Déployer Vaultwarden avec Docker

Introduction

Je vais installer la solution à auto héberger de coffre fort numerique Vaultwraden

Via le mot de passe renseigner le système derive le mot de passe, ajoute un sel et créer une clef symetrique qui permettra de chiffrer et dechiffrer les mots de passe

Vaultwarden est un fork de Bitwarden écrit en Rust qui est beaucoup plus léger que Bitwarden et qui peut être autohébergé. L'autre intérêt d'utiliser Vaultwarden en entreprise, c'est que celui-ci intégré toutes les fonctionnalité de la version payant de Bitwarden comme :

- La possibilité de limiter la création de compte à un domaine ou plusieurs domaines d'adresse de messagerie
- La gestion des organisations qui permet la partage de Mot de passe entre plusieurs utilisateurs
- La gestion des organisations permet également la réinitialisation du mot de passe maitre d'un compte

Installation via docker

Pour héberger Vaultwarden en conteneur, vous aurez besoin

- d'un serveur Linux avec Docker et Docker Compose d'installé.
- pour l'accès Web, vous aurez besoin d'un reverse proxy (Nginx ou Apache) puis d'une URL avec un certificat SSL pour la liaison HTTPS.
- d'un serveur SMTP pour l'envoie des e-mails.

Sur mon serveur Linux où Docker est installé, je vais mettre les fichiers du conteneur dans le répertoire /containers/vault.

Je clone le repo github

git clone https://git.rdr-it.com/docker/Vaultwarden.git .

```
root@VM-DOCKER:~/vault# git clone https://git.rdr-it.com/docker/Vaultwarden.g
 .
Clonage dans '.'...
remote: Enumerating objects: 15, done.
remote: Total 15 (delta 0), reused 0 (delta 0), pack-reused 15 (from 1)
Dépaquetage des objets: 100% (15/15), fait.
root@VM-DOCKER:~/vault# ls -ls
total 12
4 -rw-r--r-- 1 root root  744 avril 29 01:48 docker-compose.yml
4 -rw-r--r-- 1 root root  750 avril 29 01:48 nginx-vhost-le
4 -rw-r--r-- 1 root root 1025 avril 29 01:48 nginx-vhost-ssl
0 -rw-r--r-- 1 root root    0 avril 29 01:48 README.md
root@VM-DOCKER:~/vault#
```

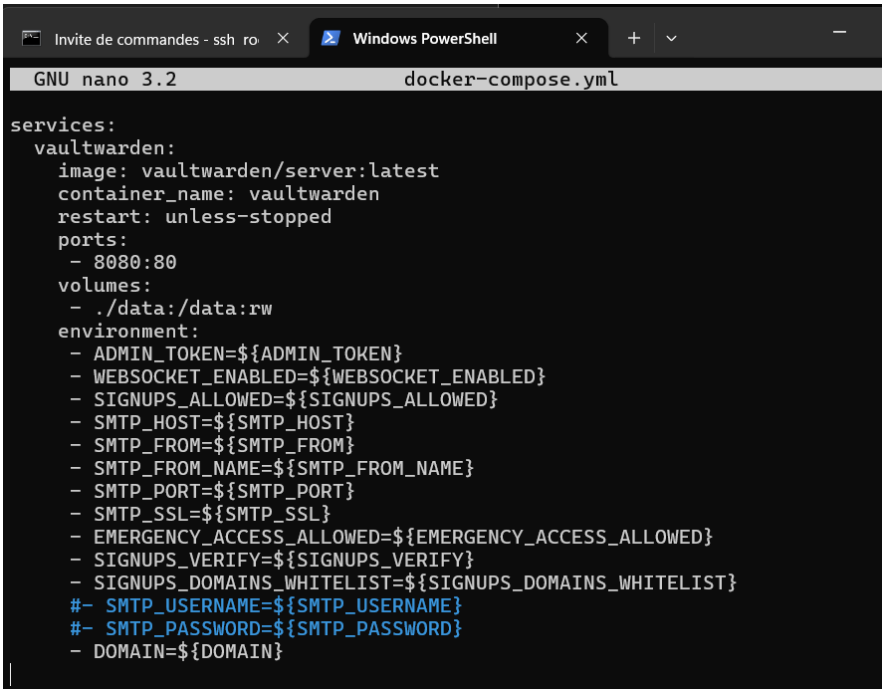
Editer le fichier .env pour configurer Vaultwarden :

nano .env

```
  GNU nano 3.2                                  .env

ADMIN_TOKEN=[redacted]
WEBSOCKET_ENABLED=true
SIGNUPS_ALLOWED=true
SMTP_HOST=192.168.0.254
SMTP_FROM=vault@sadek.ovh
SMTP_FROM_NAME=Vaultwarden
SMTP_PORT=25
SMTP_SSL=false
SMTP_USERNAME=
SMTP_PASSWORD=
DOMAIN=https://vault.sadek.ovh
EMERGENCY_ACCESS_ALLOWED=false
SIGNUPS_VERIFY=true
SIGNUPS_DOMAINS_WHITELIST=sadek.ovh
```

- ADMIN_TOKEN : mot de passe pour accéder à l'administration (le générer avec openssl rand -base64 48)
- SIGNUPS_ALLOWED : autoriser ou non l'inscription
- SMTP_HOST : adresse du serveur SMTP
- SMTP_FROM : adresse de l'expéditeur
- SMTP_FROM_NAME : nom de l'expéditeur
- SMTP_PORT : port du serveur SMTP
- SMTP_SSL : utilisation du SSL pour la communication avec le serveur SMTP

- SMTP_USERNAME : compte pour le serveur SMTP, si nécessaire décommenter dans le fichier docker-compose.yml la variable
- SMTP_PASSWORD : mot de passe pour le serveur SMTP, si nécessaire décommenter dans le fichier docker-compose.yml la variable
- DOMAIN : url d'accès à Vaultwarden
- EMERGENCY_ACCESS_ALLOWED : autorise la récupération d'urgence
- SIGNUPS_VERIFY : force la vérification de l'adresse email de l'utilisateur
- SIGNUPS_DOMAINS_WHITELIST : domaine de messagerie autorisé à créer des comptes



Je créer le dossier « data » dans le repertoire courant

Je telcharge l'image via

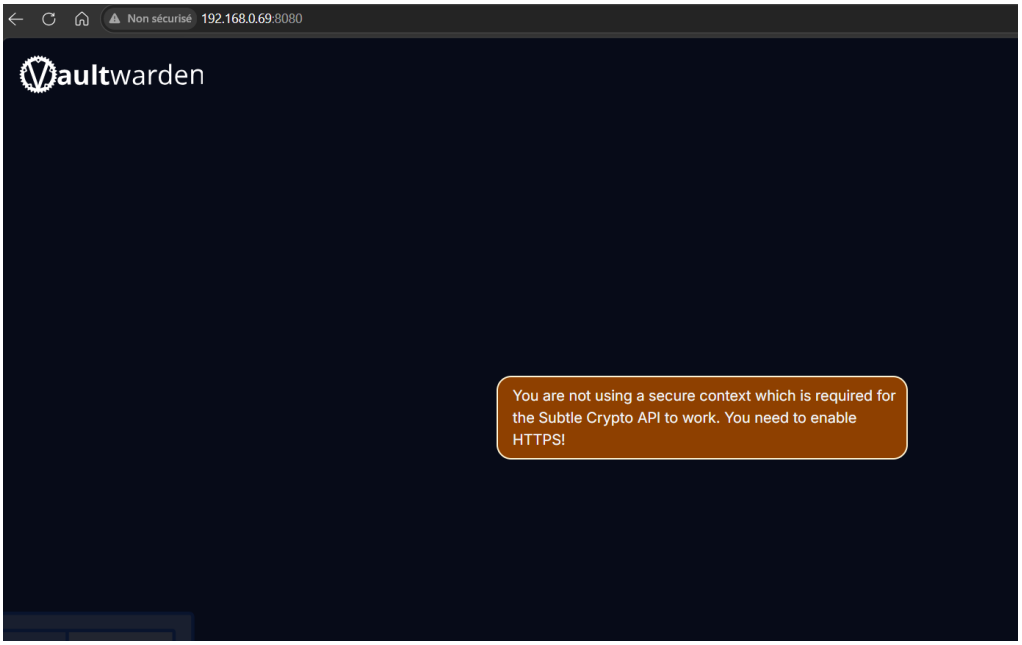
Docker compose pull

Ensuite

Docker compose up -d

```
root@VM-DOCKER:~/vault# docker compose pull
[+] Pulling 6/6
 ✔vaultwarden Pulled
   ✔3531af2bc2a9 Pull complete
   ✔8438044a2d67 Pull complete
   ✔d041f291e400 Pull complete
   ✔0c9571575998 Pull complete
   ✔995884a2b584 Pull complete
root@VM-DOCKER:~/vault# docker compose up -d
[+] Running 2/2
 ✔Network vault_default  Created
 ✔Container vaultwarden  Started
root@VM-DOCKER:~/vault#
```

Je créer l'enregistrement DNS + creation de la directive dans NGINX avec un certificat générer via letsencrypt



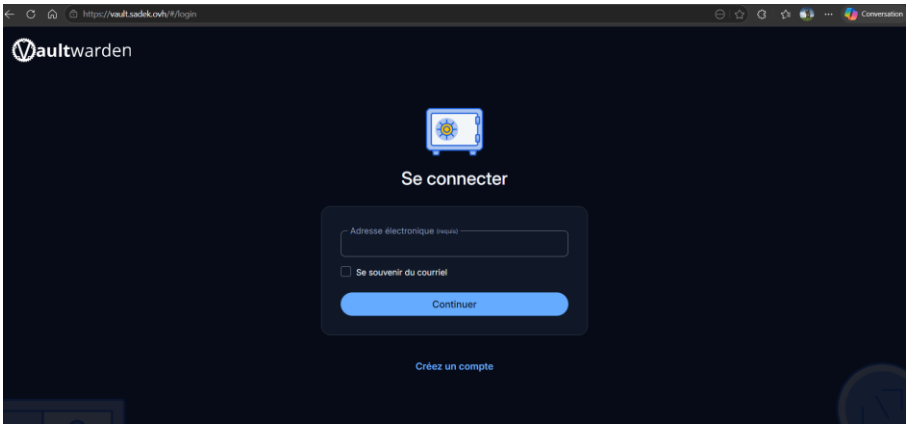
Car tout accès via http est interdit il faut absolument https

Il faut aussi modifier ce fichier pour que le serveur web ecoute en https

nginx-vhost-le

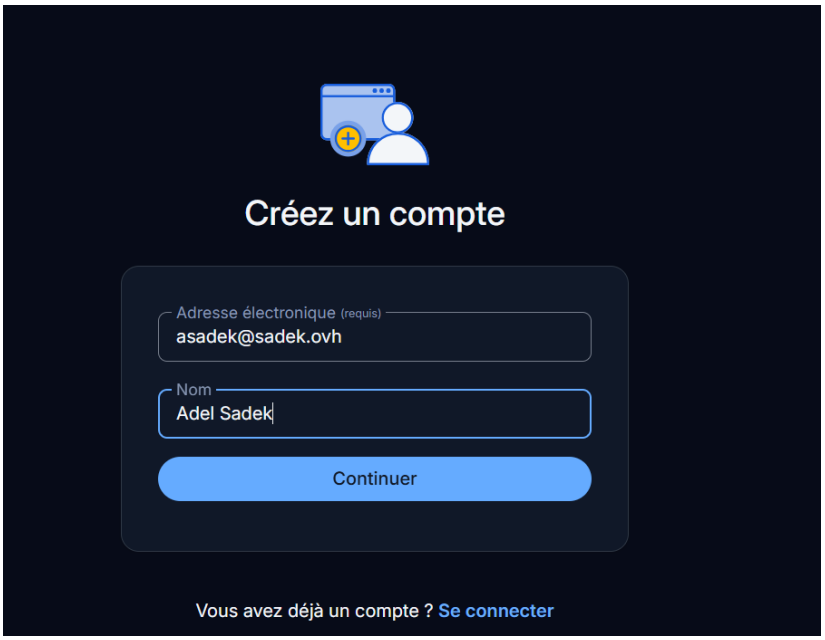
```
server{
    listen 80;
    server_name vault.domain.tld;
    access_log /var/log/nginx/vault.domain.tld_access.log;
    error_log /var/log/nginx/vault.domain.tld_access.log;

    location / {
        proxy_pass https://127.0.0.1:8080;
        proxy_ssl_verify off;
        proxy_redirect  off;
        proxy_set_header  Host  $host;
        proxy_set_header  X-Real-IP $remote_addr;
        proxy_set_header  X-Forwarded-Forwarded $proxy_add_x_forwarded_for;
        client_max_body_size  256m;
        client_body_buffer_size 128k;
        proxy_connect_timeout 90;
        proxy_send_timeout    90;
        proxy_read_timeout    90;
        proxy_buffers         32 4k;
        proxy_http_version 1.1;
        proxy_set_header Connection "";
    }
}
```

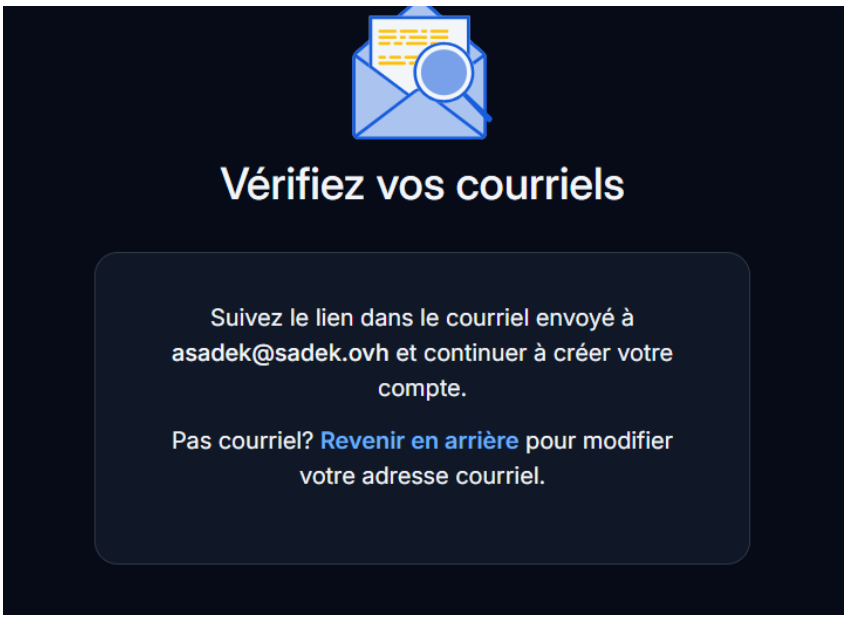
Il faut bien que nginx reverse proxy accede au serveur en http mais que le vlient accede en https



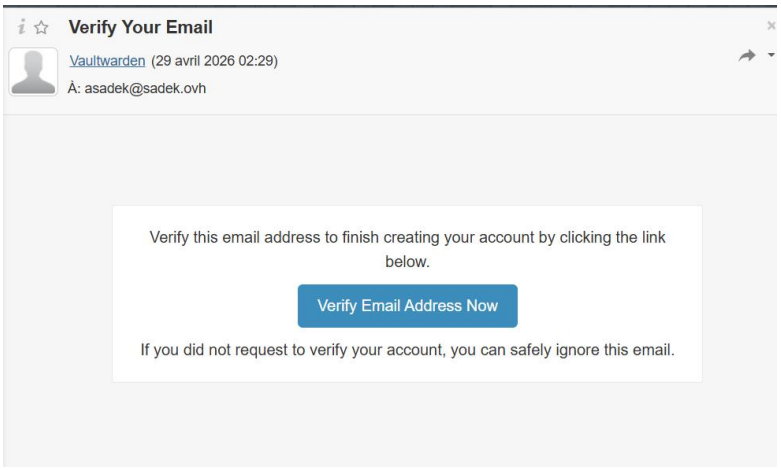
Cliquer sur Créez un compte **1**.

Entrer vos adresse e-mail **1** puis votre nom **2**, indiquer la clef maitre **3** qui permet de déverrouiller le coffre et si nécessaire un mémo **4** pour retrouver la clef et cliquer sur Créez un compte **5**.



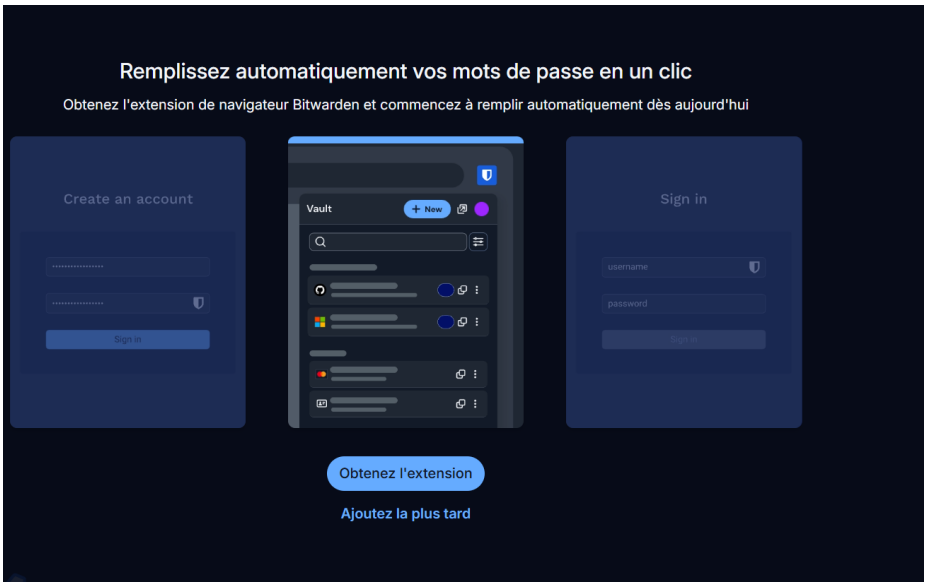


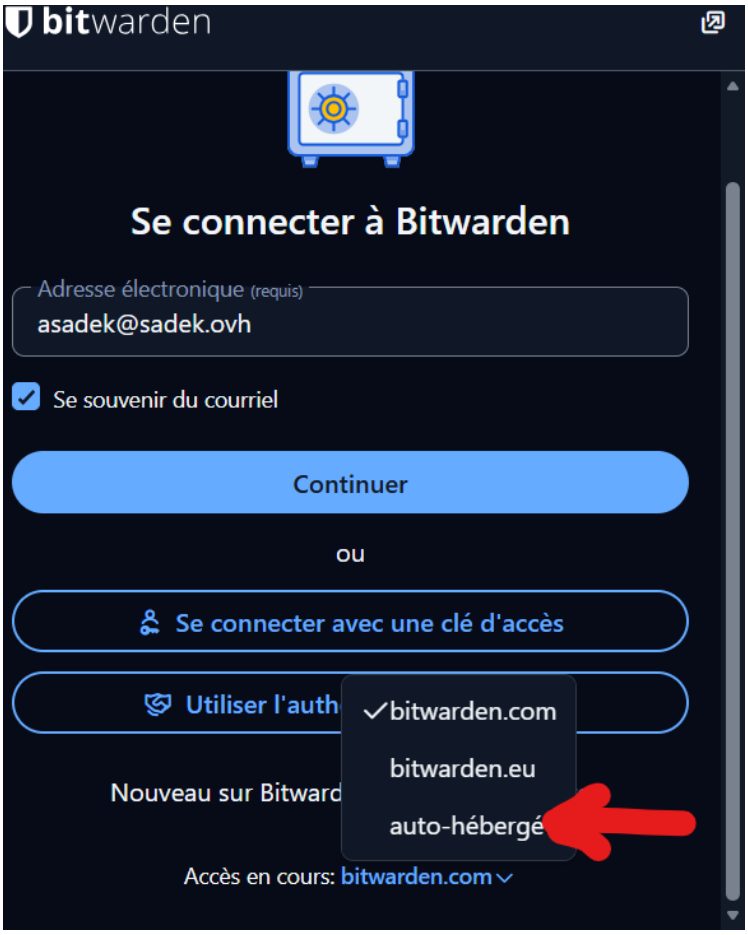
Le mail est envoyé



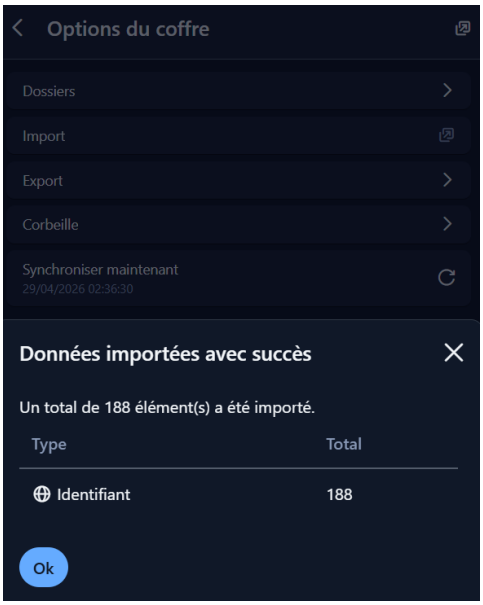
Je mets le mot de passe et son indice

J’installe aussi l’extension web une pierre deux coups

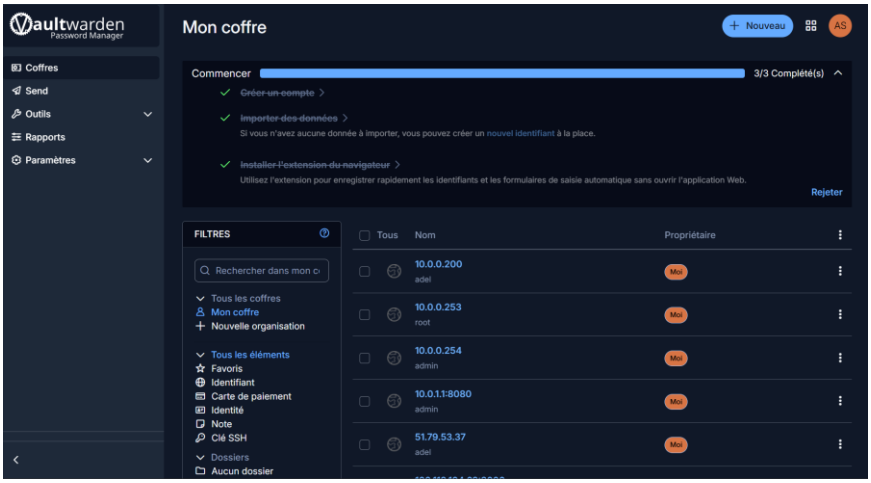




Je suis les instructions intuitives pour exporter tout mes mots de passe vers le coffre fort


Options du coffre
Dossiers
Import
Export
Corbeille
Synchroniser maintenant
29/04/2026 02:36:30
Données importées avec succès
Un total de 188 élément(s) a été importé.
Type
Total
Identifiant
188
Ok

Et voila


Vaultwarden
Password Manager
Mon coffre
Nouveau
AS
Coffres
Send
Outils
Rapports
Paramètres
Commencer
3/3 Complété(s)
Créer un compte
Importer des données
Si vous n'avez aucune donnée à importer, vous pouvez créer un nouvel identifiant à la place.
Installer l'extension du navigateur
Utilisez l'extension pour enregistrer rapidement les identifiants et les formulaires de saisie automatique sans ouvrir l'application Web.
Rejeter
FILTRES
Rechercher dans mon c
Tous les coffres
Mon coffre
Nouvelle organisation
Tous les éléments
Favoris
Identifiant
Carte de paiement
Identité
Note
Clé SSH
Dossiers
Aucun dossier
Tous
Nom
Propriétaire
10.0.0.200
adel
Moi
10.0.0.253
root
10.0.0.254
admin
10.0.1.1:8080
admin
51.79.53.37
adel

Gestion des organisations dans Vaultwarden

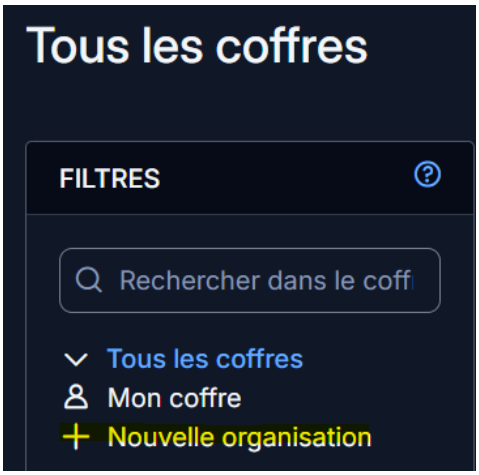
Dans cette partie, on va voir à quoi sert une organisation et comment en créer une.

Les organisations vont permettre plusieurs choses :

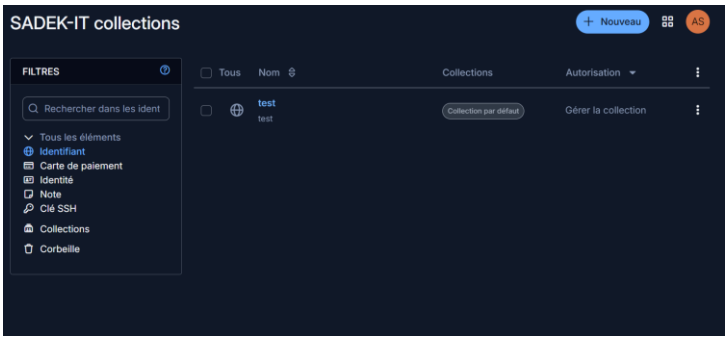
- Gestion des utilisateurs et configuration.
- Partage de mot de passe.

Créer une organisation

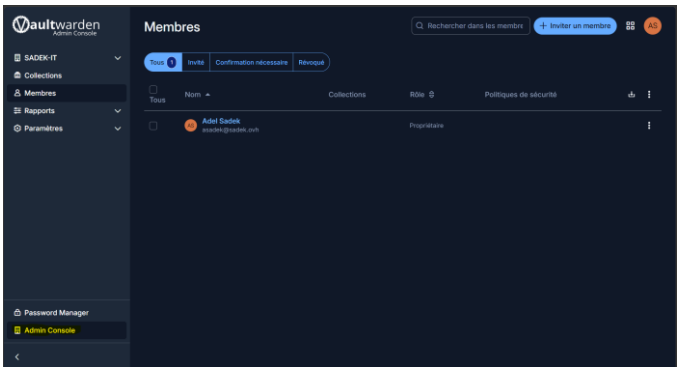
Pour créer une organisation, cliquer sur Nouvelle organisation **1**.



Je créer un mdp test



Ajouter un user dans l'organisation

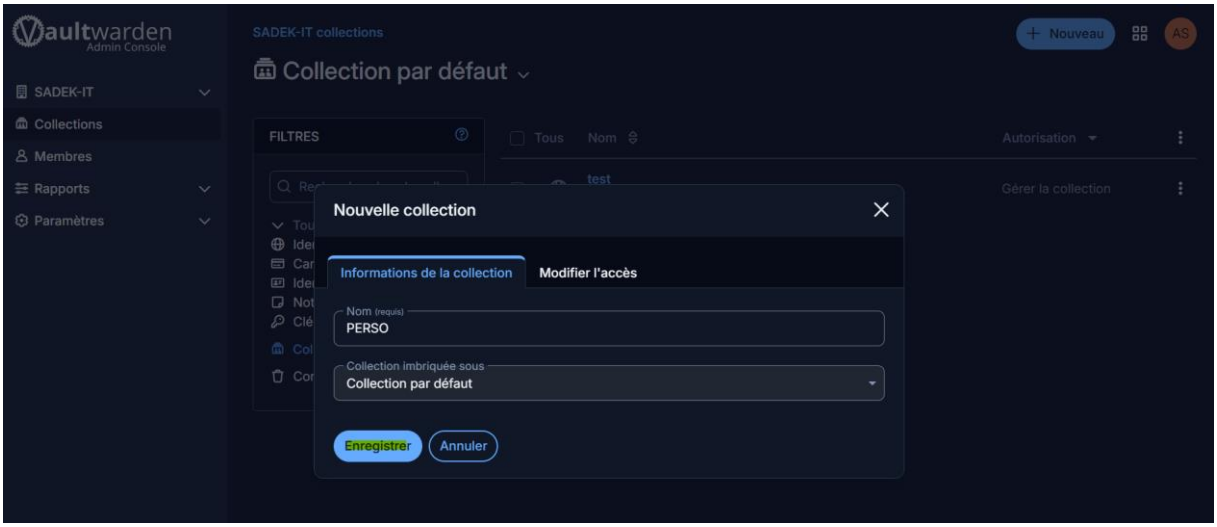


Politique de sécurité de l'organisation

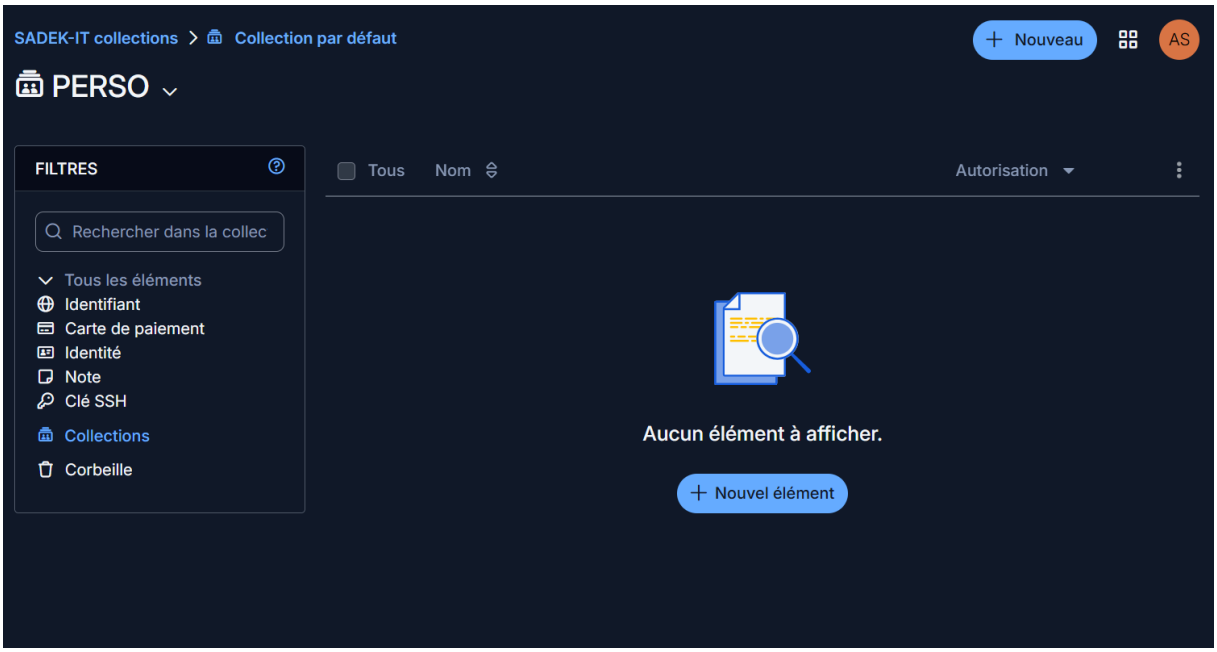
Les collections

Les collections sont des conteneurs (dossiers) sur lesquels on va pouvoir attribuer des autorisations.

Depuis le coffre, cliquer sur Nouveau **1** puis Collection **2**.



Dans le cas d'une ESN on pourrait avoir une organisation par client + différentes collections par site par exemple ou secteur

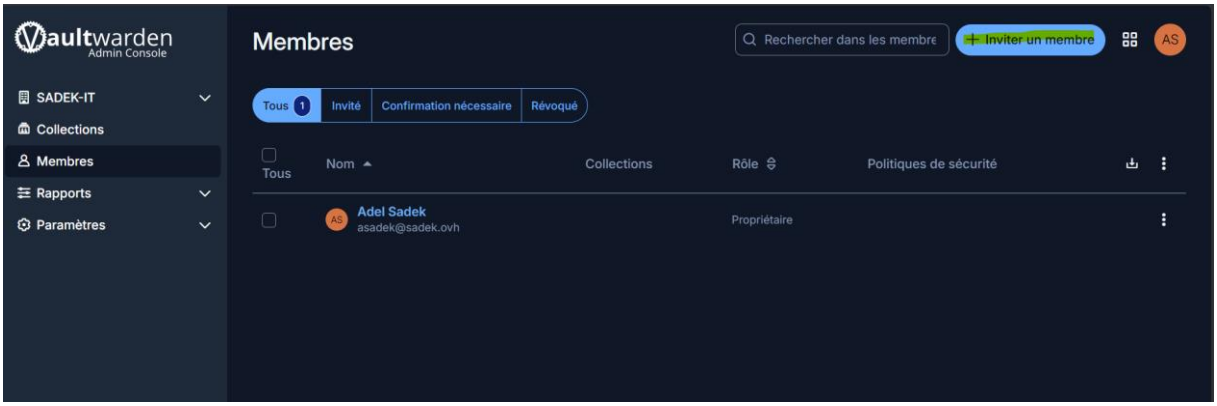


Inviter des utilisateurs depuis une collection

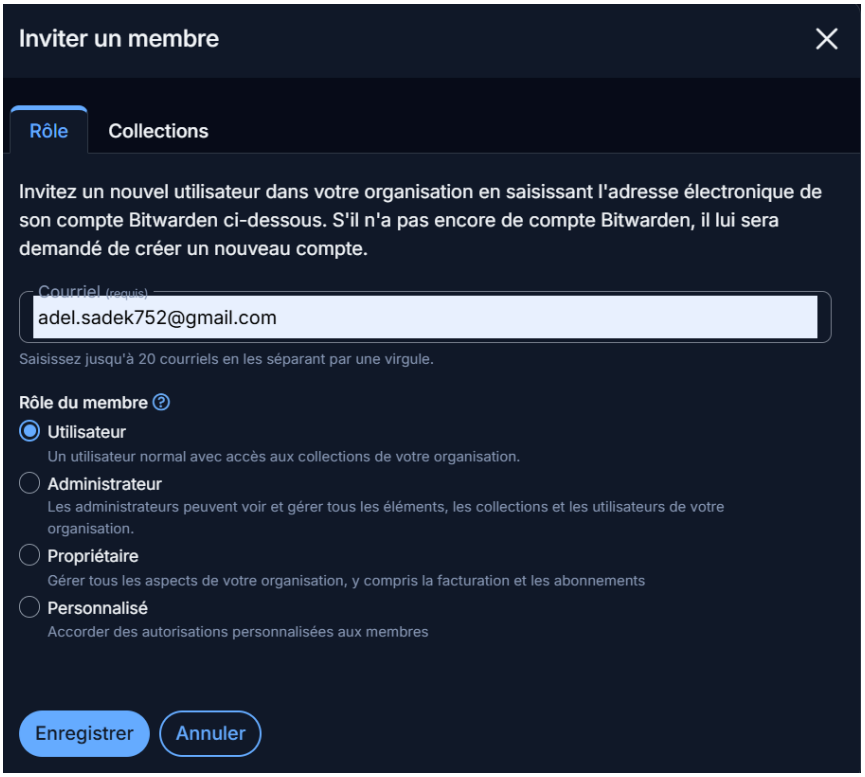
Maintenant, on va voir comment inviter des utilisateurs dans une collection.

Il est possible d'invité un utilisateur qui n'a pas de compte même si l'inscription est fermé.

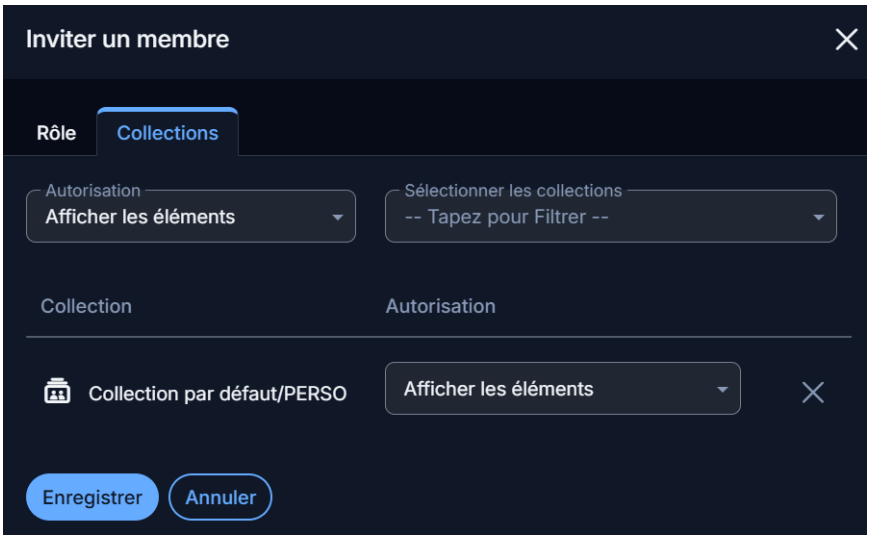
Aller sur l'onglet Membres **1** et cliquer sur Inviter un membre **2**.



Entrer l'adresse email **1** puis aller sur Collections **2**.

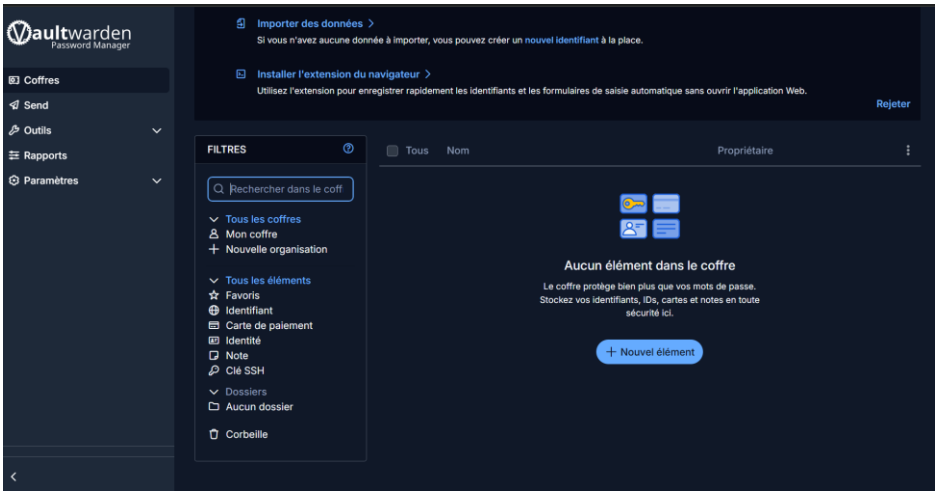


Avant de valider cliquer sur collection

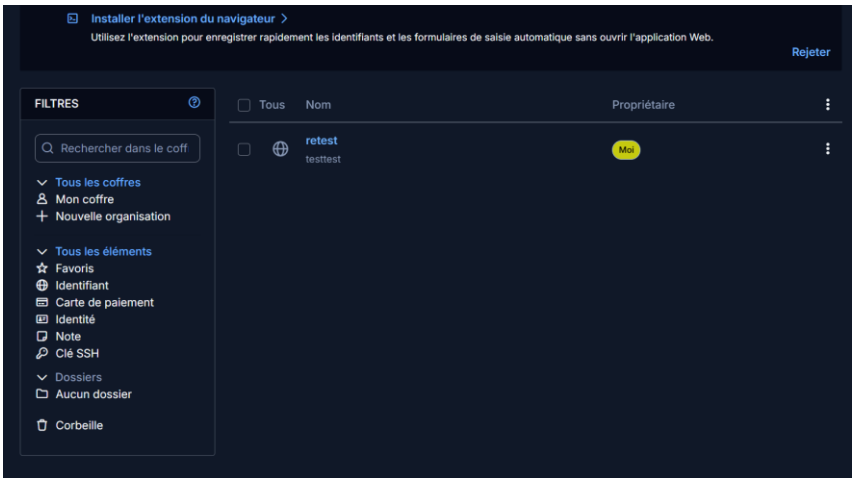


Ensuite on enregistre

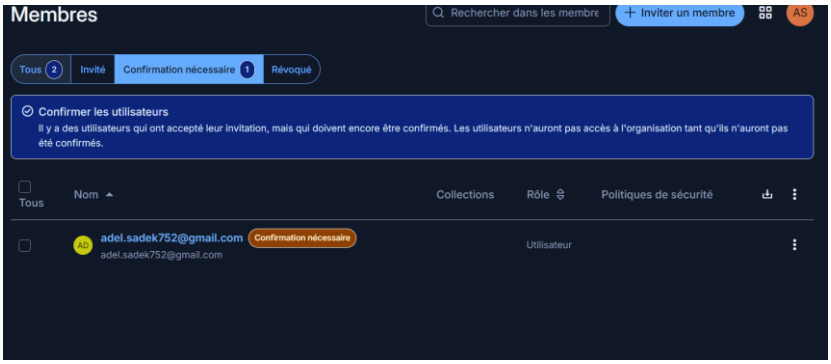
Me voila connecter avec mon second user



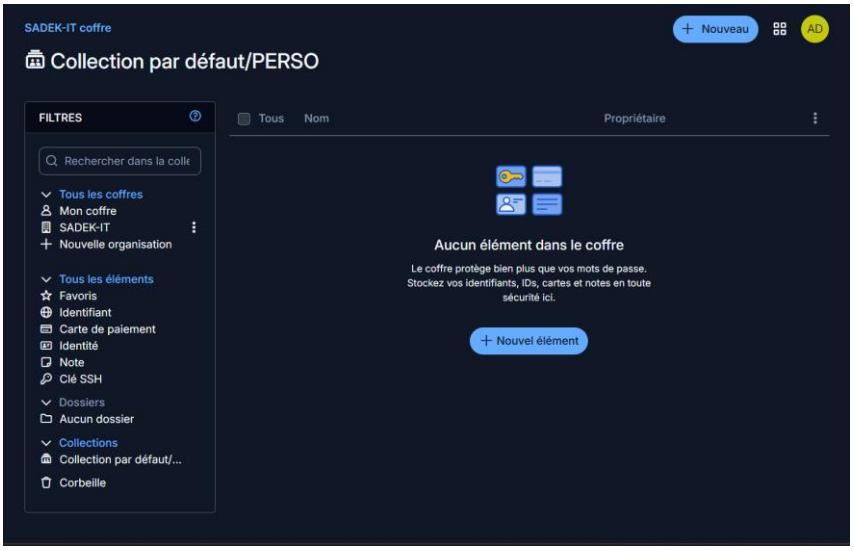
Je créer un mot de passe depuis le second user je ne vois pas de collection perso ni rien peut être que l'utilisateur est chrooter je vais voir du coté de mon user proprietaire si ça s'affiche dans la collection perso



Finalement il faut d'abord que je confirme l'utilisateur une fois qu'il c'est inscrit pour l'autoriser à accéder à la collection



Ensuite coté du second user je vois bien la collection perso



L’user peut juste afficher les infos mais ne peut rien ajouter ni modifier tant que que je ne lui ai pas accorder les droits

Par défaut Vaultwarden utilise une base SQLite, il est possible de passer sur MariaDB si vous le souhaitez : https://github.com/dani-garcia/vaultwarden/wiki/Using-the-MariaDB-(MySQL)-Backend