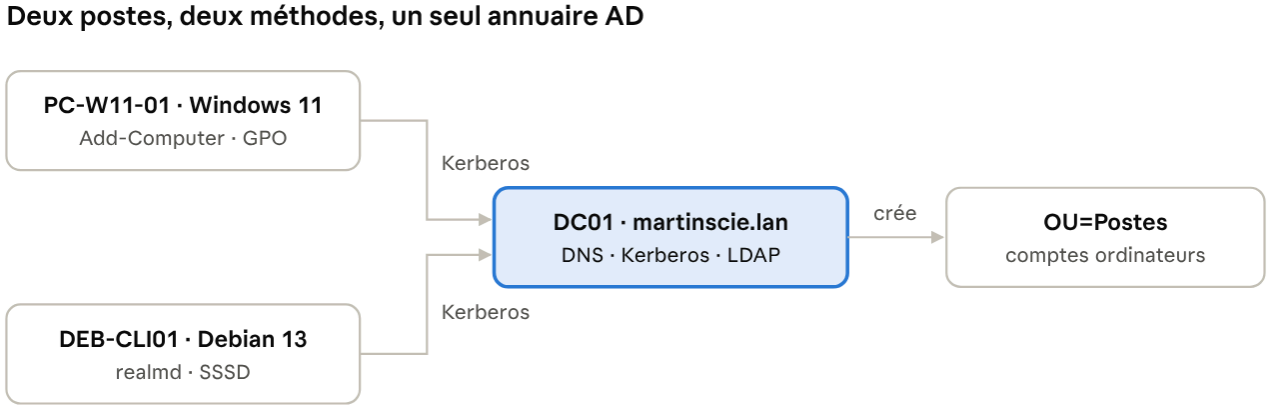
Joindre un poste Windows 11 et un poste Debian 13 au domaine Active Directory

Nov 27, 2026 · @Serge Martins

Objectif

Intégrer deux postes du VLAN 20 au domaine **martinscie.lan** géré par **DC01** (Windows Server 2025) : un poste **Windows 11** (jonction native) et un poste **Debian 13** (jonction avec realmd et SSSD). Les utilisateurs du domaine pourront ouvrir une session sur les deux postes avec leur compte AD.

Élément	Valeur
Domaine	martinscie.lan (NetBIOS : MARTINSCIE)
Contrôleur de domaine	DC01 · 192.168.10.10 (DNS et Kerberos)
Poste Windows	PC-W11-01 · Windows 11 Pro 25H2/26H2 · DHCP VLAN 20
Poste Linux	DEB-CLI01 · Debian 13 avec GNOME · DHCP VLAN 20
Unité d'organisation	OU=Postes,DC=martinscie,DC=lan
Groupe autorisé sur Linux	GG-Linux-Utilisateurs



Jonction de PC-W11-01 et DEB-CLI01 à martinscie.lan

Le poste Windows rejoint le domaine nativement, le poste Debian par realmd et SSSD ; dans les deux cas DC01 crée le compte ordinateur dans l'OU Postes et authentifie les utilisateurs par Kerberos.

Prérequis communs

- Le **DNS des postes doit être DC01** (192.168.10.10), distribué par DHCP (option 6) : sans lui, le domaine est introuvable.
- L'heure doit être synchronisée avec DC01 (écart maximal de 5 minutes pour Kerberos).
- Le pare-feu RFW01 doit laisser passer du VLAN 20 vers DC01 : DNS 53, Kerberos 88, LDAP 389, SMB 445, RPC 135 + ports dynamiques, NTP 123.
- Un compte autorisé à joindre des machines (administrateur du domaine en lab, compte délégué en production).

Sur DC01, préparer l'OU et le groupe :

```
New-ADOrganizationalUnit -Name "Postes" -Path "DC=martinscie,DC=lan"
New-ADGroup -Name "GG-Linux-Utilisateurs" -GroupScope Global -Path
"OU=Groupes,DC=martinscie,DC=lan"
New-ADGroup -Name "GG-Admins-Linux" -GroupScope Global -Path
"OU=Groupes,DC=martinscie,DC=lan"
Add-ADGroupMember "GG-Linux-Utilisateurs" -Members adurand
redircmp "OU=Postes,DC=martinscie,DC=lan"   # nouvelles machines dans l'OU
Postes
```

Partie A – Poste Windows 11

A1. Vérifier le réseau

```
ipconfig /all                        # serveur DNS = 192.168.10.10
Resolve-DnsName -Type SRV _ldap._tcp.dc._msdcs.martinscie.lan
Test-NetConnection dc01.martinscie.lan -Port 389
```

A2. Joindre le domaine

En PowerShell administrateur (édition **Pro, Entreprise ou Éducation** : l'édition Famille ne peut pas rejoindre un domaine) :

```
Add-Computer -DomainName martinscie.lan -NewName PC-W11-01 -OUPath
"OU=Postes,DC=martinscie,DC=lan" -Credential MARTINSCIE\Administrateur -
Restart
```

Équivalent graphique : **Paramètres → Comptes → Accès Professionnel ou Scolaire → Connecter → Joindre cet appareil à un domaine Active Directory local**.

A3. Vérifier

```
(Get-CimInstance Win32_ComputerSystem).Domain
nltest /sc_verify:martinscie.lan
Test-ComputerSecureChannel -Verbose
klist                                  # tickets Kerberos après ouverture de
session AD
gpresult /r
```

Ouvrir une session avec **MARTINSCIE\adurand** (ou *Autre utilisateur*), puis contrôler sur DC01 que l'objet ordinateur est bien dans l'OU Postes.

Partie B – Poste Debian 13

B1. Installer les paquets

```
sudo apt update
sudo apt install -y realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-
common-bin \
  oddjob oddjob-mkhomedir packagekit krb5-user chrony
```

À la question Kerberos, indiquer le royaume **MARTINSCIE.LAN** (en majuscules). Pointer chrony sur DC01 (`server 192.168.10.10 iburst` dans `/etc/chrony/chrony.conf`) puis `sudo systemctl restart chrony` .

B2. Découvrir et joindre le domaine

```
sudo hostnamectl set-hostname deb-cli01.martinscie.lan
realm discover martinscie.lan
sudo realm join -v -U Administrateur --computer-
ou="OU=Postes,DC=martinscie,DC=lan" martinscie.lan
```

> Avec un contrôleur Windows Server 2025, la jonction par `adcli` peut échouer avec le message *Couldn't set password for computer account: Message stream modified*. Dans ce cas, supprimer l'objet ordinateur créé sur DC01 puis relancer avec la méthode Samba : `sudo realm join -v -U Administrateur --membership-software=samba --computer-ou="OU=Postes,DC=martinscie,DC=lan" martinscie.lan` .

B3. Ajuster SSSD et PAM

Dans `/etc/sssd/sssd.conf` , section du domaine :

```
use_fully_qualified_names = False
fallback_homedir = /home/%u
default_shell = /bin/bash
ad_gpo_access_control = permissive
```

```
sudo chmod 600 /etc/sssd/sssd.conf
sudo pam-auth-update --enable mkhomedir
sudo systemctl restart sssd
```

B4. Restreindre les connexions et donner des droits sudo

```
sudo realm deny --all
sudo realm permit -g GG-Linux-Utilisateurs
echo '%GG-Admins-Linux ALL=(ALL:ALL) ALL' | sudo tee /etc/sudoers.d/ad-admins
sudo chmod 440 /etc/sudoers.d/ad-admins
```

B5. Vérifier

```
realm list
id adurand
getent passwd adurand
su - adurand            # crée /home/adurand à la première connexion
klist
```

Ouvrir enfin une session graphique GNOME avec **adurand** (lien *Non listé ?*).

Sécurité et bonnes pratiques

- Déléguer la jonction à un compte dédié limité à l'OU Postes, au lieu d'utiliser l'administrateur du domaine.
- Déployer **Windows LAPS** pour gérer le mot de passe administrateur local des postes Windows.
- Préparer la fin de NTLM : privilégier Kerberos (accès par nom DNS, pas par adresse IP) et auditer l'usage de NTLM.
- Sur Linux, limiter les connexions à un groupe AD et ne donner sudo qu'à un groupe d'administrateurs.

Dépannage

Symptôme	Piste
« Le domaine n'a pas pu être contacté »	DNS du poste différent de DC01, enregistrements SRV absents
Erreur d'horloge Kerberos	Synchroniser l'heure avec DC01 (w32tm /resync, chrony)
Relation d'approbation rompue (Windows)	`Test-ComputerSecureChannel -Repair -Credential MARTINSCIE\Administrateur`
`Message stream modified` (Debian)	Relancer la jonction avec `--membership-software=samba`
Utilisateur AD inconnu sous Linux	`sudo sss_cache -E`, journal `journalctl -u sssd`
Connexion refusée sous Linux	Utilisateur hors du groupe autorisé par `realm permit`