

문서 관리 정보

- 소속: AI Infra실 (AI Infra Department)
- 문서 버전: v0.10.5
- 최종 수정일: 2026년 7월 24일
- 대상: 시스템 관리자, DevOps/Infra 엔지니어, 보안 담당자

Postra는 단일 바이너리 배포부터 K8s 기반 다중 노드 고가용성(HA) 아키텍처까지 확장 가능하도록 Hexagonal Architecture 포트-어댑터 패턴으로 구성되어 있습니다.

```
+-----+
|                                     cmd/postr/main.go                                     |
| - CLI Subcommands / Single-binary Serve Entrypoint / Graceful Shutdown                |
+-----+
|                                     |
+-----+
|                                     internal/application                               |
| - App Core / sync.go / accounts.go / rules.go / auth.go / oidc.go / incidents.go      |
+-----+
|                                     |
+-----+
| internal/adapters | internal/adapters | internal/adapters |
| /secretstore     | /objectstore     | /persistence     |
| - LocalStore     | - LocalStore     | - SQLite3 (WAL)  |
| - DBStore        | - DBStore        | internal/adapters |
| - Envelope AES   | - Encrypted      | /pgstore         |
+-----+          +-----+          | - PostgreSQL    |
|                                     |                                     | - pgvector       |
|                                     |                                     +-----+
```

- `cmd/posra` : 서버커맨드 (`init` , `serve` , `mcp` , `account` , `secret` , `sync` , `search` 등) 핸들러 및 SIGTERM/SIGINT 수거 루틴
- `internal/application` : 비즈니스 유스케이스 코어 (`App` , `Sync` , `Account` , `Rule` , `Auth` , `OIDC` , `Incident`)

- `internal/domain` : 도메인 엔티티 정의 (`Message` , `MailAccount` , `SecretHandle` , `Incident` , `Job`)
- `internal/adapters/secretstore` : AES-256-GCM Envelope 암호화 레코드 스토어 (`LocalStore` , `DBStore`)
- `internal/adapters/objectstore` : 메일 원문 MIME 및 첨부파일 암호화 객체 스토어 (`LocalStore` , `DBObjectStore` , `EncryptedStore`)
- `internal/adapters/persistence` : SQLite3 데이터베이스 어댑터 (WAL 모드, FK 활성화)
- `internal/adapters/pgstore` : PostgreSQL + pgvector 인덱스 지원 어댑터
- `internal/adapters/mailparse` : RFC822/MIME 디코더 및 `bluemonday` HTML Safe 세니타이저
- `internal/adapters/malware` : ClamAV 및 YARA 연동 첨부파일 보안 검사 엔진
- `internal/transport/httpapi` : REST API 핸들러 (`/api/...`) 및 API 토큰 인증 미들웨어
- `internal/transport/webui` : HTML 템플릿 웹 인터페이스 (`/ui/...`)
- `internal/transport/mcpserver` : Model Context Protocol SSE 및 Streamable HTTP 서비스 (`/mcp`)

2. 배포 및 환경변수 완벽 레퍼런스 (Environment Configuration)

Postra는 설정 파일(`config.json`) 또는 환경변수(`POSTRA_*`)를 통해 동작을 정밀하게 제어합니다.

2.1 전체 환경변수 레퍼런스 표

환경변수명	기본값	설명
POSTRA_HTTP_ADDR	127.0.0.1:8480	REST API, Web UI, MCP 통합 HTTP 바인딩 주소
POSTRA_DATA_DIR	./data	DB, 원문/첨부 객체, KEK 파일 저장 루트 디렉터리
POSTRA_STORAGE_DRIVER	sqlite	데이터베이스 드라이버 (<code>sqlite</code> 또는 <code>postgres</code>)
POSTRA_DATABASE_URL	-	PostgreSQL 접속 DSN (<code>postgres://user:pass@host:5432/db?sslmode=disable</code>)
POSTRA_SECRET_STORE_DRIVER	local	비밀값 저장소 드라이버 (<code>local</code> 파일 또는 <code>db</code>)
POSTRA_OBJECT_STORE_DRIVER	local	객체 저장소 드라이버 (<code>local</code> 파일 또는 <code>db</code>)
POSTRA_KEK	-	Base64 인코딩 32-Byte 마스터 KEK 키 (외부 주입 권장)
POSTRA_ALLOW_INSECURE_MAIL	false	평문 POP3/SMTP 허용 여부 (<code>true</code> 시 개발/테스트 용 허용)
POSTRA_BOOTSTRAP_ADMIN_PASSWORD	-	시스템 최초 시작 시 생성될 어드민 비밀번호
POSTRA_API_TOKEN	-	외부 HTTP 접근 시 헤더 인증 토큰 (<code>Authorization: Bearer</code>)
POSTRA_WORKER_ENABLED	true	백그라운드 리더 선출, 스케줄러, 동기화 워커 활성화 여부
POSTRA_AUTO_SYNC_MINUTES	5	메일 자동 수집 수신 주기 (분 단위, <code>0</code> 지정 시 비활성화)
POSTRA_OIDC_ENABLED	false	OIDC/OAuth2 SSO 연동 활성화 여부
POSTRA_OIDC_ISSUER	-	OIDC Provider Issuer URL (예: <code>https://auth.company.com/realms/main</code>)
POSTRA_OIDC_CLIENT_ID	-	OIDC Client ID
POSTRA_OIDC_CLIENT_SECRET_REF	-	암호화 SecretStore에 등록된 OIDC Client Secret 참조 키
POSTRA_VECTOR_STORE_DRIVER	db	의미론적 벡터 검색 드라이버 (<code>db</code> 또는 <code>milvus</code>)
POSTRA_OPENAI_API_KEY_REF	-	AI 임베딩 생성용 OpenAI 호환 API Key 비밀값 참조 키

3. 어드민 계정 및 SSO 관리 (Identity & Authentication)

3.1 어드민 계정 역등성 초기화 (EnsureUser)

Postrа 기동 시 `bootstrapAdmin` 프로세스가 실행되어 어드민 계정(`admin@postra.local`)을 검증합니다.

- **SQLite** 쿼리: `INSERT INTO users ... ON CONFLICT(login_id) DO UPDATE SET ...`
- **PostgreSQL** 쿼리: `INSERT INTO users ... ON CONFLICT (login_id) DO UPDATE SET ...`
- `SQLSTATE 23505 (users_pkey)` 중복 키 에러가 발생하지 않도록 역등성(Idempotency)이 완벽히 보장됩니다.

3.2 OIDC / OAuth2 SSO 설정 절차

1. SecretStore에 OIDC Client Secret을 안전하게 저장합니다:

```
postra secret set --type oidc_client_secret --label "Keycloak SSO Client Secret"
# 출력을 통해 시크릿 참조 키(예: sec_a1b2c3d4) 확인
```

2. 환경변수 설정 후 서버를 실행합니다:

```
export POSTRA_OIDC_ENABLED=true
export POSTRA_OIDC_ISSUER="https://auth.company.com/realms/postrа"
export POSTRA_OIDC_CLIENT_ID="postra-client"
export POSTRA_OIDC_CLIENT_SECRET_REF="sec_a1b2c3d4"
./postra serve
```

4. Envelope Encryption & SecretStore 구조

Postrа는 사내 민감 데이터 보호를 위해 2중 봉투 암호화 메커니즘을 적용합니다.

```
+-----+
| POSTRA_KEK (Master 32-Byte Key) |
+-----+
      |
      | Encrypts / Decrypts
      v
+-----+
| Envelope Structure (crypto.Envelope) |
| - KeyVersion: 1                       |
| - EncryptedDEK: Base64(AES-GCM-KW(DEK)) |
| - Ciphertext:   Base64(AES-GCM-Payload(Data, AAD)) |
+-----+
```

4.1 SecretStore 암호화 레코드 스키마 (secrets.enc.json / db_secrets)

```
{
  "sec_8f9a2b1c": {
    "envelope": {
      "key_version": 1,
      "nonce": "...",
      "encrypted_dek": "...",
      "ciphertext": "..."
    },
    "owner": "admin",
    "type": "mail_password",
    "label": "업무 메일 수신 암호",
    "version": 1,
    "revoked": false
  }
}
```

4.2 KEK 로테이션 및 Self-Healing

- 비밀값 로테이션 (CLI):

```
postra secret rotate --ref sec_8f9a2b1c
```

- 자가 치유 (Self-Healing): KEK 변경 또는 파드 교체로 secret_acquire 에러 발생 시, Web UI 계정 편집 페이지에서 비밀번호를 다시 입력하고 저장하면 최신 KEK로 자동 재암호화 및 등록이 완료됩니다.

5. ObjectStore 백엔드 및 저장 구조 (Object Storage)

Postras는 메일 원문(RFC822 MIME) 및 첨부파일을 두 가지 어댑터 방식으로 관리합니다.

5.1 LocalObjectStore (파일 시스템 기반)

- 경로: \$POSTRA_DATA_DIR/objects/{raw|att}/xx/yyyy...
- 파일명: SHA-256 해시값 기반의 2자 서브디렉터리 분할 저장

5.2 DBObjectStore (데이터베이스 기반)

- 테이블: object_blobs
- 스키마 DDL (PostgreSQL 기준):

```
CREATE TABLE IF NOT EXISTS object_blobs (
    bucket VARCHAR(64) NOT NULL,
    object_key VARCHAR(255) NOT NULL,
    content_type VARCHAR(128) NOT NULL,
    size_bytes BIGINT NOT NULL,
    data BYTEA NOT NULL,
    created_at BIGINT NOT NULL,
    PRIMARY KEY (bucket, object_key)
);
```

6. 장애 모니터링 및 이벤트 파이프라인 (Incidents & Observability)

Postr v0.10.0+는 장애 및 시스템 이벤트 추적 파이프라인을 지원합니다.

6.1 대시보드 및 REST API

- 대시보드: `http://:8480/ui/admin/incidents`
- REST API: `GET /api/incidents?severity=error&limit=50`
- JSON 응답 구조:

```
[
  {
    "id": "inc_99a8b7c6",
    "severity": "warning",
    "category": "sync_interrupted",
    "title": "POP3 Sync Interrupted",
    "detail": "Connection reset by peer during retrieve",
    "created_at": 1774345200
  }
]
```

6.2 Prometheus 메트릭 수집 (`/metrics`)

- `postra_sync_total{status="succeeded|failed"}` : 동기화 처리 건수
- `postra_messages_fetched_total` : 수집된 신규 이메일 수
- `postra_outbox_pending_messages` : 발송 대기 큐 크기
- `postra_attachment_blocked_total` : 악성 첨부파일 차단 횟수

7. 전체 릴리즈 이력 (Release History: v0.1.0 ~ v0.10.5)

버전	릴리즈 일자	기술 세부 구현 및 변경사항
v0.1.0	2026-07-18	MVP 최초 배포: POP3/SMTP 수발신 코어, CLI, Stdio MCP 서버, REST API 기초
v0.2.0	2026-07-18	CGO-Free 정적 링크 바이너리 및 scratch 기반 Docker 샌드박스 이미지 빌더 구축
v0.3.0	2026-07-18	IMAP 수신 어댑터 추가, Prometheus /metrics 프로비저닝, 초기 Web UI 반영
v0.3.1	2026-07-18	/healthz Liveness/Readiness 헬스 체크, 검색 결과 커서 페이지네이션 구현
v0.4.0	2026-07-23	3단 반응형 Web UI 개편 및 bluemonday 보안 HTML 세니타이저 연동
v0.4.1	2026-07-23	REST, Web UI, Streamable HTTP MCP 서비스를 8480 단일 TCP 포트로 통합 바인딩
v0.5.0	2026-07-23	References / In-Reply-To RFC822 헤더 기반 대화 스레드 자동 추적 및 그룹핑
v0.5.1	2026-07-23	자동 수신 규칙 엔진 (RuleEngine) 구현 (삭제, 라벨링, Snooze, 중요 표시)
v0.5.2	2026-07-23	ClamAV / YARA 룰 기반 첨부파일 악성 코드 실시간 검사 및 차단 로깅
v0.6.0	2026-07-23	수신 소켓 타임아웃 옵션 및 대용량 메일 수집 DB 커밋 배치 성능 최적화
v0.7.0	2026-07-23	PostgreSQL DSN 연동(POSTRA_STORAGE_DRIVER=postgres), 수집 실시간 UI 인디케이터
v0.8.0	2026-07-24	MCP RBAC 권한 제어, IMAP IDLE 수신, RRF 하이브리드 검색 및 Milvus 벡터 DB 연동
v0.8.1	2026-07-24	로고/파비콘 에셋 정적 라우팅 및 Web UI 브랜드 스타일링 반영
v0.8.2	2026-07-24	어드민 재시작 시 users_pkey 중복 충돌(SQLSTATE 23505) 수정 (EnsureUser 역등성 보장)
v0.8.3	2026-07-24	수신 워커 예외 복구(defer recover()) 및 KEK 변경 시 SecretStore 자가 치유(Self-Healing)
v0.8.4	2026-07-24	메일 파싱 객체 참조 해제 및 수집 루프 메모리 가비지 컬렉션(GC) 튜닝

버전	릴리즈 일자	기술 세부 구현 및 변경사항
v0.8.5	2026-07-24	리더 선출 DB 지연 시 활성 작업 오검출 방지 (<code>RecoverStaleJobsExcept</code> 방어)
v0.9.0	2026-07-24	루프 내 <code>FreeOSMemory()</code> 제거로 OS 스레드 급사 차단, DB 암호화 <code>SecretStore(DBStore)</code> 추가
v0.9.1	2026-07-24	메일 원문 및 첨부파일 BLOB을 DB에 암호화 보관하는 <code>DBObjectStore</code> 어댑터 구현
v0.9.2	2026-07-24	<code>db_test.go</code> 자동화 테스트 구축 및 SIGTERM 수신 시 안전한 워커 Graceful Shutdown
v0.10.0	2026-07-24	장애 대시보드(<code>/ui/admin/incidents</code>) 및 장애 트래킹 REST API(<code>/api/incidents</code>) 도입
v0.10.1	2026-07-24	백그라운드 스케줄러, IDLE, 임베딩 작업 전체 2중 예외 복구 적용으로 크래시 완벽 차단
v0.10.2	2026-07-24	메모리 이상 수신 원인을 Audit Log 및 Incident에 자동 수집하는 파이프라인 탑재
v0.10.3	2026-07-24	OIDC SSO 로그인 시 기존 부트스트랩 어드민 계정과 매핑 처리 및 세션 검증 강화
v0.10.4	2026-07-24	OIDC 실패 원인 상세 표출 및 CSRF 공격 방어 하드닝
v0.10.5	2026-07-24	메일 본문 뷰어 가독성 폰트, 블루문데이 세니타이징 CSS 스타일 디자인 고도화

AI Infra실 — Postra 이메일 플랫폼 관리자 가이드 v0.10.5