

# gem-oracle-server

## 시스템 구성 · 기능 · 파일 명세서

Oracle Cloud · Ubuntu 22.04 LTS · ARM aarch64

|     |                                 |
|-----|---------------------------------|
| 작성일 | 2026-08-31                      |
| 호스트 | gem-oracle-server (138.2.12.80) |
| 리전  | ap-tokyo-1 / Always Free        |
| 가동  | 8주 4일 연속 무중단                    |
| 구성  | PM2 7종 · 도메인 6개 · DB 3개         |
| 보안  | 자격증명 값 마스킹 처리                   |

## 1. 시스템 개요

오라클 클라우드 Always Free 인스턴스 1대가 전체 시스템의 허브 역할을 한다. 항상 켜져 있는 유일한 노드로서 외부 요청을 받고, 집안 PC 2대(HP·그램)로 역방향 터널을 통해 명령을 전달하며, 외부 API를 중계한다.

### 하드웨어 · OS

|           |                                    |
|-----------|------------------------------------|
| 호스트명      | gem-oracle-server                  |
| 공인 IP     | 138.2.12.80 (ap-tokyo-1)           |
| OS        | Ubuntu 22.04.5 LTS                 |
| 커널        | 6.8.0-1049-oracle                  |
| 아키텍처      | aarch64 (ARM · Ampere A1)          |
| CPU / RAM | 2 OCPU / 12GB (사용 742MB · 여유 10GB) |
| 디스크       | 194GB 중 9.4GB 사용 (5%) · 여유 185GB   |
| 연속가동      | 8주 4일 22시간 — 무중단                   |

※ Always Free 한도는 계정 전체 합산 200GB(부트+블록). 현재 부트볼륨이 200GB 전부를 점유하고 있어, 두 번째 인스턴스 생성 시 스토리지·컴퓨터 모두 과금 대상이 된다.

## 2. 가동 서비스 (PM2 7종)

PM2가 모든 Node.js 프로세스를 관리한다. 프로세스 사망 시 자동 복구되며 각각 독립 포트를 점유한다.

| 프로세스             | 포트   | 실행 파일                  | 역할                   |
|------------------|------|------------------------|----------------------|
| mes              | 3000 | mes/server.js          | MES 본체 · 실운영         |
| lbe              | 3001 | lbe/live.js            | LBEditor · 파일 통제실    |
| gem-mcp          | 3002 | gem-mcp/server.js      | MCP 서버 · Claude 연결구  |
| download         | 3003 | download_server.js     | 파일 다운로드 서버           |
| smarththings     | 3004 | smarththings_server.js | SmartThings OAuth·제어 |
| stock            | 3030 | stock/stock.js         | 주식 시세 수집             |
| security-monitor | -    | security/monitor.js    | SSH 침입 감시·알림         |

### 프로세스별 상세

- mes (3000) — 제조실행시스템 본체. PostgreSQL MYDB 연동. 재시작 31회(최다), 메모리 81MB. 외부 미공개이며 HP·그램에서 터널로만 접근.
- lbe (3001) — LBEditor. MES 전 파일의 읽기·쓰기·패치를 담당하는 종합 통제실. 파일 수술의 관문.
- gem-mcp (3002) — Claude가 이 서버에 명령을 내리는 유일한 입구. 127.0.0.1에만 바인딩되어 Nginx를 통해서만 접근 가능. lbe\_exe·srv\_pg\_execute 등 20개 도구 제공.
- download (3003) — download.shium.org 백엔드. /files/ 인라인 서빙, /list 는 403 차단.
- smarththings (3004) — OAuth 토큰 발급·자동갱신·기기 제어 중계. /devices 는 13개 기기를 병렬 조회하여 약 400ms에 응답.
- stock (3030) — 주식 시세 수집기. 26일 연속 가동.
- security-monitor — SSH 로그인 실패 감시. 상태를 state.json에 기록. 27일 연속 가동.

## 3. 도메인 · 네트워크

### 도메인 매핑 (전 도메인 HTTPS)

| 도메인                    | 프록시 대상         | 용도     | 인증서 만료     |
|------------------------|----------------|--------|------------|
| mes.shium.org          | 127.0.0.1:3002 | MCP 입구 | 2026-09-30 |
| sys.shium.org          | 127.0.0.1:3002 | MCP 보조 | 2026-11-01 |
| download.shium.org     | 127.0.0.1:3003 | 파일 배포  | 2026-11-27 |
| smarththings.shium.org | 127.0.0.1:3004 | 홈 자동화  | 2026-11-28 |
| hp.shium.org           | 게이트 제어         | HP 원격  | 2026-11-01 |
| gram.shium.org         | 게이트 제어         | 그램 원격  | 2026-11-09 |

※ mes.shium.org 인증서가 30일 내 만료(2026-09-30). certbot 자동갱신 동작 확인 권장.

※ kakao.shium.org 인증서 잔존. 서버·Nginx 설정은 제거됐으므로 인증서만 정리 대상.

### 포트 맵

| 포트                     | 구분    | 설명                                      |
|------------------------|-------|-----------------------------------------|
| 80 / 443               | Nginx | HTTP · HTTPS 전체 진입점                     |
| 3000~3030              | 앱     | MES·LBE·MCP·download·smarththings·stock |
| 5432                   | DB    | PostgreSQL (127.0.0.1 전용)               |
| 50022                  | SSH   | 오라클 SSH 입구 (기본 22 아님)                   |
| 12225                  | 터널    | HP SSH                                  |
| 13005                  | 터널    | HP DB 직통                                |
| 14005                  | 터널    | HP MCP                                  |
| 15005                  | 터널    | HP MES                                  |
| 12224/13004/14004/1500 | 터널    | 그램 4종 (현재 미연결)                          |

터널 구조: 집 안 PC가 오라클로 SSH 역방향 터널을 연다. 따라서 오라클은 공인 IP 없는 집 PC를 127.0.0.1의 특정 포트로 접근할 수 있다. PC가 꺼지면 해당 포트가 사라진다.

#### 4. 데이터베이스

| DB       | 크기     | 내용                                                    |
|----------|--------|-------------------------------------------------------|
| SYSDB    | 14 MB  | gem_boot·gem_work_log·gem_coding_rule·gem_chat 등 운영두뇌 |
| MYDB     | 13 MB  | MES 업무 데이터 (오라클 로컬본)                                  |
| postgres | 7.6 MB | 시스템 기본 DB                                             |

##### SYSDB 주요 테이블 역할

- gem\_boot — 세션 시작 시 읽는 L0 ROM. 채널·원칙·사이클 기준표의 단일 정보.
- gem\_work\_log — 작업 로그 (L1). NEXT·ERROR·EVAL·BOOKMARK를 task\_type으로 구분.
- gem\_coding\_rule — 코딩 규칙 (L4). DEV\_QMS\_STANDARD 검사표준서 등.
- gem\_chat — Claude ↔ Claude Code 간 대화방.

#### 5. 홈 디렉토리 구조

##### 디렉토리

| 경로          | 크기   | 역할                               |
|-------------|------|----------------------------------|
| mes/        | 231M | MES 본체 + metadata (인증키·boot 로컬본) |
| lbe/        | 257M | LBEditor 본체                      |
| gem-mcp/    | 28M  | MCP 서버 · Claude 접속 관문            |
| lib/        | 701M | 공용 라이브러리 (최대 용량)                 |
| oci_venv/   | 689M | OCI CLI Python 가상환경              |
| _dbbackup/  | 129M | pg_dump 일별 덤프 (8일분 보관)           |
| _bk/        | 8.4M | file_patch 자동 백업 (BK_ 접두)        |
| downloads/  | 8.5M | download.shium.org 공개 파일         |
| shiumdrive/ | 2.0M | Claude 전용 저장소 (ref·notes·tools)  |
| security/   | 1.6M | SSH 침입 감시 모듈                     |
| stock/      | 16K  | 주식 시세 수집                         |
| research/   | 400K | 연구 자료                            |
| bin/        | 16K  | OCI CLI 실행 바이너리                  |

##### 루트 파일

| 파일                     | 크기   | 기능                           |
|------------------------|------|------------------------------|
| smarththings_server.js | 6.8K | SmartThings OAuth·웹훅·기기제어 서버 |
| sysdb_mirror.js        | 4.5K | SYSDB 미러링                    |
| download_server.js     | 2.4K | 파일 다운로드 서버                   |
| db_backup.sh           | 1.1K | 매일 18시 pg_dump 백업            |
| gram_gate.sh           | 974B | 그램 도메인 게이트 개폐                |
| hp_gate.sh             | 970B | HP 도메인 게이트 개폐                |

state.json

122B

security-monitor 상태 저장

## 6. 자동화 (crontab)

| 스케줄      | 작업                                             |
|----------|------------------------------------------------|
| 매일 18:00 | db_backup.sh — SYSDB·MYDB pg_dump 백업           |
| 매일 03:00 | smarththings.shium.org/refresh — OAuth 토큰 자동갱신 |
| 5분마다     | gem_tunnel_watch.js — 터널 상태 감시·자동 복구           |

### DB 백업 상세

- 경로: /home/ubuntu/\_dbbackup/YYYYMMDD/
- 형식: pg\_dump -Fc (커스텀 압축 포맷)
- 대상: SYSDB, MYDB 2중
- 로그: \_dbbackup/backup.log 에 성공·실패 및 용량 기록
- 현재 8일분 보관 중 (총 129MB)

### SmartThings 토큰 자동갱신

- PAT (24시간 만료) 방식을 2026-08-30 폐기하고 OAuth-In SmartApp 체계로 전환.
- access\_token 24시간 · refresh\_token 30일. 매일 03시 갱신 시 refresh\_token도 함께 재발급되어 사실상 무기한 유지.
- 갱신 이력은 shiumdrive/ref/st\_refresh.log 에 누적.

## 7. 보안 설정

|            |                              |
|------------|------------------------------|
| SSH 포트     | 50022 (기본 22 미사용)            |
| SSH 인증     | 공개키 전용 · 비밀번호 로그인 차단         |
| fail2ban   | sshd + nginx-http-auth 2중 감시 |
| iptables   | INPUT ACCEPT 규칙 13건          |
| PostgreSQL | 127.0.0.1 바인딩 — 외부 직접 접근 불가  |
| gem-mcp    | 127.0.0.1 바인딩 — Nginx 경유만 허용 |
| /list      | 403 차단 (파일 목록 노출 방지)         |

### 게이트 방식 (hp / gram)

HP·그램 도메인은 평소 닫혀 있다. 호출 시 Nginx 설정을 열림 버전으로 교체하고 at 명령으로 지정 시간 뒤 자동 닫힘을 예약한다. 기본 120분

- 열기: hp\_gate.sh open 120 → 120분 후 자동 close
- 닫기: hp\_gate.sh close / 상태: hp\_gate.sh status
- 실행 후 nginx reload 반영까지 약 3초 대기 필요

## 8. 자격증명 인벤토리

아래 항목의 실제 키 값은 본 문서에 포함하지 않는다. 값은 서버 내 해당 경로에서만 확인 가능하다.

| 용도              | 저장 경로 (shiumdrive/ref/)  | 상태        |
|-----------------|--------------------------|-----------|
| SmartThings 토큰  | smarththings_token.json  | 자동갱신 · 정상 |
| SmartThings 앱자격 | smarththings_oauth.txt   | 정상        |
| SmartThings PAT | smarththings.txt         | 폐기 대상     |
| 네이버 API HUB     | naver_api.txt            | 정상        |
| 카카오 REST API    | kakao_api.txt            | 정상        |
| YouTube Data v3 | youtube_api.txt          | 정상        |
| Google Gemini   | gemini_key.txt           | 정상        |
| fal.ai          | fal_api.txt              | 정상        |
| 공공데이터포털         | data_go_kr_api.txt       | 과거이력 한정   |
| 한국투자증권          | kis_token.txt / 기타업무.txt | 만료 확인 필요  |
| 그램 SSH 키        | gram_mcp_key (+.pub)     | 정상        |
| HP 웹 인증         | hp_basicauth.txt         | 정상        |
| HP MAC (WOL)    | hp_mac.txt               | 정상        |

OCI 서명키·SSH 키는 mes/metadata/ 하위에 별도 보관. 해당 디렉토리는 삭제 금지 — gem-mcp가 참조한다.

9. 외부 API 연동 현황

| 서비스             | 가능한 작업                          |
|-----------------|---------------------------------|
| SmartThings     | 기기 13대 조회·제어 · TV 채널 · 로봇청소기 출동 |
| 네이버 API HUB     | 뉴스·블로그·카페·지역·웹문서 검색             |
| 카카오             | 장소 검색 · 주소↔좌표 변환 · 다음 검색        |
| YouTube Data v3 | 영상 검색 · 채널 조회                   |
| Gemini          | 텍스트 생성 · 유튜브 영상 직접 요약           |
| fal.ai          | FLUX 이미지 · Seedance 영상 생성       |
| OCI CLI         | 인스턴스·스냅샷·비용·네트워크 조회             |

전용 도구

- shiumdrive/tools/yt\_summary.js — Gemini fileData 방식으로 유튜브 영상을 자막 없이 직접 분석·요약. 오라클 단독 동작.
- bin/oci — OCI CLI v3.91.0. 인스턴스·볼륨·비용 조회에 사용.

10. 점검 항목

주의 필요

- mes.shium.org 인증서 30일 내 만료 — certbot 자동갱신 동작 확인
- kakao.shium.org 인증서 잔존 — 서버 제거됨, 인증서 정리 대상
- 부트볼륨 200GB가 Always Free 한도 전부 점유 — 인스턴스 증설 시 과금
- smarthings.txt(구 PAT) 폐기 대상 — OAuth 전환 완료
- KIS 토큰 만료 여부 미확인

양호

- PM2 7종 전부 online · 8주 연속 무중단
- DB 백업 8일분 정상 누적
- SSH 실패 로그 0건 · fail2ban 차단 IP 0건
- 디스크 사용률 5% · 메모리 여유 10GB
- SmartThings 토큰 자동갱신 정상 작동