**메가존클라우드 채용확정형과정 1기 세미프로젝트2 보고서**





| **팀장** | **권승규** |
| --- | --- |

| **팀원** | **박기범** |
| --- | --- |

| **팀원** | **김수빈** |
| --- | --- |

| **팀원** | **편창은** |
| --- | --- |

**2조**



**목차**

[**1.개**](#_auspkemnn1cz)**요 ······················································** [**3**](#_auspkemnn1cz)

[**2. 프로젝트 요구사항**](#_nriyv36ubl8) **··································· 4**

[**2-1. AWS Cloud**](#_uqrd1um3dw13) **········································· 4**

[**2-2. GCP Cloud**](#_78vm5wytpl1f) **······································· 6**

[**2-3. Azure**](#_aetg0ta4m7rd) **······································· 6**

[**2-4. Alibaba**](#_2gx2vujtrg6c) **······································· 7**

[**2-5. OpenStack**](#_oj5efx53ui07) **······································· 7**

[**2-6. ESXi**](#_ioeerxa0gt3s) **······································· 8**

[**3. 기능 요구사항**](#_cf1gd0vyroa9) **·········································· 9**

[**4. 시스템 설계**](#_9j706bjktbts) **············································· 17**

[**5. 기능구현**](#_nq2yzshr305d) **················································· 18**

[**6. 결과**](#_upe4pu8p49fz) **······················································· 19**

[**7. 특이사항**](#_z6z71siejjt8) **················································· 20**

[**8. 타임라인**](#_cl5jwoqrb6y1) **················································· 21**

[**9. 참고문헌**](#_mnzu0igb32og) **················································· 22**

**1.개요**

| 프로젝트 분야 | 하이브리드 클라우드 | 직무 분야 | SA | |
| --- | --- | --- | --- | --- |
| 프로젝트 명칭 | 글로벌 인재 영입을 위한 채용프로세스 및 웹사이트 구축 | | | |
| 프로젝트 목적 | * 온 프레미스 환경과 멀티 클라우드 환경을 규합한 하이브리드 클라우드 환경을 구축할 수 있어야 함. * 라우팅 기반을 통해 트래픽 분산을 할 수 있어야함. * 서버의 문제가 발생할 시 알람을 받으며, 이에 대응할 수 있어야함. * 보안기반 접근을 할 수 있어야함. | | | |
| 프로젝트 기간 | * 2022.06.22~06.28 | | | |
| 참여인원 및 역할 | * 권승규 : 팀장, SA, Route 53, ALB, CloudFront * 김수빈 : SA, S3, OpenStack, AWS VPN, EFS * 박기범 : SA, 멀티 클라우드 웹서버, HAproxy, azure,gcp vpn,   CloudWatch & sns * 편창은 : SA, Project Manager, ESXi, File Gateway | | | |
| 요구사항 | * 온프레미스 내부 데이터 보존 필요. 글로벌 채용 시스템 구축 필요함. 태풍으로 한국 리전 블랙아웃 발생에 대한 대비 필요. 파일 및 사진으로 효율적인 웹 사이트 구축. 한국 지역 지원자 폭등으로 트래픽 과부하. 사용자 편의와 보안을 고려 필요. | | | |
| 개발 내용 | * ESXi   -DB 센터의 기능과 S3 FGW기능을 담당함.   * OpenStack   - WEB Server의 메인 DB기능을 담당하며 EFS를 통해 파일공유를 함.   * AWS * 내부 Region간 장애조치를 할 수 있어야함. * WEB Server장애조치를 할 수 있어야함. * 효율적인 파일스토리지 업로드가 가능해야함. * 타 CLOUD Service와 연동되어야함. * GCP, Azure * AWS와 연동되어 WEB Server로서의 기능을 해야함. * OpenStack과 VPN 통신을 할 수 있어야 함. * AWS S3의 파일을 자유롭게 업/다운로드 할 수 있어야 함. * Alibaba * AWS와 연동되어 WEB Server로서의 기능을 해야함. * 내부 Cloud에 DB가 설정되어 있어야함. | | | |
| 구현 및 개발 툴 | VMware, Centos7, ESXi, OpenStack, AWS, Azure, GCP, Alibaba | | | |

# **2. 프로젝트 요구사항**

# **2-1. AWS Cloud**

| VPC | * 서울, 도쿄 각각에 1개의 VPC가 있어야함. * VPC 내부에는 각각 1개의 Public Subnet이 있어야함. * VPC 내부에는 각각 1개의 ALB가 있어야함. * 서울 VPC내부에는 2개의 EC2가 있어야함. |
| --- | --- |
| EC2 | * 모든 EC2는 스냅샷이 있어 복원성을 띌 수 있어야함. * 1개의 EC2는 반드시 HAproxy기능을 해야함. * 1개의 EC2는 반드시 WEB Server로써의 기능을 해야함. * WEB Server는 반드시 VPN을 통해서 OpenStack과 연동되어야함. * 반드시 보안그룹을 생성해야함. * 보안그룹명 : SG-WEB   - 22, 80포트만 접근 가능해야함.   * 단 PING통신을 위해 ICMP는 열려있음 * 리소스 자원의 최소값은 기능 요구사항 참조 |
| ALB | * SSL인증서를 통해 HTTPS(443번 포트)로 접근할 수 있어야함. * 타겟그룹을 생성해야함. * HTTP 상태검사를 해야하며, 5연속 상태 검사 성공시 healthy, 2연속 상태 검사 실패시 unhealthy로 판단. 제한시간은 5초이며 간격은 30초 * 반드시 보안그룹을 생성해야함. * 보안그룹명 : SG-ELB   - 22, 443포트만 접근 가능해야함.   * 단 PING통신을 위해 ICMP는 열려있음 |
| VPN | * 내부 DB서버와 프라이빗 통신을 할 수 있어야함. * 외부 cloud Server와 프라이빗 통신을 할 수 있어야함. |
| EFS | * ESXi와 연동되어 파일스토리지 기능을 활용할 수 있어야 함. * 리소스 자원의 최소값은 기능 요구사항 참조 |
| SG | * 기능별 보안 계획 구축 필요함. * SG-ALB는 22, 443번 포트로의 접근을 허용해야함 * SG-WEB은 22, 80번 포트로의 접근을 허용해야함. * ICMP 는 Ping통신을 위해 개방 되어있어야함. |
| SNS | * 관리자 계정(1개)와 연동되어 있어야함. * 세부 정보 : 표준 * 주제 소유자만 구독과 알림을 받아야함. * 전송 재시도 정책은 표준(기본)을 활용해야함. |
| CloudFront | * WEB Server 운용에 필요한 파일(css, js, IMG 등)을 배포할 수 있어야함. |
| CloudWatch | * 서울리전의 WEBServer와 연동되어 있어야함. * cpu 가동률이 70%이상이 될 경우 반드시 SNS서비스와 연동되어 관리자에게 메일이 발송되어야 함. * 인스턴스 상태 검사 실패시 재부팅 후 반드시 SNS서비스와 연동되어 관리자에게 메일이 발송되어야 함. |
| S3 | * ESXi와 연동되어 있어야함. * 3개의 S3가 있어야하며 각각 S3 log, 이와 연동되는 S3-Glacier, 그리고 S3 정적 객체 관리로 지정되어야함. * S3 LOG는 연동된 서비스의 log를 기록함. * 수명주기정책(30일)을 바탕으로 log는 SG-Glacier로 이동되어야함. * S3 정적 객체 관리를 바탕으로 정적 자료를 CloudFront배포할 수 있어야 함. |
| IAM | * Root계정을 활용해서는 안되며 사용자 계정으로 접근해야 함. * 총 N개의 계정과 N개의 그룹이 있어야 함. |
| ACM | * HTTPS접근을 위해 SSL인증서를 발급받아야 함. |
| Route53 | * 사용자가 접근시 도메인으로 접근할 수 있도록 지원해야 함. * 장애 조치기반 라우팅을 사용해 서울 리전에 장애 발생시 도쿄 리전으로 연결될 수 있어야 함. |

## 

## **2-2. GCP Cloud**

| Region | * 미 오리건주에 1개의 Region을 지정해야함. |
| --- | --- |
| Zone | * 1개 혹은 그 이상의 Zone을 활용해야함. |
| Firewall | * 보안정책을 수립해 야함 * SG-WEB는 22, 80번 포트로의 접근을 허용해야함 |
| Cloud VPN | * OpenStack의 DB Server와 반드시 VPN통신이 되어야함. |
| WEB Server | * AWS CloudFront를 통해 정적 파일을 받을 수 있어야함. * HAproxy를 통해 분산받은 트레픽을 수신할 수 있어야 함. * AWS EFS를 통해 파일공유가 가능해야함. |

## **2-3. Azure**

| 리소스 그룹 | * 반드시 최소 1개이상의 리소스 그룹을 작성해야함. |
| --- | --- |
| Firewall | * 보안정책을 수립해 야함 * SG-WEB는 22, 80번 포트로의 접근을 허용해야함 |
| 리소스 | * AWS CloudFront를 통해 정적 파일을 받을 수 있어야함. * HAproxy를 통해 분산받은 트레픽을 수신할 수 있어야 함. * AWS EFS를 통해 파일공유가 가능해야함. |
| Cloud VPN | * OpenStack의 DB Server와 반드시 VPN통신이 되어야함. |

## **2-4. Alibaba**

| 리전 | * 반드시 최소 1개 이상의 리전을 작성해야함. |
| --- | --- |
| Firewall | * 보안정책을 수립해 야함 * SG-WEB는 22, 80번 포트로의 접근을 허용해야함 |
| 리소스 | * AWS CloudFront를 통해 정적 파일을 받을 수 있어야함. * HAproxy를 통해 분산받은 트레픽을 수신할 수 있어야 함. * 리소스 자원의 최소값은 기능요구사항 참조 |

## **2-5. OpenStack**

| 하드웨어 스펙 | * OS : CentOS 8-strime * SSD : 128GB(동적 생성) * RAM : 16GB * CPU : 4CORE(가상화 가능) * NETWORK : Bridge |
| --- | --- |
| 내부  DB Server 스펙 | * Centos 7 * SSD : 128 GB(동적 확장 가능) * RAM : 12GB * CPU : 4CORE(가상화 가능) |
| NETWORK | * 내부 : DHCP 로 IP 자동 할당 * 외부 : Pool IP 범위 직접 할당 |
| 계정 | * ADMIN : root * PASSWORD : Kosa0401! |
| VPN | * 퍼블릭 클라우드와 VPN연결을 통해 서로 통신이 가능함 |

## 

## **2-6. ESXi**

| 메인 스펙 | * CPU : 4CORE * RAM : 16GB * SSD : 128(동적 확장 가능) |
| --- | --- |
| 내부  Server 스펙 | * CPU : 4CORE * RAM : 12GB * SSD : 80GB(씬 프로비저닝) * Cache 150GB(씬 프로비저닝) |
| AWS File Storage Gateway | * 내부 Server구축시 반드시 OVA파일을 AWS에서 배포한 File Storage Gateway를 통해서 구축해야 함. * S3 2개와 연동이 되어야 함. * S3 Log와 연동되어 log파일을 전송할 수 있어야 함. * S3 객체관리를 통해 같은 지역 내부의 EC2와 파일 통신을 할 수 있어야 함. |

# 

# **3. 기능 요구사항**

| **Route53-01** | 전통적인 DNS 서버 및 CNAME을 활용한 도메인 네임 간 매핑 |
| --- | --- |
| **설명** | 도메인 네임 및 Health-Check 기능을 통한 웹 서버 접근 트래픽 제어 |
| **행위자** | AWS |
| **선행조건** | 1. 별도의 사용가능한 도메인(가비아)이 있어야함.    1. 없을경우 AWS에서 구매 가능 2. 모든 벤더사의 WEB Server가 구축되어 있어야함. 3. ACM이 활성화 되어 있어야함. |
| **기본동작** | 1. 사용자는 지정된 도메인을 입력함. 2. DNS 서버(가비아)는 Route 53과 ACM을 참조하여 AWS로 접근함. 3. Route 53의 단순 라우팅 기능으로 서울 리전으로 접근함. |
| **추가동작** | 1. 3이 정상적으로 작동되지 않을 시 Route 53-02 장애조치 |

| **Route53-02** | 장애조치 라우팅 |
| --- | --- |
| **설명** | 리전 장애 발생 시 상태 검사를 통해 Active -> Passive 리전으로 라우팅 |
| **행위자** | AWS |
| **선행조건** | 1. Route53-01과 동일 2. Route53-01의 3이 실행되지 않음 |
| **기본동작** | 1. 헬스 체크를 통해 서울 리전의 웹 서버 구동 여부 확인함. 2. 패시브 상태인 도쿄 리전으로 트레픽을 재전송함. |

| **ACM-01** | SSL 보안 기반 HTTPS접근 |
| --- | --- |
| **설명** | HTTPS 프로토콜을 이용하여 트래픽 전송에 대한 보안성 강화 |
| **행위자** | AWS |
| **선행조건** | Route 53에 도메인이 등록되어 있어야 함 |
| **기본동작** | 도메인 접근시 ACM에서 발부된 SSL이 참조되어 진행됨. |
| **추가동작** | DNS 검증을 통해 자동으로 DNS 검증 인증서 갱신 |

| **EC2-01** | HAproxy용 EC2 |
| --- | --- |
| **설명** | AWS CLOUD환경의 PC가 1대가 구동되어 있으며, 이 PC는 HAproxy의 기능을 함. |
| **행위자** | AWS |
| **선행조건** | 1. ALB를 통해 트래픽 수신 2. AWS를 제외한 타 퍼블릭 클라우드에 웹 서버 구축 |
| **기본동작** | 1. 스팩   t2.micro  cpu : 1  ram : 1  network performance : row  subnet : A  SSD : 8GB(EBS)  보안 그룹 : SG-ELB  22, 80, 443번 포트 및 ICMP만 개방   1. Route53을 통해 접근한 트래픽 경로를 분석함. 2. 분석된 경로를 기반으로 지정된 WEB Server로 전송됨.   3-1. / : aws seoul region WEB Server  3-2. /eu : Azure europe region london WEB Server  3-3. /us : gpc oregon region WEB Server  3-4. /ch 헤더 : alibaba hong kong region WEB Server   1. 3에서 각 서버 장애시 AWS로 라우팅됨. 2. 해당 인스턴스 장애 발생시 도쿄 리전의 HAproxy로 연결됨. |

| **EC2-02** | WEB Server 서비스 |
| --- | --- |
| **설명** | AWS, AZURE, GCP, ALIBABA 각각의 퍼블릭 클라우드에 위치 |
| **행위자** | AWS, AZURE, GCP, ALIBABA |
| **선행조건** | 1. AWS의 서울 및 도쿄 리전에 HAProxy 기능 구현 |
| **기본동작** | 1. 스팩   t2.micro(벤더별 상동 => 최소비용의 기능을 사용)  cpu : 1  ram : 1  network performance : row  subnet : A  SSD : 8GB(EBS)  보안 그룹 : SG-ELB  22, 80 포트 및 ICMP만 개방   1. SG-ALB 를 거쳐 ALB로 접근함. 2. ALB는 HAproxy EC2로 트래픽을 전송함. 3. HAproxy는 header를 기반으로 해당 WEBServer로 트래픽 전송됨. |

| **S3-01** | S3 log 서비스 |
| --- | --- |
| **설명** | S3 파일 스토리지 클래스의 Glacier 를 사용함으로써 비용 효율성 증대 |
| **행위자** | AWS |
| **선행조건** | 온프레미스와 File Gateway 연결이 되어있어야함 |
| **기본동작** | 1. 로그 파일 용량이 큰 S3 의 특정파일을 스토리지 클래스에 따라 이동 2. 기본 보관 일수와 조건을 확인 3. 수명 주기 정책을 통해 일정시간이 지나면 Glacier로 파일을 이동 |

| **S3-02** | S3 정적 파일 서비스 |
| --- | --- |
| **설명** | S3에 저장된 정적파일이 WEB Server에 배포됨 |
| **행위자** | AWS |
| **선행조건** | 1. S3 정적 서비스가 연동 되어 있어야 함. 2. 모든 벤더사의 WEB Server가 CloudFronte와 연동 되어 있어야 함. |
| **기본동작** | File Gateway를 통해 정적 파일을 S3로 업로드 |

| **CloudFront-01** | 글로벌 CDN서비스 |
| --- | --- |
| **설명** | S3와 연동된 Cloudfront를 통해 WEB Server를 배포 |
| **행위자** | AWS |
| **선행조건** | 1. S3-02가 설정되어 있어야 함. 2. CF 의 도메인 네임을 Route 53의 호스팅 영역에 등록됨. |
| **기본동작** | 사용자 접속 시 근접한 엣지 로케이션을 통해 콘텐츠 배포 |

| **AWS VPN-01** | Site to Site VPN서비스 |
| --- | --- |
| **설명** | 보안이 강화된 프라이빗한 네트워크 연결로 데이터 이동 |
| **행위자** | AWS |
| **선행조건** | 고객게이트웨이와 가상프라이빗 게이트웨이가 설정되어있어야함  터널링을 위한 정보가 필요함 (리버스완 및 오픈스완의 플랫폼을 사용) |
| **기본동작** | 1. 온프레미스 ( OpenStack) 구축 및 VPN 명령어 실행  2. AWS 내 고객 게이트웨이, 가상 프라이빗 게이트웨이 설정   1. Site to Site VPN 생성 및 연결 2. 온프레미스와 AWS 라우터 설정 3. 각각 IP 주소로 네트워크 통신 확인 |

| **AWS EFS-01** | NFS를 통한 파일 공유 서비스 |
| --- | --- |
| **설명** | AWS 의 파일 공유시스템으로 온프레미스와 연결하여 다양한 서버들이 파일 스토리지에 접근하여 데이터를 가져올수 있음 |
| **행위자** | AWS |
| **선행조건** | VPN 으로 기본연결 구축, EFS 마운트 필요 |
| **기본동작** | 1. 오픈스택과 AWS VPN 으로 연결하여 네트워크 상태 확인 2. EFS IP 마운트로 온프레미스 파일 전송 3. EC2 마운트 저장소에 파일 내려받기 |

| **AWS Storage GW-01** | File storage Gateway 서비스 |
| --- | --- |
| **설명** | 온프레미스의 데이터를 비교적 빠르고 안전하게 가져올수 있는 서비스 |
| **행위자** | AWS |
| **선행조건** | Host PC의 OS 구분 필요.(Windows, Linux 등) |
| **기본동작** | 1. 파일공유 설정 2. 윈도우 제어판의 NFS 용 서비스 설정 체크 3. 서버 파일 명령어로 윈도우에서 접근 |

| **Azure VPN-01** | Azure의 VPN 서비스 |
| --- | --- |
| **설명** | Azure와 온프레미스간 VPN통신 |
| **행위자** | Azure |
| **선행조건** | 온프레미스 구축 및 리버스완 설치 |
| **기본동작** | 1. Azure 가상 네트워크 생성 2. 가상 네트워크 게이트웨이 생성 3. 로컬 네트워크 게이트웨이 생성 4. 온프레미스 설정  * 리버스완 설정 * 내부 라우터 설정  1. VPN 연결 생성 2. 연결 확인 |

| **GCP VPN-01** | GCP VPN 서비스 |
| --- | --- |
| **설명** | GCP와 온프레미스간 VPN 통신 |
| **행위자** | GCP |
| **선행조건** | 온프레미스 구축 및 리버스완 설치 |
| **기본동작** | 1. GCP VPN 설정 2. 온프레미스 설정  * 리버스완 설정 * 라우터 설정  1. 연결 확인 |

| **온프레미스 라우팅-01** | 온프레미스 라우팅 테이블 설정 |
| --- | --- |
| **설명** | Azure, GCP가 온프레미스를 경유해 AWS의 EFS를 마운트하기 위함 |
| **행위자** | 온프레미스 |
| **선행조건** | AWS, Azure, GCP가 온프레미스와 연결되어있어야 함 |
| **기본동작** | 1. 라우팅 테이블 설정 2. 각 클라우드에서 AWS EFS의 IP로 마운트 |

| **SNS-01** | AWS SNS서비스 |
| --- | --- |
| **설명** | cloudwatch에서 경보가 발생하면 지정된 관리자에게 E-mail알람이 발생 |
| **행위자** | AWS |
| **선행조건** | 1. SNS 구독 서비스에 관리자 계정이 등록되어 있어야 함. 2. CloudWatch에 연동되어 있어야 함. |
| **기본동작** | 1.Cloudwatch에서 경보가 발생됨.  2.구독된 내용을 바탕으로 관리자에게 메일이 전송됨. |

| **CloudWatch-01** | CloudWatch 경보 발생 |
| --- | --- |
| **설명** | 등록된 EC2에 문제가 발생하면 경보를 발생시킨다. |
| **행위자** | AWS |
| **선행조건** | EC2 및 SNS-01이 활성화 되어 있어야함. |
| **기본동작** | 1. 지정된 EC2에 문제가 감지됨.  * 이때 문제는 CPU사용량이 50%를 넘었으며 이 상황이 5분 이상 지속되었음을 의미함.  1. SNS에 구독된 관리자에게 관련 내용에 대한 매일이 발송됨. |

| **CloudWatch-02** | CloudWatch 경보 발생 및 EC2 재부팅 |
| --- | --- |
| **설명** | 등록된 EC2에 문제가 발생하면 경보를 발생시키며 EC2를 재부팅한다. |
| **행위자** | AWS |
| **선행조건** | EC2 및 SNS 구독이 활성화 되어 있어야함. |
| **기본동작** | 1. 지정된 EC2에 문제가 감지됨.  * 이때 문제는 인스턴스 상태 검사 실패가 5분 이상 지속될 시  1. 자동으로 EC2가 재부팅됨. 2. 2와 동시에 SNS에 구독된 관리자에게 관련 내용에 대한 메일이 발송됨. |

# 

# 4. 시스템 설계

| **도안** |  |
| --- | --- |
| **설명** | 1. 사용자 접근 시 ACM 인증서를 참조하여 HTTPS 프로토콜 지원 2. Route 53을 통한 GSLB 3. HAproxy를 통한 경로기반 라우팅 4. VPN을 통해 퍼블릭 클라우드와 온프레미스간 연결 5. VPN을 통해 AWS EFS와 마운트 6. File Gateway를 통해 온프레미스와 AWS S3와 연결 7. Alibaba Cloud는 내부 DB(압살라)를 통해 WEB Server 지원 |

# 

# **5. 기능구현**

| **기능** | **구현** | **비고** |
| --- | --- | --- |
| Route 53 및 ACM | https://www.skk2022.shop/  HTTPS 프로토콜 지원  장애 조치 라우팅 정책  상태 검사  리전 간 fail-over를 지원 | https보안 접근(443번 포트)  3.xx.xx.xx/20이 아닌 Skk.2022로 접근 가능. |
| HAproxy기능 활용  (헤더기반 분산 접근) | Url 헤더 부분을 사용  리전 별로 구축된 웹 사이트 | /ch 중국 홍콩 리전  /eu 유럽 스페인 리전  /us 미국 지역 오레곤 리전  / 아시아 지역 한국 리전 |
| VPN 통신 | Cloud ⇔ On-Premise | Ping을 통해 통신 상태 확인  내부 주요 자료에 대한 보안 송/수신 가능. |
| Storage Gateway  (파일 시스템 연동) | FGW를 기반으로 S3파일 공유 | 정적 파일 업로드 및 활용 |
| EFS | 내부 WEB Server간 파일 공유 | EFS는 vpn통신을 기반으로 파일 공유 |
| AWS CloudWatch, SNS | CloudWatch 정상작동 확인  cpu 부하 모니터링 확인  웹 서버 작동상태 점검,  cloudwatch 알람 확인으로 문제 발생시 관리자가 직접 접근  이미지로 서버 재구축 | 최대부하 100%  => 정상 작동 테스트 |
| CloudFront | 콘텐츠의 오리진과 유저의 거리  => 엣지 로케이션을 활용 하여 신속한 콘텐츠 배포 | S3 버킷과 연결  => \* 서브 도메인으로 등록 |

# **6. 결과**

| **당면 과제** | **해결 방안** |
| --- | --- |
| 온프레미스 내부 데이터 보존 필요 | 온프레미스의 DB와 퍼블릭 클라우드를 연동  → 보안성 향상 |
| 글로벌 채용 시스템 구축 필요 | 리전 별 웹서버 + 언어 지원 글로벌 서비스 제공 |
| 태풍으로 한국 리전 블랙아웃 발생 | Route 53 장애 조치 라우팅을 활용  → 리전 별 FAIL OVER 지원 |
| 한국 지역 지원자 폭등으로 트래픽 과부하 | CloudWatch 및 SNS 를 통한 알람  → 기 생성된 이미지를 활용한 fail over 지원 |
| 파일 및 사진으로 효율적인 웹 사이트 구축 | 클라우드 파일 시스템 활용  → S3, EFS를 활용하여 자원 관리의 효율성 제고 |
| 사용자 편의와 보안을 고려한 웹사이트 | Cloudfront 및 ACM 인증서  → 웹 사이트 접속 속도 및 보안성 강화 |

# 

# 

# **7. 특이사항**

1. **Alibaba와 서울에 위치한 DB의 분할**

* 중국의 데이터보호법(제2조) 및 개인정보 보호법(3조 2항)에 의거
* 중국인의 개인정보는 중국내 DB 센터에 보관이 원칙

1. **복수 개의 퍼블릭 클라우드와 DB센터간 개별적 VPN 통신**

* 개별 퍼블릭 클라우드와 온-프레미스 환경 간 통신에 있어서의 보안성 확보
* EFS를 통해 복수 개의 서버에서 파일에 접근할 수 있는 환경 구축

# 

# **8. 타임라인**

# 

# 

# **9. 참고문헌**

* 메가존 기술 블로그 및 공식 사이트 : <https://www.megazone.com/blog/(https://www.megazone.com/)>
* Azure 공식 도큐멘트 : [https://docs.microsoft.com/ko-kr/azure/vpn-gateway/tutorial-site-to-site-porta](https://docs.microsoft.com/ko-kr/azure/vpn-gateway/tutorial-site-to-site-portal)
* GCP 공식 도큐멘트 : <https://cloud.google.com/network-connectivity/docs/vpn/deprecations/classic-vpn-deprecation?hl=ko>
* AWS 공식 도큐멘트 :

<https://docs.aws.amazon.com/>

* 메가존 클라우드 채용 확정형 과정(실무 심화), 이한기 저
* AWS Certified Solutions Architect STUDY GUIDE, 벤 페이퍼, 데이비드 클린턴 저

* 메가존 클라우드 채용확정형 과정 (실무 심화) 이한기 저
* 메가존 클라우드 채용확정형 과정 (실무 심화) 이한기 저
* 메가존 클라우드 채용확정형 과정 (실무 심화) 이한기 저
* AWS Certified Solutions Architect STUDY GUIDE, 벤 페이퍼, 데이비드 클린턴 저