

# Administration Système et Réseaux, Sécurité

## Démarrage d'un système Linux, des services, gestion des utilisateurs

Philippe Harrand

<sup>1</sup>Département Informatique  
Pôle Sciences et Technologie

<sup>2</sup>Direction Territoriale Sud Ouest  
France Télécom

10 septembre 2007

# Démarrage d'un système Linux, des services, gestion des utilisateurs

Démarrage d'un système Linux

Démarrage  
Initialisation

Démarrage des services

Gestion des utilisateurs

# Choix du support de démarrage

- ▶ Disque dur, souple, etc.
- ▶ Réseau (lecture de la ROM optionnelle de l'interface)
- ▶ USB
- ▶ autre

lecture puis exécution des octets 0 à 445 du support choisi

# Master Boot Record

Adresse		Description	Taille en octets
Hex	Dec		
0000	0	Routine	max 444
01B8	440	<i>Signature optionnelle</i>	4
01BC	444	Habituellement null ; 0x0000	2
01BE	446	<b>Table des partitions primaires</b> (Quatre entrées de 16 octets, (IBM Partition Table scheme))	64
01FE	510	Magic Number : 0xAA55	2
<b>MBR, taille totale : 444 + 2 + 64 + 2 =</b>			<b>512</b>

## Bootloader

- ▶ Standard : charge le contenu du secteur 0 de la partition marquée «amorçable »
- ▶ Lilo : charge le contenu indiqué par une adresse «physique »
- ▶ Grub : charge un fichier
- ▶ SysLinux : charge le contenu indiqué par une adresse «physique »
  - ▶ SysLinux - MS-DOS/Windows FAT
  - ▶ PXELinux - Boot réseau à la norme PXE
  - ▶ IsoLinux - ISO9660
  - ▶ ExtLinux - ext2/ext3

## SysLinux

- ▶ 446 premiers octets sur MBR
- ▶ La suite sur le répertoire désigné à l'installation
- ▶ Configuration figée
- ▶ Permet le choix d'un noyau Linux
- ▶ Ne boote que Linux...

## Linux Loader

- ▶ 446 premiers octets sur MBR ou secteur d'amorçage d'une partition accessible (Li)
- ▶ La suite sur une partition accessible (Lo)
- ▶ Configuration simple (/etc/lilo.conf)
- ▶ Nécessite d'être compilé (/sbin/lilo)

## GRand Unified Bootloader

- ▶ Mini OS
  - ▶ Capable de lire différents systèmes de fichiers
  - ▶ Muni d'un interpréteur de commandes
  - ▶ Supporte la complétion !
- ▶ GRUB peut charger n'importe quel système depuis n'importe quel support (presque)
- ▶ Pas de compilation

## Chargement du système

1. Lecture MBR  
Adressage bootloader
2. Choix du Système d'Exploitation
3. Décompression et chargement du noyau
  - 3.1 Création d'un *ramdisk* et copie de l'image indiquée
  - 3.2 Changement de racine
  - 3.3 Chargement des modules nécessaires au démarrage
  - 3.4 Retour à la racine originelle
4. Exécution de *init*

## Démarrage réseau

- ▶ Chargement du programme de la ROM de l'interface réseau
- ▶ Requête DHCP
  - ▶ Obtention d'une configuration réseau
  - ▶ Obtention de l'adresse d'un serveur TFTP et du nom d'un fichier à télécharger
- ▶ Exécution du fichier téléchargé

## Démarrage réseau

- ▶ Programmes ROM
  - ▶ **Préboot eXecution Environnement PXE** très répandu sur les interfaces haut de gamme
  - ▶ *PXEGrub* et *Etherboot* sont des alternatives libres
- ▶ Chargeurs
  - ▶ *REMBO* : très élaboré et flexible mais ni libre ni gratuit
  - ▶ *GRUB*
  - ▶ *Etherboot*

## init

- ▶ Processus n°1, ancêtre de tous les autres
- ▶ Initialise le système
- ▶ Monte les systèmes de fichier
- ▶ Lance les démons
- ▶ Gère les consoles

## init

- 0 : arrêt du PC (*halt*)
- 1 : mode mono-utilisateur ou maintenance
- 2 : mode multi-utilisateur sans **Network File System**
- 3 : mode multi-utilisateur avec réseau en mode texte
- 4 : inutilisé
- 5 : mode multi-utilisateur avec réseau et serveur graphique
- 6 : redémarrage du PC (*reboot*)

Seuls les niveaux 0,1 et 6 sont normalisés. Les autres peuvent varier suivant les distributions et votre bon plaisir.

## Le fichier `/etc/inittab`

- ▶ Indique le *runlevel* par défaut
- ▶ Lance l'exécution de `/etc/rc.d/rc.sysinit`
- ▶ Indique les répertoires contenant les scripts de démarrage et d'arrêt selon le runlevel
- ▶ Indique les consoles à gérer
- ▶ Indique que faire selon les signaux de l'onduleur

## Scripts `/etc/rcX.d/..`

- ▶ Arrêt des démons
- ▶ Démarrage des démons
- ▶ suivant le niveau d'exécution
- ▶ Nommage des liens
  - ▶ K ou S
  - ▶ Numéro d'ordre
  - ▶ Nom du script
- ▶ Les scripts sont placés dans `/etc/rc.d/init.d`
- ▶ Pour finir, `/etc/rc.d/rc.local` est exécuté (sauf Debian...)

## Les utilisateurs

- ▶ Sont identifiés par un uid unique
- ▶ Et par un « login »
- ▶ Appartiennent à un groupe principal : gid
- ▶ Peuvent appartenir à des groupes secondaires
- ▶ Sont propriétaires d'un répertoire
- ▶ Ont accès à un interpréteur de commande après identification

## Les types d'utilisateurs

- ▶ L'utilisateur root :
  - ▶ uid=gid=0
- ▶ Les utilisateurs spéciaux
  - ▶ Utilisés par les démons
  - ▶ 0 < uid=gid < 500
  - ▶ Pas d'interpréteur de commandes
- ▶ Les utilisateurs humains
  - ▶ uid et gid >= 500

## Gestion des utilisateurs

- ▶ 3 fichiers
  - ▶ /etc/passwd
  - ▶ /etc/shadow
  - ▶ /etc/group
- ▶ 1 répertoire
  - ▶ /etc/skel

## /etc/passwd

```
root :x :0 :0 :root :/root :/bin/bash
bin :x :1 :1 :bin :/bin :/bin/sh
daemon :x :2 :2 :daemon :/sbin :/bin/sh
.....
xfs :x :70 :70 :system user for xorg-x11 :/etc/X11/fs :/bin/false
apache :x :71 :71 :system user for apache-conf :/var/www :/bin/sh
sshd :x :75 :75 :system user for openssh :/var/empty :/bin/true
rpcuser :x :76 :76 :system user for nfs-utils :/var/lib/nfs :/bin/false
pharrand :x :500 :500 :Philippe Harrand :/home/pharrand :/bin/bash
ntp :x :77 :77 :system user for ntp :/etc/ntp :/bin/false
quagga :x :92 :92 :Quagga routing suite :/var/lib :/sbin/nologin
ftp :x :501 :501 : :/var/ftp :/bin/bash
ntop :x :120 :120 :system user for ntop :/var/lib/ntop :/bin/false
stagiaire :x :502 :502 :Stagiaire :/home/stagiaire :/bin/bash
```

## /etc/shadow

```
root :$1$1ueM.g/76tDRfDtJW15xE087IJR/ :13134 :0 :99999 :7 : : :
bin :* :13134 :0 :99999 :7 : : :
daemon :* :13134 :0 :99999 :7 : : :
.....
xfs :!! :13134 : : : : :
apache :!! :13134 : : : : :
sshd :!! :13134 : : : : :
rpcuser :!! :13134 : : : : :
pharrand :$1$hoz65gb2tzwxceUeN3Q1BCM/ :13134 :0 :99999 :7 : : :
ntp :!! :13235 : : : : :
quagga :!! :13250 : : : : :
ftp :!! :13286 :0 :99999 :7 : : :
ntop :!! :13321 : : : : :
stagiaire :$1$gCNyvVgbFD59nCyc8qR0 :13334 :-1 :99999 :-1 : : :
```

## Gestion des utilisateurs

- ▶ Utilisateurs
  - ▶ Ajouter : useradd ou adduser
  - ▶ Modifier : usermod
  - ▶ Supprimer : userdel ou deluser
- ▶ Groupes
  - ▶ Ajouter : groupadd
  - ▶ Modifier : groupmod
  - ▶ Supprimer : ???

## Commandes diverses

- ▶ Qui suis-je ? whoami
- ▶ Informations : id
- ▶ Quels sont mes groupes ? groups
- ▶ *Par défaut la plupart des distributions actuelles créent un groupe pour chaque nouvel utilisateur...*

## Configuration de bash

- ▶ Commune à tous les utilisateurs
  - ▶ /etc/profile
  - ▶ Les fichiers contenus dans /etc/profile.d/
- ▶ Personnelle
  - ▶ .bash\_profile exécuté à chaque login
  - ▶ .bashrc exécuté à chaque nouveau bash
  - ▶ Optionnel
    - ▶ .bash\_logout
  - ▶ .bash\_history