Contrôleur de domaine Active Directory sous Debian 13 avec Samba

Nov 27, 2026 · @Serge Martins

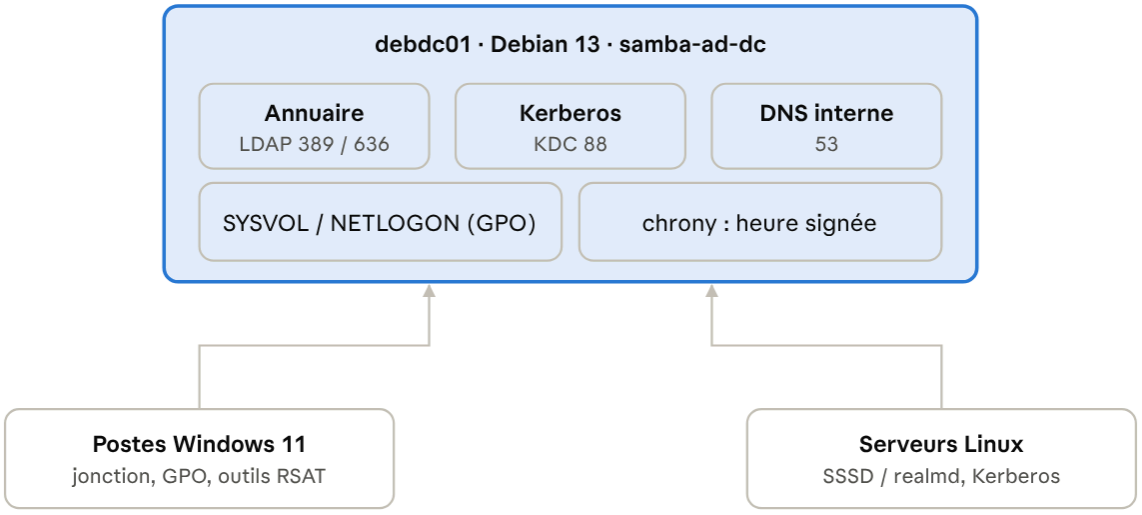
Objectif et architecture

Ce guide crée un contrôleur de domaine Active Directory **libre** sur Debian 13 « Trixie » avec Samba. Les postes Windows s'y joignent et s'administrent avec les outils RSAT habituels, comme avec un DC Windows. C'est l'alternative gratuite à DC01 sous Windows Server 2025.

Le lab utilise un domaine **distinct** de `martinscie.lan` : deux forêts ne peuvent pas porter le même nom sur le même réseau. Pour remplacer DC01, remplacer `sambalab.lan` par `martinscie.lan` dans tout le guide.

Élément	Valeur (à adapter)
Nom du serveur	`debdc01` (FQDN `debdc01.sambalab.lan`)
Adresse IP	`192.168.10.11/24` (VLAN 10 Serveurs)
Passerelle	`192.168.10.254` (pfSense RFW01)
Domaine DNS / royaume Kerberos	`sambalab.lan` / `SAMBALAB.LAN`
Nom NetBIOS	`SAMBALAB`
DNS	Serveur DNS interne de Samba, redirecteur `1.1.1.1`
Version	Samba 4.22 (paquets Debian 13)

Un seul service, samba-ad-dc, fait tout le travail du DC



Services d'un contrôleur de domaine Samba

Les postes Windows et les serveurs Linux voient debdc01 comme un contrôleur de domaine Active Directory ordinaire.

1. Prérequis

Samba lit le nom d'hôte et l'adresse IP au moment du provisionnement : ils doivent être définitifs avant de commencer. Toutes les commandes se lancent en `root`.

1.1 Machine virtuelle : Debian 13 minimale (sans environnement de bureau, avec le serveur SSH), 2 vCPU, 2 Go de RAM, 20 Go de disque.

1.2 Nom d'hôte et `/etc/hosts`

```
hostnamectl set-hostname debdc01
```

`/etc/hosts` — l'IP réelle, jamais `127.0.1.1`, face au FQDN :

```
127.0.0.1       localhost
192.168.10.11   debdc01.sambalab.lan debdc01
```

1.3 IP fixe — `/etc/network/interfaces` (adapter `ens18`) :

```
auto ens18
iface ens18 inet static
    address 192.168.10.11/24
    gateway 192.168.10.254
```

`/etc/resolv.conf` provisoire (pour installer les paquets) :

```
nameserver 192.168.10.254
```

```
systemctl restart networking
hostname -f      # doit afficher debdc01.sambalab.lan
hostname -I      # doit afficher 192.168.10.11
```

1.4 Mises à jour et heure

```
apt update && apt full-upgrade -y
timedatectl set-timezone Europe/Paris
```

2. Installation des paquets

```
apt install -y samba-ad-dc samba-ad-provision krb5-user winbind libnss-
winbind \
  libpam-winbind smbclient ldb-tools dnsutils chrony
```

Aux questions de `krb5-user` : royaume `SAMBALAB.LAN`, serveurs `debdc01.sambalab.lan` (le fichier sera de toute façon remplacé au § 3.3).

Un contrôleur de domaine Samba utilise un service unique, `samba-ad-dc`. Les services d'un serveur de fichiers classique doivent être arrêtés et masqués :

```
systemctl disable --now smbd nmbd winbind
systemctl mask smbd nmbd winbind
systemctl unmask samba-ad-dc

# Le smb.conf par défaut empêche le provisionnement
mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

3. Provisionnement du domaine

3.1 Créer la forêt

```
samba-tool domain provision \
  --server-role=dc \
  --use-rfc2307 \
  --dns-backend=SAMBA_INTERNAL \
  --realm=SAMBALAB.LAN \
  --domain=SAMBALAB \
  --option="dns forwarder = 1.1.1.1"
```

La commande demande le mot de passe du compte `Administrator` (au moins 7 caractères, 3 catégories). `--use-rfc2307` stocke les UID/GID Unix dans l'annuaire, utile pour les serveurs Linux membres.

3.2 Résolution DNS par le DC lui-même

`/etc/resolv.conf` :

```
search sambalab.lan
nameserver 127.0.0.1
```

Penser aussi à retirer toute ligne `dns-nameservers` de `/etc/network/interfaces` qui écraserait ce fichier.

3.3 Kerberos

```
cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

3.4 Démarrer le contrôleur de domaine

```
systemctl enable --now samba-ad-dc
systemctl status samba-ad-dc
```

3.5 Niveau fonctionnel 2016 (optionnel)

Samba provisionne par défaut au niveau 2008 R2. Depuis Samba 4.19, le niveau 2016 peut être activé :

```
# Dans /etc/samba/smb.conf, section [global] :
#   ad dc functional level = 2016
systemctl restart samba-ad-dc
samba-tool domain level raise --domain-level=2016 --forest-level=2016
samba-tool domain level show
```

4. Configuration

4.1 Heure signée pour les postes Windows

Les clients Windows refusent une heure non signée par le DC. Ajouter dans `/etc/chrony/chrony.conf` :

```
bindcmdaddress 192.168.10.11
allow 192.168.10.0/24
allow 192.168.20.0/24
ntpsigndsocket /var/lib/samba/ntp_signd
```

```
chown root:_chrony /var/lib/samba/ntp_signd
chmod 750 /var/lib/samba/ntp_signd
systemctl restart chrony
```

4.2 Zone DNS inverse

```
samba-tool dns zonecreate debdc01 10.168.192.in-addr.arpa -U Administrator
samba-tool dns add debdc01 10.168.192.in-addr.arpa 11 PTR
debdc01.sambalab.lan -U Administrator
```

4.3 Unités d'organisation, groupes et comptes

```
samba-tool ou add "OU=MARTINSCIE"
samba-tool ou add "OU=Utilisateurs,OU=MARTINSCIE"
samba-tool ou add "OU=Groupes,OU=MARTINSCIE"

samba-tool group add GG_RDP_Linux --groupou="OU=Groupes,OU=MARTINSCIE"
samba-tool user create jdupont --given-name=Jean --surname=Dupont \
  --userou="OU=Utilisateurs,OU=MARTINSCIE" --must-change-at-next-login
samba-tool group addmembers GG_RDP_Linux jdupont

# Politique de mots de passe
samba-tool domain passwordsettings set --min-pwd-length=12
```

4.4 DHCP : sur pfSense, le DHCP du VLAN 20 distribue `192.168.10.11` comme DNS et `sambalab.lan` comme domaine.

5. Jonction d'un poste Windows et administration

1. Sur le poste Windows 11, DNS préféré = `192.168.10.11` (ou via DHCP).
2. Vérifier : `nslookup sambalab.lan` et `nslookup -type=SRV _ldap._tcp.dc._msdcs.sambalab.lan`.
3. Paramètres > Système > Informations système > **Domaine ou groupe de travail** > Modifier > Domaine : `sambalab.lan`, compte `SAMBALAB\Administrator`. Redémarrer.
4. Installer les outils d'administration : Paramètres > Système > Fonctionnalités facultatives > **RSAT : Active Directory Domain Services**, **RSAT : DNS** et **RSAT : Gestion des stratégies de groupe**.

Se connecter avec `SAMBALAB\Administrator` : « Utilisateurs et ordinateurs Active Directory », la console DNS et la gestion des GPO fonctionnent comme avec un DC Windows.

> Les GPO sont stockées dans le partage SYSVOL du DC. Si une GPO ne s'applique pas après une modification de droits : `samba-tool ntacl sysvolreset`.

6. Vérifications, dépannage et sécurisation

6.1 Tests

```
host -t SRV _ldap._tcp.sambalab.lan
host -t SRV _kerberos._udp.sambalab.lan
host -t A debdc01.sambalab.lan
kinit administrator && klist
smbclient -L localhost -N                          # partages sysvol et
netlogon
smbclient //localhost/netlogon -U Administrator -c 'ls'
samba-tool domain level show
samba-tool dbcheck --cross-ncs                     # cohérence de la base
chronyc sources
```

6.2 Symptômes fréquents

Symptôme	Cause probable	Correction
Le provisionnement échoue	`smb.conf` existant ou nom d'hôte incorrect	Supprimer `smb.conf`, vérifier `hostname -f` et `/etc/hosts`
`samba-ad-dc` ne démarre pas	`smbd` / `nmbd` encore actifs	Les masquer (§ 2), `journalctl -u samba-ad-dc`
Pas de réponse DNS	`resolv.conf` ne pointe pas sur 127.0.0.1	Corriger § 3.2
Pas de résolution Internet	Redirecteur absent	`dns forwarder = 1.1.1.1` dans `smb.conf`
`kinit` : clock skew	Heure décalée	Vérifier chrony (§ 4.1)
Jonction Windows impossible	DNS du poste incorrect	DNS du poste = `192.168.10.11` uniquement

6.3 Sécurisation

- [ ] Appliquer les mises à jour de sécurité Debian dès leur parution (`apt update && apt upgrade`) : Samba AD a reçu plusieurs correctifs importants en 2026.
- [ ] Ne pas activer le service WINS et laisser SMB1 désactivé (réglages par défaut).
- [ ] Utiliser un compte d'administration nominatif plutôt que `Administrator`.

- [ ] Sauvegarder régulièrement : `samba-tool domain backup online --targetdir=/root/sauvegarde --server=debdc01 -U Administrator`.
- [ ] Limiter l'accès au DC sur pfSense aux ports AD depuis le VLAN 20 (53, 88, 135, 389, 445, 464, 636, 3268, 49152-65535).
- [ ] Ajouter un second DC Debian avec `samba-tool domain join sambalab.lan DC`.