# Ubuntu Server - Intégrer le serveur dans le domaine AD

> Titre de la page : <Techno> - <Titre de la procédure / du cours> (à supprimer une fois le titre placé)

Difficulté : Intermédiaire

Notions : PAM, authentification, linux, LDAP, domaine.

---

## I. Introduction

Cette procédure à pour but de présenter l'intégration des serveurs ubuntu dans le domaine Active Directory afin de permettre l'authentification et l'utilisation du serveur et des services avec des comptes du domaine.

Cela renforcera la sécurité et permettra une gestion des privilèges par groupes AD.

---

## II. Préparation

Installer les paquets nécessaire avec la commande :

```
sudo apt install -y realmd samba
```

Puis renommer le serveur en utilisant la commande :

> **Attention** : il est important de bien mettre le FQDN du serveur tel qu'il sera adressé.

```
sudo hostnamectl hostname <fqdn.du.serveur>
```

```
root@template:/home/sc4d-# hostnamectl hostname sc-prd-dml01.labs404.fr
root@template:/home/sc4d-# hostname
sc-prd-dml01.labs404.fr
```

Utiliser la commande suivante pour voir si le domaine est correctement découvert.

```
sudo realm discover <domain.ext>
```

```
root@template:/home/sc4d-# realm discover labs404.fr
labs404.fr
  type: kerberos
  realm-name: LABS404.FR
  domain-name: labs404.fr
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
```

---

# III. Intégration

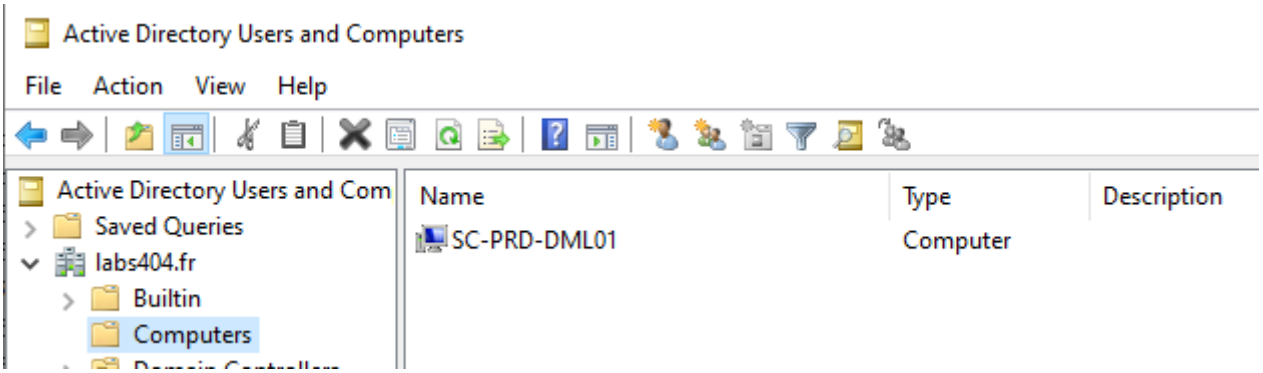
Pour joindre le serveur au domaine, Entrer la commande suivante :

```
sudo realm join -v --user='<domain\utilisateur>' --membership-software=samba --client-software=winbind  <domaine.ext>
```

```
root@sc-prd-dml01:/home/sc4d-# sudo realm join -v --user='labs404\MadSinistrator' --membership-software=samba --client-software=winbind labs404.fr
 * Resolving: _ldap._tcp.labs404.fr
 * Performing LDAP DSE lookup on: 172.16.10.1
 * Performing LDAP DSE lookup on: 172.16.10.2
 * Successfully discovered: labs404.fr
Password for labs404\MadSinistrator:
 * Unconditionally checking packages
 * Resolving required packages
 * LANG=C LOGNAME=root /usr/bin/net --configfile /var/cache/realmd/realmd-smb-conf.4OT0I2 -U labs404\MadSinistrator --use-kerberos=required ads join labs404.fr
Password for [LABS404\MadSinistrator]:DNS update failed: NT_STATUS_INVALID_PARAMETER

Using short domain name -- LABS404
Joined 'SC-PRD-DML01' to dns domain 'labs404.fr'
No DNS domain configured for sc-prd-dml01. Unable to perform DNS Update.
 * LANG=C LOGNAME=root /usr/bin/net --configfile /var/cache/realmd/realmd-smb-conf.4OT0I2 -U labs404\MadSinistrator ads keytab create
Password for [LABS404\MadSinistrator]:
 * /usr/sbin/update-rc.d winbind enable
 * /usr/sbin/service winbind restart
 * Successfully enrolled machine in realm
```

Le serveur est maintenant enregistré dans Active Directory.




> **Attention** : dans le Serveur DNS, si les sources anonymes ne sont pas autorisées à faire les enregistrement DNS, il faudra les ajouter à la main.

---

# IV. Ajout des groupes & droits

## 4.1 Déclarer la méthode d'authentification

Dans le fichier '***/etc/nsswitch.conf*** ', Modifier les deux lignes suivantes en ajoutant '***winbind***' comme source d'authentification.

```
# `info libc "Name Service Switch"' for information about this file.

passwd:         files systemd winbind
group:          files systemd winbind
```

Il est maintenant possible d'utiliser les identifiants active directory pour se connecter à la machine.

Pour vérifier si un identifiant est correctement reconnu, utiliser :

```
getent passwd <domaine>\\<utilisateur>
```

```
root@sc-prd-dml01:/home/sc4d-# getent passwd labs404\\adm.ochabran
LABS404\adm.ochabran:*:[redacted]:[redacted]::/home/adm.ochabran@LABS404:/bin/bash
```

Cela fonctionne aussi avec les groupes.

```
root@sc-prd-dml01:/home/sc4d-# getent passwd labs404\\GRP_SEC_GG_SYS_UbuntuAdministrators
LABS404\grp_sec_gg_sys_ubuntuadministrators:*:[redacted]:[redacted]::/home/grp_sec_gg_sys_ubuntuadministrators@LABS404:/bin/bash
```

# 4.1 autoriser le groupe admin dans les sudoers

Éditer le fichier des sudoers avec la commande :

```
visudo
```

Trouver les lignes suivantes et ajouter le groupe administrateur dans le fichier comme ci-dessous :

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%LABS404\\GRP_SEC_GG_SYS_UbuntuAdministrators ALL=(ALL:ALL) ALL
```

Enregistrer le fichier avec ***ctrl+o***, valider et quitter.

Vérifier le fonctionnement :

---

Revision #2
Created 2026-07-29 12:10:19 UTC by Olivier
Updated 2026-07-29 13:01:17 UTC by Olivier