UBUNTU ET DOMAINE AD

RESUME
Nous allons voir dans cette procédure comment lier un client Ubuntu à un domaine AD pas à pas.

Theo MARTIN
SIO23

Pour intégrer un client ou un serveur Ubuntu à un domaine Windows, il faut suivre attentivement les étapes qui vont suivre.

Vous pouvez réaliser ces étapes en faisant des copier-coller des commandes qui suivent (en remplaçant les informations soulignées par les vôtres).

Les variables :

Adresse IP de mon serveur DNS : 192.168.0.3

Nom de domaine : goupil.local

Nom de mon serveur Ubuntu : FOG-SERVER

Nom de mon serveur DNS : WIN-SRV-MARTIN

Pour cela connectez-vous en SSH sur le système concerné.

sudo apt install ssh

Au préalable, changez sur votre poste dans les paramètres réseaux, l'adresse du DNS pour mettre celle de votre serveur DNS (ici : 192.168.0.3). Pour le reste c'est selon votre configuration réseau (DHCP ou Manuel).

Ensuite vous pouvez vous connectez par le protocole SSH avec l'application de votre de choix ou tout simplement avec l'invite de commande de Windows.

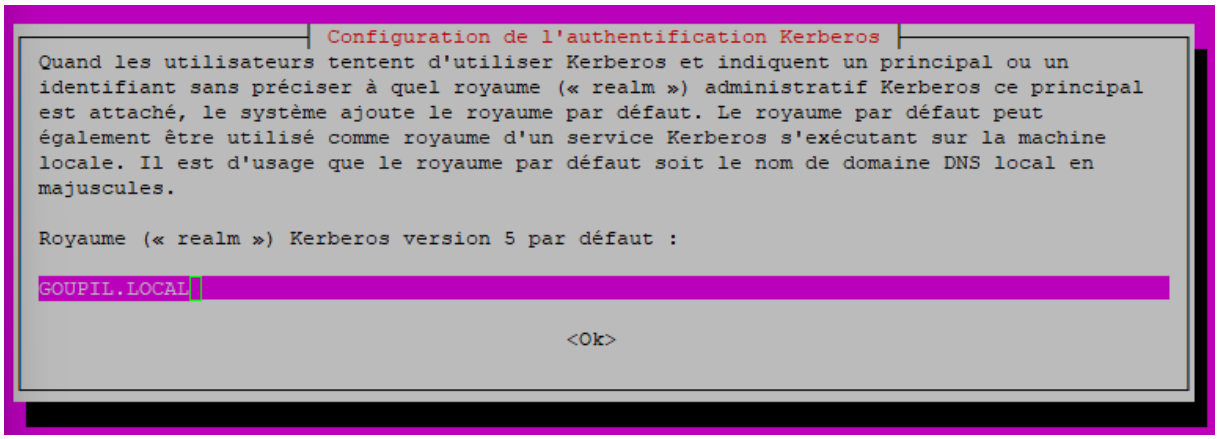
Tout d'abord il faut mettre à jour les paquets du système :

sudo apt update && sudo apt upgrade

Ensuite il faudra installer les paquets suivants :

sudo apt install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind

Lors de l'installation, vous êtes invités à entrer votre « royaume Kerberos », qui n'est autre que votre nom de domaine en MAJUSCULE (ici c'est GOUPIL.LOCAL).

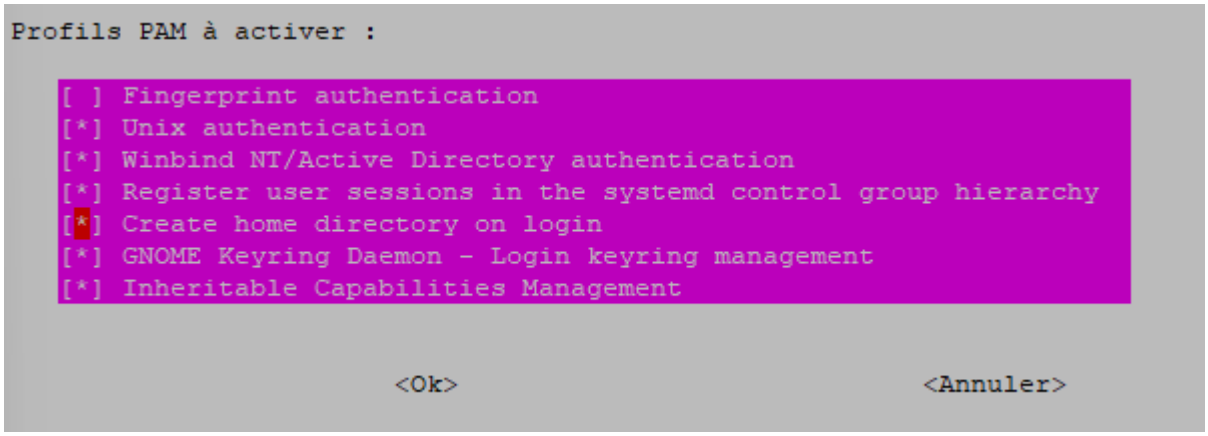


Ensuite mettez à jour la configuration PAM.

Pour cela ouvrez la page de configuration PAM avec la commande suivante :

sudo pam-auth-update

Puis allez à la ligne « ***Create home directory on login*** » et appuyez sur la touche « Espace » de votre clavier pour le cocher comme ceci et appuyez sur « Entrée » pour enregistrer.



Modifiez le fichier de configuration ***/etc/nsswitch.conf*** :

sudo nano /etc/nsswitch.conf

Et remplacez les valeurs déjà présentes par celles-ci :

passwd: compat winbind

group: compat winbind

shadow: compat

gshadow: files

Appuyez sur Ctrl+O et Entrée pour enregistrer, puis sur Ctrl+X pour quitter.

Ensuite nous allons modifier le fichier de configuration se trouvant dans le chemin suivant :

cd /etc/NetworkManager/system-connections/

ls

sudo nano 'Connexion filaire 1.nmconnection'

(Le nom du fichier peut différer, vérifier dans le dossier avec « ***ls*** ».

Et remplacez les champs suivants par vos informations dans le volet [ipv4] :

[ipv4]

dns=192.168.0.3

dns-search=goupil.local

ignore-auto-dns=true

method=auto

Appuyez sur Ctrl+O et Entrée pour enregistrer, puis sur Ctrl+X pour quitter.

Allez dans le fichier ***/etc/resolv.conf*** :

sudo nano /etc/resolv.conf

Et entrez les informations suivantes (changez l'adresse déjà présente et ajoutez la deuxième ligne) :

nameserver 192.168.0.3

search goupil.local

Appuyez sur Ctrl+O et Entrée pour enregistrer, puis sur Ctrl+X pour quitter.

Redémarrez votre machine et reconnectez-vous.

Modifiez le fichier suivant :

sudo nano /etc/hosts

Et entrez les informations suivantes :

127.0.0.1 localhost

127.0.1.1 FOG-SERVER.goupil.local FOG-SERVER

Appuyez sur Ctrl+O et Entrée pour enregistrer, puis sur Ctrl+X pour quitter.

Il va falloir maintenant modifier le fichier de configuration ***/etc/samba/smb.conf***

sudo nano /etc/samba/smb.conf

Et on copie les informations suivantes dans le volet [global] et on modifie « ***realm*** » et « ***workgroup*** ». Ne pas oublier de commenter avec « # » la deuxième ligne « ***workgroup*** » située quelques lignes en dessous de ce « pavé » (photo plus bas).

security = ads

realm = GOUPIL.LOCAL

workgroup = GOUPIL

idmap uid = 10000-20000

idmap gid = 10000-20000

winbind enum users = yes

winbind enum groups = yes

template homedir = /home/%D/%U

template shell = /bin/bash

client use spnego = yes

client ntlmv2 auth = yes

encrypt passwords = yes

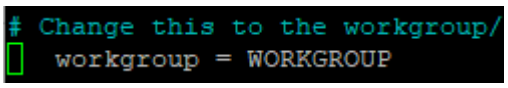
winbind use default domain = yes

restrict anonymous = 2

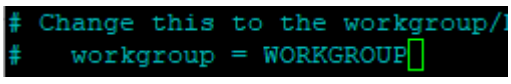
kerberos method = secrets and keytab

winbind refresh tickets = true

Avant :



Après :



Appuyez sur Ctrl+O et Entrée pour enregistrer, puis sur Ctrl+X pour quitter.

On redémarre ensuite le service smbd :

sudo systemctl restart smbd.service

On modifie ensuite notre dernier fichier de configuration ***/etc/krb5.conf*** :

sudo nano /etc/krb5.conf

Et on modifie le fichier pour avoir le même contenu dans les volets suivants :

[libdefaults]

default_realm = ***GOUPIL.LOCAL***

dns_lookup_realm = true

dns_lookup_kdc = true

[realms]

GOUPIL.LOCAL = {

kdc = ***WIN-SRV-MARTIN***

admin_server = ***WIN-SRV-MARTIN***

}

[domain_realm]

.goupil.local = ***GOUPIL.LOCAL***

goupil.local = ***GOUPIL.LOCAL***

Appuyez sur Ctrl+O et Entrée pour enregistrer, puis sur Ctrl+X pour quitter.

Vous pouvez désormais joindre votre système Ubuntu au domaine AD.

Pour cela lancer la commande suivante pour créer un ticket Kerberos (avec un utilisateur du domaine ayant les droits d'administrateur, si vous n'êtes pas sûr, laissez « administrateur » :

sudo kinit administrateur

Entrez votre mot de passe d'administrateur.

```
Password for administrateur@GOUPIL.LOCAL:
```

Nous pouvons vérifier que cela a bien fonctionné :

sudo klist

```
tmartin@FOG-SERVER:~$ sudo klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrateur@GOUPIL.LOCAL

Valid starting       Expires              Service principal
27/04/2023 01:54:55  27/04/2023 11:54:55  krbtgt/GOUPIL.LOCAL@GOUPIL.LOCAL
        renew until 28/04/2023 01:54:25
```

Le ticket expire dans 24h, nous n'allons donc pas tarder et créer un fichier keytab Kerberos :

sudo net ads keytab create -U administrateur

Entrez le mot de passe.

Puis nous joignons le domaine :

sudo net ads join -U administrateur

```
tmartin@FOG-SERVER:~$ sudo net ads join -U administrateur
Password for [GOUPIL\administrateur]:
Using short domain name -- GOUPIL
Joined 'FOG-SERVER' to dns domain 'goupil.local'
```

On redémarre le service Winbind :

sudo systemctl restart winbind.service

Nous pouvons vérifier les utilisateurs du domaine avec la commande : ***wbinfo -u***

Et les groupes avec la commande : ***wbinfo -g***

Vous pouvez ensuite redémarrer la machine et vous connectez avec l'un des comptes utilisateurs du domaine.