

Vaultwarden : Gestionnaire de mot de passe

Dans ce tutoriel, nous allons apprendre à déployer un serveur Vaultwarden sur un NAS Synology afin d'héberger notre propre solution de gestion de mots de passe ! Vous connaissez déjà sûrement Vaultwarden, car il s'agit d'une version non officielle de Bitwarden destinée à l'auto-hébergement !

Le gestionnaire de mots de passe Bitwarden peut être utilisé en mode SaaS, c'est-à-dire hébergé sur les serveurs de l'éditeur dans le Cloud, mais il peut aussi être auto-hébergé sur son propre serveur.

Par contre, il est considéré comme étant assez lourd, ce qui n'est pas très pratique si l'on veut utiliser un NAS ou pourquoi pas un Raspberry Pi.

La bonne nouvelle, c'est qu'il existe **Vaultwarden**, une **solution libre codée en Rust, beaucoup plus légère** et que l'on peut **héberger soi-même**. Avant, elle s'appelait "Bitwarden_RS" mais il y a eu un changement de nom pour une raison compréhensible : *"Ce projet était connu sous le nom de Bitwarden_RS et a été renommé pour se séparer du serveur officiel de Bitwarden dans l'espoir d'éviter toute confusion et tout problème de marque."* - Vaultwarden est totalement adapté pour un NAS, un serveur en ligne (par exemple : un VPS), un Raspberry Pi ou un serveur en local.

Vaultwarden est une solution fiable et sécurisée qui reprend les fonctionnalités clés de Bitwarden, à savoir :

- Solution de type coffre-fort numérique pour stocker vos identifiants et mots de passe, vos informations de carte de paiement, des notes, etc...
- Gestion de plusieurs utilisateurs sur un même serveur (via un système d'inscription) et gestion d'organisations pour partager les identifiants entre utilisateurs
- Accès à votre coffre-fort sur tous les appareils associés à votre compte.
- Sécurité des données grâce au chiffrement bout en bout (seul l'utilisateur peut accéder à ses données)
- Générateur de mots de passe et de passphrases pour vous faciliter la création de mots de passe robustes
- Authentification à deux facteurs pour renforcer l'accès aux comptes
- Partage de fichiers ou de texte à l'aide de la fonctionnalité Send

Plutôt sympa pour **garder la maîtrise de son coffre-fort de mots de passe**, tout en ayant accès à une solution moderne accessible via un navigateur, des extensions pour navigateur et une application mobile. D'ailleurs, **Vaultwarden est compatible avec les applications et extensions Bitwarden.**

Pour **installer Vaultwarden sur un NAS Synology**, nous allons utiliser **un container Docker via l'application Container Manager de DSM**. Ce sera stable et facile à déployer, mais il conviendra de sauvegarder les données du container compte tenu de leur criticité. Il est à noter que l'application Docker s'appelle Container Manager depuis DSM 7.2.

Créer un container Docker "Vaultwarden"

Le NAS étant équipé de Container Manager, vous allez pouvoir **créer un nouveau container Vaultwarden** (en lieu et place de *Bitwarden_rs*).

Ouvrez Container Manager, cliquez à gauche sur "**Registre**" (1), recherchez "**vaultwarden**" en haut à droite (2), puis sélectionnez "**vaultwarden/server**" dans la liste (3) et cliquez sur "**Télécharger**" (4) pour que l'image de ce container soit téléchargée sur le NAS.

image.png

Au moment où vous cliquez sur "**Télécharger**", la fenêtre "**Choisir une identification**" apparaît. Choisissez la dernière version du container via "**latest**" et validez.

image.png

Quand le téléchargement est effectué, cliquez à gauche sur "**Conteneur**" dans l'interface de Container Manager. Créez un nouveau conteneur en cliquant sur "**Créer**".

Commencez par choisir l'image "**vaultwarden/server:latest**" que vous venez de télécharger. Même si ce n'est pas obligatoire, vous pouvez **activer la limitation des ressources** comme sur l'image ci-dessous. Ce conteneur n'est pas très gourmand. Au besoin, c'est ajustable par la suite. Activez aussi le redémarrage automatique pour que le NAS essaie de le relancer automatiquement en cas de crash.

image.png

L'étape "**Paramètres des ports**" s'affiche. Les ports "**3012/TCP**" et "**80/TCP**" correspondent aux deux ports utilisés par le conteneur. Celui qui correspond à l'accès à l'interface Web, c'est bien sûr le port 80 correspondant au HTTP. L'autre port correspond au Websocket. Tout à gauche, c'est le port à attribuer au niveau du NAS.

Dans l'exemple ci-dessous, l'accès au NAS sur **le port 3012/TCP va renvoyer vers le port 3012/TCP** du conteneur. Tandis que **le port 3013/TCP va renvoyer vers le port 80/TCP** du conteneur. Vous devez utiliser des ports qui ne sont pas encore utilisés sur votre NAS (il y a des chances pour que le port 80 soit utilisé par un autre service). Vous pouvez personnaliser ces valeurs.

image.png

Vous devez prévoir un espace de stockage sur votre NAS afin que le container Vaultwarden puisse écrire ses données. Dans le répertoire "**docker**" du NAS, créez un répertoire nommé "

vaultwarden" et vous allez ensuite l'associer au container.

image.png

Dans la configuration du container, cliquez sur "ajouter un dossier", sélectionnez le répertoire "**/docker/vaultwarden**" et montez-le en "**/data**" afin que le container stocke ses données à cet endroit. Il est important de sauvegarder le répertoire "**/docker/vaultwarden**" pour protéger votre coffre-fort (vous pouvez utiliser [Hyper Backup](#), par exemple).

Ne touchez pas à la section "**Environnement**", nous allons revenir dessus par la suite.

image.png

Il n'est pas nécessaire de configurer de fonctionnalités ou d'adapter la configuration réseau. Cliquez sur "**Suivant**".

image.png

Cliquez sur "**Effectué**" pour créer le conteneur Vaultwarden !

image.png

La section "**Conteneur**" contient un petit nouveau nommé "**vaultwarden**" et qui est actif.

image.png

Afin de pouvoir accéder à l'interface Web de Vaultwarden, vous devez **autoriser le port 3013/TCP** (ou autre, selon votre configuration) dans le **pare-feu de DSM**. Enfin, ceci est vrai uniquement si vous avez activé et configuré le pare-feu de DSM, ce qui est recommandé. Pour rappel, on accède au pare-feu de cette façon : **Panneau de configuration > Sécurité > Pare-feu**.

image.png

Une fois la règle de pare-feu créée, il est possible d'accéder à Vaultwarden via un navigateur en précisant l'adresse IP du NAS et le port 3013.

image.png