INZENT

aws Qualified Software

MyData Proxy Server V1.0

Contents

1. Product Overview

이 문서에서는 이전에 AWS 를 사용해 본 적이 있고 AWS 서비스에 익숙하다고 가정합니다. AWS 를 처음 사용하는 경우 AWS 설명서(https://docs.aws.amazon.com/)를 참조하십시오. 다음 AWS 기술에도 익숙해야 합니다.

:

- ✓ Amazon VPC - Amazon Virtual Private Cloud(Amazon VPC) 서비스를 사용하면 정의한 가상 네트워크에서 AWS 서비스 및 기타 리소스를 시작할 수 있는 AWS 클라우드의 격리된 비공개 섹션을 프로비저닝할 수 있습니다. 고유한 IP 주소 범위 선택, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성을 포함하여 가상 네트워킹 환경을 완벽하게 제어할 수 있습니다.
- ✓ Amazon EC2 - Amazon Elastic Compute Cloud(Amazon EC2) 서비스를 사용하면 다양한 운영 체제에서 가상 머신 인스턴스를 시작할 수 있습니다. 기존 Amazon Machine Images(AMI)에서 선택하거나 고유한 가상 머신 이미지를 가져올 수 있습니다.
- ✓ Amazon EFS - Amazon Elastic File System (Amazon EFS)은 서버리스, set-and-forget 사용할 탄력적 파일 시스템 AWS 클라우드서비스 및 온프레미스 리소스. 애플리케이션을 중단하지 않고 온디맨드 방식으로 페타바이트 규모까지 확장되도록 구축되어, 사용자가 파일을 추가하고 제거할 때 자동으로 확장/축소되므로 데이터 증가에 맞춰 용량을 프로비저닝 및 관리할 필요가 없습니다. Amazon EFS 에는 파일 시스템을 빠르고 쉽게 만들고 구성할 수 있는 간단한 웹 서비스 인터페이스가 있습니다. 이 서비스에서 모든 파일 스토리지 인프라를 관리해 주므로 사용자는 복잡한 파일 시스템 구성을 배포, 패치 및 유지 보수하는데 따르는 복잡성에서 벗어날 수 있습니다.
- ✓ Amazon ELB - Amazon Elastic Load Balancing (Application Load Balancer) 서비스를 사용하면 둘 이상의 가용영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에

걸쳐 수신되는 트래픽을 자동으로 분산합니다. 등록된 대상의 상태를 모니터링하면서 상태가 양호한 대상으로만 트래픽을 라우팅합니다.

1.1 Introduction

MyData Proxy Server는 망 분리된 업무 환경에서 DMZ 구간에 위치하여 내부망에 있는 API GW, 업무 PC 등이 인터넷 서비스에 간접적으로 접속할 수 있게 해주는 응용 프로그램을 말합니다. MyData 데이터 수집 등의 목적으로 인터넷을 통해 데이터 수집 목적으로 OUT-BOUND 거래 시 활용되며, MyData 통신 규격에 맞는 mTLS 및 SSL 등을 지원합니다.

✓ MyData란 무엇인가?

데이터 3법이 통과되면서, "내 데이터의 주인은 나"라는 MyData 개념이 주목받고 있습니다. MyData 개념이 정립되면 소비자는 자신이 만들어낸 데이터의 주권을 행상할 수 있으며, 금융 기업은 개인의 동의하에 데이터를 제공받아 맞춤형 자산관리를 하는 등 새로운 사업 모델을 찾을 수 있습니다.

1.1.1 Prerequisites and Requirements

이 항목에서는 MyData Proxy Server를 Amazon Web Services(AWS)에서 사용하기 위한 전제 조건 및 리소스 요구 사항에 대해 설명합니다.

1. AWS 계정

MyData Proxy Server를 사용하기 위해서 AWS Account가 설정되어 있어야 합니다. 그렇지 않은 경우 링크(https://aws.amazon.com/ko/getting-started/)를 통해 AWS 계정 설정에 대한 절차를 확인해야 합니다. 등록 프로세스의 일부에는 전화를 받고 전화 키패드를 사용하여 PIN을 입력하는 작업이 포함됩니다.

2. OS

MyData Proxy Server는 AMI는 Amazon Linux에서 사용할 수 있으며 Linux에 익숙한 OS를 선택할 수 있습니다.

3. AWS 자원

MyData Proxy Server 배포 구성은 Single Configuration 과 High availability Configuration 2 개이며 선택한 배포구성에 따라 AWS Resource 가 다릅니다.

구성은 [1.1.3] Architecture Diagrams 을 참조하십시오.

A. Single Configuration

자원	개수
VPC	**1**
VPC 보안 그룹	**1**
IAM 역할	**1**
EFS	**1**
KMS	**2**
EC2 instance	**1**

B. High availability Configuration

자원	개수
VPC	**1**
VPC 보안 그룹	**1**
IAM 역할	**1**
EFS	**1**
KMS	**2**
Auto Scaling 그룹	**1**
Elastic Load Balancing(ELB)	**1**
EC2 instance	**2**

C. Optional Resource

자원	개수
Cloud Watch	**1**

4. 리소스 할당량

필요한 경우 리소스에 대한 서비스 할당량 증가를 요청할 수 있습니다. 여러 배포에서 공유되는 리소스에 대한 기본 제한을 초과하지 않도록 할당량 증가를 요청해야 합니다. ap-northeast-2 Region 의 리소스 할당량은 다음 링크에서 확인 가능합니다.

https://console.aws.amazon.com/servicequotas/home?region=ap-northeast-2#!/

➢ 리소스 할당량에 관한 자세한 내용은 아래 링크를 참조하십시오.

https://docs.aws.amazon.com/servicequotas/latest/userguide/intro.html

5. IAM 권한

MyData Proxy Server 에 대한 배포 단계를 시작하기 전 3 번 항목을 참고하시고 배포하는 자원 및 SSM 가 포함된 IAM 권한으로 AWS Management 콘솔에 로그인 해야 합니다.

- IAM 권한에 대한 모범사례는 다음 링크를 참조 하십시오.

  https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/best-practices.html#grant-least-privilege

- Session Manger 용 최종 사용자 정책은 아래를 참조 하십시오.

  https://docs.aws.amazon.com/systems-manager/latest/userguide/getting-started-restrict-access-quickstart.html

➢ IAM 내의 Administrator Access 관리형 정책은 충분한 권한을 제공하지만 조직에 더 많은 제한이 있는 사용자 지정 정책을 사용하려면 다음 링크를 참조하십시오.

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html

1.1.2 Region support

제품이 지원되는 지역은 아래와 같습니다.

Region code	Region Name	Remarks
us-east-1	US East (N. Virginia)	-
ap-northeast-2	Asia Pacific(Seoul)	-

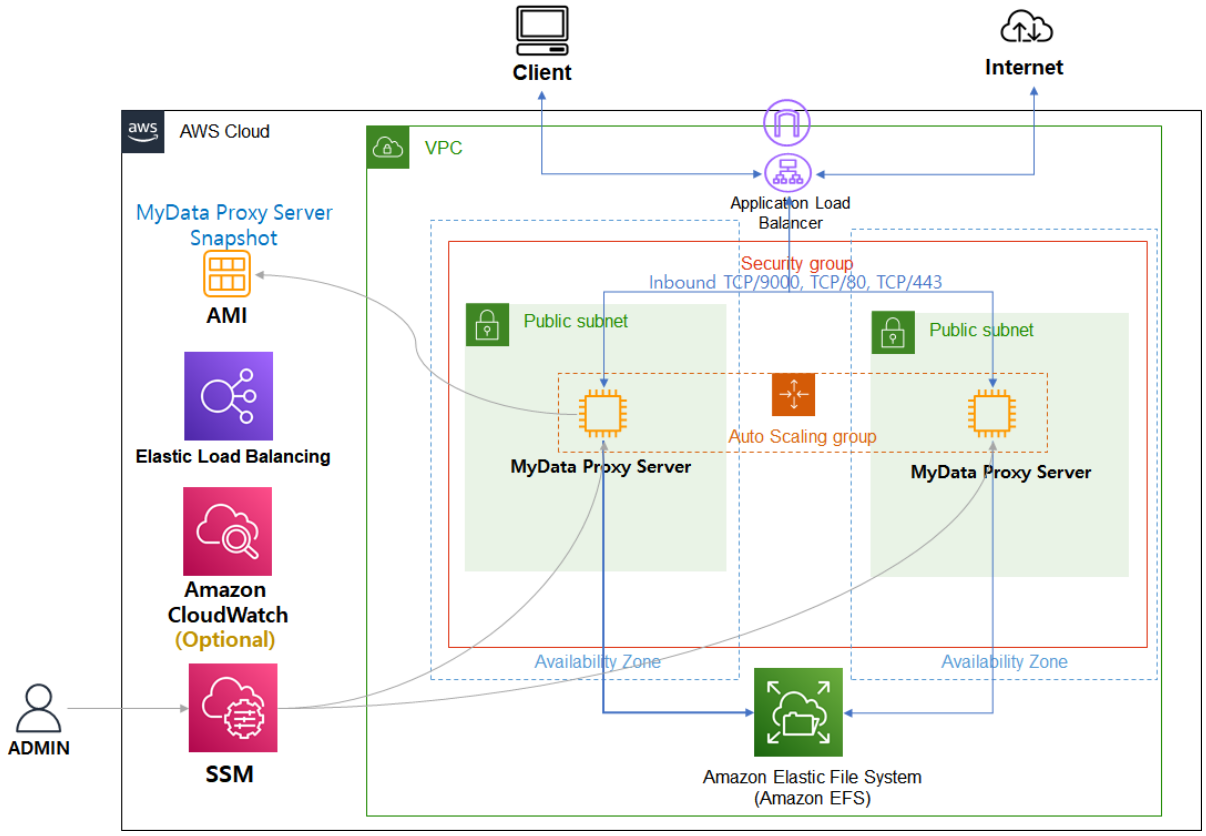
1.1.3 Architecture Diagrams

✓ 구성에 포함되는 기술

- Public Subnet, MyData Proxy Server EC2 인스턴스
- AMI(Amazon Machine Image)를 사용하여 백업 및 복수 수행
- Amazon EFS을 이용하여 MyData Proxy Server EC2 인스턴스의 파일 시스템의 공유 데이터에 액세스합니다.
- AWS System Manager 서비스의 Session Manager 기능을 통해 인스턴스에 접근합니다.
- Amazon Elastic Load Balancing 서비스의 ALB(Application Load Balancer)는 Auto Scaling 전반에 걸쳐 웹 트래픽을 분산합니다. (**High availability Configuration**).
- Amazon EC2 인스턴스의 Auto Scaling 그룹을 사용하여 실행할 수 있습니다. (**High availability Configuration**)
- Amazon Cloud Watch 서비스 사용으로 MyData Proxy Server 상태 모니터링 및 알림 **(선택사항)**

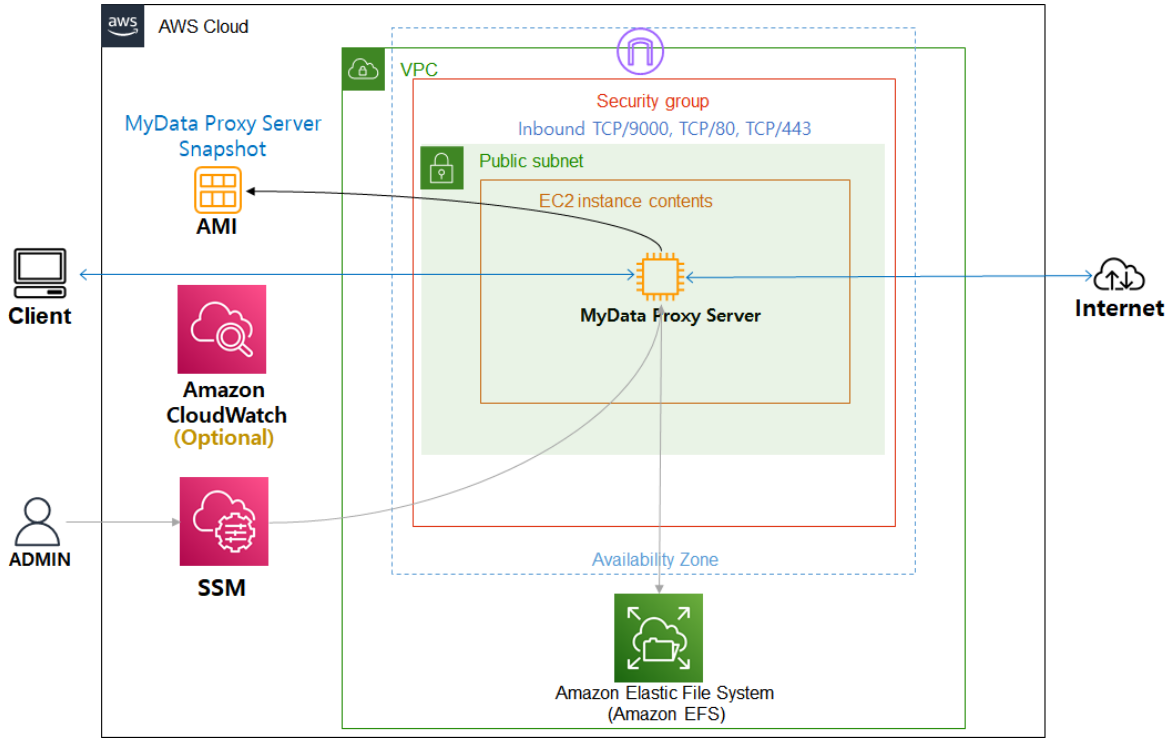
A. High availability Configuration (preferred)

High availability 배포 옵션에서 인스턴스는 Application Load Balancer 뒤에 위치하며, 2개의 가용 영역에 인스턴스가 동작하는 auto-scaled 되어 고가용성 및 재해 복구를 보장합니다. 안정성이 필요한 거래 구성을 목표로 하는 사용자에게 권고하는 구성입니다.

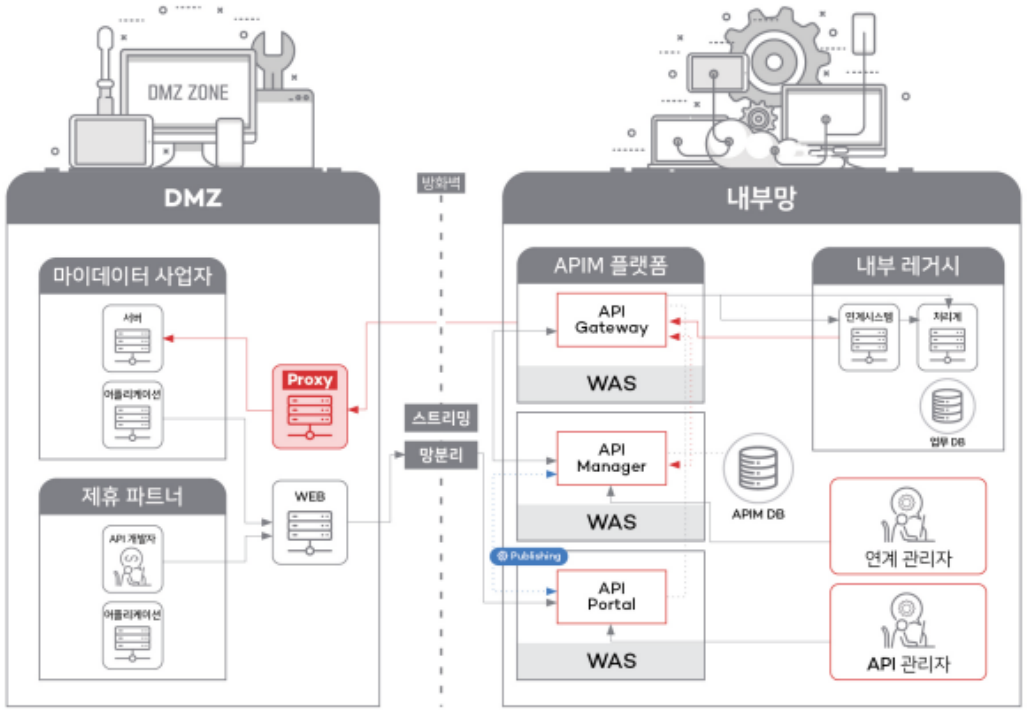


B. Single Configuration (Development and Testing)

비용절감 최우선이라면 단일 구성을 권장하지만, 단일 구성은 개발 및 테스트의 목적으로 적합하며, 고가용성 및 높은 내구성을 보장하지 않습니다.


AWS Cloud
VPC
Security group
Inbound TCP/9000, TCP/80, TCP/443
MyData Proxy Server
Snapshot
AMI
Public subnet
EC2 instance contents
MyData Proxy Server
Client
Internet
Amazon
CloudWatch
(Optional)
ADMIN
SSM
Availability Zone
Amazon Elastic File System
(Amazon EFS)

1.1.4 Use case


DMZ ZONE
DMZ
방화벽
내부망
마이데이터 사업자
서버
어플리케이션
Proxy
제휴 파트너
API 개발자
어플리케이션
WEB
스트리밍
망분리
APIM 플랫폼
API Gateway
WAS
API Manager
WAS
Publishing
API Portal
WAS
APIM DB
내부 레거시
연계시스템
처리계
업무 DB
연계 관리자
API 관리자

인젠트의 MyData Proxy Server는 망 분리된 업무 환경에서 DMZ 구간에 위치하여 내부망에 있는 API GW, 업무 PC 등이 인터넷 서비스에 간접적으로 접속할 수 있게 해주는 응용 프로그램입니다. 보편적인 Proxy처럼 Forward Proxy, Reverse Proxy 등 Proxy 서버의 기본적이 기능을 제공하여 아래 그림과 같이 보편적인 Proxy Server의 형태로도 사용도 가능합니다.

구축 위치	사용 사례
On-premise	**[KCB]** Private Cloud 기반 마이데이터 사업자 시스템 구축을 위해 Proxy Server를 사용한 사례입니다. http://www.inzent-mydata.com/board/board.php?bo_table=case&pg=1&idx=13
Public Cloud	**[교보생명]** Hybrid Cloud기반 마이데이터 플랫폼 구축에 사용된 사례입니다. http://www.inzent-mydata.com/board/board.php?bo_table=case&pg=2&idx=6

1.1.5 Deployment time

배포 단계는 최소 10분 ~ 최대 30분 정도가 소요되며, 설정 및 제품 테스트에는 최대 30분이 소요될 수 있습니다.

2. Planning Guidance

2.1 Security

보안 및 운용 :

MyData Proxy Server를 설치/제어하는데 오직 SSM 및 IAM 사용 접근만 허용됩니다.

- ➢ 접속에 AWS 루트 자격 증명을 사용하지 않습니다.

2.2 Costs and Licenses

MyData Proxy Server 제품은 무료로 제공합니다. 추가로 AMI 제공에 대해서는 아래 링크를 통해 문의하십시오.

- ✓ 관련 문의 링크 : http://www.inzent-mydata.com/Questions.php

➢ Full list of billable AWS services

귀하는 AWS 서비스 비용에 대한 책임이 있습니다. 메뉴에 의해 생성된 리소스 비용은 사용하는 인스턴스에 따라 다릅니다. 자세한 내용은 이 가이드에서 사용할 AWS 서비스의 요금 페이지 (https://aws.amazon.com/pricing/) 를 참조하십시오.

A. EC2 Instance(필수)

B. EBS(필수)

C. EFS(필수)

D. KMS(필수)

E. ELB(선택사항)

F. Cloud watch(선택 사항)

2.3 Sizing

MyData Proxy Server의 AMI는 AWS에서 아래 표와 같은 인스턴스 사양을 지원합니다. 인스턴스의 각 유형 최신정보는 옆에 링크를 참고하세요.(https://aws.amazon.com/ko/ec2/instance-types/)

Instance type	Vcpu	Memory(GiB)	EBS Volume	EBS Volume Type
t2.medium or t3.medium	2	4	10GB	General Purpose SSD (gp2)

3. Deployment steps

3.1 Mydata Proxy Server Installation

MyData Proxy Server 배포를 위해서는 아래와 같은 AWS Resources이 필요합니다.

✓ AWS Resources :

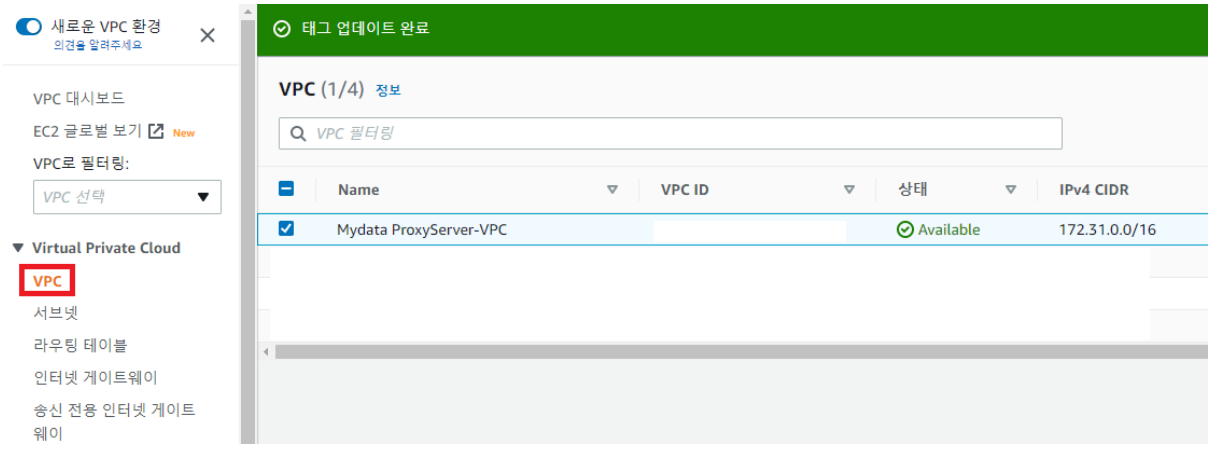
- Amazon Virtual Private Cloud(VPC)
- Internet Gateway
- Amazon VPC subnets **(public)**
- Amazon Elastic Load Balancing (Amazon ELB) Application Load Balancer (ALB) – in public subnets **(public)**
- Amazon EC2 Auto Scaling
- Amazon EC2 Instance
- Amazon Elastic File System
- Amazon Cloud Watch **(선택 사항)**

3.1.1 Create VPC and Subnet

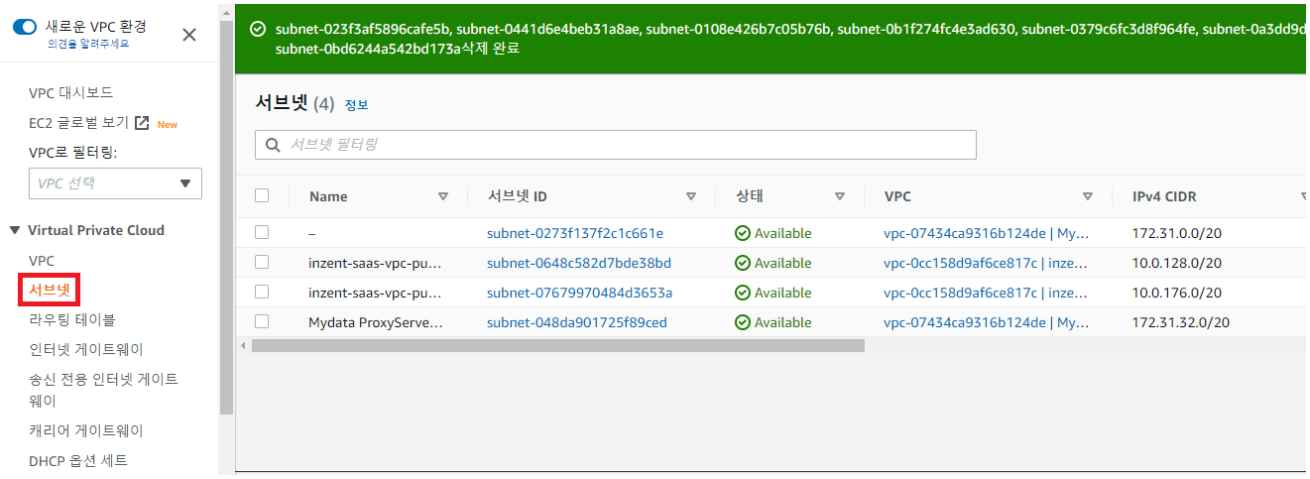
Mydata Proxy Server를 사용하기 위한 VPC 및 Public Subnet 생성

A. 기존 VPC 및 서브넷 확인

1. [콘솔 홈 > 서비스 > 네트워킹 및 콘텐츠 전송> VPC]에서 VPC설정을 확인 가능

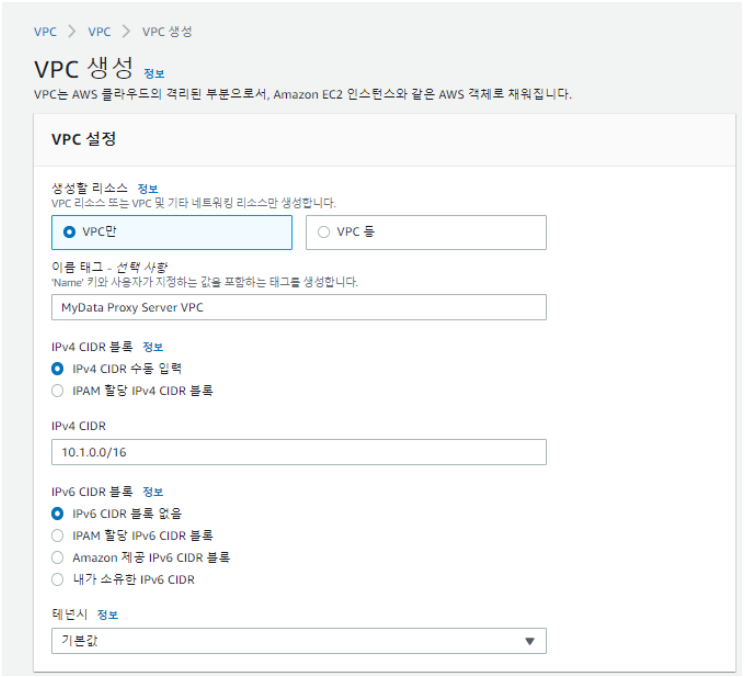


2. [콘솔 홈 > 서비스 > 네트워킹 및 콘텐츠 전송> VPC > 서브넷]에서 VPC 설정을 찾을 수 있습니다.



B. MyData Proxy Server VPC 생성

1. Amazon VPC console로 이동(https://console.aws.amazon.com/vpc).
2. 탐색창에서 VPC를 선택 후 VPC 생성을 선택.
3. VPC 생성 및 VPC의 IPv4 주소 범위 지정



C. MyData Proxy Server Subnet 1 생성

1. Amazon VPC console로 이동(https://console.aws.amazon.com/vpc).
2. 탐색창에서 서브넷을 선택 후 서브넷 생성을 선택.
3. 필요에 따라 서브넷 세부 정보를 지정하고 생성을 선택.

Menu	Input Value
서브넷 이름	MyData Proxy Server Subnet 1
VPC	[3.1.1]에서 생성한 VPC 선택
VPC CIDRS	-
가용 영역	[1.1.3] Architecture Diagrams 참고
IPv4 CIDR 블록	서브넷 그룹에 대한 정보는 다음 링크를 참조하십시오. : https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Subnets.html

D. MyData Proxy Server Subnet 2 생성

✓ **Single Configure 생략.**

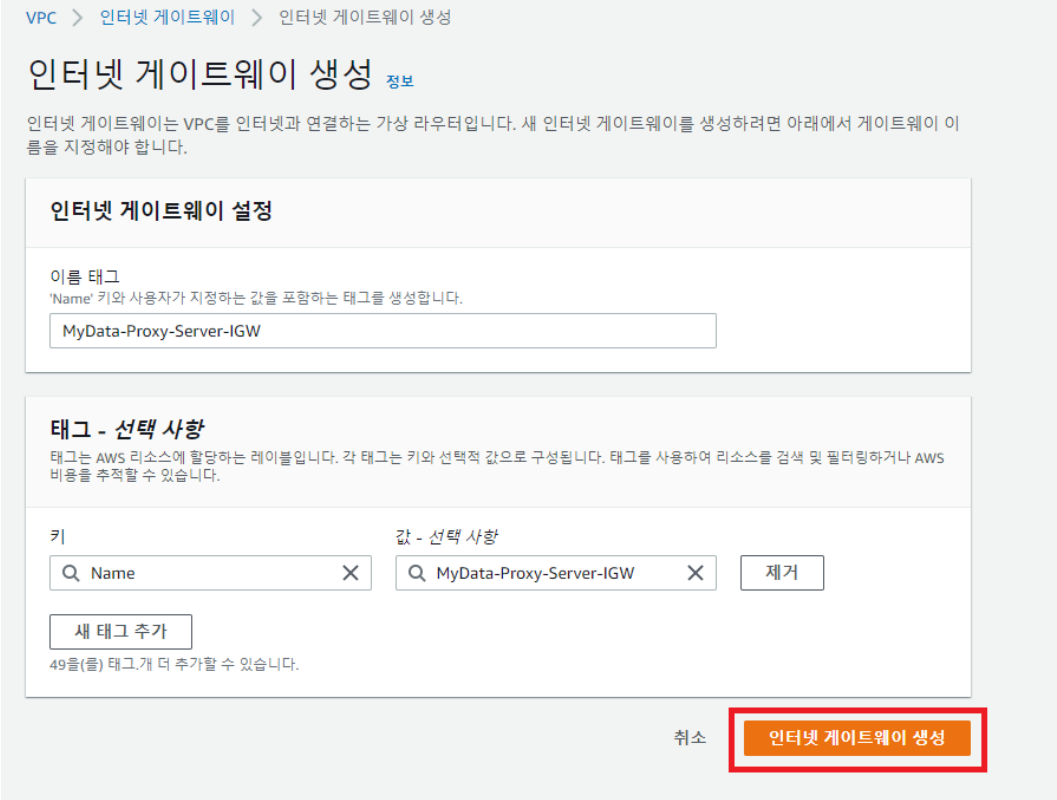
1. Amazon VPC console로 이동(https://console.aws.amazon.com/vpc).
2. 탐색창에서 서브넷을 선택 후 서브넷 생성을 선택.
3. 필요에 따라 서브넷 세부 정보를 지정하고 생성을 선택.

Menu	Input Value
서브넷 이름	MyData Proxy Server Subnet 2
VPC	[3.1.1]에서 생성한 VPC 선택
VPC CIDRS	-
가용 영역	[1.1.3] Architecture Diagrams 참고
IPv4 CIDR 블록	서브넷 그룹에 대한 정보는 다음 링크를 참조하십시오. : https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Subnets.html

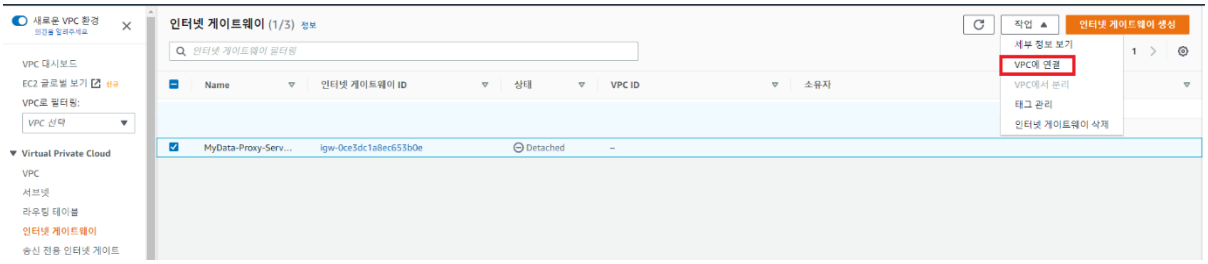
E . Create internet gateway, and attach it to VPC

1. Amazon VPC console로 이동(https://console.aws.amazon.com/vpc).

2. 탐색창에서 인터넷 게이트웨이를 선택 후 인터넷 게이트웨이 생성을 선택



3. 인터넷 게이트웨이 VPC에 연결



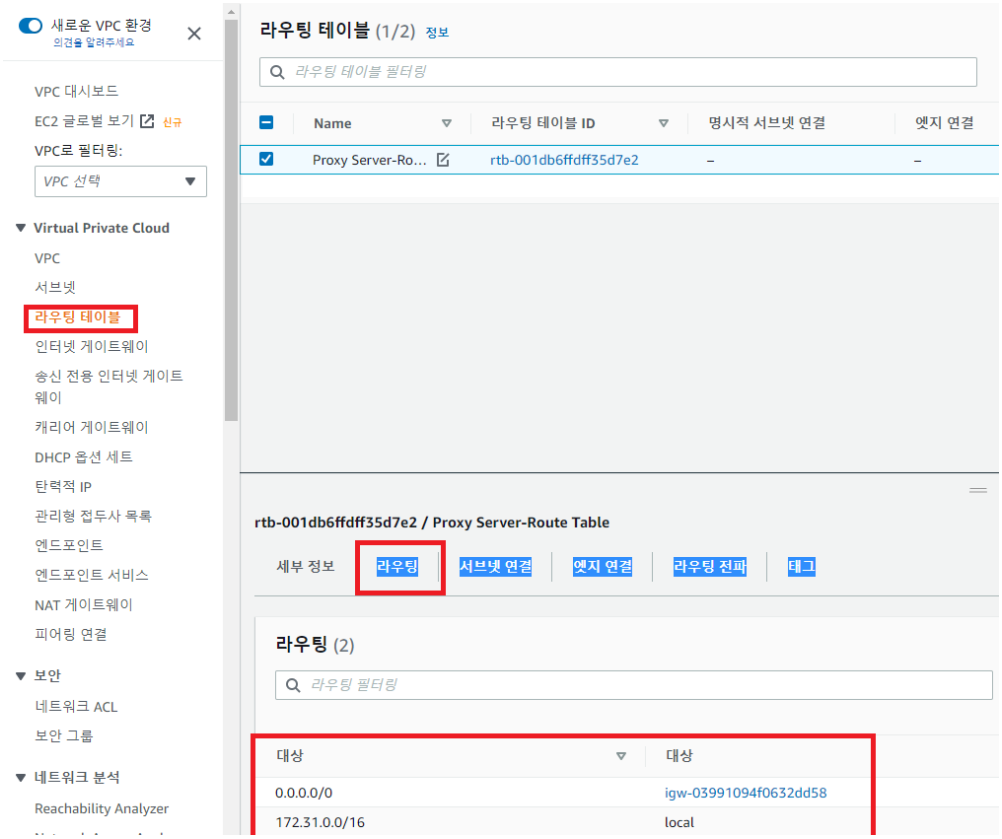
- [3.1.1] Create VPC and Subnet의 동일한 VPC와 연결

F. Create or use default route table

1. Amazon VPC console로 이동(https://console.aws.amazon.com/vpc).

2. 탐색창에서 라우팅 테이블을 선택 후 라우팅 테이블이 존재하지 않으면 생성하

고 사용할 VPC에 연결하며, 존재하면 IGW와 설정

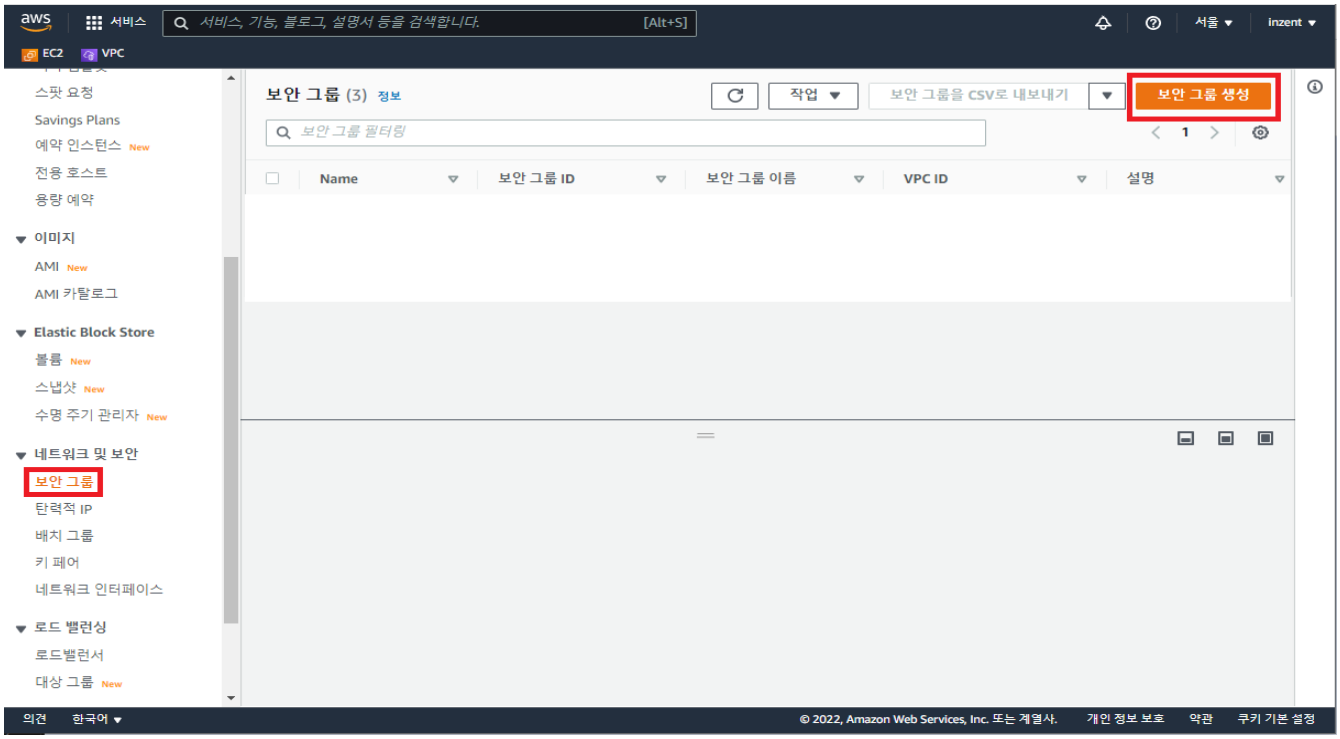


3.1.2 Create Security Group

Mydata Proxy Server의 통신하려면 보안그룹을 설정해야 합니다.

A. Create MyData Proxy Server Security Groups

1. AWS EC2 Management Console에 접속.
2. [네트워크 및 보안]에 보안그룹 버튼을 선택



B. 보안그룹 생성 및 인바운드 규칙 설정.

Menu	Input Value
보안 그룹 이름	MyData Proxy Server SG
설명	MyData Proxy Server-HTTP SG
VPC	[3.1.1]에서 생성한 VPC 선택
유형	HTTP
프로토콜	TCP
포트 범위	80
대상	0.0.0.0/0

Menu	Input Value
보안 그룹 이름	MyData Proxy Server SG
설명	MyData Proxy Server-HTTPS SG
VPC	[3.1.1]에서 생성한 VPC 선택

유형	HTTPS
프로토콜	TCP
포트 범위	443
대상	0.0.0.0/0

Menu	Input Value
보안 그룹 이름	MyData Proxy Server SG
설명	MyData Proxy Server-Client SG
VPC	[3.1.1]에서 생성한 VPC 선택
유형	사용자 지정 TCP
프로토콜	TCP
포트 범위	9000
대상	Client IP

C. 데이터 조회를 위한 아웃바운드 규칙 설정

Menu	Input Value
보안 그룹 이름	MyData Proxy Server SG
설명	MyData Proxy Server OutBound
VPC	[3.1.1]에서 생성한 VPC 선택
유형	모든 TCP
프로토콜	TCP
포트 범위	0~65535
대상	0.0.0.0/0

D. Add a Name Tag to [태그] as follows

Menu	Input Value	Menu	Input Value
Tag	이름	설명	그룹 식별을 위한 태그 지정
Value	MyData Proxy Server SG		

E. Create MyData Proxy Server-EFS Security Group

1. AWS EC2 Management Console에 접속.

2. [네트워크 및 보안]에 보안그룹 버튼을 선택

3. MyData Proxy Server-EFS 보안 그룹 인바운드 설정

Menu	Input Value
보안 그룹 이름	MyData Proxy Server-EFS SG
설명	MyData Proxy Server-EFS SG
VPC	[3.1.1]에서 생성한 VPC 선택
유형	NFS
프로토콜	TCP
포트 범위	2049
대상	보안 그룹 [MyData Proxy Server SG]의 보안 그룹 ID

4. 아웃바운드 설정

■ 보안 그룹 생성으로 Default로 생성되는 설정과 동일

5. Add a Name Tage to [태그] as follows

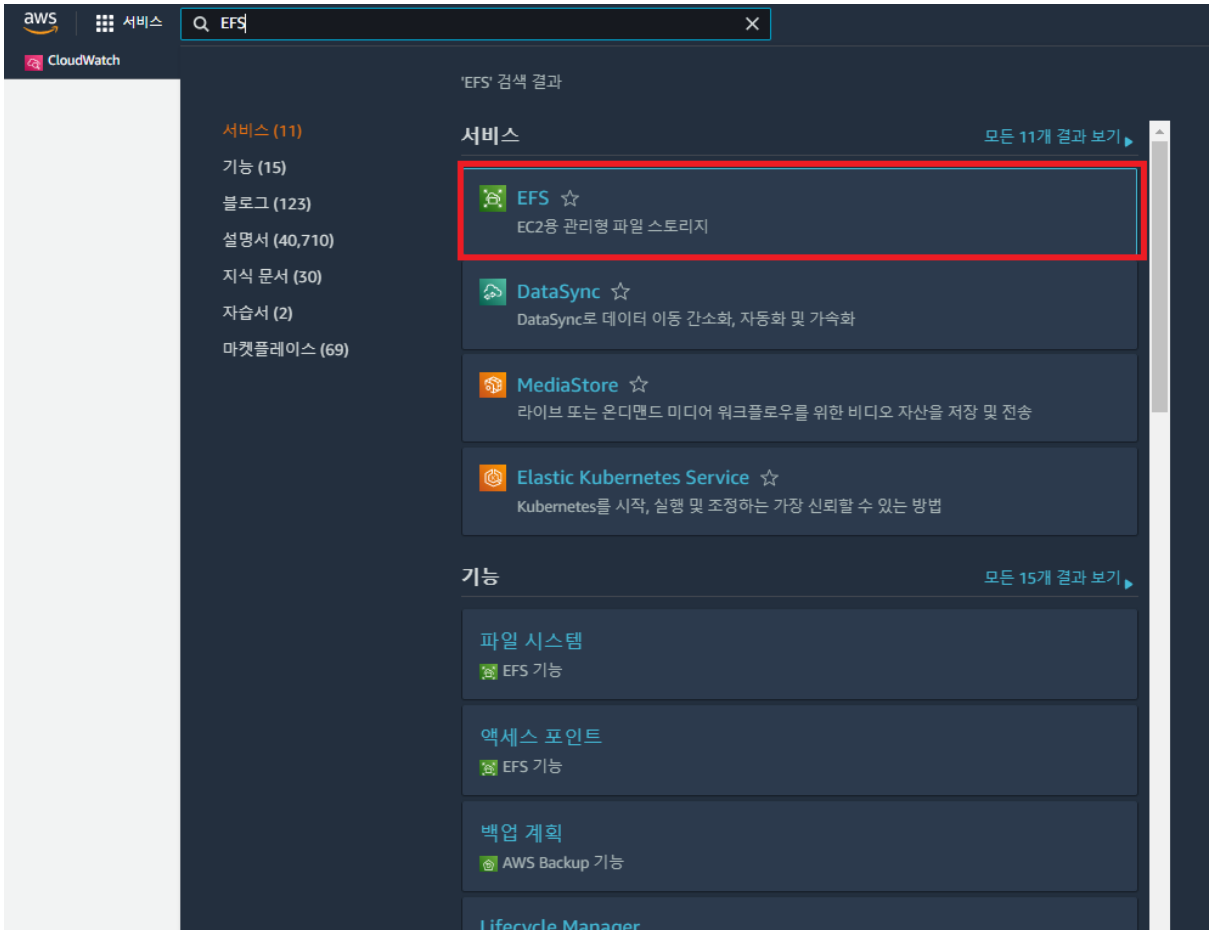
Menu	Input Value	Menu	Input Value
Tag	이름	설명	그룹 식별을 위한 태그 지정
Value	MyData Proxy Server-EFS SG		

3.1.3 Create EFS

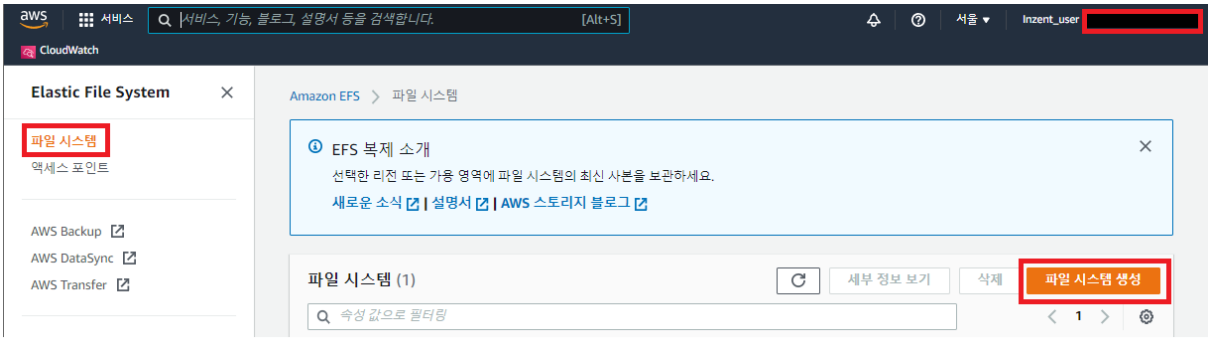
MyData Proxy Server의 로그 파일을 저장을 위해 Amazon EFS를 생성 해야 합니다.

1. 파일 시스템 생성

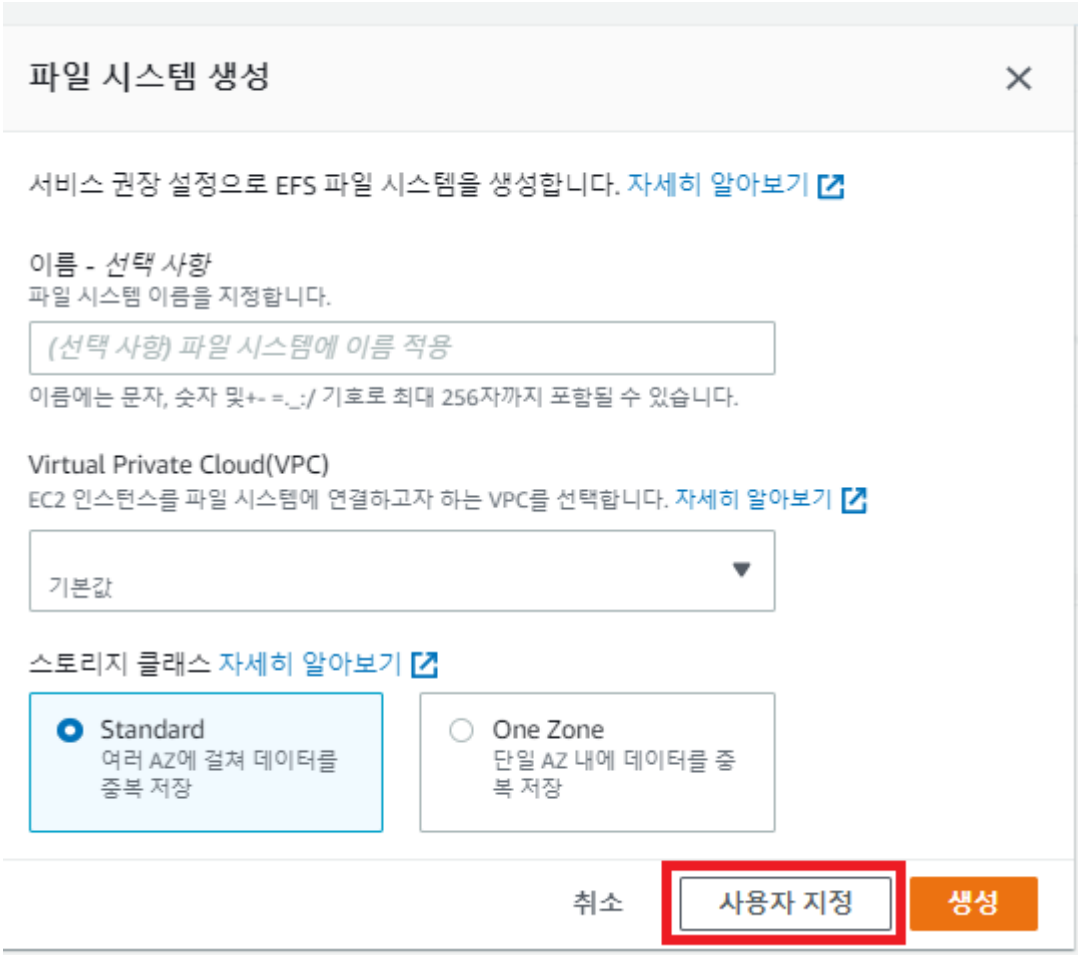
A. [콘솔 홈 > 서비스 > EFS]를 통해 EFS 메인 화면으로 접속합니다.



B. [콘솔 홈 > 서비스 > EFS > 파일 시스템 > 파일 시스템 생성]



C. 파일 시스템 생성에서 사용자 지정을 클릭합니다.



D. [Amazon EFS > 파일 시스템 > 생성 > 1단계 파일 시스템 설정]

Menu	Input value	Description
이름	MyData-Proxy-Server	파일 시스템 이름을 지정
스토리지 클래스	Standard	자세한 내용 : https://docs.aws.amazon.com/efs/latest/ug/storage-classes.html
자동 백업	**(선택 사항)**	자세한 내용 : https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html
IA로 전환	마지막으로 액세스 이후 30일 경과	EFS Intelligent-Tiering 은 수명 주기 관리를 사용하여 파일을 Standard-Infrequent Access 스토리지 클래스 사이에서 이동함으로써 애플리케이션에 적합한 가격 및 성능 블렌드를 자동으로 실현합니다. -
IA 외부로 전환	처음 액세스 할 때	

성능 모드	범용	필요한 IOPS를 기반으로 파일 시스템의 성능 모드 설정
처리량 모드	버스트	파일 시스템의 처리량 제한이 결정되는 방식 설정
암호화	유휴 시 데이터 암호화 활성화	파일 시스템의 유휴 데이터의 암호화를 활성화 하려면 선택, 기본적으로 KMS 서비스 키 (aws/elasticfilesystem)를 사용합니다. 암호화 설정 사용자 지정 및 자세한 내용에 대해서는 아래 링크를 참조하세요. https://docs.aws.amazon.com/efs/latest/ug/encryption.html
태그	태그 키 : Name	파일 시스템 식별을 위한 태그 지정
	태그 값 : MyData Proxy Server-EFS	

E. [Amazon EFS > 파일 시스템 > 생성 > 2단계 네트워크 액세스]

Menu	Input value	Description
Virtual Private Cloud (VPC)	[3.1.1]에서 생성한 VPC 선택	EC2 인스턴스를 파일 시스템에 연결하고자 하는 VPC를 선택합니다.
탑재 대상	[1.1.3] Architecture Diagrams를 참고하여 탑재 대상의 수 선택 - 가용영역 : [3.1.1] Create VPC and Subnet에서 생성한 Subnet과 동일하게 생성 - 서브넷 ID : [3.1.1] Create VPC and Subnet에서 생성한 서브넷 ID - IP 주소 : Default - 보안 그룹 : [3.1.2] Create Security Group에서 생성한 [MyData Proxy Server-EFS SG]의 보안 그룹 ID 선택	탑재 대상은 Amazon EFS 파일 시스템을 탑재할 수 있는 NFSv4 엔드 포인트를 제공합니다. 가용 영역마다 탑재 대상을 한 개씩 생성하는 것이 좋습니다.

F. [Amazon EFS > 파일 시스템 > 생성 > 3단계 파일 시스템 정책]

MyData Proxy Server에서는 기본 설정을 권장하며, 정책 설정을 원하시는 분은 아래 링크를 참조하세요.

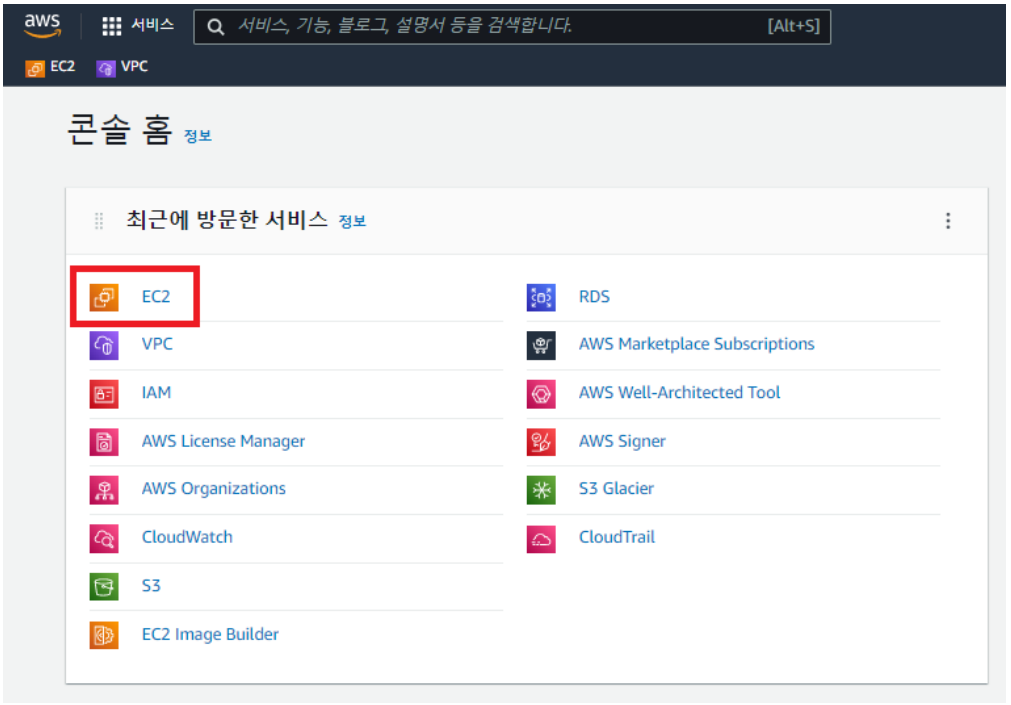
➢ https://docs.aws.amazon.com/efs/latest/ug/iam-access-control-nfs-efs.html

3.1.4 Create a Launch Template

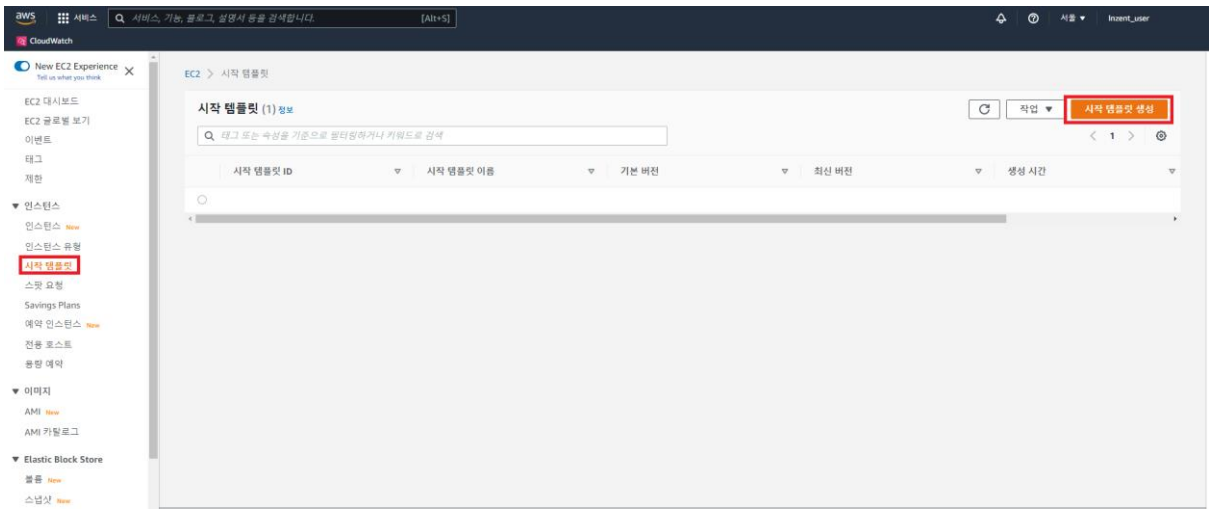
✓ MyData Proxy Server AMI로 시작 템플릿을 생성

■ AMI 제공은 [2.2] Costs and Licenses를 확인해주세요.

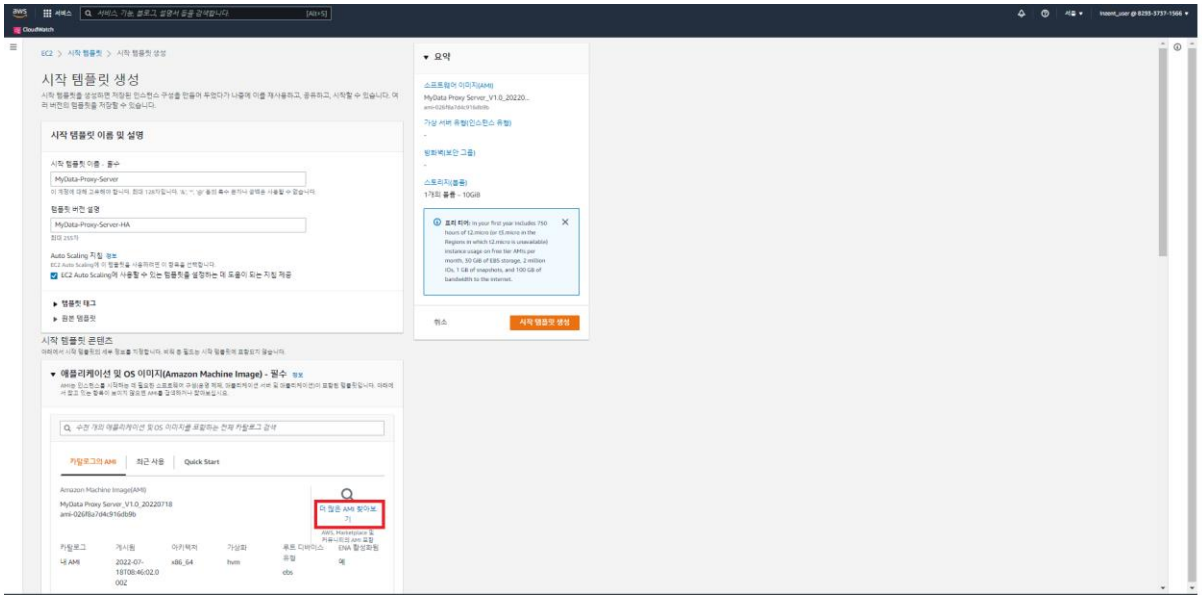
1. AWS EC2 콘솔에 로그인



2. [EC2 > 시작 템플릿]에서 시작 템플릿 생성 클릭



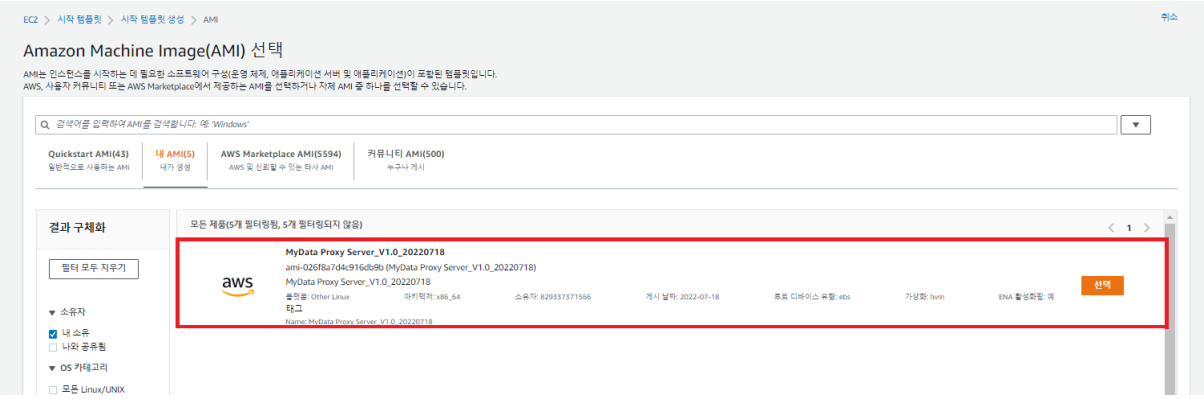
3. [EC2 > 시작 템플릿 > 시작 템플릿 생성] 시작 템플릿 이름 및 설명



매뉴	Input Value
시작 템플릿 이름	MyData-Proxy-Server
템플릿 버전 설명	Single 구성 : MyData-Proxy-Server
	HA 구성 : MyData-Proxy-Server-HA
Auto Scaling 지침	HA 구성 시 ☑ 체크

4. [EC2 > 시작 템플릿 > 시작 템플릿 생성] 시작 템플릿 콘텐츠

- 더 많은 AMI 찾아보기 클릭
- 제공 받은 AMI를 선택



5. [EC2 > 시작 템플릿 > 시작 템플릿 생성] 인스턴스 유형 및 Networking setting

Menu	Input Value
인스턴스 유형	**[2.3] Sizing** 을 보고 선택.
키 페어 이름	시작 템플릿에 포함하지 않음
서브넷	Single 구성 : [1.1.3] Architecture Diagrams 및 [3.1.1] Create VPC and Subnet 을 보고 선택
	HA 구성 : 시작 템플릿에 포함하지 않음
보안 그룹	[3.1.2] Create Security Group 를 보고 선택

6. [EC2 > 시작 템플릿 > 시작 템플릿 생성] 스토리지(볼륨)

Menu	Input Value
크기	**[2.3] Sizing** 을 보고 선택.
볼륨 유형	**[2.3] Sizing** 을 보고 선택.
종료 시 삭제	Yes
암호화됨	Yes
KMS 키	(기본값) aws/ebs 또는 [4.2] EBS Volume encryption 을 통해 생성한 KMS 키

7. [EC2 > 시작 템플릿 > 시작 템플릿 생성] 리소스 태그

- MyData Proxy Server 인스턴스 태깅

Menu	Input Value	Menu	Input Value
키	Name	설명	인스턴스 식별을 위한 태그 지정
값	MyData Proxy Server		
리소스 유형	인스턴스		

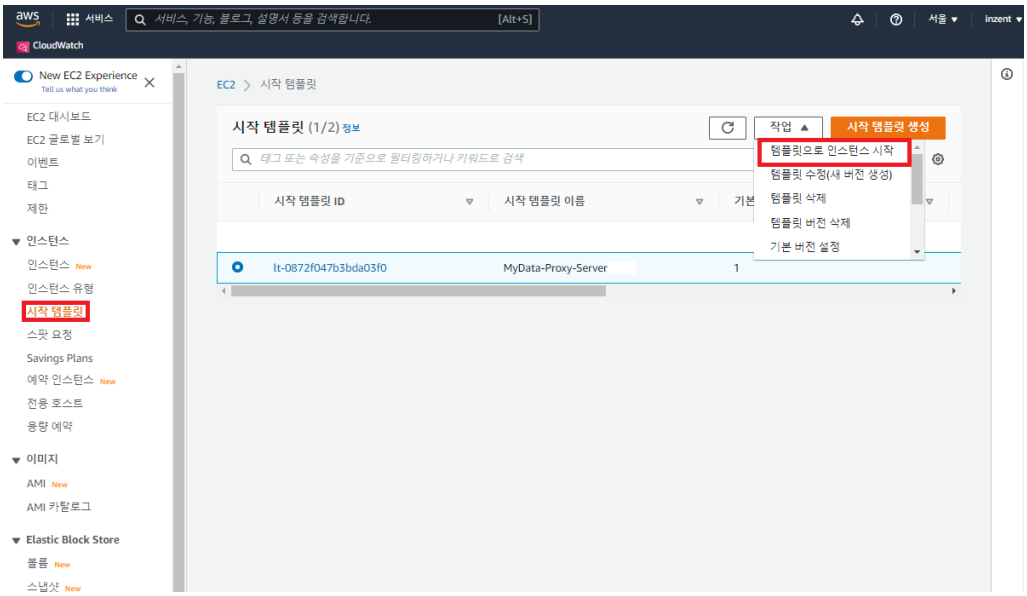
8. [EC2 > 시작 템플릿 > 시작 템플릿 생성] 고급 세부 정보

Menu	Input Value	Description
IAM 인스턴스 프로파일	[AmazonSSMRoleForInstancesQuicksetup]	SSH 를 사용하지 않고 SSM 을 사용하여 인스턴스에 접속을 위한 IAM Role
사용자 데이터	#! /bin/bash sudo mount -t efs -o tls [efs-id] /mnt/proxy/log sudo systemctl start httpd cd /app/apim-proxy/bin/ sudo /app/apim-proxy/bin/start.sh --//	인스턴스 시작시 EFS mount 및 Apache server, Proxy server 시작
etc	default	-

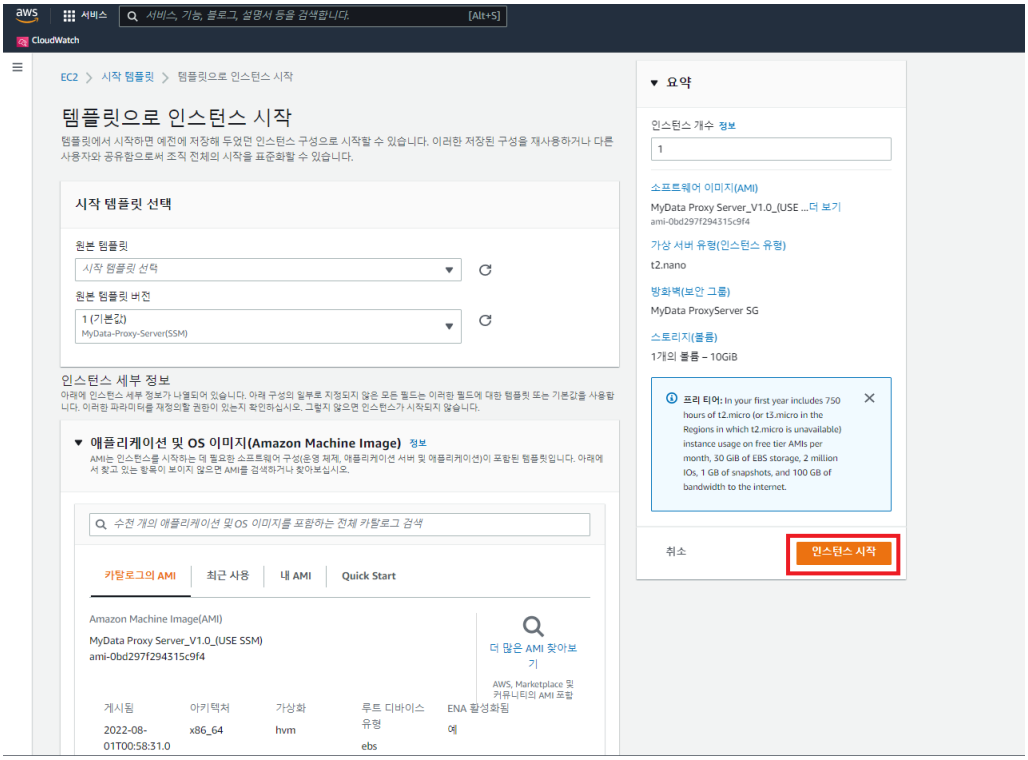
3.1.5 Launch an instance with a Template

✓ Single 구성

- [EC2 > 시작 템플릿] 템플릿으로 인스턴스 시작



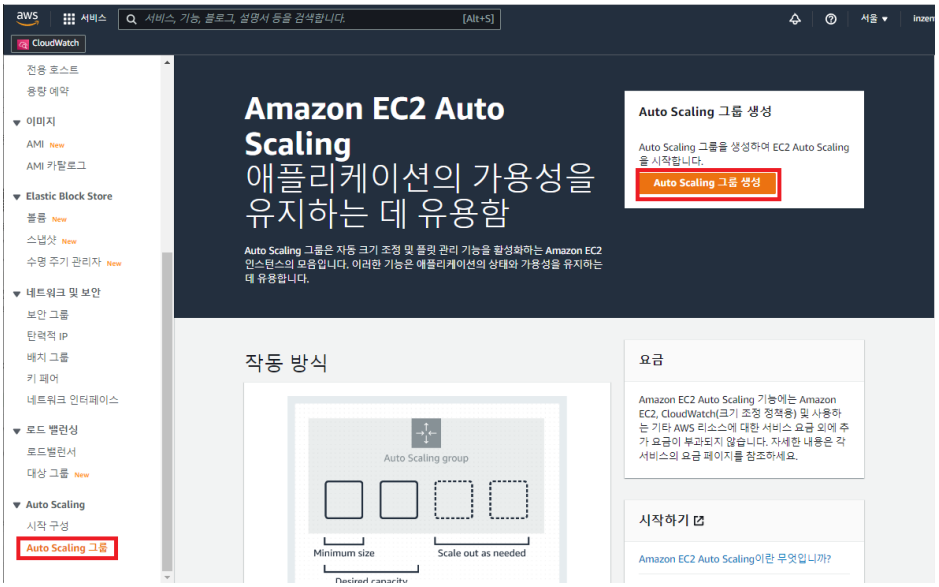
- [EC2 > 시작 템플릿 > 템플릿으로 인스턴스 시작] 인스턴스 시작 클릭



3.1.6 Create an Auto Scaling group

✓ **High availability 구성**

1. [EC2 > Auto Scaling 그룹] Auto Scaling 그룹 생성



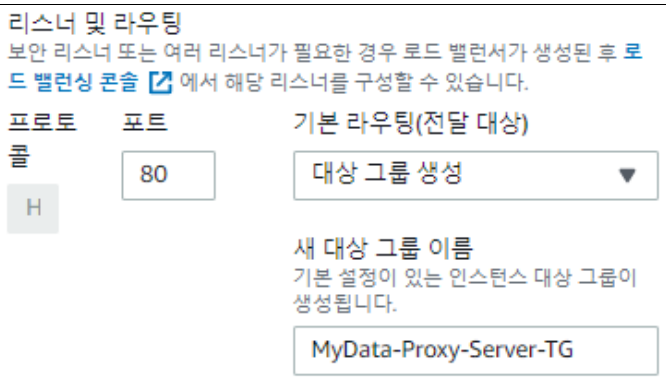
2. [EC2 > Auto Scaling 그룹 > Auto Scaling 그룹 생성] 1단계 시작 템플릿 또는 구성 선택

Menu	Input Value
Auto Scaling 그룹 이름	MyData Proxy Server_Auto-Scaling
시작 템플릿	[3.1.5] Create a Launch Template 에서 생성한 템플릿
버전	[3.1.5] Create a Launch Template 에서 HA 구성으로 생성한 템플릿 버전

3. [EC2 > Auto Scaling 그룹 > Auto Scaling 그룹 생성] 2단계 인스턴스 시작 옵션 선택

Menu	Input Value
VPC	[3.1.1] Create VPC and Subnet 에서 생성한 VPC 와 동일
가용 영역 및 서브넷	[1.1.3] Architecture Diagrams 및 [3.1.1] Create VPC and Subnet 을 보고 선택

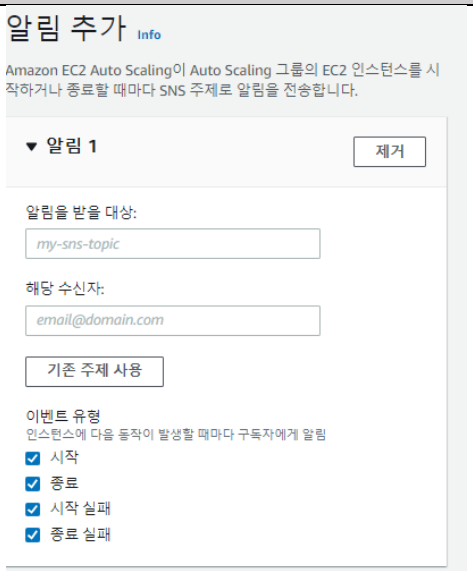
4. [EC2 > Auto Scaling > Auto Scaling 그룹 생성] 고급 옵션 구성

Menu	Input Value
로드 밸런싱	새 로드 밸런서에 연결
로드 밸런서 유형	Application Load Balancer
로드 밸런서 이름	MyData-Proxy-Server-ALB
로드 밸런서 체계	Internet-facing
VPC	[3.1.1] Create VPC and Subnet 에서 생성한 VPC 와 동일
가용 영역 및 서브넷	3 번 항목의 가용 영역 및 서브넷과 동일
리스너 및 라우팅	
상태 확인 유형	Default
모니터링**(선택 사항)**	아래 링크 참고하여 선택 https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-cloudwatch-monitoring.html?icmpid=docs_ec2as_help_panel
기본 인스턴스 워밍업 활성화**(선택 사항)**	아래 링크 참고하여 설정 https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-default-instance-warmup.html?icmpid=docs_ec2as_help_panel

5. [EC2 > Auto Scaling 그룹 > Auto Scaling 그룹 생성] 4단계 그룹 크기 및 크기 조정 정책 구성

Menu	Input Value
원하는 용량	2
최소 용량	1
최대 용량	2
ETC	Default

6. [EC2 > Auto Scaling 그룹 > Auto Sacaling 그룹 생성] 5단계 알림 추가

Menu	Input Value
알림 추가 **(선택 사항)**	

7. [EC2 > Auto Scaling 그룹 > Auto Scaling 그룹 생성] 6단계 태그 생성

Menu	Input Value	새 인스턴스에 태그 지정
Key	Name	☑
Value	MyData Proxy Server-HA	

8. [EC2 > Auto Scaling 그룹 > Auto Scaling 그룹 생성] 7단계 검토

- 설정 검토 후 Auto Scaling 그룹 생성

4. Operational Guidance

4.1 Connecting to Instances Using Session Manger

Session Manager는 대화형 원 클릭 브라우저 기반 셸 또는 AWS CLI를 통해 Amazon EC2 인스턴스를 관리할 수 있는 완전 관리형 AWS System Manager 기능입니다.

✓ Amazon EC2 콘솔을 사용하여 Session Manager를 사용하여 인스턴스에 연결

1. https://console.aws.amazon.com/ec2/ 에서 Amazon EC2 콘솔을 엽니다.

2. 탐색 창에서 **인스턴스**를 선택합니다.
3. 인스턴스를 선택하고 **연결**을 선택합니다.
4. 인스턴스에 연결에서 **Session Manager**를 선택하고 연결합니다.

✓ Session Manager의 동장에 대한 자세한 내용은 아래 링크를 참조

➢ https://docs.aws.amazon.com/ko_kr/systems-manager/latest/userguide/session-manager-working-with.html

4.2 EBS Volume encryption

EC2 인스턴스와 연결된 EBS 리소스를 위한 간단한 암호화 솔루션으로 Amazon EBS 임호화를 사용할 수 있습니다. Amazon EBS 암호화를 사용하면 자체 키 관리 인프라르 구축, 유지 관리 및 보호할 필요가 없습니다. Amazon EBS 암호화는 암호화된 볼륨 및 스냅샷을 생성할 때 AWS KMS Keys를 사용합니다.

아래 링크를 참조하여 EBS Volume에 대한 암호화 설정 및 스냅샷 볼륨 암호화 설정을 해야 합니다.

➢ https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/EBSEncryption.html

4.3 Encrypting Amazon EFS Data & Metadata at Rest

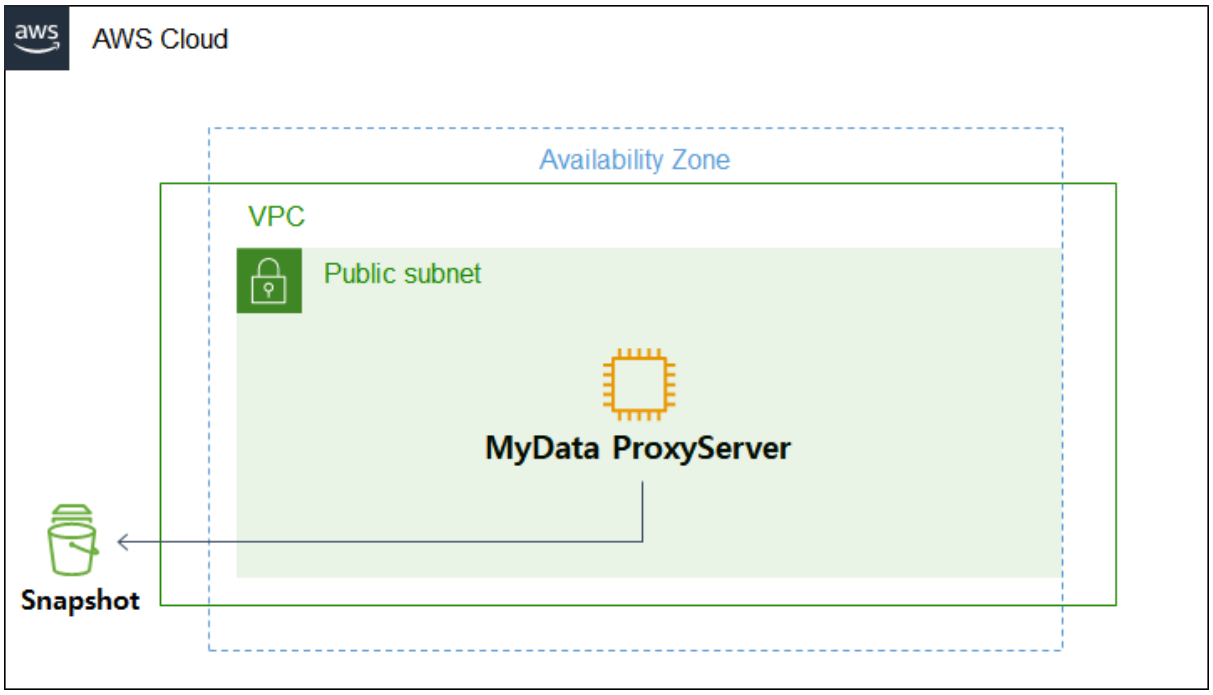
Amazon EFS는 AWS Key Management Service(KMS)와 통합되어 암호화를 지원합니다. AWS 고객 관리형 키 (CMK)를 사용하여 파일 시스템 콘텐츠의 암호화된 파일에서 데이터 및 메타 데이터는 파일에 쓰기 전에 자동으로 암호화되며, 읽을 때 해독됩니다.

아래 링크를 참조하여 EFS의 데이터를 암호화해야 합니다.

➢ https://docs.aws.amazon.com/efs/latest/ug/encryption.html

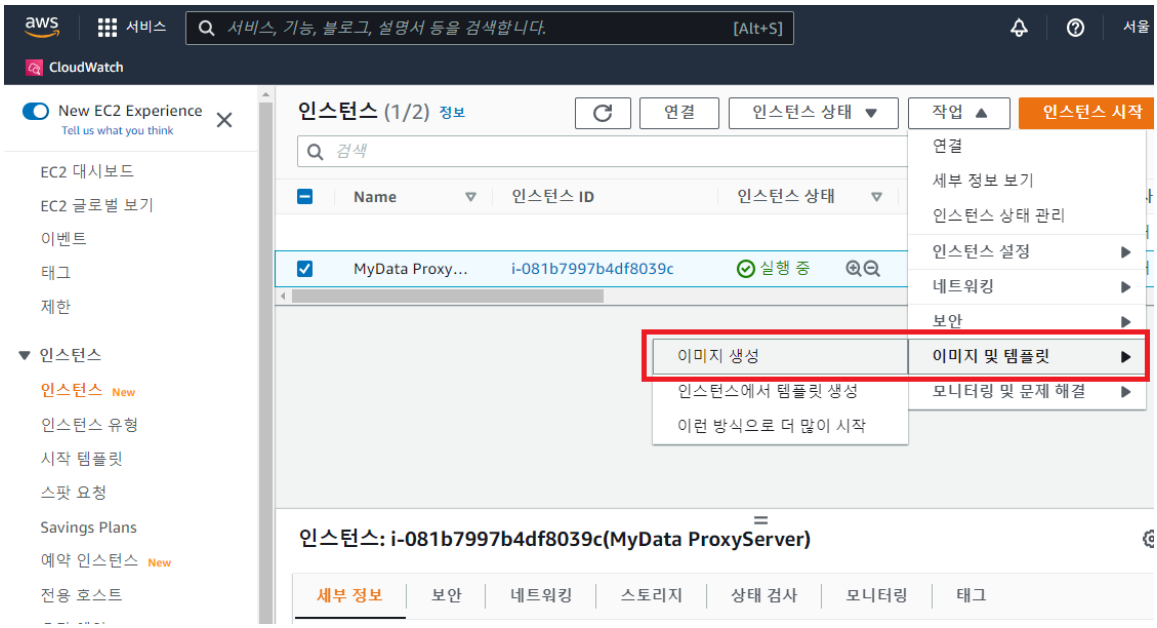
4.4 Support for MyData Proxy Server Backup and Restore in AWS

4.4.1 MyData Proxy Server Backup and Restore



A. 백업(Snapshot)

1. MyData Proxy Server의 AMI 이미지를 생성

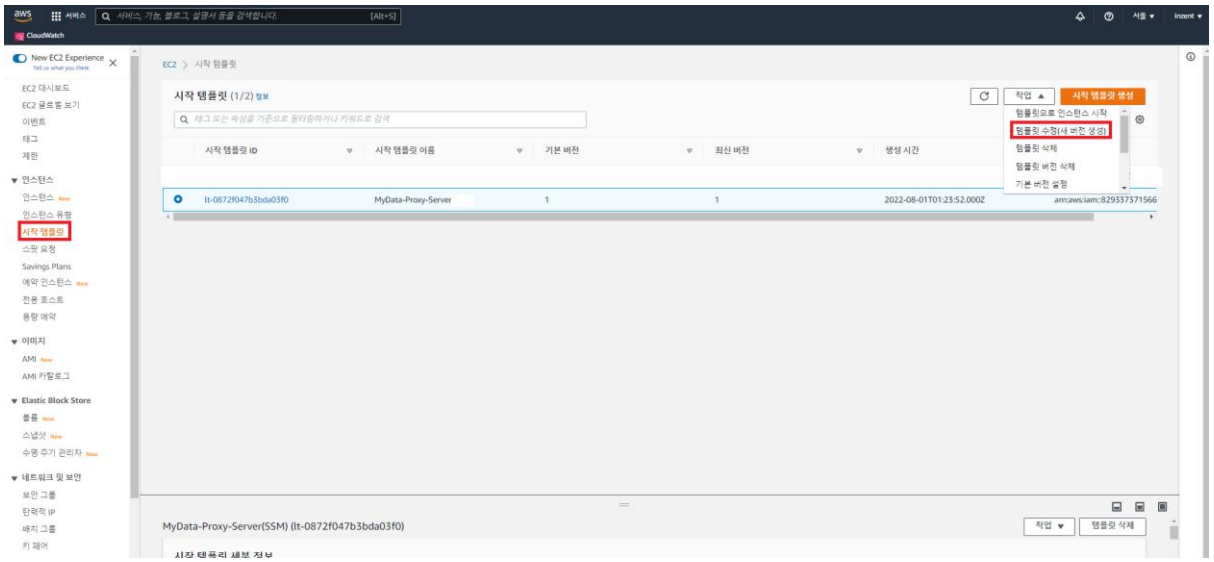


2. 이미지 생성

Menu	Input Value
이미지 이름	MyData Proxy Server backup
이미지 설명	MyData Proxy Server backup
재부팅 안함	체크 안함
인스턴스 볼륨	기본 구성

B. 복원

1. [EC2 > 시작 템플릿] 템플릿 수정(새 버전 생성)



2. 백업한 AMI(snapshot)을 선택 후 생성, **[3.1.4] Create Launch Template 참고**
3. 백업한 AMI 시작
   A. Single 구성 **[3.1.5] Launch an instance with a Template 참고**
   B. HA 구성 **[3.1.6] Create an Auto Scaling group 참고**

4.5 MyData Proxy Server Health Check with CloudWatch

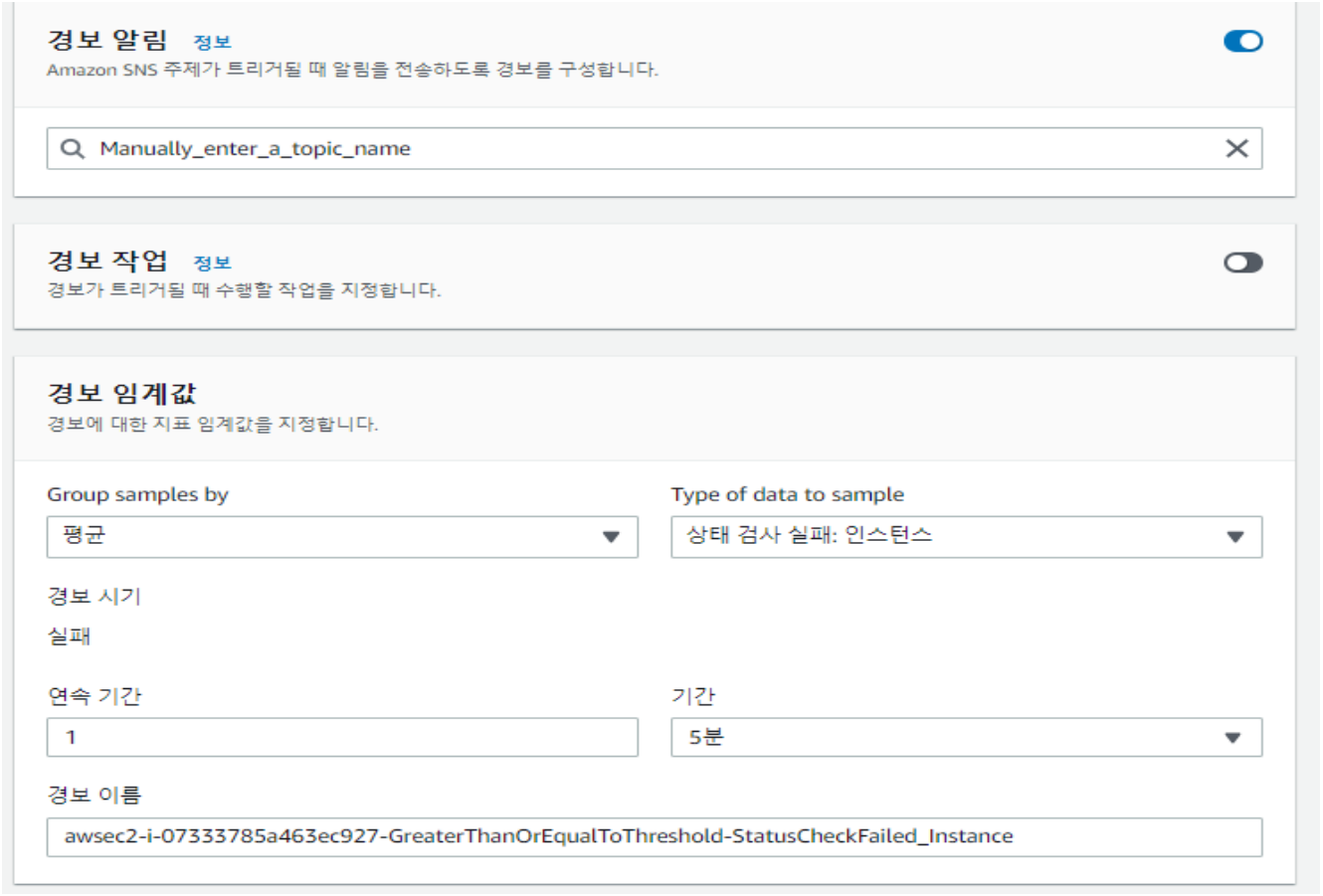
선택 사항 : CloudWatch와 통합하여 MyData Proxy Server 상태 확인을 지원

✓ Single 구성

1. 배포된 MyData Proxy Server인스턴스에 경보를 생성합니다.

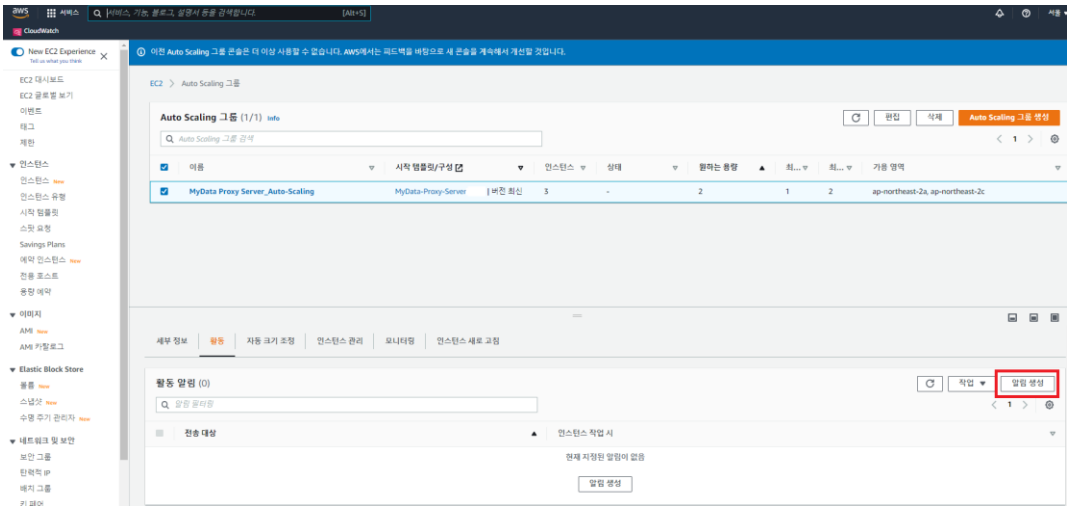
2. 아래와 같이 경보 생성 탭에서 정책을 설정한 후 경보를 생성.

Item	Input Value	Remarks
경보 알림	SNS 로 가는 알람	
경보 임계값	Type of data to sample : 상태 검사 실패 : 인스턴스 연속 기간 : 1	

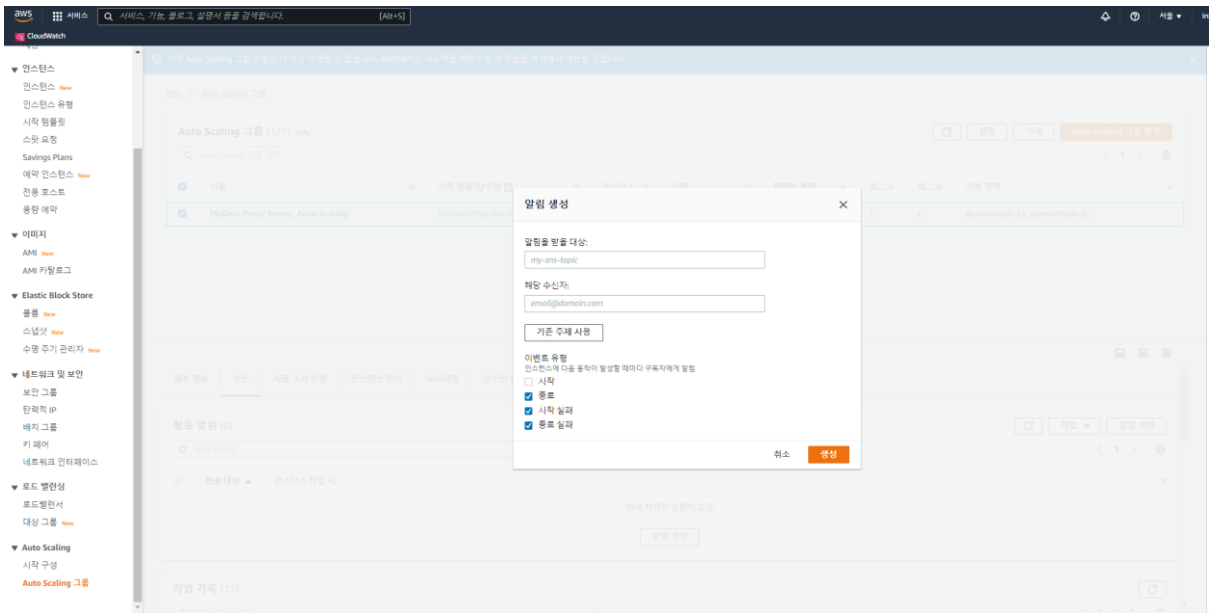


✓ HA 구성

1. [3.1.8] Create an Auto Scaling Group에서 생성한 Auto Scaling Group의 알림 생성



2. 알림을 수신할 대상 및 SNS 정보를 입력



4.6 Disable IMDSv1

선택 사항: IMDSv1기능 비활성화를 위한 AWS CLI 사용

- AWS CLI 사용을 위해 해당 인스턴스의 권한이 있는 IAM 유저의 Access key가 필요합니다. Access Key를 얻는 방법은 아래 링크를 참조하세요.

  https://docs.aws.amazon.com/ko_kr/powershell/latest/userguide/pstools-appendix-sign-up.html

  아래 링크를 통해 AWS 액세스 키 관리를 위한 모범 사례를 확인하십시오.

  https://docs.aws.amazon.com/ko_kr/general/latest/gr/aws-access-keys-best-practices.html

- IMDSv1 비/활성화

  A. SSM을 통해 인스턴스 접속

  B. [aws configure] 명령어 입력 후 정보를 등록합니다.

  - AWS CLI에 대한 자세한 설명은 아래 링크를 참조하세요.

  https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html

  C. IMDSv1 비/활성화

순서	설명	명령어
1	MyData Proxy Server IMDSv1 비활성화	sudo bash /home/ec2-user/IMDSv1/modify-ec2-idmsv2.sh [Instance-Id]
2	MyData Proxy Server IMDSv1 활성화	sudo bash /home/ec2-user/IMDSv1/restore-metadata.sh [Instance-Id]

4.7 Routine Maintenance

✓ AWS 서비스 제한 관리

MyData Proxy Server는 Amazon EC2를 사용합니다. Amazon EC2는 사용자가 사용하는 구성에 따라 서로 다른 리소스를 제공하며, 이러한 리소스는 이미지, 인스턴스, 볼륨, 및 스냅샷이 있습니다. AWS 계정을 생성하면 이러한 리소스에 제한이 리전별로 설정되어 있습니다. 리소스들에 대한 제한 관리에 대한 자세한 내용은 아래 링크를 참조해 주세요.

- Ec2 리소스에 대한 제한 관리: https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/ec2-resource-limits.html

✓ 제품 유지 보수

유지 보수 비용은 계약 정책에 따라 결정되며 최신 릴리스 개발 및 업그레이드 서비스가 포함됩니다.

유지 보수 및 기술 지원에 대한 세부 사항은 추가 계약에 따라 다를 수 있습니다.

유지 보수는 크게 다음과 같이 나뉩니다.

✓ 정기점검 : 유지 보수 계약에 따라 비상점검을 실시한다.

✓ 비상점검 : 유지 보수 계약에 따라 비상점검을 실시한다.

유지보수 범위 :

✓ 솔루션 확인

✓ 패치 및 업그레이드

4.8 Emergency Maintenance

4.8.1 Startup process

➢ User-Startup 과정

A. 시작

순서	설명	명령어
1	Session Manager로 인스턴스 연결	-
2	Proxy Server 설정 확인	cat /app/apim-proxy/conf/application.properties
3	Nano script로 Proxy Server 설정 수정	sudo nano /app/apim-proxy/conf/application.properties
4	Proxy Server 시작	cd /app/apim-proxy/bin && sudo ./start.sh
5	Apache 시작	sudo systemctl start httpd

4.8.2 Health Check

➢ MyData Proxy Server process 확인

순서	설명	명령어
1	Session Manager로 인스턴스 연결	-
2	Proxy Server process check	sudo /app/apim-proxy/bin/sp.sh

명령어 입력 후 정상 :

```
[ec2-user@ip-172-31-44-47 bin]$ source /app/apim-proxy/bin/sp.sh
ec2-user  4106  3396  1 01:42 pts/0    00:00:10 java -cp ../lib/apim-proxy.jar -
Dloader.main=com.inzent.apim.proxy.ProxyApplication org.springframework.boot.loa
der.PropertiesLauncher --spring.config.location=file:../conf/application.propert
ies -Dloader.path=../conf/client-prod.jks
ec2-user 12596  3396  0 01:57 pts/0    00:00:00 grep --color=auto lib/apim-proxy
.jar
```

명령어 입력 후 비정상 :

➢ 프로세스가 감지되지 않음

➢ Apache process 확인

순서	설명	명령어
1	Session Manager로 인스턴스 연결	-

2	Apache process check	sudo systemctl status httpd

명령어 입력 후 정상 :

```
[ec2-user@ip-172-31-44-47 bin]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-07-07 01:46:03 UTC; 16min ago
     Docs: man:httpd.service(8)
 Main PID: 6394 (httpd)
   Status: "Total requests: 3; Idle/Busy workers 100/0;Requests/sec: 0.00303; Bytes served/sec:  10 B/sec"
   CGroup: /system.slice/httpd.service
           ├─6394 /usr/sbin/httpd -DFOREGROUND
           ├─6395 /usr/sbin/httpd -DFOREGROUND
           ├─6396 /usr/sbin/httpd -DFOREGROUND
           ├─6397 /usr/sbin/httpd -DFOREGROUND
           ├─6398 /usr/sbin/httpd -DFOREGROUND
           ├─6399 /usr/sbin/httpd -DFOREGROUND
           └─6793 /usr/sbin/httpd -DFOREGROUND

Jul 07 01:46:03 ip-172-31-44-47.ap-northeast-2.compute.internal systemd[1]: Starting The Apache HTTP Server...
Jul 07 01:46:03 ip-172-31-44-47.ap-northeast-2.compute.internal systemd[1]: Started The Apache HTTP Server.
```

명령어 입력 후 비정상 :

```
[ec2-user@ip-172-31-44-47 bin]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)

Jul 07 01:46:03 ip-172-31-44-47.ap-northeast-2.compute.internal systemd[1]: Starting The Apache HTTP Server...
Jul 07 01:46:03 ip-172-31-44-47.ap-northeast-2.compute.internal systemd[1]: Started The Apache HTTP Server.
Jul 07 02:04:25 ip-172-31-44-47.ap-northeast-2.compute.internal systemd[1]: Stopping The Apache HTTP Server...
Jul 07 02:04:26 ip-172-31-44-47.ap-northeast-2.compute.internal systemd[1]: Stopped The Apache HTTP Server.
```

4.8.3 Type of MyData Proxy Server failures

- 비정상 인스턴스

4.8.4 Recovery procedure for MyData Proxy Server failure

➢ 비정상 인스턴스 발생 시

- HA 구성인 경우 비정상 인스턴스는 ALB 상태 확인 및 자동으로 감지 및 종료됩니다.

스케일링 그룹은 일시 적인 성능 문제가 발생할 수 있지만 관리자 개입이 필요하지 않습니다.

- Single 구성일 경우 [4.4.1] MyData Proxy Server Backup and Restore에서 백업한 AMI를 통해 복구 절차를 수행합니다.

4.8.5 Recovery procedure when MyData Proxy Server recovery fails

✓ 사용자

MyData Proxy Server 복구 실패 시 스냅샷이 있는지 여부에 따라 재설치 방법을 선택할 수 있습니다.

A. 기존 MyData Proxy Server 스냅샷으로 AMI 재생성

B. MyData Proxy Server 재설치 [3.1.4 Create a Launch Template] 절차를 참고.

- HA 구성 [3.1.6] Create an Auto Scaling Group 참고
- Single 구성 [3.1.5] Launch an instance with a Template 참고

4.9 RTO

MyData Proxy Server의 오류가 발생했을 때 기존 설치한 인스턴스의 스냅샷으로 AMI를 다시 만들고 설치하는 지점까지 최소 10분 ~ 최대 30분 정도 소요하며, 제품 설정 및 테스트에는 최대 30분이 소요됩니다.

5. Solution operation

제품을 사용하는 사용자는 Linux CLI 환경에 전문 지식이 있어야 합니다.

5.1 How to set

1. Session Manager로 인스턴스 연결 -> **[sudo systemctl start httpd]** 명령어를 통해 Apache 실행

2. MyData Proxy erver 제어 스크립트의 위치는 /app/apim-proxy/bin

- [ls -al /app/apim-proxy/bin] 명령어를 통해 실행 스크립트 확인

(kill.sh, **sp.sh**, **start.sh**)

```
[ec2-user@ip-172-31-44-47 apim-proxy]$ ls -al /app/apim-proxy/bin
total 12
drwxrwxr-x 2 ec2-user ec2-user  50 Jul  7 01:42 .
drwxrwxr-x 6 ec2-user ec2-user  69 Jun 21  2021 ..
-rwxrwxr-x 1 ec2-user ec2-user  79 Jun 21  2021 kill.sh
-rwxrwxr-x 1 ec2-user ec2-user  33 Jun 21  2021 sp.sh
-rwxrwxr-x 1 ec2-user ec2-user 257 Jun 21  2021 start.sh
[ec2-user@ip-172-31-44-47 apim-proxy]$
```

➢ **선택사항:** MyData Proxy Server SSL/TLS 구성

아래 링크를 통해 2단계부터 확인하세요 :

https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/SSL-on-amazon-linux-2.html

- MyData ProxyServer의 설정 파일 편집
- Nano 스크립트 편집기

  ➔ [**sudo nano /app/apim-proxy/conf/application.properties**]

```
 GNU nano 2.9.8                    /app/apim-proxy/conf/application.properties

#debug=true

spring.application.name=client

server.ssl.key-store=file:../conf/client-prod.jks
server.ssl.key-store-password=changeme
server.ssl.key-password=changeme
server.ssl.trust-store=file:/etc/pki/java/cacerts
server.ssl.trust-store-password=changeit
# Mutual TLS/SSL
server.ssl.client-auth=need
server.port=9000
server.ssl.enabled=false
proxy.ssl.client.validateCertificate=true
proxy.ssl.client.enabled=false

#proxy.ip.allow=127.0.0.1
logging.level.org.springframework.web.client.RestTemplate=DEBUG
#logging.level.org.apache.http=DEBUG
#logging.level.httpclient.wire=DEBUG
#server.ssl.reloadShell=cmd.exe /c renewCA.cmd
#server.ssl.reloadShell=sh ../conf/renewCA.sh
```

- Vi 스크립트 편집기
  - [**sudo vi /app/apim-proxy/conf/application.properties**]
- MyData Proxy Server 설정

항목	설명
server.port	프록시 서버 포트
server.ssl.key-store	jks인증서 경로
server.ssl.key-store-password	Jks인증서 비밀번호
server.ssl.key-password	Jks인증서 비밀번호
server.ssl.trust-store	Cacert Jks인증서 경로
server.ssl.trust-store-password	Cacert JKS인증서 비밀번호
server.ssl.enabled	https수신여부 설정(true/false)

proxy.ssl.client.validateCertificate	서버인증서 유효성 체크
proxy.ssl.client.enabled	클라이언트를 반드시 https 연결
server.ssl.client-auth	MTLS 설정 NEED : Client authentication is needed and mandatory. NONE: Client authentication is not wanted. WANT : Client authentication is wanted but not mandatory.
logging.level.org.springframework.web.client.RestTemplate	클라이언트 접속 로그 레벨 설정
logging.level.org.apache.http	프록시 서버 접근로그 레벨 설정
logging.level.httpclient.wire	프록시 서버 접근로그 레벨 설정

5.2 How to run

1. MyData Proxy Server 실행

2. Apache 실행

3. 실행 및 운용에 관한 명령어는 아래표를 통해 확인

✓ MyData Proxy Server 운용 명령어

➢ [cd /app/apim-proxy/bin]을 통해 스크립트 제어 스크립트 폴더로 이동합니다.

명령어	설명
sudo ./start.sh	Proxy Server 실행
sudo ./sp.sh	Proxy Server 프로세스 확인
sudo ./kill.sh	**(선택 사항)** Proxy Server 종료

✓ Apache 운용 명령어

명령어	설명
sudo systemctl start httpd	Apache 실행
sudo systemctl status httpd	Apache 프로세스 확인
sudo systemctl restart httpd	**(선택 사항)** Apache 재시작
sudo systemctl stop httpd	**(선택 사항)** Apache 중지

4. 로그 저장 위치

Apache 로그는 AWS EFS에 저장이 되며 저장 경로는 아래와 같습니다.

- /mnt/proxy/log

```
sh-4.2$ pwd
/mnt/proxy/log
sh-4.2$ ls -al
total 648
drwxr-xr-x 2 root root    107 Aug 17 04:10 .
drwxr-xr-x 3 root root     17 Aug 10 04:56 ..
-rw-r--r-- 1 root root 589457 Aug 17 03:41 access_log
-rw-r--r-- 1 root root  12306 Aug 17 04:10 error_log
-rw-r--r-- 1 root root  42853 Aug 17 04:13 ssl_access_log
-rw-r--r-- 1 root root   4164 Aug 17 04:10 ssl_error_log
-rw-r--r-- 1 root root    198 Aug 17 04:13 ssl_request_log
sh-4.2$
```

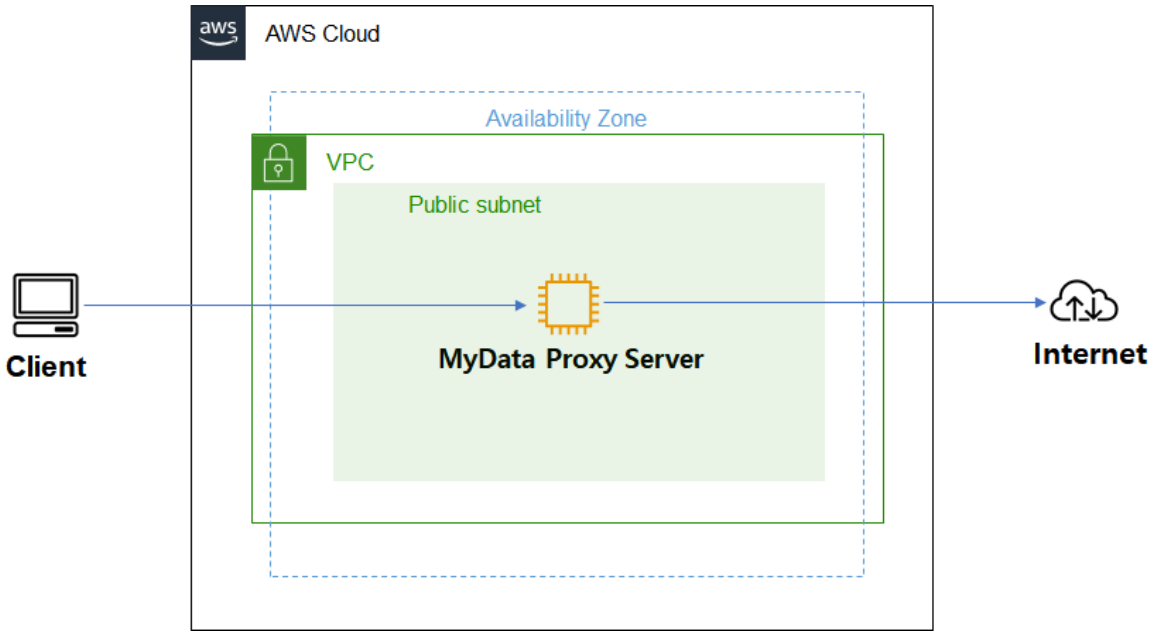
MyData Proxy Server의 Debug 로그 위치는 아래와 같습니다.

- /app/apim-proxy/log

```
[ec2-user@ip-172-31-44-47 log]$ pwd
/app/apim-proxy/log
[ec2-user@ip-172-31-44-47 log]$ ls -al
total 4
drwxrwxr-x 2 ec2-user ec2-user   24 Jul  7 01:39 .
drwxrwxr-x 6 ec2-user ec2-user   69 Jun 21  2021 ..
-rw-rw-r-- 1 ec2-user ec2-user 2987 Jul 12 07:13 output.log
[ec2-user@ip-172-31-44-47 log]$
```

5. Testing and setting up forward and reverse proxies

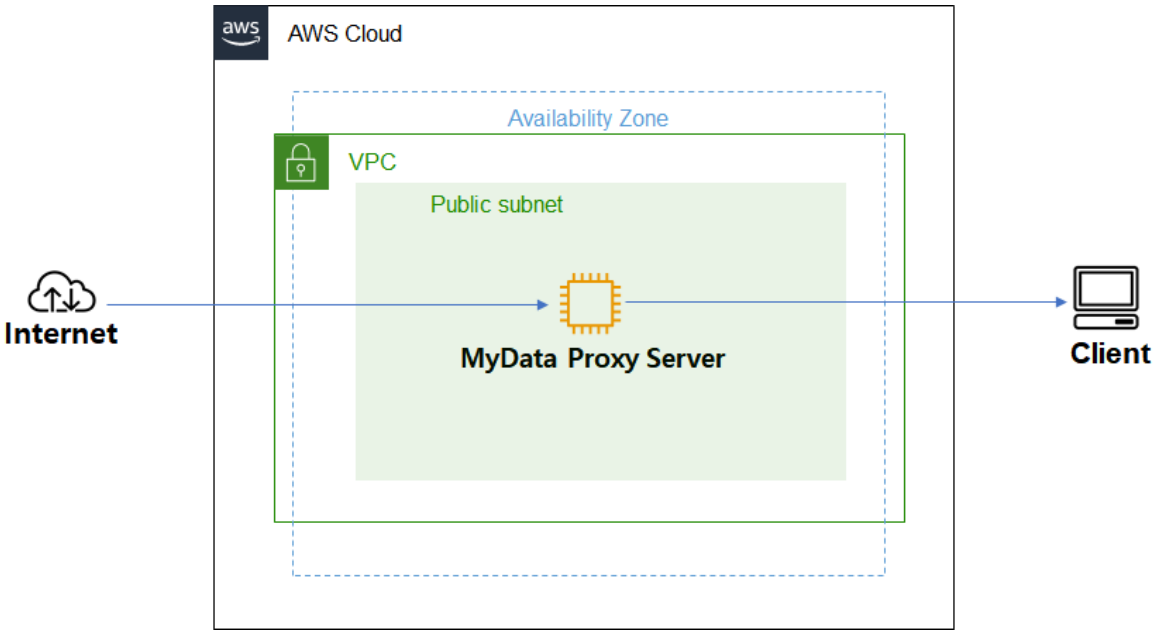
A. Forward Proxy



✓ MyData Proxy Server를 실행한 상태에서 아래 명령어를 통해 Forward Proxy 기능을 테스트 할 수 있습니다.

➔ [curl --location --request GET **[http://MyData Proxy Server-instance-IP:9000]** --header x-target-host: **[Target-host]**]

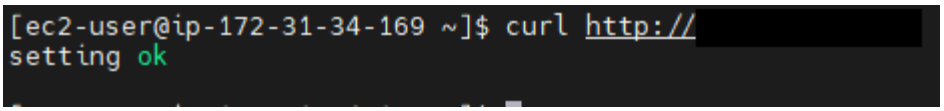
B. Reverse Proxy



➢ Reverse proxy setting for http communication

I. Apache Server 실행 후 Reverse proxy 기능 확인

➔ [**curl http://[My Data Proxy Server IP]**]



II. **[sudo nano /etc/httpd/conf/httpd.conf]** 아래를 참고하여 수정

Setting to change	How to change
ProxyPreserveHost On ProxyPass / http://www.inzent.com/ ProxyPassReverse / http://www.inzent.com/	ProxyPreserveHost On ProxyPass / [Target-Host] ProxyPassReverse / [Target-Host]

5.3 Key management

A. EBS Key 관리

필요한 경우 EBS 암호화를 지원하도록 AWS KMS keys를 사용할 수 있습니다.

아래 링크를 통해 EBS 볼륨 암호화 관리를 확인하세요 :

https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/EBSEncryption.html

B. IAM 사용자의 액세스 키 관리

IAM 사용자의 액세스 키는 외부에 노출을 피해야 하고 주기적으로 교체를 수행해야합니다.

아래 링크를 통해 액세스 키 관리를 확인하세요 :

https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/id_credentials_access-keys.html

5.4 Patches and updates management

패치/업데이트 관하여 아래 링크를 통해 문의가 가능하며 계약사항에 따라 별도로 처리됩니다.

URL : http://www.inzent-mydata.com/Questions.php

6. Support

6.1 Technical support

기술 지원 서비스는 문서에 명시된 기능에 대해서만 제공합니다.

기술 지원 범위는 다음과 같습니다.

- ➢ 설치 지원 : Github 소스제공, 설치 가이드 제공
  - ■ Github : https://github.com/InzentSaaS/MyData-Proxy-Server
- ➢ 커스터마이징 지원

기술 지원 연락처는 다음과 같습니다.

- ➢ URL : http://www.inzent-mydata.com/Questions.php
- ➢ TEL : 070)8209-6189
- ➢ E-mail : info@inzent.com

6.2 Support Costs

- Free Tier

- Free

- Technical Service Pack

- 15 hour : 2,250,000 원
- 30 Hour : 4,000,000 원
- 60 Hour : 7,500,000 원
- 120 Hour : 14,000,000 원

계약 시 :

- ➢ 커스터마이징 지원 (공수 별도산정)

6.3 SLA

- Free Tier : 소스 제공, 설치 가이드

- Technical Service Pack : 고객 요청 시, 기준 시간에 해당하는 기술 지원 수행

Request Type	Estimated Time
Emergency check	< 2 Hour
System Check and Upgrade	< 4 Hour
mTLS spec. support	< 4 Hour
Customer-required transaction configuration	< 8 Hour