TechWizard
Structuring Digital Complexity

EA-WIZARD · SÉCURITÉ

# Sécurité & multi-tenant souverain

RBAC granulaire, Row-Level Security testée sous attaque, journal d'audit immuable, AES-256 partout, et une certification de performance publiée. Conçu pour passer les audits, pas pour les éviter.

EA-Wizard offre la sécurité multi-tenant qu'attendent les banques et le secteur public — et le prouve par des résultats mesurés et publiés, plutôt que par des promesses marketing.

| 340 | 23 | 0 | 2 099 |
|---|---|---|---|
| codes de permission RBAC | tests d'isolation tenant | fuite sous attaque | méthodes de test |

## Contrôle d'accès

### RBAC — 340 codes de permission

- Motif `module__resource__action`.
- Cache Caffeine TTL 60 s ; invalidation instantanée `@CacheEvict` au changement de rôle.
- Sondé en direct via Spring Actuator.

### SSO entreprise

Intégration IAM complète avec Keycloak, LDAP et SAML 2.0. `UserStatusFilter`, `DemandStatusPolicy` et `OrganizationResolutionFilter` sont tous testés sous attaque pour bloquer l'usurpation d'identité.

### Validation de licence — HMAC-SHA256

Clés signées au format `TIER-ORGID-EXPIRY-MAXUSERS-HMAC`. Le LicenseGate frontend refuse les fonctionnalités hors périmètre — sans contournement côté client.

## Isolation multi-tenant

L'isolation des tenants n'est pas une convention applicative. C'est une frontière imposée par la base de données elle-même, via la Row-Level Security PostgreSQL sur l'ensemble du schéma.

- Rôle dédié `eaapp` avec `NOSUPERUSER` — même un développeur authentifié ne peut contourner la RLS.
- 40+ tables parentes et 60+ tables enfants couvertes ; 4 tables orphelines explicitement traitées.
- 23 tests d'isolation automatisés (cross-tenant + RLS Testcontainers) exécutés en CI.
- Fuite NULL-org auditée et corrigée (V145 / V146).

### Testé sous attaque — Gatling

| MÉTRIQUE | VALEUR |
|---|---|
| Tentatives de fuite cross-tenant | 60 |
| Rejetées (HTTP 400) | 60 |
| Enregistrements exposés | 0 |
| Latence sous attaque (p95) | 23 ms |

Ce ne sont pas des formules marketing — ce sont des résultats mesurés, versionnés dans le dépôt sous le nom `TenantIsolationSimulation`.

## Audit & traçabilité

### Journal d'audit immuable

- Trigger PostgreSQL BEFORE bloquant UPDATE et DELETE.
- Inviolable par conception — même un DBA ne peut altérer un événement d'audit.
- La protection vit dans le moteur, pas dans l'application ; RLS renforcée en V146 contre les fuites NULL-org.
- Export CSV + PDF, filtré par plage de dates, aligné sur les exigences des régulateurs européens et marocains.

### Observabilité distribuée

- Auto-instrumentation OpenTelemetry complète : chaque requête HTTP, requête SQL et hit de cache tracé.
- Configurable à chaud depuis une GUI d'administration (échantillonnage, endpoint) — sans redémarrage.
- Désactivation automatique en cas de panne de connectivité via un compteur de sondes AtomicInteger.

## Chiffrement

AES-256-GCM uniforme sur six catégories de secrets, via un unique `AesEncryptionService` : en-têtes OpenTelemetry, identifiants des connecteurs Jira et ServiceNow, identifiants SMTP, clés d'API des fournisseurs IA, et identifiants EA Chat. Un algorithme, une clé maître, un point d'audit.

## Certification de performance

Référence **EAW-PERF-CERT-V12-2026-003** — mesurée et publiée.

| MÉTRIQUE | VALEUR |
|---|---|
| Requêtes | 34 476 |
| Erreurs | 0 |
| Latence p95 | 136 ms |
| Latence p99 | 240 ms |
| Simulations versionnées | 4 |

Stack optimisée pour la production : threads Tomcat 300, accept-count 200, pool Hikari 25, timeout de connexion 5 s — dimensionnée pour un pic de 200 utilisateurs.

## Prêt pour l’audit

- 28 des 30 CVE connues corrigées.
- Journal d’audit immuable + RLS sur tout le schéma + tests d’attaque tenant en direct.

> **DISPONIBLE SUR DEMANDE**
>
> Pour les réponses à appel d’offres : catalogue complet des codes de permission RBAC, liste des politiques RLS, schéma et source du trigger d’audit, sources des simulations Gatling, le rapport de certification de performance, et le rapport de scan OWASP.