GUIDE PRATIQUE À SUIVRE

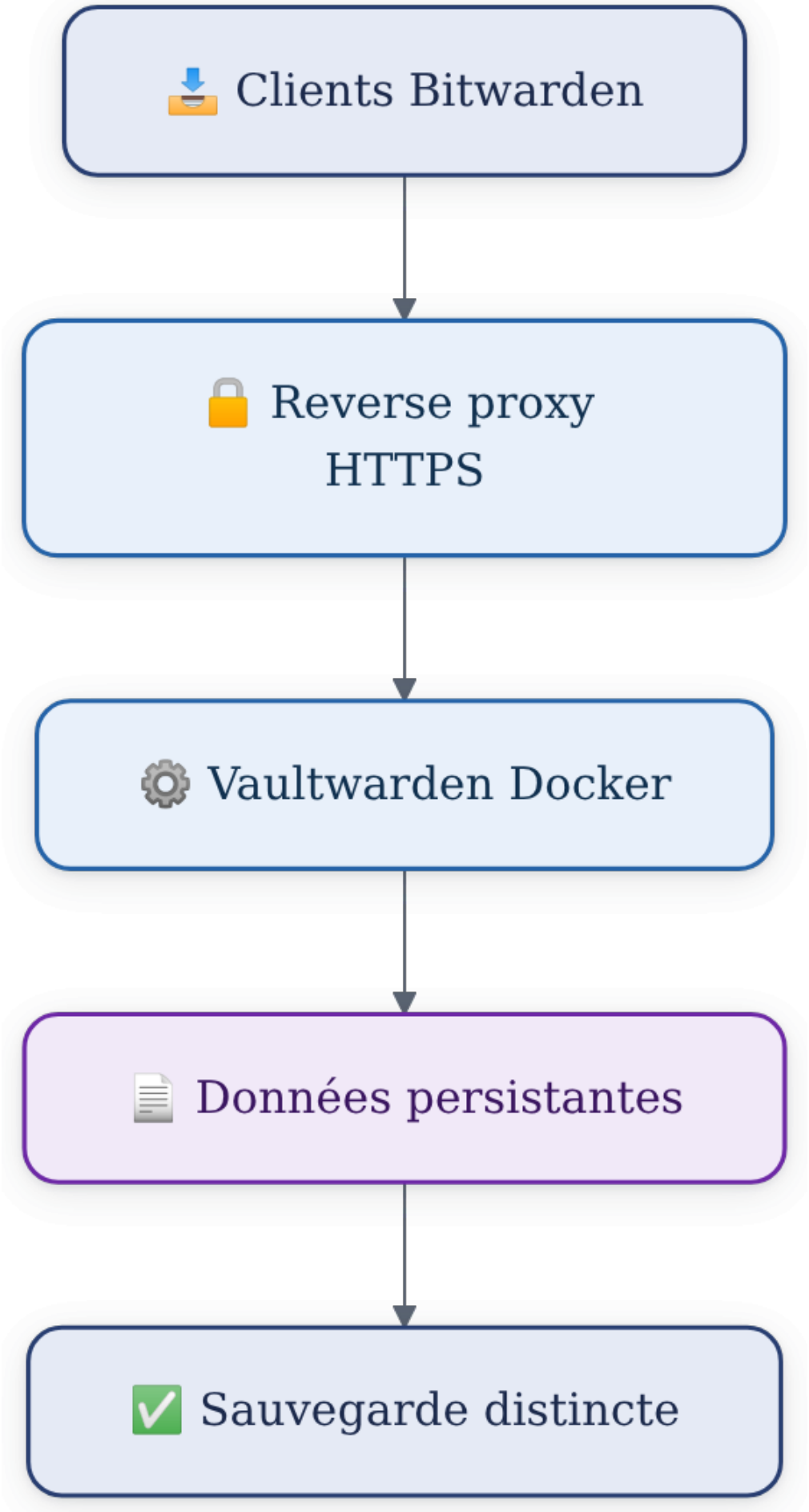
Votre parcours d'auto-hébergement Vaultwarden, du serveur à la sauvegarde

Installez un coffre de mots de passe personnel sans négliger les points qui font réellement sa fiabilité : accès HTTPS, données persistantes, restrictions d'inscription et restauration testée. Utilisez cette fiche comme fil conducteur de déploiement et d'exploitation.

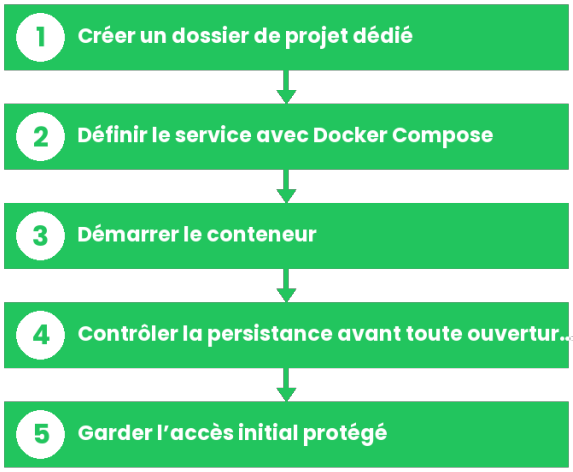
Au sommaire

1. Valider le projet avant de commencer

- [ ] **Choisir un environnement maintenu**
  Serveur Linux, NAS compatible Docker ou machine dédiée dont vous assurez les mises à jour.
- [ ] **Confirmer que Docker Engine et Docker Compose fonctionnent**
  Référez-vous à la documentation officielle Docker pour votre système.
- [ ] **Prévoir un emplacement de données persistant**
  Le volume de données doit survivre au remplacement ou à la mise à jour du conteneur.
- [ ] **Prévoir une destination de sauvegarde distincte**
  Ne conservez pas l'unique copie de sauvegarde sur le serveur Vaultwarden.
- [ ] **Décider du mode d'accès**
  Local uniquement, ou accès distant avec un nom de domaine et HTTPS.
- [ ] **Accepter la responsabilité d'exploitation**
  L'auto-hébergement implique mises à jour, surveillance et capacité de restauration.


Clients Bitwarden
Reverse proxy
HTTPS
Vaultwarden Docker
Données persistantes
Sauvegarde distincte

2. Déployer l'instance Docker



1 **Créer un dossier de projet dédié**
Isolez Vaultwarden dans son propre répertoire et créez le dossier destiné aux données persistantes.

2 **Définir le service avec Docker Compose**
Utilisez un fichier docker-compose.yml lisible et reproductible, avec le répertoire local ./data monté sur /data dans le conteneur.

3 **Démarrer le conteneur**
Lancez le service avec la commande docker compose up -d, puis vérifiez que le conteneur est bien en fonctionnement.

4 **Contrôler la persistance avant toute ouverture externe**
Vérifiez que les données sont écrites dans le volume prévu : elles ne doivent pas dépendre uniquement du cycle de vie du conteneur.

5 **Garder l'accès initial protégé**
Ne rendez pas l'instance publiquement accessible tant que le reverse proxy HTTPS et les réglages de sécurité ne sont pas finalisés.

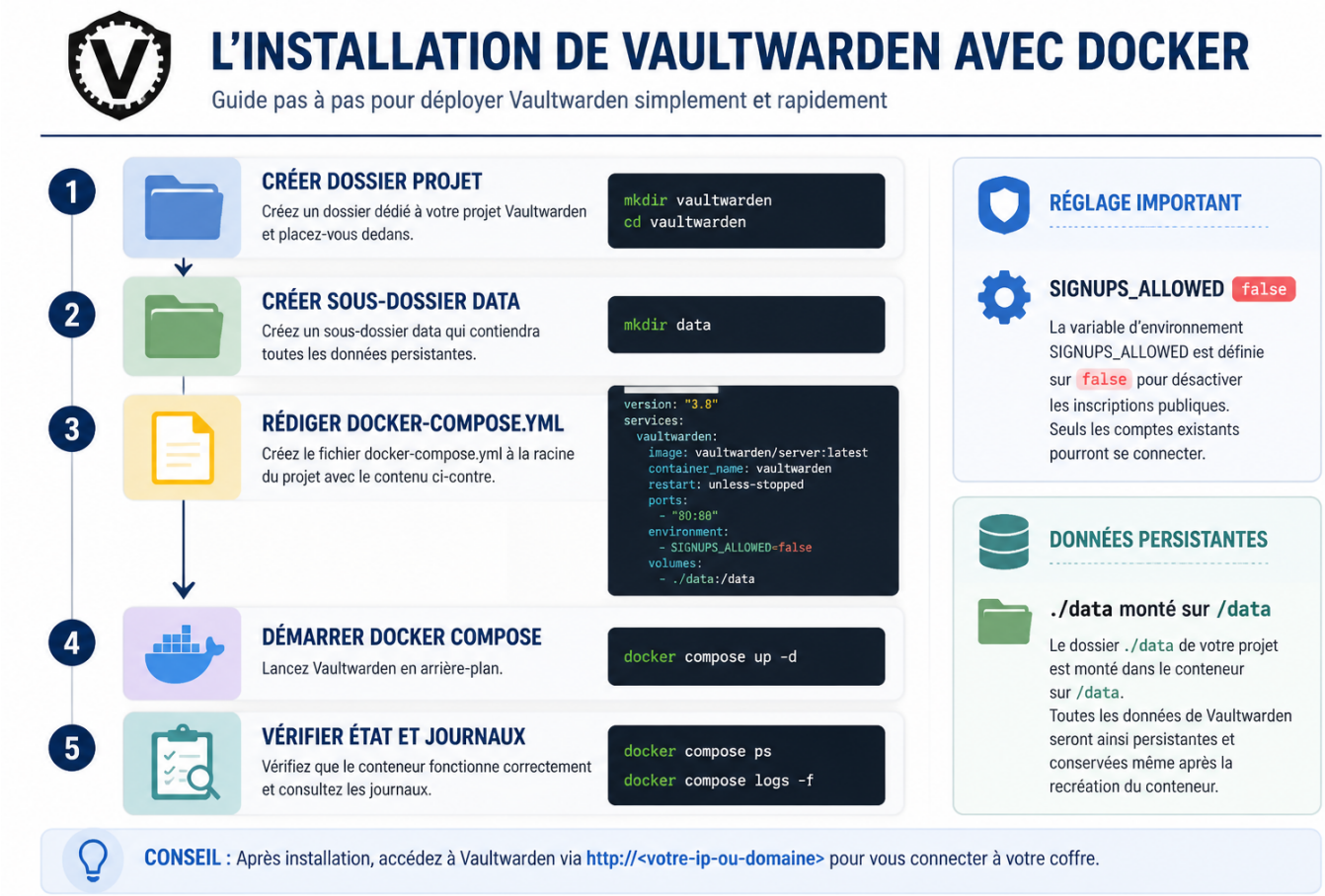


SCHÉMA *Organisation attendue : Docker Compose et volume de données persistant.*

3. Sécuriser l'accès au coffre

Placer Vaultwarden derrière un reverse proxy
Nginx ou Traefik peut recevoir les requêtes et les transmettre au conteneur.

Activer un accès HTTPS valide
Un accès distant doit utiliser une adresse HTTPS stable, notamment pour les clients Bitwarden.

Limiter la surface exposée
Le reverse proxy gère habituellement les connexions HTTP et HTTPS ; évitez d'exposer inutilement le service.

Désactiver les inscriptions publiques
N'autorisez pas la création libre de comptes sur une instance personnelle ou familiale.

Protéger l'administration
Utilisez un jeton d'administration Argon2 et conservez-le de manière sûre.

Protéger l'accès d'administration au serveur
Le système hôte et son compte d'administration font partie du périmètre de sécurité du coffre.

4. Connecter vos appareils et vérifier l'usage

1 **Créer et vérifier le compte autorisé**
Après avoir fermé les inscriptions publiques, confirmez que seuls les utilisateurs prévus peuvent utiliser l'instance.

2 **Configurer les clients Bitwarden**
Vaultwarden est compatible avec l'écosystème Bitwarden : utilisez les applications, extensions de navigateur et applications de bureau Bitwarden en mode auto-hébergé.

3 **Renseigner l'adresse de votre serveur**
Configurez les clients avec l'adresse HTTPS de votre instance pour la synchronisation.

4 **Tester depuis les appareils utiles**
Contrôlez la connexion et la synchronisation depuis un navigateur et, si nécessaire, depuis un téléphone.

5 **Anticiper l'indisponibilité**
Un serveur indisponible peut empêcher la synchronisation de nouveaux éléments et compliquer l'accès depuis un nouvel appareil.

5. Routine d'exploitation à ne pas reporter

Point de contrôle	Ce que vous devez confirmer
Mises à jour	Le système, Docker, le reverse proxy et Vaultwarden suivent une routine de mise à jour maîtrisée.
Sauvegardes	Les données persistantes sont copiées vers un emplacement distinct du serveur.
Restauration	Une restauration a été testée : une sauvegarde non restaurable ne protège pas le coffre.
HTTPS	L'adresse distante reste accessible avec un certificat valide.
Inscriptions	Les inscriptions publiques demeurent désactivées après chaque évolution de configuration.
Accès	Les clients Bitwarden se synchronisent avec l'URL auto-hébergée attendue.

! **Le critère de réussite n'est pas le démarrage du conteneur**
Un Vaultwarden auto-hébergé devient fiable grâce à la durée : HTTPS correctement configuré, accès restreint, mises à jour régulières et sauvegardes réellement restaurables. Sans cette discipline, le gain de contrôle peut augmenter le risque.

Vaultwarden est un serveur communautaire compatible avec les clients Bitwarden. Vérifiez vos réglages et testez vos sauvegardes avant de confier des données importantes à l'instance.