igame

igame 관리자 가이드

설치 · 설정 · 운영 · 보안

버전	v0.7.12
작성일	2026-09-12
문서	igame 관리자 가이드

igame 관리자 가이드

이 문서는 igame을 **설치하고 지키는 사람**을 위한 것입니다. 화면을 쓰는 방법은 사용자 가이드에 있습니다.

이 가이드의 화면은 모두 `v0.7.11` 서비스를 실제로 띄워 1440×900 데스크톱 창에서 찍은 것이며, 등장하는 이름·아이디·소속·비밀값은 전부 지어낸 예시 값입니다.

더 깊은 절차는 이미 있는 문서를 가리킵니다. 여기서는 처음부터 끝까지 한 번 세우고, 무엇을 어디서 보는지까지 다룹니다.

---

1. 구성 요소

구성 요소	형태	역할	비고
`igame`	컨테이너 1개 (`igame:v0.7.12`)	API·포털·게임 자산·MCP 엔드포인트를 모두 제공	최종 runtime은 `scratch` 기반. shell·패키지 매니저 없음
PostgreSQL	외부 서비스	사용자·설정·점수·감사 로그·게시 콘텐츠 전부	15 이상. 릴리스에 포함되지 않음
`igame-data` 볼륨	Docker named volume	컨테이너의 `/app/data`	업로드 자산을 쓰는 배포에서만 내용이 생깁니다
Keycloak	외부 서비스 (선택)	사내 SSO(OIDC)	없으면 로컬 아이디·비밀번호 로그인만 씁니다
OpenAI 호환 AI 게이트웨이	외부 서비스 (선택)	AI Game Lab	없으면 AI 메뉴 자체가 숨겨집니다
TLS 종단 프록시	외부 서비스 (권장)	HTTPS 종단, 원래 `Host` 전달	릴리스에 포함되지 않음

주고받는 것:

- 브라우저 → `igame` **8080/tcp** (HTTP). 프록시 뒤에 두는 것이 기본입니다.
- `igame` → PostgreSQL **5432/tcp**.
- `igame` → Keycloak, AI 게이트웨이 (해당 기능을 켰을 때만).
- 그 밖에 바깥으로 나가는 통신은 없습니다. Phaser를 포함한 게임 실행 자산이 전부 이미지 안에 들어 있어 브라우저가 CDN을 부르지 않습니다.

아키텍처의 배경과 설계 근거는 아키텍처를 보세요.

---

2. 설치

릴리스 자산은 `igame-vX.Y.Z.tar.gz` 하나입니다. `docker save` 한 스트림을 gzip으로 압축한 것이므로 `docker load` 후에도 이미지 이름과 태그가 그대로 유지됩니다.

지원 기준은 Linux x86-64, Docker Engine 24 이상, Compose plugin 2.20 이상, PostgreSQL 15 이상입니다. 컨테이너 호스트와 Keycloak/PostgreSQL의 시간이 맞아야 OIDC 토큰 검증이 정상 동작합니다. 반입 검사와 사설 CA 처리를 포함한 전체 절차는 오프라인 설치를 따르고, 여기서는 그대로 붙여 넣을 수 있는 최소 경로만 적습니다.

2.1 필요한 자원

항목	값
포트	컨테이너 `8080/tcp` 하나. 호스트 공개는 프록시에만 열고 외부에 직접 노출하지 않습니다
볼륨	`igame-data` → `/app/data`. 컨테이너 루트 파일시스템은 읽기 전용이고 `/tmp` 는 64 MiB tmpfs입니다
자원	2 vCPU, RAM 2 GiB에서 시작해 실제 DAU와 AI 동시 stream으로 조정
데이터베이스	전용 DB와 최소 권한 소유자. `UTF8`. 애플리케이션이 시작할 때 마이그레이션을 적용하므로 해당 DB의 스키마 변경 권한이 필요합니다

2.2 이미지 로드

```
sha256sum igame-v0.7.12.tar.gz
gzip -t igame-v0.7.12.tar.gz
gzip -dc igame-v0.7.12.tar.gz | docker load
docker image inspect igame:v0.7.12 --format '{{json .RepoTags}}'
```

2.3 환경 파일

작업 디렉터리에 버전과 일치하는 `docker-compose.yml` 을 두고 권한이 제한된 `.env` 를 만듭니다.

```
umask 077
cp .env.example .env
chmod 600 .env
```

`ENCRYPTION_KEY` 는 정확히 32바이트여야 합니다. 생성 예:

```
printf 'ENCRYPTION_KEY=base64:%s\n' "$(openssl rand -base64 32 | tr -d '\n')"
```

`.env` 에는 아래 네 줄만 둡니다. 값은 전부 예시입니다.

```
POSTGRES_DSN=postgres://igame:example-password@postgres.internal:5432/igame?sslmode=verify-full
BOOTSTRAP_ADMIN=admin
BOOTSTRAP_ADMIN_PASSWORD=example-long-random-password
ENCRYPTION_KEY=base64:ZXhhbXBsZS1rZXktZXhhbXBsZS1rZXktMzJiIQ==
```

2.4 기동과 확인

```
docker compose up -d
docker compose ps
curl --fail --max-time 5 http://127.0.0.1:8080/healthz
curl --fail --max-time 5 http://127.0.0.1:8080/readyz
bash ./scripts/smoke-test.sh http://127.0.0.1:8080
```

`/readyz` 가 `{"service":"igame","status":"ok","version":"0.7.12"}` 을 돌려주면 데이터베이스까지 붙은 것입니다.

2.5 최초 관리자 계정

`BOOTSTRAP_ADMIN` / `BOOTSTRAP_ADMIN_PASSWORD` 로 만들어진 계정이 첫 관리자입니다. 비밀번호는 12자 이상이어야 하며, 짧으면 서비스가 기동하지 않고 로그에 `configuration error` 를 남깁니다.

로그인한 뒤 **바로 다음 세 가지**를 하세요.

1. 프로필 메뉴에서 비밀번호를 바꿉니다. 본인 비밀번호를 바꾸면 다른 기기의 세션이 함께 폐기됩니다.
2. `/admin/settings` 에서 **서비스 공개 URL**을 실제 접속 주소로 채웁니다. 비어 있으면 브라우저 요청이 `csrf_rejected` 로 막히는 경우가 생깁니다.
3. 사내 SSO를 쓸 계획이면 `/admin/security` 에서 연결한 뒤, `/admin/settings` 의 **Bootstrap 관리자 로그인 사용**을 끕니다.

---

3. 설정

3.1 환경 변수

애플리케이션이 읽는 환경 변수는 이 네 개가 전부입니다. 나머지 설정은 모두 데이터베이스에 저장되며 관리자 화면에서 바꿉니다. 포트는 `8080` 으로 고정이라 환경 변수로 바꾸지 않습니다.

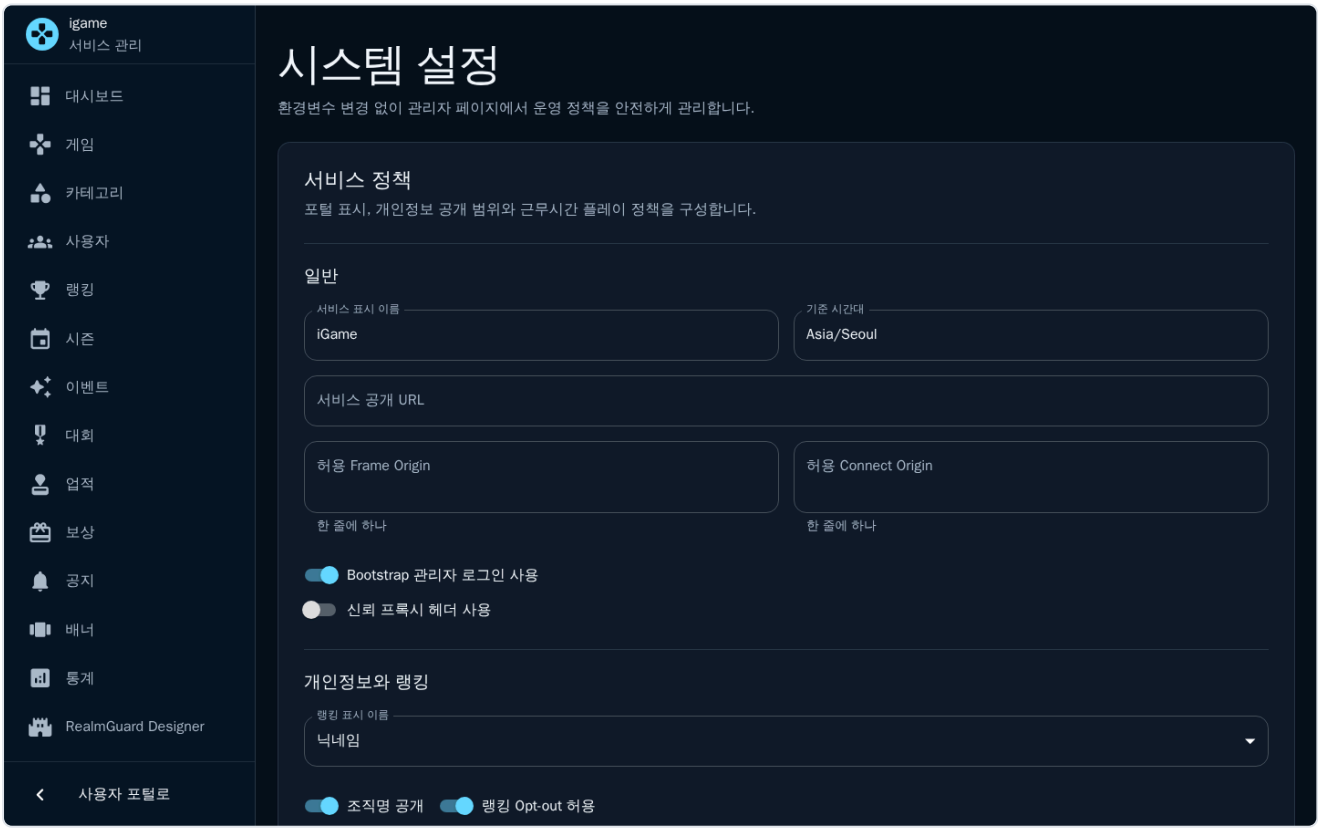
이름	기본값	필수	설명
`POSTGRES_DSN`	없음	예	PostgreSQL 연결 문자열. 운영에서는 `sslmode=verify-full` 을 씁니다
`BOOTSTRAP_ADMIN`	없음	예	최초 로컬 관리자 아이디
`BOOTSTRAP_ADMIN_PASSWORD`	없음	예	최초 로컬 관리자 비밀번호. **12자 이상**이어야 기동합니다
`ENCRYPTION_KEY`	없음	예	저장 비밀을 감싸는 마스터 키. `base64:…` · `hex:…` 또는 평문 32바이트. **정확히 32바이트로 해석되어야 합니다**

넷 중 하나라도 비어 있으면 서비스는 기동하지 않고 부족한 이름을 로그에 그대로 적습니다: `missing required environment variables: …`.

`ENCRYPTION_KEY` 를 잃어버리면 데이터베이스에 저장된 OIDC client secret과 AI API 키를 복구할 수 없습니다. 백업 파일과 **다른 곳**에 보관하세요.

3.2 관리자 화면에서 하는 설정

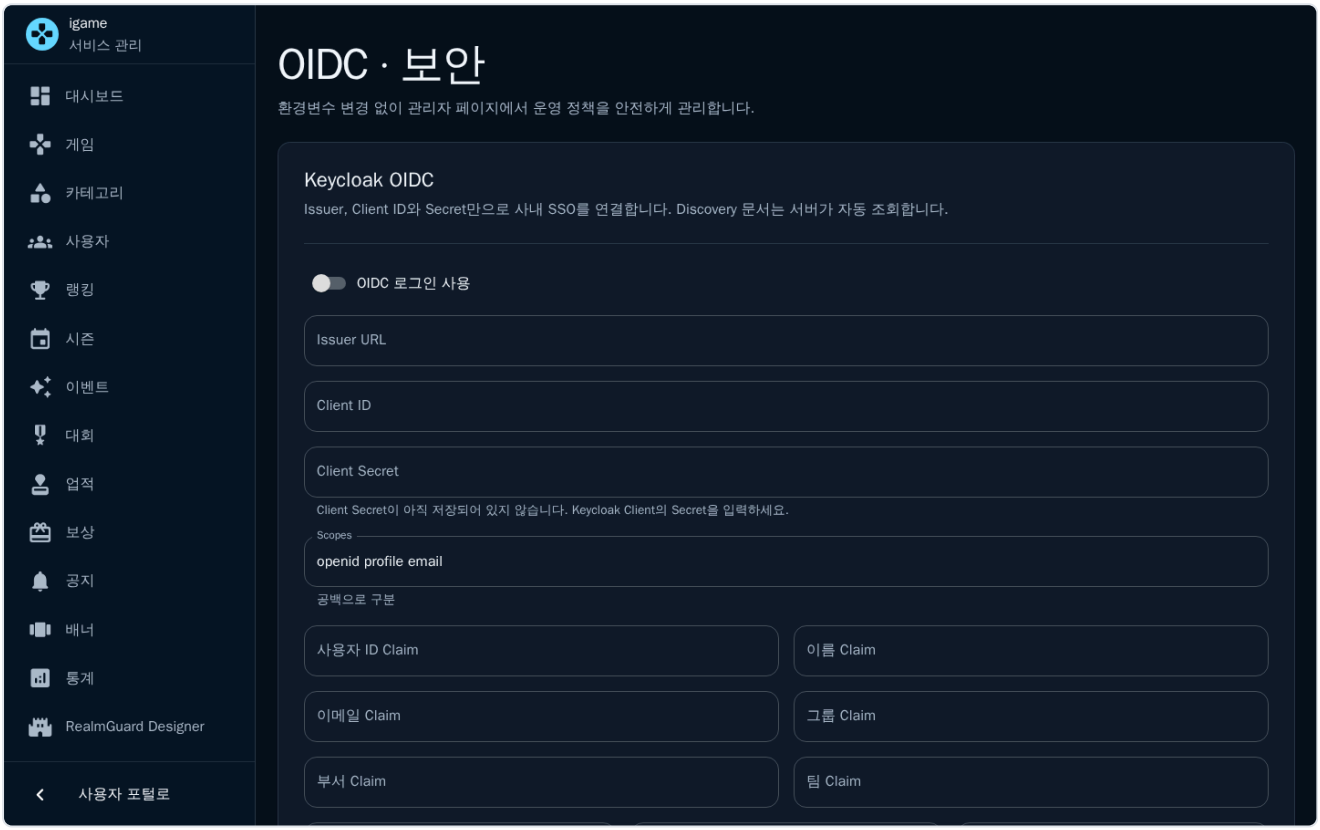
`/admin` 의 왼쪽 메뉴가 설정의 전부입니다. 요청 경로에서 읽는 설정 값은 최대 5초 동안 인스턴스 메모리에 캐시되고, 저장한 인스턴스에서는 즉시 무효화됩니다 — 저장한 화면에서는 바로, 다른 인스턴스에서는 최대 5초 뒤에 적용됩니다.



시스템 설정 — 서비스 표시명·기준 시간대·공개 URL·허용 origin과 개인정보/랭킹 정책

시스템 설정 (`/admin/settings` , 관리자 전용)

- 서비스 표시 이름, 기준 시간대(기본 `Asia/Seoul`). 플레이 허용 시간과 하루 경계가 이 시간대에서 정해집니다.
- 서비스 공개 URL, 허용 Frame Origin / 허용 Connect Origin (한 줄에 하나).
- Bootstrap 관리자 로그인 사용 — SSO를 붙였다면 끕니다.
- 신뢰 프록시 헤더 사용 — TLS를 프록시에서 끊는다면 켜고, 프록시가 원래 `Host`와 `X-Forwarded-Proto` / `X-Forwarded-Host`를 전달하게 하세요.
- 개인정보와 랭킹: 랭킹 표시 이름(닉네임/실명), 조직명 공개, 랭킹 opt-out 허용.
- 플레이 시간 정책: 허용 시간대, 일일 제한, 게임별 예외.

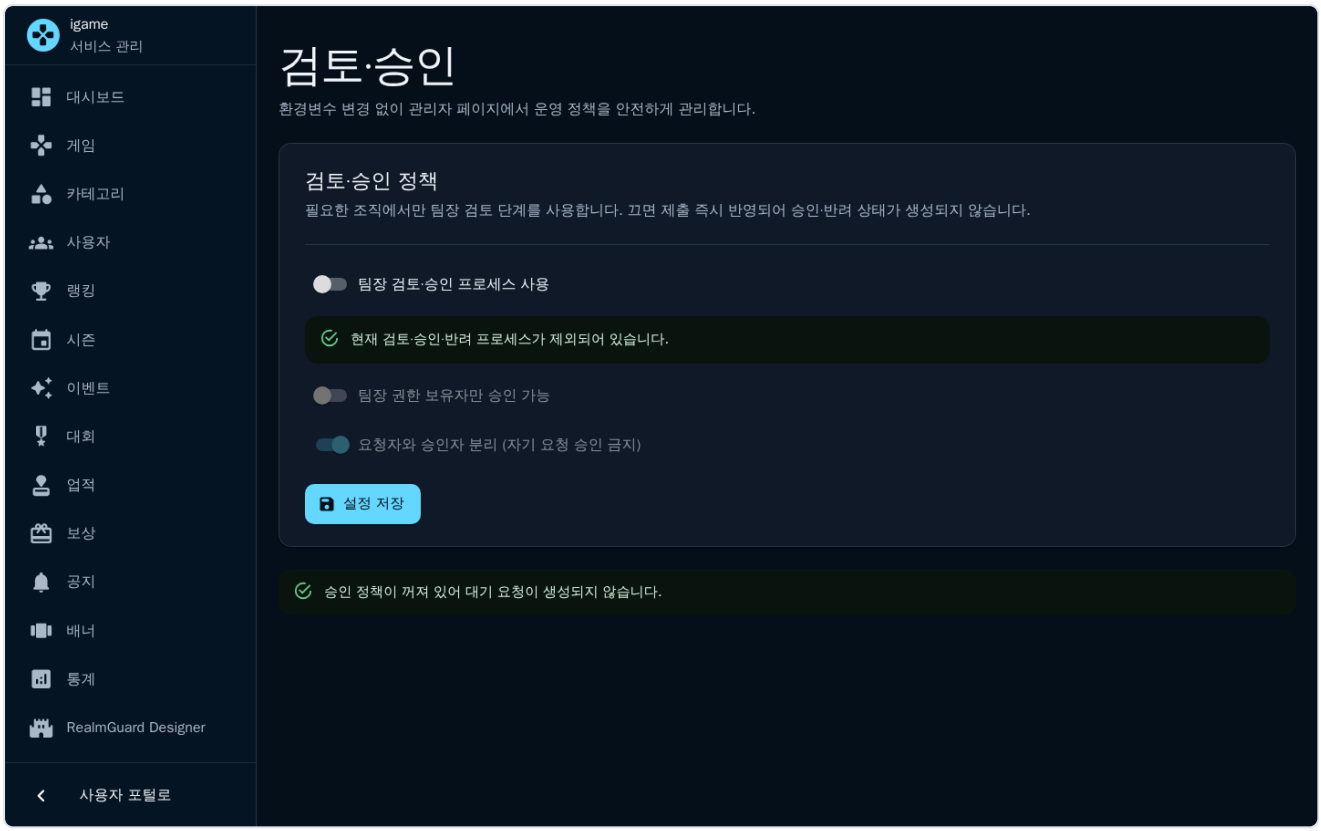


OIDC·보안 — Keycloak issuer/client와 claim 매핑

OIDC·보안 (`/admin/security`, 관리자 전용)

Issuer, Client ID, Client Secret만 넣으면 discovery 문서는 서버가 직접 읽습니다. 사용자 ID·이름·이메일·그룹·부서·팀 claim을 조직의 Keycloak 매핑에 맞춰 지정합니다. 자세한 연동은 Keycloak 연동을 보세요.

저장 화면은 Client Secret을 절대 되돌려 주지 않습니다. 그래서 secret 칸을 비운 채 저장하면 저장된 값을 그대로 유지합니다. 서버가 기존 값을 읽지 못하면 지우지 않고 `현재 저장된 OIDC 설정을 읽지 못해 저장하지 않았습니다.`로 거부합니다.



검토·승인 — 팀장 검토 단계 on/off와 자기 요청 승인 금지

검토·승인 (`/admin/approvals`)

팀장 검토 단계를 쓸지 정합니다. 꺼 두면 제출이 즉시 반영되고 승인·반려 상태 자체가 생기지 않습니다. 켜면 `/reviews`에서 검토합니다. 기본적으로 요청자는 자기 요청을 승인할 수 없고, 매니저 검토는 매니저와 작성자가 **같은, 비어 있지 않은** 팀일 때만 열립니다.

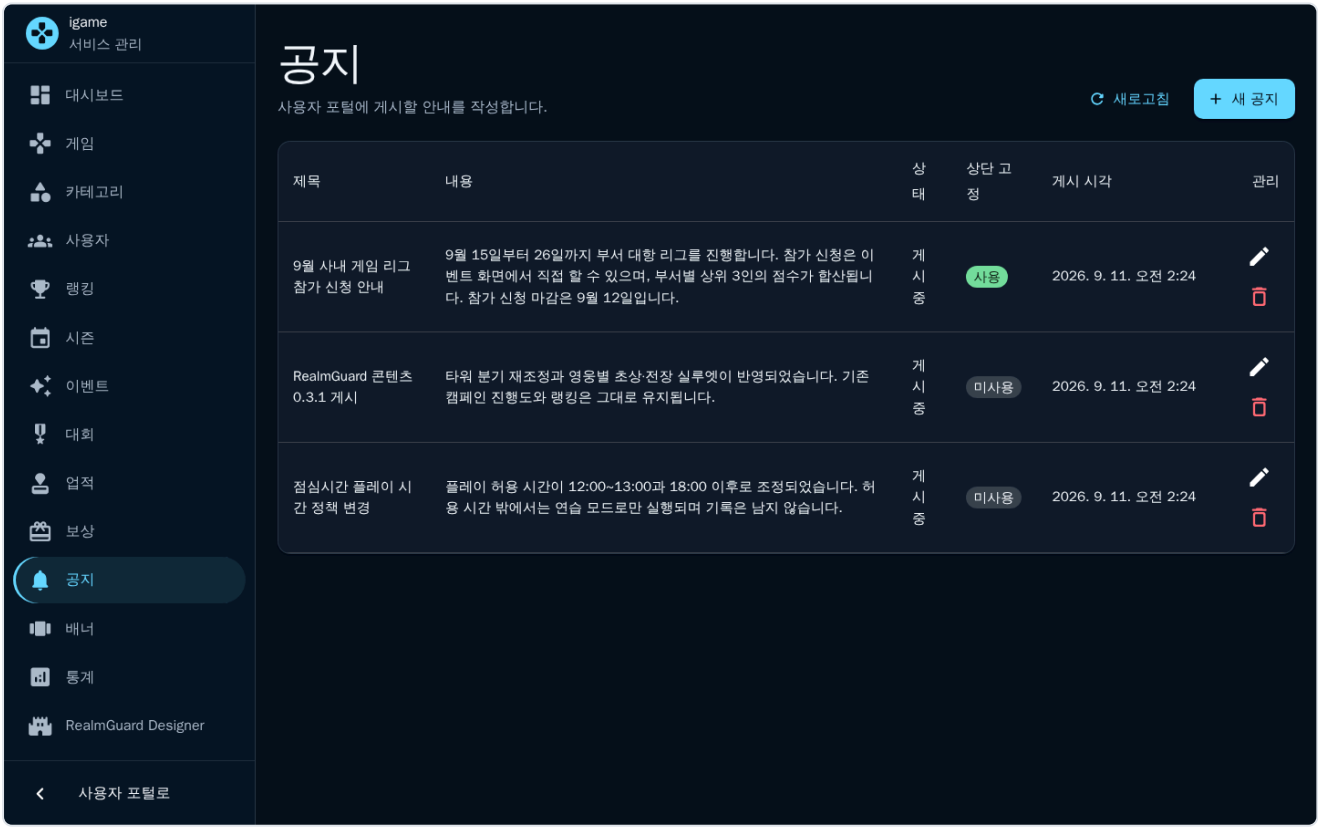
AI 설정 (`/admin/ai`, 관리자 전용) — OpenAI 호환 base URL·모델·API 키·timeout·max token 상한. 브라우저는 공급자를 직접 부르지 않고 서버가 자격 증명을 복호화해 호출합니다. AI가 꺼져 있거나 미설정이면 AI 메뉴와 게임이 숨겨집니다.

키 권한 (`/admin/keys`, 관리자 전용) — 역할별로 개인 API 키에 줄 수 있는 권한, 활성 키 개수, 최대 사용 기간.

방문 추적 (`/admin/tracking`, 관리자 전용) — 어떤 화면이 실제로 쓰이는지 재는 추적 스크립트를 화면에서 붙입니다. 기본값은 **꺼짐**이라 새로 설치한 곳에서는 아무것도 달라지지 않습니다. 설정 방법과 정책(CSP) 설명은 3.3 방문 추적에 있습니다.

콘텐츠 쪽 메뉴(게임·카테고리·랭킹·시즌·이벤트·대회·업적·보상·공지·배너)는 운영자도 쓸 수 있습니다.

게임 — 등록된 게임 목록과 상태·카테고리



공지 — 게시 상태와 고정 여부를 관리한다

3.3 방문 추적

`/admin/tracking`에서 방문 추적 스크립트를 붙입니다. `〈script〉` 한 줄을 넣는 일이 아니라 **콘텐츠 보안 정책(CSP)**을 함께 다루는 일이라, 아래 순서대로 하면 됩니다.

1. 제공자를 고릅니다.

제공자	필요한 값	정책에 더해지는 출처
Momento (사내 수집기)	수집기 주소, 사이트 ID, 환경(기본 `prd`)	프록시를 쓰면 **없음**. 끄면 수집기 주소
Google Analytics 4	측정 ID (`G-…`)	`googletagmanager.com`, `google-analytics.com`
Google Tag Manager	컨테이너 ID (`GTM-…`)	`googletagmanager.com`
Matomo	Matomo 주소, 사이트 ID	Matomo 주소
직접 붙여넣기	스니펫 (8KB 이하)	스니펫에 적힌 `http(s)` 출처 전부

Momento가 첫 자리에 있는 이유는 사내에서 직접 호스팅하는 수집기라 **데이터가 밖으로 나가지 않는 유일한 선택지**이기 때문입니다. 폐쇄망에서는 Google 계열은 동작하지 않습니다.

2. Momento는 같은 오리진 프록시를 그대로 둡니다. 기본으로 켜져 있는 "같은 오리진 프록시 사용"은 스니펫이 `/momento/tracker.js`를 부르고 이벤트를 `/momento`로 보내게 하며, 서비스가 `/momento/*`를 수집기로 넘깁니다. 브라우저는 igame 외의 주소를 부르지 않으므로 정책에 외부 출처가 아예 등장하지 않고, 수집기 주소가 바뀌어도 화면에서 주소만 고치면 됩니다. 프록시는 세션 쿠키와 Bearer 키를 떼고 넘기며, 추적이 꺼져 있거나 다른 제공자를 쓰면 `404`만 냅니다.

3. 저장하고 화면을 다시 엽니다. 저장 뒤 포털을 새로 고치면 스니펫이 `〈head〉` 끝(또는 `〈body〉` 끝)에 들어갑니다. 관리 화면(`/admin`)에는 "관리 화면에서도 추적"을 켠 경우에만 붙습니다. API·MCP·상태 경로에는 붙지 않습니다.

4. 차단된 출처가 있으면 한 번 눌러 허용합니다. 추적이 켜져 있는 동안 브라우저는 정책이 거부한 주소를 서비스에 신고하고, 같은 화면의 **브라우저가 차단한 출처** 표에 출처와 지시어가 쌓입니다. 스니펫이 부르는 픽셀·수집 주소가 여기 보이면 **허용**을 누르고 저장하세요 — 허용 출처에 더해지고 정책에 반영됩니다. 기록은 서버 메모리에 서로 다른 출처 100건까지만 남고 재시작하면 사라지며, 고친 뒤에는 **기록 비우기**로 아직 막히는 것이 있는지 확인합니다.

정책은 왜 느슨해지지 않는가. igame의 정책은 `script-src 'self'`로 잠겨 있어 스니펫을 그냥 넣으면 브라우저가 조용히 막습니다. 추적을 켜면 서비스는 **요청마다** nonce를 만들어 스니펫의 모든 `〈script〉` 태그에 붙이고 같은 값을 `script-src 'nonce-…'`로 정책에 넣습니다. 스니펫이 부르는 출처는 `script-src`·`connect-src`·`img-src`에 더해지고, 신고를 받기 위한 `report-uri`가 붙습니다. 그 외에는 아무것도 바뀌지 않습니다. `'unsafe-inline'`은 어떤 경우에도 넣지 않습니다 — 한 번 풀면 그 앱의 모든 인라인 스크립트가 함께 허용되고, 추적을 끈 뒤에도 정책은 느슨한 채로 남기 때문입니다. 추적을 끄면 정책은 원래 모양으로 돌아갑니다.

붙여넣은 값은 감사 로그에 `setting.update` / `tracking`으로 남습니다. 로그인 화면에도 스니펫이 붙지만, 서비스가 만드는 스니펫은 개인 식별 값을 보내지 않습니다.

4. 계정과 권한

역할은 네 가지입니다. 화면에 나오는 이름 그대로 씁니다.

역할	화면 표기	할 수 있는 일
`user`	일반	포털 이용, 게임 플레이, 랭킹·이벤트·공지 열람, 개인 프로필과 개인 API 키
`manager`	매니저	위 전부 + `/reviews`에서 같은 팀 구성원이 올린 콘텐츠 변경 검토·승인·반려
`operator`	운영자	위 전부 + `/admin`의 콘텐츠 운영(게임·카테고리·랭킹·시즌·이벤트·대회·업적·보상·공지·배너·통계)과 RealmGuard Designer / Defense Content Studio
`admin`	관리자	위 전부 + 사용자, 감사 로그, 키 권한, OIDC·보안, AI 설정, 시스템 설정

역할과 상태는 요청마다 다시 읽습니다. 역할을 낮추거나 계정을 사용 중지하면 이미 열려 있던 세션에도 그 즉시 적용됩니다.

사용자 — 아이디·이름·소속·팀·역할·상태를 한 화면에서 관리한다

`/admin/users`(관리자 전용)에서 검색으로 좁히고, 오른쪽 연필 아이콘으로 역할·상태·비밀번호를 바꿉니다.

- **비밀번호 재설정은 대상 사용자의 세션을 함께 폐기합니다.** 탈취된 계정을 되찾는 수단이므로, 옛 비밀번호로 열린 쿠키는 재설정과 같은 순간에 무효가 됩니다. 관리자가 이 화면에서 자기 비밀번호를 재설정할 때만 그 요청 자신의 세션이 남습니다.
- 폐기한 세션 수는 감사 로그 항목의 `sessions_revoked` 에 남습니다.
- **사용 중지** 상태는 로그인과 API 접근을 모두 막습니다. 기록은 지우지 않습니다.

SSO를 쓰는 배포에서는 사용자 자체가 첫 SSO 로그인 때 만들어집니다. 이름·소속·팀은 Keycloak claim에서 오므로 igame 화면에서 고치지 않고 Keycloak에서 고칩니다.

---

5. 운영

5.1 일상 점검

```
docker compose ps
docker compose logs --since=30m igame
curl --fail --max-time 5 http://127.0.0.1:8080/healthz
curl --fail --max-time 5 http://127.0.0.1:8080/readyz
```

- `/healthz` — 프로세스 감시용. 데이터베이스를 보지 않습니다.
- `/readyz` — 로드밸런서 readiness용. 데이터베이스까지 확인합니다.

이미지의 자체 healthcheck는 `/app/igame healthcheck` 이며, 이미 도는 `127.0.0.1:8080/healthz` 만 확인합니다. 최종 runtime에는 shell이 없으므로 컨테이너 안에서 `sh` · `curl` 로 진단할 수 없습니다. 호스트의 `docker inspect` , `docker logs` 와 바깥에서 보내는 `/readyz` 요청을 씁니다.

권장 경보는 readiness 3회 연속 실패, HTTP 5xx 비율, p95 지연, DB 연결 실패, 디스크 80%, 인증 실패 급증, 점수 이상 탐지, AI provider 오류율입니다.

5.2 서비스 상태 화면

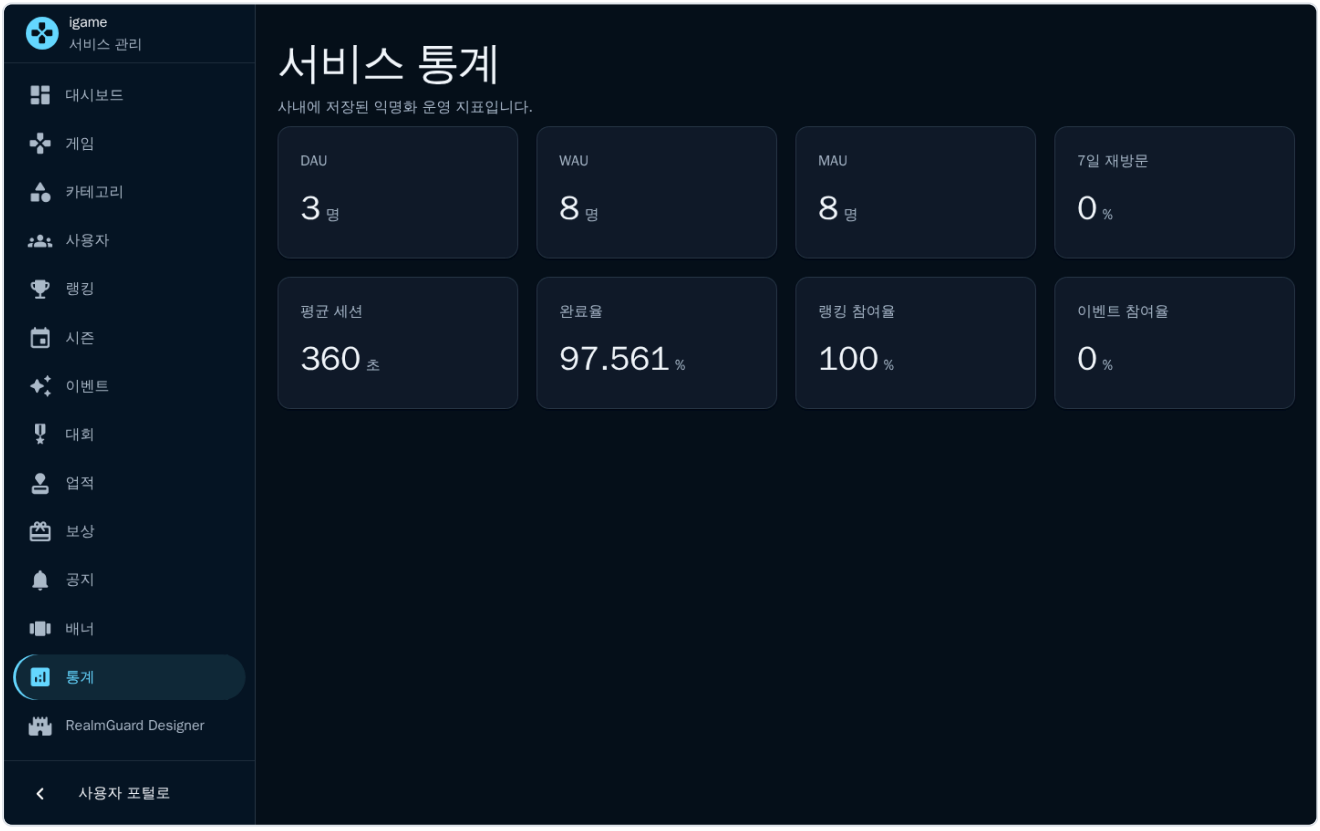
서비스 상태 — DB 연결, 서비스 버전과 시간대, 정책 on/off, 게시된 콘텐츠 버전, 누적 행 수

`/admin` 대시보드 아래쪽의 **서비스 상태** 카드가 1차 진단 지점입니다. 컨테이너 안을 볼 수 없는 이미지이므로 여기서 확인하는 것이 가장 빠릅니다.

- **데이터베이스** — 연결 여부와 응답 지연, 커넥션 pool 사용량.
- **서비스** — 버전, 기준 시간대, 공개 URL 설정 여부. 위 화면에서는 `공개 URL 미설정 또는 HTTP`가 떠 있습니다. 운영 배포에서 이 표시가 남아 있으면 `/admin/settings`에서 공개 URL을 채워야 합니다.
- **정책** — 사내 SSO / 관리자 로그인 / 승인 흐름 / AI 기능 / 플레이 시간 정책의 on-off.
- **게시된 콘텐츠** — RealmGuard와 Defense Series 세 게임의 현재 게시 버전과 게시일.
- **누적 데이터** — 감사 로그·게임 텔레메트리·게임 세션·점수의 행 수. `pg_class` 통계 기반 추정치입니다. **자동 보존·삭제 job은 없으므로** 보존 기간은 조직 정책으로 직접 관리해야 한다고 화면이 그대로 알려 줍니다.

5.3 대시보드와 통계

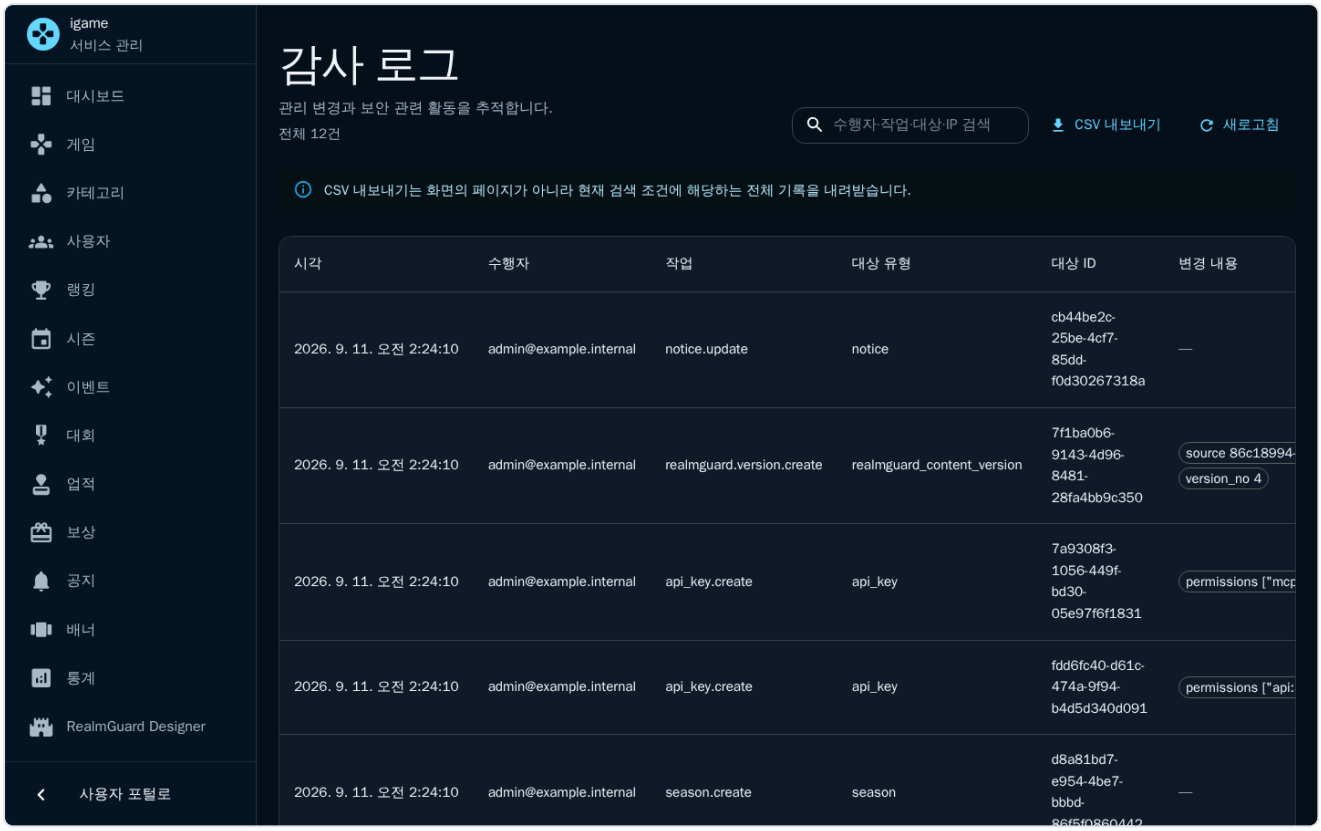
서비스 대시보드 — 활성 사용자·오늘 게임 실행·등록 점수와 인기 게임



서비스 통계 — DAU/WAU/MAU와 평균 세션, 완료율, 랭킹·이벤트 참여율

통계는 사내에 저장된 익명화 지표만 다룹니다.

5.4 감사 로그



감사 로그 — 시각·수행자·작업·대상과 CSV 내보내기

`/admin/audit` (관리자 전용)에서 수행자·작업·대상·IP로 검색하고 페이지당 25~200건을 봅니다. 목록은 현재 페이지와 함께 **필터 적용 후 전체 건수**를 표시하므로 목록이 조용히 잘리지 않습니다.

CSV 내보내기는 화면의 페이지가 아니라 조건에 맞는 전체 기록을 streaming합니다. 기록이 많으면 시간이 걸립니다. Excel이 한국어를 바르게 읽도록 UTF-8 BOM을 붙이고, 수식으로 해석될 수 있는 값(`=`, `+`, `-`, `@`로 시작)은 앞에 작은따옴표를 넣어 무력화합니다. 내보내기 실행 자체도 `audit.export` 항목으로 남습니다.

5.5 백업과 복구

PostgreSQL에 사용자·설정·암호화된 secret·키 메타데이터·게임·점수·감사 기록과 게시 콘텐츠가 모두 들어 있습니다. `/app/data`를 쓰는 배포라면 같은 복구 시점으로 함께 보관합니다.

```
umask 077
export POSTGRES_DSN='postgres://...'
bash ./scripts/backup.sh /secure/igame-backups
unset POSTGRES_DSN
```

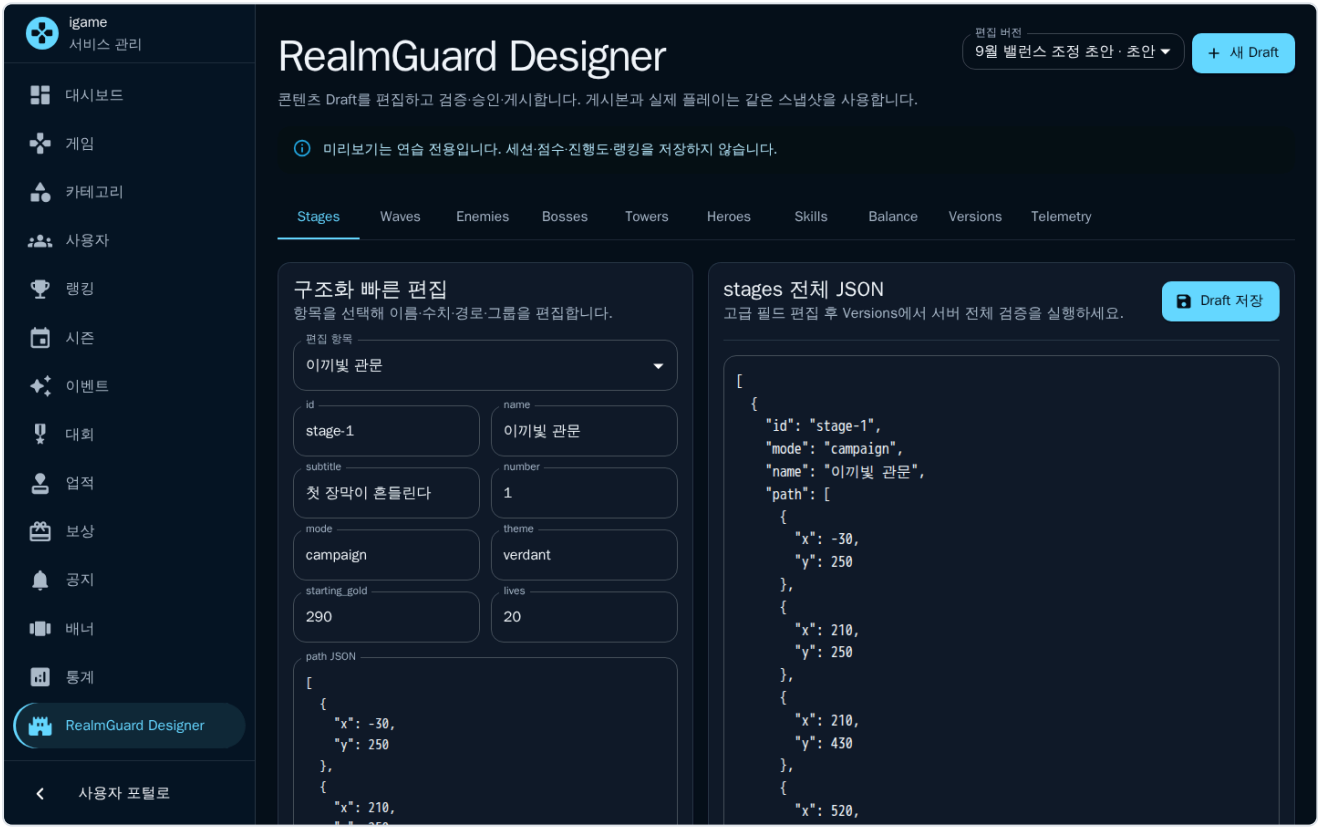
`ENCRYPTION_KEY`가 없으면 DB의 암호화된 값은 복구할 수 없습니다. **백업 파일과 같은 위치에 두지 마세요.** 보존 정책, 업로드 자산 백업, 복구 연습 절차는 백업과 복구를 따릅니다.

5.6 업그레이드와 되돌리기

1. 릴리스 checksum·SBOM 검토와 스테이징 시험을 마칩니다.
2. DB와 `/app/data`를 백업합니다.
3. 새 `igame:vX.Y.Z` 이미지를 `docker load` 합니다.
4. compose 파일의 이미지 태그를 정확한 버전으로 바꿉니다. `latest`는 쓰지 않습니다.
5. 유지보수 창에서 `docker compose up -d --no-deps igame`을 실행합니다.
6. `/readyz`, 로그인, 버전, 게임 실행, 점수 제출, 관리자 화면을 확인합니다.

되돌릴 때는 **이미지 태그만 되돌리지 마세요.** 마이그레이션은 전진 적용이 기본이라, 이전 이미지가 새 스키마와 호환된다는 릴리스 노트가 없으면 검증된 DB 백업을 함께 복구해야 합니다. 콘텐츠가 문제라면 이미지를 되돌리는 대신 알려진 정상 콘텐츠를 새 Draft로 복구해 같은 절차로 게시하는 쪽이 안전합니다.

5.7 콘텐츠 게시



RealmGuard Designer — Draft를 편집하고 검증·승인·게시한다

RealmGuard와 Defense Series 콘텐츠는 Draft → Test → (승인) → 게시 순서로 다룹니다. 새 게시물은 그 뒤에 시작한 세션에만 적용되고, 진행 중인 세션은 시작할 때 고정된 스냅샷으로 끝까지 검증됩니다. 편집 충돌은 `If-Match` checksum으로 막으므로 `stale_version`을 만나면 자동으로 덮어쓰지 말고 최신 section을 다시 읽어 병합합니다.

검증 항목과 게시 절차 전체는 RealmGuard 운영 가이드와 Defense Series 운영 가이드에 있습니다.

6. 장애 대응

6.1 기동하지 않을 때

로그(`docker compose logs igame`)에 실제로 찍히는 문구로 나눕니다. 로그는 JSON 한 줄입니다.

로그 문구	뜻	조치
`configuration error` + `missing required environment variables: …`	네 환경 변수 중 비어 있는 것이 있습니다	적힌 이름을 `.env` 에 채웁니다
`configuration error` + `BOOTSTRAP_ADMIN_PASSWORD must be at least 12 characters`	최초 관리자 비밀번호가 짧습니다	12자 이상으로 바꿉니다
`configuration error` + `ENCRYPTION_KEY: must decode to exactly 32 bytes, got …`	마스터 키 길이가 틀립니다	`openssl rand -base64 32` 로 다시 만듭니다
`startup failed`	DB 연결·마이그레이션·최초 관리자 생성 중 하나가 실패했습니다	함께 찍힌 `error` 값으로 DSN·DNS·TLS·권한을 확인합니다
`encryption initialization failed`	마스터 키로 암호화기를 만들지 못했습니다	`ENCRYPTION_KEY` 형식을 확인합니다
`HTTP server failed`	8080 포트를 열지 못했습니다	포트 충돌을 확인합니다

6.2 도는데 이상할 때

증상	확인할 곳	조치
`/healthz` 실패	프로세스 종료, OOM, 포트 충돌, 환경 변수 형식	위 표의 기동 로그부터 봅니다
`/healthz` 는 되는데 `/readyz` 만 실패	PostgreSQL DNS·TLS·권한·연결 수, 마이그레이션 오류	사용자에게는 `서비스가 아직 준비되지 않았습니다.` 로 보입니다
화면은 열리는데 저장만 `csrf_rejected`	서버 로그의 `request origin rejected` 항목 — 받은 `origin` 과 허용 목록을 함께 남깁니다	`/admin/settings` 의 공개 URL을 실제 주소로 맞추고, 프록시 뒤라면 **신뢰 프록시 헤더 사용**을 켭니다
로그인 시도가 계속 막힘	로그의 `local sign-in throttled` (아이디와 접속 IP를 함께 남김)	정상적인 잠금입니다. 급증하면 인증 공격을 의심합니다
권한 오류가 잦음	로그의 `access denied` (경로·메서드 포함)	역할 또는 개인 API 키 권한을 확인합니다
SSO redirect loop	공개 URL, 프록시 forwarded header, redirect URI, 쿠키 secure 설정	공개 URL이 `https://` 로 시작해야 세션 쿠키에 Secure가 붙습니다
토큰 검증 실패	issuer/audience, JWKS 접근, 시계 오차, Keycloak key rotation	호스트 시간 동기화를 먼저 확인합니다
AI 응답이 중간에 끊김	provider 접근, timeout, 프록시 SSE buffering, 모델 token 상한	SSE 경로의 proxy buffering을 끄고 idle timeout을 늘립니다
게임 iframe이 차단됨	허용 Frame Origin, 게임 쪽 `frame-ancestors` / `X-Frame-Options`	`/admin/settings` 의 허용 origin에 추가합니다
점수가 반영되지 않음	세션 토큰과 소유권, 같은 세션의 중복 점수, 게임별 점수·시간 규칙	RealmGuard·Defense는 전용 결과 경로로만 공식 기록이 만들어집니다
감사 로그가 비어 보임	로그의 `write audit log` 경고	감사 기록 실패는 경고로 남고 본 요청은 진행됩니다
게시 콘텐츠 관련 오류	`realmguard_config_stale` , `defense_config_stale` , `stale_version` 등	운영 및 장애 대응의 장애별 확인 표에 코드별로 정리되어 있습니다

사용자에게 보이는 오류 문구와 각각의 뜻은 사용자 가이드의 "막혔을 때"에 정리되어 있습니다. 문의를 받을 때 그 표를 먼저 보면 관리자에게 넘길 일인지 바로 갈립니다.

---

7. 보안

7.1 설치 직후 반드시 바꾸는 것

- `BOOTSTRAP_ADMIN_PASSWORD` 로 만든 첫 계정의 비밀번호. 로그인 후 즉시 바꿉니다.

- **서비스 공개 URL.** 비워 두면 브라우저 요청 판정과 세션 쿠키의 Secure 처리가 실제 배포와 어긋납니다.
- SSO를 붙였다면 **Bootstrap 관리자 로그인 사용**을 끕니다.
- `.env` 의 권한(`chmod 600`)과 소유자. 이 파일은 형상 관리에 올리지 않습니다.

7.2 외부에 열지 않는 것

- 컨테이너의 `8080/tcp` 를 인터넷이나 신뢰하지 않는 망에 직접 노출하지 않습니다. TLS 종단 프록시 뒤에 둡니다.
- PostgreSQL `5432/tcp` 는 서비스 호스트에서만 닿게 합니다. 운영에서는 `sslmode=verify-full` 을 씁니다.
- `/mcp` 엔드포인트도 같은 인증을 쓰지만, 열어 줄 대상이 없다면 프록시에서 막습니다.

7.3 계정과 키

- 역할은 최소 권한으로 줍니다. 사용자 관리·감사 로그·설정은 `admin` 만 볼 수 있습니다.
- 개인 API 키는 필요한 권한만 골라 발급하게 하고, `/admin/keys` 에서 역할별 상한과 최대 사용 기간을 정합니다. 키 값은 발급 직후 한 번만 보이며 이후에는 앞자리만 남습니다.
- 계정을 회수할 때는 **비밀번호 재설정**을 쓰세요. 재설정이 대상의 세션을 같은 순간에 폐기합니다. 역할만 낮춰도 다음 요청부터 곧바로 적용됩니다.

7.4 컨테이너 하드닝

배포되는 `docker-compose.yml` 이 이미 다음을 켜 둡니다. 임의로 풀지 마세요.

설정	값
`read_only`	`true` (루트 파일시스템 읽기 전용)
`tmpfs`	`/tmp` 64 MiB, `noexec,nosuid,nodev`
`cap_drop`	`ALL`
`security_opt`	`no-new-privileges:true`
`pids_limit`	`256`
로그	json-file, 20 MiB × 5

최종 runtime 이미지는 `scratch` 기반이라 shell도 패키지 매니저도 없습니다. 진단 편의를 위해 셸이 있는 베이스로 바꾸지 마세요 — 그 편의가 곧 공격면입니다.

7.5 방문 추적과 콘텐츠 보안 정책

방문 추적은 꺼져 있는 것이 기본이고, 켜더라도 정책의 `script-src` 에 `'unsafe-inline'` 이 들어가는 일은 없습니다 — 요청별 nonce와 스니펫이 부르는 출처만 더해집니다. 자세한 동작은 3.3 방문 추적에 있습니다. 수집기가 사내에 있어야 한다면 Momento를 고르고 같은 오리진 프록시를 그대로 두세요. 외부 수집기를 고르면 방문자의 브라우저가 그 주소를 직접 부르게 되고, 정책 위반 신고(`POST /api/v1/tracking/csp-report`)는 인증 없이 받되 메모리의 고정 크기 목록에만 담깁니다.

7.6 기록에 남지 않게 하는 것

암호, 토큰, API 키, OIDC code와 AI 프롬프트 전문은 로그에 남기지 않는 것이 운영 원칙입니다. 요청 추적은 reverse proxy access log의 correlation ID로 합니다.

키 관리와 암호화 경계의 자세한 내용은 보안 및 키 관리를 보세요.

더 읽을 것

- 사용자 가이드 — 화면 사용법과 사용자가 만나는 오류
- 오프라인 설치 — 반입 검사, 사설 CA, 파생 이미지
- 운영 및 장애 대응 — 오류 코드별 확인 표, 프록시, 용량 계획
- 백업과 복구 · 보안 및 키 관리 · Keycloak 연동
- RealmGuard 운영 가이드 · Defense Series 운영 가이드
- API 계약 · MCP 연동 · 릴리스 절차