

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

**Objectif** : Installer et configurer **Vaultwarden** (alternative légère à Bitwarden) sur un serveur personnel (Raspberry Pi, vieux PC, ou VPS) pour héberger votre propre gestionnaire de mots de passe, sans dépendre des serveurs Bitwarden, avec synchronisation gratuite et illimitée entre tous vos appareils.

**Public visé** : Intermédiaire à Avancé (quelques bases en ligne de commande sont nécessaires)

**Temps estimé** : 30 à 60 minutes

**Niveau de difficulté** : ★★★☆☆ (Moyen)

### Prérequis :

- Un serveur dédié (Raspberry Pi 3/4/5, vieux PC, ou VPS loué)
- Un nom de domaine (ou un sous-domaine gratuit)
- Docker et Docker Compose installés

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

### 1.1 Bitwarden vs Vaultwarden

	Bitwarden officiel	Vaultwarden
<b>Nature</b>	Service cloud (ou auto-hébergement lourd)	Alternative légère, auto-hébergée
<b>Ressources</b>	Nécessite 2-4 Go RAM + SQL Server	Moins de 100 Mo RAM + SQLite

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

	Bitwarden officiel	Vaultwarden
<b>Installation</b>	Complexe (Docker multi-conteneurs)	Simple (un seul conteneur)
<b>Fonctionnalités</b>	Toutes (gratuites et payantes)	<b>Toutes les fonctionnalités sont gratuites</b> (Premium inclus)
<b>Idéal pour</b>	Entreprises, auto-hébergement lourd	Particuliers, petits groupes, Raspberry Pi

💡 **Vaultwarden** (anciennement Bitwarden\_RS) est une implémentation alternative du serveur Bitwarden, écrite en Rust (donc très légère). Elle est **100% compatible** avec les applications Bitwarden officielles (extension navigateur, mobile, desktop).

### 1.2 Pourquoi auto-héberger Vaultwarden ?

Avantage	Explication
<b>Contrôle total</b>	Vos mots de passe ne quittent jamais votre serveur
<b>Gratuit (Premium inclus)</b>	Pas d'abonnement Bitwarden Premium (10 \$/an) – toutes les fonctionnalités sont disponibles
<b>Léger</b>	Fonctionne sur un Raspberry Pi 3 (512 Mo RAM)
<b>Synchronisation illimitée</b>	Autant d'appareils que vous voulez, sans limitation
<b>Souveraineté</b>	Vous choisissez où vos données sont stockées

### 1.3 Fonctionnalités Premium incluses (gratuites avec Vaultwarden)

Fonctionnalité	Bitwarden gratuit	Bitwarden Premium	Vaultwarden
Stockage illimité	✓	✓	✓

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

Fonctionnalité	Bitwarden gratuit	Bitwarden Premium	Vaultwarden
2 appareils max	⚠ 2	✓ illimité	✓ illimité
Vérification de fuite (HIBP)	✗	✓	✓
Authentificateur TOTP intégré	✗	✓	✓
Partage avec d'autres utilisateurs	✗	✓	✓
Gestionnaire d'identités	✗	✓	✓
Priorité support	✗	✓	✓

## 2. Prérequis matériels

### 2.1 Options matérielles

Solution	RAM minimale	Coût	Recommandation
Raspberry Pi 3/4/5	512 Mo	30-80 €	✓ <b>Idéal</b> – faible consommation
Vieux PC	1 Go	0 € (si déjà possédé)	✓ Très bien (consomme plus)
VPS (Infomaniak, Hetzner, OVH)	1 Go	3-6 €/mois	✓ Bonne option sans matériel
NAS (Synology, QNAP)	1 Go	200-500 €	⚠ Possible mais plus complexe

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

### 2.2 Recommandation débutant

**Chez soi** : Raspberry Pi 3/4 + carte microSD (16 Go) + Docker.

**En ligne** : VPS chez Infomaniak (Suisse, 5 €/mois) ou Hetzner (Allemagne, 4 €/mois).

### 2.3 Nom de domaine

- Achetez un nom de domaine (ex: `pass.mondomaine.fr`) chez Gandi, Infomaniak, Netim (5-15 €/an)
  - **Ou** utilisez un sous-domaine gratuit (ex: DuckDNS : `vaultwarden.duckdns.org`)
- 

## 3. Installation de Vaultwarden avec Docker

### 3.1 Étape 1 : Installer Docker

*# Sur Debian/Ubuntu (Raspberry Pi, vieux PC, VPS)*

```
sudo apt update
sudo apt install docker.io docker-compose -y
sudo systemctl enable docker
sudo systemctl start docker
```

### 3.2 Étape 2 : Créer le fichier docker-compose.yml

```
mkdir ~/vaultwarden
cd ~/vaultwarden
nano docker-compose.yml
```

Contenu du fichier :

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

yaml

version: '3'

services:

vaultwarden:

image: vaultwarden/server:latest

container\_name: vaultwarden

restart: unless-stopped

ports:

- "8080:80"

volumes:

- ./vw-data:/data

environment:

- DOMAIN=https://pass.mondomaine.fr

- SIGNUPS\_ALLOWED=true

- INVITATIONS\_ALLOWED=false

- WEBSOCKET\_ENABLED=true

- ADMIN\_TOKEN=unmotdepassefort\_pour\_admin

⚠ Remplacez :

- pass.mondomaine.fr par votre vrai nom de domaine
- unmotdepassefort\_pour\_admin par un mot de passe très fort (accès au panneau d'administration)

### Explication des variables :

Variable	Rôle
DOMAIN	URL de votre instance (doit correspondre au certificat SSL)
SIGNUPS_ALLOWED	Permet la création de nouveaux comptes (mettez false après avoir créé votre compte)
WEBSOCKET_ENABLED	Active les notifications push
ADMIN_TOKEN	Mot de passe pour accéder au panneau d'administration (optionnel mais recommandé)

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

### 3.3 Étape 3 : Démarrer Vaultwarden

```
docker-compose up -d
```

Vaultwarden est maintenant accessible sur `http://adresse_ip:8080`.

### 3.4 Étape 4 : Configurer le HTTPS (SSL) – indispensable

Pour sécuriser vos mots de passe, vous devez absolument ajouter un certificat SSL.

#### Option 1 : Avec Nginx (recommandé)

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

Créez un fichier de configuration Nginx (`/etc/nginx/sites-available/vaultwarden`) :

```
nginx
server {
    listen 80;
    server_name pass.mondomaine.fr;
    location / {
        proxy_pass http://localhost:8080;
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
    }
}
```

Activez le site :

```
bash
sudo ln -s /etc/nginx/sites-available/vaultwarden /etc/nginx/sites-enabled/
sudo nginx -t
```

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

```
sudo systemctl reload nginx
```

Obtenez le certificat SSL :

```
bash
```

```
sudo certbot --nginx -d pass.mondomaine.fr
```

### Option 2 : Avec Caddy (plus simple, tout automatique)

```
bash
```

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

Créez `/etc/caddy/Caddyfile` :

```
text
```

```
pass.mondomaine.fr {  
    reverse_proxy localhost:8080  
}  
bash
```

```
sudo systemctl enable caddy
```

```
sudo systemctl start caddy
```

Caddy gère automatiquement le SSL Let's Encrypt.

### 3.5 Étape 5 : Accéder à Vaultwarden

- Rendez-vous sur `https://pass.mondomaine.fr`
- Créez votre compte (la première inscription crée l'administrateur)
- Connectez-vous

💡 **Après avoir créé votre compte** : modifiez le `docker-compose.yml` pour désactiver les nouvelles inscriptions (`SIGNUPS_ALLOWED=false`), puis redémarrez : `docker-compose down && docker-compose up -d`

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

### 4. Accéder au panneau d'administration

Si vous avez défini `ADMIN_TOKEN`, le panneau d'administration est accessible sur <https://pass.mondomaine.fr/admin>.

Ce panneau vous permet de :

- Voir les statistiques d'utilisation
- Inviter des utilisateurs (si activé)
- Voir les logs
- Gérer les invitations



**Sécurité** : Protégez cet accès avec un mot de passe très fort.

---

### 5. Configurer les clients Bitwarden pour utiliser Vaultwarden

#### 5.1 Sur ordinateur (extension navigateur)

1. Installez l'extension **Bitwarden** depuis les stores (Chrome, Firefox, Edge, Brave)
2. Cliquez sur l'icône de l'extension
3. Cliquez sur "**Modifier**" à côté de l'URL du serveur
4. Entrez <https://pass.mondomaine.fr>
5. Connectez-vous avec votre email et mot de passe

#### 5.2 Sur ordinateur (application de bureau)

1. Téléchargez **Bitwarden Desktop** depuis <https://bitwarden.com/download/>
2. Lancez l'application
3. Cliquez sur "**Paramètres**" → "**Se connecter**"
4. Cliquez sur "**Changer de serveur**"

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

5. Entrez <https://pass.mondomaine.fr>
6. Connectez-vous

### 5.3 Sur Android

1. Installez **Bitwarden** depuis **F-Droid** (recommandé) ou Aurora Store
2. Lancez l'application
3. Cliquez sur les trois traits (menu) → "**Paramètres**"
4. Sous "**Gestion de compte**" → "**Changer de serveur**"
5. Entrez <https://pass.mondomaine.fr>
6. Connectez-vous

### 5.4 Sur iOS (iPhone)

1. Installez **Bitwarden** depuis l'App Store
  2. Lancez l'application
  3. Tapez sur les trois traits → "**Paramètres**"
  4. "**Changer de serveur**" → entrez <https://pass.mondomaine.fr>
  5. Connectez-vous
- 

## 6. Fonctionnalités avancées (gratuites avec Vaultwarden)

### 6.1 Activer la vérification de fuite de mots de passe (Have I Been Pwned)

1. Connectez-vous à votre web vault (<https://pass.mondomaine.fr>)
2. Allez dans "**Outils**" → "**Vérification de fuite de données**"
3. Cliquez sur "**Vérifier vos mots de passe**"

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

### 6.2 Activer l'authentificateur TOTP intégré

1. Dans le web vault, allez dans un élément de connexion
2. Cliquez sur **"Ajouter une nouvelle clé d'authentification"**
3. Scannez le QR code ou entrez la clé secrète

💡 Cela remplace des applications comme Aegis, mais attention : vos codes TOTP sont alors stockés dans Vaultwarden. Si vous perdez l'accès à votre serveur, vous perdez aussi vos codes. Pour une sécurité optimale, gardez un authentificateur séparé.

### 6.3 Activer le partage (organisation)

1. Dans le web vault, allez dans **"Organisations"**
2. Créez une organisation (gratuite, illimitée)
3. Invitez d'autres utilisateurs
4. Créez des collections partagées

### 6.4 Activer les notifications push (WebSocket)

Vaultwarden supporte les notifications push. Si vous avez activé `WEBSOCKET_ENABLED=true` et configuré Nginx/Caddy, les changements sur un appareil sont immédiatement synchronisés.

---

## 7. Sauvegarde et restauration

### 7.1 Sauvegarde manuelle

```
cd ~/vaultwarden
docker-compose down
```

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

```
tar -czf vaultwarden-backup-$(date +%Y%m%d).tar.gz ./vw-data
docker-compose up -d
```

### 7.2 Sauvegarde automatique avec cron (quotidienne)

```
crontab -e
```

# Ajouter :

```
0 3 * * * cd /home/votrenom/vaultwarden && docker-compose down && tar -czf /backup/vaultwarden-$(date +%Y%m%d).tar.gz ./vw-data && docker-compose up -d
```

### 7.3 Restauration

```
cd ~/vaultwarden
```

```
docker-compose down
```

```
rm -rf ./vw-data
```

```
tar -xzf vaultwarden-backup-YYYYMMDD.tar.gz
```

```
docker-compose up -d
```

💡 **Astuce** : Envoyez vos sauvegardes vers un second disque dur ou un cloud chiffré (Backblaze B2, Wasabi).

## 8. Sécuriser son instance Vaultwarden

Action	Pourquoi
HTTPS obligatoire	Chiffre les communications
Désactiver SIGNUPS_ALLOWED après création	Empêche des inconnus de créer des comptes
Utiliser un mot de passe administrateur fort (ADMIN_TOKEN)	Protège le panneau d'administration
Mettre à jour régulièrement	<code>docker-compose pull &amp;&amp; docker-compose up -d</code>

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

Action	Pourquoi
Activer la 2FA sur votre compte Bitwarden	Protection supplémentaire
Sauvegarder régulièrement	Protection contre la perte de données

### 9. Tableau récapitulatif

Action	Bénéfice
Installer Vaultwarden sur Raspberry Pi	Gestionnaire de mots de passe auto-hébergé, toutes fonctionnalités gratuites
Configurer HTTPS (Nginx ou Caddy)	Sécurise vos mots de passe pendant le transfert
Désactiver SIGNUPS_ALLOWED	Bloque la création de comptes par des inconnus
Activer la 2FA sur son compte	Sécurise l'accès à tous vos mots de passe
Sauvegarder le dossier vw-data	Permet de restaurer ses mots de passe en cas de panne

### 10. À savoir avant de se lancer

Crainte fréquente	La réalité
"Je ne suis pas assez technique"	L'installation avec Docker est simple si vous suivez les étapes. Sinon, utilisez Bitwarden officiel (gratuit, 2 appareils).
"Si mon serveur tombe en panne, je perds tous mes mots de passe."	Faites des <b>sauvegardes régulières</b> (voir section 7).

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

Crainte fréquente	La réalité
"C'est risqué d'ouvrir mon gestionnaire de mots de passe sur Internet."	Avec HTTPS + 2FA + mises à jour, le risque est maîtrisable. Pour les plus paranoïaques, n'ouvrez que sur le réseau local (pas d'accès externe).
"Ça consomme combien en électricité ?"	Sur Raspberry Pi : environ 5W → 5 €/an. Sur vieux PC : 50-100W → 50-100 €/an.
"Je préfère ne pas gérer de serveur."	Utilisez <b>Bitwarden officiel</b> (gratuit pour 2 appareils) ou <b>Proton Pass</b> .

### 11. Challenge 7 jours

**Challenge** : Pendant 7 jours, utilisez **uniquement** votre instance Vaultwarden personnelle pour tous vos mots de passe.

**Jour 1** : Installez Vaultwarden sur Raspberry Pi ou VPS

**Jour 2** : Configurez HTTPS et désactivez SIGNUPS\_ALLOWED

**Jour 3** : Installez l'extension Bitwarden sur votre navigateur et connectez-vous

**Jour 4** : Importez vos mots de passe depuis votre ancien gestionnaire

**Jour 5** : Installez l'application Bitwarden sur votre téléphone

**Jour 6** : Activez la 2FA sur votre compte Vaultwarden

**Jour 7** : Supprimez les mots de passe de votre navigateur (Chrome/Edge/Firefox)

**À la fin** : Vous aurez votre propre gestionnaire de mots de passe auto-hébergé, avec toutes les fonctionnalités Premium gratuites.

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

### 12. Alternatives et approfondissements

Si vous avez besoin de...	Essayez plutôt...
Une solution sans serveur à gérer	<b>Bitwarden officiel</b> (gratuit, 2 appareils)
Une solution sans serveur, multi-appareils	<b>Proton Pass</b> (1 Go gratuit, mais sans auto-hébergement)
Une solution hors ligne (fichier local)	<b>KeePass</b> (fiche N°16)
Une gestion d'entreprise	<b>Bitwarden officiel</b> (auto-hébergement lourd)
Une clé physique (sans serveur)	<b>YubiKey</b> + KeepassXC

### 13. En résumé – ce que vous gagnez

Action	Bénéfice
Installer <b>Vaultwarden</b>	Gestionnaire de mots de passe auto-hébergé, toutes fonctionnalités Premium gratuites
Configurer <b>HTTPS</b>	Mots de passe sécurisés sur le réseau
Désactiver <b>SIGNUPS_ALLOWED</b>	Empêche les intrus de créer des comptes
Activer <b>2FA</b>	Sécurité renforcée de votre coffre
<b>Sauvegarder</b>	Évite la perte définitive de vos mots de passe

## Fiche Pratique N°35 : Vaultwarden : Auto-hébergement Bitwarden – Votre gestionnaire de mots de passe, chez vous V1.0

### 14. Conclusion

Si vous êtes...	Choisissez...
Particulier, veut auto-héberger	<b>Vaultwarden</b> sur Raspberry Pi (léger, efficace)
Particulier, ne veut pas gérer de serveur	<b>Bitwarden officiel</b> (gratuit, 2 appareils)
Exigeant / paranoïde	<b>KeePass</b> (fichier local, hors ligne)
Déjà chez Proton	<b>Proton Pass</b>
Plusieurs utilisateurs (famille)	<b>Vaultwarden</b> (toutes fonctionnalités gratuites)

#### À retenir absolument :

- **Vaultwarden** est une pépite : léger, gratuit, toutes fonctionnalités Premium incluses.
- Il est **100% compatible** avec les applications Bitwarden officielles.
- **Sauvegardez votre dossier vw-data** – sans lui, plus jamais de mots de passe.
- **N'ouvrez pas votre instance sur Internet sans HTTPS et 2FA.**

#### Test final :

1. ☒ Vaultwarden installé et accessible via <https://pass.mondomaine.fr>
2. ☒ Un compte créé (le vôtre)
3. ☒ SIGNUPS\_ALLOWED désactivé après inscription
4. ☒ Extension navigateur Bitwarden connectée à votre serveur
5. ☒ Application mobile Bitwarden connectée à votre serveur
6. ☒ Un mot de passe ajouté, visible sur tous les appareils
7. ☒ Sauvegarde du dossier `vw-data` effectuée

Si tout fonctionne : **vous avez votre propre gestionnaire de mots de passe auto-hébergé, gratuit et illimité** ☒