규모별 보안: AWS 기반 거버넌스

온프레미스 문제를 해결해 줄 수 있는 AWS 기능 분석

2015년 10월

(이 문서의 최신 버전은 https://aws.amazon.com/compliance/aws-whitepapers/ 를 참조하십시오.)

amazon web services

목차

요약

온프레미스에서 실행하는 거의 모든 작업을 AWS에서도 실행할 수 있습니다. 웹 사이트, 애플리케이션, 데이터베이스, 모바일 앱, 이메일 캠페인, 분산 데이터 분석, 미디어 스토리지 및 프라이빗 네트워크 등이 그 예입니다. AWS가 제공하는 서비스는 다른 서비스와 함께 작동하도록 설계되었으므로 완벽한 솔루션을 구축할 수 있습니다. AWS로 워크로드를 마이그레이션할 때 종종 간과하는 한 가지 이점은, 제공되는 많은 거버넌스 설정 기능을 활용함으로써 대규모로 높은 수준의 보안을 확보할 수 있다는 것입니다. 동일한 이유로 클라우드상의 인프라를 구축할 때도 온프레미스 구축에 비해 클라우드 기반 거버넌스가 보다 높은 수준의 관리, 보안 제어 및 중앙 자동화를 제공함으로써 낮은 초기 비용, 더 쉬운 작업, 개선된 민첩성 등의 이점을 제공합니다. 이 문서에서는 AWS를 사용하여 IT 리소스를 높은 수준의 거버넌스로 유지할 수 있는 방법을 설명합니다. AWS 위험 및 규정 준수 백서 및 Auditing Security Checklist whitepaper와 함께 이 문서에서는 AWS 서비스에 내장된 보안 및 거버넌스 기능에 대해 설명하므로 AWS와 통합된 환경을 만들 때 얻을 수 있는 보안 이점에 대해 알고 모범 사례를 살펴볼 수 있습니다.

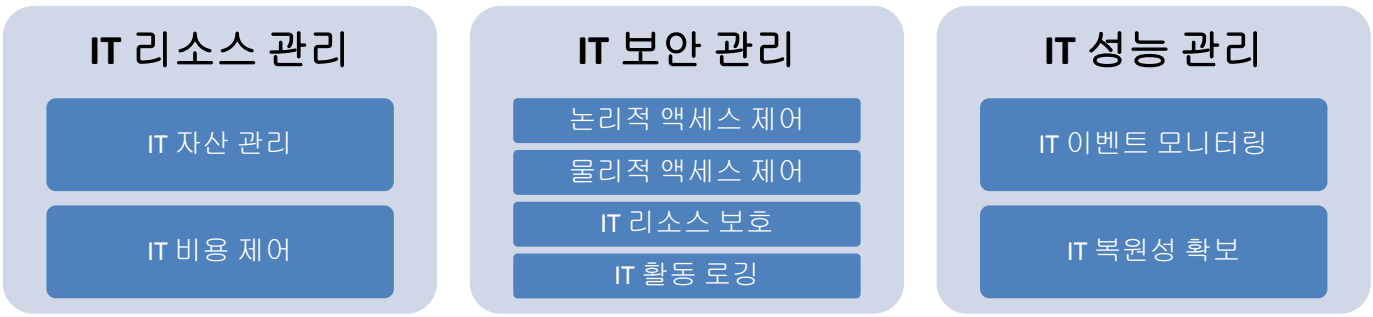
서론

산업 기관 및 규제 기관에서 광범위한 보안 및 조직적 거버넌스 방법을 의무화하는 법규를 제도화하고 있습니다. 리서치 기관에 따르면 많은 기업들이 IT 예산의 75% 상당을 인프라를 관리하는 데 쓰고 있으며, 기업의 비즈니스에 직접 관련된 IT 업무에는 IT 예산의 25%만을 사용하고 있는 것이 현실이라고 합니다. 이러한 지표를 개선할 수 있는 중요한 방법 중 하나는 백엔드 IT 거버넌스 요구 사항을 보다 효율적으로 다루는 것입니다. 이렇게 하는 쉽고 효과적인 방법은 AWS의 내장 거버넌스 기능을 활용하는 것입니다.

AWS가 다양한 IT 거버넌스 설정 기능을 제공하는 반면에, 이로 인해 AWS를 어떻게 시작해야 할지 및 무엇을 구현해야 할지를 결정하는 일은 어려울 수 있습니다. 이 문서에서는 사용 사례(또는 온프레미스 문제), AWS 설정 기능, 이러한 기능 사용과 연관된 거버넌스 가치 제안을 제공함으로써 일반적인 IT 거버넌스 도메인을 살펴봅니다. 이 문서는 사용자가 각 IT 거버넌스 도메인[1] 목표를 달성하도록 돕기 위해 작성되었습니다.

이 문서는 일반적으로 적용되는 IT 거버넌스 프레임워크(예: CoBIT, ITIL, COSO, CMMI 등)의 기본 도메인 접근법을 따릅니다. 그러나 이 문서에서 구성된 IT 거버넌스 도메인은 일반적이기 때문에 모든 고객이 이를 활용하여 AWS 사용 시 거버넌스 기능과 자신의 온프레미스 리소스 및 도구로 실행할 수 있는 작업을 비교해 볼 수 있도록 해줍니다. 다음 IT 거버넌스 도메인을 "사용 사례" 접근법을 통해 살펴보겠습니다.

개선하고 싶은 작업은...



[1] 이 문서에서는 거버넌스 설정 기능의 많은 목록을 제공하고 있지만, 새로운 기술들이 계속해서 개발되고 있으므로 제공되는 모든 기능이 포함되어 있지는 않습니다. 추가 자습서, 개발자 도구 및 설명서는 http://aws.amazon.com/resources/ 에서 찾을 수 있습니다.

IT 리소스 관리

IT 자산 관리

IT 자산을 식별하고 관리하는 것이 효과적인 IT 거버넌스의 첫 번째 단계입니다. IT 자산은 하이엔드 라우터, 스위치, 서버, 호스트 및 애플리케이션 방화벽, 서비스, 운영 체제 및 네트워크에 배포된 기타 소프트웨어 자산까지 다양합니다. 하드웨어 및 소프트웨어 자산 재고가 업데이트되면 문제 해결 및 보안상의 이유로 업그레이드 및 구매에 대해 결정을 내리고 보증 상태를 추적해야 합니다. 정확한 자산 재고 목록을 유지하여 온디맨드 뷰 및 포괄적인 보고서를 제공하는 것이 비즈니스 필수 항목이 되고 있습니다. 게다가, 특정 규정 준수 법규에서는 포괄적인 자산 재고를 특히 요구하고 있습니다. 예를 들어, FISMA, SOX, PCI DSS 및 HIPAA 모두는 요구 사항 중 하나로 정확한 자산 재고를 의무화하고 있습니다. 그러나 여러 모듈이 연계되는 온프레미스 리소스의 특성상 현행화된 재고 목록을 유지하는 것이 매우 힘들거나 최악의 경우 불가능할 수 있습니다. 조직에서는 종종 타사 솔루션을 적용하여 자산 재고 목록을 자동화해야 하는 경우가 있습니다. 이런 경우에도 단일 콘솔에서 모든 유형의 자산에 대한 자세한 재고 현황을 보는 것이 항상 가능한 것은 아닙니다.

AWS를 사용하면 AWS IT 리소스의 정확한 재고 현황을 쉽고 빠르게 확인할 수 있는 많은 기능을 사용할 수 있습니다. 이러한 기능, 관련 '사용 방법' 안내 및 기능에 대한 자세한 설명에 대한 링크가 아래에 있습니다.

AWS 거버넌스 설정 기능	대규모로 보안 설정 방법
계정 활동 페이지	리전별로 각 서비스의 사용량을 세분화하여 보여줌으로써 IT 리소스 요약 목록을 제공합니다. 자세히 알아보기.
Amazon Glacier 아카이빙 데이터 재고	Glacier에 모든 IT 리소스를 표시함으로써 Glacier 데이터 재고를 제공합니다. 자세히 알아보기.
AWS CloudHSM	키 스토리지로 고객 전용 HSM을 제공함으로써 암호화 키에 대한 가상 및 물리적 제어를 제공합니다. 자세히 알아보기.
AWS Data Pipeline 작업 실행기	작업에 AWS Data Pipeline을 폴링한 다음, 해당 작업 상태를 수행 및 보고함으로써 자동화된 작업 처리를 제공합니다. 자세히 알아보기.
AWS Management Console	AWS에서 실행 중인 모든 IT 리소스를 서비스별로 표시함으로써 자산 및 데이터의 실시간 재고를 제공합니다. 자세히 알아보기.
AWS Storage Gateway API	인터페이스, 도구 및 스크립트가 리소스를 관리하도록 프로그래밍함으로써 자산 및 데이터를 프로그래밍 방식으로 재고 관리하는 기능을 제공합니다. 자세히 알아보기.

IT 비용 제어

IT 서비스 비용을 이해함으로써 가장 비용 절감적인 방법으로 리소스를 확보하여 IT 비용을 보다 잘 제어할 수 있습니다. 그러나 온프레미스에서 지출한 IT 리소스와 관련된 비용 및 ROI를 관리하고 추적하는 것은 꽤 복잡한 계산을 요하기 때문에, 어렵고 정확하지 않을 수 있습니다. 용량 계획, 사용 예측, 구매 비용, 감가 상각, 자본 비용, 시설 비용 등은 총 소유 비용을 계산하기 어렵게 하는 요소들 중 일부일 뿐입니다.

AWS를 사용하면 IT 리소스 비용을 쉽고 정확하게 이해하고 제어할 수 있는 많은 기능을 사용할 수 있습니다. AWS를 사용하면 동등한 온프레미스 배포에 비해 최대 80%의 비용을 절약할 수 있습니다[2]. 이러한 기능, 관련 '사용 방법' 안내 및 기능에 대한 자세한 설명에 대한 링크가 아래에 있습니다.

AWS 거버넌스 설정 기능	대규모로 보안 설정 방법
계정 활동 페이지	사용되는 리소스를 서비스별로 표시하여 IT 리소스 비용을 언제든지 볼 수 있습니다. 자세히 알아보기.
Amazon EC2 멱등성 인스턴스 시작	추가 인스턴스 시작으로 인한 제한 시간 초과나 연결 오류를 방지함으로써 리소스의 잘못된 시작 및 추가 비용 발생을 방지합니다. 자세히 알아보기.
Amazon EC2 리소스 태그 지정	리소스를 컴퓨팅하는 데 사용자 지정 검색 가능 레이블을 적용하여 리소스 비용과 비즈니스 단위가 연결되도록 합니다. 자세히 알아보기.
AWS 계정 결제	사용된 리소스 및 관련 실제 컴퓨팅 발생 비용을 세분화하여 표시함으로써 결제 정보를 모니터하고 비용을 지불하도록 돕는 사용이 편한 결제 기능을 제공합니다. 자세히 알아보기.
AWS Management Console	실제 비용 및 가동률을 포함하여 AWS에서 실행 중인 모든 IT 리소스를 서비스별로 표시함으로써 비용 요인에 대한 일원화된 보기를 제공합니다. 자세히 알아보기.
AWS 서비스 요금	각 AWS 제품 및 특정 요금 특성에 따른 요금을 제공하므로 AWS IT 리소스 요금을 완벽하게 인지할 수 있습니다. 자세히 알아보기.
AWS Trusted Advisor	사용하지 않는 유휴 리소스를 식별하여 IT 리소스 비용을 최적화하도록 돕습니다. 자세히 알아보기.
결제 경보	지불 활동에 대한 알림을 전송하여 IT 리소스 비용에 대한 사전 알림을 제공합니다. 자세히 알아보기.

[2] AWS를 사용하여 얻을 수 있는 전반적인 비용 절감에 대한 자세한 내용은 총 소유 비용 백서 참조

통합 결제	여러 AWS 계정을 하나의 계산서에 결합함으로써 비용 제어를 중앙화하고 계정 간 비용을 비교해 볼 수 있습니다. 자세히 알아보기.
종량 과금제	애플리케이션에 대한 수요가 증가할 때 여러 서버로 자동으로 규모를 조정하여 초기 구입 비용이나 지속적인 유지 관리 비용을 들이지 않고 종량 과금제로 몇 분만에 애플리케이션을 만드는 데 사용할 수 있는 컴퓨팅 리소스 및 서비스를 제공합니다. 자세히 알아보기.

IT 보안 관리

IT 리소스에 대한 물리적 액세스 제어

물리적 액세스 관리는 IT 거버넌스 프로그램의 핵심 구성 요소입니다. 물리적 보안의 전통적인 구성 요소를 대변하는 잠금 장치, 보안 경보, 출입 제어 및 감시 비디오 외에도 물리적 액세스를 통한 전자적 제어도 효과적인 물리적 보안에 있어 무엇보다 중요한 요소입니다. 전통적인 물리적 보안 산업은 빠르게 전환되고 있으며, 물리적 보안을 매우 복잡하게 만드는 것이 특화 분야로 떠오르고 있습니다. 온프레미스 물리적 보안 고려 사항 및 제어가 보다 더 복잡해지면서, 독보적으로 실력이 검증되고 특화된 IT 보안 전문가에 대한 수요가 증가하고 있습니다. 이들은 물리적 보안 관련 데이터를 호스팅하는 데 필요한 카드/카드 판독기, 컨트롤러 및 시스템 서버에 대한 액세스 자격 증명을 효과적으로 물리적 제어하는 데 필요한 엄청난 양의 업무를 관리할 수 있습니다.

AWS를 사용하면 물리적 환경을 안전하게 하는 데 필요한 기술, 실력 및 리소스를 보유한 AWS 전문가에게 AWS 인프라의 물리적 보안과 관련된 제어를 쉽고 효과적으로 아웃소싱할 수 있습니다. AWS는 여러 명의 다양하고 독립적인 감사자가 일년 내내 데이터 센터의 물리적 보안을 확인하여 AWS의 물리적 보안 제어 효과에 대한 세부 테스트 및 설계를 증명하도록 합니다. 아래에서 AWS 감사 프로그램 및 관련 물리적 보안 제어에 대해 자세히 알아보십시오.

AWS 거버넌스 설정 기능	대규모 보안 설정 방법
AWS SOC 1 물리적 액세스 제어	실시 중인 제어에 투명성을 제공하여 데이터 센터에 대한 무단 액세스를 방지합니다. 독립된 감사 기관에서 제어에 대해 제대로 된 설계, 테스트 및 감사를 진행합니다. 자세히 알아보기.
AWS SOC 2-보안 물리적 액세스 제어	실시 중인 제어에 투명성을 제공하여 데이터 센터에 대한 무단 액세스를 방지합니다. 독립된 감사 기관에서 제어에 대해 제대로 된 설계, 테스트 및 감사를 진행합니다. 자세히 알아보기.
AWS PCI DSS 물리적 액세스 제어	PCI DSS(Payment Card Industry Data Security Standard)와 관련하여 실시 중인 제어에 투명성을 제공하여 데이터 센터에 대한 무단 액세스를 방지합니다. 독립된 감사 기관에서 제어에 대해 제대로 된 설계, 테스트 및 감사를 진행합니다. 자세히 알아보기.

AWS ISO 27001 물리적 액세스 제어	ISO 27002 보안 모범 사례 표준과 관련하여 실시 중인 제어에 투명성을 제공하여 데이터 센터에 대한 무단 액세스를 방지합니다. 독립된 감사 기관에서 제어에 대해 제대로 된 설계, 테스트 및 감사를 진행합니다. 자세히 알아보기.
AWS FedRAMP 물리적 액세스 제어	NIST 800-53 모범 사례 표준과 관련하여 실시 중인 제어 및 프로세스에 투명성을 제공하여 데이터 센터에 대한 무단 액세스를 방지합니다. 독립된 정부 공인 감사 기관에서 제어에 대해 제대로 된 설계, 테스트 및 감사를 진행합니다. 자세히 알아보기.

IT 리소스에 대한 논리적 액세스 제어

IT 거버넌스의 주요 목표 중 하나는 컴퓨터 시스템 및 데이터에 대한 논리적 액세스를 효과적으로 관리하는 것입니다. 그러나 최소한의 권한 규칙 설정, 리소스에 대한 권한 관리, 역할 및 정보 요구 사항 관련 변경 사항 처리, 민감한 데이터 증가 등 논리적 액세스와 관련한 고려 사항 및 복잡성이 계속해서 커지고 변화하는 상황에서 많은 조직이 이에 맞게 온프레미스 솔루션 규모를 확장하는 데 어려움을 겪고 있습니다. 온프레미스 환경에서는 논리적 액세스를 관리할 때 발생하는 지속적인 핵심 문제로 인해 다음과 같은 요소를 기반으로 사용자에게 액세스를 제공합니다.

- 역할(예: 인터넷 사용자, 계약업체, 외부 사용자, 파트너 등)
- 데이터 분류(예: 기밀, 내부 전용, 프라이빗, 퍼블릭 등)
- 데이터 유형(예: 자격 증명, 개인 데이터, 연락처 정보, 업무 관련 데이터, 디지털 인증서, 인식 암호 등)

AWS의 다양한 제어 기능을 사용하면 최소 권한 부여 원칙을 기반으로 논리적 액세스를 효과적으로 관리할 수 있습니다. 이러한 기능, 관련 '사용 방법' 안내 및 기능에 대한 자세한 설명에 대한 링크가 아래에 있습니다.

AWS 거버넌스 설정 기능	대규모 보안 설정 방법
Amazon S3 ACL(액세스 제어 목록)	특정 조건을 추가하여 사용자가 AWS를 사용하는 방법을 제어(예: 시간대, 소스 IP 주소, SSL 사용 여부, Multi-Factor Authentication 디바이스 인증 여부)함으로써 중앙 집중 권한관리 및 제어 환경을 제공합니다. 자세히 알아보기(참조 1 및 참조 2).
Amazon S3 버킷 정책	HTTP referer 및 IP 주소와 같은 요청 기반 속성뿐만 아니라 계정을 기반으로 액세스를 제한할 수 있는 기능을 사용자에게 제공함으로써 버킷 및 객체에 대한 액세스를 관리하는 조건 규칙을 만들 수 있는 기능을 제공합니다. 자세히 알아보기.
Amazon S3 쿼리 문자열 인증	쿼리 문자열에 서명값을 포함하여 HTTP 요청에 임시 접근권한을 부여하는 방식을 통해, 인증이 필요한 리소스에 대한 HTTP 또는 브라우저 접근 권한을 임시로 허용하는 기능을 제공합니다. 자세히 알아보기.

AWS CloudTrail	API 또는 콘솔 작업의 로깅(예: 버킷 정책이 변경되는 경우 또는 인스턴스가 중단되는 경우 로깅)을 제공함으로써 고급 모니터링이 가능합니다. 자세히 알아보기.
AWS IAM Multi-Factor Authentication (MFA)	로그인하고 리소스에 액세스하는 데 토큰을 요구함으로써 모든 리소스에 MFA를 적용합니다. 자세히 알아보기.
AWS IAM 암호 정책	사용자가 IAM 사용자가 사용한 암호에 대해 암호가 특정 길이 및 문자 조합을 만족해야 하는 등 암호 정책을 설정할 수 있도록 허용함으로써 사용자의 암호에 대해 품질을 관리하고 제어할 수 있는 기능을 제공합니다. 자세히 알아보기.
AWS IAM 권한	사용자가 AWS 리소스에 액세스할 수 있는 사람 및 해당 리소스에서 수행할 수 있는 작업을 지정할 수 있도록 함으로써 권한을 쉽게 관리할 수 있는 기능을 제공합니다. 자세히 알아보기.
AWS IAM 정책	사용자가 AWS 계정 내에 여러 사용자를 만들고, 이들에게 보안 자격 증명을 할당하고, 권한을 관리하도록 허용함으로써 최소 권한 액세스를 세부적으로 관리할 수 있습니다. 자세히 알아보기.
AWS IAM 역할	사용자 및 서비스에 필요한 리소스에 액세스할 수 있는 권한 집합을 정의함으로써 일반적으로는 AWS 리소스에 액세스할 수 없는 사용자나 서비스에 일시적으로 액세스를 위임할 수 있는 기능을 제공합니다. 자세히 알아보기.
AWS Trusted Advisor	가능한 보안 및 권한 문제를 식별하고 에스컬레이션함으로써 자동화된 보안 관리 평가를 제공합니다. 자세히 알아보기.

IT 리소스 보호

IT 리소스를 보호하는 것은 IT 거버넌스 프로그램의 초석입니다. 그러나 온프레미스 환경에서는, 새로운 서버가 온라인 상태가 될 때 수행해야 하는 보안 단계가 너무 많습니다. 예를 들어, 방화벽 및 액세스 제어 정책을 업데이트해야 하며, 새로 생성된 서버 이미지의 보안 정책 준수 여부를 확인해야 하고, 모든 소프트웨어 패키지를 최신 상태로 유지해야 합니다. 설사 이러한 보안 작업이 자동화되어 있고 매우 역동적인 비즈니스 요구 사항을 만족할 수 있는 방법으로 제공된다 하더라도, 전통적인 거버넌스 접근법만을 고수하는 조직은 사용자가 보안 제어를 제대로 활용할 수 없거나, 비즈니스 지연으로 인한 비용이 발생하게 됩니다.

AWS는 쉽고 효과적으로 IT 리소스를 보호할 수 있는 다양한 보안 기능을 제공합니다. 이러한 기능, 관련 '사용 방법' 안내 및 기능에 대한 자세한 설명에 대한 링크가 아래에 있습니다.

AWS 거버넌스 설정 기능	대규모 보안 설정 방법
Amazon Linux AMI	모든 인스턴스 배포에서 사용할 수 있는 프라이빗 이미지를 개발함으로써 "골드"(강화된) 이미지를 지속적으로 배포할 수 있는 기능을 제공합니다. 자세히 알아보기.
Amazon EC2 전용 인스턴스	격리된 프라이빗 가상 네트워크를 제공하고, Amazon EC2 컴퓨팅 인스턴스가 하드웨어 수준에서 격리되고 VPC로 이러한 인스턴스를 시작하도록 보장합니다. 자세히 알아보기.
Amazon EC2 인스턴스 시작 마법사	인스턴스를 시작할 때 사용할 수 있는 머신 이미지에 대해 제한을 둠으로써 일관된 시작 프로세스를 가능하게 합니다. 자세히 알아보기.
Amazon EC2 보안 그룹	방화벽으로 동작하여 하나 이상의 인스턴스에 대한 트래픽을 제어함으로써 인바운드 및 아웃바운드 트래픽을 세부적으로 제어할 수 있습니다. 자세히 알아보기.
Amazon Glacier 아카이브	기본적으로 AES 256비트 암호화를 사용하여 데이터 아카이브 및 백업을 위한 안전하고 내구성 있는 스토리지의 저렴한 장기 스토리지 서비스를 제공합니다. 자세히 알아보기.
Amazon S3 클라이언트 측 암호화	객체 데이터를 Amazon S3에 업로드하기 전에 클라이언트 측에서 이를 암호화하는 고객 본인의 라이브러리를 활용함으로써 Amazon S3에 데이터를 전송하기 전에 데이터를 암호화할 수 있는 기능을 제공합니다. Java용 AWS SDK 또한 Amazon S3에 데이터를 업로드하기 전에 자동으로 이를 암호화할 수 있습니다. 자세히 알아보기.
Amazon S3 서버 측 암호화	Amazon S3 데이터에 AES 256비트 암호화를 사용함으로써 AWS가 관리하는 키 및 유휴 객체를 암호화합니다. 자세히 알아보기.
Amazon VPC	온프레미스에서 운영되는 기존 네트워크와 매우 유사한 가상 네트워크를 AWS의 확장 가능한 인프라 사용의 이점과 함께 제공합니다. 사용자가 논리적으로 격리된 AWS 섹션을 만들 수 있도록 허용합니다. 이 섹션에서 사용자는 자신이 정의한 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. 자세히 알아보기.
Amazon VPC 논리적 격리	머신 이미지가 다른 네트워크의 리소스와 격리되도록 허용함으로써 리소스를 가상으로 격리합니다. 자세히 알아보기.

Amazon VPC 네트워크 ACL	서브넷 수준에서 인바운드 및 아웃바운드 트래픽을 제어함으로써 연결된 서브넷에 대한 방화벽 유형의 격리를 제공합니다. 자세히 알아보기.
Amazon VPC 프라이빗 IP 주소	프라이빗 IP 주소의 트래픽을 퍼블릭 서브넷에 있는 NAT(Network Address Translation) 인스턴스를 통해 라우팅함으로써 인터넷 노출로부터 보호하도록 돕습니다. 자세히 알아보기.
Amazon VPC 보안 그룹	인스턴스 수준에서 인바운드 및 아웃바운드 트래픽을 제어함으로써 연결된 Amazon EC2 인스턴스에 대한 방화벽 유형의 격리를 제공합니다. 자세히 알아보기.
AWS CloudFormation 템플릿	인프라를 스크립트와 함께 프로비저닝함으로써 특정 머신 이미지를 다른 리소스 및 구성과 함께 일관되게 배포하는 기능을 제공합니다. 자세히 알아보기.
AWS Direct Connect	사용자의 자체 환경과 AWS 데이터 센터 간에 전용 네트워크 연결을 설정함으로써 AWS에 퍼블릭 인터넷을 연결할 필요가 없습니다. 자세히 알아보기.
온프레미스 하드웨어/소프트웨어 VPN 연결	기존 네트워크에서 AWS로의 보안 연결을 허용함으로써 네트워크 보안에 대한 세부적인 제어를 제공합니다. 자세히 알아보기.
가상 프라이빗 게이트웨이	사용자의 VPC에 하드웨어 VPN 연결을 만드는 방법을 제공함으로써 네트워크 보안을 세부적으로 제어합니다. 자세히 알아보기.

IT 리소스 로깅 관리

IT 보안의 핵심 요소 중 하나는 IT 리소스 로깅입니다. 로깅은 다양한 사용 사례에서 IT 거버넌스에 매우 중요합니다. 이 사용 사례에는 의심되는 동작 감지/추적, 법의학적 분석 지원, 규정 준수 요구 사항 충족, IT/네트워킹 유지 관리 및 운영 지원, IT 보안 비용 관리/절약, 서비스 수준 모니터링, 인터넷 비즈니스 절차 지원 등이 포함되며, 이 외에도 더 있습니다. 비용 관리, 서비스 수준 및 사업부별 애플리케이션 모니터링, 기타 IT 보안 및 규정 준수 중점 활동 등의 핵심 거버넌스 기능을 지원하기 위해 조직은 점차 효과적인 로그 관리에 눈을 돌리고 있습니다. SANS Log Management Survey를 보면, 조직들이 로그를 보다 지속적으로 활용할 방안을 찾고 있지만, 온프레미스 리소스를 사용하여 이러한 로그를 수집 및 분석하는 사용 사례를 만들지는 못하고 있다는 것을 알 수 있습니다. 다양한 IT 리소스로부터 보다 많은 로그 유형을 수집 및 분석하는 조직의 경우 기능을 검색, 연관 및 보고하는 것뿐만 아니라 아주 다양한 형식의 로그 데이터를 일반화하는 데 있어 많은 수작업으로 인한 간접비용을 부담하고 있습니다. 로그 관리는 매일 발생하는 수많은 작업에 대해 보안 모니터링, 규정 준수 및 효과적인 의사 결정을 하도록 해주는 중요한 기능입니다.

AWS를 사용하면 IT 리소스 사용을 효과적으로 로깅하고 추적할 수 있는 다양한 로깅 기능을 사용할 수 있습니다. 이러한 기능, 관련 '사용 방법' 안내 및 기능에 대한 자세한 설명에 대한 링크가 아래에 있습니다.

AWS 거버넌스 설정 기능	대규모 보안 설정 방법
Amazon CloudFront 액세스 로그	객체에 대한 최종 사용자 액세스 관련 정보가 있는 로그 파일을 제공합니다. 로그를 특정 Amazon S3 버킷에 직접 배포할 수 있습니다. 자세히 알아보기.
Amazon RDS 데이터베이스 로그	Amazon RDS DB 인스턴스에서 생성한 로그 파일 수를 모니터하는 방법을 제공합니다. 데이터베이스 구성이나 성능 문제를 진단, 문제 확인 및 해결하는 데 사용됩니다. 자세히 알아보기.
Amazon S3 객체 만료	정의한 시간 이후 객체를 제거하도록 예약하고, 해당 시점에 객체 파기 로그를 제공합니다. 자세히 알아보기.
Amazon S3 서버 액세스 로그	요청 유형, 요청을 만든 리소스, 요청 처리 날짜/시간과 같은 요청 세부 정보와 함께 액세스 요청 로그가 제공됩니다. 자세히 알아보기.
AWS CloudTrail	AWS Management Console 또는 API를 통해 수행한 보안 작업의 로그를 제공합니다. 자세히 알아보기.

IT 성능 관리

이벤트 모니터링 및 응답

IT 성능 관리 및 모니터링은 IT 거버넌스 프로그램 중 전략적으로 가장 중요한 부분 중 하나가 되었습니다. IT 모니터링은 거버넌스의 필수 요소로, 성능 및/또는 보안에 영향을 줄 수 있는 IT 문제를 방지, 감지 및 수정하도록 해줍니다. IT 성능 관리와 관련하여, 온프레미스 환경에서의 주요 거버넌스 문제는 사용자가 여러 모니터링 시스템으로 IT 리소스의 모든 계층을 관리하고 독점적 관리 도구를 혼합하여 사용한다는 것과 이러한 IT 프로세스로 인해 시스템이 복잡해져서 최선의 경우 응답 시간 지연을 초래하거나, 최악의 경우 IT 성능 모니터링 및 관리 유효성에 영향을 준다는 점입니다. 게다가, 보안 위협이 점점 복잡해지고 진보함에 따라 이벤트 모니터링 및 응답 기능 또한 새롭게 발생하는 위협에 대처할 수 있도록 지속적이고 빠르게 진화할 필요가 있습니다. 이에 따라 온프레미스 성능 관리는 인프라 조달, 확장성, 다양한 지역을 포괄하는 테스트 조건 시뮬레이션 기능 등 증가하는 문제에 지속적으로 직면하고 있습니다.

AWS를 사용하면 IT 리소스를 쉽고 효과적으로 모니터 및 관리할 수 있는 다양한 모니터링 기능을 사용할 수 있습니다. 이러한 기능, 관련 '사용 방법' 안내 및 기능에 대한 자세한 설명에 대한 링크가 아래에 있습니다.

AWS 거버넌스 설정 기능	대규모 보안 설정 방법
Amazon CloudWatch	인스턴스의 작동 동작을 살펴보고, 분석하고, 경보를 설정하는 데 사용할 수 있는 통계 데이터를 제공합니다. 이 측정치에는 CPU 사용률, 네트워크 트래픽, I/O 및 지연 시간 등이 포함됩니다. 자세히 알아보기.
Amazon CloudWatch 경보	이벤트에 대한 사용자 지정 측정치, 경보 및 알림을 제공함으로써 중요한 이벤트에 대해 지속적으로 경보를 울립니다. 자세히 알아보기.
Amazon EC2 인스턴스 상태	자동화된 테스트 결과를 요약하고 인스턴스에 대해 예약된 특정 활동에 대한 정보를 제공하는 인스턴스 상태 확인을 제공합니다. 확인 작업을 자동화하여 특정 문제가 인스턴스에 영향을 미치는지를 감지합니다. 자세히 알아보기.
Amazon 인시던트 관리 팀	1년 365일 24시간 상시 대기하는 관리 직원과 함께 지속적인 인시던트 감지, 모니터링 및 관리를 제공하여 특정 보안 이벤트를 감지, 진단 및 해결하도록 지원합니다. 자세히 알아보기.
Amazon S3 TCP 선택적 인정	대량의 패킷 손실 후 복구 시간을 개선하는 기능을 제공합니다. 자세히 알아보기.
Amazon Simple Notification Service	메시지를 구독 엔드포인트 및 클라이언트에게 전달하는 작업을 관리함으로써 중요한 이벤트에 대해 지속적으로 경보를 울립니다. 자세히 알아보기.
AWS Elastic Beanstalk	용량 프로비저닝, 로드 밸런싱, 자동 조정, 애플리케이션 상태 모니터링 등 애플리케이션 배포 세부 사항을 모니터링하는 기능을 제공합니다. 자세히 알아보기.
Elastic Load Balancing	활용된 인스턴스를 탐색하고 활용되지 않은 인스턴스에 트래픽을 다시 라우팅함으로써 여러 Amazon EC2 인스턴스 간 수신 애플리케이션 트래픽을 자동으로 분산하는 기능을 제공합니다. 자세히 알아보기.

복원성 확보

데이터 보호 및 재해 복구 계획은 모든 조직의 IT 거버넌스에서 최우선 구성 요소가 되어야 합니다. 재해 복구의 가치는 말할 것도 없이, 모든 조직에서는 이벤트나 재해 발생 이후 다시 가동 상태로 돌아가 실행할 수 있는 기능에 대해 관심이 많습니다. 그러나 IT 리소스 복원성과 관련해 거버넌스를 구현하는 것은 지루하고 시간 소모적일 뿐 아니라 비용이 많이 들고 복잡할 수 있습니다. 오늘날 조직은 계획하지 않은 가동 중지나 운영 방해 요소를 야기할 수 있는 수많은 이벤트에 직면해 있습니다. 이러한 이벤트는 기술적 문제(예: 바이러스, 데이터 손상, 사용자의 실수 등)나 자연 현상(예: 화재, 홍수, 전력 차단, 날씨 관련 사고 등)에 의해 발생할 수 있습니다. 따라서, 조직은 데이터가 지속적으로 증가함에 따라 온프레미스 장애 조치 사이트의 계획, 테스트 및 운영에 있어 비용과 복잡성이 증가하는 문제를 안고 있습니다.

이러한 문제가 대두되는 상황에서 클라우드 컴퓨팅 서버 가상화는 실용적이고 저렴하기까지 한 우수한 복원 프로그램을 가능하게 합니다. AWS를 사용하면 IT 리소스에 대한 복원성을 쉽고 효과적으로 확보할 수 있는 다양한 기능을 사용할 수 있습니다. 이러한 기능, 관련 '사용 방법' 안내 및 기능에 대한 자세한 설명에 대한 링크가 아래에 있습니다.

AWS 거버넌스 설정 기능	대규모 보안 설정 방법
Amazon EBS 스냅샷	고가용성 및 고안정성의 예측 가능한 스토리지 볼륨을 서버 데이터의 증분 시점 백업 제어와 함께 제공합니다. 자세히 알아보기.
Amazon RDS 다중 AZ 배포	자동화된 가용성 제어, 동일 복원성 아키텍처를 사용하여 이벤트 발생 시 데이터를 보호하는 기능을 제공합니다. 자세히 알아보기.
AWS Import/Export	Amazon의 고속 내부 네트워크를 사용하는 Import / Export 서비스를 통해 광대한 양의 데이터를 로컬로 이동하는 기능을 제공합니다. 자세히 알아보기.
AWS Storage Gateway	게이트웨이가 EBS 스냅샷의 형태로 지정된 스케쥴에 따라 S3에 저장하는 방식으로 온프래미스 IT 환경과 AWS 스토리지 인프라 간에 원활하고 안전한 통합을 제공합니다. 자세히 알아보기.
AWS Trusted Advisor	AWS는 고객들에게 애플리케이션의 가용성 및 중복성을 증가시키는 다양한 옵션을 선택할 수 있도록 함으로써 자동화된 성능 관리 및 가용성을 제공합니다. 자세히 알아보기.
광대한 타사 솔루션	고객들은 AWS 마켓 플레이스에서 많은 데이터 저장 보안 툴이나 가용성 자동화 툴을 선택할 수 있습니다. 자세히 알아보기.
관리형 AWS No SQL/SQL 데이터베이스 서비스	데이터 항목을 리전의 여러 가용 영역에 걸쳐 자동 복제하여 확실한 고가용성과 데이터 내구성을 가진 안전하고 내구성이 뛰어난 데이터 스토리지를 제공합니다. 자세히 알아보기: • Amazon Dynamo DB • Amazon RDS

다중 리전 배포	전력망, 단층선 등 컴퓨팅 위치에 지리적 다양성을 제공하여 다양한 위치를 지원합니다. 자세히 알아보기.
Route 53 상태 확인 및 DNS 장애 조치	사용자가 액티브-액티브, 액티브-패시브 및 혼합 구성에서 DNS 장애 조치를 구성할 수 있도록 함으로써 저장된 백업 데이터의 가용성을 모니터링하여 애플리케이션 가용성을 개선합니다. 자세히 알아보기.

서비스-거버넌스 기능 인덱스

앞에서는 거버넌스 도메인별로 내용을 설명하였습니다. 참조를 위해 아래 표에서는 주요 AWS 서비스별로 거버넌스 기능을 간단히 설명합니다.

AWS 서비스	거버넌스 기능
Amazon EC2	Amazon EC2 멱등성 인스턴스 시작 Amazon EC2 리소스 태그 지정 Amazon Linux AMI Amazon EC2 전용 인스턴스 Amazon EC2 인스턴스 시작 마법사 Amazon EC2 보안 그룹
Elastic Load Balancing	Elastic Load Balancing 트래픽 배포
Amazon VPC	Amazon VPC Amazon VPC 논리적 격리 Amazon VPC 네트워크 ACL Amazon VPC 프라이빗 IP 주소 Amazon VPC 보안 그룹 온프레미스 하드웨어/소프트웨어 VPN 연결
Amazon Route 53	Amazon Route 53 지연 시간 리소스 레코드 세트 Route 53 상태 확인 및 DNS 장애 조치
AWS Direct Connect	AWS Direct Connect

Amazon S3	Amazon S3 ACL(액세스 제어 목록) Amazon S3 버킷 정책 Amazon S3 쿼리 문자열 인증 Amazon S3 클라이언트 측 암호화 Amazon S3 서버 측 암호화 Amazon S3 객체 만료 Amazon S3 서버 액세스 로그 Amazon S3 TCP 선택적 인정 Amazon S3 TCP 윈도우 조정
Amazon Glacier	Amazon Glacier 볼트 재고 Amazon Glacier 아카이브
Amazon EBS	Amazon EBS 스냅샷
AWS Import/Export	AWS Import/Export 대량 작업
AWS Storage Gateway	AWS Storage Gateway 통합 AWS Storage Gateway API
Amazon CloudFront	Amazon CloudFront Amazon CloudFront 액세스 로그
Amazon RDS	Amazon RDS 데이터베이스 로그 Amazon RDS 다중 AZ 배포 관리형 AWS 비SQL/SQL 데이터베이스 서비스
Amazon Dynamo DB	관리형 AWS 비SQL/SQL 데이터베이스 서비스

AWS Management Console	계정 활동 페이지 AWS 계정 결제 AWS 서비스 요금 AWS Trusted Advisor 결제 경보 통합 결제 종량 과금제 AWS CloudTrail Amazon 인시던트 관리 팀 Amazon Simple Notification Service 다중 리전 배포
AWS Identity and Access Management(IAM)	AWS IAM Multi-Factor Authentication (MFA) AWS IAM 암호 정책 AWS IAM 권한 AWS IAM 정책 AWS IAM 역할
Amazon CloudWatch	AWS CloudWatch 대시보드 Amazon CloudWatch 경보
AWS Elastic Beanstalk	AWS Elastic Beanstalk 모니터링
AWS CloudFormation	AWS CloudFormation 템플릿
AWS Data Pipeline	AWS Data Pipeline 작업 실행기

AWS CloudHSM	CloudHSM 키 스토리지
AWS Marketplace	광대한 타사 솔루션
데이터 센터	AWS SOC 1 물리적 액세스 제어 AWS SOC 2-보안 물리적 액세스 제어 AWS PCI DSS 물리적 액세스 제어 AWS ISO 27001 물리적 액세스 제어 AWS FedRAMP 물리적 액세스 제어

결론

IT 거버넌스의 주요 초점은 비즈니스 목표와 전략적으로 동일하게 가치를 전달하기 위해 리소스, 보안 및 성능을 관리하는 데 있습니다. 성장률과 기술 복잡성의 증가를 놓고 봤을 때, 온프레미스 환경에서 저렴한 비용으로 우수한 IT 거버넌스를 전달하는 데 필요한 기능 및 제어를 세부적으로 제공하기를 바라기는 힘듭니다. 동일한 이유로 클라우드상의 인프라를 구축할 때도 온프레미스 구축대비, 클라우드 기반 거버넌스가 보다 높은 수준의 관리 및 자동화를 제공하기 때문에 더 낮은 초기 비용, 더 쉬운 작업, 개선된 민첩성 등의 이점을 제공하며 이로 인해 조직이 자체 비즈니스에 집중할 수 있게 됩니다.

참조 자료

AWS로 할 수 있는 작업은 무엇입니까? http://aws.amazon.com/solutions/aws-solutions/.

AWS를 사용하려 하는데 처음에 어떻게 시작해야 합니까?
http://docs.aws.amazon.com/gettingstarted/latest/awsgsg-intro/gsg-aws-intro.html