AWS 보안 모범 사례

2016년 8월

(이 문서의 최신 버전은 **http://aws.amazon.com/security**를 참조)

This paper has been archived

For the latest Security, Identity and Compliance content, refer to:

https://aws.amazon.com/architecture/security-identity-compliance/

고지 사항

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

목차

요약

본 백서는 Amazon Web Services(AWS)에서 실행하는 애플리케이션의 보안 인프라 및 구성을 설계하는 기존 고객과 잠재 고객을 대상으로 합니다. 본 백서는 AWS 클라우드에 있는 데이터 및 자산을 보호할 수 있도록 ISMS(정보 보안 관리 시스템)를 정의하고 조직의 보안 정책 및 프로세스 세트를 구축하는 데 도움이 되는 보안 모범 사례를 제공합니다. 또한 AWS의 자산을 확인, 분류 및 보호하고 계정, 사용자 및 그룹을 사용한 AWS 리소스에 대한 액세스 관리 및 클라우드에서 데이터, 운영 체제, 애플리케이션 및 전반적인 인프라를 보안 조치할 수 있는 방법을 제시하는 등 다양한 보안 주제의 개요를 제공합니다.

백서는 IT 의사결정자와 보안 직원을 대상으로 하며 네트워킹, 운영 체제, 데이터 암호화 및 운영 제어 분야의 기본적인 보안 개념을 숙지하고 있다고 가정합니다.

개요

정보 보안은 Amazon Web Services(AWS) 고객에게 가장 중요한 것입니다. 보안은 우발적 또는 의도적인 도난, 유출, 무결성 손상, 삭제로부터 비즈니스 크리티컬 정보를 보호하는 핵심적 기능 요구 사항입니다.

AWS *공동 책임 모델*에 따라, AWS는 글로벌 보안 인프라 및 기반 컴퓨팅, 스토리지, 네트워킹 및 데이터베이스 서비스와 더 높은 수준의 서비스를 제공합니다. AWS는 AWS 고객의 자산 보호에 사용할 수 있는 다양한 보안 서비스와 기능을 제공합니다. AWS 고객은 클라우드에 있는 데이터의 기밀성, 무결성, 가용성을 보호하고 정보 보호에 대한 구체적인 비즈니스 요구 사항을 준수할 책임이 있습니다. AWS의 보안 기능에 대한 자세한 내용은 보안 프로세스 개요 백서를 참조하십시오.

본 백서는 AWS에 있는 조직의 자산에 대한 정보 보안 정책 및 프로세스의 모음인 ISMS(정보 보안 관리 시스템)를 구축 및 정의하는 데 활용할 수 있는 모범 사례를 설명합니다. ISMS에 대한 자세한 내용은 http://www.27000.org/iso-27001.htm의 ISO 27001을 참조하십시오. AWS 사용에 있어 ISMS 구축이 필수는 아니지만, 널리 채택된 글로벌 보안 접근 방식의 기본 빌딩 블록을 바탕으로 한 정보 보안 관리를 위한 정형화된 접근 방식을 통해 조직의 전반적인 보안 태세를 개선할 수 있다고 생각합니다.

백서는 다음 주제를 다룹니다.

- AWS와 고객이 보안 책임을 분담하는 방법
- 고객의 자산을 정의하고 분류하는 방법
- 권한을 가진 계정과 그룹을 사용하여 데이터에 대한 사용자 액세스를 관리하는 방법
- 고객의 데이터, 운영 체제 및 네트워크 보안 유지를 위한 모범 사례
- 모니터링과 알림을 통해 보안 목표를 달성하는 방법

본 백서는 이러한 분야의 보안 모범 사례를 높은 수준에서 설명합니다. (백서는 "방법론"적인 구성 지침을 제공하지 않습니다. 구성 지침은 http://aws.amazon.com/documentation의 AWS 문서를 참조하십시오.)

AWS 공동 책임 모델 알기

Amazon Web Services(AWS)는 클라우드에서 보안 글로벌 인프라와 서비스를 제공합니다. AWS를 커뮤니케이션 시스템을 가속하고 AWS 사용을 활용하는 ISMS를 설계할 수 있습니다.

AWS에서 ISMS를 설계하려면 먼저 AWS와 고객이 보안 목표를 위해 협력하는 AWS 공동 책임 모델을 숙지해야 합니다.

AWS는 보안 인프라와 서비스를 제공하고 고객은 보안 운영 체제, 플랫폼, 데이터를 책임집니다. 보안 글로벌 인프라를 위해 AWS는 인프라 구성 요소를 구성하고 사용자 및 사용자 권한을 AWS 서비스 하위 세트로 관리하는 Identity and Access Management(IAM) 서비스 등 보안 강화에 사용할 수 있는 서비스와 기능을 제공합니다. 보안 서비스를 위해 AWS는 제공하는 다양한 유형의 서비스별 공동 책임 모델을 제공합니다.

- 인프라 서비스
- 컨테이너 서비스
- 추상화된 서비스

예를 들어 Amazon Elastic Compute Cloud(Amazon EC2)와 같은 인프라 서비스의 공동 책임 모델은 AWS가 다음 자산의 보안을 관리한다고 명시합니다.

- 시설
- 하드웨어의 물리적 보안
- 네트워크 인프라
- 가상화 인프라

ISMS 자산 정의에 따라 AWS를 이러한 자산의 소유자로 간주하십시오. 이러한 AWS 제어를 활용하고 ISMS에 포함시키십시오.

예로 든 Amazon EC2의 고객은 다음 항목의 보안을 책임집니다.

- Amazon 머신 이미지(AMI)
- 운영 체제
- 애플리케이션
- 전송 중인 데이터
- 저장된 데이터
- 데이터 스토어
- 자격 증명
- 정책 및 구성

특정 서비스는 고객과 AWS가 책임을 분담하는 방법을 더 자세히 규정합니다. 자세한 내용은 http://aws.amazon.com/compliance/#third-party.를 참조하십시오.

AWS 보안 글로벌 인프라 이해

AWS가 관리하는 AWS 보안 글로벌 인프라와 서비스는 엔터프라이즈 시스템과 개별 애플리케이션을 위해 신뢰할 수 있는 기반을 제공합니다. AWS는 클라우드 내 정보 보안에 대한 높은 표준을 설정하고 소프트웨어 획득 및 개발을 통한 물리적 보안부터 직원 수명 주기 관리 및 보안 조직까지 종합적이고 전체적인 제어 목표 집합을 보유하고 있습니다. AWS 보안 글로벌 인프라 및 서비스는 정기적으로 타사 규정 준수 감사를 받아야 합니다. 자세한 내용은 Amazon Web Services 위험 및 규정 준수 백서 를 참조하십시오. (참조 자료 참조)

IAM 서비스 사용

IAM 서비스는 본 백서에서 설명하는 AWS 보안 글로벌 인프라의 한 구성 요소입니다. IAM으로 사용자가 어떤 AWS 서비스와 리소스에 액세스할 수 있는지를 제어하는 암호, 액세스 키 및 사용 권한 정책과 같은 보안 자격 증명을 한 곳에서 관리할 수 있습니다.

AWS에 가입할 때 만든 AWS 계정에는 사용자 이름(이메일 주소)과 암호가 있어야 합니다. 사용자 이름과 암호로 AWS Management Console에 로그인해 브라우저 기반 인터페이스를 사용하여 AWS 리소스를 관리할 수 있습니다. 또한 액세스 키(액세스 키 ID와 보안 액세스 키로 구성)를 만들어 명령줄 인터페이스(CLI), AWS SDK 또는 API 호출로 AWS 프로그래밍 호출을 할 때 사용할 수 있습니다.

IAM을 사용하여 AWS 계정 내에 개별 사용자를 만들고 각 사용자에게 사용자 이름, 암호, 액세스 키를 부여할 수 있습니다. 개별 사용자는 계정별 URL을 사용하여 콘솔에 로그인할 수 있습니다. 또한 사용자별 액세스 키를 만들어 AWS 리소스에 액세스할 수 있도록 프로그래밍 호출을 할 수 있습니다. 고객의 IAM 사용자가 수행한 활동에 대한 모든 요금은 고객의 AWS 계정으로 청구됩니다. 자신이 사용할 IAM 사용자도 만들어 두고 일상적인 AWS 액세스에 AWS 계정 자격 증명을 사용하지 않는 것이 가장 좋습니다. 자세한 내용은 IAM 모범 사례 를 참조하십시오.

리전, 가용 영역 및 엔드포인트

AWS 보안 글로벌 인프라의 구성 요소인 리전, 가용 영역 및 엔드포인트에 대해서도 숙지해야 합니다.

AWS 리전을 사용하면 네트워크 지연 시간과 규제 준수를 관리할 수 있습니다. 데이터를 특정 리전에 저장하면 해당 리전 밖으로 복제되지 않습니다. 회사에서 필요한 경우 리전 간에 데이터를 복제하는 일은 고객의 책임입니다. 즉, 다음과 같습니다. AWS는 국가에 대한 정보를 제공하고 필요한 경우 각 리전이 포함된 주에 대한 정보를 제공합니다. 고객은 자체 규정 준수 및 네트워크 지연 시간 요구 사항에 따라 데이터를 저장할 리전을 선택할 책임이 있습니다.

리전은 가용성을 염두에 두고 설계되며 최소 2개 이상의 가용 영역으로 구성됩니다. 가용 영역은 결함 격리를 위해 설계되었습니다. 여러 인터넷 서비스 제공업체(ISP)와 다양한 전력망에 연결되어 있습니다. 고속 링크를 사용해 상호 연결되어 있기 때문에 애플리케이션은 LAN(Local Area Network) 연결을 사용하여 같은 리전 내에 있는 가용 영역 간 통신이 가능합니다. 고객은 시스템이 상주할 가용 영역을 신중하게 선택할 책임이 있습니다. 시스템은 여러 가용 영역을 아우를 수 있습니다. 시스템을 설계할 때 재해 발생 시 가용 영역의 임시적 또는 장기적인 장애에도 유지될 수 있도록 설계하는 것이 좋습니다.

AWS는 AWS Management Console을 통해 서비스에 대한 웹 액세스를 제공하며, 이후에는 서비스별 API를 통해 제공됩니다. AWS는 애플리케이션 프로그래밍 인터페이스(API)와 명령줄 인터페이스(CLI)를 통해 서비스에 대한 프로그래밍 액세스를 제공합니다. AWS가 관리하는 서비스 엔드포인트는 관리("백플레인") 액세스를 제공합니다.

AWS 서비스에 대한 보안 공동 책임

AWS는 다양한 인프라와 플랫폼 서비스를 제공합니다. 이러한 AWS 서비스의 보안 및 공동 책임을 이해할 수 있도록 서비스를 세 가지 주요 카테고리 (인프라, 컨테이너, 추상화된 서비스)로 분류합니다. 각 카테고리에는 상호 작용과 기능 액세스 방법에 따라 조금씩 다른 보안 소유권 모델이 있습니다.

- **인프라 서비스:** 이 카테고리에는 Amazon EC2 등의 컴퓨팅 서비스, Amazon Elastic Block Store(Amazon EBS), Auto Scaling, Amazon Virtual Private Cloud(Amazon VPC) 등의 관련 서비스가 포함됩니다. 이러한 서비스를 사용하면 온프레미스 솔루션과 비슷하거나 대부분 호환되는 기술을 통해 클라우드 인프라를 설계 및 구축할 수 있습니다. 운영 체제를 제어할 수 있고 가상화 스택의 사용자 계층에 대한 액세스를 제공하는 모든 자격 증명 관리 시스템을 구성 및 운영할 수 있습니다.

- **컨테이너 서비스:** 이 카테고리의 서비스는 일반적으로 별도의 Amazon EC2나 다른 인프라 인스턴스에서 실행되지만 운영 체제나 플랫폼 계층을 관리하지 않는 경우도 있습니다. AWS는 이러한 애플리케이션 "컨테이너"에 관리형 서비스를 제공합니다. 고객은 방화벽 규칙 등의 네트워크 컨트롤을 설정 및 관리하고 플랫폼 수준의 자격 증명 및 액세스 관리를 IAM과는 별도로 관리할 책임이 있습니다. 컨테이너 서비스의 예로는 Amazon Relational Database Services(Amazon RDS), Amazon Elastic Map Reduce(Amazon EMR), AWS Elastic Beanstalk이 있습니다.
- **추상화된 서비스:** 이 카테고리에는 Amazon Simple Storage Service(Amazon S3), Amazon Glacier, Amazon DynamoDB, Amazon Simple Queuing Service(Amazon SQS), Amazon Simple Email Service(Amazon SES) 등의 상위 수준 스토리지, 데이터베이스, 메시징 서비스가 포함됩니다. 이러한 서비스는 클라우드 애플리케이션을 구축하고 운영할 수 있는 플랫폼이나 관리 계층을 추상화합니다. 고객은 AWS API를 사용하여 추상화된 서비스의 엔드포인트에 액세스하고, AWS는 기본 서비스 구성 요소, 운영 체제 및 플랫폼을 관리합니다. 고객은 기본 인프라를 공유하고, 추상화된 서비스는 고객의 데이터를 안전하게 보호하는 데 필요한 IAM 기능을 제공합니다.

다음 섹션에서는 각 서비스 유형에 대한 공동 책임을 조금 더 자세히 살펴보겠습니다.

인프라 서비스의 공동 책임 모델

Amazon EC2, Amazon EBS, Amazon VPC와 같은 인프라 서비스는 AWS 글로벌 인프라를 기반으로 실행됩니다. 이러한 서비스는 가용성과 내구성 목표 면에서 다양하지만 항상 시작되었던 특정 리전 내에서 작동합니다. 여러 가용 영역에서 복원력이 뛰어난 구성 요소를 활용하여 AWS의 개별 서비스의 목표를 초과하는 가용성 목표를 충족하는 시스템을 구축할 수 있습니다.

그림 1은 인프라 서비스 공동 책임 모델의 빌딩 블록을 보여줍니다.

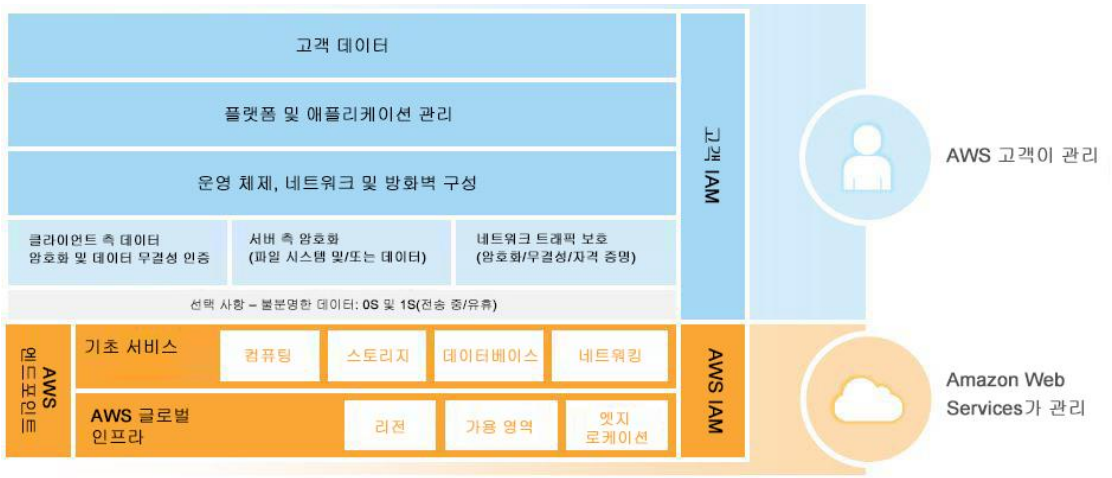

그림 1: 인프라 서비스의 공동 책임 모델

AWS 보안 글로벌 인프라를 바탕으로 자체 데이터 센터에서 온프레미스로 하는 것과 같은 방식으로 AWS 클라우드에서 운영 체제와 플랫폼을 설치 및 구성합니다. 그런 다음 플랫폼에 애플리케이션을 설치합니다. 궁극적으로는 고객의 데이터가 자체 애플리케이션에 상주하고 자체 애플리케이션을 통해 관리됩니다. 고객의 비즈니스 또는 규정 준수 요구가 매우 엄격한 경우가 아니라면, AWS 보안 글로벌 인프라가 제공하는 것 이상으로 보호 계층을 추가할 필요가 없습니다.

특정 규정 준수 요구 사항이 있는 경우 고객은 AWS 서비스와 고객의 애플리케이션 및 데이터가 상주하는 자체 운영 체제 및 플랫폼 간에 추가 보호 계층을 요구할 수 있습니다. 유휴 데이터의 보호와 전송 중인 데이터의 보호 등 추가 제어를 도입하거나 AWS 서비스와 자체 플랫폼 간의 불투명 계층을 추가할 수 있습니다. 불투명 계층에는 데이터 암호화, 데이터 무결성 인증, 소프트웨어 및 데이터 서명, 보안 타임스탬프 등이 포함됩니다.

AWS는 유휴 데이터와 전송 중인 데이터를 보호하기 위해 구현할 수 있는 기술을 제공합니다. 자세한 내용은 본 백서의 Amazon EC2 인스턴스에 대한 OS 수준의 액세스 관리와 데이터 보안 유지 섹션을 참조하십시오. 또는 자체 데이터 보호 도구를 추가하거나 AWS 파트너 상품을 활용할 수 있습니다.

이전 섹션에서는 AWS 서비스 인증이 필요한 리소스 액세스를 관리할 수 있는 방법들을 설명했습니다. 하지만 EC2 인스턴스에서 운영 체제에 액세스하려면 다른 자격 증명 세트가 필요합니다. 공동 책임 모델에서는 고객이 운영 체제 자격 증명을 소유하지만 AWS가 운영 체제에 대한 초기 액세스의 부트스트랩을 지원합니다.

표준 AMI에서 새 Amazon EC2 인스턴스를 시작하면 Secure Shell(SSH) 또는 Windows Remote Desktop Protocol(RDP) 등의 보안 원격 시스템 액세스 프로토콜을 사용하여 해당 인스턴스에 액세스할 수 있습니다. 운영 체제 수준에서 성공적으로 인증을 해야 자체 요구 사항에 따라 Amazon EC2 인스턴스에 액세스하고 이를 구성할 수 있습니다. Amazon EC2 인스턴스를 인증하고 원격으로 액세스할 수 있으면 원하는 운영 체제 인증 메커니즘을 설정할 수 있고, 여기에는 X.509 인증서 인증, Microsoft Active Directory 또는 로컬 운영 체제 계정 등이 있습니다.

AWS는 EC2 인스턴스 인증을 활성화할 수 있도록 Amazon EC2 키 페어라고 하는 비대칭 키 페어를 제공합니다. 업계 표준 RSA 키 페어입니다. 각 사용자는 여러 개의 Amazon EC2 키 페어가 있을 수 있지만 서로 다른 키 페어를 사용하여 새 인스턴스를 시작할 수 있습니다. EC2 키 페어는 앞에서 설명한 AWS 계정이나 IAM 사용자 자격 증명과는 관계가 없습니다. 이러한 자격 증명은 다른 AWS 서비스에 대한 액세스를 제어합니다. EC2 키 페어는 특정 인스턴스에 대한 액세스만 제어합니다.

OpenSSL과 같은 업계 표준 도구를 사용하여 자체 Amazon EC2 키 페어를 생성할 수 있습니다. 안전하고 신뢰할 수 있는 환경에서 키 페어를 생성하고 키 페어의 퍼블릭 키만 AWS에 가져옵니다. 프라이빗 키를 안전하게 저장합니다. 이 경우 선택하는 경우 품질이 높은 난수 생성기를 사용하는 것이 좋습니다.

AWS로 Amazon EC2 키 페어를 생성할 수 있습니다. 이 경우 인스턴스를 처음 만들었을 때 RSA 키 페어의 프라이빗 및 퍼블릭 키 모두 고객에게 제공됩니다. Amazon EC2 키 페어의 프라이빗 키를 다운로드해 안전하게 저장해야 합니다. AWS는 프라이빗 키를 저장하지 않습니다. 잃어버린 경우 새 키 페어를 생성해야 합니다.

cloud-init 서비스를 사용하는 Amazon EC2 Linux 인스턴스의 경우 표준 AWS AMI로부터 새 인스턴스가 시작되면 Amazon EC2 키 페어의 퍼블릭 키는 초기 운영 체제 사용자의 **~/.ssh/authorized_keys** 파일에 추가됩니다. 그러면 사용자는 SSH 클라이언트를 사용하여 Amazon EC2 Linux 인스턴스에 연결할 수 있습니다. 그 방법은 올바른 Amazon EC2 인스턴스 사용자의 이름을 ID(예: ec2-user)로 사용하도록 클라이언트를 구성하고 사용자 인증에 프라이빗 키 파일을 제공하는 것입니다.

ec2config 서비스를 사용한 Amazon EC2 Windows 인스턴스의 경우 표준 AWS AMI로부터 새 인스턴스가 시작되면 **ec2config** 서비스가 인스턴스에 대한 새로운 무작위 관리자 암호를 설정하고 해당 Amazon EC2 키 페어의 퍼블릭 키를 사용하여 암호화합니다. 사용자는 AWS Management Console 또는 명령줄 도구를 사용하거나 암호를 해독할 해당 Amazon EC2 프라이빗 키를 제공하여 Windows 인스턴스 암호를 받을 수 있습니다. 이 암호는 Amazon EC2 인스턴스의 기본 관리 계정과 함께 Windows 인스턴스 인증에 사용할 수 있습니다.

AWS는 Amazon EC2 키를 관리하고 새로 시작된 Amazon EC2 인스턴스의 업계 표준 인증을 제공하기 위한 유연하고 실용적인 도구 집합을 제공합니다. 보안 요구 사항이 엄격한 경우 LDAP나 Active Directory 인증 등 대체 인증 메커니즘을 구현하고 Amazon EC2 키 페어 인증을 비활성화할 수 있습니다.

컨테이너 서비스의 공동 책임 모델

AWS 공동 책임 모델은 Amazon RDS와 Amazon EMR 등 컨테이너 서비스에도 적용됩니다. 이러한 서비스에 대해 AWS는 기본 인프라와 기초 서비스, 운영 체제와 애플리케이션 플랫폼을 관리합니다. 예를 들어 Oracle용 Amazon RDS는 AWS가 Oracle 데이터베이스 플랫폼 등을 포함한 컨테이너의 모든 계층을 관리하는 관리형 데이터베이스 서비스입니다. Amazon RDS와 같은 서비스의 경우 AWS 플랫폼은 데이터 백업 및 복원 도구를 제공합니다. 하지만 비즈니스 연속성 및 재해 복구(BC/DR) 정책과 관련된 도구를 구성하고 사용할 책임은 고객에게 있습니다.

AWS 컨테이너 서비스의 경우 컨테이너 서비스 액세스를 위한 데이터와 방화벽 규칙에 대한 책임은 고객에게 있습니다. 예를 들어 Amazon RDS는 RDS 보안 그룹을 제공하고, Amazon EMR을 사용하면 Amazon EMR 인스턴스에 대한 Amazon EC2 보안 그룹을 통해 방화벽 규칙을 관리할 수 있습니다.

그림 2는 컨테이너 서비스의 공동 책임 모델을 보여줍니다.

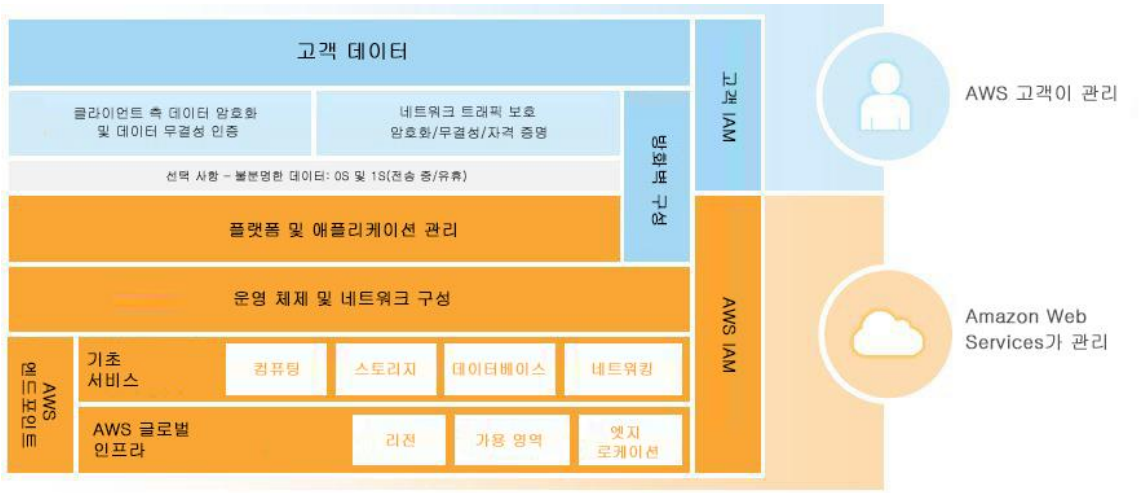

그림 2: 컨테이너 서비스의 공동 책임 모델

추상화된 서비스의 공동 책임 모델

Amazon S3 및 Amazon DynamoDB와 같은 추상화된 서비스의 경우 AWS는 인프라 계층, 운영 체제, 플랫폼을 작동하고 엔드 포인트에 액세스하여 데이터를 저장 및 검색합니다. Amazon S3와 DynamoDB는 IAM과 긴밀하게 통합됩니다. 데이터를 관리(자산 분류 등)하고 IAM 도구를 사용하여 플랫폼 수준에서 개별 리소스에 ACL 유형의 권한을 적용하거나 IAM 사용자/그룹 수준에서 사용자 ID 또는 사용자 책임에 따라 권한을 적용할 책임은 고객에게 있습니다. Amazon S3와 같은 일부 서비스의 경우 서비스로 또는 서비스에서 전송 중인 데이터 보호를 위해 유휴 데이터의 플랫폼 제공 암호화 또는 페이로드에 대한 플랫폼 수준의 HTTPS 캡슐화를 사용할 수도 있습니다.

그림 3은 AWS의 추상화된 서비스의 공동 책임 모델을 개략적으로 보여줍니다.

그림 3: 클라우드 서비스의 공동 책임 모델

Trusted Advisor 도구 사용

일부 AWS Premium Support 계획에는 Trusted Advisor 도구 액세스가 포함되는데, 이 액세스는 서비스를 한눈에 볼 수 있는 스냅샷을 제공하고 일반적인 보안 구성 오류를 확인하는 데 도움이 되며 시스템 성능 개선과 활용되지 않는 리소스에 대한 제안을 제공합니다. 이 백서에서는 Amazon EC2에 제공되는 Trusted Advisor의 보안 분야를 다룹니다.

Trusted Advisor는 다음 보안 권장 사항의 규정 준수 여부를 확인합니다.

- 일반적인 관리 포트에 대한 액세스가 작은 하위 집합의 주소로 제한. 여기에는 포트 22(SSH), 23(Telnet) 3389(RDP), 5500(VNC)이 포함됩니다.
- 일반적인 데이터베이스 포트 액세스 제한. 여기에는 포트 1433(MSSQL Server), 1434(MSSQL Monitor), 3306(MySQL), Oracle(1521), 5432(PostgreSQL)가 포함됩니다.
- IAM은 AWS 리소스의 보안 액세스 제어를 보장하도록 구성되어 있습니다.
- 멀티 팩터 인증(MFA) 토큰은 루트 AWS 계정의 2팩터 인증을 제공하도록 설정되어 있습니다.

AWS에서 자산 정의 및 분류

ISMS를 설계하기 전에 보호해야 하는 모든 정보 자산을 확인한 다음 기술적, 재정적으로 실행 가능한 보호 솔루션을 고안합니다. 모든 자산을 재정적인 기준으로 정량화하기는 어려울 수 있기 때문에 정성적인 지표(예: 미미함/낮음/중간/높음/매우 높음)를 사용하는 것이 더 나은 옵션일 수 있습니다.

자산은 두 가지 범주로 구분합니다.

- 비즈니스 정보, 프로세스, 활동 등 필수적인 요소
- 하드웨어, 소프트웨어, 인력, 사이트, 파트너 조직 등 필수적인 요소를 지원하는 구성 요소

표 1은 샘플 자산 표를 나타냅니다.

자산 이름	자산 소유자	자산 카테고리	종속성	비용
고객 대상 웹 사이트 애플리케이션	전자 상거래 팀	필수	EC2, ElastiCache, RDS, 개발,	배포, 대역폭, 유지 보수, 순운용 비용/결과
고객 신용 카드 데이터	E-C전자 상거래 팀	필수	PCI 카드 소유자 환경, 암호화, AWS PCI 서비스	
인력 데이터	COO	필수	Amazon RDS, 암호화 공급자, 개발 운영 IT, 타사	
데이터 아카이브	COO	필수	S3, Glacier, 개발 운영 IT	
HR 관리 시스템	HR	필수	EC2, S3, RDS, 개발 운영 IT, 타사	
AWS Direct Connect 인프라	CIO	네트워크	네트워크 운영, TelCo 공급자, AWS Direct Connect	
비즈니스 인텔리전스 인프라	BI 팀	소프트웨어	EMR, Redshift, Dynamo DB, S3, 개발 운영	
비즈니스 인텔리전스 서비스	COO	필수	BI 인프라, BI 분석 팀	
LDAP directory	IT 보안 팀	보안	EC2, IAM, 사용자 지정 소프트웨어, 개발 운영	

자산 이름	자산 소유자	자산 카테고리	종속성	비용
Windows AMI	서버 팀	소프트웨어	EC2, 패치 관리 소프트웨어, 개발 운영	
고객 자격 증명	규정 준수 팀	보안	일상적인 업데이트, 보관 인프라	

표 1: 샘플 자산 표

AWS에서 자산을 보호하기 위한 ISMS 설계

자산, 카테고리, 비용을 결정한 후, AWS에서 정보 보안 관리 시스템(ISMS)를 구현, 운영, 모니터링, 검토, 유지 보수, 개선하기 위한 표준을 설정합니다. 보안 요구 사항은 조직마다 다음과 같은 요인에 따라 차이가 있습니다.

- 비즈니스 요건과 목표
- 사용하는 프로세스
- 조직의 크기와 구조

이러한 모든 요소는 시간이 지나면서 변하기 때문에 이 모든 정보를 관리하는 단기적 프로세스를 구축하는 것이 좋습니다.

표 2는 AWS에서 ISMS를 설계 및 구축 시 단계별 접근 방식을 제안합니다. 또한 ISO 27001과 같은 표준 프레임워크가 ISMS 설계와 구현에 도움이 될 수 있습니다.

단계	제목	설명
1	**범위와 경계 정의.**	"범위 내에 있는" 리전, 가용 영역, 인스턴스, AWS 리소스를 정의합니다. 구성 요소를 제외하는 경우(예: AWS는 시설을 관리하기 때문에 자체 관리 시스템에서 제외할 수 있음) 제외한 것과 제외한 이유를 명시적으로 진술합니다.
2	**ISMS 정책 정의.**	다음을 포함합니다. • 정보 보안에 대한 작업 방향과 원칙을 설정하는 목표 • 법률, 계약 및 규제 요구 사항 • 조직의 위험 관리 목표 • 위험 측정 방법 • 경영진의 계획 승인 방식
3	**위험 평가 방법을 선택합니다.**	조직의 그룹으로부터 다음 요인에 대해 받은 의견에 따라 위험 평가 방법을 선택합니다. • 비즈니스 전략 • 정보 보안 요구 사항 • 정보 기술 기능 및 사용 • 법적 요구 사항 • 규제 책임 • 내부 및 외부 이해 관계자 관점 위험을 수락하고 허용 가능한 위험 수준(내결함성)을 식별하기 위한 기준을 설정해야 합니다. 위험 평가를 시작하고 자동화를 최대한 활용하는 것이 좋습니다. AWS 위험 자동화를 통해 위험 평가에 필요한 리소스의 범위를 좁힐 수 있습니다. 위험 평가 방법은 OCTAVE(Operationally Critical Threat, Asset, and Vulnerability Evaluation), ISO 31000:2009 Risk Management, ENISA(European Network and Information Security Agency), IRAM(Information Risk Analysis Methodology), NIST(National Institute of Standards & Technology) Special Publication(SP) 800-30 rev.1 Risk Management Guide 등 여러 가지가 있습니다.
4	**위험 요소를 식별합니다**	모든 자산을 위협에 매핑하여 위험 레지스터를 만든 다음 취약성 평가와 충격 분석 결과에 따라 각 AWS 환경에 대해 새로운 위험 표를 만드는 것이 좋습니다. 다음'은 위험 레지스터의 예입니다. • 자산 • 자산에 대한 위협 • 위협으로부터 침입당할 수 있는 취약성 • 침입당할 경우 취약성에 미치는 결과

단계	제목	설명
5	**위험을 분석 및 평가합니다.**	비즈니스 영향, 가능성과 확률, 위험 수준을 계산하여 위험을 분석하고 평가합니다.
6	**위험을 해결합니다.**	위험 처리를 위한 옵션을 선택합니다. 옵션에는 보안 컨트롤 적용, 위험 수락, 위험 회피 또는 위험 전가가 포함됩니다.
7	**보안 제어 프레임워크를 선택합니다.**	보안 제어를 선택할 때 ISO 27002, NIST SP 800-53, COBIT(Control Objectives for Information and related Technology), CSA-CCM(Cloud Security Alliance-Cloud Control Matrix)과 같은 프레임워크를 사용합니다. 이러한 프레임워크는 다시 사용할 수 있는 모범 사례의 집합으로 구성되고 관련 제어를 선택하는 데 도움이 됩니다.
8	**경영진 승인을 받습니다.**	모든 제어를 구현한 후에도 잔존 위험이 있습니다. 모든 잔존 위험을 인정하는 기업 경영진으로부터 승인을 받고 ISMS 구현과 운영 승인을 받는 것이 좋습니다.
9	**적용 가능성 선언**	다음 정보가 포함된 적용 가능성 선언을 작성합니다. • 선택한 제어와 선택한 이유 • 실시 중인 제어 • 실시하고자 하는 제어 • 제외한 제어 및 제외한 이유

표 2: ISMS 구축 단계

AWS 계정, IAM 사용자, 그룹 및 역할 관리

사용자가 필요한 리소스에 액세스할 수 있지만 그것을 초과하지 않는 적절한 수준의 권한을 가지고 있는 것은 모든 ISMS의 중요한 부분입니다. IAM을 사용하여 이 기능을 수행할 수 있습니다. 고객은 자신의 AWS 계정에서 *IAM 사용자를 만들고* 직접 권한을 할당하거나 권한을 할당하는 그룹에 할당합니다. AWS 계정과 IAM 사용자에 대한 자세한 내용은 다음과 같습니다.

- **AWS 계정.** 이것은 AWS에 처음 가입할 때 만드는 계정입니다. AWS 계정은 고객과 AWS 사이의 비즈니스 관계를 나타냅니다. 고객은 AWS 계정을 사용하여 AWS 리소스와 서비스를 관리합니다. AWS 계정은 모든 AWS 리소스와 서비스에 대한 루트 권한이 있기 때문에 매우 강력합니다. AWS와 일상적인 상호 작용을 할 때 루트 계정 자격 증명을 사용하지 마십시오. 조직에서 여러 개의 AWS 계정을 각 주요 부서에서 하나씩 사용하고 적절한 인력과 리소스에 대해 각 AWS 계정 내에 IAM 사용자를 만드는 경우도 있습니다.

- **IAM 사용자.** IAM으로 개별적인 보안 자격 증명을 보유한 여러 사용자를 만들어 모두 단일 AWS 계정에 따라 제어할 수 있습니다. IAM 사용자는 관리 콘솔, CLI를 통해 또는 API를 통해 직접 AWS 리소스에 액세스해야 하는 개인, 서비스 또는 애플리케이션이 될 수 있습니다. AWS 계정에서 서비스와 리소스에 액세스해야 하는 각 개인별로 IAM 사용자를 만드는 것이 좋습니다. AWS 계정에서 리소스에 대한 세부적인 권한을 만들어 자신이 만든 그룹에 적용한 다음 그룹에 사용자를 할당할 수 있습니다. 이 모범 사례를 통해 사용자는 작업을 수행하는 데 필요한 최소 권한을 가질 수 있습니다.

여러 AWS 계정을 사용하기 위한 전략

보안을 극대화하고 비즈니스 및 거버넌스 요구 사항을 따르기 위한 AWS 계정 전략을 설계합니다. 표 3에는 가능한 전략들이 설명되어 있습니다.

비즈니스 요구 사항	제안된 설계	의견
중앙 집중식 보안 관리	단일 AWS 계정	정보 보안 관리를 중앙 집중화하고 오버헤드를 최소화합니다.
프로덕션, 개발 및 테스트 환경의 분리	3개의 AWS 계정	프로덕션 서비스, 개발, 테스트에 각각의 AWS 계정을 만듭니다.
비즈니스 부서	여러 개의 AWS 계정	각각의 비즈니스 부문에 대해 별도의 AWS 계정을 만듭니다. 각 계정에 권한과 정책을 할당할 수 있습니다.
여러 개의 자율 독립 프로젝트가 포함된 중앙 집중식 보안 관리	여러 개의 AWS 계정	일반적인 프로젝트 리소스(예: DNS 서비스, Active Directory, CMS 등)에 대해 단일 AWS 계정을 만든 다음 프로젝트당 별도의 AWS 계정을 만듭니다. 각 프로젝트 계정에서 권한과 정책을 할당하고 여러 계정에서 리소스 액세스를 허용할 수 있습니다.

표 3: AWS 계정 전략

여러 계정에서 통합 결제 관계를 구성하여 각 계정별로 청구서를 관리하는 복잡한 문제를 해결하고 규모의 경제를 활용할 수 있습니다. 결제 통합을 사용할 때 여러 계정이 리소스와 자격 증명을 공유하지 않습니다.

IAM 사용자 관리

적절한 수준의 권한을 가진 IAM 사용자는 새로운 IAM 사용자를 만들거나 기존 사용자를 관리 및 삭제할 수 있습니다. 높은 권한을 가진 이 IAM 사용자는 조직 내에 있는 AWS 구성을 관리하거나 AWS 리소스를 직접 평가하는 개인, 서비스 또는 애플리케이션별로 고유 IAM 사용자를 만들 수 있습니다. 여러 개체가 동일하게 공유된 사용자 자격 증명을 사용하는 것은 가급적 피해야 합니다.

IAM 그룹 관리

IAM 그룹은 하나의 AWS 계정에 있는 IAM 사용자의 모음입니다. 기능, 조직 또는 지역별로 또는 프로젝트별로 또는 IAM 사용자들이 작업을 수행하기 위해 비슷한 AWS 리소스에 액세스해야 하는 경우에는 다른 기준으로 IAM 그룹을 만들 수 있습니다. 하나 이상의 IAM 정책을 할당하여 각 IAM 그룹에 AWS 리소스에 액세스할 권한을 제공할 수 있습니다. IAM 그룹에 할당된 모든 정책은 그룹의 구성원인 IAM 사용자가 상속합니다.

예를 들어 IAM 사용자인 John이 조직 내에서 백업을 담당하고 있는데 `Archives`라고 하는 Amazon S3 버킷의 객체를 액세스해야 한다고 가정합니다. John에게 `Archives` 버킷에 액세스할 수 있도록 직접 권한을 부여할 수 있습니다. 그런데 조직이 Sally와 Betty를 John과 같은 팀에 배치합니다. John, Sally, Betty에게 개별적으로 사용자 권한을 할당하여 `Archives` 버킷에 대한 액세스 권한을 부여할 수 있지만 그룹에 권한을 할당하고 그 그룹에 John, Sally, Betty를 배치하면 유지 및 관리가 더 쉬워집니다. 추가 사용자에게 동일한 액세스 권한이 필요하면 그룹에 이들을 추가하여 권한을 부여할 수 있습니다. 어떤 사용자가 어떤 리소스에 대한 액세스 권한이 더 이상 필요하지 않을 경우 해당 리소스에 대한 액세스 권한을 부여하는 그룹에서 제거할 수 있습니다.

IAM 그룹은 AWS 리소스에 대한 액세스 권한을 관리하는 강력한 도구입니다. 특정 리소스에 대한 액세스 권한이 필요한 사용자가 한 명이더라도 해당 액세스 권한에 대한 새 AWS 그룹을 식별하거나 만들고 그룹 멤버십을 통해 사용자 액세스 권한과 그룹 수준에서 할당된 권한 및 정책을 프로비저닝하는 것이 좋습니다.

AWS 자격 증명 관리

각 AWS 계정 또는 IAM 사용자는 고유 ID이며, 고유의 장기 자격 증명을 갖습니다. 이러한 ID와 연결된 자격 증명에는 두 가지 주요 유형, 즉 (1) AWS Management Console 및 AWS 포털 페이지에 로그인하는 데 사용되는 자격 증명, (2) AWS API에 대한 프로그래밍 방식의 액세스에 사용되는 자격 증명이 있습니다.

표 4는 두 가지 유형의 로그인 자격 증명을 설명합니다.

로그인 자격 증명 유형	세부 정보
사용자 이름/암호	AWS 계정의 사용자 이름은 항상 이메일 주소입니다. IAM 사용자 이름을 사용하면 유연성이 높아집니다. AWS 계정 암호는 어느 것으로나 정의할 수 있습니다. IAM 사용자 암호는 고객이 정의하는 정책을 강제로 준수할 수 있습니다(예를 들어 최소 암호 길이 또는 영숫자 문자 사용을 요구할 수 있음).
멀티 팩터 인증(MFA)	AWS 계정 및 IAM 사용자에 적용할 수 있는 보안 수준을 높입니다. MFA를 활성화하면 사용자가 웹 사이트에 로그인할 때 사용자 이름과 암호(첫 번째 요소–고객이 알고 있는 것)뿐만 아니라 AWS MFA 디바이스의 인증 코드(두 번째 요소–고객이 갖고 있는 것)를 입력하라는 메시지가 표시됩니다. 사용자가 S3 객체를 삭제할 때 MFA를 요구할 수도 있습니다. AWS 환경에 대한 무단 액세스를 방지하기 위해 AWS 계정과 IAM 사용자에 대해 MFA를 활성화하는 것이 좋습니다. 현재 AWS는 Gemalto 하드웨어 MFA 디바이스와 가상 MFA 디바이스를 스마트폰 애플리케이션의 형태로 지원합니다.

표 4: 로그인 자격 증명

표 5는 API에 대한 프로그래밍 방식의 액세스에 사용되는 자격 증명의 유형들을 설명합니다.

액세스 자격 증명 유형	세부 정보
액세스 키	액세스 키는 AWS 서비스에 대한 API 호출의 디지털 서명에 사용됩니다. 각 액세스 키 자격 증명은 액세스 키 ID와 비밀 키로 구성됩니다. 비밀 키 부분은 AWS 계정 소유자 또는 할당된 IAM 사용자가 보안을 유지해야 합니다. 사용자는 한 번에 두 세트의 활성 액세스 키를 가질 수 있습니다. 사용자는 정기적으로 액세스 키를 교체하는 것이 좋습니다.
API 호출용 MFA	멀티 팩터 인증(MFA)을 통해 보호되는 API 액세스 권한을 사용하려면 IAM 사용자가 유효한 MFA 코드를 입력한 특정 기능인 API를 사용해야 합니다. API의 MFA 필요 여부는 IAM에서 만드는 정책에 따라 결정됩니다. AWS Management Console이 AWS 서비스 API를 호출하기 때문에 액세스를 콘솔을 통해 하든 API를 통해 하든 API에 MFA를 적용할 수 있습니다.

표 5: 프로그래밍 방식의 액세스 자격 증명

IAM 역할 및 임시 보안 자격 증명을 사용하는 권한 위임 이해

일반적으로 AWS 리소스에 액세스할 수 없는 사용자 또는 서비스에 액세스 권한을 위임하는 시나리오가 있습니다. 아래 표 6은 그러한 액세스 권한 위임을 위한 일반 사용 사례를 개략적으로 설명합니다.

사용 사례	설명
AWS 리소스에 액세스해야 하는 Amazon EC2 인스턴스에서 실행하는 애플리케이션	Amazon EC2 인스턴스에서 실행하고 Amazon S3 버킷 또는 Amazon DynamoDB 표 등의 AWS 리소스에 대한 액세스 권한이 필요한 애플리케이션은 보안 자격 증명이 있어야 AWS에 프로그래밍 방식의 요청이 가능합니다. 개발자는 각 인스턴스에 자격 증명을 배포할 수 있고 이후 그 자격 증명을 사용하여 리소스에 액세스할 수 있지만, 각 인스턴스에 장기 자격 증명을 배포하는 것은 관리가 어렵고 잠재적인 보안 위험이 될 수 있습니다.
교차 계정 액세스	리소스에 대한 액세스 권한을 관리하려면, 프로덕션 환경에서 개발 환경을 격리하는 목적 등을 위해 여러 개의 AWS 계정을 보유할 수 있습니다. 하지만 개발 환경에서 프로덕션 환경으로의 업데이트를 승격하는 경우처럼 한 계정의 사용자들이 다른 계정의 리소스에 액세스해야 하는 경우가 있습니다. 두 계정을 모두 사용하는 사용자들이 각 계정에 별도의 ID를 보유할 수 있지만, 여러 계정에 대한 자격 증명을 관리할 경우 ID를 관리하기가 어렵습니다.

사용 사례	설명
자격 증명 연동	사용자는 이미 기업 디렉토리 등 AWS 외부에 ID를 보유할 수 있습니다. 하지만 그 사용자들이 AWS 리소스로 작업하거나 리소스에 액세스하는 애플리케이션으로 작업해야 하는 경우가 있습니다. 그런 경우, 사용자는 AWS에 요청을 하기 위해 AWS 보안 자격 증명이 필요합니다.

표 6: 일반적인 권한 위임 사용 사례

IAM 역할과 임시 보안 자격 증명이 이러한 사용 사례를 처리합니다. IAM 역할을 통해 사용자 또는 서비스에 필요한 리소스에 액세스할 수 있는 권한 집합을 정의할 수 있지만, 해당 권한이 특정 IAM 사용자 또는 그룹에 연결되지는 않습니다. 대신 IAM 사용자, 모바일 및 EC2 기반 애플리케이션 또는 AWS 서비스(Amazon EC2 등)는 프로그래밍 방식으로 역할을 부여할 수 있습니다. 역할을 부여하면 사용자 또는 애플리케이션에서 AWS에 대한 프로그래밍 요청을 작성하는 데 사용할 수 있는 임시 보안 자격 증명이 반환됩니다. 이러한 임시 보안 자격 증명은 만료를 구성할 수 있고 자동으로 교체됩니다. IAM 역할과 임시 보안 자격 증명을 사용하면 모든 사용에 대한 액세스 관한이 필요한 경제에서 장기 자격 증명과 IAM 사용자를 사용하지 않아도 됩니다.

Amazon EC2의 IAM 역할

Amazon EC2의 IAM 역할은 표 6의 첫 사용 사례를 처리하는 IAM 역할을 구체적으로 구현한 것입니다. 다음 그림에서는 개발자가 `photos`라는 이름의 Amazon S3 버킷에 대한 액세스 권한이 필요한 Amazon EC2 인스턴스에서 애플리케이션을 실행하고 있습니다. 관리자가 `Get-pics` 역할을 만듭니다. 이 역할에는 버킷에 대한 읽기 권한을 부여하고 개발자가 Amazon EC2 인스턴스로 역할을 시작할 수 있는 정책이 포함됩니다. 애플리케이션이 인스턴스에서 실행되면 역할의 임시 자격 증명을 사용하여 `photos` 버킷에 액세스할 수 있습니다. 관리자는 개발자 권한을 부여하지 않아도 `photos` 버킷에 액세스할 수 있고 개발자는 자격 증명을 전혀 공유할 필요가 없습니다.

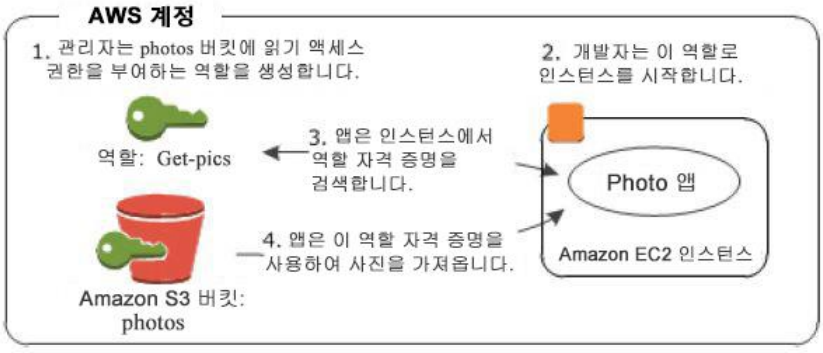

그림 4: EC2 역할의 작동 방법

1 관리자는 IAM을 사용하여 `Get-pics` 역할을 만듭니다. 이 역할에서 관리자는 Amazon EC2 인스턴스만 역할을 부여할 수 있는 것으로 규정하고 `photos` 버킷에 대한 읽기 권한만을 지정하는 정책을 사용합니다.

2 개발자는 Amazon EC2 인스턴스를 시작하고 그 인스턴스에 `Get-pics` 역할을 할당합니다.

3 애플리케이션을 실행하면 Amazon EC2 인스턴스의 인스턴스 메타데이터에서 자격 증명을 검색합니다.

4 애플리케이션은 역할 자격 증명을 사용하여 읽기 전용 권한으로 `photo` 버킷에 액세스합니다.

교차 계정 액세스

IAM 역할을 이용해 다른 AWS 계정의 IAM 사용자들이 AWS 계정 내에 있는 리소스에 액세스할 수 있게 함으로써 표 6의 두 번째 사용 사례를 처리할 수 있습니다. 이 프로세스가 교차 계정 액세스입니다. 교차 계정 액세스를 사용하면 다른 AWS 계정의 사용자와 자신의 리소스 액세스 권한을 공유할 수 있습니다.

교차 계정 액세스를 설정하려면 신뢰하는 계정(계정 A)에서 특정 리소스에 대한 액세스 권한을 신뢰할 수 있는 계정(계정 B)에 부여하는 IAM 정책을 만듭니다. 그러면 계정 B는 IAM 사용자들에게 이 액세스 권한을 위임할 수 있습니다. 계정 B는 계정 A가 부여한 권한보다 많은 액세스 권한을 IAM 사용자에게 위임할 수 없습니다.

자격 증명 연동

IAM 역할을 이용해 기업 사용자와 AWS 리소스 사이에 위치하는 자격 증명 브로커를 만들어 AWS에서 모든 사용자를 IAM 사용자로 다시 만들지 않고 인증과 권한 부여 프로세스를 관리함으로써 표 6의 세 번째 사용 사례를 처리할 수 있습니다.

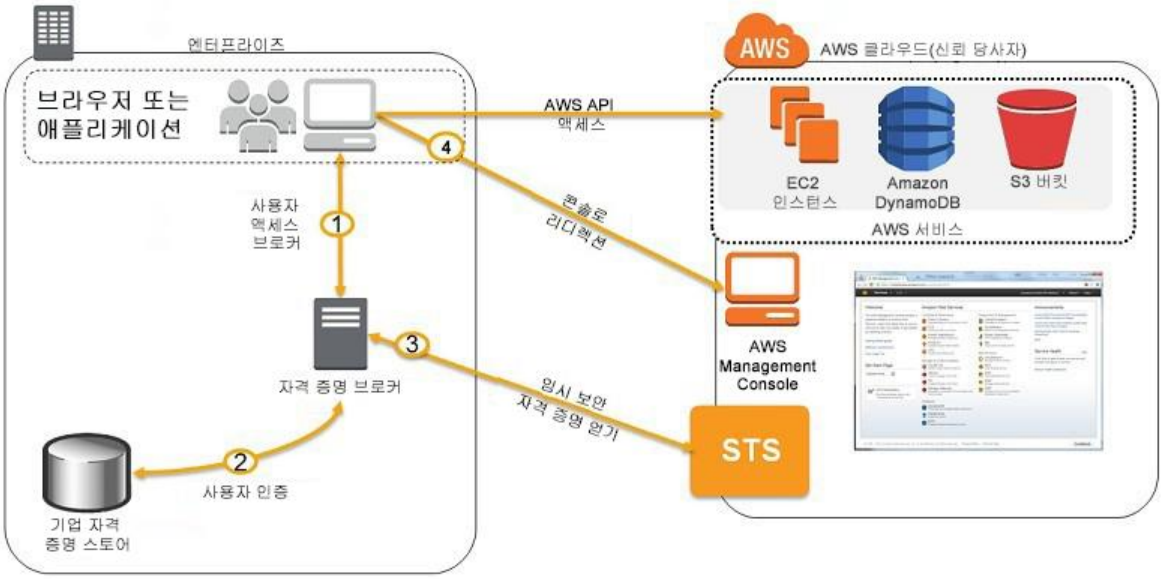

그림 5: 임시 보안 자격 증명과의 AWS 자격 증명 연동

r to:

https://aws.amazon.com/architecture/security-identity-compliance/

1. 엔터프라이즈 사용자가 자격 증명 브로커 애플리케이션에 액세스합니다.
2. 자격 증명 브로커 애플리케이션이 기업 자격 증명 스토어에 대해 사용자를 인증합니다.
3. 자격 증명 브로커 애플리케이션에 임시 보안 자격 증명을 만들 수 있도록 AWS Security Token Service(STS)에 액세스할 수 있는 권한이 있습니다.
4. 엔터프라이즈 사용자는 AWS API 또는 Management Console에 액세스할 수 있는 임시 URL을 받을 수 있습니다. AWS가 Microsoft Active Directory에 사용할 수 있는 샘플 자격 증명 브로커 애플리케이션을 제공합니다.

Amazon EC2 인스턴스에 대한 OS 수준 액세스 관리

이전 섹션에서는 AWS 서비스 인증이 필요한 리소스 액세스를 관리할 수 있는 방법들을 설명했습니다. 하지만 EC2 인스턴스에서 운영 체제에 액세스하려면 다른 자격 증명 세트가 필요합니다. 공동 책임 모델에서는 고객이 운영 체제 자격 증명을 소유하지만 AWS가 운영 체제에 대한 초기 액세스의 부트스트랩을 지원합니다.

표준 AMI에서 새 Amazon EC2 인스턴스를 시작하면 Secure Shell(SSH) 또는 Windows Remote Desktop Protocol(RDP) 등의 보안 원격 시스템 액세스 프로토콜을 사용하여 해당 인스턴스에 액세스할 수 있습니다. 운영 체제 수준에서 성공적으로 인증을 해야 자체 요구 사항에 따라 Amazon EC2 인스턴스에 액세스하고 이를 구성할 수 있습니다. Amazon EC2 인스턴스를 인증하고 원격으로 액세스할 수 있으면 원하는 운영 체제 인증 메커니즘을 설정할 수 있고, 여기에는 X.509 인증서 인증, Microsoft Active Directory 또는 로컬 운영 체제 계정 등이 있습니다.

AWS는 EC2 인스턴스 인증을 활성화할 수 있도록 Amazon EC2 키 페어라고 하는 비대칭 키 페어를 제공합니다. 업계 표준 RSA 키 페어입니다. 각 사용자는 여러 개의 Amazon EC2 키 페어가 있을 수 있지만 서로 다른 키 페어를 사용하여 새 인스턴스를 시작할 수 있습니다. EC2 키 페어는 앞에서 설명한 AWS 계정이나 IAM 사용자 자격 증명과는 관계가 없습니다. 이러한 자격 증명은 다른 AWS 서비스에 대한 액세스를 제어합니다. EC2 키 페어는 특정 인스턴스에 대한 액세스만 제어합니다.

OpenSSL과 같은 업계 표준 도구를 사용하여 자체 Amazon EC2 키 페어를 생성할 수 있습니다. 안전하고 신뢰할 수 있는 환경에서 키 페어를 생성하고 키 페어의 퍼블릭 키만 AWS에 가져옵니다. 프라이빗 키를 안전하게 저장합니다. 이 경로를 선택하는 경우 품질이 높은 난수 생성기를 사용하는 것이 좋습니다.

AWS로 Amazon EC2 키 페어를 생성할 수 있습니다. 이 경우 인스턴스를 처음 만들었을 때 RSA 키 페어의 프라이빗 및 퍼블릭 키 모두 고객에게 제공됩니다. Amazon EC2 키 페어의 프라이빗 키를 다운로드해 안전하게 저장해야 합니다. AWS는 프라이빗 키를 저장하지 않습니다. 잃어버린 경우 새 키 페어를 생성해야 합니다.

cloud-init 서비스를 사용하는 Amazon EC2 Linux 인스턴스의 경우 표준 AWS AMI로부터 새 인스턴스가 시작되면 Amazon EC2 키 페어의 퍼블릭 키는 초기 운영 체제 사용자의 **~/.ssh/authorized_keys** 파일에 추가됩니다. 그러면 사용자는 SSH 클라이언트를 사용하여 Amazon EC2 Linux 인스턴스에 연결할 수 있습니다. 그 방법은 올바른 Amazon EC2 인스턴스 사용자의 이름을 ID(예: ec2-user)로 사용하도록 클라이언트를 구성하고 사용자 인증에 프라이빗 키 파일을 제공하는 것입니다.

ec2config 서비스를 사용한 Amazon EC2 Windows 인스턴스의 경우 표준 AWS AMI로부터 새 인스턴스가 시작되면 **ec2config** 서비스가 인스턴스에 대한 새로운 무작위 관리자 암호를 설정하고 해당 Amazon EC2 키 페어의 퍼블릭 키를 사용하여 암호화합니다. 사용자는 AWS Management Console 또는 명령줄 도구를 사용하거나 암호를 해독할 해당 Amazon EC2 프라이빗 키를 제공하여 Windows 인스턴스 암호를 받을 수 있습니다. 이 암호는 Amazon EC2 인스턴스의 기본 관리 계정과 함께 Windows 인스턴스 인증에 사용할 수 있습니다.

AWS는 Amazon EC2 키를 관리하고 새로 시작된 Amazon EC2 인스턴스의 업계 표준 인증을 제공하기 위한 유연하고 실용적인 도구 집합을 제공합니다. 보안 요구 사항이 엄격한 경우 LDAP나 Active Directory 인증 등 대체 인증 메커니즘을 구현하고 Amazon EC2 키 페어 인증을 비활성화할 수 있습니다.

데이터 보호

이 섹션은 AWS 플랫폼에서의 유휴 데이터 및 전송 중인 데이터 보호를 설명합니다. 이미 자산을 식별 및 분류하고 위험 프로필에 따라 보호 목표를 설정했다고 가정합니다.

리소스 액세스 권한 부여

사용자 또는 IAM 역할이 인증되면 권한이 부여된 리소스에 액세스할 수 있습니다. 사용자가 리소스를 제어하도록 할 것인지 또는 개별 사용자 제어를 무시할 것인지에 따라 리소스 정책 또는 기능 정책을 사용하여 리소스 권한을 부여합니다.

- **리소스 정책은** 사용자가 리소스를 만든 다음 다른 사용자들에게 리소스에 대한 액세스 권한을 부여하는 경우에 적합합니다. 이 모델에서는 정책이 리소스에 직접 연결되고 누가 그 리소스로 어떤 작업을 할 수 있는지 설명합니다. 사용자는 리소스를 제어합니다. IAM 사용자에게 리소스에 대한 명시적 액세스 권한을 부여할 수 있습니다. 루트 AWS 계정은 항상 리소스 정책을 관리할 수 있는 액세스 권한이 있으며 해당 계정에서 만든 모든 리소스의 소유자입니다. 또는 사용자에게 리소스에 대한 권한을 관리할 수 있는 명시적인 액세스 권한을 부여할 수 있습니다.
- **기능 정책**(IAM 문서에서는 "사용자 기반 권한"이라고 함)은 흔히 회사 전체의 액세스 정책을 적용하는 데 사용됩니다. 기능 정책은 IAM 그룹을 사용하여 직접 또는 간접적으로 IAM 사용자에게 할당됩니다. 런타임에 부여할 역할을 할당할 수도 있습니다. 기능 정책은 사용자에게 어떤 기능(작업)이 허용 또는 거부되는지 정의합니다. 리소스 기반 정책 권한을 명시적으로 거부하면 무시됩니다.
- IAM 정책을 사용하여 리소스 권한을 특정 조건에 따라 예: 특정 날짜 및 시간 중에, 그리고 그 외의 조건에 따라 제한할 수 있습니다.
- 리소스 정책 및 기능 정책은 누적됩니다. 개별 사용자의 유효 권한은 리소스 정책과 직접 또는 그룹 멤버십을 통해 부여된 기능 권한의 조합입니다.

클라우드상의 암호화 키 저장 및 관리

암호화를 사용하는 보안 수단에는 키가 필요합니다. 클라우드에서는 온프레미스 시스템과 마찬가지로 키의 보안을 유지하는 것이 필수적입니다.

기존 프로세스를 사용하여 클라우드에서 암호화 키를 관리하거나 AWS 키 관리와 스토리지 기능에 서버 측 암호화를 활용할 수 있습니다.

자체 키 관리 프로세스를 사용하기로 결정하는 경우 다양한 접근 방식을 사용하여 키 구성 요소를 저장 및 보호할 수 있습니다. HSM(Hardware Security Module) 등 부정 조작 방지 스토리지에 키를 저장하는 것이 좋습니다. Amazon Web Services는 AWS CloudHSM이라고 하는 클라우드상의 HSM 서비스를 제공합니다. 또는 온프레미스로 키를 저장하는 HSM을 사용할 수 있고 IPSec를 통해 Amazon VPC 또는 AWS Direct Connect와 연결되는 IPSec 가상 프라이빗 네트워크(VPN) 등 보안 링크를 통해 액세스할 수 있습니다.

온프레미스 HSM 또는 CloudHSM을 사용하여 인증 및 권한 부여, 문서 서명, 트랜잭션 처리 등을 포함하여 데이터베이스 암호화, 디지털 권한 관리(DRM), 퍼블릭 키 인프라(PKI)와 같은 다양한 사용 사례와 애플리케이션을 지원할 수 있습니다. CloudHSM은 현재 SafeNet의 Luna SA HSM을 사용합니다. Luna SA는 미국 정부 보안 표준(FIPS) 140-2와 공동 표준 EAL4+ 표준에 부합하도록 제작되었으며 다양한 업계 표준 암호화 알고리즘을 지원합니다.

CloudHSM 서비스에 가입하면 CloudHSM 어플라이언스에 대한 단일 테넌트 액세스 권한을 받습니다. 각 어플라이언스는 VPC에서 리소스로 표시됩니다. AWS가 아닌 사용자가 CloudHSM의 암호화 도메인을 시작하고 관리합니다. 암호화 도메인은 사용자 키에 대한 액세스를 제한하는 논리적 및 물리적 보안 경계입니다. 오직 사용자만 자신의 키와 CloudHSM에서 수행되는 작업을 제어할 수 있습니다. Amazon 관리자는 CloudHSM 어플라이언스의 상태를 관리, 유지 보수, 모니터링하지만 암호화 도메인에 대한 액세스 권한이 없습니다. 암호화 도메인을 초기화한 후에는 EC2 인스턴스에서 클라이언트를 구성해 애플리케이션이 CloudHSM에서 제공하는 API 사용을 허용할 수 있습니다.

사용자의 애플리케이션은 PKCS#11, MS CAPI 및 Java JCA/JCE(Java Cryptography Architecture/Java Cryptography Extensions)를 포함하는 CloudHSM이 지원하는 API를 사용할 수 있습니다. CloudHSM 클라이언트는 사용자 애플리케이션에 API를 제공하며 수동으로 인증된 SSL 연결을 사용하여 CloudHSM 어플라이언스에 연결하여 각 API 호출을 구현합니다.

여러 가용 영역에서 CloudHSM을 구현하고 고가용성과 스토리지 복원성을 위해 복제할 수 있습니다.

유휴 데이터 보호

규제 또는 비즈니스 요구 사항으로 인한 이유 때문에 Amazon EBS, Amazon RDS 또는 AWS의 다른 서비스에서 Amazon S3에 저장된 유휴 데이터를 한층 더 보호해야 할 수 있습니다.

표 7에는 AWS에서 유휴 데이터 보호를 구현하는 경우 고려할 문제가 나열되어 있습니다.

문제	권장 보호 접근 방식	전략
실수로 인한 정보 노출	데이터를 기밀로 지정하고 액세스할 수 있는 사용자의 수를 제한합니다. AWS 권한을 사용하여 Amazon S3 등의 서비스 리소스에 대한 액세스 권한을 관리합니다. 암호화를 사용하여 Amazon EBS 또는 Amazon RDS에서 기밀 데이터를 보호합니다.	권한 파일, 파티션, 볼륨 또는 애플리케이션 수준의 암호화
데이터 무결성 위반	의도 또는 실수로 인한 수정으로 인해 데이터 무결성 위반이 발생하지 않도록 리소스 권한을 사용하여 데이터를 수정할 수 있는 사용자의 범위를 제한합니다. 리소스 권한을 사용하는 경우에도 권한이 있는 사용자가 실수로 삭제할 위험은 여전히 존재하기 때문에(트로이 목마가 권한이 있는 사용자의 자격 증명을 사용하여 공격할 수 있는 잠재적 가능성 등) 최소 권한 원칙이 중요함을 알 수 있습니다. 메시지 인증 코드(SHA-1/SHA-2), 또는 해시 메시지 인증 코드(HMAC), 의 자료 사용 또는 인증 암호화(AES-GCM) 등의 데이터 무결성 검사를 수행하여 데이터 무결성 위반을 감지합니다. 데이터 위반을 감지하면 백업에서 데이터를 복원할 수 있고 Amazon S3의 경우에는 이전 객체 버전에서 복원할 수 있습니다.	권한 데이터 무결성 검사(MAC/HMAC/디지털 서명/인증 암호화) 백업 버전 관리(Amazon S3)
실수로 인한 삭제	불필요한 권한과 역할 사용을 최소화하는 것은 실수로 인한 삭제나 악의적 삭제를 방지하는 가장 좋은 보호 방법입니다. Amazon S3와 같은 서비스의 경우 MFA Delete를 사용하여 멀티 팩터 인증에 객체 삭제를 요구하여 Amazon S3 객체에 대한 액세스를 권한이 있는 사용자로 제한할 수 있습니다. 데이터 위반을 감지하면 백업에서 데이터를 복원할 수 있고 Amazon S3의 경우에는 이전 객체 버전에서 복원할 수 있습니다.	권한 백업 버전 관리(Amazon S3) MFA 삭제(Amazon S3)
시스템, 인프라, 하드웨어 또는 소프트웨어 가용성	시스템 장애나 자연 재해 발생 시 백업이나 복제본에서 데이터를 복원합니다. Amazon S3 및 Amazon DynamoDB와 같은 일부 서비스는 리전 내에 있는 여러 가용 영역 간의 자동 데이터 복제를 제공합니다. 다른 서비스를 사용할 경우 고객이 복제 또는 백업을 구성해야 합니다.	백업 복제

표 7: 유휴 데이터에 대한 위협

해당하는 위협 환경을 분석하고, 다음에 간략히 설명되어 있는 것과 같이 관련 보호 기술을 활용합니다. *표 1: 샘플 자산 표* 자산을 보호하기 *위한* ISMS *설계* 섹션.

다음 섹션에서는 유휴 데이터를 보호하기 위해 AWS의 다양한 서비스를 구성하는 방법을 설명합니다.

Amazon S3에서 유휴 데이터 보호

Amazon S3는 유휴 데이터의 보호를 위해 많은 보안 기능을 제공하며, 위협 프로필에 따라 기능 사용 여부를 결정할 수 있습니다. 표 8은 이러한 기능들을 요약하여 설명합니다.

Amazon S3 기능	설명
권한	IAM 정책을 함께 버킷 수준 또는 객체 수준 권한과 사용하여 리소스를 무단 액세스로부터 보호하고 정보 누출, 데이터 무결성 위반 또는 삭제를 방지합니다.
버전 관리	Amazon S3는 객체 버전을 지원합니다. 버전 관리는 기본적으로 비활성화되어 있습니다. 버전 관리를 활성화하여 수정 또는 삭제된 객체의 새 버전을 저장하고 필요 시 손상된 객체를 복원할 수 있습니다.
복제	Amazon S3는 해당 리전 내에서 모든 가용 영역에 각 객체를 복제합니다. 복제를 하면 지리적 장애에 대 데이터 및 서비스 가용성을 제공하지만, 실수에 의한 삭제 또는 데이터 무결성 위반을 보호하지 못합니다.즉, 사본을 저장하는 모든 가용 영역에 변경 사항을 복제합니다. Amazon S3는 표준 및 RRS 옵션을 제공하는데, 옵션은 내구성 목표와 가격대가 다릅니다.
백업	Amazon S3는 자동 백업 대신 데이터 복제 및 버전 관리를 지원합니다. 하지만 애플리케이션 수준의 기술을 사용하여 Amazon S3에 저장된 데이터를 다른 AWS 리전 또는 온프레미스 백업 시스템에 백업할 수 있습니다.
암호화–서버 측	Amazon S3는 사용자 데이터의 서버 측 암호화를 지원합니다. 서버 측 암호화는 최종 사용자가 볼 수 있습니다. AWS는 각 객체에 대한 고유 암호화 키를 생성한 다음 AES-256을 사용하여 객체를 암호화합니다. 그 후 암호화 키는 AES-256을 사용하여 안전한 장소에 저장된 마스터 키로 자체적으로 암호화됩니다. 마스터 키는 정기적으로 교체됩니다.
암호화– 클라이언트 측	클라이언트 측 암호화로 자체 암호화 키를 만들고 관리합니다. 고객이 만드는 키는 클리어 텍스트로 AWS에 내보내지지 않습니다. 고객의 애플리케이션은 데이터를 암호화한 후 Amazon S3에 제출하고 Amazon S3에서 데이터를 수신한 후 해독합니다. 데이터는 암호화된 형태로 저장되고 키와 알고리즘은 고객만 알고 있습니다. 암호화 알고리즘은 데이터 암호화를 위해 대칭 또는 비대칭 키 중 어느 것이나 사용할 수 있지만 AWS에서 제공한 Java SDK는 Amazon S3에 클라이언트 측 암호화 기능을 제공합니다. 자세한 내용은 *참조 자료* 를 참조하십시오.

표 8: Amazon S3의 유휴 데이터 보호 기능

Amazon EBS에서 유휴 데이터 보호

Amazon EBS는 AWS의 추상화된 블록 스토리지 서비스입니다. 각 Amazon EBS 볼륨은 새 하드 디스크처럼 포맷되지 않은 원시 모드로 수신합니다. Amazon EBS 볼륨의 파티션 크기를 조정하고 원하는 모든 파일 시스템으로 소프트웨어 RAID 어레이를 포맷하고 최종적으로는 Amazon EBS 볼륨에서 데이터를 보호할 수 있습니다. EBS 볼륨에서 이루어지는 이 모든 결정과 작업은 AWS 작업에서 볼 수 없습니다.

Amazon EBS 볼륨을 Amazon EC2 인스턴스에 연결할 수 있습니다.

표 9에는 Amazon EC2 인스턴스에서 실행하는 운영 체제를 통한 Amazon EBS의 유휴 데이터 보호 기능에 대해 간략하게 나와 있습니다.

Amazon EBS 기능	설명
복제	각 Amazon EBS 볼륨은 파일을 저장하고 AWS는 중복성을 위해 EBS 볼륨의 사본 두 개를 만듭니다. 하지만 두 개의 사본 모두 같은 가용 영역에 상주하기 때문에 하드웨어 장애가 발생해도 Amazon EBS 복제는 유지됩니다. 장시간의 중단 또는 재해로부터 보호를 위해 사용자는 프로그램을 통해 또는 애플리케이션 수준에서 데이터를 복제하거나 백업을 만드는 것이 좋습니다.
백업	Amazon EBS는 특정 시점에 Amazon EBS 볼륨에 저장된 데이터를 포착하는 스냅샷을 제공합니다. (시스템 장애 등으로 인해) 볼륨이 손상되거나 볼륨의 데이터가 삭제되면 스냅샷에서 볼륨을 복원할 수 있습니다. Amazon EBS 스냅샷은 IAM 사용자, 그룹 및 역할에 권한을 할당할 수 있는 AWS 객체이기 때문에 권한이 있는 사용자만 Amazon EBS 백업에 액세스할 수 있습니다.
암호화: Microsoft Windows EFS	AWS에서 Microsoft Windows Server를 실행하고 데이터 기밀성의 수준을 높여야 하는 경우 EFS(Encrypted File System)를 구현하여 시스템이나 데이터 파티션에 저장된 민감한 데이터를 보호할 수 있습니다. EFS는 투명한 파일 및 폴더 암호화를 제공하는 NTFS 파일 시스템을 확장한 것으로, Windows와 Active Directory 키 관리 시설 및 PKI와 통합됩니다. EFS에서 자체적으로 키를 관리할 수 있습니다.
암호화: Microsoft Windows Bitlocker	Windows BitLocker는 Windows Server 2008 이상의 운영 체제에 포함된 볼륨(또는 단일 드라이브의 경우 파티션) 암호화 솔루션입니다. BitLocker 용도 AES 128비트 및 256비트 암호화. 기본적으로 BitLocker는 키를 저장할 수 있는 TPM(Trusted Platform Module)이 필요합니다. Amazon EC2에서는 지원하지 않습니다. 하지만 암호를 사용하도록 구성할 경우 BitLocker로 EBS 볼륨을 보호할 수 있습니다. 자세한 내용은 다음 백서를 참조하십시오. Amazon's Corporate IT Deploys SharePoint 2010 to the Amazon Web Services Cloud.

Amazon EBS 기능	설명
암호화: Linux dm-crypt	커널 버전 2.6 이상에서 실행하는 Linux 인스턴스에서는 dm-crypt를 사용하여 Amazon EBS 볼륨 및 스왑 공간에서 TDE(Transparent Data Encryption)를 구성할 수 있습니다. 키 관리에 다양한 암호와 LUKS(Linux Unified Key Setup)를 사용할 수 있습니다.
암호화: TrueCrypt	TrueCrypt는 Amazon EBS 볼륨에서 유휴 데이터의 TDE를 제공하는 타사 도구입니다. TrueCrypt는 Microsoft Windows와 Linux 운영 체제를 모두 지원합니다.
암호화 및 무결성 인증: SafeNet ProtectV	SafeNet ProtectV는 Amazon EBS 볼륨의 전체 디스크 암호화와 AMI의 부팅 전 인증을 가능하게 하는 타사 제품입니다. SafeNet ProtectV는 데이터와 기본 운영 체제의 데이터 기밀성과 데이터 무결성 인증을 제공합니다.

표 9: Amazon EBS의 유휴 데이터 보호 기능

Amazon RDS에서 유휴 데이터 보호

Amazon RDS는 Amazon EC2와 동일한 보안 인프라를 활용합니다. 추가 보호 없이 Amazon RDS 서비스를 사용할 수 있지만, 규정 준수 또는 다른 목적으로 유휴 데이터의 암호화 또는 데이터 무결성 인증이 필요한 경우 SQL 암호화 함수를 사용하여 애플리케이션 계층 또는 플랫폼 계층에서 추가적으로 보호할 수 있습니다.

예를 들면 민감한 모든 데이터베이스 필드를 암호화하는 내장 암호화 함수를 사용하고 애플리케이션 키를 사용하여 애플리케이션 계층에서 추가적으로 보호한 후 데이터베이스에 저장할 수 있습니다. 애플리케이션은 PKI 인프라의 대칭 암호화 또는 마스터 암호화 키를 제공하는 다른 비대칭 키 기술을 사용하여 키를 관리할 수 있습니다.

MySQL 암호화 함수를 사용하여 플랫폼에서 추가적으로 보호할 수 있으며, 이는 다음과 같이 설명의 형태를 띨 수 있습니다.

```
INSERT INTO Customers (CustomerFirstName,CustomerLastName) VALUES
(AES_ENCRYPT('John',@key), AES_ENCRYPT('Smith',@key);
```

플랫폼 수준의 암호화 키는 애플리케이션 수준의 암호화 키와 같이 애플리케이션 수준에서 관리할 수 있습니다. 표 10은 Amazon RDS의 플랫폼 수준 보호 옵션을 요약합니다.

Amazon RDS 플랫폼	의견
MySQL	MySQL 암호화 함수에는 암호화, 해시 및 압축이 포함됩니다. 자세한 내용은 *https://dev.mysql.com/doc/refman/5.5/en/encryption- functions.html* 섹션을 참조하십시오
Oracle	Oracle Transparent Data Encryption은 기존 보유 라이선스 사용(BYOL) 모델에 따라 Oracle Enterprise Edition용 Amazon RDS에서 지원됩니다.
Microsoft SQL	Microsoft Transact-SQL 데이터 보호 함수에는 암호화, 서명 및 해시가 포함됩니다. 자세한 내용은 *http://msdn.microsoft.com/en- us/library/ms173744* 섹션을 참조하십시오.

표 10: Amazon RDS의 플랫폼 수준 유휴 데이터 보호

SQL 범위 쿼리는 데이터의 암호화된 부분에는 더 이상 적용되지 않습니다. 예를 들어 이 쿼리는 CustomerFirstName 열의 내용이 애플리케이션 또는 플랫폼 계층에서 암호화된 경우 "John", "Jonathan", "Joan"과 같은 이름에 대해 예상된 결과를 반환하지 않습니다.

```
SELECT CustomerFirstName, CustomerLastName from Customers WHERE
CustomerName LIKE 'Jo%';"
```

다음과 같은 직접적인 비교는 CustomerFirstName이 "John"과 정확히 일치하는 모든 필드에 대한 예상 결과를 산출해 반환합니다.

```
SELECT CustomerFirstName, CustomerLastName FROM Customers WHERE
CustomerFirstName = AES_ENCRYPT('John', @key);
```

범위 쿼리는 암호화되지 않은 필드에서도 작동합니다. 예를 들어 표의 Date 필드는 범위 쿼리에서 사용할 수 있도록 암호화되지 않은 상태로 둘 수 있습니다.

단방향 함수는 고유 식별자로 사용되는 사회 보장 번호나 이에 상응하는 개인 신분증 등 개인 식별자를 난독화하는 좋은 방법입니다. 개인 식별자를 암호화하고 사용하기 전에 애플리케이션 또는 플랫폼 계층에서 해독할 수는 있지만 키 참조 HMAC-SHA1 등의 단방향 함수를 사용하여 개인 식별자를 고정 길이 해시 값으로 변환하는 것이 더 편리합니다. 상용 HMAC의 충돌은 극히 드물기 때문에 개인 식별자는 똑같이 고유합니다. 하지만 HMAC는 원래 개인 식별자로 되돌릴 수 없기 때문에 원래 개인 ID를 아는 경우가 아니라면 원래 개인으로 데이터를 다시 추적하여 동일한 키 참조 HMAC 함수를 통해 처리할 수 없습니다.

모든 리전에서 Amazon RDS는 TDE(Transparent Data Encryption)와 NNE(Native Network Encryption)를 지원하는데 모두 Oracle Database 11g Enterprise Edition의 어드밴스 보안 옵션의 구성 요소입니다. Oracle Database 11g Enterprise Edition은 기존 보유 라이선스 사용(BYOL) 모델에 따라 Amazon RDS에서 사용할 수 있습니다. 이러한 기능 사용에 따르는 추가 요금은 없습니다.

Oracle TDE는 데이터를 스토리지에 쓰기 전에 암호화하고 데이터를 스토리지에서 읽을 때 해독합니다. Oracle TDE를 사용하면 Advanced Encryption Standard(AES)와 Data Encryption Standard(Triple DES) 등의 업계 표준 암호화 알고리즘을 사용하여 표 공간 또는 특정 표 열을 암호화할 수 있습니다.

Amazon Glacier에서 유휴 데이터 보호

Amazon Glacier에 저장된 모든 데이터는 서버 측 암호화로 보호됩니다. AWS는 Amazon Glacier 아카이브에 대한 별도의 고유 암호화 키를 생성하고 AES-256을 사용하여 암호화합니다. 암호화 키는 AES-256을 사용하여 안전한 장소에 저장된 마스터 키로 자체적으로 암호화됩니다. 마스터 키는 정기적으로 교체됩니다. 더 많은 유휴 정보를 보호해야 하는 경우 Amazon Glacier에 업로드하기 전에 데이터를 암호화할 수 있습니다.

Amazon DynamoDB에서 유휴 데이터 보호

Amazon DynamoDB는 AWS의 공유 서비스입니다. 추가적인 보호 없이 DynamoDB를 사용할 수 있지만 표준 DynamoDB 서비스로 데이터 암호화 계층을 구현할 수도 있습니다. 범위 쿼리에 대한 영향 등 애플리케이션 계층에서의 데이터 보호에 대한 고려 사항은 이전 섹션을 참조하십시오.

DynamoDB는 숫자, 문자열, 원시 이진 데이터 유형의 형식을 지원합니다. DynamoDB에 암호화된 필드를 저장할 때는 원시 이진 필드 또는 Base64 인코딩 문자열 필드를 사용하는 것이 좋습니다.

Amazon EMR에서 유휴 데이터 보호

Amazon EMR은 클라우드상의 관리형 서비스입니다. AWS는 Amazon EMR을 실행하는 데 필요한 AMI를 제공하고 사용자 지정 AMI 또는 자체 EBS 볼륨을 사용할 수 없습니다. 기본적으로 Amazon EMR 인스턴스는 유휴 데이터를 암호화하지 않습니다.

Amazon EMR 클러스터는 Amazon S3 또는 DynamoDB 중 하나를 영구적인 데이터 스토어로 사용하는 경우가 많습니다. Amazon EMR 클러스터가 시작되면 영구적인 스토어에서 HDFS로 작동하거나 Amazon S3 또는 DynamoDB에서 데이터를 직접 사용하는 데 필요한 데이터를 복사할 수 있습니다.

유휴 데이터 기밀성 또는 무결성의 수준을 높이려면 표 11에 요약된 다양한 기술을 활용할 수 있습니다.

요구 사항	설명
Amazon S3 서버 측 암호화–HDFS 복사 필요 없음	데이터는 Amazon S3에만 영구적으로 저장되고 HDFS에는 전혀 복사되지 않습니다. 하둡은 Amazon S3에서 데이터를 가져오고 영구적인 로컬 사본을 만들지 않고 로컬에서 처리합니다. Amazon S3 서버 측 암호화에 대한 자세한 내용은 *Amazon S3에서 유휴 데이터 보호* 섹션을 참조하십시오.
Amazon S3 클라이언트 측 암호화	데이터는 Amazon S3에만 영구적으로 저장되고 HDFS에는 전혀 복사되지 않습니다. 하둡은 Amazon S3에서 데이터를 가져오고 영구적인 로컬 사본을 만들지 않고 로컬에서 처리합니다. 클라이언트 측 해독을 적용하려면 Hive나 Java Map Reduce 작업용 InputFormat 등의 제품에 사용자 지정 Serializer/Deserializer(SerDe)를 사용할 수 있습니다. 파일을 분할할 수 있도록 각 개별 행 또는 기록에 암호화를 적용합니다. Amazon S3 클라이언트 측 암호화에 대한 자세한 내용은 *Amazon S3에서 유휴 데이터 보호* 섹션을 참조하십시오.
애플리케이션 수준의 암호화–전체 파일 암호화	Amazon S3 또는 DynamoDB에 데이터를 저장하는 동안 애플리케이션 수준에서 데이터를 암호화하거나 데이터의 무결성을 보호할 수 있습니다(예: HMAC-SHA1 사용). 데이터를 해독하려면 Hive 또는 스크립트 또는 부트스트랩 작업에 사용자 지정 SerDe를 사용하여 Amazon S3에서 데이터를 가져오고 해독하여 처리하기 전에 HDFS로 로드합니다. 전체 파일이 암호화되기 때문에 마스터 노드 등 하나의 노드에서 이 작업을 실행해야 합니다. 특별 코덱으로 S3Distcp 등의 도구를 사용할 수 있습니다.
애플리케이션 수준의 암호화–개별 필드 암호화/구조 유지	하둡은 JSON 등 표준 SerDe를 사용할 수 있습니다. 데이터 해독은 하둡 작업의 Map 단계 중에 이루어질 수 있고 스트리밍 작업용 사용자 지정 해독 도구를 통한 표준 입력/출력 리디렉션을 사용할 수 있습니다.

요구 사항	설명
하이브리드	Amazon S3 서버 측 암호화와 클라이언트 측 암호화 및 애플리케이션 수준 암호화의 조합을 활용하는 것이 좋습니다.

표 11: Amazon EMR에서 유휴 데이터 보호

Gazzang 등의 Amazon 소프트웨어 파트너는 Amazon EMR에서 유휴 데이터와 전송 중 데이터를 보호하기 위한 특별 솔루션을 제공합니다.

데이터와 미디어의 안전한 폐기

클라우드상의 데이터 폐기는 기존의 온프레미스 환경과는 다릅니다.

AWS에 클라우드상의 데이터 삭제를 요청하면 AWS는 기본 물리적 미디어를 폐기하지 않고 스토리지 블록은 할당되지 않은 것으로 표시됩니다. AWS는 보안 메커니즘을 사용하여 블록을 다른 곳에 재할당합니다. 블록 스토리지를 프로비저닝하면 하이퍼바이저 또는 가상 머신 관리자(VMM)가 인스턴스가 쓰기를 한 블록을 추적합니다. 인스턴스에 스토리지 블록에 쓰기를 하면 이전 블록을 제로 클리어된 후 데이터 블록으로 덮어쓰기됩니다. 인스턴스가 이전에 쓰기를 한 블록으로부터 읽기를 시도하는 경우 이전에 저장된 데이터가 반환됩니다. 인스턴스가 이전에 쓰기를 하지 않은 블록으로부터 읽기를 시도하는 경우 하이퍼바이저는 디스크의 이전 데이터를 제로 클리어하고 인스턴스에 0을 반환합니다.

AWS가 미디어의 수명이 다해 하드웨어 결함이 생겼다고 판단하면 AWS는 DoD(국방부) 5220.22-M("National Industrial Security Program Operating Manual") 또는 NIST SP 800-88("Guidelines for Media Sanitization")에 설명된 기술에 따라 폐기 프로세스의 일환으로 데이터를 삭제합니다.

클라우드상의 데이터 삭제에 대한 자세한 내용은 AWS 보안 프로세스 백서를 참조하십시오. (참조 자료 참조).

데이터를 안전하게 폐기하기 위한 추가 제어가 필요한 규제 또는 비즈니스상의 이유가 있는 경우 클라우드상에 저장되지 않는 고객 관리 키를 사용하여 유휴 데이터 암호화를 구현할 수 있습니다. 이전 프로세스를 따르는 것 외에 폐기된 데이터 보호에 사용하는 키를 삭제하여 복구가 불가능하게 만듭니다.

전송 중 데이터 보호

클라우드 애플리케이션은 인터넷 등 퍼블릭 링크를 통해 통신하는 경우가 많기 때문에 클라우드에서 애플리케이션을 실행할 때 전송 중 데이터를 보호하는 것이 중요합니다. 여기에는 클라이언트와 서버 간 네트워크 트래픽과 서버 간 네트워크 트래픽을 보호하는 일이 필요합니다.

표 12에는 인터넷 등 퍼블릭 링크를 통한 통신에 대한 일반적인 문제가 나열되어 있습니다.

문제	의견	권장 보호
실수로 인한 정보 노출	기밀 데이터에 대한 액세스는 제한되어야 합니다. 데이터가 퍼블릭 네트워크를 통과할 때 암호화를 통해 누출되지 않도록 보호해야 합니다.	IPSec ESP 및/또는 SSL/TLS를 사용하여 전송 데이터를 암호화합니다.
데이터 무결성 위반	데이터가 [illegible] 또는 실수로 인한 수정으로 데이터 무결성 위반이 발생하지 않도록 해야 합니다.	IPSec ESP 및/또는 SSL/TLS를 사용하여 데이터 무결성을 인증합니다.
피어 자격 증명 위반/자격 증명 스푸핑/중간자 공격	암호화와 데이터 무결성 인증은 통신 채널 보호에 중요합니다. 연결 원격 엔드의 자격 증명을 인증하는 것도 중요합니다. 원격 엔드가 공격자이거나 의도한 수신자에 대한 연결을 릴레이하는 사기꾼일 경우 암호화된 채널이 쓸모가 없습니다.	사전에 공유한 키 또는 X.509 인증서가 있는 IKE에는 IPSec을 사용하여 원격 엔드를 인증합니다. 또는 서버 일반 이름(CN) 또는 대체 이름(AN/SAN)에 따라 서버 인증서 인증에 SSL/TLS를 사용합니다.

표 12: 전송 중 데이터에 대한 위협

AWS의 서비스는 전송 중 데이터 보호를 위한 IPSec 및 SSL/TLS 모두에 대한 지원을 제공합니다. IPSec은 대부분의 경우 네트워크 인프라에서 IP 프로토콜 스택을 확장하는 프로토콜이며 상위 계층의 애플리케이션이 수정 없이 안전하게 통신할 수 있습니다. 한편 SSL/TLS는 세션 계층에서 작동하고 타사 SSL/TLS 래퍼가 있는 동안에는 애플리케이션 계층에서도 지원이 필요한 경우가 많습니다.

다음 섹션에서는 전송 중 데이터 보호에 대한 자세한 정보를 제공합니다.

AWS 퍼블릭 클라우드 서비스에 대한 애플리케이션 및 관리자 액세스 관리

AWS 퍼블릭 클라우드에서 실행되는 애플리케이션에 액세스할 때 연결은 인터넷을 통과합니다. 대부분의 경우 보안 정책은 인터넷을 안전하지 않은 통신 미디엄으로 간주하고 전송 중에 애플리케이션 데이터 보호를 요구합니다.

표 13은 퍼블릭 클라우드 서비스에 액세스할 때 전송 중 데이터 보호에 대한 접근 방식을 간략하게 설명합니다.

프로토콜/시나리오	설명	권장 보호 접근 방식
HTTP/HTTPS 트래픽(웹 애플리케이션)	기본적으로 HTTP 트래픽은 보호되지 않습니다. HTTPS라고 하는 HTTP 트래픽의 SSL/TLS 보호는 업계 표준이며 여러 웹 서버와 브라우저가 지원합니다. HTTP 트래픽에는 웹 페이지에 대한 클라이언트 액세스뿐만 아니라 웹 서비스(REST 기반 API)도 포함됩니다.	서버 인증서 인증에 HTTPS(SSL/TLS를 통한 HTTP)를 사용합니다.
HTTPS 오프로드(웹 애플리케이션)	특히 민감한 데이터의 경우 HTTPS 사용을 권하는 경우가 많지만 SSL/TLS 처리를 하려면 웹 서버와 클라이언트 양쪽의 추가 CPU와 메모리 리소스가 필요합니다. 이로 인해 수천 개의 SSL/TLS 세션을 처리하는 웹 서버에 상당한 로드가 발생할 수 있습니다. 제한된 수의 SSL/TLS 연결만 종료되는 클라이언트가 받는 영향은 이보다 적습니다.	Elastic Load Balancing에서 HTTP 처리를 오프로드하여 전송 중 데이터 보호 중에 웹 서버에 대한 영향을 최소화합니다. SSL을 통한 HTTP 등의 애플리케이션 프로토콜을 사용하여 인스턴스에 대한 백엔드 연결을 추가로 보호합니다.
RDP(Remote Desktop Protocol) 트래픽	퍼블릭 클라우드에서 Windows Terminal Services에 액세스하는 사용자는 보통 Microsoft Remote Desktop Protocol(RDP)을 사용합니다. 기본적으로 RDP 연결은 기본 SSL/TLS 연결을 설정합니다.	최적의 보호를 위해 액세스하고 있는 Windows 서버에 신뢰할 수 있는 X.509 인증서를 발행하여 자격 증명 스푸핑 또는 중간자 공격을 방지해야 합니다. 기본적으로 Windows RDP 서버는 자체 서명 인증서를 사용하는데 신뢰할 수 없기 때문에 사용해서는 안 됩니다.

프로토콜/시나리오	설명	권장 보호 접근 방식
SSH(Secure Shell) 트래픽	SSH는 Linux 서버에 관리자 연결을 설정하는 좋은 접근 방식입니다. SSH 는 SSL처럼 클라이언트와 서버 사이에 안전한 통신 채널을 제공합니다. 또한 SSH는 SSH를 기반으로 한 X-Windows 등의 애플리케이션을 실행하고 전송 중 애플리케이션 세션을 보호하는 데 사용해야 하는 터널링도 지원합니다.	권한이 없는 사용자 계정을 사용하여 SSH 버전 2를 사용합니다.
데이터베이스 서버 트래픽	클라이언트나 서버가 클라우드상의 데이터베이스에 액세스해야 하는 경우 인터넷도 통과해야 합니다.	대부분의 최신 데이터베이스는 기본 데이터베이스 프로토콜용 SSL/TLS 래퍼를 지원합니다. Amazon EC2에서 실행하는 데이터베이스 서버의 경우 전송 중 데이터 보호에 이 접근 방식을 사용하는 것이 좋습니다. Amazon RDS는 일부 경우 SSL/TLS에 대한 지원을 제공합니다.

표 13: 퍼블릭 클라우드에 액세스할 때 전송 중 애플리케이션 데이터 보호

AWS 서비스를 관리할 때 전송 중 데이터 보호

AWS Management Console 또는 AWS API를 사용하여 Amazon EC2와 Amazon S3 등의 AWS 서비스를 관리할 수 있습니다. 서비스 관리 트래픽의 예에는 새 Amazon EC2 인스턴스 시작, Amazon S3 버킷에 객체 저장 또는 Amazon VPC에서 보안 그룹 수정이 포함됩니다.

AWS Management Console은 클라이언트 브라우저와 콘솔 서비스 엔드포인트 사이에 SSL/TLS를 사용하여 AWS 서비스 관리 트래픽을 보호합니다. 트래픽이 암호화되고 데이터 무결성이 인증되고 클라이언트 브라우저가 X.509 인증서를 사용하여 콘솔 서비스 엔드포인트의 자격 증명을 인증합니다. 클라이언트 브라우저와 콘솔 서비스 엔드포인트 사이에 SSL/TLS 세션 설정 후에는 모든 HTTP 트래픽이 SSL/TLS 세션 내에서 보호됩니다.

또는 AWS API를 사용하여 애플리케이션이나 타사 도구에서 직접 또는 SDK나 AWS 명령줄 도구를 통해 AWS의 서비스를 관리합니다. AWS API는 HTTPS를 통한 웹 서비스(REST)입니다. SSL/TLS 세션은 사용되는 API에 따라 클라이언트와 특정 AWS 서비스 엔드포인트 사이에 설정되고 SOAP/REST 엔벌로프와 사용자 페이로드 등 이후 모든 트래픽이 SSL/TLS 세션 내에서 보호됩니다.

Amazon S3로 전송 중인 데이터 보호

AWS 서비스 관리 트래픽과 마찬가지로 Amazon S3는 HTTPS를 통해 액세스됩니다. 여기에는 모든 Amazon S3 서비스 관리 요청과 Amazon S3에서 저장/검색되는 객체의 내용과 같은 사용자 페이로드 및 관련 메타데이터가 포함됩니다.

AWS 서비스 콘솔을 Amazon S3 관리에 사용하는 경우 클라이언트 브라우저와 서비스 콘솔 엔드포인트 사이에 SSL/TLS 보안 연결이 설정됩니다. 이후 모든 트래픽은 이 연결 내에서 보호됩니다.

Amazon S3 API를 직접 또는 간접적으로 사용하는 경우 클라이언트와 Amazon S3 엔드포인트 사이에 SSL/TLS 연결이 설정되고 이후 모든 HTTP, 사용자 페이로드 트래픽은 보호되는 세션 내에서 캡슐화됩니다.

Amazon RDS로 전송 중인 데이터 보호

동일한 리전의 Amazon EC2 인스턴스에서 Amazon RDS로 연결하는 경우 AWS 내부 네트워크 트래픽을 사용할 수 있으며 인터넷 통신 트래픽을 보호하기 위해 SSL/TLS를 사용하는 것이 좋습니다.

SSL/TLS는 서버 X.509 인증서, 데이터 무결성 인증 및 클라이언트와 서버 연결을 위한 데이터 암호화를 통해 피어 인증을 제공합니다.

SSL/TLS는 현재 Amazon RDS MySQL 및 Microsoft SQL 인스턴스 연결에 지원됩니다. 두 제품 모두 Amazon Web Services가 MySQL 또는 Microsoft SQL 리스너와 연결된 단일 자체 서명 인증서를 제공합니다. 자체 서명 인증서를 다운로드하고 신뢰할 수 있는 인증서로 지정할 수 있습니다. 이렇게 하면 자격 증명 인증이 가능하고 서버 측에서 중간자 또는 자격 증명 스푸핑 공격을 방지합니다. SSL/TLS는 클라이언트와 서버 사이 통신 채널의 기본 암호화와 데이터 무결성 인증을 가능하게 합니다. AWS의 모든 Amazon RDS MySQL 인스턴스에 동일한 자체 서명 인증서를 사용하고 AWS의 모든 Amazon RDS Microsoft SQL 인스턴스에서는 또 다른 단일 자체 서명 인증서를 사용하기 때문에 피어 자격 증명 인증을 통해 개별적인 인스턴스 인증을 할 수 없습니다. SSL/TLS를 통한 개별적인 서버 인증이 필요한 경우 Amazon EC2와 자체 관리하는 관계형 데이터베이스 서비스를 활용해야 합니다.

Oracle NNE용 Amazon RDS는 데이터베이스에서 송수신되는 데이터를 암호화합니다. Oracle NNE를 사용하면 AES와 Triple DES 등의 업계 표준 암호화 알고리즘을 사용하여 Oracle Net Services를 통해 이동하는 네트워크 트래픽을 암호화할 수 있습니다.

Amazon DynamoDB로 전송 중인 데이터 보호

동일한 리전의 다른 Amazon 서비스에서 Amazon DynamoDB로 연결하는 경우 AWS 네트워크의 보안을 사용할 수 있지만 인터넷으로 DynamoDB에 연결하는 경우 SSL/TLS를 통한 HTTP(HTTPS)를 사용하여 DynamoDB 서비스 엔드포인트에 연결해야 합니다. DynamoDB에 대한 액세스 및 인터넷을 통한 모든 연결에 HTTP를 사용하지 마십시오.

Amazon EMR로 전송 중인 데이터 보호

Amazon EMR에는 여러 개의 애플리케이션 통신 경로가 포함되며 각각의 경로에는 전송 중 데이터를 [illegible] 표 14는 권장하는 통신 경로와 보호 접근 방식을 간략히 설명합니다.

Amazon EMR 트래픽 유형	설명	권장 보호 접근 방식
하둡 노드 간	하둡 마스터, 작업자, 코어 노드는 모두 독점적인 일반 TCP 연결을 사용하여 서로 통신합니다. 하지만 Amazon EMR의 모든 하둡 노드는 동일한 가용 영역에 상주하고 물리적 및 인프라 계층에서 보안 표준에 의해 보호됩니다.	모든 노드가 동일한 시설에 상주하기 때문에일반적으로 추가적인 보호는 필요하지 않습니다.
하둡 클러스터와 Amazon S3 간	Amazon EMR은 HTTPS를 사용하여 DynamoDB와 Amazon EC2 사이에 데이터를 교환합니다. 자세한 내용은 *Amazon S3로 전송 중인 데이터 보호* 섹션을 *참조하십시오.*	기본적으로 HTTPS를 사용합니다.
하둡 클러스터와 Amazon DynamoDB 간	Amazon EMR은 HTTPS를 사용하여 Amazon S3와 Amazon EC2 사이에 데이터를 교환합니다. 자세한 내용은 *Amazon DynamoDB로 전송 중인 데이터 보호* 섹션을 참조하십시오.	기본적으로 HTTPS를 사용합니다.

Amazon EMR 트래픽 유형	설명	권장 보호 접근 방식
사용자 또는 애플리케이션의 하둡 클러스터 액세스	온프레미스 클라이언트나 애플리케이션은 인터넷을 통해 스크립트(SSH 기반 액세스), REST 또는 Thrift나 Avro 등의 프로토콜을 사용하여 Amazon EMR 클러스터에 액세스할 수 있습니다.	애플리케이션에 대한 대화형 액세스 또는 SSH 내의 다른 프로토콜을 터널링하는 데 SSH를 사용합니다. Thrift, REST 또는 Avro 사용 시 SSL/TLS를 사용합니다.
하둡 클러스터에 대한 관리자 액세스	Amazon EMR 클러스터 관리자는 일반적으로 SSH를 사용하여 클러스터를 관리합니다.	SSH를 Amazon EMR 마스터 노드에 사용합니다.

표 14: Amazon EMR로 전송 중인 데이터 보호

운영 체제와 애플리케이션 보호

AWS의 공동 책임 모델로 운영 체제와 애플리케이션 보안을 관리합니다. Amazon EC2는 웹 서[illegible]자 지정 애플리케이션으로 다양한 운영 체제의 인스턴스를 시작할 수 있는 진정한 가상 [illegible] 체제와 애플리케이션의 보안을 단일 보안 빌드 리포지토리 한 곳에서 관리할 수 있습니다. 사전 구성된 AMI를 보안 요구 사항에 맞게 구축 및 테스트할 수 있습니다.

권장 사항:

- 루트 API 액세스 키 및 보안 키 비활성화
- 보안 그룹을 사용해 제한적인 IP 범위의 인스턴스로 액세스를 제한할 수 있습니다.
- 암호는 사용자 시스템에서 .pem 파일을 보호합니다.
- 직원이 회사를 그만두거나 더 이상 액세스가 필요하지 않으면 인스턴스의 authorized_keys 파일에서 키를 삭제합니다.
- 자격 증명 회전(DB, 액세스 키)
- IAM 사용자 액세스 관리자 및 IAM 사용자가 마지막으로 사용한 액세스 키를 사용해 최소 권한 점검을 정기적으로 실행합니다.
- 배스천 호스트를 사용해 제어 능력과 가시성을 확보합니다.

이 섹션은 AMI에 대한 보안 강화 표준의 포괄적인 목록을 제공하기 위해 마련된 것이 아닙니다. 업계에서 허용되는 시스템 보안 강화 표준 제공 기관에는 다음이 포함되나 이에 국한되지 않습니다.

- Center for Internet Security(CIS)
- ISO(국제 표준화 기구)
- SysAdmin Audit Network Security(SANS) Institute
- NIST(National Institute of Standards Technology)

모든 시스템 구성 요소에 대한 구성 표준을 개발하는 것이 좋습니다. 이러한 표준은 알려진 모든 보안 취약성을 해결하고 업계에서 허용되는 시스템 보안 강화 표준과 일치해야 합니다.

게시된 AMI가 모범 사례를 위반했거나 AMI를 실행하는 고객에게 중대한 위험을 일으킨다는 사실이 확인된 경우 AWS는 퍼블릭 카탈로그에서 AMI를 제거하고 게시자 또는 AMI를 실행하는 사람들에게 확인된 내용을 알릴 권한을 갖습니다.

사용자 지정 AMI 생성

조직의 특정 요구 사항에 맞는 자체 AMI를 생성해 내부(프라이빗) 또는 외부(퍼블릭)용으로 게시할 수 있습니다. 고객은 AMI 게시자로서 프로덕션에 사용하는 머신 이미지의 초기 보안 태세에 대해 책임이 있습니다. AMI에 적용하는 보안 제어는 특정 시점에 효율적이며 동적이 아닙니다. 비즈니스 요건에 맞고 AWS 이용 방침을 위반하지 않는 방식으로 프라이빗 AMI를 구성할 수 있습니다. 자세한 내용은 Amazon Web Services 이용 정책 – http://*aws.amazon.com/aup/*를 참조하십시오.

하지만 AMI을 사용해서 시작하는 사용자는 보안 전문가가 아니기 때문에 특정 최소 보안 표준을 준수하는 것이 좋습니다.

AMI 게시 전에 게시된 소프트웨어가 최신 상태로 업데이트되어 있고 관련 보안 패치가 마련되어 있는지 확인하고 표 15에 나열된 정리 및 보안 강화 작업을 수행합니다.

영역	권장 작업
보안성이 낮은 애플리케이션 비활성화	네트워크를 통해 또는 보안성이 낮은 다른 방식을 통해 클리어 텍스트로 사용자를 인증하는 서비스와 프로토콜을 비활성화합니다.

영역	권장 작업
노출 최소화	스타트업 시 필수적이지 않은 네트워크 서비스를 비활성화합니다. 관리자 서비스(SSH/RDP)와 필수적인 애플리케이션에 필요한 서비스만 시작해야 합니다.
자격 증명 보호	디스크 및 구성 파일에서 모든 AWS 자격 증명을 안전하게 삭제합니다.
자격 증명 보호	디스크 및 구성 파일에서 타사 자격 증명을 모두 안전하게 삭제합니다.
자격 증명 보호	시스템에서 모든 추가 인증서 또는 키 구성 요소를 안전하게 제거합니다.
자격 증명 보호	설치된 소프트웨어가 기본 내부 계정과 암호를 사용해서는 안 됩니다.
건전한 거버넌스 실시	시스템은 Amazon Web Services 이용 방침을 위반하지 않아야 합니다. 위반의 예로는 오픈 SMTP 릴레이 또는 프록시 서버가 있습니다. 자세한 내용은 Amazon Web Services 이용 정책 – http://*aws.amazon.com/aup/*를 참조하십시오.

표 15: AMI 게시 전 정리 작업

표 16과 17에는 추가적인 운영 체제별 정리 작업이 나열되어 있습니다. 표 16에는 Linux AMI 보안 유지 단계가 나열되어 있습니다.

영역	보안 강화 활동
안전한 서비스	sshd가 퍼블릭 키 인증만 허용하도록 구성합니다. **PubkeyAuthentication** 을 **Yes** 로, **PasswordAuthentication** 을 **No** 로 설정합니다(**sshd_config**에서).
안전한 서비스	인스턴스를 만들 때 고유 SSH 호스트 키를 생성합니다. AMI가 **cloud-init**을 사용하는 경우, 이를 자동으로 처리합니다.
자격 증명 보호	로그인에 사용할 수 없고 기본 암호를 보유할 수 없도록 모든 사용자 계정의 암호를 제거하고 비활성화합니다. 각 계정에 대해 **passwd -l <USERNAME>**을 실행합니다.
자격 증명 보호	모든 사용자 SSH 퍼블릭 및 프라이빗 키 페어를 안전하게 삭제합니다.
데이터 보호	민감한 데이터가 포함된 모든 셸 기록과 시스템 로그 파일을 안전하게 삭제합니다.

표 16: Linux/UNIX AMI 보안 유지

표 17에는 Windows AMI 보안 유지 단계가 나열되어 있습니다.

영역	보안 강화 활동
자격 증명 보호	인스턴스를 생성할 때 활성화된 모든 사용자 계정에 무작위로 생성한 새 암호가 있어야 합니다. 부팅 시 관리자 계정에 대해 EC2 Config 서비스가 이 작업을 하도록 구성할 수 있지만 이미지를 번들링하기 전에 명시적으로 그렇게 해야 합니다.

영역	보안 강화 활동
자격 증명 보호	게스트 계정이 비활성화되어야 합니다.
데이터 보호	Windows 이벤트 로그를 지웁니다.
자격 증명 보호	AMI가 Windows 도메인의 일부가 아니어야 합니다.
노출 최소화	필수적이지 않지만 기본적으로 활성화되어 있는 파일 공유, 인쇄 스풀러, RPC 및 기타 Windows 서비스를 활성화하지 마십시오.

표 17: Windows AMI 보안 유지

부트스트래핑

보안이 강화된 AMI를 인스턴스화한 후에도 부트스트래핑 애플리케이션을 사용하여 보안 제어를 수정하고 업데이트할 수 있습니다. 일반적인 부트스트래핑 애플리케이션에는 Puppet, Chef, Capistrano, Cloud-Init, Cfn-Init가 있습니다. 타사 도구를 사용하지 않고도 사용자 지정 부트스트래핑 Bash 또는 Microsoft Windows PowerShell 스크립트를 실행할 수도 있습니다.

다음은 고려할 부트스트랩 작업입니다.

- 보안 소프트웨어 업데이트는 AMI의 패치 수준 이상의 최신 패치, 서비스 팩 및 중요 업데이트를 설치합니다.
- 초기 애플리케이션 패치는 AMI로 포착된 현재 애플리케이션 수준 빌드 이상의 애플리케이션 수준 업데이트를 설치합니다.
- 컨텍스트 데이터와 구성은 예를 들어 프로덕션, 테스트 또는 DMZ/내부 등 인스턴스가 시작되는 환경별 구성을 적용하는 인스턴스를 활성화합니다.
- 원격 보안 모니터링 및 관리 시스템에 인스턴스를 등록합니다.

패치 관리

AMI와 라이브 인스턴스의 패치 관리는 고객의 책임입니다. 패치 관리를 제도화하고 서면 절차를 유지하는 것이 좋습니다.

운영 체제와 주요 애플리케이션에 대해 타사 패치 관리 시스템을 사용할 수 있지만 모든 소프트웨어와 시스템 구성 요소의 재고를 보관하고 각 시스템에 설치된 보안 패치의 목록을 최신 공급업체 보안 패치 목록과 비교하여 현재 공급업체 패치가 설치되어 있는지 확인하는 것이 좋습니다.

새로운 보안 취약성을 식별하고 취약성에 위험 순위를 할당하는 프로세스를 구현하십시오. 최소한 가장 중요하고 가장 위험이 높은 취약성의 순위를 "높음"으로 지정하십시오.

퍼블릭 AMI 보안 제어

중요한 자격 증명을 공개적으로 공유할 경우 AMI에 두지 않도록 주의하십시오. 자세한 내용은 퍼블릭 AMI를 안전하게 공유하고 사용하는 방법에 대한 자습서 *http://aws.amazon.com/articles/0155828273219400*을 참조하십시오.

시스템을 맬웨어로부터 보호

바이러스, 웜, 트로이 목마, 루트킷, 봇네트, 스팸 등의 위협으로부터 기존의 인프라를 보호하는 것처럼 클라우드상의 시스템을 보호하십시오.

개별 인스턴스와 전체 클라우드 시스템에 맬웨어가 감염되는 경우의 영향을 이해해야 합니다. 즉, 사용자가 의도 또는 실수로 Linux 또는 Windows 시스템에서 프로그램을 실행하면 실행 파일은 해당 사용자에 권한을 위임합니다(일부 경우에는 다른 사용자를 가장). 코드는 시작한 사용자가 권한이 있는 모든 작업을 수행할 수 있습니다. 사용자는 신뢰할 수 있는 코드만을 실행하도록 해야 합니다.

시스템에서 신뢰할 수 없는 코드를 실행하는 경우 시스템이 통제를 벗어나 다른 사람에게 속하게 됩니다. 수퍼유저 또는 관리자 권한을 가진 사용자가 신뢰할 수 없는 프로그램을 실행하면 프로그램이 실행된 시스템을 더 이상 신뢰할 수 없게 됩니다. 악성 코드가 운영 체제의 부분들을 변경하거나 루트킷을 설치하거나 시스템을 평가하기 위한 백도어를 설정할 수 있습니다. 데이터를 삭제하거나 데이터 무결성을 위반하거나 서비스의 가용성이 저하되거나 정보가 타사에 은밀하게 또는 공공연하게 누출될 수도 있습니다.

코드가 실행된 인스턴스는 감염된 것으로 간주하십시오. 감염된 인스턴스가 Single Sign-On 환경의 일부이거나 인스턴스 간의 액세스를 위한 암시적 신뢰 모델이 있는 경우 감염은 개별 인스턴스를 넘어 전체 시스템과 그 이상으로 빠르게 퍼져나갈 수 있습니다. 이런 규모의 감염은 금세 데이터 누출, 데이터 및 서비스 위반을 초래할 수 있고 회사의 평판을 떨어뜨릴 수 있습니다. 또한 예를 들어 타사에 서비스를 노출시키거나 클라우드 리소스를 과도하게 사용하는 경우 직접적인 재정적 결과를 가져올 수 있습니다. 맬웨어의 위협을 관리해야 합니다.

표 18은 맬웨어 방지에 대한 몇 가지 일반적인 접근 방식을 간략하게 설명합니다.

요소	일반적인 접근 방식
신뢰할 수 없는 AMI	신뢰할 수 있는 AMI만을 사용하여 인스턴스를 시작합니다. 신뢰할 수 있는 AMI에는 AWS가 제공하는 표준 Windows 및 Linux AMI와 신뢰할 수 있는 타사의 AMI가 포함됩니다. 표준 및 신뢰할 수 있는 AMI로부터 자체 사용자 지정 AMI를 생성할 경우 적용할 추가 소프트웨어와 설정도 신뢰할 수 있어야 합니다. 신뢰할 수 없는 타사 AMI를 시작하면 전체 클라우드 환경이 손상 및 감염될 수 있습니다.
신뢰할 수 없는 소프트웨어	신뢰할 수 있는 소프트웨어 공급자의 신뢰할 수 있는 소프트웨어만 설치 및 실행합니다. 신뢰할 수 있는 소프트웨어 공급자는 업계에서 인정 받는 안전하고 책임감 있는 방식으로 소프트웨어를 개발하고 소프트웨어 패키지에 악성 코드를 허용하지 않는 공급자입니다. 오픈 소스 소프트웨어도 신뢰할 수 있는 소프트웨어이며 자체 실행 파일을 컴파일할 수 있어야 합니다. 소스 코드가 악성이 아닌지 확인하기 위해 세심하게 코드 리뷰를 수행하는 것이 좋습니다. 신뢰할 수 있는 소프트웨어 공급자는 다운로드하는 소프트웨어의 무결성을 확인할 수 있도록 코드 서명 인증서를 사용하여 소프트웨어에 서명하거나 제품의 MD5 또는 SHA-1 서명을 제공합니다.
신뢰할 수 없는 소프트웨어	신뢰할 수 있는 소스에서 신뢰할 수 있는 소프트웨어를 다운로드합니다. 인터넷 또는 네트워크의 다른 부분에 있는 임의의 소프트웨어 소스는 실제로 다른 경우라면 합법적이고 명성이 높았을 소프트웨어 패키지 안에서 맬웨어를 배포하고 있을 수도 있습니다. 신뢰할 수 있는 소스에서 맬웨어가 들어오는 것을 방지하기 위해 MD5 또는 SHA-1 서명을 제공할 수 있기 때문에 그러한 서명을 신뢰해서는 안 됩니다. 사용자가 설치 및 사용할 수 있는 신뢰할 수 있는 소프트웨어를 제공하는 자체 내부 소프트웨어 리포지토리를 설정하는 것이 좋습니다. 사용자는 인터넷에 있는 임의의 소스에서 소프트웨어를 다운로드하고 설치하는 위험한 행동을 피해야 합니다.
최소 권한의 원칙	사용자에게 작업을 수행하는 데 필요한 최소의 권한을 부여합니다. 그렇게 하면 사용자가 감염된 실행 파일을 실수로 시작하더라도 인스턴스와 더 넓은 클라우드 시스템에 대한 영향을 최소화할 수 있습니다.
패칭	외부로 연결되는 시스템과 내부 시스템을 최신 보안 수준으로 패칭합니다. 웜은 네트워크의 패칭되지 않은 시스템을 통해 퍼지는 경우가 많습니다.
봇네트	기존의 바이러스, 트로이 목마 또는 웜 전파 등에 의한 감염이 개별 인스턴스 이상으로 퍼지고 더 넓은 플릿을 감염시키는 경우 원격 공격자가 제어할 수 있는 감염된 호스트 네트워크인 봇네트를 만드는 악성 코드가 포함될 수 있습니다. 봇네트 감염을 방지하기 위해 이전의 모든 권장 사항을 따르십시오.
스팸	감염된 시스템은 공격자들에 의해 대량의 원치 않는 메일(스팸)을 전송하는 데 사용될 수 있습니다. AWS는 Amazon EC2 인스턴스가 보낼 수 있는 이메일의 양을 제한하는 특별한 제어 수단을 제공하지만 일차적으로 고객에게 감염을 방지할 책임이 있습니다. 스팸을 퍼뜨릴 수 있고 AWS 이용목적 제한방침을 위반할 수도 있는 SMTP 오픈 릴레이를 피합니다. 자세한 내용은 Amazon Web Services 이용 정책 – http://aws.amazon.com/aup/를 참조하십시오.

요소	일반적인 접근 방식
안티바이러스/스팸 방지 소프트웨어	반드시 시스템에 평판이 좋은 최신 안티바이러스 및 스팸 방지 솔루션을 사용합니다.
호스트 IDS 소프트웨어	많은 AWS 고객은 오픈 소스 제품인 OSSEC 등 파일 무결성 확인 및 루트킷 탐지 소프트웨어 등의 호스트 기반 IDS 소프트웨어를 설치합니다. 이러한 제품을 사용하여 중요한 시스템 파일과 폴더를 분석하고 신뢰할 수 있는 상태를 반영하는 체크섬을 계산한 후 이러한 파일이 수정되었는지 확인하고 수정되었다면 시스템 관리자에게 알립니다.

표 18: 맬웨어 방지에 대한 접근 방식

인스턴스가 감염되면 안티바이러스 소프트웨어는 감염을 탐지하고 바이러스를 제거할 수도 있습니다. 가장 안전하고 널리 권장하는 접근 방식, 즉 모든 시스템 데이터를 저장한 다음 신뢰할 수 있는 소스로부터 모든 시스템, 플랫폼 및 애플리케이션 실행 파일을 재설치하고 백업만을 사용해 데이터를 복원하는 방식이 좋습니다.

손상 및 침해 완화

AWS는 고객이 솔루션을 구축하는 기반이 되는 글로벌 인프라를 제공하는데 이 중 많은 부분이 인터넷과 연결되어 있습니다. 고객 솔루션은 인터넷 커뮤니티의 다른 부분에 해를 주지 않는 방식으로 작동해야 합니다. 즉, 침해 활동을 피해야 합니다.

침해 활동은 AWS 고객의 인스턴스 또는 다른 리소스가 악의적이거나, 불쾌감을 주거나, 불법적이거나 다른 인터넷 사이트에 피해를 주는 동작을 하는 것이 외부에서 관찰되는 경우를 말합니다.

AWS는 고객과 협력하여 AWS 리소스에서 의심스럽고 악의적인 행동을 탐지 및 해결합니다. 고객의 리소스로부터 예상치 못했거나 의심스러운 동작을 발견하는 경우 AWS 리소스가 손상되어 비즈니스에 잠재적인 위험이 발생했음을 나타내는 것일 수 있습니다.

AWS는 다음과 같은 메커니즘을 사용하여 고객 리소스로부터 침해 활동을 탐지합니다.

- AWS 내부 이벤트 모니터링
- AWS 네트워크 공간을 기준으로 한 외부 보안 인텔리전스
- AWS 리소스를 기준으로 한 인터넷 침해 불만

AWS 침해 대응 팀이 AWS에서 실행 중인 악성 침해 또는 도용 프로그램을 모니터링하고 차단하지만 대부분의 침해 불만은 AWS에서 합법적인 비즈니스를 운영 중인 고객에 대한 내용입니다. 의도하지 않은 침해 활동의 일반적인 원인은 다음과 같습니다.

- **손상된 리소스.** 예를 들어, 패칭되지 않은 Amazon EC2 인스턴스가 감염되어 봇네트 에이전트가 될 수 있습니다.
- **의도하지 않은 침해.** 예를 들어, 일부 인터넷 사이트는 지나치게 적극적인 웹 크롤러를 DOS 공격자로 분류할 수 있습니다.
- **2차적 침해.** 예를 들어, AWS 고객이 제공하는 서비스의 최종 사용자는 퍼블릭 Amazon S3 버킷에 맬웨어 파일을 게시할 수 있습니다.
- **허위 불만.** 인터넷 사용자가 합법적인 활용을 침해로 오해하는 경우가 있습니다.

AWS는 침해를 방지, 탐지 및 완화하고 피해 재발을 방지하기 위해 AWS 고객과 협력하는 면에서 최선을 다하고 있습니다. AWS 침해 경고를 수신하면 보안 및 운영 직원은 즉시 그 문제를 조사해야 합니다. 지연될 경우 다른 인터넷 사이트 피해 기간이 길어지고 고객의 평판과 법적 책임에 영향을 미칠 수 있습니다. 더 중요한 점은 관련된 침해 리소스가 악의적인 사용자에 의해 손상될 수 있고 손상을 무시하면 고객의 비즈니스 피해가 커질 수 있습니다.

AWS 리소스를 사용하여 악의적, 불법적, 또는 유해한 활동을 하는 경우 AWS 이용목적 제한방침을 위반하는 것이며 계정이 일시 중지될 수 있습니다. 자세한 내용은 Amazon Web Services 이용 정책 – http://*aws.amazon.com/aup/*를 *참조하십시오*. 인터넷 커뮤니티의 평가에 따라 모범적인 서비스를 유지할 책임은 고객에게 있습니다. AWS 고객이 보고된 침해 활동을 해결하지 않을 경우 AWS는 AWS 플랫폼과 인터넷 커뮤니티의 무결성을 보호하기 위해 AWS 계정을 일시 중지합니다.

표 19는 침해 사고에 대응하는 데 도움이 될 수 있는 모범 사례를 소개합니다.

모범 사례	설명
AWS 침해에 대한 통신을 절대로 무시하지 말 것.	침해 사례가 접수되면 AWS는 즉시 고객의 등록된 이메일 주소로'이메일 알림을 보냅니다. 고객은 침해 경고 이메일에 회신만 하면 AWS 침해 대응 팀과 정보를 교환할 수 있습니다. 모든 통신 내용은 향후 참조를 위해 AWS 침해 추적 시스템에 저장됩니다. AWS 침해 대응 팀은 고객이 불만의 성격을 이해하도록 돕기 위해 최선을 다하고 있습니다. AWS는 고객이 침해 활동을 완화하고 방지하도록 지원합니다. 계정 일시 중지는 AWS 침해 대응 팀이 침해 활동을 중지시키기 위해 취하는 최종적인 조치입니다. 당사는 문제를 완화하고 처벌 조치를 취하는 일이 없도록 고객과 협력하고 있습니다. 하지만 고객은 침해 경고에 응답하고 악의적인 활동을 중지시키기 위한 조치를 취하고 향후 재발을 방지해야 합니다. 인스턴스와 계정이 차단되는 가장 큰 이유는 고객이 응답하지 않기 때문입니다.
보안 모범 사례를 따를 것.	리소스 손상을 방지하는 가장 좋은 방법은 본 문서에 소개된 보안 모범 사례를 따르는 것입니다. AWS는 고객의 클라우드 환경을 위한 강력한 방어 수단을 설정하는 데 도움이 되는 특정 보안 도구를 제공하고 있지만 고객은 자체 데이터 센터 내에 있는 서버와 같은 보안 모범 사례를 따라야 합니다. 최신 소프트웨어 패치 적용, 방화벽 및/또는 Amazon EC2 보안 그룹을 통한 네트워크 트래픽 제한, 사용자 [illegible] 에게 채택합니다.
손상 완화.	고객의 컴퓨팅 환경이 손상 또는 감염된 경우 안전한 상태로 복구하기 위해 다음과 같은 조치를 취할 것을 권합니다. • 손상이 알려진 Amazon EC2 인스턴스 또는 AWS 리소스는 안전하지 않은 것으로 간주합니다. Amazon EC2 인스턴스가 애플리케이션 사용으로 설명할 수 없는 트래픽을 생성하고 있는 경우 인스턴스는 아마도 악성 소프트웨어로 손상 또는 감염되었을 것입니다. 해당 인스턴스를 완전히 차단하거나 재구축하여 안전한 상태로 돌아갑니다. 새로 재시작하는 것이 물리적인 환경에서는 어려울 수 있지만 클라우드상의 환경에서는 첫 번째 완화 접근 방식입니다. • 근본 원인을 탐지하려면 손상된 인스턴스에 대한 법의학적 분석을 수행해야 할 수도 있습니다. 숙련된 보안 전문가들만 그런 조사를 수행해야 하며 조사 중에는 추가적인 피해와 감염을 방지하기 위해 감염된 인스턴스를 격리해야 합니다. Amazon EC2 인스턴스를 조사 목적으로 격리하려면 매우 제한된 보안 그룹을 설정할 수 있습니다. 예를 들어, 법의학적 조사관이 인스턴스를 안전하게 검사할 수 있는 단일 IP 주소로부터 인바운드 SSH 또는 RDP 트래픽을 수락하는 목적의 포트를 제외한 모든 포트를 닫습니다. 또한 감염된 인스턴스의 오프라인 Amazon EBS 스냅샷을 만든 다음 법의학적 조사관에게 오프라인 스냅샷을 제공할 수 있습니다. AWS는 고객의 인스턴스 또는 다른 리소스 내에 있는 비공개 정보에 액세스할 수 없기 때문에 애플리케이션 계정 인계 등 게스트 운영 체제 또는 애플리케이션 수준의 손상은 탐지할 수 없습니다. AWS는 고객이 자체 도구를 통해 해당 정보를 기록하지 않는 경우 정보(예: 액세스 로그, IP 트래픽 로그 또는 기타 속성)를 소급해서 제공할 수 없습니다. 심도 있는 사고 조사와 완화 활동은 대부분 고객의 책임입니다.

모범 사례	설명
	손상된 Amazon EC2 인스턴스를 복구하기 위해 취해야 하는 마지막 단계는 핵심 비즈니스 데이터를 백업하고 감염된 인스턴스를 완전히 종료하고 새 리소스로 재시작하는 것입니다. 향후 손상을 방지하기 위해 새로 시작한 인스턴스에서 보안 제어 환경을 검토하는 것이 좋습니다. 최신 소프트웨어 패치를 적용하고 방화벽을 제한하는 것과 같은 단순한 단계만 취해도 효과가 큽니다.
보안 통신 이메일 주소를 설정할 것.	AWS 침해 대응 팀은 이메일로 침해 경고를 알립니다. 기본적으로 이 이메일은 고객의 등록된 이메일 주소이지만 대기업의 경우 전용 대응 이메일 주소를 만들 수 있습니다. **Personal Information** 페이지의 **Configure Additional Contacts**에서 추가 이메일 주소를 설정할 수 있습니다.

표 19: 침해 완화 모범 사례

추가 애플리케이션 보안 사례 사용

운영 체제와 애플리케이션에 대한 추가 일반 보안 모범 사례는 다음과 같습니다.

- 암호, SNMP(Simple Network Management Protocol) 커뮤니티 문자열 및 보안 구성 등 공급업체가 제공한 기본값을 새 AMI를 생성하기 전이나 새 애플리케이션을 배포하기 전에 반드시 변경합니다.
- 불필요한 사용자 계정을 제거 또는 비활성화합니다.
- 동일한 서버에 공존하는 수준과는 다른 보안 수준을 요구하는 함수를 유지하기 위해 Amazon EC2 인스턴스당 하나의 1차 함수를 구현합니다. 예를 들어, 웹 서버, 데이터베이스 서버, DNS를 별도의 서버에 구현합니다.
- 시스템 기능의 필요에 따라 안전한 필수 서비스, 프로토콜, 데몬 등만 활성화합니다. 필수적이지 않은 서비스는 인스턴스와 전체 시스템의 보안 위험 노출을 높이기 때문에 모두 비활성화합니다.
- 스크립트, 드라이버, 기능, 하위 시스템, EBS 볼륨 및 불필요한 웹 서버 등 불필요한 모든 기능을 비활성화 또는 제거합니다.

보안 모범 사례를 염두에 두고 모든 서비스를 구성합니다. 필요한 서비스, 프로토콜 또는 데몬의 보안 기능을 활성화합니다. Telnet 등 보안성이 낮은 상응 서비스보다는 사용자/피어 인증 보안 메커니즘, 암호화 및 데이터 무결성 인증 기능이 기본 제공되는 SSH 등의 서비스를 선택합니다. FTP와 같은 보안성이 낮은 프로토콜 대신 SSH를 사용하여 파일을 전송합니다. 보안성이 낮은 프로토콜과 서비스를 사용해야 하는 경우 IPSec 또는 다른 가상 사설 네트워크(VPN) 기술 등 추가 보안 계층을 추가해 네트워크 계층의 통신 채널을 보호하거나 GSS-API, Kerberos, SSL 또는 TLS를 추가해 애플리케이션 계층의 네트워크 트래픽을 보호합니다.

보안 거버넌스는 모든 조직에 중요하지만 보안 정책을 적용하는 것이 가장 좋습니다. 가능하면 악용을 방지하기 위해 반드시 보안 정책과 지침에 맞게 시스템 보안 파라미터를 구성합니다.

시스템과 애플리케이션에 대한 관리자 액세스를 위해 어려운 암호화 메커니즘을 사용하여 모든 비콘솔 관리자 액세스를 암호화합니다. SSH, 사용자 및 사이트별 IPSec VPN 또는 SSL/TLS 등의 기술을 사용하여 원격 시스템 관리에 보안을 강화합니다.

인프라 보안 유지

이 섹션은 AWS 플랫폼에서의 인프라 서비스 보안 유지에 대한 권장 사항을 제공합니다.

Amazon Virtual Private Cloud(VPC) 사용

Amazon Virtual Private Cloud(VPC)를 사용하면 AWS 퍼블릭 클라우드 내에 프라이빗 클라우드를 만들 수 있습니다.

각 고객 Amazon VPC는 고객이 할당한 IP 주소 공간을 사용합니다. Amazon VPC에 프라이빗 IP 주소(RFC 1918의 권장 사항)를 사용하여 인터넷에 직접 라우팅할 수 없는 클라우드상의 프라이빗 클라우드와 연결 네트워크를 구축합니다.

Amazon VPC는 프라이빗 클라우드에서 다른 고객과의 격리뿐만 아니라 인터넷으로부터의 계층 3(네트워크 계층 IP 라우팅) 격리도 가능하게 합니다. 표 20에는 Amazon VPC에서의 애플리케이션 보호 옵션이 나열되어 있습니다.

문제	설명	권장 보호 접근 방식
인터넷 전용	Amazon VPC는 온프레미스 또는 다른 곳의 어떤 인프라에도 연결되어 있지 않습니다. 온프레미스 또는 다른 곳에 상주하는 추가 인프라가 있거나 없을 수 있습니다. 인터넷 사용자의 연결을 허용해야 하는 경우 엘라스틱 IP 주소(EIP)를 필요로 하는 Amazon VPC 인스턴스에만 할당하여 인바운드 액세스를 제공할 수 있습니다. 특정 포트와 소스 IP 주소 범위 전용 보안 그룹 또는 NACL을 사용하여 인바운드 연결을 더 제한할 수 있습니다. 인터넷으로부터의 트래픽 인바운드 로드 밸런스를 유지할 수 있다면 EIP는'필요하지 않습니다. 인스턴스는 Elastic Load Balancing 뒤에 배치할 수 있습니다. 아웃바운드(인터넷으로의) 액세스의 경우 예를 들어 소프트웨어를 업데이트하거나 Amazon S3 등 AWS 퍼블릭 서비스의 데이터를 액세스하는 경우 NAT 인스턴스를 사용하여 송신 연결에 액세스 제어 기능을 제공할 수 있습니다. EIP는 필요하지 않습니다.	SSL/TLS를 사용하여 애플리케이션과 관리자 트래픽을 암호화하거나 사용자 지정 사용자 VPN 솔루션을 구축합니다. 퍼블릭 및 프라이빗 서브넷의 라우팅 및 서버 배치를 세심하게 계획합니다. 보안 그룹과 NACL을 사용합니다.
인터넷을 통한 IPSec	AWS는 업계 표준의 복원력이 뛰어난 VPC용 IPSec 종료 인프라를 제공합니다. 고객은 온프레미스 또는 다른 VPN 인프라에서 Amazon VPC로 연결되는 IPSec 터널을 설정할 수 있습니다. IPSec 터널은 AWS와 인프라 엔드포인트 사이에 설정됩니다. 클라우드상 또는 온프레미스로 실행되는 애플리케이션은'수정이 필요하지 않고 전송 중 IPSec 데이터 보호의 혜택을 즉시 받을 수 있습니다.	IKEv1을 사용하여 프라이빗 IPSec 연결을 설정하고 표준 AWS VPN 시설(Amazon VPC VPN 게이트웨이, 고객 게이트웨이, VPN 연결)을 사용하여 IPSec를 설정합니다. 또는 클라우드상 및 온프레미스에 고객별 VPN 소프트웨어 인프라를 설정합니다.

문제	설명	권장 보호 접근 방식
AWS Direct Connect(IPSec 제외)	AWS Direct Connect를 사용하면 인터넷을 사용하지 않고도 프라이빗 피어링을 사용하여 전용 링크를 통해 Amazon VPC와의 연결을 설정할 수 있습니다. 이 경우 데이터 보호 요구 사항에 따라 IPSec를 사용하지 않기로 결정할 수 있습니다.	데이터 보호 요구 사항에 따라 프라이빗 피어링을 통한 추가 보호가 필요하지 않을 수 있습니다.
AWS Direct Connect (IPSec 포함)	추가적인 종단 간 연결은 AWS Direct Connect 링크에서 IPSec를 사용할 수 있습니다.	위의 인터넷을 통한 IPSec를 참조하십시오.
하이브리드	이러한 접근 방식의 조합을 사용하는 것을 고려합니다. 사용하는 각 연결 접근 방식에 대해 충분한 보호 메커니즘을 활용합니다.	

표 20: Amazon VPC에서 리소스 액세스

Amazon VPC-IPSec 또는 VPC-AWS Direct Connect를 활용하여 Amazon VPC 리소스로 온프레미스 또는 다른 호스팅 인프라를 안전한 방식으로 원활하게 통합할 수 있습니다. 또한 게이트웨이, 방화벽 및 IPSec 연결이 전송 중 데이터를 보호하고 IPSec 또는 AWS Direct Connect 링크의 BGP는 Amazon VPC 및 온프레미스 라우팅 도메인을 통합하여 모든 애플리케이션, 심지어 기본 네트워크 보안 메커니즘을 지원하지 않는 애플리케이션까지도 투명하게 통합할 수 있습니다.

VPC-IPSec가 애플리케이션에 업계 표준의 투명한 보호를 제공하지만 VPC-IPSec 링크를 통한 SSL/TLS 등의 추가적인 수준의 보호 메커니즘을 사용할 수 있습니다.

자세한 내용은 Amazon VPC 연결 옵션 백서를 참조하십시오.

보안 영역 조정 및 네트워크 세분화 사용

보안 요구 사항이 다르면 보안 제어 수단도 달라져야 합니다. 인프라를 비슷한 보안 제어를 도입하는 영역으로 세분화하는 것이 보안 측면에서 가장 좋습니다.

대부분의 AWS 기본 인프라는 AWS 운영 및 보안 팀이 관리하지만 고객도 자체 오버레이 인프라 구성 요소를 구축할 수 있습니다. Amazon VPC, 서브넷, 라우팅 테이블, 세분화/영역 조정된 애플리케이션과 사용자 리포지토리, DNS 및 시간 서버 등의 사용자 지정 서비스 인스턴스는 AWS 관리형 클라우드 인프라를 보완합니다.

일반적으로 네트워크 엔지니어링 팀은 세분화를 일종의 인프라 설계 구성 요소로 해석하고 네트워크 중심 액세스 제어와 방화벽 규칙을 적용하여 액세스를 관리합니다. 액세스 관리를 위한 방화벽 규칙. 보안 영역 조정과 네트워크 세분화는 별개의 개념입니다. 하지만 네트워크 세그먼트는 하나의 네트워크를 다른 네트워크와 격리하며 여기에서는 보안 영역이 일반 제어와 보안 수준이 비슷한 시스템 구성 요소의 그룹을 만듭니다.

AWS에서는 다음 액세스 제어 방법을 사용하여 네트워크 세그먼트를 구축할 수 있습니다.

- **Amazon VPC** 를 사용하여 각 워크로드 또는 조직 개체의 격리된 네트워크를 정의하는 방법.
- **보안 그룹**을 사용하여 기능과 보안 요구 사항이 비슷한 인스턴스에 대한 액세스를 관리하는 방법. 보안 그룹은 허용 및 설정된 모든 TCP 세션 또는 UDP 통신 채널에 대해 양쪽 방향으로 방화벽 규칙을 활성화하는 상태 저장 방화벽입니다.
- IP 및 관련 상태 비저장 규칙을 허용하는 네트워크 액세스 제어 **목록**(NACL)을 사용하는 방법. NACL은 TCP와 UDP 세션과는 무관하지만 IP 프로토콜(예: GRE, IPSec ESP, ICMP)을 통해 세분화된 제어와 TCP 및 UDP의 IP 주소 및 포트에 대한 소스/대상 단위 제어를 가능하게 합니다. NACL은 보안 그룹과 결합하여 작동하고 보안 그룹에 도달하기 전에도 트래픽을 허용 또는 거부할 수 있습니다.
- **호스트 기반 방화벽**을 사용하여 각 인스턴스에 대한 액세스를 제어하는 방법.
- 트래픽 흐름에 **위협 방지 계층**을 만들고 모든 트래픽이 영역을 통과하게 하는 방법.
- **다른 계층에 액세스 제어**를 적용하는 방법(예: 애플리케이션 및 서비스).

기존 환경은 방화벽 등의 중앙 보안 적용 시스템을 통해 트래픽을 라우팅하려면 별도의 브로드캐스트 개체를 나타내는 별도의 네트워크 세그먼트가 필요합니다. AWS 클라우드의 보안 그룹 개념으로 인해 이러한 요구 사항이 폐기되었습니다. 보안 그룹은 인스턴스를 논리적으로 그룹화하는 것이고 이러한 인스턴스가 상주하는 서브넷과 관계없이 이러한 인스턴스에 대한 인바운드 및 아웃바운드 트래픽 규칙의 적용도 허용합니다.

보안 영역을 만들려면 네트워크 세그먼트당 추가 제어가 필요한데 여기에는 흔히 다음이 포함됩니다.

- **공유 액세스 제어** – 중앙 Identity and Access Management(IDAM) 시스템. 연동이 가능하더라도 IAM과 구분되는 경우가 많습니다.
- **공유 감사 로깅** – 공유 로깅은 이벤트 분석과 상관 관계 및 보안 이벤트 추적에 필요합니다.
- **공유 데이터 분류** – 표 1: 샘플 자산 표 자산을 보호하기 위한 ISMS 설계섹션을 참조하십시오.
- **공유 관리 인프라** - 안티바이러스/스팸 방지 시스템, 패칭 시스템, 성능 모니터링 시스템 등 다양한 구성 요소입니다.
- **공유 보안(기밀성/무결성) 요구 사항** – 주로 데이터 분류와 함께 고려합니다.

네트워크 세분화와 보안 영역 구축 시 다음 질문을 고려하십시오. 이러한 질문에 답변하십시오.

- 영역 간 통신을 제어해야 합니까? 네트워크 세분화 도구를 사용하여 보안 영역 A와 B 사이의 통신을 관리할 수 있습니까? 일반적으로 보안 그룹, ACL 및 네트워크 방화벽 등의 액세스 제어 요소는 보안 영역 간에 벽을 구축해야 합니다. Amazon VPC는 기본적으로 영역 간 격리 벽을 구축합니다.
- 비즈니스 요구 사항에 따라 IDS/IPS/DLP/SIEM/NBAD 시스템을 사용하여 영역 간 통신을 모니터링할 수 있습니까? 액세스 차단과 액세스 관리는 다른 개념입니다. 보안 영역 간의 다공성 통신을 위해서는 영역 간에 정교한 보안 모니터링 도구가 필요합니다. AWS 인스턴스의 수평 확장성으로 인해 운영 체제 수준에서 각 인스턴스의 영역을 조정하고 호스트 기반의 보안 모니터링 에이전트를 활용할 수 있습니다.
- 영역별 액세스 제어 권한을 적용할 수 있습니까? 영역 조정의 이점 중 하나는 송신 액세스를 제어하는 것입니다. Amazon S3 및 Amazon SMS 리소스 정책 등의 리소스별로 액세스를 제어하는 것은 기술적으로 가능합니다.

- 전용 관리 채널/역할을 사용하여 각 영역을 관리할 수 있습니까?
  권한 액세스에 대한 역할 기반 액세스 제어는 일반적인 요구 사항입니다. IAM으로 AWS에서 그룹과 역할을 만들어 여러 권한 수준을 만들 수 있습니다. 애플리케이션 및 시스템 사용자와 동일한 접근 방식을 모방할 수도 있습니다. Amazon VPC 기반 네트워크의 새로운 핵심 기능 중 하나는 여러 개의 ENI를 지원하는 것입니다. 보안 엔지니어는 이중 홈 인스턴스를 사용하여 관리 오버레이 네트워크를 만들 수 있습니다.
- 영역별 기밀성 및 무결성 규칙을 적용할 수 있습니까? 영역별 암호화, 데이터 분류 및 DRM은 전체 보안 태세를 강화합니다. 보안 영역별로 보안 요구 사항이 다르면 데이터 보안 요구 사항도 달라야 합니다. 그리고 각 보안 영역에 키 교체에 관한 다른 암호화 옵션을 사용하는 것은 늘 올바른 정책입니다.

AWS는 유연한 보안 영역 조정 옵션을 제공합니다. 보안 엔지니어와 설계자는 다음 AWS 기능을 활용하여 Amazon VPC 액세스 제어에 따라 AWS에 격리된 보안 영역/세그먼트를 구축할 수 있습니다.

- 서브넷별 액세스 제어
- 보안 그룹별 액세스 제어
- 인스턴스별 액세스 제어(호스트 기반)
- Amazon VPC별 라우팅 블록
- 리소스별 정책(S3/SNS/SMS)
- 영역별 IAM 정책
- 영역별 로그 관리
- 영역별 IAM 사용자, 관리 사용자
- 영역별 로그 피드
- 영역별 관리자 채널(역할, 인터페이스, 관리 콘솔)
- 영역별 AMI
- 영역별 데이터 스토리지 리소스(Amazon S3 버킷 또는 Glacier 아카이브)
- 영역별 사용자 디렉토리
- 영역별 애플리케이션/애플리케이션 제어

탄력적인 클라우드 인프라와 자동화된 배포를 사용하면 모든 AWS 리전에서 동일한 보안 제어를 적용할 수 있습니다. 반복 가능하고 균일한 배포로 전반적인 보안 태세를 개선할 수 있습니다.

네트워크 보안 강화

공동 책임 모델에 따라 AWS는 데이터 센터 네트워크, 라우터, 스위치 및 방화벽 등의 인프라 구성 요소를 안전하게 구성합니다. 클라우드상의 시스템에 대한 액세스를 제어하고 Amazon VPC 내에서의 네트워크 보안 및 인바운드와 아웃바운드 네트워크 트래픽을 구성할 책임은 고객에게 있습니다.

리소스 액세스 인증과 권한 부여 적용은 필수적이지만 그렇게 하더라도 공격자들이 네트워크 수준 액세스를 획득하고 권한이 있는 사용자를 가장하려는 시도를 막을 수 없습니다. 사용자의 네트워크 위치에 따라 애플리케이션과 서비스에 대한 액세스를 제어하면 추가적인 보안 계층이 마련됩니다. 예를 들어 강력한 사용자 인증을 [illegible] 트래픽을 특정 범위의 IP 주소로 제한하는 IP 주소 기반 방화벽과 보안 노출을 [illegible] 시스템에서 이점을 얻을 수 있습니다.

다음은 AWS 클라우드에서의 네트워크 보안 모범 사례입니다.

- 항상 보안 그룹을 사용합니다. 즉, 하이퍼바이저 수준에서 Amazon EC2 인스턴스에 대한 상태 저장 방화벽을 제공합니다. 여러 보안 그룹을 단일 인스턴스와 단일 ENI에 적용할 수 있습니다.
- 네트워크 ACL의 보안 그룹 강화: 상태 비저장이지만 신속하고 효율적인 제어를 제공합니다. 네트워크 ACL은 인스턴스별이 아니기 때문에 보안 그룹 외에 추가 제어 계층을 제공할 수 있습니다. ACL 관리 및 보안 그룹 관리에 역할 분리를 적용할 수 있습니다.
- 다른 사이트에 신뢰할 수 있는 연결을 하려면 IPSec 또는 AWS Direct Connect를 사용합니다. Amazon VPC 기반의 리소스가 원격 네트워크 연결을 요구하는 경우 가상 게이트웨이(VGW)를 사용합니다.
- 전송 중 데이터를 보호하여 데이터의 기밀성과 무결성 및 통신 당사자의 자격 증명을 확인합니다.

- 대규모 배포의 경우 네트워크 보안을 계층으로 설계합니다. 단일 네트워크 보호 계층을 만들지 않고 외부, DMZ 및 내부 계층에 네트워크 보안을 적용합니다.
- VPC 흐름 로그는 VPC의 네트워크 인터페이스에서 전송되고 수신되는 IP 트래픽에 대한 정보를 포착하도록 해주므로 가시성을 높여 줍니다.

상호 작용하는 AWS 서비스 엔드포인트 중 다수는 기본 방화벽 기능 또는 액세스 제어 목록을 제공하지 않습니다. AWS는 최신 네트워크 및 애플리케이션 수준 제어 시스템으로 이러한 엔드포인트를 모니터링하고 보호합니다. 요청의 소스 IP 주소를 기반으로 IAM 정책을 사용하여 리소스에 대한 액세스를 제한할 수 있습니다.

주변 시스템 보호: 사용자 리포지토리, DNS, NTP

오버레이 보안 제어는 보안 인프라 기반에서만 효율적입니다. 이 유형의 좋은 예가 DNS 쿼리 트래픽입니다. DNS 시스템의 보안을 적절하게 유지하지 않으면 DNS 클라이언트 트래픽을 [illegible] 스푸핑할 수 있습니다. 스푸핑은 기본 제어가 없는 인프라에 대한 단순하면서도 효율적인 공격입니다. [illegible]

일부 AWS 고객은 보안 DNS 서비스인 Amazon Route 53을 사용합니다. 내부 DNS가 필요한 경우 Amazon EC2 인스턴스에서 사용자 지정 DNS 솔루션을 구현할 수 있습니다. DNS는 솔루션 인프라의 필수적인 부분이므로 보안 관리 계획의 중요한 부분입니다. 모든 DNS 시스템과 다른 중요한 사용자 지정 인프라 구성 요소가 다음 제어의 적용 대상이어야 합니다.

일반 제어	설명
별도의 관리자 수준 액세스	역할 분리와 액세스 제어를 구현하여 흔히 애플리케이션 액세스를 위한 액세스 제어와는 분리된 그러한 디바이스에 대한 액세스 또는 인프라의 다른 부분에 대한 액세스를 제한합니다.
모니터링, 알림, 감사 추적	권한이 있는 활동과 권한이 없는 활동을 로깅 및 모니터링합니다.
네트워크 계층 액세스 제어	네트워크 액세스를 필요한 시스템으로 제한합니다. 가능한 경우 모든 네트워크 수준의 액세스 시도에 프로토콜을 적용합니다(즉, NTP 및 DNS에 대한 사용자 지정 RFC 표준 적용).
보안 패치가 포함된 최신의 안정적인	소프트웨어가 패칭되어 있고 알려진 취약성이나 다른 위험이 없는지 확인합니다.
지속적 보안 테스트(평가)	인프라를 반드시 정기적으로 테스트해야 합니다.
그 외 실시 중인 모든 보안 제어 프로세스	주변 시스템이 정보 보안 관리 시스템(ISMS)의 모범 사례와 서비스별 사용자 지정 보안 제어를 따르는지 확인합니다.

표 21: 주변 시스템 제어

DNS 외에 다른 인프라 서비스가 특정 제어를 요구할 수 있습니다.

중앙 집중식 액세스 제어는 위험 관리에 필수적입니다. IAM 서비스는 AWS에 역할 기반 자격 증명 및 액세스 관리를 제공하지만 AWS는 운영 체제와 애플리케이션에 Active Directory, LDAP 또는 RADIUS 등의 최종 사용자 리포지토리를 제공하지 않습니다. 그 대신 AAA(인증, 권한 부여 및 계정 관리) 서버, 때때로 독점적인 데이터베이스 테이블과 함께 사용자 식별 및 인증 시스템을 설정합니다. 사용자 플랫폼 및 애플리케이션의 모든 자격 증명 및 액세스 관리 서버는 보안에 중요하고 특별한 관심이 필요합니다.

시간 서버도 중요한 사용자 지정 서비스입니다. 로그 타임스탬프와 인증서 검증 등 많은 보안 관련 트랜잭션에 필수적입니다. 중앙 집중식 시간 서버를 사용하고 모든 시스템을 동일한 시간 서버와 동기화하는 것이 중요합니다. PCI DSS(Payment Card Industry Data Security Standard)는 시간 동기화에 대한 좋은 접근 방식을 제안합니다.

- 시간 동기화 기술을 구현하고 최신 상태로 유지하는지 확인합니다.

- 조직 내에서 올바른 시간을 가져오고 배포하고 저장하기 위한 프로세스를 확보하여 검토하고 시스템 구성 요소 표본에서 시간 관련 시스템 파라미터 설정을 검토합니다.
- 지정된 중앙 시간 서버만 외부 소스에서 시간 신호를 수신하고 외부 소스에서 오는 시간 신호가 국제 원자시(IAT) 또는 협정 세계시(UTC)를 기반으로 하는지 확인합니다.
- 지정된 중앙 시간 서버가 다른 시간 서버(및 기타 내부 서버)와 함께 정확한 시간을 유지하고 중앙 시간 서버에서만 시간을 수신하는지 확인합니다.
- 시스템 구성과 시간 동기화 설정을 검토하여 시간 데이터에 대한 액세스가 업무와 관련하여 시간 데이터에 액세스할 필요가 있는 담당자로 제한되는지 확인합니다.
- 시스템 구성, 시간 동기화 설정 및 프로세스를 검토하여 중요한 시스템의 시간 설정 변경 사항이 기록, 모니터링 및 검토되는지 확인합니다.
- 시간 서버가 업계에서 인정을 받는 특정 외부 소스로부터 시간 업데이트를 수락하는지 확인합니다. (이렇게 함으로써 악의를 가진 개인이 시계를 바꿀 수 없습니다). 대칭 키로 암호화된 이러한 업데이트를 수신할 수 있고 업데이트될 클라이언트 머신의 IP 주소를 지정하는 액세스 제어 목록을 만들 수 있습니다. (이를 통해 내부 시간 서버를 권한 없이 사용할 수 없도록 합니다.)

사용자 지정 인프라의 보안 검증은 클라우드상의 보안을 관리하는 일에서 필수적인 부분입니다.

위협 방지 계층 구축

많은 수의 조직이 계층화된 보안을 네트워크 인프라 보호의 가장 좋은 방법으로 보고 있습니다. 클라우드에서 Amazon VPC, 하이퍼바이저 계층의 암시적 방화벽 규칙과 함께 네트워크 액세스 제어 목록, 보안 그룹, 호스트 기반 방화벽, IDS/IPS 시스템의 조합을 사용하여 네트워크 보안을 위한 계층화된 솔루션을 마련할 수 있습니다.

보안 그룹, NACL, 호스트 기반 방화벽이 많은 고객의 요구에 부응할 수 있지만 심층적인 방어가 필요한 경우에는 네트워크 수준의 보안 제어 어플라이언스를 배포할 수 있고 트래픽을 애플리케이션 서버 등 최종 대상에 전달하기 전에 가로채 분석하는 인라인에서 배포해야 합니다.

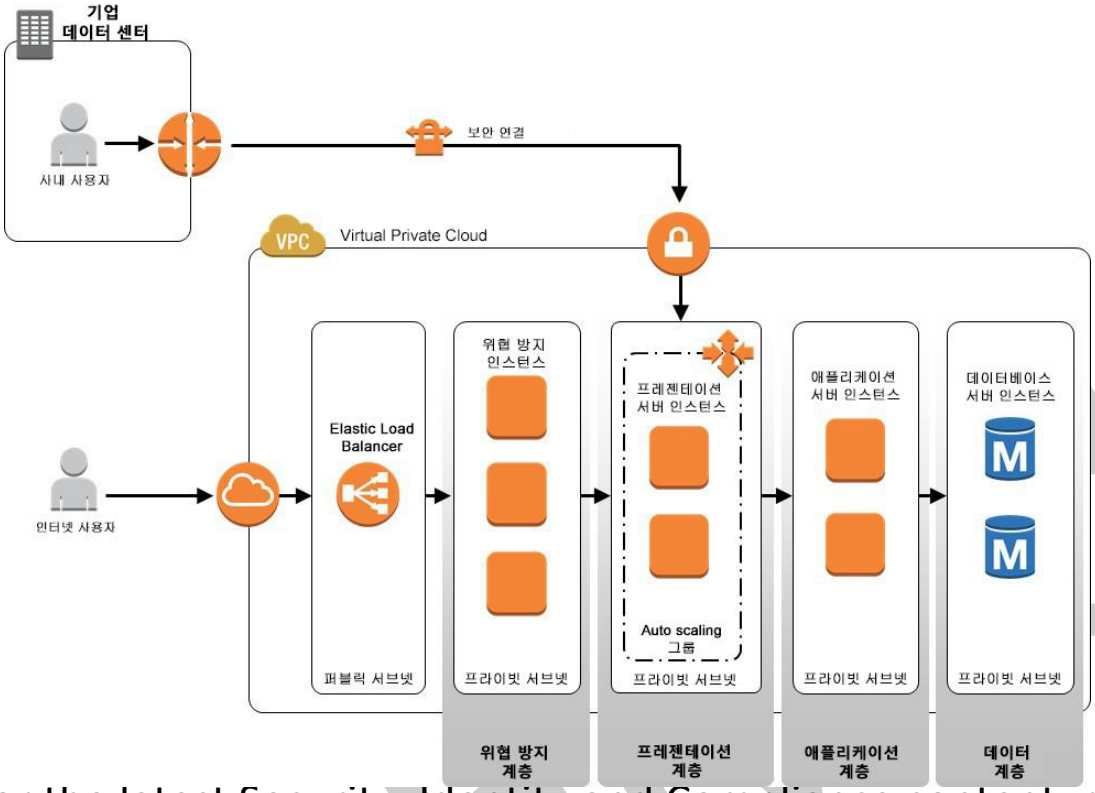

그림 6: 클라우드상의 계층화된 네트워크 방어

인라인 위협 방지 기술의 예는 다음과 같습니다.

- Amazon EC2 인스턴스에 설치된 타사 방화벽 디바이스 (소프트 블레이드라고도 함)
- 통합 위협 관리(UTM) 게이트웨이
- 침입 방지 시스템
- 데이터 손실 관리 게이트웨이
- 이상 탐지 게이트웨이
- 어드밴스 지속 위협 탐지 게이트웨이

Amazon VPC 인프라의 다음 핵심 기능은 위협 방지 계층 기술 배포를 지원합니다.

- **로드 밸런서의 다중 계층 지원:** 위협 방지 게이트웨이를 사용하여 웹 서버, 애플리케이션 서버 또는 기타 중요 서버의 보안을 유지하는 경우 확장성이 핵심적인 문제입니다. AWS 참조 아키텍처는 위협 관리 및 내부 서버 로드 배포 및 고가용성을 위한 외부 및 내부 로드 밸런서의 배포를 강조합니다. 다계층 설계에 Elastic Load Balancing 또는 사용자 지정 로드 밸런서 인스턴스를 활용할 수 있습니다. 상태 저장 게이트웨이 배포를 위한 로드 밸런서 수준에서 세션 지속성을 관리해야 합니다.

- **다중 IP 주소 지원:** 위협 방지 게이트웨이가 여러 인스턴스(예: 웹 서버, 이메일 서버, 애플리케이션 서버)로 구성된 프레젠테이션 계층을 보호하는 경우 이러한 다중 인스턴스는 다대일 관계에서 하나의 보안 게이트웨이를 사용해야 합니다. AWS는 단일 네트워크 인터페이스에 대해 다중 IP 주소 지원을 제공합니다.

- **다중 엘라스틱 네트워크 인터페이스(ENI) 지원:** 위협 방지 게이트웨이는 이중 홈이어야 하며 많은 경우 네트워크의 복잡성에 따라 여러 개의 인터페이스가 있어야 합니다. AWS는 ENI의 개념을 사용하여 여러 인스턴스 유형에서 여러 개의 네트워크 인터페이스를 지원하는데 이를 통해 다중 영역 보안 기능을 배포할 수 있습니다.

지연 시간, 복잡성 및 기타 아키텍처 제약으로 인해 인라인 위협 관리 계층을 구현할 수 없는 경우가 있으며 이때는 다음 대안 중 하나를 선택할 수 있습니다.

- **분산 위협 방지 솔루션:** 이 접근 방식은 클라우드상의 개별 인스턴스에 위협 방지 에이전트를 설치합니다. 중앙 위협 관리 서버는 로그 수집, 분석, 상관 관계, 능동적인 위협 대응 목적을 위해 모든 호스트 기반 위협 관리 에이전트와 통신합니다.

- **오버레이 네트워크 위협 방지 솔루션:** Amazon VPC를 기반으로 GRE 터널, vtun 인터페이스 등의 기술을 사용하거나 다른 ENI의 트래픽을 중앙 집중식 네트워크 트래픽 분석 및 침입 탐지 시스템에 전달함으로써 오버레이 네트워크를 구축하여 능동적 또는 수동적으로 위협에 대응합니다.

테스트 보안

모든 ISMS는 보안 제어와 정책의 효율성을 정기적으로 검토해야 합니다. 새로운 위협과 취약성에 대한 제어의 효율성을 보장하기 위해 고객은 인프라가 공격으로부터 보호되고 있는지 확인해야 합니다.

기존 제어를 확인하려면 테스트가 필요합니다. AWS 고객은 여러 가지 테스트 접근 방식을 사용해야 합니다.

- **외부 취약성 평가:** 타사가 인프라와 구성 요소에 대한 지식이 거의 또는 전혀 없이 시스템 취약성을 평가하는 것입니다.
- **외부 침투 테스트:** 시스템에 대한 지식이 거의 또는 전혀 없는 타사가 제어된 방식에 따라 능동적으로 시스템 침투를 시도하는 것입니다.
- **애플리케이션 및 플랫폼의 내부 그레이/화이트 박스 검토:** 시스템에 대한 어느 정도 또는 자세한 지식을 가지고 있는 테스터가 실시되고 있는 제어의 효율성을 검증하거나 애플리케이션과 플랫폼의 알려진 취약성을 평가하는 것입니다.

AWS 이용 방침은 AWS 클라우드에서 허용 또는 금지된 행동을 소개하고 보안 위반과 네트워크 침해를 정의합니다. AWS는 클라우드상의 인바운드 및 아웃바운드 침투 테스트를 모두 지원합니다. 단, 고객이 침투 테스트 실시 권한을 요청해야 합니다. 자세한 내용은 Amazon Web Services 이용 정책 – http://*aws.amazon.com/aup/를 참조하십시오.*

리소스에 대한 침투 테스트를 요청하려면 AWS 취약성 침투 테스트 요청 양식을 작성하여 제출하십시오. 테스트할 인스턴스와 관련된 자격 증명을 사용하여 AWS Management Console에 로그인해야 합니다. 그렇지 않으면 양식에 올바르게 사전 입력되지 않습니다. 타사 침투 테스트의 경우 직접 양식을 작성한 다음 AWS 승인 시 타사에 알려야 합니다.

이 양식에는 테스트할 인스턴스, 원하는 시작 날짜와 종료 날짜, 그리고 테스트 시간에 대한 다양한 정보가 포함되며, 침투 테스트 및 테스트용 도구 사용에 관한 약관을 읽고 이에 동의해야 합니다. AWS는 정책상 m1.small 또는 t1.micro의 테스트를 허용하지 않습니다. 인스턴스 유형. 양식을 제출한 후 1일(영업일 기준) 이내에 요청을 수신했음을 확인하는 응답을 받을 수 있습니다.

추가로 테스트할 시간이 필요한 경우 권한 부여 이메일에 회신하여 테스트 기간 연장을 요청할 수 있습니다. 각 요청은 별도의 승인 프로세스를 거칩니다.

측정치 및 개선 관리

제어의 효율성 측정은 각 ISMS에 필수적인 프로세스입니다. 측정치를 통해 제어가 환경을 얼마나 효율적으로 보호하고 있는지 확인할 수 있습니다. 위험 관리는 많은 경우 정성적, 정량적 측정치를 기반으로 합니다. 표 22는 측정 및 개선 모범 사례를 소개합니다.

모범 사례	개선
절차와 다른 제어 모니터링 및 검토	• 신속한 처리 결과 오류 탐지 • 보안 위반 및 사고 시도 및 성공의 신속한 식별 • 경영진이 직원에게 위임되었거나 정보 기술이 구현한 보안 활동이 기대한 바에 따라 수행되고 있는지 확인하도록 지원 • 표시 기호의 사용을 통한 보안 이벤트 탐지 지원 및 보안 사고 방지 • 보안 위반을 해결하기 위해 취한 조치의 효율성 확인
ISMS의 효율성에 대한 정기적인 검토	• 보안 감사, 사고, 효율성 측정 결과 검토 및 관련된 모든 당사자로부터의 제안 및 피드백 • ISMS가 정책과 목표에 부응하는지 확인 • 보안 제어 검토
제어의 효율성 측정	• 보안 요구 사항의 충족 여부 확인
정기적인 위험 평가 검토	• 잔존 위험과 식별된 위험의 허용 가능 수준 검토 시 고려할 점: • 조직의 변화, 기술, 비즈니스 목표 및 프로세스, 식별된 위협 • 구현된 제어의 효율성 • 법적 또는 규제 환경 변화, 계약 의무 변경 사항, 사회적 풍토 변화 등 외부 이벤트
내부 ISMS 감사	• 1차 당사자 감사(내부 감사)는 조직 자체 또는 조직을 대신해 내부적인 목적으로 실시하는 것입니다.
정기 관리 검토	• 범위가 적절한지 확인 • ISMS 프로세스 개선 사항 식별
보안 계획 업데이트	• 모니터링 및 검토 활동에서 확인된 사실 고려 • ISMS 효율성 또는 성과에 영향을 줄 수 있는 작업 및 이벤트 기록

표 22: 측정치 측정 및 개선

DoS 및 DDoS 공격 완화 및 방지

인터넷 애플리케이션을 실행하는 조직은 경쟁사, 활동가 또는 개인의 DoS(Denial of Service) 또는 DDoS(Distributed Denial of Service) 공격의 대상이 될 수 있는 위험을 인지합니다. 위험 프로필은 비즈니스의 성격, 최근 이벤트, 정치적인 상황 및 기술 노출에 따라 달라집니다. 완화 및 방지 기술은 온프레미스에서 사용하는 것과 비슷합니다.

DoS/DDoS 공격 방지 및 완화 문제에 대해 우려하고 있다면 공격 완화 또는 AWS에서의 환경에서 지속적으로 일어나는 사고를 억제하는 프로세스에서 선행적 및 후행적으로 AWS 지원 서비스를 받을 수 있도록 AWS Premium Support 서비스에 등록하는 것이 좋습니다.

Amazon S3와 같은 일부 서비스는 공유 인프라를 사용하는데, 따라서 여러 AWS 계정이 동일한 Amazon S3 인프라 구성 요소 세트에 액세스하고 데이터를 저장합니다. 이러한 경우 추상화된 서비스에 대한 DoS/DDoS 공격이 여러 고객에게 영향을 미칠 수 있습니다. AWS는 공격 발생 시 고객에게 미칠 영향을 최소화하기 위해 AWS의 추상화된 서비스에 대해 DoS/DDoS 완화 및 방어 제어 기능을 모두 제공합니다. 그러한 서비스에 추가적인 DoS/DDoS 보호를 제공할 필요는 없지만 본 백서에 소개된 모범 사례를 따르는 것이 좋습니다.

Amazon EC2 등의 다른 서비스는 공유된 물리적 인프라를 사용하지만 고객은 운영 체제, 플랫폼 및 고객 데이터를 관리해야 합니다. 그러한 서비스의 경우 효율적인 DDoS 완화 및 방지를 위해 협력해야 합니다.

AWS는 독점 기술을 사용하여 AWS 플랫폼에 대한 DoS/DDoS 공격을 완화하고 억제합니다. 하지만 실제 사용자 트래픽에 대한 방해가 없도록 하기 위해 공동 책임 모델에 따라 AWS는 개별 Amazon EC2 인스턴스에 영향을 미치는 네트워크 트래픽을 완화하거나 능동적으로 차단하지 않습니다. 과도한 트래픽이 예상된 것이고 무해한 것인지 아니면 DoS/DDoS 공격의 일환으로 발생하는지는 고객만이 확인할 수 있습니다.

클라우드상의 DoS/DDoS 공격을 완화하는 데 여러 가지 기술이 사용될 수 있지만 정상적인 상황에서 시스템 파라미터를 캡처하는 보안 및 성능 기준을 설정하고 잠재적으로 비즈니스에 적용 가능한 일일, 주간, 연간 또는 기타 패턴도 고려하는 것이 좋습니다. 통계 및 동작 모델 등 일부 DoS/DDoS 방지 기술을 통해 기준 정상 작동 패턴과 비교해 이상을 탐지할 수 있습니다. 예를 들어 하루 중 특정 시간에 보통 2,000개의 동시 세션이 진행될 것으로 예상하는 고객의 경우 현재 동시 세션의 수가 그 수의 두 배(4,000개)를 초과할 경우 Amazon CloudWatch 및 Amazon SNS를 사용하여 경보를 트리거할 수 있습니다.

클라우드상의 보안 입지를 설정할 때 온프레미스 배포에 적용되는 동일한 구성 요소를 고려하십시오.

표 23은 클라우드상의 일반적인 DoS/DDoS 완화 및 방지 접근 방식을 소개합니다.

기술	설명	DoS/DDoS 공격 방지
방화벽: 보안 그룹, 네트워크 액세스 제어 목록 및 호스트 기반 방화벽	기존 방화벽 어플라이언스는 잠재적인 공격자의 공격 대상 영역을 제한하고 공격 대상 소스에서 송수신하는 트래픽을 거부합니다.	• 허용된 대상 포트 및 IP 주소(IP 주소 및 TCP/UDP 포트)의 목록 관리 • 허용된 트래픽 프로토콜 소스 목록 관리 • 명시적으로 특정 IP 주소의 액세스를 임시적 또는 영구적으로 거부 • 허용된 목록 관리
웹 애플리케이션 방화벽(WAF)	웹 애플리케이션 방화벽은 웹 트래픽에 대한 정밀 패킷 검사를 제공합니다.	• 플랫폼 및 애플리케이션별 공격 • 프로토콜 안전성 공격 • 무단 사용자 액세스
호스트 기반 또는 인라인 IDS/IPS 시스템	IDS/IPS 시스템은 통계/동작 또는 서명 기반 알고리즘을 사용하여 네트워크 공격과 트로이 목마를 탐지 및 억제할 수 있습니다.	• 모든 유형의 공격
트래픽 성형/속도 제한	DoS/DDoS 공격은 많은 경우 네트워크와 시스템 리소스를 고갈시킵니다. 속도 제한은 귀중한 리소스가 과도하게 사용되지 않도록 방지하는 데 효과적인 기술입니다.	• ICMP 홍수 • 애플리케이션 요청 홍수

기술	설명	DoS/DDoS 공격 방지
초기 세션 제한	TCP SYN 홍수 공격은 단순한 형태나 분산된 형태 모두 발생할 수 있습니다. 두 가지 경우 모두 시스템 기준이 있다면 반개방(초기) TCP 세션의 수가 기준을 상당히 벗어났음을 탐지하고 특정 소스로부터 추가 TCP SYN 패킷을 모두 거부할 수 있습니다.	• TCP SYN 홍수

표 23: DoS/DDoS 공격 완화 및 방지 기술

DoS/DDoS 공격 완화 및 방지를 위한 기존의 접근 방식과 함께 AWS 클라우드는 탄력성을 기반으로 한 기능을 제공합니다. DoS/DDoS 공격은 제한된 컴퓨팅, 메모리, 디스크 또는 네트워크 리소스를 고갈시켜 운영에 어려움을 주기 위해 방해하려는 시도입니다. 하지만 AWS 클라우드는 정의상 새로운 리소스를 필요한 [illegible] 웹 서버로 이루어지는 정당한 사용자 요청과 구분할 수 없도록 초당 수십만 건의 요청을 생성하는 봇넷에 의한 DDoS 공격을 받을 수 있습니다. 기존의 업계 기술을 사용하는 경우에는 유효한 고객은 없고 공격자만 있다는 가정 하에 먼저 특정 소스, 많은 경우 전체 지리적 위치의 트래픽을 거부합니다. 하지만 이러한 가정과 조치로 인해 고객에게 서비스가 거부될 수도 있습니다.

클라우드에서는 그러한 공격을 흡수할 수 있습니다. Elastic Load Balancing과 Auto Scaling 등의 AWS 기술을 사용하면 웹 서버를 공격을 받을 때 확장하고(로드에 따라) 공격이 중지되면 축소하도록 구성할 수 있습니다. 심각한 공격이 있을 때에도 클라우드 탄력성을 활용하여 웹 서버가 확장하고 최적의 사용자 경험을 제공할 수 있습니다. 공격을 흡수하는 경우 추가 AWS 서비스 비용이 발생할 수 있지만 그러한 공격을 유지하는 것이 재정적으로 부담스러운 일이기 때문에 공격을 흡수할 경우 지속될 가능성이 적습니다.

또한 Amazon CloudFront를 사용하여 DoS/DDoS 홍수 공격을 흡수할 수 있습니다. AWS WAF는 애플리케이션 가용성을 저해하거나 보안을 위협하거나 과도한 리소스를 소비할 수 있는 일반적인 웹 도용에서 웹 애플리케이션을 보호하는 데 도움을 주는 AWS CloudFront와 통합됩니다. CloudFront에 대한 콘텐츠를 공격하려고 하는 잠재적인 공격자는 CloudFront 엣지 로케이션에 대부분 또는 모든 요청을 보낼 가능성이 높은데, 이 경우 AWS 인프라가 추가 요청을 흡수하여 백엔드 고객 웹 서버에 대한 영향을 최소화하거나 제거합니다. 언급했듯이 공격을 흡수하는 경우 추가 AWS 서비스 요금이 발생할 수 있지만 공격자가 공격을 지속하기 위해 부담해야 하는 비용을 고려하여 이 비용을 평가해보아야 할 것입니다.

DoS/DDoS 공격에 대한 노출을 효율적으로 완화, 억제 및 일반적으로 관리하기 위해서는 본 문서의 다른 부분에 소개되어 있는 계층 방어 모델을 구축해야 합니다

보안 모니터링, 알림, 감사 추적 및 사고 대응 관리 **This paper has been archived**

공동 책임 모델을 사용하면 환경을 운영 체제와 상위 계층에서 모니터링 및 관리해야 합니다. 온프레미스와 다른 환경에서 이미 이러한 작업을 하고 있을 것이므로 기존 프로세스, 도구 및 방법을 클라우드에서 사용할 수 있도록 조정할 수 있습니다.

보안 모니터링에 대한 광범위한 지침은 ENISA Procure Secure 백서를 참조하십시오. 이 백서에서는 클라우드상의 지속적인 보안 모니터링 개념을 소개하고 있습니다(참조 자료 참조).

보안 모니터링은 다음 질문에 대한 답을 찾는 것으로부터 시작됩니다.

- 어떤 파라미터를 측정해야 합니까?
- 어떻게 측정해야 합니까?
- 이러한 파라미터의 임계값은 얼마입니까?
- 에스컬레이션 프로세스는 어떻게 작동합니까?
- 데이터는 어디에 보관합니까?

답을 찾아야 하는 가장 중요한 질문은 아마도 "로깅해야 하는 내용은 무엇입니까?" 일 것입니다. 로깅과 분석에 대한 다음 영역을 구성하는 것이 좋습니다.

- 루트 또는 관리 권한을 가진 개인이 수행한 작업
- 모든 감사 추적에 대한 액세스
- 잘못된 논리적 액세스 시도
- 식별 및 인증 메커니즘 사용
- 감사 로그 초기화
- 시스템 수준의 객체 생성 및 삭제

로그 파일을 설계할 때 표 24의 고려 사항을 염두에 두십시오.

영역	고려 사항
로그 수집	로그 파일이 수집되는 방식에 유의하십시오. 운영 체제, 애플리케이션 또는 타사/미들웨어 에이전트가 로그 파일 정보를 수집하는 경우가 많습니다.
로그 전송	로그 파일이 중앙 집중식일 경우 안전하고 안정적이며 시기 적절하게 중앙 위치로 전송하십시오.
로그 스토리지	여러 인스턴스의 로그 파일을 중앙 집중화하여 보존 정책과 분석 및 상관 관계를 지원하십시오.
로그 분류 체계	다양한 카테고리의 로그 파일을 분석에 적합한 형식으로 제공하십시오.
로그 분석/ 상관 관계	로그 파일은 분석 및 로그 파일 내의 이벤트 상관 관계 설정 후 보안 인텔리전스를 제공합니다. 실시간으로 또는 정기적으로 로그를 분석할 수 있습니다.
로그 보호/ 보안	로그 파일을 인가합니다. 네트워크 제어, 자격 증명 및 액세스 관리, 암호화, 데이터 무결성 인증 및 부정 조작 방지 타임스탬프를 통해 로그 파일을 보호하십시오.

표 24: 로그 파일 고려 사항

보안 로그 소스는 여러 개가 있을 수 있습니다. 방화벽, IDP, DLP, AV 시스템, 운영 체제, 플랫폼 및 애플리케이션 등의 다양한 네트워크 구성 요소에서 로그 파일이 생성됩니다. 이 중 많은 수는 보안과 관련되어 있으며 이런 로그 파일을 로그 파일 전략에 포함시켜야 합니다. 보안과 관련되지 않은 다른 로그 파일은 전략에서 제외하는 것이 좋습니다. 로그에는 모든 사용자 활동, 예외, 보안 이벤트가 포함되어 있어야 하며 향후 조사를 위해 사전에 결정된 시간 동안 보관해야 합니다.

어떤 로그 파일을 포함시켜야 하는지 결정하려면 다음 질문에 답하십시오.

- 클라우드 시스템의 사용자는 누구입니까? 이들은 리소스에 액세스하기 위해 어떻게 등록, 인증하고 권한을 받습니까?
- 어떤 애플리케이션이 클라우드 시스템에 액세스합니까? 이들은 액세스를 하기 위해 어떻게 자격 증명을 받고 인증하고 권한을 받습니까?

- 어떤 사용자가 AWS 인프라, 운영 체제 및 애플리케이션에 권한 액세스(관리자 수준 액세스)를 할 수 있습니까? 이들은 어떻게 인증하고 그러한 액세스 권한을 받습니까?

많은 서비스는 액세스 제어 감사 추적 기능(예: Amazon S3와 Amazon EMR이 그러한 로그 제공)이 기본으로 제공되지만 일부 경우에 로깅에 대한 고객의 비즈니스 요구 사항이 기본 서비스 로그보다 높을 수 있습니다. 그런 경우에는 권한 에스컬레이션 게이트웨이를 사용하여 액세스 제어 로그와 권한 부여를 관리하는 방법을 고려할 수 있습니다.

권한 에스컬레이션 게이트웨이를 사용하는 경우 단일(클러스터 방식의) 게이트웨이를 통해 시스템에 대한 모든 액세스를 중앙 집중화하는 것입니다. AWS 인프라, 고객의 운영 체제 또는 애플리케이션에 직접 호출을 하지 않고 모든 요청은 신뢰할 수 있는 인프라 중개자 역할을 하는 프록시 시스템을 통해 수행됩니다. 대부분의 경우 그러한 시스템은 다음을 제공하거나 수행해야 합니다.

- **자동화 암호 관리**를 통한 권한 액세스: 권한 액세스 제어 시스템은 Microsoft Active Directory, UNIX, LDAP, MYSQL 등에 대한 기본 제공 커넥터를 자동으로 사용하여 기준 정책에 따라 암호와 자격 증명을 교체할 수 있습니다.
- **AWS IAM 사용자 액세스 관리자 및 AWS IAM 사용자가 마지막으로 사용한 액세스 키를 사용해** 최소 권한 점검을 정기적으로 실행합니다.
- **사용자 인증**을 프런트 엔드에 사용하고 백엔드에서 AWS 서비스 액세스 위임: 일반적으로 모든 사용자에게 Single Sign-On을 제공하는 웹 사이트입니다. 사용자는 권한 부여 프로필에 따라 액세스 권한을 할당 받습니다. 일반적인 접근 방식은 웹 사이트에 토큰 기반 인증을 사용하고 사용자 프로필에서 허용된 다른 시스템에 대한 클릭 액세스를 획득하는 것입니다.
- **부정 조작 방지 감사 추적** 모든 중요 활동의 스토리지입니다.
- **공유 계정에 대한 서로 다른 로그인 자격 증명:** 여러 사용자가 동일한 암호를 공유해야 하는 경우가 있습니다. 권한 에스컬레이션 게이트웨이를 사용하면 공유 계정을 공개할 필요 없이 원격 액세스가 허용될 수 있습니다.
- **립프로깅 또는 원격 데스크톱 호핑을 제한하기 위해** 대상 시스템에 대한 액세스만 허용합니다.

- **명령 관리**는 세션 중에 사용할 수 있습니다. SSH 또는 어플라이언스 관리 또는 AWS CLI 등의 대화형 세션의 경우 그러한 솔루션은 사용 가능한 명령과 작업의 범위를 제한하여 정책을 적용할 수 있습니다.
- **단말기 감사 추적 및 GUI 기반 세션**을 제공하여 규정 준수 및 보안 관련 목적을 달성합니다.
- **모든 사항 로깅** 및 정책의 기준 임계값에 따른 알림을 제공합니다.

변경 관리 로그 사용

보안 로그를 관리함으로써 변경 사항도 추적할 수 있습니다. 여기에는 조직의 변화 제어 프로세스에 포함된 정기적 변경 사항(MACD–이동/추가/변경/삭제라고도 함), 특별 변경 사항 또는 사고 등 예기치 않은 변경 사항도 포함됩니다. 시스템의 인프라 측에서 변경이 이루어지기도 하지만 코드 리포지토리 변경, 골드 이미지/애플리케이션 인벤토리 변경, 프로세스 및 정책 변경 또는 문서 변경 등 다른 카테고리와 관련된 경우도 있을 수 있습니다. 위의 모든 변경 카테고리에 대해 부정 조작 방지 로그 리포지토리를 활용하는 것이 가장 좋습니다. 변경 관리 및 로그 관리 시스템의 상호 관계를 설정하고 상호 연결하십시오.

변경 로그를 삭제 또는 수정하려면 권한이 있는 전용 사용자가 필요합니다. 대부분의 시스템, 디바이스 및 애플리케이션의 경우 변경 로그는 부정 조작이 방지되어야 하며 일반 사용자는 로그 관리 권한을 가질 수 없습니다. 일반 사용자는 변경 로그에서 증거를 삭제할 수 없어야 합니다. AWS 고객은 로그에 파일 무결성 모니터링 또는 변경 탐지 소프트웨어를 사용하여 알림을 생성하지 않고는 기존 로그 데이터를 변경할 수 없는 경우가 있습니다. 단, 새로 입력할 경우 알림이 생성되지 않습니다.

시스템 구성 요소의 모든 로그는 최소 매일 검토해야 합니다. 로그 검토에는 침입 탐지 시스템(IDS), AAA(인증, 권한 부여 및 계정 관리 프로토콜) 서버 등 보안 기능을 수행하는 서버(예: RADIUS 서버)가 포함되어야 합니다. 이 프로세스를 돕기 위해 로그 수확, 구문 분석 및 알림 도구를 사용할 수 있습니다.

중요 트랜잭션 로그 관리

중요한 애플리케이션의 경우 모든 추가, 변경/수정 및 삭제 활동 또는 트랜잭션은 로그 항목을 생성해야 합니다. 각 로그 항목에는 다음 정보가 포함되어야 합니다.

- 사용자 식별 정보
- 이벤트 유형
- 날짜 및 타임스탬프
- 성공 또는 실패 표시
- 이벤트가 시작된 지점
- 영향을 받은 데이터, 시스템 구성 요소 또는 리소스의 ID나 이름

로그 정보 보호

로깅 시설 및 로그 정보는 변조 및 무단 액세스로부터 보호되어야 합니다. 관리자와 연산자 로그는 활동 추적 삭제의 대상이 되는 경우가 많습니다.

로그 정보 보호의 일반적인 제어 수단은 다음과 같습니다.

- 감사 내역이 시스템 구성 요소에 대해 사용 설정되어 있고 현재 실행 중인지 확인
- 업무와 관련하여 필요한 개인만 감사 추적 파일을 볼 수 있는지 확인
- 현재 감사 내역 파일이 액세스 제어 메커니즘, 물리적 격리 및/또는 네트워크 격리를 통한 무단 수정으로부터 보호되는지 확인
- 현재 감사 추적 파일이 중앙 집중식 로그 서버 또는 변경하기 어려운 미디어에 지체 없이 백업되는지 확인
- 외부로 연결되는 기술(예: 무선, 방화벽, DNS, 메일)에 대한 로그가 안전한 내부의 중앙 집중식 서버나 미디어로 이동되거나 복사되는지 확인
- 시스템 설정과 모니터링된 파일 및 모니터링 활동의 결과를 검사하여 로그에 파일 무결성 모니터링 또는 변경 탐지 소프트웨어를 사용
- 보안 정책 및 절차를 확보하고 검사하여 적어도 하루에 한 번 보안 로그를 검토하기 위한 절차가 포함되어 있고 예외에 대한 후속 조치가 요구되는지 확인
- 정기적으로 모든 시스템 구성 요소에 대한 로그를 검토하고 있는지 확인
- 보안 정책 및 절차에 감사 로그 보존 정책이 포함되고 비즈니스 및 규정 준수 요구 사항으로 정의된 일정 기간 동안의 감사 로그 보존이 필요한지 확인

로깅 결함

MACD 이벤트를 모니터링하는 것 외에, 소프트웨어 또는 구성 요소 결함을 모니터링하십시오. 결함은 하드웨어 또는 소프트웨어 장애의 결과일 수 있으며 서비스와 데이터 가용성에 영향을 줄 수 있지만 보안 사고와는 관련되지 않을 수 있습니다. 아니면 서비스 결함은 서비스 공격 거부 등 의도적이고 악의적인 활동의 결과일 수 있습니다. 어찌 됐든 결함이 발생하면 알림이 생성되어야 하고 이벤트 분석 및 상관 관계 기술을 사용하여 결함의 원인과 보안 응답을 트리거해야 하는지 확인해야 합니다.

결론

AWS 클라우드 플랫폼은 유연성, 탄력성, 유틸리티 결제 및 출시 시간 단축 등 현재 기업에 여러 가지 중요한 이점을 제공합니다. AWS에서는 자산과 데이터 보안 관리에 사용할 수 있는 다양한 보안 서비스와 기능을 제공합니다. AWS는 인프라 또는 플랫폼 서비스에 관한 유무와 서비스 관리 계층을 제공하지만 기업은 클라우드상의 데이터의 기밀성, 무결성 및 가용성을 보호하고 특정 정보 보호 비즈니스 요구 사항을 준수할 책임이 있습니다.

클라우드상에도 가중의 보안 및 규정 준수 개념이 적용됩니다. 이 백서에서 강조하는 다양한 모범 사례를 사용하여 조직의 보안 정책 및 프로세스 집합을 구축함으로써 신속하고 안전하게 애플리케이션과 데이터를 배포하는 것이 좋습니다.

기고자

- Dob Todorov
- Yinal Ozkan

참조 자료

- Amazon Web Services: 보안 프로세스의 개요– http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
- Amazon Web Services 위험 및 규정 준수 백서– http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf
- 재해 복구를 위한 Amazon Web Services 사용– http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
- Amazon VPC Network Connectivity Options– http://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf
- Active Directory 사용 사례를 위한 자격 증명 연동 샘플 애플리케이션– http://aws.amazon.com/code/1288653099190193
- Single Sign-on with Windows ADFS to Amazon EC2 .NET Applications– http://aws.amazon.com/articles/3698?_encoding=UTF8&queryArg=searchQuery&x=20&y=25&fromSearch=1&searchPath=all&searchQuery=identity%20federation
- 토큰 벤딩 머신을 사용한 AWS 모바일 애플리케이션 사용자 인증– http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
- Java용 AWS SDK 및 Amazon S3를 사용하는 클라이언트 측 데이터 암호화– http://aws.amazon.com/articles/2850096021478074
- Amazon's Corporate IT Deploys SharePoint 2010 to the Amazon Web Services Cloud– http://media.amazonwebservices.com/AWS_Amazon_SharePoint_Deployment.pdf
- Amazon Web Services 이용 정책 – http://aws.amazon.com/aup/
- ENISA Procure Secure: A Guide to Monitoring of Security Service Levels in Cloud Contracts– http://www.enisa.europa.eu/activities/application-

security/cloud-computing/procure-secure-a-guide-to- monitoring-of- security-service-levels-in-cloud-contracts

- The PCI Data Security Standard– https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0
- ISO/IEC 27001:2005– http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103
- AWS 사용을 위한 보안 감사 체크리스트– http://media.amazonwebservices.com/AWS_Auditing_Security_Checklist.pdf