

Administration d'un réseau informatique sous Linux

I- Fichiers de paramétrage et scripts :

- */etc/hosts* :

Ce fichier contient toutes les adresses IP connues de l'ordinateur local. Il permet de résoudre la correspondance entre les noms des ordinateurs et leurs adresses IP.

Exemple :

```
# /etc/hosts
# IP          Ordinateur          Alias
127.0.0.1     localhost.localdomain localhost
```

- */etc/networks* :

Ce fichier permet de résoudre la correspondance entre les noms des réseaux et les adresses réseau.

Exemple :

```
# /etc/networks
0.0.0.0        default
127.0.0.0      loopback
169.254.0.0    link-local
192.168.1.0    2tri.lan
```

- */etc/host.conf* :

Ce fichier contient des paramètres nécessaires pour le pilotage de la bibliothèque de résolution des noms (Resolver).

Exemple :

```
# /etc/host.conf
order  hosts, bind
multi  on
```

- */etc/resolv.conf* :

Ce fichier joue également un rôle très important dans la configuration de la bibliothèque Resolver. Si ce fichier est présent, c'est le serveur de noms qui apparaît en premier qui est interrogé.

Exemple :

```
# /etc/resolv.conf
search 2tri.lan
# Adresse du serveur de noms
nameserver 192.168.1.254
```

- */etc/sysconfig/network* :

Le fichier */etc/sysconfig/network* précise les informations de routage et le nom de l'hôte pour toutes les interfaces réseau.

Exemple :

```
NETWORKING=yes
HOSTNAME=Serv1.2tri.lan
GATEWAY=192.168.1.254
```

- */etc/rc.d/init.d/network* :

Le script */etc/rc.d/init.d/network* est responsable de l'initialisation de toutes les interfaces réseau aussi bien au démarrage du poste de travail que via la commande :

```
service network [start|stop|status]
```

- Les fichiers de répertoire */etc/sysconfig/network-script* :

Le répertoire */etc/sysconfig/network-script* contient normalement les fichiers suivants (des scripts) :

- */etc/sysconfig/network-script/ifup*
- */etc/sysconfig/network-script/ifdown*
- */etc/sysconfig/network-script/ifcfg-NomInterface*
- */etc/sysconfig/network-script/ifcfg-NomInterface-NomClone*
- */etc/sysconfig/network-script/ifcfg-NomInterface:NomAlias*

Les scripts *ifup* et *ifdown* reçoivent en paramètre le nom de l'interface à activer ou à désactiver.

```
ifup      NomInterface
ifdown    NomInterface
```

Le fichier *ifcfg-NomInterface* est un fichier de paramétrage d'interface spécifie les paramètres qui sont requis pour l'initialisation de chacun des interfaces réseau.

Exemple de fichier : */etc/sysconfig/network-script/ifcfg-eth0* :

```
# Intel Corporation 8254EM Gigabit Ethernet Controller
DEVICE=eth0                ; nom de l'interface
HWADDR=08:00:27:32:b1:ba   ; Adresse MAC de l'interface
BOOTPROTO=dhcp             ; dhcp: Attribution dynamique / none : Attribution statique
ONBOOT=yes                 ; Activation de l'interface au démarrage de la machine
IPADDR=192.168.1.254        ; Adresse IP statique
NETMASK=255.255.255.0      ; Masque de sous réseau
PREFIX=24                   ; le préfixe du masque
DNS1=192.168.1.254         ; l'adresse IP du serveur DNS
```

Pour l'interface loopback on écrit :

```
ifcfg-lo
```

Le fichier *ifcfg-NomInterface-NomClone* permet de spécifier des options complémentaires pour une interface.

Exemple de fichier : */etc/sysconfig/network-script/ifcfg-eth0-user* :

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
USERCTL=yes
```

Le fichier *ifcfg-NomInterface:NomAlias* permet de définir plusieurs adresses IP pour une même interface.

Exemple de fichier : */etc/sysconfig/network-script/ifcfg-eth0:0* :

```
DEVICE=eth0
BOOTPROTO=none
IPADDR=192.168.1.254
NETMASK=255.255.255.0
ONBOOT=yes
```

II- Configuration des cartes réseaux :

Pour paramétrer des interfaces réseau, on utilise la commande *ifconfig*. Elle permet de paramétrer une interface réseau où :

- Interface : est le nom de l'interface;
 - Adresse : est l'adresse IP associée à cette interface;
 - Addr : est le masque de réseau.
- ```
ifconfig 'interface' 'adresse' netmask 'addr' -gw 'Passerelle'
```

Exemple:

```
ifconfig eth0 192.168.1.254 netmask 255.255.255.0
```

Pour afficher les paramètres réseau utiliser la commande *ifconfig* comme ceci :

```
ifconfig -a
```

Ou la commande *netstat* :

```
netstat -i
```

La commande *ifconfig* permet aussi d'activer et de désactiver une interface réseau :

```
ifconfig interface [down|up]
```

Maintenant que votre interface *loopback* est paramétrée il suffit de vérifier son fonctionnement avec la commande *ping* :

```
ping 127.0.0.1
```

Après tout ça, vous devez redémarrer les services réseau :

```
service network restart
service NetworkManager restart
```

### III- Configuration des services : *(avant toutes les configurations essayez de désactiver les pare feu)*

**A. DHCP :** « Dynamic Host Configuration protocol » c'est un protocole qui permet la configuration des hôtes automatiquement. Il fonctionne avec UDP/67 pour le serveur et UDP/68 pour le client.

1- Vérifier que le package contenant dhcpd (dhcp-xxx.rpm) est installé:

```
Rpm -qa | grep dhcp
Ou installer les packages :
Rpm -ivh dhcp-xxx.rpm
```

2- Configuration globale du fichier `/etc/dhcp/dhcpd.conf` :

```
Nom de domaine
option domain-name "2tri.lan";
Serveur DNS
option domain-name-servers 192.168.1.254;
La durée de bail
default-lease-time 21600;
max-lease-time 43200;
#Activer ou désactiver les mises à jour dynamiques
ddns-update-style none/interim/ad-hoc;
L'étendue (l'adresse réseau et le masque)
subnet 192.168.1.0 netmask 255.255.255.0 {
La plage d'adresses qui sera attribué dynamiquement par le serveur DHCP
range 192.168.1.10 192.168.1.100;
Passerelle par défaut
option routers 192.168.1.1;
Nom de domaine
option domain-name "2tri.lan";
Serveur DNS
option domain-name-servers 192.168.1.254;
option broadcast-address 192.168.1.255 ;
La durée de bail
default-lease-time 21600;
max-lease-time 43200;
}

Attribution statique « Réservation » :
host poste1 {
Adresse MAC du poste1
hardware ethernet 00:48:54:6E:4F:31;
Adresse IP qui sera attribué au serveur 1
fixed-address 192.168.1.33;
}
```

3- Gérer le service DHCP :

```
service dhcp [start|restart|status|stop]
```

4- Afficher les baux attribués à partir du serveur DHCP: `# cat /var/lib/dhcpd/dhcpd.leases`

**B. DNS (BIND) :** « Berkeley Internet Name Daemon » c'est une base de données hiérarchique qui contient les mappages des FDQN et leurs adresses IP, il permet de transférer les noms d'hôtes en des adresses IP (c'est la principale méthode). Il fonctionne avec TCP et UDP avec un numéro de port 53.

1- Installer les packages nécessaires :

```
- verifier l' installation des packages :
rpm -qa | grep bind
```

Sinon installez bind :  
# rpm -ivh bind-xxxx.

## 2- Configuration globale du fichier */etc/named.conf* :

```
vim /etc/named.conf
options {
 listen-on port 53 { 127.0.0.1;192.168.1.254; }; # le port et l' Adresse des serveurs a contacter
 directory "/var/named" # le dossier qui contient les fichiers des zones
 allow-query { localhost;192.168.1.0/24; }; # l'adresse réseau des clients DNS
};
zone "2tri.lan" IN { # Déclaration d'une zone directe
 type master; # Type de zone (master=principale ; slave=secondaire)
 file "2tri.lan.zone"; # Fichier de la zone
};
zone "1.168.192.in-addr.arpa" IN { # Déclaration d'une zone inversée
 type master; # Type de zone (master=principale ; slave=secondaire)
 file "2tri.lan.rev"; # Fichier de la zone
}
```

## 3- Configuration des fichiers des zones :

### • Fichier de zone directe :

```
Durée de vie maximale
$TTL 86400
Déclaration de l'enregistrement SOA (Start Of Authority)
@ IN SOA Serv1.2tri.lan. root.2tri.lan. (
 2000101500 ; numéro de série
 28800 ; rafraîchissement toutes les 8 heures
 14400 ; nouvel essai toutes les 4 heures
 604800 ; expiration dans 7 jours
 86400) ; temps de vie minimal 24 heures
Déclaration de l'enregistrement NS (NameServer)
IN NS Serv1.2tri.lan.
Déclaration de l'enregistrement A (Host) : Les mappages des noms d'hôte et leurs adresses IP
Serv1 IN A 192.168.1.254
Client1 IN A 192.168.1.33
Déclaration de l'enregistrement MX (Mail eXchange) : serveur de messagerie
@ IN MX 10 mail.2tri.lan.
mail IN CNAME Serv1.2tri.lan.
```

### • Fichier de zone inversée :

```
Durée de vie maximale
$TTL 86400
Déclaration de l'enregistrement SOA (Start Of Authority)
@ IN SOA Serv1.2tri.lan. root.2tri.lan. (
 2000101500 ; numéro de série
 28800 ; rafraîchissement toutes les 8 heures
 14400 ; nouvel essai toutes les 4 heures
 604800 ; expiration dans 7 jours
 86400) ; temps de vie minimal 24 heures
Déclaration de l'enregistrement NS (NameServer)
IN NS Serv1.2tri.lan.
Déclaration de l'enregistrement PTR (Pointer)
254 IN PTR Serv1.2tri.lan.
33 IN PTR Client1.2tri.lan.
```

4- Configuration de fichier /etc/resolv.conf  
 search 2tri.lan  
 nameserver 192.168.1.254

5- Gérer le service DNS :

# service named [start|restart|status|stop]

6- Vérifier, sous les machines serveurs et clients, avec la commande (Utilitaire) “nslookup”.

**C. FTP :** « File Transfer Protocol » C’est un protocole qui permet de partager des ressources (dossier et fichier). Il fonctionne avec TCP/21.

1- Installer le package FTP :

# rpm -ivh ftp-xxxx.rpm

2- Configuration du fichier /etc/vsftp/vsftp.conf :

|                                |                                                            |
|--------------------------------|------------------------------------------------------------|
| Anonymous_enable=YES/NO        | # Activer ou désactiver les connexions anonymes            |
| Local_enable=YES/NO            | # Activer ou non l'utilisation des listes des utilisateurs |
| Write_enable=YES/NO            | # Activer ou non l'option d'écriture                       |
| Local_umask=022                | # Définir les droits d'accès                               |
| Dirmessage=YES/NO              | # Accéder certain dossier                                  |
| Xferlog_std_format=YES/NO      | # Activer ou non les fichiers log                          |
| Connect_from_port_20=YES/NO    | # Activer ou non le port 20                                |
| anon_mkdir_write_enable=YES/NO | # Activer ou non la création des dossiers                  |
| Ftpd_banner=Bienvenue ...      | # message de bienvenue                                     |

3- Gérer le service FTP :

# service vsftpd [start|restart|status]

4- Vérifier sur la machine client comme suit : Ouvrir la machine → Ouvrir le navigateur « Internet Explorer » → taper « ftp ://192.168.1.254 » (vous devez trouver un dossier partagé pour tous les utilisateurs FTP, il est partagé par le serveur FTP)

**D. SAMBA :** permet de partager les ressources ‘imprimante, scanner, ... ) dans les systèmes Linux/Windows, utilise le protocole SMB (Server Message Block). Le protocole SMB fonctionne avec UDP/445.

1- Installation des packages :

rpm -ivh samba-xxxx

2- Configuration du fichier /etc/samba/smb.conf :

#-----Configuration globale-----

[global]

|                              |                                                  |
|------------------------------|--------------------------------------------------|
| workgroup = 2tri             | #Le nom du groupe                                |
| server string = samba server | # Le serveur SAMBA                               |
| hosts allow = 192.168.1.     | # La partie réseau                               |
| security = user              | # Méthode d'authentification (user/domain/share) |

#-----Dossier partagé-----

[partage1]

|                                |                                              |
|--------------------------------|----------------------------------------------|
| comment = Répertoire partagé 1 | # Commentaire                                |
| path = /opt/partage1           | # Le chemin du fichier partagé               |
| browseable = yes/no            | # Activer ou non l'option parcourir          |
| public = yes/no                | # Activer ou non le partage en mode publique |
| writable = yes/no              | # Activer ou non l'option d'écriture         |
| printable = yes/no             | # Activer ou non l'impression du partage     |
| group = partage                | # Le groupe du partage                       |

#-----Imprimante partagée-----

**[Printer]**

|                                |                                                                |
|--------------------------------|----------------------------------------------------------------|
| comment = Laserjet 2100        | <i># Commentaire</i>                                           |
| printer = lj2100               | <i># Nom de l'imprimante partagée</i>                          |
| valid users = riri fifi loulou | <i># les utilisateurs valides à utiliser cette imprimante.</i> |
| path = /var/spool/lj2100       | <i># Le chemin du fichier partagé</i>                          |
| public = no/yes                | <i># Activer ou non le partage en mode publique</i>            |
| writable = no/yes              | <i># Activer ou non l'option d'écriture</i>                    |
| printable = yes/no             | <i># Activer ou non l'impression du partage</i>                |
| browseable = yes/no            | <i># Activer ou non l'option parcourir</i>                     |

- 3- Créer un utilisateur :  
 useradd samba-1  
 smbpasswd -a samba-1
  - 4- Gérer le service SAMBA :  
 Service smb [start|restart|status]
  - 5- Vérifier sur la machine client : ouvrir la session avec l'utilisateur que vous avez créé précédemment. Puis accéder le serveur SAMBA (Exécuter → \\192.168.100.1), vous devez trouver les fichiers de SAMBA.
- E. NFS :** est un protocole qui permet de partager ou accéder des fichiers dans les réseaux IP sur les systèmes Linux/Unix. Il fonctionne avec UDP/2049.

- 1- Installation du package :  
 rpm -ivh nfs-xxxx  
 rpm -ivh portmap-xxxx
- 2- Configuration du fichier
  - a- Créer un répertoire « 2tri »  
 mkdir /root/2tri  
 chmod 777 /root/2tri
  - b- Configurer le fichier */etc/exports*  
 /root/2tri \*(rw)      *# \* ou l'adresse IP des utilisateurs qui peuvent accéder le dossier partagé, (rw) activer la lecture et écriture.*
- 3- Gérer le service NFS :  
 service nfs [start|restart|status]  
 service portmap [start|restart|status]
- 4- Configuration de la machine Client :  
 Démarrer le service portmap :  
 # service portmap restart  
  
 Créer un dossier de partage :  
 # mkdir /root/partage1  
 # monter le dossier « 2tri », déjà créé dans le serveur NFS, vers le dossier « partage1 » :  
 mount -t nfs 192.168.1.254:/root/2tri /root/partage1
- 5- Vérifier avec la création des fichiers, sous le serveur NFS, dans le répertoire « 2tri » puis accéder ces fichiers à partir de la machine client. (ls /root/partage1).

**F. TELNET :** (TERminal NETwork ou TELecommunication NETwork), il fonctionne avec 23/tcp, il permet de créer ou d'accéder une session Telnet sur une machine distante.

- 1- Installation du package :  
 # rpm -ivh xinetd-xxxx  
 # rpm -ivh telnet-xxxx

**2- Configuration du fichier */etc/xinetd.d/telnet* :**

```

service telnet
{
 disable = no # Activer le service telnet
 port = 23 # Préciser le numéro de port telnet
 user = root # Super utilisateur
 socket_type = stream # Type de session
 wait = no/yes # Avec ou pas d'attente
 log_on_failure = USERID # Enregistrer l'ID de l'utilisateur lors de l'authentification échouée
}

```

**3- Créer un utilisateur :**

```

useradd client-telnet
passwd client-telnet

```

**4- Gérer le service TELNET :**

```

service xinetd start

```

**5- Au niveau client : (sous l'invite de commande)**

```

>telnet
>open
>'@_IP_du_serveur
>login+password_of_client

```

**G. OpenSSH :**

SSH (Secure SHell), il fonctionne avec TCP/22, c'est un protocole de communication sécurisé, ainsi qu'il permet d'ouvrir une session à distance mais plus sécurisé que Telnet.

**1- Installation du package :**

```

rpm -ivh openssh-xxxx
rpm -ivh openssh-server-xxxx

```

**2- Configuration du fichier */etc/ssh/sshd\_config* :**

```

Port 22 # Numéro de port SSH
Protocole 2 # Numéro de port SSH
ListenAddress '@_du_serveur # Adresse IP du serveur SSH
PermitRootLogin yes # Autorise les connexions de root

```

**3- Gérer le service SSH :**

```

service sshd restart

```

**4- sur la machine client on démarre le logiciel 'Putty', puis on va faire ça :**

```

Host name = @_IP_du_serveur
root + mot de passe de root

```

**H. OpenLDAP :**

OpenLDAP est un annuaire informatique qui fonctionne sur le modèle client/serveur (Comme AD sous windows), c'est une implémentation libre du protocole LDAP (LDAP = Lightweight Directory Access Protocol), il fonctionne avec 389/tcp.

#####Au niveau du serveur#####

**I- Installation et configuration de DNS :****1- Installation des packages :**

```

rpm -ivh --replacepkgs bind-9...
rpm -ivh --replacepkgs bind-chroot....

```

**2- Configuration du fichier */etc/named.conf***

```

-Création des zones : Zone directe et Zone inversé
-Configuration des fichiers des zones

```

3- Configuration de fichier */etc/resolv.conf*

```
search 2tri.lan
nameserver 192.168.1.254
```

## 4- Démarrage de service BIND

```
service named restart
```

## II- Installation des packages nécessaires pour LDAP :

```
rpm -ivh ...
•Openldap-...
•Openldap-servers-...
•Openldap-clients-...
•Openldap-devel-...
•Cyrus-...
```

## III- Fixer un mot de passe pour le root LDAP

```
slappasswd
copier : « {SSHA}.... »
```

IV- Editer le fichier */etc/openldap/slapd.conf*

```
suffix "dc=2tri, dc=lan"
rootdn "cn=manager,dc=2tri,dc=lan"
rootpw (Coller "{SSHA}...")
```

---

## V- Démarrer le service ldap

```
service slapd start
```

## VI- Créer des utilisateurs (les informations des utilisateurs sont stocké dans un fichier .ldif :

```
useradd user1
passwd user1
grep user1 /etc/passwd
user1:x:501:501::/home/user1:/bin/bash
grep user1 /etc/passwd > users.passwd
```

VII- Utilisation du fichier *"/usr/share/openldap/migration/migrate\_passwd.pl"* :

```
/usr/share/openldap/migration/migrate_passwd.pl users.passwd users.ldif
```

On va changer le nom du domaine sur le fichier *users.ldif* :

```
dn: uid=user1,ou=People,dc=2tri,dc=lan
uid: user1
cn: user1
ObjectClass: ...
```

## VIII- Créer un autre fichier .ldif qui contient le domaine et les unités d'organisation :

```
dn: dc=2tri,dc=lan
dc: 2tri
objectClass: dcObject
objectClass: organizationalUnit
ou: rootobject

dn: ou=People,dc=2tri,dc=lan
ou: People
description: utilisateurs
objectClass: organizationalUnit
```

## IX- Ajouter les informations sous les fichiers .ldif à la base de données LDAP

```
ldapadd -xW -D "cn=Manager,dc=2tri,dc=lan" -f 2tri.lan.ldif
Entrer la mot de passe de ldap
```



```
ldapadd -xW -D "cn=Manager,dc=2tri,dc=lan" -f users.ldif
Entrer la mot de passe de ldap
```

X- Partager /home avec tous les utilisateurs clients on utilisant NFS :  
/home 192.168.1.0/24(rw,sync)

Taper la commande d'exportation :  
exportfs -a

XI- Démarrer les services nfs et portmap :  
# service portmap start  
# service nfs start  
# chkconfig portmap on  
# chkconfig nfs on  
→chkconfig permet de gérer les services (commande d'admin).

#####Au niveau du client#####

I- Installation des packages nécessaires pour LDAP :

```
rpm -ivh ...
•Openldap-...
•Openldap-clients-...
•Openldap-devel-...
```

II- Renommer le /home par /home.local (on va monter le /home du serveur donc il faut séparer les 2 homes)

```
mv /home /home.local
```

III- Créer un nouveau /home :

```
mkdir /home
```

IV- monter le home partagé :

```
mount 192.168.1.254:/home /home
```

V- Activer ldap : (on va rendre la machine membre au domaine)

```
authconfig --enableldap --enableldapauth --ldapserver=192.168.1.254 --
ldapbasedn="dc=2tri,dc=lan" --enablemd5 --enabeshadow
(MD5 est un algorithme de cryptage)
```

« On va obtenir une fenêtre bleue de configuration de l'authentification (dans cette fenêtre on va cocher : Utiliser LDAP + Utiliser les mots de passe MD5 + Utiliser les mots de passe masqués + Utiliser l'authentification LDAP + suivant + ok »

VI- Redémarrer la machine et ouvrir la session avec l'utilisateur user1 qu'on déjà créer sur le serveur.