CONSOLE ADMIN > GESTION DES UTILISATEURS >

Synchronisation avec Active Directory ou LDAP

Synchronisation avec Active Directory ou LDAP

Cet article vous aidera à commencer à utiliser Directory Connector pour synchroniser les utilisateurs et les groupes de votre service LDAP ou Active Directory vers votre organisation Bitwarden. Bitwarden propose des connecteurs intégrés pour les serveurs de répertoire LDAP les plus populaires, y compris :

- Microsoft Active Directory
- Serveur de répertoire Apache (ApacheDS)
- Apple Open Directory
- Serveur de répertoire Fedora
- Novell eDirectory
- OpenDS
- OpenLDAP
- Sun Directory Server Enterprise Edition (DSEE)
- Tout serveur de répertoire LDAP générique

Connectez-vous à votre serveur

Suivez les étapes suivantes pour configurer le connecteur de répertoire pour utiliser votre LDAP ou Active Directory :

1. Ouvrez l'application de bureau Directory Connector.
2. Allez dans l'onglet **Paramètres**.
3. Dans le menu déroulant **Type**, sélectionnez **Active Directory ou LDAP**.

   Les champs disponibles dans cette section changeront en fonction du type sélectionné.
4. Configurez les options suivantes :

Option	Description	Exemples
Nom d'hôte du serveur	Nom d'hôte de votre serveur de répertoire.	`ad.exemple.com`, `ldap.entreprise.org`
Port du serveur	Port sur lequel votre serveur de répertoire écoute.	`389` ou `10389`
Chemin Racine	Chemin racine où Directory Connector doit démarrer toutes les requêtes.	`cn=utilisateurs,dc=ad,dc=exemple,dc=com,d`

Option	Description	Exemples
		`c=ldap`, `dc=entreprise`, `dc=org`
Ce serveur utilise Active Directory	Cochez cette case si le serveur est un serveur Active Directory.	
Ce serveur pagine les résultats de recherche	Cochez cette case si le serveur pagine les résultats de recherche (uniquement LDAP).	
Ce serveur utilise une connexion cryptée	Cocher cette case vous invitera à sélectionner l'une des options suivantes : **Utiliser SSL** (LDAPS) Si votre serveur LDAPS utilise un certificat non approuvé, vous pouvez configurer les options de certificat sur cet écran. **Utilisez TSL** (STARTTLS) Si votre serveur LDAP utilise un certificat auto-signé pour STARTTLS, vous pouvez configurer les options de certification sur cet écran.	
Nom d'utilisateur	Le nom distingué d'un utilisateur administratif que l'application utilisera lors de la connexion au serveur de répertoire. Pour **Active Directory**, si la synchronisation de l'état des utilisateurs supprimés du répertoire est souhaitée, l'utilisateur doit être un membre du groupe administrateurs intégré.	
Mot de passe	Le mot de passe de l'utilisateur spécifié ci-dessus. Le mot de passe est stocké en toute sécurité dans le gestionnaire de références d'identification natif du système d'exploitation.	

Configurer les options de synchronisation

> **Tip**
>
> Lorsque vous avez terminé la configuration, allez dans l'onglet **Plus** et sélectionnez le bouton **Effacer le cache de synchronisation** pour éviter d'éventuels conflits avec les opérations de synchronisation précédentes. Pour plus d'informations, consultez Vider le cache de synchronisation.

Suivez les étapes suivantes pour configurer les paramètres utilisés lors de la synchronisation à l'aide de Directory Connector:

> **Note**
> Si vous utilisez Active Directory, beaucoup de ces paramètres sont prédéterminés pour vous et ne sont donc pas affichés.

1. Ouvrez l'application de bureau Directory Connector.
2. Allez dans l'onglet **Paramètres**.
3. Dans la section **Synchronisation**, configurez les options suivantes comme vous le souhaitez :

Option	Description
Intervalle	Temps entre la vérification automatique de synchronisation (en minutes).
Supprimer les utilisateurs désactivés lors de la synchronisation	Cochez cette case pour supprimer les utilisateurs de l'organisation Bitwarden qui ont été désactivés dans votre organisation.
Remplacer les utilisateurs existants de l'organisation en fonction des paramètres de synchronisation actuels	Cochez cette case pour remplacer complètement l'utilisateur défini à chaque synchronisation, y compris la suppression des utilisateurs de votre organisation lorsqu'ils sont absents de l'ensemble des utilisateurs du répertoire. **Si pour une raison quelconque une synchronisation vide est exécutée lorsque cette option est activée, Directory Connector supprimera tous les utilisateurs.** Exécutez toujours une synchronisation de test avant de synchroniser après avoir activé cette option.
Plus de 2000 utilisateurs ou groupes sont prévus pour la synchronisation	Cochez cette case si vous prévoyez de synchroniser plus de 2000 utilisateurs ou groupes. Si vous ne cochez pas cette case, Directory Connector limitera une synchronisation à 2000 utilisateurs ou groupes.
Attribut de membre	Nom de l'attribut utilisé par le répertoire pour définir l'adhésion d'un groupe (par exemple, `uniqueMember`).
Attribut de date de création	Nom de l'attribut utilisé par le répertoire pour spécifier quand une entrée a été créée (par exemple, `whenCreated`).

Option	Description
Attribut de date de révision	Nom de l'attribut utilisé par le répertoire pour spécifier quand une entrée a été modifiée pour la dernière fois (par exemple, `whenChanged`).
Si un utilisateur n'a pas d'adresse e-mail, combinez un préfixe de nom d'utilisateur avec une valeur de suffixe pour former une adresse e-mail	Cochez cette case pour former des options d'adresses e-mail valides pour les utilisateurs qui n'ont pas d'adresse e-mail. **Les utilisateurs sans adresses e-mail réelles ou formées seront ignorés par Directory Connector.** E-mail formé = **Attribut du Préfixe de l'e-mail** + **Suffixe de l'e-mail**
Attribut du Préfixe de l'e-mail	Attribut utilisé pour créer un préfixe pour les adresses e-mail formées.
Suffixe de l'e-mail	Une chaîne (`@example.com`) utilisée pour créer un suffixe pour les adresses e-mail formées.
Synchronisation des utilisateurs	Cochez cette case pour synchroniser les utilisateurs à votre organisation. Cocher cette case vous permettra de spécifier un **Filtre d'utilisateur**, un **Chemin d'utilisateur**, une **Classe d'objet utilisateur**, et un **Attribut d'e-mail d'utilisateur**.
Filtre Utilisateur	Consultez Spécifier les filtres de synchronisation.
Chemin d'utilisateur	Attribut utilisé avec le **Chemin racine** spécifié pour rechercher des utilisateurs (par exemple, `ou=users`). Si aucune valeur n'est fournie, la recherche de sous-arborescence commencera à partir du chemin racine.
Classe d'objet utilisateur	Nom de la classe utilisée pour l'objet utilisateur LDAP (par exemple, `user`).
Attribut d'e-mail d'utilisateur	Attribut à utiliser pour charger l'adresse e-mail enregistrée d'un utilisateur.

Option	Description
Synchroniser les groupes	Cochez cette case pour synchroniser les groupes à votre organisation. Cocher cette case vous permettra de spécifier un **Filtre de groupe**, un **Chemin de groupe**, une **Classe d'objet de groupe**, **Attribut de nom de groupe**.
Filtre de groupe	Consultez Spécifier les filtres de synchronisation.
Chemin de groupe	Attribut utilisé avec le **Chemin racine** spécifié pour rechercher des groupes (par exemple, `ou=groups`). Si aucune valeur n'est fournie, la recherche de sous-arborescence commencera à partir du chemin racine.
Classe d'objet groupe	Nom de la classe utilisée pour l'objet de groupe LDAP (par exemple, `groupOfUniqueNames`).
Attribut de nom de groupe	Nom de l'attribut utilisé par le répertoire pour définir le nom d'un groupe (par exemple, `name`).

Spécifiez les filtres de synchronisation

Les filtres d'utilisateur et de groupe peuvent être sous la forme de n'importe quel filtre de recherche compatible avec LDAP.

Active Directory offre des options avancées et des limitations pour écrire des filtres de recherche, par rapport aux directives LDAP standard. Apprenez-en plus sur comment écrire des filtres de recherche Active Directory ici.

> **Note**
> Les groupes imbriqués peuvent synchroniser plusieurs objets de groupe avec un seul référent dans Directory Connector. Faites cela en créant un groupe dont les membres sont d'autres groupes.

Échantillons

Pour filtrer une synchronisation pour toutes les entrées qui ont `objectClass=user` et `cn` (nom commun) contenant `Marketing` :

```
Bash

(&(objectClass=user)(cn=*Marketing*))
```

(**LDAP-uniquement**) Pour filtrer une synchronisation pour toutes les entrées avec un composant `ou` (unité d'organisation) de leur `dn` (nom distinctif) qui est soit `Miami` soit `Orlando` :

```
Bash

(|(ou:dn:=Miami)(ou:dn:=Orlando))
```

(**LDAP-uniquement**) Pour exclure les entités qui correspondent à une expression, par exemple toutes les entrées `ou=Chicago` *sauf* celles qui correspondent également à un attribut `ou=Wrigleyville` :

```
Bash

(&(ou:dn:=Chicago)(!(ou:dn:=Wrigleyville)))
```

(**AD uniquement**) Pour filtrer une synchronisation pour les utilisateurs dans le groupe `Heroes` :

```
Bash

(&(objectCategory=Person)(sAMAccountName=*)(memberOf=cn=Heroes,ou=users,dc=company,dc=com))
```

(**AD uniquement**) Pour filtrer une synchronisation pour les utilisateurs qui sont membres du groupe `Heroes`, soit par annuaire, soit par imbrication :

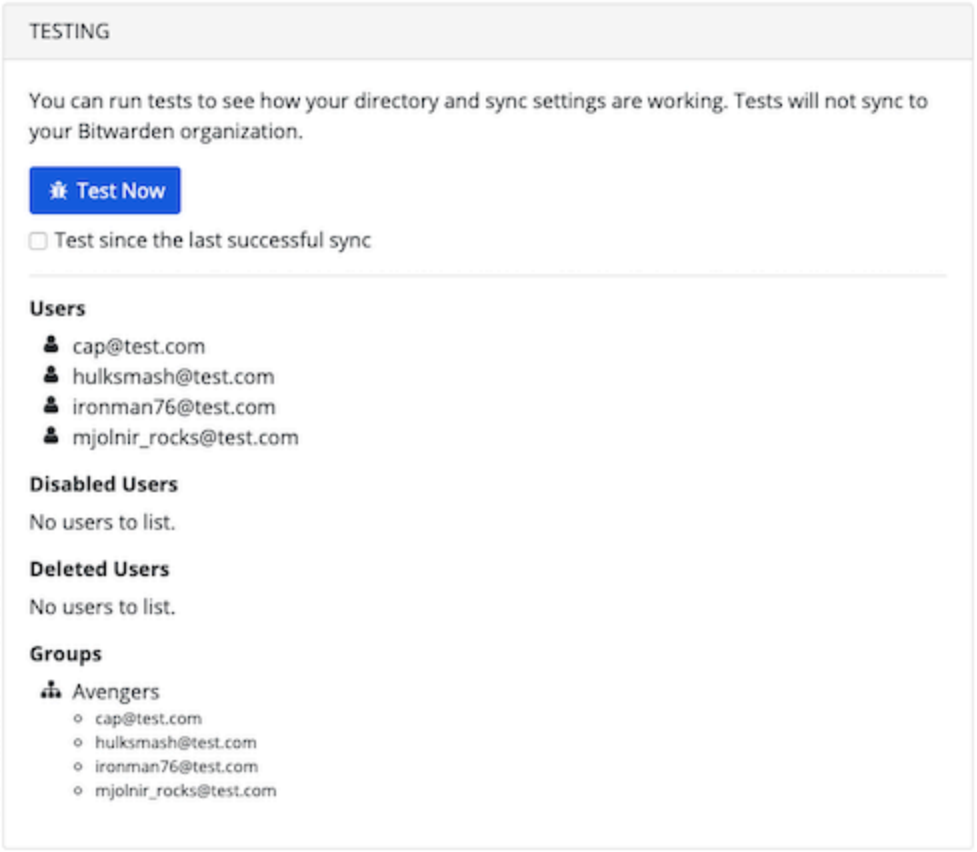
```
Bash

(&(objectCategory=Person)(sAMAccountName=*)(memberOf:1.2.840.113556.1.4.1941:=cn=Heroes,ou=users,dc=company,dc=com))
```

Testez une synchronisation

> **Tip**
> Avant de tester ou d'exécuter une synchronisation, vérifiez que Directory Connector est connecté au bon serveur cloud (par exemple, US ou EU) ou au serveur auto-hébergé. Apprenez comment faire avec l'application de bureau ou le CLI.

Pour vérifier si Directory Connector se connectera avec succès à votre répertoire et renverra les utilisateurs et les groupes souhaités, allez dans l'onglet **Tableau de bord** et sélectionnez le bouton **Tester maintenant**. Si la synchronisation réussit, les utilisateurs et les groupes seront affichés dans la fenêtre du Directory Connector selon les options de synchronisation et les filtres spécifiés :



Résultats du test de synchronisation

Démarrer la synchronisation automatique

Une fois que les options de synchronisation et les filtres sont configurés et testés, vous pouvez commencer à synchroniser. Suivez les étapes suivantes pour commencer la synchronisation automatique avec Directory Connector :

1. Ouvrez l'application de bureau Directory Connector.
2. Allez dans l'onglet **Tableau de bord**.
3. Dans la section **Synchronisation**, sélectionnez le bouton **Démarrer la synchronisation**.

   Vous pouvez également sélectionner le bouton **Synchroniser maintenant** pour exécuter une synchronisation manuelle unique.

Directory Connector commencera à interroger votre répertoire en fonction des options de synchronisation et des filtres configurés.

Si vous quittez ou fermez l'application, la synchronisation automatique s'arrêtera. Pour garder Directory Connector en cours d'exécution en arrière-plan, minimisez l'application ou cachez-la dans la barre des tâches.

> **Note**
>
> Si vous êtes sur le plan Teams Starter, vous êtes limité à 10 membres. Directory Connector affichera une erreur et arrêtera de synchroniser si vous essayez de synchroniser plus de 10 membres.

Dépannage de la synchronisation avec Active Directory

Limite de valeur atteinte lors de la synchronisation depuis une instance Active Directory :

Le `MaxValRange` de l'Active Directory a un paramètre par défaut de 1500. Si un attribut, tel que `membres` sur un groupe a plus de 1500 valeurs, Active Directory renverra à la fois un attribut `membres` vide, ainsi qu'une liste tronquée de `membres` sur des attributs séparés, jusqu'à la valeur de `MaxValRange`.

- Vous pouvez ajuster la politique de `MaxValRange` à une valeur supérieure au nombre de membres de votre plus grand groupe dans Active Directory. Consultez la documentation de Microsoft pour définir les politiques de sécurité LDAP d'Active Directory en utilisant l'utilitaire ntdsutll.exe.