

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**.

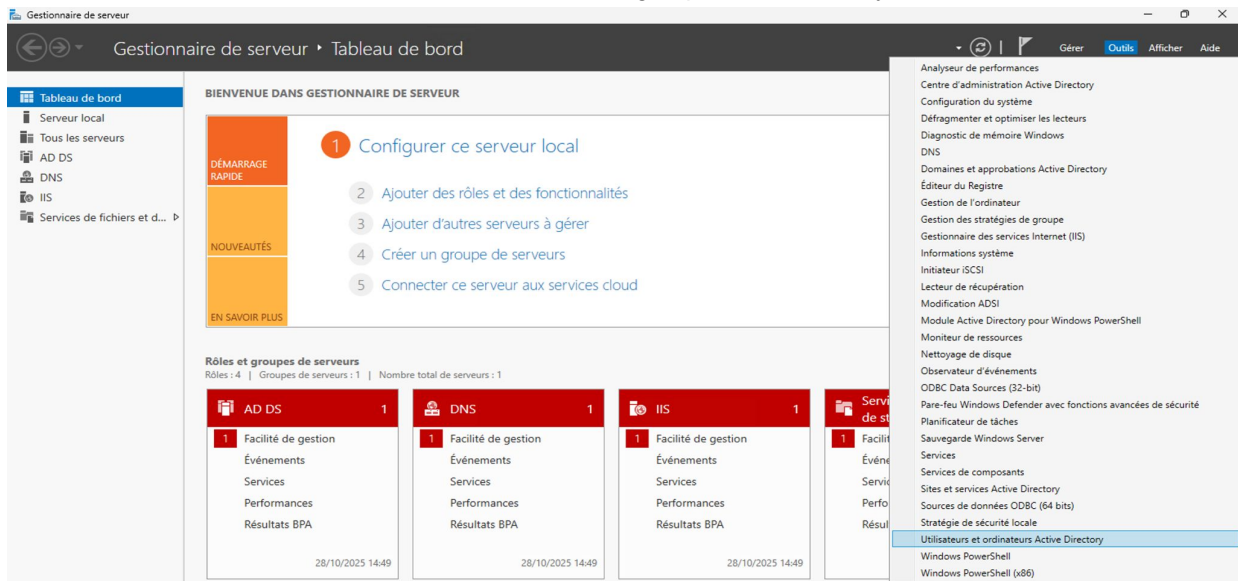
En effet, la méthode "Active Directory" dans Proxmox apporte une intégration native avec les mécanismes Windows, ce qui simplifie la configuration et renforce la sécurité, par rapport à un LDAP configuré manuellement.

Compte de services

Avant la configuration sur Proxmox, 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”.



The screenshot shows the Windows Server Management console. The left sidebar contains the 'Tableau de bord' (Dashboard) and a list of roles: 'Serveur local', 'Tous les serveurs', 'AD DS', 'DNS', 'IIS', and 'Services de fichiers et d...'. The main area displays a 'BIENVENUE DANS GESTIONNAIRE DE SERVEUR' (Welcome to Server Manager) page with a '1 Configurer ce serveur local' (Configure this server locally) task. Below this, there are sections for 'Rôles et groupes de serveurs' (Server roles and groups) and a list of installed roles: 'AD DS', 'DNS', 'IIS', and 'Services de fichiers et d...'. The 'AD DS' role is expanded, showing 'Facilité de gestion' (Management console), 'Événements' (Events), 'Services', 'Performances', and 'Résultats BPA' (BPA results). The 'Tools' menu is open, showing a list of tools including 'Analyseur de performances' (Performance analyzer), 'Centre d'administration Active Directory' (Active Directory Administrative Center), 'Configuration du système' (System configuration), 'Défragmenter et optimiser les lecteurs' (Defragment and optimize drives), 'Diagnostic de mémoire Windows' (Windows Memory Diagnostic), 'DNS', 'Domaines et approbations Active Directory' (Active Directory Domains and Groups), 'Éditeur du Registre' (Registry Editor), 'Gestion de l'ordinateur' (Computer Management), 'Gestion des stratégies de groupe' (Group Policy Management), 'Gestionnaire des services Internet (IIS)' (Internet Information Services (IIS) Manager), 'Informations système' (System Information), 'Initiateur iSCSI' (iSCSI Initiator), 'Lecteur de récupération' (Recovery Console), 'Modification ADSI' (ADSI Edit), 'Module Active Directory pour Windows PowerShell' (Active Directory Module for Windows PowerShell), 'Moniteur de ressources' (Resource Monitor), 'Nettoyage de disque' (Disk Cleanup), 'Observateur d'événements' (Event Viewer), 'ODBC Data Sources (32-bit)' (ODBC Data Sources (32-bit)), 'Pare-feu Windows Defender avec fonctions avancées de sécurité' (Windows Defender Firewall with Advanced Security), 'Planificateur de tâches' (Task Scheduler), 'Sauvegarde Windows Server' (Windows Server Backup), 'Services', 'Services de composants' (Component Services), 'Sites et services Active Directory' (Active Directory Sites and Services), 'Sources de données ODBC (64 bits)' (ODBC Data Sources (64-bit)), 'Stratégie de sécurité locale' (Local Security Policy), 'Utilisateurs et ordinateurs Active Directory' (Active Directory Users and Computers), 'Windows PowerShell', and 'Windows PowerShell (x86)'. The 'Utilisateurs et ordinateurs Active Directory' option is highlighted, and an arrow points to it.

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

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Utilisateurs et ordinateurs Active Directory

- Requêtes enregistrées
- bts.sio
 - btsSIO
 - SISR
 - SLAM
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users
 - Comptes de service

Nouvel objet - Utilisateur

Créer dans : bts.sio/Comptes de service

Prénom : Initiales :

Nom :

Nom complet : cs-ldap

Nom d'ouverture de session de l'utilisateur : cs-ldap @bts.sio

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : BTS\cs-ldap

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☒ L'utilisateur ne peut pas changer de mot de passe

☒ Le mot de passe n'expire jamais

☐ Le compte est désactivé

< Précédent Suivant > Annuler

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



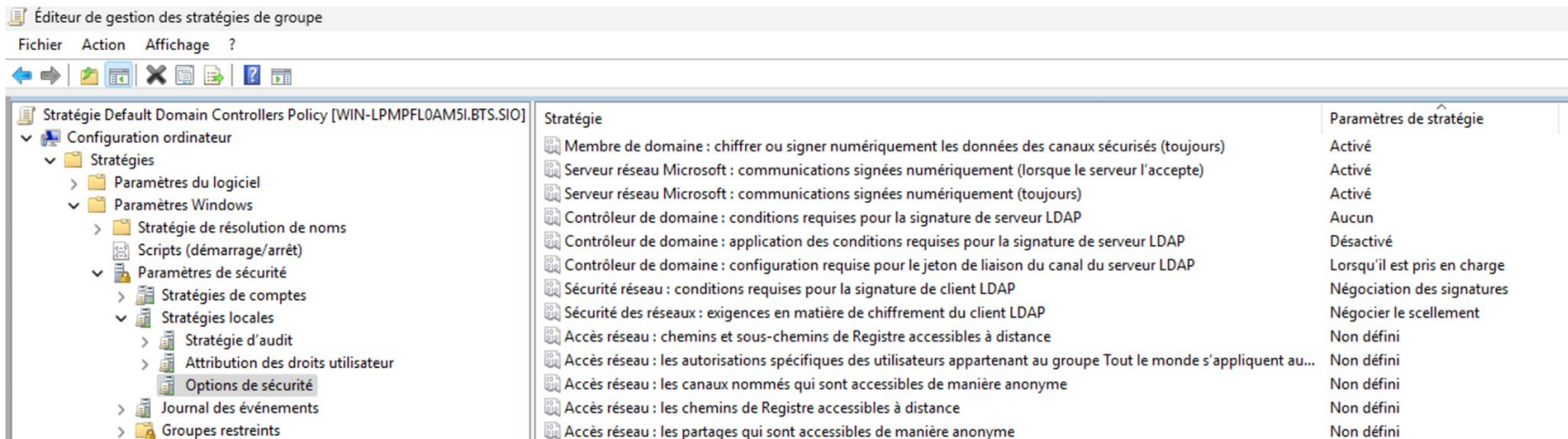
GPO permissive pour LDAP (bypass du HTTPS)

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 :

The screenshot shows the Group Policy Management console. On the left, the tree view is expanded to 'bts.sio' > 'Domain Controllers' > 'Default Domain Controllers Policy'. The right pane shows the 'Default Domain Controllers Policy' settings. Under the 'Liaisons' (Links) tab, the 'Afficher les liaisons à cet emplacement' (Show links at this location) is set to 'bts.sio'. Below this, a table lists the sites, domains, and organizational units linked to this GPO.

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



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**

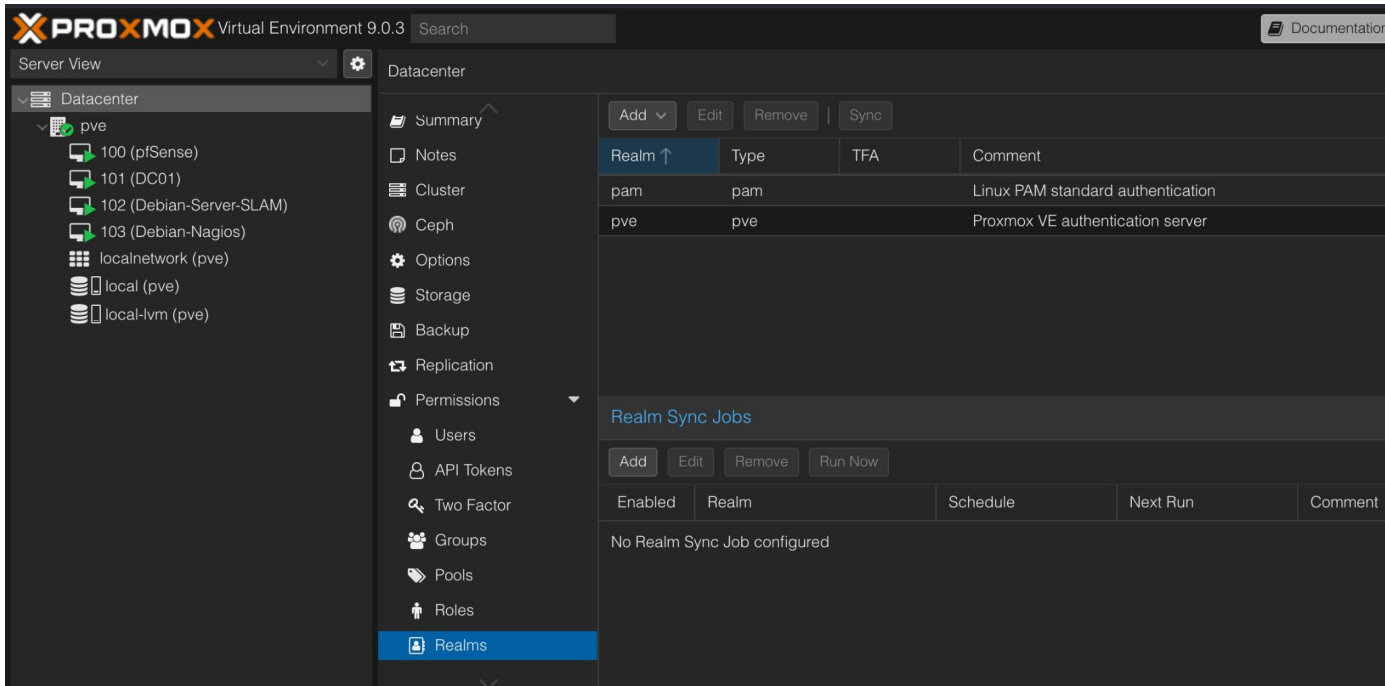
Ensuite mettre à jour la stratégie sur le DC01 en ouvrant une invite de commande en mode admin :

```
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 web interface. The left sidebar displays the 'Datacenter' tree with nodes: pve, 100 (pfSense), 101 (DC01), 102 (Debian-Server-SLAM), 103 (Debian-Nagios), localnetwork (pve), local (pve), and local-lvm (pve). The main panel is titled 'Datacenter' and shows the 'Realms' configuration page. The 'Realms' table lists two realms: 'pam' (Linux PAM standard authentication) and 'pve' (Proxmox VE authentication server). Below the table, the 'Realm Sync Jobs' section shows 'No Realm Sync Job configured'.

PROXMOX Virtual Environment 9.0.3 Search Documentation

Server View Datacenter

Datacenter

- ▼ Datacenter
 - ▼ pve
 - 100 (pfSense)
 - 101 (DC01)
 - 102 (Debian-Server-SLAM)
 - 103 (Debian-Nagios)
 - localnetwork (pve)
 - local (pve)
 - local-lvm (pve)

Summary

Notes

Cluster

Ceph

Options

Storage

Backup

Replication

Permissions

Users

API Tokens

Two Factor

Groups

Pools

Roles

Realms

Add Edit Remove Sync


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

Realm Sync Jobs

Add Edit Remove Run Now

Enabled	Realm	Schedule	Next Run	Comment
No Realm Sync Job configured				

Cliquer sur Add → Active Directory Server → onglet General



Edit: Active Directory Server

General

Sync Options

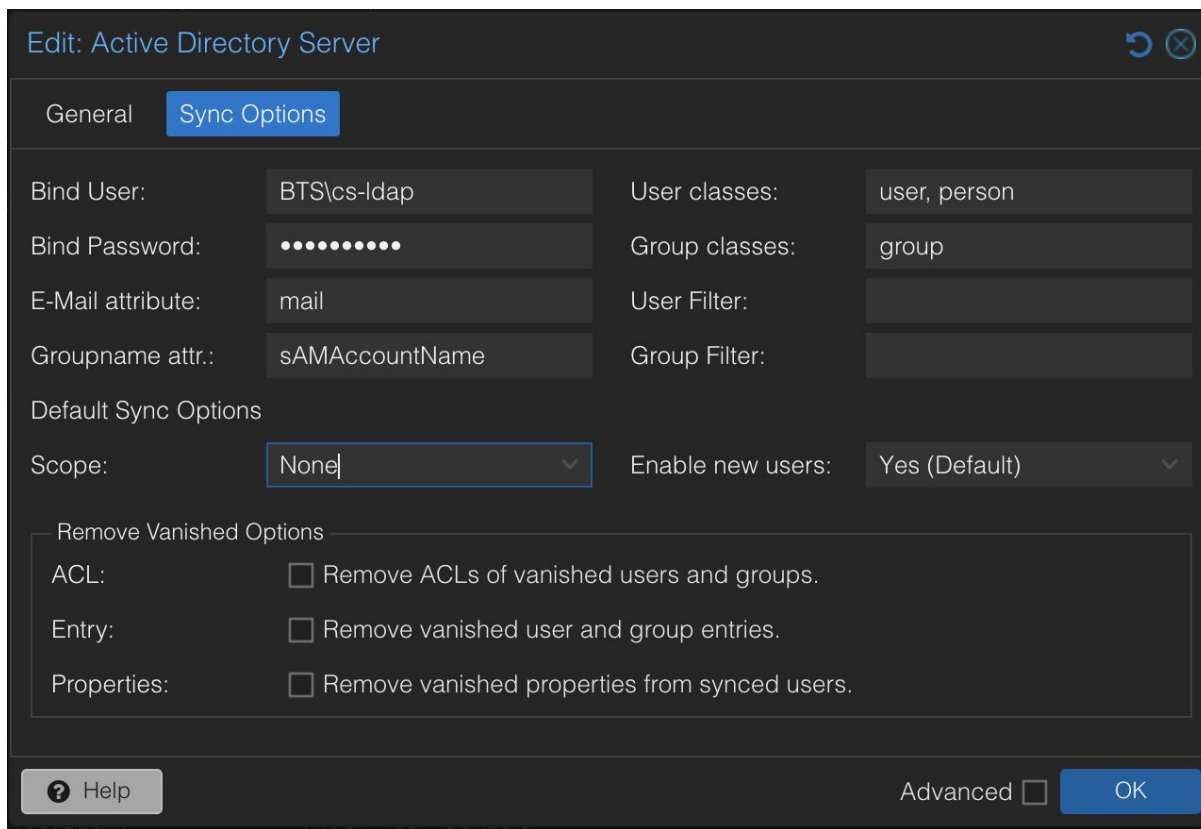
Realm:	BTS.SIO	Server:	192.168.100.3
Domain:	bts.sio	Fallback Server:	
Case-Sensitive:	<input type="checkbox"/>	Port:	Default
Default:	<input type="checkbox"/>	Mode:	LDAP
		Verify Certificate:	<input type="checkbox"/>
		Require TFA:	none
Comment:	Liaison Active Directory		

Help

Advanced ☐

OK

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



The screenshot shows the 'Edit: Active Directory Server' dialog box with the 'Sync Options' tab selected. The dialog has a title bar with a refresh icon and a close button. Below the title bar are two tabs: 'General' and 'Sync Options'. The 'Sync Options' tab contains several input fields and checkboxes. The 'Bind User' field is set to 'BTS\cs-ldap', 'Bind Password' is masked with dots, 'E-Mail attribute' is 'mail', and 'Groupname attr.' is 'sAMAccountName'. The 'User classes' field is 'user, person' and 'Group classes' is 'group'. The 'User Filter' and 'Group Filter' fields are empty. Under 'Default Sync Options', the 'Scope' dropdown is set to 'None' and 'Enable new users' is set to 'Yes (Default)'. A section titled 'Remove Vanished Options' contains three checkboxes, all of which are unchecked: 'ACL: Remove ACLs of vanished users and groups.', 'Entry: Remove vanished user and group entries.', and 'Properties: Remove vanished properties from synced users.'. At the bottom left is a 'Help' button with a question mark icon. At the bottom right are an 'Advanced' checkbox (unchecked) and an 'OK' button.

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: ☐ Remove ACLs of vanished users and groups.

Entry: ☐ Remove vanished user and group entries.

Properties: ☐ Remove vanished properties from synced users.

? Help Advanced ☐ OK

Cliquer sur Sync

Add ▾

Edit

Remove

|

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

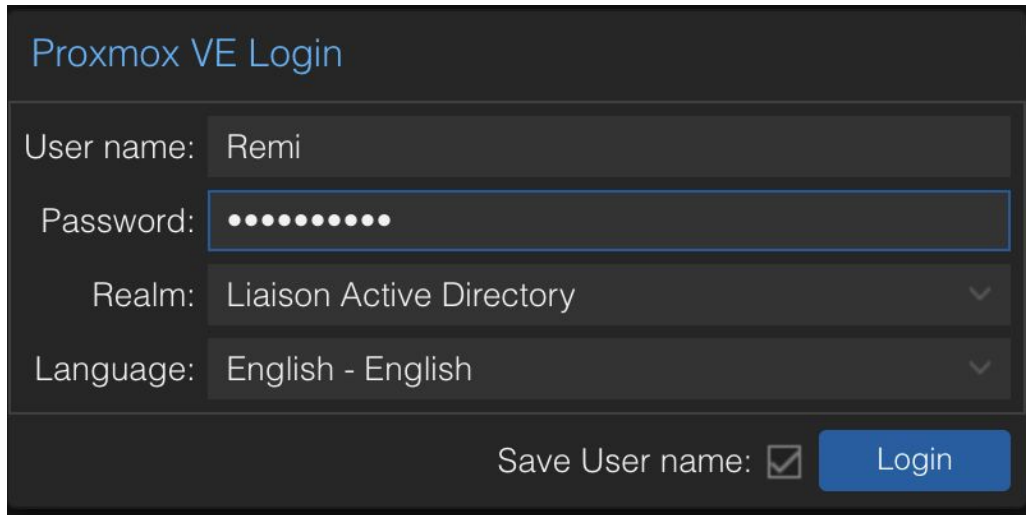
Sync



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



The image shows a Proxmox VE Login window with a dark background. The title 'Proxmox VE Login' is in blue. There are four input fields: 'User name' with 'Remi', 'Password' with masked dots, 'Realm' with 'Liaison Active Directory', and 'Language' with 'English - English'. At the bottom right, there is a 'Save User name' checkbox (checked) and a blue 'Login' button.

Proxmox VE Login

User name: Remi

Password: ••••••••

Realm: Liaison Active Directory

Language: English - English

Save User name: ☒ Login