AWS 소개
보안 프로세스

2016년 6월

(본 문서의 최신 버전을 보려면 다음을 참조하십시오. **http://aws.amazon.com/security/**)

고지 사항

이 문서는 정보 제공 목적으로만 제공됩니다. 본 문서의 발행일 당시 AWS의 현재 제품 및 실행방법을 설명하며, 예고 없이 변경될 수 있습니다. 고객은 본 문서에 포함된 정보나 AWS 제품 또는 서비스의 사용을 독립적으로 평가할 책임이 있으며, 각 정보 및 제품은 명시적이든 묵시적이든 어떠한 종류의 보증 없이 "있는 그대로" 제공됩니다. 본 문서는 AWS, 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 보증, 표현, 계약 약속, 조건 또는 보증을 구성하지 않습니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

목차

소개

Amazon Web Services(AWS)는 높은 가용성과 신뢰성을 갖춘 확장 가능한 클라우드 컴퓨팅 플랫폼을 제공하며, 고객들이 다양한 애플리케이션을 실행하는 데 필요한 도구를 제공합니다. AWS는 고객의 시스템과 데이터의 기밀성, 무결성 및 가용성을 지키고 고객의 믿음과 신뢰를 유지하는 것을 최우선으로 생각합니다. 본 문서는 "AWS가 내 데이터를 보호하는 데 어떠한 도움을 줄 수 있는가?"라는 질문에 답변을 제시할 목적으로 마련되었습니다. 특히 AWS의 물리적 운영 보안 프로세스는 AWS에서 관리하는 네트워크 및 서버 인프라뿐 아니라 서비스별 보안 구현에 대해서도 설명되어 있습니다.

책임 분담 보안 모델

AWS 서비스를 이용하는 고객은 콘텐츠를 완벽하게 제어할 수 있으며, 다음과 같은 중요 콘텐츠 보안 요구 사항을 관리해야 할 책임이 있습니다.

- AWS에 저장하기로 결정한 콘텐츠
- 콘텐츠에 사용되는 AWS 서비스
- 콘텐츠가 저장되는 국가
- 콘텐츠의 형식과 구조 및 마스크, 익명화 또는 암호화 여부
- 콘텐츠에 액세스할 수 있는 사용자 및 그러한 액세스 권한을 부여, 관리 및 취소하는 방법

AWS 고객은 데이터에 대한 제어 권한을 가지고 있기 때문에 AWS "공동 책임" 모델에 따라 해당 콘텐츠에 대한 책임도 져야 합니다. 이 공동 책임 모델은 클라우드 보안 원칙의 맥락에서 고객과 AWS 각자의 역할을 이해하기 위한 기본 전제입니다.

공동 책임 모델에서는 AWS가 호스트 운영 체제 및 가상화 계층에서 서비스 운영 시설의 물리적 보안에 이르기까지 구성 요소를 운영, 관리, 제어합니다. 이에 대해 고객은 AWS가 제공하는 보안 그룹 방화벽 구성, 운영 체제(업데이트 및 보안 패치 포함) 및 기타 관련 애플리케이션 소프트웨어에 대한 관리를 책임집니다. 사용하는 서비스, 서비스를 IT 환경에 통합하는 과정 및 준거법과 규제에 따라 책임 범위가 다르기 때문에 고객은 선택하고자 하는 서비스를 신중하게 고려해야 합니다. 호스트 기반 방화벽, 호스트 기반 침입 탐지/방지, 암호화 등의 기술을 활용하여 보안을 향상하거나 더욱 엄격한 규정 준수 요구 사항을 충족할 수 있습니다. AWS는 고객이 확장된 IT 환경에서 컨트롤이 효과적으로 작동하고 있는지를 검토하고 검증하는 데 도움이 되는 도구와 정보를 제공합니다. 자세한 내용은 AWS 규정 준수 센터(http://aws.amazon.com/compliance)를 참조하십시오.

그림 1: AWS 책임 분담 보안 모델

수행해야 할 보안 구성 작업의 양은 선택한 서비스 및 보유한 데이터의 민감도에 따라 달라집니다. 하지만 개별 사용자 계정 및 자격 증명, 데이터 전송을 위한 SSL/TLS, 사용자 활동 로깅 등의 특정 보안 기능은 어떤 AWS 서비스를 사용하든 사용자가 반드시 구성해야 합니다. 이러한 보안 기능에 대한 자세한 내용은 아래 "AWS 계정 보안 기능" 단원을 참조하십시오.

AWS 보안 책임

AWS는 AWS 클라우드에 제공된 모든 서비스를 실행하는 글로벌 인프라를 보호해야 합니다. 이 인프라는 AWS 서비스를 실행하는 하드웨어, 소프트웨어, 네트워킹, 시설로 구성됩니다. 이 인프라를 보호하는 것은 AWS의 최우선 과제이며 고객이 AWS 데이터 센터나 사옥에 방문하여 직접 확인할 수는 없지만, 각종 컴퓨터 보안 표준과 규정에 대한 준수 사실을 확인한 타사 감사자의 보고서를 제공합니다(자세한 내용은 aws.amazon.com/compliance 참조).

AWS는 이 글로벌 인프라를 보호할 뿐만 아니라, 관리형 서비스로 간주되는 해당 제품의 보안 구성도 책임집니다. 이러한 유형의 서비스에는 Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon WorkSpaces 및 여러 다른 서비스가 포함됩니다. 이러한 서비스는 클라우드 기반 리소스의 확장성 및 유연성과 더불어 관리형 서비스의 장점까지 제공합니다. 이러한 서비스의 경우, 게스트 운영 체제(OS), 데이터베이스 패치, 방화벽 구성, 재해 복구 등의 기본 보안 작업을 AWS가 처리합니다. 이러한 관리형 서비스를 선택하는 고객은 주로 해당 리소스에 대한 논리적 액세스 제어를 구성하고 계정 자격 증명을 보호하기만 하면 됩니다. 이 중 일부는 데이터베이스 사용자 계정 설정 등 추가 작업을 필요로 할 수 있으나 전반적으로 보안 구성 작업은 서비스를 통해 제공됩니다.

고객 보안 책임

AWS 클라우드를 이용하는 고객은 몇 주가 아닌 몇 분만에 가상 서버, 스토리지, 데이터베이스, 데스크톱을 프로비저닝할 수 있습니다. 클라우드 기반 분석 및 워크플로우 도구를 사용해 데이터가 필요할 때 이를 처리한 후 클라우드나 전용 데이터 센터에 저장할 수 있습니다. 어떤 AWS 서비스를 사용하느냐에 따라 고객이 보안 책임의 일부로 수행해야 하는 구성 작업의 범위가 결정됩니다.

Amazon EC2, Amazon VPC처럼 잘 알려진 IaaS(서비스로서의 인프라) 범주에 해당하는 AWS 제품은 고객이 전적으로 제어하기 때문에 필요한 모든 보안 구성과 관리 작업을 직접 수행해야 합니다. 예를 들어 EC2 인스턴스의 경우 사용자는 게스트 OS(업데이트 및 보안 패치 포함)를 비롯하여 인스턴스에 설치한 모든 애플리케이션 소프트웨어나 유틸리티의 관리, 그리고 각 인스턴스에 대해 AWS에서 제공한 방화벽(보안 그룹이라고 부름)의 구성을 책임져야 합니다. 이는 서버 위치와 상관없이 기존에 수행했던 보안 작업과 기본적으로 동일합니다.

Amazon RDS나 Amazon Redshift 같은 AWS 관리형 서비스는 고객이 특정 작업을 수행하는 데 필요한 모든 리소스를 제공하지만 이에 수반될 수 있는 구성 작업은 서비스하지 않습니다. 관리형 서비스를 이용하면 인스턴스의 시작 및 유지 관리 또는 게스트 OS나 데이터베이스 패치 작업 또는 데이터베이스 복제에 대해 걱정할 필요가 없습니다. AWS에서 대신 모두 처리해 드립니다. 하지만 모든 서비스가 그렇듯이 고객은 AWS 계정 자격 증명을 보호하고 Amazon 자격 증명 및 액세스 관리(IAM)를 통해 개별 사용자 계정을 설정하여, 각 사용자에게 고유한 자격 증명을 부여하는 한편 고객의 업무 분리를 실현해야 합니다. 또한 AWS 리소스와의 통신에 SSL/TLS를 사용해야 하는 멀티 팩터 인증(MFA)을 각 계정에 사용하고, AWS CloudTrail을 이용해 API/사용자 활동 기록을 설정하는 것이 좋습니다. 고객이 취할 수 있는 추가 조치에 대한 자세한 내용은 AWS 보안 리소스 웹페이지를 참조하십시오.

AWS 글로벌 보안 인프라

AWS는 고객이 처리 및 스토리지와 같은 다양한 기본적 컴퓨팅 리소스를 프로비저닝하는 데 사용하는 글로벌 클라우드 인프라를 운영합니다. AWS 글로벌 인프라에는 시설, 네트워크 및 하드웨어, 그리고 이러한 리소스의 프로비저닝 및 사용을 지원하는 운영 소프트웨어(예: 호스트 OS, 가상화 소프트웨어 등)가 포함됩니다. AWS 글로벌 인프라는 다양한 보안 규정 준수 표준과 보안 모범 사례에 따라 설계 및 관리됩니다. AWS 고객은 세계에서 보안성이 가장 뛰어난 컴퓨팅 인프라를 기반으로 웹 아키텍처를 구축하고 있는 것이므로 안심할 수 있습니다.

AWS 규정 준수 프로그램

Amazon Web Services 규정 준수는 고객이 클라우드에서 보안과 데이터 보호를 유지하기 위해 AWS에서 시행하고 있는 강력한 통제 항목을 파악하도록 지원합니다. 시스템이 AWS 클라우드 인프라를 기반으로 하여 구축되었기 때문에 규정 준수 책임은 AWS와 고객 간에 공유됩니다. 해당되는 규정 준수 또는 감사 표준과 거버넌스 중심의 감사에 적합한 서비스 기능을 한 데 묶어 놓은 AWS 규정 준수 프로그램은 기존 프로그램 위에 구축되어 있기 때문에 고객이 AWS 보안 제어 환경에서 설정하고 작동할 수 있습니다. AWS가 고객에게 제공하는 IT 인프라는 다음과 같은 다양한 IT 보안 표준과 보안 모범 사례에 맞게 설계 및 관리됩니다.

- SOC 1/SSAE 16/ISAE 3402(이전의 SAS70)
- SOC 2
- SOC 3
- FISMA
- FedRAMP
- DOD SRG 레벨 2 및 4
- PCI DSS Level 1
- EU 모델 조항
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- ITAR
- IRAP
- FIPS 140-2
- MLPS 레벨 3
- MTCS

또한 고객은 AWS 플랫폼이 제공하는 유연성 및 제어 기능으로 특정 산업 표준에 부합하는 솔루션을 배포할 수 있는데 이러한 산업 표준은 다음과 같습니다.

- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- 가족 교육권 및 개인 정보 보호법(FERPA)
- 미국 건강 보험 양도 및 책임에 관한 법(HIPAA)
- 미국영화협회(MPAA)

AWS는 백서, 보고서, 자격증, 승인 및 기타 타사 증명을 통해, IT 제어 환경에 관한 광범위한 정보를 고객에게 제공합니다. 자세한 정보는 http://aws.amazon.com/compliance/에 제공된 위험 및 규정 준수 백서를 참조하십시오.

물리적 및 환경적 보안

AWS의 데이터 센터는 혁신적인 아키텍처 및 엔지니어링 접근 방식을 활용하는 최첨단 센터입니다. AWS는 대규모 데이터 센터를 설계, 구축 및 운영하는 데 있어 유구한 경험을 자랑합니다. AWS 플랫폼과 인프라에 적용하였습니다. AWS 데이터 센터는 평범해 보이는 건물에 구축되어 있습니다. 건물 주위와 입구 지점에서 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단을 활용하여 전문 보안 직원에 의해 이들 건물에 대한 물리적인 접근을 엄격하게 통제하고 있습니다. 허가받은 직원이 데이터 센터에 접근하려면 2가지 요소를 이용한 신원확인과정을 최소 두 번 통과해야 합니다. 모든 방문자 및 계약자는 신분증을 제시해야 하며, 통과한 후에는 허가받은 직원의 지속적인 안내를 받습니다.

AWS는 합법적인 업무 목적으로 이러한 권한이 필요한 계약업체와 직원에게만 데이터 센터 접근 권한 및 정보를 제공합니다. 직원에게 사업상 이러한 권한이 더 이상 필요 없게 되면, 접근 권한은 즉시 해지됩니다. 이는 해당 직원이 Amazon 또는 Amazon Web Services의 직원 신분을 유지해도 마찬가지입니다. AWS 직원의 데이터 센터에 대한 물리적인 접근은 모두 기록되며 정기적으로 감사를 받습니다.

화재 감지 및 진압

위험을 줄이기 위해 자동 화재 감지 및 소화 장비가 설치되었습니다. 화재 감지 시스템은 모든 데이터 센터 환경, 기계 및 전기 장비실, 냉각실 및 발전기 장비실에서 연기 감지 센서를 활용합니다. 이 구역은 습식 파이프, 이중 연동 준비작동식 시스템 또는 기체 스프링클러 시스템으로 보호됩니다.

전력

데이터 센터 전력 시스템은 전이중 방식으로 설계 및 유지관리되도록 설계되어 운영에 전혀 영향을 미치지 않고 365일 항시 사용 가능합니다. 무정전 전원 공급 장치(UPS)는 시설의 중요하고 필수적인 부하에 전력 공급 장애가 발생할 경우에 대비해 백업 전력을 제공합니다. 데이터 센터는 발전기를 사용하여 전체 시설에 백업 전력을 제공합니다.

기후 및 온도

기후 제어는 서버 및 기타 하드웨어의 운영 온도를 일정하게 유지하는 데 필요하며, 이는 과열을 방지하고 서비스 중단 가능성을 줄입니다. 데이터 센터는 최상의 대기 상태 조건을 유지하도록 되어 있습니다. 담당자는 시스템을 통해 적절한 수준의 온도와 습도를 모니터링 및 제어합니다.

관리

AWS는 전기, 기계 및 수명 지원 시스템과 장비를 모니터링하여 어떤 문제든지 즉시 파악할 수 있습니다. 예방적 유지관리는 장비의 지속적인 운영상태를 유지하기 위해 수행됩니다.

스토리지 장치 폐기

스토리지 디바이스의 수명이 다했을 경우 권한이 없는 개인에게 고객 데이터가 노출되는 것을 방지하기 위해 고안된 폐기 프로세스가 AWS 내에 마련되어 있습니다. AWS는 NIST 800-88(“Guidelines for Media Sanitization”)에 폐기 프로세스의 일부로 자세히 설명된 기술을 사용합니다.

비즈니스 연속성 관리

AWS의 인프라는 높은 수준의 가용성을 보장하며, 고객에게 탄력적인 IT 아키텍처를 구현할 수 있는 기능을 제공합니다. AWS는 시스템 또는 하드웨어 장애가 고객에게 미치는 영향을 최소화하도록 시스템을 설계했습니다. AWS에서의 데이터 센터 비즈니스 연속성 관리는 Amazon 인프라 그룹의 내부 지침을 준수하고 있습니다.

가용성

데이터 센터는 전 세계 여러 리전에 클러스터 형태로 구축됩니다. 모든 데이터 센터는 온라인으로 고객에게 서비스를 제공하며, 어떤 데이터 센터도 “정지(cold)”되지 않습니다. 장애 시 자동화된 프로세스는 고객 데이터 트래픽을 장애 지역에서 먼 곳으로 이동합니다. 핵심 애플리케이션이 N+1 구성으로 구현되어, 데이터 센터 장애가 발생할 경우에도 나머지 사이트로 트래픽을 균형 있게 분산시킬 수 있는 충분한 용량을 갖추고 있습니다.

AWS는 각 리전 내의 여러 가용 영역뿐 아니라 여러 지리적 리전 내에 인스턴스를 배치하고 데이터를 저장하는 유연성을 고객에게 제공합니다. 각 가용 영역은 독립된 장애 영역으로 설계되었습니다. 즉 가용 영역은 일반적인 대도시 지역 내에 물리적으로 고립되어 있으며 홍수 위험성이 낮은 지대에 위치합니다(자세한 홍수 지대 분류는 리전에 따라 차이가 있음). 또한, 무정전 전원 공급 장치(UPS)와 현장 백업 발전 시설을 분리하여 독립적인 유틸리티의 서로 다른 그리드를 통해 전력을 공급받음으로써 단일장애점(Single-point-of-Failure)을 더욱 줄여줍니다. 가용 영역은 여러 티어1 전송 서비스 제공자에게 모두 중복으로 연결됩니다.

고객은 다수의 리전 및 가용 영역의 이점을 활용하여 AWS 아키텍처를 구축해야 합니다. 여러 개의 가용 영역에 애플리케이션을 분산함으로써 자연 재해나 시스템 장애 등 대부분의 장애 모드에 직면한 경우에도 시스템을 유지할 수 있게 합니다.

인시던트 대응

Amazon 사고 관리 팀은 비즈니스에 영향을 미치는 이벤트 발생 시 해결책을 모색하기 위해 업계 표준의 진단 절차를 사용합니다. 관리 직원은 상시 사고를 감지하고 이들이 미치는 영향과 해결방안을 관리합니다.

전사적 경영진의 검토

Amazon의 내부 감사 그룹에서는 AWS 복구 계획을 정기적으로 검토합니다. 이 계획은 고위 경영 팀의 구성원 및 이사회 감사 위원회에서도 정기적으로 검토하고 있습니다.

통신

AWS는 다양한 내부 커뮤니케이션 방법을 전사적으로 구현하여 직원들이 자신의 역할과 책임을 이해하고 중요한 사안을 적시에 의논할 수 있도록 돕습니다. 이러한 방법은 신입 직원을 위한 오리엔테이션 및 교육 프로그램, 최근 비즈니스 실적 및 기타 사안에 관한 경영진 정기 회의 그리고 비디오 컨퍼런스, 이메일 메시지, Amazon 인트라넷을 통한 정보 게시 같은 디지털 방식으로 구성됩니다.

AWS는 또한 서비스를 사용하는 고객층과 커뮤니티를 지원하기 위해 다양한 외부 통신 방법을 제공합니다. 고객 지원 팀이 고객의 경험에 영향을 미치는 운영 문제를 전달받을 수 있도록 방법이 마련되어 있습니다. 고객 지원 팀에서 제공 및 관리하는 "서비스 상태 대시보드"는 고객에게 광범위하게 영향을 미칠 수 있는 모든 문제를 알려줍니다. "AWS 보안 센터"를 통해 AWS에 관한 보안 및 규정 준수 세부 정보를 제공 받을 수 있습니다. 또한 고객은 AWS Support 서비스에 가입하여 고객 지원 팀에 직접 문의하거나 고객에게 영향을 미치는 모든 문제를 사전에 통보받을 수 있습니다.

AWS 액세스

AWS 프로덕션 네트워크는 Amazon 사내 네트워크와 분리되어 있으며, 논리적 액세스를 위해서는 별도의 자격 증명 세트가 필요합니다. Amazon 사내 네트워크는 사용자 ID, 암호 및 Kerberos를 사용하여, AWS 프로덕션 네트워크는 배스천 호스트를 통한 SSH 퍼블릭 키 인증을 요구합니다.

AWS 클라우드 구성 요소에 액세스해야 하는 Amazon 사내 네트워크의 AWS 개발자와 관리자는 AWS 액세스 관리 시스템을 통해 명시적으로 액세스 권한을 요청해야 합니다. 모든 요청은 해당 소유자 또는 관리자의 검토와 승인을 거칩니다.

계정 검토 및 감사

계정은 90일마다 검토되고 명시적으로 다시 승인되어야 합니다. 그러지 않으면 리소스에 대한 액세스 권한이 자동으로 취소됩니다. 직원의 기록이 Amazon의 인사관리 시스템에서 제거되는 경우에도 액세스 권한이 자동으로 취소됩니다. Windows 및 UNIX 계정이 비활성화되고 Amazon의 권한 관리 시스템에서 해당 사용자를 모든 시스템에서 삭제합니다.

액세스 권한 변경이 요청되면 Amazon 권한 관리 도구 감사 로그에 캡처됩니다. 직원의 직무가 변경된 경우, 리소스에 계속 액세스하려면 명시적으로 승인받아야 하며, 그러지 않으면 액세스 권한이 자동 취소됩니다.

배경 조회

AWS는 AWS 플랫폼 및 인프라 호스트에 대한 논리적인 액세스의 최소 표준을 제시하기 위해 공식적인 정책 및 절차를 수립했습니다. AWS는 직원에 대한 채용 전 심사 과정의 일환으로 직원의 직급과 액세스 수준에 비례해 법적으로 허용되는 전과 기록 확인을 실시합니다. 또한 이 정책은 논리적인 액세스 및 보안 관리에 대한 기능적인 책임도 명시합니다.

자격 증명 정책

AWS 보안은 필수 설정 및 만료 간격을 포함하는 자격 증명 정책을 수립했습니다. 암호는 복잡해야 하고 90일에 한 번씩 반드시 변경해야 합니다.

보안 설계의 원칙

AWS의 개발 프로세스는 AWS 보안 팀의 공식적인 디자인 검토, 위협 모델링 및 일체의 리스크 평가 등 최선의 보안 소프트웨어 개발 원칙을 준수하고 있습니다. 표준 구축 프로세스의 일환으로 정적 코드 분석 도구를 사용하며, 구현된 모든 소프트웨어는 엄선된 업계 전문가의 반복 침투 테스트를 거칩니다. 보안상의 리스크 평가 검토가 설계 단계에서 시작되어 서비스 시작에서 운영 기간에 이르기까지 지속적으로 이루어집니다

변경 관리

기존 AWS 인프라에 대한 정기적, 긴급 및 구성 변경은 유사한 시스템에 대한 업계 표준에 따라 허가, 기록, 테스트, 승인, 문서화 과정을 거칩니다. AWS의 인프라 업데이트는 고객 및 고객의 서비스 사용에 미치는 영향을 최소화하는 방식으로 이루어집니다. AWS는 서비스 이용에 피해가 예상될 때, AWS 서비스 상태 대시보드 또는 이메일을 통해 고객에게 이 내용을 전달합니다.

소프트웨어

AWS는 변경 관리에 체계적인 접근 방법을 적용하므로 고객에게 영향을 미치는 서비스 변경 사항은 철저한 검토, 테스트, 승인을 거쳐 효과적으로 전달됩니다. AWS의 변경 관리 프로세스는 고객 서비스의 무결성을 유지하고 갑작스런 서비스 중단을 방지하도록 설계되었습니다. 운영 환경에 배포되는 변경 사항은 아래와 같습니다.

- 검토됨: 변경 사항의 기술적 부분에 대한 피어 검토가 요구됩니다.
- 테스트됨: 적용 중인 변경 사항이 예상대로 작동하고 성능을 떨어뜨리지 않는지 확인하기 위해 테스트를 거칩니다.
- 승인됨: 모든 변경 사항은 비즈니스 영향에 대한 적절한 감독과 이해를 위해 반드시 허가를 받아야 합니다.

변경 사항은 일반적으로 영향력이 가장 낮은 영역부터 시작하여 생산단계에 이르기까지 단계별로 적용됩니다. 배포된 사항은 단일 시스템에서 테스트하고 면밀하게 모니터링하여 영향력을 평가할 수 있습니다. 서비스 소유자는 서비스의 업스트림 연관 항목의 상태를 측정하는 여러 개의 설정 가능한 측정치를 보유하고 있습니다. 이 메트릭을 임계치와 경보로 자세히 모니터링합니다. 롤백 절차는 변경 관리(CM) 티켓에 설명되어 있습니다.

가능한 경우, 정규 변경 기간 동안 변경 일정을 수립합니다. 표준 변경 관리 절차와 구별되는 운영 시스템에 대한 긴급 변경 사항은 인시던트와 연관되며 적절한 기록과 승인이 필요합니다.

AWS는 핵심 서비스 변경 사항을 주기적으로 자체 감사하여 품질 모니터링, 높은 수준의 표준 유지 및 변경 관리 프로세스의 지속적인 향상을 도모합니다. 근본 원인을 파악하기 위해 모든 예외사항을 분석하며, 변경 내용이 표준을 준수하도록 하거나 필요한 경우 변경 내용을 롤백하도록 적절한 조치를 취합니다. 그런 다음 프로세스 및 사용자 관련 문제를 해결 및 개선하기 위한 조치를 취합니다.

인프라

Amazon의 기업 애플리케이션 팀은 타사 개발 소프트웨어 공급 분야의 UNIX/Linux 호스트 및 내부적으로 개발된 소프트웨어와 구성 관리 분야에서 IT 프로세스를 자동화하기 위한 소프트웨어를 개발, 관리합니다. 인프라 팀은 하드웨어 확장성, 가용성, 감사 및 보안 관리 작업을 처리하기 위한 UNIX/Linux 구성 관리 프레임워크를 관리 및 운영합니다. 변경사항을 관리하는 자동화된 프로세스를 사용해 호스트를 중앙에서 관리함으로써 AWS는 높은 가용성, 반복성, 확장성, 보안성 및 재해 복구 목표를 달성할 수 있습니다. 시스템 및 네트워크 엔지니어는 지속적으로 이러한 자동화된 도구 상태를 모니터링하며, 구성정보 및 소프트웨어를 확보하거나 업데이트하지 못한 호스트에 대해 보고사항을 검토합니다.

새로운 하드웨어가 지원되면 내부적으로 개발된 구성 관리 소프트웨어가 설치됩니다. 이러한 도구가 구성되었는지 그리고 호스트에 할당된 역할에 따라 결정된 기준을 준수하여 소프트웨어가 설치되었는지 확인하기 위해 모든 UNIX 호스트에서 이를 실행합니다. 이 구성 관리 소프트웨어는 또한 호스트에 이미 설치된 패키지를 정기적으로 업데이트하는 데 도움이 됩니다. 승인 서비스를 통해 허가받은 직원들만 중앙 구성 관리 서버에 로그인할 수 있습니다.

AWS 계정 보안 기능

AWS는 AWS 계정과 리소스가 무단으로 사용되지 않도록 보호하기 위해 사용할 수 있는 다양한 도구와 기능을 제공합니다. 여기에는 액세스 제어를 위한 자격 증명, 암호화된 데이터 전송을 위한 HTTPS 엔드포인트, 별도의 IAM 사용자 계정 생성, 보안 모니터링을 위한 사용자 활동 기록, Trusted Advisor 보안 검사가 포함됩니다. 어떤 AWS 서비스를 선택하든 이 모든 보안 도구를 활용할 수 있습니다.

AWS 자격 증명

권한 있는 사용자와 프로세스만 AWS 계정과 리소스에 액세스할 수 있도록 보장하기 위해 AWS는 다양한 종류의 자격 증명을 사용해 인증합니다. 여기에는 암호, 암호화 키, 디지털 서명, 인증서가 포함됩니다. 또한 AWS 계정이나 IAM 사용자 계정에 로그인할 때 멀티 팩터 인증(MFA)을 요구하는 옵션도 제공합니다. 다음 표는 다양한 AWS 자격 증명과 용도를 강조해서 보여줍니다.

자격 증명 유형	사용	설명
암호	AWS 루트 계정이나 IAM 사용자 계정으로 AWS 관리 콘솔에 로그인	AWS 계정이나 IAM 계정에 로그인하는 데 사용되는 문자열. AWS 암호는 최소 6자, 최대 128자여야 합니다.
멀티 팩터 인증(MFA)	AWS 루트 계정이나 IAM 사용자 계정으로 AWS 관리 콘솔에 로그인	암호와 더불어 AWS 계정이나 IAM 사용자 계정에 로그인하는 데 필요한 6자리 일회용 코드.
액세스 키	디지털로 서명한 AWS API 요청(AWS SDK, CLI 또는 REST/Query API 사용)	액세스 키 ID 및 보안 액세스 키를 포함합니다. 액세스 키를 이용하여 AWS에 대한 프로그래밍 요청을 디지털로 서명합니다.
키 페어	• EC2 인스턴스에 대한 SSH 로그인 • CloudFront 서명 URL • Windows 인스턴스	인스턴스에 로그인하려면 키 페어를 만들고, 인스턴스를 시작할 때 키 페어의 이름을 지정하고, 인스턴스에 연결할 때 프라이빗 키를 제공해야 합니다. Linux 인스턴스는 암호가 없으므로 키 페어를 사용하여 SSH를 통해 로그인합니다. Windows 인스턴스에서는 키 페어를 사용하여 관리자 암호를 가져오고 RDP를 사용하여 로그인합니다.
X.509 인증서	• AWS API에 대한 디지털 서명 SOAP 요청 • HTTPS에 대한 SSL 서버 인증서	X.509 인증서는 SOAP 기반 요청(현재 Amazon S3에서만 사용됨)을 서명하는 용도로만 사용됩니다. AWS에서는 고객이 다운로드할 수 있는 X.509 인증서와 프라이빗 키를 생성하거나, 자격 증명 보고서를 이용해 전용 인증서를 업로드할 수 있습니다.

보안 자격 증명 페이지에서 언제든지 고객 계정에 대한 자격 증명 보고서를 다운로드할 수 있습니다. 이 보고서에는 계정의 사용자와 이들의 자격 증명 상태가 모두 나열됩니다. 즉 사용자의 암호 사용 여부, 암호 만료 여부 및 정기적인 변경 필요성, 암호를 마지막으로 변경한 시점, 액세스 키를 마지막으로 교체한 시점, MFA 활성화 여부가 표시됩니다.

보안상의 이유로, 자격 증명을 분실했거나 잊어버린 경우 복구하거나 다시 다운로드할 수 없습니다. 그 대신, 새 자격 증명을 만든 후 이전 자격 증명 세트를 비활성화하거나 삭제할 수 있습니다.

사실 AWS는 액세스 키와 인증서를 정기적으로 변경(교체)할 것을 권장합니다. AWS는 다중 동시 액세스 키와 인증서를 지원하고 있어서 혹시라도 사용자의 애플리케이션 가용성에 영향을 주는 일 없이 키 교체 작업을 수행할 수 있습니다. 이 기능 덕분에 사용할 키와 인증서를 애플리케이션 다운타임 없이 정기적으로 교체할 수 있습니다. 액세스 키 또는 인증서를 분실하거나 훼손할 위험을 줄일 수 있습니다. AWS IAM API는 고객이 IAM 사용자 계정뿐 아니라 AWS 계정에 대해서도 액세스 키를 교체할 수 있게 해줍니다.

암호

AWS 계정, 개별 IAM 사용자 계정, AWS 토론 포럼, AWS 지원 센터에 액세스하기 위해서는 암호가 필요합니다. 계정을 처음 만들 때 암호를 지정한 후 보안 자격 증명 페이지에서 언제든 변경할 수 있습니다. AWS 암호는 최대 128자 길이이며 특수 문자를 포함할 수 있습니다. 따라서 쉽게 추측할 수 없는 강력한 암호를 만들 것을 권장합니다.

IAM 사용자 계정에 암호 정책을 설정하여, 사용자들이 강력한 암호를 사용하고 자주 변경하도록 할 수 있습니다. 암호 정책은 IAM 사용자가 설정할 수 있는 암호의 유형을 정의한 규칙 세트입니다. 암호 정책에 관한 자세한 내용은 IAM을 이용한 암호 관리를 참조하십시오.

AWS Multi-Factor Authentication(AWS MFA)

AWS Multi-Factor Authentication(AWS MFA)은 AWS 서비스에 액세스하기 위한 추가 보안 계층입니다. 이 옵트인(opt-in) 기능을 활성화한 경우, 고객은 표준 사용자 이름과 암호 자격 증명 외에 6자리 일회용 코드를 입력해야 고객의 AWS 계정 설정 또는 AWS 서비스 및 리소스 액세스 권한이 부여됩니다. 이 일회용 코드는 물리적으로 소유하고 있는 인증 디바이스에서 얻을 수 있습니다. 액세스 권한을 부여하기 전에 복수의 인증 팩터, 즉 암호(고객이 알고 있는 것)와 인증 디바이스(고객이 소유하고 있는 것)로부터의 정확한 코드를 확인하므로 이를 멀티 팩터 인증이라고 합니다. 고객은 MFA 계정뿐 아니라 AWS IAM을 이용해 AWS 계정에 만든 사용자들에 대해서도 MFA 디바이스를 사용하도록 설정할 수 있습니다. 또한 하나의 AWS 계정 하에서 생성한 사용자가 IAM 역할을 이용해 다른 AWS 계정에 속한 리소스에 액세스하도록 허용하려면, AWS 계정 전체의 액세스에 대해 MFA 보호를 추가할 수 있습니다. 사용자가 역할을 수행하기 전에 추가 보안 계층으로 MFA를 사용하도록 요구할 수 있습니다.

AWS MFA는 하드웨어 토큰 및 가상 MFA 디바이스의 사용을 모두 지원합니다. 가상 MFA 디바이스는 물리적 MFA 디바이스와 동일한 프로토콜을 사용하지만, 스마트폰을 비롯한 모바일 하드웨어 디바이스에서만 실행할 수 있습니다. 가상 MFA 디바이스는 시간 기반 일회용 암호(TOTP) 표준(RFC 6238 참조)을 준수하는 6자리 인증 코드를 생성하는 소프트웨어 애플리케이션을 사용합니다. 대부분의 가상 MFA 애플리케이션은 여러 개의 가상 MFA 디바이스를 호스트할 수 있기 때문에 하드웨어 MFA 디바이스보다 편리하게 이용할 수 있습니다. 그러나 가상 MFA는 스마트폰과 같이 보안 수준이 떨어지는 디바이스에서 실행될 수 있으므로 가상 MFA가 하드웨어 MFA 디바이스와 동일한 보안 수준을 제공하지 못할 수 있다는 점에 유의해야 합니다.

또한 Amazon EC2 인스턴스를 종료하거나 Amazon S3에 저장된 중요한 데이터를 읽는 것과 같은 강력한 또는 권한 있는 작업에 대해 추가 보호 계층을 제공하기 위해 AWS 서비스 API에 MFA 인증을 적용할 수도 있습니다. 이렇게 하려면 IAM 액세스 정책에 MFA 인증 요구 사항을 추가합니다. 이러한 액세스 정책을 Amazon S3 버킷, SQS 대기열, SNS 주제와 같은 ACL(액세스 제어 목록)을 지원하는 IAM 사용자, IAM 그룹 또는 리소스에 연결할 수 있습니다.

참여하는 타사 공급자로부터 하드웨어 토큰을, 또는 AppStore에서 가상 MFA 애플리케이션을 입수하여 AWS 웹 사이트를 통해 사용을 설정하는 절차는 간단합니다. AWS MFA에 대한 자세한 정보는 AWS 웹 사이트를 참조하십시오.

액세스 키

AWS는 모든 API 요청에 서명을 요구합니다. 즉, AWS가 요청자의 ID를 확인하는 데 사용할 수 있는 디지털 서명을 포함해야 합니다. 암호화 해시 함수를 이용해 디지털 서명을 계산할 수 있습니다. 이 경우 해시 함수에 대한 입력에는 요청 텍스트와 보안 액세스 키가 포함됩니다. AWS SDK를 이용해 요청을 생성하는 경우 디지털 서명 계산은 자동으로 이루어집니다. 또는, AWS 설명서의 지시에 따라 애플리케이션에 계산을 맡긴 후 그 결과를 REST나 Query 요청에 포함시키는 방법도 있습니다.

서명 프로세스는 요청이 전송되는 동안 훼손을 방지하여 메시지의 무결성을 보호할 뿐만 아니라 재생 공격의 가능성을 차단하는 역할도 합니다. 요청서의 타임스탬프 시간으로부터 15분 이내에 AWS에 요청이 도착해야 합니다. 그렇지 않으면 AWS가 요청을 거부합니다.

최신 버전의 디지털 서명 계산 프로세스는 서명 버전 4로서, HMAC-SHA256 프로토콜을 이용해 서명을 계산합니다. 버전 4는 보안 액세스 키 자체를 사용하기보다는 보안 액세스 키에서 추출한 키를 이용해 메시지에 서명하도록 요구함으로써 이전 버전에 추가적인 보호 조치를 취했습니다. 게다가 자격 증명 범위를 기반으로 서명 키를 추출하기 때문에 서명 키의 암호화 분리가 용이합니다.

액세스 키가 악의적인 사람 손에 들어가면 오용될 수 있기 때문에 안전한 위치에 저장하고 코드에 통합하지 않는 것이 좋습니다. 탄력적으로 확장 가능한 대용량 EC2 인스턴스 집합을 보유한 고객은 IAM 역할을 사용해 액세스 키의 배포를 관리하는 편이 더 안전하고 편리할 수 있습니다. IAM 역할은 대상 인스턴스에 자동으로 로드될 뿐만 아니라 하루에 여러 번 자동으로 교체되는 임시 자격 증명을 제공합니다.

키 페어

Amazon EC2는 퍼블릭 키 암호화 기법을 사용하여 로그인 정보를 암호화 및 해독합니다. 공개 키 암호화 기법은 공개 키를 사용하여 암호 등의 데이터를 암호화하고, 수신자가 개인 키를 사용하여 해당 데이터를 해독하는 방식입니다. 퍼블릭 키와 프라이빗 키를 *키 페어*라고 합니다.

인스턴스에 로그인하려면 키 페어를 만들고, 인스턴스를 시작할 때 키 페어의 이름을 지정하고, 인스턴스에 연결할 때 프라이빗 키를 제공해야 합니다. Linux 인스턴스는 암호가 없으므로 키 페어를 사용하여 SSH를 통해 로그인합니다. Windows 인스턴스에서는 키 페어를 사용하여 관리자 암호를 가져오고 RDP를 사용하여 로그인합니다.

키 페어 만들기

Amazon EC2를 사용하여 키 페어를 만들 수 있습니다. 자세한 내용은 Amazon EC2를 이용한 키 페어 만들기를 참조하십시오.

또는 타사 도구를 사용하고 Amazon EC2로 퍼블릭 키를 가져올 수도 있습니다. 자세한 내용은 Amazon EC2로 사용자의 키 페어 가져오기를 참조하십시오. 각 키 페어에는 이름이 필요합니다. 이름은 당연히 기억하기 쉬워야 합니다. Amazon EC2에서 퍼블릭 키는 키 이름으로 지정한 이름에 연결됩니다.

퍼블릭 키는 Amazon EC2에 저장되며 프라이빗 키는 사용자가 저장합니다. 프라이빗 키 소유자는 임의로 로그인 정보를 해독할 수 있으므로 보안된 장소에 프라이빗 키를 저장해 두는 것이 중요합니다. Amazon EC2에서 사용되는 키는 2048비트 SSH-2 RSA 키입니다. 키 페어는 리전당 최대 5천 개까지 보유할 수 있습니다.

X.509 인증서

X.509 인증서는 SOAP 기반 요청을 서명하는 용도로 사용됩니다. X.509 인증서에는 퍼블릭 키와 추가 메타데이터(인증서가 업로드되는 시점에 AWS가 확인한 만료 날짜 등)가 포함되며 프라이빗 키와 연결됩니다. 요청을 만들려면 프라이빗 키로 디지털 서명을 만든 후 인증서와 함께 이 서명을 요청에 포함해야 합니다. AWS는 인증서에 포함된 퍼블릭 키로 서명을 해독하여 귀하가 발신자임을 확인합니다. AWS는 전송된 인증서가 AWS에 업로드했던 인증서와 일치하는지도 확인합니다.

고객 AWS 계정의 경우, AWS에서 고객이 다운로드할 수 있는 X.509 인증서와 프라이빗 키를 생성하거나, 보안 자격 증명 페이지를 이용해 전용 인증서를 업로드할 수 있습니다. IAM 사용자의 경우, 타사 소프트웨어를 이용해 X.509 인증서(서명 인증서)를 생성해야 합니다. 루트 계정 자격 증명과 달리 AWS는 IAM 사용자용 X.509 인증서를 생성할 수 없습니다. 인증서를 생성한 후 IAM을 이용해 IAM 사용자에게 연결할 수 있습니다.

X.509 인증서는 SOAP 요청뿐만 아니라, HTTPS를 이용해 전송을 암호화하려는 고객의 SSL/TLS 서버 인증서로 사용됩니다. HTTPS에 사용하기 위해 OpenSSL 같은 오픈 소스 도구를 이용하여 고유한 프라이빗 키를 생성할 수 있습니다. 서버 인증서를 얻기 위해 인증 기관(CA)에 제출할 인증서 서명 요청(CSR)을 생성하려면 프라이빗 키가 필요합니다. 그런 다음 AWS CLI를 이용해 인증서, 프라이빗 키, 인증서 체인을 IAM에 업로드합니다.

EC2 인스턴스를 위한 사용자 지정 Linux AMI를 생성할 때도 X.509 인증서가 필요합니다. 이 인증서는 EBS 지원 AMI와 다른 인스턴스 지원 AMI를 생성하는 경우에만 필요합니다. AWS에서는 고객이 다운로드할 수 있는 X.509 인증서와 프라이빗 키를 생성하거나, 보안 자격 증명 페이지를 이용해 전용 인증서를 업로드할 수 있습니다.

개별 사용자 계정

AWS는 AWS 계정 내에서 개별 사용자를 생성하고 관리할 수 있도록 AWS 자격 증명 및 액세스 관리(IAM)라는 중앙 집중화된 메커니즘을 제공합니다. 사용자는 프로그래밍 방식으로 또는 AWS 관리 콘솔이나 AWS 명령줄 인터페이스(CLI)를 통해 AWS 리소스와 상호 작용하는 개인, 시스템 또는 애플리케이션일 수 있습니다. 각 사용자는 AWS 계정 내에서 다른 사용자와 공유하지 않는 고유한 이름과 고유한 보안 자격 증명 세트를 보유합니다. AWS IAM은 암호나 키를 공유할 필요를 없애는 동시에 고객의 AWS 계정 자격 증명 사용 횟수를 최소화합니다.

IAM의 경우, 사용자가 어떤 AWS 서비스에 액세스하여 어떤 작업을 수행할 수 있는지 제어하는 정책을 정의합니다. 사용자가 작업을 수행하는 데 필요한 최소 권한만 부여할 수 있습니다. 자세한 내용은 아래 AWS 자격 증명 및 액세스 관리(AWS IAM) 단원을 참조하십시오.

보안 HTTPS 액세스 포인트

AWS 리소스에 대한 액세스의 통신 보안을 강화하려면 데이터 전송 시 +HTTP 대신 HTTPS를 사용해야 합니다. HTTPS는 퍼블릭 키 암호화로 염탐, 훼손 및 위조를 방지하는 SSL/TLS 프로토콜을 사용합니다. 모든 AWS 서비스는 고객이 보안 HTTPS 통신 세션을 구축할 수 있도록 보안 고객 액세스 포인트(API 엔드포인트라고도 지칭)를 제공합니다.

현재 여러 서비스를 통해 Elliptic Curve Diffie-Hellman Ephemeral(ECDHE) 프로토콜을 사용하는 고급 암호 그룹도 제공하고 있습니다. ECDHE를 통해 SSL/TLS 클라이언트는 임시적이고 어디에도 저장되지 않는 세션 키를 사용하는 PFS(Perfect Forward Secrecy)를 제공할 수 있습니다. 이렇게 하면 기밀 장기 키 자체가 훼손되더라도 제3자가 무단 캡처한 데이터의 디코딩을 방지할 수 있습니다.

보안 로그

보안 문제를 예방하는 데 있어서 자격 증명 및 암호화된 엔드포인트가 중요한 것처럼, 문제가 발생한 후 이벤트를 이해하기 위해서는 로그가 매우 중요합니다. 보안 도구로서 효과적이려면, 언제 어떤 이벤트가 발생했는지 명시된 목록뿐만 아니라 소스 식별 정보도 로그에 포함되어야 합니다. 사후 조사와 거의 실시간 침입 탐지에 도움을 주기 위해 AWS CloudTrail은 지원되는 서비스의 계정 내에 AWS 리소스 요청 로그를 제공합니다. 각 이벤트에 어떤 서비스가 액세스되었고 어떤 조치가 취해졌는지, 누가 요청했는지 알 수 있습니다. CloudTrail은 로그인 이벤트를 포함해 지원되는 모든 AWS 리소스에 대한 모든 API 호출 관련 정보를 캡처합니다.

CloudTrail을 활성화하면 이벤트 로그가 5분 단위로 제공됩니다. CloudTrail이 여러 리전의 로그 파일을 하나의 Amazon S3 버킷에 집계하도록 구성할 수 있습니다. 그러면 원하는 로그 관리 및 분석 솔루션에 이를 업로드해 보안 분석을 수행하고 사용자 행동 패턴을 감지할 수 있습니다. 기본적으로 로그 파일은 Amazon S3에 안전하게 저장되지만 감사 및 규정 준수 요구 사항에 부합하도록 Amazon Glacier에 아카이브할 수도 있습니다.

CloudTrail의 사용자 활동 로그 외에 Amazon CloudWatch Logs 기능을 사용하여 EC2 인스턴스 및 기타 소스에서 시스템, 애플리케이션, 사용자 지정 로그 파일을 거의 실시간으로 수집하고 모니터링할 수도 있습니다. 예를 들어, 유효하지 않은 사용자 메시지에 대한 웹 서버의 로그 파일을 모니터링하여 게스트 OS에 대한 무단 로그인 시도를 찾아낼 수 있습니다.

AWS Trusted Advisor 보안 검사

AWS Trusted Advisor 고객 지원 서비스는 클라우드 성능 및 복원성만 모니터링하는 것이 아니라 클라우드 보안도 모니터링합니다. Trusted Advisor는 고객의 AWS 환경을 검사하고 비용 절감, 시스템 성능 개선 또는 보안 결함 방지의 여지가 있을 때 권장 사항을 알려 줍니다. 또한 발생할 수 있는 몇몇 가장 일반적인 보안 구성 오류에 대해 알림을 제공합니다. 이러한 오류에는 특정 포트를 열어 두어 해킹 및 무단 액세스에 취약한 상태로 만드는 경우, 내부 사용자를 위한 IAM 계정을 만들지 않은 경우, Amazon S3 버킷에 대해 퍼블릭 액세스를 허용하는 경우, 사용자 활동 로깅(AWS CloudTrail)을 켜지 않은 경우 또는 루트 AWS 계정에서 MFA를 사용하지 않는 경우가 포함됩니다. 조직 내 보안 팀이 자동으로 Trusted Advisor 보안 검사 업데이트 상태에 관한 주간 이메일을 수신하도록 선택할 수도 있습니다. AWS Trusted Advisor 서비스는 제한되지 않은 특정 포트, IAM 사용, 루트 계정의 MFA 등 세 가지 중요한 보안 검사를 포함한 네 가지 검사를 추가 비용 없이 모든 사용자에게 제공합니다. 비즈니스급 또는 엔터프라이즈급 AWS Support에 가입하면 모든 Trusted Advisor 검사에 액세스할 수 있습니다.

네트워킹 서비스

Amazon Web Services를 통해 고객이 정의한 논리적으로 격리된 네트워크를 만들고 AWS 클라우드에 대한 사설 네트워크 연결을 설정할 수 있습니다. 또한 가용성 및 확장성이 높은 DNS 서비스를 사용할 수 있도록 하며, 콘텐츠 전송 웹 서비스를 통해 지연 시간은 짧고 데이터 전송 속도는 높은 상태에서 최종 사용자에게 콘텐츠를 전달할 수 있도록 하는 광범위한 네트워킹 서비스를 제공합니다.

Amazon Elastic Load Balancing 보안

Amazon Elastic Load Balancing은 한 그룹의 Amazon EC2 인스턴스에서 트래픽을 관리하여 인스턴스에 대한 트래픽을 특정 리전의 모든 가용 영역으로 배포합니다. Elastic Load Balancing은 온프레미스 로드 밸런서의 모든 장점 이외에 여러 가지 보안상 이점을 제공합니다.

- Amazon EC2 인스턴스를 대신해 암호화 및 복호화 작업을 수행하고 로드 밸런서에서 중앙집중식으로 관리
- 클라이언트에 단일 접점을 제공하며 네트워크 공격에 대한 1차 방어선의 역할도 수행
- Amazon VPC를 사용하는 경우, Elastic Load Balancing과 연결된 보안 그룹의 생성 및 관리를 지원하여 추가적인 네트워킹 및 보안 옵션을 제공
- 보안 HTTP(HTTPS) 연결을 사용하는 네트워크에서 TLS(이전에는 SSL)를 이용한 종단 간 트래픽 암호화를 지원. TLS를 사용하는 경우, 클라이언트 연결을 종료하는 데 사용된 TLS 서버 인증서를 개별 인스턴스에서가 아니라 로드 밸런서에서 중앙집중식으로 관리할 수 있습니다.

HTTPS/TLS는 장기 보안 키를 사용하여 서버와 브라우저 사이에서 암호화 메시지를 생성하는 데 사용할 단기 세션 키를 생성합니다. Amazon Elastic Load Balancing은 클라이언트와 고객의 로드 밸런서 사이에 연결이 설정되면 TLS 협상에 사용되는 사전 정의된 암호 집합을 사용해 로드 밸런서를 구성합니다. 사전 정의된 암호 집합은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 그러나 일부 고객은 표준 준수를 보장하기 위해 클라이언트에서 특정 암호와 프로토콜(PCI, SOX 등)만 허용하도록 요구할 수 있습니다. 이런 경우, Amazon Elastic Load Balancing이 TLS 프로토콜 및 암호에 대해 서로 다른 구성을 선택할 수 있는 옵션을 제공합니다. 고객은 특정 요구 사항에 따라 암호를 활성화 또는 비활성화하도록 선택할 수 있습니다.

보안 연결을 구성할 때 새롭고 강력한 암호 그룹이 사용되도록 보장하기 위해 클라이언트-서버 협상 중에 로드 밸런서가 암호 그룹 선택 시 최종 결정권을 갖도록 구성할 수 있습니다. Server Order Preference 옵션을 선택하면 로드 밸런서는 클라이언트가 아닌 서버의 암호 그룹 우선순위에 따라 암호 그룹을 선택합니다. 그 결과, 클라이언트가 로드 밸런서에 연결하는 데 사용하는 보안 수준을 더 폭넓게 통제할 수 있습니다.

통신 정보 보호를 더욱 강화하기 위해 Amazon Elastic Load Balancer는 Perfect Forward Secrecy(PFS) 사용을 허용합니다. 이 PFS는 임시적이고 어디에도 저장되지 않는 세션 키를 사용합니다. 이렇게 하면 기밀 장기 키 자체가 훼손되더라도 캡처된 데이터의 디코딩을 방지할 수 있습니다.

HTTPS나 TCP 로드 밸런싱 중 무엇을 사용하든, Amazon Elastic Load Balancing을 통해 서버에 연결된 클라이언트의 원본 IP 주소를 식별할 수 있습니다. 일반적으로 요청이 로드 밸런서를 통해 프록시되면 IP 주소와 포트 등의 클라이언트 연결 정보는 손실됩니다. 이는 로드 밸런서가 클라이언트 대신 서버로 요청을 보내 마치 로드 밸런서가 클라이언트를 요청하는 것처럼 보이기 때문입니다. 연결 통계를 수집하고 트래픽 로그를 분석하거나 IP 주소의 화이트리스트를 관리하기 위해 애플리케이션 방문자에 대한 추가 정보가 필요할 경우 원본 클라이언트 IP 주소 정보가 유용합니다.

Amazon Elastic Load Balancing 액세스 로그에는 로드 밸런서에서 처리하는 각 HTTP와 TCP 요청에 관한 정보가 포함되어 있습니다. 여기에는 요청하는 클라이언트의 IP 주소와 포트, 요청을 처리하는 인스턴스의 백엔드 IP 주소, 요청 및 응답의 크기, 클라이언트의 실제 요청 줄(예를 들어 GET http://www.example.com: 80/HTTP/1.1)이 포함됩니다. 백엔드 인스턴스로 전달되지 않는 요청을 포함해 로드 밸런서로 보낸 모든 요청이 기록됩니다.

Amazon Virtual Private Cloud(Amazon VPC) 보안

통상적으로 고객이 시작하는 Amazon EC2 인스턴스에 Amazon EC2 주소 공간의 퍼블릭 IP 주소가 임의로 할당됩니다. Amazon VPC를 사용하면 AWS 클라우드의 격리된 부분을 만들고, 선택한 범위(예: 10.0.0.0/16)에 프라이빗(RFC 1918) 주소가 있는 Amazon EC2 인스턴스를 시작할 수 있습니다. IP 주소 범위를 기반으로 유사한 인스턴스를 그룹화하여 VPC 내에서 서브넷을 정의한 다음, 라우팅 및 보안을 설정하여 인스턴스 및 서브넷을 드나드는 트래픽 흐름을 제어할 수 있습니다.

AWS는 다음과 같은 여러 수준의 퍼블릭 액세스를 제공하는 구성을 포함하는 다양한 VPC 아키텍처 템플릿을 제공합니다.

- **단일 퍼블릭 서브넷만 있는 VPC.** 고객의 인스턴스는 AWS 클라우드의 프라이빗 격리 섹션에서 실행되며 인터넷에 직접 액세스합니다. 네트워크 ACL 및 보안 그룹을 사용하여 인스턴스를 드나드는 인바운드 및 아웃바운드 네트워크 트래픽을 엄격히 제어할 수 있습니다.
- **퍼블릭 및 프라이빗 서브넷이 있는 VPC.** 이 구성은 퍼블릿 서브넷을 포함하는 이외에 인터넷에서 인스턴스의 주소를 지정할 수 없는 프라이빗 서브넷을 추가합니다. 프라이빗 서브넷의 인스턴스는 NAT(Network Address Translation)를 사용하는 퍼블릭 서브넷을 통해 인터넷과 아웃바운드 연결을 설정할 수 있습니다.
- **퍼블릭 및 프라이빗 서브넷이 있고 하드웨어 VPN 액세스를 제공하는 VPC.** 이 구성은 Amazon VPC와 데이터 센터 사이에 IPsec VPN 연결을 추가하여 데이터 센터를 효과적으로 클라우드까지 확장하는 한편 Amazon VPC의 퍼블릭 서브넷 인스턴스에게 직접 인터넷 액세스를 제공합니다. 이 구성에서는 고객이 기업 데이터 센터 측에 VPN 어플라이언스를 추가할 수 있습니다.
- **프라이빗 서브넷만 있고 하드웨어 VPN 액세스를 제공하는 VPC.** 고객의 인스턴스가 AWS 클라우드의 프라이빗 격리 섹션에서 실행되고 인터넷에서 인스턴스의 주소를 지정할 수 없는 프라이빗 서브넷이 포함됩니다. 이 프라이빗 서브넷을 IPsec VPN 터널을 통해 기업 데이터 센터에 연결할 수 있습니다.

프라이빗 IP 주소를 이용해 두 VPC를 연결하여 두 VPC의 인스턴스가 마치 같은 네트워크에 있는 것처럼 서로 통신하도록 허용할 수도 있습니다. 자체 VPC 간의 VPC 피어링 연결, 또는 단일 리전 내에 있는 다른 AWS 계정에서 VPC와의 VPC 피어링 연결을 만들 수 있습니다.

Amazon VPC 내 보안 기능에는 보안 그룹, 네트워크 ACL, 라우팅 테이블, 외부 게이트웨이가 포함됩니다. 이러한 각 항목은 직접 인터넷 접근 또는 다른 네트워크에 대한 사설 연결을 선택적으로 사용해 확장 가능한 안전하고 격리된 네트워크를 제공함으로써 상호 보완됩니다. Amazon VPC에서 실행되는 Amazon EC2 인스턴스는 아래에서 설명하는 게스트 OS 및 패킷 스니핑으로부터 보호와 관련된 장점을 모두 계승합니다.

단, 고객은 자신의 Amazon VPC만을 위한 VPC 보안 그룹을 생성해야 합니다. Amazon VPC 내부에서는 고객이 생성한 Amazon EC2 보안 그룹이 작용하지 않습니다. 또한 Amazon VPC 보안 그룹은 인스턴스 시작 후 보안 그룹을 변경하는 기능, (TCP, UDP 또는 ICMP만 사용하는 방식이 아니라) 표준 프로토콜 번호를 사용하여 프로토콜을 지정하는 기능 등 EC2 보안 그룹에는 없는 추가 기능을 제공합니다.

각 Amazon VPC는 클라우드상에서 별도로 격리된 네트워크입니다. 각 Amazon VPC에서의 네트워크 트래픽은 다른 모든 Amazon VPC와 격리됩니다. Amazon VPC를 생성할 때 각각에 대해 IP 주소 범위를 선택합니다. 고객은 아래의 제어 방법에 따라 외부 연결을 설정하기 위해 인터넷 게이트웨이, 가상 프라이빗 게이트웨이, 또는 둘 모두를 생성하여 연결할 수 있습니다.

API 액세스: Amazon VPC를 생성 및 삭제하고, 라우팅, 보안 그룹 및 네트워크 ACL 파라미터를 변경하며 그 밖에 다른 기능을 수행하기 위한 호출은 모두 고객의 Amazon 보안 액세스 키를 사용하여 서명이 이루어집니다. 이때 AWS 계정 보안 액세스 키를 사용하거나 AWS IAM을 이용해 만든 사용자의 보안 액세스 키를 사용할 수도 있습니다. 고객의 보안 액세스 키에 액세스하지 않고서는 고객을 대신하여 Amazon VPC API 호출을 생성할 수 없습니다. 또한 기밀성을 유지하기 위해 API 호출을 SSL로 암호화할 수 있습니다. Amazon은 항상 SSL로 보호되는 API 엔드포인트를 사용하도록 권장하고 있습니다. AWS IAM은 또한 고객이 새로 생성된 사용자가 권한을 갖는 API 가운데 어느 것을 호출할 지를 선택할 수 있게 합니다.

서브넷 및 라우팅 테이블: 각 Amazon VPC에 하나 이상의 서브넷을 만들 수 있습니다. Amazon VPC에서 시작되는 각 인스턴스는 하나의 서브넷에 연결됩니다. MAC 스푸핑 및 ARP 스푸핑 등 기존의 계층 2에 대한 보안 공격이 차단됩니다.

Amazon VPC의 각 서브넷은 라우팅 테이블 하나씩과 연결되어 있으며, 서브넷에서 전송되는 모든 네트워크 트래픽은 라우팅 테이블에서 목적지 결정을 위한 처리를 받게 됩니다.

방화벽(보안 그룹): Amazon EC2와 마찬가지로 Amazon VPC는 인스턴스의 수신 및 발신 트래픽을 모두 필터링할 수 있는 완벽한 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.

방화벽은 게스트 운영 체제를 통해 제어할 수 없으며, Amazon VPC API 호출을 통해서만 수정이 가능합니다. AWS는 다양한 인스턴스 및 방화벽 관리 기능에 대해 단계별 액세스 권한을 부여하는 기능을 지원합니다. 따라서 고객은 역할 분리를 통해 추가 보안을 구현할 수 있습니다. 방화벽에서 제공하는 보안 수준은 어느 포트를 어느 기간 동안 어떤 목적으로 개방할 것인지 결정합니다. 정보 기반의 트래픽 관리 및 보안 설계가 인스턴스별로 필요합니다. AWS에서는 IPtable 또는 Windows 방화벽과 같은 호스트 기반 방화벽이 있는 인스턴스별 추가 필터를 사용할 것을 권장합니다.

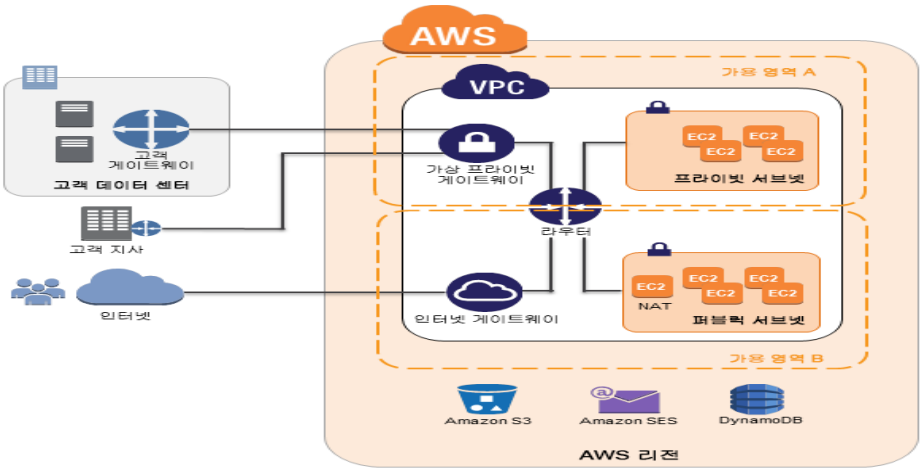

그림 5: Amazon VPC 네트워크 아키텍처

네트워크 액세스 제어 목록: Amazon VPC에 보안 계층을 추가하기 위해 네트워크 ACL을 구성할 수 있습니다. 이 네트워크 ACL은 Amazon VPC 내 서브넷에서 인바운드 또는 아웃바운드하는 모든 트래픽에 적용되는 상태 비저장 트래픽 필터입니다. 이러한 ACL은 IP 프로토콜, 서비스 포트, 원본/대상 IP 주소에 따라 트래픽을 허용 또는 거부하는 정렬된 규칙도 포함할 수 있습니다.

보안 그룹과 마찬가지로, 네트워크 ACL은 Amazon VPC API를 통해서 뿐만 아니라 추가적인 보호 계층과 역할 분리를 통해 추가 보안을 설정함으로써 관리됩니다. 아래 그림에서는 위의 보안 관리 기법이 네트워크 트래픽의 흐름을 완벽하게 제어하는 한편 유연한 네트워크 토폴로지를 구현할 수 있도록 하기 위해 어떻게 상호 연관되는지를 보여 줍니다.

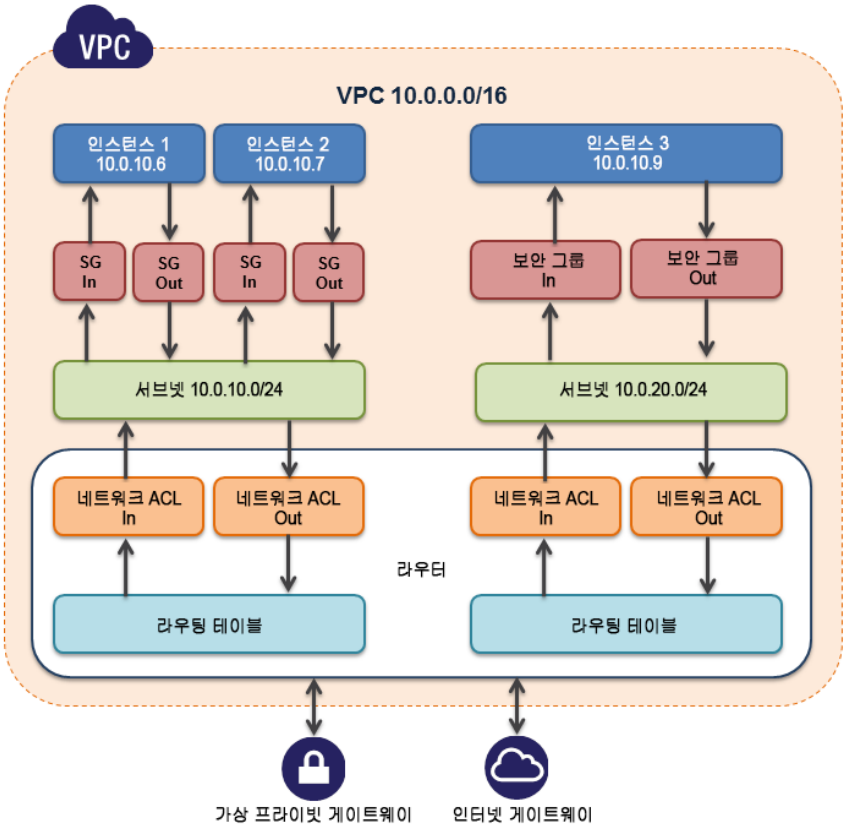

그림 6: 유연 네트워크 토폴로지

가상 프라이빗 게이트웨이: 가상 프라이빗 게이트웨이를 통해 Amazon VPC와 다른 네트워크 사이에 프라이빗 연결이 가능합니다. 각 가상 프라이빗 게이트웨이의 네트워크 트래픽은 다른 모든 가상 프라이빗 게이트웨이의 네트워크 트래픽으로부터 격리됩니다. 고객의 프레미스에 위치하는 게이트웨이 디바이스로부터 가상 프라이빗 게이트웨이와 VPN 연결을 설정할 수 있습니다. 각 연결은 고객 게이트웨이 장치의 IP 주소와 관련된 사전 공유된 키로 보호됩니다.

인터넷 게이트웨이: 인터넷 게이트웨이는 Amazon S3, 다른 AWS 서비스 및 인터넷에 직접 연결이 가능하도록 Amazon VPC에 연결할 수 있습니다. 이러한 접근이 필요한 각 인스턴스는 해당 접근과 관련된 엘라스틱 IP를 보유하거나 NAT 인스턴스를 통해 트래픽을 라우팅해야 합니다. 또한, 인터넷 게이트웨이로 직접 트래픽을 보내도록 네트워크 경로를 구성합니다(위 참조). AWS는 네트워크 로깅, 정밀 패킷 검사, 애플리케이션 계층 필터링 또는 기타 보안 관리를 수행하기 위해 확장이 가능한 참조 NAT AMI를 제공합니다.

이 접근 권한은 Amazon VPC API 호출을 통해서만 수정할 수 있습니다. AWS는 인스턴스 및 인터넷 게이트웨이의 서로 다른 관리 기능에 대한 세부적인 접근 권한을 부여하는 기능을 지원합니다. 따라서 고객은 역할 구분을 통해 추가 보안을 구현할 수 있습니다.

전용 인스턴스: VPC에서는 고객이 호스트 하드웨어 수준에서 물리적으로 분리된 Amazon EC2 인스턴스를 시작할 수 있습니다(이러한 인스턴스는 단일 테넌트 하드웨어에서 실행됨). '전용' 테넌시를 이용해 Amazon VPC를 생성할 수 있습니다. 그러면 Amazon VPC에서 시작되는 모든 인스턴스가 이 기능을 사용합니다. 또는 '기본' 테넌시를 이용해 Amazon VPC를 생성할 수 있습니다. 하지만 이 Amazon VPC에서 시작되는 특정 인스턴스에 대해 전용 테넌시를 지정할 수 있습니다.

탄력적 네트워크 인터페이스: 각 Amazon EC2 인스턴스는 고객의 Amazon VPC 네트워크에서 프라이빗 IP 주소로 지정된 기본 네트워크 인터페이스를 갖습니다. 고객은 ENI(엘라스틱 네트워크 인터페이스)로 알려진 추가 네트워크 인터페이스를 생성한 후 Amazon VPC의 Amazon EC2 인스턴스에 연결하여 인스턴스당 총 2개의 네트워크 인터페이스를 사용할 수 있습니다. 네트워크 인스턴스에 복수의 네트워크 인터페이스를 연결할 경우 관리 네트워크를 만들거나, Amazon VPC에서 네트워크 및 보안 어플라이언스를 사용하거나, 별도의 서브넷에 워크로드/역할이 있는 이중 홈 인스턴스를 만들 때 유용합니다. 프라이빗 IP 주소, 탄력적 IP 주소, MAC 주소 등 ENI의 속성은 인스턴스와 연결될 때, 또는 한 인스턴스에서 분리되어 다른 인스턴스로 연결될 때의 ENI를 따릅니다. Amazon VPC에 대한 자세한 정보는 AWS 웹 사이트를 참조하십시오. http://aws.amazon.com/vpc/

EC2-VPC를 통한 추가 네트워크 액세스 제어

AWS가 새 EC2-VPC 기능(기본 VPC라고도 함)을 시작하기 전에 인스턴스를 실행한 적이 없는 리전에서 인스턴스를 시작할 경우, 모든 인스턴스가 즉시 사용 가능한 기본 VPC에서 자동으로 프로비저닝됩니다. 고객은 추가 VPC를 생성할 수도 있고, AWS가 EC2-VPC를 시작하기 전에 이미 인스턴스를 실행한 적이 있는 리전의 인스턴스를 위해 VPC를 생성할 수도 있습니다.

일반 VPC를 사용하여 나중에 VPC를 생성하는 경우 CIDR 블록을 지정하고, 서브넷을 생성하고, 생성한 서브넷에 대해 라우팅 및 보안을 입력하고, 서브넷 중 하나를 인터넷과 연결하려는 경우 인터넷 게이트웨이 또는 NAT 인스턴스를 프로비저닝합니다. EC2 인스턴스를 EC2-VPC에서 시작할 때 이 작업이 대부분 자동으로 실행됩니다. EC2-VPC를 사용하여 기본 VPC에서 인스턴스를 시작하면 AWS가 다음 작업을 수행하여 인스턴스를 설정합니다.

- 각 가용 영역에서 기본 서브넷을 생성합니다
- 인터넷 게이트웨이를 생성하여 기본 VPC와 연결합니다
- 인터넷으로 향하는 모든 트래픽을 인터넷 게이트웨이로 전송하는 규칙을 사용하여 기본 VPC에 대한 기본 라우팅 테이블을 생성합니다
- 기본 보안 그룹을 만들어 기본 VPC와 연결합니다
- 네트워크 ACL(액세스 제어 목록)을 생성하여 기본 VPC와 연결합니다
- AWS 계정에서 설정된 기본 DHCP 옵션을 기본 VPC와 연결합니다

기본 VPC가 자체 프라이빗 IP 범위를 갖는 이외에, 기본 VPC에서 시작한 EC2 인스턴스에도 퍼블릭 IP가 할당됩니다.

다음 표는 EC2-Classic, 기본 VPC, 그리고 기본값 아닌 VPC에서 시작되는 인스턴스의 차이점을 요약한 것입니다.

특성	EC2-Classic	EC2-VPC(기본 VPC)	일반 VPC
퍼블릭 IP 주소	인스턴스에 퍼블 IP 주소가 할당됩니다.	시작 시 다르게 지정하지 않은 한, 기본 서브넷에서 시작한 인스턴스에는 기본적으로 퍼블릭 IP 주소가 할당됩니다.	시작 시 다르게 지정하지 않은 한, 인스턴스에는 기본적으로 퍼블릭 IP 주소가 할당되지 않습니다.
프라이빗 IP 주소	인스턴스를 시작할 때마다 EC2-Classic 범위 내의 프라이빗 IP 주소가 할당됩니다.	인스턴스를 시작할 때 마다 기본 VPC 범위 내의 사설 프라이빗 IP 주소가 할당됩니다.	인스턴스를 시작할 때 마다 사용 VPC 범위 내의 프라이빗 고정 IP 주소가 할당됩니다.
다중 프라이빗 IP 주소	AWS가 사용자의 인스턴스를 위해 단일 IP 주소를 선택합니다. 다중 IP 주소는 지원하지 않습니다.	인스턴스에 다중 프라이빗 IP 주소를 할당할 수 있습니다.	인스턴스에 다중 프라이빗 IP 주소를 할당할 수 있습니다.
탄력적 IP 주소	인스턴스를 중지하면, EIP는 더이상 그 인스턴스와 무관하게 됩니다.	인스턴스를 중지해도 EIP는 여전히 그 인스턴스의 IP입니다.	인스턴스를 중지해도 EIP는 여전히 그 인스턴스의 IP입니다.
DNS 호스트 이름	기본적으로 DNS 호스트 이름을 사용하도록 되어있습니다.	기본적으로 DNS 호스트 이름을 사용하도록 되어있습니다.	기본적으로 DNS 호스트 이름을 사용하지 않도록 되어있습니다.
보안 그룹	보안 그룹에서 다른 AWS 계정에 속한 보안 그룹을 참조할 수 있습니다.	보안 그룹에서는 사용자의 VPC 내 보안 그룹만 참조할 수 있습니다.	보안 그룹에서는 사용자의 VPC 내 보안 그룹만 참조할 수 있습니다.
보안 그룹 연결	보안 그룹을 변경하려면 인스턴스를 종료해야 합니다.	실행 중인 인스턴스의 보안 그룹을 변경할 수 있습니다.	실행 중인 인스턴스의 보안 그룹을 변경할 수 있습니다.
보안 그룹 규칙	인바운드 트래픽에만 규칙을 추가할 수 있습니다.	인바운드 및 아웃바운드 모두에 규칙을 지정 할 수 있습니다.	인바운드 및 아웃바운드 모두에 규칙을 지정 할 수 있습니다.

테넌시	인스턴스가 공유된 하드웨어에서 실행됩니다. 단일 테넌트 하드웨어에서는 인스턴스를 실행할 수 없습니다.	공유된 하드웨어나 단일 테넌트 하드웨어에서 인스턴스를 실행할 수 있습니다.	공유된 하드웨어나 단일 테넌트 하드웨어에서 인스턴스를 실행할 수 있습니다.

EC2-Classic 인스턴스의 보안 그룹은 EC2-VPC 인스턴스의 보안 그룹과 약간 다릅니다. 예를 들어, EC2-Classic의 경우 인바운드 트래픽에 대한 규칙을 추가할 수 있지만, EC2-VPC의 경우 인바운드 및 아웃바운드 트래픽 모두에 대한 규칙을 추가할 수 있습니다. EC2-Classic에서는 인스턴스가 시작된 후에는 인스턴스에 할당된 보안 그룹을 변경할 수 없지만, EC2-VPC에서는 인스턴스가 시작된 후에도 인스턴스에 할당된 보안 그룹을 변경할 수 있습니다. 또한 EC2-Classic에서 사용하기 위해 생성한 보안 그룹을 VPC의 인스턴스에서는 사용할 수 없습니다. VPC 인스턴스 전용으로 보안 그룹을 생성해야 합니다. VPC용 보안 그룹에서 사용하기 위해 생성한 규칙은 EC2-Classic용 보안 그룹을 참조할 수 없으며 그 반대의 경우도 마찬가지입니다.

Amazon Route 53 보안

Amazon Route 53는 가용성과 확장성이 우수한 DNS(도메인 이름 시스템) 서비스로, DNS 쿼리에 응답하여 컴퓨터가 서로 통신할 수 있도록 도메인 이름을 IP 주소로 변환합니다. Route 53를 사용하여 AWS에서 실행 중인 인프라(예: Amazon EC2 인터페이스, Amazon S3 버킷) 또는 AWS 외부 인프라에 사용자 요청을 연결할 수 있습니다.

Amazon Route 53는 도메인 이름에 대해 나열된 IP 주소(레코드)를 관리하고 특정 도메인 이름을 해당 IP 주소로 변환하라는 요청(쿼리)에 응답합니다. 지연 시간을 최소화하기 위해 도메인에 대한 쿼리는 anycast를 사용하여 인근 DNS 서버에 자동으로 라우팅됩니다. Route 53

를 사용하면 지연 시간 기반 라우팅(LBR), 지역 DNS, 가중치 기반 라운드 로빈(WRR) 등 다양한 라우팅 유형을 통해 전 세계 트래픽을 관리할 수 있으며 모든 방식에 DNS 장애 조치를 결합하여 짧은 지연 시간과 내결함성을 달성할 수 있습니다. Amazon Route 53가 실행하는 장애 조치 알고리즘은 트래픽을 정상적인 엔드포인트로 라우팅할 뿐만 아니라 상태 확인 및 애플리케이션의 구성 오류, 엔드포인트 오버로드, 분할 오류 등으로 인해 재난 시나리오가 악화되는 것을 피하기 위해 설계되었습니다.

Route 53에서는 도메인 이름 등록도 지원하므로, 사용자는 example.com과 같은 도메인 이름을 구매하여 관리할 수 있으며 Route 53에서 도메인에 대한 기본 DNS 설정을 자동으로 구성하게 됩니다. 다양한 범위의 일반 및 국가별 TLD(최상위 도메인) 중에서 선택하여 도메인을 구입하여 관리하고 내부 및 외부로 전송할 수 있습니다. 등록 과정에서 도메인에 개인 정보 보호를 활성화할 수 있는 옵션이 있습니다. 이 옵션은 스크랩과 스팸을 차단하기 위해 퍼블릭 Whois 데이터베이스에서 대부분의 개인 정보를 숨깁니다.

Amazon Route 53는 AWS의 가용성이 높고 신뢰할 수 있는 인프라를 사용하여 개발하였습니다. AWS DNS 서버의 분산 특성 덕분에 최종 사용자는 해당 애플리케이션으로 일관되게 라우팅됩니다. Route 53는 상태 확인 및 DNS 장애 조치 기능을 제공하여 웹사이트의 가용성도 보장합니다. 정기적으로 웹 사이트(SSL을 통해서만 이용할 수 있는 보안 웹 사이트 포함) 상태를 점검하여 기본 사이트가 응답하지 않을 경우 백업 사이트로 전환하도록 Route 53를 손쉽게 구성할 수 있습니다.

모든 AWS 서비스와 마찬가지로 Amazon Route 53는 제어 API에 대한 모든 요청을 인증하여 인증받은 사용자만 Route 53에 액세스하고 관리할 수 있도록 합니다. 요청에서 계산된 HMAC-SHA1 또는 HMAC-SHA256 서명과 사용자의 AWS 보안 액세스 키를 사용하여 AWS 요청에 서명합니다. 또한, Amazon Route 53의 제어 API는 SSL로 암호화된 엔드포인트를 통해서만 액세스할 수 있습니다. Route 53는 IPv4 라우팅과 IPv6 라우팅을 모두 지원합니다.

DNS IAM을 사용하여 AWS 계정 아래에 사용자를 생성하고 이러한 사용자가 수행할 권한이 있는 Route 53 작업을 제어하는 방식으로 Amazon Route 53 DNS 관리 기능에 대한 액세스를 제어할 수 있습니다.

Amazon CloudFront 보안

Amazon CloudFront를 사용하면 짧은 지연 시간과 높은 데이터 전송 속도로 최종 사용자에게 콘텐츠를 배포할 수 있습니다. Amazon CloudFront는 엣지 로케이션의 글로벌 네트워크를 사용해 동적, 정적 및 스트리밍 콘텐츠를 전송합니다. 고객의 객체에 대한 요청이 가장 가까운 엣지 로케이션으로 자동 라우팅되므로 콘텐츠 전송 성능이 뛰어납니다. Amazon CloudFront는 Amazon S3, Amazon EC2, Elastic Load Balancing 및 Amazon Route 53와 같은 다른 AWS 서비스와 연동하도록 최적화되어 있습니다. 또한 AWS 오리진 서버는 아니지만 원본 및 최종 파일 버전을 저장하는 모든 서버와도 원활하게 연동됩니다.

Amazon CloudFront는 대상 API에 대한 모든 요청에 대해 인증을 요구하여 권한 있는 사용자만 Amazon CloudFront에서 배포하는 정보를 생성, 변경, 또는 삭제할 수 있도록 합니다. 요청 메시지는 이 요청 메시지 및 사용자의 개인 키에서 계산한 HMAC-SHA1 서명으로 서명합니다. 또한, Amazon CloudFront의 제어 API는 SSL 지원 엔드포인트를 통해서만 접근할 수 있습니다.

Amazon CloudFront의 엣지 로케이션에서는 데이터의 지속성을 보장하지 않습니다. 이 서비스는 빈번하게 요청되지 않는 객체를 엣지 로케이션에서 수시로 삭제할 수도 있습니다. Amazon CloudFront에서 제공하는 한정된 수의 객체 원본을 보유하는 Amazon CloudFront의 오리진 서버 역할을 하는 Amazon S3에서만 데이터의 지속성이 보장됩니다.
Amazon CloudFront로부터 콘텐츠를 다운로드할 수 있는 사람들을 제한하고자 할 경우, 서비스의 콘텐츠 비공개 기능을 사용하도록 설정할 수 있습니다. 이 기능은 다음 두 가지 구성 요소로 구성되어 있습니다. 첫 번째는 Amazon CloudFront 엣지 로케이션에서 인터넷의 최종 사용자에게 콘텐츠를 전달하는 방법을 제어합니다. 두 번째는 Amazon CloudFront 엣지 로케이션에서 Amazon S3에 있는 고객 소유 객체에 액세스하는 방법을 제어합니다. CloudFront는 최종 사용자의 지리적 위치를 기반으로 콘텐츠에 대한 액세스를 제한하는 지역 제한도 지원합니다.

Amazon CloudFront는 Amazon S3에 있는 고객 소유의 객체 원본 복사본에 대한 접근을 통제하기 위해 하나 이상의 "원본 액세스 ID"를 만들어 이들을 고객이 배포하는 사본과 연결할 수 있게 해줍니다. 원본 액세스 ID가 Amazon CloudFront 배포판 하나와 연결되어 있을 경우, 이 배포판은 Amazon S3에서 이 ID를 사용하여 객체를 검색하게 됩니다. 그런 다음 Amazon S3의 ACL 기능을 사용하여 원본 액세스 ID에 대한 액세스를 제한함으로써 해당 객체의 원본 복사본을 공개적으로 읽을 수 없게 할 수 있습니다.

Amazon CloudFront 엣지 로케이션에서 객체를 다운로드 할 수 있는 사용자를 제한하기 위해 이 서비스는 서명된 URL 인증 시스템을 사용합니다. 이 시스템을 사용하려면 먼저 퍼블릭-프라이빗 키 쌍을 만든 후 AWS 관리 콘솔을 통해 공개 키를 자신의 계정에 업로드합니다. 둘째, 요청 승인이 허가된 계정을 표시하기 위해 Amazon CloudFront 배포판을 구성하여 요청 승인을 위해 신뢰할 수 있는 최대 다섯 개의 AWS 계정을 제시할 수 있습니다. 셋째, Amazon CloudFront가 고객의 콘텐츠 지원 조건을 제시하는 정책 자료를 요청 수신 시 작성하는 것입니다. 이러한 정책 자료에는 요청받은 객체의 이름, 요청 날짜 및 시간, 요청하는 클라이언트의 원본 IP(또는 CIDR 범위)를 제시할 수 있습니다. 그런 다음 정책 문서의 SHA1 해시를 계산하고 프라이빗 키를 이용해 서명합니다. 마지막으로, 객체를 참조할 때 인코딩된 정책 문서와 서명을 쿼리 문자열 파라미터로 포함합니다. Amazon CloudFront가 요청을 받으면 공개 키를 사용하여 서명을 디코딩합니다. Amazon CloudFront는 유효한 정책 문서와 해당 서명을 포함한 요청만 제공합니다.

콘텐츠 비공개는 CloudFront 배포 기능 설정 시 선택해야 하는 옵션 기능입니다. 이 기능을 사용하지 않고 제공된 콘텐츠는 공개적으로 읽기 가능합니다.

Amazon CloudFront는 암호화된 연결(HTTPS)을 통해 콘텐츠를 전송하는 옵션을 제공합니다. 기본적으로 CloudFront는 HTTP와 HTTPS 프로토콜 모두를 통해 요청을 수락합니다. 하지만 모든 요청에 대해 HTTPS를 요구하거나 HTTP 요청을 HTTPS로 리디렉션하도록 CloudFront를 설정할 수도 있습니다. 일부 객체에 HTTP를 허용하지만 다른 객체에는 HTTPS를 요구하도록 CloudFront 배포를 구성할 수도 있습니다.

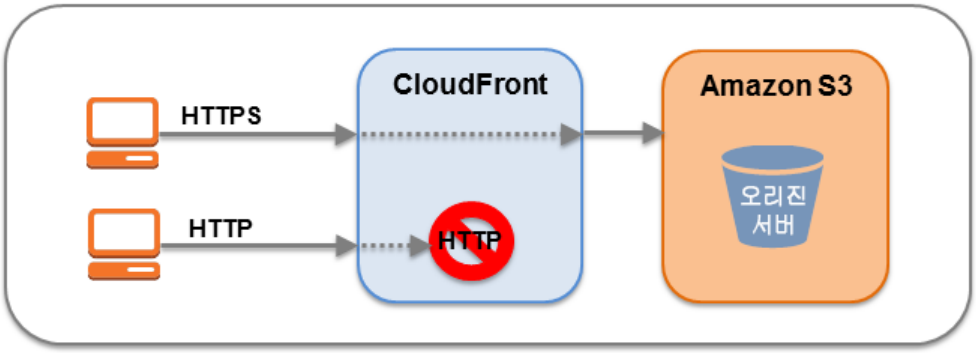

그림 7: Amazon CloudFront 암호화된 전송

오리진에서 객체를 가져올 때 최종 사용자가 객체를 요청하는 데 사용한 프로토콜을 사용할 것을 CloudFront에 요구하도록 하나 이상의 CloudFront 오리진을 구성할 수 있습니다. 예를 들면 이 CloudFront 설정을 사용하며 최종 사용자가 HTTPS를 사용하여 CloudFront에서 객체를 요청하는 경우 CloudFront에서도 HTTPS를 사용하여 해당 요청을 오리진으로 전달합니다.

Amazon CloudFront는 CloudFront와 사용자 지정 오리진 웹서버 간 HTTPS 연결에 TLSv1.1 및 TLSv1.2 프로토콜을(SSLv3 및 TLSv1.0과 함께) 지원하고, 최종 사용자와 오리진 모두에 대한 연결에 Elliptic Curve Diffie-Hellman Ephemeral(ECDHE) 프로토콜을 포함한 여러 암호 그룹을 지원합니다. ECDHE를 통해 SSL/TLS 클라이언트는 임시적이고 어디에도 저장되지 않는 세션 키를 사용하는 PFS(Perfect Forward Secrecy)를 제공할 수 있습니다. 이렇게 하면 기밀 장기 키 자체가 훼손되더라도 제3자가 무단 캡처한 데이터의 디코딩을 방지할 수 있습니다.

전용 서버를 오리진으로 사용하려는 경우와 최종 사용자와 CloudFront 사이, CloudFront와 오리진 사이에 모두 HTTPS를 사용하려는 경우, VeriSign이나 DigiCert 같이 타사 인증 기관에서 서명한 HTTP 서버에 유효한 SSL 인증서를 설치해야 합니다.

기본적으로, URL에 CloudFront 배포 도메인 이름(예: https://dxxxxx.cloudfront.net/image.jpg)을 사용하여 HTTPS를 통해 최종 사용자에게 콘텐츠를 전송할 수 있습니다. 사용자의 도메인 이름과 자체 SSL 인증서를 사용하여 HTTPS로 콘텐츠를 전송하려면 SNI 사용자 지정 SSL 또는 전용 IP 사용자 지정 SSL을 사용하면 됩니다. 서버 이름 표시(SNI) 사용자 지정 SSL 사용 시, CloudFront는 대부분의 최신 웹 브라우저에서 지원되는 TLS 프로토콜의 SNI 확장 기능을 활용합니다. 하지만 이전 브라우저가 SNI를 지원하지 않기 때문에 일부 사용자는 콘텐츠에 액세스하지 못할 수 있습니다. 전용 IP 사용자 정의 SSL 사용 시, CloudFront가 수신 요청과 적절한 SSL 인증서를 연결할 수 있도록 SSL 인증서의 각 CloudFront 엣지 로케이션에 IP 주소를 할당합니다.

Amazon CloudFront 액세스 로그에는 콘텐츠 요청에 대한 종합적인 정보(예: 요청한 객체, 요청 날짜 및 시간, 요청을 처리하는 엣지 로케이션, 클라이언트 IP 주소, 참조 페이지(referrer), 사용자 에이전트)가 포함됩니다. 액세스 로그를 사용하려면 Amazon CloudFront 배포 설정 시 로그를 저장할 Amazon S3 버킷의 이름을 지정하면 됩니다.

AWS Direct Connect 보안

AWS Direct Connect 고객은 처리량이 높은 전용 연결을 사용하여 내부 네트워크와 AWS 리전 사이에 직접 링크를 프로비저닝할 수 있습니다. 이렇게 하면 네트워크 비용이 줄고, 처리량이 개선되거나 더욱 일관된 네트워크 환경을 제공할 수 있습니다. 이 전용 연결을 구성하면 AWS 클라우드(예: Amazon EC2 및 Amazon S3)로 직접 가상 인터페이스를 생성할 수 있습니다.

AWS Direct Connect를 사용하면 네트워크 경로 내 인터넷 서비스 공급자를 우회합니다. AWS Direct Connect 위치를 수용하는 시설 내에 랙 공간을 마련하고 근처에 장비를 설치할 수 있습니다. 장비를 설치한 후에는 상호 연결 방식으로 AWS Direct Connect에 연결할 수 있습니다. 각 AWS Direct Connect 위치는 지리적으로 가장 가까운 AWS 리전으로 연결할 수 있습니다. 해당 리전에서 사용 가능한 모든 AWS 서비스에 액세스할 수 있습니다. 미국의 AWS Direct Connect 위치는 퍼블릭 가상 인터페이스를 이용해 다른 AWS 리전의 퍼블릭 엔드포인트에도 액세스할 수 있습니다.

전용 연결은 산업 표준 802.1q VLAN을 사용하여 여러 가상 인터페이스로 분할할 수 있습니다. 이렇게 하면 공용 환경과 사설 환경 간의 네트워크 분리를 유지하면서도 동일한 연결을 사용하여 공용 리소스 (예: 공개 IP 주소 공간을 사용하는 Amazon S3에 저장된 객체)뿐 아니라 개인 리소스 (예: 사설 IP 공간을 사용하는 Amazon VPC)에서 실행되고 있는 Amazon EC2 인스턴스)에도 액세스할 수 있습니다.

AWS Direct Connect에는 Border Gateway Protocol(BGP)과 자율 시스템 번호(ASN)를 사용해야 합니다. 가상 인터페이스를 생성하려면 메시지 인증에 MD5 암호화 키를 사용합니다. MD5는 비밀 키를 이용해 키가 추가된 해시를 생성합니다. AWS가 자동으로 BGP MD5 키를 생성하도록 설정하거나 직접 입력할 수 있습니다.

참고 문헌

https://aws.amazon.com/security/security-resources/

AWS 보안 프로세스 소개
AWS 보안 개요 — 스토리지 서비스
AWS 보안 개요 — 데이터베이스 서비스 개요
AWS 보안 개요 — 컴퓨팅 서비스 개요
AWS 보안 개요 — 애플리케이션 서비스
AWS 보안 개요 — 분석, 모바일 및 애플리케이션 서비스
AWS 보안 개요 — 네트워크 서비스

부록 — 용어

액세스 키 ID: 각 AWS 사용자를 고유하게 식별하기 위해 AWS가 배포하는 문자열입니다. 이 문자열은 보안 액세스 키와 연결된 영숫자 토큰입니다.

ACL(액세스 제어 목록): 객체나 네트워크 리소스에 액세스하기 위한 권한 또는 규칙의 목록입니다. Amazon EC2에서 보안 그룹은 인스턴스 수준에서 ACL로 작용하여 어떤 사용자가 특정 인스턴스에 액세스할 권한이 있는지를 제어합니다. Amazon S3에서는 ACL을 사용하여 사용자 그룹에게 버킷이나 객체에 대한 읽기 또는 쓰기 액세스 권한을 부여할 수 있습니다. Amazon VPC에서 ACL은 네트워크 방화벽과 같이 작용하며 서브넷 수준에서 액세스를 제어합니다.

AMI: Amazon 머신 이미지(AMI)는 Amazon S3에 저장된 암호화된 머신 이미지입니다. 여기에는 고객 소프트웨어의 인스턴스를 부팅하는 데 필요한 모든 정보가 들어 있습니다.

API: 애플리케이션 프로그래밍 인터페이스(API)는 컴퓨터 공학 분야의 인터페이스로서 애플리케이션 프로그램이 서비스 라이브러리 및/또는 운영 체제에서 서비스를 요청하는 방식을 정의합니다.

아카이브: Amazon Glacier의 아카이브는 저장해야 하는 파일이며 Amazon Glacier 내 스토리지의 기본 단위입니다. 아카이브는 사진, 동영상 또는 문서 등의 데이터일 수 있습니다. 각 아카이브는 고유 ID가 있으며 선택 사항으로 설명을 추가할 수 있습니다.

인증: 인증이란 어떠한 사람이 주장하는 개체 또는 무엇에 부합하는지에 대한 여부를 판단하는 과정입니다. 사용자를 인증해야 할 뿐 아니라, AWS API에서 공개하는 기능을 호출하려는 모든 프로그램을 인증해야 합니다. AWS에서는 암호화 해시 함수를 사용하여 디지털 방식으로 서명하는 방식으로 모든 요청을 인증해야 합니다.

Auto Scaling: 고객이 직접 정의하는 조건에 따라 Amazon EC2 용량을 자동으로 상향 및 하향 조정할 수 있는 AWS 서비스입니다.

가용 영역: Amazon EC2는 리전과 가용 영역 내 위치합니다. 가용 영역은 다른 가용 영역에 장애가 발생할 경우 분리되도록 설계된 개별적인 지점으로, 동일 리전 내의 다른 가용 영역에 저렴하고, 지연 시간이 짧은 네트워크 연결을 제공합니다.

배스천 호스트: 공격을 견딜 수 있도록 특별히 구성된 컴퓨터입니다. 일반적으로 완충 영역(DMZ)의 외부 영역이나 공개 영역 또는 방화벽 외부에 배치됩니다. 퍼블릭 서브넷을 Amazon VPC의 일부로 설정하여 Amazon EC2 인스턴스를 SSH 배스천 호스트로 설정할 수 있습니다.

버킷: Amazon S3에 저장된 객체에 대한 컨테이너입니다. 모든 객체는 하나의 버킷에 들어갑니다. 예를 들어, photos/puppy.jpg로 명명된 객체는 johnsmith 버킷에 저장되며, 다음 URL을 사용하여 주소를 지정할 수 있습니다. http://johnsmith.s3.amazonaws.com/photos/puppy.jpg.

인증서: 일부 AWS 제품에서 AWS 계정과 사용자를 인증하기 위해 사용하는 자격 증명입니다. X.509 인증서라고도 합니다. 인증서는 프라이빗 키와 연결됩니다.

CIDR 블록: IP 주소의 클래스 없는 도메인 간 라우팅 블록입니다.

클라이언트측 암호화: Amazon S3에 데이터를 업로드하기 전에 클라이언트 측에서 데이터를 암호화하는 작업입니다.

CloudFormation: 애플리케이션을 실행하는 데 필요한 AWS 리소스의 기준 구성을 기록하여 이러한 리소스를 순서에 따라 예측 가능한 방식으로 프로비저닝하고 업데이트할 수 있는 AWS 프로비저닝 도구입니다.

Cognito: 사용자 인증 및 여러 디바이스, 플랫폼, 애플리케이션에 걸쳐 이루어지는 데이터 저장, 관리, 동기화 작업을 간소화하는 AWS 서비스입니다. 여러 기존 ID 공급자와 호환되며, 인증되지 않은 게스트 사용자도 지원합니다.

자격 증명: 사용자나 프로세스가 서비스에 액세스하기 위해 권한을 부여 받는 인증 프로세스 중에 AWS 서비스를 확인하기 위해 가지고 있어야 하는 항목입니다. AWS 자격 증명에는 암호, 보안 액세스 키 및
X.509 인증서, 다중 요소 토큰이 포함됩니다.

전용 인스턴스: 호스트 하드웨어 수준에서 물리적으로 격리된 Amazon EC2 인스턴스입니다. 이들 인스턴스는 단일 테넌트 하드웨어에서 실행됩니다.

디지털 서명: 디지털 서명은 디지털 메시지 또는 문서의 신뢰성을 증명하기 위한 암호화 방법입니다. 유효한 디지털 서명은 권한 있는 발신자가 메시지를 작성했으며 전송 중에 메시지가 변경되지 않았음을 확신할 수 있는 이유를 수신자에게 제공합니다. 디지털 서명은 고객이 인증 프로세스의 일부로서 AWS API에 대한 요청에 서명하기 위해 사용합니다.

Direct Connect 서비스: 처리량이 높은 전용 연결을 사용하여 내부 네트워크와 AWS 리전 간에 직접 링크를 프로비저닝할 수 있는 Amazon 서비스입니다. 이 전용 연결을 구성하면 네트워크 경로에서 인터넷 서비스 공급자를 우회하여 AWS 클라우드(예: Amazon EC2 및 Amazon S3)와 Amazon VPC로 직접 논리적 연결을 생성할 수 있습니다.

DynamoDB 서비스: 원활한 확장성과 함께 빠르고 예측 가능한 성능을 제공하는 AWS의 완전 관리형 NoSQL 데이터베이스 서비스입니다.

EBS: Amazon Elastic Block Store(EBS)는 Amazon EC2 인스턴스와 함께 사용할 블록 수준의 스토리지 볼륨을 제공합니다. Amazon EBS 볼륨은 인스턴스 수명에 관계없는 영구적인 오프 인스턴스 스토리지입니다.

ElastiCache: 클라우드상의 분산 인 메모리 캐시 환경을 설정 및 관리하고 확장할 수 있는 AWS 웹 서비스입니다. 이 서비스는 더 느린 디스크 기반 데이터베이스에 전적으로 의존하기보다는, 신속하며 관리되는 인 메모리 캐싱 시스템에서 정보를 검색할 수 있는 기능을 지원해 웹 애플리케이션의 성능을 향상시킵니다.

Elastic Beanstalk: 고객 애플리케이션에 대한 용량 프로비저닝, 로드 밸런싱 및 Auto Scaling 기능을 자동화하는 AWS 배포 및 관리 도구입니다.

탄력적 IP 주소: Amazon VPC의 인스턴스에 할당하여 인스턴스를 퍼블릭으로 만들 수 있는 고정 퍼블릭 IP 주소입니다. 또한 탄력적 IP 주소를 사용하면 퍼블릭 IP 주소를 VPC의 모든 인스턴스에 신속하게 다시 매핑하여 인스턴스 장애를 숨길 수 있습니다.

Elastic Load Balancing: 전체 Amazon EC2 인스턴스에서 트래픽을 관리하여 인스턴스에 대한 트래픽을 한 리전 내의 모든 가용 영역에 분산하는 데 사용되는 AWS 서비스입니다. Elastic Load Balancing은 온프레미스 로드 밸런서의 모든 장점 외에도, EC2 인스턴스에서 암호화/해독 작업을 인계하여 로드 밸런서에서 중심적으로 관리하는 등의 여러 가지 보안 이점도 갖추고 있습니다.

Elastic MapReduce(EMR) 서비스: 호스팅되는 하둡 프레임워크를 사용하는 AWS 서비스입니다. 하둡 프레임워크는 Amazon EC2와 Amazon S3의 웹 스케일 인프라 상에서 실행됩니다. Elastic MapReduce를 사용하면 대량의 데이터("빅 데이터")를 쉽고도 경제적으로 처리할 수 있습니다.

Elastic Network Interface: Amazon VPC 내에서 Elastic Network Interface는 EC2 인스턴스에 연결할 수 있는 선택적인 두 번째 네트워크 인터페이스입니다. Elastic Network Interface는 Amazon VPC에서 관리 네트워크를 생성하거나 네트워크 또는 보안 어플라이언스를 사용하는 데 유용할 수 있습니다. 이 인터페이스는 인스턴스에서 쉽게 분리하여 다른 인스턴스에 연결할 수 있습니다.

Endpoint: AWS 서비스의 진입점인 URL입니다. 애플리케이션에서의 데이터 지연 시간을 줄일 수 있도록 대부분의 AWS 서비스에서 요청을 작성할 리전 엔드포인트를 선택할 수 있습니다. 일부 웹 서비스에서는 리전을 지정하지 않는 일반 엔드포인트를 사용할 수 있지만, 이러한 일반 엔드포인트는 서비스의 us-east-1 엔드포인트로 확인됩니다. SSL을 사용하는 HTTP 또는 보안 HTTP(HTTPS)를 통해 AWS 엔드포인트에 연결할 수 있습니다.

연동 사용자: 현재 AWS 서비스에 액세스할 권한이 없지만 임시로 액세스 권한을 제공하고자 하는 사용자, 시스템 또는 애플리케이션입니다. 이러한 액세스는 AWS 보안 토큰 서비스(STS) API를 사용하여 제공됩니다.

방화벽: 특정 규칙 세트에 따라 들어오거나 나가는 네트워크 트래픽을 제어하는 하드웨어 또는 소프트웨어 구성 요소입니다. Amazon EC2에서는 방화벽 규칙을 사용하여 인스턴스에 접속할 수 있는 프로토콜, 포트 및 소스 IP 주소 범위를 지정합니다. 이러한 규칙은 수신되는 어떤 네트워크 트래픽을 해당 인스턴스에 전달해야 하는지를 지정합니다(예: 포트 80에서 웹 트래픽 수락). Amazon VPC는 인스턴스의 수신 및 발신 트래픽을 모두 필터링할 수 있는 완벽한 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.

게스트 OS: 가상 머신 환경에서는 단일 하드웨어에서 여러 운영 체제를 실행할 수 있습니다. 이러한 각 인스턴스는 호스트 하드웨어에서 게스트로 간주되며 고유의 OS를 사용합니다.

Hash: 암호화 해시 함수는 AWS API에 대한 요청에 서명하기 위해 디지털 서명을 계산하는 데 사용됩니다. 암호화 해시는 입력을 기반으로 고유의 해시 값을 반환하는 단방향 함수입니다. 해시 함수에 대한 입력에는 요청 텍스트와 보안 액세스 키가 포함됩니다. 해시 함수는 요청에 서명으로 포함하는 해시 값을 반환합니다.

HMAC-SHA1/HMAC-SHA256: 암호화에서 키 해시 메시지 인증 코드(HMAC 또는 KHMAC)는 보안 키와 조합하여 암호화 해시 함수를 포함한 특정 알고리즘을 사용하여 계산되는 일종의 메시지 인증 코드(MAC)입니다. 모든 MAC과 마찬가지로, 동시에 데이터 무결성 및 메시지의 진위를 확인하는 데 사용할 수 있습니다. SHA-1 또는 SHA-256와 같은 반복 암호화 해시 함수가 HMAC 계산에 사용될 수 있으며, 따라서 결과적인 MAC 알고리즘을 HMAC-SHA1 또는 HMAC-SHA256라고 합니다. HMAC의 암호화 강도는 기본 해시 함수의 암호화 강도, 키의 크기와 품질 및 비트 단위 해시 출력 길이에 따라 다릅니다.

하드웨어 보안 모듈(HSM): HSM은 변조 방지 하드웨어 디바이스 내에 보안 암호 키 스토리지와 작업을 제공하는 어플라이언스입니다. HSM은 암호화 키 자료를 안전하게 보관하고 어플라이언스의 암호화 경계 외부에 노출하지 않고 키 자료를 사용하도록 설계되었습니다. AWS CloudHSM 서비스는 HSM 어플라이언스에 대한 전용 단일 테넌트 액세스 권한을 고객에게 제공합니다.

하이퍼바이저: VMM(Virtual Machine Manager)이라고도 하며, 호스트 컴퓨터에서 여러 운영 체제를 동시에 실행할 수 있는 컴퓨터 소프트웨어/하드웨어 플랫폼 가상화 소프트웨어입니다.

Identity and Access Management(IAM): AWS IAM을 이용하면 본인의 AWS 계정을 이용하여 여러 사용자를 생성하고, 각 사용자의 권한을 관리할 수 있습니다.

ID 풀: 해당 AWS 계정에 고유한 Amazon Cognito 내 사용자 ID 정보 스토어입니다. ID 풀은 IAM 역할을 사용하는데 이는 특정 IAM 사용자나 그룹에 연결되지 않고 임시 보안 자격 증명을 이용해 해당 역할에 정의된 AWS 리소스에 대해 인증하는 권한을 뜻합니다.

ID 공급자: 이 서비스나 다른 협력 서비스와 상호 작용하기를 원하는 사용자에게 ID 정보를 발급하는 온라인 서비스입니다. ID 공급자의 예로는 Facebook, Google, Amazon 등이 있습니다.

Import/Export 서비스: 이동식 스토리지 디바이스를 안전한 AWS 시설로 물리적으로 전달하여 대용량의 데이터를 Amazon S3 또는 EBS 스토리지로 전송하는 AWS 서비스입니다.

인스턴스: 인스턴스는 자체 하드웨어 리소스와 게스트 OS를 사용하는 가상 서버이며 가상 머신(VM)이라고도 합니다. EC2에서 인스턴스는 Amazon 머신 이미지(AMI) 사본을 실행 중인 인스턴스를 나타냅니다.

IP 주소: 인터넷 프로토콜(IP) 주소는 숫자로 구성되며, 해당 노드 간 통신에 인터넷 프로토콜을 활용하여 컴퓨터 네트워크에 참여하는 장치에 할당됩니다.

IP 스푸핑: 위조된 소스 IP 주소를 사용하여 IP 패킷을 생성하는 것을 스푸핑이라고 하며, 발신자의 신원을 감추거나 다른 컴퓨팅 시스템을 가장하려는 목적으로 사용됩니다.

키: 암호화에서 키는 암호화 알고리즘(해싱 알고리즘)의 출력을 결정하는 파라미터입니다. 키 페어는 사용자의 신원을 전자적으로 증명하는 데 사용하는 보안 자격 증명으로, 퍼블릭 키와 프라이빗 키로 구성됩니다.

키 교체: 데이터를 암호화하거나 요청에 디지털로 서명하는 데 사용되는 암호화 키를 주기적으로 변경하는 프로세스입니다. 암호 변경과 마찬가지로 키를 교체하면 침입자가 키를 획득하거나 키 값을 결정한 경우에 무단 액세스 위험을 최소화할 수 있습니다. AWS는 여러 개의 동시 액세스 키와 인증서를 지원하므로, 고객이 작업 중이나 작업 후에 애플리케이션을 중지하지 않고 키와 인증서를 정기적으로 교체할 수 있습니다.

Mobile Analytics: 모바일 애플리케이션 사용량 데이터를 수집, 시각화, 분석하는 AWS 서비스입니다. 이를 통해 고객 행동을 추적하고 측정치를 집계하고 모바일 애플리케이션에서 의미 있는 패턴을 식별할 수 있습니다.

멀티 팩터 인증(MFA): 두 개 이상의 인증 팩터를 사용합니다. 인증 팩터에는 사용자가 알고 있는 요소(예: 암호) 또는 사용자가 가지고 있는 요소(예: 난수를 생성하는 토큰)가 있습니다. AWS IAM에서는 사용자 이름과 암호 자격 증명 외에 6자리의 일회용 코드를 사용할 수 있습니다. 고객은 물리적으로 소유하고 있는 인증 디바이스(물리적 토큰 디바이스 또는 스마트폰의 가상 토큰)에서 이 일회용 코드를 가져옵니다.

네트워크 ACL: Amazon VPC 내 서브넷에서 인바운드 또는 아웃바운드하는 모든 트래픽에 적용되는 상태 비저장 트래픽 필터입니다. 네트워크 ACL은 IP 프로토콜, 서비스 포트, 원본/대상 IP 주소에 따라 트래픽을 허용 또는 거부하는 정렬된 규칙도 포함할 수 있습니다.

객체: Amazon S3에 저장되는 기본 개체입니다. 객체는 객체 데이터와 메타데이터로 구성됩니다. 이 데이터 부분은 Amazon S3에서 볼 수 없습니다. 메타데이터는 객체를 설명하는 이름-값 페어의 집합입니다. 여기에는 마지막으로 수정한 날짜와 같은 몇 가지 기본 메타데이터 및 콘텐츠 형식과 같은 표준 HTTP 메타데이터가 포함됩니다. 개발자는 또한 객체를 저장할 때 사용자 정의 메타데이터를 지정할 수도 있습니다.

반가상화: 컴퓨팅에서 반가상화는 기본 하드웨어의 경우와 비슷하지만 동일하지는 않은 가상 머신에 소프트웨어 인터페이스를 제공하는 가상화 기술입니다.

피어링: VPC 피어링 연결은 프라이빗 IP 주소를 사용하여 두 VPC 간에 트래픽을 라우팅할 수 있도록 하기 위한 두 VPC 사이의 네트워킹 연결입니다. 동일한 네트워크에 속하는 경우와 같이 VPC의 인스턴스가 서로 통신할 수 있습니다.

포트 스캐닝: 포트 스캔은 컴퓨터에 침입하려는 누군가가 보낸 일련의 메시지로서, 어떤 컴퓨터 네트워크가 사용되는지, 각 네트워크가 컴퓨터가 제공하는 '잘 알려진' 포트 번호에 연결되어 있는지를 확인하기 위해 사용됩니다.

리전: 동일한 지리적 영역에 있는 명명된 AWS 리소스 집합입니다. 각 리전에는 두 개 이상의 가용 영역이 있습니다.

복제: 일반적으로 재해 복구를 위해 데이터베이스의 두 번째 버전을 유지하기 위해 데이터베이스에서 데이터를 지속적으로 복사합니다. 고객은 Amazon RDS 데이터베이스 복제를 위해 여러 AZ를 사용할 수 있으며, MySQL을 사용할 경우 읽기 전용 복제본을 사용할 수 있습니다.

Relational Database Service(RDS): 관계형 데이터베이스(DB) 인스턴스를 신속하게 만들고, 애플리케이션 요구에 맞춰 관련 컴퓨팅 리소스 및 스토리지 용량을 유연하게 확장할 수 있도록 해주는 AWS 서비스입니다. Amazon RDS는 Amazon Aurora, MySQL, PostgreSQL, Oracle, Microsoft SQL Server, MariaDB 데이터베이스 엔진에 사용할 수 있습니다.

역할: 다른 엔터티가 가정할 수 있는 일련의 권한을 보유한 AWS IAM의 엔터티입니다. 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에서 AWS 서비스 리소스에 안전하게 액세스할 수 있도록 활성화할 수 있습니다. 역할에 특정 권한을 부여하고, 역할을 사용하여 Amazon EC2 인스턴스를 시작하고, EC2를 통해 Amazon EC2에서 실행되는 애플리케이션에 대한 AWS 자격 증명 관리를 자동으로 처리할 수 있습니다.

Route 53: 컴퓨터 간에 서로 통신할 수 있도록 DNS 쿼리에 응답하고 도메인 이름을 IP 주소로 변환하여 개발자가 퍼블릭 DNS 이름을 관리하는 데 사용할 수 있는 업데이트 메커니즘을 제공하는 신뢰할 수 있는 DNS 시스템입니다.

보안 액세스 키: AWS 계정에 가입할 때 AWS에서 할당하는 키입니다. API를 호출하거나 명령줄 인터페이스를 사용하기 위해 각 AWS 사용자는 보안 액세스 키와 액세스 키 ID가 있어야 합니다. 사용자는 보안 액세스 키로 각 요청에 서명하고 액세스 키 ID를 요청에 포함합니다. AWS 계정의 보안을 보장하기 위해 보안 액세스 키는 키 및 사용자 생성 중에만 액세스할 수 있습니다. 키를 다시 액세스하려면 안전하게 보관된 텍스트 파일 등에 키를 저장해야 합니다.

보안 그룹: 보안 그룹을 통해 Amazon EC2 인스턴스를 접속하도록 허용된 프로토콜, 포트 및 소스 IP 주소 범위를 제어할 수 있습니다. 즉, 보안 그룹은 인스턴스에 대한 방화벽 규칙을 정의합니다. 이러한 규칙은 수신되는 어떤 네트워크 트래픽을 해당 인스턴스에 전달해야 하는지를 지정합니다(예: 포트 80에서 웹 트래픽 수락).

보안 토큰 서비스(STS): AWS STS API는 보안 토큰, 액세스 키 ID 및 보안 액세스 키로 구성된 임시 보안 자격 증명을 반환합니다. STS를 사용하여 리소스에 임시로 액세스해야 하는 사용자에게 보안 자격 증명을 발급할 수 있습니다. 이러한 사용자는 기존 IAM 사용자, 비 AWS 사용자(연동 ID), 시스템, AWS 리소스에 액세스해야 하는 애플리케이션 등이 될 수 있습니다.

서버 측 암호화(SSE): 유휴 데이터를 자동으로 암호화하는 Amazon S3 스토리지 옵션입니다. Amazon S3 SSE를 사용하면 고객이 객체를 기록할 때 별도의 요청 헤더를 추가하는 것만으로 업로드 시 데이터를 암호화할 수 있습니다. 암호 해독은 데이터를 검색할 때 자동으로 이루어집니다.

서비스: 네트워크에서 제공되는 소프트웨어 또는 컴퓨팅 기능(예: Amazon EC2, Amazon S3)입니다.

샤드: Amazon Kinesis에서 샤드는 Amazon Kinesis stream에서 고유하게 식별된 데이터 레코드 그룹입니다. Kinesis 스트림은 각각 고정된 용량 단위를 제공하는 여러 개의 샤드로 구성됩니다.

Signature: 수학적인 방식으로 디지털 메시지의 신뢰성을 확인하는 디지털 서명을 의미합니다. AWS는 암호화 알고리즘과 프라이빗 키로 계산된 서명을 사용하여 고객이 AWS 웹 서비스로 보낸 요청을 인증합니다.

Simple Data Base(Simple DB): AWS 고객이 웹 서비스 요청을 통해 데이터 항목을 저장 및 쿼리할 수 있도록 해주는 비관계형 데이터 스토리지입니다. Amazon SimpleDB는 여러 지역에 분산된 고객의 데이터 복제본을 자동으로 생성 및 관리하여 높은 가용성과 데이터 내구성을 확보합니다.

Simple Email Service(SES): 비즈니스와 개발자에게 확장 가능한 대량 및 트랜잭션 이메일 전송 서비스를 제공하는 AWS 서비스입니다. 발신자의 발송률과 신뢰성을 극대화하기 위해 Amazon SES는 의심스러운 콘텐츠가 발송되지 않도록 차단하는 조치를 사전 예방적으로 수행하며 이에 따라 ISP는 해당 서비스를 신뢰할 수 있는 이메일 오리진으로 간주합니다.

Simple Mail Transfer Protocol(SMTP): IP 네트워크를 통해 이메일을 전송하기 위한 인터넷 표준인 SMTP가 Amazon Simple Email Service에서 사용됩니다. Amazon SES를 사용하는 고객은 SMTP 인터페이스를 사용하여 이메일을 보낼 수 있지만, TLS를 통해 SMTP 엔드포인트에 연결해야 합니다.

Simple Notification Service(SNS): 클라우드에서 알림을 쉽게 설정, 운영, 전송할 수 있도록 지원하는 AWS 서비스입니다. Amazon SNS는 애플리케이션에서 메시지를 게시하고 즉시 이를 구독자 또는 다른 애플리케이션으로 전달할 수 있는 기능을 개발자에게 제공합니다.

Simple Queue Service(SQS): 애플리케이션의 분산된 구성 요소 간에 비동기 메시지 기반 통신을 가능하게 해주는 AWS의 확장 가능한 메시지 대기열 서비스입니다. 이 구성 요소는 컴퓨터 또는 Amazon EC2 인스턴스이거나 이 두 가지가 결합된 형태일 수 있습니다.

Simple Storage Service(Amazon S3): 객체 파일에 대한 보안 스토리지를 제공하는 AWS 서비스입니다. 파일 또는 버킷 수준에서 객체에 대한 액세스를 제어하고 요청 IP 소스, 요청 시간 등과 같은 다른 조건을 기반으로 액세스를 세부적으로 제한할 수 있습니다. 또한 AES-256 암호화를 사용하여 파일을 자동으로 암호화할 수 있습니다.

Simple Workflow Service(SWF): 분산된 구성 요소에 대해 작업을 조정하는 애플리케이션을 구축할 수 있는 AWS 서비스입니다. 개발자는 Amazon SWF를 이용해 애플리케이션에서 다양한 처리 단계를 태스크"로 구조화하여 분산 애플리케이션에서 작업을 실행할 수 있습니다. Amazon SWF는 개발자의 애플리케이션 논리에 따라 작업 실행 종속성, 일정 및 동시성을 관리하여 이러한 작업을 조정합니다.

Single Sign-On: 한 번의 로그인으로 여러 애플리케이션 및 시스템에 액세스할 수 있는 기능입니다. 임시 보안 자격 증명을 AWS 관리 콘솔에 전달하는 URL을 생성하여 연동 사용자(AWS 사용자 및 비 AWS 사용자)에게 보안 Single Sign-On 기능을 제공할 수 있습니다.

스냅샷: Amazon S3에 저장되는 EBS 볼륨에 대해 고객이 실행한 백업 또는 Amazon RDS에 저장되는 RDS 데이터베이스에 대해 고객이 실행한 백업입니다. 스냅샷을 새 EBS 볼륨 또는 Amazon RDS 데이터베이스에 대한 시작점으로 사용하거나 장기 내구성 및 복구를 위해 데이터를 보호하는 데 사용할 수 있습니다.

Secure Sockets Layer(SSL): 애플리케이션 계층에서 인터넷을 통해 보호하는 암호화 프로토콜입니다. TLS 1.0 프로토콜 사양과 SSL 3.0 프로토콜 사양은 모두 암호화 메커니즘을 사용하여 보안 TCP/IP 연결을 설정하여 유지 관리하는 보안 서비스를 구현합니다. 보안 연결은 염탐, 훼손 또는 메시지 위조를 방지합니다. SSL을 사용하는 HTTP 또는 보안 HTTP(HTTPS)를 통해 AWS 엔드포인트에 연결할 수 있습니다.

상태 저장 방화벽: 컴퓨팅에서, 상태 저장 방화벽(상태 저장 패킷 검사(SPI) 또는 상태 저장 검사를 수행하는 모든 방화벽)은 네트워크 연결(예: TCP 스트림, UDP 통신) 상태를 추적하는 방화벽입니다.

Storage Gateway: VMware ESXi Hypervisor를 실행하는 데이터 센터의 호스트에 배포한 VM을 사용하여 고객의 온프레미스 소프트웨어 어플라이언스를 Amazon S3 스토리지에 안전하게 연결하는 AWS 서비스입니다. 데이터는 SSL을 통해 고객의 온프레미스 스토리지 하드웨어에서 AWS로 비동기적으로 전송된 다음 Amazon S3에서 AES-256을 사용하여 암호화된 상태로 저장됩니다.

임시 보안 자격 증명: AWS 서비스에 대한 임시 액세스 권한을 제공하는 AWS 자격 증명입니다. 임시 보안 자격 증명을 사용하여 고객의 자격 증명 및 권한 부여 시스템 내 AWS 서비스와 비 AWS 사용자 간 자격 증명 연동을 제공할 수 있습니다. 임시 보안 자격 증명은 보안 토큰, 액세스 키 ID 및 보안 액세스 키로 구성됩니다.

Transcoder: 미디어 파일(오디오 또는 비디오)의 형식, 크기 또는 품질을 트랜스코딩(변환)하는 시스템입니다. Amazon Elastic Transcoder를 사용하면 확장 가능하고 비용 효과적인 방식으로 손쉽게 비디오 파일을 트랜스코딩할 수 있습니다.

TLS(전송 계층 보안): 애플리케이션 계층에서 인터넷을 통해 보호하는 암호화 프로토콜입니다. Amazon Simple Email Service를 사용하는 고객은 TLS를 통해 SMTP 엔드포인트에 연결해야 합니다.

트리 해시: 트리 해시는 메가바이트 크기의 각 데이터 세그먼트에 대한 해시를 계산한 뒤 데이터의 인접 세그먼트가 증가하는 것을 나타내는 트리 방식으로 해시를 결합해 생성됩니다. Amazon Glacier는 해시가 중간에 바뀌지 않았는지 확인하기 위해 데이터와 비교 검사합니다.

볼트: Amazon Glacier에서 볼트는 아카이브 보관용 컨테이너입니다. 볼트를 만들려면 이름을 지정하고 볼트를 생성할 AWS 리전을 선택해야 합니다. 각 볼트 리소스에는 고유한 주소가 있습니다.

버전 관리: Amazon S3의 모든 객체에는 키와 버전 ID가 있습니다. 키는 동일하지만 버전 ID가 다른 객체를 동일한 버킷에 저장할 수 있습니다. 버전 관리는 버킷 계층에서 PUT 버킷 버전 관리를 통해 활성화됩니다.

가상 인스턴스: AMI를 실행하고 나면, 결과 실행 시스템이 인스턴스로 참조됩니다. 같은 AMI를 갖는 모든 인스턴스는 동일하게 시작되며, 인스턴스가 종료되거나 장애가 발생하는 경우 인스턴스의 모든 정보는 손실됩니다.

가상 MFA: 사용자가 토큰/fob가 아닌 스마트폰에서 6자리의 일회용 MFA 코드를 가져올 수 있도록 해주는 기능입니다. MFA는 인증을 위해 사용자 이름 및 암호화 함께 추가적인 단계(일회용 코드)를 사용합니다.

Virtual Private Cloud(VPC): IP 주소 범위 선택, 서브넷 정의, 라우팅 테이블 및 네트워크 게이트웨이 구성을 비롯하여 고객이 AWS 클라우드의 격리된 영역을 프로비저닝하는 데 사용하는 AWS 서비스입니다.

가상 프라이빗 네트워크(VPN): 인터넷과 같은 퍼블릭 네트워크를 통해 두 위치 간에 프라이빗 보안 네트워크를 생성하는 기능입니다. AWS 고객은 Amazon VPC와 데이터 센터 사이에 IPsec VPN 연결을 추가하여 데이터 센터를 클라우드까지 효과적으로 확장하는 한편 Amazon VPC의 퍼블릭 서브넷 인스턴스에 직접 인터넷 액세스를 제공합니다. 이 구성에서는 고객이 기업 데이터 센터 측에 VPN 어플라이언스를 추가할 수 있습니다.

WorkSpaces: 사용자를 위해 클라우드 기반 데스크톱을 프로비저닝하고, 사용자가 고유한 자격 증명이나 일반적인 Active Directory 자격 증명을 이용해 로그인하도록 허용하는 AWS 관리형 데스크톱 서비스입니다.

X.509: 암호화 기법에서 X.509는 Single Sign-On을 위한 퍼블릭 키 인프라(PKI) 및 권한 관리 인프라(PMI)에 대한 표준입니다. X.509는 퍼블릭 키 인증서, 인증서 해지 목록, 속성 인증서 및 인증 경로 유효성 검사 알고리즘에 대한 표준 형식을 지정합니다. 일부 AWS 제품은 보안 액세스 키 대신 X.509 인증서를 사용하여 특정 인터페이스에 액세스합니다. 예를 들어 Amazon EC2는 보안 액세스 키를 사용하여 쿼리 인터페이스에 액세스하지만, SOAP 인터페이스와 명령줄 인터페이스에 액세스하는 데에는 서명 인증서를 사용합니다.

WorkDocs: 사용자 협업을 위한 피드백 기능을 갖춘 AWS 관리형 엔터프라이즈 스토리지 및 공유 서비스입니다.

문서 수정

2016년 6월

- 규정 준수 프로그램 업데이트
- 리전 업데이트

2014년 11월

- 규정 준수 프로그램 업데이트
- 책임 분담 보안 모델 업데이트
- AWS 계정 보안 기능 업데이트
- 서비스 카테고리 재구성
- 여러 서비스에 다음 기능 업데이트: CloudWatch, CloudTrail, CloudFront, EBS, ElastiCache, Redshift, Route 53, S3, Trusted Advisor, WorkSpaces
- Cognito 보안 추가
- Mobile Analytics 보안 추가
- WorkDocs 보안 추가

2013년 11월

- 리전 업데이트
- 여러 서비스에 다음 기능 업데이트: CloudFront, DirectConnect, DynamoDB, EBS, ELB, EMR, Amazon Glacier, IAM, OpsWorks, RDS, Redshift, Route 53, Storage Gateway, VPC
- AppStream 보안 추가
- CloudTrail 보안 추가
- Kinesis 보안 추가
- WorkSpaces 보안 추가

2013년 5월

- 역할과 API 액세스를 포함하도록 IAM 업데이트
- 고객이 지정한 권한 있는 작업에 대한 API 액세스를 위해 MFA 업데이트
- SQL Server 2012에 이벤트 알림, 멀티 AZ 및 SSL을 추가하도록 RDS 업데이트
- 기본적으로 여러 IP 주소, 고정 라우팅 VPN 및 VPC를 추가하도록 VPC 업데이트
- 여러 다른 서비스에 다음 기능 업데이트: CloudFront, CloudWatch, EBS, ElastiCache, Elastic Beanstalk, Route 53, S3, Storage Gateway
- Glacier 보안 추가
- RedShift 보안 추가
- Data Pipeline 보안 추가
- Transcoder 보안 추가
- Trusted Advisor 보안 추가
- OpsWorks 보안 추가
- CloudHSM 보안 추가