# Connexion aux sessions sur Linux via les utilisateurs Active Directory

## Sommaire



---

# Partie 1 - Présentation

Nous allons permettre à l’ensemble de machine Linux de pouvoir s’authentifier via l’Active Directory. La méthode la plus robuste et moderne actuelle est d'utiliser SSSD (System Security Services Daemon) couplé avec Realmd.

---

# Partie 1 - Prérequis

1) Utiliser le serveur AD en tant que DNS (192.168.30.1) et search technova.local
2) Avoir joint la machine au domaine
3) Synchronisation NTP : L'heure doit être parfaitement synchronisée entre le Linux et l'AD (écart max 5 min) : timedatectl set-timezone Europe/Paris

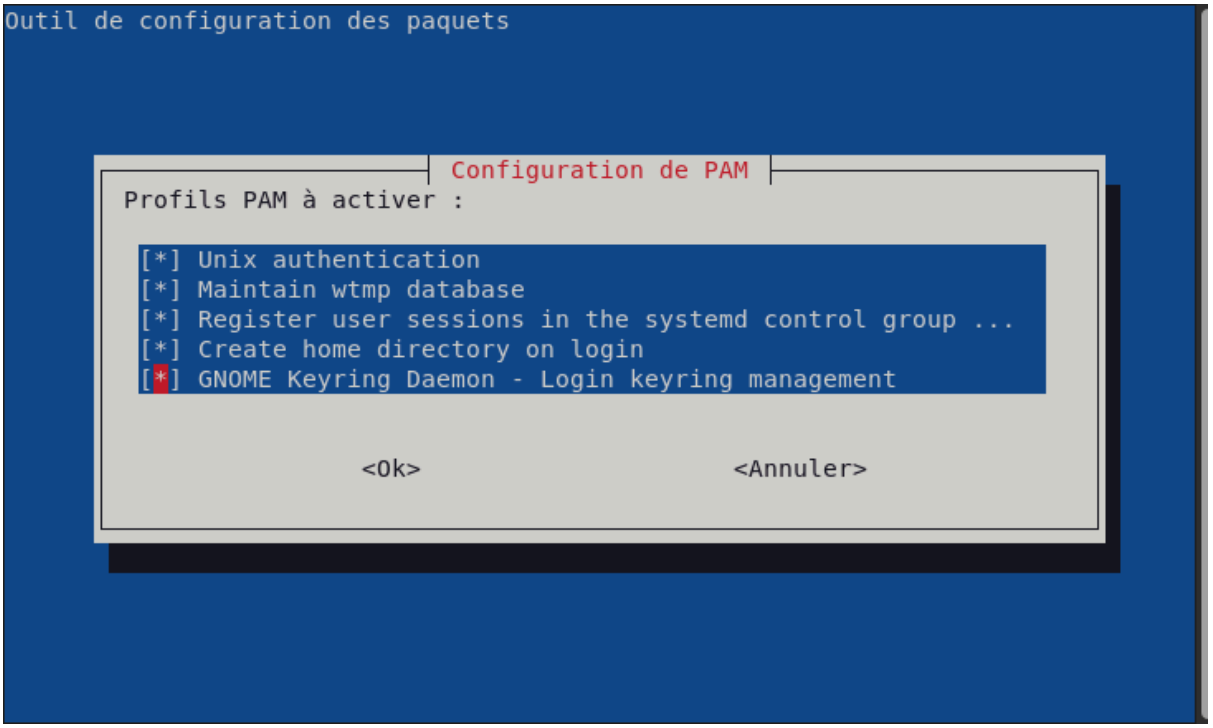
# Partie 3 - Configuration de la création automatique du “Home Directory”

Par défaut, si un utilisateur AD se connecte, il n'aura pas de dossier /home/utilisateur. Il faut activer sa création automatique via PAM.

```
apt update
```

```
apt install sudo
```

```
sudo pam-auth-update
```




# Partie 4 - Gestion des droits “Sudo”

Nos administrateurs Active Directory doivent devenir root sur les serveurs sans utiliser le compte local.

Nous utiliserons le groupe GG_INFORMATIQUE. Il faudra prendre soin de bien ajouter les utilisateurs à l'intérieur mais cela à été lors d'une précédente procédure.

Nous allons donc éditer notre fichier de sudoers :

```
nano /etc/sudoers.d/GG_INFORMATIQUE
```

Ajoutez cette ligne (notez le % pour indiquer un groupe et l'échappement des espaces si besoin) :

```
%GG_INFORMATIQUE@technova.local ALL=(ALL:ALL) ALL
```

---

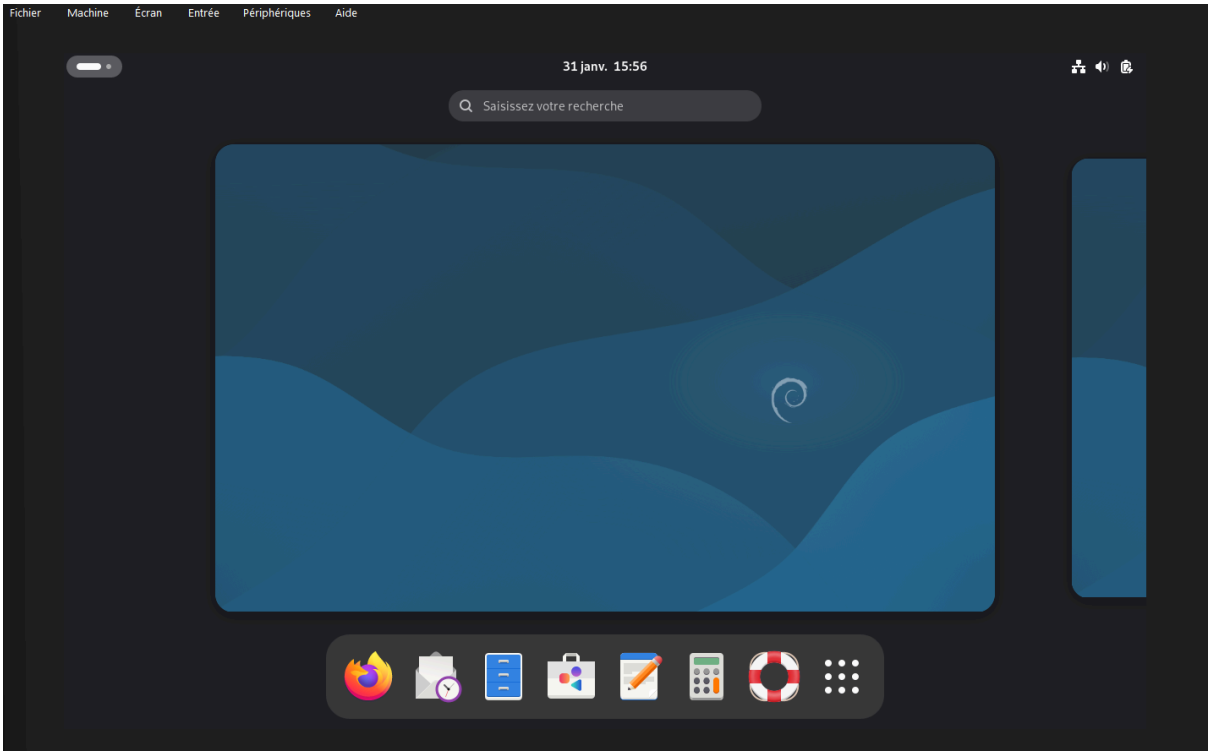
# Partie 5 - Test finaux

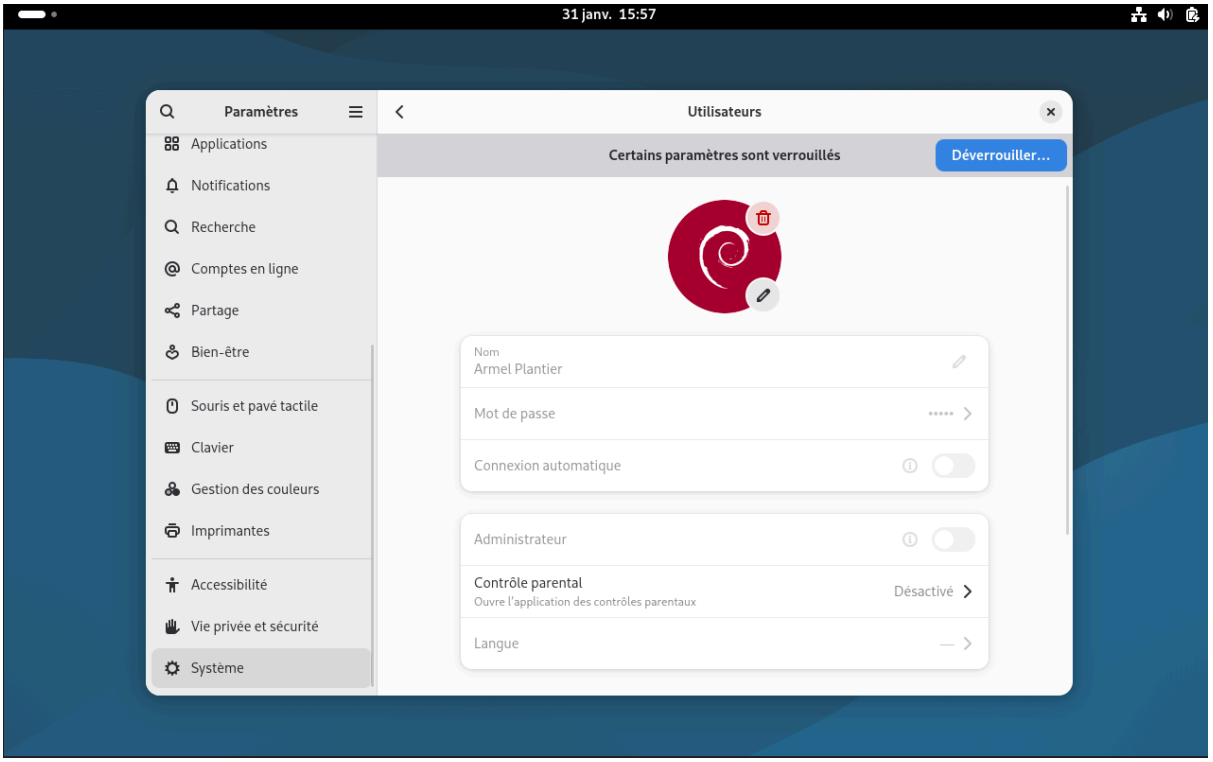
Nous prendrons TNV-04 comme exemple. Sur la page de connexion il faudra cliquer sur "Absent de la liste"


Ensuite :

1) aplantier@technova.local
2) Entrez le mot de passe

Ensuite la session s'ouvrira !




Par contre nous devons vérifier si on peut se connecter avec un compte d'un autre OU, le service R&D par exemple (amartin). Dans notre cas actuel, amartin peut se connecter avec ses identifiants sur une machine linux mais elle n'est pas sudoers (comme elle ne fait pas partie du groupe informatique.)

Il faudra renseigner 2 commandes qui permettront :

1) Refuser l’accès à tout le domaine
2) Autoriser ensuite le groupe INFORMATIQUE

```
/usr/sbin/realm deny --all
```

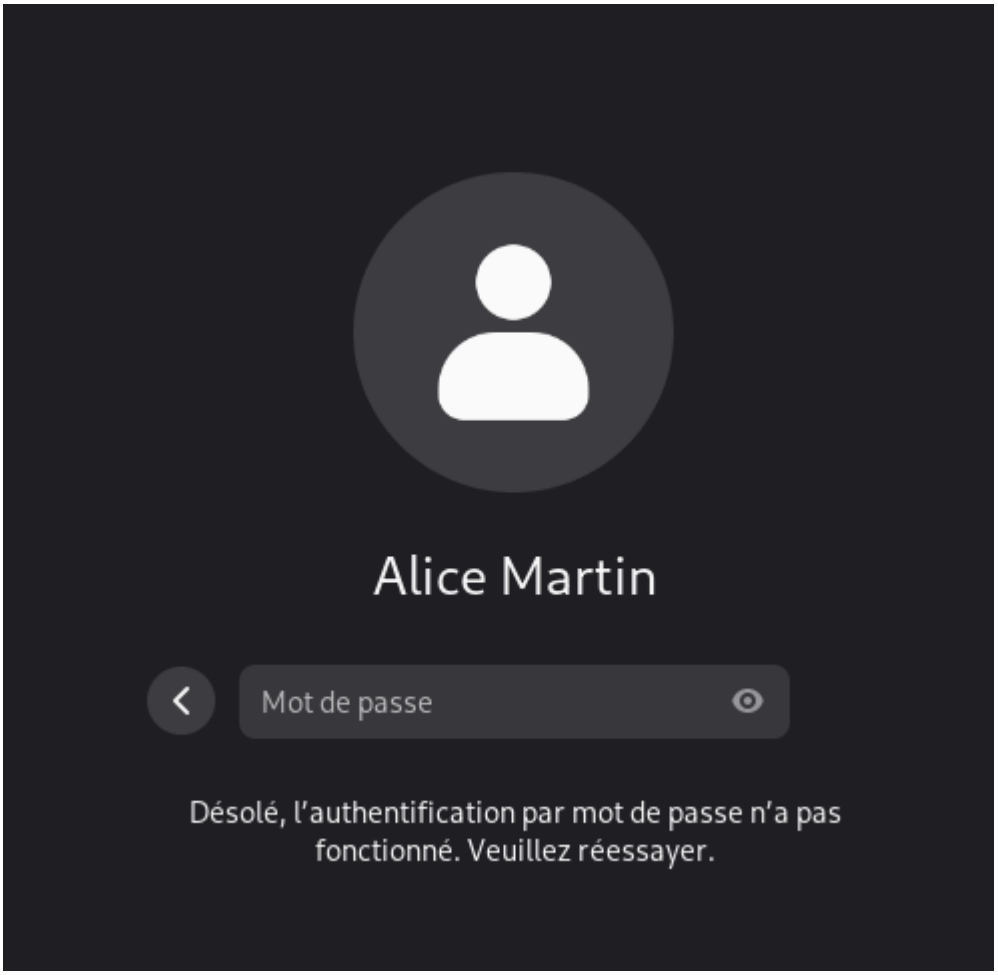
```
/usr/sbin/realm permit -g GG_INFORMATIQUE
```

et pour vérifier :

```
/usr/sbin/realm list
```

```
root@TNV-04:/home/armel# /usr/sbin/realm list
technova.local
  type: kerberos
  realm-name: TECHNOVA.LOCAL
  domain-name: technova.local
  configured: kerberos-member
  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
  login-formats: %U@technova.local
  login-policy: allow-permitted-logins
  permitted-logins:
  permitted-groups: GG_INFORMATIQUE
root@TNV-04:/home/armel#
```

On peut ensuite essayer avec amartin


Alice Martin
Mot de passe
Désolé, l'authentification par mot de passe n'a pas fonctionné. Veuillez réessayer.