

Vendra

관리자 가이드

설치 · 설정 · 계정과 권한 · 운영 · 장애 대응 · 보안

버전	v0.7.49
작성일	2026-09-11
문서	관리자 가이드

Vendra 관리자 가이드

- 대상: 시스템 관리자, DevOps·보안 담당자, 구매 시스템 운영 책임자
- 기준 버전: v0.7.49
- 관련 문서: [사용자 가이드](#) · [운영 문서](#) · [보안 문서](#) · [아키텍처](#) · [README](#)

화면을 쓰는 방법은 [사용자 가이드](#)에 있습니다. 이 문서는 그 화면을 띄워 놓고 지키는 쪽의 일 — 설치·설정·계정·운영·장애 대응·보안 — 만 다룹니다. 실린 화면은 모두 v0.7.49 를 실제로 띄워 1440x900 에서 찍은 것이며, 등장하는 회사·사람·주소는 지어낸 데모 데이터입니다.

1. 구성 요소

구성 요소	무엇	필수
vendra 컨테이너	React UI, REST/OpenAPI API, MCP 서버, 시간 기반 백그라운드 작업을 한 프로세스가 제공	필수
PostgreSQL 15 이상	모든 업무 데이터·설정·세션·감사로그. 스키마 마이그레이션은 기동 시 자동	필수
vendra_documents 볼륨	업로드된 문서의 실체. 기본 경로 <code>/var/lib/vendra/documents</code>	필수
Keycloak 등 OIDC 공급자	SSO. 쓰지 않으면 로컬 계정만으로 동작	선택
OpenAI 호환 모델 엔드포인트	AI Analyst 와 계약 분석	선택

Redis·Kafka·Elasticsearch 같은 별도 미들웨어는 쓰지 않습니다. 런타임은 외부 인터넷 연결 없이 동작합니다 — AI 를 켜 경우에만 관리자가 지정한 모델 엔드포인트로 나갑니다.

주고받는 것:

방향	상대	프로토콜	비고
안으로	사용자 브라우저, MCP 클라이언트	HTTP :8080	앞에 TLS 중단 프록시를 두세요
밖으로	PostgreSQL	PGSTGRES_DSN	운영에서는 <code>sslmode=require</code> 이상
밖으로	OIDC 공급자	HTTPS	Discovery + Authorization Code + PKCE
밖으로	AI 모델	HTTPS	관리자 화면에서 켤 때만
밖으로	알림 어댑터	PostgreSQL Job/Notification	관리자 화면에서 설정

2. 설치

릴리즈 자산(`vendra-v0.7.49.tar.gz`)으로 처음부터 끝까지 세우는 절차입니다. 인터넷이 없는 망에서도 같습니다.

2.1 준비

항목	값
포트	8080/tcp (컨테이너 → 호스트). PostgreSQL 은 별도
볼륨	<code>vendra_documents</code> → <code>/var/lib/vendra/documents</code>
자원	최소 1 vCPU / 512 MB. 데이터베이스는 별도 산정
사용자	컨테이너는 비-root(<code>vendra</code>)로, 루트 파일시스템은 read-only 로 실행
시간대	이미지 기본 <code>TZ=Asia/Seoul</code> . 다른 지역은 <code>-e TZ=...</code> 로 바꿉니다

PostgreSQL 데이터베이스와 전용 사용자를 먼저 만듭니다.

```
CREATE USER vendra WITH PASSWORD 'replace-with-a-long-random-password';
CREATE DATABASE vendra OWNER vendra;
```

2.2 이미지 적재와 기동

```
docker load < vendra-v0.7.49.tar.gz
cp .env.example .env
openssl rand -base64 32 # 출력값을 .env 의 ENCRYPTION_KEY 에 넣습니다
${EDITOR:-vi} .env
docker compose up -d
```

compose.yaml 은 vendra:latest 를 씁니다. 릴리즈 아카이브가 버전 태그와 함께 latest 태그도 담고 있으므로, 업그레이드할 때 compose 파일을 고칠 일이 없습니다. 특정 버전으로 고정하려면 VENDRA_IMAGE=vendra:v0.7.49 를 .env 에 넣습니다.

compose 없이 직접 띄우려면:

```
docker run -d --name vendra -p 8080:8080 \
-e POSTGRES_DSN="postgres://vendra:replace-me@postgres.internal:5432/vendra?sslmode=require" \
-e BOOTSTRAP_ADMIN="admin@example.com" \
-e BOOTSTRAP_ADMIN_PASSWORD="replace-with-a-long-random-password" \
-e ENCRYPTION_KEY="$(openssl rand -base64 32)" \
-v vendra_documents:/var/lib/vendra/documents \
--read-only --cap-drop ALL --security-opt no-new-privileges:true \
--tmpfs /tmp:size=64m,mode=1777 \
vendra:v0.7.49
```

2.3 기동 확인과 최초 관리자

```
curl -fsS http://localhost:8080/health/live # {"status":"ok"}
curl -fsS http://localhost:8080/health/ready # {"status":"ready"} — DB 까지 확인
curl -fsS http://localhost:8080/api/version # 버전 · 커밋 · 빌드 시각
```

첫 기동에서 BOOTSTRAP_ADMIN 이메일로 시스템 관리자 계정이 만들어집니다. http://<서버>:8080 에 그 이메일과 BOOTSTRAP_ADMIN_PASSWORD 로 로그인합니다.

첫 로그인 직후 할 일 두 가지:

1. **개인화 및 키 관리** → **세션 및 보안**에서 비밀번호를 바꿉니다. 환경변수의 비밀번호는 계정을 만들 때 한 번만 쓰이며, 재시작해도 기존 비밀번호를 덮어쓰지 않습니다. 따라서 바꾼 뒤에는 .env 의 값이 더 이상 유효한 자격증명이 아닙니다.
2. **서비스 관리**에서 조직·역할·사용자와 운영 정책을 설정합니다(4장·5장).

2.4 스키마 마이그레이션

마이그레이션은 기동할 때 자동으로 적용됩니다. 여러 인스턴스를 동시에 띄워도 안전하도록 잠금을 잡고 진행하므로, 롤링 업데이트 중에 중복 적용되지 않습니다. 수동으로 실행할 명령은 없습니다.

3. 설정

3.1 환경 변수 — 전수

애플리케이션이 읽는 환경 변수는 네 개뿐입니다(internal/config). 나머지 운영 설정은 전부 관리자 화면에서 저장되어 PostgreSQL 에 남습니다.

이름	기본 값	필 수	설명
POSTGRES_DSN	없음	필 수	PostgreSQL 연결 문자열. 운영에서는 sslmode=require 이상을 권장합니다. 예: postgres://vendra:…@postgres.internal:5432/vendra?sslmode=require
BOOTSTRAP_ADMIN	없음	필 수	최초 시스템 관리자 이메일. 이 주소로 계정이 없으면 첫 기동에서 만듭니다.
BOOTSTRAP_ADMIN_PASSWORD	없음	필 수	그 계정의 최초 비밀번호. 최대 72바이트(한글 1자 = 3바이트, 즉 24자)까지만 가능하며 넘으면 기동이 거부됩니다. 10자 미만이면 경고를 남기고 기동은 계속합니다. 계정 생성에만 쓰이고 기존 비밀번호를 덮어쓰지 않습니다.
ENCRYPTION_KEY	없음	필 수	Secret·계좌정보 암호화용 base64 인코딩 32바이트 키. openssl rand -base64 32 로 만듭니다. 형식이 다르면 기동이 거부됩니다.

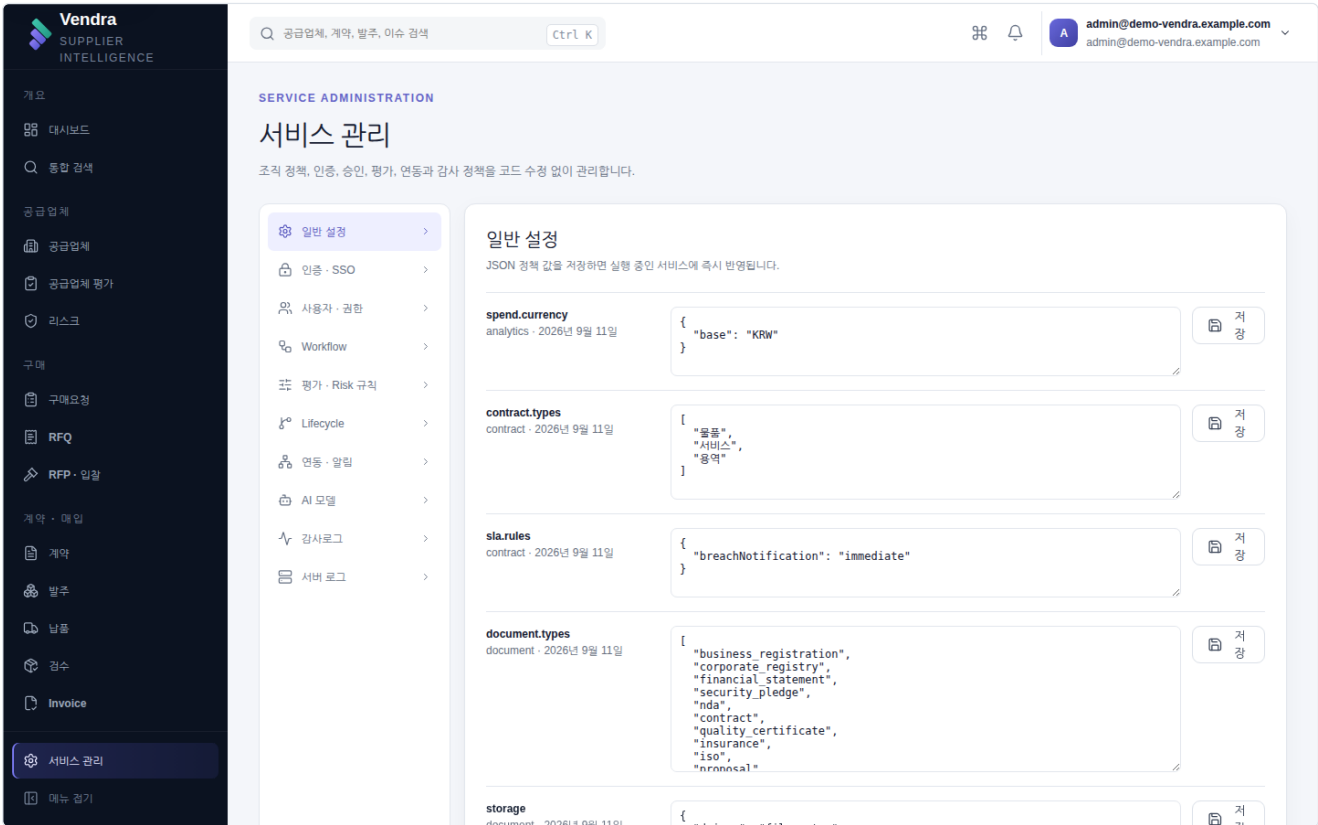
컨테이너 이미지가 함께 정하는 값:

이름	기본값	설명
TZ	Asia/Seoul	마감일· current_date 판정의 기준 시간대. 다른 지역에서는 반드시 바꿉니다.
VENDRA_IMAGE	vendra:latest	compose.yaml 이 읽는 값. 특정 버전으로 고정할 때만 씁니다(애플리케이션은 읽지 않습니다).

ENCRYPTION_KEY 는 AES-256-GCM 마스터 키입니다. Keycloak Client Secret, 공급업체 계좌정보, 개인 API 키의 비밀값이 이 키로 암호화되어 저장됩니다. 이 키를 잃으면 그 값들은 복구할 수 없습니다 — 데이터베이스 백업과 같은 수준으로, 다른 장소에 보관하세요.

3.2 운영 설정 — 서비스 관리 화면

나머지는 전부 왼쪽 메뉴 서비스 관리에서 저장하며, 저장 즉시 실행 중인 서비스에 반영됩니다.



서비스 관리 → 일반 설정 — 정책 값을 JSON 으로 직접 편집한다

왼쪽 갈래는 일반 설정 인증 · SSO 사용자 · 권한 Workflow 평가 · Risk 규칙 Lifecycle 연동 · 알림 AI 모델 감사로그 서버 로그 입니다.

배포와 함께 설치되는 설정 키:

분류	키	기본값	하는 일
general	branding	서비스명·로그인 문구	로그인 화면과 머리글에 나오는 문구
identity	oidc	enabled:false , autoCreate:true , defaultRole:business_user	OIDC 연동 (3.3)
security	security.login	maxFailures:5 , windowMinutes:15 , lockoutMinutes:15 , maxAddressFailures:25	로그인 실패 임계값과 잠금 시간
security	security.password	minLength:10 , requireClasses:0	비밀번호 정책
security	security.session	ttlHours:12 , secureCookie:false	세션 수명과 쿠키 Secure 속성
security	maintenance.retention	expiredSessionDays:7 , loginAttemptDays:30	만료 세션·로그인 시도 기록 보존 기간
workflow	workflow.approval_enabled	false	전체 승인 절차 On/Off. 꺼져 있으면 모든 상신이 즉시 승인됩니다
workflow	workflow.separation_of_duties	blockSelfApproval:false	자기 기안 건의 자기 승인 차단
supplier	supplier.grades	S≥90 / A≥80 / B≥70 / C...	평가 총점 → 등급 기준
supplier	supplier.risk_levels	LOW≥0 / MEDIUM≥25 / HIGH...	리스크 점수 → 등급 기준
supplier	supplier.registration	requireEmailVerification:true , bankChangeApproval:true , similarNameThreshold	등록 정책과 유사 업체명 판정 임계값
supplier	supplier.types / certification.types	제조·유통·서비스·용역·IT / ISO 9001 외	품의 선택지
contract	contract.types / sla.rules	물품·서비스·용역 / breachNotification:immediate	계약 유형과 SLA 위반 통보
procurement	sourcing.score_weights	price 30 / quality 20 / delivery 15 / risk 15 / technical 20	RFQ 비교 Matrix 의 가중치
procurement	procurement.categories / rfp.templates	비어 있음	품목 분류와 RFP 서식
document	storage	driver:filesystem , path:/var/lib/vendra/documents	문서 저장 위치
document	document.types	사업자등록증·법인등기부 외	문서 분류
analytics	spend.currency	base:KRW	지출 리포트의 기준 통화 표기
risk	risk.rules	continuousMonitoring:true , criticalStopReview:true	리스크 감시 정책
notification	notification.adapters	비어 있음	알림 전달 어댑터
ai	ai	enabled:false , timeoutSeconds:60	AI 모델 연결 (3.4)

승인 절차는 기본이 꺼집니다. workflow.approval_enabled 를 켜지 않으면 아무리 규칙을 세워도 모든 상신이 그 자리에서 승인 처리됩니다. Workflow 화면 맨 위의 서비스 검토 · 승인 프로세스 토크가 이 값입니다.

3.3 OIDC (Keycloak) 연동

서비스 관리 → 인증 · SSO 에서 Issuer, Client ID, Client Secret 세 가지만 넣으면 Discovery 로 나머지를 가져옵니다. Authorization Code + PKCE(S256)를 씁니다.

Keycloak(또는 다른 공급자)에 등록할 Valid Redirect URI:

```
https://vendra.internal/api/auth/oidc/callback
```

- 이 경로는 /api/v1 아래가 아닙니다. /api/v1/... 로 등록하면 SSO 를 마치고 돌아온 사용자가 세션 인증 마들웨어에 걸려 401 로그인에 필요합니다 를 받습니다 → 방금 로그인한 사람에게 가장 헛갈리는 응답입니다.
- 서비스 관리에서 공개 URL 을 설정하면 서버가 <공개 URL>/api/auth/oidc/callback 을 authorization 요청과 token 교환 양쪽에 같은 문자열로 씁니다. 비워 두면 요청에서 유추하므로, 프록시와 원본처럼 이름이 둘 이상인 배포에서는 redirect_uri_mismatch 가 날 수 있습니다.
- autoCreate 가 켜져 있으면 처음 로그인한 사용자에게 defaultRole (기본 business_user) 역할로 계정을 만듭니다. 고면 미리 만들어 둔 계정만 들어옵니다.
- Client Secret 은 ENCRYPTION_KEY 로 암호화되어 저장되며 화면에 다시 표시되지 않습니다.

3.4 AI 모델 연결

서비스 관리 → AI 모델 에서 OpenAI 호환 엔드포인트의 Base URL·모델명·API 키·타임아웃 (기본 60초)을 넣고 겁니다. 그러면 AI Analyst 화면은 답하지 않습니다. 폐쇄망에 서는 사내에 띄운 호환 엔드포인트를 가리키면 됩니다.

선택한 업무 데이터만 그 엔드포인트로 나갑니다. 어디로 나가는지가 곧 데이터 반출 경로이므로, 켜기 전에 그 주소가 어디인지 확인하세요.

4. 계정과 권한

서비스 관리 → 사용자 · 권한 한 화면에 사용자 역할 · RBAC 조직 위임 · 임시 권한 네 탭이 있습니다.

The screenshot shows the Vendra Supplier Intelligence interface. The left sidebar contains navigation links for Overview, Dashboard, Search, Supplier Management, Supplier Evaluation, Risk, Procurement, RFQ, RFP, Contract Management, Contract, Invoice, and Supplier Management. The main content area is titled 'SERVICE ADMINISTRATION' and '서비스 관리'. It includes a search bar and a list of users. The 'Users' tab is selected, showing a table of users with columns for Name, Type, Role, Organization, Status, and Last Login.

사용자	유형	역할	조직	상태	최근 로그인
누리소개 배주원 portal@muri.example.com	supplier	공급업체 사용자	—	active	2026년 9월 11일
대성전자 문가은 portal@daesung.example.com	supplier	공급업체 사용자	—	active	2026년 9월 11일
한빛정밀 서지호 portal@hanbit.example.com	supplier	공급업체 사용자	—	active	2026년 9월 11일
품질담당 윤채원 quality@demo-vendra.example.com	internal	협업 담당자	품질본부	active	—
계약담당 오세진 contract@demo-vendra.example.com	internal	계약 담당자	구매본부	active	—
구매담당 강나은 buyer@demo-vendra.example.com	internal	구매 관리자	구매본부	active	—
admin@demo-vendra.example.com	internal	시스템 관리자	—	active	2026년 9월 11일

사용자 · 권한 — 계정 목록과 유형·역할·조직·상태·최근 로그인

4.1 계정

- 사용자 추가 로 이메일·이름·유형 (internal / supplier)·조직·역할·초기 비밀번호를 정합니다.
- 공급업체 계정은 supplier 유형이며 반드시 한 공급업체에 묶입니다. 그 계정은 내부 화면 대신 포털을 보고, 서버가 그 업체의 레코드만 돌려줍니다.
- 계정을 지우지 말고 비활성화하세요. 감사로그·승인 기록이 그 계정을 가리킵니다.
- 비밀번호 재설정 같은 작업은 같은 목록에서 합니다. 재설정하면 그 사용자의 다른 세션은 폐기됩니다.

4.2 역할과 권한

배포와 함께 열 개 역할이 설치됩니다.

코드	화면에 나오는 이름	기본 데이터 범위	대략의 범위
system_admin	시스템 관리자	company	* — 모든 것
procurement_manager	구매 관리자	company	공급업체·구매 전 과정·승인
contract_manager	계약 담당자	company	공급업체 조회, 계약·문서, 승인
business_user	현업 담당자	department	자기 업무 등록·조회
finance	재무 담당자	company	Invoice·지급·Spend
legal	준법·법무 담당자	company	계약 검토, 준법 리스크
security	보안 담당자	company	보안 심사·보안 리스크
auditor	감사 담당자	company	audit.read 와 전 영역 읽기
executive	경영진	company	대시보드·분석·요약 읽기
supplier_user	공급업체 사용자	own	포털(portal.*)만

권한 문자열은 <영역>.<동작> 형태이며 * 와 <영역>.* 를 씁니다(예: contract.* , *.read). 업무 유형마다 .read ,.create ,.update 와 금액을 여는 .amount.read 가 있습니다. 역할은 화면에서 새로 만들고 고칠 수 있습니다.

4.3 데이터 범위 (Data Scope)

역할마다 데이터 범위가 붙습니다. 권한이 "무엇을 할 수 있는가"라면 범위는 "어느 레코드에 대해서인가"입니다.

값	보이는 것
company	전사
division	자기 조직의 상위 묶음까지
department	자기 조직과 그 하위 조직
own	자기가 담당(소유)인 레코드

공급업체 계정은 데이터 범위와 별개로, 계정에 묶인 공급업체의 레코드만 서버가 돌려줍니다.

own 범위 계정에게는 소유자 필드가 곧 가시성입니다. 담당자가 바뀌는 조직이라면 department 를 쓰는 편이 안전합니다.

4.4 조직

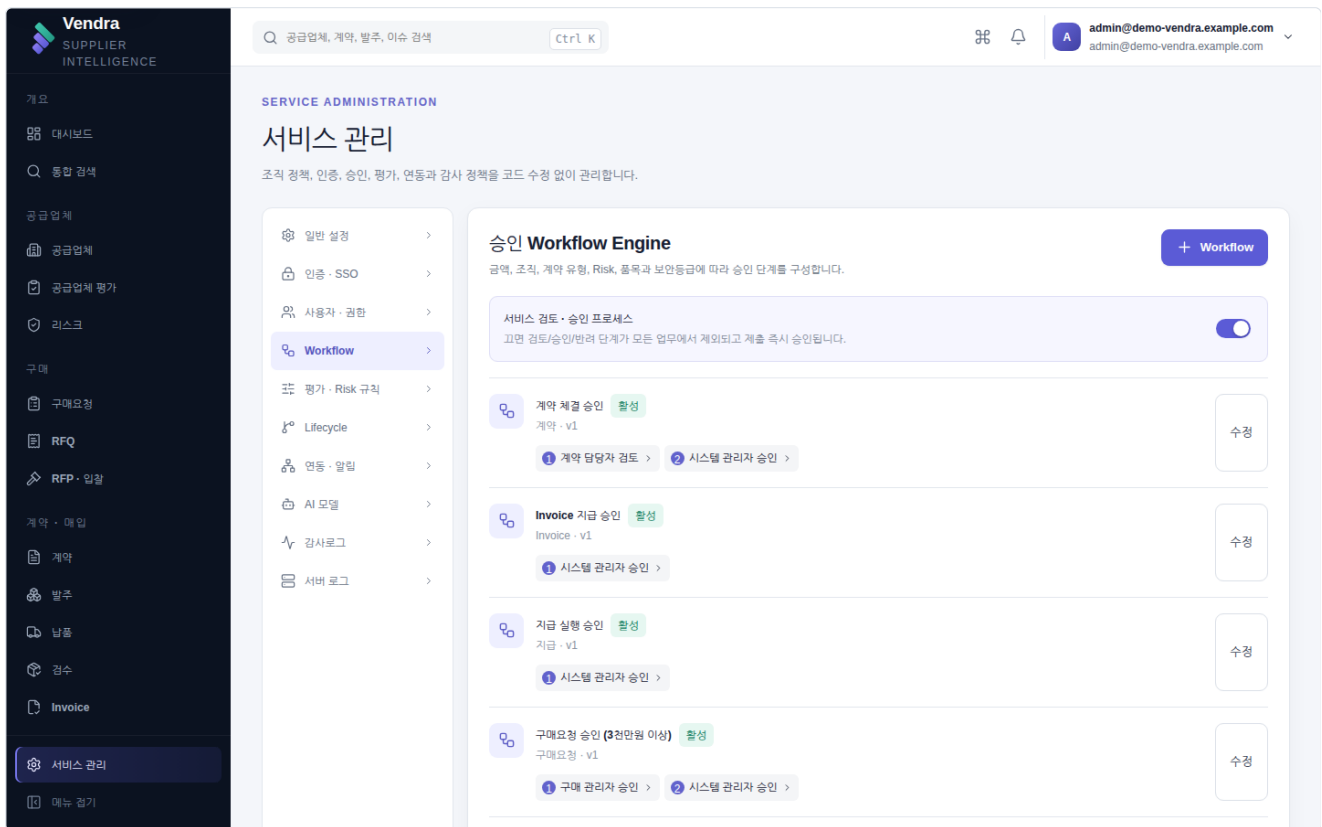
조직 탭에서 계층을 만듭니다. 조직은 데이터 범위의 단위이면서 Spend 리포트의 묶음 기준입니다. 공급업체와 업무 객체는 등록 시점의 조직에 묶입니다.

4.5 위임 · 임시 권한

휴가·대행처럼 기간이 정해진 권한을 부여합니다. 기간이 지나면 자동으로 사라지고, 부여와 회수가 모두 감사로그에 남습니다. 상시 권한을 여기로 대신하지 마세요.

4.6 승인 규칙 (Workflow)

서비스 관리 → Workflow 에서 업무 유형별로 규칙을 세웁니다.



Workflow — 대상 유형·조건·다단계 승인 규칙과 전체 On/Off 토크

- 맨 위 토크가 `workflow.approval_enabled` 입니다. **꺼져 있으면 아래 규칙은 하나도 적용되지 않습니다.**
- 규칙 하나는 **대상 유형 + 조건 + 순서가 있는 승인 단계**로 이루어집니다. 조건은 최소/최대 금액, 조직, 리스크 등급, 계약 유형, 품목 분류, 프로젝트, 보안등급입니다. 조건이 비어 있으면 그 유형의 모든 건에 걸립니다.
- 단계마다 **승인할 역할**을 지정합니다. 그 역할을 가진 계정의 내 승인함 에 나타납니다.
- 상신된 건은 위에서부터 규칙을 훑어 **처음 맞는 하나**에 걸립니다. 겹치는 규칙을 여러 개 두면 어느 것이 먼저 닿을지 화면에서 읽기 어려우니, 조건을 겹치지 않게 쓰세요.
- 이미 쓴 규칙은 **수정** 으로 이름·활성 여부·조건·단계를 고칠 수 있습니다. **대상 유형은 고칠 수 없습니다** — 잘못 지정했다면 그 규칙을 끄고 새로 만듭니다.
- 규칙에 걸리지 않은 상신은 즉시 승인됩니다. 이것이 의도인지 아닌지를 배포마다 확인하세요.

4.7 평가 · Risk 규칙

서비스 관리 → 평가 · Risk 규칙 에서 스코어카드 항목·가중치·등급 기준과 심사 서식을 정합니다.

Vendra

SUPPLIER INTELLIGENCE

개요

대시보드

통합 검색

공급 업체

공급 업체

공급 업체 평가

리스크

구매

구매요청

RFQ

RFP · 입찰

계약 · 매입

계약

발주

납품

검수

Invoice

서비스 관리

매뉴얼 보기

공급 업체, 계약, 발주, 이슈 검색

Ctrl K

admin@demo-vendra.example.com

admin@demo-vendra.example.com

SERVICE ADMINISTRATION

서비스 관리

조직 정책, 인증, 승인, 평가, 연동과 감사 정책을 코드 수정 없이 관리합니다.

일반 설정

인증 · SSO

사용자 · 권한

Workflow

평가 · Risk 규칙

Lifecycle

연동 · 알림

AI 모델

감사 로그

서버 로그

평가 · 심사 · Risk 규칙

평가 항목별 가중치, 등급 기준, 등록 심사 및 필수 문서를 동적으로 구성합니다.

성과 평가 Scorecard

기본 공급 업체 평가
periodic · 활성

가격 경쟁력

20%

품질

25%

납기

20%

서비스

10%

기술력

10%

보안

5%

재무 안정성

5%

ESG

5%

신규 공급 업체 심사

기본 공급 업체 종합 심사
활성 · 필수 문서 3종

기본 적격성

10%

신용

10%

기술

10%

개인 정보

10%

ESG

5%

재무

15%

품질

15%

보안

10%

준법

10%

공급망

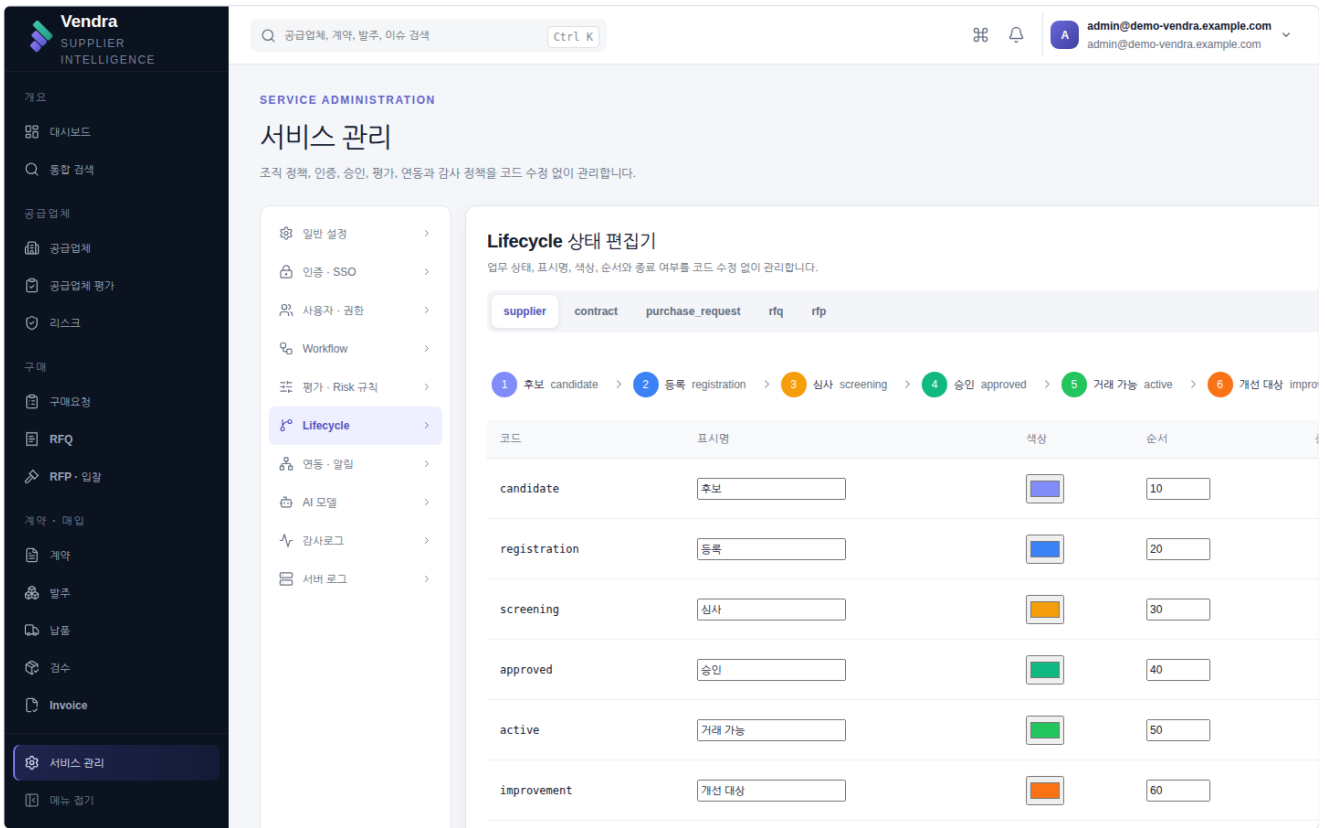
5%

평가 · Risk 규칙 — 평가 항목과 가중치, 등급 기준

- 항목의 가중치 합이 100 이 되게 맞추세요. 총점은 항목 점수 × 가중치 / 100 의 합입니다.
- 평가자가 항목을 하나라도 비우면 저장이 거부됩니다 — 비운 항목을 0점으로 채점해 실제보다 낮은 등급을 만들지 않기 위해서입니다.
- 항목을 바꿔도 이미 저장된 평가의 점수는 다시 계산되지 않습니다. 기간 중간에 항목을 같아 끼우면 앞뒤 평가가 다른 기준이 됩니다.

4.8 Lifecycle

서비스 관리 → Lifecycle 에서 업무 유형별 상태 목록(코드·이름·색·순서·종료 여부)을 정합니다.



Lifecycle — 업무 유형별 상태와 순서

승인 절차가 쓰는 `pending_approval` `approved` `rejected` `returned` 는 시스템이 소유하는 상태입니다. 여기서 만든 상태로 그 넷을 대신하지 마세요.

5. 운영

5.1 상태 점검

엔드포인트	메서드	답	쓰임
<code>/health/live</code>	GET	<code>{"status":"ok"}</code>	프로세스가 살아 있는지. liveness probe
<code>/health/ready</code>	GET	<code>{"status":"ready"}</code> / 503 <code>{"status":"not_ready"}</code>	DB 까지 닿는지. readiness probe
<code>/metrics</code>	GET	Prometheus 텍스트	아래 지표
<code>/api/version</code>	GET	버전·커밋·빌드 시각	지금 도는 것이 무엇인지

컨테이너 이미지에 `/health/ready` 를 30초마다 부르는 `HEALTHCHECK` 가 들어 있습니다.

주요 지표:

지표	보는 이유
<code>vendra_http_requests_total</code> , <code>vendra_http_request_errors_total</code>	요청량과 오류율
<code>vendra_http_request_duration_seconds</code>	응답 시간 분포
<code>vendra_http_requests_in_flight</code>	동시 처리 중인 요청
<code>vendra_login_failures_total</code> , <code>vendra_login_lockouts_total</code>	로그인 실패와 잠금 — 무차별 대입의 신호
<code>vendra_postgres_connections</code>	커넥션 풀 사용량
<code>vendra_background_passes_total</code> , <code>vendra_background_pass_failures_total</code> , <code>vendra_background_last_pass_timestamp_seconds</code>	백그라운드 작업(5.2)이 도는지
<code>vendra_build_info</code>	버전·커밋 라벨

5.2 백그라운드 작업

프로세스 안에서 1시간 간격으로 세 가지를 돕니다. 한 회차의 제한 시간은 30분입니다.

1. 알림 예약 — 기한이 다가오는 업무·만료가 가까운 계약과 문서
2. 알림 발송 — 설정된 어댑터로 전달
3. 보존 기간 정리 — 만료 세션과 오래된 로그인 시도 기록 삭제 (maintenance.retention)

`vendra_background_last_pass_timestamp_seconds` 가 한 시간 넘게 갱신되지 않으면 이 셋이 모두 멈춰 있다는 뜻입니다.

5.3 로그

- 표준 출력에 JSON 한 줄씩 나옵니다. `docker logs vendra` 로 봅니다.
- 최근 로그는 **서비스 관리** → **서버 로그**에서 화면으로도 봅니다. 레벨과 문구로 좁힐 수 있어 서버에 들어가지 않고 확인할 때 씁니다.

Vendra
SUPPLIER INTELLIGENCE

- 개요
- 대시보드**
- 통합 검색
- 공급업체
- 공급업체 평가
- 리스크
- 구매
- 구매요청
- RFP
- RFP 입찰
- 계약 · 매입
- 계약
- 발주
- 납품
- 검수
- Invoice
- 서비스 관리**
- 매뉴얼 보기

Ctrl K

SERVICE ADMINISTRATION

서비스 관리

조직 정책, 인증, 승인, 평가, 연동과 감사 정책을 코드 수정 없이 관리합니다.

- 일반 설정 >
- 인증 · SSO >
- 사용자 · 권한 >
- Workflow >
- 평가 · Risk 규칙 >
- Lifecycle >
- 연동 · 알림 >
- API 모델 >
- 감사로그 >
- 서버 로그 >**

서버 로그

현재 Vendra 프로세스의 구조화 로그를 실시간으로 확인합니다. 민감한 속성은 수집 단계에서 마스킹됩니다.

보관 중
277
최대 3,000건

INFO
277

WARN
0

ERROR
0

메시지, Request ID, 경로, 컴포넌트 검색

전체 레벨 ▾

09. 11. 00:24:22 경신

09. 11. 00:24:21	INFO	request	/api/v1/me/notifications · Request YaviMS-a7LuZfDCi	>
09. 11. 00:24:21	INFO	request	/api/v1/me · Request 7eLaRrAGRL5yc1I5	>
09. 11. 00:24:21	INFO	request	/api/version · Request ccjoRFwsi-1f4F8V	>
09. 11. 00:24:21	INFO	request	/admin/logs · Request OFGLGWNliqwMaI H	>
09. 11. 00:24:23	INFO	request	/api/v1/admin/audit · Request MrRCQtLv7bg8UffN	>
09. 11. 00:24:22	INFO	request	/api/v1/me/notifications · Request -aEPdofjqXHmoJSx	>

서버 로그 — 관리자 화면에서 최근 로그를 레벨과 문구로 좁혀 본다

- 이 화면의 로그는 메모리에 있는 최근 분량입니다. 영구 보관은 컨테이너 로그를 수집해 하세요.

5.4 감사로그

계약 체결, 계좌정보 변경, 승인·반려, 평가·권한 변경, 로그인 실패·잠금, 문서 다운로드가 행위자·IP 와 함께 남습니다.

개요

대시보드

통합 검색

공급업체

공급업체 평가

리스크

구매

구매요청

RFQ

RFP · 입찰

계약 · 매입

계약

발주

납품

검수

Invoice

서비스 관리

매뉴얼 보기

공급업체, 계약, 발주, 이슈 검색

Ctrl K

admin@demo-vendra.example.com

admin@demo-vendra.example.com

SERVICE ADMINISTRATION

서비스 관리

조직 정책, 인증, 승인, 평가, 연동과 감사 정책을 코드 수정 없이 관리합니다.

일반 설정

인증 · SSO

사용자 · 권한

Workflow

평가 · Risk 규칙

Lifecycle

연동 · 알림

AI 모델

감사로그

서버 로그

감사로그

사용자, 시간, 작업, 대상, 변경 전후 값, 선택과 Request ID를 보여줍니다.

시간	사용자	작업	대상	REQUEST ID
2026년 9월 11일	admin@demo-vendra.example.com	login	user 25fca9de-7eb3-4dff-a370-6d42b5f8da6d	NnybEcgvRU0oiswo
2026년 9월 11일	portal@nuri.example.com	submitted	sourcing_response 2cd01df9-9242-4456-b768-3c2d0e17ee8a	-dmwTvGHjqVIp6H
2026년 9월 11일	portal@nuri.example.com	login	user c5a3db5a-e19f-4880-8c59-b2ebd0e1cb1b	Pm5fInVZAB8rVpiI
2026년 9월 11일	portal@daesung.example.com	submitted	sourcing_response 10cb6fc8-41ca-4058-ba68-1935ba5e011f	BohJCP0_zbpfvvcy
2026년 9월 11일	portal@daesung.example.com	login	user 7ad47cd0-db2c-4140-94c6-89fe0d21b658	WQ122d_sY2ecXJ1z
2026년 9월 11일	portal@hanbit.example.com	submitted	sourcing_response 130d7d42-e35d-4ec5-a2d7-e8df202b6b3	x01rD_rCB1b4av-o
2026년 9월 11일	portal@hanbit.example.com	login	user a2914c45-46c4-4ec8-acda-8d510417b6e6	QZ95XTuFP8ae768p
2026년 9월 11일	admin@demo-vendra.example.com	create	user c5a3db5a-e19f-4880-8c59-b2ebd0e1cb1b	_YyVcQ0GgAqm-sLfd

내보내기

감사로그 — 행위·대상·행위자·시간

감사 담당자에게는 auditor 역할을 주세요 — 감사로그 읽기와 전 영역 읽기만 가능하고 쓰지 못합니다.

5.5 백업

들을 같은 시점으로 묶어 받아야 복구됩니다.

```
# 1) 데이터베이스
docker exec -t <postgres> pg_dump -U vendra -Fc vendra > vendra-$(date +%F).dump

# 2) 문서 볼륨
docker run --rm -v vendra_documents:/data:ro -v "$PWD":/backup alpine \
  tar czf /backup/vendra-documents-$(date +%F).tar.gz -C /data .
```

그리고 ENCRYPTION_KEY 를 이들과 다른 장소에 보관합니다. 세 가지가 다 있어야 복구가 완결됩니다 — 키가 없으면 덤프 안의 Secret·계좌정보는 열리지 않습니다.

5.6 복구

```
docker compose down

# 데이터베이스
docker exec -i <postgres> pg_restore -U vendra -d vendra --clean --if-exists < vendra-YYYY-MM-DD.dump

# 문서 볼륨
docker run --rm -v vendra_documents:/data -v "$PWD":/backup alpine \
  sh -c 'rm -rf /data/* && tar xzf /backup/vendra-documents-YYYY-MM-DD.tar.gz -C /data'

# 백업 시점과 같은 ENCRYPTION_KEY 로 기동
docker compose up -d
curl -fsS http://localhost:8080/health/ready
```

복구 뒤에는 서비스 관리 → 인증 · SSO 를 열어 Client Secret 이 살아 있는지, 공급업체 한 곳의 계좌정보가 읽히는지 확인하세요. 여기서 깨지면 ENCRYPTION_KEY 가 다른 것입니다.

5.7 업그레이드

```
# 1) 지금 도는 버전을 적어 둡니다 — 되돌릴 때 필요합니다
curl -fsS http://localhost:8080/api/version

# 2) 데이터베이스와 문서 볼륨을 백업합니다 (5.5) — 마이그레이션은 되돌아가지 않습니다

# 3) 새 이미지를 적재하고 다시 띄웁니다
docker load < vendra-v0.7.50.tar.gz
docker compose up -d

# 4) 확인
curl -fsS http://localhost:8080/health/ready
curl -fsS http://localhost:8080/api/version
```

기동 중에 스키마 마이그레이션이 자동으로 적용됩니다. 여러 인스턴스가 동시에 올라와도 안전합니다.

되돌리기: 스키마 마이그레이션은 앞으로만 갑니다. 새 버전이 만든 스키마 위에서 옛 바이너리는 동작을 보장하지 않으므로, 되돌리려면 업그레이드 직전 백업을 복원한 뒤 옛 이미지로 기동합니다.

```
docker compose down
# 5.6 절차로 업그레이드 직전 덤프와 문서 볼륨을 복원
VENDRA_IMAGE=vendra:v0.7.49 docker compose up -d
```

되돌리기가 백업 복원을 뜻하므로, 업그레이드 직전 백업은 선택이 아니라 절차의 일부입니다.

5.8 화면 캡처 다시 만들기 (문서 관리자용)

이 문서와 사용자 가이드의 그림은 `scripts/guide-screenshots.mjs` 가 만듭니다.

```
VENDRA_GUIDE_URL=http://127.0.0.1:8080 \
VENDRA_GUIDE_ADMIN=admin@demo-vendra.example.com \
VENDRA_GUIDE_ADMIN_PASSWORD='...' \
VENDRA_GUIDE_DEMO_PASSWORD='...' \
node scripts/guide-screenshots.mjs
```

이 스크립트는 데모 데이터를 만들어 넣습니다. 버려도 되는 빈 데이터베이스를 가리키는 배포에만 올리세요. 대상 주소는 전용 변수에서만 읽고, 로컬이 아닌 호스트는 `VENDRA_GUIDE_ALLOW_REMOTE=1` 없이는 거절합니다. 전역 설정은 `workflow.approval_enabled` 하나만 잠시 켜다가 끝나면 원래 값으로 되돌립니다. 이미 데이터가 있는 배포에서는 아무것도 쓰지 않고 캡처만 합니다.

비밀번호는 둘 다 환경 변수로만 받습니다. `VENDRA_GUIDE_ADMIN_PASSWORD` 는 관리자 로그인에, `VENDRA_GUIDE_DEMO_PASSWORD` 는 스크립트가 만드는 데모 계정(내부 사용자·포털 사용자) 전부에 씁니다 — 비밀번호 정책(기본 10자 이상)을 통과하는 값이어야 합니다. 스크립트 파일에는 어떤 비밀번호도 적혀 있지 않으며, 그렇게 유지하세요.

PDF 는 공용 도구로 제공합니다.

```
node .../aidev/tools/guide/md2pdf.mjs docs/USER_GUIDE.md docs/USER_GUIDE.pdf \
--title "사용자 가이드" --subtitle "..." --project "Vendra" --version "v0.7.49"
```

6. 장애 대응

증상	확인할 곳	조치
컨테이너가 바로 죽는다	<code>docker logs vendra</code> 첫 줄 — <code>{"level":"ERROR","msg":"configuration error"}</code>	<code>POSTGRES_DSN · BOOTSTRAP_ADMIN · BOOTSTRAP_ADMIN_PASSWORD · ENCRYPTION_KEY</code> 중 빠진 것이 메시지에 적혀 있습니다. <code>ENCRYPTION_KEY</code> must be a base64-encoded 32-byte key 면 <code>openssl rand -base64 32</code> 로 다시 만듭니다. <code>BOOTSTRAP_ADMIN_PASSWORD</code> must be at most 72 bytes 면 비밀번호를 줄입니다(한 글 1자 = 3바이트).
기동은 하는데 접속이 안 된다	<code>{"msg":"database startup failed"}</code>	DSN 의 호스트·자격증명· <code>sslmode</code> 와 방화벽을 확인합니다.
<code>/health/ready</code> 가 503	<code>{"status":"not_ready"}</code> , DB 쪽 커넥션 수	PostgreSQL 이 살아 있는지, 커넥션 상한에 닿았는지 확인합니다 (<code>vendra_postgres_connections</code>).
로그인 화면에 "서비스가 재 시작 중이거나 데이터베이스에 접근할 수 없습니다" 를 받는다	<code>/health/ready</code>	위와 같습니다.
사용자가 "일시적으로 로그인 처리할 수 없습니다" 를 받는다	서버 로그의 <code>auth_unavailable</code>	세션 조화가 DB 에 닿지 못한 상태입니다. DB 를 먼저 봅니다.
특정 사용지만 로그인 못 함	감사로그의 <code>login_failed</code> / <code>login_locked</code>	잠금이면 <code>lockoutMinutes</code> 만큼 기다리거나 <code>security.login</code> 을 조정합니다. 본인이 시도한 적 없다면 무차별 대입을 의심하고 <code>vendra_login_lockouts_total</code> 을 봅니다.
SSO 후 401 로그인 이 필요합니다	OIDC 공급자의 Redirect URI 등록값	<code>/api/auth/oidc/callback</code> 으로 등록되어 있는지 확인합니다(3.3).
SSO 가 <code>redirect_uri_mismatch</code>	서비스 관리의 공개 URL	프록시 뒤라면 공개 URL 을 명시합니다.
상신했는데 즉시 승인된다	Workflow 토글, 규칙의 조건	<code>workflow.approval_enabled</code> 가 꺼져 있거나, 맞는 규칙이 없습니다(4.6).
승인함 이 비어 있다	규칙의 단계 역할, 사용자 역할	단계에 지정한 역할을 가진 계정이 있는지 확인합니다.
사용자가 "〈권한〉 권한이 필요합니다" 를 받는다	그 사용자의 역할	메시지에 적힌 권한을 역할에 더합니다.
사용자가 "데이터 접근 범위를 벗어났습니다" 를 받는다	역할의 데이터 범위, 레코드의 조직·담당자	범위를 넓히거나 레코드를 그 사람의 조직·담당으로 옮깁니다(4.3).
문서 다운로드가 실패한다	<code>storage</code> 설정의 <code>path</code> , 볼륨 마운트	볼륨이 붙어 있는지, 컨테이너 사용자가 쓸 수 있는지 확인합니다.
계좌정보·Client Secret 이 깨진다	<code>ENCRYPTION_KEY</code>	백업 시점과 다른 키로 기동한 것입니다. 원래 키로 다시 띄웁니다.
알림이 오지 않는다	<code>vendra_background_last_pass_timestamp_seconds</code> , 서버 로그의 <code>notification dispatch failed</code>	마지막 회차 시각이 한 시간 넘게 멈춰 있으면 백그라운드 루프를 봅니다(5.2).
AI Analyst 가 답하지 않는다	서비스 관리 → AI 모델	<code>enabled</code> 와 Base URL·모델명·키, 그리고 그 주소로 나가는 경로가 열려 있는지 확인합니다.

7. 보안

7.1 기본값 중 반드시 바꿔야 하는 것

항목	기본	해야 할 것
BOOTSTRAP_ADMIN_PASSWORD	.env 의 값	첫 로그인 직후 화면에서 변경. .env 의 값은 그 뒤로 유효하지 않습니다
ENCRYPTION_KEY	예시값	openssl rand -base64 32 로 배포마다 새로 생성. 예시값을 그대로 쓰지 마세요
security.session 의 secureCookie	false	HTTPS 로 서비스하면 true 로, 세션 쿠키가 평문 경로로 나가지 않게 합니다
security.password 의 minLength	10	조직 정책에 맞춰 올리고 requireClasses 를 함께 씁니다
workflow.approval_enabled	false	승인 통제가 필요하면 켜야 합니다 — 켜지 않으면 모든 상신이 자동 승인입니다
workflow.separation_of_duties	blockSelfApproval:false	자기 기안 자기 승인을 막으려면 켵니다
POSTGRES_DSN 의 sslmode	.env.example 은 require	disable 로 낮추지 마세요

7.2 외부에 열면 안 되는 것

- PostgreSQL 포트를 애플리케이션 밖으로 노출하지 마세요.
- 8080 은 평문 HTTP 입니다. TLS 종단 프록시 뒤에 두고, 프록시에서만 접근을 받습니다.
- /metrics 는 인증이 없습니다. 사내 모니터링 망에서만 달게 하세요.
- /mcp 와 /api/v1 은 인증이 걸려 있지만, 인터넷에 여는 것은 공급업체 포털을 쓰는 경우로 한정하고 프록시에서 WAF·속도 제한을 함께 두세요.

7.3 컨테이너

이미지는 비-root(vendra)로 돌고, compose 는 read_only: true · cap_drop: ALL · no-new-privileges:true 로 띄웁니다. 쓰기가 필요한 곳은 /tmp (tmpfs)와 문서 볼륨뿐입니다. 직접 docker run 할 때도 같은 옵션을 주세요(2.2).

7.4 계정·키

- 개인 API/MCP 키는 조회 전용이며 자기 권한을 넘는 범위를 담을 수 없습니다. 만료는 1~365일에서 고르게 되어 있으니 짧게 잡고 회전시키세요.
- 퇴사자 계정은 삭제가 아니라 비활성화입니다. 그 계정이 발급한 키도 함께 막으세요.
- 공급업체 포털 초대 링크는 그 자체가 자격증명입니다. 잘못 나갔으면 Supplier 360 의 포털 초대 모달에서 회수하세요. 이미 가입에 쓰인 초대는 회수되지 않으므로, 그때는 만들어진 계정을 비활성화합니다.
- 감사가 필요한 사람에게는 auditor 역할을 줍니다 — 시스템 관리자 권한을 나눠 주지 마세요.

7.5 데이터 반출 경로

밖으로 나가는 길은 셋뿐입니다. 각각을 알고 있으세요.

1. AI 모델 엔드포인트 — 컨 경우, 질의에 담긴 업무 데이터가 그 주소로 갑니다.
2. OIDC 공급자 — 인증 정보만 오갑니다.
3. 알림 어댑터 — 설정한 대상으로 알림 내용이 갑니다.

셋 다 서비스 관리에서 꺼 둘 수 있고, 꺼 두면 런타임은 외부와 통신하지 않습니다.