


보안 설정

 보안 설정 정보를 정리하는 페이지입니다.

OS 보안

로컬 전용 바인딩

기본적으로 Debian/Ubuntu 패키지는 `listen_addresses = 'localhost'` 로 설정되어 외부 접속이 차단됩니다.

경로:

- 메인 설정: `/etc/postgresql/16/main/postgresql.conf`
- 인증 설정: `/etc/postgresql/16/main/pg_hba.conf`

확인:

```
1 sudo grep -E "^#?listen_addresses|^#?port" /etc/postgresql/16/main/postgresql.conf
2 sudo systemctl restart postgresql
3
4
```

2단계에서 WAS/QnA 서버 IP만 화이트리스트 허용하도록
`listen_addresses/UFW/pg_hba.conf`를 업데이트합니다.

외부 서버 바인딩

설정 변경 (모두 sudo 필요)

- `postgresql.conf` 수정: 외부 접속 허용

```
1 sudo nano /etc/postgresql/15/main/postgresql.conf
2 # 수정
3 listen_addresses = '*'
4
5
```

- `pg_hba.conf` 수정: 서비스 서버 IP 허용

```
1 sudo nano /etc/postgresql/15/main/pg_hba.conf
2 # 추가
3 host      all             all             3.37.57.105/32      md5
4
```

• DB 재시작

```
1 sudo systemctl restart postgresql
2
3
```

최소권한 계정 예시(SQL)

```
1 -- postgres OS 계정으로: sudo -u postgres psql
2 CREATE USER svc_app WITH LOGIN PASSWORD 'IOT_was_123!@#';
3 CREATE USER svc_qna WITH LOGIN PASSWORD 'IOT_qna_123!@#';
4 CREATE USER svc_dev WITH LOGIN PASSWORD 'IOT_dev_123!@#';
5
6 -- 데이터베이스 접속 권한
7 GRANT CONNECT ON DATABASE iot_care TO svc_app, svc_qna, svc_dev;
8
9 -- 스키마 권한 (예: public 사용 시)
10 \c iotcare;
11 GRANT USAGE ON SCHEMA public TO svc_app, svc_qna, svc_dev;
12
13 -- 예: 앱은 쓰기/읽기, QnA는 읽기 전용
14 GRANT SELECT, INSERT, UPDATE ON ALL TABLES IN SCHEMA public TO svc_app, svc_dev;
15 GRANT SELECT ON ALL TABLES IN SCHEMA public TO svc_qna;
16
17 -- 앞으로 생성될 테이블에 대한 기본 권한도 설정(중요)
18 ALTER DEFAULT PRIVILEGES IN SCHEMA public
19 GRANT SELECT, INSERT, UPDATE ON TABLES TO svc_app, svc_dev;;
20
21 ALTER DEFAULT PRIVILEGES IN SCHEMA public
22 GRANT SELECT ON TABLES TO svc_qna;
23
24
```

연결 테스트

A. WAS/QnA 서버에서 psql

```
1 # 클라이언트 설치
2 sudo apt -y install postgresql-client-16
3
4 # 접속 테스트
5 # WAS Server
6 psql 'host=ec2-52-79-78-247.ap-northeast-2.compute.amazonaws.com port=5432 dbname=iot_care
  user=svc_app password=IOT_was_123!@#!'
7
8 # QnA Server
9 psql 'host=ec2-52-79-78-247.ap-northeast-2.compute.amazonaws.com port=5432 dbname=iot_care
  user=svc_qna password=IOT_qna_123!@#!'
10
11 # 또는
12 PGPASSWORD=Strong_App_Pw! psql -h <DB서버_IP> -p 5432 -U svc_app -d iotcare -c "SELECT
  now();"

```

