Amazon Web Services: 보안 프로세스의 개요

2013년 11월

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

목차

책임 공유 환경 6

AWS 인프라 보안 6

AWS 규정 준수 프로그램 6

물리적 및 환경적 보안 7

화재 감지 및 진압 7

전력 7

기후 및 온도 7

관리 7

스토리지 디바이스 폐기 8

비즈니스 연속성 관리 8

가용성 8

인시던트 대응 8

전사적 경영진의 검토 8

통신 8

네트워크 보안 9

보안 네트워크 아키텍처 9

보안 액세스 포인트 9

전송 보호 9

Amazon 사내 분리 10

내결함성 설계 10

네트워크 모니터링 및 보안 11

AWS 액세스 13

계정 검토 및 감사 13

배경 조회 13
자격 증명 정책 13
보안 설계의 원칙 14
변경 관리 14
소프트웨어 14
인프라 15
AWS 계정 보안 기능 15
AWS Identity and Access Management(AWS IAM) 15
임시 보안 자격 증명 16
역할 16
AWS Multi-Factor Authentication(AWS MFA) 17
키 관리 및 교체 17
AWS Trusted Advisor 보안 검사 17
AWS 서비스별 보안 18
Amazon Elastic Compute Cloud(Amazon EC2) 보안 18
여러 단계의 보안기법 18
하이퍼바이저 18
인스턴스 격리 18
Elastic Block Storage(Amazon EBS) 보안 21
Amazon Elastic Load Balancing 보안 22
Auto Scaling 보안 22
Amazon Virtual Private Cloud(Amazon VPC) 보안 23
EC2-VPC 를 통한 추가 네트워크 액세스 제어 26
Amazon Direct Connect 보안 28
Amazon Simple Storage Service(Amazon S3) 보안 28

데이터 액세스 28
데이터 전송 29
데이터 저장 29
데이터 내구성 및 신뢰성 30
액세스 로그 30
CORS(Cross-Origin Resource Sharing) 30
AWS Glacier 보안 30
데이터 업로드 31
데이터 검색 31
데이터 저장 31
데이터 액세스 32
AWS Storage Gateway 보안 32
AWS Import/Export 보안 33
AWS Data Pipeline 34
Amazon Simple Database(SimpleDB) 보안 34
Amazon DynamoDB 보안 35
Amazon Relational Database Service(Amazon RDS) 보안 36
액세스 제어 36
네트워크 격리 36
암호화 37
자동 백업 및 DB 스냅샷 38
복제 38
자동 소프트웨어 패치 38
이벤트 알림 39
Amazon RedShift 보안 39

클러스터 액세스 39
데이터 백업 40
데이터 암호화 40
자동 소프트웨어 패치 40
SSL 연결 41
Amazon ElastiCache 보안 41
Amazon Simple Queue Service(Amazon SQS) 보안 42
Amazon Simple Notification Service(Amazon SNS) 보안 42
Amazon Simple Workflow Service(Amazon SWF) 보안 43
Amazon Simple Email Service(Amazon SES) 보안 43
Amazon Elastic Transcoder 서비스 보안 45
Amazon CloudWatch 보안 46
Amazon CloudFront 보안 46
Amazon Elastic MapReduce(Amazon EMR) 보안 48
Amazon Route 53 보안 48
Amazon CloudSearch 보안 49
AWS Elastic Beanstalk 보안 50
AWS CloudFormation 보안 51
AWS OpsWorks 보안 51
AWS CloudHSM 보안 53
부록 – 용어 54

Amazon Web Services(AWS)는 높은 가용성과 신뢰성을 갖춘 확장 가능한 클라우드 컴퓨팅 플랫폼을 제공하며, 이를 통해 고객들이 다양한 애플리케이션을 구축할 수 있도록 유연성을 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 공유 환경

IT 인프라를 AWS로 이전할 경우 고객과 AWS 간에 책임 공유 모델이 만들어집니다. 이 공유 모델을 통해 고객은 운영 부담을 덜 수 있습니다. AWS가 호스트 운영 체제 및 가상화 계층에서 서비스 운영 시설의 물리적 보안에 이르기까지 구성 요소를 운영, 관리, 제어하기 때문입니다. 고객은 게스트 운영 체제(업데이트 및 보안 패치 포함) 및 기타 관련 애플리케이션 소프트웨어에 대한 책임과 관리, AWS가 제공하는 보안 그룹 방화벽의 구성을 담당합니다. 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.

AWS 인프라 보안

AWS는 고객이 처리 및 스토리지와 같은 다양한 기본적 컴퓨팅 리소스를 프로비저닝하는 데 사용하는 클라우드 인프라를 운영합니다. AWS 인프라에는 시설, 네트워크 및 하드웨어, 그리고 이러한 리소스의 프로비저닝 및 사용을 지원하는 일부 운영 소프트웨어(예: 호스트 OS, 가상화 소프트웨어 등)가 포함됩니다. AWS 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

AWS 규정 준수 프로그램은 고객이 강력한 보안을 이해할 수 있도록 지원한 뒤 보안 및 데이터 보호에 대한 업계와 정부의 요구 사항에 맞춰 규정 준수를 능률화할 수 있도록 돕습니다. AWS가 고객에게 제공하는 IT 인프라는 다음과 같은 다양한 IT 보안 표준과 보안 모범 사례에 맞게 설계 및 관리됩니다.

- SOC 1/SSAE 16/ISAE 3402(이전 명칭 SAS 70 Type II)
- SOC 2
- SOC 3
- FISMA, DIACAP 및 FedRAMP
- PCI DSS 레벨 1
- ISO 27001
- ITAR
- FIPS 140-2

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

- HIPAA
- Cloud Security Alliance(CSA)
- Motion Picture Association of America(MPAA)

AWS는 백서, 보고서, 자격증, 승인 및 기타 타사 증명을 통해, IT 제어 환경에 관한 광범위한 정보를 고객에게 제공합니다. 자세한 정보는 웹 사이트(http://aws.amazon.com/security)에서 제공되는 위험 및 규정 준수 백서를 참조하십시오.

물리적 및 환경적 보안

AWS의 데이터 센터는 혁신적인 아키텍처 및 엔지니어링 접근 방식을 활용하는 최첨단 센터입니다. Amazon은 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. 인력 및 시스템은 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 디바이스 폐기

스토리지 디바이스의 수명이 다했을 경우 권한이 없는 개인에게 고객 데이터가 노출되는 것을 방지하기 위해 고안된 폐기 프로세스가 AWS 내에 마련되어 있습니다. AWS는 DoD 5220.22-M("국가 산업 보안 프로그램 운영 매뉴얼") 또는 NIST 800-88("미디어 삭제 가이드라인")에서 설명하는 기술을 사용해 폐기 프로세스에 따라 데이터를 제거합니다. 모든 폐기된 마그네틱 스토리지 디바이스는 업계 표준 관행에 따라서 자기 소거되고 물리적으로 파쇄됩니다.

비즈니스 연속성 관리

Amazon의 인프라는 높은 수준의 가용성을 제공하며, 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 최근 AWS 서비스 복구 계획을 검토한 바 있습니다. 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. 이 방법에는 신입 사원을 위한 오리엔테이션 및 교육 프로그램, 사업 성과 및 기타 사항을 알리기 위한 정기적인 임원 회의, 전자 수단(화상 회의, 이메일 메시지 및 Amazon 인트라넷에 정보 게시 등)도 포함됩니다.

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. "보안 및 규정 준수 센터"를 제공하여 고객이 AWS에 관한 보안 및 규정 준수 세부 정보를 단일 위치에서 제공받을 수 있습니다. 또한 고객은 AWS Support 서비스에 가입하여 고객 지원 팀에 직접 문의하거나 고객에게 영향을 미치는 모든 문제를 사전에 통보받을 수 있습니다.

네트워크 보안

AWS 네트워크는 고객이 자신의 워크로드에 적합한 수준의 보안과 복원성을 선택할 수 있도록 구축되었습니다. 클라우드 리소스와 함께 지리적으로 분산되고 내결함성이 있는 아키텍처를 구성하기 위해 AWS는 신중한 모니터링과 관리를 거치는 세계 최고의 네트워크 인프라를 구현했습니다.

보안 네트워크 아키텍처

방화벽 및 기타 경계 장치를 포함한 네트워크 디바이스가 네트워크의 외부 경계 및 주요 내부 경계에서 통신을 모니터링하고 제어합니다. 이러한 경계 디바이스는 규칙 세트, ACL(액세스 제어 목록) 및 구성을 사용하여 특정 정보 시스템 서비스에 대한 정보 흐름을 적용합니다.

각 관리형 인터페이스에 대해 트래픽 흐름을 관리 및 적용하는 ACL, 즉 트래픽 흐름 정책이 수립됩니다. ACL 정책은 Amazon Information Security에서 승인합니다. 이들 정책은 AWS의 ACL 관리 도구를 사용하여 자동으로 푸시되므로 이러한 관리형 인터페이스가 가장 최신의 ACL을 적용할 수 있습니다.

보안 액세스 포인트

AWS는 인바운드/아웃바운드 통신 및 네트워크 트래픽을 보다 포괄적으로 모니터링하기 위해 클라우드에 대한 제한된 수의 액세스 포인트를 전략적으로 배치하고 있습니다. API 엔드포인트라고 부르는 이러한 고객 액세스 포인트는 고객이 AWS 내에서 스토리지와 보안 통신 세션을 구축하고 인스턴스를 컴퓨팅할 수 있는 보안 HTTP 액세스(HTTPS)를 허용합니다. 고객이 FIPS 140-2 요건을 충족할 수 있도록 AWS GovCloud(US)의 Amazon Virtual Private Cloud VPN 엔드포인트와 SSL-terminating 로드 밸런서는 FIPS 140-2 Level 2 검증 하드웨어를 이용하여 작동합니다.

또한 AWS는 인터넷 서비스 공급자(ISP)와의 인터페이스 통신을 관리하는 전용으로 사용되는 네트워크 디바이스를 구현했습니다. AWS는 AWS 네트워크의 각 인터넷 경계 엣지에서 복수의 통신 서비스에 대한 중복 연결을 사용합니다. 각 연결에는 전용 네트워크 디바이스가 있습니다.

전송 보호

고객은 염탐, 훼손 및 메시지 위조를 방지하도록 설계된 암호화 프로토콜인 Secure Sockets Layer(SSL)를 사용하는 HTTP 또는 HTTPS를 통해 AWS 액세스 포인트에 연결할 수 있습니다.

네트워크 보안의 추가 계층을 필요로 하는 고객을 위해 AWS는 AWS 클라우드 내에서 프라이빗 서브넷을 제공하고, Amazon Virtual Private Cloud(VPC)와 데이터 센터 간에 암호화된 터널을 제공하기 위해 IPsec VPN(가상 프라이빗 네트워크) 디바이스를 사용할 수 있는 방법을 제시합니다. VPC 구성 옵션에 대한 자세한 정보는 아래의 Amazon Virtual Private Cloud(VPC) 보안 섹션을 참조하십시오.

Amazon 사내 분리

논리적으로, AWS 프로덕션 네트워크는 일련의 복잡한 네트워크 보안/분리 디바이스를 통해 Amazon 사내 네트워크와 분리되어 있습니다. 관리 목적으로 AWS 클라우드 구성 요소에 액세스해야 하는 AWS 사내 네트워크 개발자 및 관리자는 AWS 티켓 시스템을 통해 명시적으로 액세스 권한을 요청해야 합니다. 모든 요청은 해당 서비스 소유자의 검토와 승인을 거칩니다.

그러면 승인된 AWS 직원이 네트워크 디바이스 및 기타 클라우드 구성 요소에 대한 액세스를 제한하고 보안 리뷰를 위해 모든 활동을 로깅하는 배스천 호스트를 통해 AWS 네트워크에 연결하고 모든 작업이 보안 합니다. 배스천 호스트에 액세스하려면 호스트의 모든 사용자 계정에 대해 SSH 퍼블릭 키 인증이 필요합니다. AWS 개발자 및 관리자 논리적 액세스에 대한 자세한 정보는 아래의 *AWS 액세스*를 참조하십시오.

내결함성 설계

Amazon의 인프라는 높은 수준의 가용성을 제공하며, 고객에게 탄력적인 IT 아키텍처를 구현할 수 있는 역량을 제공합니다. AWS는 시스템 또는 하드웨어 장애가 고객에게 미치는 영향을 최소화하도록 시스템을 설계했습니다.

데이터 센터는 전 세계 여러 *리전*에 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 발전기를 사용하여 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 시나리오에 직면한 경우에도 시스템을 유지할 수 있게 합니다. 단, EU 데이터 개인 정보 보호 지침과 같은 위치별 개인 정보 보호 및 규정 준수 요건을 주의해야 합니다. 데이터는 사용자가 원하지 않는 한 리전 간에는 복제되지 않습니다. 따라서 이러한 유형의 데이터 배치 및 개인 정보 보호 요구 조건을 갖춘 고객은 규제 요건에 부합하는 환경을 마련할 수 있는 것입니다. 리전 간 통신은 모두 퍼블릭 인터넷 인프라를 통해 이루어집니다. 따라서 중요한 데이터를 보호하기 위해 적절한 암호화 방법을 사용해야 합니다.

이 문서의 작성일 현재, 미국 동부(버지니아 북부), 미국 서부(오레곤), 미국 서부(캘리포니아 북부), AWS GovCloud(오레곤), EU(아일랜드), 아시아 태평양(싱가포르), 아시아 태평양(도쿄), 아시아 태평양(시드니), 남아메리카(상파울루)의 9개 리전이 있습니다.

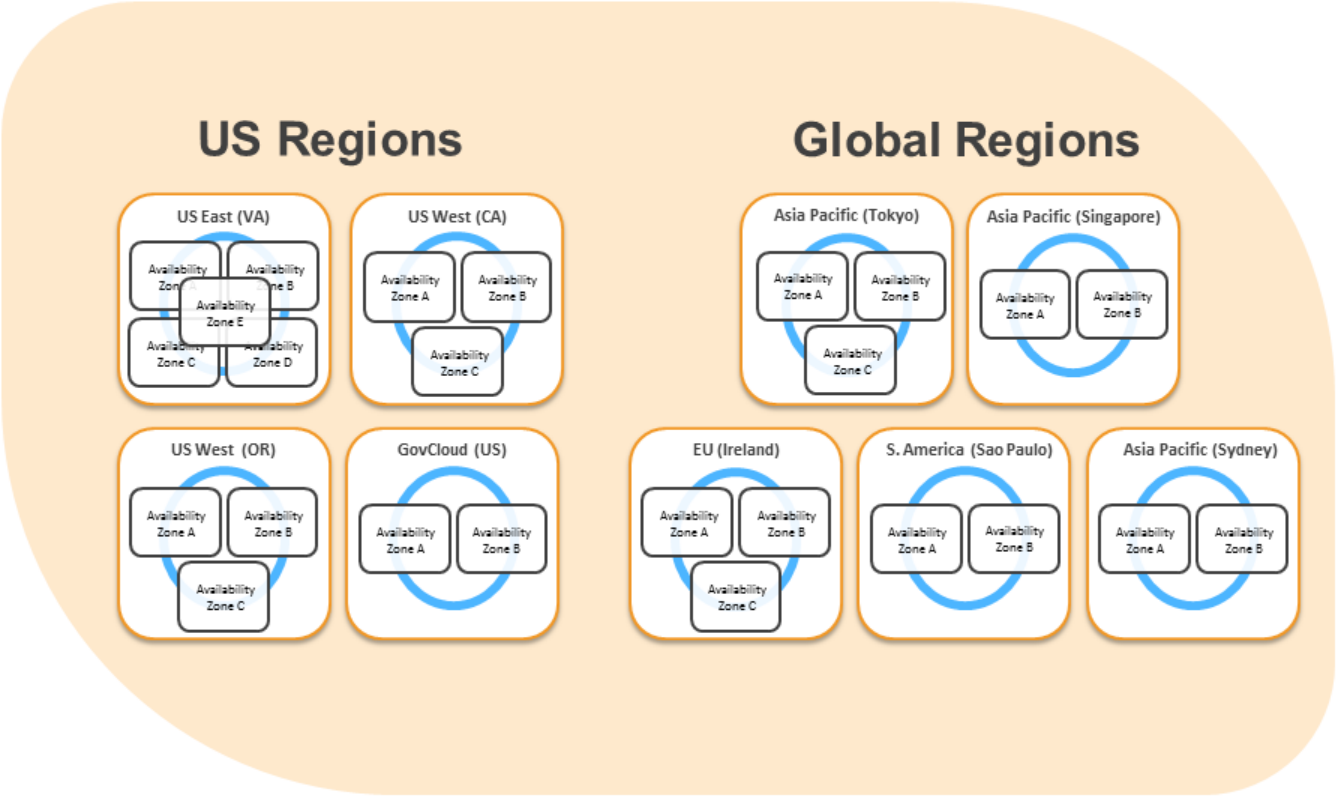


그림 1: 리전 및 가용 영역

가용 영역 수는 변경될 수 있습니다.

AWS GovCloud(미국)는 미국 정부 또는 미국 정부 기능/서비스와 직간접적으로 연결되는 미국 기업으로 제한된 AWS의 정부 커뮤니티 클라우드입니다. AWS GovCloud(미국) 리전은 미국 정부의 ITAR 규정을 충족하는 정부 및 상용 워크로드를 위한 전용 CONUS 기반 리전을 제공합니다. GovCloud 리전을 사용하는 AWS 고객은 미국 국적의 AWS 직원만 그 구성 요소를 관리하므로 안심할 수 있습니다. GovCloud는 ITAR만을 위한 것이 아닙니다. 이 리전은 미국 수출통제 제한이 적용되는 상용 IT 시스템을 포함하여 모든 CUI(Controlled Unclassified Information) 워크로드를 지원합니다. CUI 범주에는 농업, 저작권, 중요 인프라, 수출통제(ITAR), 재무, 이민, 인텔리전스, 법집행, 법률, 핵, 특허, 개인정보보호, 전매(IP), 통계, 세금 및 운송이 포함됩니다(EO 13556에 따름, http://www.archives.gov/cui/ 참조). GovCloud 리전은 다른 리전과 동일하게 2개 가용 영역을 포함하는 내결함성 설계를 제공하며 FIPS 140-2 준수 액세스 포인트를 제공합니다. 또한 모든 GovCloud 계정은 기본적으로 AWS Virtual Private Cloud(VPC) 서비스를 사용하여 AWS 클라우드의 격리된 부분을 생성하고 프라이빗(RFC 1918) 주소를 갖는 Amazon EC2 인스턴스를 시작합니다. GovCloud에 대한 자세한 정보는 AWS 웹 사이트(http://aws.amazon.com/govcloud-us/)를 참조하십시오.

네트워크 모니터링 및 보안

AWS는 높은 수준의 서비스 성능 및 가용성을 제공하기 위해 여러 가지 자동화된 모니터링 시스템을 활용합니다. AWS 모니터링 도구는 인바운드 및 아웃바운드 통신 지점에서 비정상적이거나 승인되지 않은 활동 및 조건을 감지하도록 설계되어 있습니다. 이러한 도구는 서버 및 네트워크 사용, 포트 스캐닝 활동, 애플리케이션 사용 및 승인되지 않은 침입 시도를 모니터링합니다. 도구에는 비정상적 활동에 대해 사용자 지정 성능 지표 임계값을 설정하는 기능이 있습니다.

AWS 내 시스템은 주요 운영 측정치를 모니터링하기 위해 광범위하게 활용됩니다. 주요 운영 측정치가 초기 경고 임계값을 초과하는 경우 운영 담당자에게 자동으로 통보하도록 경보가 구성되어 있습니다. 담당자가 항상 운영 문제에 대응할 수 있도록 대기 일정을 구성합니다. 무선 호출 시스템을 통해 경보가 신속하고 안정적으로 운영 담당자에게 전달되도록 합니다.

인시던트 또는 문제를 처리하는 운영 담당자에게 도움이 되는 정보를 제공할 수 있도록 설명서를 유지 관리합니다. 문제 해결에 협업이 필요할 경우, 커뮤니케이션 및 로깅 기능을 지원하는 회의 시스템이 사용됩니다. 협업을 필요로 하는 운영 문제를 처리하는 동안 숙련된 회의 진행자가 커뮤니케이션 및 진행을 용이하게 합니다. 사후 평가는 외부 영향에 관계없이 모든 중요 운영 문제 해결 후 수행하며, 근본 원인을 파악하고 차후 예방 조치를 취할 수 있도록 오류 원인(COE) 분석 문서의 초안을 작성합니다. 주간 운영 회의에서 예방 조치의 진행 현황을 검토합니다.

AWS 보안 모니터링 도구는 분산, 폭주 및 소프트웨어/논리적 공격을 포함한 다양한 유형의 서비스 거부(DoS) 공격에 대한 탐지를 도와줍니다. DoS 공격이 식별되면 AWS 사고 대응 프로세스가 개시됩니다. DoS 방지 도구 이외에, 각 리전의 중복 통신 사업자와 추가 용량이 DoS 공격 가능성으로부터 보호합니다.

AWS 네트워크는 기존의 네트워크 보안 문제와 관련하여 중요한 보호 방법을 제공합니다. 고객은 추가 보호 방법을 실행할 수도 있습니다. 다음은 몇 가지 예입니다.

- **DDoS(분산 서비스 거부) 공격.** AWS API 엔드포인트는 엔지니어링 분야 전문 지식을 바탕으로 Amazon을 세계 최대의 온라인 소매업체로 발전시킨 세계적인 수준의 인터넷 기반 대규모 인프라에서 호스팅합니다. 독점적인 DDoS 완화 기법이 사용됩니다. 또한, AWS의 네트워크는 다양한 인터넷 접근 방법을 제공하기 위해 여러 공급자들을 통해 멀티 홈 방식으로 제공됩니다.
- **MITM(중간자) 공격.** 모든 AWS API는 SSL을 보호하는 endpoint를 통해 서버 인증을 제공합니다. Amazon EC2 AMI는 최초 부팅 시 새 SSH 호스트 인증서를 자동으로 생성하고 해당 인스턴스 관련 콘솔에 기록합니다. 그러면 고객은 보안 API를 사용하여 이 콘솔을 호출하고 호스트 인증서에 액세스한 다음 최초로 이 인스턴스에 로그인할 수 있습니다. AWS와의 모든 상호 작용에서 SSL을 사용할 것을 권장합니다.
- **IP 스푸핑.** Amazon EC2 인스턴스는 스푸핑된 네트워크 트래픽을 전송할 수 없습니다. AWS가 제어하는 호스트 기반의 방화벽 인프라는 인스턴스 자체의 원본 IP 또는 MAC 주소를 사용하지 않는 경우 트래픽 전송을 허용하지 않습니다.
- **포트 스캐닝**. Amazon EC2 고객의 무단 포트 스캔은 AWS 이용 방침을 위반하는 것입니다. AWS 이용 방침 위반은 심각한 사안이며 모든 위반 사안 보고에 대해 조사하도록 되어 있습니다. 고객은 Amazon 웹 사이트(http://aws.amazon.com/contact-us/report-abuse/)에 제공되는 연락처를 통해 의심되는 침해 사례를 신고할 수 있습니다. AWS에서 무단 포트 스캐닝을 탐지하는 경우 스캐닝이 중단 및 차단됩니다. 일반적으로 Amazon EC2 인스턴스의 포트 스캔은 효과가 없습니다. 기본적으로 Amazon EC2 인스턴스의 모든 인바운드 포트는 폐쇄되어 있고 고객에게만 액세스가 허용되기 때문입니다. 고객은 보안 그룹을 엄격하게 관리하여 포트 스캔의 위협을 더욱 완화할 수 있습니다. 고객이 어떠한 소스에서 특정 포트로 트래픽을 허용하도록 보안 그룹을 구성하는 경우 해당 특정 포트는 포트 스캔에 취약해집니다. 이러한 경우 고객은 자신의 애플리케이션에 꼭 필요할 수 있는 청취 서비스가 무단 포트 스캔에 의해 발견되지 않도록 보호하기 위해 적절한 보안 조치를 사용해야 합니다. 예를 들어, 웹 서버는 명확하게 포트 80(HTTP)을 개방해야 합니다. 이 서버의 관리자는 Apache와 같은 HTTP 서버 소프트웨어의 보안을 책임집니다. 고객은 특정 규정 준수 요구 사항을 충족하기 위해 필요에 따라 취약성을 스캔할 수 있는 권한을 요청할 수 있습니다. 이러한 스캔은 고객의 자체 인스턴스로 제한되어야 하며 AWS의 이용 정책을 위반하지 않아야 합니다. 이러한 유형의 스캔에 대한 고급 승인은 요청서를 웹 사이트(https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest)를 통해 제출함으로써 시작할 수 있습니다.

- **다른 테넌트에 의한 패킷 스니핑.** 무차별 모드에서 실행되는 가상 인스턴스가 다른 가상 인스턴스를 위한 트래픽을 수신하거나 "스니프"하는 것은 불가능합니다. 고객은 인터페이스를 무차별 모드로 운영할 수는 있지만 하이퍼바이저는 고객에게 보내는 트래픽이 아닌 경우 고객에게 전달하지 않습니다. 같은 물리적 호스트에 있으며 소유자가 같은 두 가상 인스턴스는 서로 상대방의 트래픽을 수신할 수 없습니다. ARP 캐시 중독과 같은 공격은 Amazon EC2 및 Amazon VPC 내에서 작동하지 않습니다. Amazon EC2는 실수로 또는 악의적으로 다른 사람의 데이터를 볼 수 없도록 충분히 보호하지만 표준 관행에 따라 민감한 트래픽을 암호화해야 합니다.

모니터링뿐 아니라 다양한 도구를 사용하여 AWS 환경의 호스트 운영 체제, 웹 애플리케이션, 데이터베이스에 대해 정기적으로 취약성 검사를 수행합니다. 또한 AWS 보안 팀은 관련 공급업체 결함에 대한 뉴스 피드를 구독하고 새로운 패치를 확인하기 위해 공급업체의 웹 사이트 및 타 관련 매체를 사전에 모니터링합니다. AWS 고객은 AWS 취약성 보고 웹 사이트(http://aws.amazon.com/security/vulnerability-reporting/)를 통해 AWS에 문제를 보고할 수도 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 설계 검토, 위협 모델링 및 일체의 리스크 평가 등 최선의 보안 소프트웨어 개발 모범 사례를 따릅니다. 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(http://status.aws.amazon.com/) 또는 이메일을 통해 고객에게 이를 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. 생산 환경에 적용되는 변경사항은 아래와 같습니다.

- 검토: 변경의 기술적 측면에 대해 동료가 검토함 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 건전성 여부를 측정하기 위해 여러 개의 설정 가능한 메트릭을 갖추고 있습니다. 이 메트릭을 임계치와 경보로 자세히 모니터링합니다. 롤백 절차는 변경 관리(CM) 티켓에 설명되어 있습니다.

가능한 경우, 일상적인 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 Amazon은 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 고객이 자신의 신원을 확인하고 안전하게 자신의 AWS 계정에 액세스할 수 있는 여러 가지 방법을 제공합니다. AWS에서 지원하는 자격 증명의 전체 목록은 나의 계정의 보안 자격 증명 페이지에서 찾을 수 있습니다. 또한 AWS는 AWS Identity and Access Management(IAM), 키 관리 및 교체, 임시 보안 자격 증명, Multi-Factor Authentication(MFA)과 같이 AWS 계정을 추가로 보호하고 액세스를 제어할 수 있는 보안 옵션을 추가로 제공합니다.

AWS Identity and Access Management(AWS IAM)

AWS IAM을 사용하면 AWS 계정 내에서 여러 사용자를 생성하고, 이러한 사용자 각각의 권한을 관리할 수 있습니다. 사용자란 AWS 서비스에 액세스하는 데 사용할 수 있는 고유한 보안 자격 증명을 포함하는 일종의 AWS 계정 ID입니다. AWS IAM을 사용하면 암호나 액세스 키를 공유할 필요가 없으며 상황에 따라 사용자의 액세스 권한을 쉽게 활성화하거나 비활성화할 수 있습니다.

AWS IAM을 사용하면 보안 모범 사례를 구현할 수 있습니다. 예를 들어, 고객의 AWS 계정 내에 있는 모든 사용자에게 고유의 자격 증명을 부여하여 사용자에게 작업을 수행하는 데 필요한 AWS 서비스 및 리소스에 대한 액세스 권한만 주는 것입니다. AWS IAM에는 보안이 기본값으로 설정되어 있습니다. 신규 사용자는 구체적으로 권한이 부여되기 전까지 AWS에 접근할 수 없습니다.

AWS IAM은 AWS Marketplace와도 통합되어, 고객의 조직 내에서 누가 Marketplace에서 제공하는 소프트웨어 및 서비스를 구독할 수 있는지 제어할 수 있습니다. Marketplace에서 특정 소프트웨어를 구독하면 EC2 인스턴스가 시작하여 해당 소프트웨어를 실행하므로 이것은 중요한 액세스 제어 기능입니다. AWS IAM을 사용하여 AWS Marketplace 액세스를 제어하면 AWS 계정 소유자가 사용 및 소프트웨어 비용을 세부적으로 제어할 수 있습니다.

AWS IAM은 고객의 AWS 계정 자격 증명 사용 횟수를 최소화해줍니다. AWS IAM 사용자 계정을 만든 후에는 AWS 서비스 및 리소스와의 모든 상호 작용이 AWS IAM 사용자 보안 자격 증명을 사용해 이루어져야 합니다. AWS IAM에 대한 자세한 정보는 AWS 웹 사이트(http://aws.amazon.com/iam/)를 참조하십시오.

임시 보안 자격 증명

AWS IAM을 사용하면 제한된 시간 동안만 유효한 보안 자격 증명을 통해 보안 AWS 리소스에 대한 임시 액세스를 사용자에게 제공할 수 있습니다. 이러한 자격 증명은 유효 기간이 짧다는 점(기본 만료 시간이 12시간)과 만료 후 재사용이 불가능하다는 점 때문에 향상된 보안을 제공합니다. 이는 특정 상황에서 제어 가능한 제한적 액세스 권한을 제공하는 데 특히 유용합니다.

- **연동(비 AWS) 사용자 액세스.** 연동 사용자는 AWS 계정을 보유하지 않은 사용자(또는 애플리케이션)입니다. 고객은 임시 보안 자격 증명을 통해 연동 사용자에게 제한된 시간 동안 AWS 리소스에 대한 액세스 권한을 부여할 수 있습니다. 이는 고객에게 Microsoft Active Directory, LDAP 또는 Kerberos와 같은 외부 서비스를 사용하여 인증할 수 있는 비 AWS 사용자가 있을 경우 유용합니다. 임시 AWS 자격 증명은 고객의 사내 자격 증명 및 권한 부여 시스템 내 비 AWS 사용자와 AWS 간 자격 증명 연동을 제공합니다.
- **Single Sign-On.** 고객은 연동 사용자에게 AWS에 로그인하도록 요구할 필요가 없이 사내 자격 증명 및 권한 부여 시스템을 통해 AWS Management Console에 대한 Single-Sign-On(SSO) 액세스를 제공할 수 있습니다. Single-Sign-On(SSO) 액세스를 제공하기 위해 고객은 임시 보안 자격 증명을 AWS Management Console로 전달하는 URL을 만듭니다. 이 URL은 생성 후 15분간만 유효합니다.

임시 자격 증명은 보안 토큰, 액세스 키 ID 및 보안 액세스 키를 포함합니다. 특정 리소스에 대한 사용자 액세스를 제공하기 위해 고객은 임시 액세스 권한을 제공하려는 사용자에게 임시 보안 자격 증명을 배포합니다. 사용자는 리소스를 호출할 때 토큰 및 액세스 키 ID를 전달하고 보안 액세스 키를 사용하여 요청에 서명합니다. 이 토큰은 다른 액세스 키에서는 작동하지 않습니다. 사용자가 토큰을 전달하는 방식은 API 그리고 사용자가 호출하는 AWS 제품의 버전에 따라 다릅니다. 임시 보안 자격 증명에 대한 자세한 정보는 AWS 웹 사이트(http://docs.amazonwebservices.com/STS)를 참조하십시오.

임시 자격 증명의 사용은 추가 보호를 의미합니다. 임시 사용자에게 장기 자격 증명을 배포 또는 관리할 필요가 없기 때문입니다. 또한 임시 자격 증명은 대상 인스턴스에 자동으로 로드되므로 코드와 같이 어딘가 안전하지 않은 위치에 자격 증명을 포함할 필요가 없습니다. 임시 자격 증명은 작업하지 않아도 자동으로 하루에 여러 번 교체 또는 변경되며 기본적으로 안전하게 저장됩니다.

역할

*역할*이라고 하는 AWS IAM 기능은 임시 보안 자격 증명을 사용하여 고객이 일반적으로 조직의 AWS 리소스에 대한 액세스 권한이 없는 사용자 또는 서비스에게 액세스 권한을 위임할 수 있게 해줍니다. 역할이란 특정 AWS 리소스에 액세스하기 위한 권한 집합이지만 이러한 권한은 특정 IAM 사용자에만 한정되지 않습니다. 권한이 부여된 엔티티(예: 모바일 사용자, EC2 인스턴스)는 역할을 부여받고 역할에서 정의된 리소스에 대해 인증받기 위한 임시 보안 자격 증명을 수신합니다. 역할을 사용하면 대량의 인스턴스 또는 AWS Auto Scaling을 사용하여 탄력적으로 조정되는 집합을 관리하는 고객이 시간을 상당히 절약할 수 있습니다. EC2 인스턴스에서 키를 자동으로 프로비저닝하기 위한 IAM 역할 사용에 대한 자세한 정보는 AWS 웹 사이트(http://docs.amazonwebservices.com/IAM)에서 *Using IAM* 가이드를 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.

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 사이트(http://aws.amazon.com/ko/iam/details/mfa/)를 참조하십시오.

키 관리 및 교체

암호를 자주 변경하는 것이 중요한 것과 마찬가지로, AWS는 액세스 키와 인증서를 정기적으로 교체할 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 API 계정뿐 아니라 AWS IAM을 이용해 AWS 계정에 만든 사용자에 대해서도 액세스 키를 교체할 수 있게 해줍니다.

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, S3 버킷에 대해 퍼블릭 액세스를 허용하는 경우 또는 루트 AWS 계정에서 MFA를 사용하지 않는 경우가 포함됩니다. AWS Trusted Advisor 서비스는 기업 또는 엔터프라이즈 수준의 AWS Support에 등록한 AWS 고객에게 제공됩니다.

AWS 서비스별 보안

보안이 AWS 인프라 모든 계층뿐만 아니라 해당 인프라에서 제공되는 각 서비스에도 기본적으로 제공됩니다. AWS 서비스는 모든 AWS 네트워크 및 플랫폼과 효율적으로 안전하게 작동하도록 구축되었습니다. 각 서비스는 고객이 중요한 데이터와 애플리케이션을 보호할 수 있도록 광범위한 보안 기능을 제공합니다.

Amazon Elastic Compute Cloud(Amazon EC2) 보안

Elastic Compute Cloud(EC2)는 Amazon의 IaaS(서비스로서의 인프라)로서 AWS 데이터 센터의 서버 인스턴스를 사용하여 규모를 조정할 수 있는 컴퓨팅 용량을 제공합니다. Amazon EC2는 고객이 간편하게 필요한 용량을 얻고 구성함으로써 보다 손쉽게 웹 규모의 컴퓨팅을 할 수 있도록 설계되었습니다. 고객은 플랫폼 하드웨어 및 소프트웨어 모음인 *인스턴스*를 만들고 실행합니다.

여러 단계의 보안기법

Amazon EC2의 보안은 호스트 플랫폼의 OS(운영 체제), 가상 인스턴스 OS 또는 게스트 OS, 방화벽 및 서명된 API 호출 등 여러 수준에서 제공됩니다. 각 항목은 다른 항목의 기능 위에 구축되어 있습니다. 목표는 Amazon EC2에 포함된 데이터를 무단 시스템이나 사용자가 가로채지 못하도록 데이터를 보호하고, 고객이 요구하는 구성 유연성을 희생하지 않고도 가능한 한 안전한 Amazon EC2 인스턴스를 제공하는 것입니다.

하이퍼바이저

Amazon EC2는 현재 고도로 맞춤화된 버전의 Xen 하이퍼바이저를 이용하며 Linux 게스트의 경우는 반가상화(paravirtualization)를 활용합니다. 반가상화된 게스트는 일반적으로 액세스 권한을 요구하는 작업을 지원할 때 하이퍼바이저를 이용하기 때문에, 게스트 OS는 CPU에 대한 고급 액세스 권한이 없습니다. CPU는 *링이라고 하는 0-3 단계의 별도 권한 모드를 제공합니다.* 링 0이 가장 높은 권한이며 3은 가장 낮습니다. 호스트 OS는 링 0에서 실행됩니다. 그러나 게스트 OS는 대부분의 운영 체제와 마찬가지로 링 0에서 실행되지 않고 더 낮은 권한의 링 1에서 실행되며, 애플리케이션은 최소 권한을 갖는 링 3에서 실행됩니다. 이와 같이 물리적 자원을 구체적으로 가상화하여 게스트와 하이퍼바이저를 명확히 구분함으로써 이들 사이에 추가적인 보안 격리가 가능하게 합니다.

인스턴스 격리

동일한 물리적 장비에서 실행되는 서로 다른 인스턴스는 Xen 하이퍼바이저를 통해 상호 격리됩니다. Amazon은 최신 개발 동향에 대한 이해를 돕기 위해 Xen 커뮤니티에서 적극적으로 활동하고 있습니다. 또한, AWS 방화벽은 물리적 네트워크 인터페이스와 인스턴스의 가상 인터페이스의 중간인 하이퍼바이저 계층 내에 존재합니다. 모든 패킷은 이 계층을 통과해야 하며, 따라서, 어떤 인스턴스에 이웃해 있는 다른 인스턴스가 인터넷에 있는 다른 호스트와 마찬가지로 이 인스턴스에 접근할 수 없고 마치 별도의 물리적 호스트에 있는 것처럼 처리될 수 있습니다. 물리적 RAM도 비슷한 방식으로 구분됩니다.

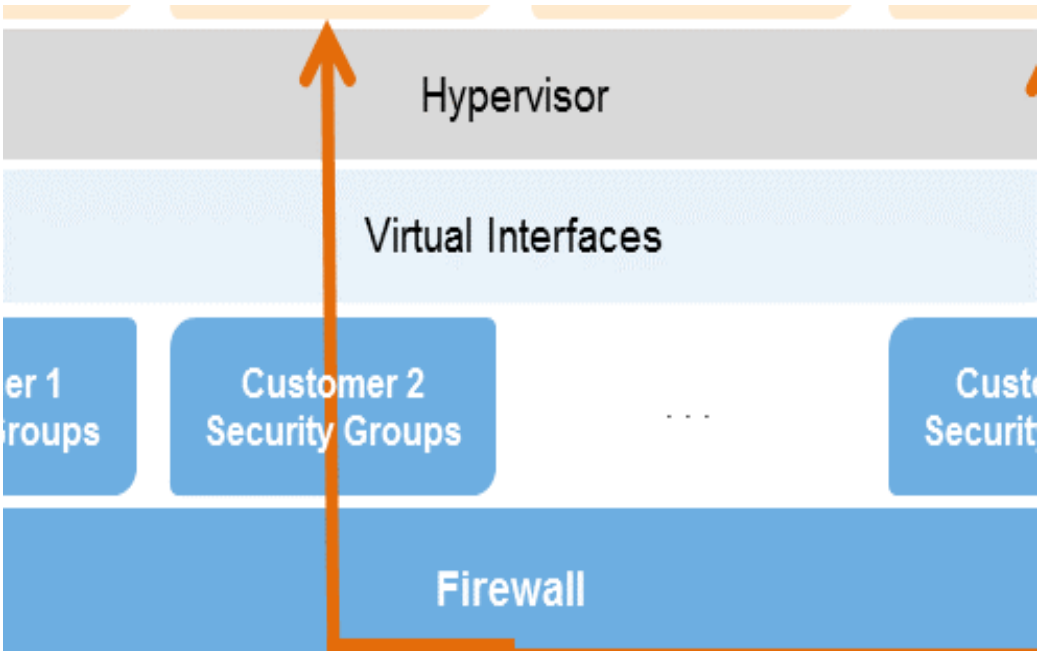


그림 2: Amazon EC2 다중 보안 계층

고객 인스턴스는 원시 디스크 장치에 접근할 수는 없으나, 대신 가상화 디스크를 통해 제공됩니다. AWS 전용 디스크 가상화 계층은 고객이 사용하는 스토리지의 모든 블록을 자동으로 리셋하여 고객 데이터가 절대 실수로 타인에게 노출되지 않게 합니다. AWS에서는 적절한 수단을 사용하여 데이터를 추가로 보호할 것을 권장합니다. 한 가지 일반적인 해법은 가상화 디스크 장치에서 암호화된 파일 시스템을 실행하는 것입니다.

호스트 운영 체제: 업무와 관련하여 관리 평면에 액세스해야 하는 관리자는 다중 요소 인증을 사용하여 특정 관리 호스트에 액세스하는 데 필요한 액세스 권한을 얻어야 합니다. 이러한 관리 호스트는 클라우드의 관리 평면을 보호하기 위해 특별히 설계, 구축, 구성 및 강화된 시스템입니다. 이러한 접근은 모두 기록되고 감사됩니다. 어떤 직원이 업무와 관련하여 관리 평면을 더 이상 액세스할 필요가 없게 될 경우, 이러한 호스트 및 관련 시스템에 대한 권한과 액세스 권한은 해지됩니다.

게스트 운영 체제: 가상 인스턴스는 오직 고객만 제어할 수 있습니다. 고객은 계정, 서비스 및 애플리케이션에 대한 전체 루트 액세스 또는 관리 제어 권한을 가집니다. AWS는 고객의 인스턴스 또는 게스트 OS에 대한 어떤 액세스 권한도 갖지 않습니다. AWS는 기본적인 보안 모범 사례를 따를 것을 권장합니다. 여기에는 암호만을 사용한 게스트 액세스를 금지하는 방법과 멀티 팩터 인증 형식으로 인스턴스에 액세스(또는 최소 인증서 기반 SSH 버전 2 액세스)를 부여하는 방법이 포함됩니다. 또한 고객은 사용자별 로그인을 이용한 권한 상승 방법을 사용해야 합니다. 예를 들어, 게스트 OS가 Linux일 경우, 인스턴스를 강화하면 가상 인스턴스에 액세스할 때 인증서 기반의 SSHv2를 사용하며, 원격 루트 로그인을 비활성화하고, 명령줄 로깅을 사용하며, 권한 상승을 위해 'sudo'를 사용해야 합니다. 고객은 고유한 키 페어를 생성하여 다른 고객 또는 AWS와 공유되지 않도록 해야 합니다.

또한 AWS는 고객이 UNIX/Linux EC2 인스턴스에 안전하게 로그인할 수 있도록 Secure Shell(SSH) 네트워크 프로토콜의 사용을 지원합니다. AWS에서 사용되는 SSH 인증은 인스턴스에 대한 무단 액세스 위험을 줄이기 위해 퍼블릭/프라이빗 키 페어를 통해 이루어집니다. 또한 고객의 인스턴스에 대해 생성된 원격 데스크톱 프로토콜(RDP) 인증서를 사용하여 RDP를 사용하는 Windows 인스턴스에 원격으로 연결할 수도 있습니다.

고객은 보안 업데이트를 포함해 게스트 OS 업데이트 및 패치 적용도 관리합니다. Amazon이 제공하는 Windows 및 Linux 기반 AMI는 주기적으로 최신 패치로 업데이트됩니다. 그러므로 실행 중 Amazon AMI 인스턴스에서 데이터 또는 사용자 지정을 보존할 필요가 없을 경우, 간단히 최신 업데이트가 적용된 AMI를 이용해 새 인스턴스를 다시 시작할 수 있습니다. 또한 Amazon Linux AMI에 대한 업데이트가 Amazon Linux yum 리포지토리를 통해 제공됩니다.

방화벽: Amazon EC2는 완전한 방화벽 솔루션을 제공합니다. 이 필수 인바운드 방화벽은 기본적으로 '모두 거부' 모드로 구성됩니다. Amazon EC2 고객은 인바운드 트래픽을 허용하는 데 필요한 포트를 분명히 개방해야 합니다. 이때 트래픽은 프로토콜, 서비스 포트, 또는 원본 IP 주소에 의해 제한될 수 있습니다(개별 IP 또는 Classless Inter-Domain Routing(CIDR) 블록).

인스턴스 클래스별로 다른 규칙을 사용하는 그룹에 대해 방화벽을 설정할 수 있습니다. 기존의 3계층 웹 애플리케이션을 예로 들어 보겠습니다. 웹 서버 그룹에는 인터넷에 개방된 포트 80(HTTP) 및/또는 포트 443(HTTPS)이 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. 고도의 안전성을 요구하는 애플리케이션은 이러한 방식을 사용하여 구현할 수 있습니다.

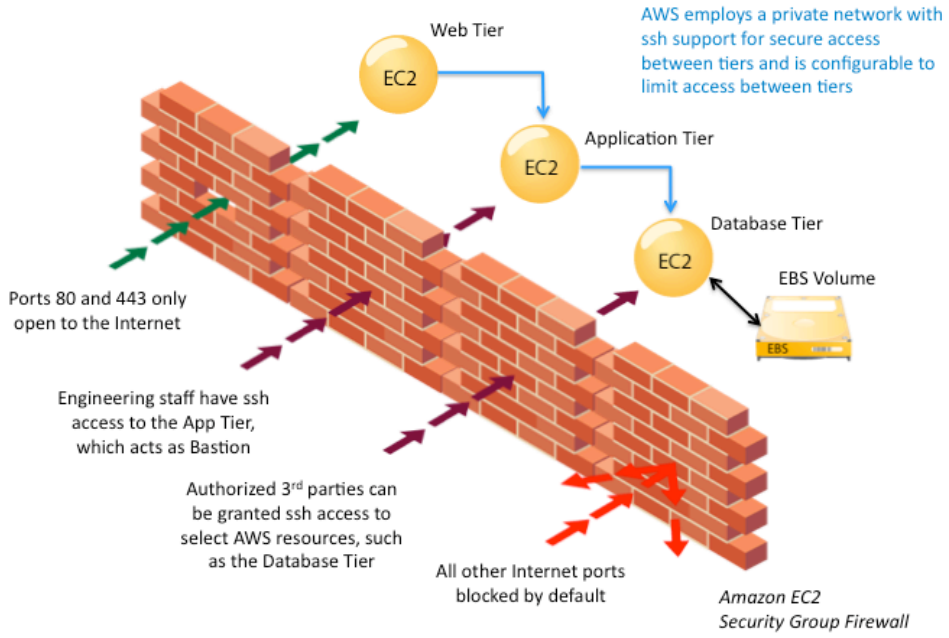


그림 3: Amazon EC2 보안 그룹 방화벽

방화벽은 게스트 운영 체제를 통해 제어할 수 없습니다. 그보다는 고객의 X.509 인증서 및 키를 사용하여 변경 사항을 인증하므로 추가 보안 계층이 필요합니다. 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. 기본 상태는 모든 수신 트래픽을 거부하는 것이며, 고객은 애플리케이션 구축 및 보안 시 어떤 포트를 개방할 것인지를 신중하게 계획해야 합니다. 정보 기반의 트래픽 관리 및 보안 설계가 인스턴스별로 필요합니다. AWS에서는 IPtable 또는 Windows 방화벽 및 VPN과 같은 호스트 기반 방화벽이 있는 인스턴스별 추가 필터를 사용할 것을 권장합니다. 그러면 인바운드 및 아웃바운드 트래픽을 모두 제한할 수 있습니다.

API 액세스: 인스턴스를 시작 및 종료하고, 방화벽 파라미터를 변경하고, 다른 기능을 수행하기 위한 API 호출은 모두 고객의 Amazon 보안 액세스 키로 서명됩니다. 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 EC2 API 호출을 생성할 수 없습니다. 또한, API 호출은 기밀성을 유지하기 위해 SSL로 암호화할 수 있습니다. Amazon은 항상 SSL로 보호되는 API 엔드포인트를 사용하도록 권장하고 있습니다. 또한 고객은 AWS IAM을 이용해 만든 사용자가 호출할 권한이 있는 API를 세부적으로 제어할 수 있습니다.

Elastic Block Storage(Amazon EBS) 보안

Amazon Elastic Block Store(EBS)에서는 Amazon EC2 인스턴스에서 디바이스로서 마운트할 수 있는 스토리지 볼륨을 1GB에서 1TB까지 생성할 수 있습니다. 스토리지 볼륨은 사용자가 정의한 디바이스 이름과 블록 디바이스 인터페이스를 사용하며 포맷되지 않은 원시 블록 디바이스처럼 작동합니다. Amazon EBS 볼륨에 파일 시스템을 생성하거나 하드 드라이브와 같은 블록 디바이스를 사용하는 것처럼 Amazon EBS 볼륨을 사용할 수 있습니다. Amazon EBS의 볼륨에 대한 접근이 해당 볼륨을 생성한 AWS 계정 및 AWS IAM을 이용해 만든 AWS 계정 사용자(사용자가 EBS 작업에 대한 접근 권한이 있는 경우)로 제한되므로, 다른 모든 AWS 계정 및 사용자에게는 볼륨을 보거나 접근하는 권한이 거부됩니다.

Amazon EBS에 저장된 데이터는 정상적인 서비스를 위해 물리적으로 여러 지점에 중복 보관됩니다. 이때 추가 비용도 들지 않습니다. 하지만 Amazon EBS 복사본은 여러 영역이 아닌, 단일한 가용 영역에 저장됩니다. 따라서 장기적으로 데이터를 안전하게 보관하기 위해서는 정기적으로 스냅샷을 생성해 Amazon S3에 저장하는 것이 좋습니다. EBS를 사용하여 복잡한 트랜잭션 데이터베이스를 설계한 경우에는 분산된 트랜잭션과 로그를 검사할 수 있도록 데이터베이스 관리 시스템을 통해 Amazon S3에 백업하는 것이 좋습니다. AWS는 Amazon E2에서 실행되는 인스턴스에 연결된 가상 디스크상에 유지되는 데이터는 백업하지 않습니다.

Amazon EBS 볼륨 스냅샷은 다른 AWS 계정에도 공유하여 자체 볼륨 생성의 기반으로 사용할 수 있습니다. Amazon EBS 볼륨 스냅샷을 공유해도 원본 스냅샷을 변경 또는 삭제할 수 있는 권한은 명시적으로 볼륨을 생성한 AWS 계정에 있으므로 다른 AWS 계정은 원본 스냅샷을 변경 또는 삭제할 수 없습니다. EBS 스냅샷은 전체 EBS 볼륨을 블록 수준으로 나타낸 것입니다. 삭제된 파일과 같이 볼륨의 파일 시스템에서 표시되지 않는 데이터가 EBS 스냅샷에 존재할 수도 있습니다. 공유 스냅샷은 신중하게 만들어야 합니다. 볼륨이 중요한 데이터를 보유하고 있거나 파일을 삭제한 경우, 새로운 EBS 볼륨을 만들어야 합니다. 공유 스냅샷에 포함할 데이터는 새 볼륨과 새 볼륨에서 만든 스냅샷에 복사해야 합니다.

Amazon EBS 볼륨은 포맷되지 않은 원시 블록 디바이스로 사용자에게 제공되며 저장된 데이터는 사전에 삭제됩니다. 데이터는 재사용 바로 전에 삭제되기 때문에 삭제 프로세스가 확실히 완료된 상태로 제공됩니다. DoD 5220.22-M("국가 산업 보안 프로그램 운영 매뉴얼") 또는 NIST 800-88("미디어 삭제 가이드라인")에 자세히 명시된 것과 같이 특정 방법을 통해 모든 데이터를 삭제해야 할 절차가 있는 경우 Amazon EBS에도 이를 적용할 수 있습니다. 마련된 요건 준수를 위해 볼륨을 삭제하기 전에 전문적인 삭제 절차를 수행해야 합니다. 중요한 데이터를 암호화하는 것은 일반적으로 보안에 관한 모범 사례에 해당합니다. AWS는 해당 보안 정책에 부합하는 알고리즘을 통해 중요한 데이터를 암호화할 것을 권장합니다.

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(HTTPS/SSL) 연결을 사용하는 네트워크에서 종단 간 트래픽 암호화를 지원. SSL을 사용하는 경우, 클라이언트 연결을 종료하는 데 사용된 SSL 서버 인증서를 개별 인스턴스에서가 아니라 로드 밸런서에서 중앙집중식으로 관리할 수 있습니다.

HTTPS/SSL을 프런트 엔드 연결로 선택하는 경우 사전 정의된 SSL 암호 집합을 사용하거나 고객이 원하는 암호 집합을 사용하여 특정 요구 사항을 기반으로 암호화 및 프로토콜을 활성화 또는 비활성화할 수 있습니다. Secure Sockets Layer(SSL) 프로토콜은 프로토콜과 알고리즘의 조합을 사용하여 인터넷에서 정보를 보호합니다. SSL 암호는 암호화 키를 사용하여 암호화된(코딩된) 메시지를 생성하는 암호화 알고리즘입니다. SSL 암호 알고리즘 및 프로토콜은 여러 형식을 사용할 수 있습니다. Amazon Elastic Load Balancing은 클라이언트와 고객의 로드 밸런서 사이에 연결이 설정되면 SSL 협상에 사용되는 사전 정의된 암호 집합을 사용해 로드 밸런서를 구성합니다. 사전 정의된 암호 집합은 광범위한 클라이언트와 호환되며 강력한 암호화 알고리즘을 사용합니다. 그러나 일부 고객은 네트워크 상의 모든 데이터를 암호화해야 하고 특정 암호만 허용되는 요구 사항이 있을 수 있습니다. 일부 경우에는 표준 준수를 위해 클라이언트에서 특정 프로토콜(예: PCI, SOX 등)이 요구될 수 있습니다. 이런 경우, Amazon Elastic Load Balancing이 SSL 프로토콜 및 암호에 대해 서로 다른 구성을 선택할 수 있는 옵션을 제공합니다. 고객은 특정 요구 사항에 따라 암호를 활성화 또는 비활성화하도록 선택할 수 있습니다.

Auto Scaling 보안

Auto Scaling을 이용해 고객이 지정한 조건에 따라 Amazon EC2 용량을 자동으로 늘리거나 줄일 수 있습니다. 즉, 요구량이 상승할 때에는 사용하는 Amazon EC2 인스턴스의 수를 원활하게 확장하여 성능을 유지하고, 요구량이 감소할 때에는 자동으로 용량을 축소해 비용을 절감합니다.

다른 AWS 서비스와 마찬가지로 Auto Scaling은 제어 API에 대한 모든 요청을 인증하여 인증받은 사용자만 Auto Scaling에 접근하고 관리할 수 있도록 합니다. 요청 메시지는 이 요청 메시지 및 사용자의 개인 키에서 계산한 HMAC-SHA1 서명으로 서명합니다. 그러나 대규모 또는 탄력적으로 조정되는 집합의 경우 Auto-Scaling을 이용해 시작된 새 EC2 인스턴스로 자격 증명을 제공하는 프로세스가 쉽지 않을 수 있습니다. 이 프로세스를 간소화하기 위해 IAM 내 *역할*을 사용할 수 있습니다. 그러면 역할을 이용해 시작된 새 인스턴스로 자격 증명이 자동으로 제공됩니다. IAM 역할을 이용해 EC2 인스턴스를 시작하면 역할에 의해 지정된 권한을 포함하는 임시 AWS 보안 자격 증명이 안전하게 인스턴스로 프로비저닝되고 Amazon EC2 Instance Metadata Service를 통해 고객의 애플리케이션에서 사용할 수 있게 됩니다. Metadata Service가 현재 활성 자격 증명이 만료되기 전에 새로운 임시 보안 자격 증명을 제공하므로 인스턴스에서 유효한 자격 증명을 항상 사용할 수 있습니다. 또한 임시 보안 자격 증명이 하루에 여러 번 자동으로 교체되므로 향상된 보안을 제공합니다. 고객은 AWS IAM을 이용해 AWS 계정에 사용자들을 만들어 이 사용자들이 호출할 권한이 있는 Auto Scaling API를 지정하여 Auto Scaling에 대한 액세스 권한을 추가로 제어할 수 있습니다. 인스턴스 시작 시 역할 사용에 대한 자세한 정보는 AWS 웹 사이트(http://docs.amazonwebservices.com/AWSEC2/latest/UserGuide/UsingIAM)에서 Amazon EC2 사용 설명서를 참조하십시오.

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.

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 호스트 OS, 게스트 OS, 하이퍼바이저, 인스턴스 격리 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, API 호출은 기밀성을 유지하기 위해 SSL로 암호화할 수 있습니다. Amazon은 항상 SSL로 보호되는 API 끝점을 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 진출입 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.

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.

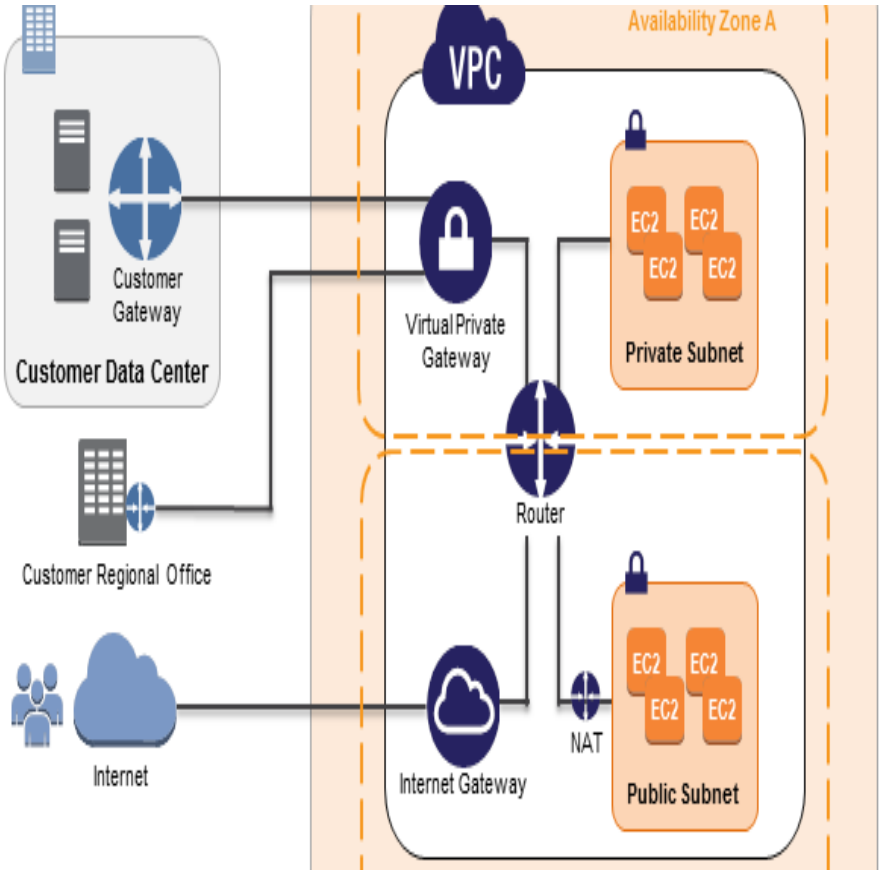


그림 4: Amazon VPC 네트워크 아키텍처

네트워크 ACL(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.

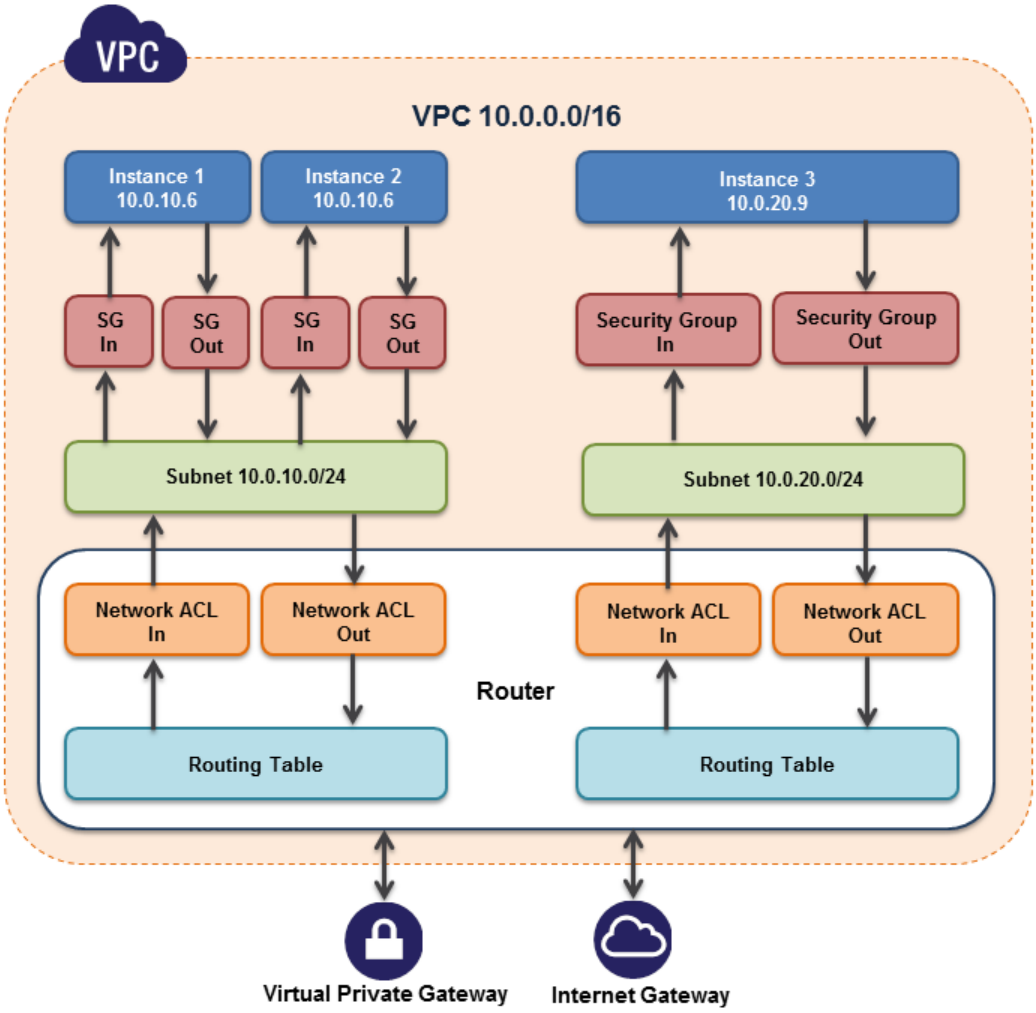


그림 5: 유연 네트워크 토폴로지

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 유동 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.

ENI: 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, 엘라스틱 IP 주소, MAC 주소 등 ENI의 속성은 인스턴스와 연결될 때, 또는 한 인스턴스에서 분리되어 다른 인스턴스로 연결될 때의 ENI를 따릅니다. Amazon VPC에 대한 자세한 내용은 AWS 웹 사이트(http://aws.amazon.com/ko/vpc/)를 참조하십시오.

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 서브넷 생성
- 인터넷 게이트웨이를 생성하여 기본 VPC와 연결
- 인터넷으로 향하는 모든 트래픽을 인터넷 게이트웨이로 전송하는 규칙을 사용하여 기본 VPC에 대한 기본 라우팅 테이블 생성
- 기본 보안 그룹을 생성하여 기본 VPC와 연결
- 네트워크 ACL(액세스 제어 목록)을 생성하여 기본 VPC와 연결
- AWS 계정에서 설정된 기본 DHCP 옵션을 기본 VPC와 연결

기본 VPC가 자체 프라이빗 IP 범위를 갖는 이외에, 기본 VPC의 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	인스터스를 시작할 때마다 EC2-Classic 범위 내의 프라이빗 IP 주소가 할당됩니다.	인스터스를 시작할 때 마다 기본 VPC 범위 내의 사설 프라이빗 IP 주소가 할당됩니다.	인스터스를 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.
Elastic IP 주소	인스턴스를 중지하면, EIP는 더이상 그 인스턴스와 무관하게 됩니다.	인스턴스를 중지해도 EIP는 여전히 그 이슨턴스의 IP입니다.	인스턴스를 중지해도 EIP는 여전히 그 이슨턴스의 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 Direct Connect 보안

고객은 처리량이 높은 전용 연결을 사용하여 내부 네트워크와 AWS 리전 사이에 직접 링크를 프로비저닝할 수 있습니다. 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.

이 서비스를 사용하려면 AWS Direct Connect 위치와 연결해야 합니다. 각 AWS Direct Connect 위치는 지리적으로 가장 가까운 AWS 리전으로 연결할 수 있습니다. Direct Connect 솔루션 업체는 고객 위치에서 AWS Direct Connect 위치까지 연결을 돕습니다.

Amazon Simple Storage Service(Amazon S3) 보안

Amazon Simple Storage Service(S3)를 이용하면 인터넷을 통해 언제 어디서든 데이터를 업로드하고 검색할 수 있습니다. Amazon S3는 데이터를 *버킷* 내에 *객체*로 저장합니다. 텍스트 파일, 사진, 동영상 및 기타 모든 종류의 파일이 객체가 될 수 있습니다. 파일을 Amazon S3에 추가할 때 원하는 경우 파일에 메타데이터를 포함하고 파일에 대한 액세스 제어 권한을 설정할 수 있습니다. 버킷 각각에 대해, 버킷에 대한 액세스를 제어하고(버킷에 객체를 만들고 삭제하고 확인하는 등의 작업을 수행할 수 있는 사용자 지정) 버킷과 버킷의 객체에 대한 액세스 로그를 보고 Amazon S3가 버킷과 버킷의 콘텐츠를 저장할 지역을 선택할 수 있습니다.

데이터 액세스

Amazon S3에 저장된 데이터에 대한 액세스는 기본적으로 제한됩니다. 버킷 및 객체 소유자만 자신이 생성한 Amazon S3 리소스에 액세스할 수 있습니다. (버킷/객체 소유자는 해당 버킷/객체를 만든 사용자가 아니라 AWS 계정 소유자입니다.) 버킷 및 객체에 대한 액세스를 제어하는 방법은 여러 가지가 있습니다.

- **자격 증명 및 액세스 관리(IAM) 정책.** 직원이 여러 명인 조직은 AWS IAM을 통해 하나의 AWS 계정에서 여러 사용자를 생성하고 관리할 수 있습니다. IAM 정책이 사용자에게 연결되어 AWS 계정 내 사용자의 권한을 중앙집중식으로 관리할 수 있습니다. IAM 정책을 사용하면 *자체 AWS 계정 내의 사용자*에게만 자체 Amazon S3 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다.
- **ACL(액세스 제어 목록).** Amazon S3에서 ACL을 사용하여 사용자 그룹에게 버킷 또는 객체에 대한 읽기 또는 쓰기 액세스 권한을 부여할 수 있습니다. ACL을 사용하면 *다른 AWS 계정*(특정 사용자가 아님)에게만 자체 Amazon S3 리소스에 대한 액세스 권한을 부여할 수 있습니다.
- **버킷 정책.** Amazon S3의 버킷 정책은 단일 버킷 내의 일부 또는 모든 객체에 대해 권한을 추가 또는 거부하는 데 사용할 수 있습니다. 정책을 사용자, 그룹 또는 Amazon S3 버킷에 연결해 권한을 중앙 집중식으로 관리할 수 있습니다. 버킷 정책을 사용하면 자체 AWS 계정 내 사용자 *또는* 다른 AWS 계정 내 사용자에게 S3 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다.

액세스 제어 유형	AWS 계정 수준 제어?	사용자 수준 제어?
IAM 정책	아니요	예
ACL	예	아니요
버킷 정책	예	예

특정 조건을 기준으로 특정 리소스에 대한 액세스를 추가로 제한할 수 있습니다. 예를 들어 요청 시간(날짜 조건), 요청이 SSL을 사용하여 전송되었는지 여부(부울 조건), 요청자의 IP 주소(IP 주소 조건), 또는 요청자의 클라이언트 애플리케이션(문자열 조건)을 기준으로 액세스를 제한할 수 있습니다. 이들 조건을 식별하기 위해 *정책 키*를 사용합니다. Amazon S3에서 사용 가능한 작업별 정책 키에 대한 자세한 정보는 Amazon Simple Storage Service 개발자 안내서를 참조하십시오.

또한 Amazon S3는 개발자에게 *쿼리 문자열 인증*을 사용할 수 있는 옵션을 제공합니다. 이 옵션을 사용하면 개발자가 사전 정의된 시간 동안 유효한 URL을 통해 Amazon S3 객체를 공유할 수 있습니다. 쿼리 문자열 인증은 통상적으로는 인증이 필요한 리소스에 HTTP 또는 브라우저 액세스를 부여할 때 유용합니다. 쿼리 문자열 내 서명이 요청을 보호합니다.

데이터 전송

보안을 극대화하기 위해 SSL 암호화 엔드포인트를 통해 Amazon S3에 안전하게 데이터를 업로드하거나 다운로드할 수 있습니다. 암호화 엔드포인트는 인터넷과 Amazon EC2 내에서 액세스할 수 있으므로 데이터가 AWS 내부와 AWS 외부 소스 사이에서 안전하게 전송됩니다.

데이터 저장

Amazon S3는 휴면 상태의 데이터를 보호하기 위한 여러 가지 옵션을 제공합니다. 직접 암호화 키를 관리하려면 Amazon S3 암호화 클라이언트와 같은 클라이언트 암호화 라이브러리를 사용하여 데이터를 암호화한 후 Amazon S3에 업로드할 수 있습니다. 반면 Amazon S3에서 암호화 키를 관리하도록 하려면 Amazon S3 Server Side Encryption(SSE)을 사용할 수 있습니다. Amazon S3 SSE를 사용하면 객체를 기록할 때 별도의 요청 헤더를 추가하는 것만으로 업로드 시 데이터를 암호화할 수 있습니다. 암호 해독은 데이터를 검색할 때 자동으로 이루어집니다.

객체에 포함되는 메타데이터는 암호화되지 않습니다. 따라서 AWS는 S3 메타데이터에 중요한 정보를 포함시키지 않을 것을 권장합니다.

Amazon S3 SSE는 현재 가장 강력한 블록 암호 중 하나인 256비트 고급 암호화 표준(AES-256)을 사용합니다. Amazon S3 SSE를 사용하면 보호되는 모든 객체가 고유한 암호화 키로 암호화됩니다. 그러면 이 객체 키가 정기적으로 교체되는 마스터 키를 사용하여 자체적으로 암호화됩니다. Amazon S3 SSE는 암호화된 데이터와 암호화 키를 다른 호스트에 저장해 보안을 강화합니다. Amazon S3 SSE에서는 암호화 요구 사항도 적용할 수 있습니다. 예를 들어, 암호화된 데이터만 버킷에 업로드해야 하는 버킷 정책을 생성해 적용할 수 있습니다.

장기 저장 시 S3 버킷의 콘텐츠를 Glacier라고 하는 AWS의 보관 서비스에 자동으로 보관할 수 있습니다. S3에 어떤 객체를 언제 Glacier에 보관할 것인지 설명하는 수명 주기 규칙을 생성하여 특정한 간격으로 데이터를 Glacier에 전송할 수 있습니다. 데이터 관리 전략의 한 부분으로 객체를 삭제하기 위해 S3에 배치한 후에 얼마나 오래 기다려야 하는지 지정할 수도 있습니다.

Amazon S3에서 객체 하나를 삭제하면 이 객체에 대한 공개 이름의 매핑이 즉시 제거되는데 이 작업은 분산된 시스템을 대상으로 일반적으로 몇 초 이내에 완료됩니다. 일단 매핑이 제거되면 삭제된 객체에 원격으로 접근할 수 없습니다. 이때 사용된 스토리지 영역은 시스템에서 사용하기 위해 회수됩니다.

데이터 내구성 및 신뢰성

Amazon S3는 연간 99.999999999%의 객체 내구성과 99.99%의 가용성을 제공하도록 설계되었습니다. 객체는 Amazon S3 리전에서 여러 시설의 다양한 디바이스에 중복 저장됩니다. 내구성을 보장하기 위해 Amazon S3 PUT 및 COPY 작업으로 고객 데이터를 여러 시설에 동기식으로 저장한 후에 SUCCESS를 반환합니다. 데이터가 저장되면 Amazon S3가 손실된 중복성을 빠르게 감지 및 복구하여 객체의 지속성을 유지합니다. 또한 Amazon S3는 체크섬을 사용해 저장된 데이터의 무결성을 정기적으로 검사합니다. 손상이 감지된 경우 중복 데이터를 사용하여 복원합니다. 이 외에도 Amazon S3는 데이터를 저장 또는 검색할 때 모든 네트워크 트래픽에서 체크섬을 계산하여 데이터 패킷 손상을 감지합니다.

Amazon S3는 버전 관리를 통해 추가적인 보호 기능을 제공합니다. 버전 관리를 사용하면 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원할 수 있습니다. 또한, 의도하지 않은 사용자 작업 및 애플리케이션 장애로부터 쉽게 복구할 수 있습니다. 기본적으로 요청을 통해 가장 최근에 기록된 버전을 검색합니다. 이전 버전의 객체는 요청에 버전을 지정하여 검색할 수 있습니다. Amazon S3 버전 관리의 MFA 삭제 기능을 사용하여 버전을 추가로 보호할 수 있습니다. S3 버킷에 활성화되면 각 버전 삭제 요청에는 멀티 팩터 인증 디바이스의 6자리 코드와 일련 번호가 포함되어 있어야 합니다.

액세스 로그

Amazon S3 버킷은 버킷과 버킷 내의 객체에 대한 액세스를 로그하도록 설정할 수 있습니다. 액세스 로그에는 요청 유형, 요청한 자원, 요청자의 IP, 요청 시간 및 날짜 등 각 액세스 요청에 대한 정보가 포함됩니다. 버킷에 대한 로깅을 선택하면, 로그 기록이 주기적으로 로그 파일 내에 추가되어 지정된 Amazon S3 버킷으로 전달됩니다.

CORS(Cross-Origin Resource Sharing)

S3를 사용하여 정적 웹 페이지를 호스팅하거나 다른 웹 페이지가 사용하는 객체를 저장하는 AWS 고객은 S3 버킷을 교차 원본 요청을 명시적으로 활성화하도록 구성하여 안전하게 로드할 수 있습니다. 최신 브라우저는 악성 콘텐츠가 평판이 나쁜 출처(교차 사이트 스크립팅 공격 등)에서 로드되지 않도록 보장하는 방법으로써 동일 원본 정책을 사용하여 JavaScript 또는 HTML5가 요청을 통해 다른 사이트 또는 도메인에서 콘텐츠를 로드하지 않도록 차단합니다. 교차 원본 리소스 공유(CORS) 정책이 활성화되면 S3 버킷에 저장된 웹 폰트 및 이미지 등의 자산은 외부 웹 페이지, 스타일 시트 및 HTML5 애플리케이션에서 안전하게 참조할 수 있습니다.

AWS Glacier 보안

Amazon Glacier 서비스는 Amazon S3와 같이 저렴하고 안전하며 내구성이 뛰어난 스토리지를 제공합니다. 하지만 S3가 신속한 검색을 위해 설계된 반면 Glacier는 자주 액세스하지 않고 검색 시간이 여러 시간 걸려도 괜찮은 데이터의 보관 서비스로 사용할 목적으로 개발되었습니다.

Amazon Glacier는 파일을 *아카이브* 단위로 *볼트* 내에 저장합니다. 아카이브는 사진, 동영상 또는 문서 등 모든 데이터가 될 수 있고 하나 또는 여러 개의 파일이 포함되어 있을 수 있습니다. 단일 볼트에 아카이브를 무제한 저장할 수 있고 리전당 최대 1,000개의 볼트를 생성할 수 있습니다. 각 아카이브에 최대 40TB의 데이터를 포함할 수 있습니다.

데이터 업로드

Amazon Glacier 볼트로 데이터를 전송하기 위해 단일 업로드 작업이나 멀티파트 작업으로 아카이브를 업로드할 수 있습니다. 단일 업로드 작업으로 최대 4GB 크기의 아카이브를 업로드할 수 있습니다. 그러나 고객은 멀티파트 업로드 API를 사용할 경우 100MB가 넘는 아카이브를 업로드할 수 있어 더 나은 결과를 얻을 수 있습니다. 멀티파트 업로드 API를 사용하면 최대 40,000GB 가량의 대형 아카이브를 업로드할 수 있습니다. 멀티파트 업로드 API 호출은 대용량 아카이브에 대한 업로드 환경을 개선하기 위해 설계되었으며, 파트를 아무 순서대로 동시에 개별적으로 업로드할 수 있습니다. 멀티파트 업로드가 실패할 경우 전체 아카이브가 아니라 실패한 파트만 다시 업로드하면 됩니다.

Glacier에 데이터를 업로드할 때에는 트리 해시를 계산해 공급해야 합니다. Glacier는 해시가 중간에 바뀌지 않았는지 확인하기 위해 데이터와 비교 검사합니다. 트리 해시는 메가바이트 크기의 각 데이터 세그먼트에 대한 해시를 계산한 뒤 데이터의 인접 세그먼트가 증가하는 것을 나타내는 트리 방식으로 해시를 결합해 생성됩니다.

Amazon Glacier에 많은 양의 데이터를 업로드해야 하는 고객은 멀티파트 업로드 기능을 사용하는 대신 AWS Import/Export 서비스를 사용하여 데이터를 전송하는 방법을 고려해 볼 수 있습니다. AWS Import/Export는 데이터 전송 시 이동식 스토리지 디바이스를 사용하여 AWS로 간편하게 많은 양의 데이터를 이동할 수 있습니다. AWS는 인터넷을 우회하는 Amazon의 고속 내부 네트워크를 사용하여 스토리지 디바이스에서 데이터를 전송합니다.

특정한 간격으로 Glacier에 데이터를 전송하도록 S3를 설정할 수도 있습니다. S3에서 Glacier에 어떤 객체를 언제 보관할 것인지 설명하는 수명 주기 규칙을 생성할 수 있습니다. 객체를 삭제하기 위해 S3에 배치한 후에 얼마나 오래 기다려야 하는지도 지정할 수 있습니다.

더 높은 수준의 보안을 달성하기 위해 SSL 암호화 엔드포인트를 통해 Amazon Glacier에 안전하게 데이터를 업로드하거나 다운로드할 수 있습니다. 암호화 엔드포인트는 인터넷과 Amazon EC2 내에서 액세스할 수 있으므로 데이터가 AWS 내부와 AWS 외부 소스 사이에서 안전하게 전송됩니다.

데이터 검색

Amazon Glacier에서 아카이브를 검색하려면 검색 작업을 시작해야 하는데 이 작업은 대체로 3~5시간이면 완료됩니다. 그러면 바이트 범위 요청이 포함된 HTTP GET 요청을 통해 데이터에 액세스할 수 있습니다. 데이터는 24시간 동안 사용 가능한 상태로 유지됩니다.

바이트 범위 검색을 사용하여 검색 요금을 줄이거나 없앨 수 있습니다. 바이트 범위 검색을 사용하는 경우는 여러 개의 파일을 집계하여 단일 아카이브로 업로드했다가 그 파일 중 적은 수를 선택해 검색해야 하는 경우인데 이때 필요한 파일이 들어있는 아카이브의 범위만을 검색할 수 있습니다. 이유를 불문하고 아카이브 조각을 검색할 때 검색된 범위와 전체 아카이브의 트리 해시와 일치시키면 제공된 체크섬을 사용하여 파일의 무결성을 확인할 수 있습니다.

데이터 저장

Amazon Glacier는 AES-256을 사용하여 데이터를 자동으로 암호화하고 변경이 불가능한 형태로 내구성을 고려해 저장합니다. Amazon Glacier는 아카이브에 대해 연평균 99.999999999%의 내구성을 제공하도록 설계되었습니다. 여러 시설 및 여러 디바이스에 각 아카이브를 저장합니다. 어려운 데이터 검증 및 수동 복구 작업이 필요할 수 있는 일반적인 시스템과 달리 Glacier는 정기적이고 체계적인 데이터 무결성 검사를 수행하며 자동으로 자가 치유 기능을 실행하도록 설계되어 있습니다.

데이터 액세스

계정을 통해서만 Amazon Glacier에서 자신의 데이터에 액세스할 수 있습니다. Amazon Glacier에서 데이터 액세스를 제어하려면, AWS IAM을 사용하여 계정 내에서 어떤 사용자에게 지정된 볼트에 대한 작업 권한이 있는지 지정합니다.

AWS Storage Gateway 보안

AWS Storage Gateway는 온프레미스 소프트웨어 어플라이언스를 클라우드 기반 스토리지에 연결하는 서비스로, IT 환경과 AWS의 스토리지 인프라를 원활하고 안전하게 통합할 수 있게 해줍니다. 이 서비스를 사용하면 AWS의 확장 가능하고 안정적이고 안전한 S3 스토리지 서비스에 데이터를 안전하게 업로드할 수 있으므로 비용 효율적인 백업과 신속한 재해 복구가 가능합니다.

AWS Storage Gateway는 데이터를 사이트 외부의 Amazon S3에 Amazon EBS 스냅샷 형태로 투명하게 백업합니다. Amazon S3는 이러한 스냅샷을 여러 설비의 여러 디바이스에 중복 저장하고 중복성 손실을 감지하여 복구합니다. Amazon EBS 스냅샷은 온프레미스에서 복원하거나 새로운 Amazon EBS 볼륨을 인스턴스화하는 데 사용할 수 있는 지정 시점 백업을 제공합니다. 데이터는 지정한 단일 리전에 저장됩니다.

AWS Storage Gateway는 두 가지 옵션을 제공합니다.

- **게이트웨이 저장 볼륨(클라우드가 백업되는 경우)**. 이 옵션에서는 볼륨 데이터가 로컬로 저장된 다음 Amazon S3로 푸시되고 중복 암호화된 형태로 저장되며 Elastic Block Store(EBS) 스냅샷의 형태로 사용 가능하게 됩니다. 이 모델을 사용하면 온프레미스 스토리지가 기본이기 때문에 전체 데이터 세트에 지연 시간이 낮은 액세스를 제공하고 클라우드 스토리지가 백업이 됩니다.
- **게이트웨이 캐싱 볼륨(클라우드가 기본인 경우)**. 이 옵션에서는 볼륨 데이터가 Amazon S3에 암호화되어 저장되고 iSCSI 인터페이스를 통해 엔터프라이즈의 네트워크 내에 표시됩니다. 최근에 액세스한 데이터는 지연 시간이 낮은 로컬 액세스를 위해 온프레미스에 캐싱됩니다. 이 모델을 사용하면 클라우드 스토리지가 기본이지만 온프레미스에서 캐싱된 볼륨에 설정된 활성 작동 세트에 대한 지연 시간이 낮은 액세스를 얻을 수 있습니다.

어떤 옵션을 선택하든 데이터는 온프레미스 스토리지 하드웨어에서 SSL을 통해 AWS로 비동기식으로 전송됩니다. 256비트 암호화 키를 사용하는 대칭 키 암호화 표준인 AES(Advanced Encryption Standard) 256을 사용하여 데이터가 암호화되어 Amazon S3에 저장됩니다. 변경된 데이터만을 업로드하기 때문에 인터넷을 통한 데이터 전송량을 최소화할 수 있습니다.

AWS Storage Gateway는 VMware ESXi Hypervisor v 4.1 또는 v 5 또는 Microsoft Hyper-V(설정 프로세스 중에 VMware 소프트웨어 다운로드)를 실행하는 데이터 센터에 호스트로 배포하는 가상 머신(VM)으로 실행됩니다. 해당 가상 머신에 iSCSI(Internet Small Computer System Interface) 스토리지 볼륨(대상)을 생성할 수 있습니다. 온프레미스 애플리케이션(이니시에이터)이 이에 접속하여 데이터를 저장하면, 데이터가 AWS로 업로드됩니다.

설치하고 구성하는 동안 게이트웨이당 최대 12개의 iSCSI 스토리지 볼륨을 만들 수 있습니다. 설치하면 각 게이트웨이는 업데이트와 패치를 자동으로 다운로드, 설치 및 배포합니다. 이 작업은 게이트웨이별로 설정된 유지 관리 기간 동안 일어납니다.

iSCSI 프로토콜은 CHAP(Challenge-Handshake 인증 프로토콜)을 통한 대상과 이니시에이터 간 인증을 지원합니다. CHAP은 주기적으로 iSCSI 이니시에이터의 ID를 스토리지 볼륨 대상에 액세스하기 위해 인증된 것으로 확인하여 중간자 및 재생 공격으로부터 보호합니다. CHAP를 설정하려면 AWS Storage Gateway 콘솔 및 대상에 연결하기 위해 사용된 iSCSI 이니시에이터 소프트웨어 모두에 구성해야 합니다.

AWS Storage Gateway VM을 배포한 다음 AWS Storage Gateway 콘솔을 사용하여 게이트웨이를 활성화해야 합니다. 정품 인증 프로세스는 게이트웨이와 AWS 계정을 연결합니다. 이 연결을 설정하면 콘솔에서 게이트웨이의 거의 모든 측면을 관리할 수 있습니다. 정품 인증하는 동안 게이트웨이의 IP 주소 및 이름, 스냅샷 백업을 저장할 AWS 리전 및 게이트웨이 시간대를 지정합니다.

AWS Import/Export 보안

AWS Import/Export는 AWS S3 또는 EBS 스토리지에 대량의 데이터를 물리적으로 전송하는 간단하고 안전한 메서드입니다. 이 서비스는 대체로 데이터가 100GB를 초과하거나 연결 속도가 느려 인터넷을 통한 전송 속도가 느린 고객이 사용합니다. AWS Import/Export를 사용하면 안전한 AWS 시설로 배송하는 휴대용 스토리지 디바이스를 준비할 수 있습니다. AWS는 Amazon의 고속 내부 네트워크를 사용하여 스토리지 디바이스에서 데이터를 전송함으로써 인터넷을 우회합니다. 반대로, 데이터는 AWS에서 휴대용 스토리지 디바이스로 내보낼 수도 있습니다

AWS Import/Export 서비스는 다른 모든 AWS 서비스와 마찬가지로 스토리지 디바이스를 안전하게 식별 및 인증해야 합니다. 이 경우 Amazon S3 버킷, Amazon EBS 리전, AWS 액세스 키 ID, 반품 배송 주소를 포함한 작업 요청을 AWS에 전송합니다. 사용자는 해당 작업의 고유 식별자, 디바이스 인증을 위한 디지털 서명, 스토리지 디바이스를 배송할 AWS 주소를 받게 됩니다. Amazon S3의 경우 디바이스의 루트 디렉토리에 서명 파일을 저장합니다. Amazon EBS의 경우 디바이스 외부에 서명 바코드를 테이프로 부착합니다. 서명 파일은 인증에만 사용되고 S3 또는 EBS에 업로드되지 않습니다.

S3로 전송하려면 고객이 데이터를 업로드해야 하는 특정 버킷을 지정하고 로드를 하고 있는 계정이 버킷 쓰기 권한이 있는지 확인해야 합니다. 또한 S3에 로드된 각 객체에 적용할 액세스 제어 목록을 지정해야 합니다.

EBS에 전송하려면 EBS 가져오기 작업을 위한 대상 리전을 지정합니다. 스토리지 디바이스가 최대 볼륨 크기인 1TB보다 작거나 같으면 해당 콘텐츠가 직접 Amazon EBS 스냅샷으로 로드됩니다. 스토리지 디바이스 용량이 1TB를 초과하는 경우 지정된 Amazon S3 로그 버킷 내에 디바이스 이미지가 저장됩니다. 그러면 Logical Volume Manager와 같은 소프트웨어를 사용해 Amazon EBS 볼륨의 RAID를 만들고 이미지를 Amazon S3에서 이 새로운 볼륨으로 복사할 수 있습니다.

업로드가 완료된 후 AWS가 스토리지 디바이스의 콘텐츠를 삭제하게 하려는지 여부를 지정할 수 있습니다. 이 옵션을 선택하면 스토리지 디바이스의 쓰기 가능한 모든 블록이 0으로 덮어쓰기됩니다. 디바이스가 지워진 후에는 디바이스를 다시 파티셔닝하고 포맷해야 합니다.

디바이스를 국제 배송할 경우 AWS에 전송되는 매니페스트 파일에 세관 옵션 및 특정 필수 하위 필드가 필요합니다. AWS Import/Export는 이러한 값을 사용하여 인바운드 배송을 검증하고 아웃바운드 세관 서류를 준비합니다. 이 옵션 중 두 가지는 디바이스에 저장된 데이터가 암호화되었는지 여부와 암호화 소프트웨어의 분류입니다. 미국 내외로 암호화된 데이터를 배송하는 경우 미국 수출 관리 규정(United States Export Administration Regulations)에 따라 암호화 소프트웨어를 5D992로 분류해야 합니다.

AWS Data Pipeline

AWS Data Pipeline 서비스는 데이터 중심 워크플로우 및 기본 제공되는 종속성 확인 기능을 사용하여 여러 데이터 소스 간에 지정된 간격으로 데이터를 안정적으로 처리하고 이동할 수 있도록 도와줍니다. 파이프라인을 생성하면 데이터 소스, 전제 조건, 대상, 처리 단계 및 운영 일정을 정의하게 됩니다. 파이프라인을 정의 및 활성화하면 지정한 일정에 따라 자동으로 실행됩니다.

AWS Data Pipeline을 사용하면 리소스 가용성 확인, 작업 간 종속성 관리, 일시적 실패/시간 초과로 인한 개별 작업 재시도, 실패 알림 생성 시스템 등에 대해 염려하지 않아도 됩니다. AWS Data Pipeline은 파이프라인이 데이터를 처리하는 데 필요한 AWS 서비스 및 리소스(예: Amazon EC2 또는 EMR)를 시작하고 스토리지(예: Amazon S3, RDS, DynamoDB 또는 EMR)에 결과를 전송하는 일을 담당합니다.

콘솔을 사용하는 경우 AWS Data Pipeline이 신뢰할 수 있는 필요한 엔터티 목록 등의 IAM 역할 및 정책을 생성합니다. IAM 역할은 파이프라인이 액세스할 수 있는 것과 수행할 수 있는 작업을 결정합니다. 또한 파이프라인이 EC2 인스턴스 등의 리소스를 생성하면 IAM 역할이 EC2 인스턴스의 허용된 리소스 및 작업을 결정합니다. 파이프라인을 생성하면 파이프라인을 통제하는 IAM 역할 하나와 파이프라인의 리소스를 통제하는 또 다른 IAM 역할("리소스 역할"이라 함)을 지정하는데 두 가지 모두 같은 역할일 수 있습니다. 최소 권한 부여 방식의 보안 모범 사례의 한 부분으로 파이프라인이 작업을 수행하고 이에 따라 IAM 역할을 정의하는 데 필요한 최소 권한을 고려하는 것이 좋습니다.

대부분의 AWS 서비스와 마찬가지로, AWS Data Pipeline도 SSL을 통한 액세스를 위해 안전(HTTPS) 엔드포인트 옵션을 제공합니다.

Amazon Simple Database(SimpleDB) 보안

Amazon SimpleDB는 데이터베이스 관리 작업 부담을 덜어주어 웹 서비스 요청을 통해 데이터 항목을 간단하게 저장 및 쿼리할 수 있는 비관계형 데이터 스토리지입니다. Amazon SimpleDB는 여러 지역에 분산된 데이터 복제본을 자동으로 생성 및 관리하여 높은 가용성과 데이터 내구성을 확보합니다.

Amazon SimpleDB의 데이터는 도메인에 저장되며 여러 도메인에서 기능을 수행할 수 없다는 점을 제외하면 데이터베이스 테이블과 유사합니다. Amazon SimpleDB API는 도메인 생성자에게 허가된 접근만 허용하는 도메인 차원의 제어 기능을 제공합니다. 따라서 사용자 데이터에 대한 접근권을 갖는 사용자들에 대한 통제 권한을 사용자가 갖습니다.

Amazon SimpleDB는 자체적으로 리소스 기반 권한 시스템을 제공하지 않습니다. 하지만 서비스가 AWS IAM과 통합되어 있으므로 사용자는 AWS 계정의 다른 사용자에게 AWS 계정 내 Amazon SimpleDB 도메인에 대한 액세스 권한을 부여할 수 있습니다. 각 개별 도메인에 대한 액세스 권한은 인증된 사용자를 고객이 소유한 도메인에 매핑한 별도의 ACL을 통해 관리됩니다. AWS IAM을 이용하여 생성한 사용자는 정책에 따라 권한이 부여된 작업과 도메인에만 액세스할 수 있습니다.

또한 SimpleDB 서비스에 대한 각 요청에는 유효한 HMAC-SHA 서명이 포함되어 있어야 하며, 그렇지 않은 경우 요청이 거부됩니다. AWS SDK 중 하나를 사용하여 Amazon SimpleDB에 액세스하는 경우 SDK가 사용자 대신 인증 프로세스를 처리합니다. 그렇지만 REST 요청을 사용하여 Amazon SimpleDB에 액세스하는 경우 사용자는 AWS 액세스 키 ID, 유효한 HMAC-SHA 서명(HMAC-SHA1 또는 HMAC-SHA256 중 하나) 및 타임스탬프를 제공해야 요청에 대한 인증을 받을 수 있습니다. AWS는 사용자의 액세스 키 ID를 사용하여 보안 액세스 키를 검색하고 요청에 전송된 서명을 계산하는 데 사용하는 동일한 알고리즘을 사용하여 요청 데이터 및 보안 액세스 키로부터 서명을 생성합니다. AWS에서 생성된 서명이 사용자가 요청을 통해 보낸 서명과 일치하는 경우 요청이 인증된 것으로 간주됩니다. 서명이 일치하지 않는 경우 요청이 삭제되고 AWS는 오류를 반환합니다.

Amazon SimpleDB는 SSL로 암호화된 엔드포인트를 통해 액세스할 수 있습니다. 이 암호화된 엔드포인트에는 인터넷과 Amazon EC2에서 모두 액세스할 수 있습니다. Amazon SimpleDB에 저장된 데이터는 AWS에서 암호화하지 않습니다. 그러나 고객은 Amazon SimpleDB에 업로드하기 전에 데이터를 암호화할 수 있습니다. 이와 같이 암호화된 속성은 Get 작업을 통해서만 검색할 수 있으며, 쿼리 필터링 조건으로는 사용할 수 없습니다. Amazon SimpleDB에 전송하기 전에 데이터를 암호화하면AWS를 포함한 어떤 장치에서든 중요한 고객 데이터에 접근하지 못하도록 보호합니다.

Amazon SimpleDB에서 도메인 하나를 삭제하면 이 도메인에 대한 매핑이 즉시 제거되는데 이 작업은 분산된 시스템을 대상으로 일반적으로 몇 초 이내에 완료됩니다. 일단 매핑이 제거되면 삭제된 도메인에 원격으로 액세스할 수 없습니다.

항목과 속성 데이터를 도메인에서 삭제하면 도메인 내의 매핑이 즉시 제거되며 이 작업도 일반적으로 몇 초 이내에 완료됩니다. 일단 매핑이 제거되면 삭제된 데이터에 원격으로 액세스할 수 없습니다. 저장 영역은 쓰기 작업에만 사용할 수 있으며, 데이터는 새로 저장한 데이터로 업데이트됩니다.

Amazon SimpleDB에 저장된 데이터는 정규 서비스 작업의 일부로 추가 비용 없이 여러 물리적 위치에 중복 저장됩니다. Amazon SimpleDB는 초기 쓰기 과정에서 여러 가용 영역에 객체를 여러 번 저장하여 객체의 내구성을 제공하고 이후에 디바이스를 사용할 수 없거나 비트 손상(bit-rot)이 감지될 경우에 대비하여 추가로 복제하는 적극적인 조치를 취합니다.

Amazon DynamoDB 보안

Amazon DynamoDB는 완벽하게 관리되는 NoSQL 데이터베이스 서비스로서 원활한 확장성과 함께 빠르고 예측 가능한 성능을 제공합니다. Amazon DynamoDB를 통해 분산 데이터베이스를 운영하고 AWS로 조정하는 데 따른 관리 부담에서 벗어날 수 있으며, 하드웨어 프로비저닝, 설정 및 구성, 복제, 소프트웨어 패치 또는 클러스터 조정에 대해서도 걱정할 필요가 없습니다.

데이터 규모에 관계없이 데이터를 저장 및 검색하고, 어떤 수준의 요청 트래픽이라도 처리할 수 있는 데이터베이스 테이블을 생성할 수 있습니다. DynamoDB는 테이블의 데이터와 트래픽을 충분한 수의 서버로 자동 분산하여 지정된 요청 용량과 저장된 데이터 양을 처리하면서도 일관되고 빠른 성능을 유지합니다. 모든 데이터 항목이 SSD(Solid State Drive)에 저장되고 리전의 여러 가용 영역에 걸쳐 자동 복제되기 때문에 확실한 고가용성과 데이터 내구성을 보여줍니다.

Amazon DynamoDB는 자체적으로 리소스 기반 권한 시스템을 제공하지 않습니다. 하지만 서비스가 AWS IAM Security Token Service와 통합되어 있으므로 사용자는 AWS 계정의 다른 사용자에게 AWS 계정 내 Amazon DynamoDB 테이블에 대한 액세스 권한을 부여할 수 있습니다. 각 개별 테이블에 대한 액세스 권한은 인증된 사용자를 고객이 소유한 테이블에 매핑한 별도의 ACL을 통해 관리됩니다. AWS IAM을 이용하여 생성한 사용자는 정책에 따라 권한이 부여된 작업과 테이블에만 액세스할 수 있습니다.

Amazon DynamoDB를 사용하려면 사용자가 인증 프로세스가 신속하고 효율적으로 진행될 수 있도록 AWS Security Token Service로부터 자격 증명을 얻어야 합니다. AWS Security Token Service가 임시 보안 자격 증명을 생성하면 자격 증명이 얼마나 오래 유효한지 지정할 수 있습니다. 보안상의 이유로 AWS 계정의 루트 자격 증명에 대한 보안 토큰의 수명은 1시간으로 제한됩니다. 단, IAM 사용자의 임시 자격 증명 또는 IAM 사용자가 검색하는 연동된 사용자 자격 증명은 최대 36시간 동안 유효할 수 있습니다.

또한 DynamoDB 서비스에 대한 각 요청에는 유효한 HMAC-SHA256 서명이 포함되어야 하며, 포함되지 않은 경우 요청이 거부됩니다. AWS SDK는 자동으로 요청에 서명하고 Amazon DynamoDB에 필요한 AWS Security Token Service 자격 증명을 관리합니다. 하지만 사용자가 자체적으로 HTTP POST 요청을 작성하려는 경우 Amazon DynamoDB에 대한 요청 헤더에 서명을 제공해야 합니다. 서명을 계산하려면 AWS Security Token Service에 임시 보안 자격 증명을 요청해야 합니다. 임시 보안 자격 증명을 사용하여 Amazon DynamoDB에 대한 요청에 서명합니다.

Amazon DynamoDB는 SSL로 암호화된 엔드포인트를 통해 액세스할 수 있습니다. 이 암호화된 엔드포인트에는 인터넷과 Amazon EC2에서 모두 액세스할 수 있습니다.

Amazon Relational Database Service(Amazon RDS) 보안

Amazon RDS를 통해 관계형 데이터베이스(DB) 인스턴스를 신속하게 만들고, 애플리케이션 요구에 맞춰 관련 컴퓨팅 리소스 및 스토리지 용량을 유연하게 확장할 수 있습니다. Amazon RDS는 백업 수행, 장애 조치 처리, 및 데이터베이스 소프트웨어 유지관리를 통해 고객을 대신하여 데이터베이스 인스턴스를 관리합니다. 현재 Amazon RDS는 MySQL, Oracle 또는 Microsoft SQL Server 데이터베이스 엔진에 사용할 수 있습니다.

Amazon RDS에는 DB 보안 그룹, 사용 권한, SSL 연결, 자동화된 백업, DB 스냅샷, 다중 AZ 배포를 포함해 중요한 프로덕션 데이터베이스의 안정성을 높여 주는 여러 가지 기능이 있습니다. DB 인스턴스는 추가 네트워크 격리를 위해 Amazon VPC에도 배포할 수 있습니다.

액세스 제어

Amazon RDS 내에서 처음 DB 인스턴스를 생성할 경우 DB 인스턴스에 대한 액세스를 제어하기 위해 Amazon RDS 컨텍스트 안에서만 사용되는 마스터 사용자 계정을 만듭니다. 마스터 사용자 계정은 모든 데이터베이스 권한을 사용하여 DB 인스턴스에 로그인할 수 있도록 허용하는 기본 데이터베이스 사용자 계정입니다. DB 인스턴스를 만들 때 각 DB 인스턴스에 연결할 마스터 사용자 이름과 암호를 지정할 수 있습니다. DB 인스턴스를 만들면 마스터 사용자 자격 증명을 사용하여 데이터베이스에 연결할 수 있습니다. 그 다음으로 DB 인스턴스에 액세스 가능한 사용자를 제한할 수 있도록 추가 사용자 계정을 생성할 수 있습니다.

Amazon EC2 보안 그룹과 비슷하지만 동일하게 사용할 수 없는 DB 보안 그룹을 통해 Amazon RDS DB 인스턴스를 제어할 수 있습니다. DB 보안 그룹은 DB 인스턴스에 대한 네트워크 액세스를 제어하는 방화벽과 비슷한 역할을 합니다. 데이터베이스 보안 그룹 기본값은 '모두 거부' 액세스 모드입니다. 따라서 고객이 네트워크 진입을 명확하게 허가해야만 합니다. 이를 위한 두 가지 방법은 일정한 네트워크 IP 범위를 허가하거나 기존 Amazon EC2 보안 그룹을 허가하는 것입니다. DB 보안 그룹은 데이터베이스 서버 포트(다른 모든 포트는 차단됨)에 대한 액세스를 허용하고 Amazon RDS DB 인스턴스를 다시 시작하지 않고도 업데이트할 수 있습니다. 이렇게 하면 고객이 자신의 데이터베이스 액세스 권한을 원활하게 제어할 수 있습니다. AWS IAM을 사용하여 RDS DB 인스턴스에 대한 액세스를 추가로 제어할 수 있습니다. AWS IAM을 사용하면 개별 사용자가 어떤 RDS 작업을 호출할 수 있는지 제어할 수 있습니다.

네트워크 격리

추가 네트워크 액세스 제어를 위해 Amazon VPC에서 DB 인스턴스를 실행할 수 있습니다. Amazon VPC에서는 사용하려는 IP 범위를 지정하여 DB 인스턴스를 분리하고, 업계 표준 암호화 방식의 IPsec VPN을 사용하여 기존 IT 인프라에 접속할 수 있습니다. 현재 Amazon VPC 기능은 MySQL DB 엔진에서만 사용할 수 있습니다.

VPC에서 Amazon RDS를 실행하면 프라이빗 서브넷 내에 DB 인스턴스를 만들 수 있습니다. 가상 프라이빗 게이트웨이를 설정해 사내 네트워크를 VPC로 확장하여 해당 VPC의 RDS DB 인스턴스에 액세스할 수 있도록 하는 방법도 있습니다. 자세한 내용은 Amazon VPC User Guide를 참조하십시오.

다중 AZ 배포의 경우, 특정 리전의 모든 가용 영역에 서브넷을 정의하면 Amazon RDS가 필요한 경우 다른 가용 영역에 새로운 예비 복제본을 만들 수 있습니다. VPC에서 RDS DB 인스턴스에 대해 지정할 수 있는 서브넷의 모음인 DB 서브넷 그룹을 생성할 수 있습니다. 각 DB 서브넷 그룹에는 특정 리전의 가용 영역마다 하나 이상의 서브넷이 있어야 합니다. 이 경우 VPC에 DB 인스턴스를 생성하면 DB 서브넷 그룹을 선택하게 됩니다. 그러면 Amazon RDS가 해당 DB 서브넷 그룹 및 원하는 가용 영역을 사용하여 해당 서브넷 내에서 서브넷과 IP 주소를 선택합니다. Amazon RDS가 엘라스틱 네트워크 인터페이스를 만든 다음 해당 IP 주소를 가진 DB 인스턴스에 연결합니다.

Amazon VPC에 배포된 DB 인스턴스는 인터넷에서 액세스하거나 VPN 또는 퍼블릭 서브넷에서 실행할 수 있는 배스천 호스트를 통해 VPC 외부의 Amazon EC2 인스턴스에서 액세스할 수 있습니다. 배스천 호스트를 사용하려면 SSH 접속 역할을 하는 EC2 인스턴스를 사용하여 퍼블릭 서브넷을 설정해야 합니다. 이 퍼블릭 서브넷은 SSH 호스트를 통해 트래픽을 제어할 수 있는 인터넷 게이트웨이 또는 라우팅 규칙이 필요합니다. 또한, SSH 호스트에서 Amazon RDS DB 인스턴스의 프라이빗 IP 주소로 요청을 전달할 수 있어야 합니다.

DB 보안 그룹을 사용하면 Amazon VPC의 DB 인스턴스를 보호할 수 있습니다. 또한 네트워크 각 서브넷에 출입하는 네트워크 트래픽은 네트워크 ACL를 통해 허용하거나 거부할 수 있습니다. IPsec VPN 연결을 통해 Amazon VPC에 출입하는 모든 네트워크 트래픽은 네트워크 방화벽, 침입 탐지 시스템 등 온프레미스 보안 인프라에서 모니터링할 수 있습니다.

암호화

SSL을 사용하여 애플리케이션과 DB 인스턴스 사이의 연결을 암호화할 수 있습니다. MySQL 및 SQL Server의 경우 RDS가 SSL 인증서를 생성하고, 인스턴스가 프로비저닝되면 DB 인스턴스에 인증서를 설치합니다. MySQL의 경우 연결을 암호화하기 위해 --ssl_ca 파라미터를 사용해 mysql 클라이언트를 시작하고 퍼블릭 키를 참조합니다. SQL Server의 경우 퍼블릭 키를 다운로드하고 Windows 운영 체제로 인증서를 가져오십시오. Oracle RDS는 DB 인스턴스와 함께 Oracle 기본 네트워크 암호화를 사용합니다. 옵션 그룹에 기본 네트워크 암호화 옵션을 추가하고 해당 옵션 그룹을 DB 인스턴스와 연결하기만 하면 됩니다. 암호화된 연결이 설정되면 DB 인스턴스와 애플리케이션 간에 전송되는 데이터는 전송 중에 암호화됩니다. DB 인스턴스에서 암호화된 연결만 허용하도록 요구할 수 있습니다.

데이터베이스에 "상주"해 있는 MySQL 또는 SQL Server 데이터를 암호화해야 하는 경우 애플리케이션이 데이터의 암호화 및 복호화를 관리해야 합니다. Amazon RDS는 Oracle Enterprise Edition에서 지원되는 Oracle Advanced Security 옵션의 기능인 Oracle Transparent Data Encryption(TDE)을 지원합니다. 이 기능은 스토리지에 데이터를 쓰기 전에 자동으로 데이터를 암호화한 뒤에 스토리지에서 읽을 때 다시 자동으로 해독합니다.

Amazon RDS 내에서 SSL 지원은 애플리케이션과 DB 인스턴스 간에 연결을 암호화하기 위한 것으로, DB 인스턴스 자체를 인증하기 위한 용도로 사용해서는 안 됩니다.

SSL은 보안 이점을 제공하지만 SSL 암호화는 컴퓨팅 중심의 작업이며 데이터베이스 연결의 지연 시간을 늘립니다. MySQL에서 SSL을 사용하는 방법에 대한 자세한 내용은 여기에 있는 MySQL 문서를 직접 참조하십시오. SSL이 SQL Server와 연동되는 방식에 대한 자세한 내용은 RDS 사용 설명서에서 자세히 알아볼 수 있습니다.

자동 백업 및 DB 스냅샷

Amazon RDS는 DB 인스턴스 백업 및 복구를 위한 두 가지 방법, 즉 자동 백업 및 데이터베이스 스냅샷(DB 스냅샷)을 제공합니다.

Amazon RDS의 백업 자동화 기능은 기본적으로 활성화되어 있으며, 이를 통해 DB 인스턴스에 대한 지정 시간 복구가 가능합니다. Amazon RDS는 데이터베이스 및 트랜잭션 로그를 백업하고 두 로그를 모두 사용자가 지정한 보존 기간 동안 저장합니다. 이를 통해 DB 인스턴스를 보존 기간 중 어느 시점(초)으로나 복원할 수 있습니다(마지막 5분까지 가능). 자동 백업 보존 기간은 최대 35일로 구성할 수 있습니다.

백업 기간 중에 데이터가 백업되는 동안 스토리지 I/O가 일시적으로 중단될 수 있습니다. 이 I/O 일시 중단 시간은 일반적으로 몇 분 정도 걸립니다. 다중 AZ DB 배포를 사용하면 백업이 예비 복제본에서 수행되므로 이처럼 I/O가 일시 중단되는 문제를 방지할 수 있습니다.

DB 스냅샷은 사용자가 시작한 DB 인스턴스 백업입니다. 이러한 전체 데이터베이스 백업은 사용자가 명시적으로 삭제할 때까지는 Amazon RDS에 저장됩니다. 원하는 경우 언제나 DB 스냅샷에서 새 DB 인스턴스를 생성할 수 있습니다.

복제

Amazon RDS는 서로 다르지만 상호 보완적인 두 가지 복제 기능, 즉 다중 가용 영역(다중 AZ) 배포 및 읽기 전용 복제본을 제공합니다. 다중 AZ 배포와 읽기 전용 복제본을 함께 사용하면 데이터베이스 가용성이 향상되고, 예기치 않은 정전에 대비해 최신 데이터베이스 업데이트를 보호할 수 있습니다. 또한, 단일 DB 인스턴스의 용량을 한도 이상으로 확장해, 읽기 중심의 데이터베이스 워크로드도 원활히 처리할 수 있습니다. 현재 다중 AZ 배포 및 읽기 복제본은 MySQL 데이터베이스 엔진에서 지원됩니다. 자세한 내용은 MySQL용 Amazon RDS를 참조하십시오.

자동 소프트웨어 패치

Amazon RDS는 최신 패치를 통해 배포를 지원하는 관계형 데이터베이스 소프트웨어가 최신 상태로 유지되도록 합니다. 필요한 경우 제어 가능한 유지 관리 기간 중에 패치를 적용합니다. Amazon RDS 유지 관리 기간은 요청이나 필요에 따라 DB 인스턴스를 수정(DB 인스턴스 클래스 확장 등) 하거나 소프트웨어 패치를 적용하는 시기를 조정할 수 있는 기간입니다. "유지 관리" 작업이 특정 주에 예정되어 있는 경우, 사용자가 지정하는 30분의 유지 관리 기간 중 특정 시점에 시작되고 완료됩니다.

스케일 계산 작업(일반적으로 시작에서 완료까지 몇 분 밖에 걸리지 않음) 또는 필수 소프트웨어 패치 적용 시에만 Amazon RDS가 DB 인스턴스를 오프라인으로 설정합니다. 필수 패치 적용은 보안 및 내구성과 관련된 패치에 대해서만 자동으로 예약됩니다. 이러한 패치 적용은 자주 발생하는 것은 아닙니다(일반적으로 몇 달에 한 번). 또한 유지 관리 시간에서 차지하는 비중도 크지 않습니다. DB 인스턴스를 만들 때 기본 주별 유지 관리 기간을 지정하지 않으면 30분이 기본값으로 지정됩니다. 사용자를 대신해 자동으로 유지 관리를 수행하는 시기를 수정하려면 AWS Management Console에서 DB 인스턴스를 수정하거나 ModifyDBInstance API를 사용하면 됩니다. 원하는 경우 각 DB 인스턴스에 서로 다른 기본 유지 관리 기간을 설정할 수 있습니다.

DB 인스턴스를 다중 AZ 배포로 실행하면 유지 관리 작업으로 인한 영향을 더욱 줄일 수 있습니다. Amazon RDS는 1) 대기 목록에서 유지 관리 수행, 2) 대기 목록을 기본 목록으로 승격, 3) 이전에 기본 목록이었지만 현재는 새로운 대기 목록인 유지 관리를 수행하는 단계로 유지 관리를 실행하기 때문입니다.

Amazon RDS DB 인스턴스 삭제 API(DeleteDBInstance)를 실행하면 DB 인스턴스는 삭제 대기 상태가 됩니다. 인스턴스에 더 이상 '삭제' 상태가 표시되지 않으면 제거된 것입니다. 이때부터는 이 인스턴스를 더 이상 접근할 수 없으며, 마지막 스냅샷 복사본를 요청하지 않은 경우 복구할 수 없으며, 어떠한 도구나 API를 통해서도 출력할 수 없게 됩니다.

이벤트 알림

인스턴스가 종료되었거나, 백업이 시작되었거나, 장애 조치가 발생했거나, 보안 그룹이 변경되었거나, 스토리지 공간이 부족한지 여부와 같이 RDS 인스턴스에서 발생할 수 있는 다양한 중요 이벤트의 알림을 받을 수 있습니다. Amazon RDS 서비스는 고객이 구독할 수 있는 카테고리로 이벤트를 그룹화합니다. 따라서 고객은 해당 카테고리의 이벤트가 발생했을 때 이에 대한 알림을 받을 수 있습니다. 구독 가능한 이벤트 카테고리로는 DB 인스턴스, DB 스냅샷, DB 보안 그룹 또는 DB 파라미터 그룹 등이 있습니다. RDS 이벤트는 AWS SNS를 통해 게시되며 고객에게 이메일이나 문자 메시지로 전송됩니다. RDS 알림 이벤트 카테고리에 대한 자세한 내용은 RDS 사용 설명서를 참조하십시오.

Amazon RedShift 보안

Amazon Redshift는 매우 최적화되고 완전히 관리되는 AWS 컴퓨팅 및 스토리지 리소스에서 실행되는 페타바이트급 SQL 데이터 웨어하우스 서비스입니다. 이 서비스의 설계 목적은 신속하게 확장 또는 축소하는 것뿐 아니라 매우 방대한 데이터 세트에서도 쿼리 속도를 —크게 개선하는 것이기도 합니다. 성능을 높이기 위해 Redshift는 컬럼 방식 스토리지, 데이터 압축 및 영역 지도 등의 기술을 사용하여 쿼리 수행에 필요한 IO의 수를 줄입니다. 또한 대량 병렬 처리(MPP) 아키텍처를 사용하므로 SQL 작업을 병렬 처리하고 분산하여 사용 가능한 리소스를 모두 활용할 수 있습니다.

Redshift 데이터 웨어하우스를 생성하면 단일 노드 또는 멀티 노드 클러스터를 프로비저닝하여 클러스터를 구성하게 되는 노드의 유형과 수를 지정합니다. 노드 유형은 각 노드의 스토리지 크기, 메모리 및 CPU를 결정합니다. 각 다중 노드 클러스터에는 리더 노드 1개와 컴퓨팅 노드 2개 이상이 포함됩니다. 리더 노드는 컴퓨팅 노드에서 연결을 관리하고, 쿼리를 구문 분석하고, 실행 계획을 수립하고, 쿼리 실행을 관리합니다. 컴퓨팅 노드는 리더 노드의 안내에 따라 데이터를 저장하고, 계산을 수행하고, 쿼리를 실행합니다. 각 클러스터의 리더 노드는 표준 PostgreSQL 드라이버를 사용하여 ODBC 및 JDBC 엔드포인트를 통해 액세스할 수 있습니다. 컴퓨팅 노드는 격리된 개별 네트워크에서 실행되며 직접 액세스할 수 없습니다.

클러스터를 프로비저닝한 후 일반 SQL 기반 도구 및 비즈니스 인텔리전스 애플리케이션을 사용하여 데이터 세트를 업로드하고 데이터 분석 쿼리를 수행할 수 있습니다.

클러스터 액세스

기본적으로 내가 만든 클러스터는 다른 사용자에게 공개되지 않습니다. Amazon Redshift를 사용하면 데이터 웨어하우스 클러스터에 대한 네트워크 액세스를 제어하도록 방화벽 규칙(보안 그룹)을 구성할 수 있습니다. 또한 Amazon VPC 내에서 Redshift를 실행하여 가상 네트워크에 있는 데이터 웨어하우스 클러스터를 격리하고, 암호화된 IPsec VPN을 사용하여 기존 IT 인프라에 연결할 수도 있습니다.

클러스터를 생성한 AWS 계정은 클러스터에 대해 모든 권한을 가집니다. AWS 계정 내에서 AWS IAM을 사용하여 사용자 계정을 생성하고 해당 계정에 대한 권한을 관리할 수 있습니다. IAM을 사용하면 다른 사용자에게 업무에 필요한 클러스터 작업만 수행할 수 있는 권한을 부여할 수 있습니다.

모든 데이터베이스와 마찬가지로 Redshift를 통해 리소스 수준에서 액세스 권한을 부여할 뿐 아니라 데이터베이스 수준에서 사용 권한을 부여해야 합니다. 데이터베이스 사용자는 데이터베이스에 연결할 수 있는 사용자 계정으로 지정되며 Amazon Redshift에 로그인할 때 인증됩니다. Redshift에서는 테이블 대신 클러스터 단위로 데이터베이스 사용자에게 권한을 부여합니다. 하지만 사용자는 자신의 활동에 의해 생성된 테이블 행의 데이터만 볼 수 있고, 다른 사용자가 생성한 행은 볼 수 없습니다.

데이터베이스 객체를 생성한 사용자는 해당 객체의 소유자입니다. 기본적으로 수퍼유저 또는 객체의 소유자만 객체에 대한 권한을 쿼리, 수정 또는 부여할 수 있습니다. 사용자가 객체를 사용하려면 사용자 또는 해당 사용자가 포함된 그룹에 필요한 권한을 부여해야 합니다. 객체의 소유자만 객체를 수정하거나 삭제할 수 있습니다.

데이터 백업

Amazon Redshift는 클러스터의 모든 컴퓨팅 노드에 데이터를 분산합니다. 두 개 이상의 컴퓨팅 노드에서 클러스터를 실행할 경우 각 노드의 데이터가 다른 노드의 디스크에 항상 미러링되므로 데이터가 손실될 위험이 감소됩니다. 또한 클러스터 내의 노드에 기록된 모든 데이터는 스냅샷을 사용하여 Amazon S3에 지속적으로 백업됩니다. Redshift는 사용자가 지정한 기간(최대 35일) 동안 스냅샷을 보관합니다. 또한 언제든지 사용자 스냅샷을 만들 수 있습니다. 이러한 스냅샷은 모든 기존 시스템 스냅샷을 활용하며 명시적으로 삭제할 때까지 보존됩니다.

Amazon Redshift는 계속해서 클러스터 상태를 모니터링하고 자동으로 실패한 드라이브의 데이터를 다시 복제하며 필요에 따라 노드를 교체합니다. 다시 복제하는 동안 약간의 성능 저하가 발생할 수 있지만, 이러한 모든 작업은 사용자의 별도 조치 없이 자동으로 수행됩니다.

AWS Management Console 또는 Amazon Redshift API를 사용하여 클러스터를 복구하기 위해 시스템 또는 사용자 스냅샷을 사용할 수 있습니다. 클러스터는 시스템 메타데이터가 복구되는 대로 사용이 가능하며 사용자 데이터가 백그라운드에서 스풀링되는 동안 쿼리 실행을 시작할 수 있습니다.

데이터 암호화

클러스터를 생성할 때 클러스터 암호화 옵션을 선택할 수 있습니다. 클러스터에서 암호화를 활성화한 경우 Amazon Redshift는 하드웨어 가속화된 AES-256 암호화를 사용하여 사용자가 생성한 테이블에 모든 데이터를 암호화된 형식으로 저장합니다. 여기에는 디스크에 기록된 모든 데이터와 모든 백업이 포함됩니다. 클러스터에서 암호화를 활성화하면 하드웨어가 가속화되더라도 성능에 영향을 줍니다. 암호화는 백업에도 적용됩니다. 암호화된 스냅샷에서 복원할 경우 새 클러스터도 암호화됩니다.

테이블 로드 데이터 파일을 Amazon S3에 업로드할 때 암호화하려면 Amazon S3 서버 측 암호화를 사용할 수 있습니다. Amazon S3에서 데이터를 로드할 때 COPY 명령은 테이블을 로드하면서 데이터의 암호를 해독합니다.

자동 소프트웨어 패치

Amazon Redshift는 용량 프로비저닝, 클러스터 모니터링, Amazon Redshift 엔진에 패치 및 업그레이드 적용 등을 비롯하여 데이터 웨어하우스를 설정, 운영, 조정하는 모든 작업을 관리합니다. 패치는 지정된 유지 관리 기간 동안에만 적용됩니다.

SSL 연결

AWS 클라우드 내에서 전송 중인 데이터를 보호하기 위해 Amazon Redshift는 하드웨어 가속화 SSL을 사용하여 Amazon S3 또는 Amazon DynamoDB와 COPY, UNLOAD, 백업 및 복원 작업에 대해 통신합니다. 클러스터와 연결된 파라미터 그룹에서 SSL을 지정하여 클라이언트와 클러스터 간의 연결을 암호화할 수 있습니다. 클라이언트에서도 Redshift 서버를 인증하도록 하려면 클라이언트에 SSL 인증서에 대한 퍼블릭 키(.pem 파일)를 설치하고 해당 키를 사용하여 클러스터에 연결할 수 있습니다.

Amazon ElastiCache 보안

Amazon ElastiCache는 클라우드상의 분산 인 메모리 캐시 환경을 손쉽게 설정 및 관리하고 및 확장할 수 있는 웹 서비스입니다. 본 서비스는 더 느린 디스크 기반 데이터베이스에 전적으로 의존하기보다는, 신속하며 관리되는 인 메모리 캐싱 시스템에서 정보를 검색할 수 있는 기능을 지원해 웹 애플리케이션의 성능을 향상시킵니다. Amazon ElastiCache를 사용하면 읽기 중심의 여러 애플리케이션 워크로드(예: 소셜 네트워킹, 게임, 미디어 공유 및 Q&A 포털) 또는 컴퓨팅 중심의 워크로드(예: 추천 엔진)에서 지연 시간을 크게 단축하고 처리량을 상당히 높일 수 있습니다. 캐싱은 중요한 데이터를 메모리에 저장함으로써 액세스 지연 시간을 줄여 애플리케이션 성능을 향상시킵니다. 캐싱된 정보에는 I/O 중심의 데이터베이스 쿼리 결과 또는 컴퓨팅 중심의 계산 결과가 포함될 수 있습니다.

Amazon ElastiCache 서비스는 패치 관리, 장애 탐지, 복구 등 인 메모리 캐시 환경을 위한 시간 소모적인 관리 작업을 자동화합니다. 또한 다른 Amazon Web Services(예: Amazon EC2, Amazon CloudWatch, Amazon SNS)와 연동하여 고성능의 안전하게 관리되는 인 메모리 캐시를 제공합니다. 예를 들어 Amazon EC2에서 실행 중인 애플리케이션은 동일한 리전의 지연 시간이 매우 짧은 Amazon ElastiCache 클러스터에 안전하게 액세스할 수 있습니다.

Amazon ElastiCache 서비스를 사용하여 캐시 클러스터를 생성합니다. 캐시 클러스터는 각각 Memcached 서비스 인스턴스를 실행하는 하나 이상의 캐시 노드 모음입니다. 캐시 노드는 안전한 네트워크에 연결된 RAM의 크기가 고정된 청크입니다. 각 캐시 노드는 Memcached 서비스 인스턴스에서 실행되고, 고유한 DNS 이름과 포트를 갖고 있습니다. 여러 유형의 캐시 노드가 지원되며 연결된 메모리 양은 각각 다릅니다. 특정 수의 캐시 노드 및 각 캐시 노드에 대한 속성을 제어하는 캐시 파라미터 그룹을 사용하여 캐시 클러스터를 설정할 수 있습니다. 캐시 클러스터 하나에 속한 모든 캐시 노드는 노드 유형, 파라미터 그리고 보안 그룹 설정이 모두 동일합니다.

Amazon ElastiCache에서는 캐시 보안 그룹을 사용하여 캐시 클러스터 액세스를 제어할 수 있습니다. 캐시 보안 그룹은 캐시 클러스터에 대한 네트워크 액세스를 제어하는 방화벽 역할을 합니다. 기본적으로 캐시 클러스터에 대한 네트워크 액세스는 꺼져 있습니다. 애플리케이션에 캐시 클러스터에 대한 액세스 권한을 부여하려면 특정 EC2 보안 그룹에 있는 호스트의 액세스를 명시적으로 활성화해야 합니다. 인바운드 규칙이 설정되면 동일한 규칙이 해당 캐시 보안 그룹과 관련된 모든 캐시 클러스터에 적용됩니다.

캐시 클러스터 네트워크 액세스를 허용하려면 캐시 보안 그룹을 생성하고 Authorize Cache Security Group Ingress API 또는 CLI 명령을 사용하여 원하는 EC2 보안 그룹(허용된 EC2 인스턴스를 지정하는)에 권한을 부여합니다. 현재 IP 범위 기반 액세스 제어는 캐시 클러스터에 사용할 수 없습니다. 캐시 클러스터에 액세스하는 모든 클라이언트는 EC2 네트워크 내에 있어야 하며, 캐시 보안 그룹을 통해 승인을 받아야 합니다.

Amazon Simple Queue Service(Amazon SQS) 보안

Amazon SQS는 하나의 애플리케이션 내에 분산 수용되어 있는 구성 요소 사이에 비동기식 메시지 기반 통신을 가능하게 하는 매우 안정적이고 확장 가능한 메시지 큐 서비스입니다. 이 구성 요소는 컴퓨터 또는 Amazon EC2 인스턴스이거나 이 두 가지가 결합된 형태일 수 있습니다. Amazon SQS를 사용하면 구성 요소에서 Amazon SQS 대기열로 언제든지 많은 메시지를 전송할 수 있습니다. 이 메시지는 동일 구성 요소 또는 다른 구성 요소에서 바로 또는 4일 이내에 검색 가능합니다. 메시지는 지속성이 뛰어나며, 각 메시지는 매우 안정적인 고가용성 큐에 영구 저장됩니다. 여러 프로세스가 서로 충돌하지 않고 Amazon SQS 큐를 동시에 읽거나 이 큐에 쓸 수 있습니다.

Amazon SQS에 대한 접근 권한은 AWS 계정 또는 AWS IAM을 이용해 만든 사용자에 따라 부여됩니다. AWS 계정의 인증이 이루어지면 모든 사용자 작업을 모두 이용할 수 있습니다. 그러나 AWS IAM 사용자는 정책을 통해 권한이 부여된 작업과 대기열에만 접근할 수 있습니다. 기본적으로 각 대기열에 대한 접근 권한은 이 대기열을 생성한 AWS 계정으로 제한됩니다. 하지만 SQS에서 생성되거나 사용자가 작성한 정책을 사용하여 대기열에 다른 액세스를 허용할 수 있습니다.

Amazon SQS는 SSL로 암호화된 끝점을 통해 접근할 수 있습니다. 이 암호화된 엔드포인트에는 인터넷과 Amazon EC2에서 모두 액세스할 수 있습니다. Amazon SQS에 저장된 데이터는 AWS에서 암호화하지 않습니다. 그러나 사용자는 Amazon SQS에 업로드하기 전에 데이터를 암호화할 수 있습니다. 단, 대기열을 사용하는 애플리케이션이 검색 시 메시지를 해독하는 방법을 제공하는 경우에 한합니다. Amazon SQS에 전송하기 전에 메시지를 암호화하면 AWS를 포함하여 인증받지 않은 개인이 중요한 고객 데이터에 접근하지 못하도록 보호합니다.

Amazon Simple Notification Service(Amazon SNS) 보안

Amazon Simple Notification Service(Amazon SNS)는 클라우드에서 손쉽게 알림 기능을 설정, 작동 및 전송할 수 있는 웹 서비스입니다. 확장성이 뛰어나고, 유연하며, 비용면에서 효율적인 웹 서비스입니다. 개발자들은 Amazon SNS를 통해 애플리케이션 메시지를 게시하고 이를 가입자들이나 다른 애플리케이션에 즉시 전달할 수 있습니다.

Amazon SNS는 애플리케이션이나 사용자에게 알릴 주제를 만들고, 이러한 주제를 클라이언트가 구독하게 하며, 메시지를 게시하고, 이러한 메시지를 클라이언트가 선택한 프로토콜(HTTP/HTTPS, 이메일 등)을 통해 전달할 수 있는 간편한 웹 서비스를 제공합니다. Amazon SNS는 새로운 정보와 업데이트를 정기적으로 확인하거나 "폴링"할 필요가 없이 “푸시” 방식으로 고객에게 전달합니다. Amazon SNS를 사용하면 복잡한 미들웨어와 애플리케이션을 관리할 필요 없이 신뢰성이 뛰어나고, 이벤트 주도형 워크플로를 갖는 메시징 애플리케이션을 만들 수 있습니다. Amazon SNS는 모니터링 애플리케이션, 워크플로 시스템, 시급한 정보 업데이트, 모바일 애플리케이션 등에 사용할 수 있습니다. Amazon SNS는 액세스 제어 기법을 통해 주제와 메시지를 무단으로 이용하지 못하도록 보호합니다. 주제의 소유자가 주제 별로 일정한 정책을 수립해 주제를 게시하거나 구독할 수 있는 대상을 제한할 수 있습니다. 또한 주제 소유자는 전송 방식을 HTTPS로 지정하여 전송을 암호화할 수도 있습니다.

Amazon SNS의 접근 권한은 AWS 계정 또는 AWS IAM을 이용해 만든 사용자 별로 부여됩니다. AWS 계정의 인증이 이루어지면 모든 사용자 작업을 모두 이용할 수 있습니다. 그러나 AWS IAM 사용자는 정책을 통해 권한이 부여된 작업과 주제에만 액세스할 수 있습니다. 기본적으로 각 주제에 대한 접근 권한은 이 주제를 생성한 AWS 계정으로 제한됩니다. 하지만 SNS에서 생성되거나 사용자가 작성한 정책을 사용하여 SNS에 다른 액세스를 허용할 수 있습니다.

Amazon Simple Workflow Service(Amazon SWF) 보안

Amazon Simple Workflow Service(SWF)를 사용하면 분산된 구성 요소에 대해 작업을 조정하는 애플리케이션을 쉽게 구축할 수 있습니다. Amazon SWF를 사용하면 애플리케이션의 여러 처리 단계를, 분산된 애플리케이션에서 작업을 수행하는 "작업"으로 구조화할 수 있으며, Amazon SWF는 이러한 작업을 안정적이고 확장 가능하게 조정합니다. Amazon SWF는 개발자의 애플리케이션 논리에 기초하여 태스크 실행 종속성, 일정 및 동시성을 관리합니다. 이 서비스는 작업을 저장하고, 이러한 작업을 애플리케이션 구성 요소에 보내며, 진행 상황을 추적하여 최신 상태를 확인합니다.

Amazon SWF가 제공하는 간단한 API 호출 기능은 모든 종류의 언어로 작성된 코드로 실행될 수 있으며, EC2 인스턴스는 물론 인터넷에 액세스할 수 있는 전 세계 모든 장소의 모든 컴퓨터에서 실행 가능합니다. Amazon SWF는 애플리케이션 호스트와 상호 작용하는 코디네이션 허브 역할을 합니다. 사용자는 관련 작업과 함께 워크플로를 만들고 적용할 조건 논리가 있는 경우 지정하여 Amazon SWF에 저장합니다.

Amazon SWF 액세스 권한은 AWS 계정에 따라 또는 AWS IAM을 사용하여 사용자에 따라 부여됩니다. 결정자, 활동 작업자, 워크플로우 관리자 등 워크플로우의 실행에 참여하는 모든 행위자는 Amazon SWF 리소스를 소유한 AWS 계정의 IAM 사용자여야 합니다. 개발자는 다른 AWS 계정에 연결된 사용자에게 자신의 Amazon SWF 워크플로우에 대한 액세스 권한을 부여할 수 없습니다. 그러나 AWS IAM 사용자는 정책을 통해 권한이 부여된 워크플로우와 리소스에만 액세스할 수 있습니다.

Amazon Simple Email Service(Amazon SES) 보안

Amazon Simple Email Service(Amazon SES)는 기업 및 개발자가 대량의 트랜잭션 이메일 전송을 쉽게 처리할 수 있게 해주는 확장성이 우수하고 비용 효율적인 서비스입니다. Amazon SES는 사내 이메일 솔루션을 구축하거나 타사 이메일 서비스를 라이센싱, 설치 및 운영하는 데 따르는 복잡성과 비용을 없애줍니다. Amazon SES 서비스는 다른 AWS 서비스와 통합되기 때문에 Amazon EC2와 같은 서비스에서 호스팅되는 애플리케이션에서 이메일을 쉽게 전송할 수 있습니다.

안타깝게도 원치 않는 사람들에게 의도적으로 대용량 이메일 또는 스팸을 보내고 다른 사람의 ID를 스푸핑하여 위장하려는 사람들이 있습니다. 이러한 문제를 완화하기 위해 Amazon SES에서는 새로운 사용자에게 이메일 또는 도메인이 자신의 소유인지를 확인하도록 하여 다른 사용자의 도용을 방지합니다. 또한 AWS에서는 도메인 확인 상태를 주기적으로 검토하여 더 이상 유효하지 않을 경우 확인을 해지합니다.

Amazon SES는 사전 대응적인 조치를 취하여 의심되는 콘텐츠를 받아보지 않도록 차단합니다. 따라서 ISP는 항상 필요한 정보를 담은 이메일을 받게 되므로, Amazon SES 서비스를 거친 이메일을 신뢰하게 됩니다. 이러한 기능은 당사의 서비스를 이용하는 모든 발신자의 도달 가능성 및 신뢰성을 최대화합니다. 아래는 몇 가지 준비된 보호 조치입니다.

- ISP는 갑작스럽게 이메일 양이 증가하면 스팸이 늘어나는 것으로 여겨서 이메일을 차단하여 대응하는 경우도 흔히 있습니다. 이 위험을 피할 수 있도록 Amazon SES는 목표 볼륨에 도달하기 전까지 서비스를 통해 전송할 수 있는 이메일 양을 자동으로 늘립니다.
- Amazon SES는 콘텐츠 필터링 기술을 사용하여 스팸이나 맬웨어를 포함한 메시지를 감지하여 발신 전에 미리 차단합니다.
- Amazon SES는 주요 ISP의 수신 거부 피드백 루프를 유지관리합니다. 수신 거부 피드백 루프는 수신자가 스팸이라고 표시한 이메일을 가리킵니다. Amazon SES에서는 이메일 캠페인을 위한 이러한 전송 Metric을 이용할 수 있기 때문에, 전송 전략을 추진하는 데 도움이 됩니다.

Amazon SES는 SMTP(Simple Mail Transfer Protocol)를 사용하여 이메일을 보냅니다. SMTP는 자체적으로 인증을 제공하지 않으므로, 스패머가 실제 오리진을 숨기고 다른 사용자가 오리진인 것처럼 위장하여 이메일 메시지를 보낼 수 있습니다. 대부분의 ISP는 이메일이 합법적인지 여부를 평가하기 위한 조치를 완료했습니다. ISP가 고려하는 그런 작업으로는 이메일 인증이 있습니다. 이메일 인증에서 발신자는 자신이 이메일을 보내고 있는 계정의 소유자라는 증거를 제공해야 합니다. 경우에 따라 ISP는 인증되지 않은 이메일의 전달을 거부합니다. Amazon SES는 이메일이 합법적인지 여부를 확인하기 위해 ISP가 사용하는 세 가지 인증 메커니즘(SPF, 발신자 ID, DKIM 등)을 지원합니다. AWS는 발송률을 최적화하기 위해 SES 고객이 이러한 표준을 따를 것을 권장합니다.

- SPF(Sender Policy Framework)는 이메일 메시지를 추적하여 발송된 시스템으로 다시 보내는 기능을 제공합니다. SPF를 준수하기 위해 이메일 발신자는 보내는 도메인의 ID를 설정하는 하나 이상의 DNS 레코드를 게시합니다. 이러한 DNS 레코드는 일반적으로 TXT(텍스트)로 지정되며, 이메일을 보낼 수 있는 권한이 부여된 일련의 호스트를 식별합니다. DNS 레코드가 생성되어 게시되면 ISP는 IP 주소를 SPF 레코드에 지정된 IP 주소 집합과 비교하여 호스트를 인증할 수 있습니다. SPF에 대한 자세한 내용은 www.openspf.org 및 RFC 4408을 참조하십시오.
- 발신자 ID는 SPF와 비슷한 인증 시스템입니다. SPF와 마찬가지로 발신자 ID는 발신자와 ISP 간의 협력을 통해 이메일 메시지를 발신된 시스템으로 다시 추적할 수 있는지 확인합니다. 발신자 ID를 준수하기 위해 이메일 발신자는 보내는 도메인의 ID를 설정하는 하나 이상의 DNS 레코드를 게시합니다. 발신자 ID에 대한 자세한 내용은 http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx and RFC 4406을 참조하십시오.
- DomainKeys Identified Mail(DKIM)은 발신자가 디지털 서명을 사용하여 이메일 메시지에 서명하고 ISP가 해당 서명을 사용하여 메시지가 합법적인지를 확인할 수 있도록 해주는 표준입니다. 메시지를 수신하는 ISP는 발신자의 DNS 레코드에 게시된 퍼블릭 키로 암호화 서명을 디코딩하여 메시지가 인증되었는지를 확인할 수 있습니다. DKIM 규격 ISP를 사용하여 메일의 발송률을 높이려면 DKIM을 사용하여 이메일 메시지에 서명하면 됩니다. DKIM에 대한 자세한 내용은 http://www.dkim.org/를 참조하십시오.

Amazon SES SMTP 인터페이스를 사용하려면 먼저 SMTP 사용자 이름과 암호를 만들어야 합니다. SMTP 사용자 이름과 암호는 AWS 액세스 키 ID 및 보안 액세스 키와 다릅니다. SMTP 자격 증명을 가져온 후 이메일 클라이언트 애플리케이션을 사용하여 Amazon SES를 통해 이메일을 보낼 수 있습니다. 단, 이메일 클라이언트 애플리케이션이 SMTP를 통해 통신하고 TLS(전송 계층 보안)를 사용하여 SMTP 엔드포인트에 연결할 수 있어야 합니다. 이메일 클라이언트를 구성하려면 SMTP 사용자 이름 및 암호와 함께 Amazon SES SMTP 인터페이스 호스트 이름(email-smtp.us-east-1.amazonaws.com) 및 포트 번호를 제공해야 합니다.

Amazon SES SMTP 엔드포인트(email-smtp.us-east-1.amazonaws.com)에서는 TLS를 사용하여 모든 연결을 암호화해야 합니다. Amazon SES는 암호화된 연결 설정을 위한 두 가지 메커니즘 즉, STARTTLS 및 TLS 래퍼를 지원합니다. 소프트웨어에서 STARTTLS 또는 TLS 래퍼를 지원하지 않는 경우 오픈 소스 stunnel("보안 터널") 프로그램을 사용하여 암호화된 연결을 설정한 다음 보안 터널을 사용하여 Amazon SES SMTP 엔드포인트에 연결합니다.

Amazon SWF에 대한 액세스 권한은 AWS 계정 또는 AWS IAM을 이용해 만든 사용자에 따라 부여됩니다. 그러나 AWS IAM 사용자는 정책을 통해 권한이 부여된 관리 기능에만 액세스할 수 있습니다.

Amazon Elastic Transcoder 서비스 보안

Amazon Elastic Transcoder 서비스는 일반적으로 미디어 파일을 다른 형식, 크기 또는 품질로 변환하는 복잡한 프로세스를 간소화하고 자동화합니다. Elastic Transcoder 서비스는 SD(표준 화질) 또는 HD(고화질) 비디오 파일과 오디오 파일을 모두 변환합니다. 또한 Amazon S3 버킷의 입력을 읽고, 트랜스코딩하고, 결과 파일을 다른 S3 버킷에 씁니다. 입력과 출력에 동일한 버킷을 사용할 수 있으며, 버킷은 아무 AWS 리전에나 있어도 됩니다. Elastic Transcoder는 다양한 웹 형식, 소비자 형식 및 프로페셔널 형식의 입력 파일을 사용합니다. 출력 파일 형식에는 H.264 또는 VP8 비디오와 AAC 또는 Vorbis 오디오를 저장하는 MP4, TS, WebM 컨테이너 형식이 있습니다.

하나 이상의 입력 파일로 시작한 후 각 파일에 대해 트랜스코딩 파이프라인이라는 워크플로우 유형의 트랜스코딩 작업을 만들어야 합니다. 파이프라인을 생성할 때 입력 및 출력 버킷과 IAM 역할을 지정합니다. 각 작업은 트랜스코딩 프리셋이라는 미디어 변환 템플릿을 참조해야 하며, 하나 이상의 출력 파일을 생성합니다. 프리셋은 Elastic Transcoder에 특정 입력 파일을 처리할 때 사용할 설정을 알려 줍니다. 프리셋을 생성할 때 샘플 비율, 비트 속도, 해상도(출력 높이 및 너비), 참조 및 키 프레임 수, 비디오 비트 속도, 일부 썸네일 생성 옵션 등을 비롯한 다양한 설정을 지정할 수 있습니다.

작업은 가능한 한 제출된 순서로 시작되지만, 그렇지 않은 경우도 있습니다. 또한 여러 작업이 병렬로 수행되고 복잡도가 다르므로 작업이 완료되는 순서는 정해져 있지 않습니다. 필요한 경우 파이프라인을 일시 정지했다가 다시 시작할 수 있습니다.

Elastic Transcoder는 각 작업을 시작하고 마칠 때 그리고 오류 또는 경고 조건이 감지되었음을 알려야 할 때 SNS 알림을 사용하도록 지원합니다. SNS 알림 파라미터는 각 파이프라인에 연결됩니다. 또한 [List Jobs By Status] 기능을 사용하여 지정된 상태(예: Completed)를 가진 모든 작업을 찾거나 [Read Job] 기능을 사용하여 특정 작업에 대한 자세한 정보를 검색할 수 있습니다.

다른 모든 AWS 서비스와 마찬가지로 Elastic Transcoder는 AWS Identity and Access Management(IAM)과 통합되어 있으므로, Elastic Transcoder에 필요한 다른 AWS 리소스 및 서비스(Amazon S3 버킷, Amazon SNS 주제 등)에 대한 액세스를 제어할 수 있습니다. 기본적으로 IAM 사용자는 Elastic Transcoder 또는 Elastic Transcoder에서 사용되는 리소스에 액세스할 수 없습니다. IAM 사용자가 Elastic Transcoder를 사용하도록 허용하려면 해당 사용자에게 권한을 명시적으로 부여해야 합니다.

Amazon Elastic Transcoder는 대상 API에 대한 모든 요청을 인증받도록 하여 허가받은 프로세스 또는 사용자만 Amazon Transcoder 파이프라인 및 프리셋을 생성, 변경 또는 삭제할 수 있도록 합니다. 요청에서 계산된 HMAC-SHA256 서명과 사용자의 비밀 키에서 파생된 키를 사용하여 요청에 서명합니다. 또한, Amazon Elastic Transcoder API는 SSL로 암호화된 엔드포인트를 통해서만 액세스할 수 있습니다.

Amazon S3에서는 Amazon S3 리전의 여러 시설에 있는 여러 디바이스에 미디어 파일을 중복으로 저장하여 내구성을 제공합니다. 사용자가 실수로 미디어 파일을 삭제하지 않도록 보호하기 위해 S3의 버전 관리 기능을 사용하여 Amazon S3 버킷에 저장된 모든 객체의 모든 버전을 유지, 검색 및 복원할 수 있습니다. Amazon S3 버전 관리의 MFA 삭제 기능을 사용하여 버전을 추가로 보호할 수 있습니다. S3 버킷에 활성화되면 각 버전 삭제 요청에는 멀티 팩터 인증 디바이스의 6자리 코드와 일련 번호가 포함되어 있어야 합니다.

Amazon CloudWatch 보안

Amazon CloudWatch는 AWS 클라우드 자원에 대한 모니터링 기능을 제공하는 웹 서비스로, Amazon EC2에서 시작합니다. 이 서비스는 CPU 사용률, 디스크 읽기/쓰기, 네트워크 트래픽과 같은 메트릭을 포함한 자원 이용률, 작동 성능, 전반적인 수요 패턴을 파악할 수 있는 기능을 제공합니다. 고객은 CloudWatch 경보를 설정하여 특정 임계값에 도달한 경우 알리거나 Auto-Scaling이 활성화된 경우 EC2 인스턴스 추가 또는 제거와 같은 다른 자동화된 작업을 수행할 수 있습니다.

모든 AWS 서비스와 마찬가지로 Amazon CloudWatch는 제어 API에 대한 모든 요청을 인증하여 인증받은 사용자만 CloudWatch에 액세스하고 관리할 수 있도록 합니다. 요청 메시지는 이 요청 메시지 및 사용자의 개인 키에서 계산한 HMAC-SHA1 서명으로 서명합니다. 또한, Amazon CloudWatch 제어 API는 SSL로 암호화된 끝점을 통해서만 접근할 수 있습니다.

AWS IAM을 사용하여 AWS 계정에 사용자를 생성하고, 이 사용자들이 호출할 수 있는 CloudWatch 작업을 제어함으로써 Amazon CloudWatch에 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 엣지의 글로벌 네트워크를 사용해 동적, 정적 및 스트리밍 콘텐츠를 전송합니다. 고객의 객체에 대한 요청이 가장 가까운 엣지로 자동 라우팅되므로 콘텐츠 전송 성능이 뛰어납니다. Amazon CloudFront는 Amazon S3, Amazon EC2, Amazon 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 허가받은 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 CloudFront 의 제어 API는 SSL로 암호화된 끝점을 통해서만 접근할 수 있습니다.

Amazon CloudFront의 에지에서는 데이터의 지속성을 보장하지 않습니다. 이 서비스는 빈번하게 요청되지 않는 객체를 에지에서 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 기능에는 다음의 두 가지 구성 요소가 있습니다. 첫 번째는 Amazon CloudFront 엣지에서 Amazon S3에 있는 고객 소유 객체에 액세스하는 방법을 제어합니다. 두 번째는 Amazon CloudFront 엣지에서 인터넷의 최종 사용자에게 콘텐츠를 전달하는 방법을 제어합니다. 또한 CloudFront의 프라이빗 콘텐츠 기능을 타사 지리적 위치 제품과 함께 사용하여 웹 애플리케이션에 지리적 제한 로직을 추가함으로써 최종 사용자의 지리적 위치에 따라 콘텐츠에 대한 액세스를 차단하도록 사용자 지정할 수 있습니다.

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 엣지에서 객체를 다운로드 할 수 있는 사용자를 제한하기 위해 이 서비스는 서명된 URL 인증 시스템을 사용합니다. 이 시스템을 사용하려면 먼저 개인 키와 공개 키 쌍을 만든 후 AWS 웹 사이트를 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 RSA SHA1 인코딩을 계산하고 개인 키로 문서에 서명합니다. 넷째, 고객 소유의 객체를 조회할 때 인코딩된 정책 자료와 서명을 쿼리 문자열 매개 변수로 포함시킵니다. Amazon CloudFront가 요청을 받으면 공개 키를 사용하여 서명을 디코딩합니다. Amazon CloudFront는 정책 문서가 유효하고 서명이 일치하는 요청만 처리합니다.

콘텐츠 비공개는 CloudFront 배포 기능 설정 시 선택해야 하는 옵션 기능입니다. 이 기능을 선택하지 않고 전달한 콘텐츠는 공개적으로 누구나 읽을 수 있습니다.

Amazon CloudFront는 또한 사용자에게 전달되는 콘텐츠를 인증할 수 있도록 암호화된 연결(HTTPS)을 통해 콘텐츠를 전달하는 기능을 제공합니다. Amazon CloudFront는 기본적으로 HTTP 및 HTTPS 프로토콜을 통해 요청을 수락합니다. 필요한 경우, 모든 요청에 대해 HTTPS를 요구하고 HTTP 요청은 모두 허용하지 않도록 Amazon CloudFront를 설정할 수도 있습니다.

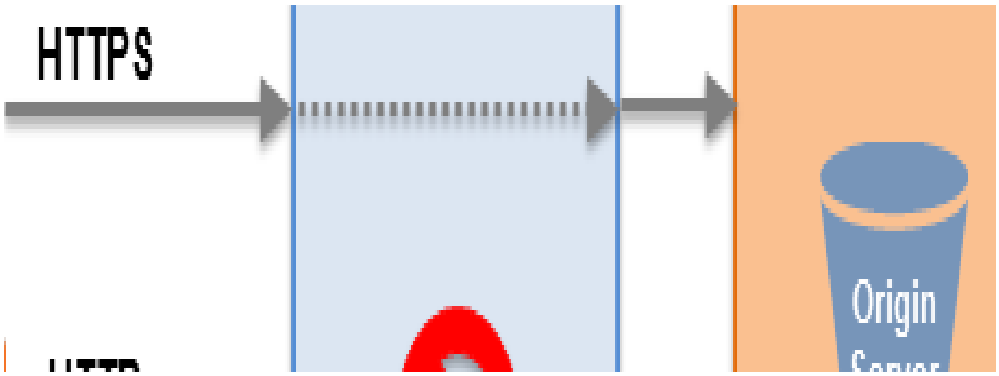


그림 6: Amazon CloudFront 암호화된 전송

URL에 CloudFront 배포 도메인 이름을 사용하거나 자신의 도메인 이름을 사용하여 최종 사용자에게 HTTPS를 통해 콘텐츠를 전달할 수 있습니다. 고유의 도메인 이름을 사용하려면 SSL 인증서를 AWS IAM 인증서 스토리지에 업로드한 후 해당 인증서를 CloudFront 배포에 연결해야 합니다. HTTPS 요청의 경우, Amazon CloudFront에서는 또한 HTTPS를 활용하여 Amazon S3에서 객체를 검색하여 객체를 전송할 때마다 암호화합니다.

Amazon CloudFront 액세스 로그에는 콘텐츠 요청에 대한 종합적인 정보(예: 요청한 객체, 요청 날짜 및 시간, 요청을 처리하는 엣지, 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.

Amazon Elastic MapReduce(Amazon EMR) 보안

Amazon Elastic MapReduce(Amazon EMR)는 대량의 데이터를 쉽고 경제적으로 처리할 수 있도록 지원하는 웹 서비스입니다. 본 서비스는 호스팅되는 하둡 프레임워크를 사용합니다. 하둡 프레임워크는 Amazon EC2와 Amazon S3의 웹 스케일 인프라 상에서 실행됩니다.

먼저 입력 데이터와 데이터 처리 애플리케이션을 Amazon S3에 업로드합니다. 그러면 Amazon Elastic MapReduce에서 지정된 수의 Amazon EC2 인스턴스를 시작합니다. 서비스가 작업 흐름을 실행하면서, Amazon S3의 입력 데이터를 Amazon EC2 실행 인스턴스로 가져옵니다. 작업 흐름이 완료되면, Amazon Elastic MapReduce는 출력 데이터를 Amazon S3로 전달합니다. 그러면 Amazon S3에서 고객은 출력 데이터를 검색하거나 이 데이터를 다른 작업 흐름에서 입력 데이터로 사용할 수 있습니다.

Amazon Elastic MapReduce는 API에 대한 모든 요청을 허가하여 허가받은 사용자만 작업 흐름을 생성, 조회, 종료할 수 있게 합니다. 요청 메시지는 이 요청 메시지 및 사용자의 개인 키에서 계산한 HMAC-SHA1 서명으로 서명합니다. Amazon Elastic MapReduce는 웹 서비스 API 및 콘솔에 대한 접근을 위해 SSL 끝점을 제공합니다.

고객을 대신하여 작업 흐름을 시작할 경우 Amazon Elastic MapReduce는 마스터 노드와 슬레이브 노드에 대해 각각 하나씩 두 개의 Amazon EC2 보안 그룹을 설정합니다. 마스터 보안 그룹에는 통신을 위해 열려 있는 포트가 있어, 이것을 사용하여 서비스를 실시하고 있습니다. 또한 SSH 포트가 열려 있고, 시작할 때 지정한 키를 사용하여 SSH를 인스턴스에 허용할 수 있습니다. 슬레이브는 다른 보안 그룹에서 시작합니다. 이 보안 그룹은 마스터 인스턴스와의 상호작용만 허용합니다. 기본적으로 두 보안 그룹 모두 다른 고객에게 속한 Amazon EC2 인스턴스와 같은 외부 소스가 액세스하지 못하도록 설정되어 있습니다. 계정에 보안 그룹이 있는 경우, 표준 EC2 도구나 대시보드를 사용하여 보안 그룹을 다시 설정할 수 있습니다. Amazon Elastic MapReduce는 고객의 입출력 데이터 세트를 보호하기 위해 Amazon S3와 주고받는 데이터를 SSL을 사용하여 전송합니다.

보안을 강화를 위해, Amazon S3에 입력 데이터를 업로드하기 전에 일반 데이터 암호화 도구를 사용하여 이러한 입력 데이터를 암호화할 수 있습니다. 데이터를 업로드하기 전에 암호화할 경우 Amazon Elastic MapReduce가 Amazon S3에서 데이터를 가져올 때 작업 흐름의 시작 부분에 암호 해독 단계를 추가해야 합니다.

Amazon Route 53 보안

Amazon Route 53는 신뢰할 수 있는 DNS 시스템입니다. 신뢰할 수 있는 DNS 시스템은 공용 DNS 이름을 관리하는 데 사용할 수 있는 업데이트 메커니즘을 제공합니다. 이 메커니즘을 통해 DNS 시스템은 DNS 쿼리에 응답하고 도메인 이름을 IP 주소로 변환합니다. 그러면 컴퓨터가 서로 통신할 수 있게 됩니다. 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 두 가지 DNS 기능을 수행합니다. 즉, 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. 또한 가중치 기반 라운드 로빈(WRR), 지연 시간 기반 라우팅(LBR) 및 DNS 장애 조치를 활용하여 시스템에서 회신할 DNS 응답을 동적으로 결정하는 라우팅 정책을 관리할 수 있습니다.

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 IPv4 라우팅과 IPv6 라우팅을 모두 지원합니다.

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.

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 CloudSearch 보안

Amazon CloudSearch는 클라우드의 완전 관리형 서비스로, 이를 이용해 웹 사이트 또는 애플리케이션을 위한 검색 솔루션을 쉽게 설치, 관리 및 확장할 수 있습니다. Amazon CloudSearch를 사용하면 웹 페이지, 문서 파일, 포럼 게시물 또는 제품 정보와 같은 방대한 데이터 모음을 검색할 수 있습니다. 검색 전문가가 아닐지라도 하드웨어 프로비저닝, 설치 및 유지 관리에 관한 걱정 없이 웹 사이트에 검색 기능을 빠르게 추가할 수 있습니다. 데이터 용량과 트래픽의 변화에 따라 Amazon CloudSearch는 고객의 요구에 맞춰 자동으로 확장합니다.

Amazon CloudSearch 도메인은 검색할 데이터 모음, 검색 요청을 처리하는 검색 인스턴스, 데이터를 인덱싱하고 검색하는 방법을 제어하는 구성 등을 캡슐화합니다. 검색 가능하게 만들 데이터 집합에 대해 별도의 검색 도메인을 생성합니다. 각 도메인에 대해 인덱스에 포함할 필드를 설명하는 인덱싱 옵션, 인덱싱 옵션을 사용할 방법, 도메인별 불용어, 어간 및 동의어를 정의하는 텍스트 옵션, 검색 결과 순위 지정 방법을 사용자 지정하는 데 사용할 수 있는 차수 식, 도메인의 문서 및 검색 엔드포인트에 대한 액세스를 제어하는 액세스 정책 등을 구성합니다.

권한 있는 호스트만 문서를 제출하고 검색 요청을 보낼 수 있도록 검색 도메인의 엔드포인트에 대한 액세스는 IP 주소별로 제한됩니다. IP 주소 권한 부여는 문서 및 검색 엔드포인트에 대한 액세스를 제어하는 데에만 사용됩니다. 표준 AWS 인증을 사용하여 모든 Amazon CloudSearch 구성 요청을 인증해야 합니다.

Amazon CloudSearch는 구성, 검색 및 문서 서비스에 액세스하기 위해 별도의 엔드포인트를 제공합니다.

- 구성 서비스는 일반 엔드포인트인 cloudsearch.us-east-1.amazonaws.com을 통해 액세스됩니다.
- 문서 서비스 엔드포인트는 인덱싱을 위해 도메인에 문서를 제출하는 데 사용되며 도메인별 엔드포인트인 http://doc-domainname-domainid.us-east-1.cloudsearch.amazonaws.com을 통해 액세스됩니다.
- 검색 엔드포인트는 도메인에 대한 검색 요청을 제출하는 데 사용되며 도메인별 엔드포인트인 http://search-domainname-domainid.us-east-1.cloudsearch.amazonaws.com 을 통해 액세스됩니다.

고정 IP 주소가 없는 경우 IP 주소가 변경될 때마다 컴퓨터를 다시 인증해야 합니다. IP 주소가 동적으로 할당되는 경우 해당 주소가 네트워크 상의 다른 컴퓨터와 공유될 수도 있습니다. 즉, IP 주소를 승인하면 해당 IP 주소를 공유하는 모든 컴퓨터에서 검색 도메인의 문서 서비스 엔드포인트에 액세스할 수 있습니다.

모든 AWS 서비스와 마찬가지로 Amazon CloudSearch는 제어 API에 대한 모든 요청을 인증하여 인증받은 사용자만 CloudSearch 도메인에 액세스하고 관리할 수 있도록 합니다. 요청에서 계산된 HMAC-SHA1 또는 HMAC-SHA256 서명과 사용자의 AWS 보안 액세스 키를 사용하여 AWS 요청에 서명합니다. 또한, Amazon CloudSearch의 제어 API는 SSL로 암호화된 엔드포인트를 통해 액세스할 수 있습니다. AWS IAM을 사용하여 AWS 계정 아래에 사용자를 생성하고 이러한 사용자가 수행할 권한이 있는 CloudSearch 작업을 제어하는 방식으로 Amazon CloudSearch 관리 기능에 대한 액세스를 제어할 수 있습니다.

AWS Elastic Beanstalk 보안

AWS Elastic Beanstalk는 애플리케이션에 대한 용량 프로비저닝, 로드 밸런싱 및 Auto Scaling 기능을 자동화하는 배포 및 관리 도구입니다. 배포 가능한 코드를 업로드하면 AWS Elastic Beanstalk이 나머지 작업을 수행합니다. 애플리케이션이 실행되면 Elastic Beanstalk는 모니터링, 애플리케이션 버전 배포, 로그 파일 스냅샷, 상태 확인 등과 같은 관리 작업을 자동화하고, 애플리케이션이 계속 실행될 수 있도록 하기 위해 상태가 좋지 않다고 간주되는 리소스(예: EC2 인스턴스)를 교체합니다.

AWS Elastic Beanstalk는 Amazon EC2, Amazon RDS, Elastic Load Balancing, Auto Scaling, Amazon S3, Amazon SNS 같은 여러 AWS 기능과 서비스를 사용하여 애플리케이션을 완벽하게 실행하는 환경을 만듭니다. 또한 안전하게 구성된 AMI를 사용하여 하나 이상의 EC2 인스턴스를 자동으로 시작하고, S3에 애플리케이션을 저장하고, 로드 밸런싱 및 Auto-Scaling을 시작하고, 애플리케이션 환경의 상태를 모니터링합니다.

애플리케이션에서 AWS 서비스 API(예: DynamoDB 또는 CloudWatch)를 호출해야 하는 경우 Elastic Beanstalk 환경 변수를 사용하여 AWS 액세스 키와 비밀 키를 애플리케이션에 전달하거나 IAM 역할을 사용하여 임시 자격 증명을 생성할 수 있습니다. IAM 역할을 생성하면 애플리케이션에서 해당 역할에 연결된 인스턴스 프로필을 사용하여 AWS API를 호출하기 위한 임시 보안 자격 증명을 가져옵니다. 애플리케이션을 AWS Elastic Beanstalk에 배포하면 Elastic Beanstalk는 지정된 인스턴스 프로필을 사용하여 EC2 인스턴스를 시작합니다. 애플리케이션은 EC2 인스턴스에서 사용할 수 있는 역할 자격 증명을 사용합니다. 애플리케이션은 Instance Meta Data Service(IMDS)에서 역할 자격 증명을 가져온 다음, 해당 자격 증명을 사용하여 AWS 서비스에 대한 API 호출을 수행합니다. IAM 역할을 사용할 경우 보안상의 이점은 하루에 여러 번 임시 자격 증명이 자동으로 교체된다는 것입니다.

추가 계층의 개인 정보 보호를 위해 Virtual Private Cloud(VPC) 내에서 Elastic Beanstalk 애플리케이션을 실행할 수도 있습니다. AWS 클라우드에서 프라이빗 가상 네트워크를 정의하고 프로비저닝한 다음 VPN 연결을 사용하여 기업 네트워크에 연결할 수 있습니다. 이렇게 하면 Elastic Beanstalk에서 더욱 다양한 애플리케이션을 실행할 수 있습니다. 예를 들어, 문제 티켓 애플리케이션 또는 Elastic Beanstalk의 보고 사이트와 같은 인트라넷 애플리케이션을 실행할 수 있습니다.

Elastic Beanstalk가 애플리케이션의 프로비저닝과 배포를 자동화하더라도, Elastic Beanstalk 콘솔을 사용하여 AWS 리소스에 대한 기본 설정을 수동으로 재정의할 수 있으며 기본 인프라에 대한 제어를 원하는 만큼 유지할 수 있습니다. 또한 다음과 같은 다양한 모니터링 및 보안 기능을 구성할 수 있습니다.

- 로드 밸런서에서 HTTPS를 활성화하여 애플리케이션과 양방향으로 데이터의 보안 전송 적용
- 애플리케이션 상태가 바뀌거나 애플리케이션 서버가 추가 또는 제거되면 Amazon Simple Notification Service(Amazon SNS)를 통해 이메일 알림 수신
- HTTPS를 알림 프로토콜로 지정하여 이메일 알림의 보안 전송 활성화
- AWS 리소스에 대해 인증하기 위해 애플리케이션에 필요한 AWS 보안 액세스 키를 포함하여 애플리케이션 서버 설정 조정 및 환경 변수 전달
- 즉각적이고 직접적인 문제 해결을 위해 Amazon EC2 인스턴스에 대한 보안 로그인 액세스 활성화
- 고객의 EC2 인스턴스 로그 파일을 애플리케이션과 연결된 S3 버킷으로 매시간 복사하는 로그 파일 로테이션 활성화
- Amazon CloudWatch의 모니터링 지표(평균 CPU 사용률, 요청 수, 평균 지연 시간 등) 보기

모든 AWS Elastic Beanstalk 엔드포인트는 액세스에 HTTPS 프로토콜을 사용합니다. IAM 정책을 사용하여 Elastic Beanstalk 서비스에 대한 액세스를 제어할 수 있습니다. AWS Elastic Beanstalk에 대한 액세스 권한 부여 프로세스를 단순화하기 위해 AWS IAM 콘솔에서 정책 템플릿 중 하나를 사용하여 시작할 수 있습니다. AWS Elastic Beanstalk는 읽기 전용 액세스 템플릿과 모든 권한 템플릿이라는 두 가지 템플릿을 제공합니다. 읽기 전용 템플릿은 AWS Elastic Beanstalk 리소스에 대한 읽기 액세스를 허용합니다. 모든 권한 액세스 템플릿은 모든 AWS Elastic Beanstalk 작업에 대한 모든 권한뿐 아니라 Elastic Load Balancing 및 Auto Scaling과 같은 종속 리소스를 관리하는 권한도 부여합니다. 또한 AWS 정책 생성기를 사용하여 애플리케이션, 애플리케이션 버전 및 환경과 같은 특정 AWS Elastic Beanstalk 리소스에 대한 권한을 허용하거나 거부하는 사용자 지정 정책을 생성할 수 있습니다.

AWS CloudFormation 보안

AWS CloudFormation은 애플리케이션을 실행하는 데 필요한 AWS 리소스의 기준 구성을 기록하여 이러한 리소스를 순서에 따라 예측 가능한 방식으로 프로비저닝하고 업데이트할 수 있는 프로비저닝 도구입니다. 애플리케이션을 실행하는 데 필요한 AWS 리소스는 템플릿이라는 간단한 텍스트 파일에 정의합니다. 템플릿이란 같은 리소스 스택의 동일한 사본을 작성하기 위해 반복적으로 사용하거나 새로운 스택을 시작하기 위한 기초로 사용할 수 있는 파일입니다. 파라미터를 사용하여 Amazon EC2 AMI, EBS 스냅샷 이름, RDS 데이터베이스 크기 등의 리전별 인프라 변형을 캡처하고 제어할 수 있습니다. 파라미터를 사용하면 스택을 생성할 때 템플릿에 전달할 수 있는 값을 선언할 수 있습니다. 또한 파라미터는 템플릿 자체에 저장하면 안 되는 사용자 이름 및 암호와 같은 민감한 정보를 지정하기 위한 효과적인 방법입니다.

AWS CloudFormation을 사용하면 기존 리소스의 속성 업데이트와 같은 간단한 변경을 수행하거나 스택에서 리소스 추가 또는 제거와 같은 복잡한 변경을 수행할 수 있습니다. 스택에 대한 변경은 템플릿을 수정하고 스택을 업데이트하여 수행됩니다. AWS CloudFormation은 현재 템플릿과 새로운 템플릿 간의 차이를 이해하며 그에 따라 스택을 수정합니다.

CloudFormer 도구를 사용하여 AWS 리소스 및 관련 종속성 또는 런타임 파라미터에 대해 기술하는 고유의 템플릿을 생성하거나, AWS CloudFormation의 샘플 템플릿을 사용할 수 있습니다. AWS Elastic Beanstalk와 마찬가지로, CloudFormation은 리소스를 자동으로 배포하므로 AWS 리소스를 프로비저닝해야 하는 순서나 해당 종속성을 적용하는 방법을 자세히 이해할 필요가 없습니다.

AWS CloudFormation은 각 스택의 생성과 삭제를 기록하므로 스택에 대해 프로비저닝된 모든 리소스의 목록과 프로비저닝 이벤트 기록을 볼 수 있습니다. 템플릿은 텍스트 파일이므로 다른 애플리케이션 작업 결과와 마찬가지로 버전을 제어할 수 있습니다. AWS CloudFormation을 사용하면 애플리케이션 소스의 버전 제어와 똑같은 방법으로 인프라 정의의 버전을 제어할 수 있습니다.

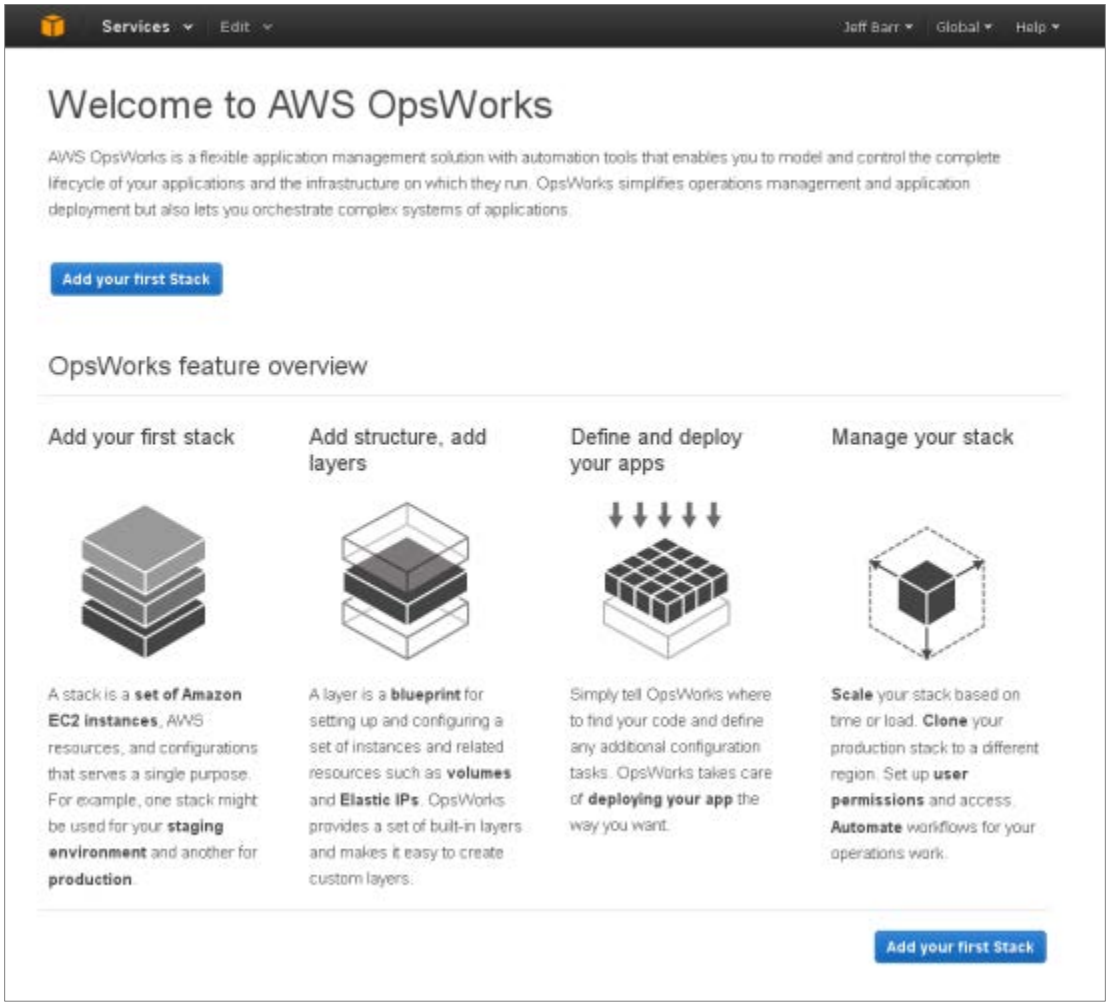
모든 AWS CloudFormation 엔드포인트는 HTTPS 프로토콜을 액세스에 사용합니다. AWS IAM을 사용하여 AWS 계정 아래에 사용자를 생성하고 이러한 사용자가 수행할 권한이 있는 CloudFormation 작업을 제어하는 방식으로 AWS CloudFormation 템플릿 생성 및 관리 기능에 대한 액세스를 제어할 수 있습니다.

AWS OpsWorks 보안

AWS OpsWorks는 전체 애플리케이션 수명 주기를 제어하는 데 도움이 되는 애플리케이션 관리 서비스입니다. 이 서비스를 사용하면 리소스 프로비저닝, 구성 관리, 애플리케이션 배포, 소프트웨어 업데이트, 모니터링 및 액세스 제어를 포함하여 애플리케이션 배포에 관련된 모든 프로세스를 자동화하고 관리할 수 있습니다.

먼저 *스택*을 생성하는 것으로 시작합니다. 스택은 EC2 인스턴스와 *계층*의 컬렉션이며, 계층은 인스턴스를 구성, 시작 및 관리하는 데 사용되는 블루프린트입니다. 설치 스크립트 및 초기화 작업을 포함하여 각 계층의 소프트웨어 구성을 정의합니다. 인스턴스가 layer에 추가되면 OpsWorks는 자동으로 지정된 구성을 적용합니다.

각 스택은 하나 이상의 애플리케이션을 호스팅하며 애플리케이션에 필요할 수 있는 다른 AWS 리소스(EBS 볼륨 및 엘라스틱 IP 주소)의 컨테이너 및 애플리케이션과 관련된 사용자 권한의 역할도 수행합니다. OpsWorks를 사용하여 Git나 Subversion과 같은 하나 이상의 코드 리포지토리에서 코드를 가져오거나, HTTP 요청을 통해 가져오거나, S3 버킷에서 다운로드하는 방법으로 EC2 인스턴스에서 애플리케이션을 설치하게 합니다.



스택, 계층 및 애플리케이션을 정의한 후 EC2 인스턴스를 생성하고 특정 계층에 할당합니다. 인스턴스를 수동으로 시작하거나, 로드를 기준으로 또는 시간별로 조정을 정의할 수 있습니다. 어떤 방법을 사용하든, 인스턴스 유형, 가용 영역, 보안 그룹 및 운영 체제를 완전히 제어할 수 있습니다. 인스턴스를 시작하면 인스턴스가 포함된 계층에 대해 정의한 레시피를 사용하여 사양에 맞게 인스턴스가 구성됩니다.

AWS IAM을 사용하여 사용자가 OpsWorks와 상호 작용할 수 있는 방식(스택 관리 및 SSH를 사용한 EC2 인스턴스에 연결 등)을 제어할 수 있습니다. AWS OpsWorks에 대한 액세스를 허용하지만 Amazon EC2와 같은 종속 서비스에 대한 직접 액세스는 거부할 수도 있습니다. 예를 들어, AWS OpsWorks를 사용하여 인스턴스를 중지할 수 있는 사용자 권한을 제공하지만, Amazon EC2 콘솔이나 API를 사용하여 인스턴스를 종료할 수 있는 권한은 거부할 수 있습니다.

IAM을 사용하면 OpsWorks가 사용자를 대신하여 스택 리소스를 관리할 수 있는 방법과, AWS OpsWorks가 제어하는 인스턴스에서 실행되는 앱이 AWS 리소스에 액세스할 수 있는 방법도 제어할 수 있습니다. 이 기능은 EC2 인스턴스에서 역할을 통해 다른 AWS 서비스에 액세스하고 해당 서비스의 자격 증명을 얻는 앱을 배포하는 경우에만 적용됩니다.

AWS OpsWorks를 사용하면 *배포 키*를 사용하여 Github 리포지토리에서 앱을 가져오도록 요구할 수 있습니다. 배포 키는 추가 정보를 입력할 필요 없이 AWS OpsWorks가 프라이빗 Github 리포지토리에서 앱이나 쿡북을 비동기적으로 배포할 수 있도록 허용하는, 암호 없는 SSH 키입니다.

또한 AWS OpsWorks API는 SSL로 암호화된 엔드포인트(opsworks.us-east-1.amazonaws.com)를 통해서만 액세스할 수 있습니다. OpsWorks에 액세스하려면 이 엔드포인트에 연결해야 하지만, API를 사용하여 AWS OpsWorks에서 모든 AWS 리전에 스택을 생성할 수 있습니다.

AWS CloudHSM 보안

AWS CloudHSM 서비스는 고객에게 하드웨어 보안 모듈 또는 HSM에 대한 전용 액세스 권한을 제공합니다. HSM은 변조된 흔적이 있는 침입 방지 디바이스 내에서 보안 암호화 키 스토리지 및 작업을 제공하도록 설계된 어플라이언스입니다. 데이터 암호화에 사용한 암호화 키를 안전하게 생성, 저장, 관리할 수 있으며 이 경우, 사용자만 자신의 암호화 키를 사용할 수 있습니다. AWS CloudHSM 어플라이언스는 데이터베이스 암호화, 디지털 권한 관리(DRM), 퍼블릭 키 인프라(PKI), 인증 및 권한 부여, 문서 서명, 트랜잭션 처리 등의 다양한 사용을 위해 암호화 키 구성 요소를 안전하게 저장하고 처리하도록 설계되었습니다. 이 어플라이언스는 AES, RSA, ECC 및 기타 다수를 포함하여 사용 가능한 가장 강력한 일부 암호화 알고리즘을 지원합니다.

AWS CloudHSM 서비스는 EC2 및 VPC와 함께 사용하여 프라이빗 서브넷 내에서 고유의 프라이빗 IP를 어플라이언스에 제공하도록 설계되었습니다. 양방향 디지털 인증서 인증 및 256비트 SSL 암호화를 사용하여 보안 통신 채널을 제공하는 SSL/TLS를 통해 EC2 서버에서 CloudHSM 어플라이언스에 연결할 수 있습니다.

EC2 인스턴스와 동일한 리전에서 CloudHSM 서비스를 선택하면 네트워크 지연 시간이 감소되므로 애플리케이션 성능을 향상할 수 있습니다. 애플리케이션에서 PKCS#11, MS CAPI 및 Java JCA/JCE(Java Cryptography Architecture/Java Cryptography Extensions) 등의 HSM이 제공하는 API를 사용할 수 있도록 EC2 인스턴스에서 클라이언트를 구성할 수 있습니다.

HSM 사용을 시작하기 전에 어플라이언스에서 최소 하나 이상의 파티션을 설정해야 합니다. 이 암호화 파티션은 키에 대한 액세스를 제한하는 논리 및 물리적 보안 경계이므로, 자신만이 HSM에서 수행되는 키와 작업을 제어할 수 있습니다. AWS는 이 어플라이언스에 대한 관리 자격 증명을 가지고 있지만 이러한 자격 증명은 어플라이언스의 HSM 파티션이 아니라 어플라이언스를 관리하는 데에만 사용할 수 있습니다. AWS는 이러한 자격 증명을 사용하여 어플라이언스의 상태나 가용성을 모니터링하고 관리합니다. AWS는 키를 추출할 수 없으며 AWS는 어플라이언스가 키를 사용하여 암호화 작업을 수행하도록 할 수 없습니다.

HSM 어플라이언스는 변조가 감지될 경우 암호화 키 구성 요소를 지우고 이벤트 로그를 생성하는 물리적 및 논리적 변조 방지 및 응답 메커니즘을 갖추고 있습니다. HSM은 HSM 어플라이언스의 물리적 장벽에 대한 침범이 발생할 경우 변조를 감지하도록 설계되었습니다. 또한 HSM 관리자 자격 증명을 사용한 HSM 파티션 액세스에 3회 실패하면 그 후 HSM 어플라이언스가 HSM 파티션을 삭제합니다.

CloudHSM 구독이 종료되고 HSM 콘텐츠가 더 이상 필요 없음이 확인되면 각 파티션과 해당 콘텐츠 및 모든 로그를 삭제해야 합니다. 서비스 해제 프로세스의 일부로서 AWS는 어플라이언스를 0으로 채워 모든 키 구성 요소를 영구적으로 지웁니다.

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.

인증: 인증은 누군가 또는 무언가를 어떤 사람 또는 어떤 사물로 선언할 것인지를 정하는 프로세스입니다. 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 EC2 지점은 리전과 가용 영역으로 구성됩니다. 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: AmazonS3에 저장된 객체를 저장하는 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 블록.

클라이언트 측 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.

자격 증명: 사용자나 프로세스가 서비스에 액세스하기 위해 권한을 부여 받는 인증 프로세스 중에 AWS 서비스를 확인하기 위해 가지고 있어야 하는 항목입니다. AWS 자격 증명에는 액세스 키 ID 및 보안 액세스 키뿐 아니라 X.509 인증서와 다중 요소 토큰도 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 수명과 관계없이 지속되는 오프 인스턴스 스토리지입니다.

ElastiCache: 클라우드상의 분산 인 메모리 캐시 환경을 손쉽게 설정 및 관리하고 및 확장할 수 있는 웹 서비스입니다. . 본 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.

엘라스틱 IP 주소: Amazon VPC의 인스턴스에 할당하여 인스턴스를 퍼블릭으로 만들 수 있는 고정 퍼블릭 IP 주소입니다. 또한 엘라스틱 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: Amazon EC2 및 Amazon S3의 웹 스케일 인프라에서 실행되는 호스팅된 하둡 프레임워크를 이용하는 AWS 웹 서비스입니다. 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.

엔드포인트: 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.

해시: 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.

하이퍼바이저: 하이퍼바이저는 가상 머신 모니터(VMM)라고도 불리며, 호스트 컴퓨터에서 여러 운영 체제를 동시에 실행할 수 있도록 하는 컴퓨터 소프트웨어/하드웨어 플랫폼 가상화 소프트웨어입니다.

Identity and Access Management(IAM): AWS IAM을 사용하면 AWS 계정 내에서 여러 사용자를 생성하고 이러한 각 사용자의 권한을 관리할 수 있습니다.

Import/Export 서비스: 이동식 스토리지 디바이스를 안전한 AWS 시설로 물리적으로 전달하여 대용량의 데이터를 AWS 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.

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 저장된 기본 엔터티입니다. 객체는 객체 데이터와 메타데이터로 구성됩니다. 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 하드웨어와 유사하지만 동일하지는 않은 가상 머신에 소프트웨어 인터페이스를 제공하는 가상화 기술입니다.

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 MySQL, Oracle 또는 Microsoft SQL Server 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).

Security Token Service(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 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.

Simple DataBase(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(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 Management Console에 전달하는 URL을 생성하여 외부 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.

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

버전 관리: Amazon S3의 모든 객체는 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: AMI가 시작되면, 그 결과 실행되는 시스템을 인스턴스라고 부릅니다. 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.

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.

최신 버전 이후의 변경 사항(2013년 5월/6월):

- 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
- 다음과 같은 새로운 기능으로 여러 다른 서비스 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

최신 버전 이후의 변경 사항(2011년 5월):

- 인프라와 서비스별 보안을 효율적으로 구별하여 식별하도록 재구성
- 제어 환경 요약 머리글을 AWS 규정 준수 프로그램으로 변경
- 정보 및 구성 머리글을 관리 및 통신으로 변경
- 직원 수명 주기 머리글을 논리적 액세스로 변경
- 구성 관리 머리글을 변경 관리로 변경
- 환경 보호 섹션을 물리적 보안 섹션과 병합
- 백업 섹션의 정보를 S3, SimpleDB 및 EBS 섹션에 통합
- SSAE 16에 대한 SAS70 이름 변경과 FedRAMP 추가를 반영하도록 인증서 업데이트
- 보안 네트워크 아키텍처와 네트워크 모니터링 및 보호를 추가하도록 네트워크 보안 섹션 업데이트
- 역할/키 프로비저닝, 가상 MFA, 임시 보안 자격 증명 및 Single Sign On을 통합하도록 IAM 업데이트
- 새로운 리전과 GovCloud 설명을 포함하도록 리전 업데이트
- 서비스 및 보안을 명료하게 설명하도록 EBS, S3, SimpleDB, RDS 및 EMR 업데이트
- 구성 옵션, VPN 및 Elastic Network Interface를 추가하도록 VPC 업데이트
- Amazon Direct Connect 보안 섹션 추가
- Amazon Elastic Load Balancing 보안 추가
- AWS Storage Gateway 보안 추가
- AWS Import/Export 보안 추가
- Auto Scaling 보안 내용 추가
- Amazon DynamoDB 보안 추가
- Amazon ElastiCache 보안 추가
- Amazon Simple Workflow Service(Amazon SWS) 보안 추가
- Amazon Simple Email Service(Amazon SES) 보안 추가
- Amazon Route 53 보안 추가
- Amazon CloudSearch 보안 추가
- AWS Elastic Beanstalk 보안 추가
- AWS CloudFormation 보안 추가
- 업데이트된 용어 정의

최신 버전 이후의 변경 사항(2010년 8월):

- AWS Identity and Access Management(AWS IAM) 내용 추가
- Amazon Simple Notification Service(SNS) 보안 내용 추가
- Amazon CloudWatch 보안 내용 추가
- Auto Scaling 보안 내용 추가
- Amazon Virtual Private Cloud(Amazon VPC)에 대한 업데이트
- 관리 환경에 대한 업데이트
- 리스크 관리 내용 삭제(별도 백서에서 자세히 설명)

최신 버전 이후의 변경 사항(2009년 11월)

- 주요 내용 개정

최신 버전 이후의 변경 사항(2009년 6월)

- SAA70 반영을 위해 인증서 및 인가 섹션 변경
- Amazon Virtual Private Cloud(Amazon VPC) 내용 추가
- AWS Multi-Factor Authentication및 키 회전에 대한 보안 자격 증명 섹션 내용 추가
- Amazon Relational Database Service(Amazon RDS) 보안 내용 추가

최신 버전 이후의 변경 사항(2008년 9월)

- 보안 설계 원칙 내용 추가
- 물리적 보안 정보 업데이트 및 배경 검사 내용 수정
- Amazon EBS 관련 내용의 명확성을 위해 백업 섹션 업데이트
- Amazon EC2 보안 섹션 업데이트에는 다음이 포함됩니다
- 인증서 기반 SSHv2
- 다계층 보안 그룹 세부 사항 및 그림
- 하이퍼바이저 설명 및 인스턴스 격리 그림
- 장애 분리
- 구성 관리 내용 추가
- 세부 사항 및 명료성을 위해 Amazon S3 섹션 업데이트
- Storage Device Decommissioning 내용 추가
- Amazon SQS 보안 내용 추가
- Amazon CloudFront 보안 내용 추가
- Amazon Elastic MapReduce 보안 내용 추가

고지 사항