Correction TP Linux et AD

Phase 1 : Mise en œuvre du réseau

Dans mon cas tout est virtualisé avec VMware Workstation y compris le routeur NAT.

Voici le plan d'adressage retenu :

Routeur NAT :

- IP publique DHCP
- IP LAN1 : 10.10.10.1/24
- IP LAN2 : 20.20.20.1/24

Routeur LAN 2 LAN

- IP Externe : 10.10.10.2/24
- IP Interne : 192.168.10.254/24

Serveur GLPI :

- IP LAN : 192.168.10.3/24

Serveur de fichiers

- IP LAN : 192.168.10.2/24

Serveur de domaine Active Directory

- IP LAN : 192.168.10.1/24

ROUTEUR NAT

Ce routeur NAT dispose de 3 interfaces :

Eth0 : Bridged

Eth1 : VMnet1

Eth2 : VMnet2

Voici la configuration :

```
# The primary network interface
allow-hotplug eth0
auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
address 10.10.10.1
netmask 255.255.255.0
```

```
auto eth2
iface eth2 inet static
address 20.20.20.1
netmask 255.255.255.0

# Cette ligne permet de restaurer les règles iptables
post-up iptables-restore < /etc/iptsave

# Ces lignes ajoutent les routes vers les réseaux LAN
post-up route add –net 192.168.10.0 netmask 255.255.255.0 gw 10.10.10.2 dev eth1
post-up route add –net 192.168.20.0 netmask 255.255.255.0 gw 20.20.20.2 dev eth2
```

Installer le service serveur DHCP (dhcp3-server) puis le configurer correctement :

```
default-lease-time 600;
max-lease-time 7200;

#Etendue Subnet 10.10.10.0
subnet 10.10.10.0 netmask 255.255.255.0 {
range 10.10.10.5 10.10.10.10;
}

#Etendue Subnet 20.20.20.0
subnet 20.20.20.0 netmask 255.255.255.0 {
range 20.20.20.5 20.20.20.20;
}

#Etendue Subnet 192.168.10.0
subnet 192.168.10.0 netmask 255.255.255.0 {
range 192.168.10.5 192.168.10.250;
option routers 192.168.10.254;
option domain-name-servers 192.168.10.1;
option domain-name "lejeune.dom";
}

#Etendue Subnet 192.168.20.0
subnet 192.168.20.0 netmask 255.255.255.0 {
range 192.168.20.5 192.168.20.250;
}
```

Il faut ensuite activer le routage :

```
echo "1" > /proc/sys/net/ipv4/ip_forward

echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
```

Puis ajouter la règle NAT :

```
iptables –t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Et ajouter le transfert de port vers GLPI :

```
iptables –t nat -A PREROUTING -i eth0 -p tcp -m tcp --dport 8076 -j
DNAT --to-destination 192.168.10.3:80
```

On enregistre la configuration :

```
iptables-save > /etc/iptsave
```

ROUTEUR LAN 2 LAN

Eth0 : VMnet1

Eth1 : VMnet3

Il faut commencer par activer la fonction de routage

```
echo "1" > /proc/sys/net/ipv4/ip_forward

echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
```

Puis modifier les configurations des interfaces

```
# The primary network interface
allow-hotplug eth0
auto eth0
iface eth0 inet static
address 10.10.10.2
netmask 255.255.255.0
gateway 10.10.10.1

# The secondary network interface
allow-hotplug eth1
auto eth1
iface eth1 inet static
address 192.168.10.254
netmask 255.255.255.0
```

Configurer l'agent de relais dhcp (dhcp3-relay) :

```
# What servers should the DHCP relay forward requests to?
SERVERS="10.10.10.1"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP
requests?
INTERFACES=""

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
```

Serveur GLPI

Ajouter les lignes suivantes dans le fichier `/etc/apt/sources.list`

```
deb http://ftp.fr.debian.org/debian/ wheezy main non-free contrib
deb-src http://ftp.fr.debian.org/debian/ wheezy main non-free contrib
# La ligne ci-dessous sera utile pour l'installation de l'agent fusion
deb http://backports.debian.org/debian-backports squeeze-backports main
```

Faire un `apt-get update` puis installer les paquets suivants :

```
apache2, php5, mysql-server, php5-mysql, libapache2-mod-php5,
libwww-perl, php5-ldap
```

Récupérer le fichier d'installation de GLPI, puis l'extraire vers `/var/www`

Changer les droits et propriétaire du dossier glpi

```
chmod –R 755 /var/www/glpi
```

```
chown –R www-data:www-data /var/www/glpi
```

Procéder à l'installation de GLPI depuis un navigateur

Vu que le paquet php5-ldap est installé, il est désormais possible de configurer l'authentification ldap.

Installation du plugins fusion inventory

Récupérer le fichier de plugin fusion-inventory et procéder à son installation.

Il est alors possible de procéder à l'installation de l'agent fusion sur ce serveur :

```
apt-get install –t squeeze-backports fusioninventory-agent
```

Puis :

```
echo "server = http://URL DU GLPI/plugins/fusioninventory/" >>
/etc/fusioninventory/agent.cfg
```

et enfin :

```
fusioninventory-agent
```

Ces quelques opérations seront à répéter sur chaque machine linux.

Serveur de fichiers

Ajouter un disque dur dédié aux partage,

Créer la partition en `ext4` via l'utilitaire `cfdisk`

Créer un dossier "`partage`" à la racine du système.

Editer le fichier `/etc/fstab` et y ajouter la ligne correspondant au disque ajouté et son point de montage :

```
/dev/sdb1  /partage   auto
```

Installation des outils serveur de fichiers

Je ne corrige pas la mise en œuvre du serveur Active Directory, toutefois, voici quelques éléments à prendre en compte :

Nom de domaine FQDN : seine.dom

Nom de domaine netbios : SEINE

OU et groupes :

- Base
  - Info
    - Groupe g-info
  - Production
    - Groupe g-prod
  - Compta
    - Groupe g-compta
  - Market
    - Groupe g-market

Il faut commencer par installer les paquets suivants :

```
krb5-config,krb5-user,krb5-doc,winbind,samba,ntp,dnsutils
```

Puis mettre à jour la date du serveur avec la commande date

```
date mmjjhhmm
```

Editer puis modifier `/etc/ntp.conf`

Et remplacer les lignes

```
server 0.debian.pool.ntp.org iburst
server 1.debian.pool.ntp.org iburst
server 2.debian.pool.ntp.org iburst
server 3.debian.pool.ntp.org iburst
```

par

```
server 0.fr.pool.ntp.org iburst dynamic
server 1.fr.pool.ntp.org iburst dynamic
server 2.fr.pool.ntp.org iburst dynamic
server 3.fr.pool.ntp.org iburst dynamic
```

et redémarrer le service ntp.

Tests de connectivité

Commencer par tester la connexion dns au domaine :

```
nslookup seine.dom
```

qui retourne dans mon cas :

```
Server:    192.168.10.1
Address:   192.168.10.1#53

Name:      seine.dom
Address:   192.168.10.1
```

Puis faire un `ping seine.dom` et `nomduserver2008.seine.dom` qui doivent tout deux retourner l'adresse 192.168.10.1 (dans mon cas)

Puis renseigner le nom du serveur linux souhaité dans le fichier `/etc/hostname`

```
files
```

Ensuite, il faut modifier le fichier /etc/hosts comme suit

```
127.0.0.1  files.seine.dom
127.0.1.1  files.seine.dom      files
```

Et redémarrer le serveur.

Editer le fichier `/etc/krb5.conf` puis modifier/ajouter les lignes suivantes

Dans la section `libdefaults` modifiez la valeur `default_realm` :

```
        default_realm = seine.dom
```

Dans la section realms ajouter

```
        SEINE.DOM = {
                kdc = SRV2K8.SEINE.DOM
                admin_server = SRV2K8.SEINE.DOM
                default_domain = SEINE.DOM
                }
```

Dans `domain_realm` ajouter à la fin de la section

```
        .SEINE.DOM=SEINE.DOM
```

Tester la connexion à l'AD

```
kinit administrateur@SEINE.DOM
```

puis

```
klist
```

Cette commande doit retourner quelque chose dans ce genre :

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrateur@SEINE.DOM

Valid starting       Expires              Service principal
21/03/2013 16:48:05  22/03/2014 02:48:46
krbtgt/SEINE.DOM@SEINE.DOM
        renew until 22/03/2014 02:48:05
```

Si ce n'est pas le cas, revérifier le fichier krb5.conf et/ou rebooter le serveur

Modifier le fichier `/etc/samba/smb.conf` en fonction de vos besoins : (en gras les valeurs à modifier)

```
[global]

workgroup = SEINE
realm = SEINE.DOM
load printers = no
preferred master = no
local master = no
server string = fileserver
password server = 192.168.10.1
encrypt passwords = yes
security = ADS
netbios name = files
client signing = Yes
dns proxy = No
wins server = 192.168.10.1
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind separator = +
winbind enum users = Yes
winbind enum groups = Yes
winbind use default domain = Yes
```

Attention, vérifier que certaines de ses options n'apparaissent pas en double avec des valeurs différentes dans votre fichier smb.conf (surtout la ligne Workgroup=)

Redémarrer le service samba

Intégrer le serveur Linux au domaine :

```
net ads join -U administrateur
```

Lister les utilisateurs et groupes du domaine AD :

```
wbinfo -u (pour les utilisateurs)
wbinfo - g (pour les groupes)
```

Si cela n'affiche pas les utilisateurs et groupes du domaine, rebooter le serveur.

Modifier le fichier `/etc/nsswitch.conf` comme suit :

```
passwd:     compat winbind
shadow:     compat winbind
group:      compat winbind
```

Créer un partage accessible au groupe utilisateurs du domaine (Active Directory)

Créer les dossiers suivants :

```
/partage/commun
/partage/market
/partage/compta
/partage/info
/partage/prod
```

Sur chaque dossier, ajouter les droits d'écriture pour le groupe puis modifier le groupe pour que groupe active directory :

```
drwxrwx--- 3root   utilisateurs du domaine   4096   dec.   18     12:00  commun
drwxrwx--- 3root   g-market                  4096   dec.   18     12:00  market
drwxrwx--- 3root   g-compta                  4096   dec.   18     12:00  compta
drwxrwx--- 3root   g-info                    4096   dec.   18     12:00  info
drwxrwx--- 3root   g-prod                    4096   dec.   18     12:00  prod
```

Dans le fichier `/etc/samba/smb.conf` ajouter la section suivante :

```
[commun]
path = /partage/commun
valid users = @"utilisateurs du domaine"
browseable = yes
writeable = yes

[market]
path = /partage/market
valid users = @"g-market"
browseable = yes
writeable = yes

[compta]
```

```
path = /partage/compta
valid users = @"g-compta"
browseable = yes
writeable = yes

[info]
path = /partage/info
valid users = @"g-info"
browseable = yes
writeable = yes

[prod]
path = /partage/prod
valid users = @"g-prod"
browseable = yes
writeable = yes
```

Enregistrer puis quitter le fichier, redémarrer le service Samba.

Accès depuis un compte AD sur le client du domaine fonctionnant sous Windows.