

## Projet POE ASR | SOFTEAM

### Administration Windows Server et intégration d'un client Ubuntu à un domaine AD

Instructeur : Youssef SAGAF | Youssef.SAGAF@vizionyd.fr

Dans ce projet, on considère une machine sous Windows server 2016 et une machine client sous Ubuntu 20.04 sous Oracle Virtual Box.

Remarque :

**Vous avez le choix d'utiliser votre propre configuration (nom de domaine, nom et IP des machines, etc) au choix, l'essentiel c'est de réaliser toutes les étapes, peu importe la manière.**

Etape 0 : Installation et configuration du serveur Windows :

1. Installer une machine Windows Server 2016 sous Virtual Box.
2. Procéder aux configurations de base du serveur comme vu en TP (IP du serveur Windows 2016 : **192.168.91.1/16** et le nom de la machine : **WS2016**)
3. Ajouter le rôle DNS
4. Ajoute le rôle AD avec le nom de domaine : « **SENTP.ORG** ».
5. Créer l'OU « **ordinateurs** » à la racine de votre AD.
6. Installer et configurer le serveur FTP.

Etape 1 : Configuration réseaux et mise à jour des paquets :

Procéder aux configurations de base chez dans la machine client Ubuntu (configurations de base lors de l'installation, session, heure et localisation, etc.). On vérifie si la carte réseau est bien activée. On commence par intégrer ce client sur le réseau en lui attribuant les configurations réseaux suivant :

Connect automatically

Wired 802.1x Security IPv4 Settings IPv6 Settings

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.91.161	255.255.255.0	192.168.91.1

DNS servers: 172.16.81.254, 172.16.91.254

Il faut par la suite configurer manuellement le proxy, on va utiliser ici l'adresse 172.16.0.247 ainsi que le port 8080 à toutes les lignes.



A cette étape, il faut effectuer un ping vers votre machine Windows server **WS2016** afin de vérifier que la configuration réseau est opérationnelle : **ping 192.168.91.1**

Mettez à jour votre système maintenant que vous avez accès à internet avec la commande : **sudo apt-get update**

### Etape 2 : Installation des paquets en vue de l'intégration au domaine AD :

On s'intéresse ici à l'installation des paquets nécessaires à la bonne intégration du client sous l'architecture de l'Active Directory **WS2016**.

J'installe en premier le paquet « **likewise-open** » qui permet de simplifier l'intégration de la machine client au domaine, à l'aide de la commande suivant :

```
sudo apt-get install likewise-open
```

On installe par la suite le paquet suivant : « **libpam-moun** » qui permet le montage des volumes de sessions d'utilisateurs avec la commande suivante :

```
sudo apt-get install libpam-mount
```

On installe par la suite le paquet « **smbfs** » qui permet le partage de ressources réseaux sous le système Windows.

### Etape 3 : Nouveau configuration réseau :

Après la configuration réseaux précédente permettant le téléchargement des paquets nécessaires à la bonne intégration du client Ubuntu aux serveur AD, configurer votre carte réseaux pour que le client fasse partie du réseaux « **SENTP.ORG** ».

Pour cela, des modifications au fichier interfaces du système sont nécessaires.

```
user@ubuntucient:/etc/network$ sudo nano interfaces
```

```
user@ubuntuclient: /etc/network
GNU nano 2.2.6 File: interfaces

auto lo
iface lo inet loopback

auto eth0
    iface eth0 inet static
    address 192.168.100.42
    network 192.168.100.0
    netmask 255.255.255.0
    broadcast 192.168.100.255
    gateway 192.168.100.1
    dns-nameservers 192.168.100.10 192.168.100.20
    dns-search sentp.org
```

Ouvrez le fichier `interfaces` avec un éditeur de texte « **nano** » ou « **vim** ». Avant de procéder aux modifications, faites une copie de ce fichier avec un nom différent au cas où l'on ait besoin de récupérer la configuration initiale. Cette carte réseau est configurée en IP statique, ce client a pour adresse IP : **192.168.100.42**. Il faut par la suite configurer la passerelle, le masque de sous-réseau, ainsi que le nom de domaine « **SENTP.ORG** » afin d'intégrer ce poste à l'Active Directory.

Par la suite, on se rend dans le fichier « **resolv.conf** » qui est le fichier de configuration de la bibliothèque « **resolver** » permettant de déterminer, entre autres, quel(s) serveur(s) DNS utiliser pour résoudre un nom de domaine. Le fichier n'est pas encore configuré, mais en modifiant une option dans le fichier « **NetworkManager.conf** », les informations devront s'ajouter automatiquement.

Accéder au fichier et modifier la ligne « **managed** » en remplaçant « **false** » par « **true** », pour activer le management automatique. Il faut par la suite, redémarrer la machine.

```
user@ubuntuclient: /etc/NetworkManager
GNU nano 2.2.6 File: NetworkManager.conf

[main]
plugins=ifupdown,keyfile
dns=dnsmasq

no-auto-default=00:0C:29:D5:DE:B7,

[ifupdown]
managed=true
```

```
user@ubuntuclient: ~
GNU nano 2.2.6 File: /etc/resolv.conf

# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.100.10
nameserver 192.168.100.20
nameserver 127.0.0.1
search sentp.org
```

Une fois la machine redémarrée, retournez voir le fichier « **resolv.conf** » et vous verrez que toutes les informations ont été complétées.

Dans ce fichier, on y trouve 2 options de configurations :

- **nameserver** : serveur de nom d'adresse IP
- **search** : liste de recherche pour les noms d'hôte

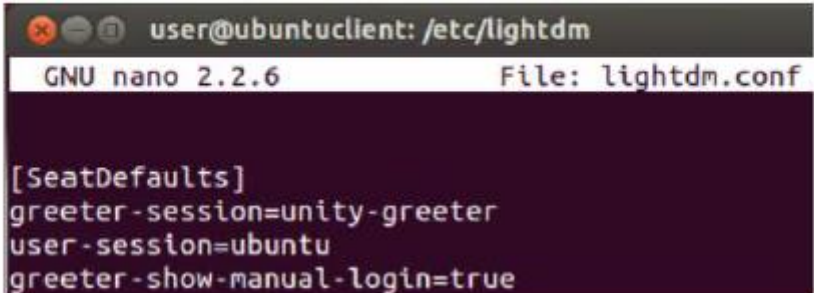
Utilisez la commande « **ifconfig** » pour vérifier si la manipulation a bien fonctionné.

```
user@ubuntuclient:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:d5:de:b7
          inet addr:192.168.100.42  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed5:deb7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:655 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:795 (795.0 B)  TX bytes:49511 (49.5 KB)
```

#### Etape 4 : Configurer du login :

Par défaut, l'écran du login ne présente que les utilisateurs créés sur la station de travail, pour que les sessions créées dans l'Active Directory puissent être accessibles sur le poste Ubuntu. Il faut donc modifier le fichier « **lightdm.conf** ».

```
user@ubuntuclient:/etc/lightdm$ sudo nano lightdm.conf
```



```
[SeatDefaults]
greeter-session=unity-greeter
user-session=ubuntu
greeter-show-manual-login=true
```

Dans ce fichier, on y ajoute la ligne « **greeter-show-manual-login=true** », cette ligne permet au démarrage de pouvoir y ajouter une session d'utilisateur manuellement.

#### Etape 5 : Intégration de la station au contrôleur de domaine :

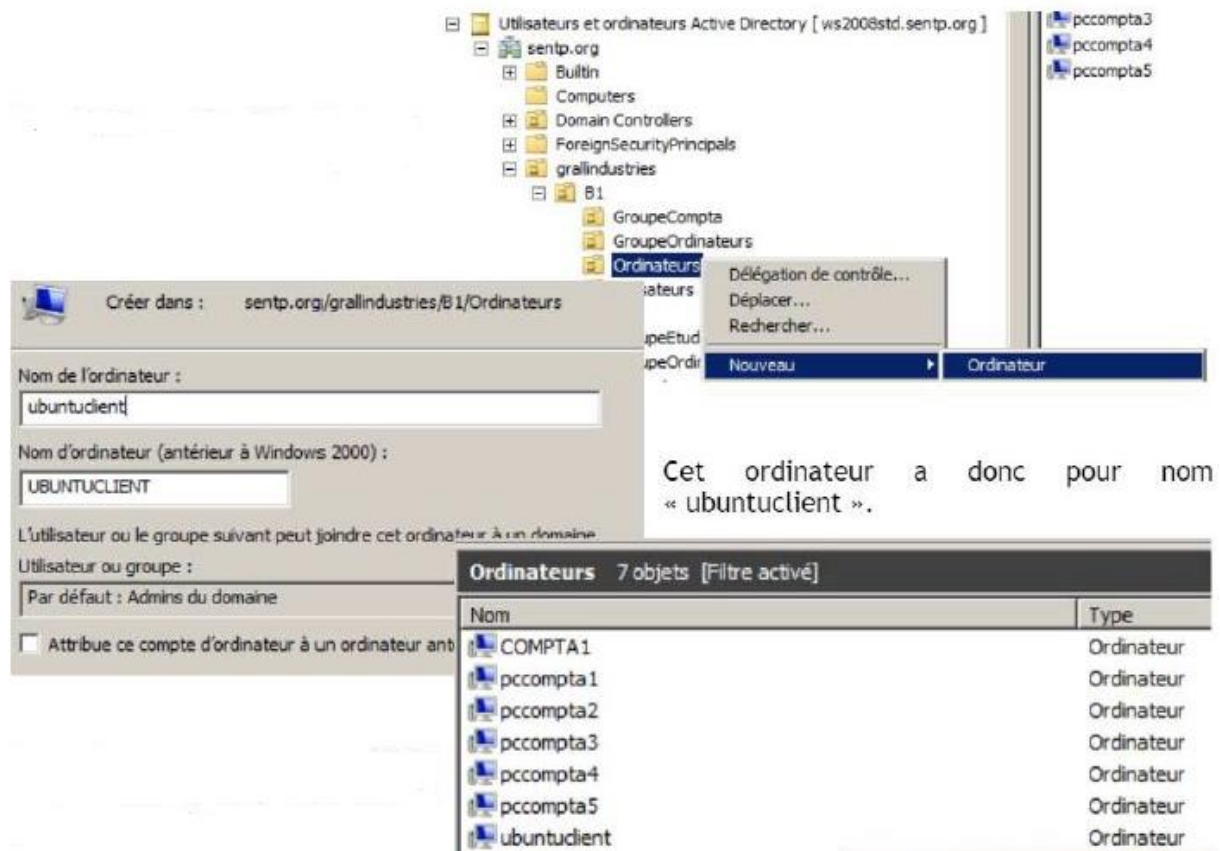
Pour intégrer le poste client au domaine « **SENT.P.ORG** », utiliser la commande suivante :

```
sudo domainejoin-cli join sentp.org administrateur
```

Au démarrage, lorsqu'on arrive à la sélection de session, il y aura un nouveau choix qui apparaît « **login** ». C'est à cet endroit que vous pouvez vous connecter avec une session faisant partie de l'Active Directory à partir du Windows Serveur.



A cette étape, vous pouvez passer à la configuration pour ajouter la machine client dans le serveur Windows serveur. Créez donc un nouvel ordinateur dans le Windows Serveur. Cet ordinateur porte le nom de « **ubuntuclient** ». Vérifier, que l'ordinateur est bien dans la liste des autres postes existants.



Sous le poste Ubuntu, vous pouvez vous connecter avec une session faisant appel à l'AD. Pour cela, mettez « **sentp** » suivi de « **\** » et du nom de la session. Vous pouvez tester avec n'importe quelle machine, ici, « **compta1** ».

```
SENTP\pccompta1@ubuntuclient: ~
SENTP\pccompta1@ubuntuclient:~$
```





## Etape 6 : Authentification lors du montage des volumes :

Afin d'autoriser le montage de volumes, vous pouvez changer les droits d'utilisateur à l'aide de la commande « **chmod** », le « **+s** » donne les droits d'administrateur à l'utilisateur lors de l'exécution du script, en utilisant la commande : **sudo chmod +s /usr/bin/smbmount**

« **smbmount** » est un lien symbolique vers « **/sbin/mount.smbfs** ». Le lien passe rouge pour signifier que les modifications des droits d'exécutions ont été prise en compte, comme l'illustre la figure suivante :

```
user@ubuntuclient:~$ ls -l /usr/bin/smbmount
lrwxrwxrwx 1 root root 17 mai 16 2013 /usr/bin/smbmount -> /sbin/mount.smbfs
```

## Etape 7 : Authentification lors du montage des volumes :

Créer un fichier « **common-pammount** » qui va permettre d'utiliser les identifiants afin de donner l'accès à son dossier personnel partagé sur le Windows server. Pour cela, dans **/etc/pam.d**, créer votre fichier avec la commande suivante :

```
user@ubuntuclient:/etc/pam.d$ sudo nano common-pammount
```

```
GNU nano 2.2.6 File: common-pammount
auth optional pam_mount.so use_first_pass
session optional pam_mount.so
```

Dans ce fichier, on y ajoute le contenu ci-dessus, « **use\_first\_pass** » signifie qu'on ne demande pas de mot de passe à l'utilisateur lorsqu'il voudra accéder à son dossier partagé.

## Etape 8 : Configuration du démarrage de session :

```
user@ubuntuclient:/etc/pam.d
GNU nano 2.2.6 File: lightdm Modified

#%PAM-1.0
auth requisite pam_nologin.so
auth sufficient pam_permit.so
@include common-account
auth optional pam_limits.so
@include common-session
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so
session optional pam_limits.so
session required pam_env.so readenv=1
session required pam_env.so readenv=1 user_readenv=1 envfile=/etc/default/S
@include common-password
@include common-pammount

user@ubuntuclient:/etc/pam.d
GNU nano 2.2.6 File: lightdm-autologin Modified

#%PAM-1.0
auth requisite pam_nologin.so
auth required pam_permit.so
@include common-account
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.S
session required pam_limits.so
session optional pam_env.so readenv=1
session required pam_env.so readenv=1 user_readenv=1 envfile=/etc/default/S
@include common-password
@include common-pammount
```

Vous pouvez maintenant modifier les fichiers « **lightdm** » et « **lightdm-autologin** », « **lightdm** », étant le gestionnaire graphique de sélection des sessions au démarrage, dans ces deux fichiers, pour y ajouter la ligne « **@include common-pammount** » qui est le fichier configuré précédemment qui va permettre de pouvoir se logger sans devoir entrer son mot de passe car il se rappellera le mot de passe entré lors de la première fois.

## Etape 9 : Déclaration des volumes à monter :

Il faut configurer le script « `pam_mount.con.xml` » en utilisant la commande « `sudo nano pam_mount.conf.xml` », pour y ajouter les deux lignes illustrées par la figure suivante :

```
<volume user="*" mountpoint="/partage" path="/partage" server="192.168.100.10" fstype="smbfs"/>
<volume user="*" mountpoint="/SENTP/%(USER)" path="/%(USER)" server="192.168.100.10" fstype="smbfs"/>
```

La première ligne représente le lecteur « `partage` » qui est le partage commun entre tous les utilisateurs. La deuxième ligne représente le lecteur personnel de chaque utilisateur qui est monté lors de l'ouverture de leur session.

## Etape 10 : Test de la station Ubuntu dans le domaine AD « SENTP.ORG » :

Test sous session graphique de l'accès au répertoire « `utilisateur` ».



Test sous le terminal de l'accès au répertoire « `utilisateur` ».

```
SENTP\pccompta1@ubuntuclient:~$ cd SENTP
SENTP\pccompta1@ubuntuclient:~/SENTP$ ls
SENTP\pccompta1
SENTP\pccompta1@ubuntuclient:~/SENTP$ cd SENTP\pccompta1/
SENTP\pccompta1@ubuntuclient:~/SENTP/SENTP\pccompta1$ ls
test
SENTP\pccompta1@ubuntuclient:~/SENTP/SENTP\pccompta1$ mkdir test2
SENTP\pccompta1@ubuntuclient:~/SENTP/SENTP\pccompta1$ ls
test test2
```

Avec le terminal, vous devez pouvoir voir que vous accédez à votre dossier personnel et voir un dossier « `test` » que vous aurez créé dans la session graphique, et voir aussi que vous avez les droits identiques à la version graphique. Vous pouvez aussi créer un deuxième dossier « `test2` » avec la commande « `mkdir` ».

## Etape 10 : Test de l'accès au serveur FTP

En étant dans la machine Linux, tester l'accès au serveur FTP, en utilisant un client FTP ou en ligne de commande.