Gestion des secrets

Gestion des secrets

> *Dernière mise à jour : 2026-05-10*

Inventaire des secrets

Secret	Stocké où	Rotation	Critique ?
`COOKIE_SECRET`	env var Unraid	À la création du container	Élevé : compromission = forge sessions
`FIRST_ADMIN_PASSWORD`	env var Unraid (boot only)	Une seule fois	Faible après boot (changé via `/me`)
Hash password users	SQLite (argon2id)	Par user via reset	N/A (hash, pas le clair)
Token de session	Map RAM (jamais persistée)	À chaque login	N/A (rotation auto)
`BGG_API_TOKEN`	env var Unraid	Manuel	Faible (API publique fonctionne sans)
`SMTP_USER` / `SMTP_PASS`	env var Unraid	Manuel	Moyen (compromission = spam from your domain)
Clé privée SSH oracle (`id_ed25519`)	Volume `/app/ssh/` (RO dans le container)	6 mois recommandé	**Critique** : compromission = exécution arbitraire sur la VM oracle
`.credentials.json` Anthropic	Sur la VM oracle uniquement	À la rotation Anthropic	Élevé : compromission = quota du compte
`REGISTRY_USER` / `REGISTRY_PASSWORD`	Gitea Secrets	À la rotation Gitea	Moyen (compromission = push d'images compromises)

Règles

- **Jamais dans git** : `.env` est dans `.gitignore`. `Dockerfile` touche un `.env` vide pour que les npm scripts (qui passent `--env-file=.env`) ne crashent pas, mais le contenu reste passé via Docker `-e` ou Unraid UI.
- **Jamais dans les logs** : le logger ne logue jamais une env var en clair. Vérifier avec `grep` régulièrement.
- **Jamais dans la doc** : utiliser des placeholders (`<your-token-here>`) dans `.env.example`.

Rotation

`COOKIE_SECRET`

- Effet d'une rotation : toutes les sessions in-memory sont invalidées au restart
- Pas urgent sauf compromission. À faire si tu soupçonnes une fuite.

```
# Générer un nouveau secret
node -e "console.log(require('crypto').randomBytes(32).toString('hex'))"

# Mettre dans .env Unraid + restart
docker compose -f /mnt/user/appdata/boardgame-referee/docker-compose.yml restart app
```

Clé SSH oracle

Cf. `securite/ssh-oracle.md` § "Rotation de la clé SSH". Procédure complète en 7 étapes.

`.credentials.json` Anthropic

Sur la VM oracle :

```
# Sur ton compte admin VM
cp ~/.claude/.credentials.json /home/oracle/.claude/.credentials.json
chown oracle:oracle /home/oracle/.claude/.credentials.json
```

Tokens API (BGG, registry)

Régénérer côté provider, mettre à jour dans Unraid UI / Gitea Secrets, restart.

Stockage long terme

Recommandation : utiliser **Bitwarden self-hosted** (vaultwarden) pour les secrets :

- `COOKIE_SECRET` (genre "boardgame-referee — cookie secret")
- Clé privée SSH oracle (en attachement chiffré)
- Credentials Anthropic
- Tokens registry, BGG, SMTP

Backup régulier de Bitwarden lui-même + clé maître mémorisée par toi seul.

Pas de secrets dans le code source

Vérifier régulièrement avec `git secrets` ou `gitleaks` :

```
# Installer gitleaks (binary release sur GitHub)
gitleaks detect --source . --no-git
```

Pas de scan auto en CI actuellement — peut être ajouté facilement (job `gitleaks` dans `.gitea/workflows/build.yml`).

Si compromission

Suspecté : `COOKIE_SECRET`

1. Régénérer immédiatement
2. Restart container (sessions invalidées)
3. Vérifier les logs récents pour activité anormale (logins multiples, IPs inhabituelles)

Suspecté : clé SSH oracle

1. Rotation immédiate (cf. ssh-oracle.md)
2. Vérifier `/home/oracle/.claude/.credentials.json` — exfiltration possible si Read l'a vu (mais le settings.json le bloque normalement)
3. Vérifier les logs `auth.log` côté VM pour SSH inattendus

Suspecté : credentials Anthropic

1. Révoquer le token côté console.anthropic.com
2. Générer une nouvelle session sur la VM oracle (`claude login` côté oracle)
3. Audit des appels API récents côté Anthropic dashboard

Revision #1
Created 2026-05-10 15:20:18 UTC by thymon
Updated 2026-05-10 15:20:18 UTC by thymon