

# GUARDiA ITSM

## 개방망(Open Network) 구현 가이드

v2.0.0 | 2026-05-30 | (주)지오정보기술

서버: 101.79.17.164 | AI 기반 레거시 인프라 자율 운영 플랫폼

### 목 차

| 순서 | 섹션      | 페이지 |
|----|---------|-----|
| 1  | 개요 및 배경 | 2   |
| 2  | 아키텍처    | 2   |
| 3  | 구현 내용   | 3   |
| 4  | 설치 및 설정 | 4   |
| 5  | API 사용법 | 5   |
| 6  | 보안 설정   | 6   |
| 7  | 테스트 결과  | 7   |
| 8  | 운영 절차   | 7   |

# 1. 개요 및 배경

GUARDiA ITSM은 기본적으로 폐쇄망(Closed Network) 환경에서 운영됩니다. 그러나 외부 메신저(카카오톡, 네이버웹스, Slack)와의 연동, 공공기관 포털 연계, 재택/원격 관리 등의 요구사항이 증가함에 따라 개방망 지원 기능을 추가하였습니다.

## 1-1. 폐쇄망 vs 개방망 비교

| 항목            | 폐쇄망 (기본)         | 개방망 (이 가이드)      |
|---------------|------------------|------------------|
| 접근 범위         | 내부망 only         | 인터넷 외부 접근 허용     |
| CORS 정책       | localhost 만 허용   | 지정 외부 도메인 허용     |
| HTTPS         | 선택               | 필수 (TLS 1.2/1.3) |
| API 인증        | JWT              | JWT + API Key    |
| 외부 AI 호출      | 금지 (Ollama only) | 금지 유지 (변경 불가)    |
| Rate Limiting | 기본               | 강화 (30 req/min)  |
| 보안 헤더         | 기본               | HSTS 포함 강화       |

핵심 원칙 유지: 개방망 모드에서도 Ollama(LLM)는 내부 전용 유지. 외부 AI API(OpenAI, Anthropic 등) 절대 사용 금지.

# 2. 개방망 아키텍처

## 2-1. 시스템 구성도

외부 클라이언트는 Nginx를 통해 TLS 암호화된 채널로 GUARDiA API에 접근합니다. LLM(Ollama)과 데이터베이스(PostgreSQL)는 외부 직접 접근이 불가하며, API 서버를 통해서만 간접 이용 가능합니다.

| 구성 요소                  | 역할                         | 외부 접근           |
|------------------------|----------------------------|-----------------|
| Nginx (443, 8443)      | TLS 종료 + Rate Limit + 보안헤더 | 허용              |
| GUARDiA FastAPI (8001) | 비즈니스 로직 + CORS + 보안 미들웨어   | Nginx 통해서만      |
| PostgreSQL (5432)      | 데이터 저장                     | 금지 (127.0.0.1만) |
| Ollama LLM (11434)     | 온프레미스 AI 추론                | 금지 (127.0.0.1만) |

## 2-2. 포트 구성

| 포트   | 프로토콜  | 서비스                 | 외부 접근   |
|------|-------|---------------------|---------|
| 80   | HTTP  | 홈페이지 (HTTPS 리다이렉트)  | 허용      |
| 443  | HTTPS | 홈페이지 SSL            | 허용      |
| 8001 | HTTP  | GUARDiA API (내부 직접) | 권장하지 않음 |

|       |       |                        |    |
|-------|-------|------------------------|----|
| 8443  | HTTPS | GUARDiA API (외부 접근 권장) | 허용 |
| 5432  | TCP   | PostgreSQL             | 차단 |
| 11434 | HTTP  | Ollama LLM             | 차단 |

## 3. 구현 내용

### 3-1. 신규 추가 파일

| 파일                        | 내용                                    |
|---------------------------|---------------------------------------|
| core/external_security.py | API Key 생성/검증/감사 유틸리티                 |
| routers/external_api.py   | 외부 API 라우터 (헬스체크, SR, 웹훅, API Key 관리) |
| .env.open                 | 개방망 운영 환경변수 템플릿                       |
| deploy/nginx_opennet.py   | Nginx HTTPS 설정 배포 스크립트                |

### 3-2. 수정된 파일

| 파일        | 변경 내용   |
|-----------|---|
| main.py   | CORS 환경변수 기반 동적 설정, 보안 헤더 미들웨어, external_api 라우터 등록 |
| models.py | APIKey ORM 모델 추가 (tb_api_key 테이블)                   |

### 3-3. 개방망 모드 CORS 동작 방식

환경변수 GUARDIA\_NETWORK\_MODE에 따라 CORS 정책이 자동 전환됩니다:

- closed (기본): localhost만 허용
- open: GUARDIA\_ALLOWED\_ORIGINS에 지정된 외부 도메인도 허용
- 정규식 패턴 허용으로 서브도메인 일괄 허용 가능

## 4. 설치 및 설정

### 4-1. .env 개방망 설정

다음 환경변수를 /opt/guardia/app/.env 에 설정합니다:

| 환경변수                    | 값 예시                       | 설명               |
|-------------------------|----------------------------|------------------|
| GUARDIA_NETWORK_MODE    | open                       | 개방망 모드 활성화       |
| GUARDIA_ALLOWED_ORIGINS | https://itsm.zioinfo.co.kr | 허용 외부 출처         |
| GUARDIA_WEBHOOK_SECRET  | <강력한 랜덤 값>                 | 웹훅 HMAC 서명 키     |
| DATABASE_URL            | postgresql+asyncpg://...   | @ 포함 시 %40으로 인코딩 |

### 4-2. SSL 인증서

도메인이 있는 경우 Let's Encrypt 인증서 사용을 권장합니다. IP만 있는 경우 자체 서명 인증서를 생성합니다.

```
■■■ ■■: certbot --nginx -d itsm.zioinfo.co.kr
```

```
IP ■■: openssl req -x509 -nodes -days 3650 -newkey rsa:2048 ...
```

## 5. 외부 API 사용법

### 5-1. API 엔드포인트 목록

| 엔드포인트                   | 메서드    | 인증              | 설명           |
|-------------------------|--------|-----------------|--------------|
| /api/external/health    | GET    | 없음              | 헬스체크         |
| /api/external/status    | GET    | 없음              | 시스템 공개 상태    |
| /api/external/keys      | POST   | JWT (관리자)       | API Key 발급   |
| /api/external/keys/{id} | DELETE | JWT (관리자)       | API Key 비활성화 |
| /api/external/sr        | GET    | API Key (read)  | SR 목록 조회     |
| /api/external/sr        | POST   | API Key (write) | SR 등록        |
| /api/external/webhook   | POST   | HMAC (선택)       | 외부 메신저 웹훅    |
| /docs                   | GET    | 없음              | OpenAPI 문서   |

### 5-2. API Key 권한 스코프

| 스코프     | 허용 API       | 사용 예시          |
|---------|--------------|----------------|
| read    | SR 목록 조회     | 모니터링 시스템       |
| write   | SR 등록, 상태 변경 | 외부 티켓 시스템      |
| admin   | 모든 외부 API    | 통합 관리 도구       |
| webhook | 웹훅 수신        | 카카오휴크, Slack 봇 |

### 5-3. 외부 메신저 웹훅 연동 구조

외부 메신저(카카오휴크, 네이버웍스, Slack 등)는 GUARDiA 웹훅 엔드포인트로 자연어 명령을 전송합니다. GUARDiA는 Ollama LLM으로 명령을 파싱하여 처리합니다.

| 메신저    | 웹훅 URL                     | 인증 방식                      |
|--------|----------------------------|----------------------------|
| 카카오휴크  | POST /api/external/webhook | X-GUARDiA-Signature (HMAC) |
| 네이버웍스  | POST /api/external/webhook | X-GUARDiA-Signature (HMAC) |
| Slack  | POST /api/external/webhook | X-Source: slack            |
| Teams  | POST /api/external/webhook | X-Source: teams            |
| 사용자 정의 | POST /api/external/webhook | 선택 (HMAC 권장)               |

## 6. 보안 설정

### 6-1. 적용된 보안 헤더

| 헤더                        | 값                                   | 효과              |
|---------------------------|-------------------------------------|-----------------|
| Strict-Transport-Security | max-age=31536000; includeSubDomains | 브라우저가 HTTPS만 사용 |
| X-Frame-Options           | DENY                                | Clickjacking 방지 |
| X-Content-Type-Options    | nosniff                             | MIME 스니핑 방지     |
| X-XSS-Protection          | 1; mode=block                       | XSS 차단          |
| Referrer-Policy           | strict-origin-when-cross-origin     | Referrer 정보 제한  |

## 6-2. 변경 불가 보안 정책

개방망 모드에서도 다음 핵심 보안 정책은 절대 변경 불가합니다:

| 정책              | 내용   |
|-----------------|--|
| 외부 LLM 금지       | Ollama(localhost) 전용. OpenAI/Claude 등 외부 API 완전 금지 |
| SSH 자격증명 보호     | IP, 비밀번호, SSH 계정을 API 응답에 절대 포함 금지                 |
| AES-256-GCM 암호화 | 서버 자격증명은 암호화 저장 (os_pw_enc 컬럼)                     |
| root SSH 금지     | opsagent 전용 계정만 사용                                 |
| 감사 로그           | 모든 외부 API 호출 TB_AUDIT_LOG에 기록                      |

## 7. 테스트 결과

테스트 환경: Ubuntu 24.04, GUARDiA 2.0.0, Nginx 1.24 | 2026-05-30

| #   | 테스트 항목            | 기대값              | 실제값         | 결과   |
|-----|-------------------|------------------|-------------|------|
| T1  | HTTP 헬스체크 (8001)  | 200 OK           | 200 OK      | PASS |
| T2  | HTTPS 헬스체크 (8443) | 200 OK           | 200 OK      | PASS |
| T3  | 홈페이지 HTTPS (443)  | 200 OK           | 200 OK      | PASS |
| T4  | 미인증 API 접근 차단     | 401              | 401         | PASS |
| T5  | CORS 외부 출처 허용     | Allow-Origin 헤더  | 헤더 포함       | PASS |
| T6  | HSTS 헤더 적용        | max-age=31536000 | 적용됨         | PASS |
| T7  | X-Frame-Options   | DENY             | DENY        | PASS |
| T8  | Rate Limiting 설정  | zone 설정 확인       | 1개 zone     | PASS |
| T9  | 공개 시스템 상태         | operational      | operational | PASS |
| T10 | 개방망 모드 활성화        | open             | open        | PASS |

전체 10개 테스트 모두 통과 (10/10 PASS)

## 8. 운영 절차

### 8-1. 모드 전환 명령

| 작업         | 명령어   |
|------------|---|
| 폐쇄망→개방망    | echo GUARDIA_NETWORK_MODE=open >> .env && systemctl restart guardia                       |
| 개방망→폐쇄망    | sed -i 's/open/closed/' .env && systemctl restart guardia                                 |
| HTTPS 활성화  | ln -sf sites-available/guardia-https sites-enabled/ && nginx -t && systemctl reload nginx |
| HTTPS 비활성화 | rm sites-enabled/guardia-https && systemctl reload nginx                                  |

### 8-2. 서비스 접속 정보

| 서비스                | URL                                      | 용도             |
|--------------------|--|----------------|
| GUARDiA ITSM HTTP  | http://101.79.17.164:8001                | 내부망 직접 접근      |
| GUARDiA ITSM HTTPS | https://101.79.17.164:8443               | 개방망 외부 접근 (권장) |
| 외부 API             | https://101.79.17.164:8443/api/external/ | API Key 인증     |
| OpenAPI 문서         | https://101.79.17.164:8443/docs          | API 명세서 (공개)   |
| 홈페이지 HTTPS         | https://101.79.17.164                    | 지오정보기술 홈페이지    |