Fiche Pratique N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous V1.1

7 nov, 2026 · @Gabriel

Objectif : *Installer et configurer* ***Vaultwarden*** *(serveur léger compatible Bitwarden) sur un serveur personnel (Raspberry Pi, vieux PC ou VPS) pour héberger vous-même votre gestionnaire de mots de passe, synchronisé entre tous vos appareils avec les applications Bitwarden.*

- ***Public visé :*** *Intermédiaire à avancé (quelques bases en ligne de commande sont nécessaires)*
- ***Temps estimé :*** *30 à 60 minutes*
- ***Difficulté :*** *★★★☆☆ (Moyen)*
- ***Prérequis :*** *un serveur (Raspberry Pi 3, 4 ou 5, vieux PC ou VPS), un nom de domaine, Docker (ou un serveur YunoHost)*
- ***Fiches associées :*** *N°16 (gestionnaires de mots de passe), N°18 (double authentification), N°20 (YunoHost), N°20a (WireGuard)*

1. Qu'est-ce que Vaultwarden ? Pourquoi l'auto-héberger ?

1.1. Bitwarden ou Vaultwarden

Critère	Bitwarden (officiel)	Vaultwarden
Nature	Service en ligne, ou serveur auto-hébergé officiel	Serveur alternatif, auto-hébergé, développé par une communauté indépendante
Ressources	Plusieurs conteneurs, environ 2 Go de RAM ou plus	Un seul conteneur, quelques dizaines de Mo de RAM, base SQLite
Installation	Plus lourde	Simple
Fonctions	Selon l'abonnement	La plupart des fonctions payantes de Bitwarden sont disponibles sans abonnement
Idéal pour	Particuliers (service en ligne) et entreprises	Particuliers, familles, petites associations

💡 **Vaultwarden** (anciennement « bitwarden_rs ») réimplémente le serveur Bitwarden en Rust, d'où sa légèreté. Il fonctionne avec les **applications Bitwarden officielles** (extension de navigateur, mobile, bureau). Il n'est pas affilié à la société Bitwarden.

1.2. Pourquoi auto-héberger ?

Avantage	Explication
Contrôle	Votre coffre chiffré est stocké sur votre serveur

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous V1.1

Avantage	Explication
Fonctions avancées sans abonnement	Authentificateur intégré, rapports, pièces jointes, accès d'urgence…
Léger	Fonctionne sur un Raspberry Pi
Partage familial	Organisations et partages sans limite de membres
Souveraineté	Vous choisissez où sont stockées vos données

Le risque : vous devenez responsable de la disponibilité, des mises à jour et des sauvegardes. Si le serveur est perdu sans sauvegarde, le coffre l'est aussi (les applications gardent toutefois une copie hors ligne, en lecture).

1.3. Ce que vous gagnez par rapport à Bitwarden gratuit

Fonction	Bitwarden gratuit	Bitwarden Premium (19,80 $/an depuis 2026)	Vaultwarden
Mots de passe et appareils	✅ Illimités	✅ Illimités	✅ Illimités
Partage	⚠️ Avec une seule autre personne	⚠️ Comme l'offre gratuite (familles : offre dédiée)	✅ Organisations sans limite
Authentificateur TOTP intégré	❌	✅	✅
Rapports (mots de passe faibles, réutilisés, fuites)	❌	✅	✅
Pièces jointes chiffrées	❌	✅	✅
Accès d'urgence	❌	✅	✅
Support	Communauté	Prioritaire	Communauté Vaultwarden

⚠️ Bitwarden gratuit n'est **pas** limité en nombre d'appareils : si vous ne voulez pas gérer de serveur, il reste une excellente option (fiche N°16).

2. Prérequis

2.1. Options matérielles

Solution	RAM	Coût	Recommandation
Raspberry Pi 3, 4 ou 5	1 Go ou plus	40 à 100 €	✅ Idéal à la maison, faible consommation

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous V1.1

Solution	RAM	Coût	Recommandation
Vieux PC	1 Go ou plus	0 € si vous l'avez déjà	✅ Consomme davantage
VPS (Infomaniak, Hetzner, OVHcloud)	1 Go	Quelques euros par mois	✅ Sans matériel chez vous
NAS (Synology, QNAP)	Selon le modèle	–	⚠️ Possible avec Docker (Container Manager)
Serveur YunoHost (fiche N°20)	–	–	✅ Le plus simple : Vaultwarden est dans le catalogue

2.2. Nom de domaine

- Un sous-domaine de votre domaine (exemple : pass.mondomaine.fr), acheté chez un registrar européen (fiche N°28) ;
- ou un domaine gratuit (DuckDNS, ou les domaines gratuits de YunoHost).

⚠️ **HTTPS est obligatoire :** le coffre web et les applications refusent de fonctionner correctement sans certificat valide.

3. Installation la plus simple : YunoHost

Si vous avez un serveur YunoHost (fiche N°20) :

1. **Applications** › **Installer** › **Vaultwarden**.
2. Choisissez un domaine dédié (exemple : pass.mondomaine.fr) et l'administrateur.
3. Lancez l'installation.

Vous devez voir :

- le coffre web de Vaultwarden à l'adresse choisie, en HTTPS.

YunoHost gère le certificat, les mises à jour et les sauvegardes.

4. Installation avec Docker

Étape 1 : Installez Docker

Installez Docker et le greffon Compose depuis le dépôt officiel de Docker (par exemple avec le script d'installation officiel) :

```
curl -fsSL https://get.docker.com | sudo sh
```

Vous devez voir :

- `docker compose version` qui affiche un numéro de version.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous V1.1

Étape 2 : Générez le jeton d'administration

```
docker run --rm -it vaultwarden/server /vaultwarden hash
```

Saisissez deux fois un mot de passe fort : la commande affiche une chaîne qui commence par `$argon2id$`. Copiez-la.

Étape 3 : Créez le fichier de configuration

```
mkdir -p ~/vaultwarden && cd ~/vaultwarden
nano .env
```

Contenu du fichier `.env` (les apostrophes protègent les caractères `$`) :

```
VW_ADMIN_TOKEN='$argon2id$v=19$m=65540,t=3,p=4$...'
```

Puis le fichier `docker-compose.yml` :

```
services:
  vaultwarden:
    image: vaultwarden/server:latest
    container_name: vaultwarden
    restart: unless-stopped
    ports:
      - "127.0.0.1:8080:80"
    volumes:
      - ./vw-data:/data
    environment:
      DOMAIN: "https://pass.mondomaine.fr"
      SIGNUPS_ALLOWED: "true"
      ADMIN_TOKEN: ${VW_ADMIN_TOKEN}
```

⚠️ Remplacez pass.mondomaine.fr par votre domaine.

Variable	Rôle
`DOMAIN`	Adresse publique de votre instance (doit correspondre au certificat HTTPS)
`SIGNUPS_ALLOWED`	Autorise la création de comptes : à passer à `false` après avoir créé les vôtres
`ADMIN_TOKEN`	Mot de passe (haché) du panneau d'administration `/admin`

La variable `WEBSOCKET_ENABLED` n'est plus nécessaire depuis Vaultwarden 1.29 : les notifications passent par le port principal.

Étape 4 : Démarrez Vaultwarden

```
docker compose up -d
```

Le port 8080 n'écoute que sur la machine elle-même (127.0.0.1) : l'accès se fait par le proxy HTTPS de l'étape suivante.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous V1.1

Étape 5 : Configurez le HTTPS (indispensable)

Option 1 : Caddy (le plus simple, certificat automatique)

```
sudo apt install caddy -y
```

Contenu de `/etc/caddy/Caddyfile` :

```
pass.mondomaine.fr {
  reverse_proxy 127.0.0.1:8080
}
```

```
sudo systemctl reload caddy
```

Option 2 : Nginx + Certbot

```
sudo apt install nginx certbot python3-certbot-nginx -y
```

Contenu de `/etc/nginx/sites-available/vaultwarden` :

```
server {
  listen 80;
  server_name pass.mondomaine.fr;
  client_max_body_size 525M;
  location / {
    proxy_pass http://127.0.0.1:8080;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
  }
}
```

```
sudo ln -s /etc/nginx/sites-available/vaultwarden /etc/nginx/sites-enabled/
sudo nginx -t && sudo systemctl reload nginx
sudo certbot --nginx -d pass.mondomaine.fr
```

Étape 6 : Créez votre compte

1. Rendez-vous sur https://pass.mondomaine.fr.
2. Cliquez sur **Créer un compte** et choisissez un **mot de passe principal** très fort (phrase de passe de 5 mots ou plus). Notez-le sur papier, rangé en lieu sûr : il ne peut pas être récupéré.
3. Créez de même les comptes de vos proches.
4. Désactivez les inscriptions : passez `SIGNUPS_ALLOWED` à `"false"`, puis :

```
docker compose up -d
```

Vous devez voir :

- votre coffre vide ; la page de création de compte refuse ensuite les nouvelles inscriptions.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous V1.1

5. Le panneau d'administration

Le panneau est accessible sur https://pass.mondomaine.fr/admin, avec le mot de passe choisi à l'étape 2 (pas avec votre compte utilisateur).

Il permet de :

- voir les comptes et les organisations ;
- inviter des utilisateurs (si l'envoi d'emails est configuré) ;
- modifier certains réglages et consulter l'état du serveur.

⚠️ Les réglages enregistrés depuis le panneau priment ensuite sur les variables d'environnement.

6. Connecter les applications Bitwarden à votre serveur

Sur toutes les applications Bitwarden, le choix du serveur se fait sur l'**écran de connexion**.

6.1. Extension de navigateur

1. Installez l'extension **Bitwarden** (Firefox, Chrome, Edge, Brave, Safari).
2. Sur l'écran de connexion, ouvrez le menu **Connexion sur** (bitwarden.com par défaut) › **Auto-hébergé**.
3. Saisissez https://pass.mondomaine.fr et enregistrez.
4. Connectez-vous avec votre email et votre mot de passe principal.

6.2. Application de bureau

1. Téléchargez **Bitwarden** pour Windows, macOS ou Linux sur bitwarden.com › **Télécharger**.
2. Sur l'écran de connexion : **Connexion sur** › **Auto-hébergé** › https://pass.mondomaine.fr.
3. Connectez-vous.

6.3. Android

1. Installez **Bitwarden** depuis Google Play, ou depuis le dépôt F-Droid de Bitwarden (à ajouter dans F-Droid).
2. Sur l'écran de connexion : **Connexion sur** › **Auto-hébergé** › https://pass.mondomaine.fr.
3. Connectez-vous, puis activez le **remplissage automatique** dans les réglages d'Android.

6.4. iPhone

1. Installez **Bitwarden** depuis l'App Store.
2. Même réglage sur l'écran de connexion (**Auto-hébergé**).
3. Activez le remplissage automatique : **Réglages** › **Général** › **Remplissage automatique et mots de passe** › **Bitwarden**.

Vous devez voir :

gabriel.ananda@mailo.com
CC BY SA

- sur chaque appareil, le même coffre, avec la mention de votre serveur dans les paramètres du compte.

7. Fonctions avancées

7.1. Rapports sur vos mots de passe

1. Dans le coffre web, ouvrez **Rapports**.
2. Lancez les rapports **Mots de passe exposés** (vérification auprès de Have I Been Pwned, sans envoyer vos mots de passe), **réutilisés** et **faibles**.
3. Changez en priorité les mots de passe exposés et réutilisés.

7.2. Authentificateur TOTP intégré

1. Ouvrez un identifiant dans le coffre et modifiez-le.
2. Collez la clé secrète TOTP du site (ou scannez le QR code depuis l'application mobile).
3. Enregistrez : le code à 6 chiffres s'affiche et se copie lors du remplissage.

💡 Pratique, mais vos mots de passe et vos seconds facteurs sont alors au même endroit. Pour les comptes les plus sensibles (email principal, banque), gardez un authentificateur séparé comme Aegis ou Ente Auth (fiche N°18).

7.3. Partager avec votre famille

1. Dans le coffre web : **Nouvelle organisation**.
2. Invitez les membres (ou ajoutez-les s'ils ont déjà un compte sur votre serveur).
3. Créez des **collections** (exemple : « Maison », « Banque ») et attribuez-les.

7.4. Double authentification sur votre compte

1. Coffre web › **Paramètres** › **Sécurité** › **Connexion en deux étapes**.
2. Activez **Application d'authentification** et scannez le QR code avec Aegis ou Ente Auth.
3. Rangez le **code de récupération** en lieu sûr.

8. Sauvegarde et restauration

Le dossier `vw-data` contient tout : la base `db.sqlite3`, les pièces jointes, les envois et les clés.

8.1. Sauvegarde manuelle

```
cd ~/vaultwarden
docker compose stop
tar -czf vaultwarden-$(date +%Y%m%d).tar.gz ./vw-data
docker compose start
```


gabriel.ananda@mailo.com
CC BY SA

8.2. Sauvegarde automatique (tous les jours à 3 h)

```
crontab -e
# Ligne à ajouter (le signe % doit être échappé dans crontab) :
0 3 * * * cd /home/votrenom/vaultwarden && docker compose stop && tar
-czf /sauvegardes/vaultwarden-$(date +\%Y\%m\%d).tar.gz ./vw-data && docker
compose start
```

Copiez ensuite les archives **hors du serveur** (disque externe, NAS, stockage européen chiffré : fiches N°19 et N°31).

8.3. Restauration

```
cd ~/vaultwarden
docker compose down
mv vw-data vw-data.ancien
tar -xzf vaultwarden-AAAAMMJJ.tar.gz
docker compose up -d
```

Testez une restauration au moins une fois, sur une autre machine si possible.

Filet de sécurité supplémentaire : exportez régulièrement votre coffre depuis le coffre web (**Outils** › **Exporter le coffre**, au format **.json chiffré**) et rangez l'export hors ligne.

9. Sécuriser votre instance

Action	Pourquoi
HTTPS obligatoire	Protège les échanges et permet le fonctionnement du coffre web
`SIGNUPS_ALLOWED=false` après la création des comptes	Empêche des inconnus de créer des comptes
Jeton d'administration haché (argon2)	Protège le panneau `/admin`
Mises à jour régulières : `docker compose pull && docker compose up -d`	Corrige les failles
Double authentification sur chaque compte	Protège même si un mot de passe principal fuit
Accès limité : réseau local + VPN WireGuard (fiche N°20a)	Ne pas exposer le serveur sur Internet si vous n'en avez pas besoin
Sauvegardes hors du serveur	Protège contre la perte du serveur

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous V1.1

10. Dépannage

Symptôme	Cause possible	Action
Le coffre web affiche une erreur liée au chiffrement	Accès sans HTTPS	Passez par https://pass.mondomaine.fr
L'application refuse de se connecter	Mauvaise adresse de serveur, ou certificat invalide	Vérifiez le réglage **Auto-hébergé** et le certificat dans un navigateur
Avertissement « plain text ADMIN_TOKEN »	Jeton non haché, ou réglages enregistrés depuis le panneau	Utilisez un jeton haché (étape 2)
Les changements n'apparaissent pas tout de suite sur les autres appareils	Notifications bloquées par le proxy	Vérifiez les en-têtes `Upgrade` et `Connection` (Nginx)
Avertissement Compose sur des variables non définies	Les $ du jeton haché sont interprétés	Utilisez le fichier `.env` avec des apostrophes, ou doublez chaque $

11. À savoir avant de se lancer

Crainte fréquente	La réalité
« Je ne suis pas assez technique. »	Avec YunoHost, l'installation est guidée. Sinon, Bitwarden gratuit (appareils illimités) reste une excellente option.
« Si mon serveur tombe en panne, je perds tout. »	Les applications gardent une copie hors ligne du coffre, et vos sauvegardes permettent de restaurer le serveur.
« C'est risqué d'exposer mon gestionnaire sur Internet. »	Le coffre est chiffré de bout en bout, mais limitez la surface d'attaque : HTTPS, double authentification, mises à jour, ou accès par VPN uniquement.
« Combien ça consomme ? »	Un Raspberry Pi (environ 5 W) consomme autour de 45 kWh par an, soit une dizaine d'euros ; un vieux PC bien davantage.
« Je ne veux pas gérer de serveur. »	Bitwarden (gratuit ou Premium) ou Proton Pass (fiche N°16).

12. Challenge 7 jours

Challenge : pendant 7 jours, utilisez uniquement votre instance Vaultwarden pour vos mots de passe.

- **Jour 1 :** installez Vaultwarden (YunoHost ou Docker).
- **Jour 2 :** configurez HTTPS, créez votre compte, désactivez les inscriptions.

gabriel.ananda@mailo.com
CC BY SA

- **Jour 3 :** installez l'extension de navigateur et connectez-la à votre serveur.
- **Jour 4 :** importez vos mots de passe depuis votre ancien gestionnaire ou votre navigateur (coffre web › **Outils** › **Importer des données**).
- **Jour 5 :** installez l'application mobile et activez le remplissage automatique.
- **Jour 6 :** activez la double authentification et lancez les rapports.
- **Jour 7 :** supprimez les mots de passe enregistrés dans votre navigateur et faites une première sauvegarde.

Vous allez constater :

- votre coffre est synchronisé sur tous vos appareils, depuis votre serveur ;
- vous disposez des fonctions avancées sans abonnement.

13. Alternatives et approfondissements

Si vous avez besoin de…	Essayez plutôt…
Une solution sans serveur à gérer	**Bitwarden** (gratuit, appareils illimités)
Une solution sans serveur, déjà chez Proton	**Proton Pass**
Une solution hors ligne (fichier local)	**KeePassXC** / **KeePassDX** (fiche N°16), synchronisé avec Syncthing (fiche N°29)
Une solution pour une entreprise	**Bitwarden** auto-hébergé officiel, ou offres professionnelles
Une clé physique	**YubiKey** ou **Nitrokey** comme second facteur, avec Vaultwarden (WebAuthn) ou KeePassXC

14. En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Installer **Vaultwarden**	Gestionnaire auto-hébergé, fonctions avancées sans abonnement	Sections 3 et 4
Configurer **HTTPS**	Échanges protégés, coffre web fonctionnel	Étape 5
Désactiver les **inscriptions**	Aucun inconnu sur votre serveur	Étape 6
Activer la **double authentification**	Coffre protégé même en cas de fuite du mot de passe	Section 7.4
Sauvegarder `vw-data` hors du serveur	Vous ne perdez jamais vos mots de passe	Section 8

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°35 : Vaultwarden, auto-hébergement de Bitwarden – Votre gestionnaire de mots de passe chez vous V1.1

15. Conclusion

Si vous êtes…	Choisissez…
Particulier qui veut auto-héberger	Vaultwarden sur YunoHost ou Raspberry Pi
Particulier qui ne veut pas gérer de serveur	Bitwarden (gratuit)
Très exigeant, sans serveur	KeePassXC (fichier local chiffré)
Déjà chez Proton	Proton Pass
Famille ou petite association	Vaultwarden, avec une organisation partagée

À retenir absolument

- **Vaultwarden est léger et compatible avec les applications Bitwarden officielles.**
- **Bitwarden gratuit n'est pas limité en appareils :** Vaultwarden apporte surtout l'auto-hébergement et les fonctions avancées.
- **HTTPS, double authentification et inscriptions fermées** sont indispensables.
- **Sauvegardez `vw-data` hors du serveur** et testez la restauration.

Test final :

1. Vaultwarden accessible en HTTPS sur https://pass.mondomaine.fr.
2. Votre compte créé, inscriptions désactivées.
3. Extension de navigateur connectée à votre serveur.
4. Application mobile connectée à votre serveur.
5. Un mot de passe ajouté sur l'ordinateur, visible sur le téléphone.
6. Double authentification activée.
7. Sauvegarde de `vw-data` effectuée et copiée hors du serveur.
8. Si tout fonctionne : vous avez votre propre gestionnaire de mots de passe auto-hébergé ✅

Références

- Vaultwarden – Wiki : activer la page d'administration (ADMIN_TOKEN haché avec argon2)
- Forum Vaultwarden – WEBSOCKET_ENABLED n'est plus nécessaire depuis la version 1.29.0
- PricingSaaS – Bitwarden Premium passe à 19,80 $ par an (2026)
- Costbench – Offre gratuite de Bitwarden (appareils et mots de passe illimités)
- Bitwarden – Dépôt F-Droid officiel

gabriel.ananda@mailo.com
CC BY SA