Liaison entre Proxmox et AD (ldap)

Configuration ldap sur Proxmox

Sommaire

Méthodes

Il existe deux méthodes principales pour intégrer Proxmox à un annuaire Windows :

- **L’authentification Active Directory (AD)** : méthode native, utilisant le protocole sécurisé Kerberos. Elle permet une intégration directe avec les contrôleurs de domaine Windows, offrant une meilleure sécurité, une gestion centralisée des permissions et la prise en charge des stratégies de groupe.

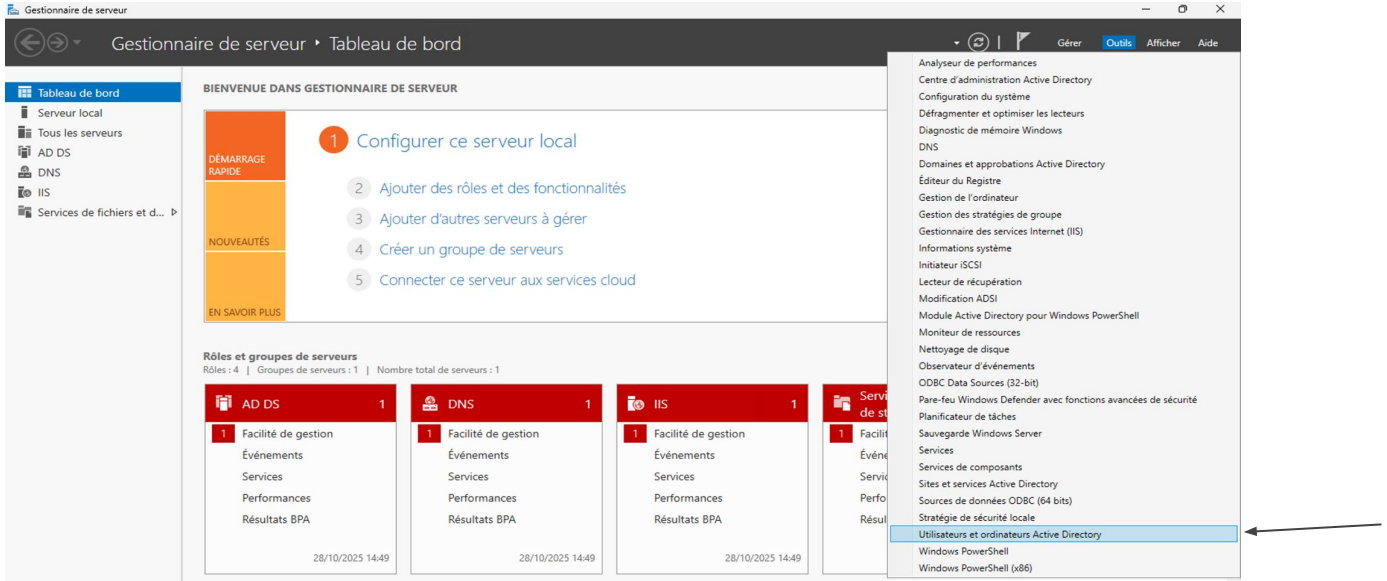
- **L’authentification LDAP ou LDAPS** : méthode basée sur le protocole LDAP (avec LDAPS pour la version sécurisée). Elle est plus flexible et peut être utilisée avec d’autres annuaires que Microsoft, mais nécessite davantage de configuration manuelle, notamment pour le chiffrement et la gestion des droits.

Parmi les deux méthodes disponibles, nous privilégierons l’intégration via **Active Directory**.
En effet, la méthode “Active Directory” dans Proxmox apporte une intégration native avec les mécanismes Windows, ce qui simplifie la configuration et renforce la sécurité, par rapport à un LDAP configuré manuellement.

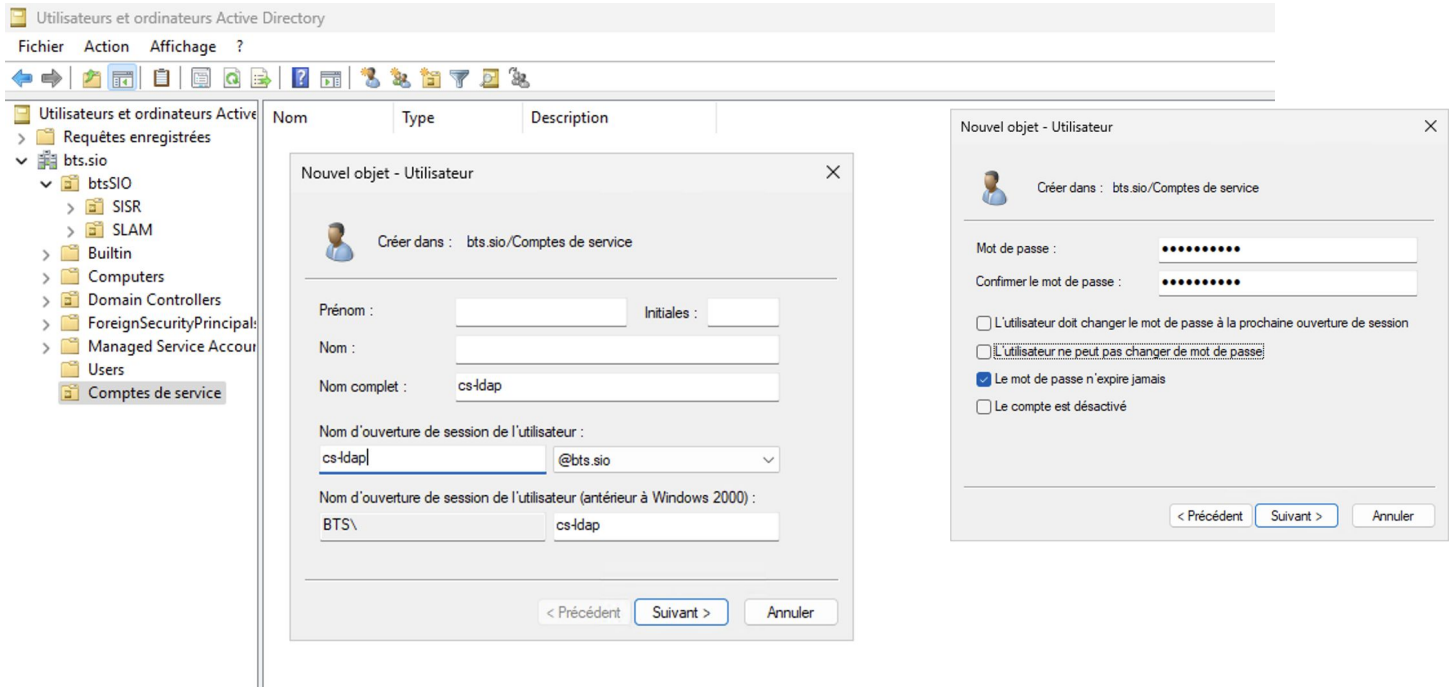
Compte de services

Avant la configuration sur Proxmox, ldap nécessite de créer un “compte de service”.
Un compte de service est un utilisateur dédié pour un service. Dans notre cas, ldap nécessite un accès d’authentification sur l’AD via un utilisateur. Cet utilisateur sera notre compte de service.

Sur le contrôleur de domaine DC01, ouvrir l’outil “utilisateur et groupe active directory”.



Créer le compte de service (utilisateur) dans l'Active Directory. Nous allons le nommer "**cs-ldap**"

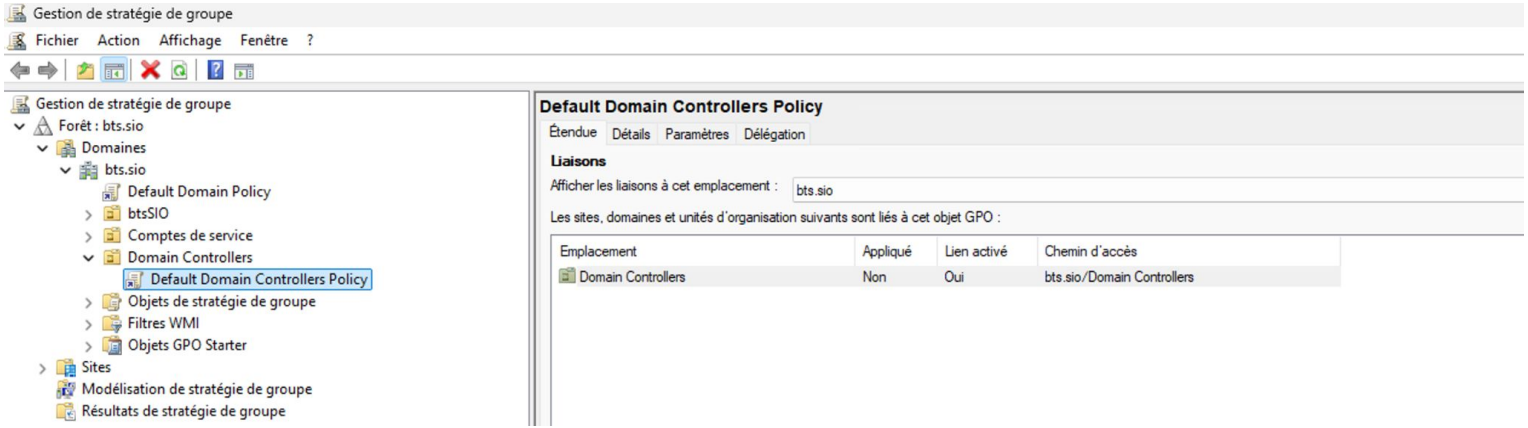


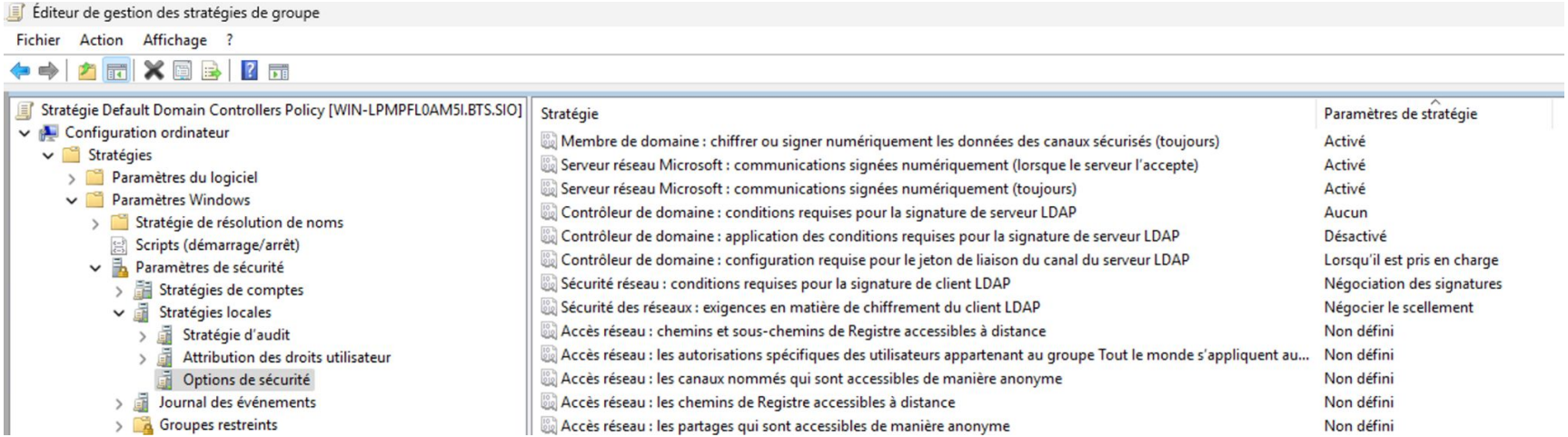
Ce compte servira à prendre les informations sur notre Active Directory via le protocole ldap.

GPO permissive pour LDAP (bypass du HTTPS)

Pour utiliser ldap sur le port 389, il faut modifier la stratégie de groupe du contrôleur de domaine afin de la rendre plus permissible.

Aller dans “gestion des stratégies de groupes” sur le DC01, puis modifier la stratégie appliquée au contrôleur de domaine :





Modifier :

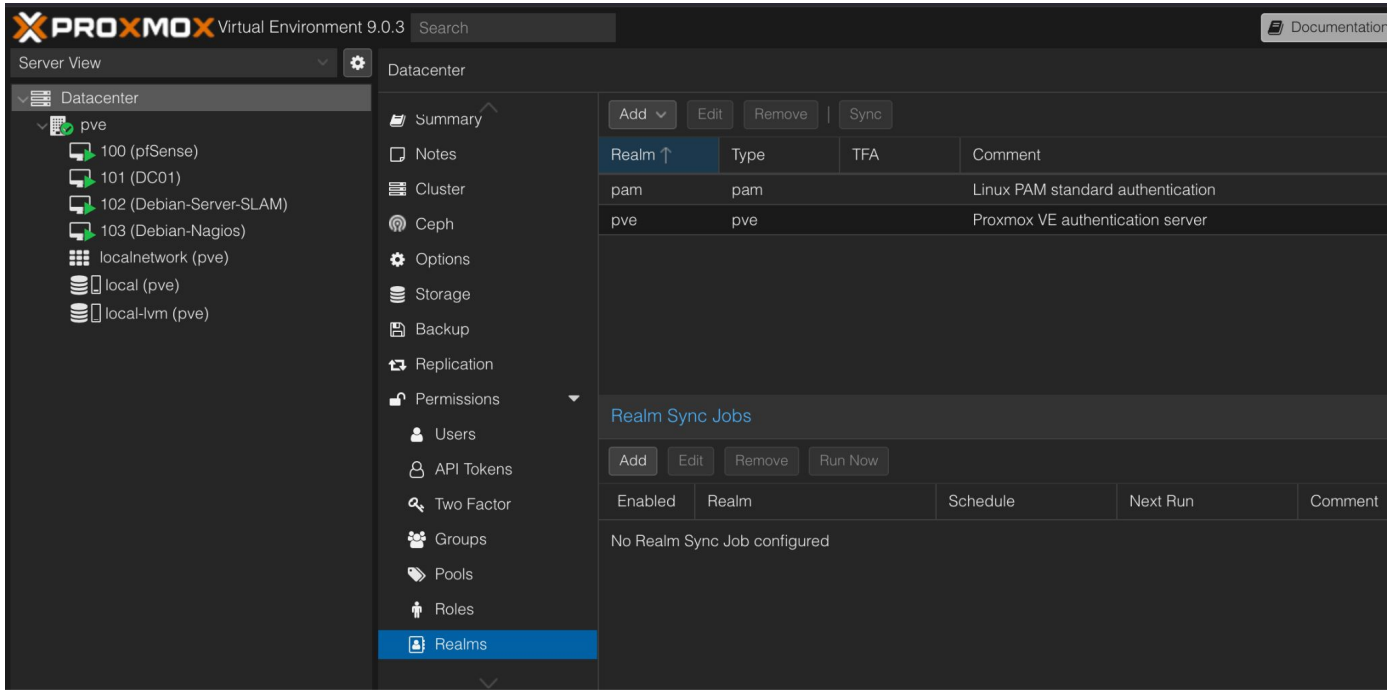
- Contrôleur de domaine : conditions requises pour la signature de serveur LDAP → **Désactivé**
- Contrôleur de domaine : application des conditions requises pour la signature de serveur LDAP → **Aucun**
- Contrôleur de domaine : configuration requise pour le jeton de liaison du canal du serveur LDAP → **Lorsqu'il est pris en charge**
- Sécurité réseau : conditions requise pour le jeton de liaison du canal du serveur LDAP → **Lorsqu'il est pris en charge**
- Sécurité des réseaux : exigences en matière de chiffrement du client LDAP → **Négocier le scellement**

Ensuite mettre à jour la stratégie sur le DC01 en ouvrant une invite de commande en mode admin :

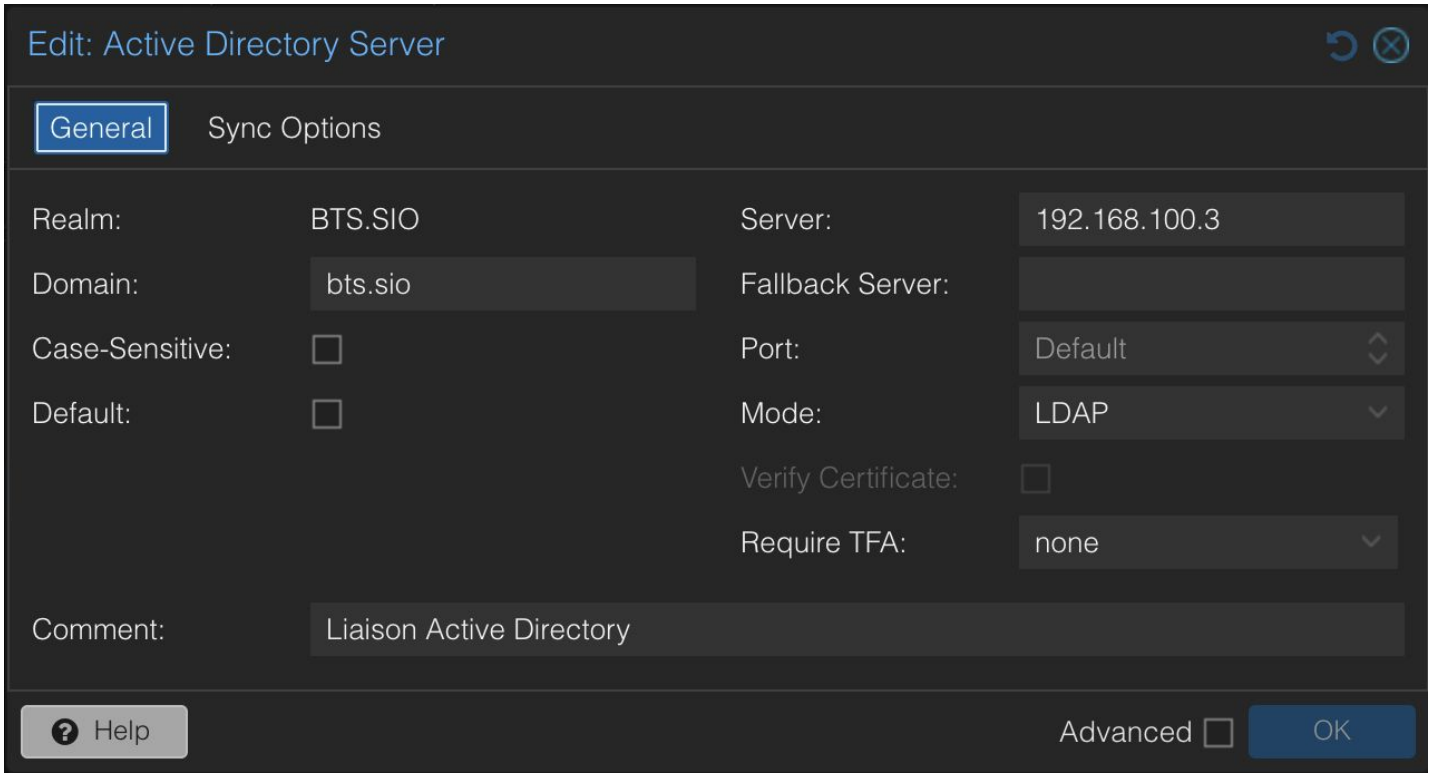
```
C:\Windows\System32>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

Liaison sur Proxmox

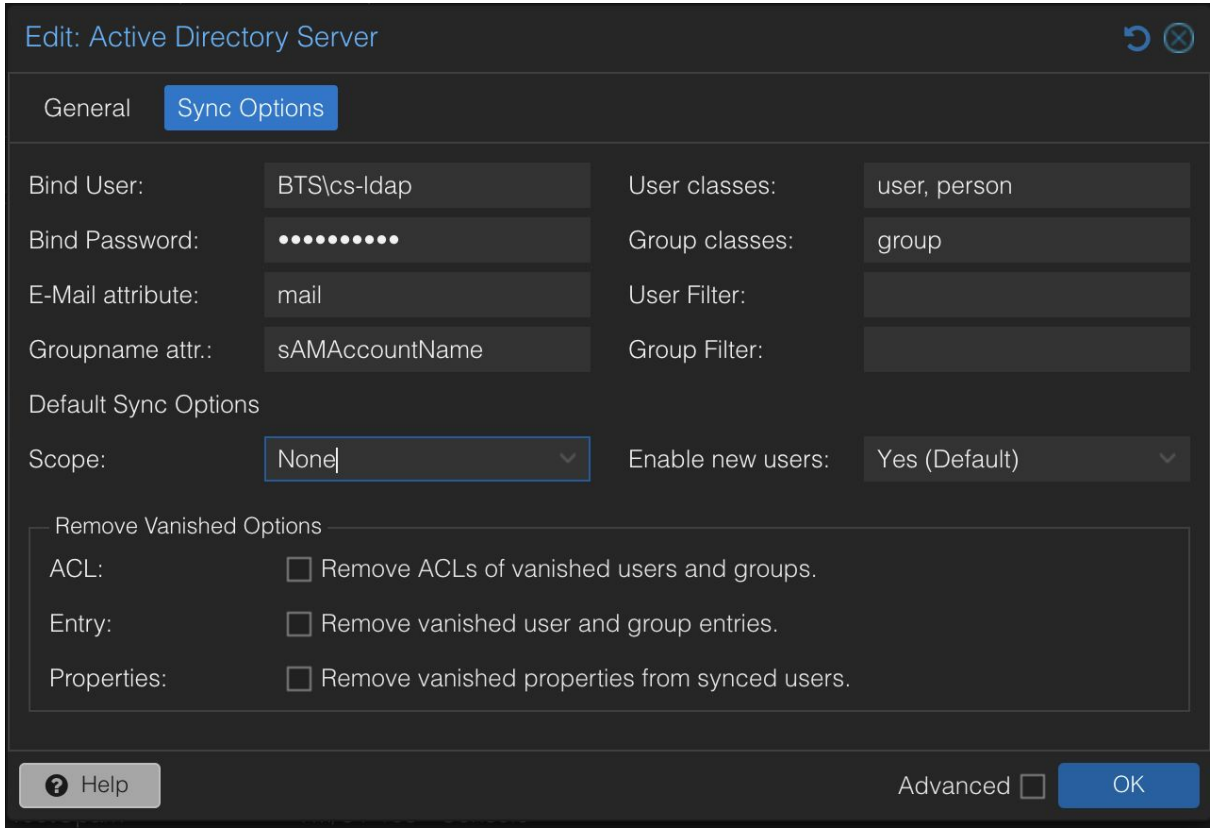
Aller dans Datacenter → Realms



Cliquer sur Add → Active Directory Server → onglet General

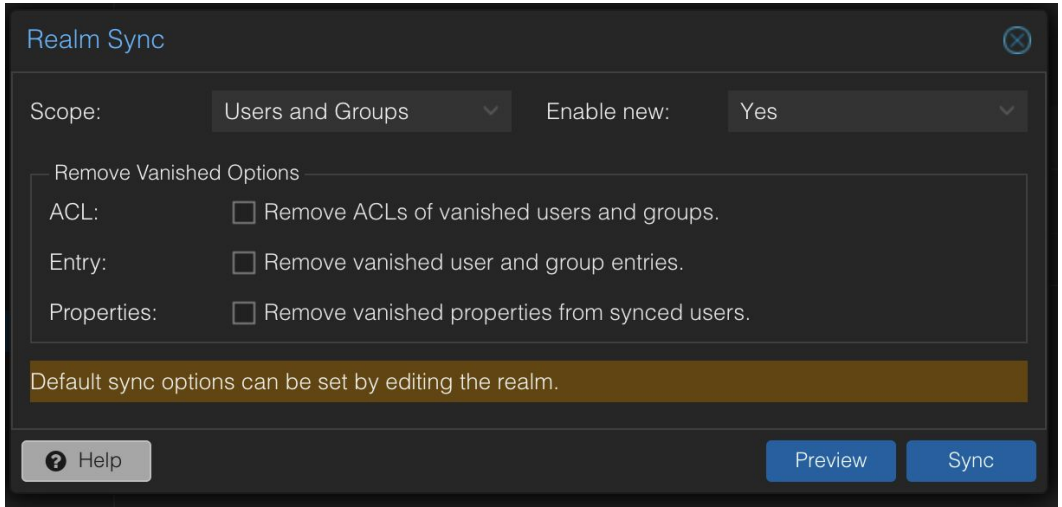


onglet Sync Options, renseigner les informations du compte de service :



Cliquer sur Sync

Ajouter “User and Group” pour synchroniser les deux, puis cliquer sur “Sync”



Connexion

- Utiliser le “sAmaccountName” c'est-à-dire le nom de connexion uniquement, ici “Remi”.
- Choisir le Realm “Liaison Active Directory

Ensuite cliquer sur Login