Debian13 - Joindre au domaine active directory

Difficulté : Confirmé

Notions : AD, LDAP, Linux, domaine.

I. Introduction

Cette procédure à pour but de décrire comment ajouter une machine debian13 au domaine Active directory et permettre le login des utilisateurs et la gestion de droits.

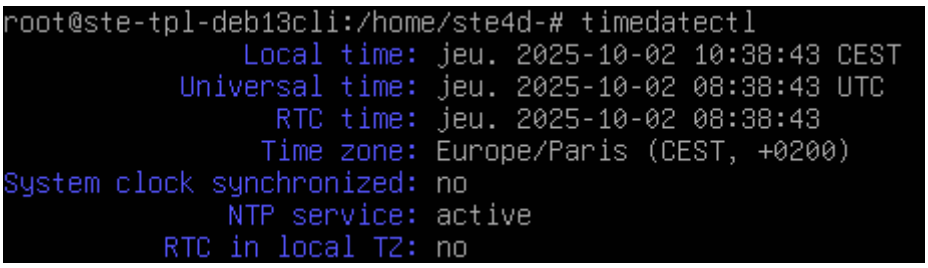
> **Prérequis** : le domaine doit exister. Vérifier la concordance fuseau horaire, date, heure.

II. Vérification des prérequis

2.1 synchroniser l'heure avec le DC

Utiliser la commande suivante pour vérifier l'heure :

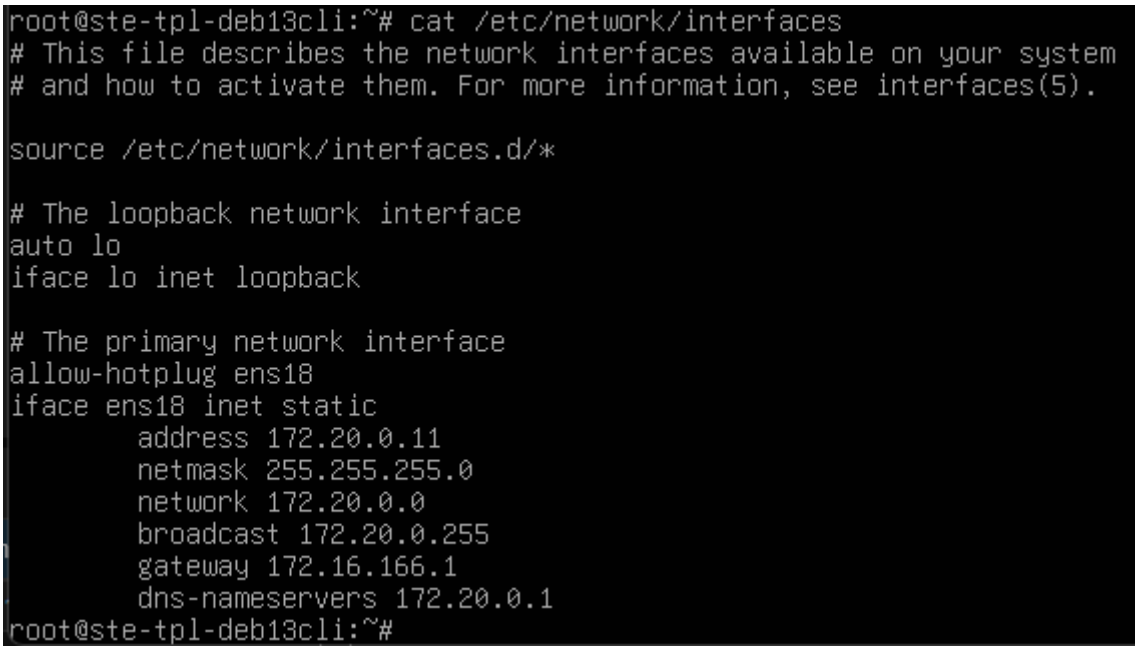
```
timedatectl
```



2.2 configuration réseau & DNS

Éditer le fichier '***/etc/network/interfaces***' pour refléter la configuration voulue.

Faire notamment attention à ce que le serveur DNS soit bien celui du domaine.



Éditer le fichier '***/etc/resolv.conf***' pour y configurer les DNS du domaine et le domaine de recherche.

```
root@ste-tpl-deb13cli:~# cat /etc/resolv.conf
# Generated by dhcpcd from ens18.dhcp
# /etc/resolv.conf.head can replace this line
domain olivier.local
nameserver 172.20.0.1
# /etc/resolv.conf.tail can replace this line
root@ste-tpl-deb13cli:~# _
```

Relancer la couche réseau.

```
systemctl restart networking.service
```

vérifier la configuration ip.

```
ip a
```

```
root@ste-tpl-deb13cli:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:ba:92:f4 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    altname enxbc2411ba92f4
    inet 172.20.0.11/24 brd 172.20.0.255 scope global ens18
       valid_lft forever preferred_lft forever
```

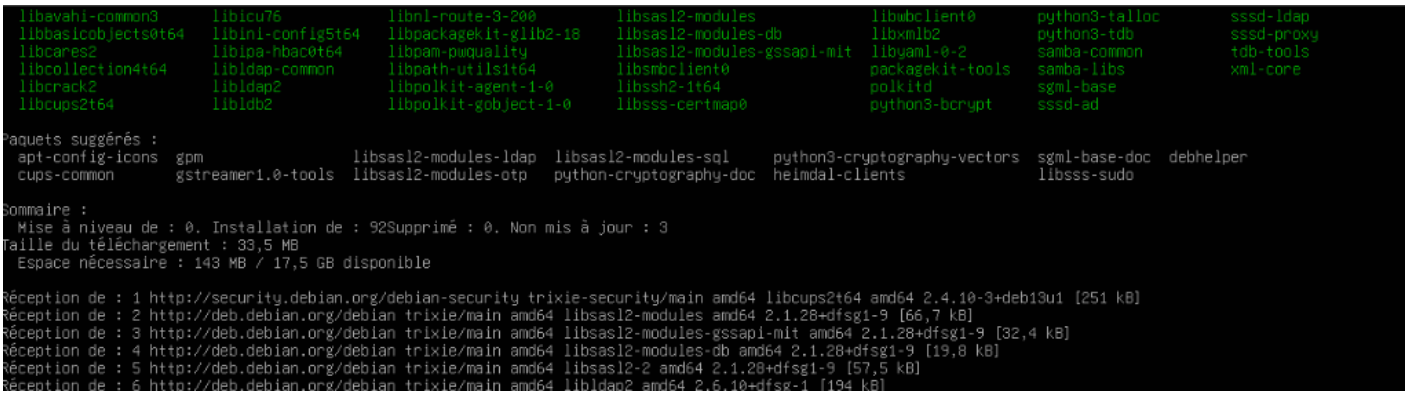
Vérifier la résolution du nom de serveur :

```
root@ste-tpl-deb13cli:/home/ste4d-# ping och-lab-adds01.olivier.local
PING och-lab-adds01.olivier.local (172.20.0.1) 56(84) bytes of data.
^C64 bytes from 172.20.0.1: icmp_seq=1 ttl=128 time=0.318 ms
```

III. Installer les paquets

Afin de joindre le domaine, il faut installer le client realmd ainsi que les extensions nécessaires.

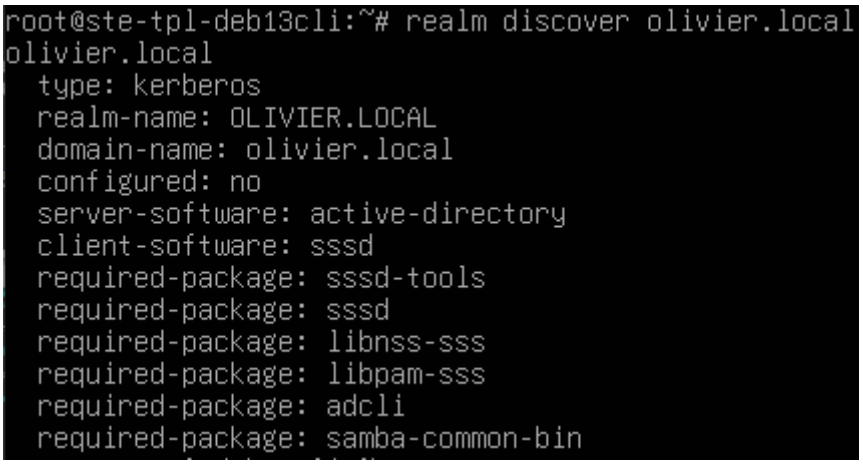
```
apt install -y realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin oddjob
oddjob-mkhomedir packagekit
```



IV. Joindre le domaine

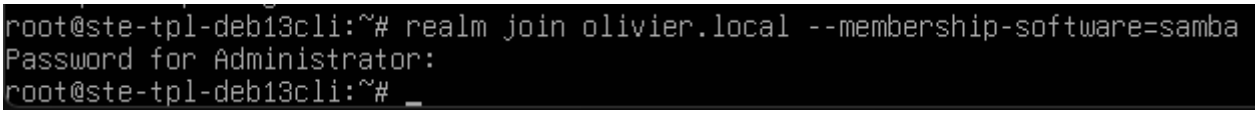
Détecter le domaine avec la commande suivante :

```
realm discover <domaine>
```



Joindre le domaine en tapant cette commande et

```
realm join <NomDuDomaine> --membership-software=samba
```



Pour tester le fonctionnement, il est possible d'interroger le LDAP pour avoir les informations sur un utilisateur.

```
id <username>@<domain>
```

redémarrer.

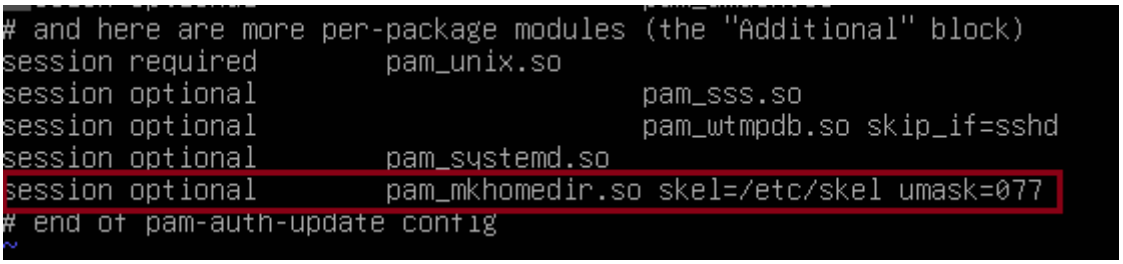
```
systemctl reboot
```

V. Ajuster les paramètres

5.1 Création automatique des répertoires dans /home

Éditer le fichier '***/etc/pam.d/common-session***' pour y ajouter la ligne :

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```



Le répertoire utilisateur sera créé à la première connexion.

5.2 Permettre l'omission du domaine

Pour pouvoir permettre de se connecter sans avoir à spécifier le domaine à chaque fois, éditer le fichier '***/etc/sssd/sssd.conf*** '

Changer la ligne suivante :

`use_fully_qualified_names = True` en `use_fully_qualified_names = False`

Puis relancer le service sssd.

```
systemctl restart sssd
```

Il est possible de tester les ID sans le domaine :

5.3 Gérer des Id fixes

Cette modification peut être utile afin d'uniformiser les SID sur l'ensemble des linux du domaine.

> **Prérequis** : Les attributs unix pour les utilisateurs doivent avoir été ajoutés sur les utilisateurs AD concernés. Voir : Active Directory - Attributs UNIX

Par défaut, les uid et guid sont attribués aléatoirement. Si l'on souhaite le fixer depuis l'AD et utiliser ceux-ci plutôt que ceux générés par le système, il faudra faire les modifications suivantes.

Éditer le fichier '***/etc/sssd/sssd.conf*** '

Changer la ligne suivante :

```
ldap_id_mapping = True
```

en

```
ldap_id_mapping = False
```

Ajouter également les lignes en fin de fichier :

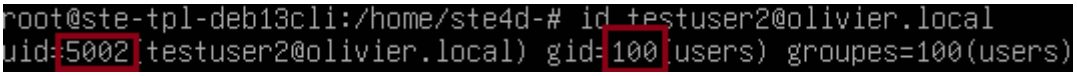
```
ldap_user_uid_number = uidNumber
ldap_user_gid_number = gidNumber
```

Puis, vider le cache et relancer le service sssd.

```
rm -f /var/lib/sss/db/*
systemctl restart sssd
```

Il est possible de tester les ID :

```
id <NomUtilisateur>
```

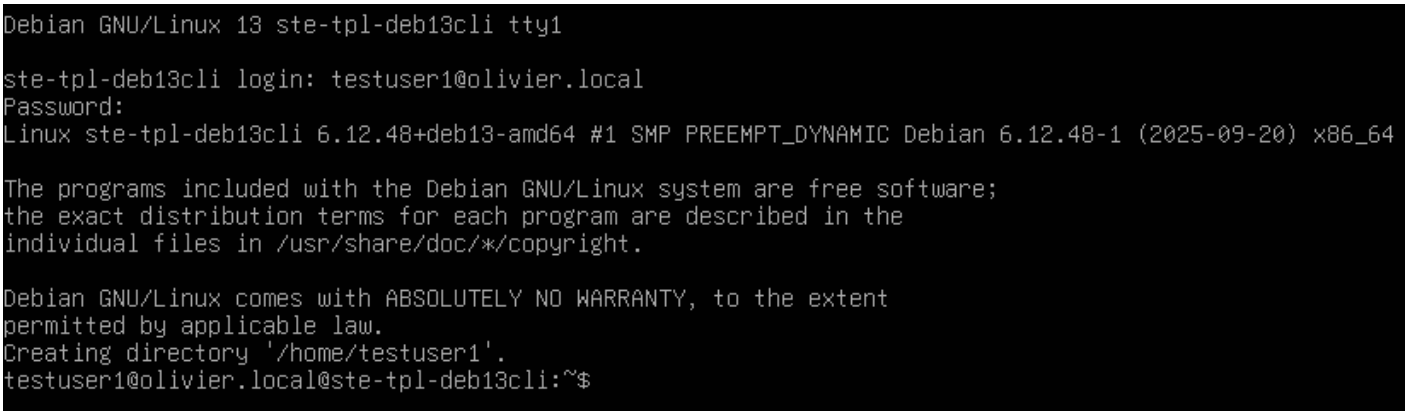


VI. Tester la connexion

Se déconnecter des sessions avec :

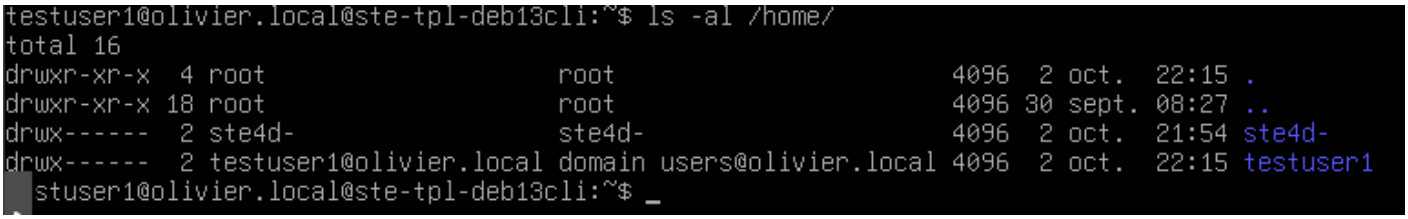
```
exit
```

Puis tenter une connexion avec l'utilisateur du domaine.



Vérifier que le home a été bien créé :

```
ls -al /home/
```



Revision #2
Created 2026-07-29 09:36:51 UTC by Olivier
Updated 2026-07-29 09:40:04 UTC by Olivier