**클라우드 사용계획서**

|  |  |
| --- | --- |
| 프로젝트명 | 클라우드 기반 SIEM(통합 보안 관제 솔루션) |
| 프로젝트 팀명 | 3조 |
| 프로젝트 팀장 | 김한진 |
| 프로젝트 팀원 | 공경선, 금소영, 김동관, 김범, 서용석, 최병섭 |

**텍스트, 클립아트이(가) 표시된 사진

자동 생성된 설명**

**제/개정 이력**

|  |  |  |  |
| --- | --- | --- | --- |
| **버젼/릴리스** | **작성일자** | **작성자** | **개요** |
| 1.0 | 2021.04.28 | 전영재 | 클라우드 사용계획서 초안 작성 |
| 2.0 | 2021.04.30 | 김한진 | 클라우드 사용계획서 작성 |
| 2.1 | 2021.4.30 | 서용석 | 클라우드 사용계획서 작성 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**목 차**

[1. 개요 4](#_Toc70515291)

[1.1. 목적 4](#_Toc70515292)

[1.2. 시스템명 4](#_Toc70515293)

[1.3. 사용기간 4](#_Toc70515294)

[1.4. 배경 및 목적 4](#_Toc70515295)

[2. 클라우드 구성 5](#_Toc70515296)

[2.1. 기본 사항 5](#_Toc70515297)

[2.2. 구성도 5](#_Toc70515298)

[2.3. 구성 내용 5](#_Toc70515299)

[2.4. 예상 비용 6](#_Toc70515300)

1. 개요

## 목적

본 문서는 클라우드 융합 최종 프로젝트에서 사용할 클라우드 시스템에 대한 사용 계획서로 제한된 자원을 효율적으로 사용하고, 나아가 본 프로젝트를 원활하게 진행하기 위한 클라우드 시스템 구축을 위한 기본 설계 문서로 활용하기 위함

## 시스템명

클라우드 기반 SIEM(통합 보안 관제 솔루션)

## 사용기간

2021년 04월 28일 ~ 2021년 06월 30일

## 배경 및 목적

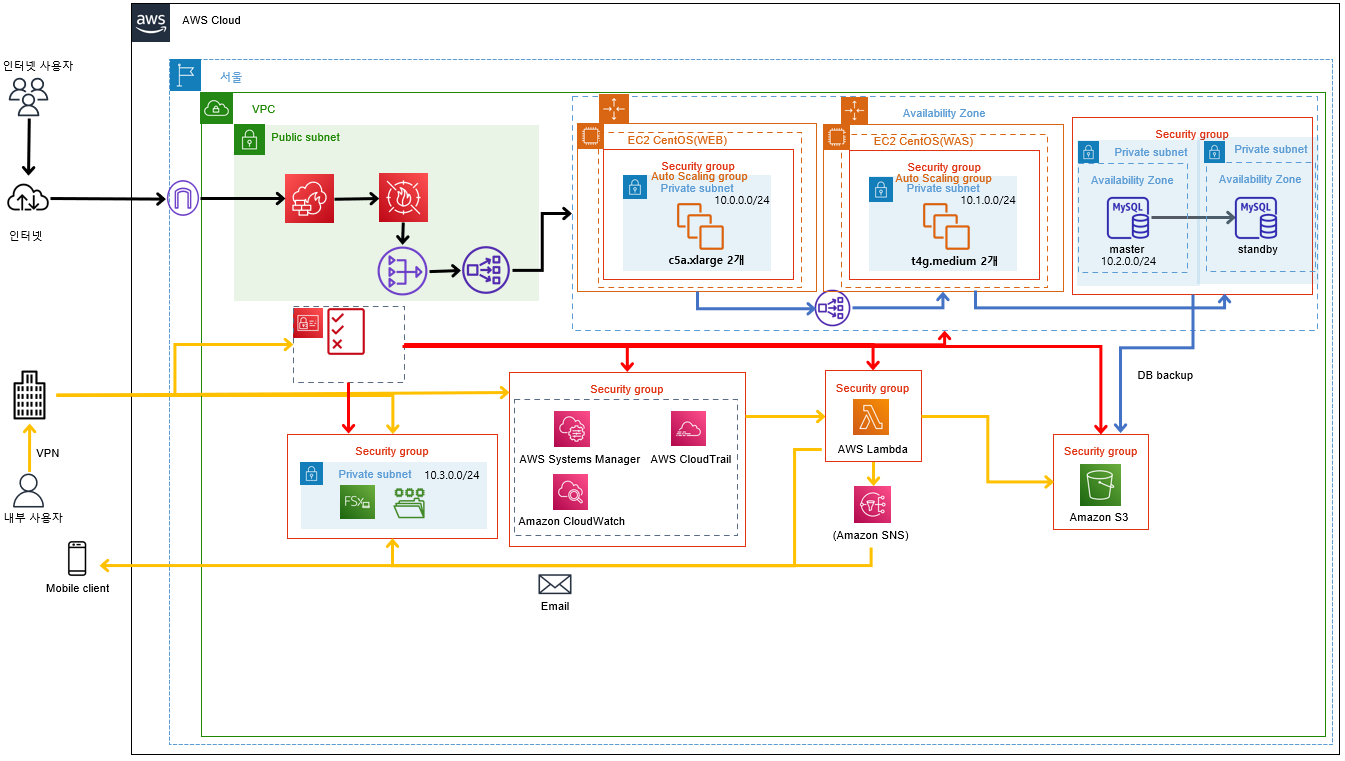
현재 많은 금융권 회사들이 자사의 멤버쉽 서비스 등을 기존의 온프레미스 환경에서 클라우드 시스템으로 서비스들을 마이그레이션 하고 있다. 하지만 클라우드 환경에서의 보안 문제는 쉽게 해결하지 못하고 있는 것이 현실이다. 그리하여 우리는 클라우드 환경에서 가상의 은행을 만들고 클라우드 기반의 보안 이벤트 탐지와 분석 등을 할 수 있는 클라우드 기반 SIEM을 개발해 보기로 하였다.

1. 클라우드 구성

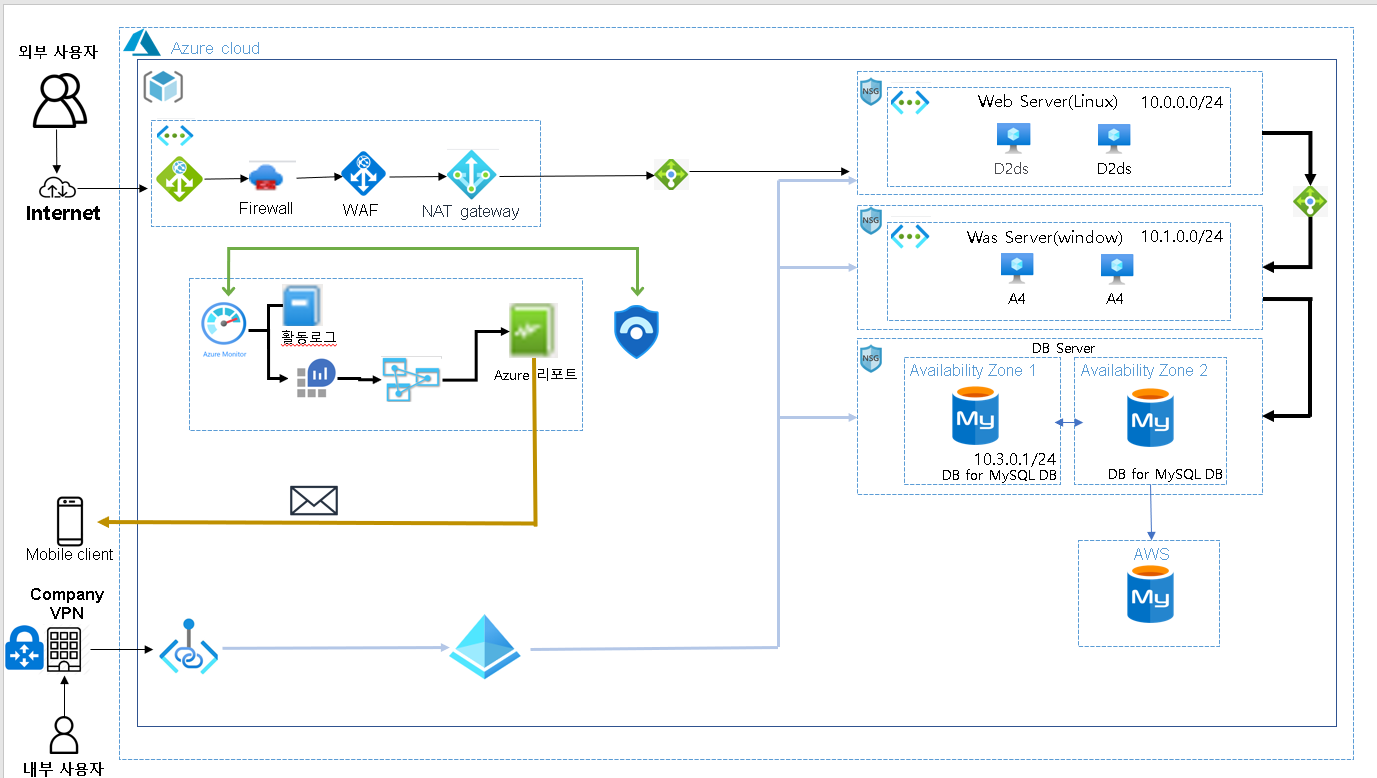
## 기본 사항

| **Region** | **Service** | **VPC(VNets)** | **일일 사용 시간** | **총 사용 일수** |
| --- | --- | --- | --- | --- |
| 서울, 부산 | 33개 | 2개 | 4시간 | 30일 |

## AWS 구성도



## Azure 구성도



## 사용 서비스

| **서비스명** | **수량** | **용도** |
| --- | --- | --- |
| Amazon EC2 | 4 | * 웹 서버로 외부망 접근(80 포트) 사용 * WAS 서버 2개, WEB 서버 2개 사용 * 사용가 증가시 Auto Scaling 으로 서버 자동 증설 |
| Amazon RDS for MySQL | 1 | * 고객 정보 저장 및 관리 * Mult-AZ로 고가용성 확보 * 가상의 은행임으로 MySQL을 기반으로 한다. |
| Amazon Simple Storage Service(S3) | 1 | * Lambda 서비스를 위한 스토리지 * 데이터베이스 데이터 백업 * Lambda로 자동화하여 생성된 보고서 및 보안 이벤트 로그등을 백업 |
| Elastic Load Balancing | 2 | * WEB 서버의 부하 분산 * WAS 서버의 부하 분산 |
| AWS Web Application Firewall(WAF) | 1 | * 웹 애플리케이션의 보안을 탐지 및 차단 * 로그 데이터들은 Lambda로 보내어 Lambda에서 자동으로 보고서를 작성하게 한다. |
| Amazon FSx for Lustre | 1 | * 파일 서버로 회사 내의 직원들이 파일을 업로드하고 다운받을 수 있게 한다. * Lambda에서 자동으로 생성한 보고서를 저장한다. |
| AWS CloudTrail | 1 | * AWS 계정의 거버넌스, 규정 준수, 운영 감사 및 위험 감사를 지원하는 서비스 * AWS 인프라의 작업과 관련된 계정 활동을 로깅하고 연속적으로 모니터링한다. |
| AWS Systems Manager | 1 | * AWS의 인프라에 대한 가시성과 제어 기능을 제공한다. * 여러 AWS 서비스의 운영 데이터를 볼 수 있다. * AWS 리소스 전체에서 운영 작업을 자동화할 수 있다. |
| Amazon Virtual Private Cloud(VPC) | 1 | * Aws 클라우드의 논리적으로 격리된 섹션을 프로비저닝하여 정의한 가상 네트워크를 통해 그 섹션에서 AWS 리소스를 실행한다. |
| AWS NAT | 1 | * 외부망에서 사설망 내부로 접근이 불가능하다. * 보안상으로 보면 프로토콜을 숨겨줄 수 있다. |
| Amazon SNS | 1 | * 애플리케이션 간 및 애플리케이션과 사용자 간 통신 모두를 위한 완전관리형 메시징 서비스 |
| Amazon Lambda | 1 | * 서버 없이 코드를 실행할 수 있기에 SIEM을 구축한다. * 주기적으로 감사 보고서를 생성하고 이상 탐지가 있을 경우 자동 조치 후 보고서를 생성한다. * Amazon SNS와 연동하여 보고서들을 메일로 관리자에게 보낸다. |
| AWS VPN | 1 | * 회사에서 AWS 내부 시스템에 접근할 때 사용한다. |

## 예상 비용

| **Region** | **Service 명 (유형)** | **수량** | **일사용** | **총사용** | **예상비용(약)** | **비고** |
| --- | --- | --- | --- | --- | --- | --- |
| 서울 | Amazon EC2  (t4g. medium) | 2 | 4H | 122H | 10.15 USD | vCPU: 2, MEM: 4G  SSD: 40GB, OS: Linux |
| 서울 | Amazon EC2  (c5a.xlarge) | 2 | 4H | 122H | 51.09 USD | vCPU: 4, MEM: 8G  SSD: 40GB, OS: Linux |
| 서울 | Amazon RDS  (MySQL) | 1 | 4H | 122H | 120 USD | vCPU: 4, MEM: 16G  SSD: 100GB |
| 서울 | Amazon S3 | 1 | 4H | 122H | 2.50 USD | S3 Standard : 100GB |
| 서울 | Elastic Load Balancing | 2 | 4H | 122H | 41.61 USD | Network Load  Balancer |
| 서울 | AWS Web Application Firewall (WAF) | 1 | 4H | 122H | 9.60 USD | 기본 값으로 측정하여  정확한 비용은 불확실 |
| 서울 | Amazon FSx for Lustre | 1 | 4H | 122H | 83.792 USD | Throughput Capacity : 50MBps/TiB  SSD : 1.2TB  Backup Storage : 1TB |
| 서울 | AWS CloudTrail | 1 | 24H | 730H | 0 USD | 기본 값으로 측정하여  정확한 비용은 불확실 |
| 서울 | AWS Systems Manager | 1 | 24H | 730H | 35.32 USD | 기본 값으로 측정하여  정확한 비용은 불확실 |
| 서울 | AWS Lambda | 1 | 4 | 122H | 0 USD | 현재 정확한 값을 측정할 수 없어 불확실 |
| 서울 | Amazon SNS | 1 | 24H | 730H | 21.60 USD | 기본 값으로 측정하여  정확한 비용은 불확실 |
| 서울 | Amazon VPC(NAT) | 1 | 4 | 122H | 86.14 USD | NAT 게이트웨이당 처리된 데이터 :  1GB per hour |
| 서울 | Amazon VPC(VPN) | 1 | 4 | 122H | 791.35 USD | Site-to-Site VPN 연결 수 : 100 |

* 상기 비용은 대략적인 값이나 기본값 1을 넣어서 측정했습니다.
* 가상의 은행이기에 비용을 최대한 저렴하게 하여 개발할 예정입니다.
* 향후 새로운 상품이나 서비스를 추가할 예정입니다.
* 서비스 개발 및 테스트에 들어갈 값이 늘어나게되면 가격이 상승할 수 있습니다.
* 현재 대략적인 클라우드 서비스 사용에 대한 비용 계산 결과 총 약 2082.51 USD로

한화 약 231만 6792.38원 입니다.

## 사용 서비스

| **서비스명** | **수량** | **용도** |
| --- | --- | --- |
| 가상머신 | 4 | * 웹 서버로 외부망 접근(22, 80, 443, 3389 포트) * 사용가 증가시 서버 추가 증설 |
| 가상 네트워크 | 4 | * 가상 네트워크 영역을 만듭니다. |
| 어플리케이션 게이트웨이 | 1 | * 웹 애플리케이션에 대한 트래픽을 관리할 수 있도록 하는 웹 트래픽 부하 분산 장치 |
| Load Balancer | 2 | * 어플리케이션에 고가용성 및 네트워크 성능 제공 |
| Azure Firewall | 1 | * Azure Virtual Network 리소스를 보호하는 관리되는 클라우드 기반 네트워크 보안 서비스 |
| Azure WAF | 1 | * 웹앱을 위한 강력하 보호를 제공하는 클라우드 네이티브 WAF서비스 |
| Azure NAT gateway | 1 | * 가상 네트워크에 있는 하나 이상의 서브넷에 대한 아웃바운드 인터넷 연결을 제공 |
| Azure Database for mysql | 1 | * 앱 개발자용 관리되는 MySQL 데이터베이스 |
| Azure monitor | 1 | * 클라우드 및 온-프레미스 환경에서 원격 분석의 수집, 분석 및 작업에 대한 포괄적인 솔루션을 제공 |
| Azure private link | 1 | * Azure 플랫폼에서 호스트되는 서비스에 대한 프라이빗 액세스, Microsoft 네트워크에 데이터 보관 |
| Azure sentinel | 1 | * 클라우드 네이티브 SIEM 및 인텔리전트 보안 분석을 적용하여 엔터프라이즈 보호 |

## 예상 비용

| **Region** | **Service 명 (유형)** | **수량** | **일사용** | **총사용** | **예상비용** | **비고** |
| --- | --- | --- | --- | --- | --- | --- |
| 서울 | 가상 네트워크 | 4 | 4H | 730H | 8,997USD | Vnet |
| 서울 | Azure 방화벽 | 1 | 4H | 730H | 42,475USD | Firewall 서비스 |
| 서울 | 부하 균형 | 2 | 4H | 730H | 52,296USD | Load Balancer |
| 서울 | 가상머신 | 2 | 4H | 730H | 1282USD | 2 vCPU, 8 GB RAM, 75 GB 임시 저장 |
| 서울 | 가상머신 | 2 | 4H | 730H | 3000USD | 4 vCPUs, 8 GB RAM, 40 GB 임시 저장 |
| 호주 | Azure 활성 디렉토리 | 1 | 4H | 730H | 71,527USD | default |
| 서울 | MySQL용 Azure 데이터베이스 | 1 | 4H | 730H | 17,328USD | D2 v4, 2 vCore |
| 서울 | Azure 개인 링크 | 1 | 4H | 730H | 2,294USD | default |
| 서울 | Azure 함수 | 1 | - | - | 0USD | default |
| 서울 | 모니터 | 1 | - | - | 11,246USD | 응용 프로그램 인사이트 |
| 서울 | 모니터 | 1 | - | - | 38,474USD | 로그분석 |
| 서울 | 모니터 | 1 | - | - | 12,607USD | 경고 |
| 서울 | Azure 센티넬 | 1 | - | - | 178,538USD | default |

* 상기 비용은 대략적인 값이나 기본값 1을 넣어서 측정했습니다.
* 가상의 은행이기에 비용을 최대한 저렴하게 하여 개발할 예정입니다.
* 향후 새로운 상품이나 서비스를 추가할 예정입니다.
* 서비스 개발 및 테스트에 들어갈 값이 늘어나게되면 가격이 상승할 수 있습니다.
* 현재 대략적인 클라우드 서비스 사용에 대한 비용 계산 결과 총 약 391.53USD로

한화 약 440,331.91원입니다.