

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
```

```
root@ste-tpl-deb13cli:/home/ste4d-# timedatectl
      Local time: jeu. 2025-10-02 10:38:43 CEST
      Universal time: jeu. 2025-10-02 08:38:43 UTC
          RTC time: jeu. 2025-10-02 08:38:43
      Time zone: Europe/Paris (CEST, +0200)
System clock synchronized: no
      NTP service: active
      RTC in local TZ: no
```

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.

```
root@ste-tpl-deb13cli:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens18
iface ens18 inet static
    address 172.20.0.11
    netmask 255.255.255.0
    network 172.20.0.0
    broadcast 172.20.0.255
    gateway 172.16.166.1
    dns-nameservers 172.20.0.1
root@ste-tpl-deb13cli:~#
```

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 dhcpd 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
```

```
libavahi-common3 libicu76 libnl-route-3-200 libnss-sss libpam-sss libpython3-talloc sssd-ldap  
libbasicobjects0t64 libbinutils2t64 libpackagekit-glib2-18 libpython3-tdb sssd-proxy  
libcares2 libbpf-hbac0t64 libpam-pwquality libpython3-gssapi-mit libxaml-0-2 sssd-tools  
libcollection4t64 libldap-common libpath-utils1t64 libpython3-ldb libxaml-0-2 sssd-tools  
libcrack2 libldap2 libpolkit-agent-1-0 libssh2-1t64 libsssd-client0 libxaml-0-2 sssd-tools  
libcupst64 libldb2 libpolkit-gobject-1-0 libsssd-certmap0 libxaml-0-2 sssd-tools  
Paquets suggérés :  
apt-config-icons gpm libnss-sss libpam-sss python3-cryptography-vectors sgml-base-doc debhelper  
cups-common gstreamer1.0-tools libnss-sss libpam-sss python-cryptography-doc heimdal-clients libsssd-sudo  
Sommaire :  
Mise à niveau de : 0. Installation de : 92 Supprimé : 0. Non mis à jour : 3  
Taille du téléchargement : 33,5 MB  
Espace nécessaire : 143 MB / 17,5 GB disponible  
Réception de : 1 http://security.debian.org/debian-security trixie-security/main amd64 libcupst64 amd64 2.4.10-3+deb13u1 [251 kB]  
Réception de : 2 http://deb.debian.org/debian trixie/main amd64 libnss-sss amd64 2.1.28+dfsg1-9 [66,7 kB]  
Réception de : 3 http://deb.debian.org/debian trixie/main amd64 libpython3-gssapi-mit amd64 2.1.28+dfsg1-9 [32,4 kB]  
Réception de : 4 http://deb.debian.org/debian trixie/main amd64 libpython3-ldb amd64 2.1.28+dfsg1-9 [19,8 kB]  
Réception de : 5 http://deb.debian.org/debian trixie/main amd64 libpython3-ldb amd64 2.1.28+dfsg1-9 [57,5 kB]  
Réception de : 6 http://deb.debian.org/debian trixie/main amd64 libldap2 amd64 2.6.10+dfsg-1 [194 kB]
```

IV. Joindre le domaine

Détecter le domaine avec la commande suivante :

```
realm discover <domaine>
```

```
root@ste-tpl-deb13cli:~# realm discover olivier.local  
olivier.local  
type: kerberos  
realm-name: OLIVIER.LOCAL  
domain-name: olivier.local  
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
```

Joindre le domaine en tapant cette commande et

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

```
root@ste-tpl-deb13cli:~# realm join olivier.local --membership-software=samba
Password for Administrator:
root@ste-tpl-deb13cli:~# _
```

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

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

```
root@ste-tpl-deb13cli:~# id testuser1@olivier.local
uid=284201103(testuser1@olivier.local) gid=284200513(domain users@olivier.local) groupes=284200513(domain users@olivier.local)
```

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
```

```
# and here are more per-package modules (the "Additional" block)
session required      pam_unix.so
session optional      pam_sss.so
session optional      pam_wtmpdb.so skip_if=sshd
session optional      pam_systemd.so
session optional      pam_mkhomedir.so skel=/etc/skel umask=077
# end of pam-auth-update config
```

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/sss/sss.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/sss/sss.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>
```

```
root@ste-tpl-deb13cli:/home/ste4d-# id testuser2@olivier.local  
uid=5002(testuser2@olivier.local) gid=100(users) groupes=100(users)
```

VI. Tester la connexion

Se déconnecter des sessions avec :

```
exit
```

Puis tenter une connexion avec l'utilisateur du domaine.

```
Debian GNU/Linux 13 ste-tpl-deb13cli tty1
ste-tpl-deb13cli login: testuser1@olivier.local
Password:
Linux ste-tpl-deb13cli 6.12.48+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.48-1 (2025-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creating directory '/home/testuser1'.
testuser1@olivier.local@ste-tpl-deb13cli:~$
```

Vérifier que le home a été bien créé :

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

```
testuser1@olivier.local@ste-tpl-deb13cli:~$ ls -al /home/
total 16
drwxr-xr-x  4 root                                root                4096  2 oct.  22:15 .
drwxr-xr-x 18 root                                root                4096 30 sept.  08:27 ..
drwx-----  2 ste4d-                            ste4d-              4096  2 oct.  21:54 ste4d-
drwx-----  2 testuser1@olivier.local domain users@olivier.local 4096  2 oct.  22:15 testuser1
testuser1@olivier.local@ste-tpl-deb13cli:~$ _
```

Revision #2

Created 2026-07-29 09:36:51 UTC by Olivier

Updated 2026-07-29 09:40:04 UTC by Olivier