INZENT

aws Qualified Software

MyData Shield 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 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.

1.1 Introduction

MyData Shield는 MyData 사업자가 정보제공자의 MyData를 분석하기 위하여 Json 형태의 MyData안에 포함되어 있는 개인 정보를 가명/익명 처리 해주는 역할을 수행합니다. 기존 MyData API 규격에 맞게 설정된 가명 처리가 필요한 '항목명'을 설정하면 해당 데이터를 탐색하여 유동적으로 가명 처리를 수행하며, '항목명'이 할당되지 않은 데이터에 예측할 수 있는 개인 정보 데이터 또한 가명/익명 처리를 해주는 기능을 수행합니다.

- 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 Shield를 Amazon Web Services(AWS)에서 사용하기 위한 전제 조건 및 리소스 요구 사항에 대해 설명합니다.

- **전제 조건**

MyData Shield AMI는 독립적인 솔루션으로 추가로 소프트웨어를 설치할 필요가 없습니다. 기본적인 AWS 기술을 통하여 MyData Shield의 배포가 가능하며, AWS EC2만을 포함하여 배포합니다.

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

MyData Shield의 데이터베이스는 Postgresql기반의 eXperDB Standard가 배포되는 이미지에 설치되어 있습니다.

- **요구 사항**

MyData Shield 를 설치하려면 가상 머신(VMs)가 필요합니다.

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

개수는 고객 환경에 따라 변경될 수 있습니다.

1.1.2 Region support

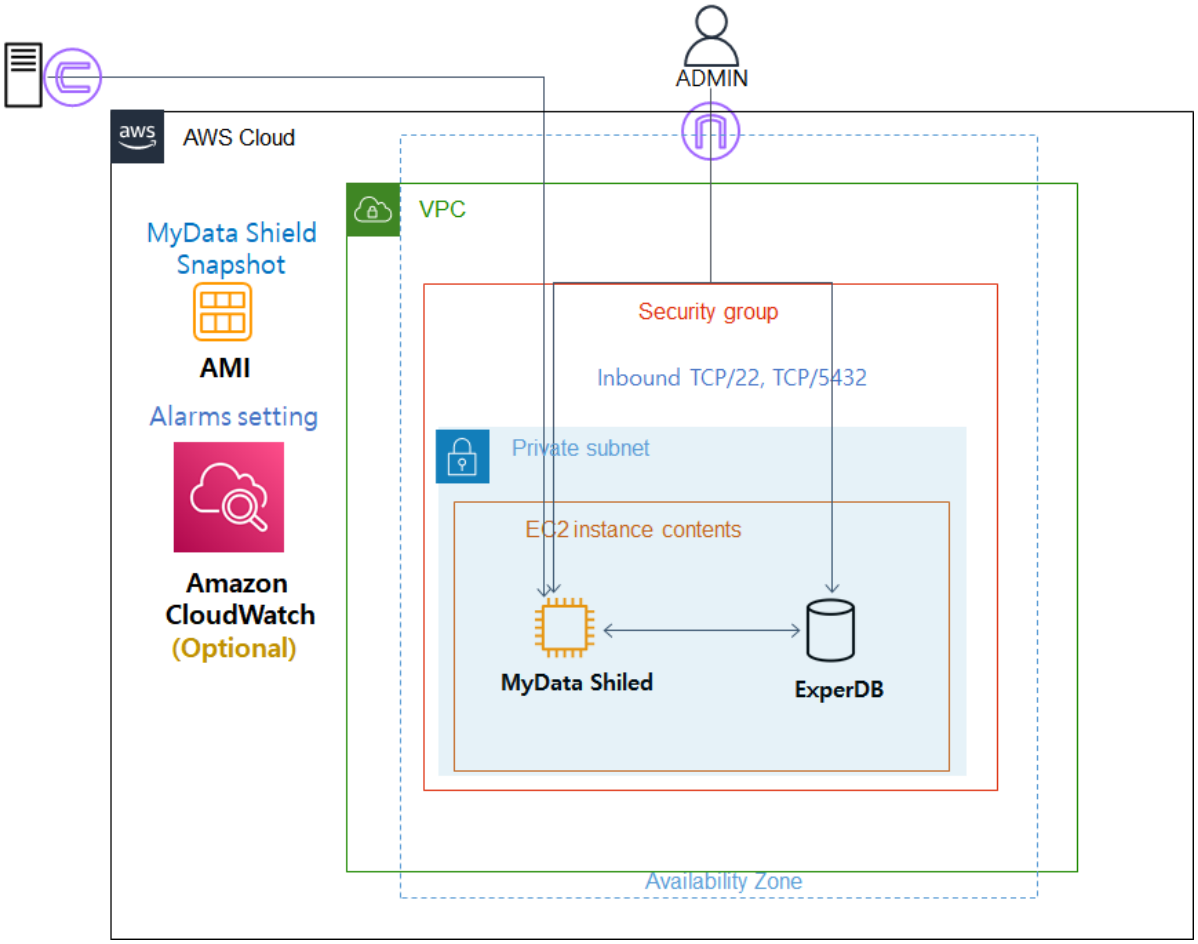
제품이 지원되는 지역은 아래와 같습니다.

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

1.1.3 Architecture Diagrams

- 프라이빗 서브넷, MyData Shield EC2 인스턴스
- AMI(Amazon Machine Image)를 사용하여 백업 및 복수 수행
- **(선택사항)** Amazon Cloud Watch 서비스 사용으로 MyData Shield 상태 모니터링 및 알림

- **MyData Shield 구성도**



1.1.4 use case

아래 링크는 MyData Shield의 가명 처리 기능을 사용하여 전처리를 수행한 프로젝트 사례입니다.

https://m.etnews.com/20211223000103?obj=Tzo4OiJzdGRDbGFzcyI6Mjp7czo3OiJyZWZlcmVyIjtOO3M6NzoiZm9yd2FyZCI7czoxMzoid2ViIHRvIG1vYmlsZSI7fQ%3D%3D

2. Planning Guidance

2.1 Security

보안 및 운용 :

MyData Shield를 설치/제어하는데 오직 SSH 접근만 허용됩니다. (키 기반 인증/sudo 또는 유사한

매커니즘을 선호함)

- 접속에 AWS 루트 자격 증명을 사용하지 않습니다..

2.2 Costs and Licenses

MyData Shield 제품은 무료로 제공합니다. 추가로 EC2 제품 안에 존재하는 사용자 구성 정보와 데이터베이스 구성 정보 및 AMI 제공에 대해서는 아래 링크를 통해 문의하십시오.

관련 문의 링크 : http://www.inzent.com/board/board.php?bo_table=faq&pageName=main

- 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. Cloudwatch(선택 사항)

  D. Secret Manager(선택사항)

2.3 Sizing

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

Count of data	Instance type	Vcpu	Memory(GiB)	EBS Volume	EBS Volume Type
~5000000	t2.medium or t3.medium	2	4	50GB	General Purpose SSD (gp2)
~100000000	t2.large or t3.large	2	8	1T	General Purpose SSD (gp2)
~1000000000	t2.large or t3.large	2	8	10T	General Purpose SSD

					(gp2)

3. Deployment steps

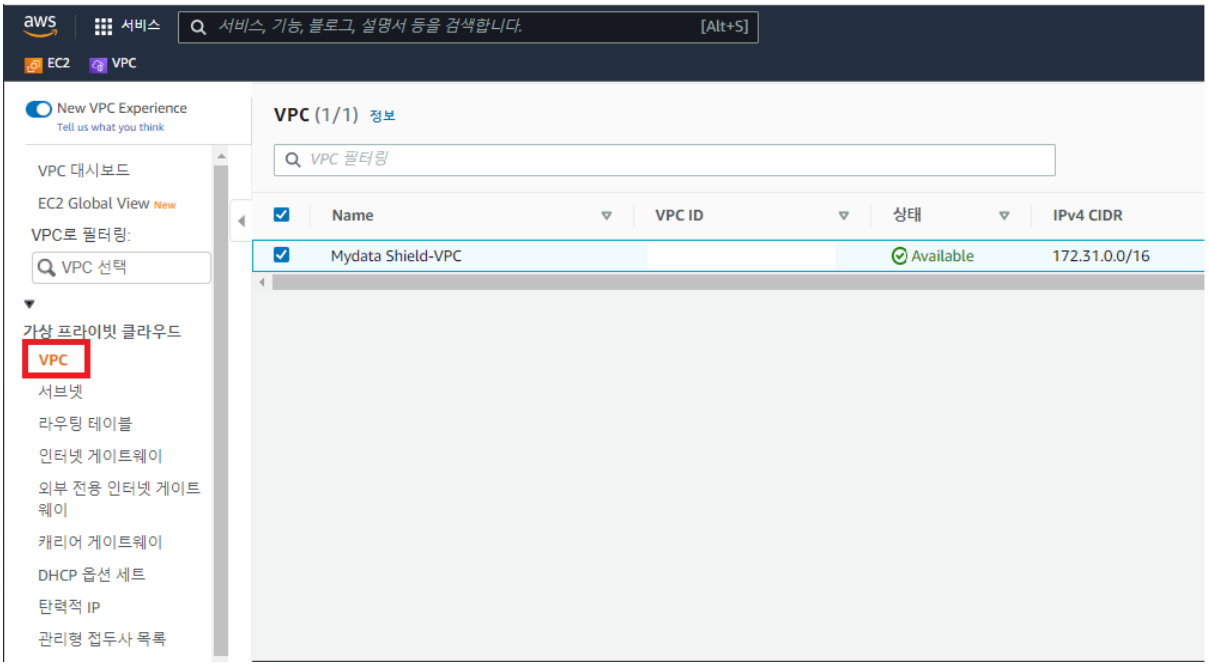
3.1 Mydata Shield Installation

3.1.1 Create VPC AND Subnet

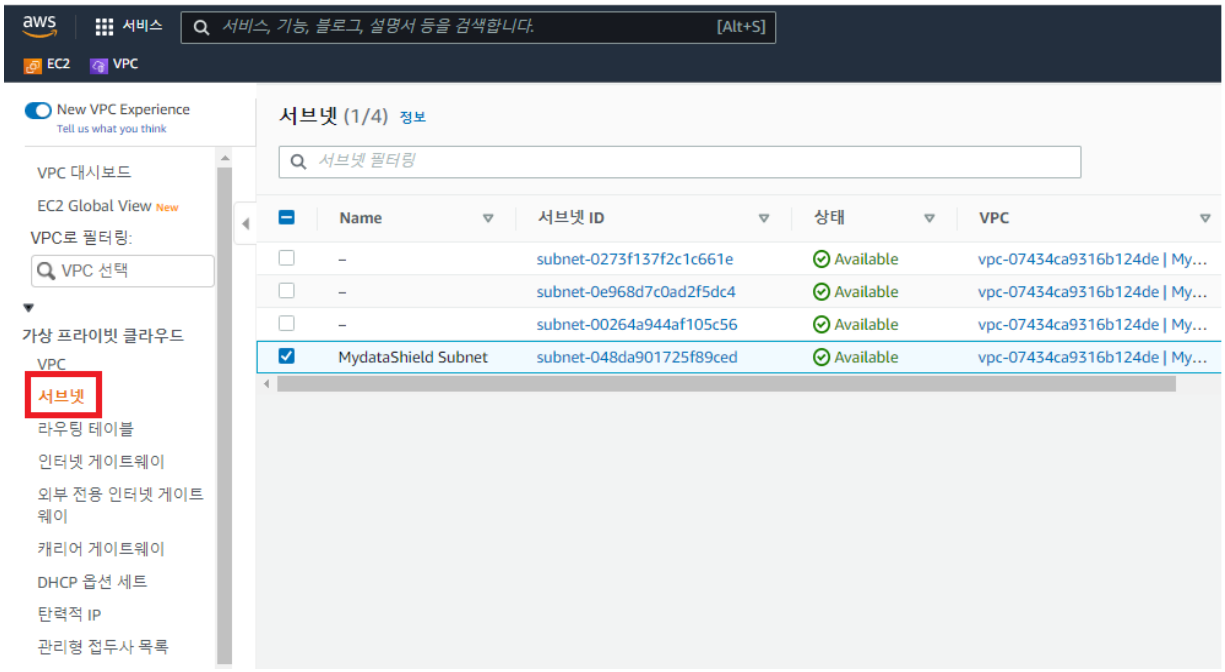
Mydata Shield를 관리하는 서브넷 설정입니다.

- 기존 VPC 및 서브넷 확인

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



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



- MyData Shield 서브넷 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 Shield Subnet
VPC	사용자 웹 계층과 동일한 기존 VPC 선택
VPC CIDRS	-
가용 영역	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

3.1.2 Create Network ACLs

Optional : 추가로 보안 계층이 필요한 경우 네트워크 ACL을 생성하고 규칙을 추가할 수

있습니다 .

- MyData Shield Network ACL 생성

1. Amazon VPC 콘솔에 접속(https://console.aws.amazon.com/vpc/).

2. 탐색창에 있는 Network ACL 선택 .

3. 네트워크 ACL 생성 선택.

4. 네트워크 ACL 설정에 있는 목록에 VPC의 ID 및 이름을 설정

Menu	Input Value
이름	MyData Shield NACL
VPC	사용자 및 MyData 저장장치의 웹계층에 맞게 선택

5. 탐색창에 있는 Network ACL 선택.

6. 세부 정보에 추가해야하는 규칙유형에 따라 인바운드 규칙, 아웃바운드 규칙 탭을 선택하여 편집.

- 인바운드 규칙

규칙 번호	소스	프로토콜	포트	허용/거부	설명
100	솔루션 운용자의 IP 주소 범위	TCP	22	Allow	솔루션 사용자의 SSH 트래픽 허용
110	MyData 저장 장치의 IP 주소 범위	TCP	5432	허용	MyData 저장 장치에서 들어오는 RDB 트래픽 허용
*	0.0.0.0/0	모두	모두	거부	-

- 아웃바운드 규칙

규칙 번호	소스	프로토콜	포트	허용/거부	설명

100	사용자가 데이터를 활용하고 싶은 장치의 IPv4 주소 범위	TCP	5432	허용	Mydata Shield RDB 네트워크에 대한 아웃바운드 응답 허용
*	0.0.0.0/0	모두	모두	거부	-

7. 완료 후 저장.

8. 서브넷을 네트워크 ACL과 연결하기 위해 목록에서 네트워크 ACL을 선택한 다음 [MyData Shield NACL]을 선택합니다.

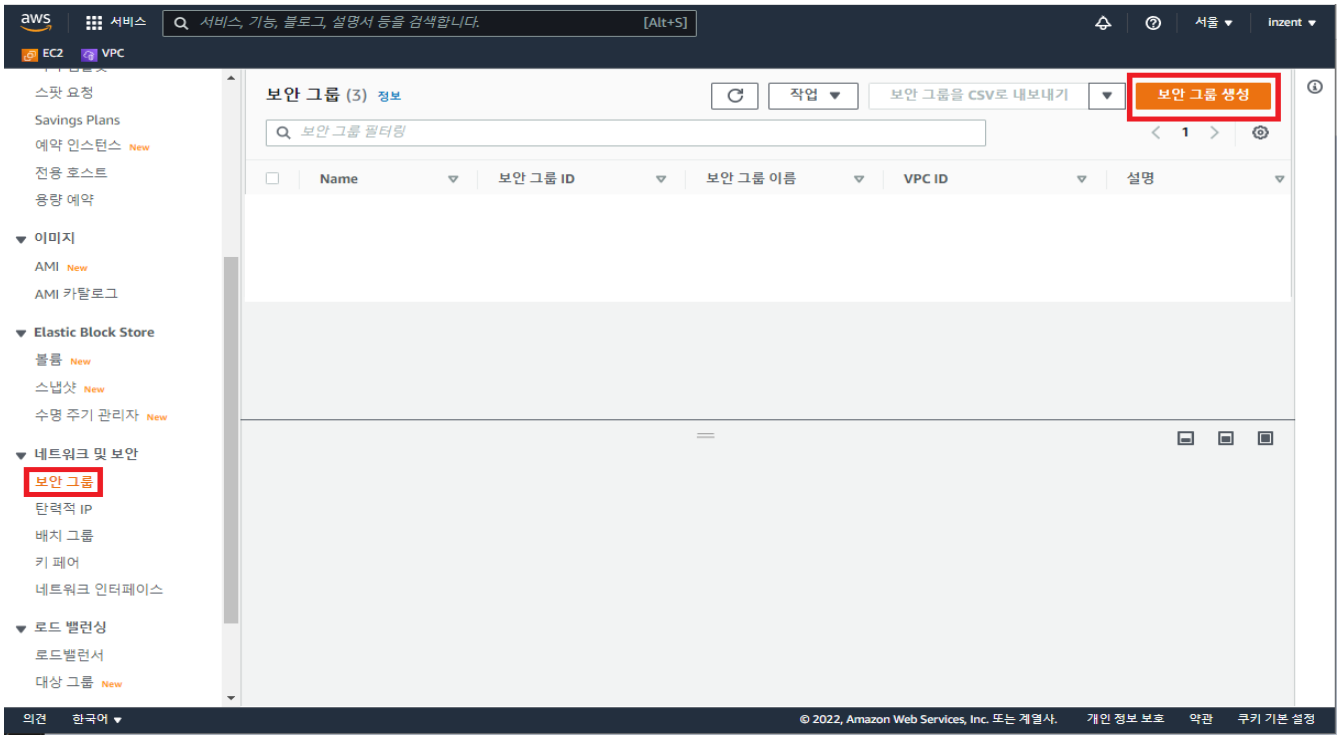
9. 세부 정보화면의 서브넷 연결 탭에서 편집을 선택합니다. 네트워크 ACL과 연결할 [Mydata Shield Subnet]에 대한 연결 확인란을 선택한 다음 저장을 선택합니다.

3.1.3 Create Security Group

Mydata Shield서버와 사용자, Mydata 저장 장치가 서로 통신하려면 보안그룹을 설정해야 합니다.

- Create MyData Shield Securiy Groups

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



3. 보안그룹 생성 및 인바운드 규칙 설정.

Menu	Input Value
보안 그룹 이름	MyData Shield-SSH SG
설명	MyData Shield-SSH SG
VPC	운용자가 사용하는 장치와 동일한 VPC를 선택
유형	SSH
프로토콜	TCP
포트 범위	22
대상	사용자 IP 및 사용자가 사용할 장치 IP

Menu	Input Value
보안 그룹 이름	MyData Shield-DB SG
설명	MyData Shield-DB SG
VPC	운용자가 사용하는 장치와 동일한 VPC를 선택
유형	PostgreSQL
프로토콜	TCP
포트 범위	5432
대상	MyData 저장 장치 IP

4. 데이터 조회를 위한 아웃바운드 규칙 설정

Menu	Input Value
보안 그룹 이름	MyData Shield-DB SG
설명	MyData Shield-DB SG
VPC	운용자가 사용하는 장치와 동일한 VPC를 선택
유형	PostgreSQL
프로토콜	TCP
포트 범위	5432
대상	데이터를 조회하고 싶은 장치 IP

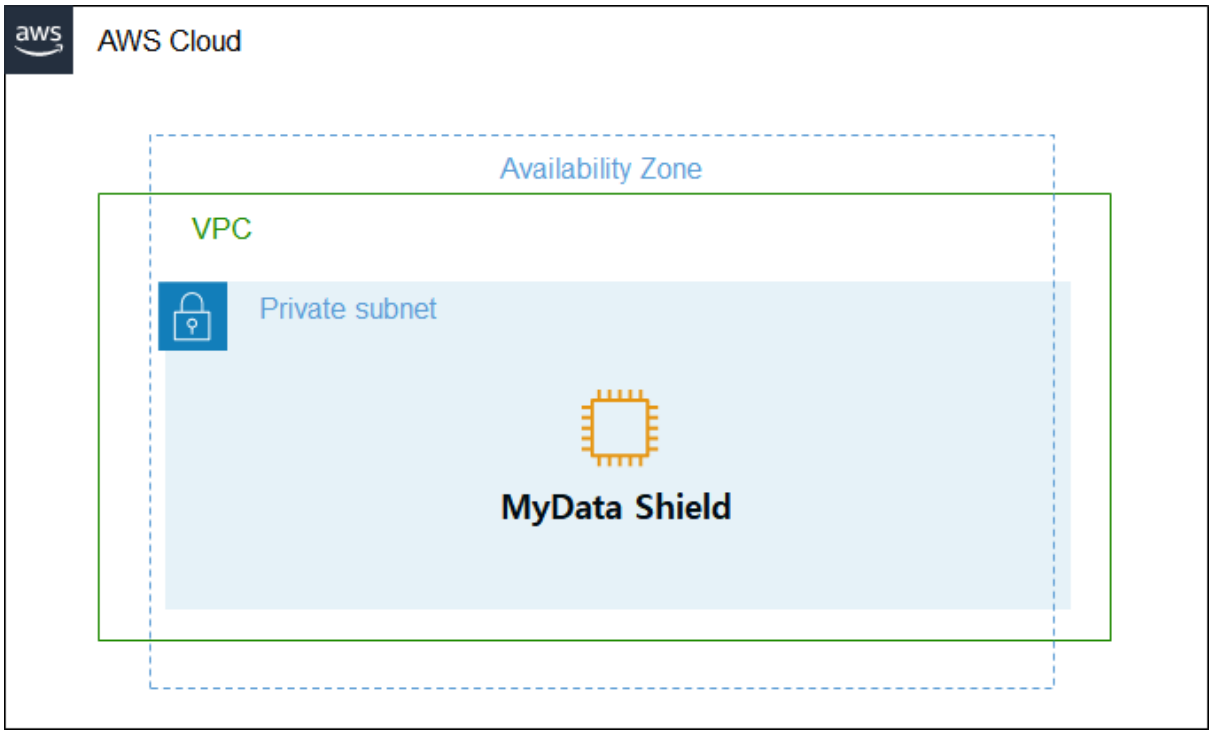
5. Add a Name Tage to [태크] as follows

Menu	Input Value	Menu	Input Value
Tag	이름	설명	그룹 식별을 위한 태그 지정
Value	MyData Shield-SSH SG		

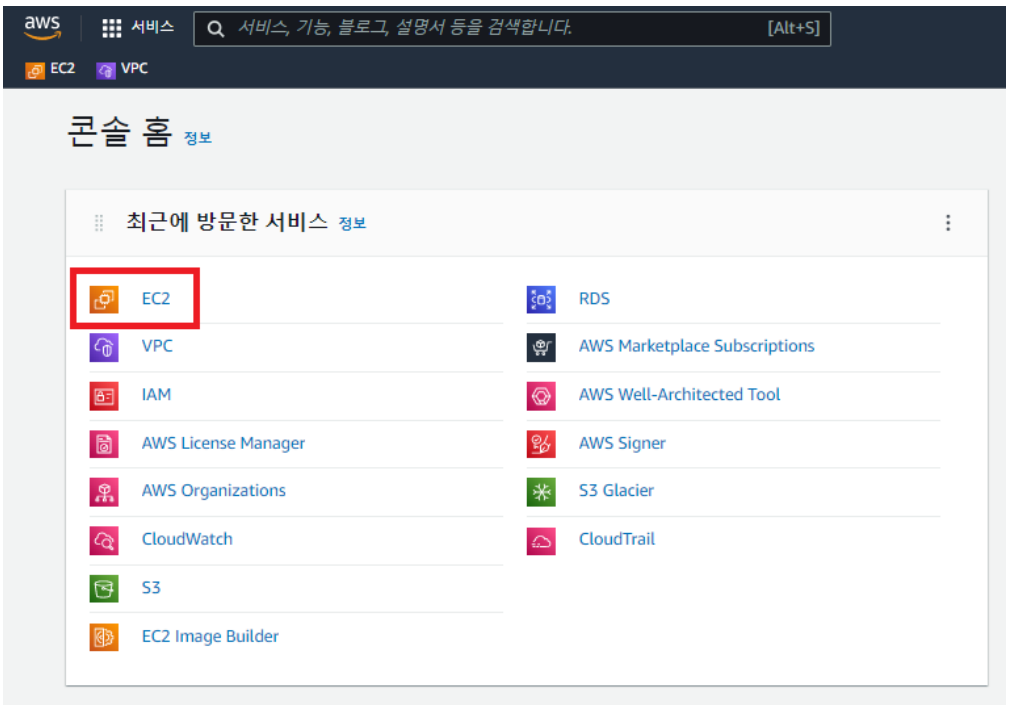
Menu	Input Value	Menu	Input Value
Tag	이름	설명	그룹 식별을 위한 태그 지정
Value	MyData Shield-DB SG		

3.1.4 Create Instance

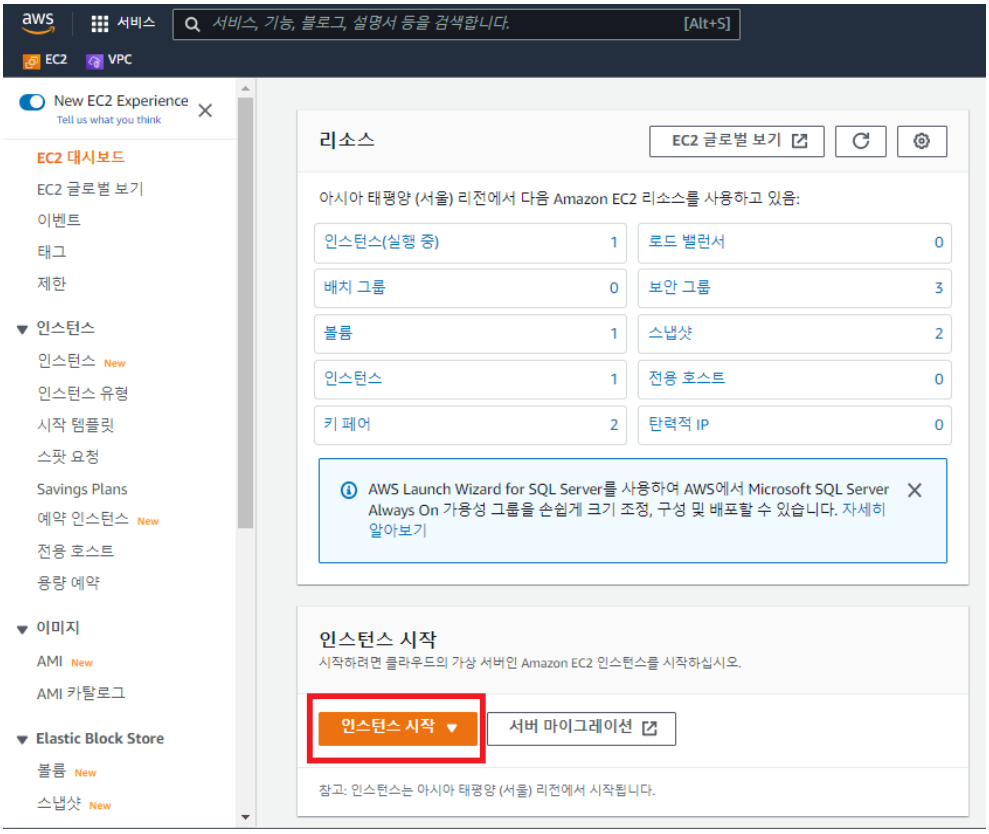
- MyData Shield AMI는 공급업체로부터 AMI를 공유 받아 인스턴스를 생성합니다.



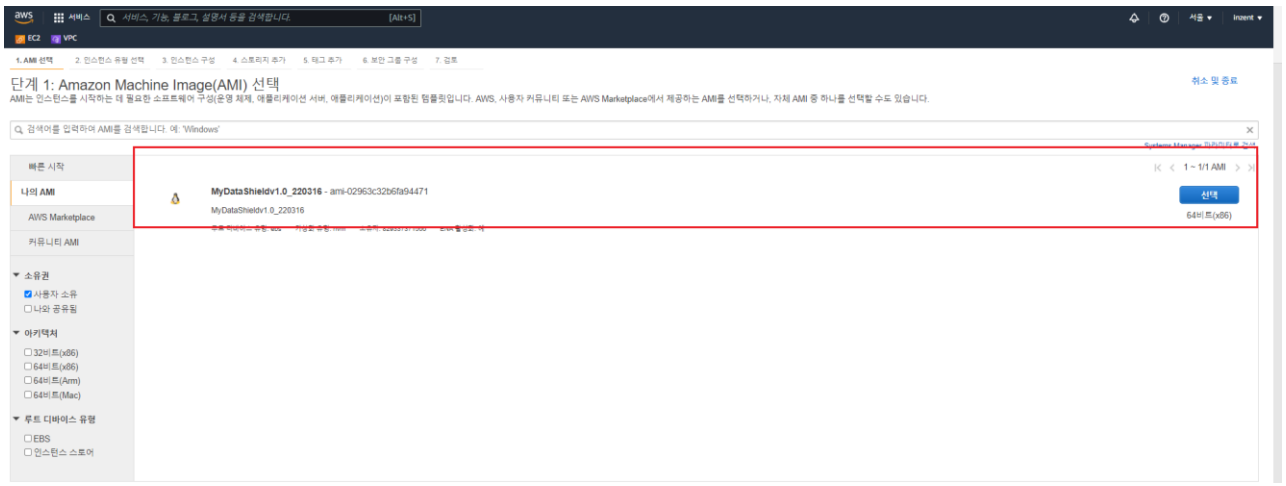
1. AWS EC2 콘솔에 로그인



2. 인스턴스 시작 클릭



3. 공유 받은 AMI 인스턴스 생성



4. 인스턴스 유형 선택

- **[2.3 Sizing]**을 보고 선택.

Menu	Input Value
인스턴스 세부 정보 구성	● 인스턴스 개수 : 1

	● 네트워크 : VPC 정보에 대해서는 링크 참조: https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/working-with-vpcs.html ● 서브넷 : 서브넷 정보에 대해서는 링크 참고 : https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/working-with-vpcs.html ● 퍼블릭 IP 자동 할당 : 서브넷 사용 설정(활성화) ● IAM 역할 : 없음
ETC	해당사항 없으면 기본 옵션 선택

5. 스토리지 추가

   - [2.3 Sizing]을 보고 선택.

6. 태그 추가

   - MyData Shield EC2 인스턴스 태깅

Menu	Input Value	Menu	Input Value
태그 키	이름	설명	인스턴스 식별을 위한 태그 지정
값	MyData Shield		

7. 보안 그룹 구성

   - 기존 보안그룹 선택 : [MyData Shield-SSH SG], [MyData Shield-DB SG]

8. 기존 키 페어 선택 또는 새 키 페어 생성

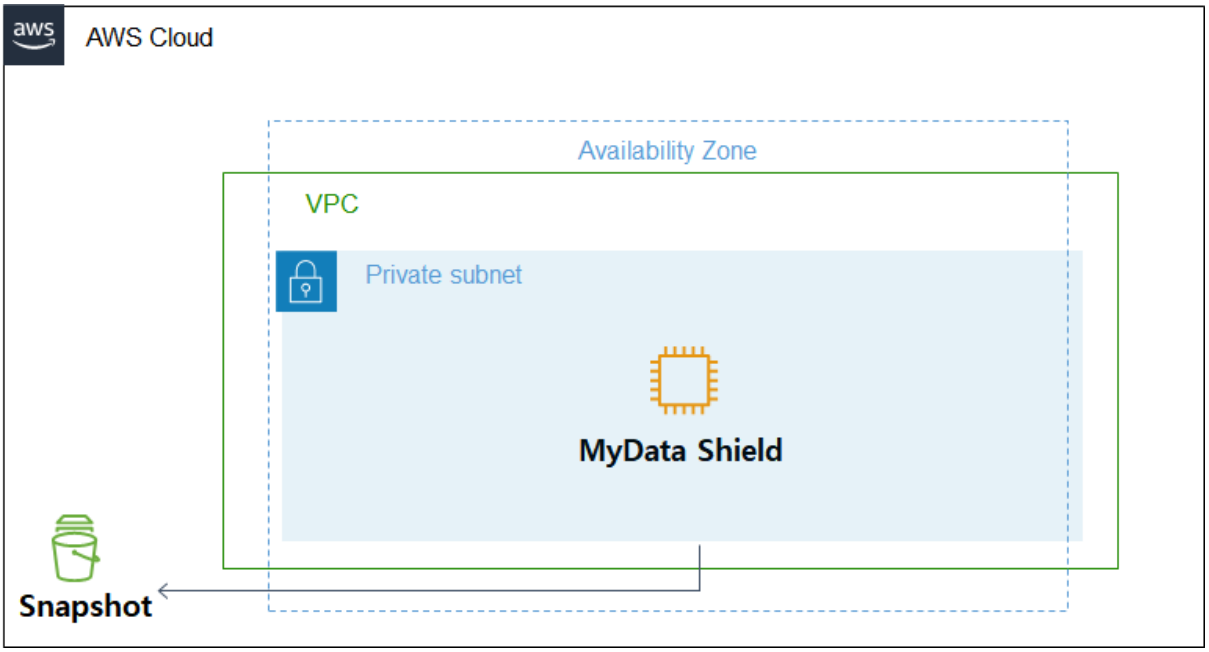
- 기존에 사용하실 키 페어가 존재하면 기존 키 페어 선택을 통해 인스턴스를 시작

- 기존 키 페어가 존재하지 않으면 새 키 페어 생성을 통해 SSH로 연결할 수 있는 키 페어를 생성합니다.

4. Operational Guidance

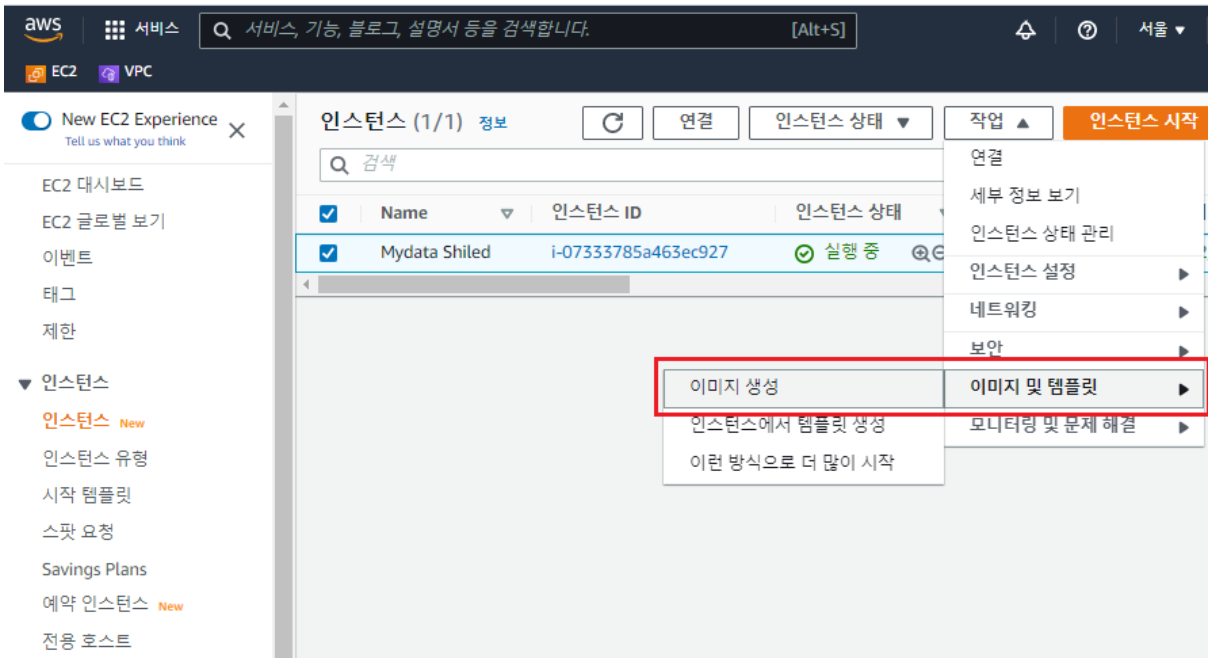
4.1 Support for MyData Shield Backup and Restore in AWS

4.1.1 MyData Shield Backup and Restore



A. 백업(Snapshot)

1. MyData Shield의 AMI 이미지를 생성

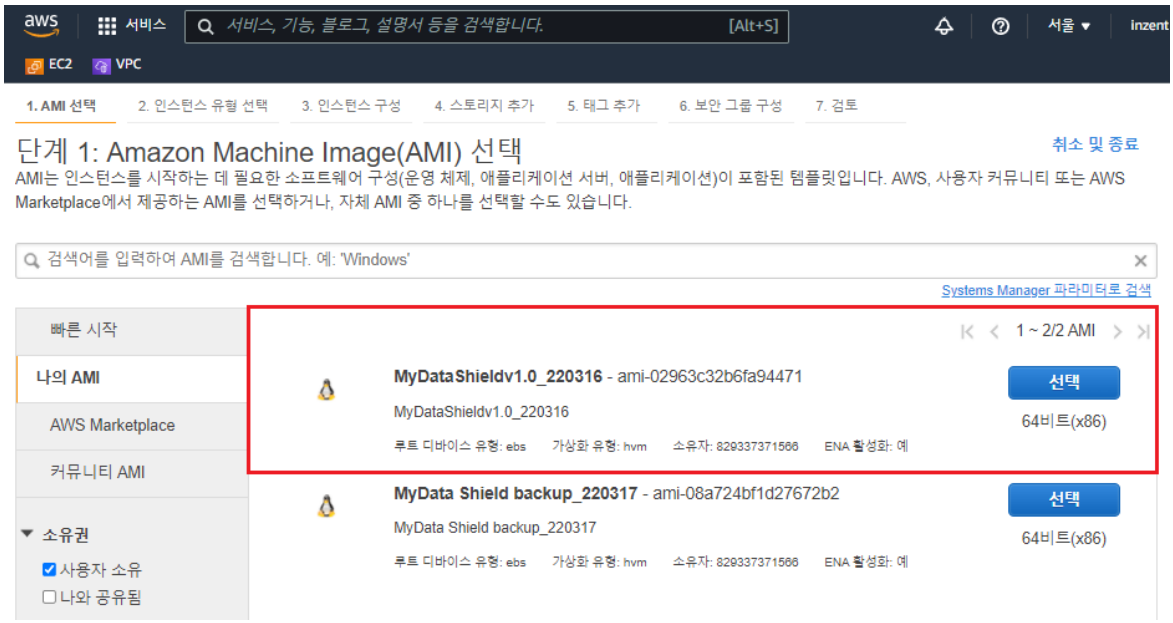


2. 이미지 생성

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

B. 복원

1. Amazon Machine Image (AMI)를 선택

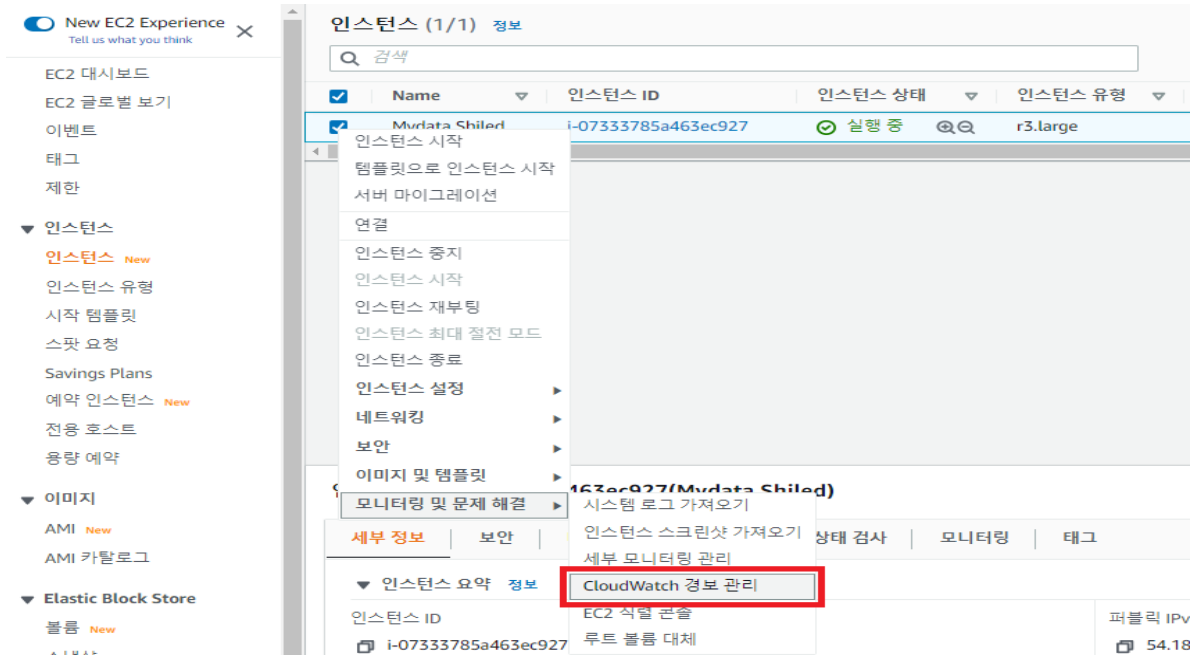


2. AMI(snapshot)을 선택 후 생성, **[3.1.4 인스턴스 생성] 참고**

4.2 MyData Shield Health Check with CloudWatch

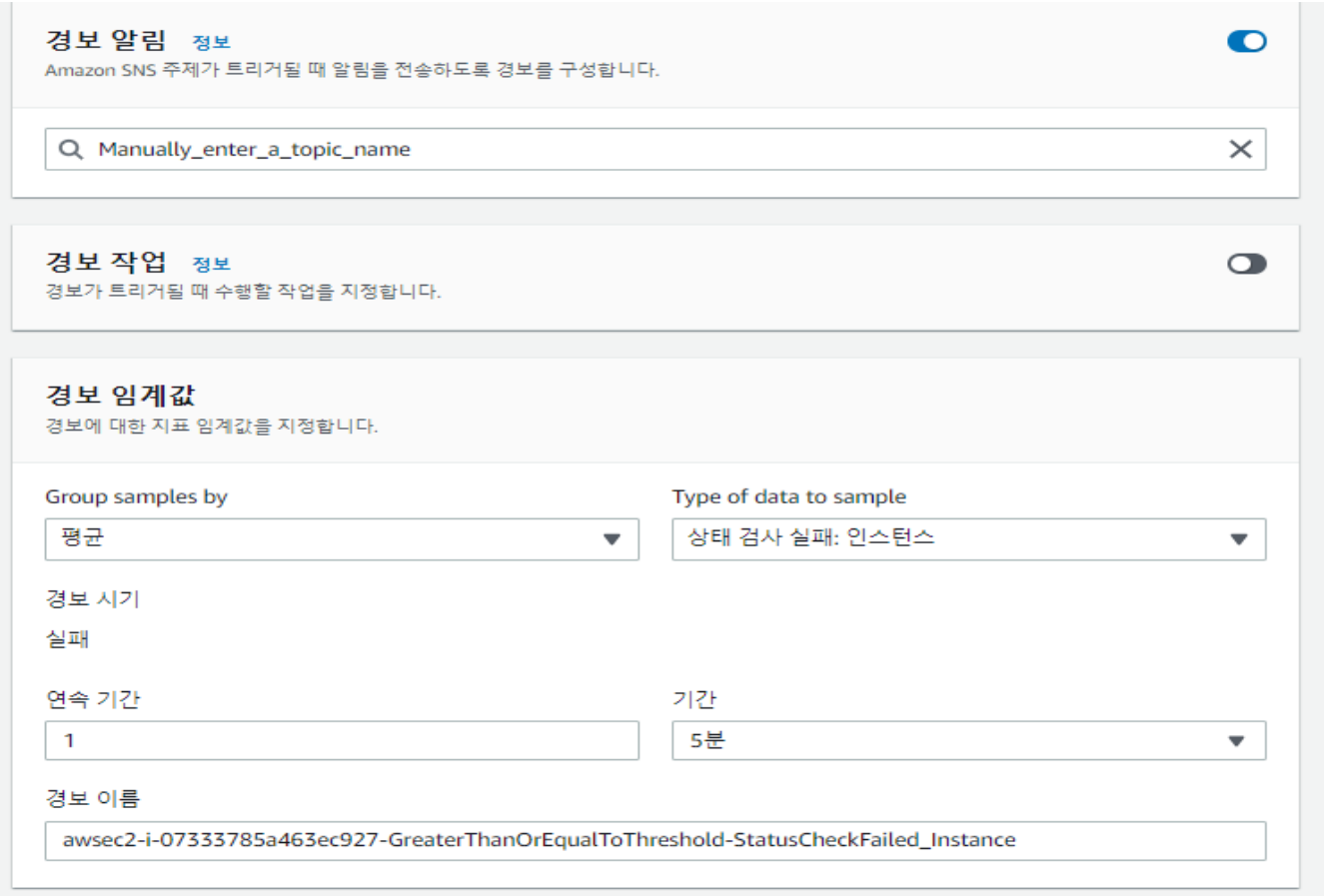
선택 사항 : CloudWatch와 통합하여 MyData Shield상태 확인을 지원

1. 배포된 MyData Shield 인스턴스에 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	



4.3 Database Credentials

MyData Shield의 DB 정보는 [2.2] 항목의 링크를 통해 제공 받을 수 있습니다.

- **선택사항:** Secret Manager를 이용하여 MyData Shield의 데이터 베이스 자격정보를 관리할 수 있습니다. 아래 링크를 통해 시작이 하십시오.

  https://docs.aws.amazon.com/ko_kr/secretsmanager/latest/userguide/managing-secrets.html

4.4 Routine Maintenance

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

4.5 Emergency Maintenance

4.5.1 Startup process

- User-Startup 과정

A. 시작

순서	설명	명령어
1	[mydata] 계정으로 SSH 로그인	-
2	Config.py 설정 확인	cat /home/mydata/MyData-Shield-Batch/MyData-Shield/Config.py
3	Nano script로 Config.py 설정 수정	source /home/mydata Config.sh
4	[experdb] 계정으로 로그인	su - experdb
5	eXperDB 시작	pg_ctl start

4.5.2 Health Check

- eXperDB process 확인

순서	설명	명령어
1	[experdb] 계정으로 SSH 로그인	-
2	eXperDB process check	ps -ef | grep experdb
명령어 입력 후 정상 :		

```
[experdb@ip-172-31-37-143 ~]$ ps -ef | grep experdb
root        8747    8723  0 08:58 pts/0    00:00:00 su - experdb
experdb     8751    8747  0 08:58 pts/0    00:00:00 -bash
experdb     8819    8751  0 09:20 pts/0    00:00:00 psql
root        8858    8833  0 09:23 pts/0    00:00:00 su - experdb
experdb     8859    8858  0 09:23 pts/0    00:00:00 -bash
experdb     8887       1  0 09:23 ?        00:00:00 /experdb/app/postgres/bin/po
stgres
experdb     8888    8887  0 09:23 ?        00:00:00 postgres: logger
experdb     8890    8887  0 09:23 ?        00:00:00 postgres: checkpointer
experdb     8891    8887  0 09:23 ?        00:00:00 postgres: background writer
experdb     8892    8887  0 09:23 ?        00:00:00 postgres: walwriter
experdb     8893    8887  0 09:23 ?        00:00:00 postgres: autovacuum launche
r
experdb     8894    8887  0 09:23 ?        00:00:00 postgres: archiver
experdb     8895    8887  0 09:23 ?        00:00:00 postgres: stats collector
experdb     8896    8887  0 09:23 ?        00:00:00 postgres: logical replicatio
n launcher
experdb     8926    8859  0 09:27 pts/0    00:00:00 ps -ef
experdb     8927    8859  0 09:27 pts/0    00:00:00 grep --color=auto experdb
[experdb@ip-172-31-37-143 ~]$
```

명령어 입력 후 비정상 :

- 프로세스가 감지되지 않음

- MyData Shield process 확인

순서	설명	명령어
1	[mydata] 계정으로 SSH 로그인	-
2	MyData Shield process check	ps -ef | grep main.py

명령어 입력 후 정상 :

```
(env) [mydata@ip-172-31-34-99 ~]$ ps -ef | grep main.py
mydata      3242    3178  3 14:03 pts/1    00:00:00 python /home/mydata/MyData-S
hield-Batch/MyData-Shield/main.py
```

명령어 입력 후 비정상 :

- 프로세스가 감지되지 않음

4.5.3 Type of MyData Shield failures

- 서비스 리소스 부족 – EBS 용량

4.5.4 Recovery procedure for MyData Shield failure

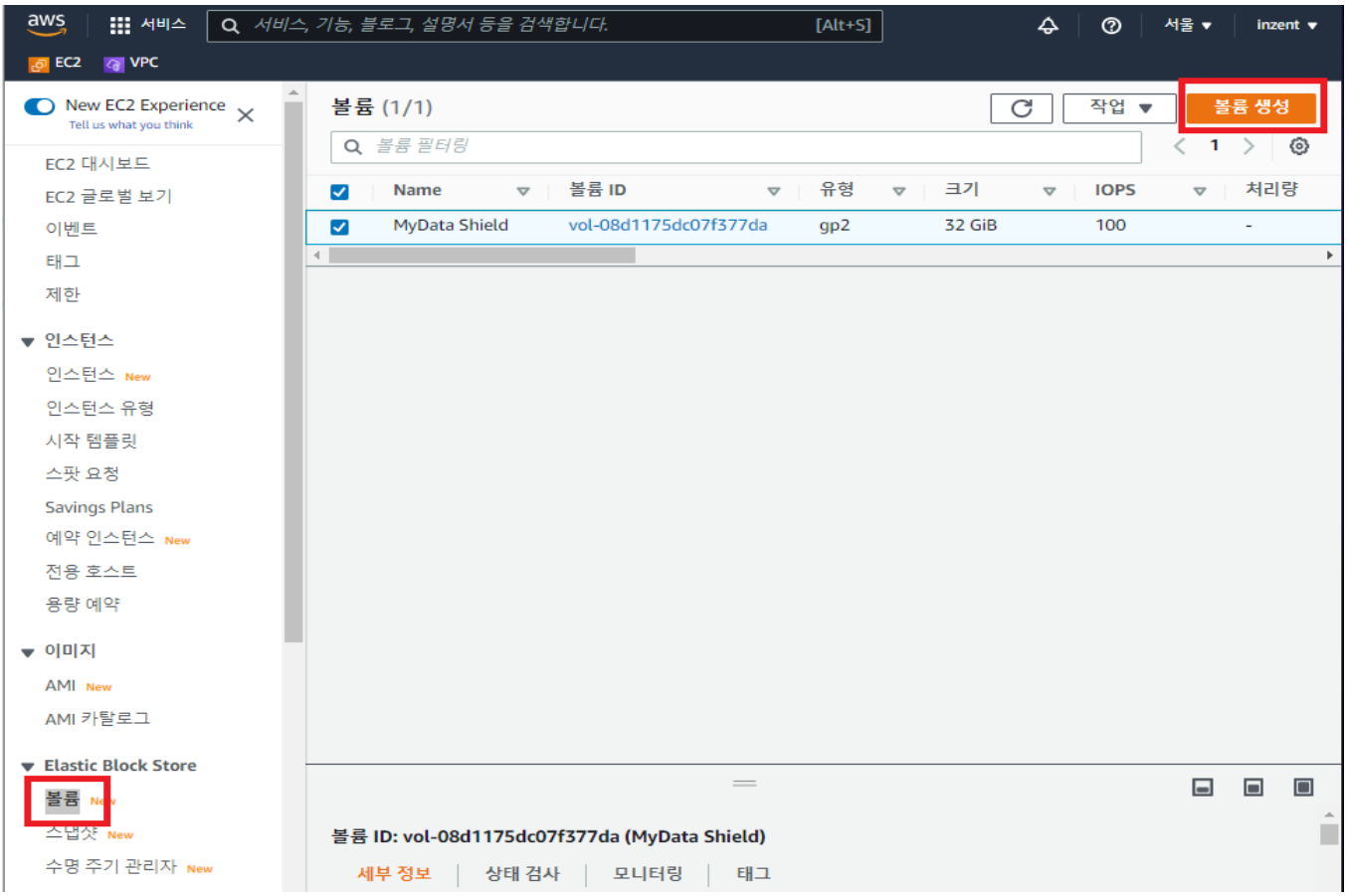
1) 서비스 리소스 부족 – EBS 용량

1. 용량이 100%인 경우

A. 가명/익명 처리가 완료된 MyData을 확인 후 필요 없는 데이터는 삭제.

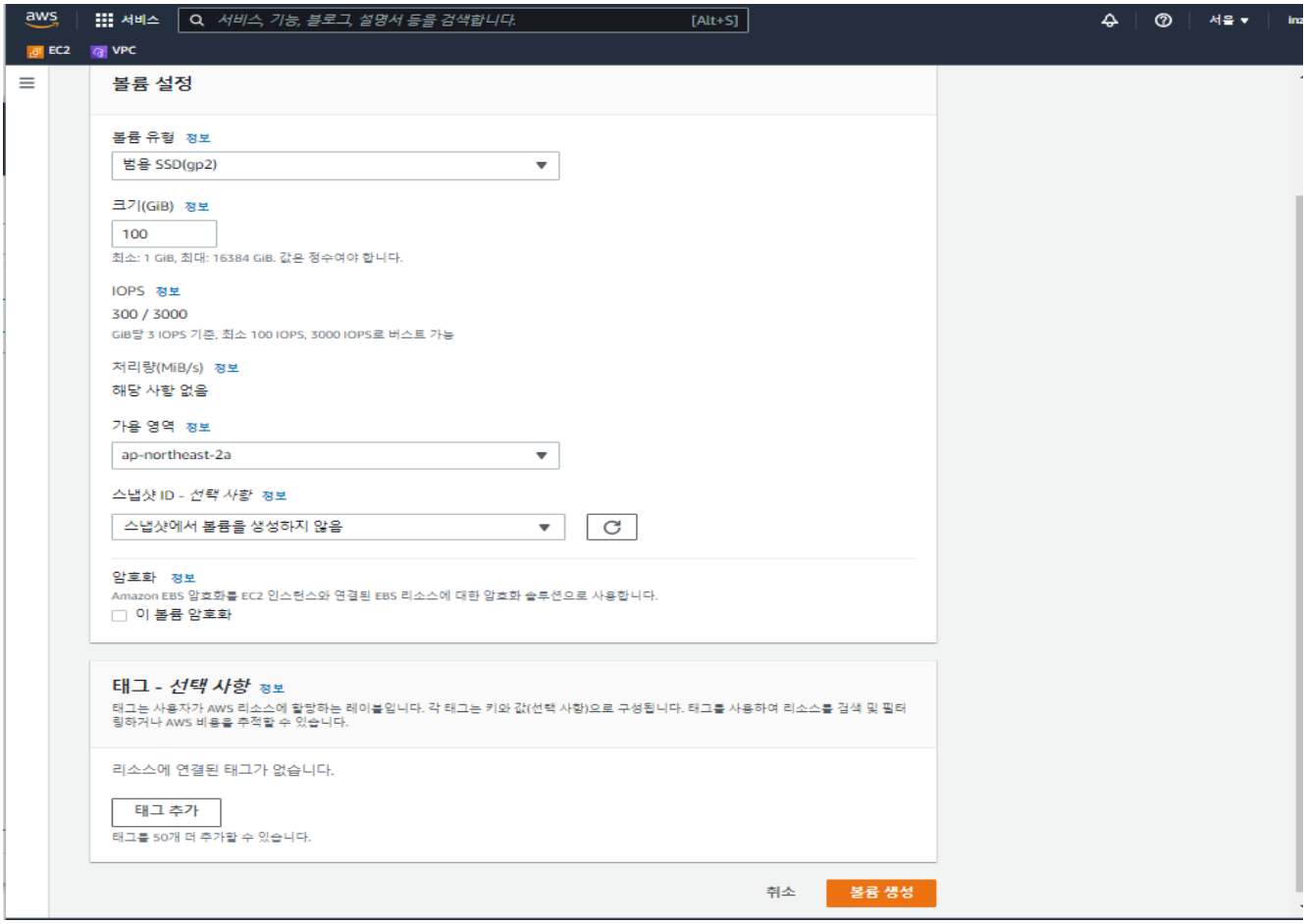
B. 추가로 EBS 용량 확장이 필요한 경우

- AWS EC2 콘솔 > Elastic Block Store > 볼륨 > [MyData Shield] 인스턴스 선택 > 볼륨생성 클릭



- 볼륨 설정은 처리할 MyData 크기에 맞게 설정.

메뉴	설정 값
볼륨 유형	범용 SSD(gp2)
크기(GIB)	처리할 MyData크기



C. MyData Shield Instance reboot

4.5.5 Recovery procedure when MyData Shield recovery fails

- 사용자

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

A. 기존 MyData Shield 스냅샷으로 AMI 재생성

B. MyData Shield 재설치 [3.1.4 Create Instance] 절차를 참고.

4.5.6 RTO

MyData shield의 오류가 발생했을 때 기존 설치한 인스턴스의 스냅샷으로 AMI를 다시 만들고 설치하는 지점까지 최소 10분 ~ 최대 30분 정도 소요합니다.

5. Solution operation

제품을 사용하는 사용자는 Linux CLI 환경 및 Python Script에 대한 지식과 PostgreSQL 전문 지식이 있어야 합니다.

5.1 How to set

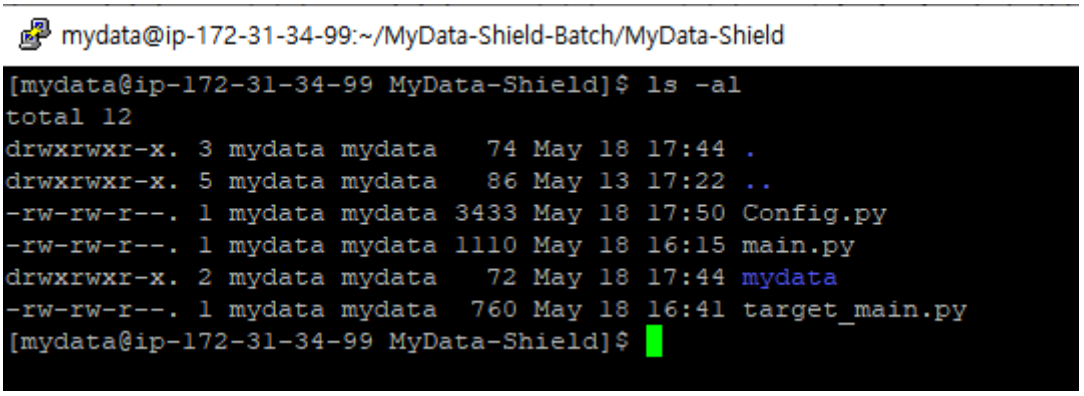
1. **[experdb]** SSH 계정으로 로그인 -> **[pg_ctl start]** 명령어를 통해 eXperDB 실행

2. 실행 스크립트의 위치는 /home/mydata

- [su – mydata] 명령어를 통해 **[mydata]** SSH 로그인

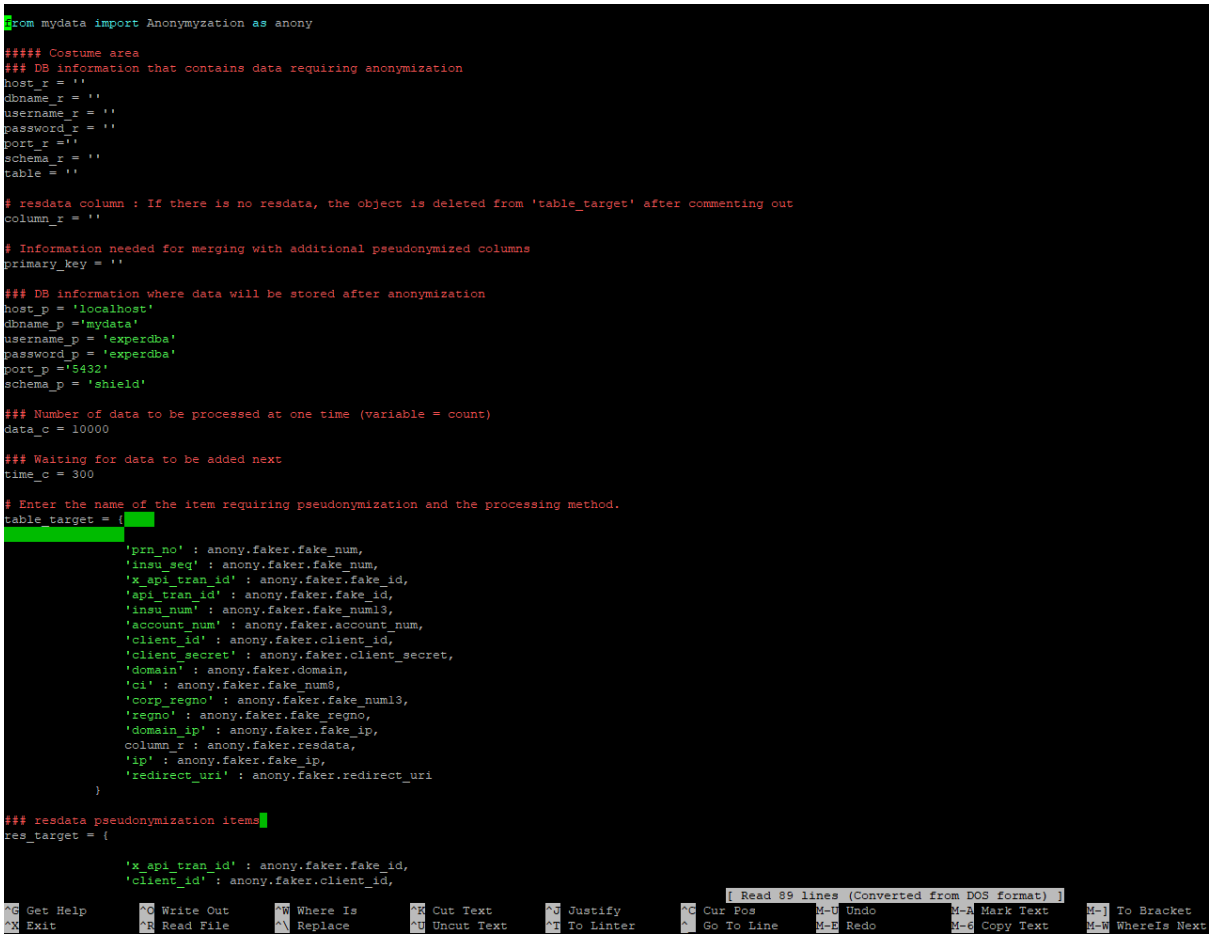
- [ls -al /home/mydata/MyData-Shield-Batch/MyData-Shield] 모듈 확인

(main.py, **target_main.py**, **Config.py**)



3. mydata home으로 돌아가 nano 스크립트 편집기를 사용하여 주석 정보에 따라 DB 정보 및 가명 처리할 '항목명'을 입력해 준다. **(PostgreSQL TO PostgreSQL만 가능)**

- [cd] -> [source /home/mydata/Config.sh]



- Vi 편집기 사용 가능

- sudo vi /home/mydata/MyData-Shield-Batch/MyData-Shield /Config.py

4. MyData 저장 장치 관련 설정이 필요한 항목

- (https://github.com/jw0245/MyData-Shield)의 **내용 참고**

항목	설정 값
host_r	MyData가 존재하는 장치의 Hostname
dbname_r	MyData가 존재하는 DB명
user_r	MyData DB 유저이름
password_r	MyData DB Password
port_r,	MyData DB port
table	MyData table명

column_r	MyData [Json type]데이터가 존재하는 컬럼명
Primary_key	MyData 테이블에 식별키

5. MyData Shield 인스턴스 eXperDB 정보

항목	설정 값
host_p	MyData Shield Hostname
dbname_p	MyData를 저장할 DB이름
user_p	MyData Shield DB 유저이름
password_p	MyDataShield DB Password
port_p	MyDataShield Postgresql port
schema_p	가명 처리한 MyData를 분류할 schema 명

6. MyData API 표준 규격 관련 설정

항목	설정 값
table_target	MyData 테이블안에 가명처리가 필요한 칼럼에 대한 설정
res_target	MyData API 표준규격을 참고하여 가명처리가 필요한 '항목명'에 대한 설정 (JSON Type에 해당하는 컬럼 및 값에 맞게 설정)

7. 데이터 처리 수

항목	설정값
data_c	읽어 온 데이터에 대해서 나눠서 처리할 데이터 수
time_c	모든 프로세스를 종료했을 때 새로운 데이터를 확인하는 주기

5.2 How to run

- Config 설정 후 mydata 홈[cd /home/mydata]으로 이동
- Python 모듈의 실행을 위해 가상 환경 실행
- 원하는 프로세스 아래 명령어를 통해 실행

명령어	설명
source env.sh	모듈을 실행하기 위한 가상 환경 실행

source Start.sh	MyData Store 의 데이터를 가명처리를 수행 후 인스턴스의 eXperDB 에 설정한 저장소에 저장되는 프로세스 실행
source add_target.sh	**(선택 사항)** 새로 추가된 데이터는 없지만, MyData(Json type)의 '힝목명' 중 가명 처리를 원하는 '항목명'이 추가 설정되었을 때, 해당 '항목명'에 해당하는 데이터를 추가로 가명 처리 후 eXperDB 에 저장되는 프로세스 실행

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. Secret Manager 키 관리

필요한 경우 Secret Manager를 통한 DB 정보 암호화를 지원하도록 AWS KMS keys를 사용할 수 있습니다. 아래 링크를 통해 확인하세요 :

https://docs.aws.amazon.com/secretsmanager/latest/userguide/security-encryption.html

5.4 Patches and updates management

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

URL : http://www.inzent.com/board/board.php?bo_table=faq&pageName=main

6. Support

6.1 Technical support

기술 지원 서비스는 문서에 명시된 기능에 대해서만 제공합니다.

기술 지원 범위는 다음과 같습니다.

A. 설치 지원 : 설치 가이드 제공, Github 을 통한 소스 제공

➔ Github : https://github.com/jw0245/MyData-Shield

B. 커스터마이징 지원

C. 실시간 Rest API 기능 추가 제공

D. 가명처리 기능 데모 페이지

➔ https://mydapi.inzent.com/shield

기술 지원 연락처는 다음과 같습니다.

E. URL : http://www.inzent.com/board/board.php?bo_table=faq&pageName=main

F. TEL : 02-787-3600

- 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 :

- 실시간 Rest API 기능 추가 제공
- 커스터마이징 지원 (공수 별도산정)

6.3 SLA

- Free Tier : 소스 제공, 설치 가이드
- Technical Service Pack : 고객 요청 시, 기준시간에 해당하는 기술지원 수행