🗄️ Documentation Technique: Infrastructure Docker & Sécurité

Serveur : Debian 4GB (Hetzner)
Projet : Auth Infrastructure (SuperTokens, Nginx, Node.js)
Mise à jour : 08 Décembre 2025

---

1. Configuration du Démon Docker

Fichier modifié : `/etc/docker/daemon.json`

Le moteur Docker a été configuré selon les bonnes pratiques CIS & OWASP pour renforcer la stabilité et la sécurité.

Paramètre	Valeur	Justification
`log-driver`	`json-file`	Standard, adapté aux petites infrastructures
`max-size: 10m` / `max-file: 3`	Rotation des logs	Empêche la saturation du disque de 4GB
`live-restore: true`	✓ Activé	Maintient les conteneurs actifs même si Docker redémarre
`no-new-privileges: true`	✓ Activé	Bloque toute élévation de privilèges interne

---

2. Sécurisation des Conteneurs (Docker Compose)

Fichier modifié : `/opt/auth-infrastructure/docker-compose.yml`

A. Limitation des Ressources (Anti-crash)

Empêche un conteneur défaillant de saturer la RAM ou le CPU.

Service	RAM max	CPU max
Backend / DB	512MB	0.5 CPU
Frontend / Nginx	256–512MB	0.25 CPU

B. Cloisonnement Réseau (Network Segmentation)

Deux réseaux créés pour séparer les services publics et les services critiques.

- **public_net** → Exposé, connecté : Nginx / Frontend / Backend
- **internal_net** → Interne (internal: true), connecté : Backend ↔ Base de données

➡️ *En cas de compromission du serveur web, la base de données reste isolée.*

C. Gestion des Privilèges (Principe du Moindre Droit)

- `security_opt: no-new-privileges:true` activé sur **tous les services**.
- Utilisation d'**images minimales Alpine Linux** pour réduire la surface d'attaque.

D. Fiabilité & Vérifications (Healthchecks)

Ajout de tests automatiques pour détecter les crashs.

- **PostgreSQL** → `pg_isready`
- **Backend** → `wget` de la page d'accueil toutes les 30s

Si un service devient `unhealthy`, Docker redémarre automatiquement le conteneur.

---

3. Gestion des Fichiers et des Secrets

🔑 Variables d'Environnement

- Le fichier `.env` a été déplacé à la racine du projet pour corriger un bug de build.
- **Action obligatoire : Rotation des clés API (Google / Apple / GitHub)** → exposition accidentelle.

🧹 .dockerignore

Fichier ajouté pour ne pas envoyer de fichiers sensibles dans les images :

Exclus : - `.git` (trop volumineux) - `node_modules` (inutile, source de conflits) - `.env` (sécurité)

---

4. Guide de Maintenance (Cheat Sheet)

🔄 1. Mettre à jour l'application

```
docker compose up -d --build --remove-orphans
```

🩺 2. Vérifier l'état des services

```
docker compose ps
```

🧹 3. Nettoyer le disque (recommandé : 1 fois / semaine)

```
docker system prune -a -f
```

💾 4. Sauvegarder la base de données

```
docker exec -t auth-infrastructure-supertokens-postgresql-1 \
pg_dumpall -c -U supertokens_user > backup_$(date +%F).sql
```

---

5. Checklist de Sécurité (État Final)

Catégorie	État
Host Security	✅ Validé
Image Security	✅ Validé
Runtime Security	✅ Validé
Network Security	✅ Validé
Logging	✅ Validé
Filesystem	⚠️ Partiel (Mode DEV : Vite nécessite écriture)
