SERIE 3/UN
Romain DESCAMPS
Quentin GILMART
Frédéric HUBERT
Thomas VAN GELDER
Robert WORONKO

Fiche d'installation d'un Serveur Samba

Objectif

Intégrer un serveur de fichiers Linux dans un environnement Windows.

Difficulté

Avancé.

Contexte du sujet

Une école d'informatique aimerait utiliser un serveur Linux comme serveur de fichiers au même titre que d'autres serveurs de fichiers Windows. Avant d'utiliser cette solution, elle désire avoir un « Proof of Concept » dont voici les spécificités.
Sur ce serveur Linux, un répertoire public sera partagé pour tout le monde. Ce répertoire contiendra des ressources utiles pour tous les étudiants. Ce répertoire sera mis à jour par les administrateurs systèmes et sera accessible en lecture pour tout le monde.
Il y aura également sur ce serveur Linux le répertoire personnel(privé) de quelques étudiants (5).
L'école dispose déjà d'un Active Directory Windows pour la gestion d'identité et ne compte pas en changer. L'école insiste sur le fait que l'objectif est de faire en sorte que le serveur Linux puisse être utilisé au même titre que d'autre serveurs fichiers Windows. On doit donc pouvoir créer dans L'AD un compte étudiant ayant un disque Z:\ (son répertoire personnel) situé sur le serveur Linux.
Sur les serveurs de fichiers Windows, le répertoire personnel d'un utilisateur n'est accessible que pour cet utilisateur et l'administrateur(droits). Ceci devrait être identique sur le serveur Linux.
Réfléchissez également au fait que le but sera de placer beaucoup plus de répertoires personnels par la suite. Faut-il prévoir de l'automatisation ou autre chose ?

Prérequis

- Un serveur Linux Debian (nous avons utilisé la version 8)
- Un serveur Windows Server, sur lequel sera installé un Windows Active Directory (nous avons utilisé la version de Windows Serveur 2016)
- Un client Windows (Nous avons utilisé une version de Windows 10)

Instructions d'installations

NOTE : Tous les fichiers de configuration devront être adaptés selon vos besoins

1. Installer le serveur Windows Server 2016 ainsi que le serveur Active Directory et DNS.
   ➔ Cf. : Cours d'administration Windows de Mr. Marguos
2. Installer le Windows 10 et l'intégrer au domaine que l'on vient de créer.
   ➔ Cf. Cours d'administration Windows de Mr. Marguos
3. Installer le serveur Debian.
   ➔ Cf. Fiche 1 du cours d'administration Unix Exercices

4. Configurer le serveur en IP statique
    a. On vérifie l'état de notre interface réseau
        i. **Ifconfig**

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:2c:e6:5f
          inet addr:192.168.0.45  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2c:e65f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:405 errors:0 dropped:0 overruns:0 frame:0
          TX packets:254 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:139914 (136.6 KiB)  TX bytes:29475 (28.7 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12949 (12.6 KiB)  TX bytes:12949 (12.6 KiB)
```

    b. On va modifier la configuration de la carte **eht0** qui nous intéresse ici dans le fichier **/etc/network/interfaces** afin de définir notre adresse IP statique.
        i. **vi /etc/network/interfaces**

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interfaces
allow-hotplug eth0
iface eth0 inet static
        address 192.168.0.45
        netmask 255.255.255.0
        gateway 192.168.0.1
        network 192.168.0.0
        broadcast 192.168.0.255
```

    c. On recharge la configuration de notre interface **eth0**.
        i. **Ifdown eth0**
        ii. **Iquery** (Vérification de nos paramètres modifiés)
        iii. **Ifup eth0**
    d. Vérifiez vos paramètres définis plus tôt
        i. **Ifconfig**
5. Il faut ensuite ajouter dans le fichier de résolution de nom notre serveur DNS (le serveur Windows Server 2016 sur lequel on a installé l'AD)
    a. On modifie pour cela le fichier **/etc/hosts**.
        i. **vi /etc/hosts**

Romain DESCAMPS · Quentin GILMART · Frédéric HUBERT · Thomas VAN GELDER · Robert WORONKO

```
127.0.0.1       localhost
127.0.1.1       debian.samba.royaume     debian
192.168.0.46    samba.royaume
192.168.0.46    VWS001.samba.royaume     VWS001
```

1. LE FQDN (Le Fully Qualified Domain Name) de notre server Debian
2. Le nom de notre domaine, ici samba.royaume, associé à l'adresse IP de notre serveur DNS
3. Le nom de domaine de notre serveur d'AD et DNS.

b. Pour tester la configuration il suffit de **Ping** vers le nom de domaine.

6. Entrer toutes les machines du domaine dans le fichier **/etc/hosts** est impossible, c'est pourquoi nous allons indiquer le serveur DNS de notre domaine.
   a. Il faut installer le package **resolvconf**.
      i. **apt-get install resolvconf**
   b. Une fois installé, on retourne dans notre fichier de configuration réseau **/etc/network/interfaces**.
      i. **vi /etc/network/interfaces**

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interfaces
allow-hotplug eth0
iface eth0 inet static
        address 192.168.0.45
        netmask 255.255.255.0
        gateway 192.168.0.1
        network 192.168.0.0
        broadcast 192.168.0.255
        dns-search samba.royaume
        dns-nameservers 192.168.0.46
```

7. Il est très important que notre serveur Debian soit à la même heure que notre serveur Wiindows Server 2016, en effet l'AD est très pointilleux sur l'heure système.
    a. Il faut installer le package **NTP** (Network Time Protocol)
        i. **apt-get install ntp**
    b. Il faut à présent configurer **ntpdate** en éditant le fichier **/etc/default/ntpdate**.
        i. **vi /etc/default/ntpdate**

```
# The settings in this file are used by the program ntpdate-debian, but not
# by the upstream program ntpdate.

# Set to "yes" to take the server list from /etc/ntp.conf, from package ntp,
# so you only have to keep it in one place.
NTPDATE_USE_NTP_CONF=no

# List of NTP servers to use  (Separate multiple servers with spaces.)
# Not used if NTPDATE_USE_NTP_CONF is yes.
NTPSERVERS="VWS001.samba.royaume"

# Additional options to pass to ntpdate
NTPOPTIONS="-u"
```

    c. On teste la synchronisation
        i. **/usr/sbin/ntpdate-debian**
    d. Pour éviter les dérives du temps, et donc une désynchronisation on va lancer des tâches planifiées qui vont lancer **ntpdate** à une certaine heure et aussi au démarrage de la machine.
        i. **Crontab -e**

```
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
# SYNCHRO NTP
18 1 * * * /usr/sbin/ntpdate-debian #synchronise l'horloge à 18h01 tous les jours
@reboot /usr/sbin/ntpdate-debian #lance la syncrhonisation au redémarrage
```

        1. *18 1 * * * /usr/sbin/ntpdate-debian #synchronise l'horloge à 18h01 tous les jours*
        2. *@reboot /usr/sbin/ntpdate-debian #lance la synchronisation au redémarrage*
    ii.

Romain DESCAMPS · Quentin GILMART · Frédéric HUBERT · Thomas VAN GELDER · Robert WORONKO

8. On va maintenant intégrer notre serveur Debian au domaine.
    a. Pour cela nous devons installer un package, **krb5-user**, qui va nous permettre d'utiliser le protocole **Kerberos**. Ce protocole est un protocole d'authentification réseau qui va permettre de s'authentifier sur le Windows Server 2016.
        i. **apt-get install krb5-user**
    b. Passons à la configuration de **Kerberos** pour pouvoir se connecter.
        i. **vi /etc/krb5.conf**

```
[libdefaults]
        ticket_lifetime = 24h
        renew_lifetime = 7d
        default_realm = SAMBA.ROYAUME
        forwardable = true
        proxiable = true
        dns_fallback = no
        dns_lookup_realm = false
        dns_lookup_kdc = false

[realms]
        SAMBA.ROYAUME = {
                kdc = VWS001.samba.royaume
                admin_server = VWS001.samba.royaume
        }

[domain_realm]
        .samba.royaume = SAMBA.ROYAUME
        samba.royaume = SAMBA.ROYAUME
```

    c. Testons notre configuration
        i. **kinit -V <Utilisateur Autorisé>@<NomNETBIOSDuDomaine>**

```
root@192:/home/thomas# kinit -V Administrator@SAMBA.ROYAUME
Using default cache: /tmp/krb5cc_0
Using principal: Administrator@SAMBA.ROYAUME
Password for Administrator@SAMBA.ROYAUME:
Authenticated to Kerberos v5
root@192:/home/thomas# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@SAMBA.ROYAUME

Valid starting       Expires              Service principal
12/09/2017 13:15:09  12/09/2017 23:15:09  krbtgt/SAMBA.ROYAUME@SAMBA.ROYAUME
        renew until 12/16/2017 13:15:04
```

    d. Pour continuer il vaut mieux détruire le ticket pour éviter les résidus.
        i. **Kdestroy**
9. Passons maintenant à la jonction au domaine avec SAMBA et WINBIND.
   WINBIND : Permet de se loguer sur la machine Linux avec des identifiants Windows.
    a. Il faut installer ces deux paquets :
        i. **apt-get install samba winbind**

b. Configurons Samba grâce au fichier de configuration **/etc/samba/smb.conf** :
   i. **vi /etc/samba/smb.conf**

```
[global]
        security = ADS
        encrypt passwords = yes
        realm = SAMBA.ROYAUME
        password server = VWS001.samba.royaume
        workgroup = SAMBA
        domain logons = no
        winbind separator = /
        idmap uid = 16777216-33554431
        idmap gid = 16777216-33554431
        winbind enum users = yes
        winbind enum groups = yes
        winbind use default domain = yes
        template homedir = /home/SAMBA/%D/%U
        template shell = /bin/bash
        client use spnego = yes
        # empêche le client de devenir maitre explorateur
        domain master = no
        local master = no
        preferred master = no
        os level = 0
        winbind offline logon = yes
        map to guest = bad user
        guest account = nobody
```

c. On teste nos paramètres :
   i. **testparm**

```
root@192:/home/thomas# testparm
Load smb config files from /etc/samba/smb.conf
WARNING: The "idmap uid" option is deprecated
WARNING: The "idmap gid" option is deprecated
Processing section "[partage]"
Processing section "[public]"
Loaded services file OK.
WARNING: The setting 'security=ads' should NOT be combined with the 'password server' parameter.
(by default Samba will discover the correct DC to contact automatically).

Server role: ROLE_DOMAIN_MEMBER
```

d. On redémarre Samba pour recharger la configuration :
   i. **service smb restart**

e. On se connecte à l'Active Directory depuis notre serveur Debian
   i. **net join ads -U <utilisateur autorisé> -S <FQDN du contrôleur de domaine>**

```
root@debian:/home/thomas# net join ads -U Administrator -S VWS001.samba.royaume
Enter Administrator's password:
Using short domain name -- SAMBA
Joined 'DEBIAN' to dns domain 'samba.royaume'
```

f. On redémarre **winbind** pour mettre à jour les sources d'authentifications
   i. **service winbind restart**

g. On teste si on arrive à récupérer les Users/Groups de l'AD

i. **wbinfo -u**

```
root@debian:/home/thomas# wbinfo -u
administrator
guest
defaultaccount
admin
krbtgt
student1
student2
student3
student4
student5
```

ii. **wbinfo -g**

```
root@debian:/home/thomas# wbinfo -g
domain computers
domain controllers
schema admins
enterprise admins
cert publishers
domain admins
domain users
domain guests
group policy creator owners
ras and ias servers
allowed rodc password replication group
denied rodc password replication group
read-only domain controllers
enterprise read-only domain controllers
cloneable domain controllers
protected users
key admins
enterprise key admins
dnsadmins
dnsupdateproxy
```

10. On configure l'authentification de compte Windows sur Linux.

a. On modifie le fichier **/etc/nsswitch.conf**.

i. **vi /etc /nsswitch.conf**

```
# /etc/nsswitch.conf

passwd:         compat winbind
group:          compat winbind
shadow:         compat
gshadow:        files

hosts:          files myhostname mdns4_minimal [NOTFOUND=return] dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

b. On teste la prise en compte des modifications

i. **getent passwd**

```
root@debian:/home/thomas# getent passwd
root:x:0:0:root:/root:/bin/bash
admin:*:16777219:16777216:Admin:/home/SAMBA/SAMBA/admin:/bin/bash
krbtgt:*:16777220:16777216:krbtgt:/home/SAMBA/SAMBA/krbtgt:/bin/bash
student1:*:16777221:16777216:student1:/home/SAMBA/SAMBA/student1:/bin/bash
student2:*:16777222:16777216:student2:/home/SAMBA/SAMBA/student2:/bin/bash
student3:*:16777223:16777216:student3:/home/SAMBA/SAMBA/student3:/bin/bash
student4:*:16777224:16777216:student4:/home/SAMBA/SAMBA/student4:/bin/bash
student5:*:16777225:16777216:student5:/home/SAMBA/SAMBA/student5:/bin/bash
```

ii. **getent group**

```
root@debian:/home/thomas# getent group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
domain computers:x:16777218:
domain controllers:x:16777219:
schema admins:x:16777220:
enterprise admins:x:16777221:
cert publishers:x:16777222:
domain admins:x:16777223:
domain users:x:16777216:
domain guests:x:16777217:
group policy creator owners:x:16777224:
ras and ias servers:x:16777225:
allowed rodc password replication group:x:16777226:
denied rodc password replication group:x:16777227:
read-only domain controllers:x:16777228:
enterprise read-only domain controllers:x:16777229:
cloneable domain controllers:x:16777230:
protected users:x:16777231:
key admins:x:16777232:
enterprise key admins:x:16777233:
dnsadmins:x:16777234:
dnsupdateproxy:x:16777235:_
```

c. Les utilisateurs et groupes sont bien ajoutés au système

d. Il faut ensuite activer le module PAM winbind dans la configuration de PAM, afin de permettre l'ouverture de session avec un utilisateur du domaine. On modifie le fichier **/etc/pam.d/common-account**

   i. vi /etc/pam.d/common-account

```
# here are the per-package modules (the "Primary" block)
account [success=2 new_authtok_reqd=done default=ignore]        pam_unix.so
account [success=1 new_authtok_reqd=done default=ignore]        pam_winbind.so
# here's the fallback if no module succeeds
account requisite       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
account required        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

   ii. vi /etc/pam.d/common-auth

```
# here are the per-package modules (the "Primary" block)
auth    [success=2 default=ignore]      pam_unix.so nullok_secure
auth    [success=1 default=ignore]      pam_winbind.so krb5_auth krb5_ccache_type=FILE cached_login try_first_pass
# here's the fallback if no module succeeds
auth    requisite       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

iii. vi /etc/pam.d/common-session

```
# here are the per-package modules (the "Primary" block)
session [default=1]                     pam_permit.so
# here's the fallback if no module succeeds
session requisite       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required        pam_permit.so
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session optional                        pam_winbind.so
session optional        pam_systemd.so

session required        pam_mkhomedir.so umask=0022 skel=/etc/skel
```

e. On crée le répertoire pour les données locales des utilisateurs du domaine.
   i. mkdir /home/<nom du domaine>
   ii. chmod 751 /home/<nom du domaine>

11. Il ne nous reste plus qu'à peaufiner la configuration de Samba pour que les utilisateurs retrouvent leur home directory sur /home/SAMBA/<nom utilisaeur>
    a. On modifie le fichier de configuration de samba
        i. vi /etc/samba/smb.conf

```
[home]
        comment = public folder of users
        path = /home/SAMBA/%D/%U
        valid users = @"domain users"
        read only = no
        writable = yes
        browseable = yes
        inherit acls = yes
        force create mode = 0660
        create mask = 700
        directory mask = 700
        access based share enum = yes
```

    b. On peut aussi créer un dossier ou tous les utilisateurs peuvent lire/écrire
        i. vi /etc/samba/smb.conf

```
[public]
        comment = Public
        path = /home/public
        public = yes
        guest ok = yes
        read only = no
        browseable = yes
        writable = yes
        printable = no
        create mode = 0777
        directory mode = 0777
```

    c. La configuration à faire pour chaque utilisateur dans l'AD