액센추어의 AWS 보안 프레임워크

싱가포르 통화청(Monetary Authority of Singapore) 지침

accenture

목차

1 개요 4

2 액센추어의 AWS 보안 프레임워크의 지도원리 5

2.1 AWS 공유 책임 모델 6

3 액센추어의 AWS 보안 프레임워크 개관 7

3.1 분리 및 네트워크 흐름 제어 7

3.2 데이터 보호 및 액세스 관리 8

3.3 감사 및 구성 관리 9

4 제어 프레임워크 개요 10

5 싱가포르 통화청 지침 관련 싱가포르 은행연합회의 주요 제어 준수 12

5.1 암호화 및 토큰화 13

5.1.1 이동 중 데이터의 보호 13

5.1.2 저장 데이터의 보호 14

5.1.4 토큰화 15

5.1.5 키 관리 15

5.2 전용 장비 또는 사설 클라우드 16

5.2.1 인스턴스 격리 16

5.2.2 데이터 위치 16

5.2.3 AWS 계정의 분리 16

5.2.4 Amazon VPC 17

5.2.5 보안 그룹 20

5.2.6 보안 제어 모니터링 21

5.3 변경 관리 및 사용자 접근 권한 관리(PUAM) 22

5.4 가상 환경 보안 23

5.4.1 사용자 및 그룹 24

5.4.2 역할 기반 액세스 24

5.4.3 ID 연계 25

5.4.4 임시 보안 자격증명 25

5.4.5 사용자 작업 감사 26

5.5 협력적 재해 복구 테스트 27

5.5.1 중요 작업의 재해 복구 테스트 27

5.5.2 비중요 작업의 재해 복구 테스트 27

5.5.3 중요 작업에 대한 재해 복구 아키텍처 27

5.5.4 비중요 작업에 대한 재해 복구 아키텍처 28

5.6 보안 이벤트 모니터링 및 사고 관리 29
5.6.1 사고 관리 30
5.7 침투 테스트 및 취약성 관리 31
5.7.1 침투 테스트 31
5.7.2 패치 관리 31
5.7.3 자동 AMI 생성 프로세스 31
5.8 관리자 원격 액세스 32
5.9 안전한 소프트웨어 개발 라이프사이클 및 코드 검토 33
5.9.1 보안 테스트 33
5.9.2 프로덕션 데이터의 분리 34
5.9.3 역할 기반 액세스 제어(RBAC) 34
5.9.4 버전 제어 34
5.10 보안 로그 및 백업 35
6 결론 36
6.1 도움을 주신 분들 36

1 개요

싱가포르 통화청(Monetary Authority of Singapore: MAS)은 공용 클라우드의 활용을 지지합니다! 아웃소싱 지침을 인용하자면, "싱가포르 통화청은 (…) 기관들이 (클라우드 서비스)를 활용함으로써 사업 운영과 서비스 효율성을 개선하는 한편 클라우드 서비스의 확장가능하고 표준화되며 보안을 갖춘 인프라 혜택을 누릴 수 있다는 점을 인식하고 있습니다"[1]. 또한 싱가포르 통화청은 금융서비스기관들이 더 이상 클라우드 서비스 이용에 앞서 이를 신고하거나 싱가포르 통화청의 승인을 얻을 필요가 없다는 점을 공표하였습니다[2]. 다만, 금융서비스기관은 여전히 "아웃소싱의 위험성과 중요성에 상응하는" 정도의 실사와 위험평가를 수행하고 특정 계약 조항을 유지하여야 하며, 그 이후에야 독자적인 판단에 따라 AWS 를 이용할 수 있습니다. 논의의 주제는 "클라우드 서비스 이용이 가능한지, 클라우드가 안전한지"에서 "어디서부터 시작해야 하는지, 적법한 솔루션을 만들기 위해서 AWS 가 제공하는 제어를 어떻게 이용해야 하는지"로 나아갔습니다.

"액센추어의 AWS 보안 프레임워크"는 금융서비스기관들이 새로운 싱가포르 통화청의 지침을 준수하면서 AWS 서비스를 도입 및 이용하는 방식에 관한 메커니즘을 제공합니다. 보안 제어를 고안하기 위하여 사용된 방법론은 AWS 클라우드 도입 프레임워크(AWS Cloud Adoption Framework) 전반과 밀접하게 연관됩니다. 클라우드 도입 프레임워크는 클라우드 기반 IT 시스템 시행에 관련된 수많은 요소들로 이루어진 각각의 구조들을 조직화 하는지침을 제공합니다.

액센추어의 AWS 보안 프레임워크는 금융기관에게 싱가포르 통화청 및 싱가포르 은행연합회(Association of Banks in Singapore: ABS)의 요건을 준수하면서 철저한 보안 환경을 유지할 수 있는 총체적 프레임워크를 제공합니다. 본 프레임워크는 AWS 플랫폼 상의 중요 작업 및 비중요 작업 모두의 보안을 유지함과 동시에 클라우드의 유연성, 민첩성, 비용절감 효과를 활용합니다.

그림 1: AWS 클라우드 도입 프레임워크

본 문서는 액센추어의 AWS 보안 프레임워크를 정의하는 주요 애플리케이션 빌딩 블록들(building blocks)을 설명하기 위하여 액센추어 보안요원(Accenture Security)과 AWS 클라우드 아키텍트(Cloud Architects for AWS)의 지식, 전문성 및 경험을 수렴하였습니다. 본 프레임워크는 싱가포르 통화청이 명시하는 규제 요건을 충족하기 위하여 빌딩 블록들을 싱가포르 은행연합회가 추천하는 주요 구성요소 제어와 연결시키는 최상의 방법에 관한 총제적 문서입니다.

---

[1] http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/Outsourcing%20Guidelines_Jul%202016.pdf

[2] http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/MAS-Issues-New-Guidelines-on-Outsourcing-Risk-Management.aspx

2 액센추어의 AWS 보안 프레임워크의 지도원리

우선, 본 프레임워크는 가능한 경우 AWS 보안 우수 사례 백서(AWS Security Best Practice Whitepaper)[3]에 명시된 AWS 고유의 보안 서비스 및 우수 사례를 활용하고자 합니다. 이는 AWS 플랫폼의 정신에 따라 민첩성과 투자수익성에 주안점을 두는 통합적 보안 서비스를 보장하기 위함입니다.

본 프레임워크의 기본적인 원칙은 비중요 데이터 관리에 대해서는 AWS 서비스와 함께 애자일(agile) 개발 방법론을 활용하고, 동시에 각자의 환경에서 익숙한 단단하게 결합된 제어 메커니즘을 제공하는 보안 제어를 이용함으로써 금융서비스기관에게 AWS 에서 중요 데이터를 관리할 수 있다는 신뢰를 제공하는 것입니다.

따라서 본 프레임워크는 중요 업무에 대해서는 전통적인 IT 보안 모델을 따르는 클라우드 기반 환경을 만들며, 이는 현재 기업 조직에 존재하는 기존의 도구와 프로세스를 활용합니다. 금융서비스기관은 AWS 플랫폼을 이용함으로써 기존의 투자를 활용하면서도, 효과적인 클라우드 기반의 보안 접근법을 구축할 수 있습니다.

비중요 데이터 관리에 관한 애자일 방법론은 클라우드 내 보안에 관한 사고방식에 새로운 접근법을 제시합니다. AWS 플랫폼은 보안 위협에 대한 대처에 있어 특히 강점을 가지나, 이러한 강점을 온전히 활용하기 위해서는 IT 보안에 관한 사고방식을 바꾸어야 합니다. 이러한 사고방식의 변화는 비중요 데이터 관리에 관한 지배적인 지도원리가 될 것입니다. 방어에서 공격으로 이전하고, 보안 위협의 필연성을 수용하며, 위협에 따른 결과에 최선으로 맞서기 위한 플랫폼과 프로세스를 확립하여야 합니다. 목표는 보안에 관한 사고방식을 하나의 문화로서 달성 및 교육함으로써 더욱 복원성 있고 안정적이며 보안된 시스템을 이끌어내는 것입니다.

비중요 데이터 보안에 관한 본 프레임워크의 지도원리는 소프트웨어 개발 및 배포 주기 동안 "코드로서의 인프라(infrastructure as code)"의 관리방법에 주목합니다. 애플리케이션 및 인프라 개발과 구성에 관한 변경사항은 템플릿에 입력되고, 기존 환경에 변경사항을 반영하는 것이 아닌 완전히 새로운 환경이 구축됩니다. 신속하게 새로운 환경을 구축하고 기존 환경을 제거함에 따라 기존의 환경과 관련된 문제점과 보안 이슈, 예컨대 기록되지 않은 구성과 손상된 호스트를 이용하여 공격자가 환경 내에서 장기적으로 기반을 확보하는 등의 문제를 제거합니다. 더욱이, 플랫폼을 "하이드레이팅(hydrating)"함으로써 코드 업데이트 및 구성 변동을 올바른 위치에 저장하도록 하며 기존의 보안 방법으로는 감지될 수 없었던 손상된 호스트를 제거합니다. 이러한 접근법은 복원성, 재해 복구, 백업 등을 수행할 수 있는 새로운 방법을 가능케 합니다. 사업자들의 부담은 각각의 서버 및 그 고유의 콘텐츠에서 개별 애플리케이션 환경의 각 반복(iteration)의 연속성에 핵심이 되는 환경 템플릿, 애플리케이션 소스코드, 데이터베이스 등 보다 전략적인 콘텐츠로 옮겨가게 됩니다.

[3] https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

2.1 AWS 공유 책임 모델[4]

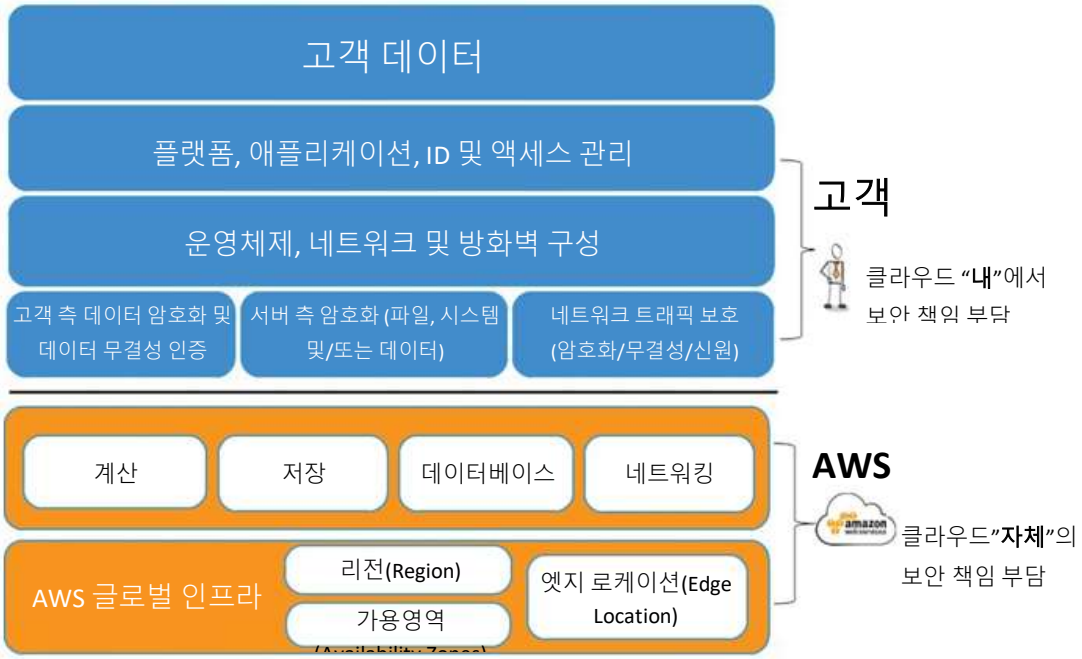

그림 2: AWS 공유 책임 모델

AWS 공유 책임 모델은 액센추어의 AWS 보안 프레임워크의 근간을 이룹니다. 공유 책임 모델 하에서, AWS 는 서비스가 가상화 단계에서부터 서비스가 운영되는 설비의 물리적 보안에 이르는 구성요소를 운영, 관리 및 제어합니다. 결국, 서비스 제공자는 직접적인 관리 하에 있는 구성요소에 대한 책임을 부담합니다. 그 예로는 호스트 운영체제(업데이트 및 보안 패치 포함), 호스트 상에서 운영하는 모든 애플리케이션 소프트웨어, 네트워크의 구성(보안그룹 방화벽, ID 및 액세스 관리, 로그 및 모니터링 등 AWS 가 제공하는 제어 기능의 구성 등) 등이 있습니다.

[4] https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

3 액센추어의 AWS 보안 프레임워크 개관

액센추어의 AWS 보안 프레임워크는 계층화된 보안 접근법을 적용함으로써 특정 작업에 필요한 보안 요소를 구축합니다.

3.1 분리 및 네트워크 흐름 제어

민감 데이터를 격리하기 위하여, 액센추어의 AWS 보안 프레임워크 내에서 다음과 같은 분리 및 네트워크 흐름 제어를 사용합니다:

그림 3: 네트워크 흐름 제어

- ✓ AWS 계정[5]은 다른 계정과 분리되어 AWS 리소스를 보관합니다. 각 계정은 고유의 사용자, 그룹 및 AWS ID 및 액세스 관리(IAM) 서비스에 의해 뒷받침되는 역할을 가지게 됩니다.
- ✓ Amazon 가상 사설 클라우드(Amazon Virtual Private Cloud: VPC)[6]는 AWS 플랫폼 상의 다른 가상 네트워크와 논리적 분리를 제공하는 AWS 계정의 전용 가상 네트워크입니다.
- ✓ 서브넷은 VPC 내에서 추가적인 네트워크 분리를 가능케 하며 보안그룹은 서브넷 내부에서 호스팅되는 EC2 인스턴스 상의 트래픽 흐름을 제어하는 데 사용됩니다.
- ✓ VPC 피어링은 상이한 VPC 간의 연결을 허용하기 위하여 사용됩니다.
- ✓ 초기설정 VPC 를 제외하고, VPC 는 인터넷 게이트웨이를 부착함으로써 명시적으로 연결을 생성하지 않는 한 외부 연결이 차단됩니다.
- ✓ AWS 직접연결(Direct Connect)은 고객의 데이터센터를 AWS 플랫폼에 연결하는 데 사용됩니다.
- ✓ 라우팅 케이블은 서브넷, VPC 및 인터넷 간의 트래픽 흐름을 허용하기 위하여 사용됩니다. 서브넷은 외부 연결을 허용하지 않는 것을 초기설정으로 합니다. 라우팅은 라우팅 케이블 내에서 명시적으로 정의되어야 합니다.
- ✓ 보안 그룹은 컴퓨트 인스턴스, 서브넷 및 VPC 간의 트래픽을 제어하기 위하여 사용되는 가상의 방화벽입니다.

[5] https://aws.amazon.com/account/

[6] https://aws.amazon.com/vpc/

3.2 데이터 보호 및 액세스 관리

데이터 보호 및 액세스 관리를 위하여 다음과 같은 제어가 사용됩니다:

그림 4: 데이터 보호 및 액세스 관리 제어

- ✓ 역할 기반 액세스 제어는 AWS 서비스에 대한 액세스를 제어하고 응용 프로그램 인터페이스(Application Programming Interface: API)에 대한 무단 접근을 방지합니다.
- ✓ 키 관리는 암호화 키의 주기를 키를 사용하는 서비스로부터 분리하여 생성, 저장 및 관리하기 위하여 사용됩니다.
- ✓ 인증 및 액세스 제어는 권한있는 사용자의 ID 를 확인하고 이들이 권한있는 서비스에만 액세스하도록 합니다.
- ✓ 암호화 및 토큰화는 민감한 데이터의 기밀성과 무결성을 보장하기 위하여 사용됩니다.
- ✓ 암호화 저장 볼륨은 전체 드라이브를 암호화함으로써 저장 데이터(data at rest)를 보호하기 위하여 사용됩니다.
- ✓ 전송 중 암호화는 시스템 간에 이동하는 데이터를 보호하기 위하여 사용됩니다.

3.3 감사 및 구성 관리

감사 및 구성 관리를 지원하기 위하여 다음과 같은 제어가 사용됩니다:

그림 5: 감사 및 구성 관리 제어

- ✓ 인프라, 운영체제 및 애플리케이션 로그를 캡처 및 저장합니다.
- ✓ 지표(metrics)를 정의하고 모니터링하여 보안 이슈 및 위반을 확인합니다.
- ✓ 경고 및 알림을 정의하고, 대응절차를 정의 및 테스트합니다.
- ✓ 구성 및 변동 관리 절차는 중요 업무에 대한 엄격한 ITIL 준수에서부터 비중요 업무에 대한 좀 더 유연한 변동 관리 지침에 이르기까지 특정 환경에 맞추어져서 빠른 혁신을 가능하게 합니다.
- ✓ 지속적 배포는 애플리케이션에 신속하게 작은 업데이트들을 하는 애자일(agile) 개발에 사용되어 테스트를 간소화합니다.
- ✓ 하이드레이션(hydration)은 개발이 반복될 때마다 템플릿으로부터 완전히 새로운 환경을 이용하는 것입니다. 이것은 정기적으로 완전한 정리 및 재구축 과정을 거치기 때문에, 위협 요소가 환경 내에서 장기적으로 기반을 확보할 가능성을 줄여줍니다.

4 제어 프레임워크 개요

아래 표는 싱가포르 통화청 지침(MAS)에 서술된 싱가포르 은행연합회(ABS)의 주요 제어를 이에 대응하여 해당 제어를 다루기 위하여 사용되는 액센추어 보안 프레임워크 및 AWS 서비스와 비교하여 요약 설명한 것입니다.

MAS 지침을 충족하기 위하여 정의된 ABS 주요 제어	액센추어의 AWS 보안 프레임워크 요소	AWS 서비스	제 3 자
암호화 및 토큰화	**데이터 보호 및 액세스 관리** ▪ 암호화 및 토큰화 ▪ 키 외부화 ▪ 전송 중 암호화	AWS Certificate Manager EBS Full Disk Encryption S3 Encryption AWS Key Management Service	Native DN TDE CipherCloud Cloud HSM
전용 장비 또는 사설 클라우드	**흐름 제어** ▪ 계정, 가용 영역 ▪ VPC, 서브넷, 게이트웨이, 라우팅 케이블 ▪ FW 및 보안 그룹	Amazon VPC Availability Zones AWS IAM Internet Gateway VPC Route Tables and Subnets AWS Config Security Groups and Network ACLs	
변동 관리 및 사용자 액세스 관리	**감사 및 구성 관리** ▪ 로그 캡쳐 ▪ 구성 및 변동 관리	Amazon CloudWatch AWS CloudTrail AWS Config	CyberArk PUAM
가상화 환경	**감사 및 구성 관리** ▪ 구성 및 변동 관리 ▪ 지속적 배포	Amazon Amazon Machine Image(AMI) AWS Inspector	QualysGuard
사용자 액세스 관리 및 업무 분리	**데이터 보호 및 액세스 관리** ▪ 역할 기반 액세스 제어 ▪ 인증 및 액세스 제어 **플로우 제어** ▪ 계정 **감사 및 구성 관리** ▪ 조작방지 로그 및 플로우 캡쳐	AWS IAM Amazon CloudWatch AWS 계정	Ping Federate MS Active Directory Splunk
협력적 재해 복구 테스트	**데이터 보호 및 액세스 관리** ▪ 역할 기반 액세스 **플로우 제어** ▪ VPC **감사 및 구성 관리**	Amazon EBS Snapshot RDS Snapshot AmazonS3 Amazon RDS Amazon ELB AWS CloudFormation AWS	CommVault GitHub

MAS 지침을 충족하기 위하여 정의된 ABS 주요 제어	액센추어의 AWS 보안 프레임워크 요소	AWS 서비스	제 3 자
	▪ 변동 관리 ▪ 지속적 배포 ▪ 하이드레이션	CodeCommitRepository AWS CodeDeploy	
보안사고 모니터링 및 사고 관리	**감사 및 구성 관리** ▪ 조작방지 로그 및 플로우 캡쳐 ▪ 조치 및 경고 ▪ 지속적 배포 ▪ 하이드레이션	AWS IAM Amazon CloudWatch AWS CloudTrail AWS 계정 AWS CodeDeploy	Splunk
침투 테스트 및 취약성 관리	**감사 및 구성 관리** ▪ 변동 관리 ▪ 지속적 배포	AMI AWS CodeCommitRepository AWS CodeDeploy	QualysGuard
관리자 원격 액세스	**플로우 제어** ▪ 계정 **데이터 보호 및 액세스 관리** ▪ 역할 기반 액세스 제어	AWS IAM AWS DirectConnect	Active Directory Ping Federate
보안 소프트웨어 배포 주기 및 코드 검토	**감사 및 구성 관리** ▪ 변동 관리 ▪ 지속적 배포 ▪ 하이드레이션	AMI AWS CloudFormation AWS CodeCommitRepository AWS CodeDeploy	GitHub
로그 및 백업 확보	**감사 및 구성 관리** ▪ 조작방지 로그 및 플로우 캡쳐	AmazonS3 EBS Snapshot AWS CloudTrail AWS Config	Splunk

표 1: 싱가포르 은행연합회의 주요 제어 도식화

5 싱가포르 통화청 지침 관련 싱가포르 은행연합회의 주요 제어 준수

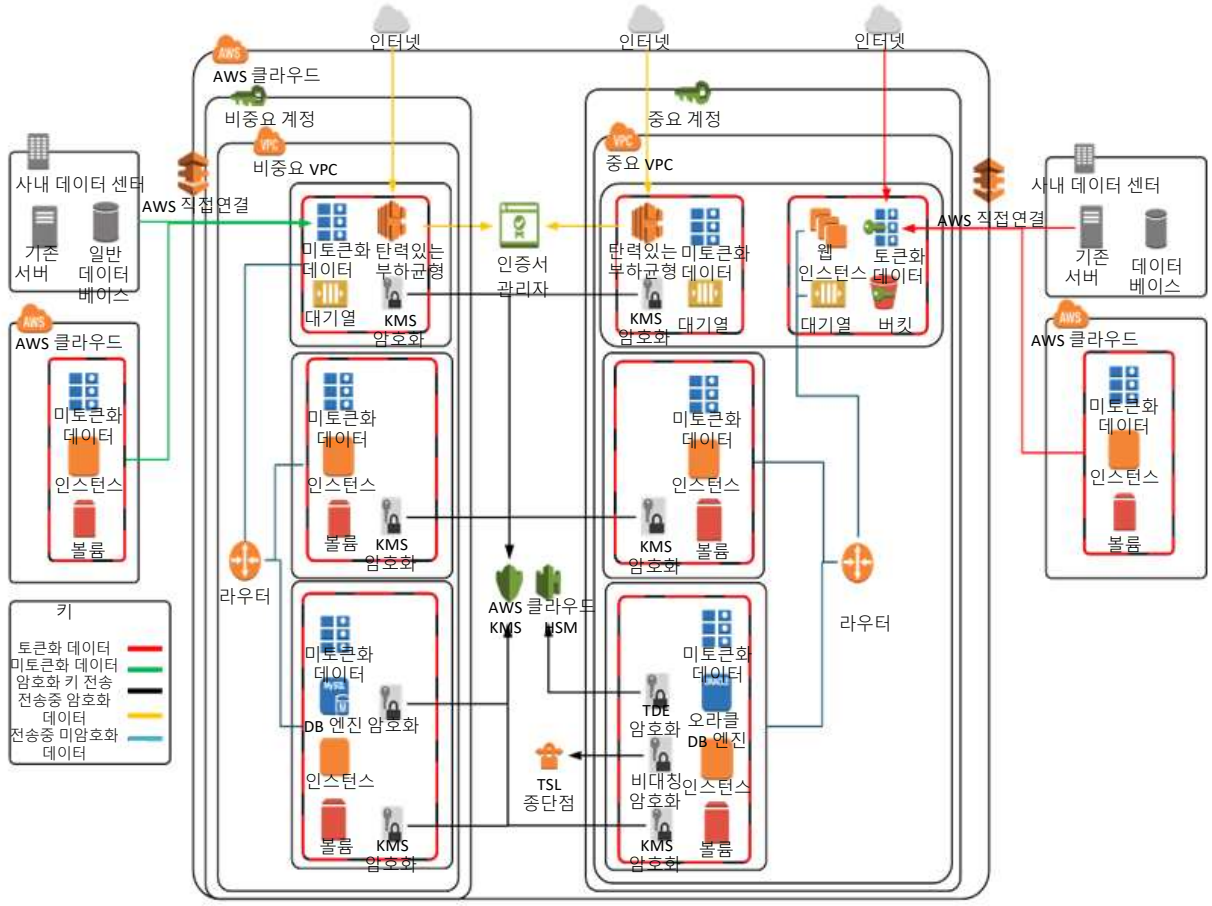

그림 6: 암호화 및 토큰화 플로우

싱가포르 은행연합회는 싱가포르 통화청 지침과 관련하여 클라우드 아웃소싱 시 10 가지 주요 제어를 권장합니다. 이하에서는 액센추어의 AWS 금융보안 프레임워크가 AWS 및 제 3 자의 기능 및 제품을 이용하여 해당 제어를 충족하는 방식을 설명합니다.

5.1 암호화 및 토큰화

액센추어의 AWS 보안 프레임워크는 중요 및 비중요 데이터 모두의 암호화와 비공개 개인정보, 카드소유자 정보와 같은 중요 데이터의 토큰화를 매우 중시합니다. 본 장에서는 암호화 및 토큰화와 관련된 3 가지 주요 분야에 초점을 맞추어 설명하겠습니다.

- 이동 중 데이터의 보호
- 저장 데이터의 보호
- 키 관리

5.1.1 이동 중 데이터의 보호

액센추어의 AWS 보안 프레임워크는 AWS 계정 및 서비스를 관리하기 위하여 웹 콘솔, AWS 명령어 인터페이스(Command Line Interface: CLI), API 엔드포인트(endpoints) 등 3 가지 선택지를 제공합니다. 이 선택지들은 모두 초기설정값으로 HTTPS 에 대한 보안 연결을 강화합니다.

AWS 는 오로지 보안 암호 및 프로토콜만을 지원하도록 모든 액세스 방법을 설정함으로써 메시지 도청, 조작 또는 위조를 방지합니다. 그 예외는 S3 로, IAM 및/또는 프레임워크가 지원하는 버킷 정책을 통해 실행할 수 있습니다.

액센추어의 AWS 보안 프레임워크는 AWS 인증서 관리자[7]를 활용하여 인터넷에서 접속하는 웹사이트에 대한 TLS/SSL 인증서를 자동으로 제공 및 갱신함으로써 인증서의 주기를 제공, 갱신 및 관리하는 업무를 자동화합니다.

웹, 애플리케이션, 데이터베이스 서버 등 구성요소 간 네트워크 연결 역시 엔드투엔드(end-to-end) 암호화를 사용하도록 설정되어 민감한 데이터의 기밀성과 무결성을 확보합니다.

[7] https://aws.amazon.com/certificate-manager/

5.1.2 저장 데이터의 보호

저장 데이터의 보호에는 Amazon EBS 볼륨의 암호화, 데이터베이스의 투명한 암호화, 데이터베이스 필드(field) 계층 암호화 및 토큰화 등 몇 가지 메커니즘을 포함합니다.

액센추어의 AWS 보안 프레임워크는 중요 및 비중요 데이터 모두에 있어 Amazon EC2(Elastic Compute Cloud)[8] 및 Amazon EBS(Elastic Block Store)[9]의 전체 디스크 암호화 볼륨을 활용합니다. EBS 는 AWS 키 관리 서비스(AWS Key Management Service)[10]에서 자동으로 관리되는 키들로써 볼륨을 암호화합니다. EBS 암호화[11]는 IOPS 성능에 영향을 미치지 않고, 액세스 지연에는 최소한의 영향만 주며, 추가 비용을 초래하지 않기 때문에 AWS 상 보안 관리에 있어 필수적입니다.

또한, 액센추어의 AWS 보안 프레임워크는 Amazon S3(Simple Storage Service)[12]의 서버 측 암호화를 통해 서비스에 업로드되는 파일을 자동으로 암호화 할 수 있도록 합니다. 중요 데이터의 경우 금융서비스기관 고객들이 제공하는 모든 키는 AWS CloudHSM 솔루션을 활용하고, 비중요 데이터의 경우 AWS 가 제공하는 키를 활용합니다. 이러한 비중요 데이터용 키는 AWS 가 관리하는 키 주기를 가짐으로써 더욱 민첩한 서비스 관리 접근법을 구현합니다. AWS KMS 는 AWS 플랫폼과 API 에 완전히 통합되어 비중요 작업에 대하여 간결하고 민첩한 원칙을 적용할 수 있도록 해줍니다.

중요 정보의 경우, 액센추어의 AWS 보안 프레임워크는 투명한 데이터베이스 암호화(Transparent Database Encryption: TDE) 및/또는 필드 레벨 암호화를 활용합니다. TDE 는 데이터를 디스크에 쓰여진 그대로 투명하게 암호화하여 응용 계층에서의 변경을 요하지 않습니다. TDE 데이터베이스 암호화 키는 관리된 서비스 제공자가 제어하는 키 관리 인프라 및 HSM 을 통해 관리됨으로써 플랫폼과 키를 관리하는 AWS 의 공유 책임을 둘러싼 모든 우려사항(그 정당성 여부를 불문하고)을 제거합니다.

필드 레벨 암호화는 필드가 데이터베이스에 쓰여지기 전에 또는 쓰여질 때 필드를 암호화하는 응용 계층 방법입니다. 필드 레벨 암호화를 적용하기 위해서는 애플리케이션은 구체적으로 작성되어야 합니다. 애플리케이션이 필드 레벨 암호화를 지원하는 경우, AWS CloudHSM 이 지원하는 암호화 키를 사용합니다[13].

[8] https://aws.amazon.com/ec2/?nc2=h_m1

[9] https://aws.amazon.com/ebs/?nc2=h_m1

[10] https://aws.amazon.com/kms/?nc2=h_m1

[11] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

[12] https://aws.amazon.com/s3/?nc2=h_m1

[13] https://aws.amazon.com/cloudhsm/?nc2=h_m1

5.1.4 토큰화

액센추어의 AWS 보안 프레임워크는 AWS 중요 계정 및 VPC 에서 다른 VPC 및 네트워크 환경으로 전송하는 모든 중요 데이터를 대체하기 위하여 토큰화를 사용합니다. CipherCloud 는 토큰화 게이트웨이로서 사용되는데, 이는 금융서비스기관이 신뢰 환경 외부로 민감 데이터를 전송하지 않고 Salesforce, SAP, Service Now 와 같은 SaaS 솔루션의 완전한 기능을 이용할 수 있도록 합니다.

토큰화는 민감 데이터를 2 차 시스템 또는 제 3 자에게 전달하기에 앞서 비민감 토큰으로 대체함으로써 데이터 전파를 최소화하기 위한 방식입니다. 원본 데이터가 토큰으로부터 재구성될 수 없으므로, 토큰화는 민감 데이터의 준법 준수 및 보안 범위가 참조 시스템 정도로 축소됩니다. 토큰화는 종종 결제카드 및 기타 민감한 개인정보와 관련하여 사용됩니다.

기본적으로, 액센추어의 AWS 보안 프레임워크는 현재의 데이터 분류를 검토하고 AWS 플랫폼 상에서 어떻게 해당 분류를 관리할지를 결정할 것을 권장합니다. 이는 중요 환경 외부의 데이터에 대하여 토큰화가 필요한지 여부를 결정하는 데 도움이 됩니다.

5.1.5 키 관리

액센추어의 AWS 보안 프레임워크가 AWS 사용을 위하여 채택하는 키 관리 인프라(Key Management Infrastructure: KMI)의 두 가지 주요 모델은 다음과 같습니다:

- AWS 키 관리 서비스를 이용하는 AWS 관리형 KMI
- AWS CloudHSM 를 이용하는 고객 관리형 KMI

AWS 키 관리 서비스를 이용하는 AWS 관리형 KMI[14]는 비중요 데이터에 이용됩니다. AWS 는 키 관리 서비스(KMS)를 이용하여 키 주기를 자동으로 생성 및 관리합니다. KMS 는 다수의 AWS 서비스와 통합되어, 고객 데이터를 보호하기 위해 암호화 서비스의 간단한 체크박스 활성화를 가능하게 합니다. 액센추어의 AWS 보안 프레임워크는 준법준수 지침을 따르기 위하여 KMS 키에 대한 키 순환 정책을 가동합니다. 이 모델은 가격 대비 높은 가치(value for money)를 제공하면서도 비중요 데이터 지원에 요구되는 보안과 민첩성에는 전혀 영향을 미치지 않습니다.

액센추어는 AWS 의 키 관리를 AWS CloudHSM 을 사용하는 KMI 와 분리할 것입니다. 이 솔루션은 애플리케이션 및 데이터베이스 차원의 모든 중요 데이터에 사용됩니다.

금융서비스기관이 중요 데이터 등 키 관리에 관한 업무 분리에 대하여 우려사항이 있다면, AWS CloudHSM 서비스를 사용하여 암호화 키 주기를 제공 및 관리할 수 있습니다. Amazon 은 CloudHSM 내 키에는 액세스할 수 없기 때문에 보안 서비스 제공자 및/또는 고객이 키 관리 및 사용하는 암호화 방법에 관하여 완전한 제어권을 보장받습니다. 이 모델은 업무 분리에 관한 우려사항(그 정당성 여부를 불문하고)을 해결하지만 높은 투자 및 전문성을 요기 때문에, 위험한 프로필 또는 민감 데이터의 준법 준수 요건에 따라 요구되는 경우에 한하여 그 사용이 권장됩니다.

[14] AWS 키 관리 서비스 암호화 관련 세부사항(AWS Key Management Service Cryptographic Details)

5.2 전용 장비 또는 사설 클라우드

액센추어의 AWS 금융보안 프레임워크 는 AWS 계정 및 Amazon VPC 를 사용하여 다른 계정 및 테넌트(tenant)와 논리적으로 분리된 환경을 제공합니다. 각 계정 내에서 Amazon VPC 는 개인 네트워크 공간을 생성하도록 구성됩니다. 네트워크 공간 내에는 VPC 내의 트래픽을 분리하기 위해 보안 흐름 제어를 제공하는 액세스 목록 및 보안 그룹과 같은 추가 제어 기능이 있습니다. 각 계정에 Amazon VPC 를 갖춘 여러 AWS 계정을 사용하여 애플리케이션의 유형, 역할 및 민감도에 따라 작업을 분리합니다.

5.2.1 인스턴스 격리

액센추어의 AWS 보안 프레임워크는 젠 하이퍼바이저(Xen hypervisor)를 통해 AWS 인스턴스 격리 메커니즘을 활용합니다. 하이퍼바이저 계층과 모든 네트워크 내에서 트래픽은 해당 계층을 통과하여야 하고, 이는 인접 인스턴스가 해당 인스턴스에 엑세스하지 못하도록 합니다. 이러한 메커니즘은 가상 서버를 물리적 호스트처럼 취급되도록 합니다.

액센추어의 AWS 보안 프레임워크는 추가 제어 기능을 제공하여 고객 데이터를 추가적으로 보호합니다. 이러한 제어에 대해서는 뒷부분에서 더욱 심도 있게 설명합니다.

5.2.2 데이터 위치

본 문서의 목적 상[15], 모든 데이터 및 서비스는 AWS 싱가포르 리전(region)에서 호스팅됩니다. 이를 통해 싱가포르 리전에 소재한 데이터는 해당 리전에 남아있도록 보장할 수 있습니다. 고객이 명시적으로 데이터 전송을 시작하거나 법적으로 요구되지 않는 한, AWS 는 고객이 선택한 리전 외부로 콘텐츠를 이동하지 않습니다.

특정 리전 내에서 데이터는 복원, 백업 및 재해 복구를 위해 여러 가용영역(Availability Zone: AZ)에 복제됩니다.

5.2.3 AWS 계정의 분리

AWS 계정은 보안 및 리소스 목적에 대한 관리상 경계가 되므로 고객의 운영, 보안, 거버넌스 및 재정적 필요를 지원하는 정확한 계정 구조를 고려해야 합니다.

AWS 계정은 다른 계정과의 분리를 제공하는 AWS 리소스를 가지고 있습니다. 각 계정은 AWS ID 및 액세스 관리(Identity & Access Management: IAM)[16] 서비스를 지원받아 자체적인 사용자, 그룹 및 역할을 가집니다. 별도의 AWS 계정을 여러 개 사용함으로써 업무를 분리할 수 있고 서로 다른 환경 유형을 효과적으로 분리할 수 있습니다.

액센추어의 AWS 금융보안 프레임워크는 계정에 내재된 논리적 분리도 사용하는데, 이는 계정 손상, 악의적 공격, 구성 오류 등의 주요 파괴적 이벤트의 "폭발 반경(blast radius)"을 제한합니다. 권장 계정 구조는 아래 표에 설명된 바와 같습니다:

[15] 싱가포르 통화청 지침은 데이터 주권에 관한 엄격한 규정을 명시하지 않고 있어 금융서비스기관은 여타 AWS 리전에서도 솔루션을 이용할 수 있을 것입니다.

[16] https://aws.amazon.com/iam/?nc2=h_m1

계정명	기능	설계 사유
비중요	모든 비핵심 뱅킹 데이터 및 애플리케이션 지원	최전선과 작업장에서 핵심 뱅킹 데이터를 분리하여 비중요 작업에 대한 민첩한 접근을 가능하게 합니다.
비중요 서비스	비핵심 데이터를 지원하는 애자일 린 서비스(Agile lean service) 모델	핵심 비즈니스 데이터에 대한 액세스 격리를 제공하여, 비중요 작업에 대한 시스템 관리에 대해 새로운 클라우드식 접근법을 채택할 수 있습니다.
중요	은행 업무에 필수적인 핵심 뱅킹 모놀리식 애플리케이션 및 데이터 지원	승인 및 사용자 액세스 분리는 고도로 제어되며 집중적인 감시 하에 있습니다.
중요 서비스	핵심 뱅킹 데이터를 위한 시스템 관리 서비스 제공	전통적인 제어 기반 정책 및 ITIL 방법론에 중점을 둡니다.
IAM	계정이 고객의 액티브 디렉토리와 연계. 사용자에게 다른 계정에 액세스할 수 있는 계정, 그룹 및 역할을 제공. 사용자 관리를 중앙집중화하기 위하여, IAM 계정이 아닌 다른 계정에서는 사용자가 생성되지 않음.	단일 제어점을 통한 계정 관리의 중앙집중화. 다른 AWS 계정에 역할에 따른 정책 기반 권한 부여로 높은 수준의 보안 기반 액세스를 제공합니다.
보안 및 감사	보안 서비스 및 로그의 호스팅 및 격리 계정	보안 역할 및 데이터 격리. 루트 자격증명을 사용할 때마다 경고가 설정됩니다.

표 2: 계정 구조

5.2.4 Amazon VPC

Amazon VPC(Virtual Private Cloud)는 AWS 계정 내에서 생성되는 가상 네트워크입니다. 각 VPC 는 AWS 플랫폼의 다른 가상 네트워크와 논리적으로 격리됩니다. Amazon EC2, ELB, Amazon RDS, Amazon EMR, Amazon Redshift, AWS Elastic Beanstalk, Amazon WorkSpaces 등 다양한 유형의 AWS 서비스를 Amazon VPC 에 배치할 수 있습니다. 또한 VPC 에서 AWS Lambda 나 Amazon S3 와 같은 사설 엔드포인트(endpoints)을 통해 액세스할 수 있는 서비스가 있습니다.

Amazon VPC 구조는 아래 다이어그램과 같습니다:

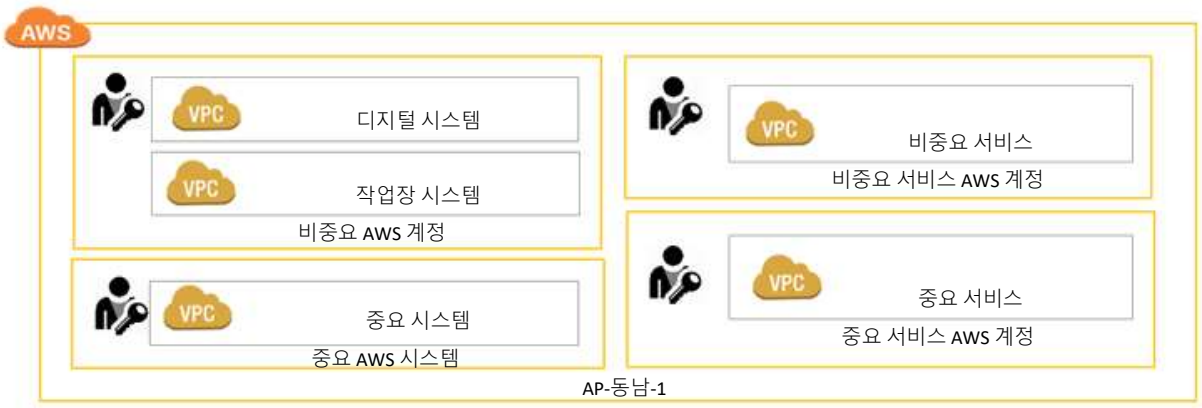

그림 7: Amazon VPC 설계

Amazon VPC 각각의 목적과 설계 사유는 다음과 같습니다:

VPC 명	기능	사유
디지털	고객을 직접 응대하고, 매우 민첩하고 역동적인 디지털 비즈니스를 위한 데이터 호스팅	최전선 및 작업장 데이터로부터 핵심 뱅킹 데이터의 플랫폼 분리
작업장	클라우드 기반 서비스를 지원하도록 재설계할 수 있는 비핵심 뱅킹 데이터 및 애플리케이션 호스팅	핵심 비즈니스 데이터의 네트워크 격리 제공
중요	핵심 뱅킹 데이터 및 애플리케이션 호스팅	핵심 비즈니스 데이터의 네트워크 분리 제공
비중요 서비스	NTP, AD, DNS 와 같은 호스트 서비스를 위한 액세스 플랫폼 제공	애자일(agile) 클라우드 기반 방식으로 서비스를 제공하는 비즈니스 애플리케이션과 네트워크 분리
중요 서비스	Amazon VPC 는 핵심 뱅킹 데이터 및 애플리케이션 모니터링과 같은 시스템 관리 서비스에 사용됩니다.	비즈니스 애플리케이션 데이터로부터 관리 서비스의 플랫폼 분리

표 3: Amazon VPC 명칭, 기능 및 설계 사유

Amazon VPC 간의 라우팅은 환경 분리를 유지하는 한편 Amazon VPC 및 AWS 계정에서 전체 환경을 효과적으로 관리하기 위하여 설계되었습니다. 작업을 처리하는 Amazon VPC 는 서비스 Amazon VPC 및 구내(on-premise) 네트워크와 연결할 수 있으나, 서로 연결할 수는 없습니다. 아래 다이어그램과 표는 Amazon VPC 라우팅 및 게이트웨이의 설계를 보여줍니다.

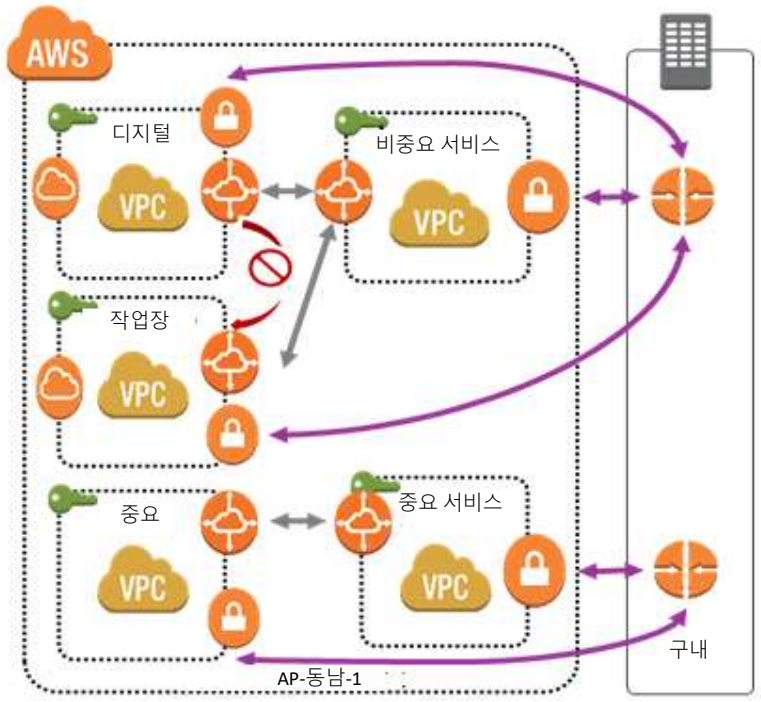

그림 8: 라우팅 및 게이트웨이 아키텍처

게이트웨이	결정	사유
인터넷	디지털 및 작업장 데이터는 VPC 내 전단부 서브넷을 통해서만 인터넷에 액세스할 수 있습니다.	인터넷에 액세스해야 하는 서비스 및 애플리케이션만이 이러한 VPC 에서 호스팅됩니다.
가상 사설망	모든 VPC 내의 전단부 서브넷은 직접 연결 서비스 및/또는 IPSEC VPN 을 통해 사내 네트워크에 다시 연결됩니다.	보안 네트워크 경로를 통해 AWS 에서 호스팅되는 애플리케이션에 대한 내부 B2B 및 C2B 액세스 메커니즘을 제공합니다
비중요 피어링	디지털 VPC 가 작업장 Amazon VPC 와 피어링됩니다.	B2B 서비스에 보다 민첩하고 역동적인 접근 방식을 제공합니다.
비중요 서비스 피어링	비중요 서비스 VPC 가 디지털 및 작업장 VPC 와 피어링됩니다.	기민한 전달을 지원하는 클라우드 기반 서비스와 이러한 서비스를 지원하는 시스템 관리 서비스를 제공합니다.
NAT	디지털 및 작업장 VPC 는 전단부 서브넷 설치된 NAT 게이트웨이를 가지게 됩니다.	후단부 서브넷에서부터 공용 IP 뒤에 보안된 인터넷까지 나가는 트래픽만 제공합니다
중요 피어링	핵심 VPC 는 핵심 서비스 인 VPC 와만 피어링되며 작업장 및 디지털 VPC 와는 피어링되지 않습니다. B2B 의 모든 흐름은 사내 네트워크를 통해 이루어집니다.	작업장 및 디지털 VPC 의 클라우드 기반 서비스의 오고 가는 플로우에 대하여 안전한 전통적 잠금 접근을 제공합니다

표 4: VPC 게이트웨이 및 피어링

5.2.5 보안 그룹

보안 그룹은 AWS EC2 인스턴스에 대한 상태 전체의 가상 방화벽입니다. 이들은 인스턴스 그룹에 대한 출입 트래픽을 모두 제어하고 VPC 계층의 서브넷이 아닌 인스턴스 계층에서 작동합니다. 따라서 VPC 의 서브넷에 있는 각 인스턴스를 다른 보안 그룹 세트에 할당할 수 있습니다. 액센추어의 AWS 보안 프레임워크는 애플리케이션, 인스턴스를 호스팅하는 서브넷, 운영체제 및 인스턴스와 애플리케이션을 지원하는 데 필요한 서비스 관리 도구를 기반으로 다수의 보안 그룹을 할당합니다. 아래 표는 인스턴스에 적용되는 각 보안 그룹의 기능을 설명합니다.

기능	결정	사유
전단부 보안그룹	인터넷이나 내부 피어링된 VPC 및 네트워크에서 부하 분산장치에 액세스할 수 있는 메커니즘을 제공합니다.	공용 인터넷 IP 주소를 할당하지 않고 프론트 엔드(front end) 서버에 액세스하기 위한 보안 메커니즘
후단부 보안그룹	벡엔드(backend) 보안그룹은 특정 포트의 남북쪽 프론트엔드 보안그룹 및 동서쪽 백엔드 보안 그룹에서만 액세스할 수 있습니다.	B2B 애플리케이션 특정 흐름 제어를 위한 보안 메커니즘 제공
데이터 보안그룹	특정 포트를 통해 연결하는 벡엔드 애플리케이션 보안그룹만 제공합니다.	데이터베이스에 대한 B2B 애플리케이션 특정 흐름을 위한 보안 메커니즘 제공

비중요 서비스 보안그룹	Std 서비스 VPC 전용의 특정 서비스 포트에 대한 액세스를 허용합니다.	서비스 VPC 에 대한 흐름 제어를 위한 보안 메커니즘
중요 서비스 보안그룹	시스템 관리 VPC 의 특정 IP 주소 및 포트에 대한 코어 뱅킹 서비스에 대한 액세스를 제공합니다.	핵심 뱅킹 시스템을 관리하기 위한 보안 제어 시스템
원격 액세스 보안그룹	내부 네트워크의 SSH 또는 RDP 포트에 대한 외부 액세스를 제공합니다. 코어 뱅킹의 경우 코어 서비스 VPC 만 해당합니다.	VPC 에서 운영 체제에 안전하게 액세스하는 메커니즘
운영체제 보안그룹	RDP 및 요새(Bastion) 서비스가 시스템 관리를 위하여 보안 프로토콜을 통해 운영체제에 액세스할 수 있도록 허용합니다.	VPC 내 운영체제에 대하여 안전한 권한이 부여된 액세스 제공

표 5: 보안 그룹

5.2.6 보안 제어 모니터링

액센추어의 AWS 보안 프레임워크는 보안 제어를 모니터링하기 위하여 AWS Config[17]를 활용합니다. AWS Config 는 기반 AWS 리소스 인벤토리, 구성 기록 및 구성 변경 알림을 제공하여 구성 변경시 컴플라이언스를 가능하게 합니다. Amazon VPC, 보안그룹과 같은 관련 리소스의 최적 구성은 AWS Config 규칙에 의해 정의됩니다. AWS Config 는 이 규칙에 따라 모든 구성 변경 사항을 모니터링하고 평가를 수행하여 변경 사항의 준수여부를 확인합니다.

[17] https://aws.amazon.com/config/

5.3 변경 관리 및 사용자 접근 권한 관리(PUAM)

변경 관리(Change Management) 및 사용자 접근 권한 관리(Privileged User Access Management: PUAM) 제어는 클라우드 환경에서 수행되는 모든 관리자 작업을 거의 실시간으로 볼 수 있게 해줍니다. AWS Cloud Watch[18]는 AWS 에서 실행되는 AWS 클라우드 리소스를 모니터링하는 데 사용됩니다. AWS CloudTrail[19]은 모든 관리자 로그인 및 작업을 기록함으로써 모든 작업이 지정된 사용자에게 연결되도록 합니다.

AWS Config 는 현재 구성 및 과거 상태의 히스토리를 보여주는 데도 사용됩니다. AWS CloudWatch, AWS CloudTrail 및 AWS Config 의 데이터를 종합하면, 관리자 사용자가 언제 어떤 변경 작업을 수행했는지에 관한 전체 그림을 파악할 수 있습니다. 이후 이 데이터를 변경 관리 시스템과 비교 감사하여 환경에 대한 모든 변경 사항을 권한 부여에 연결할 수 있도록 합니다.

AWS 는 기저 인프라 및 서비스에 대한 강력한 변경 관리 프로세스를 갖추고 있습니다. 이 프로세스는 고객에게 서비스의 연속성을 제공하기 위한 것이므로 성능 또는 서비스 가용성에 대한 영향 없이 대부분의 변경 사항을 검토, 테스트, 승인 및 구현합니다. 고객에게 영향을 미칠 수 있는 변경 사항의 경우, AWS 는 고객에게 알리고 계정 관리자는 고객과 협력하여 고객이 준비되었는지 확인합니다.

AWS 에서 실행되는 작업의 사용자 접근 권한 관리는 CyberArk PUAM 소프트웨어에서 제공합니다. 이 소프트웨어는 환경에 대한 단일 접근점을 적용하고 사용자가 취한 모든 작업을 기록합니다. 이러한 기록(logs)은 저장 및 분석을 위해 보안 및 감사 계정으로 전달됩니다.

---

[18] https://aws.amazon.com/cloudwatch/

[19] https://aws.amazon.com/cloudtrail/

5.4 가상 환경 보안

액센추어의 AWS 보안 프레임워크는 AWS 가 제공하는 기저 인프라 보안의 상단에 몇 가지 제어를 추가합니다.

Amazon Machine Images(AMI)[20] 는 클라우드의 가상 서버 템플릿을 정의합니다. AMI 는 AWS Quick start 카탈로그에서 제공되며 고객의 요구에 맞게 강화 및 커스터마이징됩니다. AMI 는 테스트 및 승인 후 등록되며 등록된 후에는 변경할 수 없습니다. 등록된 AMI 만이 특정 계정 내에서 시작될 수 있습니다.

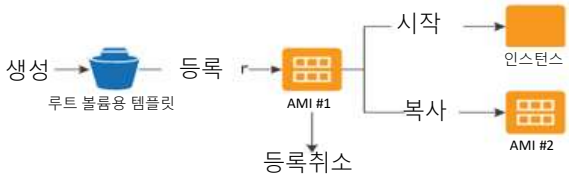

그림 9: AMI 구축 자동화

기존의 예방적 엔드포인트 보안 제어는 관련 서버에 안티 바이러스, 방화벽 호스트 IDS/IPS, 데이터 손실 방지, 애플리케이션 허용 목록 및 파일 무결성 모니터링을 이용하였습니다.

정기적인 침투 테스트는 환경 전체의 보안을 테스트하는 데 사용됩니다. 모든 침투 테스트는 AWS 의 허가를 요합니다. 허가를 요청하려면 AWS 취약성/침투 테스트 요청서[21]를 제출하십시오. 액센추어 보안팀은 AWS 환경에서 실행되는 작업에 대해 매년 종합 침투 테스트를 수행합니다. 이는 AWS Inspector[22]를 사용한 모든 배포 후 취약성 평가와 QualysGuard 취약성 검색 도구를 이용한 분기별 환경 취약성 검사로 개선됩니다. 이후 보안팀은 운영팀과 협력하여 취약점을 평가하고 치료합니다.

사용자 액세스 관리 및 업무 분리

사용자 액세스 관리 및 업무 분리는 환경 보안에 있어 가장 중요합니다. 이러한 제어는 사용자임을 증명하고 사용자가 작업을 완료하는 데 필요한 리소스에만 액세스하도록 허용하는 한편 중요한 활동의 경우 적절한 감독 없이는 개별 사용자가 작업을 수행할 수 없도록 합니다.

액센추어의 AWS 보안 프레임워크에는 사용자 액세스 관리 및 업무 분리를 지원하기 위하여 다음과 같은 기능을 통합합니다.

- 사용자 및 그룹
- 역할 기반 액세스 제어
- ID 연계
- 임시 보안 자격증명
- 다중요소 증명
- 사용자 작업 감사

---

20 http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html

21 https://aws.amazon.com/forms/penetration-testing-request

22 https://aws.amazon.com/inspector/

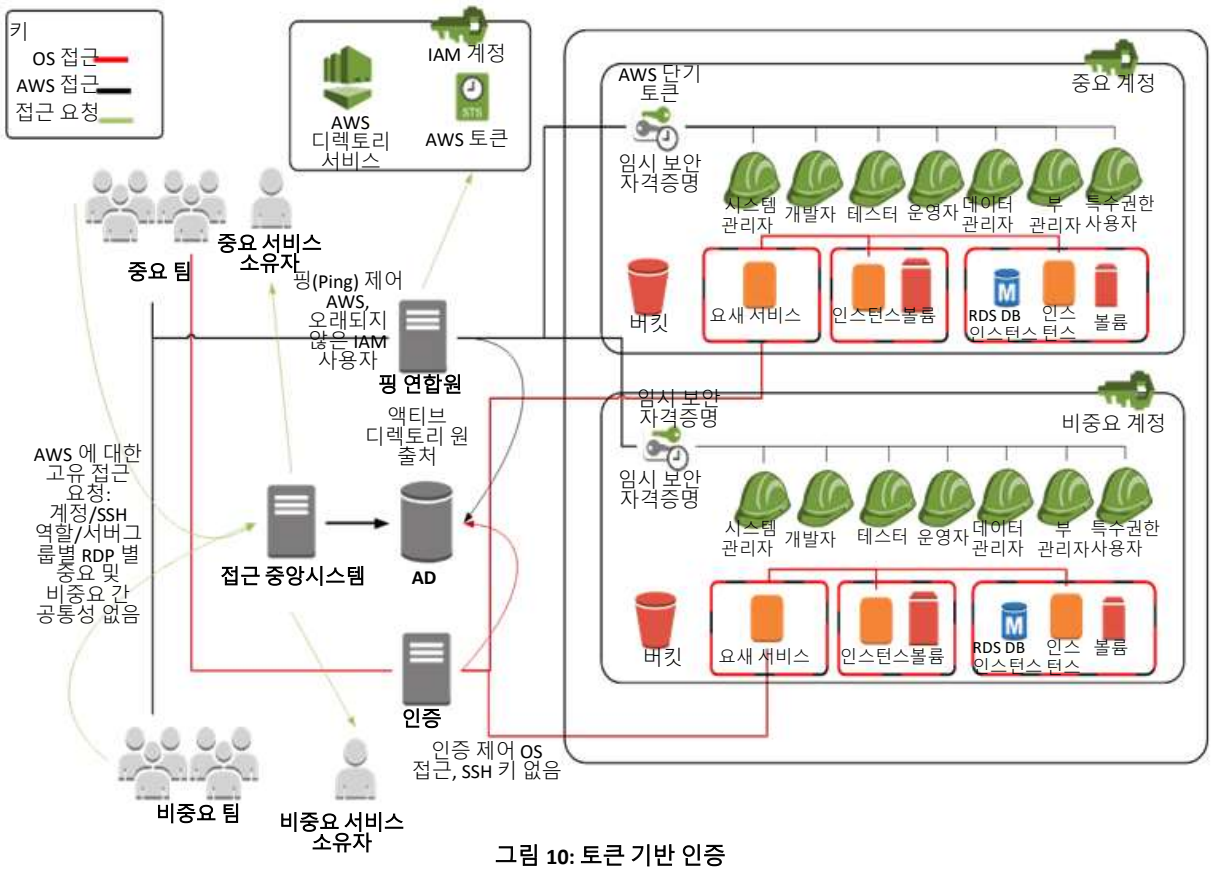

그림 10: 토큰 기반 인증

5.4.1 사용자 및 그룹

제 5.2.3 절에서 설명하였듯, 모든 사용자와 그룹은 AWS IAM 서비스에서 정의됩니다. 액센추어의 AWS 보안 프레임워크 내에서 IAM 사용자는 AWS IAM 계정에서만 생성됩니다. 다른 AWS 계정에서는 어떠한 사용자도 정의되지 않습니다. 각 AWS 계정의 루트 계정에는 제 3 자 서비스가 관리하는 키를 보유합니다. AWS 보안 프레임워크는 AWS 리소스에 대한 액세스를 위해 사용자와 그룹을 관리할 수 있는 안전한 대안을 제공하는 "액세스 대여(Leased Access)"메커니즘을 통해 임시 액세스를 제공하는 데 중점을 둡니다.

5.4.2 역할 기반 액세스

각 AWS 계정에는 AWS IAM 에 정의된 액센추어의 AWS 보안 프레임워크의 사전 정의된 역할이 있습니다. 이를 통해 어떤 범위의 사용자 그룹에게 업무 역할에 따른 사용 권한 및 정책을 할당할 수 있습니다. 개별 사용자가 아닌 역할에 권한을 할당하고 AWS IAM 계정의 IAM 사용자만 다른 계정의 역할에 액세스할 수 있게끔 생성되도록 허용함으로써 보안이 향상됩니다. 이를 통해 사용자가 중앙집중된 장소에서 관리되고 감사를 위한 권한이 적게 요구되므로, 사용자 감사가 간단해집니다. 또한 감사인은 사용자에게 할당된 각 권한을 분석하는 대신 사용자가 해당 역할에 액세스할 필요가 있는지만 분석하면 됩니다. IAM 정책은 사용자 그룹에 할당 된 IAM 역할에 사용권한을 할당하기 위하여 사용됩니다.

액센추어의 AWS 보안 프레임워크는 다음과 같은 기본 역할부터 시작하여, 고객의 보안 및 컴플라이언스 요구 사항을 충족시키기 위해 고객 맞춤형 서비스도 제공합니다.

역할	세부사항
인프라 관리자	IAM, 보안 및 결제 계정을 제외한 환경의 AWS 저장소, 컴퓨트 및 네트워킹 서비스 관리를 위한 관리자 액세스
개발자	개발 환경에 대한 OS 및 애플리케이션 계층 액세스.
테스트 엔지니어	테스트 환경에 대한 OS 및 애플리케이션 계층 액세스
운영	프로덕션 환경에 대한 OS 및 애플리케이션 계층 액세스
데이터베이스 관리자	데이터베이스 생성 및 관리를 위한 전체 관리자 액세스.
보안 관리자	IAM 사용자 및 역할을 생성 및 관리하기 위한 액세스. SIEM, 로그 관리 시스템, 보안 및 감사 계정 관리. 모든 계정의 여타항목에 대한 읽기 전용 액세스.
고급 권한 사용자	프로덕션 애플리케이션에 대해 고급 권한을 가진 사용자. 이 역할은 해당 사용자의 작업을 높은 수준으로 철저히 검토하기 위하여 설계되었습니다

표 6: 사용자 역할

5.4.3 ID 연계

핑 연계(Ping Federate)는 금융서비스기관의 사내 액티브 디렉토리(Active Directory: AD)를 AWS 플랫폼에 연결하는 데 사용됩니다. 이를 통해 단일점으로 사용자 관리를 할 수 있고, 사용자는 일반 사용자 자격증명을 사용하여 SSO(Single Sign On)를 통해 AWS 리소스에 액세스할 수 있습니다. 기존 AD 관리 프로세스를 사용하여 AWS IAM 그룹, 역할 및 권한에 맵핑되는 AD 그룹에 사용자를 추가할 수 있으므로, 사용자 관리가 간단해집니다.

또한 임시 자격증명을 사용하여 보안이 향상됩니다. 연계 사용자가 IAM 에 자격을 증명하면, AWS 서비스에 액세스하기 위한 임시 자격증명이 제공됩니다. 장기 액세스를 제공할 수 있는 사용자명 및 암호와 달리, 임시 자격증명은 최대 1 시간까지 지속되므로 공격자가 자격증명 액세스를 얻은 경우라도 리소스에 대한 지속적인 액세스를 방지합니다.

5.4.4 임시 보안 자격증명

임시 보안 자격증명은 한정된 기간 동안 신뢰할 수 있는 사용자에게 정의된 AWS 리소스에 대한 액세스를 제공하는 데 사용됩니다. 액센추어의 AWS 프레임워크는 임시 보안 자격증명을 사용하여 API 호출 또는 콘솔을 통한 임시 로그온을 통해 AWS 리소스를 요청합니다. 임시 보안 자격증명에 관한 보안상의 이점은 다음과 같습니다:

- 고객은 애플리케이션에 대한 장기 AWS 보안 자격증명을 배포하거나 개발할 필요가 없습니다.
- IAM 에서 관리 및 유지 관리하지 않고도 AWS 리소스에 대한 액세스를 사용자에게 제공할 수 있습니다. 그 대신 역할 및 연계 ID 원칙에 따라 임시 자격증명이 작동합니다.
- 임시 자격증명은 만료된 후 재사용될 수 없습니다. 이 제한된 기한은 자격증명을 순환시키거나 제거해야 하는 오버헤드(overhead)을 줄여줍니다.

중요 및 비중요 데이터 모두에 관하여 AWS 리소스 및 서비스에 대한 액세스는 연계된 ID 및 임시 보안 자격증명과 다중요소 인증을 통합니다.

액센추어의 AWS 보안 프레임워크는 핑 연계를 사용하여 AWS 리소스 및 AWS 에서 실행되는 서버에 액세스할 때 다중요소 인증을 요구합니다. 다중요소 인증은 손상된 사용자명과 암호만으로는 중요한 인프라에 액세스할 수 없도록 함으로써 보안을 강화합니다. 이로써 모든 권한있는 사용자에 대하여 다중요소 인증을 요구하는 금융 산업의 규제를 준수합니다.

5.4.5 사용자 작업 감사

AWS CloudTrail 은 모든 관리자 로그인을 AWS 에 기록하고 플랫폼에서 수행 한 모든 관리 작업을 기록하는 데 사용됩니다. 이로써 감사 목적상 관리자 작업과 식별된 사용자를 연결하는 로그 기록을 생성합니다. 각 계정의 AWS CloudTrail 로그 피드는 보안 및 감사 계정으로 통합됩니다.

또한 AWS CloudWatch 로그, 애플리케이션 로그 및 Windows 및 Linux 운영체제 로그는 상관관계, 경고 및 기록 보관 목적상 보안 및 감사 계정으로 전달됩니다. 보안팀만이 보안 및 감사 계정에 액세스할 수 있으므로 다른 사용자가 다른 AWS 계정에서 전체 관리자 권한을 가지고 있더라도 로그를 조작할 수 없습니다.

Splunk Enterprise Security 는 로그를 분석하고 보안 이슈에 대하여 경고하는 데 사용되는 보안 정보 및 이벤트 관리 시스템(SIEM)입니다. 로그 분석 및 상관관계 엔진이 갖추고 있으며 다량의 사전 정의 된 경고, 대시보드 및 보고를 포함합니다. 본 프레임워크는 사전 정의되고 커스터마이징된 템플릿 보고서 및 보안 대시 보드를 사용하여 구축되었기 때문에 관리하는 AWS 환경의 보안 상태에 관한 통찰을 제공하고 내·외부 보안 위협에 신속하게 경고하고 대응합니다.

5.5 협력적 재해 복구 테스트

클라우드 호스팅은 재해 복구에 대한 새로운 접근법을 제공하여 기존 재해복구 접근법의 노력과 비용 일부를 완벽하게 지원합니다. 액센추어의 AWS 보안 프레임워크의 지도원리를 따르고 이를 재해 복구의 상황에 적용하여 본 프레임워크는 중요 데이터에 대한 재해 복구는 전통적인 접근방식을 추구하는데, 이에 따라 가용영역에서 데이터를 복제하고 "예열(warm)" 또는 "상시 대기(hot standby)" 재해 복구 개념을 사용하는 플랫폼 구축을 미러링합니다.

타당한 비중요 작업의 경우에는 매우 복원성이 높고 변경할 수 없으며, 본질상 수명이 길지 않은 인프라에 중점을 둘 것입니다. 이것은 RTO 와 RPO 주변의 비기능적 요구사항을 지원하기 위한 기초가 될 것입니다. 비중요 데이터에 대한 테스트는 DevOps 에 적용되는 계속적 전달 및 통합 기술을 통해 수행됩니다.

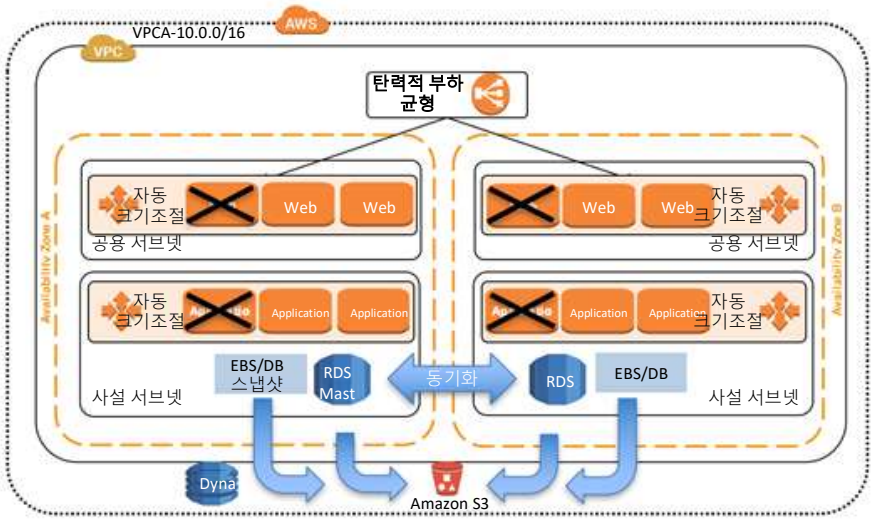

그림 11: 예열 대기 아키텍처

5.5.1 중요 작업의 재해 복구 테스트

전통적인 재해 복구 계획은 중요 작업을 위한 것이지만, 백업 테스트간에 유휴 상태로 있는 백업 하드웨어에 대한 비용을 지급하지 않는 등 클라우드의 장점을 그대로 활용합니다.

재해 복구 상황 테스트에서 중요 데이터의 경우, 하나의 가용영역을 종료하고 모든 트래픽 및 데이터가 다른 가용영역에서 사용 가능하도록 하는 데 중점을 둡니다.

또한 모든 가용영역에 정전이 발생하고 이미지 및 볼륨의 백업을 복원해야 하는 경우 재해 복구 프로세스를 지원하려면 백업 및 이미지를 위한 내구성 있는 저장소가 필요합니다. 액센추어의 AWS 보안 프레임워크는 암호화된 백업 데이터를 템플릿 및 소스코드와 같은 다른 지원 데이터와 함께 Amazon S3 에 저장합니다. Amazon S3 는 기업이 사내 데이터 저장소 솔루션으로는 맞추기 어려운 비용으로 매우 높은 수준의 내구성을 제공합니다.

5.5.2 비중요 작업의 재해 복구 테스트

비중요 데이터의 경우 테스트는 지속적 배포 프로세스 및 소프트웨어 전달 주기 동안 사용되는 동일한 배포 도구 및 변경불가능한 인프라 구성요소를 사용하여 재해 복구 환경을 만들어 수행됩니다. 테스트 및 검증이 완료되면 환경은 없어지고 고객은 사용기간 동안에 대한 AWS 서비스 비용만 지불하며, 이에 따라 기존 백업 인프라 및 프로세스와 비교할 때 시간, 노력 및 비용이 크게 절감됩니다. 또한 대기(standby) 환경이 없어 TCO 가 낮아질 뿐 아니라 플랫폼이 대기 모드나 라이브 모드가 아니기 때문에 보안 침해의 폭발 영역을 줄입니다.

5.5.3 중요 작업에 대한 재해 복구 아키텍처

- 다중 가용영역(AZ) 배포는 리전 내 높은 가용성을 설계하기 위하여 사용됩니다

- Amazon RDS, Dynamo DB 또는 S3 복제 메커니즘을 사용하여 다중화를 구현합니다.
- Amazon RDS 는다중 가용영역 데이터베이스 복제를 위해 구성됩니다.
- 애플리케이션 데이터 백업을 위해 Amazon Elastic Block Storage(EBS) 스냅샷이 Amazon S3 에 저장됩니다.
- 애플리케이션 및 구워진 AMI 가 Code Commit 을 통해 Code Depository 로 푸시됩니다.
- 플랫폼이 코드로 구성되고 CloudFormation 템플릿으로 작성됩니다.
- S3 가 각 애플리케이션에 대해 구운 AMI 및 CloudFormation 템플릿을 저장합니다.
- 재해 복구 이벤트 중에 CloudFormation 템플릿을 이용하도록 CodeDeploy 를 구성합니다.

5.5.4 비중요 작업에 대한 재해 복구 아키텍처

비중요 작업에 대한 재해 복구는 클라우드 형성 스택을 통해 애플리케이션 및 플랫폼을 배포하기 위하여 애자일 소프트웨어 전달 주기 방법론의 원칙을 따릅니다.

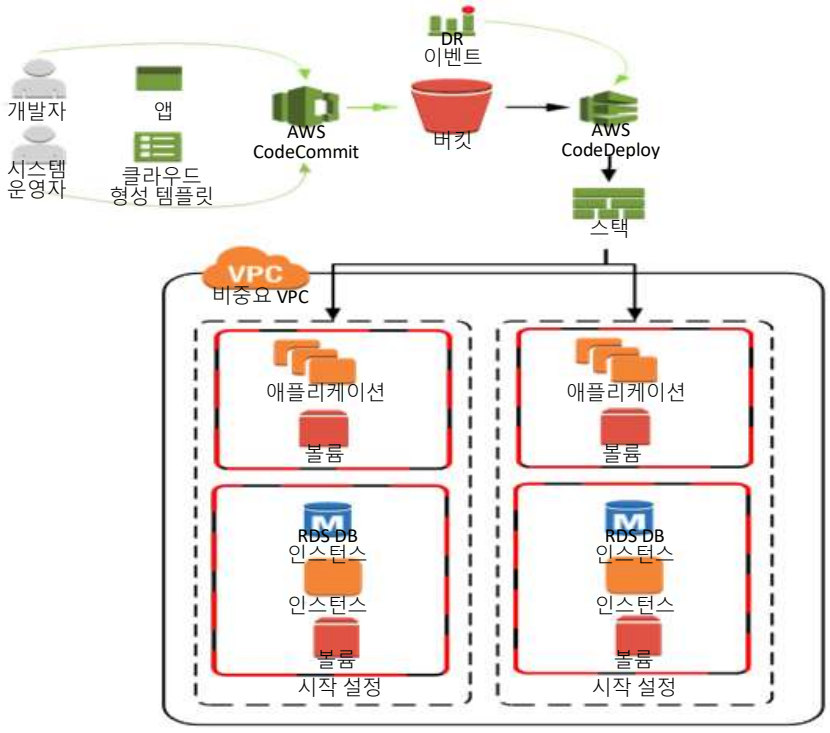

그림 12 CICD 및 애자일 방법론을 이용한 DR 아키텍처

5.6 보안 이벤트 모니터링 및 사고 관리

액센추어의 AWS 보안 프레임워크는 종합적인 보안 이벤트 모니터링 및 사고 관리 기능을 제공하여 기존의 AWS 기능 위에 이벤트 수집 및 분석 도구를 계층화함으로써 고객이 자신의 환경에서 보안 이벤트에 대한 완전한 통찰력을 갖도록 합니다.

보안 이벤트 모니터링 및 사고 관리를 지원하기 위하여 사용되는 도구는 다음과 같습니다.

- AWS CloudTrail
- AWS CloudWatch
- AWS Simple Notification Service[23](SNS)
- Splunk Enterprise Security

그림 13 이벤트 로그 아키텍처

[23] https://aws.amazon.com/sns/

액센추어의 AWS 보안 프레임워크는 이러한 도구를 사용하여 모든 AWS 계정에 대한 모든 관리 작업을 기록하고 이를 특정 사용자에게 태그합니다. 모든 서버 및 서비스의 상태를 모니터링하고, 환경 구성 변경을 모니터링 및 경고하며, 이러한 로그를 안전하게 수집하여 Splunk Enterprise Security 에 저장합니다.

Splunk Enterprise Security 는 보안 이벤트를 수집, 연계, 분석 및 보고하는 보안 정보 및 이벤트 관리 시스템입니다. Splunk 는 보안 및 감사 전용 AWS 계정 내에 있습니다. IAM 권한은 Splunk 가 다른 계정의 로그를 수신할 수 있게끔 하는 한편 다른 계정의 로그를 변경하거나 삭제하는 기능은 제거합니다. Enterprise Security 기능은 로그를 분석 및 연계시키고 광범위한 사전정의된 규칙, 경고, 보고 및 대시 보드를 제공합니다.

액센추어의 AWS 보안 프레임워크는 고객이 가장 관련있는 정보에 집중하고 내·외부 위협 및 공격에 신속하게 대응할 수 있도록 Splunk 대시 보드 및 경고를 커스터마이징합니다.

5.6.1 사고 관리

액센추어는 직원이 24 시간 근무하는 보안 운영 센터를 통해 보안 사고를 신속하게 파악하고 대응할 수 있는 종합적인 보안 운영 서비스를 제공합니다. AWS, 다른 공급업체 및 고객과 협업함으로써, 보안팀은 안티바이러스 및 SIEM 시스템과 같은 보안 감지 시스템이나 AWS, 공급업체 또는 고객으로부터 제기된 사건에 신속하게 대응합니다. Accenture 의 고도로 숙련된 보안 운영팀은 다른 글로벌 보안팀과 긴밀히 협력합니다. 종합적인 사고 관리 절차 및 실행서를 사용함으로써 비즈니스 프로세스의 중단을 최소화하는 한편 사고에 신속하고 적절하게 대응할 수 있습니다.

또한 클라우드 기반 애플리케이션 개발을 통해 기존의 애플리케이션 및 데이터센터에서는 불가능했던 새로운 사고 관리 접근법을 구현할 수 있습니다. 전체 애플리케이션 환경을 몇 분 이내에 신속하게 제공할 수 있는 기능을 활용함으로써, 보안 및 운영팀은 사고가 발생한 환경을 격리시키고 서비스 제공을 계속할 수 있는 새로운 환경을 제공할 수 있습니다. 격리된 환경에서 보안 및 운영 팀은 근본적인 원인 분석 및 손상된 호스트로부터의 포렌직 증거 수집을 위해 더 많은 시간을 확보할 수 있습니다.

5.7 침투 테스트 및 취약성 관리

그림 14 AMI 구축 자동화

5.7.1 침투 테스트

AWS Security 는 정기적으로 모든 AWS 인터넷 연결 서비스의 엔드포인트 IP 주소에 대한 취약점을 검사합니다. AWS Security 는 관련 당사자에게 식별된 취약점을 치료하도록 통지합니다. 또한 외부 취약성 위협평가는 독립적인 보안 회사로부터 정기적으로 수행됩니다. 이러한 평가의 결과 및 권고사항은 시정을 위해 카테고리화 되어 AWS 에 전달됩니다.

액센추어 보안팀은 AWS 환경에서 실행되는 작업에 대해 매년 종합적인 침투 테스트를 수행합니다. 이는 QualysGuard 취약성 검사 도구를 사용하는 분기별 환경 취약성 검사로 강화됩니다. 이후 보안팀은 운영팀과 협력하여 취약점을 평가하고 치료합니다.

5.7.2 패치 관리

취약점을 최소화하기 위해서는 효과적인 패치 관리가 중요합니다. AWS 는 필요에 따라 주기적으로 서비스의 패치를 수행합니다. AWS 패치 주기는 고객에 대한 서비스 중단을 최소화하도록 설계되었으며 대부분의 업데이트는 AWS 서비스에서 실행되는 작업에서 전혀 볼 수 없는 방식으로 이루어집니다. 업데이트가 고객 작업에 영향을 미칠 수 있는 경우, 해당 고객에게는 업데이트 프로세스에 대비할 수 있도록 최대한 많은 알림과 통지를 제공합니다.

AWS 공유 책임 모델에 따라, 클라우드에서 실행되는 운영체제 및 애플리케이션의 패치 작업은 AWS 플랫폼을 관리하는 서비스 공급자의 책임입니다. 액센추어의 AWS 금융보안 프레임워크는 중요 작업의 전통적인 패치 관리를 수행하는데, 공급 업체의 패치 배포, 패치 테스트, 이용 및 변경 관리를 통합합니다. 비중요 작업의 경우 패치작업은 소프트웨어 전달 주기를 통해 관리되는데, amazon Machine Images(AMIs)가 Q & A 및 배포을 위해 소프트웨어 저장소에 구워지고 등록됩니다.

5.7.3 자동 AMI 생성 프로세스

본 프레임워크는 자동화 AMI 구축 프로세스를 구축 파이프라인에 통합하여, 새로운 보안 패치 승인을 기반으로 새로운 이미지를 구축합니다. 구축 프로세스의 생산물로서 업데이트된 AMI 는 배포에 앞서 보안 승인을 위해 전송 될 수 있습니다.

클라우드 기반 비중요 작업의 경우, 패치 관리가 기존 방식보다 간소화됩니다. 지속적 배포 프로세스를 통해, 최신 업데이트를 사용하여 각각의 새로운 배포를 자동으로 구축할 수 있습니다. 패치 배포 프로세스는 추가 단계 없이 정기적인 배포 프로세스의 일부가 됩니다. 보안팀이 중요한 패치를 즉시 배포할 것을 권고하는 경우, 표준화된 자동 구축 및 테스트 프로세스를 통해 최소한의 노력으로 짧은 시간 내에 전체 애플리케이션 환경을 업데이트할 수 있습니다.

5.8 관리자 원격 액세스

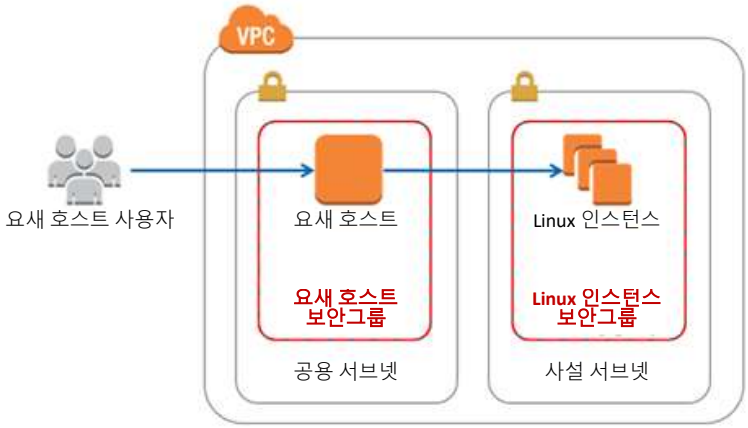

그림 15: 요새 서버 아키텍처

AWS 웹 콘솔에 대한 관리자 원격 액세스와 AWS 플랫폼에서 실행되는 작업은, 액세스하는 네트워크의 신뢰도 차이와 관리 인터페이스에 대한 무단 액세스에 따른 높은 잠재적 보안 영향으로 인해 엄격한 보안 제어가 필요합니다.

AWS 권장 아키텍처를 위한 액센추어 보안 프레임워크는 AWS Direct Connect[24]를 통해 고객의 구내 네트워크를 AWS 플랫폼에 연결하는 것입니다. (기본적으로 더 넓은 인터넷에 노출되는) AWS 웹 콘솔에 대한 액세스는 사전정의된 고객 네트워크의 IP 범주에서만 액세스할 수 있는 IAM 정책이 사용되어 잠겨 있습니다. 이 액세스는 중요 및 비중요 작업에 대한 AWS 서비스 계정 및 Amazon VPC 에 대해서만 부여됩니다.

따라서 AWS 작업에 대한 원격 액세스는 고객의 기존 클라이언트 가상사설망(VPN) 솔루션을 사용하여 고객의 사내 구축형 네트워크를 통해 AWS 웹 콘솔 또는 Amazon VPC 에 연결합니다. 이 접근 방식은 이중 인증 및 엔드포인트 보안 상태 확인과 같은 기존 VPN 액세스 제어 기능을 활용하여 원격 관리자 활동에 대한 안전한 연결을 보장합니다. 고객이 클라이언트 VPN 을 가지고 있지 않은 경우, 액센추어는 고객의 요구사항을 충족하는 적합한 보안 VPN 솔루션을 제공할 수 있습니다.

액센추어의 AWS 보안 프레임워크는 공용 서브넷에 대한 액세스를 보호 및 제어하기 위하여 요새 호스트 아키텍처를 사용합니다.

또한 각 AWS 서비스 계정과 Amazon VPC 내에서는 서비스 외 작업에 대한 원격 액세스를 허용하는 요새 서비스가 호스팅됩니다. 요새 서비스는 잠겨 있으며 모든 로그는 보안 VPC 로 전송됩니다.

AWS 계정에 대한 루트 액세스는 잠겨 있으며 응급 복구를 위한 일시중지 상황에서만 사용됩니다. 각 계정 루트 자격증명은 금고에서 보호됩니다. Splunk SIEM 시스템은 루트 자격증명의 사용에 대해 경고하도록 구성되어 인증된 예외사항과 비교하여 그 수행에 대한 유효성 검사를 할 수 있습니다.

[24] https://aws.amazon.com/directconnect/

5.9 안전한 소프트웨어 개발 주기 및 코드 검토

클라우드 기반 애자일 소프트웨어 개발은 보안 요구사항을 충족하기 위하여 여러 제어들과 함께 새로운 개발 주기를 허용합니다. 전통적인 분리형 개발, 테스트 및 제공 환경을 대신하여, 개발에서부터 테스트, 제공, 폐기 단계까지 단일 애플리케이션 환경으로 이동하고, 개발주기의 다음 반복을 서비스하기 위하여 한 걸음 뒤에서 또 다른 환경을 구축하게 됩니다.

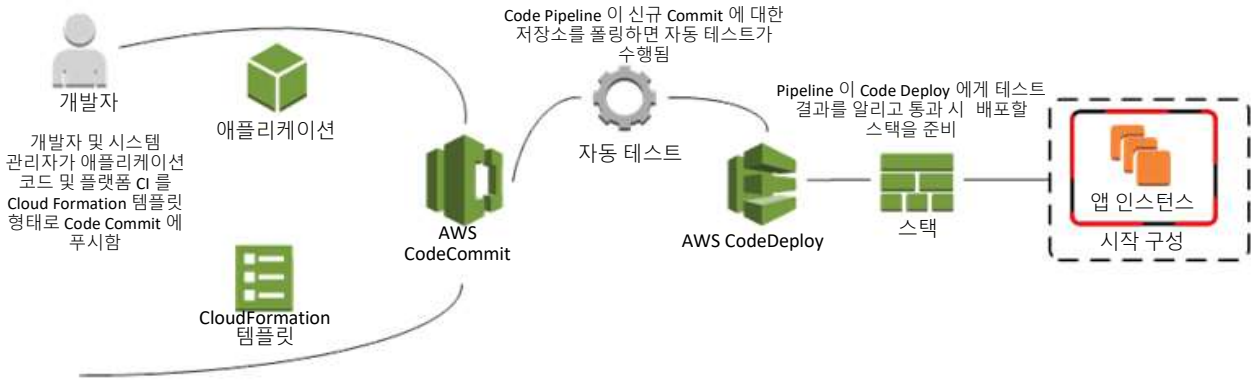

도표 16 AWS 소프트웨어 전달 주기에 대한 액첸추어의 보안 프레임워크

액센추어의 AWS 보안 프레임워크는 소프트웨어 개발 주기의 보안을 보장하기 위해 몇 가지 보안 제어 기능을 사용합니다.

여기에는 다음이 포함됩니다.

- 환경이 하나의 상태에서 다른 상태로 승격되기에 앞서 보안 테스트를 통과하도록 보장합니다.
- 중요 및 비중요 데이터, 백업, 보안 로그, 시스템 관리 서비스 및 도구를 분리합니다.
- 역할 기반 액세스 제어를 통해 중요 데이터, 시스템 관리, 비중요, 보안 및 백업 역할이 세그먼트 전체에 배포되지 않도록 합니다.
- 강력한 버전 제어를 통해애플리케이션 소스코드의 전체 히스토리를 유지할 수 있도록 합니다.

개발팀은 비중요 세그먼트 내에서 이러한 제어를 달성하기 위하여 최신 DevOps 툴링을 사용할 수 있습니다.

5.9.1 보안 테스트[25]

전통적으로, 자동화된 테스트는 애플리케이션의 기능 요소에만 중점을 둡니다. 본 프레임워크의 방법론에서는 이 범위가 보안 테스트를 포함하도록 확장됩니다. 보안 테스트는 자동, 수동 예약 등 두 가지 방식으로 실행됩니다. 다음 유형의 테스트는 자동 테스트의 일환으로 수행됩니다. 자동 테스트는 AWS CodePipeline[26]에서 관리하는 코드 배포 오케스트레이션(orchestration) 프로세스의 일부로서 AWS CodeCommit[27]을 사용하여 코드를 체크인 할 때 실행됩니다.

1. 인증 및 로그아웃과 같은 보안 기능을 확인하는 기능 보안 테스트
2. 애플리케이션이 SSL 구 버전 또는 미흡한 쿠키 처리와 같은 위협에 노출되어 있는지를 확인하는 특정 비기능 테스트
3. 애플리케이션이 보안 관점에서 올바르게 작동하는지(예: HTTP 게시물 변경이 의도된 보안

[25] https://www.owasp.org/images/9/99/AutomatedSecurityTestingofWebApplications-StephendeVries.pdf

[26] https://aws.amazon.com/de/codepipeline/

[27] https://aws.amazon.com/codecommit/

기능을 우회하지 않는지)를 확인하는 애플리케이션 로직 테스트

이러한 테스트는 전통적인 테스트 범주, 단위, 통합 및 승인 테스트의 일부로 수행되는데, AWS CodePipelin 의 단위 테스트를 사용하고 통합 및 승인 테스트를 위해서는 AWS CodeDeploy[28]의 배포 후 단계를 사용합니다. 단위 테스트는 특히 중요한데, 보안 문제의 대부분이 구성요소 수준에서 발생하기 때문입니다. 단위 테스트를 통해 가장 빠른 가시성과 가장 낮은 실패 비용을 제공하는 보다 간단한 테스트가 가능하므로, 교정은 빨라지고 끼치는 영향은 작습니다.

또한 애플리케이션 환경의 보안 검사는 코드가 프로덕션에 출시되기 전에 수동으로 예약해야 합니다. 코드를 체크인 할 때 자동으로 실행되도록 하지 말아야 하는 이유는 두 가지입니다.

1. 보안 검사를 실행하는 데 시간이 오래 걸릴 수 있습니다.
2. 보안 검사를 실행하기 전에 AWS 에게 통보하고 승인을 받아야 합니다. AWS 플랫폼은 보안성이 높기 때문에 계정에 예외 표시를 하지 않고 취약성 검사를 실행할 경우 보호조치가 자동으로 실행될 수 있습니다.

5.9.2 프로덕션 데이터의 분리

제 5.2.3 절 및 제 5.2.4 절에 설명 된 Amazon 계정 및 VPC 는 환경 경계를 정의하는 데 사용됩니다. 중요 데이터는 비중요 데이터와 다른 계정에 위치합니다. 계정 내에서 VPC 는 다양한 애플리케이션 유형을 분리하는 데 사용됩니다. N 계층 아키텍처는 VPC 내에서 보관된 프로덕션 데이터가 애플리케이션 및 프레젠테이션 계층과 다른 네트워크 세그먼트에 저장되어 액세스를 제한하도록 보장합니다. 이 데이터는 Amazon S3, Amazon RDS, Amazon DynamoDB, Amazon Redshift 등에 위치할 수 있습니다. 각 서비스는 네트워크 제어 및 보안 그룹 방화벽 규칙을 사용하여 세그먼트화됩니다.

5.9.3 역할 기반 액세스 제어(RBAC)

AWS 환경 액세스의 경우 각 AWS 계정은 제 5.4.2 절에서 설명한 특정 역할을 갖습니다. 역할은 원하는 결과를 얻기 위하여 AWS 의 다양한 리소스 조합에 액세스하는 데 대한 일관된 보안 상태를 정의하는 AWS IAM 서비스에서 생성됩니다. 각 팀별로 AWS 플랫폼에서 업무를 수행할 수 있게끔 하는 역할에 액세스합니다. 사내 인사변동이 있는 경우, 이는 단순히 그룹 간에 사용자를 이동시킴으로써 반영될 수 있습니다.

애플리케이션 최종 사용자 액세스의 경우 AWS Directory Service[29] 는 관리되는 액티브 디렉토리 선택지를 제공합니다. 이러한 디렉토리 서비스는 역할 및 그룹을 제공합니다. 즉, AWS 서비스가 아닌 애플리케이션 리소스를 제외하고는, 위에서 언급한 것과 유사한 방식으로 RBAC 를 구현할 수 있습니다.

5.9.4 버전 제어

버전 제어는 업계 표준 방법으로 관리됩니다. 버전이 표시된 코드는 AWS CodeCommit 을 사용하여 깃(Git)에 저장됩니다. AWS CodeCommit 은 소스 제어 활동을 단순화하고 버전 변경을 시각화하는 관리 서비스로, 코드 변경의 역사적 영향을 완벽하게 보여줍니다. AWS CodePipeline 과 결합하면 코드 변경을 추적할 수 있을 뿐 아니라 구축, 테스트, 구성 변경 및 배포 스크립트를 포함하여 해당 코드의 출시와 관련된 모든 활동에 대한 종합적인 로그를 볼 수 있습니다.

추가 참고자료:

https://devops.com/automated-security-testing-continuous-delivery-pipeline/

http://techbeacon.com/how-overcome-common-objections-automated-security-testing

[28] https://aws.amazon.com/codedeploy/

[29] https://aws.amazon.com/directoryservice/

5.10 보안 로그 및 백업

로그는 전용 보안 및 감사 계정 내의 AWS S3 버킷으로 통합되어 저장됩니다. 이를 통해 로깅 버킷 주변의 관리 경계를 정의함으로써 로그 데이터에 대한 액세스를 제어할 수 있습니다.

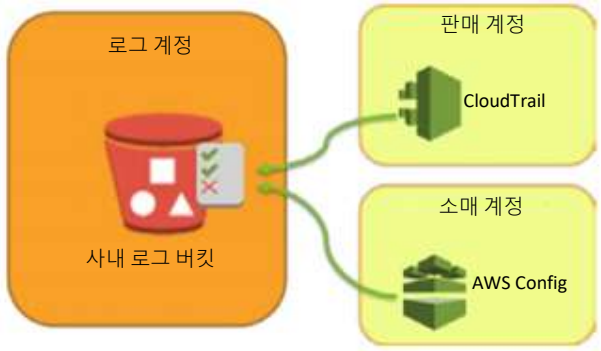

그림 17 로그 및 백업 계정 설치

애플리케이션은 여러 가용영역에 걸쳐 중복성을 갖도록 설계되어 구성요소 오류가 발생하는 경우에도 작업의 연속성을 보장합니다. 백업은 보안 또는 복원을 위해 필요한 경우 특정 시점으로 환경을 돌려놓을 수 있습니다.

전통적인 모놀리식 애플리케이션을 실행하는 중요 작업의 경우에는, 보다 전통적인 방식으로 백업을 수행합니다. CommVault 기업용 백업 소프트웨어를 사용하여 호스트를 백업하고 암호화된 백업을 저렴한 가격으로 내구성 있는 Amazon S3 저장소에 기록합니다. CommVault 는 데이터 중복 제거, 인덱싱, 특정 시점 복구, 심층적 애플리케이션 및 데이터베이스 인식, 재해 복구 오케스트레이션 등 광범위한 최신 백업 소프트웨어 기능을 지원합니다. 백업 내역은 전용 백업 AWS 계정에 작성됨으로써 업무 분리를 보장하고 프로덕션 환경이 손상된 경우 영향 범위를 줄입니다.

비중요인 클라우드 기반 애플리케이션은 백업에 대한 다른 접근법을 채택함으로써 애플리케이션 아키텍처와 AWS 서비스를 활용하여 프로세스를 단순화하는 한편 특정 시점의 데이터 복구를 허용합니다. 지속적인 개발 및 배포 모델을 사용함으로써, 서비스의 연속성은 애플리케이션 서버가 아닌 환경 템플릿, 소스코드 및 데이터베이스에 종속됩니다. 환경 템플릿과 소스코드는 Amazon S3 에 저장됩니다. 파일 버전관리는 모든 이전 버전의 소스코드가 유지되도록 하며, Amazon S3 권한은 개발자가 이전 버전의 템플릿 및 소스코드를 삭제할 권한이 없도록 합니다. 데이터 주기 규칙은 데이터를 장기 보존 아카이브 저장소로 자동 이전하여 고객의 법률 및 규정 준수 요구사항을 충족합니다.

Amazon RDS 는 자동 프로세스를 사용하여 데이터베이스를 저장하고 백업합니다. 이는일일 백업을 필요로 하며, 변경 로그와 함께 보관되어야 합니다. 이러한 구성요소를 함께 사용하면 저렴한 비용으로 자동 백업을 수행할 수 있으므로 몇 분 내에 특정 시점으로 환경을 신속하게 복원할 수 있습니다.

6 결론

싱가포르 통화청은 공용 클라우드 이용을 도입하기 위하여 기존의 장애물을 제거하였습니다. 클라우드 도입을 돕기 위하여, 싱가포르 은행연합회는 아웃소싱 및 클라우드 도입에 관한 싱가포르 통화청의 지침을 충족할 수 있도록 고안된 몇 가지 주요 제어를 식별해 내었습니다. AWS 플랫폼에서 제공되는 서비스 구성이 매우 많다는 점을 고려하면, 많은 기관들은 AWS 구현이 ABS 주요 제어 지침을 충족하는지에 관하여 의문을 가질 수 있습니다. 액센추어의 AWS 보안 프레임워크와 그것을 싱가포르 통화청 지침과 연계시키는 방법은 ABS 주요 제어를 다루면서 MAS 요구사항을 준수하기 위하여 AWS 서비스를 설계 및 구성하는 규범적 방법을 제공함으로써 그러한 불확실성을 제거합니다.

액센추어의 AWS 보안 프레임워크는 올바른 AWS 서비스 및 플랫폼을 구현하기 위한 간단한 규범적 방법을 설명하며, 이를 통해 어떤 기관이라도 아웃소싱 및 클라우드 도입에 있어 싱가포르 통화청의 요건을 충족할 수 있을 것입니다. ABS 가 기술한 각각의 주요 제어에 대하여, 액센추어의 AWS 프레임워크는 적용될 수 있는 AWS 서비스와 ABS 가 나열한 주요 제어를 충족하기 위해서 어떻게 배치되어야 하는지를 개괄합니다.

본 프레임워크는 금융서비스 부문에게 기관 내 모든 작업을 지원하는 안전하고 복원력 있는 AWS 플랫폼을 구축함으로써, 클라우드 기반 개발 및 보안 기술의 도입하면서도 데이터를 안전하게 관리할 수 있다는 신뢰를 제공합니다.

6.1 도움을 주신 분들

Campbell Abbey – 액센추어 아마존 사업그룹 APAC 대표(Accenture Amazon Business Group APAC lead) @ Accenture

Gary Park – AWS 액센추어 보안 아키텍트(AWS Accenture Security Architect) @ Accenture

Umesh Thakkar – 응용기술 및 아키텍처(Advance Technology and Architecture) @ Accenture

Chris Scott- 액센추어 아마존 사업그룹 SA(Accenture Amazon Business Group SA) @ Accenture