**bin/**

Programmes utilisateurs essentiels au démarrage

**boot/**

Bootloader, initrd, kernel…

**dev/**

Accès aux périphériques

**etc/**

Configuration

**Apt/ -sources.list** Liste des dépôts

**passwd/** User infos

Username, passwd, UID, GID, UID infos, Home directory, Shell (or cmd)

**Shells/** Shells valides.

**Shadow/** User passwd infos.

* Username
* Hash : $1$ MD5, $2a$ Blowfish, $5$ SHA 256, $6$ SHA 512

$X$ SALT $ HASH

* LastChanged : UNIX format (1970)
* Min : #days between Passwd changes.
* Max : #days valid
* Warn : #days before receiving warning.
* Inactive : #days after passwd expires : disabling.
* Expire : Absolute date which acount expires.

**Skel/** Fichiers copiés dans le répertoire du user lors de sa création

**Group/** Name :mdp :GID :member1, member2…

**Gshadow/**

**pam.d/** Configuration des services utilisant PAM

**fstab/** Liste des périphériques montés automatiquement au démarrage

**init.d/** Fichiers de scripts de services (start stop etc pour chaque services)

**-login.defs :** Conf for **new** users acount

**-Os-release**

**-services :** Ports -> Portname

**-hostname**

**-resolv.conf :** Serveurs DNS

**Home/**

**Initrd/**

Construction image noyau en RAM

**lib/**

Librairies partagées essentielles au démarrage

.a = lib that contains many .o / .so = shared lib / lib linked to /bin /sbin

**Modules/** Modules du noyau

**Security/** Librairies PAM

**mnt/**

Point de montage temporaire

**opts/**

Applications tierces (non issues de la distribution)

**proc/**

Pseudo fichier, occupe 0 octets en mémoire dans l’espace de mémoire kernel

**LIRE LE MAN !!!**

**Core(5)**

**Cpuset(7)**

**Mmap(2)**

**Clone(2)**

**Numa(7)**

**XX/** PID processus en exec

**-cgroup** Control groups : les cgroups permettent de limiter les ressources d’un groupe de processus. Fichier présent si CONFIG\_CGROUPS validée lors de la compilation.

Un enfant hérite du cgroup de son parent et ne peut le changer : Permet de retrouver l’affiliation, quand un processus peut devenir enfant d’init ou bien se renommer.

**-clear\_refs** Efface le soft\_dirty d’un processus : Permet de savoir les pages qu’un processus a souillé des que clear\_refs est RAZ.

Fichier présent si CONFIG\_PROC\_PAGE\_MONITOR validé lors de la compilation.

**-cmdline** Commande qui a lancé le processus, sauf pour les zombies.

**-coredump\_filter**

**-cpuset**

**Cwd/** Current working directory : lien symbolique vers le cwd

**-environ** Variables d’environnement du processus.

**-exe** Lien symbolique vers l’exécutable

**Fd/** Tous les descripteurs de fichier ouverts par le processus.

0 entrée standard, 1 sortie standard 2 erreur…

**Fdinfo/** Offset dans le fichier, flags (droits…) de chaque fichiers ouverts par le processus.

-**io** Statistiques d’E/S pour le processus : Nombre d’octets lus, écrits…

**-limits** Affiche les ressources limites du processus (RAM maxi etc…)

**Map\_files/**

**-maps** Mapping mémoire du processus :

@, droits, position, majeur :mineur, inode, chemin

**-mem** Accès à la mémoire du processus au travers de open(), read() et

Lseek().

**-mountinfo**

**-mounts**

**-mountstats**

**Ns/** Espace de nom du processus : en rapport avec la limitation des

Ressources.

**-numa\_maps**

**-oom\_adj** Déprécié : utilisé oom\_score\_adj

**-oom\_score** indique le score du processus : lorsque mémoire saturée, le noyau

Peut alors sélectionner un processus pour le kill.

Se base sur ses forks, son nice, son CPU, oom\_score\_adj…

**-oom\_score\_adjust** 0 : ne jamais tuer et 1000 : toujours tuer.

**-root** root directory of this process

**-smaps** Informations mémoire mais différente de maps

**-stack** Stack noyau du processus.

**-stat** process status utilisé par ps par exemple.

**-statm** process memory status

**-status** process status (-h ^^) se base sur stat et statm

**acpi/** Liste des devices permettant de sortir de veille prolongée

**bus/**

**-cmdline** Kernel cmd line

**-cpuinfo**

**-crypto** tous les algos installés et utilisables

**-devices** Tous les periph blocs et caractères du système.

**-Filesystems** Tous les VFS pris en compte.

**-Interrupts** Liste des IRQ par proc (niquel pour checker si NAPI enabled)

#IRQ #interrupts/CPU interrupt\_controller device[,device…. Si shared]

**-Iomem** @RAM utilisés

**-Ioports**

**Irq/**

**-Kcore** Représente la RAM du système

**-Loadavg** Charge moyenne depuis 1, 5, 15 min, #process, PID dernier process utilisé

**-Meminfo** Usage de la RAM

**-Modules** Modules chargés par le noyau

**-Mounts** Lien symbolique, table de montage

**-Net** Lien symbolique, accès aux tables ARP, routage, sockets…

**-Partitions**

**-Swaps** Infos sur le swap du système

**sys/** Fichiers de conf du kernel

**kernel/ -pid-max :** Valeur du PID-max

**-uptime** Temps écoulé en secondes depuis démarrage et durée d’inactivité

**-version** : version du noyau (pae = physical adress extension = jusqu’à 64 Go de RAM).

**-vmallocinfo :** Infos sur la mémoire virtuelle

**sys/**

Pseudo fichier, occupe 0 octets en RAM

**root/**

**sbin/**

Programmes systèmes essentiels au démarrage

**tmp/**

**usr/**

**bin/**

**sbin/**

**lib/** Linked to /usr/bin /usr/sbin

**var/**

**lib/ dpkg/ info/** Scripts de configuration des paquets installés.

**-status** Status de chaque paquets installés.