EPIC 2 — Durcissement serveur & réseau (Ops / Sec RGPD)

---

1. Objectif de l'EPIC

Mettre en place un **environnement serveur et réseau fortement durci**, destiné à héberger une plateforme IA manipulant des **données hautement sensibles** (comptabilité, santé, juridique), en garantissant un niveau élevé de :

- **Confidentialité**
- **Intégrité**
- **Disponibilité**
- **Résilience opérationnelle**

📌**Cadre RGPD**
Cet EPIC couvre exclusivement les **mesures de sécurité techniques et organisationnelles** au sens de l'**article 32 du RGPD**.

Les droits des personnes concernées (consentement, accès, effacement, portabilité) sont **hors périmètre** et traités dans **EPIC 5**.

---

2. Positionnement dans la roadmap

- EPIC 1 — Socle applicatif sécurisé (IAM, multi-tenant, Gateway LLM)
- **EPIC 2 — Durcissement serveur & réseau (ce document)**
- EPIC 3 — Validation technique IA locale (POC contrôlé)
- EPIC 4 — Stockage IA & données utilisateur RGPD
- EPIC 5 — Pipeline RGPD (droits des personnes)
- EPIC 6 — Stack IA Docker RGPD-ready (industrialisation)
- EPIC 7 — Kit conformité & audit

---

3. Périmètre couvert

Inclus

- Sécurisation du **système d'exploitation** (OS)
- Sécurisation réseau et **exposition minimale**
- Accès administrateur et gestion des privilèges
- Chiffrement des communications
- Supervision sécurité et détection d'incidents
- Politique de mises à jour et correctifs
- Sauvegardes sécurisées (disponibilité / intégrité)
- **Conditions d'exécution sécurisées du bootstrap plateforme** (EPIC 1)

Exclus

- Logique applicative (EPIC 1)
- Runtime et orchestration IA (EPIC 3, EPIC 6)
- Stockage fonctionnel des données IA (EPIC 4)
- Droits RGPD des personnes (EPIC 5)

---

4. Principes directeurs (non négociables)

- Principe du **moindre privilège** (utilisateurs, services, réseau)
- **Surface d'attaque minimale** (deny-by-default)
- Chiffrement systématique des flux exposés
- Traçabilité des accès administrateurs
- Défense en profondeur (prévention + détection)

---

5. Architecture cible (vue infrastructure)

- Serveur **Linux LTS** durci
- Pare-feu hôte (nftables / iptables)
- Reverse proxy TLS en frontal
- Réseau interne isolé (services non exposés)
- Accès administrateur contrôlé (SSH par clés)
- Environnement Docker cloisonné (préparation EPIC 6)

---

6. Bootstrap plateforme — contraintes d'infrastructure

📌Cette section **complète EPIC 1** et précise les **pré-requis Ops/Sec** nécessaires à l'exécution sécurisée du bootstrap plateforme (superadmin, tenants).

Exigences :

- Le **bootstrap est exécuté localement sur le serveur** (CLI uniquement)
- Accès réservé à un **administrateur système autorisé**
- Aucun port réseau supplémentaire ouvert pour le bootstrap
- Les secrets nécessaires (DB, crypto) sont fournis via **mécanisme sécurisé** (env protégées / secrets Docker / vault)
- Les commandes de bootstrap sont **journalisées au niveau système** (audit admin), sans exposer de données sensibles

📌Le bootstrap ne doit **jamais** dépendre d'un endpoint HTTP public.

---

7. User Stories & exigences

US-1 — Durcissement du système d’exploitation

Je veux un OS configuré selon les bonnes pratiques de sécurité.

Exigences : - OS Linux LTS maintenu et supporté - Désactivation des services inutiles - Permissions fichiers strictes - Protection contre l’escalade de privilèges - Journalisation système active

---

US-2 — Accès administrateur sécurisé

Je veux contrôler strictement les accès administrateurs.

Exigences : - Accès SSH par clés uniquement - Login root direct interdit - MFA pour accès admin si possible - Journalisation des connexions

---

US-3 — Pare-feu & exposition réseau minimale

Je veux limiter strictement l’exposition réseau.

Exigences : - Politique réseau deny-all par défaut - Ouverture explicite des ports nécessaires - Filtrage IP si applicable - Rate limiting réseau

---

US-4 — Chiffrement des communications

Je veux garantir la confidentialité des flux.

Exigences : - HTTPS obligatoire (TLS récent) - Certificats valides et renouvelés automatiquement - HTTP non chiffré interdit

---

US-5 — Isolation réseau interne

Je veux empêcher tout accès direct aux composants internes.

Exigences : - Réseau interne non exposé publiquement - Segmentation stricte entre services - Bases de données et moteurs IA non exposés

---

US-6 — Supervision & détection d’intrusion

Je veux détecter rapidement les comportements anormaux.

Exigences : - IDS / IPS ou équivalent - Alertes sur tentatives suspectes - Monitoring ressources (CPU, RAM, disque) - Centralisation des logs système

---

US-7 — Politique de mises à jour & correctifs

Je veux maintenir le serveur à jour.

Exigences : - Mises à jour de sécurité automatiques - Revue périodique manuelle - Redémarrages planifiés si nécessaires

---

US-8 — Sauvegardes sécurisées

Je veux protéger les données contre la perte.

Exigences : - Sauvegardes chiffrées - Stockage isolé et protégé - Accès strictement limité - Politique de rétention documentée et auditée

📌**Clarification RGPD** : - Les sauvegardes garantissent la disponibilité et l'intégrité (art. 32 RGPD) - Les droits à l'effacement ne s'appliquent pas immédiatement aux backups - L'effacement RGPD est assuré via rétention maîtrisée et crypto-shredding (EPIC 5)

---

8. Dépendances

- Dépend de : **EPIC 1** (socle applicatif, bootstrap)
- Prérequis pour : EPIC 3, EPIC 4, EPIC 5, EPIC 6, EPIC 7

---

9. Livrables

- Serveur Linux durci opérationnel
- Pare-feu configuré
- Accès administrateur sécurisé et journalisé
- HTTPS actif
- Supervision et alerting en place
- Politique de sauvegarde validée
- Procédure d'installation incluant le bootstrap plateforme

---

10. Risques & points de vigilance

- Mauvaise configuration réseau → **exposition critique**
- Oubli de mises à jour → vulnérabilités connues
- Alertes non traitées → faux sentiment de sécurité
- Accès admin non maîtrisé → compromission totale

---

11. Definition of Done (DoD)

- Aucun port inutile exposé

- Accès administrateur journalisé
- Communications chiffrées
- Sauvegardes testées
- Bootstrap exécutable uniquement dans un environnement sécurisé
- Checklist sécurité validée

Fin EPIC 2