INZENT

MyData Proxy Server V1.0

Contents

1. Product Overview

This article assumes you have used AWS before and are familiar with AWS services. If you are new to AWS, please refer to the AWS documentation (https://docs.aws.amazon.com/). You should also be familiar with the following AWS technologies:

:

- Amazon Virtual Private Cloud(Amazon VPC) - The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
- Amazon EC2 – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.
- Amazon EFS – Amazon Elastic File System (Amazon EFS) is a serverless, set-and-forget elastic file system for use with AWS cloud services and on-premises resources. Built to scale to petabytes on demand without disrupting applications, it automatically scales up and down as users add and remove files, eliminating the need to provision and manage capacity as data grows. Amazon EFS has a simple web service interface that allows you to quickly and easily create and configure file systems. The service manages all of your file storage infrastructure, freeing you from the complexity of deploying, patching, and maintaining complex file system configurations.

1.1 Introduction

MyData Proxy Server is an application program that is located in the DMZ section in a network-separated business environment and allows API GW and business PCs in the internal network to indirectly access Internet services. It is used for OUT-BOUND transactions for the purpose of data collection through the Internet for the purpose of collecting MyData, etc., and supports SSL that meets the MyData communication standard.

- What is MyData?

As Korea's 3 data law was passed, the MyData concept of "I am the owner of my data" is attracting attention. Once the MyData concept is established, consumers can peddle the sovereignty of the data they create, and financial companies can find new business models such as customized asset management by receiving data with individual consent.

1.1.1 Prerequisites and Requirements

This topic describes the prerequisites and resource requirements for using MyData Proxy Server with Amazon Web Services (AWS).

- **Prerequisites**

1. AWS Account
   You must have an AWS account set-up. If you don't, we recommend that you visit the following site : https://aws.amazon.com/getting-started/

2. OS
   MyData Proxy Server AMI is available an Amazon Linux, and you can choose an OS familiar with Linux.

3. AWS Resource
   AWS Resources for using MyData Proxy Server are for configuration, please refer to [1.1.3] Architecture Diagrams.

자원	개수
VPC	**1**
VPC Security Groups	**1**
IAM 역할	**1**
EFS	**1**
KMS	**2**
EC2 instance	**1**

4. Service quotas
   If necessary, you can request an increase in the service quota for a resource.

You should request a quota increase to no exceed the default limit for resources shared across multiple deployments. The resource quotas for the ap-northeast-2 Region can be found at the following link.
https://console.aws.amazon.com/servicequotas/home?region=ap-northeast-2#!/

- For more information about resource quotas, please refer to the link below.

5. IAM

Before Starting the deployment steps for MyData Proxy Server, refer to list 3 and access the AWS Management Console with IAM permission for the resource and SSM to be deployed.

- See the following link for best practices for IAM permissions
  https://docs.aws.amazon.com/ko_kr/IAM/latest/UserGuide/best-practices.html#grant-least-privilege
- The Administrator Access managed policy within IAM provides sufficient permissions, but if you want to use a custom policy that has more restrictions for your organization, please refer to the following link.
  https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html
  .

- **Requirements**

Virtual Machines(VMs) are required to install MyData Proxy Server

VM Name (Tag)	VM type	Default VM Count
MyData Proxy Server	t2.medium or t3.medium	**1**

The number may change according to customer environment.

1.1.2 Region support

The regions where the product is supported are as follows

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

1.1.3 Architecture Diagrams

- Public subnet, MyData Proxy Server EC2 instance

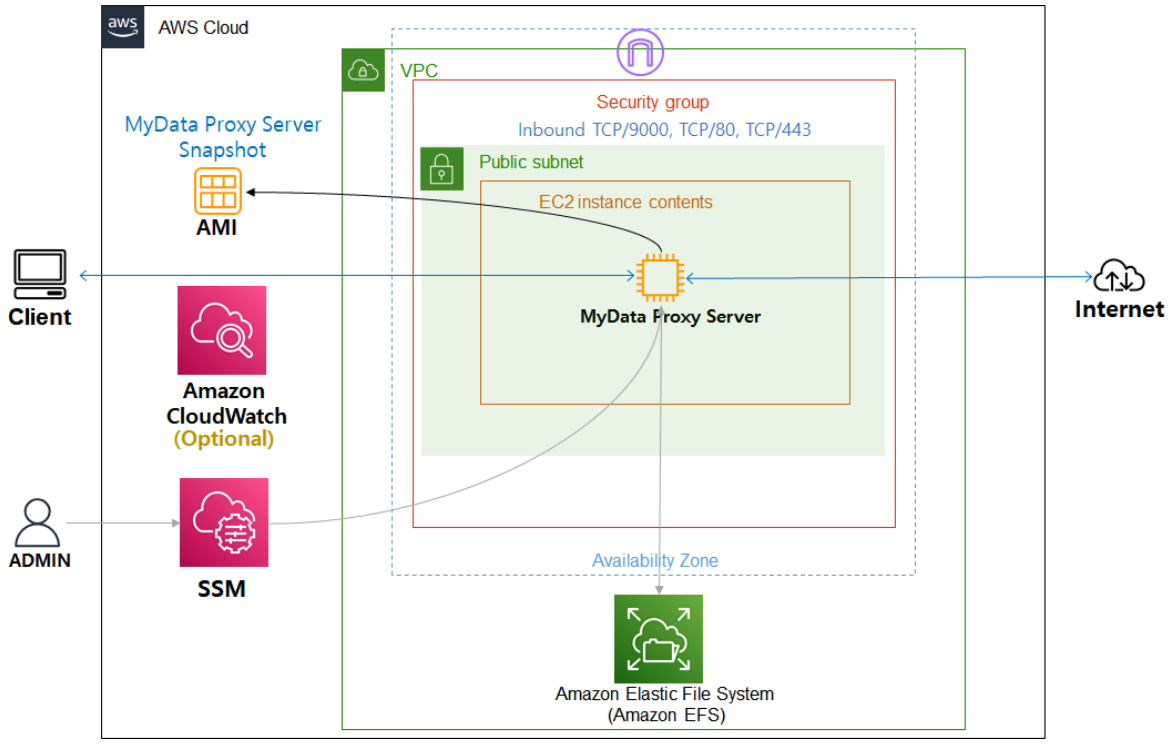
- Backup and Multiplex Using Amazon Machine Image(AMI)

- Use Amazon EFS to access shared data on the file system of the MyData Proxy Server EC2 instance.

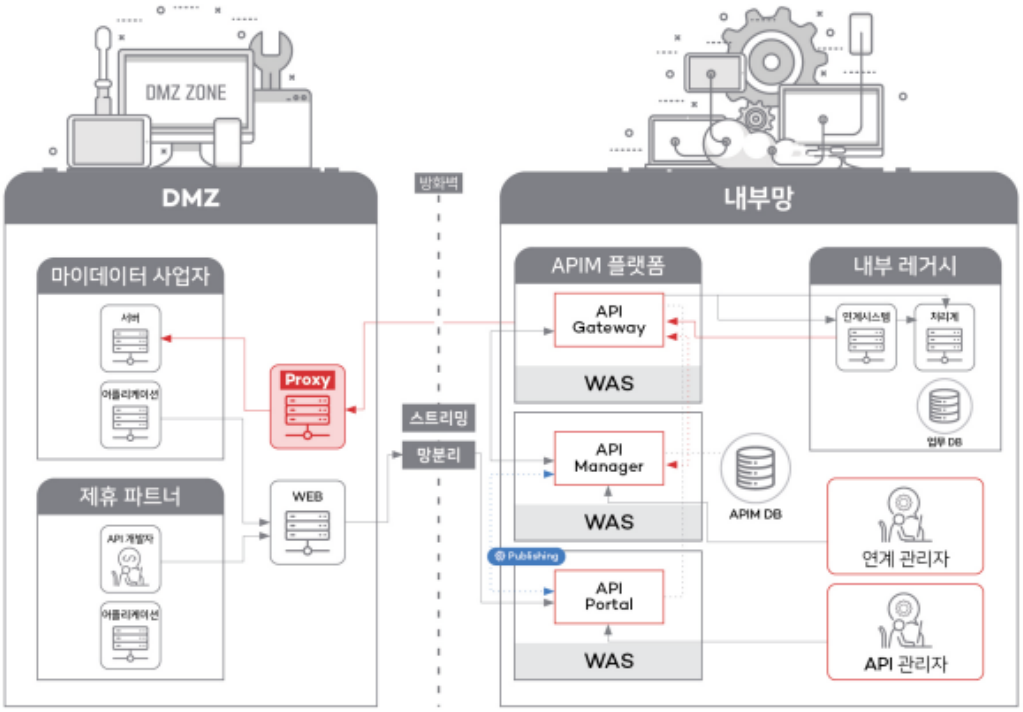
- You access the instance through the Session Manager feature of the AWS System Manager service.

- **(optional)** MyData Proxy Server health monitoring and notification using Amazon Cloud Watch service.

➢ MyData Proxy Server Architecture Diagrams



1.1.4 Use case



INZEN's MyData Proxy Server is located in the DMZ section in a network-separated work environment and is an application that allows API GW and work PCs in the internal network to indirectly access internet services. Like a general proxy, it provides basic functions of a proxy server such as Forward Proxy and Reverse Proxy, so it can be used as a general proxy server as shown in the figure below.

Environment	Use case
On-premise	**[KCB]** This an example of using a proxy server to build a private cloud-based MyData operator system http://www.inzent-mydata.com/board/board.php?bo_table=case&pg=1&idx=13
Public Cloud	**[교보생명]** This is a case used to build a Hybird Cloud-based MyData platform. http://www.inzent-mydata.com/board/board.php?bo_table=case&pg=2&idx=6

1.1.5 Deployment time

The deployment phase can take a minimum of 10 minutes to as maximum of 30 minutes,

and setup and product testing can take up to 30 minutes.

2. Planning Guidance

2.1 Security

All you need to install/control your MyData Proxy Server deployment is instance access via SSM or SSH access(key-based authentication/sudo or similar mechanism is preferred)

- Not using AWS root credentials for access

2.2 Costs and Licenses

MyData Proxy Server product is provided free of charge. For additional AMIs, please contact us through the link below.

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

- Full list of billable AWS services

You are responsible for the cost of AWS services. The cost of the resources generated by the menu depends on the instance you use. For more information, see the pricing pages for the AWS services you use in this guide (https://aws.amazon.com/pricing/).

A. EC2 Instance(essential)
B. EBS(essential)
C. EFS (essential)
D. KMS(essential)
E. Cloud watch(optional)

2.3 Sizing

MyData Proxy Server의 AMI support the instance specifications shown in the table below on AWS. For up-to-date information on each type of instance, please refer to the link next to it. (https://aws.amazon.com/ko/ec2/instance-types/)

size of logs	Instance type	Vcpu	Memory(GiB)	EBS Volume	EBS Volume Type
~5GB	t2.medium or t3.medium	2	4	10GB	General Purpose SSD (gp2)

3. Deployment steps

3.1 Mydata Proxy Server Installation

The following AWS Resources are required for MyData Proxy Server deployment.

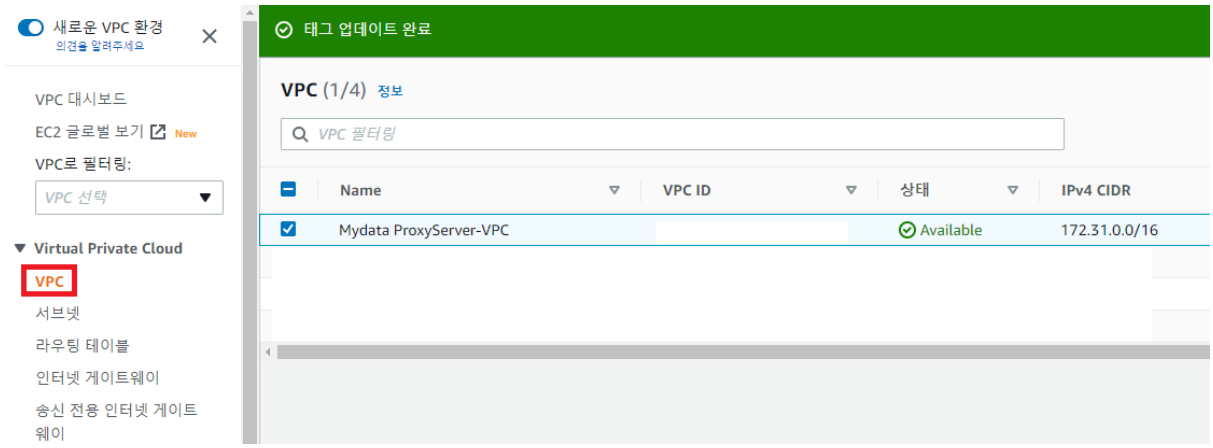
- ✓ AWS Resources :
  - Amazon Virtual Private Cloud(VPC)
  - Internet Gateway
  - Amazon VPC subnets **(public)**
  - Amazon EC2 Instance
  - Amazon Elastic File System
  - Amazon Cloud Watch **(Optional)**

3.1.1 Create VPC AND Subnet

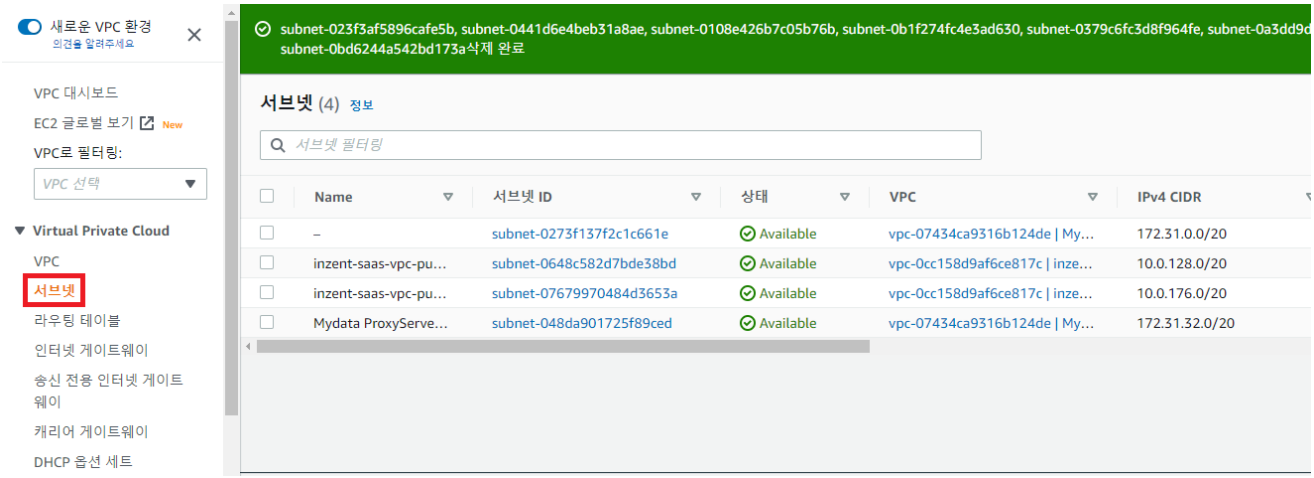
Subnet Setting that manage MyData Proxy Server

- ➢ Check existing VPCs and subnets

1. [console home > service> Networking and Content delivery > VPC] You can check the VPC setting

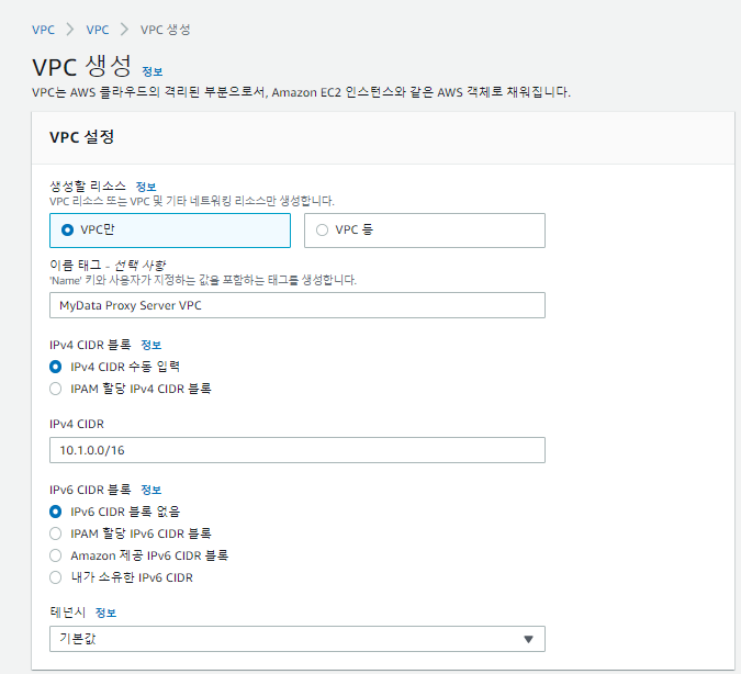


2. [console home > service> Networking and Content delivery > VPC > subnet] You can check the subnet setting



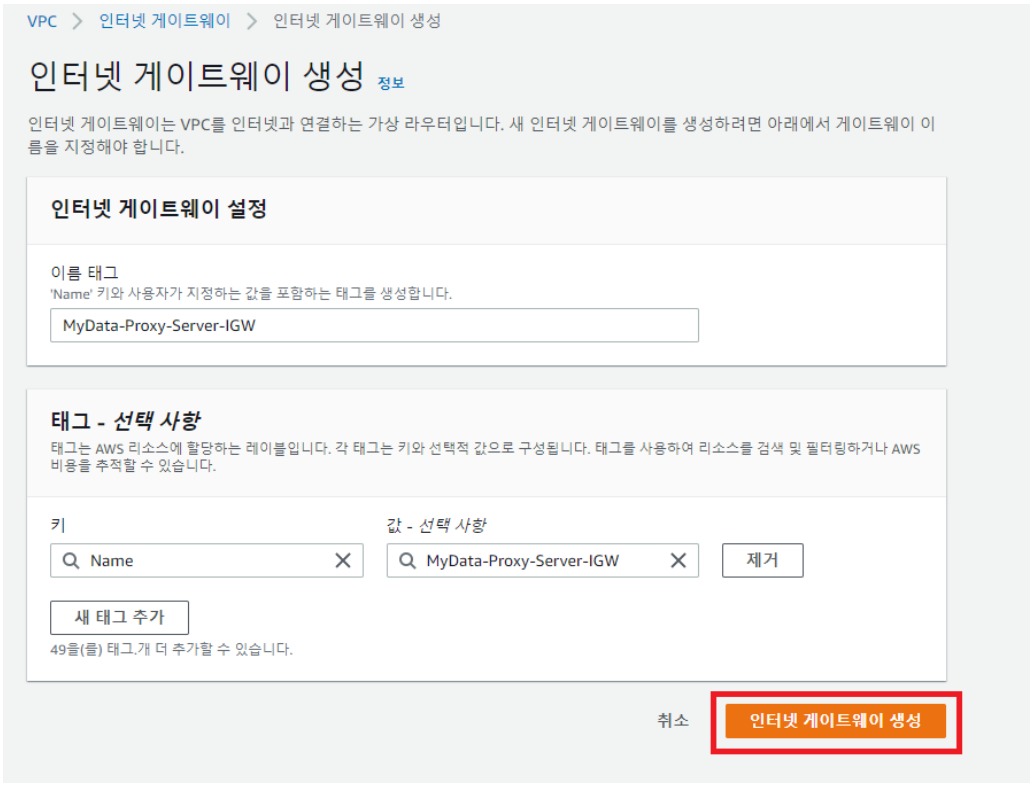
➢ Create MyData Proxy Server VPC

1. Go to Amazon VPC console (https://console.aws.amazon.com/vpc).
2. In the navigation pane, select VPC and then select Create VPC.
3. Create a VPC and specify a range of IPv4 addresses for the VPC.

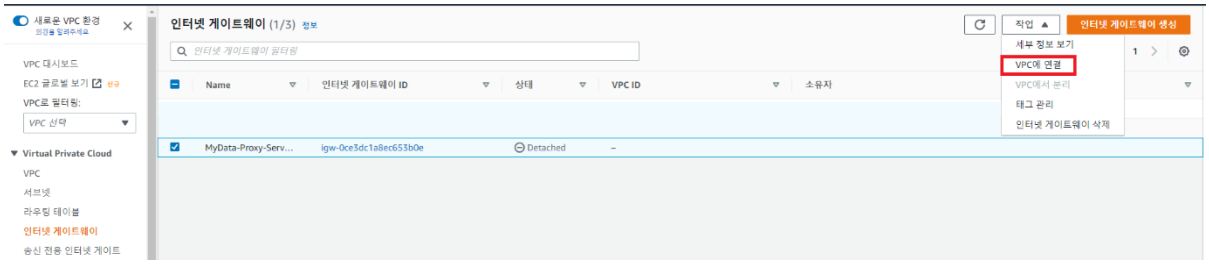


➢ Create Internet gateway, and attach it to VPC

1. Go to Amazon VPC console (https://console.aws.amazon.com/vpc).
2. In the navigation pane. Select Internet Gateway and then select Create Internet Gateway



3. Attach to Internet Gateway VPC



➢ Create MyData Proxy Server subnet

1. Go to Amazon VPC console (https://console.aws.amazon.com/vpc).
2. In the navigation pane, select Subnet and then select Create Subnet.
3. Optionally specify subnet details and choose Create.

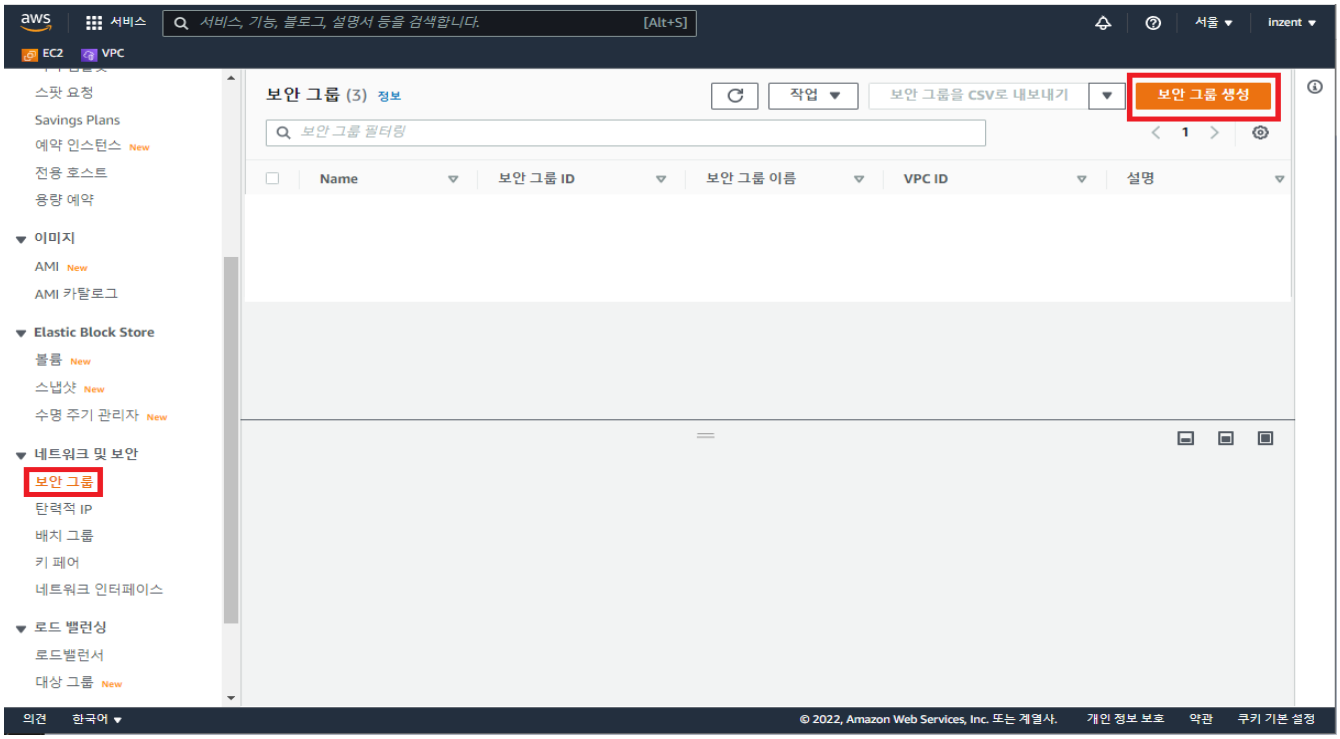
Menu	Input Value
Subnet name	MyData Proxy Server Subnet
VPC	Choose an existing VPC that is the same as your web tier
VPC CIDRS	-
Availability Zone	Refer [1.1.3] Architecture Diagrams
IPv4 CIDR block	For information about Subnet group, see the following link : https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Subnets.html

3.1.2 Create Security Group

You need to set up security groups for the MyData Proxy Server and Client, Internet to communicate with each other

➢ Create MyData Proxy Server Security Groups

1. Access the AWS EC2 Management Console.
2. Select [NETWORK & SECURITY > security Groups] and click on the Create Security Group button.



3. As shown below, add a new rule to the Inbound rule.

Menu	Input Value
Security Group name	MyData Proxy Server SG
Description	MyData Proxy Server-SSH SG
VPC	Choose the same VPC as the device used by the operator
Type	SSH
Protocol	TCP
Port Range	22
Source	User IP or Device IP to be used by user

Menu	Input Value
Security Group name	MyData Proxy Server SG
Description	MyData Proxy Server-HTTP SG
VPC	Choose the same VPC as the device used by the operator

Type	HTTP
Protocol	TCP
Port Range	80
Source	0.0.0.0/0

Menu	Input Value
Security Group name	MyData Proxy Server SG
Description	MyData Proxy Server-HTTPS SG
VPC	Choose the same VPC as the device used by the operator
Type	HTTPS
Protocol	TCP
Port Range	443
Source	0.0.0.0/0

Menu	Input Value
Security Group name	MyData Proxy Server SG
Description	MyData Proxy Server-SSH SG
VPC	Choose the same VPC as the device used by the operator
Type	Custom TCP
Protocol	TCP
Port Range	9000
Source	Client IP

4. Set up outbound rules for data communication

Menu	Input Value
Security Group name	MyData Proxy Server SG
Description	MyData Proxy Server OutBound
VPC	Choose the same VPC as the device used by the operator

Type	All TCP
Protocol	TCP
Port Range	0~65535
Source	0.0.0.0/0

5. Add a Name Tag to [Tags] as follows

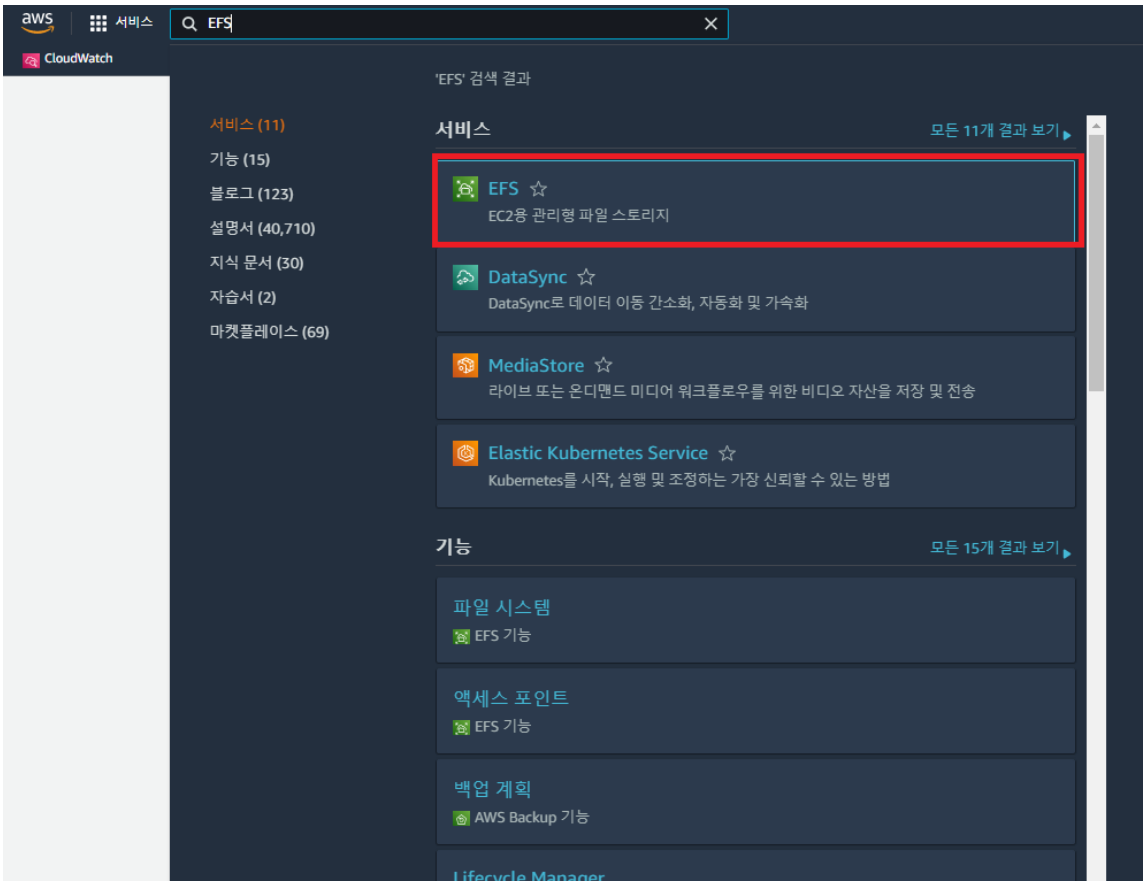
Menu	Input Value	Menu	Input Value
Tag	Name	Description	Tagging to identify groups
Value	MyData Proxy Server SG		

3.1.3 Create EFS

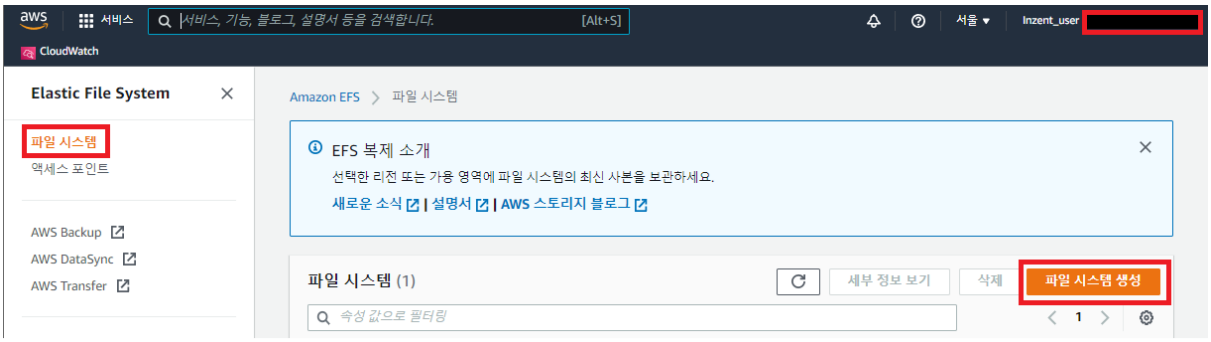
You need to create Amazon EFS to store the log files of MyData Proxy Server

- Create a file system

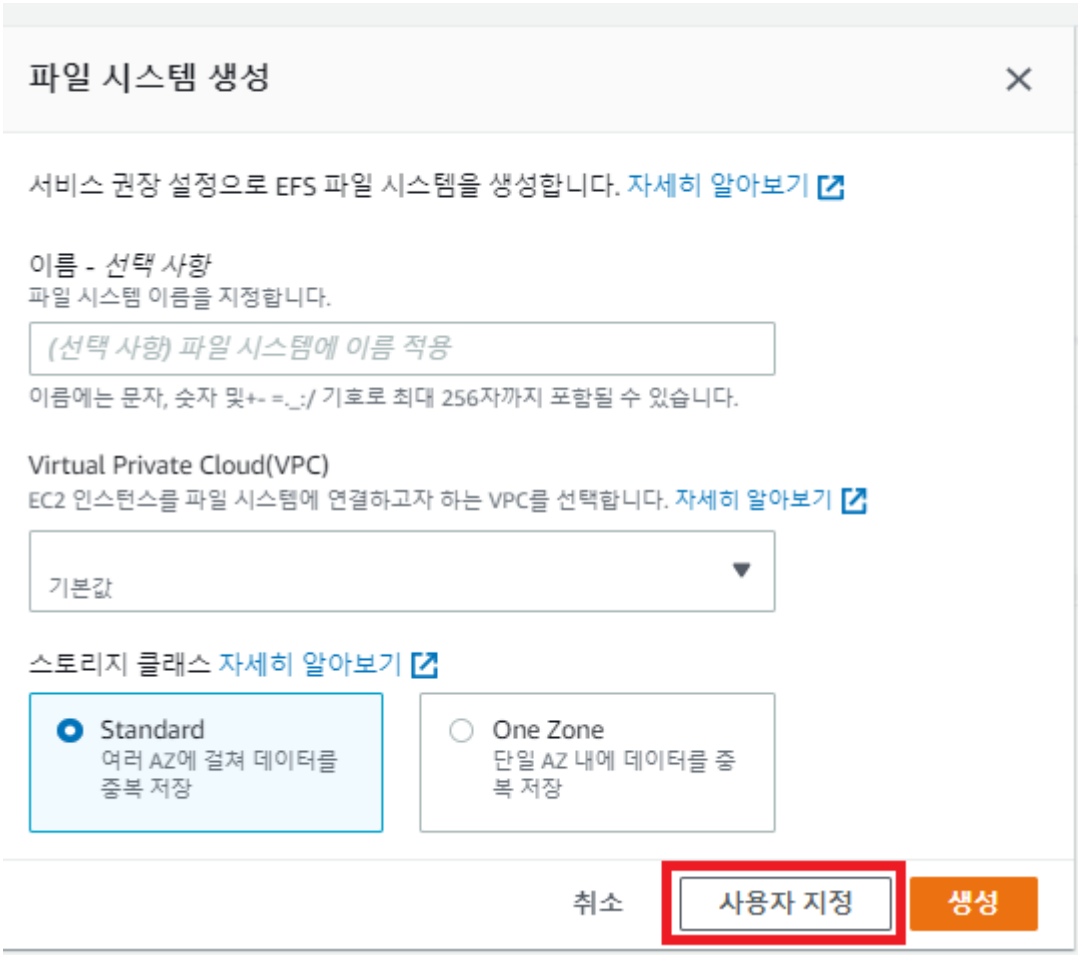
A. Access the EFS main screen through [Console Home > Service > EFS]



B. [Console Home > Service > EFS > File System > Create File System]



C. Under Create File System, click Customize



D. [Amazon EFS > File System > Create Step 1 File System Setup]

Menu	Input value	Description
Name	MyData-Proxy-Server	Specifies the file system name

Storage class	Standard	More details : https://docs.aws.amazon.com/efs/latest/ug/storage-classes.html
Automatic backup	**(Optional)**	More details : https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html
Switch to IA	30 days since last access	EFS Intelligent-Tiering uses lifecycle management to automatically achieve the right price and performance blend for your application by moving files between Standard-Infrequent Access storage classes -
Transition outside IA	when first accessed	
Performance mode	universal	Set performance mode for file system based on required IOPS
Throughput mode	burst	Setting how the throughput limit of the file system is determined
Encryption	Enable data encryption at rest	Optional to enable encryption of data at rest in the file system, by default the KMS service key (aws/elasticfilesystem) is used. See the link below for more information and customization of encryption settings.https://docs.aws.amazon.com/efs/latest/ug/encryption.html
Tag	Tag key : Name	Tagging to identify file systems
	Tag value : MyData Proxy Server-EFS	

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

Menu	Input value	Description
Virtual Private Cloud (VPC)	Select the VPC created in [3.1.1]	Choose the VPC in which you want to connect your EC2 instances to your file system.
Mount target	[1.1.3] Select the number of mount targets by referring to the Architecture Diagrams	A mount target provides an NFSv4 endpoint on which you can mount an Amazon EFS file system. We

	- Availability Zone: [3.1.1] Create the same subnet as created in Create VPC and Subnet - Subnet ID : [3.1.1] Subnet ID created in Create VPC and Subnet - IP address: Default - Security group: Select the security group ID of [MyData Proxy Server-EFS SG] created in [3.1.2] Create Security Group	recommend that you create one mount target for each Availability Zone.

F. [Amazon EFS > File System > Create > Step 3 File System Policy]

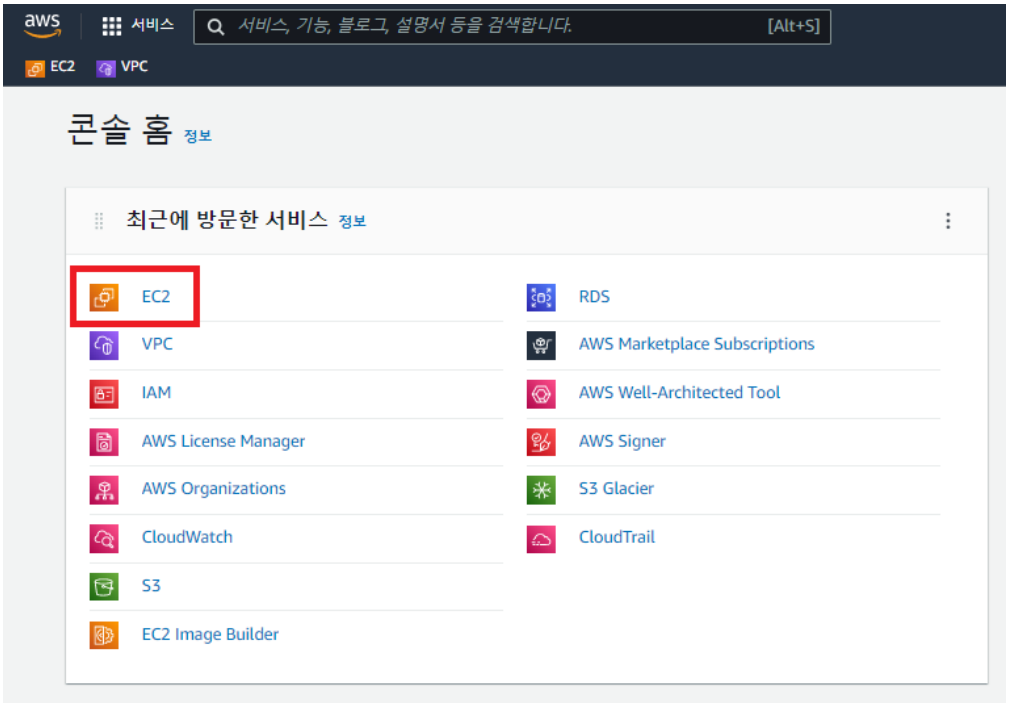
MyData Proxy Server recommends default settings, and if you want to set policies, refer to the link below.

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

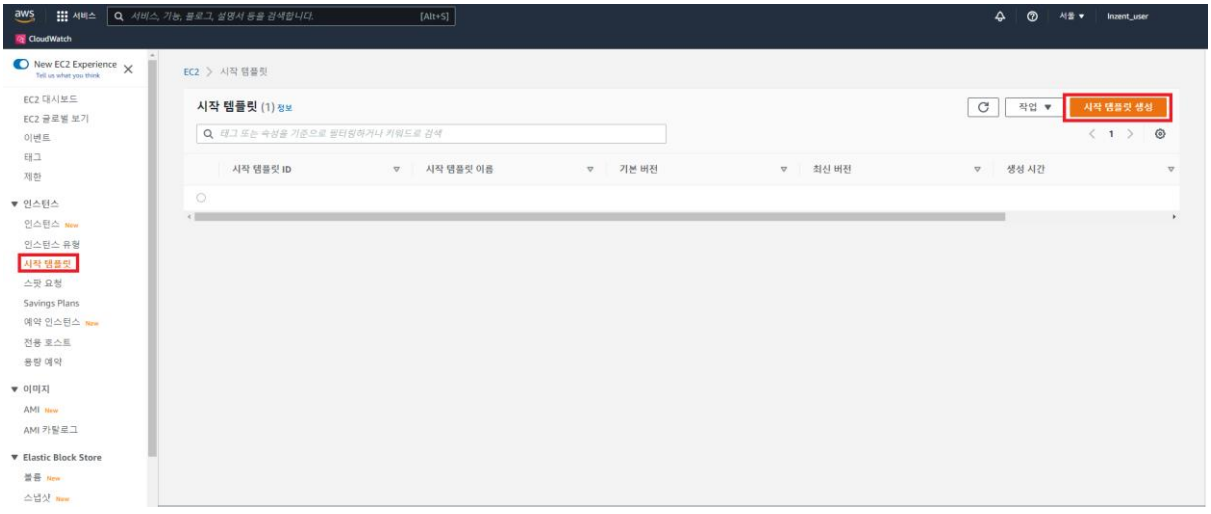
3.1.4 Create a Launch Template

- ✓ Create launch template with MyData Proxy Server AMI

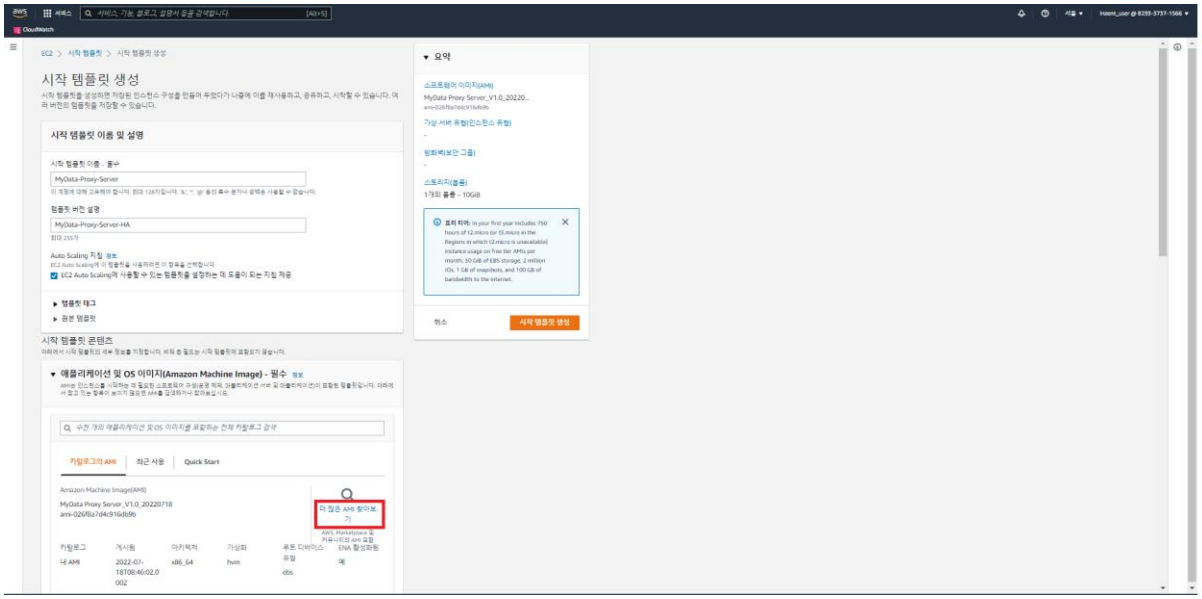
1. Access the AWS EC2 console



2. Click Create Launch Template in [EC2 > Launch Templates]



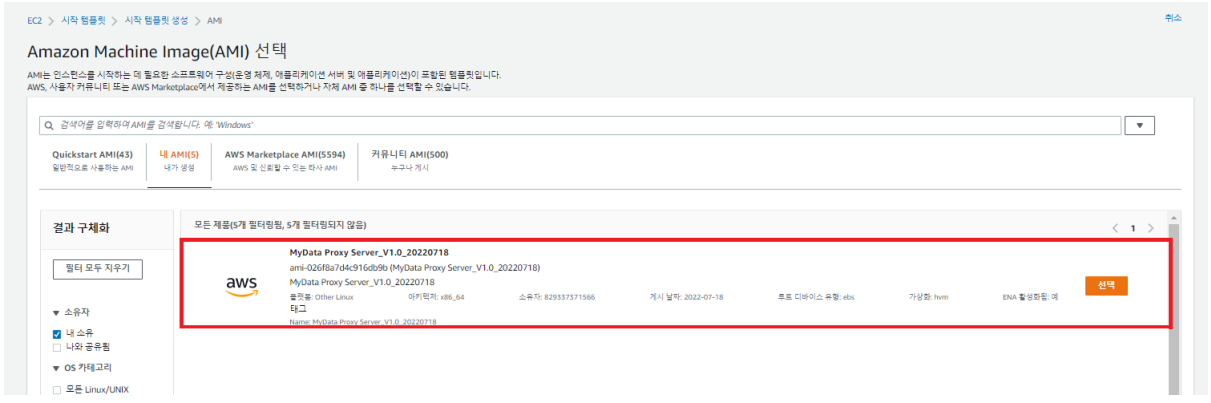
3. [EC2 > Launch Templates > Create Launch Template] Launch Template Name and Description



매뉴	Input Value
Startup template name	MyData-Proxy-Server
Template Version Description	1.0
Auto Scaling Guidelines	**Optional**

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

   - ➢ Click Browse More AMI
   - ➢ Select the provided AMI



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

Menu	Input Value
Instance type	**[2.3] Sizing See and select**
Key pair name	No included in launch template
Subnet	See [1.1.3] Architecture Diagrams and [3.1.1] Create VPC and Subnet
Security group	See [3.1.2] Create Security Group

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

Menu	Input Value
Size	**See [2.3] Sizing**
Volume type	**See [2.3] Sizing**
Delete on exit	Yes
Encrypted	Yes
KMS key	(default) aws/ebs or KMS key generated, See [4.2] EBS Volume encryption

7. [EC2 > Launch Templates > Create Launch Template] Resource Tag

➢ Tagging MyData Proxy Server instance

Menu	Input Value	Menu	Input Value
Key	Name	Description	Tagging to identify instances
Value	MyData Proxy Server		
Resource type	Instance		

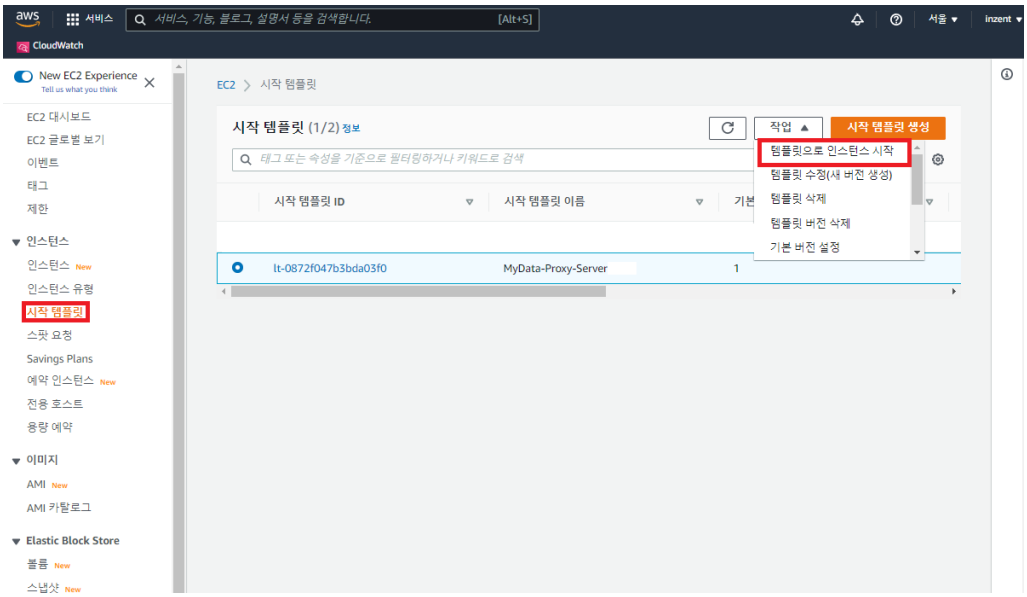
8. [EC2 > Launch Templates > Create Launch Template] Advanced Details

Menu	Input Value	Description
IAM Instance Profile	[AmazonSSMRoleForInstancesQuicksetup]	IAM Role to connect to the instance using SSM

user data	#! /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 --//	EFS mount and Apche server, Proxy server start when instance starts
etc	default	-

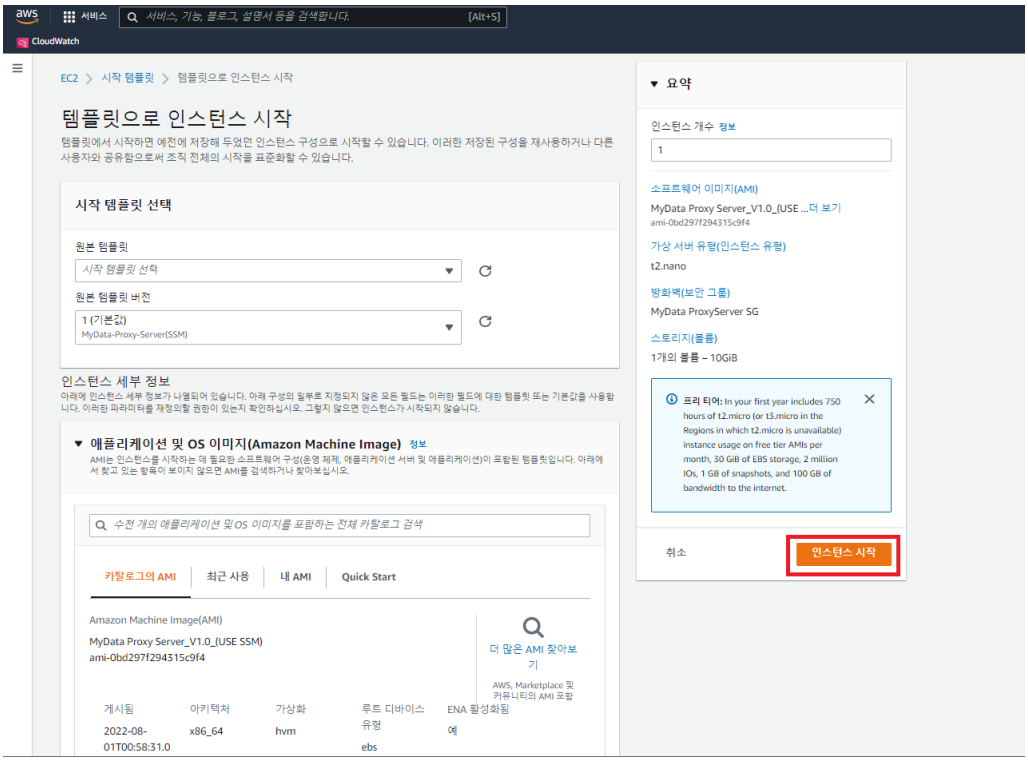
3.1.5 Launch an instance with a Template

1. [EC2 > Launch Template] Launch an instance with a template



2. [EC2 > Launch Template > Launch Instance with Template] Click Launch Instance

   ✓ Key pair **(Optional)**



4. Operational Guidance

4.1 Connecting to Instances Using Session Manger

Session Manager is a fully managed AWS System Manager feature that lets you manage your Amazon EC2 instances through an interactive, one-click browser-based shell or the AWS CLI.

- Connect to your instance using Session Manager using the Amazon EC2 console

  1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/
  2. In the navigation pane, choose Instances.
  3. Choose your instance and choose **Connect.**
  4. In Connect to Instance, select **Session Manager** and connect.

- For more information about **Session Manager**, refer to the link below.

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

4.2 EBS Volume encryption

You can use Amazon EBS Encryption as a simple encryption solution for EBS resources associated with EC2 instances. Amazon EBS encryption eliminates the need to build, maintain, and secure your own key management infrastructure. Amazon EBS encryption uses AWS KMS Keys when creating encrypted volumes and snapshots.

You need to set up encryption settings for EBS Volume and encryption settings for snapshot volumes by referring to the link below.

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

4.3 Encrypting Amazon EFS Data & Metadata at Rest

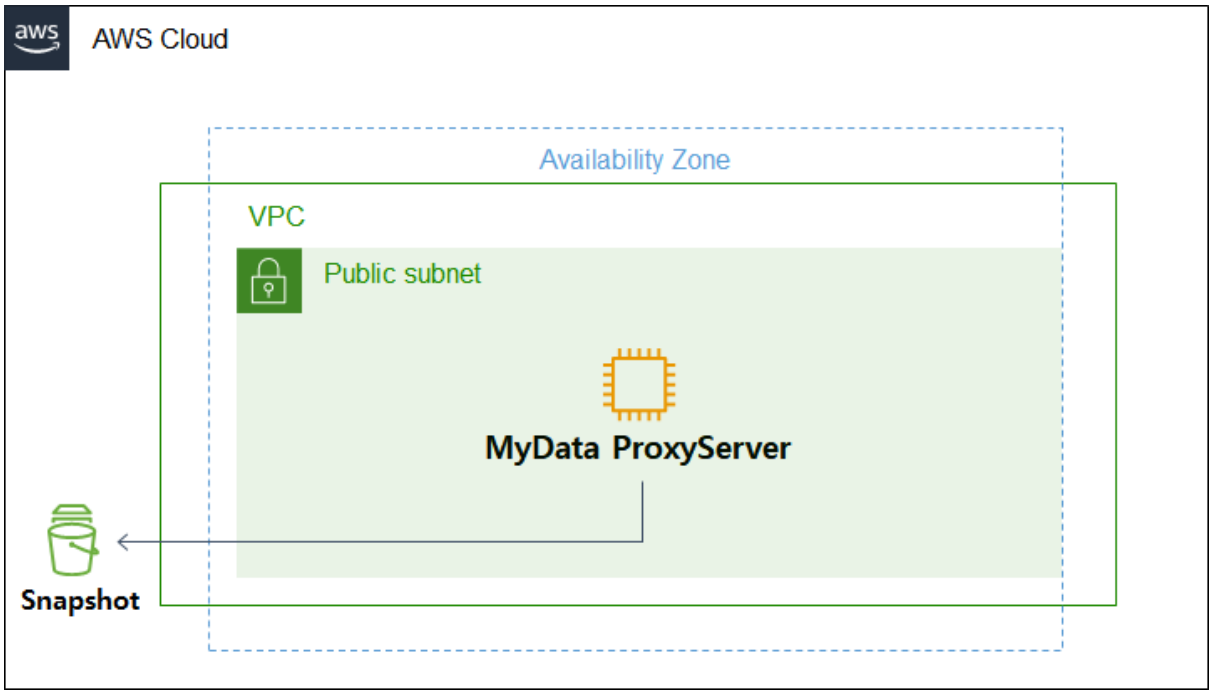
Amazon EFS is integrated with AWS Key Management Service (KMS) to support encryption. Data and metadata in files that are encrypted using AWS customer managed keys (CMKs) are automatically encrypted before being written to the file and decrypted when read.

You need to encrypt your data in EFS by referring to the link below.

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

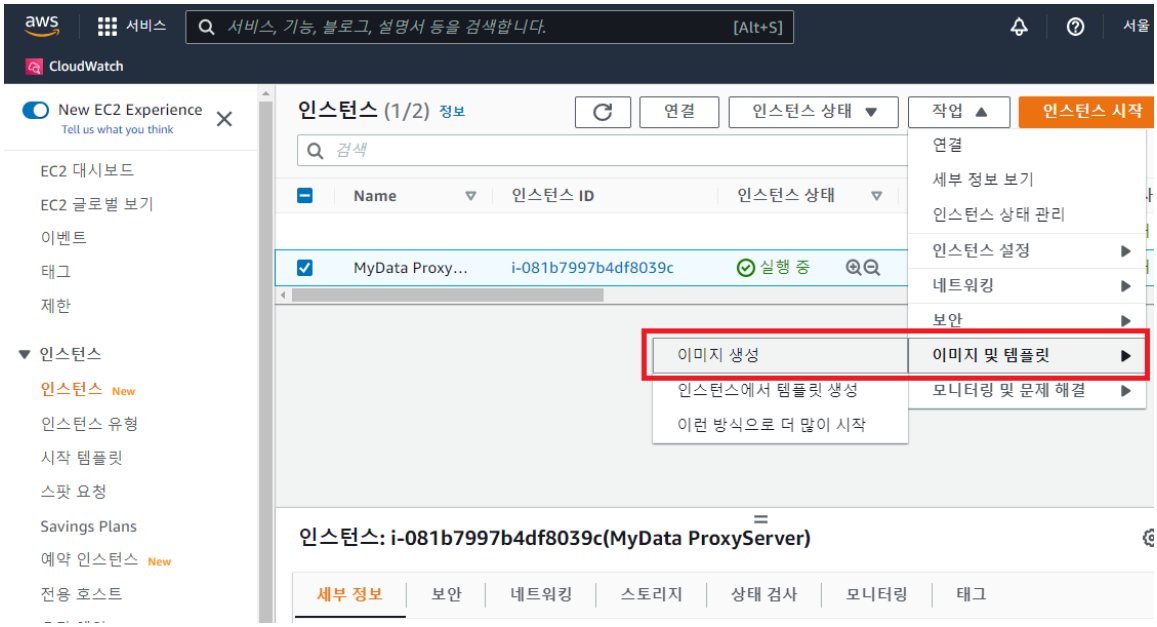
4.4 Support for MyData Proxy Server Backup and Restore in AWS

4.4.1 MyData Proxy Server Backup and Restore



A. Backup(Snapshot)

1. Create an AMI image of MyData Proxy Server

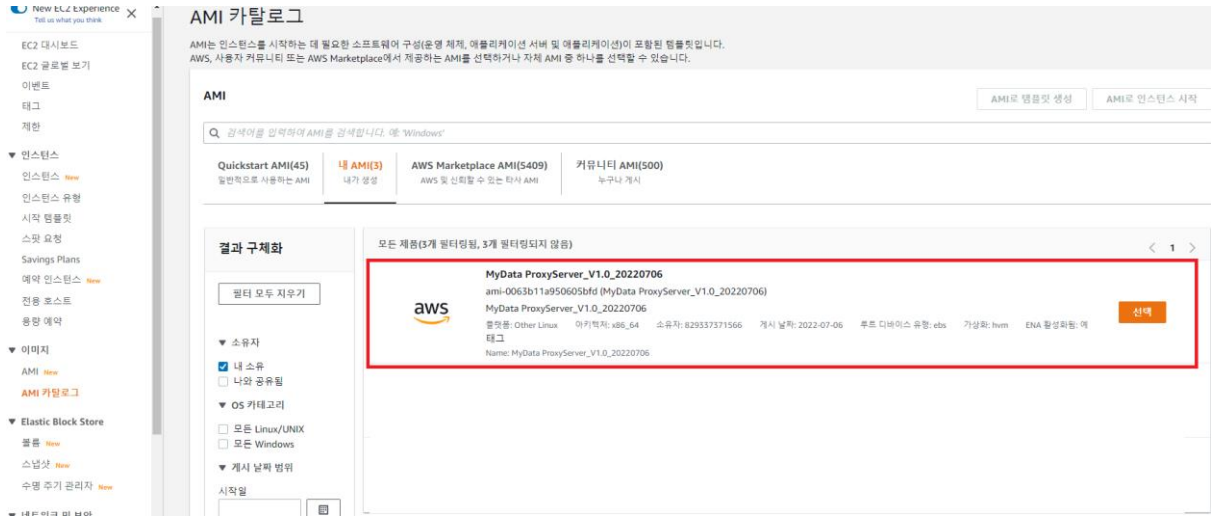


2. Create Image

Menu	Input Value
Image name	MyData Proxy Server backup
Image description	MyData Proxy Server backup
No reboot	Uncheck
Instance Volumes	Default configure

B. Restore

1. Choose an Amazon Machine Image (AMI)



2. Select to create AMI(snapshot), see **[3.1.4] Create a Launch Template**

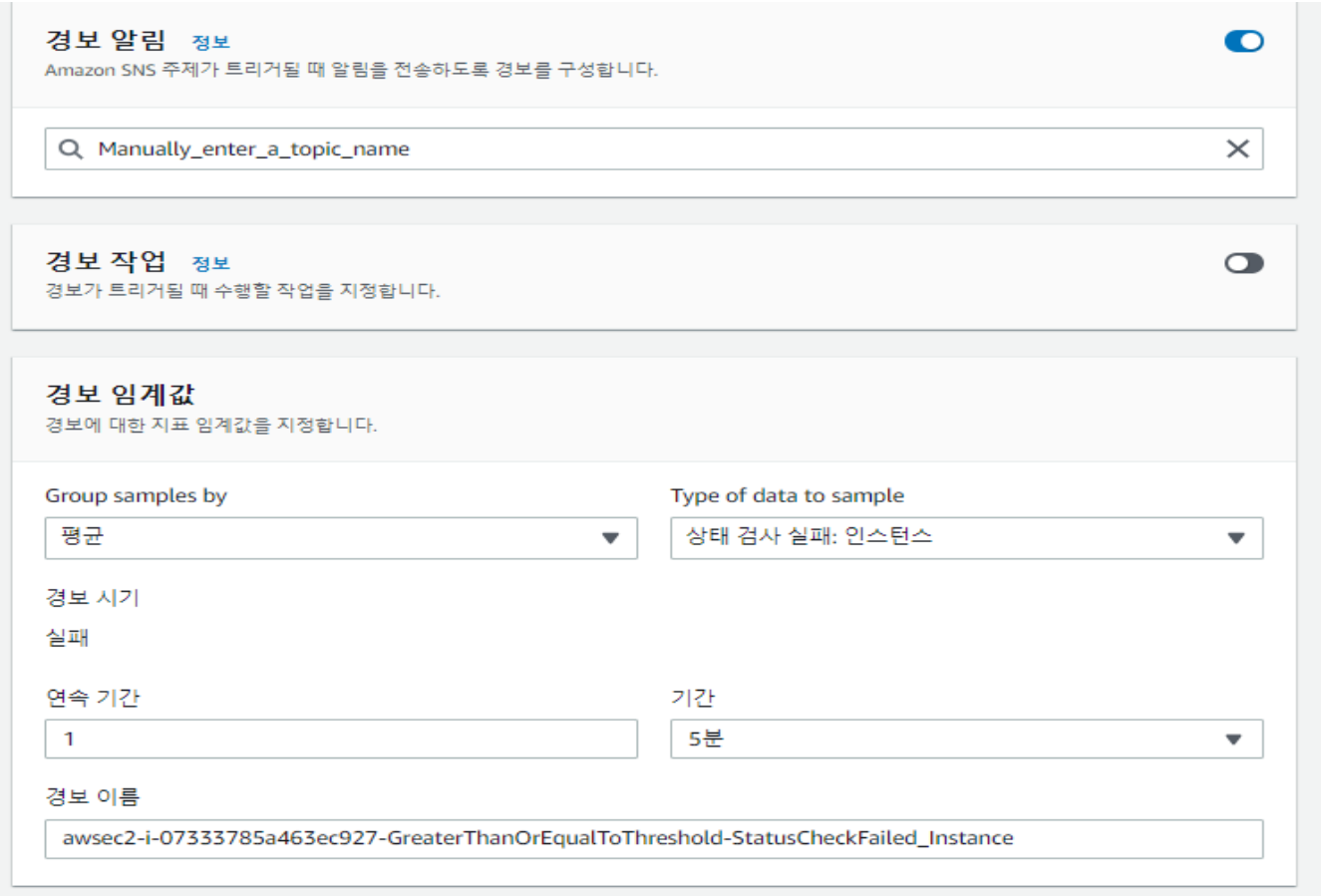
4.5 MyData Proxy Server Health Check with CloudWatch

Optional : Intergrate with CloudWatch to support MyData Shield health check

1. Create an alarm on the deployed MyData Shield instance.

2. Create an alarm after setting the policy in the Create Alarm tab as shown below.

Item	Input Value	Remarks
Alarm notification	Alarm to SNS	
Alarm threshold	Type of data to sample : Status Scan failed : Instance Continuous : 1	



4.6 Disable IMDSv1

Optional: Using AWS CLI to Disable IMDSv1 Feature

- To use the AWS CLI, you need the access key of an IAM user with privileges for the instance. Please refer to the link below for how to obtain an Access Key.

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

  Check out the best practices for AWS access key management via the link below.

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

- Disable/Enable IMDSv1

  A. Connect to instance through SSM

B. After entering the [aws configure] command, register the information.

➢ For detailed description of the AWS CLI, please refer to the link below.

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

C. Disable/Enable IMDSv1

	Description	Command
1	Disable MyData Proxy Server IMDSv1	sudo bash /home/ec2-user/IMDSv1/modify-ec2-idmsv2.sh [Instance-Id]
2	Enable MyData Proxy Server IMDSv1	sudo bash /home/ec2-user/IMDSv1/restore-metadata.sh [Instance-Id]

4.7 Routine Maintenance

✓ Managing AWS Service Limits

MyData Proxy Server uses Amazon EC2. Amazon EC2 provides different resources depending on the configuration you use, such as images, instances, volumes, and snapshots. When you create an AWS account, limits are set for these resources on a per-region basis. For more information on managing limits on resources, please see the link below.

➢ Manage limits for EC2 resources: https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/ec2-resource-limits.html

✓ Product maintenance

Maintenance fees are determined by contract policy and include latest release development and upgrade services

Details of maintenance and technical support may vary under additional agreements Maintenance is broadly divided into :

- Regular inspection : Conduct emergency inspections according to the maintenance contract
- Emergency inspection : Conduct emergency inspection according to the maintenance contract.

Maintenance scope :

- Check solution
- Patch and Upgrade

4.8 Emergency Maintenance

4.8.1 Startup process

➢ User-Startup process

A. Start up

Order	Description	Command
1	Connecting to Instances Through Session Manager or [ec2-user] SSH login with your account	-
2	Check Proxy Server settings	cat /app/apim-proxy/conf/application.properties
3	Modify Proxy Server setting using script editor	sudo nano /app/apim-proxy/conf/application.properties
4	Start Proxy Server	cd /app/apim-proxy/bin && sudo ./start.sh
5	Start Apache	sudo systemctl start httpd

4.8.2 Health Check

- Check MyData Proxy Server process

Order	Description	Command
1	Connecting to Instances Through Session Manager or [ec2-user] SSH login with your account	-
2	Proxy Server process check	source /app/apim-proxy/bin/sp.sh

Normal after entering the command :

```
[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
```

Abnormal after entering the command :

- Process no detected

- Check Apache process

Order	Description	Command
1	Connecting to Instances Through Session Manager or [ec2-user] SSH login with your account	-
2	Check Apache process	sudo systemctl status httpd

Normal after entering the command :

```
[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.
```

Abnormal after entering the command :

```
[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

- Abnormal instance

4.8.4 Recovery procedure for MyData Proxy Server failure

➢ When an abnormal instance occurs

- [4.4.1] Perform the recovery procedure from the AMI backed up by MyData Proxy Server Backup and Restore.

- Instance reboot

4.8.5 Recovery procedure when MyData Proxy Server recovery fails

- User

  If the MyData Proxy Server recovery fails, you can choose how to reinstall it depending on whether you have a snapshot or not

  A. Recreate AMI with snapshot of existing MyData Proxy Server

  B. Reinstall MyData Proxy Server according to **[3.1.4] Launch an instance with a Template** procedure

4.8.6 RTO

When MyData Proxy Server fails, it takes at least 10 to 30 minutes to recreate and install an AMI with a snapshot of the previously installed instance, and up to 30 minutes to set up and test the product.

5. Solution operation

Users of the product should have expertise in the Linux CLI environment.

5.1 How to set

1. Login with **[ec2-user]** SSH account -> Run Apache through the commend **[sudo systemctl start httpd]**
2. The location of the MyData Proxy Server script is **/app/apim-proxy/bin**

- Check the executable script using the [ls -al /app/apim-proxy/bin] command

  (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]$
```

3. **Optional :** Configure MyData Proxy Server SSL/TLS

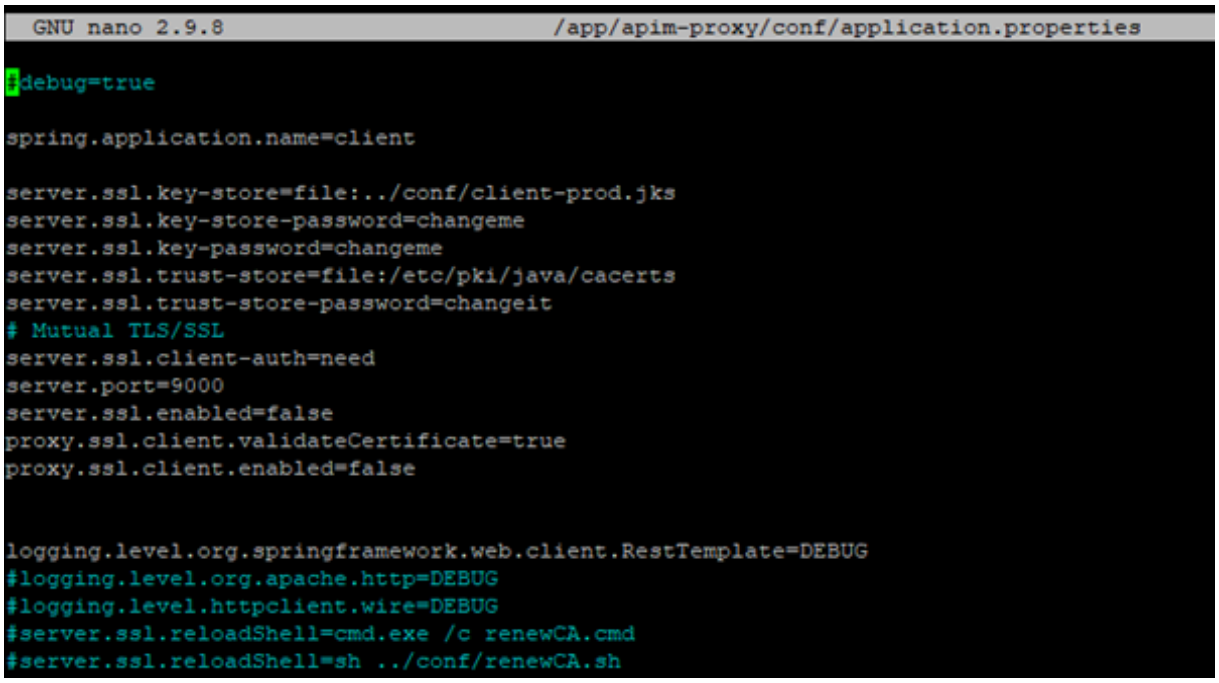
   Follow the link below to check out the 2nd step process:

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

4. Edit the configuration file of MyData Proxy Server

- Nano script editor

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



- Vi script editor

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

5. MyData Proxy Server Setting

Setting Items	Description
server.port	Proxy server port
server.ssl.key-store	Jks certificate path
server.ssl.key-store-password	Jks certificate password
server.ssl.key-password	Jks certificate password
server.ssl.trust-store	CAcert Jks certificate path

server.ssl.trust-store-password	CAcert JKS certificate password
server.ssl.enabled	Set whether to receive https (true/false)
proxy.ssl.client.validateCertificate	Server certificate validation
proxy.ssl.client.enabled	The client must connect to https
server.ssl.client-auth	mTLS settings 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	Setting the client connection log level
logging.level.org.apache.http	Proxy server access log level setting
logging.level.httpclient.wire	Proxy server access log level setting

5.2 How to run

1. Running MyData Proxy Server

2. Running Apache

3. Check the table below for commands related to execution and operation

- MyData Proxy Server Operation Commands
  - Use the [cd /app/apim-proxy/bin] command to move to the folder where the script is located

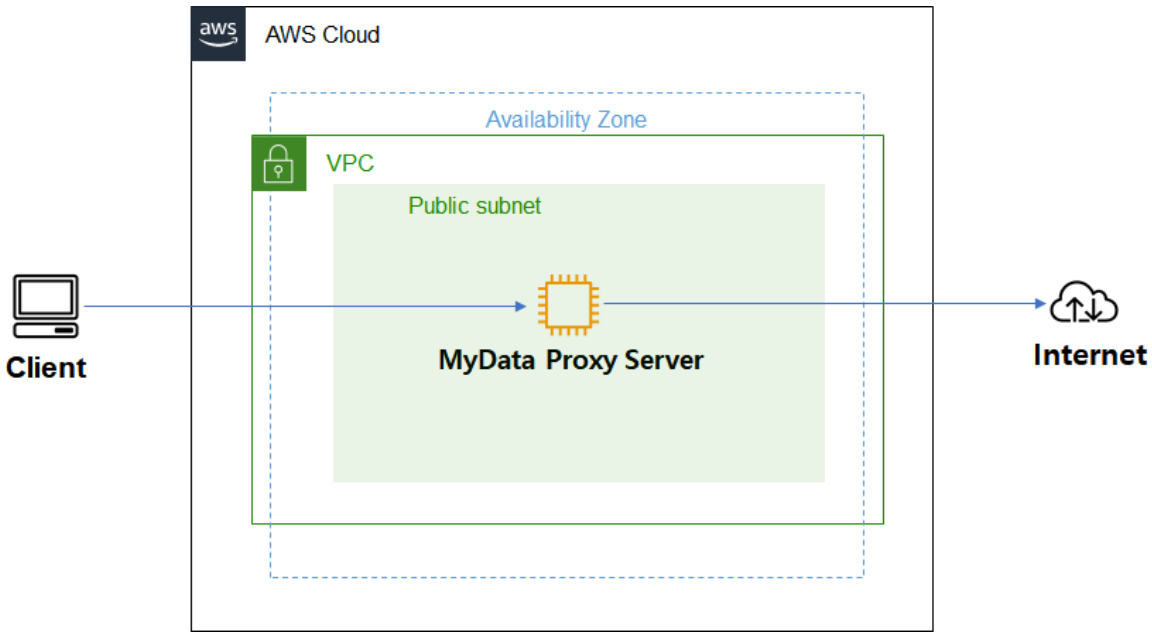
Command	Description
sudo ./start.sh	Running Proxy Server
sudo ./sp.sh	Check the Proxy Server process
sudo ./kill.sh	**(Optional)** Shut Down the Proxy Server

- Apache operating commands

Command	Description
sudo systemctl start httpd	Running Apache
sudo systemctl status httpd	Check the Apache process
sudo systemctl restart httpd	Restart Apache
sudo systemctl stop httpd	Stop Apache

4. Testing and setting up forward and reverse proxies

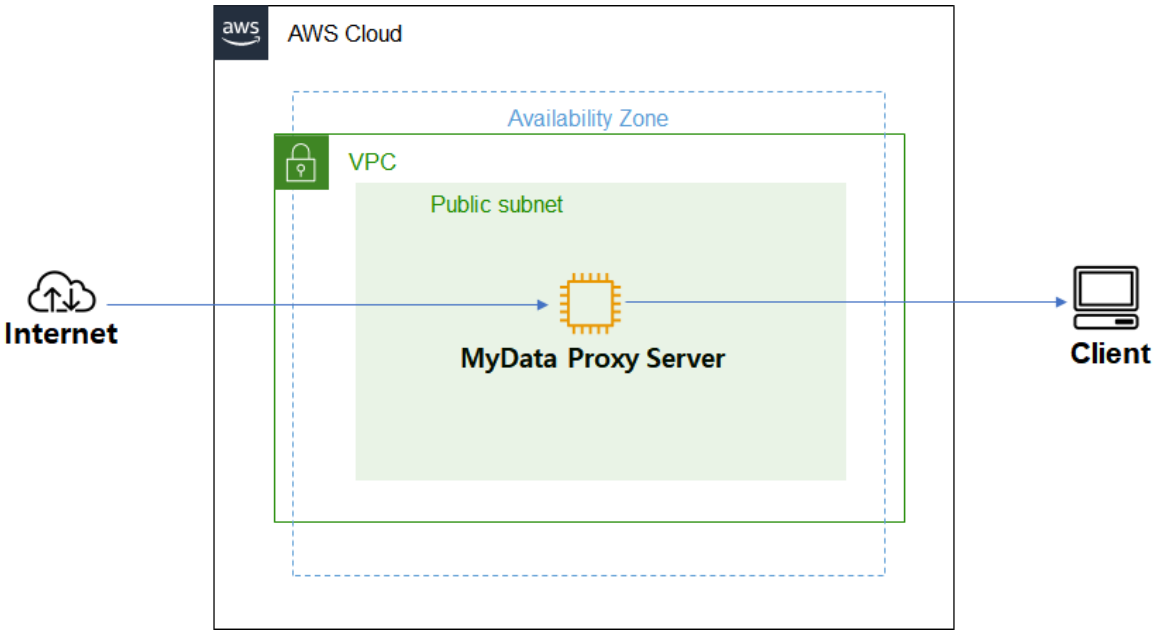
A. Forward Proxy



- With the MyData Proxy Server running, test the Forward Proxy through the command below.
  - Ex) [curl --location --request GET 'http://localhost:9000' --header 'x-target-host: http://www.inzent.com/ ']
- To check the forward proxy operation in the client, refer to the command below.

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

B. Reverse Proxy



➢ Reverse proxy setting for http communication

I. After running the Apache Server, check the revere proxy operation through the [**curl http://[My Data Proxy Server IP]**]

```
[ec2-user@ip-172-31-34-169 ~]$ curl http://
setting ok
```

II. **[sudo nano /etc/httpd/conf/httpd.conf]** through the modifications below.

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

➢ **Optional** : [5.1 How to set] If you set the SSL/TLS certificate through list 3

I. **[sudo nano /etc/httpd/conf.d/ssl.conf]** through the modifications below

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

5. log storage location

A . Apache log location

- /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$
```

B . MyData Proxy Server log location

- /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]$
```

5.3 Key management

A. EBS Key Management

You can use AWS KMS keys to support EBS encryption if needed. Check out EBS Volume Encryption Management via the link below.

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

B. Manage Access Keys for IAM Users

IAM users' access keys should be avoided externally and should be rotated periodically.

Check out access key management via the link below:

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

5.4 Patches and updates management

Inquiries about patches/updates can be made through the link below and will be handled separately according to the contact.

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

6. Support

6.1 Technical support

The technical support service is provided only for the features specified in the document.

Technical support covers the following areas:

- Installation support : Deployment guide provided, source provided through Github
  - ➔ Github : https://github.com/InzentSaaS/MyData-Proxy-Server
- Customization support.

Technical support contacts.

- 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 won
- 30 Hour : 4,000,000 won
- 60 Hour : 7,500,000 won
- 120 Hour : 14,000,000 won

Provided upon contract :

- Customization support (man-hour calculated separately)

6.3 SLA

- Free Tier : Deployment guide
- Technical Service Pack : At the request of customer, technical support corresponding to the standard time is provided

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