



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

VII. ajiConfiguration des services sous linux :

Linux est un *système d'exploitation* , un logiciel important qui contrôle un ordinateur. Il est semblable à Microsoft Windows, mais il est entièrement libre. Son vrai nom est *GNU/Linux* , mais "Linux" est utilisé plus souvent.

Linux n'est pas le produit d'une seule société, mais de nombreuses sociétés et groupes de personnes qui y contribuent.

1. DNS :

a. Présentation DNS :

DNS (Domain Name System) est un service de noms statique et hiérarchisé. Il est très lié à Internet. Son rôle consiste à faire correspondre des adresses IP à des noms d'ordinateurs. Ceci permet à l'utilisateur d'utiliser le nom de l'ordinateur dans une commande plutôt que son adresse IP difficile à retenir. Le système de noms est conçu de telle manière que la mémorisation des noms des ordinateurs est facile.

B. DNS :

Après avoir installé *bind* et *named* , il est possible d'attribuer le nom de domaine *poste.ma* en éditant le fichier */etc/named.conf* comme suivant :



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

```
zone "poste.ma" IN {
    type master;
    file "poste.ma.zone";
};

zone "0.13.10.in-addr.arpa" IN {
    type master;
    file "poste.ma.rev";
};
```

Ici on a crée la zone de recherche directe

Et la zone inversée poste.ma.rev

Sur le chemin /var/named on crée le fichier de la zone poste.ma.zone

Et le fichier de zone poste.ma.rev

◆ Le fichier /var/named/Poste.ma.zone

Le paramètre @, signifie qu'il s'agit du domaine 'Poste.ma'. Le paramètre 'IN', signifie qu'il s'agit d'un enregistrement de type Internet.

```
@                IN SOA  server.poste.ma.    root.poste.ma. (
                                42          ; serial (d. adams)
                                3H          ; refresh
                                15M         ; retry
                                1W          ; expiry
                                1D )        ; minimum

server.poste.ma.  IN NS   server.poste.ma.
server.poste.ma. IN NS   10.13.0.2
postel            IN A    10.13.0.55
formation        IN A    10.13.0.34
```

Le contenu de fichier de zone : poste.ma

◆ Le fichier /var/named/Poste.ma.rev



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

Il s'agit de la résolution de nom inverse de la zone **poste.ma**

```
$TTL      86400
@         IN SOA  server.poste.ma.  root.poste.ma. (
                        42          ; serial (d. adams)
                        3H          ; refresh
                        15M         ; retry
                        1W          ; expiry
                        1D )        ; minimum

                IN NS      server.poste.ma.
2              IN PTR     server.poste.ma.
34             IN PTR     formateur
```

Le contenu de
fichier
de zone : poste.ma
.rev

- ◆ Après l'enregistrement de cette modification en redémarre le service réseau avec la commande :
 - **Service network start**
- ◆ En suit on démarre le service named
 - **Service named start**
- ◆ Puis en doit teste on utilisant l'utilitaire:
 - **Nslookup**

```
[root@server named]# nslookup
> 10.13.0.2
Server:          10.13.0.2
Address:         10.13.0.2#53

2.0.13.10.in-addr.arpa  name = server.poste.ma.0.13.10.in-addr.arpa.
```

2. DHCP



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

DHCP (Dynamic Host Configuration Protocol) est un protocole permettant de configurer automatiquement la partie réseau des machines clientes. Il permet de donner une adresse IP à un ordinateur, lui indique l'adresse IP de la passerelle, celles des DNS, etc.

Configuration dhcp :

Avec ces paramètres, la configuration de base suivante est obtenue (contenu du fichier dhcpd.conf) :

```
subnet 10.13.0.0 netmask 255.255.255.0 {  
# --- default gateway  
    option routers          10.13.0.1;  
    option subnet-mask     255.255.255.0;  
    option domain-name     "poste.ma";  
    option domain-name-servers 10.13.0.2;  
  
    option time-offset     -18000; # Eastern Standard Time  
#    option ntp-servers    192.168.1.1;  
#    option netbios-name-servers 192.168.1.1;  
# --- Selects point-to-point node (default is hybrid). Don't change this unless  
# -- you understand Netbios very well  
#    option netbios-node-type 2;  
  
    range dynamic-bootp 10.13.0.2 10.13.0.30;
```

Une fois le service DHCP est installé et configuré, vous pouvez démarrer le service DHCP en lançant la commande :

```
[root]# /etc/init.d/dhcp start
```

coté client :

Pour configurer côté client, il suffit d'aller dans les paramètres réseaux et d'indiquer que l'on désire mettre en oeuvre le service DHCP pour la recherche de l'adresse IP (obtenir automatiquement une adresse IP).

Pour vérifier le bon fonctionnement, le moyen le plus rapide est d'utiliser la commande suivante :

➤ Sous Windows

```
C:\> ipconfig/all
```

➤ Sous Linux

```
[root]# ifconfig
```



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

3. OPEN LDAP

a) Présentation :

LDAP est un protocole basé sur TCP/IP qui permet de partager des bases de données d'information sur un réseau (interne ou externe). Ces bases de données sont appelées annuaire électronique (Directory en anglais), elles peuvent contenir tout type d'informations, des informations sur les personnes, à des données systèmes.

b) Configuration :

- On va créer un annuaire **LDAP** pour votre domaine privé **poste.ma**. On doit modifier le fichier **slapd.conf**.

```
access to attr=userpassword
    by self write
    by anonymous auth
    by dn="cn=Manager,dc=poste,dc=ma" write
    by * none

access to *
    by dn="cn=Manager,dc=poste,dc=ma" write
    by * read

#####
# ldbm and/or bdb database definitions
#####
database        bdb
suffix          "dc=poste,dc=ma"
rootdn         "cn=Manager,dc=poste,dc=ma"
# Cleartext passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw          secret
rootpw         {CRYPT}Kcel3ELQNwx3s
```

- Après cette modification il faut redémarrer le service on utilisant la commande :



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

Service ldap restart

- Dans le répertoire `/usr/share/openldap/migration`, on va modifier le fichier `migrate_common.ph`, on doit y indiquer son nom de domaine, de `exemple.com` par `poste.ma`

```
$DEFAULT_MAIL_HOST = "mail.poste.ma";
```

```
# Default DNS domain
```

```
$DEFAULT_MAIL_DOMAIN = "poste.ma";
```

```
# Default base
```

```
$DEFAULT_BASE = "dc=post, dc=ma";
```

- En suite on doit ajouter un nouveau enregistrement dans l'annuaire, et pour l'ajouter il suffit de créer un nouveau fichier « `temp.ldif` » sous le répertoire `/etc` :



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

```
dn: dc=poste,dc=ma
ObjectClass: dcObject
ObjectClass: organization
dc: poste
o: poste.ma

dn: ou=Group,dc=poste,dc=ma
ou: Group
ObjectClass: organizationalUnit
description: groupes d'utilisateurs

dn: ou=People,dc=poste,dc=ma
ou: People
ObjectClass: top
ObjectClass: organizationalUnit
description: Utilisateurs de systeme
```

- Après cette création On rajoutera l'enregistrement en utilisant la syntaxe suivante :

Ldapadd -x -D "cn=Manager, dc=poste, dc=ma" -W -f temp.ldif

Enter LDAP Password: entrer le mot de passe

- Ensuite sous le fichier ldap.conf on doit modifier le nom de domaine et enlever les commentaires.

host 10.13.0.2

base dc=poste,dc=ma



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

binddn cn=Manager,dc=poste,dc=ma

bindpw secret

pam_filter objectclass=account

pam_login_attribute uid

pam_password crypt

nss_base_passwd ou=People,dc=poste,dc=ma?one

nss_base_shadow ou=People,dc=poste,dc=ma?one

nss_base_group ou=Group,dc=poste,dc=ma?one

- Dans le fichier **/etc/nsswitch.conf** on modifiera les lignes suivantes pour lire:
Passwd : files ldap
Shadow : files ldap
Group : files ldap
- maintenant on va éditer le fichier **/etc/pam.d/login** pour l'authentification d'un utilisateur à la connexion sur une machine (login)



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

```
root@server:/etc/pam.d
Fichier  Édition  Affichage  Terminal  Onglets  Aide
#%PAM-1.0
auth      required      pam_securetty.so
auth      required      pam_stack.so service=system-auth
auth      required      pam_nologin.so
auth      sufficient   /lib/security/pam_ldap.so
account   sufficient   /lib/security/pam_ldap.so
account   required     pam_stack.so service=system-auth
password  sufficient   /lib/security/pam_ldap.so
password  required     pam_stack.so service=system-auth
password  sufficient   /lib/security/pam_ldap.so
# pam_selinux.so close should be the first session rule
session   sufficient   /lib/security/pam_ldap.so
session   required     pam_selinux.so close
session   required     pam_stack.so service=system-auth
session   required     pam_loginuid.so
session   optional     pam_console.so
# pam_selinux.so open should be the last session rule
session   required     pam_selinux.so open
```

La même chose pour les fichiers SU et GDM on doit ajouter les mêmes lignes :

auth sufficient /lib/security/pam_ldap.so

account sufficient /lib/security/pam_ldap.so

password sufficient /lib/security/pam_ldap.so

Ces lignes permettent aux utilisateurs de se connecter Sous ROOT

- maintenant on doit créer un nouveau fichier « **newuser** » pour que chaque nouvelle requête doit être enregistré directement dans la base de données LDAP.



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

```
root@ server: /tmp
Fichier  Édition  Affichage  Terminal  Onglets  Aide
dn: uid=formatateur,ou=people,dc=poste,dc=ma
uid: formatateur
cn: formatateur
ObjectClass: account
ObjectClass: posix Account
ObjectClass: top
ObjectClass: shadow Account
userpassword:{CRYPT}sq/qGy5bIMCH6
shadowlastChange: 11858
shadowMax: 99999
shadowWarring: 7
shadowInactive: -1
shadowExpire:-1
Login shell: /leeb/bach
uidNumber: 5010
gidNumber: 5010
homeDirectory: /home/formatateur
gecos: formatateur
```

- Dernièrement redémarrer le service et suivre la même méthode sous client linux.

a) Présentation Ssh :

Ssh (Secure Shell) : Sécuriser des connexions à distance.

– SSH permet de sécuriser les communications des réseaux

- Utilise pour cela de la cryptographie.
- SSH est composé d'un ensemble d'outils permettant des connexions Sécurisées entre des machines. Ces outils ont pour but



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

de remplacer les utilitaires de connexions classiques n'utilisant pas de chiffage.

– Remplace : rcp, rlogin, rsh, telnet (ftp par sftp en SSH V2)

- SSH chiffre et compresse un canal de communication qui sécurise les données transmises. ainsi les informations circulant sur le réseau entre les deux machines le sont aussi.

b) Configuration SSH :

Coté serveur :

Pour configurer un serveur Ssh on doit modifier le fichier ssh_config comme suite :

- Donner l'adresse de serveur Ssh : 10.13.0.2

```
Port  
Prot #LoginGraceTime 2m  
List PermitRootLogin yes  
#Lis #StrictModes yes  
#MaxAuthTries 6
```

- Permet la connexion de super utilisateur.



WWW.RESEAUMAROC.COM

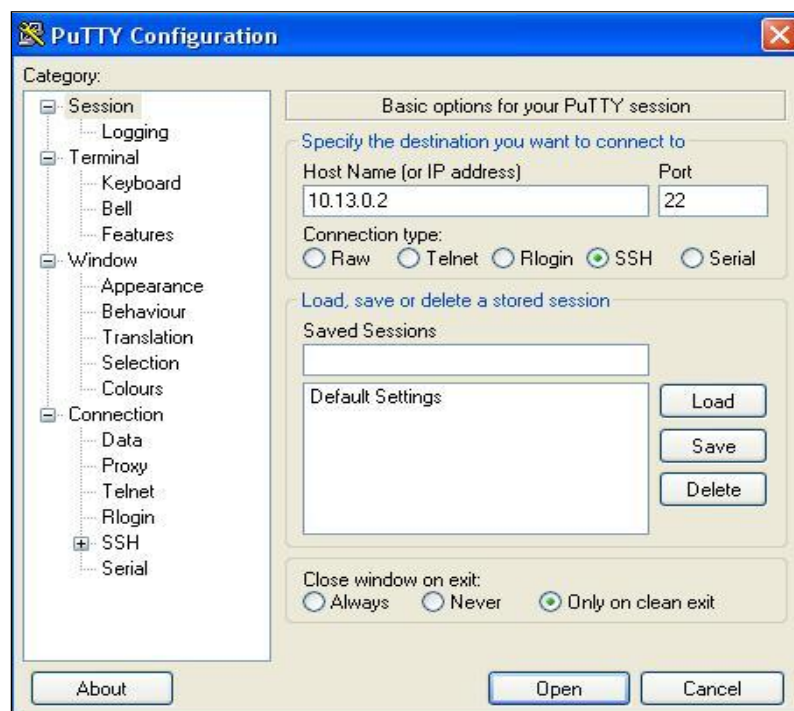
Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

Coté client

➤ Windows

Premièrement on doit télécharger PUTTY et l'installer sous client, puis double clique sur l'icône et remplir le champ suivant : Host Name Et valider « **open** » pour lancer la connexion.



- ◆ Ajout de la clé publique dans la base de registres, Répondre par « Yes » pour passer à la suite.



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

- ◆ Taper le login après le prompt «login as», Puis entrer le mot de passe pour ce connecté au serveur :

```
10.13.0.2 - PuTTY
login as: toto
toto's password:
Last login: Tue 21:21:39 2009
[toto@serveur ~]$
```

➤ Linux

La même chose pour le client Linux, taper le « login as » et entrer le mot de passe :

```
[root@client ~]# ssh toto@10.13.0.2
The authenticity of host 10.13.0.2 ' can't be established.
RSA key fingerprint is 1f:79:0f:25:39:66:97:67:42:5c:99:e4:9a:ea:0e:9c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added ' 10.13.0.2 ' (RSA) to the list of known hosts.
toto@10.13.0.2 's password:
Last login: 13 20:30:59 2009 from 10.13.0.2
[toto@serveur ~]$
```



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

a) Présentation Telnet

Telnet est un protocole permettant d'émuler un terminal à distance, cela signifie qu'il permet d'exécuter des commandes saisies au clavier sur une machine distante. L'outil Telnet est une implémentation du protocole Telnet. Telnet fonctionne dans un environnement client/serveur, c'est-à-dire que la machine distante est configurée en serveur et par conséquent attend qu'une machine lui demande un service. Ainsi, étant donné que la machine distante envoie les données à afficher, l'utilisateur a l'impression de travailler directement sur la machine distante

b) Configuration Telnet

Coté serveur:

Pou configurer un serveur Telnet on doit accéder au répertoire **/etc/xinetd.d**, ensuite éditer le fichier Telnet :

Dans ce fichier on ajoute une ligne « port = 23 »

```
service telnet
{
    disable = no
    flags           = REUSE
    socket_type     = stream
    wait           = no
    port           = 23
    user           = root
    server         = /usr/sbin/in.telnetd
    log_on_failure += USERID
}
```



WWW.RESEAUMAROC.COM

Cours/formation /Video en informatique: Linux,Cisco,2003 Server,securité,Réseaux.

Contact : tssri-reseaux@hotmail.fr TEL : 00212669324964

- ensuite démarrer le service xinetd on utilisant la commande :

Service xinetd start

- Maintenant on doit créer un utilisateur pour se connecter en mode à distance :

```
[root@serveur xinetd.d]# useradd toto
[root@serveur xinetd.d]# passwd toto
Changing password for user toto.
New UNIX password:
Retype new UNIX password:
```

Coté client XP :

Avec l'invite de commande sous Windows ou terminal sous linux

Taper le nom d'utilisateur qu'on a déjà créé « toto » et le mot de passe pour ce connecté au serveur