AWS 구성 매뉴얼

문서 기록

|  |  |  |
| --- | --- | --- |
| 작성자 | 날짜 | 설명 |
| 김다운 | 2022-02-07 | Ver 1.0 : 처음 생성 |
| 김다운 | 2022-02-10 | Ver 2.0, Ver 3.0 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

목차

[**구성도** 6](#_Toc95465688)

[**NACL** 6](#_Toc95465689)

[**1.** **VPC(도로)** 8](#_Toc95465690)

[**1.1** **VPC 생성** 9](#_Toc95465691)

[**1.2** **서브넷 생성** 11](#_Toc95465692)

[**1.3** **인터넷 게이트웨이 생성** 14](#_Toc95465693)

[**1.4** **라우팅 테이블** 16](#_Toc95465694)

[1) 라우팅 편집 16](#_Toc95465695)

[1) 서브넷 연결 19](#_Toc95465696)

[**2.** **네트워크 ACL(톨게이트)** 21](#_Toc95465697)

[**2.1** **Web**(default 사용) 21](#_Toc95465698)

[1) 서브넷 연결 22](#_Toc95465699)

[2) 인/아웃바운드 규칙 23](#_Toc95465700)

[**2.2** **Was** 25](#_Toc95465701)

[1) NACL 생성 25](#_Toc95465702)

[2) 서브넷 연결 26](#_Toc95465703)

[3) 인/아웃바운드 규칙 27](#_Toc95465704)

[**2.3** **DB** 30](#_Toc95465705)

[1) NACL 생성 30](#_Toc95465706)

[2) 서브넷 연결 31](#_Toc95465707)

[3) 인/아웃바운드 규칙 32](#_Toc95465708)

[**3.** **보안그룹(현관문)** 34](#_Toc95465709)

[**3.1** **WEB -** nginx 34](#_Toc95465710)

[1) 인/아웃바운드 규칙 35](#_Toc95465711)

[**3.2** **API** – flask 37](#_Toc95465712)

[1) 보안 그룹 생성 37](#_Toc95465713)

[2) 인/아웃바운드 규칙 38](#_Toc95465714)

[**3.3** **DB** – maria 39](#_Toc95465715)

[1) 보안 그룹 생성 39](#_Toc95465716)

[2) 인/아웃바운드 규칙 40](#_Toc95465717)

[**4.** **EC2** 41](#_Toc95465718)

[**4.1** **인스턴스 생성** 41](#_Toc95465719)

[1) AMI 선택 41](#_Toc95465720)

[2) 인스턴스 유형 선택 42](#_Toc95465721)

[3) 인스턴스 구성 42](#_Toc95465722)

[4) 스토리지 43](#_Toc95465723)

[5) 태그 추가 44](#_Toc95465724)

[6) 보안 그룹 구성 44](#_Toc95465725)

[7) 키페어 46](#_Toc95465726)

[**4.2** **탄력적 IP** 49](#_Toc95465727)

[1) 탄력적 IP 주소 할당 49](#_Toc95465728)

[2) 탄력적 IP 주소 연결 51](#_Toc95465729)

[**4.3** **SSH** 52](#_Toc95465730)

[1) Putty 56](#_Toc95465731)

[2) 명령프롬프트 59](#_Toc95465732)

[3) Nginx 60](#_Toc95465733)

[**5.** **데이터베이스** 61](#_Toc95465734)

[**5.1** **서브넷 그룹 생성** 61](#_Toc95465735)

[**5.2** **데이터베이스 생성** 64](#_Toc95465736)

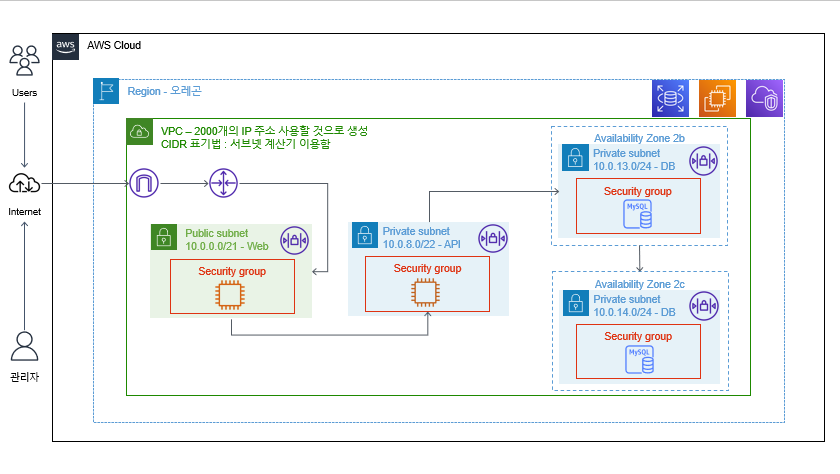
[**5.3** **RDS 외부 작업 – MySQL 접속** 69](#_Toc95465737)

[1) rds-sg 인바운드 규칙 편집 69](#_Toc95465738)

[2) .ppk -> .pem 변환 69](#_Toc95465739)

[3) MySQL Workbench 70](#_Toc95465740)

# **구성도**



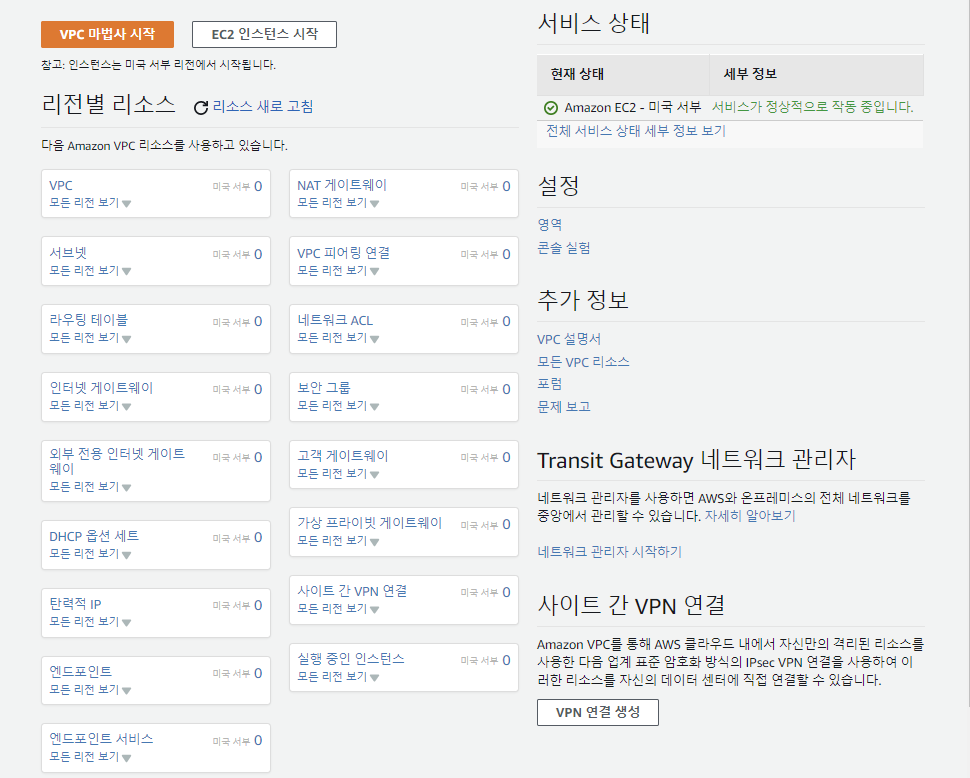
# **NACL**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 필요한 IP 개수 |  | 사용가능 범위 |  |
| **CIDR** | 2000 |  |  |  |
| 10.0.0.0 |  |  |  |  |
| 10.0.0.0/20 | 4000 |  | 10.0.0.0 - 10.0.15.255 |  |
|  |  |  |  |  |
|  | 예상 | 실제 사용수 | 사용가능 범위 | CIDR |
| 웹 서버 | 1000 | 200 | 10.0.0.0 - 10.0.3.255 | 10.0.0.0/21 |
| API(WAS) 서버 | 500 | 100 | 10.0.8.0 - 10.0.9.255 | 10.0.8.0/22 |
| DB 서버 | 20 | 3 | 10.0.13.0 - 10.0.13.255 | 10.0.13.0/24 |
|  |  |  | 10.0.14.0 - 10.0.14.255 | 10.0.14.0/24 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Network ACL** |  | | |
| 범위 | 포트 | | 설명 |
|  | 인 | 아웃 |
| 10.0.0.0/21 | 80 | 80 | 인터넷 - http |
|  | 443 | 443 | 인터넷 보안 - https |
| 10.0.8.0/22 | 5000 | 5000 | Flask : TCP |
| 10.0.13.0/24 | 3306 | 3306 | Maria / MySQL : TCP |

|  |  |  |  |
| --- | --- | --- | --- |
| **보안 그룹(SG)** |  | | |
| 범위 | 포트 | | 설명 |
| 인 | 아웃 |
| 10.0.0.0/21 | 80 | 80 | 인터넷 - http |
| 443 | 443 | 인터넷 보안 - https |
| 10.0.8.0/22 | 5000 | 5000 | Flask : TCP |
| 10.0.13.0/24 | 3306 | 3306 | Maria / MySQL : TCP |

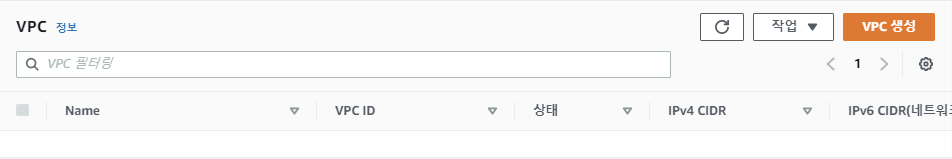
# **VPC(도로)**



## **VPC 생성**

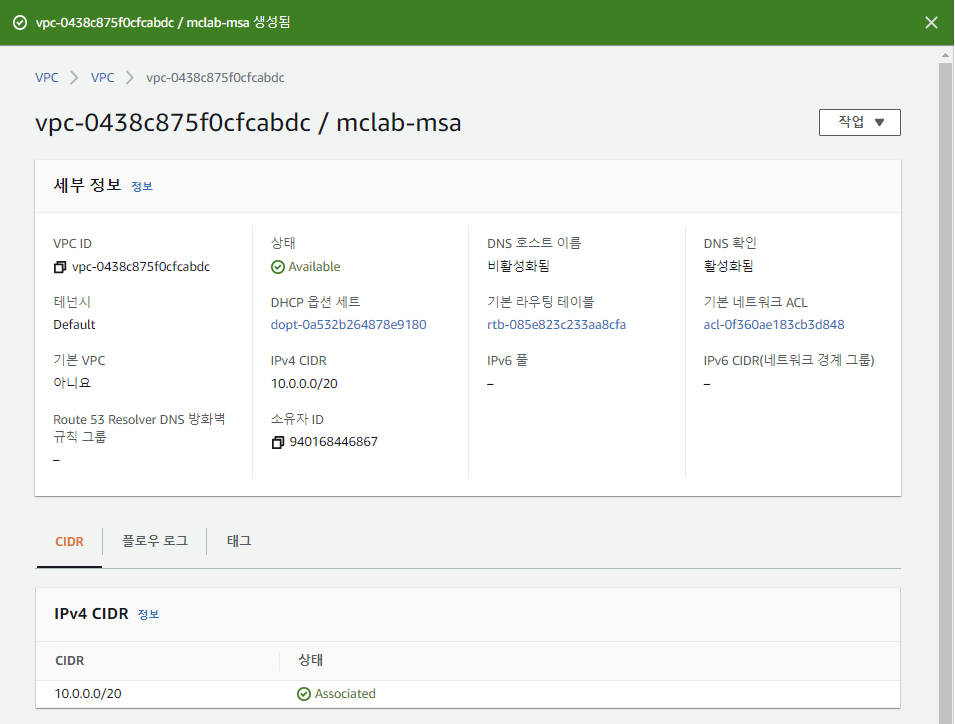
텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

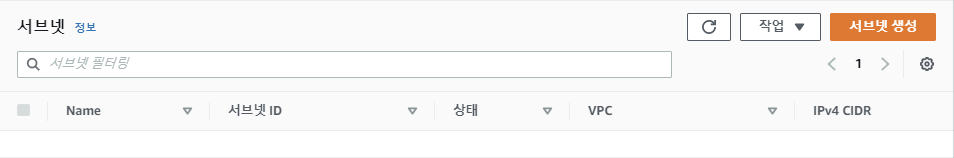
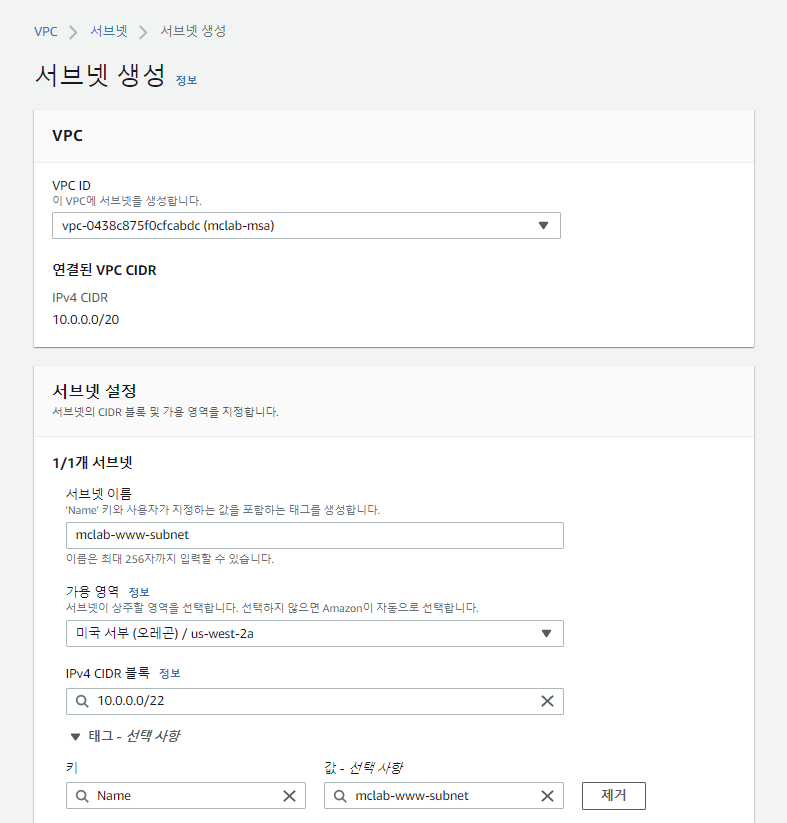
자동 생성된 설명

**CIDR 계산기를 이용해 값 입력**

텍스트이(가) 표시된 사진

자동 생성된 설명

## **서브넷 생성**

**Web 서버**

텍스트이(가) 표시된 사진

자동 생성된 설명

**API 서버**

**텍스트이(가) 표시된 사진

자동 생성된 설명**

**DB 서버(RDS1, 2)**

**텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명**

**테이블이(가) 표시된 사진

자동 생성된 설명**

## **인터넷 게이트웨이 생성**

VPC와 인터넷 간의 연결을 위해

테이블이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

인터넷 게이트웨이를 VPC에 연결

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

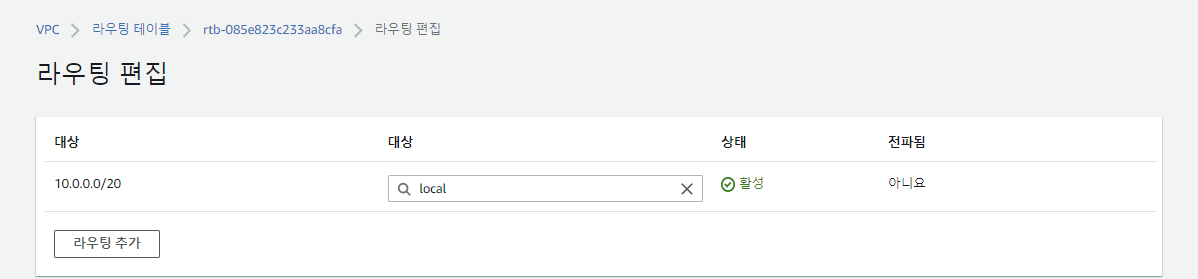
## **라우팅 테이블**

### 라우팅 편집

인터넷 연결을 위해

텍스트이(가) 표시된 사진

자동 생성된 설명



텍스트이(가) 표시된 사진

자동 생성된 설명

생성한 인터넷게이트웨이 선택 (해야 탄력적 IP 연결 됨)

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

### 서브넷 연결

텍스트이(가) 표시된 사진

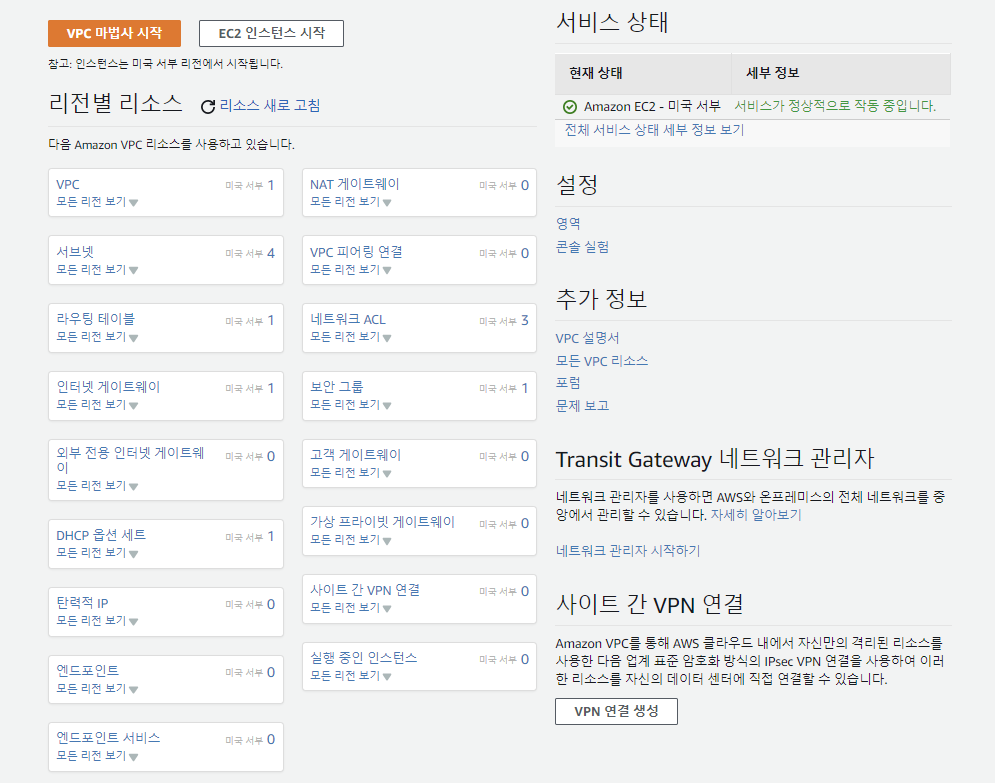
자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

라우팅테이블에 있는 dafault를 web서브넷과 연결

VPC 생성 확인



# **네트워크 ACL(톨게이트)**

서브넷에 대한 트래픽 제어하기 위한 방화벽 역할

규칙번호는 낮은 순으로 적용

## **2.1 Web**(default 사용)

텍스트이(가) 표시된 사진

자동 생성된 설명

이름 변경

### 서브넷 연결

텍스트이(가) 표시된 사진

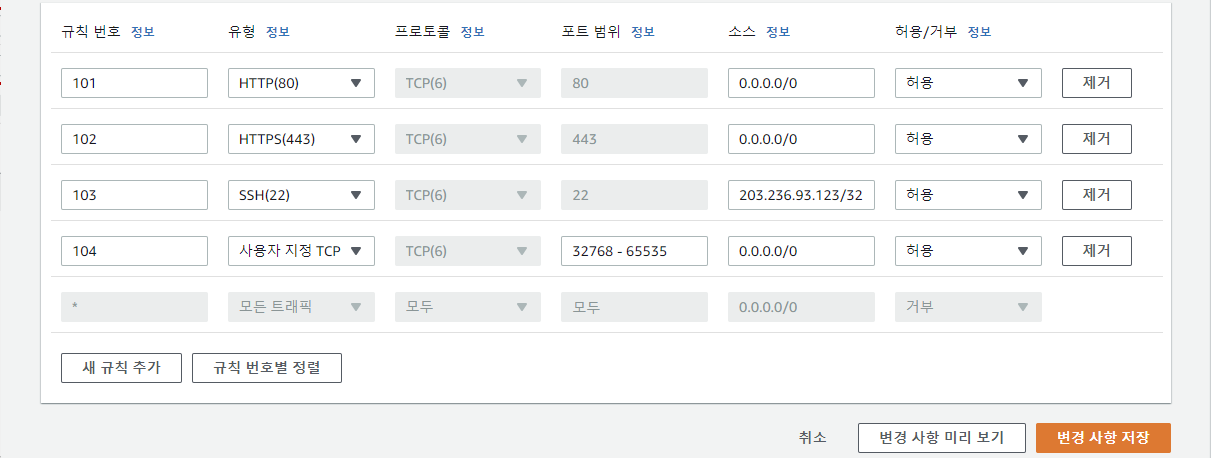
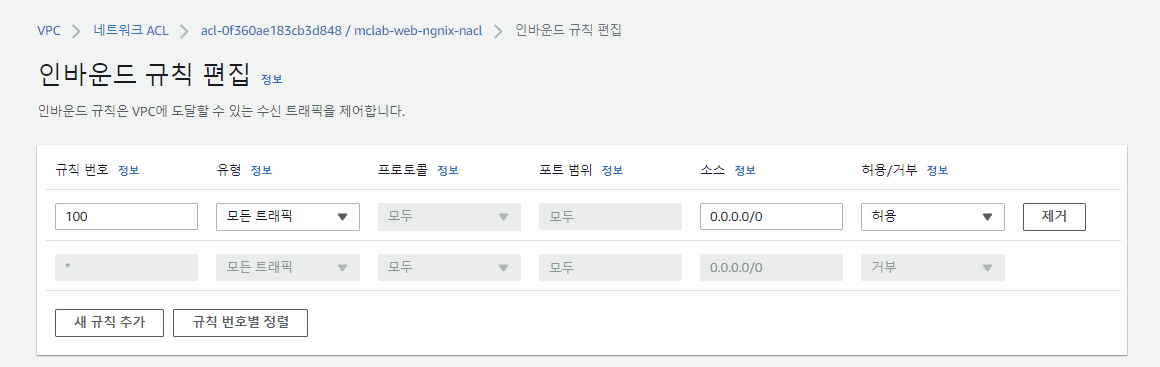
자동 생성된 설명

내가 만든 서브넷은 기본NACL에 연결되기 때문에 변동없음

### 인/아웃바운드 규칙

텍스트이(가) 표시된 사진

자동 생성된 설명



내IP/32

텍스트, 테이블이(가) 표시된 사진

자동 생성된 설명

내IP/32

#### 아웃바운드 규칙 – 변동없음

테이블이(가) 표시된 사진

자동 생성된 설명

## **2.2 Was**

### NACL 생성

**텍스트이(가) 표시된 사진

자동 생성된 설명**

### 서브넷 연결

텍스트이(가) 표시된 사진

자동 생성된 설명



텍스트이(가) 표시된 사진

자동 생성된 설명

### 인/아웃바운드 규칙

텍스트, 테이블이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

#### 아웃바운드 규칙

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

## **2.3 DB**

### NACL 생성

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

### 서브넷 연결

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트, 테이블이(가) 표시된 사진

자동 생성된 설명

### 인/아웃바운드 규칙

* 인바운드 규칙

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

* 아웃바운드 규칙

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

# **보안그룹(현관문)**

## **3.1 WEB -** nginx

Default -> WEB용으로 수정

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

### 인/아웃바운드 규칙

* 인바운드 규칙

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명





* 아웃바운드 규칙 – 변동없음

테이블이(가) 표시된 사진

자동 생성된 설명

## **3.2 API** – flask

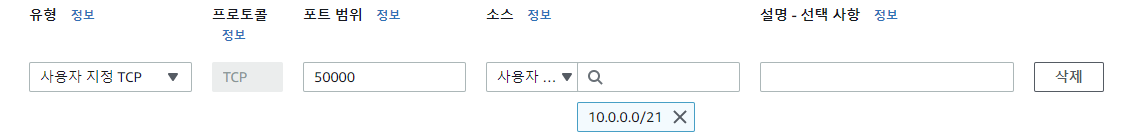
### 보안 그룹 생성

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명



텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

### 인/아웃바운드 규칙

테이블이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

## **3.3 DB** – maria

### 보안**텍스트이(가) 표시된 사진 자동 생성된 설명**텍스트, 스크린샷, 실내이(가) 표시된 사진 자동 생성된 설명 그룹 생성

텍스트이(가) 표시된 사진

자동 생성된 설명

### 텍스트이(가) 표시된 사진 자동 생성된 설명인/아웃바운드 규칙

텍스트이(가) 표시된 사진

자동 생성된 설명

테이블이(가) 표시된 사진

자동 생성된 설명

확인

텍스트이(가) 표시된 사진

자동 생성된 설명

# **EC2**

텍스트이(가) 표시된 사진

자동 생성된 설명

## **인스턴스 생성**

텍스트이(가) 표시된 사진

자동 생성된 설명

### AMI 선택

텍스트이(가) 표시된 사진

자동 생성된 설명

### 인스턴스 유형 선택

테이블이(가) 표시된 사진

자동 생성된 설명

### 인스턴스 구성

텍스트이(가) 표시된 사진

자동 생성된 설명

Web subnet 선택

텍스트이(가) 표시된 사진

자동 생성된 설명



### 스토리지

최저 8GB

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

### 태그 추가

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

### 보안 그룹 구성

텍스트이(가) 표시된 사진

자동 생성된 설명

Web용 보안그룹 선택

* 22번 포트를 허용하지 않았을 때

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

### 키페어

텍스트이(가) 표시된 사진

자동 생성된 설명

인스턴스 생성 확인

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

## **탄력적 IP**

퍼블릭 주소를 생성하기 위해

인스턴스 – 네트워크 및 보안 – 탄력적 IP

### 탄력적 IP 주소 할당

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

### 탄력적 IP 주소 연결

생성된 공인IP를 인스턴스와 연결

테이블이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

공인IP 할당 -> 인스턴스 연결버튼 활성화됨

## **4.3 SSH**

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

주소 복사 후 명령 프롬프트(키페어가 있는 위치에서)로 ssh 접속

텍스트이(가) 표시된 사진

자동 생성된 설명

#### .pem 파일 권한 설정

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

**계정명**

텍스트이(가) 표시된 사진

자동 생성된 설명

**계정명**

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

**계정명**

텍스트이(가) 표시된 사진

자동 생성된 설명

**계정명**

텍스트이(가) 표시된 사진

자동 생성된 설명

**계정명**

**계정명**

텍스트이(가) 표시된 사진

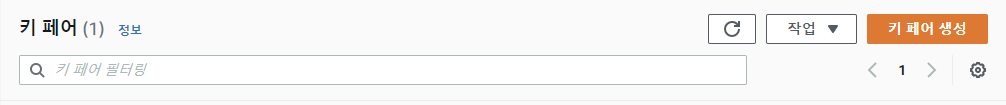
자동 생성된 설명

**계정명**

#### Putty

Putty는 .ppk만 사용 가능

* 인스턴스 생성 전 .ppk 키페어 생성



텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

* 텍스트이(가) 표시된 사진

  자동 생성된 설명.pem -> .ppk**텍스트이(가) 표시된 사진

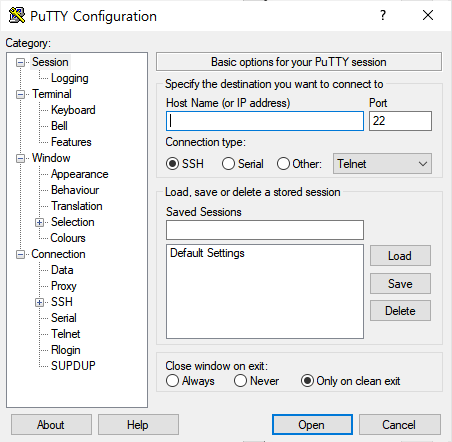
  자동 생성된 설명**

.ppk파일로 변환해 저장

.pem파일 Load

**Putty로 ssh 접속**

텍스트이(가) 표시된 사진

자동 생성된 설명

**인스턴스 퍼블릭IP 입력**

.ppk파일 로드 후 ssh 연결

텍스트이(가) 표시된 사진

자동 생성된 설명

**사용자 이름 입력(ubuntu)**

텍스트이(가) 표시된 사진

자동 생성된 설명

키파일을 Load해줬기 때문에 비밀번호 없이 접속 가능

### 명령프롬프트

텍스트이(가) 표시된 사진

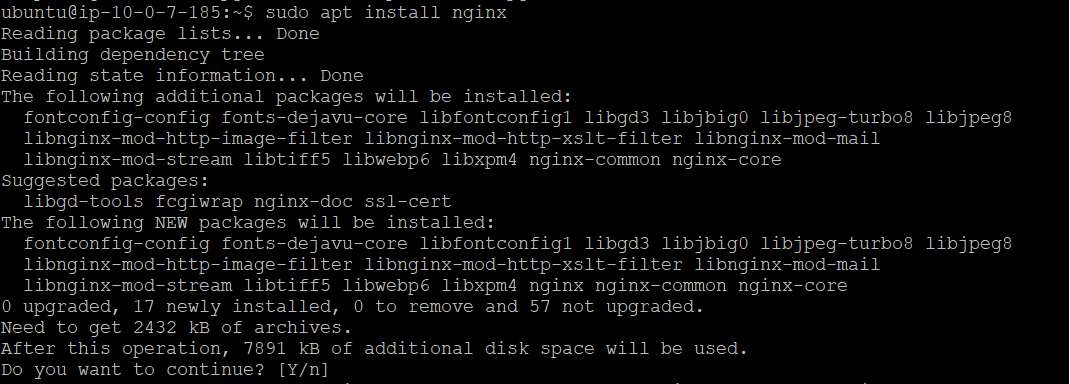
자동 생성된 설명

ssh 접속해 인스턴스에 연결 완료

### Nginx



* nginx 설치



Y or Enter 입력

* nginx연결 확인

퍼블릭IP

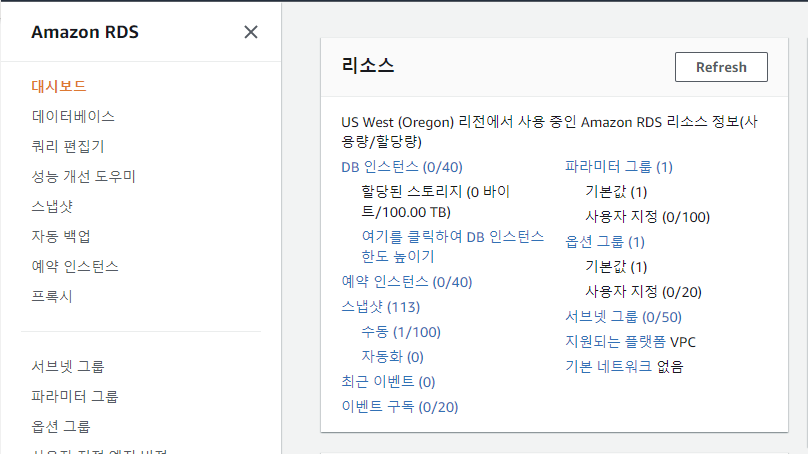
퍼블릭IP

텍스트이(가) 표시된 사진

자동 생성된 설명

주소창에 [인스턴스의 퍼블릭 IPv4 주소] 입력해 nginx연결 확인

# **데이터베이스**



## **서브넷 그룹 생성**

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

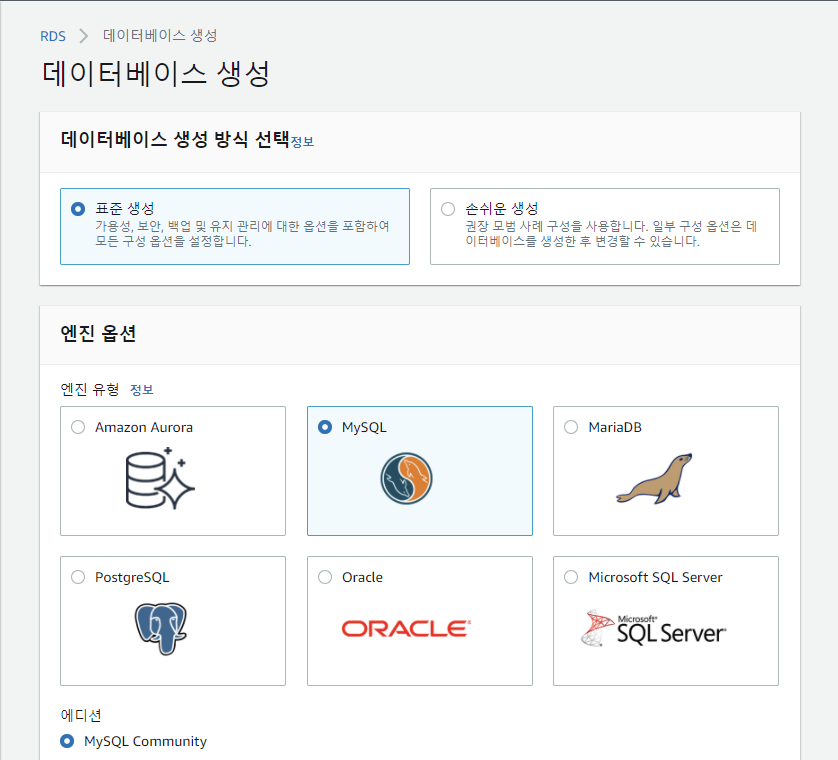
자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

## **데이터베이스 생성**

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

**DB용 보안 그룹 선택**

**백업 X**

**유지 관리 X**

텍스트이(가) 표시된 사진

자동 생성된 설명

## **5.3 RDS 외부 작업 – MySQL 접속**

### 1) rds-sg 인바운드 규칙 편집

10.0.8.0/22 -> 10.0.0.0/20(인터넷 연결이 가능한)

테이블이(가) 표시된 사진

자동 생성된 설명

### 2) .ppk -> .pem 변환

PuTTYgen

텍스트이(가) 표시된 사진

자동 생성된 설명

.ppk파일 Load - Conversions - Export OpenSSH key - .ppk파일 선택 후 확장자명 .pem으로 변경 - 저장

### MySQL Workbench

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

**사용자 이름(ssh 연결했을 때)**

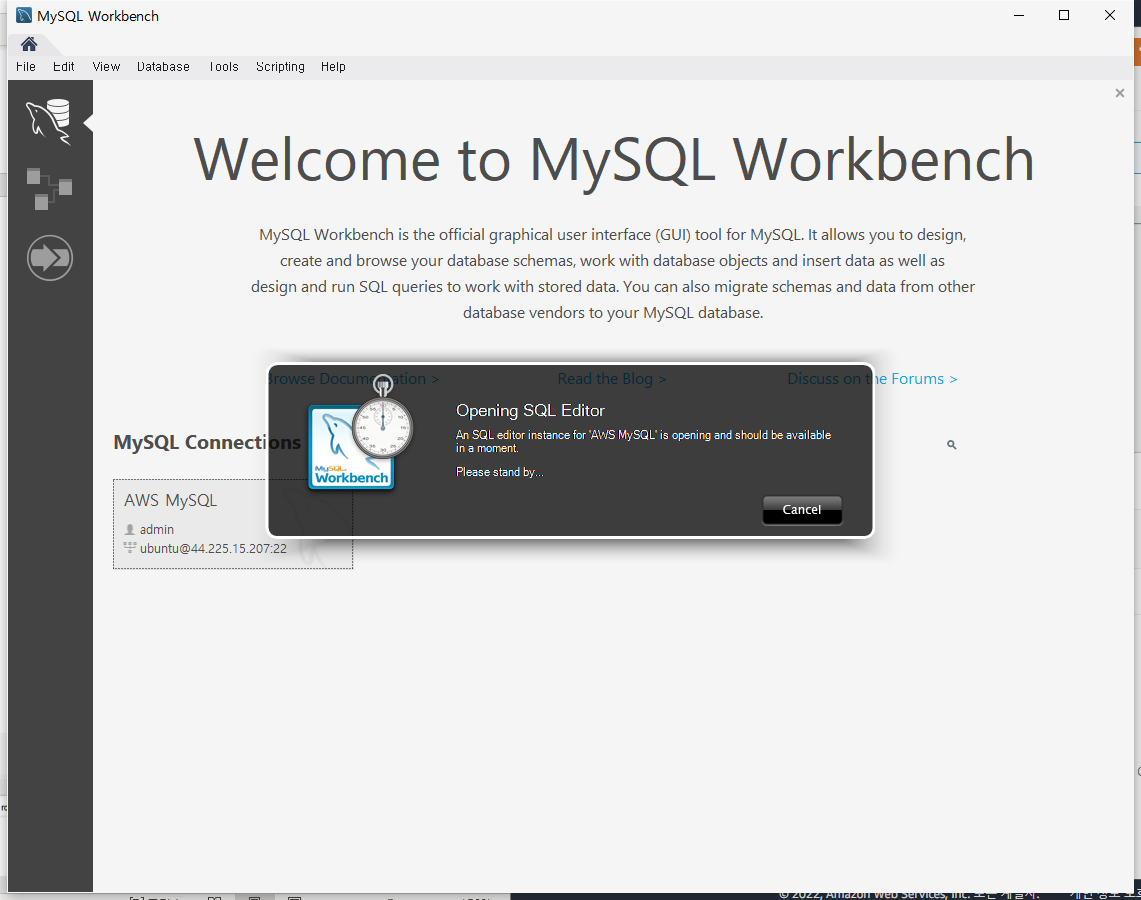
**마스터 사용자 이름**

**퍼블릭 IP:22**

**DB 이름**

**키페어(.pem) Load**

Connection Method - Standard TCP/IP over SSH 선택

텍스트이(가) 표시된 사진

자동 생성된 설명

더블클릭

텍스트이(가) 표시된 사진

자동 생성된 설명