

Vaultwarden

- [01 - Description](#)
- [02 - Installation](#)
- [03 - Configuration](#)

01 - Description

Environnement de déploiement

Parametre	Valeur
OS	Debian 12
IP de la VM	192.168.99.6
Ressources VM	1 vCPU, 512 Mo RAM, 8 Go disque
Hyperviseur	Proxmox
Moteur de conteneur	Docker Engine 29.5.2
Port expose	8443 (HTTPS)

Qu'est-ce que Vaultwarden ?

Vaultwarden est une implementation open-source et allégée du serveur Bitwarden, écrite en Rust. Il permet d'auto-heberger un gestionnaire de mots de passe complet sur sa propre infrastructure, sans dépendance à des services cloud externes.

Contrairement au serveur officiel Bitwarden qui nécessite des ressources importantes, Vaultwarden est conçu pour fonctionner sur des machines modestes tout en offrant les mêmes fonctionnalités essentielles : coffre-fort chiffré, organisation des secrets, partage entre utilisateurs et interface web accessible depuis un navigateur.

Utilite dans le projet IRS-SI

Dans le cadre du projet IRS-SI, plusieurs services ont été déployés sur des machines virtuelles distinctes : Asterisk, Zabbix, NoDogSplash, le NAS Synology, le WAP150, le PDU ATEN, etc. Chacun de ces équipements possède des identifiants d'administration qu'il est nécessaire de stocker de manière sécurisée et accessible à l'ensemble de l'équipe.

Vaultwarden répond précisément à ce besoin en offrant :

- Un coffre-fort chiffré centralisé pour tous les mots de passe du projet
- Un partage sécurisé via l'organisation Projet-IRS entre les trois membres de l'équipe
- Une interface web accessible depuis n'importe quel poste du réseau local
- Un déploiement entièrement en local, cohérent avec la politique de sécurité du projet

02 - Installation

Installation Docker

Docker n'est pas inclus dans les depots Debian par default. La procedure suivante utilise le script d'installation officiel de Docker :

```
sudo apt update && sudo apt install -y curl
curl -fsSL https://get.docker.com | sh
sudo usermod -aG docker $USER
```

Après l'ajout au groupe docker, il est necessaire de se deconnecter puis de se reconnecter pour que le changement prenne effet.

Generation du certificat SSL auto-signe

Vaultwarden exige une connexion HTTPS pour fonctionner. En environnement local sans autorite de certification, un certificat auto-signe est genere avec OpenSSL :

```
sudo mkdir /vw-ssl
sudo openssl req -x509 -nodes -days 3650 -newkey rsa:2048 \
-keyout /vw-ssl/vaultwarden.key \
-out /vw-ssl/vaultwarden.crt \
-subj "/CN=192.168.99.6"
```

Ce certificat est valable 10 ans et genere une cle RSA 2048 bits. Le navigateur affichera un avertissement de securite lors du premier acces, qu'il faudra accepter manuellement.

Creation du script de demarrage

Pour faciliter le demarrage du conteneur et eviter les problemes de saisie dans la console Proxmox, la commande Docker est enregistree dans un script bash :

```
nano start.sh
```

Contenu du fichier start.sh :

```
#!/bin/bash
sudo docker run -d --name vaultwarden --restart unless-stopped \
  -e ADMIN_TOKEN=IRS-SI-Admin2026 \
  -e ROCKET_TLS='{certs="/ssl/vaultwarden.crt",key="/ssl/vaultwarden.key"}' \
  -v /vw-data:/data \
  -v /vw-ssl:/ssl \
  -p 8443:80 \
  vaultwarden/server:latest
```

Description des parametres :

- -d : execution en arriere-plan (mode detache)
- --name vaultwarden : nom du conteneur
- --restart unless-stopped : redemarrage automatique au boot
- -e ADMIN_TOKEN : token d'accès au panel d'administration
- -e ROCKET_TLS : chemin vers le certificat et la cle SSL
- -v /vw-data:/data : volume de donnees persistant
- -v /vw-ssl:/ssl : volume du certificat SSL
- -p 8443:80 : exposition du port 8443 en HTTPS

Lancement du conteneur

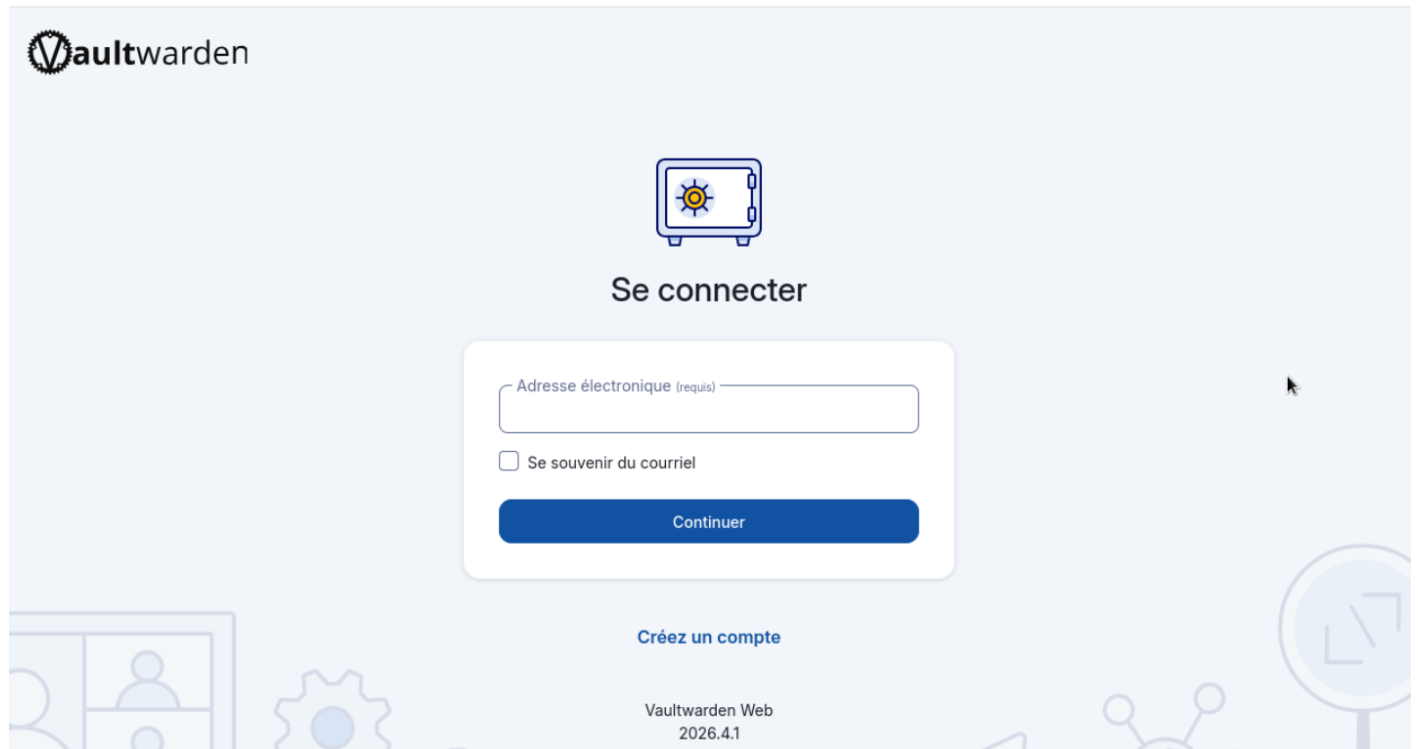
```
chmod +x start.sh
./start.sh
```

Verification que le conteneur est bien en cours d'execution :

```
sudo docker ps
```

Le statut doit afficher 'Up' pour le conteneur vaultwarden. L'interface est ensuite accessible depuis un navigateur a l'adresse :

https://192.168.99.6:8443



03 - Configuration

Creation du compte administrateur

Lors du premier acces a l'interface web, aucun compte n'existe. Il faut en creer un en cliquant sur 'Creez un compte' en bas de la page de connexion. Ce premier compte sera automatiquement proprietaire de l'instance.

Champs a renseigner lors de la creation du compte :

- Adresse electronique : kermorvant.m@stjolorient.fr
- Nom : Matheo
- Mot de passe principal : mot de passe fort (min. 12 caracteres)

Important : le mot de passe principal est le seul a devoir etre memorise. Il ne peut pas etre recupere en cas d'oubli car Vaultwarden utilise un chiffrement cote client (le serveur ne connait jamais le mot de passe en clair).

Acces au panel d'administration

Le panel d'administration Vaultwarden permet de gerer les utilisateurs, confirmer les comptes et superviser l'instance sans passer par un compte utilisateur. Il est accessible a l'adresse :

```
https://192.168.99.6:8443/admin
```

Le token d'accès est celui défini lors du lancement du conteneur : IRS-SI-Admin2026

Depuis ce panel, les actions disponibles sont :

- Consulter et gerer tous les utilisateurs enregistres

- Confirmer les inscriptions sans envoyer d'email
- Supprimer ou desactiver des comptes
- Consulter les organisations et collections
- Configurer les parametres SMTP si un serveur mail est disponible

Creation de l'organisation partagee

Une organisation dans Vaultwarden permet de partager des mots de passe entre plusieurs membres. Pour creer l'organisation du projet :

- Dans l'interface web, cliquer sur l'icone grille en haut a droite
- Cliquer sur 'Nouvelle organisation'
- Nom : Projet-IRS
- Plan : Gratuit
- Valider la creation

L'organisation Projet-IRS apparait ensuite dans le menu lateral gauche sous 'Coffres'.



Vaultwarden
Password Manager

Coffres
Send
Outils
Rapports
Paramètres
Password Manager
Admin Console

Nouvelle organisation

Les organisations permettent de partager des parties de votre coffre avec d'autres personnes ainsi que de gérer des utilisateurs pour une entité spécifique comme une famille, une petite équipe ou une grande entreprise.

Informations générales

Nom de l'organisation (requis)
Projet-IRS

Courriel (requis)
kermorvant.m@stjolorient.fr

Soumettre

Gestion des membres

Pour inviter les autres membres du projet dans l'organisation :

- Aller dans Admin Console (menu bas gauche)
- Cliquer sur 'Membres' puis 'Inviter un membre'
- Saisir l'email du membre a inviter
- Le membre doit ensuite creer son compte sur <https://192.168.99.6:8443>
- Une fois le compte cree, aller dans l'onglet 'Confirmation necessaire' et confirmer

Membres de l'organisation Projet-IRS :

Membre	Email
Kermorvant Matheo	kermorvant.m@stjolorient.fr
Le Garrec Raphael	legarrec.r@stjolorient.fr
Le Galliot Ilian	legalliot.i@stjolorient.fr

Gestion des collections

Les collections permettent de classer les mots de passe par categorie au sein de l'organisation. Une collection par default est creee automatiquement. Il est recommande de creer des collections thematiques pour le projet :

- Reseau : credentials des equipements reseau (switch, routeur, WAP150)
- Serveurs : acces Proxmox, VMs, services (Zabbix, Asterisk, NoDogSplash)
- Supervision : comptes Zabbix, SNMP credentials
- Infrastructure : PDU ATEN, onduleur APC, NAS Synology

Pour creer une collection : Admin Console > Collections > bouton Nouveau.

Ajout d'un mot de passe

Pour ajouter un identifiant dans l'organisation :

- Aller dans Coffres > Projet-IRS

- Cliquer sur '+ Nouveau'
- Choisir le type : Identifiant
- Renseigner le nom, l'URL, le nom d'utilisateur et le mot de passe
- Sélectionner le propriétaire : Projet-IRS (organisation)
- Sélectionner la collection appropriée
- Enregistrer

Les mots de passe ajoutés dans une collection de l'organisation sont visibles par tous les membres ayant accès à cette collection. Les mots de passe dans 'Mon coffre' restent privés.

Recommandations de sécurité

Dans le cadre du projet IRS-SI, les mesures de sécurité suivantes ont été appliquées :

- Accès HTTPS exclusif via certificat TLS, le HTTP n'est pas exposé
- Token ADMIN_TOKEN protège l'accès au panel d'administration
- Les données sont stockées dans /vw-data isolé du conteneur
- Le conteneur est configuré avec --restart unless-stopped pour la disponibilité
- L'accès est limité au réseau local du projet (192.168.99.0/24)
- Chaque membre dispose de son propre compte avec identifiants uniques

The screenshot shows the Vaultwarden Admin Console interface. On the left is a sidebar with the following menu items: 'Projet-IRS', 'Collections' (highlighted), 'Membres', 'Rapports', and 'Paramètres'. At the bottom of the sidebar are 'Password Manager' and 'Admin Console'. The main area is titled 'Projet-IRS collections' and features a '+ Nouveau' button, a grid icon, and a user profile icon labeled 'MA'. Below the title is a 'FILTRES' section with a search input 'Rechercher dans |' and a list of filter categories: 'Tous les éléments', 'Identifiant', 'Carte de paiement...', 'Identité', 'Note', 'Clé SSH', 'Collections' (highlighted), and 'Corbeille'. To the right is a table of collections:

<input type="checkbox"/> Tous	Nom ↕	Autorisation ^	⋮
<input type="checkbox"/>	Non attribué	Modifier les items	
<input type="checkbox"/>	Infrastructure	Gérer la collection	⋮
<input type="checkbox"/>	Réseau	Gérer la collection	⋮
<input type="checkbox"/>	Servers	Gérer la collection	⋮
<input type="checkbox"/>	Supervision	Gérer la collection	⋮