VaultWarden

Vaultwarden (anciennement appelé *bitwarden_rs*) est une version légère, auto-hébergeable et compatible de Bitwarden, un gestionnaire de mots de passe open source. Il permet de stocker, organiser et partager des mots de passe en toute sécurité, via une interface web ou une application mobile.

Vaultwarden est conçu pour être simple à déployer, même sur des machines avec peu de ressources.

Présentation

Qu’est-ce que Vaultwarden ?

Vaultwarden (anciennement appelé *bitwarden_rs*) est une version légère, auto-hébergeable et compatible de Bitwarden, un gestionnaire de mots de passe open source. Il permet de stocker, organiser et partager des mots de passe en toute sécurité, via une interface web ou une application mobile.

Vaultwarden est conçu pour être simple à déployer, même sur des machines avec peu de ressources.

À quoi sert Vaultwarden ?

Vaultwarden permet de centraliser tous ses mots de passe et informations sensibles dans un coffre-fort chiffré. L’objectif est de ne plus avoir à mémoriser de nombreux mots de passe complexes, tout en améliorant la sécurité.

Il est utilisé autant par des particuliers que des équipes ou entreprises pour stocker, retrouver et partager des identifiants de manière sécurisée.

Comment fonctionne Vaultwarden ?

Vaultwarden fonctionne comme un serveur web accessible depuis un navigateur ou une application Bitwarden officielle. Il héberge un coffre-fort chiffré que seul l’utilisateur peut déchiffrer avec son mot de passe maître.

Toutes les données sont chiffrées côté client, ce qui signifie que même l’administrateur du serveur n’a pas accès aux mots de passe.

Pourquoi utiliser Vaultwarden ?

Vaultwarden est particulièrement apprécié pour sa légèreté, sa simplicité de mise en place, et sa compatibilité avec les clients Bitwarden. Il est idéal pour ceux qui souhaitent une solution privée et sécurisée, sans passer par le service cloud officiel.

C’est une alternative efficace et économique pour gérer ses mots de passe soi-même, tout en gardant la compatibilité avec les outils Bitwarden.

Cas d’usage courants

Vaultwarden est utilisé pour :

- Stocker des mots de passe, notes sécurisées, identifiants bancaires, etc.,
- Organiser ses mots de passe en collections ou dossiers,
- Partager des accès de manière sécurisée avec d’autres utilisateurs,
- Centraliser l’authentification dans une équipe ou un foyer,
- Intégrer un gestionnaire de mots de passe à d’autres services via API.

En résumé

Vaultwarden est une solution simple, sécurisée et auto-hébergeable pour gérer ses mots de passe. Compatible avec Bitwarden, léger à déployer, il permet de garder le contrôle total de ses données sensibles.

Installation

Fichier docker-compose

Dans cette procédure, nous allons utiliser **Docker**. Une documentation préalable à ce sujet est disponible ici.
Commençons par créer un fichier `docker-compose.yaml`, adapté à nos besoins :

```
services:
  vaultwarden:
    image: vaultwarden/server:latest  # Utilise l'image officielle Vaultwarden, en dernière version disponible
    container_name: vaultwarden       # Nomme explicitement le conteneur pour faciliter son identification
    restart: always                   # Redémarre automatiquement le conteneur en cas de crash ou redémarrage de l'hôte

    ports:
      - "82:80"                       # Expose l'interface HTTP sur le port 82 de la machine (interne 80)
      - "4443:443"                   # Expose l'interface HTTPS sur le port 4443 de la machine (interne 443)

    volumes:
      - /vw-data:/data               # Monte le dossier /data du conteneur (où sont stockées les données) dans /vw-data de l'hôte

    environment:
      - ROCKET_PROFILE=release       # Active le mode production pour de meilleures performances
      - ROCKET_ADDRESS=0.0.0.0       # Écoute sur toutes les interfaces réseau disponibles
```

```
      - ROCKET_PORT=80               # Définit le port HTTP interne à 80
      - DEBIAN_FRONTEND=noninteractive  # Supprime les interactions lors des mises à jour système (bonne pratique en conteneur)
      - ADMIN_TOKEN=<clé>            # Jeton d'administration haché permettant l'accès à l'interface d'administration Vaultwarden

    command: ["/start.sh"]            # Démarre le script de lancement officiel du conteneur

    healthcheck:
      test: ["CMD", "/healthcheck.sh"]  # Vérifie la santé du conteneur via un script toutes les 60 secondes
      interval: 60s
      timeout: 10s
```

Pour obtenir la clé "ADMIN_TOKEN", c'est très simple, on génère une clé SSL :

```
openssl rand -base64 48
```

cela renvoi un résultat similaire à cela :

```
mjLUlEhDYJr1kxJqGWkkc1qUCpqV3aektjfbGFSNbZwuE+2+GDhvyLZhnAfEdhW9
```

Démarrage

Une fois le fichier `docker-compose.yaml` créé, nous pouvons **lancer VaultWarden** avec la commande suivante :

```
docker compose up -d
```

Settings

Avant propos

Une fois Vaultwarden installé, on peut se rendre sur l'adresse, et comme nous avons enregistré une variable ADMIN_TOKEN, le panel d'administration est activé.
Pour s'y rendre il s'uffit d'ajouter /admin enfin d'URL : https://<domaine>/admin
Une fois sur le panel d'admin, il va falloir définir un mot de passe, et le hash avec argon2, installable sur Linux via :

```
apt update
apt install -y argon2
```

Puis ont hash le mot de passe voulu :

```
echo -n "Mot de Passe" | argon2 "$(openssl rand -base64 32)" -e -id -k 65540 -t 3 -p 4
```

Ce qui nous renvoit alors :

```
$argon2id$v=19$m=65540,t=3,p=4$YWdQV0pURXNQMnhhWXhFZTNMUUkyNXZKRXdmcGdqQnBnR1E0UFAzK2FPTT0$+Gz
htE21VtpcR/NW3re4m6DgUDq/GX0pX2ssTg+4YY0
```

On entre le résultat dans le champs "Admin token/Argon2 PHC" de la section "General Settings" et on oublie pas de cliquer sur "Save" en bas de page.

Voila, l'accès au panel d'administration est sécurisé par un mot de passe !

Les sections de Settings

General settings

Cette section permet de définir le comportement global de Vaultwarden. Elle agit comme le cœur de la configuration de ton service.

- **Domain URL** : C'est l'adresse publique à laquelle tes utilisateurs accèdent à Vaultwarden. Elle est aussi utilisée pour les liens envoyés par mail (réinitialisation, invitations...).
- **Allow Sends** : Permet aux utilisateurs de créer des *Sends*, c'est-à-dire des partages sécurisés de texte ou de fichiers. Cela peut être désactivé si tu veux limiter cette fonctionnalité.
- **HIBP API Key** : Si tu renseignes une clé API de Have I Been Pwned, Vaultwarden pourra alerter les utilisateurs si leurs mots de passe ont fuité dans des bases de données compromises. Cela renforce la sécurité, mais nécessite un abonnement API.
- **Per-user / per-organization attachment storage limit** : Tu peux limiter la taille totale des pièces jointes (fichiers) qu'un utilisateur ou une organisation peut stocker.
  - **Per-user** : limite par utilisateur
  - **Per-organization** : limite partagée par toute l'organisation
- **Per-user send storage limit** : Définit la taille maximale totale des *Sends* qu'un utilisateur peut créer. Cela permet d'éviter les abus de stockage ou le partage de gros fichiers via la plateforme.
- **Trash auto-delete days** : Les éléments placés à la corbeille sont automatiquement supprimés définitivement après ce nombre de jours. Cela évite de surcharger la base de données avec des éléments inutiles.
- **Incomplete 2FA time limit** : Temps (en minutes) autorisé pour terminer une tentative de connexion avec double authentification (2FA). Si ce délai est dépassé, la tentative est rejetée.
- **Disable icon downloads** : Si activé, Vaultwarden ne télécharge pas les icônes de sites web (favicon) associés à tes mots de passe. Cela améliore la confidentialité, surtout en réseau local ou sans accès Internet.
- **Allow new signups** : Autorise les utilisateurs à créer un compte librement. Désactive cette option si tu veux garder un contrôle strict sur qui peut rejoindre l'instance.
- **Require email verification on signups** : Si activé, les nouveaux comptes ne pourront pas se connecter tant que leur adresse email n'est pas vérifiée via un lien reçu par mail.
- **Auto re-send verification email** : Si l'utilisateur n'a pas reçu ou utilisé le mail de vérification après un certain temps, le système renvoie automatiquement un nouveau mail.
- **Email verification resend limit** : Limite le nombre de renvois automatiques d'email de vérification en cas de tentatives répétées de connexion. Une sécurité contre les abus ou le spam.
- **Email domain whitelist** :
  Tu peux restreindre la création de comptes aux emails appartenant à un ou plusieurs domaines spécifiques (ex. : `@entreprise.fr`), ce qui est utile pour des usages internes.
- **Org creation users** : Permet de limiter quels utilisateurs peuvent créer des organisations. Laisser vide signifie que tous les utilisateurs peuvent le faire.
- **Allow invitations** : Permet aux membres d'une organisation d'inviter d'autres utilisateurs à la rejoindre.

- **Enable emergency access** : Active la fonctionnalité d'accès d'urgence. Elle permet à un utilisateur de désigner une personne de confiance pouvant accéder à son coffre en cas de problème (maladie, décès...).
- **Allow email change** : Permet aux utilisateurs de modifier eux-mêmes leur adresse email dans leur profil.
- **Password iterations** : Nombre d'itérations utilisées pour le dérivage des mots de passe. Plus le nombre est élevé, plus la sécurité est renforcée (mais cela peut allonger légèrement le temps de connexion). Vaultwarden recommande entre 100 000 et 1 000 000.
- **Allow password hints** : Autorise les utilisateurs à définir un indice pour leur mot de passe maître.
- **Show password hint** : Si activé, l'indice est visible sur l'écran de connexion. Attention, cela peut être un risque de sécurité si l'indice est trop explicite.
- **Admin token / Argon2 PHC** : Champ permettant de définir ou coller le **hash Argon2** du mot de passe d'administration. Ce hash est utilisé pour sécuriser l'accès à `/admin`.
- **Invitation organization name** : Nom personnalisé qui apparaîtra dans les invitations envoyées par email lors d'un ajout à une organisation.

Advanced settings

Cette section rassemble des réglages qui influencent le comportement plus technique ou précis de Vaultwarden. Ces options permettent d'ajuster la sécurité, la gestion des icônes, la gestion des sessions, et d'autres détails.

- **Client IP header** : Par défaut, Vaultwarden regarde l'en-tête `X-Real-IP` pour détecter l'adresse IP réelle du client qui se connecte. Cela est particulièrement utile si Vaultwarden est derrière un proxy (comme un reverse proxy Apache ou Nginx). Cela permet d'avoir des logs précis et une meilleure gestion de la sécurité.
- **Icon redirect code** : Quand Vaultwarden télécharge une icône (favicon) d'un site web, il suit les redirections HTTP. Le code `302` indique une redirection temporaire, et Vaultwarden utilise ce code pour gérer ces transferts d'icônes.
- **Positive icon cache expiry** : Durée (en secondes) pendant laquelle une icône correctement téléchargée est conservée en cache avant d'être retéléchargée. Par défaut, 2592000 secondes (soit 30 jours). Cela améliore la vitesse et réduit la charge réseau.
- **Negative icon cache expiry** : Durée (en secondes) pendant laquelle une tentative de téléchargement d'icône ayant échoué est mise en cache pour éviter de retenter trop souvent. Par défaut, 259200 secondes (environ 3 jours). Cela évite d'essayer sans arrêt des icônes non disponibles.
- **Icon download timeout** : Durée maximale (en secondes) autorisée pour télécharger une icône. Par défaut, 10 secondes. Cela empêche Vaultwarden de rester bloqué trop longtemps sur un site lent.
- **Block HTTP domains/IPs by Regex** : Permet d'indiquer des expressions régulières (regex) pour bloquer certains domaines ou adresses IP spécifiques. Cela renforce la sécurité en empêchant la connexion à des ressources non fiables.

- **Block non global IPs** : Cette option empêche les connexions provenant d'adresses IP privées ou locales (comme 192.168.x.x ou 10.x.x.x), sauf si explicitement autorisées. Cela évite que des utilisateurs hors réseau accèdent à Vaultwarden quand ce n'est pas souhaité.
- **Disable Two-Factor remember** : Si activé, Vaultwarden ne « se souvient » pas des appareils déjà authentifiés en 2FA. Cela signifie que les utilisateurs devront entrer leur code 2FA à chaque connexion, pour plus de sécurité.
- **Disable authenticator time drifted codes to be valid** : Certains générateurs de code 2FA peuvent avoir un léger décalage dans l'heure (time drift). Par défaut, Vaultwarden accepte ce décalage pour éviter les erreurs. En activant cette option, seuls les codes parfaitement synchronisés seront acceptés.
- **Require new device emails** : Si activé, chaque nouvelle connexion depuis un appareil non reconnu déclenche l'envoi d'un mail d'alerte à l'utilisateur. Cela renforce la surveillance des connexions.
- **Reload templates (Dev)** : Cette option est surtout utilisée par les développeurs pour recharger les fichiers de templates HTML sans redémarrer le serveur, utile lors de la personnalisation de l'interface.
- **Log timestamp format** : Format utilisé pour afficher la date et l'heure dans les logs. Exemple : `%Y-%m-%d %H:%M:%S.%3f` produit un affichage précis avec millisecondes. Ce format facilite la lecture et la recherche dans les journaux.
- **Allowed iframe ancestors (Know the risks!)** : Liste des sites autorisés à afficher Vaultwarden via une iframe. Cette option peut être utilisée pour intégrer Vaultwarden dans d'autres sites, mais elle peut aussi créer des risques de sécurité (clickjacking).
- **Admin session lifetime** : Durée (en heures) de validité d'une session d'administration. Par défaut, `20` heures. Passé ce délai, l'administrateur devra se reconnecter pour accéder à la console d'administration.
- **Increase note size limit (Know the risks!)** : Permet d'augmenter la taille maximale des notes dans le coffre. Utile pour stocker de longues informations, mais cela peut alourdir la base de données et ralentir le service.

Yubikey settings

La section **YubiKey Settings** permet d'activer l'authentification à deux facteurs (2FA) avec une **clé physique de sécurité YubiKey**. Ce dispositif ajoute une couche de protection très fiable, en plus du mot de passe classique.

- **Enabled** : Cela signifie que l'utilisation de YubiKey est autorisée sur votre instance. Si vous désactivez cette case, les utilisateurs ne pourront plus configurer ni utiliser leur YubiKey pour se connecter.
- **Client ID** : Il s'agit de l'identifiant public fourni par **Yubico** (le fabricant des YubiKeys). Il est requis pour que Vaultwarden puisse vérifier les codes générés par une YubiKey.
  Par défaut, Vaultwarden utilise l'ID public de démonstration `107623`. Cela permet de tester le service sans s'enregistrer. Pour un usage en production, il est recommandé de s'enregistrer sur le site de Yubico afin d'obtenir un **Client ID** personnalisé.

- **Secret Key** : Il s’agit de la **clé secrète** associée au Client ID. Elle est utilisée pour authentifier les requêtes de vérification envoyées aux serveurs Yubico. Elle doit être conservée confidentielle.
  Comme pour le Client ID, une clé de démonstration est utilisable temporairement, mais il est fortement recommandé d’obtenir vos propres identifiants.
- **Server** : Il est possible de remplacer cette URL si vous disposez de votre propre infrastructure de validation YubiKey, pour une utilisation totalement privée.

Global duo settings

La section **Global Duo Settings** permet d’activer l’authentification à deux facteurs via le service **Duo Security** (filiale de Cisco). Ce service propose une vérification d’identité forte, par notification mobile, appel ou code temporaire, pour sécuriser davantage les connexions.

Contrairement à une clé physique comme YubiKey, Duo repose sur une application mobile, ce qui le rend plus souple à déployer dans certains contextes (notamment en entreprise).

- **Enabled** : Ce paramètre active la possibilité d'utiliser Duo pour la double authentification.
  Si ce champ est désactivé, aucun utilisateur ne pourra configurer Duo dans son compte.
- **Client ID** : Il s’agit de l’identifiant public fourni par **Duo** lorsque vous créez une nouvelle application dans votre espace administrateur Duo.
  C’est une valeur unique qui identifie votre instance Vaultwarden auprès du service Duo.
- **Client Secret** : Il s’agit de la **clé secrète** associée au Client ID. Elle permet de signer les requêtes envoyées à Duo.
  Cette valeur doit rester confidentielle, car elle est essentielle pour établir une communication sécurisée entre Vaultwarden et Duo.
- **Host** : Ce champ correspond à l’adresse du serveur Duo à utiliser, généralement sous la forme `api-xxxx.duosecurity.com`.
  C’est l’URL que Vaultwarden utilisera pour envoyer les demandes de vérification lors des connexions utilisateurs.

SMTP Email settings

La section **SMTP Email Settings** permet de configurer l’envoi des e-mails par Vaultwarden. Ces e-mails sont utilisés pour plusieurs fonctions importantes : vérification d’adresse lors de l’inscription, notifications de sécurité (nouvelle connexion, partage, demande d'accès), envoi de liens d’urgence ou de réinitialisation de mot de passe.

Vaultwarden n’héberge pas de serveur de messagerie. Il s’appuie donc sur un **serveur SMTP externe** (comme celui de Zimbra, Gmail, ProtonMail, etc.) pour envoyer les e-mails.

```
echo -n "Mot de Passe" | argon2 "$(openssl rand -base64 32)" -e -id -k 65540 -t 3 -p 4
```

- **Enabled** : Active ou désactive la fonction d'envoi d'e-mails. Si cette option est désactivée, Vaultwarden ne pourra plus envoyer aucun message, ce qui rendra certaines fonctions inaccessibles (inscription, récupération de mot de passe, etc.).
- **Use Sendmail** : Permet d'utiliser la commande `sendmail` locale si disponible, au lieu de se connecter à un serveur SMTP distant. Cette option est rarement utilisée, sauf sur des serveurs configurés spécifiquement.
- **Host** : Exemple : `mail.domaine.com` indique que Vaultwarden va utiliser le serveur mail de ton instance Zimbra pour envoyer les messages.
- **Secure SMTP** : Spécifie le protocole de chiffrement utilisé pour sécuriser la communication SMTP.
  - `force_tls` : Vaultwarden exigera que la connexion soit chiffrée via TLS.
    C'est l'option recommandée.
- **Port** : Le port utilisé pour se connecter au serveur SMTP.
  Le port **465** est standard pour les connexions SMTP avec chiffrement SSL/TLS immédiat.
- **From Address** : Adresse e-mail qui apparaîtra comme expéditeur des messages envoyés par Vaultwarden.
  Exemple : `vaultwarden@domaine.com`
- **From Name** : Nom affiché à côté de l'adresse d'expéditeur dans les clients mail.
  Exemple : *Rakouns Coffre-Fort* donne une touche plus humaine ou identifiable à l'expéditeur.
- **Username / Password** : Méthode d'authentification utilisée par Vaultwarden pour s'identifier auprès du serveur SMTP.
  `LOGIN` est une méthode courante et compatible avec la majorité des serveurs.
- **SMTP connection timeout** : Durée maximale (en secondes) que Vaultwarden attend pour établir la connexion au serveur SMTP.
  Une valeur raisonnable comme **30** permet de ne pas bloquer le système trop longtemps en cas de problème réseau.
- **Server name sent during HELO** : Nom que Vaultwarden envoie au serveur SMTP pendant la phase d'introduction (commande HELO ou EHLO).
  Ce champ peut être laissé vide ou personnalisé, surtout dans les environnements internes où certains serveurs imposent des noms valides.
- **Embed images as email attachments** : Permet d'inclure les images directement dans les e-mails (sous forme de pièces jointes), au lieu de les charger via une URL externe. Cela améliore la compatibilité et évite que les images soient bloquées.
- **Accept Invalid Certs** : Si activé, Vaultwarden acceptera des certificats SSL invalides (auto-signés ou expirés).
  ⚠ **Fortement déconseillé**, sauf pour des tests ou dans des environnements totalement maîtrisés.
- **Accept Invalid Hostnames** : Permet d'ignorer les erreurs de nom d'hôte dans les certificats (ex : CN ne correspondant pas au domaine utilisé).
  Comme le paramètre précédent, ce n'est **pas recommandé en production**.
- **Test SMTP** : Permet de tester immédiatement la configuration SMTP depuis l'interface admin. Vaultwarden tentera d'envoyer un e-mail à l'administrateur pour valider les paramètres.

Email 2FA settings

La section **Email 2FA Settings** permet d’activer un système d’authentification à deux facteurs (2FA) basé sur la réception d’un code par e-mail. C’est une méthode simple et accessible, mais **moins sécurisée** que les solutions classiques comme les applications d’authentification ou les clés physiques (comme YubiKey).

- **Enabled** : Active ou désactive la possibilité pour les utilisateurs d’utiliser l’e-mail comme second facteur d’authentification.
  Lorsque c’est activé, Vaultwarden peut envoyer un code de sécurité temporaire par e-mail lors de la connexion.
- **Email token size** : Définit le nombre de chiffres du code envoyé par e-mail.
  Exemple : 6 enverra un code comme `827319`.
- **Token expiration time** : Durée (en secondes) pendant laquelle le code est valide.
  600 secondes signifie que l’utilisateur a 10 minutes pour saisir le code reçu par e-mail avant qu’il n’expire.
- **Maximum attempts** : Nombre maximal de tentatives autorisées pour entrer le bon code.
  Au-delà de cette limite, l’accès est refusé pour éviter les attaques par bruteforce.
- **Automatically enforce at login** : Si activé, **tous les utilisateurs devront utiliser l’authentification 2FA par e-mail** s’ils n’ont pas déjà configuré une autre méthode.
  Cela permet de forcer un minimum de sécurité sur toutes les connexions.
- **Auto-enable 2FA (Know the risks!)** : Si cette option est activée, **Vaultwarden activera automatiquement le 2FA par e-mail pour tous les utilisateurs**, sans qu’ils aient besoin de le faire eux-mêmes.
  ⚠ Cela peut poser des problèmes si certains utilisateurs ne peuvent pas recevoir d’e-mails ou si la configuration SMTP échoue. C’est pourquoi cette option est marquée comme risquée.

Voila la déscription des principaux paramètres de VaultWarden !