BLUE FOX

Vaultwarden : aide-mémoire d'administration

Ce qu'il faut régler, sauvegarder et surveiller sur une instance auto-hébergée. Compagnon technique de l'article « Vaultwarden : votre coffre de mots de passe, chez vous ».

Les cinq réglages du premier jour

1. **Jeton d'administration**
   Remplacer le jeton en clair par une empreinte Argon2 (commande vaultwarden hash, offerte depuis la 1.28). Laissé en clair, quiconque lit le fichier de configuration devient administrateur du coffre.
2. **Inscriptions fermées**
   Couper l'inscription libre et fonctionner par invitation, sinon n'importe qui trouvant l'adresse se crée un compte.
3. **HTTPS par proxy inverse**
   Le TLS intégré au serveur n'est pas jugé prêt pour la production par le projet lui-même. Proxy inverse devant, vrai certificat.
4. **Deuxième facteur imposé**
   WebAuthn ou FIDO2, TOTP, ou YubiKey OTP. Un coffre derrière un seul mot de passe déplace le problème au lieu de le régler.
5. **Collections par équipe**
   Cloisonner par département dès le départ. Un coffre commun unique reproduit le chiffrier qu'on cherchait à quitter.

Durcissement

- Désactiver l'affichage de l'indice de mot de passe sur la page de connexion.
- Bloquer l'accès par adresse IP directe (SNI strict) pour sortir des balayages automatisés.
- Exécuter le conteneur en uid/gid 1000 plutôt qu'en root, et monter en lecture seule ce que le service ne doit pas écrire.
- fail2ban sur les échecs d'authentification répétés.
- Caviarder le paramètre access_token dans les journaux du proxy inverse : il apparaît dans les requêtes de notification.

Ce que le serveur ne fait pas

- Ouvrir le coffre avec une clé d'accès. WebAuthn fonctionne en deuxième facteur, pas comme identifiant principal.
- Protection à la connexion depuis un nouvel appareil.
- API d'organisation complète : partielle, pour le connecteur d'annuaire seulement.
- Peu probables à terme : rôles sur mesure, et les politiques « imposer l'authentification unique », « forcer l'expiration de session » et « bloquer l'export du coffre personnel ».
- Rapport de fuites par adresse courriel : demande une clé d'API Have I Been Pwned payante (HIBP_API_KEY). Les rapports de réutilisation et de faiblesse, eux, se calculent à partir du seul contenu du coffre.

Ce qu'il faut sauvegarder

db.sqlite3
Presque tout : entrées, usagers, organisations. Passer par la commande de sauvegarde SQLite ou VACUUM INTO, jamais une copie à chaud.

attachments/
Les pièces jointes des entrées. Rien d'autre ne les contient.

config.json
Les réglages, plus le jeton d'administration et les identifiants SMTP en clair. À chiffrer dès qu'il quitte la machine.

rsa_key.der / .pem / .pub.der
Signature des jetons de session. Les perdre déconnecte tout le monde et invalide les invitations. La clé privée qui fuit permet de forger une session d'administrateur.

sends/ et icon_cache/
Optionnels. Sauter le premier casse les Send existants après une restauration, le second se reconstruit seul.

> Le coffre est chiffré de bout en bout : une sauvegarde volée reste inexploitable, mais une sauvegarde perdue est définitive. Personne ne peut la déchiffrer, ni Bitwarden, ni l'hébergeur. Vérifier la restauration, pas le voyant vert.

Authentification unique (OIDC)

- Documentée officiellement, avec des exemples par fournisseur : Authentik, Keycloak, Microsoft Entra ID, Zitadel, Kanidm, Casdoor, Authelia, GitLab, Google, Rauthy, Slack. Auth0 est signalé non fonctionnel par le projet.

> Le mot de passe maître reste exigé et n'est pas géré par le fournisseur d'identité : la clé de déchiffrement du coffre en dérive. L'authentification unique retire une identité à gérer, pas un secret à taper.

- L'inscription est bloquée si le fournisseur déclare l'adresse courriel non vérifiée. Un changement d'adresse demande une action de l'usager.

Repères

Version
1.37.1, publiée le 29 juillet 2026. Licence AGPLv3 : l'héberger pour des usagers oblige à pouvoir leur remettre le code source.

Audits
BSI, programme CAOS, analyse statique et dynamique de la v1.30.3, rapports 2024. ERNW, octobre 2024, trois vulnérabilités dont un contournement d'authentification, corrigé en 1.32.5.

Documentation
github.com/dani-garcia/vaultwarden/wiki