

# PostgreSQL

## 서비스 생성

(Creating PostgreSQL service)

October 2024

## 시나리오 구성

### 1. PostgreSQL 서비스 생성

#### 학습 목표

#PostgreSQL #Virtual Private Cloud(VPC) #Subnet #Firewall #Public IP #Internet Gateway(IGW) #Security Group #Virtual Server

본 PostgreSQL 서비스 생성 시나리오는 Public Subnet으로 Bastion Host(VM)를 생성하고, Database서 비스를 Private Subnet으로 생성하여 Bastion Host에서 접근하는 시나리오입니다.

SCP 환경에서 PostgreSQL(DBaaS)에 대한 안정적인 접속을 위해서는 Bastion Host에 대한 생성과 이를 이용한 네트워크연결이 필수적입니다. 본 가이드에서는 안정적이고 높은 보안 수준을 충족시키기 위해 Database 서비스의 경우 Private Subnet 환경, Bastion Host는 제한적인 Public Subnet 환경에서 구성하 기를 권고합니다. 이러한 구성은 단일 인스턴스나 중요 데이터의 안정적인 관리를 위해고가용성 구성, 읽 기/복제, 백업/복구, 패치, 파라미터 관리, 감사, 모니터링 등 DB 관리기능을 추가하여 데이터베이스의 생 명 주기 내 업무를 자동화 할 수 있습니다.

본 시나리오는 크게 Bastion Host 생성하고 서버와 DB 접속을 위한 Security Group를 적용하는 것과, DB 접속 툴(pgadmin)을 설치하여 Database 접속이 가능한 환경을 구성하는 것으로 이루어져 있습니다.

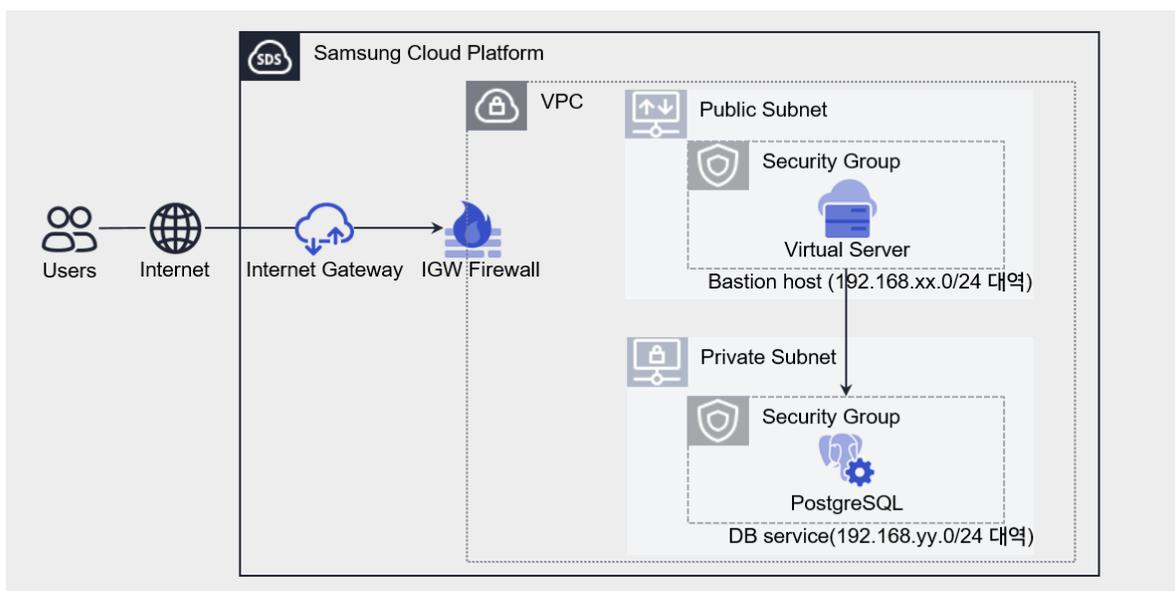


그림 1. PostgreSQL 서비스 생성 시나리오 구성도

#### 사전 작업

#### <사용되는 상품 리스트>

- PostgreSQL

- VPC
- Security Group
- Firewall
- 공인 IP
- Virtual Server

## 따라하기

### 사전 작업 준비하기

#### 1. 서버 Key pair 상품 신청하기

- ① **Management > 서버 Key pair** 메뉴에서 **상품신청** 버튼을 클릭하세요. **서버 Key pair 신청** 화면으로 이동합니다.
- ② **서버 Key pair** 화면에서 서버 Key pair 정보를 입력하세요.

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	서버 Key pair명	keyTest

- ③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.
- ④ 신청이 완료되면, 해당 Private Key 가 개인 저장 공간에 다운로드 됩니다.

### 서버 생성하기

#### 2. VPC 상품 신청하기

- ① **Networking > VPC > VPC** 메뉴에서 **상품신청** 버튼을 클릭하세요. **VPC-VPC 신청** 화면으로 이동합니다.
- ② **VPC-VPC 신청** 화면에서 VPC 필수 정보를 입력하세요.

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	VPC명	VPCtest

- ③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

#### 3. Subnet 서비스 생성하기

① **Networking > VPC > 서브넷** 메뉴에서 **상품신청** 버튼을 클릭하세요. **VPC-서브넷 생성** 화면으로 이동합니다.

- 본 시나리오에서는 Bastion Host 용 Public Subnet 과 Database 용 Private Subnet 을 각각 한 개씩 생성합니다.

② **VPC-서브넷 생성** 화면에서 해당 Subnet 의 필수 정보를 입력하세요.

화면	필수 입력 요소 항목	입력 값
필수 정보 입력 #1	VPC	생성한 VPC 선택
	사용 용도	일반 - Public
	서브넷명	<b>PUBSUBtest</b>
	IP 대역	192.168.xx.0/24

화면	필수 입력 요소 항목	입력 값
필수 정보 입력 #2	VPC	생성한 VPC 선택
	사용 용도	일반 - Private
	서브넷명	<b>DBSUBtest</b>
	IP 대역	192.168.yy.0/24

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

#### 4. Security Group 상품 신청하기

① **Networking > Security Group** 메뉴에서 **상품신청** 버튼을 클릭하세요. **Security Group 신청** 화면으로 이동합니다.

- 본 시나리오에서는 2 개의 Security Group 을 생성합니다.

② **Security Group 신청** 화면에서 해당 Security Group 의 필수 정보를 입력하세요.

화면	필수 입력 요소 항목	입력 값
#1	Security Group 명	<b>DBSGtest</b>
	VPC	생성한 VPC 선택
	로그인 여부	사용 안함

화면	필수 입력 요소 항목	입력 값
필수 정보 입력 #2	Security Group 명	BastionSGtest
	VPC	생성한 VPC 선택
	로깅 여부	사용 안함

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

5. Internet Gateway 서비스 생성하기

① **Networking > VPC > Internet Gateway** 메뉴에서 **IGW 생성** 버튼을 클릭하세요. **VPC-Internet Gateway 생성** 화면으로 이동합니다.

② **Internet Gateway 생성** 화면에서 해당 Internet Gateway의 필수 정보를 입력하세요.

- Firewall 사용을 선택해 인터넷 접근 제어를 위한 방화벽을 생성합니다.

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	VPC	생성한 VPC 선택
	구분	Internet Gateway
	Firewall 사용	사용

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

6. Public IP 예약하기

① **Networking > VPC > Public IP** 메뉴에서 **IP 예약** 버튼을 클릭하세요. **VPC-Public IP 예약** 화면으로 이동합니다.

② **VPC-Public IP 예약** 화면에서 필수 정보를 입력하세요.

화면	필수 입력 요소 항목	입력 값
필수 정보 입력	구분	Internet Gateway

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

7. PostgreSQL(DBaaS) 상품 신청하기

① **Database > PostgreSQL(DBaaS)** 메뉴에서 **상품신청** 버튼을 클릭하세요. **PostgreSQL(DBaaS) 신청** 화면으로 이동합니다.

② **PostgreSQL(DBaaS) 신청** 화면에서 이미지를 선택하고, 상품 구성 및 필수 정보를 입력하세요.

화면	필수 입력 요소 항목	입력 값
이미지 선택	이미지	PostgreSQL Community
	이미지 버전	PostgreSQL Community 15.5
상품 구성	서버명 (Prefix)	pdb-test
	클러스터명	pdclsTest
	상품 유형 - Block Storage	(DATA) 10GB
	네트워크 - VPC	생성한 VPC 선택
	네트워크 - 일반 서브넷	생성한 Private Subnet 선택
	Security Group	생성한 Database용 Security Group 선택
필수 정보 입력	Database명	dbTest
	Database 사용자명	usrtest
	Database 비밀번호	사용할 비밀번호 입력
	Database 비밀번호 확인	사용할 비밀번호 입력
	Database Port번호	2866
Replica 구성	Replica 구성	사용 안함

③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

#### 8. Bastion Host 용 Virtual Server 상품 신청하기

- ① **Compute > Virtual Server > Virtual Server** 메뉴에서 **상품신청** 버튼을 클릭하세요. **Virtual Server-Virtual Server 신청** 화면으로 이동합니다.
- ② **Virtual Server 신청** 화면에서 이미지를 선택하고, 상품 구성 및 필수 정보를 입력하세요.
  - 서버에 접속하기 위한 Key pair 는 미리 생성된 Key 를 선택하거나 새롭게 생성할 수 있습니다.
  - 미리 생성한 VPC, Subnet, Public IP, Security Group 을 선택하여 연결하기 위해 적용 정책은 '서버별 설정'을 선택하세요.

화면	필수 입력 요소 항목	입력 값
----	-------------	------

이미지 선택	이미지	표준 - Windows
	이미지 버전	Windows 2019 Standard ENG (64bit)
상품 구성	서버 수	1
	(Block Storage) 기본 OS	bs-bastionTest
필수 정보 입력	서버 Key pair	생성한 Key pair 선택
	서버명	bastionTest
	네트워크 설정 - NAT	사용
	네트워크 설정 - NAT IP	예약된 Public IP 선택
	Security Group	생성한 Bastion Host용 Security Group 선택

- ③ 신청 정보를 확인하고, **완료** 버튼을 클릭하세요.

9. Database 용 Security Group 보안 규칙 추가하기

- ① **Networking > Security Group** 메뉴에서 **자원관리** 버튼을 클릭하세요. **Security Group 목록** 화면으로 이동합니다.
- ② **Security Group 목록** 화면에서 미리 생성한 Database 용 Security Group 을 선택하세요.
- ③ 해당 **Security Group 상세** 화면의 **규칙** 탭에서 **규칙 추가** 버튼을 클릭하세요. **규칙 추가** 팝업창이 열립니다.
- ④ **규칙 추가** 팝업창에서 해당 트래픽 관련 필수 정보를 입력하고, **확인** 버튼을 클릭하세요.

화면	필수 입력 요소 항목	입력 값
규칙 추가	방향	Inbound 규칙
	대상주소	Public Subnet의 CIDR (192.168.xx.0/24)
	프로토콜	TCP
	허용포트	직접입력(2866)

10. Bastion Host 용 Security Group 보안 규칙 추가하기

- ① **Networking > Security Group** 메뉴에서 **자원관리** 버튼을 클릭하세요. **Security Group 목록** 화면으로 이동합니다.

- ② **Security Group 목록** 화면에서 미리 생성한 Bastion Host 용 Security Group 을 선택하세요.
- ③ 해당 **Security Group 상세** 화면의 **규칙** 탭에서 **규칙 추가** 버튼을 클릭하세요. **규칙 추가** 팝업창이 열립니다.
- ④ **규칙 추가** 팝업창에서 해당 트래픽 관련 필수 정보를 입력하고, **확인** 버튼을 클릭하세요.

화면	필수 입력 요소 항목	입력 값
규칙 추가 #1	방향	Inbound 규칙
	대상주소	사용자 PC 공인 IP
	프로토콜	TCP
	허용포트	RDP(3389)

화면	필수 입력 요소 항목	입력 값
규칙 추가 #2	방향	Inbound 규칙
	대상주소	Bastion Host IP (192.168.xx.a)
	프로토콜	TCP
	허용포트	직접입력(2866)

화면	필수 입력 요소 항목	입력 값
규칙 추가 #3	방향	Outbound 규칙
	대상주소	Database 서버 IP (192.168.yy.b)
	프로토콜	TCP
	허용포트	직접입력(2866)

11. IGW Firewall 규칙 추가하기

- ⑤ **Networking > Firewall** 메뉴에서 **자원관리** 버튼을 클릭하세요. **Firewall 목록** 화면으로 이동합니다.
- ⑥ **Firewall 목록** 화면에서 미리 생성한 Internet Gateway 의 Firewall 을 선택하세요.

- ⑦ Firewall 상세 화면의 규칙 탭에서 규칙 추가 버튼을 클릭하세요. 규칙 추가 팝업창이 열립니다.
- ⑧ 규칙 추가 팝업창에서 해당 트래픽 관련 필수 정보를 입력하고, 확인 버튼을 클릭하세요.

화면	필수 입력 요소 항목	입력 값
규칙 추가 #1	출발지 IP	사용자 PC 공인 IP
	목적지 IP	Bastion Host IP (192.168.xx.a)
	프로토콜	TCP
	허용포트	RDP(3389)
	동작	Allow
	방향	Inbound

### Bastion Host 접속하기

#### 12. RDP Password 조회하기

- ① Compute > Virtual Server > Virtual Server 메뉴에서 자원관리 버튼을 클릭하세요. Virtual Server- Virtual Server 목록 화면으로 이동합니다.
- ② Virtual Server-Virtual Server 목록 화면에서 미리 생성한 Bastion Host (Virtual Server)를 선택하세요.
- ③ Virtual Server- Virtual Server 상세 화면의 상세정보 탭에서 서버 Key pair 의 RDP Password 조회 버튼을 클릭하세요. RDP Password 조회 팝업창이 열립니다.
- ④ RDP Password 조회 팝업창에서 다운로드한 Private key(\*.pem 파일 형식)를 등록하고, ID 와 Password 를 확인하세요.

#### 13. 원격 데스크톱 연결하기

- ① Windows 환경에서 "원격 데스크톱 연결"을 실행한 후, 미리 생성한 Bastion Host 의 NAT IP 를 입력하고 연결 버튼을 클릭하세요.
- ② 원격 데스크톱 연결에 성공하면 사용자 자격 증명 입력창이 열립니다. 계정과 비밀번호를 입력하고, 확인 버튼을 클릭하세요.

#### 14. Bastion Host 내 Database 접속 툴(pgadmin) 설치하기

- ① 사용자 PC 에서 Database 접속 툴인 pgadmin 프로그램을 다운로드 하세요.
  - 다운로드 경로: <https://www.pgadmin.org/download/pgadmin-4-windows/>
- ② Bastion host로 해당 파일을 업로드하기 위해 사용자 PC의 하드 드라이브를 연결하세요.

“원격 데스크톱 연결”의 로컬 리소스 탭에서 로컬 장치 및 리소스 항목의 자세히 버튼을 클릭하세요. “드라이브”에 파일을 다운로드 받은 위치의 로컬 디스크를 선택하고 확인 버튼을 클릭하세요.

- ③ 다운로드 받은 파일을 복사하여 Bastion Host 에 업로드하고, pgadmin 설치 파일을 클릭하여 설치하세요.

15. pgadmin 을 활용하여 Database 접속하기

- ① pgadmin 프로그램을 실행하여 설정할 Master password 를 입력하고, **Add New Server** 버튼을 클릭하세요.
- ② **General** 탭과 **Connection** 탭에 기존에 생성한 Database 서버 정보를 입력하고, **Save** 버튼을 클릭하세요.

화면	필수 입력 요소 항목	입력 값
General 탭	Name	postgreDB
	Host name/address	Database 서버 IP
Connection 탭	Port	2866
	Maintenance database	생성한 Database명
	Password	생성한 Database 비밀번호

- ③ pgadmin 브라우저 상에 생성된 데이터베이스 명을 클릭하여 접속을 수행하세요. 접속 후에 간단한 Query 등을 수행해 볼 수 있습니다.

**정리하기**

- SCP 에서 PostgreSQL(DBaaS)를 접속 및 운영하기 위해서는 pgadmin 과 같은 DB 접속 툴이 반드시 필요합니다.
  - pgadmin 관련한 자세한 정보는 공식사이트(<https://www.pgadmin.org/>)를 참고하세요.
- Bastion host 는 인터넷 연결이 가능한 Public Subnet 으로 구성해야 하며, Database 는 반드시 Private Subnet 에서 구성해야 합니다.
- Security Group 의 기본 정책은 Deny All 입니다.
  - Security Group 의 경우 클라우드 자원 생성 시 적용한 자원의 IP 에 적용되는 정책이므로 허용하고자 하는 IP 만 등록하면 됩니다.

- Virtual Server 별, 또는 Database 별 작은 단위로 동일한 보안 규칙을 공유하는 그룹끼리만 Security Group 을 적용하는 것이 정밀한 접근제어 및 관리에 좋습니다.
- In/Outbound All Open(Any IP, Any Port) 정책은 클라우드 자원을 외부의 위협에 그대로 노출시킬 수 있습니다. 가능하면 필요한 IP 와 포트를 특정하여 정책을 설정할 필요가 있습니다.

## 연관 콘텐츠