SELF-HOST > PLAN FOR DEPLOYMENT

Auto-hébergez une Organisation

Auto-hébergez une Organisation

Étape 1 : Installez et déployez votre serveur

Avant de pouvoir auto-héberger une organisation, vous devrez installer et déployer Bitwarden sur votre serveur. Bitwarden peut être exécuté, en utilisant Docker, sur des machines Linux et Windows. Bien qu'il existe une variété de méthodes pour installer Bitwarden, y compris des méthodes pour des environnements hors ligne ou isolés, nous recommandons de commencer avec l'un de ces guides :

- Installer et Déployer - Linux
- Installer et Déployer - Windows

Étape 2 : Configurez les variables d'environnement de l'organisation

Certaines fonctionnalités utilisées par les organisations Bitwarden ne sont pas configurées par la procédure d'installation standard documentée dans les articles ci-dessus. Pour équiper votre serveur auto-hébergé avec toutes les fonctionnalités disponibles pour les organisations Bitwarden, définissez les variables suivantes dans votre fichier `./bwdata/env/global.override.env` :

Variable	Description	Utilise
globalSettings__mail__smtp__host=	Le nom d'hôte de votre serveur SMTP (recommandé) ou adresse IP.	Utilisé pour inviter des utilisateurs à votre organisation.
globalSettings__mail__smtp__port=	Le port SMTP utilisé par le serveur SMTP.	Utilisé pour inviter des utilisateurs à votre organisation.
globalSettings__mail__smtp__ssl=	(Boolean) Si votre serveur SMTP utilise un protocole de chiffrement : `vrai` = SSL `faux` = TLS	Utilisé pour inviter des utilisateurs à votre organisation.
globalSettings__mail__smtp__nomd'utilisateur=	Un nom d'utilisateur valide pour le `smtp__host`.	Utilisé pour inviter des utilisateurs à votre organisation.
globalSettings__mail__smtp__motdepasse=	Un mot de passe valide pour le `smtp__username`.	Utilisé pour inviter des utilisateurs à votre organisation.

Variable	Description	Utilise
globalSettings__enableCloudCommunication=	Définissez sur `vrai` pour permettre la communication entre votre serveur et notre système cloud.	Utilisé pour la facturation et la synchronisation de licence.
globalSettings__duo__aKey=	Une clé Duo générée aléatoirement. Pour plus d'informations, consultez la Documentation de Duo.	Utilisé pour l'identifiant en deux étapes à l'échelle de l'organisation via Duo.
globalSettings__hibpApiKey=	Votre clé API HavelBeenPwned (HIBP), disponible ici.	Permet aux utilisateurs d'exécuter le rapport de brèche de données et de vérifier la présence de leur mot de passe principal dans les brèches lorsqu'ils créent un compte.
globalSettings__désactiverEnregistrementUtilisateur=	Spécifiez `vrai` pour désactiver l'inscription de nouveaux utilisateurs à un compte sur cette instance via la page d'inscription.	Utilisé pour limiter les utilisateurs sur le serveur à ceux invités à l'organisation.
globalSettings__sso__enforceSsoPolicyForAllUsers=	Spécifiez `vrai` pour appliquer la politique de Exiger l'authentification SSO pour les rôles de propriétaire et d'admin.	Utilisé pour appliquer la politique de Exiger l'authentification SSO pour les rôles de propriétaire et d'admin.

Une fois que vous avez apporté des modifications à vos variables d'environnement, effectuez un `./bitwarden.sh restart` pour appliquer les modifications à votre serveur.

Étape 3 : Commencez votre organisation

Commencez une organisation cloud

À ce stade, vous êtes prêt à démarrer votre organisation et à la transférer sur votre serveur auto-hébergé. Pour des raisons de facturation, les organisations doivent d'abord être créées dans le coffre web cloud Bitwarden (https://vault.bitwarden.com). Suivez ces instructions pour créer une organisation.

Commencez une organisation auto-hébergée

Une fois votre organisation cloud créée, suivez ces instructions pour récupérer votre licence du cloud et la téléverser sur votre serveur auto-hébergé afin de créer une copie auto-hébergée de l'organisation.

Les organisations Bitwarden auto-hébergées pourront utiliser toutes les fonctionnalités payantes fournies par leur plan choisi. Seules les Familles et les organisations Entreprise peuvent être importées sur des serveurs auto-hébergés. En savoir plus ici.

Étape 4 : Configurer la facturation et synchroniser la licence

Ensuite, configurez votre organisation auto-hébergée pour la facturation et la synchronisation de licence depuis votre organisation cloud. Le faire est facultatif, mais aura quelques avantages :

- Permettre une mise à jour de licence plus facile lorsque vous changez le nombre de sièges de votre organisation.
- Permettant une mise à jour de licence plus facile lorsque votre abonnement arrive à sa date de renouvellement.
- Débloquez des organisations familiales parrainées pour les membres des organisations Enterprise.

Suivez ces instructions pour configurer la facturation et la synchronisation de licence pour votre organisation.

> **ⓘ Note**
>
> La facturation et la synchronisation des licences nécessitent que la variable d'environnement `paramètresGlobaux__activerCommunicationCloud=` soit définie sur `vrai` (en savoir plus).

Étape 5 : Commencez l'administration de l'organisation

Vous êtes maintenant prêt à commencer à administrer votre organisation auto-hébergée ! Voici comment vous pourriez l'aborder :

⇒Gestionnaire de Mots de Passe

Invitez votre équipe admin

Chaque organisation all-star a besoin d'une équipe admin all-star. Commencez à inviter des membres hautement privilégiés qui peuvent vous aider à construire une base pour le partage sécurisé des identifiants avec Bitwarden. Si vous construisez une organisation d'Entreprise, vous pouvez donner aux membres des autorisations personnalisées hautement flexibles pour répondre à vos besoins.

Pour une redondance protectrice, nous recommandons d'inclure au moins un autre **propriétaire d'organisation** dans votre nouvelle équipe admin.

Définir les politiques de sécurité (uniquement pour l'Entreprise)

Votre entreprise a des besoins de sécurité uniques. Utilisez les politiques de sécurité pour construire un déploiement et une expérience cohérents pour tous les membres de l'équipe, comme exiger une authentification SSO ou inscrire les membres dans la réinitialisation du mot de passe admin. Pour préparer votre organisation à accueillir plus de membres d'équipe, il est important de définir vos politiques de sécurité tôt.

Importez votre donnée

Votre entreprise passe-t-elle à Bitwarden à partir d'un autre gestionnaire de mots de passe? Bonne nouvelle ! Vous pouvez importer ces données directement dans votre organisation pour éviter une journée douloureuse de copier-coller.

Construisez des groupes et des collections

Une fois que vous avez des éléments dans votre coffre, c'est le bon moment pour configurer des collections et des groupes pour garantir que les bons utilisateurs ont accès aux bonnes informations d'identification. Chaque organisation est différente, mais voici quelques conseils pour vous aider à commencer avec les collections et à commencer avec les groupes.

Invitez votre équipe

Il est enfin temps de commencer à inviter les utilisateurs ! Si vous utilisez un fournisseur d'identité ou un service d'annuaire comme Azure Active Directory, utilisez SCIM ou Directory Connector pour synchroniser automatiquement les utilisateurs. Sinon, suivez les mêmes étapes que vous avez prises pour construire votre équipe admin pour inviter plus d'utilisateurs à l'organisation.

⇒Secrets Manager

Invitez votre équipe admin

Chaque organisation de tous les étoiles a besoin d'une équipe admin de tous les étoiles. Commencez à inviter des membres hautement privilégiés qui peuvent vous aider à construire une base pour le partage sécurisé de secrets avec Bitwarden.

Pour une redondance protectrice, nous recommandons d'inclure au moins un autre **propriétaire d'organisation** dans votre nouvelle équipe admin.

Définir les politiques de sécurité

Votre entreprise a des besoins de sécurité uniques. Utilisez les politiques de sécurité pour construire un déploiement et une expérience cohérents pour tous les membres de l'équipe, comme exiger une authentification SSO ou inscrire les membres dans la réinitialisation du mot de passe admin. Pour préparer votre organisation à accueillir plus de membres d'équipe, il est important de définir vos politiques de sécurité tôt.

Importez votre donnée

Votre entreprise passe-t-elle à Bitwarden à partir d'un autre Secrets Manager ? Bonne nouvelle ! Vous pouvez importer ces données directement dans votre organisation pour éviter une journée douloureuse de copier-coller.

Invitez votre équipe

Il est enfin temps de commencer à inviter des utilisateurs ! Si vous utilisez un fournisseur d'identité ou un service d'annuaire comme Azure Active Directory, utilisez SCIM ou Directory Connector pour synchroniser automatiquement les utilisateurs. Sinon, suivez les mêmes étapes que vous avez prises pour construire votre équipe admin pour inviter plus d'utilisateurs à l'organisation. Une fois que tout le monde est intégré, commencez à donner aux utilisateurs l'accès à Secrets Manager.