Table des matières :

Avant-Propos

Compétences :

- A1.1.1 Analyse du cahier des charges d'un service à produire
- A1.2.4 Déterminer des tests nécessaires à la validation d'un service (3)
- A4.1.9 Rédaction d'une documentation technique

```
iface eth0 inet static
                address 192.168.1.144
                netmask 255.255.255.0
                gateway 192.168.1.254
```

La suite de logiciels Samba est une ré-implémentation en logiciels libres des protocoles réseau clients et serveurs de Microsoft. Jusqu'ici, Samba 3 était capable de couvrir l'ensemble des fonctionnalités d'un réseau de type NT4 avec un certain nombre d'améliorations, comme la possibilité d'utiliser OpenLDAP comme backend de stockage ou encore un fonctionnement en cluster. Samba 3 gère notamment l'authentification en mode serveur maître/esclave (PDC/BDC pour Primary Domain Controler et Backup domain controler) et la fourniture des services de partage de fichiers et d'impression.

La compatibilité avec l'Active Directory de Microsoft est cependant limitée à la possibilité de joindre un domaine – au sens domaine de sécurité – et il devenait de plus en plus pressant de rattraper le retard accumulé. En effet, Active Directory est sorti en 2000, samba 4 a été démarrée en 2003

Objectif :

Dans cette procédure, nous allons montrer comment installer et configurer samba 4 en contrôleur de domaine sous Debian.

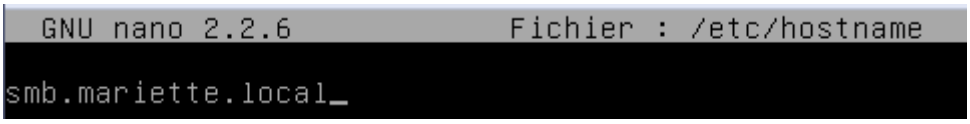
OS	Distribution	Version
Debian	Linux	8.5

1. Mise en place d'un domaine sous Samba 4

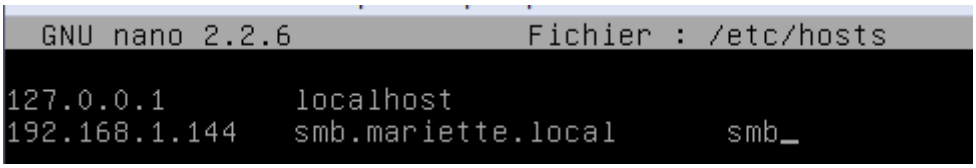
Le DNS est élément clé d'une architecture Active directory. Les clients notamment recherchent les contrôleurs de domaine via des requêtes DNS de type srv, afin de localiser un contrôleur de domaine et certain nombre de mise à jour DNS dynamique se font via Kerberos.

a. Préparation du serveur

On Modifie d'abord le fichier /etc/hostname pour qu'il contienne le nom FQDN de la machine



Modifier le fichier /etc/hosts pour qu'il contienne la résolution DNS du FQDN de la machine sur son IP, avec le nom long puis le nom court.



On configure le DNS pour pointer sur lui-même dans le fichier /etc/resolv.conf en renseignant 127.0.0.1

```
  GNU nano 2.2.6            Fichier : /etc/resolv.conf

domain sio.local
search sio.local
search mariette.local
nameserver 127.0.0.1_
nameserver 192.168.1.49
nameserver 192.168.1.50
nameserver 8.8.8.8
nameserver 81.253.149.6
nameserver 80.10.246.136
nameserver 192.168.1.254
```

On reboot ensuite la VM

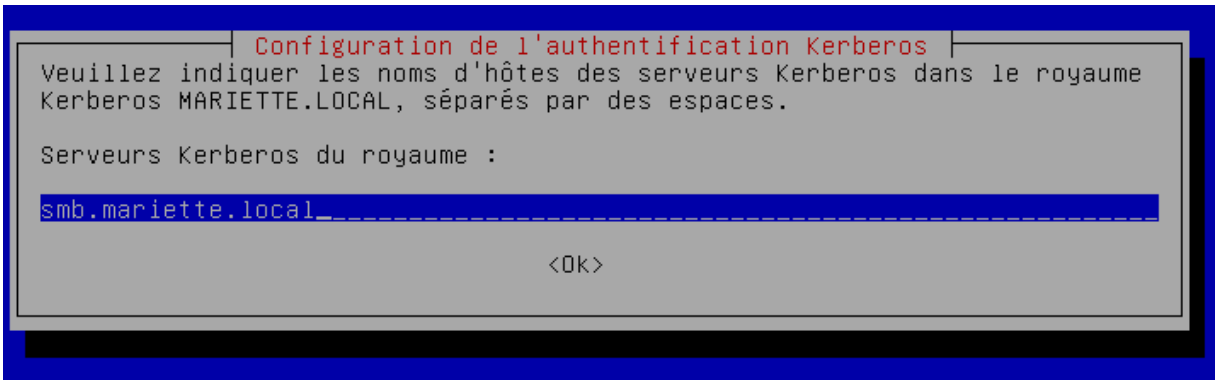
```
root@debian8:~# reboot_
```

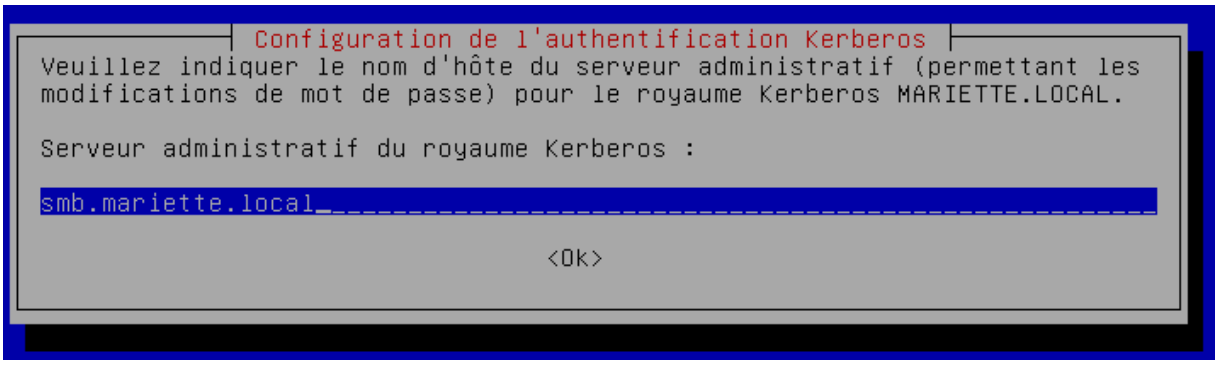
On installe ensuite les paquets suivant pour la compilation de samba et pour son bon fonctionnement.

On fait un installe update juste avant pour vérification :

```
root@smb:~# apt update_
```

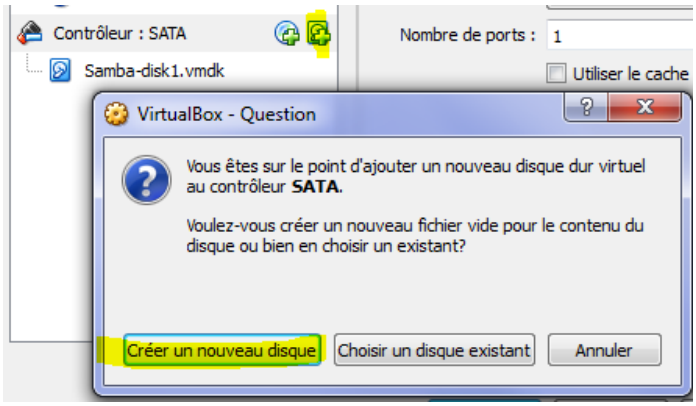
```
root@smb:~# apt-get install build-essential libacl1-dev libattr1-dev libblkid-de
v libgnutls28-dev libreadline-dev python-dev libpam0g-dev python-dnspython gdb p
kg-config libpopt-dev libldap2-dev dnsutils libbsd-dev attr krb5-user docbook-xs
l libcups2-dev acl_
```





Le système de fichiers et le montage de vos partitions doit prendre en charge les ACL et les attributs étendus. Il vous faudra donc modifier le fichier /etc/fstab en conséquence.

1. on ajoute un second disque à votre machine virtuelle.



2. Formater-la en ex4.

```
root@smb:~# dmesg | grep sdb
[   13.475128] sd 1:0:0:0: [sdb] 20971520 512-byte logical blocks: (10.7 GB/10.0
 GiB)
[   13.475165] sd 1:0:0:0: [sdb] Write Protect is off
[   13.475169] sd 1:0:0:0: [sdb] Mode Sense: 00 3a 00 00
[   13.475184] sd 1:0:0:0: [sdb] Write cache: enabled, read cache: enabled, does
n't support DPO or FUA
[   13.514417]  sdb: unknown partition table
[   13.514851] sd 1:0:0:0: [sdb] Attached SCSI disk
```

```
fdisk /dev/sdb_
```

```
Commande (m pour l'aide) : n
Type de partition
   p   primaire (0 primaire, 0 étendue, 4 libre)
   e   étendue (conteneur pour partitions logiques)
Sélectionnez (p par défaut) : p
Numéro de partition (1-4, 1 par défaut) : 1
Premier secteur (2048-20971519, 2048 par défaut) : 2048
Dernier secteur, +secteurs ou +taille{K,M,G,T,P} (2048-20971519, 20971519 par dé
faut) : 20971519

Une nouvelle partition 1 de type « Linux » et de taille 10 GiB a été créée.

Commande (m pour l'aide) : w
La table de partitions a été altérée.
Appel d'ioctl() pour relire la table de partitions.
Synchronisation des disques.
```

On peut faire un fdisk –l

```
Device     Boot Start      End  Sectors Size Id Type
/dev/sdb1        2048 20971519 20969472  10G 83 Linux
```

On formate en ex4

```
root@smb:~# mkfs.ext4 /dev/sdb1
mke2fs 1.42.12 (29-Aug-2014)
En train de créer un système de fichiers avec 2621184 4k blocs et 655360 i-noeud
s.
UUID de système de fichiers=54a7c8a5-915c-40a2-a194-eda926621315
Superblocs de secours stockés sur les blocs :
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocation des tables de groupe : complété
Écriture des tables d'i-noeuds : complété
Création du journal (32768 blocs) : complété
Écriture des superblocs et de l'information de comptabilité du système de
fichiers : complété
```

3. Monter cette partition avec les ACL dans le fichier /etc/fstab.

/dev/sbd1/samba ext4 user_xattr, acl, errors=remount-ro 0 1

```
root@smb:~# nano /etc/fstab _
```

```
  GNU nano 2.2.6              Fichier : /etc/fstab                        Modifié

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=4a49dc2d-9919-4860-8bf7-b8c1c63cb92d /               ext4    errors=remoun$
# /home was on /dev/sda8 during installation
UUID=cf73df85-2dd6-4f55-a9fa-20721c8866c8 /home           ext4    defaults     $
# /tmp was on /dev/sda7 during installation
UUID=24b51c3e-dabe-4ebe-b78f-d695acd01117 /tmp            ext4    defaults     $
# /var was on /dev/sda5 during installation
UUID=25385142-83d5-462b-bb89-562f62cb65ca /var            ext4    defaults     $
# swap was on /dev/sda6 during installation
UUID=2fd9d80c-f49a-4f96-ba59-ce78e1074c0b none            swap    sw           $
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
/dev/sdb1       /samba  ext4    user_xattr,acl,errors=remount-ro 0 1
```

ip add

4. Créer le répertoire samba qui contiendra les partages.

```
root@smb:~# mkdir /samba_
```

Pour que les utilisateurs « standards » puissent également définir des ACL, il est nécessaire d'ajouter l'option user_xattr.

Pour éviter de redémarrer le serveur pour les partitions actives, il est possible de les remonter avec les options adéquates de cette façon :

```
root@smb:~# mount -o remount,rw,acl,user_xattr /
```

On redémarre la vm

```
root@smb:~# reboot_
```

Le protocole d'authentification par défaut de l'Active Directory étant Kerberos v5, il est important que les horloges soient à l'heure. Le serveur NTPD doit être installé. Il faut donc indiquer le serveur NTP source et le firewall du réseau devra autoriser les requêtes NTP vers l'exterieur. Cela revient à definir le parametre serveurs du fichier /etc/ntpd.conf. Ce paramètre peut etre multivalué. Je vous recommande d'utiliser fr.pool.org afin d'avoir une liste de serveurs sources fiables et disponibles.

```
root@smb:~# apt-get install ntpdate_
```

```
root@smb:~# ntpdate fr.pool.ntp.org
14 Oct 15:40:26 ntpdate[1003]: the NTP socket is in use, exiting
```

```
root@smb:~# apt-get install ntp_
```

On relance ntp

```
root@smb:~# systemctl restart ntp_
```

Maintenant que votre serveur de temps est configuré, vérifier qu'il est bien synchronisé :

```
root@smb:~# ntpq -pn
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*151.80.124.104  210.240.96.206   2 u    1   64    3   26.728   23.159  31.431
 195.154.41.195  195.13.23.5      3 u   56   64    1   24.897   13.825  32.598
 5.196.160.139   10.21.137.1      2 u   55   64    1   27.998   12.518  29.592
 194.177.34.115  200.93.81.94     3 u   54   64    1   24.774   13.517  32.850
root@smb:~#
```

b. Compilation et installation

Récupérer le tar.gz, compiler et installer (ça peut prendre 10-15 minutes)

```
root@smb:~# cd /root
root@smb:~# wget --no-check-certificate https://download.samba.org/pub/samba/sam
ba-4.5.0.tar.gz_
```

```
root@smb:~# tar -zxvf samba-4.5.0.tar.gz _
```

```
root@smb:~# cd samba-4.5.0/
```

```
root@smb:~/samba-4.5.0# ./configure_
```

Ajoute le chemin vers les binaires Samba au PATH de votre shell.

```
root@smb:~/samba-4.5.0# echo "export PATH=$PATH:/usr/local/samba/bin/:/usr/local
/samba/sbin/:" >> ~/.bashrc && source ~/.bashrc
```

c. Création du domaine

1. faire une copie du fichier /etc/krb5.conf

```
root@smb:/etc# cp krb5.conf save.krb5.conf_
```

2. Pour configurer kerberos locale, modifier le fichier /etc/krb5.conf, supprimer tout ce qu'il y a dedans et rajouter :

```
  GNU nano 2.2.6                Fichier : krb5.conf

[libdefaults]
 dns_lookup_realm = false
 dns_lookup_kdc = true
 default_realm = MARIETTE.LOCAL_
```

Effacer le fichier smb.conf s'il a déjà été généré (il va être régénéré par la commande de rpovisionning samba-tool juste après)

```
root@smb:/etc# rm -f /usr/local/samba/etc/smb.conf
```

Pour crée le domaine de samba4 en DC :

```
root@smb:~# samba-tool domain provision --use-rfc2307 --realm=MARIETTE.LOCAL --d
omain MARIETTE --adminpass Password1234 --server-role=dc --interactive_
```

Le mot de passe (Password1234) doit respecter un certain niveau de complexité (>=8 caractères avec des chiffres et caractères spéciaux).

Le schéma RFC2307 est une extension LDAP qui permet de renseigner les options pour Unix de l'AD (SFU, service for Unix) et avoir des UID /GID correctement renseigné et mappé entre tous les serveurs du domaine.

```
root@smb:~# samba-tool domain provision --use-rfc2307 --realm=MARIETTE.LOCAL --d
omain MARIETTE --adminpass Password1234 --server-role=dc --interactive
Realm [MARIETTE.LOCAL]:
 Domain [MARIETTE]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:

 DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]:
Administrator password:
Retype password:
```

```
Server Role:           active directory domain controller
Hostname:              smb
NetBIOS Domain:        MARIETTE
DNS Domain:            mariette.local
DOMAIN SID:            S-1-5-21-2849176768-326007168-2752918802
```

On remarque ci-dessous notre info.

Il est possible de changer le mot de passe du compte administrateur avec les droits superutilisateur (root) avec la commande :

Samba-tool user setpassword administrator

d. Création du domaine

Pour démarrer l'ensemble des processus, rien de plus simple, il suffit de lancer la commande samba. Pour l'arrêter, un killall samba suffit.

Pour connaître l'ensemble des services démarrés par samba :

```
root@smb:~# samba
root@smb:~# samba-tool processes
 Service:                  PID
-----------------------------
dnsupdate                21185
cldap_server             21178
rpc_server               21174
nbt_server               21175
winbind_server           21186
kdc_server               21180
notify-daemon            21191
kccsrv                   21184
samba                        0
dreplsrv                 21181
dnssrv                   21189
```

e. Tests

Tester que le kerberos est bien configuré, attention, l'administrateur par défaut est administrator en anglais (taper le mot de passe, si ça ne renvoie rien ou qu'il parle juste de l'expiration de mot de passe, c'est que ça marche).

```
root@smb:~# kinit administrator
Password for administrator@MARIETTE.LOCAL:
Warning: Your password will expire in 41 days on ven. 25 nov. 2016 15:32:44 CET
```

Pour visualiser le ticket reçu :

```
root@smb:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@MARIETTE.LOCAL

Valid starting       Expires              Service principal
14/10/2016 16:44:09  15/10/2016 02:44:09  krbtgt/MARIETTE.LOCAL@MARIETTE.LOCAL
        renew until 15/10/2016 16:44:03
```

Tester les DNS

```
root@smb:~# dig @localhost google.fr
```

```
root@smb:~# dig @localhost smb.mariette.local
```

```
root@smb:~# dig -t SRV @localhost _ldap._tcp.mariette.local_
```

```
root@smb:~# dig -t SRV @localhost _kerberos._udp.mariette.local_
```

```
oot@smb:~# smbclient -L localhost -U%
omain=[MARIETTE] OS=[Windows 6.1] Server=[Samba 4.5.0]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.5.0)
omain=[MARIETTE] OS=[Windows 6.1] Server=[Samba 4.5.0]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

Pour tester l'authentification à un partage tel que netlogon en tant qu'administrateur :

```
root@smb:~# smbclient //localhost/netlogon -UAdministrator -c 'ls'
Enter Administrator's password:
Domain=[MARIETTE] OS=[Windows 6.1] Server=[Samba 4.5.0]
  .                                   D        0  Fri Oct 14 16:32:32 2016
  ..                                  D        0  Fri Oct 14 16:32:44 2016

                3596128 blocks of size 1024. 1784728 blocks available
```

f. Intégrer un poste au domaine

Pour intégrer un poste windows à un domaine AD, il faut obligatoirement une version professionnelle, les versions famillliales n'étant pas prise en charge. Que ce soit en IP fixe ou en DHCP, le poste client devra parvenir à résoudre votre zone DNS. Enfi, et ceci est une contrainte inhérente au protcole Kerberos, il ne doit pas y avoir unn décalage d'horloge de plus de cinq minutes entre KDC et le client.

Avant toute chose, s'assurer que le client utilise le serveur Samba en tant que serveur DNS et que le nom de domaine DNS est bien mariette.local.

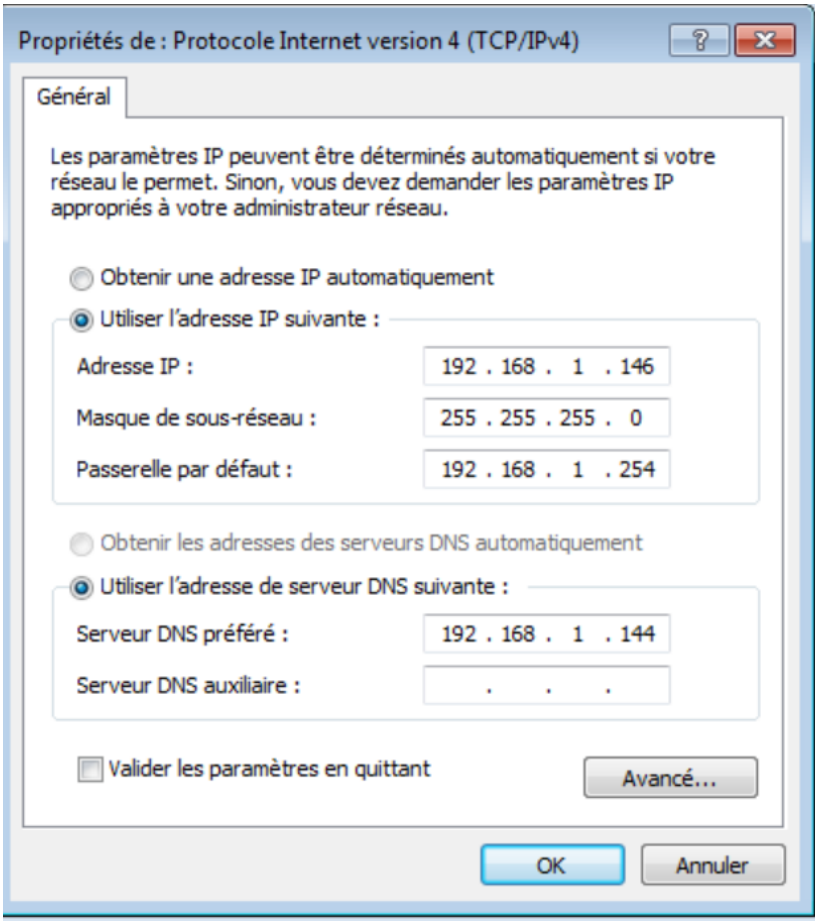
Pour faire rejoindre le client windows au domaine mariette en utilisant le compte Administrator, vous pouvez le faire graphiquement ou par ligne de commande.

Netdom /domain :mariette.local :user :administrateur /password :secret MEMBER PC-TEST /joindomain

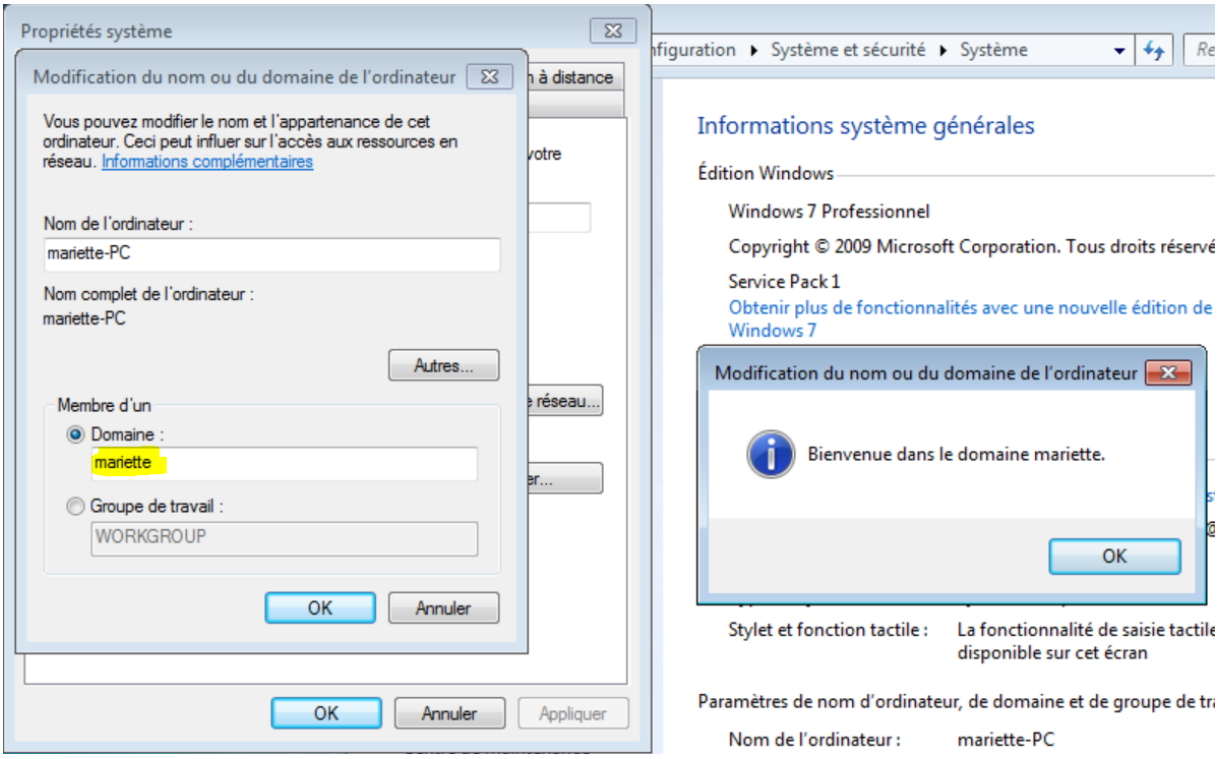
Pour ce TP, on a choisi la méthode graphique :

Ne pas oublier d'ajouter les additions invités qui sont Périphérique > insérée l'image CD des additions invités

On commence par mettre une adresse ip :



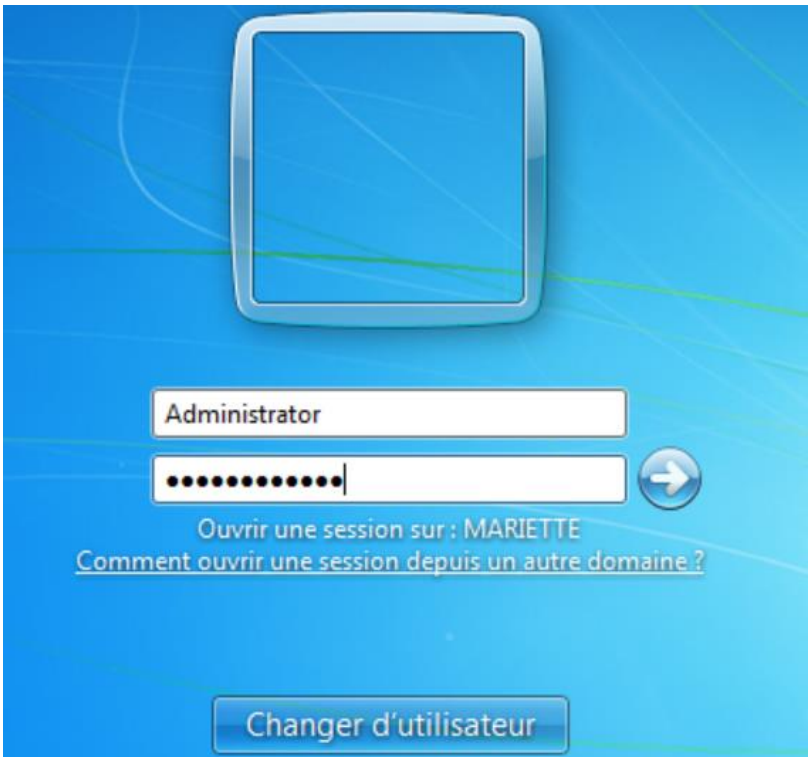
On ajoute ensuite le pc au domaine : (lors de l'ajout du domaine, les identifiants du superutilisateur seront demandés) (administrator et Password1234)



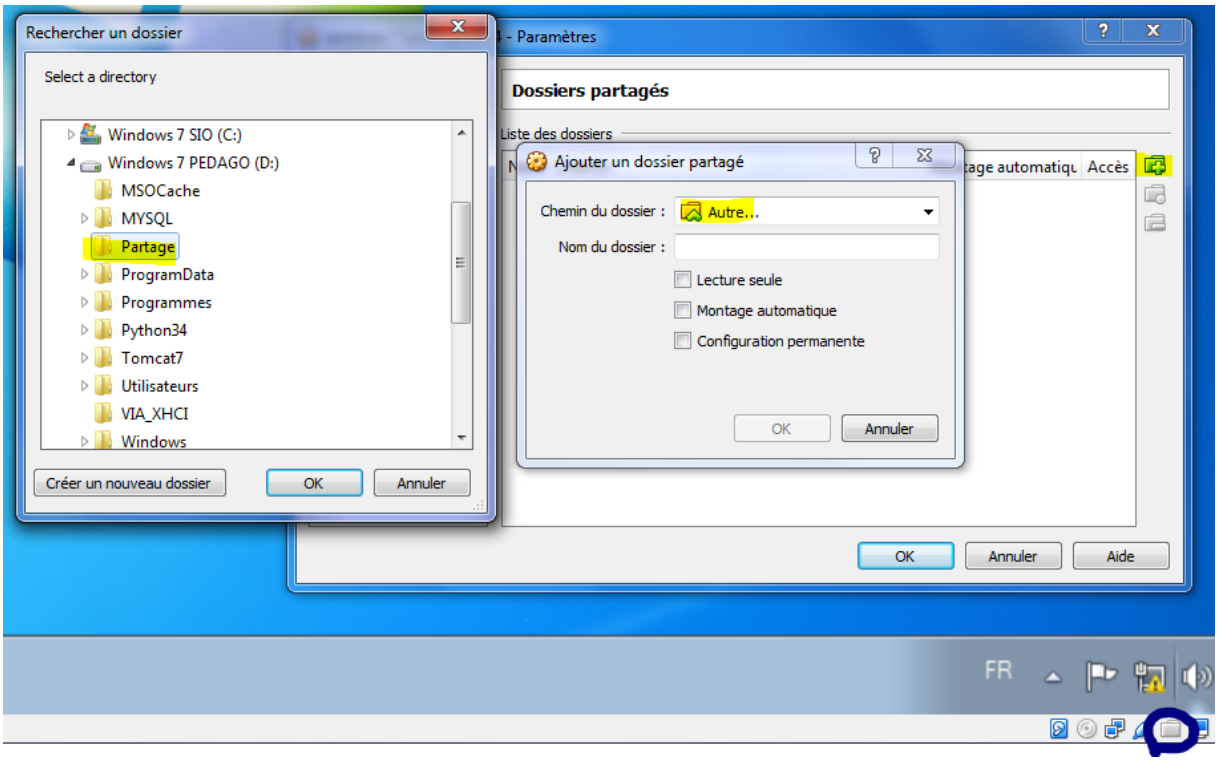
g. Installation de RSAT (remote server administration tools) sur le client

Les outils d'administration de serveur distant pour windows 7 avec SP1 permettent aux administrateurs informatiques de gérer des roles et des fonctionnalités installés sur des ordinateurs Windows Server et Samba 4.

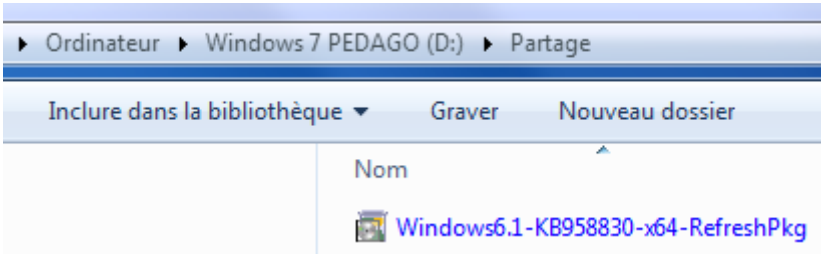
Apres le redémarrage, il faudra se connecter en tante qu'Administrator :



Il faut ensuite ajouter un dossier permanent :



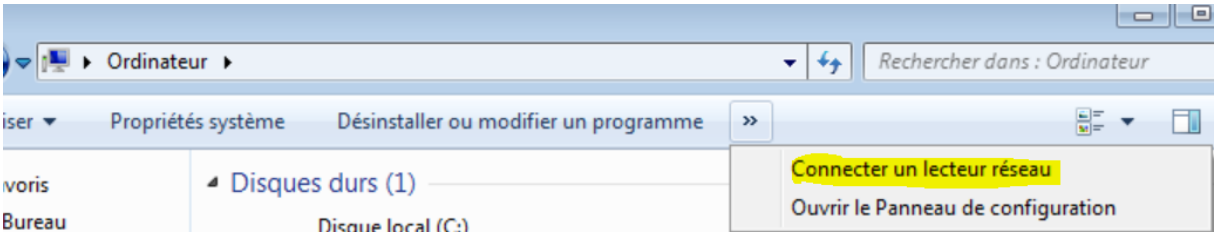
Le dossier partage a été créé avant, il contient les outils d'administration de serveur.

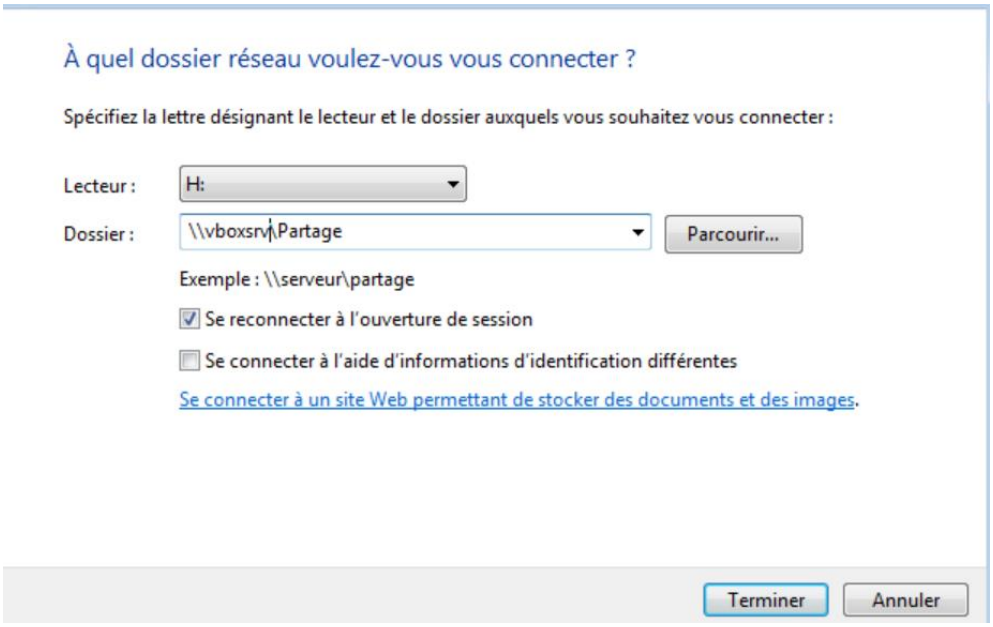


On installe ensuite le KB (l'installation est très longue, 10 minutes)

Pour cela on doit récupérer le fichier sous le client windows 7 :

On va donc dans ordinateurs pour connecter un lecteur réseau :



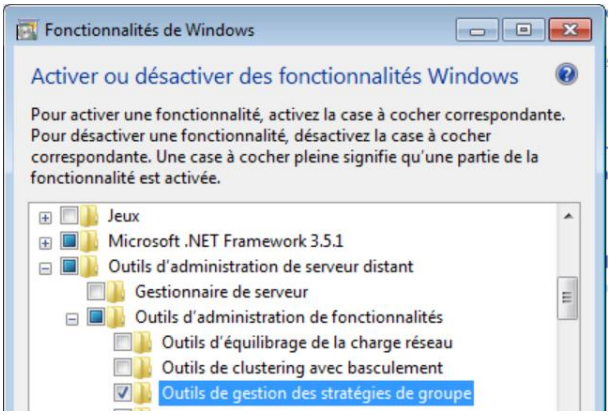


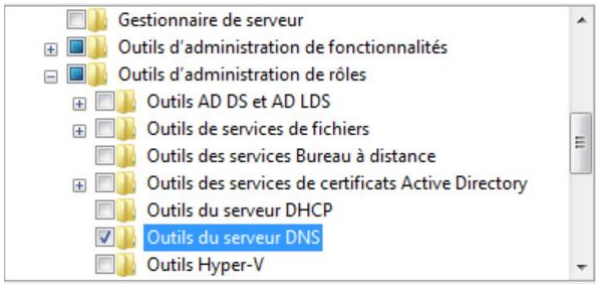
On peut maintenant lancer l'installation

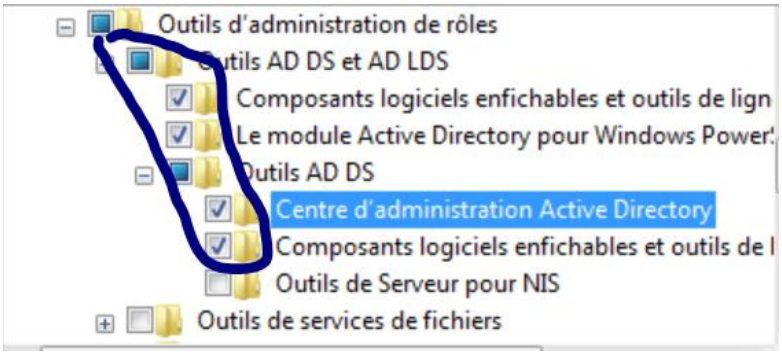
On accepte les termes de contrats.

Une fois installer, il faut aller dans démarrer > panneau de configuration > Programmes > activer ou désactiver des fonctionnalités windows

Il faut cocher les fonctionnalités suivantes :



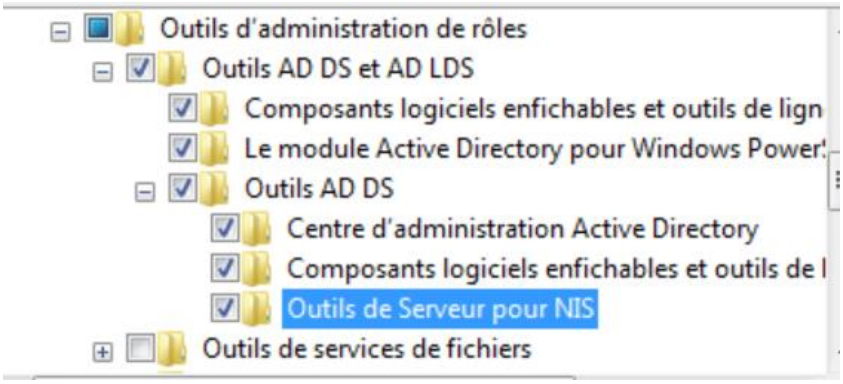




On valide les changements :

Si vous avez configuré votre serveur samba4 avec l'option RFC2307, ou que vous avez mis à jour à samba3NT4 vers samba4, il faut alors gerer les uid/gid linux des utilisateurs et activer en plus les options NIS :

(Dans notre cas, on l'active)



Les consoles MMC se trouvent dans Panneau de configuration/Système et sécurité/Outils d'administration.

On peut utiliser les différentes consoles MMC (gestion AD, DNS, GPO, …)

3. L'outil samba-tool

Samba 4 est entièrement administrable en ligne de commandes. La commande samba-tool permet de réaliser l'ensemble des tâches courantes d'administration d'un réseau Microsoft windows. La syntaxe de la commande est très bien détaillée dans l'aide contextuelle. Les paramètres additionnels

sont documentés en indiquant le paramètre –H à la sous-commande désirée sans indiquer de paramètre.

3.1. Création du domaine

```
root@smb:~# samba-tool domain info 192.168.1.144
Forest           : mariette.local
Domain           : mariette.local
Netbios domain   : MARIETTE
DC name          : smb.mariette.local
DC netbios name  : SMB
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
```

3.2. Modification de la stratégie du mot de passe

Dans samba4 la stratégie de mot de passe domaine est gérée en ligne de commande

- Pour la complexité (par défaut activé)
- Pour la taille minimale du mot de passe (par défaut 7 caractères)
- Pour l'Age minimal/maximal du mot de passe (par défaut min 1/max 42)
- Pour la durée d'expiration du mot de passe (365 jours au lieu de 42 jours par défaut).

Pour voir la configuration en place :

```
root@smb:~# samba-tool domain passwordsettings show
Password informations for domain 'DC=mariette,DC=local'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Voici l'exemple d'une configuration complexité (ne pas le faire)

samba-tool domain passwordsettings set --complexity=off

samba-tool domain passwordsettings set --history-length=0

samba-tool domain passwordsettings set --min-pwd-age=0

samba-tool domain passwordsettings set --max-pwd-age=0

samba-tool domain passwordsettings set --min-pwd-length=6

samba-tool domain passwordsettings set --min-pwd-length=7 --max-pwd-age=365

Affichage des rôles FSMO (Flexible Single Master operation)

```
root@smb:~# samba-tool fsmo show
SchemaMasterRole owner: CN=NTDS Settings,CN=SMB,CN=Servers,CN=Default-First-Site
-Name,CN=Sites,CN=Configuration,DC=mariette,DC=local
InfrastructureMasterRole owner: CN=NTDS Settings,CN=SMB,CN=Servers,CN=Default-Fi
rst-Site-Name,CN=Sites,CN=Configuration,DC=mariette,DC=local
RidAllocationMasterRole owner: CN=NTDS Settings,CN=SMB,CN=Servers,CN=Default-Fir
st-Site-Name,CN=Sites,CN=Configuration,DC=mariette,DC=local
PdcEmulationMasterRole owner: CN=NTDS Settings,CN=SMB,CN=Servers,CN=Default-Firs
t-Site-Name,CN=Sites,CN=Configuration,DC=mariette,DC=local
DomainNamingMasterRole owner: CN=NTDS Settings,CN=SMB,CN=Servers,CN=Default-Firs
t-Site-Name,CN=Sites,CN=Configuration,DC=mariette,DC=local
DomainDnsZonesMasterRole owner: CN=NTDS Settings,CN=SMB,CN=Servers,CN=Default-Fi
rst-Site-Name,CN=Sites,CN=Configuration,DC=mariette,DC=local
ForestDnsZonesMasterRole owner: CN=NTDS Settings,CN=SMB,CN=Servers,CN=Default-Fi
rst-Site-Name,CN=Sites,CN=Configuration,DC=mariette,DC=local
```

3.3. Gestions des utilisateurs

Pour créer un utilisateur : bob et mdp : Azerty1+

```
root@smb:~# samba-tool user create bob Azerty1+
User 'bob' created successfully
```

Pour connaître le numéro UID et SID d'un utilisateur :

```
root@smb:~# wbinfo --name-to-sid bob
S-1-5-21-2849176768-326007168-2752918802-1104 SID_USER (1)
```

Pour lister les utilisateurs :

```
root@smb:~# samba-tool user list
Administrator
krbtgt
Guest
bob
```

3.4. Gestions des groupes

Création d'un groupe :

```
root@smb:~# samba-tool group add "rt2a"
Added group rt2a
```

On ajoute l'utilisateur bob au groupe :

```
root@smb:~# samba-tool group addmembers "rt2a" bob
Added members to group rt2a
```

Liste des membres d'un groupe :

```
root@smb:~# samba-tool group listmembers "rt2a"
bob
```

4. La société exemple