라 시간을 허비하지 않고 고객에게 더욱 집중할 수 있습니다.


클라우드에는 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



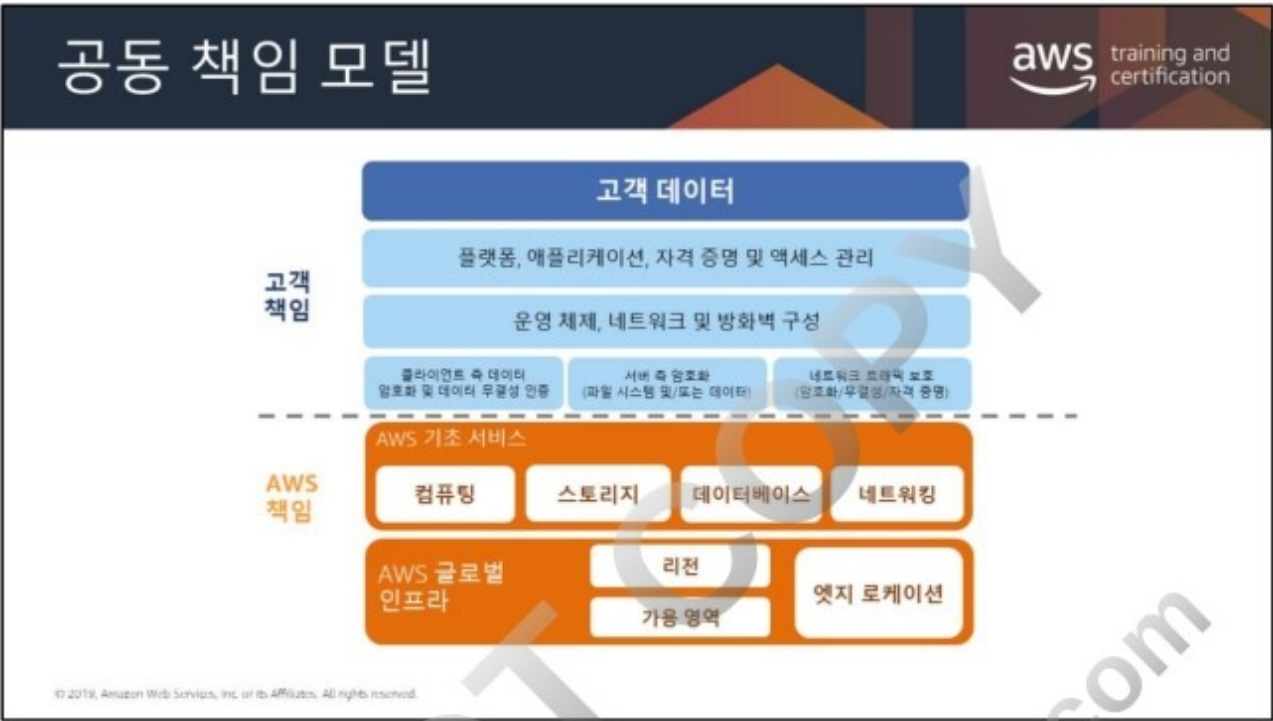
## 몇 분 만에 전 세계에 배포

- 전 세계에 분포된 여러 AWS 리전
- 애플리케이션을 사용자와 가까이 유지
- 고가용성 및 재해 복구 촉진



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

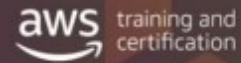
몇 번의 클릭이면 전 세계 여러 리전에 애플리케이션을 배포할 수 있습니다. 그러므로 최소한의 비용으로 간단하게 지연 시간을 단축하고 고객 경험을 개선할 수 있습니다.



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 Shield**는 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).

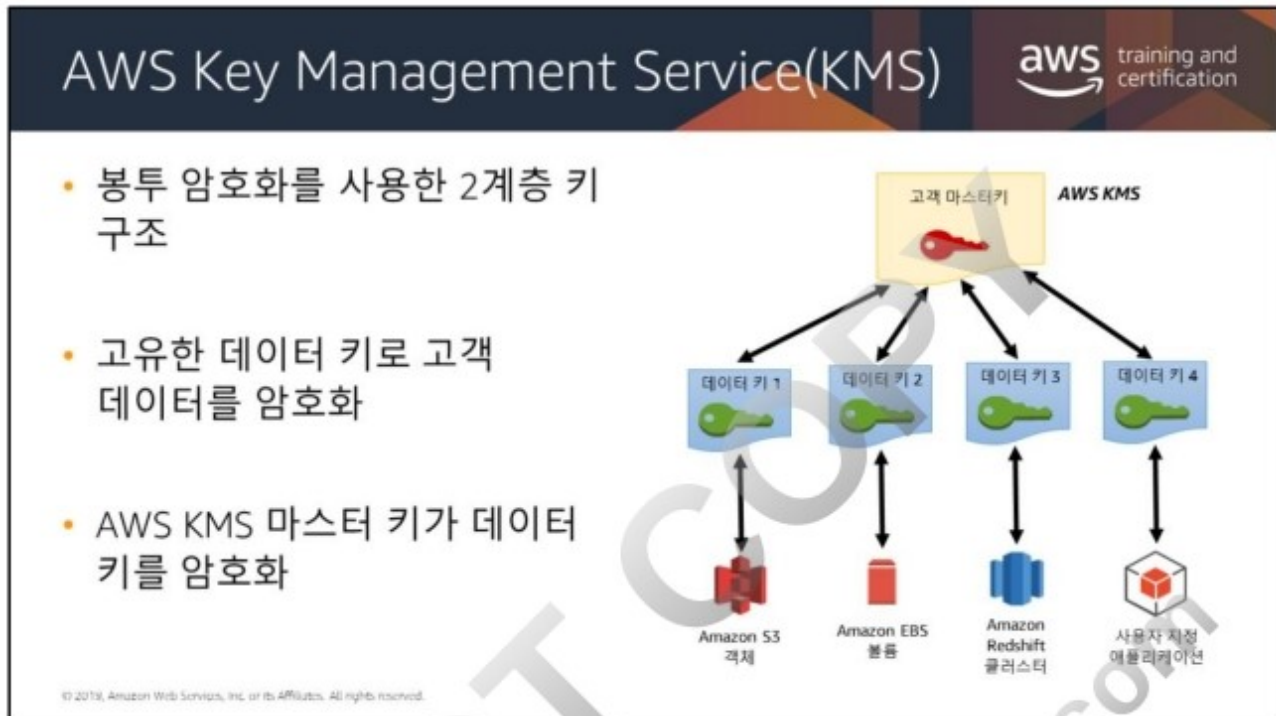
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

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.

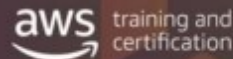
AWS Shield Advanced는 계층 3 및 계층 4 DDoS 공격 완화를 관리합니다. 즉, 사용자가 지정한 웹 애플리케이션을 UDP flood 또는 TCP SYN flood와 같은 공격으로부터 보호합니다. 또한, 애플리케이션 계층(계층 7) 공격의 경우 AWS WAF를 사용하여 자체 완화 기능을 적용하거나, 고객을 대신하여 계층 7 DDoS 공격을 완화하는 규칙을 작성할 수 있는 24X7 AWS DDoS Response Team (DRT)을 이용할 수도 있습니다.



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



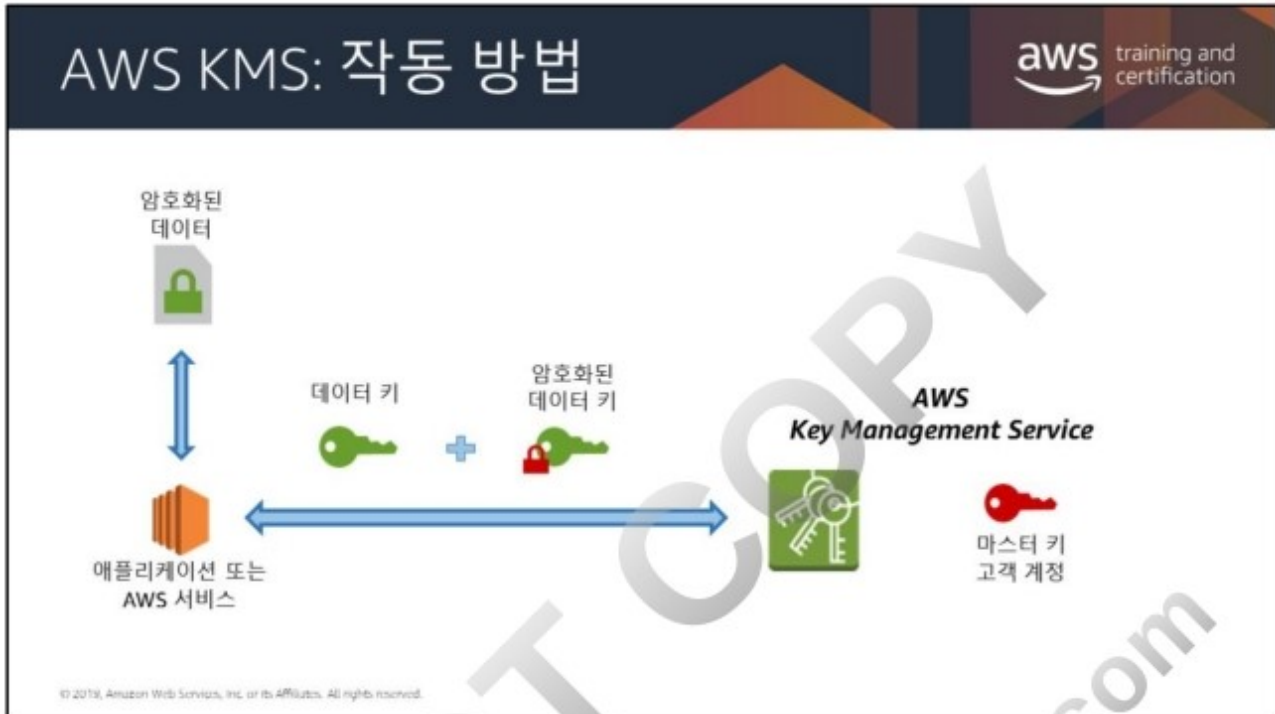
- 마스터 키에는 절대 접근할 수 없습니다.
- 고객은 데이터 키를 직접 사용할 수 있으며, 이 데이터 키는 암호화된 객체마다 고유한 값을 갖습니다.
  - 키 하나가 손상되더라도 해당 키로 다른 객체의 암호화를 해제할 수는 없습니다.
- 손상된 데이터 키로 인한 위험은 매우 적습니다.
- 대용량 데이터에 대한 암호화 성능이 향상되었습니다.
- 수백만 개의 데이터 키보다 소수의 마스터 키를 관리하기가 쉽습니다.

© 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



training and certification

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.

