AWS 사용 감사에 대한 소개

2015년 10월

고지 사항

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

목차

요약

AWS에서 보안은 최우선의 일입니다. 모든 AWS 고객은 보안에 민감한 대부분의 조직의 요구를 만족하기 위해 구축된 데이터 센터와 네트워크 아키텍처의 혜택을 받습니다. 이러한 요구를 충족하기 위해 시행되는 AWS 규정 준수를 통해 고객은 AWS에 클라우드의 보안 및 데이터 보호를 유지할 수 있는 강력한 제어 장치가 마련되어 있음을 이해할 수 있습니다.

시스템이 AWS 클라우드 인프라를 기반으로 하여 구축되었기 때문에 규정 준수 책임은 AWS와 고객간에 공유됩니다. 해당되는 규정 준수 또는 감사 표준과 거버넌스 중심의 감사에 적합한 서비스 기능을 한 데 묶어 놓은 AWS 규정 준수 프로그램은 기존 프로그램 위에 구축되어 있기 때문에 고객이 AWS 보안 제어 환경에서 설정하고 작동할 수 있습니다.

AWS는 기본 인프라를 관리하고 고객은 AWS에서 배포하는 모든 것에 대한 보안을 관리합니다. 최신 플랫폼인 AWS를 사용하면 고객은 모든 AWS 고객 계정마다 구축된 안정적이고 확인 가능한 자동화 기술 및 작동 프로세스를 통해 보안 설계 및 감사 제어 형식을 갖출 수 있습니다. 클라우드는 관리자 및 이를 실행하는 IT 부서의 시스템 사용을 간소화하며, AWS에서 기존 감사 샘플 테스팅 대비 100% 검증 가능하도록 바꿀 수 있기 때문에 더욱 단순해진 AWS 환경에서 감사를 위한 샘플 테스팅을 수행할 수 있습니다.

또한, AWS에서 특별히 만든 도구는 고객 요구 사항, 확장성 및 감사 목적에 맞게 조정할 수 있을 뿐 아니라 AWS CloudTrail, Config, CloudWatch와 같은 내부 도구를 사용하여 실시간 확인 및 보고를 수행할 수 있도록 조정할 수 있습니다. 이러한 도구는 고객의 서비스, 데이터 및 애플리케이션을 최대한 보호할 수 있도록 구축되었습니다. 즉, AWS 고객은 일상적인 보안 및 감사 작업에 시간을 적게 들이면서도 AWS 고객 환경의 보안을 높이고 감사 기능을 향상시킬 수 있는 예방 조치를 취하는 데 더 집중할 수 있습니다.

소개

점점 더 많은 고객이 클라우드에서의 작업이 많아지면서 감사자는 클라우드 작동 방법뿐 아니라 감사를 수행할 때 클라우드 컴퓨팅 능력을 유리하게 활용할 수 있는 방법도 파악해야 하는 상황이 되었습니다. AWS 클라우드는 감사자가 백분율 기반 샘플 테스팅에서 광범위한 실시간 감사 보기로 변경할 수 있도록 하여 고객 환경을 100% 감사할 수 있을 뿐 아니라 실시간 위험 관리도 수행할 수 있습니다.

AWS Management Console은 명령줄 인터페이스와 마찬가지로 여러 규제 기관, 표준 및 산업 기관의 감사자를 위해 강력한 결과를 생성할 수 있습니다. 이는 AWS에서 다음을 사용하여 보안, 설계별 규정 준수, 실시간 감사 기능을 설정할 수 있는 다수의 보안 구성을 지원함으로써 가능한 결과입니다.

- **자동화** – 스크립트 가능한 인프라(예: 코드형 인프라)를 통해 고객은 프로그램 가능한 (API 구동) 서비스 배포를 활용하는 방식으로 반복적이고 안정적이며, 안전한 배포 시스템을 만들 수 있습니다.

- **스크립트 가능한 아키텍처** – "특별한" 환경 및 Amazon 머신 이미지(AMI)를 안정적이고 감사 가능한 서비스에 배포하고, 실시간 위험 관리를 수행하도록 할 수 있습니다.

- **배포** – 시스템 관리자는 AWS CloudFormation에서 제공하는 기능을 사용하여 손쉽게 관련 AWS 리소스 모음을 생성하고 순서에 따라 예측 가능한 방식으로 프로비저닝할 수 있습니다.

- **확인 가능**– AWS CloudTrail, Amazon CloudWatch, AWS OpsWorks, AWS CloudHSM을 사용하여 증거 수집 기능을 활용할 수 있습니다.

AWS 감사 가이드 사용을 위한 접근 방식

검사관

AWS 서비스를 사용하는 조직을 평가할 때 반드시 AWS와 고객 간 "책임 공유" 모델을 이해해야 합니다. 감사 가이드는 요구 사항을 공통 보안 프로그램 제어 및 제어 영역으로 체계화합니다. 각각의 제어는 해당하는 감사 요구 사항을 참조합니다.

일반적으로 AWS 서비스는 고객이 서비스 및 애플리케이션을 작동하는 데 일반적으로 사용해 왔던 온프레미스 인프라 서비스와 유사한 방식으로 이해되어야 합니다. AWS에서 해당 기능을 제공하는 경우 장치 및 서버에 적용되는 정책 및 프로세스도 유사한 방식으로 적용되어야 합니다. 정책 또는 절차에만 관련된 제어는 일반적으로 전적으로 고객의 책임입니다. 이와 비슷하게 AWS 콘솔 또는 명령줄 API를 통한 AWS 관리는 권한이 많은 관리자 액세스처럼 다루어야 합니다. 자세한 내용은 부록 및 참조된 항목을 참조하십시오.

AWS에서 제공하는 증거

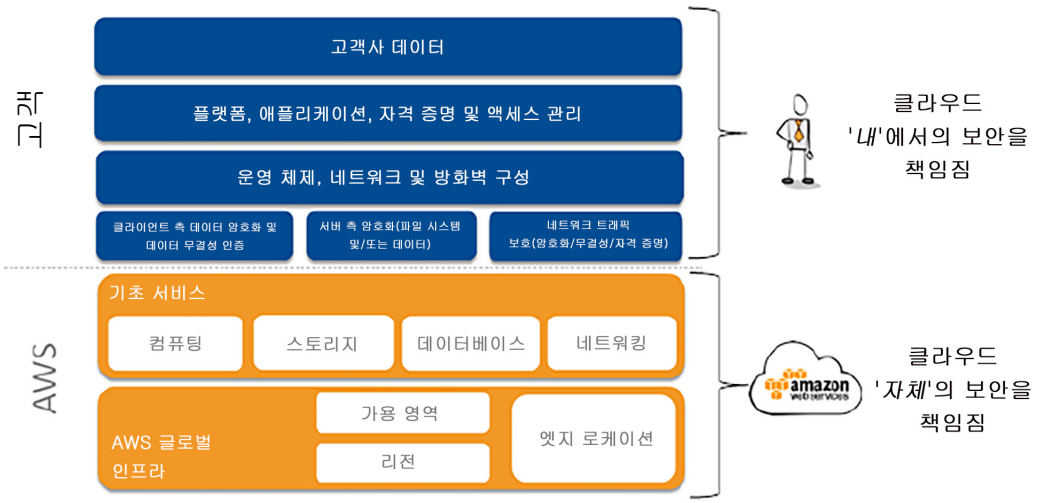
Amazon Web Services 클라우드 규정 준수를 시행하면 고객은 AWS에 클라우드의 보안 및 데이터 보호를 유지할 수 있는 강력한 제어 장치가 마련되어 있음을 이해할 수 있습니다. 시스템이 AWS 클라우드 인프라를 기반으로 하여 구축되었기 때문에 규정 준수 책임은 공유됩니다. 각 자격증은 특정 보안 제어가 마련되어 있으며 의도한 대로 작동 중임을 감사자가 확인했다는 의미입니다. AWS 계정 담당자에게 문의하여 해당되는 규정 준수 보고서를 볼 수 있습니다. AWS가 준수하는 보안 규정 및 표준에 대한 자세한 내용을 보려면 AWS 규정 준수 웹 페이지를 방문하십시오. AWS는 특정 정부, 산업 및 회사 보안 표준과 규제를 충족하도록 돕기 위해 AWS 클라우드 인프라가 광범위한 글로벌 보안 표준 목록의 요구 사항을 어떻게 충족하는지에 대해 설명하는 자격증 보고서를 제공합니다. 이러한 표준에는 다음이 포함됩니다. ISO 27001, SOC, PCI Data Security Standard, FedRAMP, Australian Signals Directorate(ASD) Information Security Manual, Singapore Multi-Tier Cloud Security Standard(MTCS SS 584)가 준수하는 보안 규정 및 표준에 대한 자세한 내용을 보려면 AWS 규정 준수 웹 페이지를 참조하십시오.

AWS 사용 감사 개념

다음 개념은 AWS에서 조직의 시스템 및 데이터에 대한 보안 감사를 수행하는 동안 고려해야 합니다.

- 클라우드 서비스 공급자(AWS)가 구현 및 운용하는 보안 측정 방법 – "클라우드의 보안"
- 고객의 콘텐츠 및 AWS 서비스를 사용하는 애플리케이션 보안과 관련하여 고객이 구현하고 운용하는 보안 측정 방법 – "클라우드 내에서의 보안"

AWS는 클라우드 **자체의** 보안을 관리하지만 클라우드 **내에서의** 보안을 유지하는 것은 고객의 몫입니다. 고객은 자신의 콘텐츠, 플랫폼, 애플리케이션, 시스템 및 네트워크를 보호하기 위해 구현하도록 선택한 보안에 대한 제어권을 보유하고 있으며, 이는 온사이트 데이터 센터의 애플리케이션에 적용되는 보안과 다르지 않습니다.



추가 세부 정보는 AWS 보안 센터, AWS 규정 준수 및 공개적으로 열람 가능한 AWS 백서(AWS 백서)에서 찾아볼 수 있습니다.

AWS의 자산 식별

고객의 AWS 자산은 인스턴스, 데이터 저장소, 애플리케이션 및 데이터 자체일 수 있습니다. 일반적으로 AWS 사용 감사는 자산을 식별하는 것에서 출발합니다. 퍼블릭 클라우드 인프라의 자산은 사내 환경과 절대적으로 다르지 않으며 AWS는 관리 중인 자산에 대한 가시성을 제공하므로 어떤 경우에는 자산목록에 대한 파악을 더 간단하게 할 수 있습니다.

AWS 계정 식별자

AWS는 각 AWS 계정에 AWS 계정 ID 및 정식 사용자 ID와 같은 고유 ID 2개를 할당합니다. AWS 계정 ID는 12자리 숫자(예: 123456789012)로 Amazon 리소스 이름(ARN)을 구성하는 데 사용합니다. IAM 사용자 또는 Amazon Clacier 볼트와 같은 리소스를 참조하는 경우 계정 ID는 다른 AWS 계정의 리소스와 사용자의 리소스를 구분합니다.

Amazon 리소스 이름(ARN) 및 AWS 서비스 네임스페이스

Amazon 리소스 이름(ARN)은 AWS 리소스를 고유하게 식별합니다. IAM 정책, Amazon Relational Database Service(RDS) 태그 및 API 호출과 같은 모든 AWS에서 리소스를 명료하게 지정해야 하는 경우 ARN이 필요합니다.

ARN 형식 예:

```
    <!-- Elastic Beanstalk application version -->
arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/My App/MyEnvironment

<!-- IAM user name -->
arn:aws:iam::123456789012:user/David

<!-- Amazon RDS tag -->
arn:aws:rds:eu-west-1:001234567890:db:mysql-db

<!-- Amazon S3 bucket (and all objects in it)-->
arn:aws:s3:::my_corporate_bucket/*
```

계정 식별자, Amazon 리소스 이름(ARN) 및 AWS 서비스 네임스페이스뿐 아니라 각각의 AWS 서비스는 고유 서비스 식별자(예: Amazon Elastic Compute Cloud(EC2) 인스턴스 ID: i-3d68c5cb 또는 Amazon Elastic Block Store(Amazon EBS) 볼륨 ID vol-ecd8c122)를 생성합니다. 이 식별자는 환경 자산 재고를 생성하는 데 사용할 수 있으며, 감사 및 재고 영역에 대한 작업 문서 내에서 사용할 수 있습니다.

각 자격증은 특정 보안 제어가 마련되어 있으며 의도한 대로 작동 중임을 감사자가 확인했다는 의미입니다.

1. 거버넌스

정의: 거버넌스는 고객의 방향 및 의도가 고객의 보안적 대처에 반영되었음을 확인합니다. 거버넌스는 정보 보안 프로그램 구현을 위한 구조화된 접근 방식을 사용하여 시행할 수 있습니다. 이 감사 계획은 어떤 AWS 서비스를 구매했는지, AWS 서비스와 함께 사용할 시스템 및 정보는 무엇인지, 이 서비스에 적용되는 정책, 절차 및 계획이 무엇인지에 대해 이해하는 것입니다.

주요 감사 대상: 어떤 AWS 서비스 및 리소스가 사용되고 있는지를 이해하고, 보안 또는 위험 관리 프로그램이 퍼블릭 클라우드 환경 사용에 고려되었는지를 확인합니다.

감사 접근 방식: 이 감사의 일환으로 조직 내 어떤 사람이 AWS 계정 및 리소스 소유자이며 이 소유자가 어떤 AWS 서비스 및 리소스를 사용 중인지 확인합니다. 정책, 계획 및 절차에 클라우드 개념이 포함되어 있으며 클라우드가 고객의 감사 프로그램 범위에 포함되어 있는지 확인합니다.

거버넌스 체크리스트

	체크리스트 항목
☐	조직 내 AWS 사용을 이해합니다. 다음과 같은 접근 방식이 있을 수 있습니다. • IT 및 개발 팀 투표 또는 인터뷰 • 네트워크 스캔 또는 심층적 침투 테스트 수행 ▪ Amazon.com 또는 AWS와 관련된 지출 보고서 및/또는 구매 주문서(PO) 지급을 검토하여 어떤 서비스를 사용 중인지 확인합니다. 신용 카드 대금은 "AMAZON WEB SERVICES AWS.AMAZON.CO WA" 또는 이와 비슷하게 표시됩니다. 참고: 조직의 개인이 개인 계정으로 AWS 계정에 가입했을 수 있으며 그런 경우 IT 및 개발 팀 투표 또는 인터뷰 사례인지 확인합니다.
☐	**자산을 식별합니다.** 각 AWS 계정에는 문의 전자 메일 주소가 연결되어 있으며 이 메일 주소로 계정 소유자를 식별할 수 있습니다. 사용자가 등록할 때 지정한 전자 메일 주소에 따라 이 전자 메일 주소가 퍼블릭 전자 메일 서비스 공급자가 제공하는 주소인지 확인해야 합니다. • 각 AWS 계정 또는 자산 소유자와 공식 모임을 갖고 AWS에 배포되어 있는 항목, 관리 방법, 이 항목이 조직의 보안 정책, 절차 및 표준과 어떻게 통합되었는지를 알아볼 수 있습니다.

	체크리스트 항목
	참고: AWS 계정 소유자는 경리부 또는 조달부의 누군가일 수 있지만, 조직의 AWS 리소스 사용을 *구현하는* 사람은 IT 부서에 속할 수 있습니다. 그런 경우 두 사람 모두 인터뷰해 보아야 할 수 있습니다.
☐	**검토할 AWS 경계를 정의합니다.** 검토할 범위를 정해야 합니다. 클라우드가 아닌 형태 현재 또는 미래의 클라우드 구현에 있어서 조직의 핵심 비즈니스 프로세스와 IT에 대한 조직의 지지를 확인합니다. • 사용 중이거나 사용을 고려하고 있는 AWS 서비스에 대한 설명을 듣습니다. • 사용 중이거나 사용을 고려하고 있는 AWS 서비스 유형을 식별한 후 검토에 포함할 서비스 및 비즈니스 솔루션을 결정합니다. • 이전 감사 보고서를 가져와서 수정 계획과 함께 확인합니다. • 이전 감사 보고서에서 미결된 문제를 파악하고 이 문제와 관련된 문서의 업데이트를 평가합니다.
☐	**정책을 평가합니다.** 조직의 보안, 개인 정보 보호, 데이터 분류 정책을 평가 및 검토하여 어떤 정책이 AWS 서비스 환경에 적용되는지 확인합니다. • AWS 서비스 취득에 대한 공식적인 정책 및/또는 프로세스가 존재하는지를 확인하여 어떻게 AWS 서비스 구매가 허가되었는지를 확인합니다. • 조직의 변경 관리 프로세스 및 정책에 AWS 서비스가 고려되었는지 확인합니다.
☐	**위험 요소를 식별합니다.** 해당되는 자산의 위험 요소 평가가 수행되었는지 여부를 확인합니다.
☐	**위험 요소를 검토합니다.** 위험 요소 평가 보고서의 복사본을 얻어 현재 환경이 반영되는지를 확인하고 남아 있는 위험 환경을 정확하게 기술합니다.
☐	**위험 문서를 검토합니다.** 각 요소를 검토한 후 위험 요소 처리 계획, 위험 요소 관리 정책 및 절차에 대한 일정/마일스톤을 검토합니다.
☐	**문서 및 재고.** AWS 네트워크가 완전히 문서화되었으며 모든 AWS 중요 시스템이

	체크리스트 항목
	자산목록 문서에 포함되어 있고 이 문서에 접근이 제한되는지 확인합니다. • AWS 리소스 재고에 대한 AWS Config 및 리소스 구성 내역을 검토합니다 *(예제 API 호출, 1)*. • 리소스에 태그가 적절히 지정되었으며 애플리케이션 데이터와 연결되었는지 확인합니다. • 애플리케이션 아키텍처를 검토하여 데이터 흐름, 데이터를 포함하는 애플리케이션 구성 요소 및 리소스 간 계획된 연결을 식별합니다. • 다음을 검토하여 네트워크와 AWS 플랫폼 간 모든 연결을 검토합니다. ▪ 고객 온프레미스 퍼블릭 IP가 고객이 소유한 모든 VPC의 고객 게이트웨이와 매핑된 VPN 연결 *(예제 API 호출, 2 및 3)* 고객이 소유한 하나 이상의 VPC와 매핑되었을 수 있는 Direct Connect 프라이빗 연결 *(예제 API 호출, 4)*
☐	**위험을 평가합니다.** 조직의 전체 위험 목록 및 위험 허용치에 대한 AWS 배포 데이터의 중요성을 평가합니다. 이러한 AWS 자산이 조직의 공식 위험 평가 프로그램과 통합되어 있는지 확인합니다. • AWS 자산을 식별해야 하며 AWS 자산에 위험 프로필에 따라 연결된 보호 목표가 있어야 합니다.
☐	**AWS 사용을 위험 평가에 통합합니다.** 조직 위험 평가 프로세스에 AWS 서비스 요소를 수행 및/또는 통합합니다. 주요 위험은 다음과 같을 수 있습니다. • AWS 사용과 관련된 기업 위험을 식별하고 기업 소유자 및 주요 이해관계자를 파악합니다. • 기밀성, 무결성 및 가용성 보호를 위한 AWS 서비스 사용 및 조직의 보안 기준 내에서 기업 위험이 정렬되고 등급이 매겨지거나 분류되었는지 확인합니다. • AWS 서비스(SOC, PCI, NIST 800-53 관련 감사 등)와 관련된 이전 감사를 검토합니다. • 이전에 식별된 위험이 적절하게 처리되었는지 확인합니다. • AWS 검토를 수행하기 위해 전체 위험을 평가합니다. • 위험 평가를 기준으로 하여 감사 범위 변경을 확인합니다. • IT 관리 부서와 함께 위험에 대해 논의하고 위험 평가를 조정합니다.

	체크리스트 항목
☐	**IT 보안 프로그램 및 정책.** 고객이 보안, 비용, 성능 및 내결함성의 4가지 항목에 대한 모범 사례 및 지침을 제공하는 AWS 서비스 Trusted Advisor 내에 강조 표시된 AWS 계정 수준 모범 사례를 비롯하여 AWS 서비스를 보안 정책 및 절차에 포함했는지 확인합니다. • 정보 보안 정책을 검토하고 여기에 AWS 서비스가 포함되어 있는지 확인합니다. • 직원에게 AWS 사용 및 보안에 대한 지휘권을 부여했으며, 최고 정보 보안 책임자를 비롯한 언급된 주요 역할에 대해 역할이 정의되었는지 확인합니다. **참고:** 정보 보안 아키텍처 및 프로세스를 모델링하는 데 사용한 게시된 사이버 보안 위험 관리 프로세스 표준 • AWS 타사 자격증 검토를 비롯한 AWS 서비스에 대해 수행된 감사를 지원할 수 있는 설명서를 보유하고 있는지 확인합니다. • AWS 보안(예: Amazon IAM 사용, Amazon EC2 보안 그룹) 및 Amazon EC2 인스턴스에 대한 원격 액세스가 내부 교육 기록에 포함되었는지 확인합니다. • 사이버 보안 대응 정책 및 AWS 서비스 교육이 유지되고 있는지 확인합니다. **참고**: 특히 고객의 AWS 서비스 사용과 관련된 보험 및 결과적으로 사이버 보안 보안 사고로 기인한 손실 및 지출과 관련된 청구
☐	**서비스 공급자 감독.** AWS와의 계약에 사이버 보안 요구 사항에 대한 개인 정보 보호 및 보안 보호를 구현하고 유지하기 위한 요구 사항이 포함되는지 확인합니다.

2. 네트워크 구성 및 관리

정의: AWS에서 네트워크 관리는 방화벽 및 라우터가 가상이라는 점의 네트워크 구성 요소를 제외하면 네트워크 관리 온프레미스와 매우 유사합니다. 고객은 네트워크 아키텍처가 조직의 보안 요구 사항을 따르는지 확인해야 합니다. 이 요구 사항에는 퍼블릭 및 프라이빗(신뢰할 수 없거나 신뢰할 수 있는) 리소스를 구분하기 위한 DMZ 사용, 서브넷 및 라우팅 테이블을 사용한 리소스 분리, DNS의 보안 구성, VPN 형식으로 추가 전송 보호가 필요한지 여부, 인바운드 및 아웃바운드 트래픽을 제한할지 여부가 포함됩니다. 네트워크 모니터링을 수행해야 하는 고객은 호스트 기반 침입 탐지 및 모니터링 시스템을 사용하여 이를 수행할 수 있습니다.

주요 감사 대상: 보안 노출로 이어질 수 있는 외부 액세스/네트워크 보안과 관련된 누락되거나 부적절하게 구성된 보안 제어

감사 접근 방식: 고객 AWS 리소스의 네트워크 아키텍처, 퍼블릭 인터넷 및 고객의 프라이빗 네트워크에서 외부 액세스를 허용하도록 리소스가 구성된 방법을 이해해야 합니다. 참고: AWS Trusted Advisor를 AWS 구성 설정 검증 및 확인에 활용할 수 있습니다.

네트워크 구성 및 관리 체크리스트

	체크리스트 항목
☐	**네트워크 제어.** 네트워크 세그먼트가 AWS 환경 내에서 적용되는 방식을 식별합니다. • AWS 보안 그룹 구현, 네트워크 세분화, ACL, 방화벽 설정 또는 AWS 서비스를 적절하게 구현하기 위한 AWS Direct Connect 및 Amazon VPN 구성*(예제 API 호출, 5 - 8)* • Amazon EC2 네트워크 및 시스템에 대한 AWS 콘솔 액세스 및 원격 액세스를 수행하기 위해 원격, 인터넷 또는 VPN 액세스 권한을 직원에게 부여할 수 있는 절차가 있는지 확인합니다. • 기업 환경과 구분된 소프트웨어 및 애플리케이션의 테스트 및 개발 환경을 유지하기 위해 다음 사항을 검토합니다. ▪ VPC 격리가 기업 환경 및 테스트 및 개발용으로 사용되는 환경 사이에 수행되고 있음 ▪ VPC 간 VPC 피어링 연결을 검토하여 네트워크 격리가 VPC 사이에 수행되고 있는지 확인 ▪ 서브넷 격리가 기업 환경 및 테스트 및 개발용으로 사용되는 환경 사이에 수행되고 있음 ▪ 기업 및 테스트/개발 환경이 위치해 있는 서브넷과 연관된 NACL을 검토하여 네트워크 격리가 수행되고 있는지 확인 ▪ Amazon EC2 인스턴스 격리가 기업 환경 및 테스트 및 개발용으로 사용되는 환경 사이에 수행되고 있음 ▪ 기업, 테스트 또는 개발 환경과 연관된 하나 이상의 인스턴스와 연관된 보안 그룹을 검토하여 Amazon EC2 인스턴스 사이에 네트워크 격리가 시행되고 있는지 확인 ▪ 다음과 같은 DDoS 솔루션의 일부로 활용되는 AWS 검토 구성 요소에서 직접 작동되는 실행 중인 DDoS 계층화된 방어 솔루션을 검토합니다. ▪ Amazon CloudFront 구성 ▪ Amazon S3 구성 ▪ Amazon Route 53 ▪ ELB 구성

	체크리스트 항목
	▪ 참고: 위 서비스는 고객이 소유한 퍼블릭 IP 주소를 사용하지 않으며 DoS AWS 상속 DoS 완화 기능을 제공합니다. ▪ 프록시 또는 WAF에 대한 Amazon EC2 사용 자세한 지침은 "DDoS 복원력에 대한 AWS 모범 사례 백서"에서 확인할 수 있습니다.
☐	**악의적인 코드 제어.** Amazon EC2 인스턴스의 맬웨어 방지 소프트웨어 구현 및 관리를 물리적 시스템에서와 비슷한 방식으로 평가합니다.

3. 자산 구성 및 관리

정의: AWS 고객은 AWS 리소스에 설치된 모든 항목 또는 AWS 리소스 연결에 대한 보안을 유지할 책임이 있습니다. 고객이 수행하는 AWS 리소스 보안 관리는 어떤 리소스를 사용 중인지(자산 목록), 리소스에 게스트 OS 및 애플리케이션이 안전하게 구성되었는지(안전한 구성 설정, 패치 적용 및 맬웨어 방지 소프트웨어), 리소스에 대한 변경을 어떻게 제어하고 있는지(변경 관리)를 알고 있는 것입니다.

Major audit focus: 운영 체제와 애플리케이션 보안 취약성을 관리하여 보안, 안정성, 자산의 무결성을 보호합니다.

감사 접근 방식: OS 및 애플리케이션이 정책, 절차 및 표준에 따라 설계, 구성, 패치 적용 및 강화되었는지 검증합니다. 모든 OS 및 애플리케이션 관리 사례는 온프레미스 및 AWS 시스템과 서비스 간에 공통될 수 있습니다.

자산 구성 및 관리 체크리스트

	체크리스트 항목
☐	**자산 구성 관리.** 모든 AWS 시스템 구성 요소에 대한 구성 관리 사용 사례를 확인하고 이러한 표준이 기준 구성을 충족하는지 검증합니다. • 정해진 요구 사항 준수를 위해 볼륨을 삭제하기 전에 특수화된 초기화 절차를 수행하기 위한 절차를 검토합니다. • Identity Access Management 시스템을 검토합니다. 이 시스템은 AWS 서비스를 기반으로 호스트되는 애플리케이션에 대한 허가된 액세스를 허용하는 데 사용할 수 있습니다. • 침투 테스트가 완료되었는지 확인합니다.
☐	**변경 관리 제어.** AWS 서비스 사용이 내부 시리즈와 동일한 변경 제어 프로세스를 따르는지 확인합니다. • AWS 서비스가 내부 패치 관리 프로세스 내에 포함되어 있는지 확인합니다. Amazon EC2 인스턴스의 구성 및 패치 적용에 대해 문서화된 프로세스를 검토합니다. ▪ Amazon 머신 이미지(AMI)*(예제 API 호출, 9 - 10)* ▪ 운영 체제 ▪ 애플리케이션 • IT 자산이 적절하게 폐기되었는지 확인하기 위해 삭제 호출에 대한 범위 내 서비스를 위한 API 호출을 검토합니다.

4. 논리적 액세스 제어

정의: 논리적 액세스 제어는 특정 시스템 리소스에 대한 액세스 권한을 가질 수 있는 사람 또는 항목만 결정하는 것이 아니라 리소스에서 수행할 수 있는 작업 유형(읽기, 쓰기 등)도 결정합니다. AWS 리소스에 대한 액세스 제어의 일부로, 사용자 및 프로세스는 자격 증명을 제공하여 특정 기능을 수행할 수 있음을 허가받았거나 특정 리소스에 대한 액세스 권한이 있음을 확인해야 합니다. AWS에서 요구하는 자격 증명은 서비스 유형 및 액세스 방식에 따라 다양하며 암호, 암호화 키 및 인증서가 포함됩니다. AWS 리소스에 대한 액세스는 AWS 계정, AWS 계정으로 생성된 개별 AWS Identify and Access Management(IAM) 사용자 계정 또는 고객의 회사 디렉토리와 자격 증명 연동(single sign-on)을 통해 수행할 수 있습니다. AWS Identity and Access Management(IAM)를 통해 사용자는 AWS 서비스와 리소스에 대한 액세스를 안전하게 제어할 수 있습니다. IAM을 사용하면 AWS 사용자 및 그룹을 생성하고 관리하며, 권한을 사용하여 AWS 리소스에 대한 권한을 허용 및 거부할 수 있습니다.

Major audit focus: 이 감사 부분에서는 AWS 서비스에 대해 사용자 및 권한을 설정하는 방법을 식별하는 데 중점을 둡니다. 모든 AWS 계정과 연결된 자격 증명을 안전하게 관리하고 있는지를 확인하는 것도 중요합니다.

감사 접근 방식: AWS 자산에 대한 권한이 조직의 정책, 절차 및 프로세스에 따라 관리되고 있는지 검증합니다. 참고: AWS Trusted Advisor를 활용하여 IAM 사용자, 그룹 및 역할 구성을 검증 및 확인할 수 있습니다.

논리적 액세스 제어 체크리스트

	체크리스트 항목
☐	**액세스 관리, 인증 및 권한 부여.** AWS 서비스 및 Amazon EC2 인스턴스에 대한 액세스를 관리하기 위한 내부 정책 및 절차가 있는지 확인합니다. • AWS 액세스 제어 사용 및 구성에 대한 문서를 확인합니다. 예제 및 옵션은 아래에 요약되어 있습니다. ▪ Amazon IAM이 액세스 관리에 사용되는 방법 설명 ▪ Amazon IAM이 관리에 사용되는 제어 목록 – 리소스 관리, 보안 그룹, VPN, 객체 권한 등 ▪ 고유 AWS 액세스 제어 사용 또는 액세스가 개방형 표준 Security Assertion Markup Language(SAML) 2.0을 활용하는 연동된 인증을 통해 관리되는지 여부 ▪ AWS 계정, 역할, 그룹 및 사용자, 정책 및 사용자, 그룹, 역할에 연결된 정책*(예제 API 호출, 11)* ▪ Amazon IAM 계정, 역할 및 모니터링 방식에 대한 설명 ▪ EC2 내의 시스템 설명 및 구성
☐	**원격 액세스.** 승인 프로세스, 로깅 프로세스가 있거나 허가되지 않은 원격 액세스를 금지하는 제어가 있는지 확인합니다. 참고: AWS 및 Amazon EC2 인스턴스에 대한 모든 액세스는 Direct Connect가 구성되지 않는 경우 "원격 액세스"로 정의됩니다. • 허가되지 않은 액세스를 금지하기 위한 프로세스를 검토합니다. 허가되지 않은 액세스에는 다음이 포함될 수 있습니다. ▪ 서비스 수준 API 호출 로깅을 위한 AWS CloudTrail ▪ 로깅 객체를 충족하기 위한 AWS CloudWatch 로그

	체크리스트 항목
	▪ 허가되지 않은 액세스 금지 제어를 위한 IAM 정책, S3 버킷 정책, 보안 그룹 ▪ 회사 네트워크와 AWS 사이의 연결을 검토합니다. ▪ VPC와 회사 네트워크 사이의 VPN 연결. ▪ 회사 및 AWS 간 Direct Connect(교차 연결 및 프라이빗 인터페이스) ▪ AWS 및 네트워크 간 액세스를 제어하기 위해 정의된 보안 그룹, 네트워크 액세스 제어 목록 및 라우팅 테이블
☐	**인력 제어.** AWS 서비스에 대한 사용자 제한이 비즈니스 기능에서 엄격하게 지켜지는지를 확인합니다 *(예제 API 호출, 12)*. • AWS 서비스와 연관되므로 준비된 액세스 제어 유형을 검토합니다. ▪ AWS 수준의 AWS 액세스 제어 – 네트워크 내에서 Amazon EC2 인스턴스 관리(시작/중지/종료)를 제어하기 위해 태그 지정을 지원하는 IAM 사용 ▪ 고객 액세스 제어 – 운영 체제/애플리케이션 계층에서 네트워크에 존재하는 리소스에 대한 액세스를 관리하기 위해 IAM(LDAP 솔루션) 사용 ▪ 네트워크 액세스 제어 – 고객이 소유한 VPC 내의 리소스에 대한 네트워크 액세스를 제어하기 위해 AWS 보안 그룹(SG), 네트워크 액세스 제어 목록(NACL), 라우팅 테이블, VPN 연결, VPN 피어링 사용

5. 데이터 암호화

정의: AWS 소유자만 자신이 생성한 AWS 리소스에 액세스할 수 있기 때문에 AWS에 저장된 데이터는 기본적으로 안전합니다. 하지만 민감한 데이터가 있는 고객의 경우 AWS에 데이터를 저장할 때 암호화를 수행하여 보호를 강화해야 할 수 있습니다. 현재 Amazon S3 서비스에서만 자동화된 서버 측 암호화 기능을 제공하며 이를 통해 고객은 데이터가 저장되기 전에 고객 측에서 암호화를 수행할 수 있습니다. 기타 AWS 데이터 스토리지 옵션의 경우 고객이 데이터 암호화를 수행해야 합니다.

Major audit focus: 저장된 데이터는 온프레미스 데이터가 보호되는 것과 동일한 방식으로 암호화해야 합니다. 또한, 대부분의 보안 정책은 인터넷을 안전하지 않은 통신 미디엄으로 간주하고 전송 중에 데이터 암호화를 요구합니다. 부적절한 데이터 보호는 보안 노출로 이어질 수 있습니다.

감사 접근 방식: 데이터가 상주하는 위치를 확인하고, 저장된 데이터 및 전송 중("이동 중"인 데이터라고도 함)인 데이터를 보호하는 데 사용되는 방식을 검증합니다. 참고: AWS Trusted Advisor를 활용하여 데이터 자산에 대한 권한 및 액세스를 검증 및 확인할 수 있습니다.

데이터 암호화 체크리스트

	체크리스트 항목
☐	**암호화 제어.** AWS 서비스를 사용하는 동안 전송 중인 기밀 정보를 보호하기 위해 적합한 제어가 수행되고 있는지 확인합니다. ▪ 암호화를 강화하기 위해 AWS 콘솔에 대한 연결, API, S3, RDS 및 Amazon EC2 VPN 관리에 대한 방식을 검토합니다. ▪ AWS 서비스 및 Amazon EC2 인스턴스를 포함하여 키 관리를 위한 내부 정책 및 절차가 있는지 확인합니다. ▪ 저장된 PIN을 보호하는 데 사용된 암호화 방식 검토 – AWS는 저장된 데이터 암호화를 수행하는 데 사용할 수 있는 다양한 키 관리 서비스(예: KMS, CloudHSM 및 S3에 대한 서버 측 암호화)를 제공합니다*(예제 API 호출, 13-15)*.

6. 보안 로깅 및 모니터링

정의: 감사는 정보 시스템 및 네트워크 내에서 발생하는 다양한 이벤트를 기록합니다. 감사 로그는 해당 시스템의 보안에 영향을 미칠 수 있는 작업을 실시간으로 또는 해당 작업이 발생한 후에 식별하는 데 사용되므로 로그를 적절하게 구성하고 보호해야 합니다.

Major audit focus: 시스템은 온프레미스 시스템과 똑같이 로깅 및 모니터해야 합니다. 전체 회사 보안 계획에 AWS 시스템이 포함되어 있지 않은 경우 중요한 시스템이 모니터링 범위에서 생략될 수 있습니다.

감사 접근 방식: 게스트 OS 및 Amazon EC2 인스턴스에 설치된 중요한 애플리케이션에서 감사 로깅이 수행되고 있는지 검증합니다. 특히, 감사 로깅은 로그 저장, 보호 및 분석과 관련되므로 해당 구현이 정책 및 절차에 맞게 조정되었는지 검증합니다.

보안 로깅 및 모니터링 체크리스트:

	체크리스트 항목
☐	**평가 추적 로깅 및 모니터링.** 타당성, 보존성, 정의된 임계값 및 안전한 유지 관리, 특히 AWS 서비스의 허가되지 않은 작업 감지에 대한 로깅 및 모니터링 정책과 절차를 검토합니다. • 로깅 및 모니터링 정책과 절차를 검토하고 보안 관련 이벤트에 대해 Amazon EC2 인스턴스를 비롯한 AWS 서비스가 포함되었는지 확인합니다. • 중앙 집중식 서버에 로그를 전송하도록 로깅 메커니즘이 구성되었는지 확인하고 Amazon EC2 인스턴스의 경우 적합한 로그 유형 및 형식이 물리적 시스템과 비슷한 방식으로 유지되고 있는지 확인합니다. • AWS CloudWatch를 사용하는 고객의 경우 네트워크 모니터링 사용 프로세스 및 기록을 검토합니다. • 이벤트 분석이 방어 조치 및 정책을 개선하는 데 활용되는지 확인합니다. • 허가되지 않은 사용자에 대한 AWS IAM 자격 증명 보고서, AWS Config 및 허가되지 않은 장치에 대한 리소스 태그 지정을 검토합니다*(예제 API 호출, 16)*. • 다음과 같은 AWS 서비스를 사용하여 여러 소스의 이벤트 데이터 집계 및 상호 연관을 확인합니다. ▪ VPC에 들어가는 수락되거나 거부된 네트워크 패킷을 식별하기 위한 VPC 흐름 로그 ▪ AWS 서비스에 대한 인증되지 않았고 허가되지 않은 API 호출을 식별하기 위한 AWS CloudTrail ▪ ELB 로깅 – 로드 밸런서 로깅 ▪ AWS CloudFront 로깅 – CDN 배포 로깅
☐	**침입 탐지 및 대응.** Amazon EC2 인스턴스의 호스트 기반 IDS를 물리적 시스템에서와 비슷한 방식으로 검토합니다. • 어디서 침입 탐지 프로세스가 발생했는지에 대한 정보를 검토할 수 있는 AWS가 제공하는 증거를 검토합니다.

7. 보안 사고 대응

정의: 책임 공유 모델에서 보안 이벤트는 AWS 및 AWS 고객 모두의 상호 작용으로 모니터할 수 있습니다. AWS는 하이퍼바이저 및 기본 인프라에 영향을 미치는 이벤트를 탐색하고 이에 대응합니다. 고객은 게스트 운영 체제에서 애플리케이션까지 이벤트를 관리합니다. 인시던트 대응 책임을 이해해야 하며 기존 보안 모니터링/경보/감사 도구 및 AWS 리소스에 대한 프로세스를 조정해야 합니다.

Major audit focus: 보안 이벤트는 자산 위치와 상관없이 모니터되어야 합니다. 감사자는 모든 환경의 보안 사고 관리 제어 배포에 대한 일관성을 평가할 수 있으며 테스팅을 통해 전체 범위를 검증할 수 있습니다.

감사 접근 방식: AWS 환경에서 시스템의 보안사고 관리 제어가 존재하는지 여부와 작동으로 발생하는 영향을 평가합니다.

보안 사고 대응 체크리스트:

	체크리스트 항목
☐	**사고 대응 보고.** 보안 사고 대응 계획 및 사이버 보안 사고에 대한 정책에 AWS 서비스가 포함되어 있으며 사이버 보안 사고를 완화하고 복구를 도와주는 제어 기능이 있는지 확인합니다. • 기존 보안사고 모니터링 도구뿐 아니라 사용 가능한 AWS 도구를 활용하여 AWS 서비스 사용을 모니터하는지 확인합니다. • 보안 사고 대응 계획을 주기적으로 검토하고 AWS와 관련된 변경이 필요에 따라 이루어지고 있는지 확인합니다. • 보안사고 대응 계획에 알림 절차가 있으며, 고객이 공격과 관련된 손실 또는 침입으로 인한 영향에 대처하는 방법을 확인합니다.

8. 재해 복구

정의: AWS는 고객이 복원력이 뛰어난 애플리케이션을 구축할 수 있고 주요 보안 사고 또는 재난 시나리오에 재빨리 대응할 수 있는 고가용성 인프라를 제공합니다. 하지만 고객은 AWS에서 제공하는 여러 리전 및 가용 영역을 활용하여 고가용성이나 빠른 복구 시간이 보장되도록 시스템을 구성하고 있는지 확인해야 합니다.

Major audit focus: 통합된 오류 단일 지점 및/또는 재난 복구 시나리오를 처리하기에 부적합한 계획은 중대한 영향을 불러올 수 있습니다. AWS에서 개별 인스턴스/서비스 수준에 서비스 수준 계약(SLA)을 제공하고 있지만 이러한 계약을 목표 복구 시간(RTO) 목표 복구 시점(RPO)과 같은 고객의 비즈니스 연속성(BC) 및 재해 복구(DR) 목표와 혼동하면 안 됩니다. BC/DR 파라미터는 각 솔루션 설계와 연결됩니다. 복원력이 뛰어난 설계는 다양한 AWS 가용 영역의 여러 구성 요소를 활용하고 데이터 복제에도 관련됩니다.

감사 접근 방식: DR을 이해하고 중요 자산에 적용된 장애허용 아키텍처를 확인합니다. 참고: AWS Trusted Advisor를 활용하여 고객의 복원 기능 측면을 검증 및 확인할 수 있습니다.

재해 복구 체크리스트:

	체크리스트 항목
☐	**비즈니스 연속성 계획(BCP).** 활용되고 있는 AWS 서비스에 대한 포괄적인 BCP가 있는지 확인합니다. 이 BCP는 사이버 보안 사고의 영향을 완화하거나 해당 사고에 대한 복구를 수행합니다. • 이 계획 내에서 긴급 준비, 위험 관리 요소, 선임 관리자의 감독 책임 및 테스팅 계획에 AWS가 포함되어 있는지 확인합니다.
☐	**백업 및 스토리지 제어.** 고객이 AWS 서비스에 대한 백업 시스템을 주기적으로 테스트한 결과를 검토합니다*(예제 API 호출, 17-18)*. 1. 오프사이트 백업으로 AWS 서비스에 백업한 데이터의 목록을 검토합니다.

9. 상속된 제어

정의: Amazon은 대규모의 데이터 센터를 디자인하고 구축하고 운영하는 데에서 축적한 수 년간의 경험을 AWS 플랫폼과 인프라에 적용하였습니다. AWS 데이터 센터는 평범해 보이는 건물에 구축되어 있으며, AWS 데이터 센터라고 명시되지 않습니다. 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 직원은 2단계 인증을 최소 두 번 통과해야 데이터 센터에 접근할 수 있습니다.
모든 방문자 및 계약자는 신분증을 제시해야 하며, 통과한 후에는 허가받은 직원의 지속적인 안내를 받습니다.

AWS는 합법적인 업무 목적으로 이러한 권한이 필요한 계약직원과 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 모든 물리적인 접근은 기록되어 정기적으로 감사를 받습니다.

Major audit focus: 이 감사 섹션은 서비스 공급자를 선택하는 데 합당한 실사를 수행했음을 증명하기 위해 존재합니다.

감사 접근 방식: 제어 목표와 제어의 설계 및 운용 효과를 합리적으로 보증하기 위해 제3자 증명 및 인증서를 요청하고 평가할 수 있는 방법을 이해합니다.
상속된 제어 체크리스트

	체크리스트 항목
☐	**물리적 보안 및 환경 제어.** 물리적 보안 제어를 위해 AWS에서 관리하는 침입 탐지 프로세스에 대한 정보를 검토할 수 있는 AWS 제공 증거를 자세히 검토합니다.

결론

평가 수행에 도움이 될 만한 타사 도구는 많습니다. AWS 고객은 자신의 운영 체제, 네트워크 설정, 트래픽 라우팅을 전체적으로 제어하고 있으며, 사내에서 사용되는 도구 대부분을 AWS에서 자산을 평가하고 감사하는 데 사용할 수 있습니다.

AWS에서 제공하는 유용한 도구는 AWS Trusted Advisor 도구입니다. AWS Trusted Advisor는 수십 만의 AWS 고객에게 서비스를 제공한 AWS의 운영 내역 집계에서 확인된 모범 사례를 활용합니다. AWS Trusted Advisor는 고객의 AWS 환경에서 몇 가지 기본 요소를 검사하고 비용 절감, 시스템 성능 개선 또는 보안 격차를 해결할 기회가 생기면 이를 권장합니다.

이 도구는 조직의 감사 및 평가 프로세스를 개선하고 지원하기 위한 감사 체크리스트의 일부를 수행하는 데 활용할 수 있습니다.

부록 A: 참조 자료

1. Amazon Web Services: Overview of Security Processes - https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf
2. Amazon Web Services Risk and Compliance Whitepaper - https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
3. AWS OCIE Cybersecurity Workbook - https://d0.awsstatic.com/whitepapers/compliance/AWS_SEC_Workbook.pdf
4. Using Amazon Web Services for Disaster Recovery - http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf
5. Identity federation sample application for an Active Directory use case - http://aws.amazon.com/code/1288653099190193
6. 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
7. Authenticating Users of AWS Mobile Applications with a Token Vending Machine http://aws.amazon.com/articles/4611615499399490?_encoding=UTF8&queryArg=searchQuery&fromSearch=1&searchQuery=Token%20Vending%20machine
8. Client-Side Data Encryption with the AWS SDK for Java and Amazon S3 - http://aws.amazon.com/articles/2850096021478074
9. AWS Command Line Interface - http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html
10. Amazon Web Services Acceptable Use Policy - http://aws.amazon.com/aup/

부록 B: 용어 정의

인증: 인증이란 어떠한 사람이 주장하는 개체 또는 무엇에 부합하는지에 대한 여부를 판단하는 과정입니다.

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

EC2: Amazon Elastic Compute Cloud(EC2)는 클라우드에서 컴퓨팅 파워의 규모를 자유자재로 변경할 수 있는 웹 서비스입니다. 개발자가 보다 쉽게 웹 규모 클라우드 컴퓨팅 작업을 할 수 있도록 설계되었습니다.

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

IAM: AWS Identity and Access Management(IAM)는 IAM 고객이 AWS에서 사용자 및 사용자 권한을 관리할 수 있도록 하는 웹 서비스입니다.

객체: Amazon S3에 저장되는 기본 개체입니다. 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.

서비스: 네트워크 전체에 걸쳐 제공되는 소프트웨어 또는 컴퓨팅 기능(예: EC2, S3, VPC 등)입니다.

부록 C: API 호출

AWS 명령줄 인터페이스는 AWS 서비스를 관리하는 통합 도구입니다.
http://docs.aws.amazon.com/cli/latest/reference/index.html#cli-aws

1. 태그가 지정된 모든 리소스 나열
    - aws ec2 describe-tags

http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-tags.html

2. 고객 AWS 계정의 모든 고객 게이트웨이 나열:
    - aws ec2 describe-customer-gateways –output table
3. 고객 AWS 계정의 모든 VPN 연결 나열
    - aws ec2 describe-vpn-connections
4. 모든 고객 Direct Connect 연결 나열
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
5. List all Customer Gateways on the customers AWS account:
    - aws ec2 describe-customer-gateways –output table
6. List all VPN connections on the customers AWS account
    - aws ec2 describe-vpn-connections
7. List all Customer Direct Connect connections
    - aws directconnect describe-connections
    - aws directconnect describe-interconnects
    - aws directconnect describe-connections-on-interconnect
    - aws directconnect describe-virtual-interfaces
8. 보안 그룹에 중점을 둔 CLI를 대신 사용:
    - aws ec2 describe-security-groups
9. 현재 고객이 소유/등록한 AMI 나열
    - aws ec2 describe-images –owners self

10. 특정 AMI로 시작된 모든 인스턴스 나열
    - aws ec2-describe-instances --filters "Name=image-id,Values=XXXXX" (XXXX = image-id 값, 예: ami-12345a12)
11. IAM 역할/그룹/사용자 나열
    - aws iam list-roles
    - aws iam list-groups
    - aws iam list-users
12. 그룹/역할/사용자에 할당된 정책 나열:
    - aws iam list-attached-role-policies --role-name XXXX
    - aws iam list-attached-group-policies --group-name XXXX
    - aws iam list-attached-user-policies --user-name XXXX

    여기서 XXXX는 고객 AWS 계정 내 리소스 이름입니다.
13. KMS 키 나열
    - aws kms list-aliases
14. 키 교체 정책 나열
    - aws kms get-key-rotation-status –key-id XXX(XXX = AWS 계정의 key-id)
15. KMS 키로 암호화된 EBS 볼륨 나열
    - aws ec2 describe-volumes "Name=encrypted,Values=true"
    - targeted e.g. us-east-1)
16. 자격 증명 보고서
    - aws iam generate-credential-report
    - aws iam get-credential-report
17. EBS 볼륨의 스냅샷/백업 생성
    - aws ec2 create-snapshot --volume-id XXXXXXX
    - (XXXXXX = AWS 계정 내 볼륨의 ID)
18. 완료된 스냅샷/백업 확인
    - aws ec2 describe-snapshots --filters "Name=volume-id,Values=XXXXXX)