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 chaques 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

Ce qui peut vouloir dire que l'ensemble des autres ports sont dans le même VLAN par défaut.

2.2 Les services à rattacher à xinetd

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

2.3 Filtrage d'accès

Il existe deux moyens pour filtre l'accès au serveur telnet :
- via les fichiers `/etc/hosts.allow` et `/etc/hosts.deny`,
- dans le fichier de configuration de chaque service.

2.3.1 `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
```

Ainsi, avec la ligne suivante on n'autorise personne (`ALL`) pour le service telnet (`in.telnetd`) avec pour exception le réseau local (`192.168.3.0`).

2.3.2 fichier de configuration

2.3.3 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 de la machine.

3 Partie 3 : Serveurs d'accès distant

3.1 Attache à xinetd

Pour le rattacher, il suffit de créer un fichier de configuration pour notre nouveau service, en ajoutant le paramètre :

```
# 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
}
```