

Liaison entre Proxmox et AD (ldap)

Configuration ldap sur Proxmox



Sommaire

- [Méthodes](#)
- [Compte de services](#)
- [GPO \(bypass HTTPS\)](#)
- [Liaison sur Proxmox](#)
- [Connexion](#)



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**.

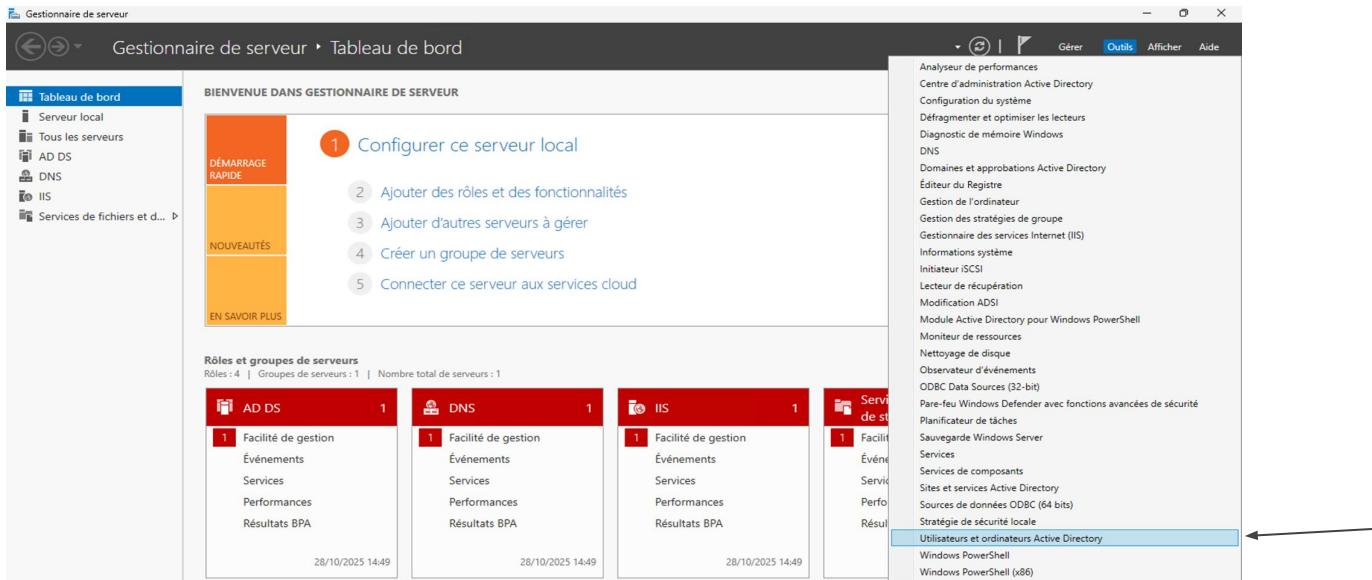
En effet, la méthode “Active Directory” dans Proxmox apporte une intégration native avec les mécanismes Windows, ce qui simplifie la configuration et renforce la sécurité, par rapport à un LDAP configuré manuellement.

Compte de services

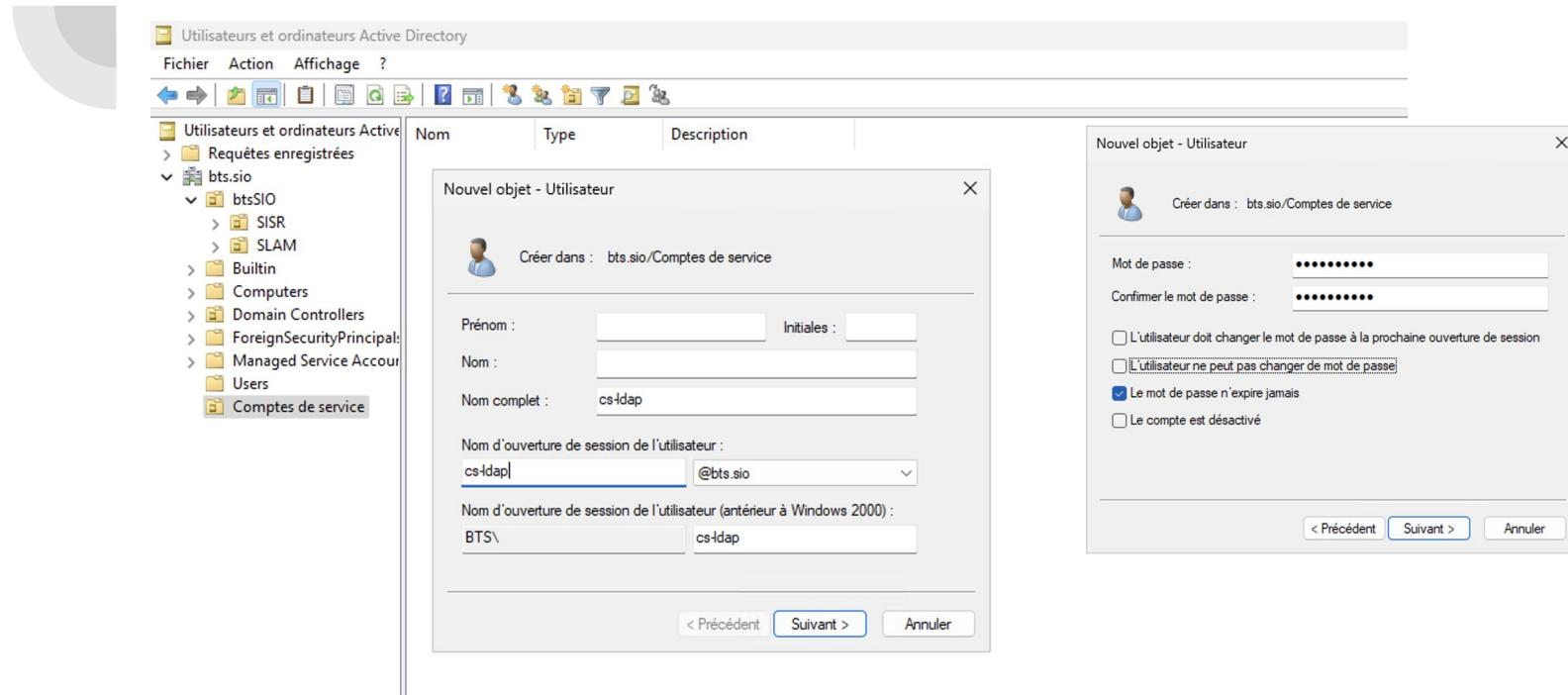
Avant la configuration sur Proxmox, l'ldap nécessite de créer un “compte de service”.

Un compte de service est un utilisateur dédié pour un service. Dans notre cas, l'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 permissive.

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

Gestion de stratégie de groupe

Fichier Action Affichage Fenêtre ?

Forêt : bts.sio

Domaines

bts.sio

- Default Domain Policy
- btsSIO
- Comptes de service
- Domain Controllers
- Default Domain Controllers Policy**
- Objets de stratégie de groupe
- Filtres WMI
- Objets GPO Starter

Sites

Modélisation de stratégie de groupe

Résultats de stratégie de groupe

Default Domain Controllers Policy

Étendue Détails Paramètres Délégation

Liaisons

Afficher les liaisons à cet emplacement : bts.sio

Les sites, domaines et unités d'organisation suivants sont liés à cet objet GPO :

Emplacement	Appliqué	Lien activé	Chemin d'accès
Domain Controllers	Non	Oui	bts.sio/Domain Controllers

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?



Stratégie	Paramètres de stratégie
Membre de domaine : chiffrer ou signer numériquement les données des canaux sécurisés (toujours)	Activé
Serveur réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)	Activé
Serveur réseau Microsoft : communications signées numériquement (toujours)	Activé
Contrôleur de domaine : conditions requises pour la signature de serveur LDAP	Aucun
Contrôleur de domaine : application des conditions requises pour la signature de serveur LDAP	Désactivé
Contrôleur de domaine : configuration requise pour le jeton de liaison du canal du serveur LDAP	Lorsqu'il est pris en charge
Sécurité réseau : conditions requises pour la signature de client LDAP	Négociation des signatures
Sécurité des réseaux : exigences en matière de chiffrement du client LDAP	Négocier le scellement
Accès réseau : chemins et sous-chemins de Registre accessibles à distance	Non défini
Accès réseau : les autorisations spécifiques des utilisateurs appartenant au groupe Tout le monde s'appliquent au...	Non défini
Accès réseau : les canaux nommés qui sont accessibles de manière anonyme	Non défini
Accès réseau : les chemins de Registre accessibles à distance	Non défini
Accès réseau : les partages qui sont accessibles de manière anonyme	Non défini

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

The screenshot shows the Proxmox Virtual Environment 9.0.3 interface. The left sidebar is titled "Server View" and shows a tree structure under "Datacenter". The "pve" node is expanded, showing sub-nodes: 100 (pfSense), 101 (DC01), 102 (Debian-Server-SLAM), 103 (Debian-Nagios), localnetwork (pve), local (pve), and local-lvm (pve). The "Realms" item in the sidebar is highlighted with a blue bar at the bottom.

The main panel is titled "Datacenter" and contains a "Realms" section. At the top of this section are buttons: "Add", "Edit", "Remove", and "Sync". Below these are two rows of data in a table:

Realm ↑	Type	TFA	Comment
pam	pam		Linux PAM standard authentication
pve	pve		Proxmox VE authentication server

Below the table is a section titled "Realm Sync Jobs" with buttons: "Add", "Edit", "Remove", and "Run Now". A message below states: "No Realm Sync Job configured".

Cliquer sur Add → Active Directory Server → onglet General

Edit: Active Directory Server

General Sync Options

Realm:	BTS.SIO	Server:	192.168.100.3
Domain:	bts.sio	Fallback Server:	
Case-Sensitive:	<input type="checkbox"/>	Port:	Default
Default:	<input type="checkbox"/>	Mode:	LDAP
		Verify Certificate:	<input type="checkbox"/>
		Require TFA:	none
Comment:	Liaison Active Directory		

Help Advanced OK

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

Edit: Active Directory Server

General Sync Options

Bind User:	BTS\cs-ldap	User classes:	user, person
Bind Password:	*****	Group classes:	group
E-Mail attribute:	mail	User Filter:	
Groupname attr.:	sAMAccountName	Group Filter:	

Default Sync Options

Scope:	None	Enable new users:	Yes (Default)
--------	------	-------------------	---------------

Remove Vanished Options

ACL:	<input type="checkbox"/> Remove ACLs of vanished users and groups.
Entry:	<input type="checkbox"/> Remove vanished user and group entries.
Properties:	<input type="checkbox"/> Remove vanished properties from synced users.

Help Advanced □ OK

Cliquer sur Sync



Realm ↑	Type	TFA	Comment
BTS.SIO	ad		Liaison Active Directory
pam	pam		Linux PAM standard authentication
pve	pve		Proxmox VE authentication server

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

Realm Sync

Scope: **Users and Groups** Enable new: **Yes**

Remove Vanished Options

ACL: Remove ACLs of vanished users and groups.

Entry: Remove vanished user and group entries.

Properties: Remove vanished properties from synced users.

Default sync options can be set by editing the realm.

Help Preview 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

Proxmox VE Login

User name: Remi

Password: (The password field is highlighted with a blue border.)

Realm: Liaison Active Directory

Language: English - English

Save User name: Login