Déploiement Hors Ligne de Windows

Déploiement Hors Ligne de Windows

Cet article vous guidera à travers la procédure pour installer et déployer Bitwarden sur votre propre serveur Windows dans un environnement **hors ligne ou isolé**. Veuillez consulter la documentation de soutien à la version logicielle de Bitwarden.

> ⚠ **Warning**
>
> **Les installations manuelles ne doivent être effectuées que par des utilisateurs avancés.** Ne poursuivez que si vous êtes très familier avec les technologies Docker et que vous désirez plus de contrôle sur votre installation Bitwarden.
>
> Les installations manuelles n'ont pas la capacité de mettre à jour automatiquement certaines dépendances de l'installation de Bitwarden. Lorsque vous passez d'une version de Bitwarden à la suivante, vous serez responsable des modifications des variables d'environnement requises, des modifications de nginx `default.conf`, des modifications de `docker-compose.yml`, et ainsi de suite.
>
> Nous essaierons de mettre en évidence ces points dans les notes de version sur GitHub. Vous pouvez également surveiller les modifications apportées aux modèles de dépendance utilisés par le script d'installation de Bitwarden sur GitHub.

Exigences

Avant de procéder à l'installation, veuillez vous assurer que les exigences suivantes sont remplies :

- Docker Engine et Docker Compose sont installés et prêts à être utilisés sur votre serveur. Pendant cette configuration, vous devez **décocher** l'option **Utiliser WSL2 au lieu de Hyper-V (recommandé)**.
- En utilisant une machine avec accès à Internet, vous avez téléchargé le dernier fichier `docker-stub.zip` de la page des versions du dépôt du serveur Bitwarden et transféré ce fichier sur votre serveur.
- Un serveur SMTP hors ligne est configuré et actif dans votre environnement.
- (**Facultatif**) Les binaires OpenSSL pour Windows sont installés et prêts à être utilisés sur votre serveur. Vous pouvez utiliser un certificat auto-signé au lieu d'OpenSSL si vous le souhaitez.

Spécifications du système

	Minimum	Recommandé
Processeur	x64, 1.4GHz	x64, Dual Core de 2GHz
Mémoire	6GB de RAM	8+ Go RAM
Stockage	76GB	90Go
Version de Docker	Moteur 19+ et Compose 1.24+	Moteur 19+ et Compose 1.24+

Virtualisation imbriquée

L'exécution de Bitwarden sur un serveur Windows nécessite l'utilisation de la virtualisation imbriquée. Veuillez consulter la documentation de votre hyperviseur pour savoir si la virtualisation imbriquée est prise en charge et comment l'activer.

> **Tip**
>
> Si vous exécutez Windows Server en tant que VM Azure, nous recommandons une **Machine Virtuelle Standard D2s v3 exécutant Windows Server 2022**, qui répond à toutes les exigences système y compris le support pour l'imbriquer de la virtualisation. Vous devrez également sélectionner **Type de Sécurité** : **Standard** plutôt que le choix par défaut **Machines virtuelles de lancement de confiance**.

Procédure d'installation

Configurez votre domaine

Par défaut, Bitwarden sera servi via les ports 80 (`http`) et 443 (`https`) sur la machine hôte. Ouvrez ces ports afin que Bitwarden puisse être accessible depuis l'intérieur et/ou l'extérieur du réseau. Vous pouvez choisir différents ports lors de l'installation.

> **Tip**
>
> **Si vous utilisez Windows Firewall**, Docker Desktop pour Windows n'ajoutera pas automatiquement une exception pour lui-même dans Windows Firewall. Ajoutez des exceptions pour les ports TCP 80 et 443 (ou des ports alternatifs choisis) pour prévenir les erreurs associées.

Nous recommandons de configurer un nom de domaine avec des enregistrements DNS qui pointent vers votre machine hôte (par exemple, `bitwarden.example.com`), surtout si vous servez Bitwarden sur Internet.

Créer un utilisateur local Bitwarden & répertoire

Ouvrez PowerShell et créez un utilisateur local Bitwarden en exécutant la commande suivante:

```Bash
PS C:\> $Password = Read-Host -AsSecureString
```

Après avoir exécuté la commande ci-dessus, entrez le mot de passe souhaité dans la boîte de dialogue de saisie de texte. Après avoir spécifié un mot de passe, exécutez la commande suivante :

```Bash
New-LocalUser "Bitwarden" -Password $Password -Description "Bitwarden Local Admin"
```

En tant que nouvel utilisateur, créez un dossier Bitwarden sous `C:\`:

```Bash
PS C:\> mkdir Bitwarden
```

Une fois que vous avez installé Docker Desktop, naviguez vers **Paramètres** → **Ressources** → **Partage de fichiers** et ajoutez le répertoire créé (`C:\Bitwarden`) à la liste des ressources. Sélectionnez **Appliquer & Redémarrer** pour appliquer vos modifications.

Nous recommandons de se connecter en tant que nouvel utilisateur créé avant de terminer toutes les procédures ultérieures dans ce document.

Configurez votre machine

Pour configurer votre machine avec les ressources nécessaires pour votre serveur Bitwarden :

> **Tip**
>
> Si vous avez créé un utilisateur et un répertoire Bitwarden, complétez ce qui suit en tant qu'utilisateur `Bitwarden`.

1. Créez un nouveau répertoire dans `C:\Bitwarden` nommé `bwdata` et extrayez `docker-stub.zip` dedans.

   Une fois décompressé, le répertoire `bwdata` correspondra à ce que le fichier `docker-compose.yml` attend pour le mappage de volume. Vous pouvez, si vous le souhaitez, modifier l'emplacement de ces mappages sur la machine hôte.

2. Dans `bwdata\env\global.override.env`, éditer les variables d'environnement suivantes :

   - `globalSettings__baseServiceUri__vault=`: Entrez le domaine de votre instance Bitwarden.
   - `globalSettings__sqlServer__ConnectionString=`: Remplacez le `MOT_DE_PASSE_ALÉATOIRE_DE_LA_BASE_DE_DONNÉES` par un mot de passe sécurisé à utiliser dans une étape ultérieure.
   - `globalSettings__identityServer__certificatePassword=`: Définissez un mot de passe de certificat sécurisé à utiliser dans une étape ultérieure.
   - `globalSettings__internalIdentityKey=`: Remplacez `RANDOM_IDENTITY_KEY` par une chaîne de clé aléatoire.
   - `globalSettings__oidcIdentityClientKey=`: Remplacez `RANDOM_IDENTITY_KEY` par une chaîne de clés aléatoire.
   - `globalSettings__duo__aKey=`: Remplacez `RANDOM_DUO_AKEY` par une chaîne de clés aléatoire.
   - `globalSettings__installation__id=`: Entrez un identifiant d'installation récupéré depuis https://bitwarden.com/host.
   - `globalSettings__installation__key=`: Entrez une clé d'installation récupérée depuis https://bitwarden.com/host.
   - `globalSettings__pushRelayBaseUri=`: Cette variable devrait être vide. Voir Configurer le relais Push pour plus d'informations.

     > **Tip**
     >
     > À ce moment, envisagez également de définir des valeurs pour toutes les variables `globalSettings__mail__smtp__` et pour `adminSettings__admins`. En faisant cela, vous configurerez le serveur de messagerie SMTP utilisé pour envoyer des invitations aux nouveaux membres de l'organisation et fournir l'accès au Portail de l'Administrateur Système.
     >
     > En savoir plus sur les variables d'environnement.

3. Générez un certificat `identité.pfx` pour le conteneur d'identité. Vous pouvez le faire en utilisant OpenSSL ou n'importe quel outil pour générer un certificat auto-signé. Si vous utilisez OpenSSL, exécutez les commandes suivantes :

```
Bash

openssl req -x509 -newkey rsa:4096 -sha256 -nodes -keyout identity.key -out identity.crt -subj
"/CN=Bitwarden IdentityServer" -days 10950
```

et

```
Bash

openssl pkcs12 -export -out ./identity/identity.pfx -inkey identity.key -in identity.crt -passou
t pass:IDENTITY_CERT_PASSWORD
```

Dans la commande ci-dessus, remplacez `IDENTITY_CERT_PASSWORD` par le mot de passe du certificat créé et utilisé dans **Étape 2**.

4. Déplacez `identité.pfx` vers le répertoire du volume mappé (par défaut, `.\bwdata\identité`).
5. Copier `identity.pfx` dans le répertoire `.\bwdata\ssl`.
6. Créez un sous-répertoire dans `.\bwdata\ssl` nommé pour votre domaine.
7. Fournissez un certificat SSL de confiance et une clé privée dans le sous-répertoire nouvellement créé `.\bwdata\ssl\bitwarden.example.com`.

> **Note**
> Ce répertoire est mappé au conteneur NGINX à `\etc\ssl`. Si vous ne pouvez pas fournir un certificat SSL de confiance, placez devant l'installation un proxy qui fournit un point de terminaison HTTPS aux applications client Bitwarden.

8. Dans `.\bwdata\nginx\default.conf`:
    1. Remplacez toutes les instances de `bitwarden.example.com` par votre domaine, y compris dans l'en-tête `Politique de Sécurité de Contenu`.
    2. Définissez les variables `ssl_certificate` et `ssl_certificate_key` sur les chemins du certificat et de la clé privée fournis dans **l'étape 6**.
    3. Effectuez l'une des actions suivantes, en fonction de la configuration de votre certificat :
        - Si vous utilisez un certificat SSL de confiance, définissez la variable `ssl_trusted_certificate` sur le chemin d'accès à votre certificat.
        - Si vous utilisez un certificat auto-signé, mettez en commentaire les variables `ssl_trusted_certificate`.
9. Dans `.\bwdata\env\mssql.override.env`, remplacez `RANDOM_DATABASE_PASSWORD` par le mot de passe créé à **l'étape 2**.
10. Dans `.\bwdata\web\app-id.json`, remplacez `bitwarden.example.com` par votre domaine.

Télécharger & transférer des images

Pour obtenir des images Docker pour utilisation sur votre machine hors ligne :

1. Depuis une machine connectée à Internet, téléchargez toutes les images Docker `bitwarden/xxx:dernières`, telles qu'elles sont répertoriées dans le fichier `docker-compose.yml` dans `docker-stub.zip`.

2. Enregistrez chaque image dans un fichier `.img`, par exemple :

```
Bash

docker image save -o mssql.img bitwarden/mssql:version
```

3. Transférez tous les fichiers `.img` sur votre machine hors ligne.

4. Sur votre machine hors ligne, chargez chaque fichier `.img` pour créer vos images Docker locales, par exemple :

```
Bash

docker image load -i mssql.img
```

Démarrez votre serveur

Démarrez votre serveur Bitwarden avec la commande suivante :

```
Bash

docker compose -f ./docker/docker-compose.yml up -d
```

Vérifiez que tous les conteneurs fonctionnent correctement :

```
Bash

docker ps
```

Liste montrant des Conteneurs Sains

Félicitations ! Bitwarden est maintenant opérationnel à l'adresse `https://your.domain.com`. Visitez le coffre web dans votre navigateur pour confirmer qu'il fonctionne.

Vous pouvez maintenant enregistrer un nouveau compte et vous connecter. Vous devrez avoir configuré les variables d'environnement SMTP (voir Variables d'Environnement) afin de vérifier le courriel pour votre nouveau compte.

Prochaines étapes :

- Si vous prévoyez d'auto-héberger une organisation Bitwarden, consultez auto-héberger une organisation pour commencer.
- Pour plus d'informations, consultez les FAQ sur l'auto-hébergement.

Mettez à jour votre serveur

Mettre à jour un serveur auto-hébergé qui a été installé et déployé manuellement est différent de la procédure de mise à jour standard. Pour mettre à jour votre serveur installé manuellement :

1. Téléchargez la dernière archive `docker-stub.zip` depuis les pages de versions sur GitHub.
2. Décompressez la nouvelle archive `docker-stub.zip` et comparez son contenu avec ce qui se trouve actuellement dans votre répertoire `bwdata`, en copiant tout ce qui est nouveau dans les fichiers préexistants de `bwdata`.
   Ne pas écraser votre répertoire `bwdata` existant avec le contenu de la nouvelle archive `docker-stub.zip`, car cela écraserait tout travail de configuration personnalisé que vous avez effectué.
3. Téléchargez les dernières images de conteneur et transférez-les sur votre machine hors ligne comme documenté ci-dessus.
4. Exécutez la commande suivante pour redémarrer votre serveur avec votre configuration mise à jour et les derniers conteneurs :

```bash
docker compose -f ./docker/docker-compose.yml down && docker compose -f ./docker/docker-compose.yml up -d
```