

# La configuration réseau sous Linux (2)

Arnaud Goulut et Ludovic Terrier

Avril 2010

## 1 Partie 1 : Les niveaux d'exécution

### 1.1 Paramétrage du service réseau

On retrouve le paramétrage du service réseau dans le fichier : `/etc/init.d/network` :

```
#!/bin/bash
#
# network          Bring up/down networking
#
# chkconfig: 2345 10 90
# description: Activates/Deactivates all network interfaces configured to \
#              start at boot time.
#
### BEGIN INIT INFO
# Provides: $network
# Should-Start: iptables ip6tables
### END INIT INFO
```

La ligne contenant `chkconfig` nous indique que ce service est par défaut démarré dans les runlevels 2, 3, 4 et 5 avec la priorité 10. De plus, il est stoppé dans les autres runlevels (1 et 6) avec la priorité 90.

### 1.2 Exécution des scripts

Les commandes liées à l'exécution des scripts sont situées dans le dossier `/etc/init.d/` qui sont les cibles des liens symboliques situées dans le dossier `/etc/rcX.d`, où `X` est le numéro du runlevel.

### 1.3 La commande `chkconfig`

Cette commande permet de modifier le paramétrage des différents services dont celui du réseau. On peut tout d'abord vérifier les états au démarrage d'un service donné pour chaque runlevels avec la commande :

```
chkconfig --list network
```

De plus, on peut modifier l'état au démarrage d'un service pour les runlevels avec la commande :

```
chkconfig --level 5 network off
```

Dans ce cas, le service `network` ne démarrera pas dans le runlevel 5.

## 2 Partie 2 : le super-serveur xinetd

### 2.1 Configuration de telnetd

Dans le cadre du TP la configuration de telnetd pour xinetd a simplement consisté en l'installation de ces deux paquets. En effet, en installant telnet sur une machine xinetd s'installe automatiquement. De plus, l'installation crée automatiquement le fichier de configuration du service telnet pour xinetd dans le répertoire `/etc/xinet.d/telnet`. Dans ce fichier il faudra cependant mettre `no` à la place de `yes` à la ligne suivante :

```
disable          = no
```

### 2.2 Les services à rattacher à xinetd

Il est préférable de rattacher à xinetd des services qui sont peu utilisés, tels des services d'accès à distance. En revanche, pour des services recevant de nombreuses connections (tel que web, ldap et messagerie) on n'utilisera pas xinetd.

### 2.3 Capture de session telnet

### 2.4 Filtrage d'accès

Il existe deux moyens pour filtrer l'accès à un service :

- via les fichiers `/etc/hosts.allow` et `/etc/hosts.deny` (utilisant le TCP Wrapper),
- dans le fichier de configuration du service.

#### 2.4.1 `host.deny` et `host.allow`

Pré-requis : le fichier `allow` est prioritaire sur le fichier `deny`.

```
# /etc/hosts.deny: list of hosts that are not allowed to access the system.  
ALL EXCEPT in.telnetd: 192.168.3.0/255.255.255.0
```

Ainsi, avec la ligne suivante on autorise personne (**ALL**) sauf pour le service telnet (`in.telnetd`) qui sera autorisé pour le réseau local (192.168.3.0).

#### 2.4.2 fichier de configuration

```
# default: on  
service in.telnetd  
{  
    flags          = REUSE  
    socket_type    = stream  
    wait           = no  
    user           = root  
    server         = /usr/sbin/in.telnetd  
    only_from      = 192.168.3.0  
    log_on_failure += USERID  
    disable        = no  
}
```

### 2.4.3 permissif ou restrictif?

La stratégie qui semble la plus sûre est celle utilisant un filtrage restrictif puisque l'on spécifie explicitement ce que l'on veut autoriser ; donnant plus de contrôle sur les accès à destination de la machine.

## 3 Partie 3 : Serveurs d'accès distant

### 3.1 Attache à xinetd

Pour rattacher un nouveau service à xinetd, il suffit de créer un fichier de configuration dans `/etc/xinet.d/` en ajoutant le paramètre `server_args = -i` et en stoppant le service ssh :

```
# default: on
service ssh
{
    flags                = REUSE
    socket_type          = stream
    wait                 = no
    user                 = root
    server               = /usr/sbin/sshd
    server_args          = -i
    log_on_failure       += USERID
    disable              = no
}
```

Après divers tests on s'aperçoit que le temps d'accès au service ssh n'est que sensiblement augmenté après le rattachement de celui-ci à xinetd.