

Formation à GNU/Linux

Michaël Launay <michaellaunay@ecreall.com>

Ecreall 2020 update de la version 2009 pour Ubuntu 20.04

###Title### Page : ###Page###

Objectif

Cette formation a pour but de fournir les bases indispensables à l'utilisation et à l'administration des systèmes GNU/Linux.

La formation privilégie la distribution Ubuntu.

Introduction

En 1991, l'étudiant finlandais Linus Torvalds publie sur internet l'intégralité du code source d'un noyau Unix qu'il a écrit en C et en assembleur et qui fonctionne sur PC AT 386(486).

Depuis cette date GNU/Linux ne cesse d'évoluer. Il occupe en 2015 1,6%¹ du marché mondial des systèmes d'exploitation pour ordinateur personnel, plus de 60% des serveurs web, près de 75% du Cloud et plus de 80% des smartphones (Android étant basé sur GNU/Linux) et est en outre utilisé en France par la Gendarmerie (Ubuntu) et par l'Assemblée Nationale (Ubuntu), dans la Freebox, par l'entreprise Google (Android) et la fondation Wikipedia (serveur Ubuntu).

Historique

UNIX (les racines)

Ken Thompson, ingénieur d'AT&T travaille en collaboration avec le MIT au Bell Labs sur Multics.

En 1969 il créait un système d'exploitation inspiré de Multics. Brian Kernighan le nommera Unics.

¹http://en.wikipedia.org/wiki/Comparison_of_operating_systems

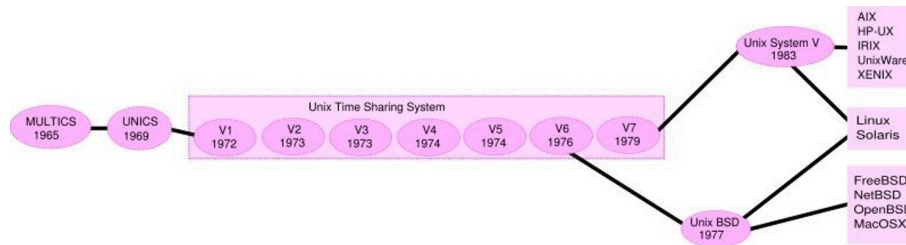


Figure 1: Histoire des Unix (source wikipedia)

En 1971 Unics devient Unix et est alors réécrit en C spécialement développé pour cela par Dennis Ritchie.

1973 AT&T diffuse Unix avec ses sources à ses clients (première licence open source).

1974 l'Université de Californie Berkeley (UCB) commence ses recherches sur UNIX en collaboration étroite avec AT&T.

1977 Bill Joy alors étudiant à l'UCB réalise la première version de BSD (Berkeley Software Distribution).

À partir de là, les éditions se succèdent (SYSTEM III puis V en 1985 et SVR2 à SVR4 pour AT&T, 4.2BSD pour l'UCB en 1983).

La DARPA finance BSD ce qui aboutit à l'intégration de la première pile TCP/IP en 1983 qui sera intégrée telle quel dans Windows en raison de sa licence permissive.

1985 la 4.3 BSD n'est plus livrée avec les sources de AT&T en raison du prix excessif de la licence.

Face à ce problème, l'UCB réécrit et nettoie complètement son UNIX qui sort en 1989 sous le nom NetBSD. Le noyau est alors le MACH de l'université de Carnegie-Mellon. L'accès aux sources et à la distribution complète devient gratuit.

1991 Sun Microsystems co-fondé en 1982 par Bill Joy sort SunOS qui deviendra Solaris.

1992 Procès AT&T BSD

FreeBSD apparaît en 1993 comme le portage de NetBSD sur i386

1998 Solaris supporte le 64 bits

1999 Mac OS X (server)

2005 Open Solaris

Octobre 2008 version 4.0.1 de NetBSD

Janvier 2009 version 7.1 de FreeBSD

La Free Software Foundation (FSF), le projet GNU

1983 Richard Stallman (RMS) qui travaillait au laboratoire d'intelligence artificielle du MIT crée le projet GNU.

GNU est un acronyme récursif (GNU's Not Unix).

GNU a pour objectif de fournir un système d'exploitation compatible avec UNIX sans dépendre des ayant droits (AT&T et BSD) dont RMS récuse les licences.

1985 création de la Free Software Foundation (FSF) organisation américaine à but non lucratif pour le soutien du logiciel libre.

1987 Rob Pike, Ken Thompson et Dennis Ritchie débutent les travaux de Plan 9 qui inspirera les UNIX modernes.

1989 écriture de la GNU GPL (GNU Genral Public Licence ou GPL) version 1.

1990 le système GNU possède son propre éditeur (Emacs), d'un compilateur C (GCC), et d'une réécriture de la plupart des bibliothèques système d'UNIX.

1991 le noyau Linux utilise la GPL et GCC.

1997 lancement de GNOME un environnement graphique dont l'objectif était de fournir une alternative libre à l'environnement KDE qui utilisait la bibliothèque Qt alors non libre.

La licence BSD versus la licence GPL

Il existe presque plusieurs centaines de licences appliquées aux logiciels libres, mais dans la majorité des cas on peut les séparer en deux catégories selon qu'elles sont compatibles avec la licence BSD ou la licence GPL.

La licence GPL

La licence GPL a pour but de protéger l'auteur et l'utilisateur en garantissant les droits suivants (appelés libertés) :

1. La liberté d'exécuter le logiciel, pour n'importe quel usage ;
2. La liberté d'étudier le fonctionnement d'un programme et de l'adapter à ses besoins, ce qui passe par l'accès aux codes sources ;
3. La liberté de redistribuer des copies ;
4. La liberté d'améliorer le programme et de rendre publiques les modifications afin que l'ensemble de la communauté en bénéficie.

En contrepartie l'utilisation du logiciel est au risque et péril de l'utilisateur.

Le gauche d'auteur

Le code n'est pas dans le domaine public.

Il est protégé par le droit d’auteur.

L’exécution du logiciel et la diffusion des sources modifiées ne sont possibles qu’à la condition de respecter les obligations de la licence.

Notamment :

Le droit de redistribuer est garanti seulement si l’utilisateur fournit le code source de la version modifiée. En outre, les copies distribuées, incluant les modifications, doivent être aussi sous les termes de la GPL.

Cette condition est connue sous le nom de copyleft.

Puisque le logiciel est protégé par les droits d’auteurs, l’utilisateur ne peut le modifier ou le redistribuer, sauf sous les termes du copyleft. En conséquence l’utilisateur doit à son tour fournir les sources et placer ses modifications sous GPL.

Puisque le copyleft des versions 1 et 2 de la GPL ne s’appliquait pas aux entrées sorties du programme, il était possible dans le cas par exemple d’un service web de contourner l’obligation de diffusion des sources. De même, il suffisait de transformer tout code GPL en bibliothèque dynamique pour ne pas propager la GPL aux extensions apportées à un programme existant.

Cette faille a été corrigée avec la version GPL v3 qui accorde aux utilisateurs d’un programme accédé par réseau les mêmes droits que les utilisateurs d’un programme installé localement.

La GPL a été adaptée au droit Français par le CEA, CNRS, INRIA sous le nom de CECILL. Sa version 2 est compatible avec la licence publique générale GNU.

Le 28 mars 2007 le tribunal de grande instance de Paris a jugé applicable la licence GPL (v2).

La licence BSD

La licence BSD permet l’utilisation du logiciel et la réutilisation de n’importe quelle partie de son code source sans restriction. La seule obligation était la mention des auteurs initiaux.

Pour pouvoir utiliser le logiciel écrit sous licence BSD l’utilisateur accepte de ne pas se retourner contre les auteurs en cas de problèmes.

Un logiciel propriétaire peut donc être réalisé à partir du code source d’un logiciel BSD (C.f. pile TCP/IP dans Windows).

GNU/Linux

Linux est développé sur internet par des milliers de contributeurs distants de nationalité et de culture différentes. C’est l’un des projets collaboratifs les plus

importants.

Les distributions

Qu'est-ce qu'un noyau ?

Pour définir le noyau, nous pouvons nous baser sur les services qu'il fournit :

Abstraction du matériel (fourniture d'interface) Gestion des interruptions
Gestion des tâches et autres logiciels Gestion des utilisateurs Gestion des droits d'accès

Historiquement on distingue les micro-noyaux des noyaux monolithiques. Cette séparation vient de ce que le noyau est censé gérer (kernel space) et donc de ce qui est de la responsabilité des utilisateurs (user space). Dans les faits aujourd'hui même les noyaux monolithiques comme Linux sont modulaires et ne charge les modules que si nécessaire pendant l'utilisation.

Qu'est ce qu'une distribution ?

Une distribution est un ensemble cohérent de logiciels fourni avec un noyau (Linux ou BSD). Les logiciels sont choisis pour utiliser les mêmes versions de bibliothèque et être compatibles les uns avec les autres ce qui a pour conséquence d'augmenter la stabilité et d'améliorer l'utilisation.

Elles comprennent des outils d'installation et de configuration.

Il en existe de nombreuses couvrant des besoins et des usages différents (ordinateur personnel, de bureau, serveur, passerelle, intrusion, multimédia center), ou des matériels spécifiques.

Les différentes distributions GNU/Linux

Sont orientées vers les utilisateurs débutants :

- Suse
- Ubuntu Desktop,

Pour les serveurs :

- Ubuntu Server
- Debian
- Gentoo
- Red Hat
- CentOS

Pour les développeurs :

- Fedora
- Red Hat

Les métas distributions :

- Red hat -> Fedora, CentOS
- Debian -> Ubuntu, Knoppix,
- Gentoo -> Aurora

Les principales distributions

Debian reste très orienté administrateur. Il est important d'être à l'aise avec la ligne de commande. Les versions stables sortent en moyenne tous les 2 ans.

Ubuntu reprend les outils Debian mais les versions sortent tous les 6 mois.

Gentoo permet une optimisation poussée du système. Il propose en priorité de compiler les sources de chacun des logiciels et donc de ne garder que les fonctionnalités voulues par l'utilisateur, en tenant compte des nombreux paramètres locaux.

Distributions commerciales :

- Red Hat (<http://www.redhat.com>),
- Novell/SUSE (<http://www.novell.com/linux/>).

Distributions "communautaires" :

- Gentoo (<http://www.gentoo.org>)
- CentOS (<http://www.centos.org>)
- Debian (<http://www.debian.org>)
- Fedora (<http://fedoraproject.org/>)
- Ubuntu (<http://www.ubuntu.com>)

Linus Torvalds défend la multiplicité des distributions.

Installation

Le choix d'une distribution doit se faire en fonction :

- du besoin technique,
- des performances voulues,
- de la pérennité désirée,
- du niveau de sécurisation attendu.

Une fois ces exigences connues, il ne reste plus qu'à se procurer les images des distributions adéquates, soit directement sur les sites des distributions, soit sur un miroir.

Installation de GNU/Linux Ubuntu version pc de bureau

Les versions desktop d'Ubuntu sont fournies avec l'environnement graphique Gnome, des outils de maintenance, la suite open-office, le lecteur de courrier evo-

lution, le logiciel de dessin Gimp, le navigateur firefox, un client vnc permettant de se connecter à distance, des jeux, des logiciels multimédias.

Elles conviennent parfaitement à un poste de travail, mais sont à proscrire pour un serveur en raison du nombre de services fonctionnant par défaut.

Installation d'Ubuntu 20.04

Choisir l'image "iso" d'Ubuntu correspondant à sa machine à l'adresse <https://releases.ubuntu.com/20.04/>

La différence entre Desktop et Server est que dans la Desktop vous aurez tout l'environnement graphique, alors que la version Server suppose une utilisation en ligne de commande.

Créer un disque d'amorçage en suivant <https://help.ubuntu.com/community/BurningIsoHowto>

Insérer la clé dans votre lecteur usb. Redémarrer votre ordinateur pour pouvoir modifier les paramètres du **bios**. Selon la marque de votre ordinateur la touche pour entrer dans le bios lors du démarrage est soit Ech, Entrée, F2, ou Suppr. Modifier votre bios pour qu'il démarre sur la clé usb (généralement le menu boot). Enregistrer et quitter le bios. L'ordinateur va alors démarrer sur la clé et charger Ubuntu comme système d'exploitation. Ubuntu commence par vérifier qu'il n'y a pas eu de corruption de la clé. Puis il affiche différents écrans que nous allons expliquer ici.

Étape 01

Si vous cliquez sur le bouton "Essayer Ubuntu" vous pourrez tester Ubuntu sans rien installer sur votre machine, les logiciels utilisés seront ceux présents sur la clé usb (vous pourrez en installer d'autres). C'est un excellent moyen de dépanner une machine pour par exemple accéder à vos disques lorsque votre l'OS de votre machine ne fonctionne plus.

Étape 02

Les différents choix déterminent comment vous allez pouvoir saisir les caractères comme œ. Par exemple avec le choix de clavier "alt." il suffira de faire "Alt Gr" "o", pour avoir œ. Vous pouvez tester les touches du clavier dans la zone de saisie du texte.

Étape 03

L'installation minimale n'installe pas les logiciels comme libre office vous laissant le faire par la suite. Demander la mise à jour lors de l'installation suppose d'être relié à internet.

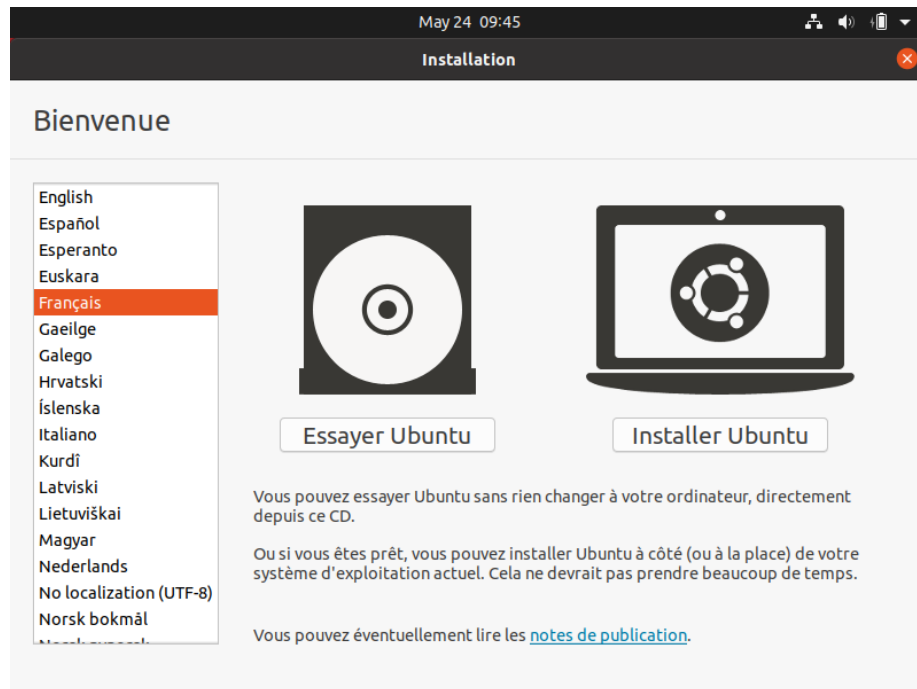


Figure 2: Choix de la langue du live usb. Et choix entre tester Ubuntu ou lancer l'installation.

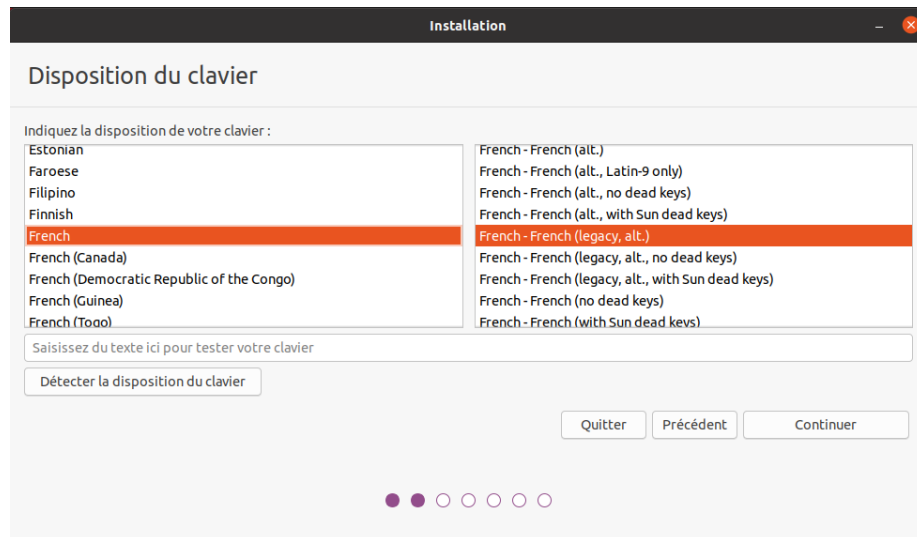


Figure 3: Choix de la disposition du clavier.

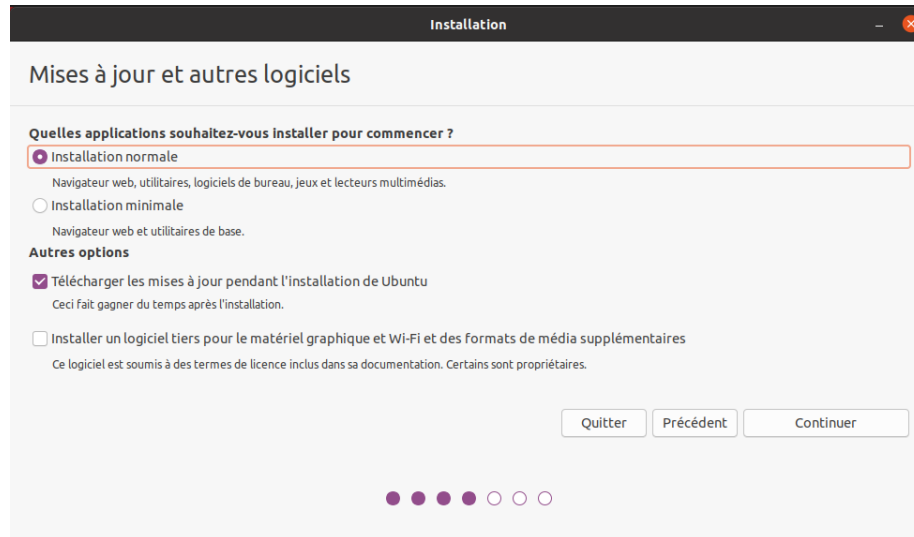


Figure 4: Type d'installation avec mise à jour ou non.

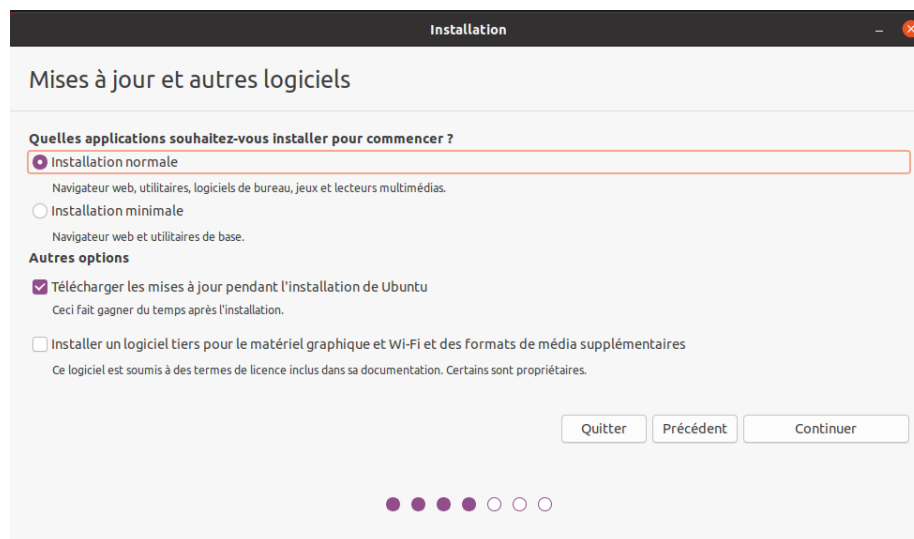


Figure 5: Choix du partitionnement si l'on clique sur "autre chose" on pourra créer ses partitions.

Étape 04

Par défaut le disque sera formaté et une partition racine sera créée ainsi qu'une partition swap. La partition de swap est utilisée pour stocker temporairement la mémoire d'un programme qui s'exécutait, mais qui n'est pas celui en cours d'utilisation. Par exemple si vous n'avez que très peu de mémoire et que vous lancez plusieurs programmes, celui avec lequel vous interagissez sera en mémoire et les autres peuvent être dans le swap.

Si votre swap a la même taille que votre mémoire vive vous pourrez "hiberner" votre ordinateur, ainsi toute la mémoire vive sera copiée dans le swap et l'ordinateur sera éteint, lorsqu'il sera rallumé tout le swap sera recopié en mémoire vive et les programmes reprendront là où ils en étaient.

C'est pour cela qu'il est intéressant de créer et paramétrer ses partitions et au minimum de créer une partition `/home` pour préserver le contenu de ses données en cas de crash sévère de l'OS, nous allons voir comment partitionner le disque.

Nous détaillerons le partitionnement ci-après.

Étape 05

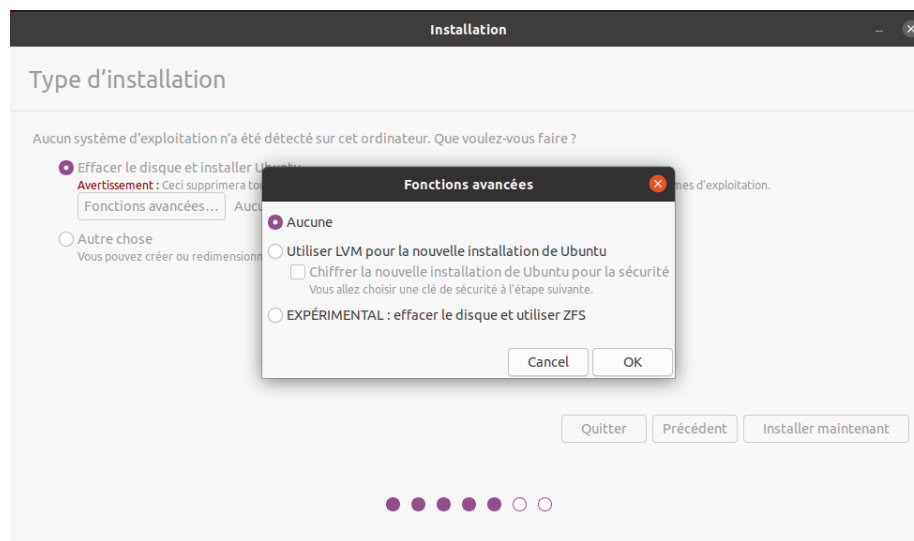


Figure 6: Ubuntu propose d'utiliser LVM.

LVM (Logical Volume Manager) est un gestionnaire de volumes logiques qui vous permettra de créer des partitions virtuelles afin de pouvoir les retailler ou d'en créer de nouvelles. Linux crée alors une couche intermédiaire entre le(s) disque(s) physique(s) et l'OS, c'est dans cette couche virtuelle que vous aurez vos partitions virtuelles qui seront écrites dans la partition réelle. Toutefois si

la partition physique est abîmée, on perd les partitions virtuelles écrites dessus, c'est pourquoi il faut faire des copies de sauvegardes ou avoir des disques montés en raid. Vous pouvez également chiffrer la partition LVM.

Étape 06

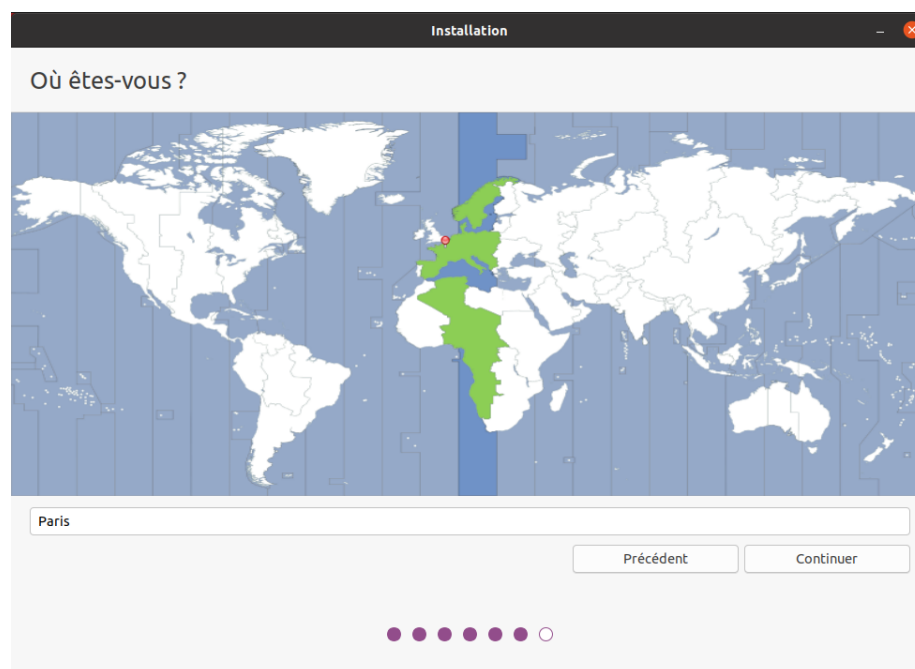


Figure 7: Choix du fuseau horaire.

Si vous êtes en France métropolitaine, choisissez le fuseau passant par la France.

Étape 07

Sous Ubuntu cet utilisateur aura la particularité de pouvoir mettre à jour le système et plus généralement de pouvoir devenir super utilisateur (root).

Étape 08

Ubuntu affiche un récapitulatif des choix réalisés, la confirmation lance alors le partitionnement des disques, leur formatage puis l'installation du système.

En fin d'installation un écran vous invite à retirer la clé usb et à redémarrer l'ordinateur.

Une fois redémarré saisissez votre identifiant et votre mot de passe (ceux donnés à l'étape 07)

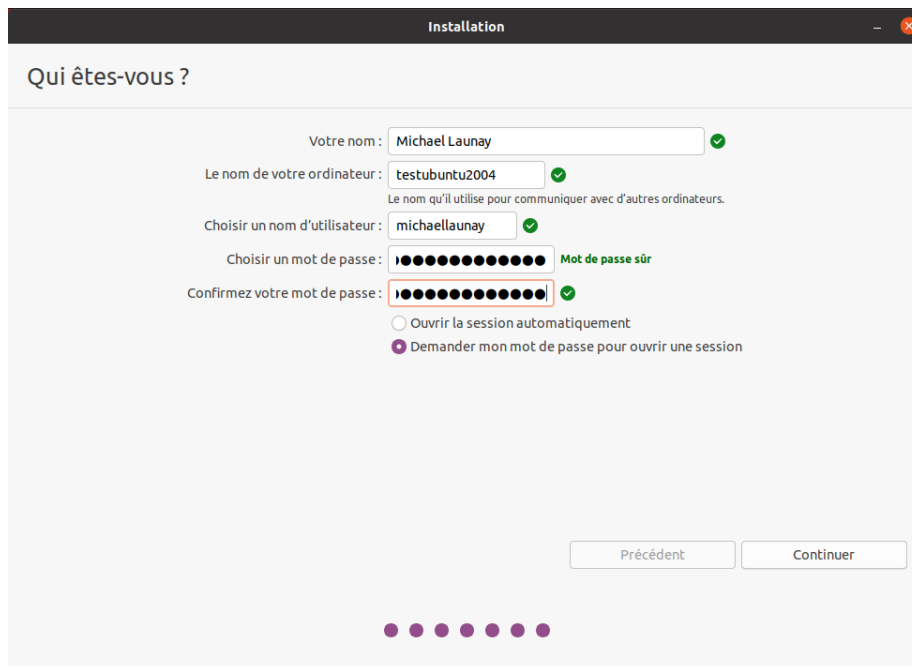


Figure 8: Création du 1er compte utilisateur.

Vous pouvez alors associer votre machine à vos comptes google et microsoft pour par exemple voir vos agendas et recevoir vos notifications.

Vous pouvez associer votre machine au mécanisme livepatch de Canonical l'éditeur d'Ubuntu pour faire automatiquement la mise à jour de votre machine.

Vous pouvez aider Canonical à corriger les bogues en autorisant la remontée des incidents.

Il est possible de permettre la géolocalisation.

On peut installer immédiatement les applications compatibles avec Ubuntu 20.04

Étape alternative 04 bis

Le partitionnement est l'étape la plus importante, car il est difficile de corriger les erreurs.

Pour les serveurs cette étape influence directement la sécurité du système (/var/lib, /var/log, /var/spool, /var/www, /tmp), la sécurité est alors physique et ne repose pas seulement sur le mécanisme des quotas. De plus, l'analyse post-mortem d'une partition dédiée est plus facile que celle d'un énorme fourre-tout.

Au minimum, il est recommandé d'avoir une partition /, /home et swap.

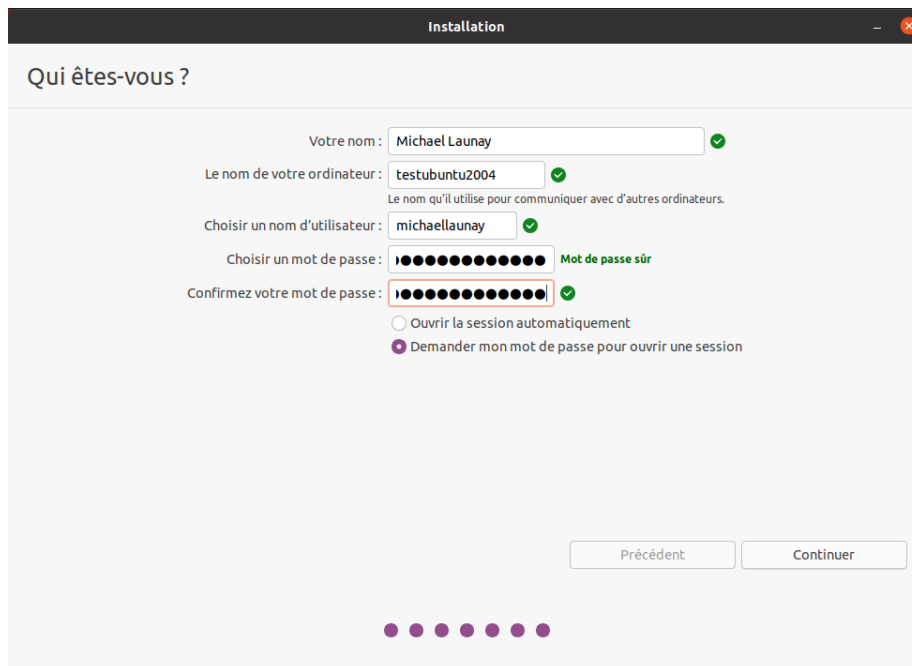


Figure 9: Une fois les choix confirmés, l'installation commence.

Pour activer le partitionnement manuelle, il suffit de cocher sur le bouton "Autre chose" à l'étape 04.

Il faut alors choisir un disque.

Le bouton "+" permet de créer de nouvelle partition

Dans notre cas nous allons créer 3 partitions /, /home et swap.

Sur le même principe, on crée "/home" On peut cocher la case "formater" pour purger le disque de ce qu'il contenait avant.

Puis vient la partition de "swap".

N'oubliez pas que la taille du swap doit être au moins égale à celle de la mémoire vive (RAM) pour permettre l'hibernation.

Installation de GNU/Linux Ubuntu en version serveur

La philosophie des distributions serveur est moins il y a de programmes installés plus le système est stable et moins il y a de faille de sécurité.

En conséquence, les interfaces graphiques ne sont disponibles qu'en option et le moyen privilégié d'administrer le système est la ligne de commande.

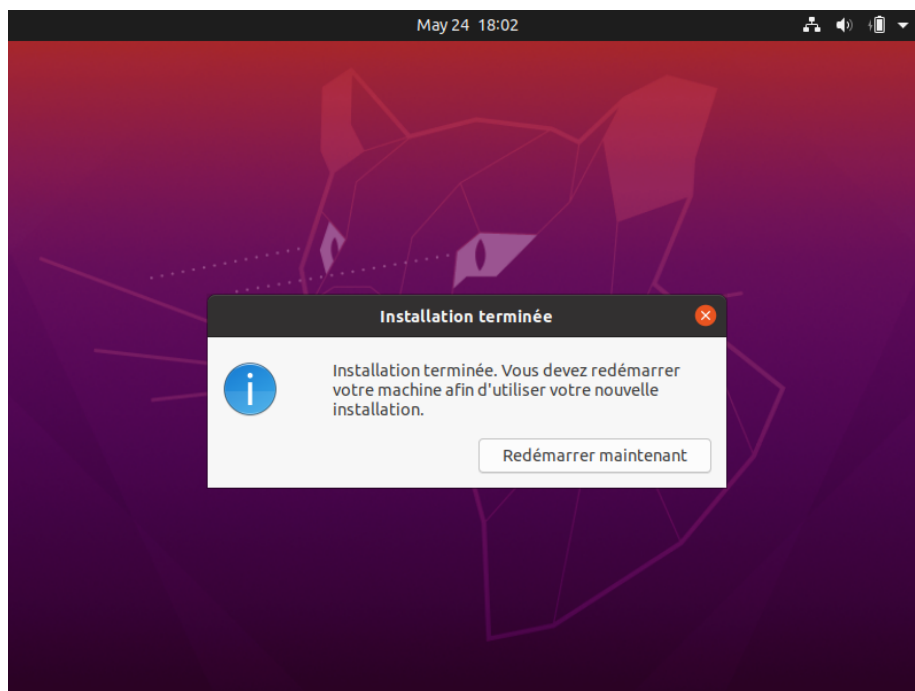


Figure 10: Fin d'installation.

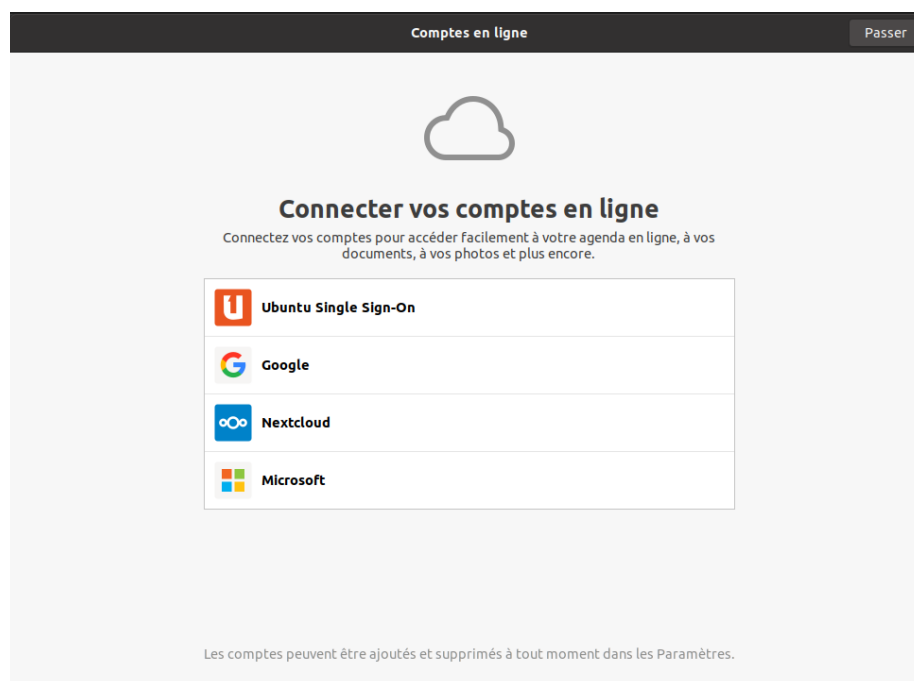


Figure 11: Configuration des comptes en lignes.

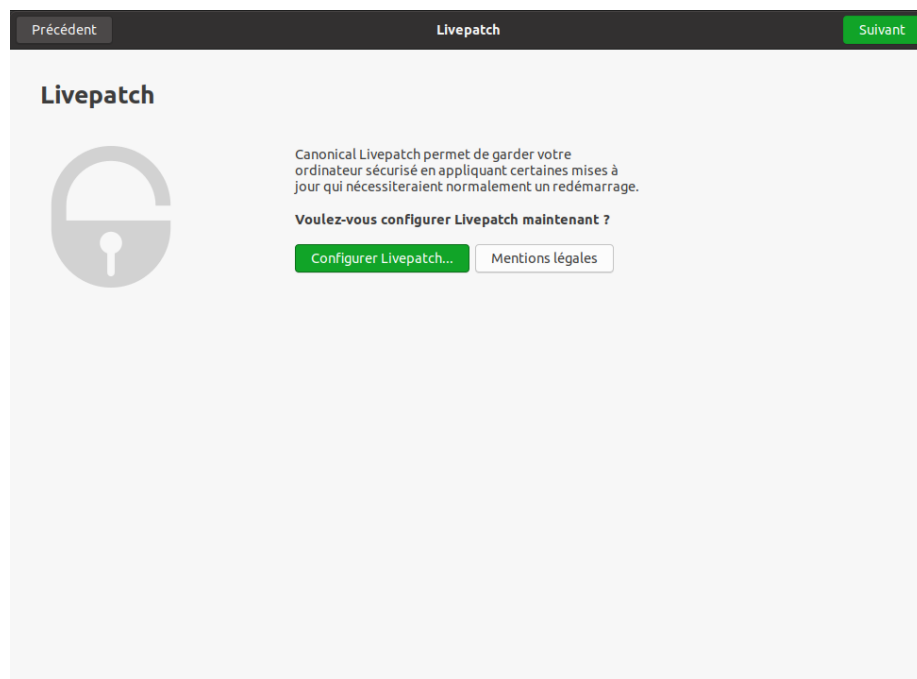



Figure 12: Configuration de votre compte Ubuntu pour le live patch.

[Précédent](#)[Aidez-nous à améliorer Ubuntu](#)[Suivant](#)

Aidez-nous à améliorer Ubuntu



Ubuntu peut envoyer des informations qui aident les développeurs à l'améliorer. Cela inclut des éléments tels que le modèle d'ordinateur, le logiciel installé et l'emplacement approximatif que vous avez choisi (Europe/-Paris).

[Afficher le premier rapport](#)[Mentions légales](#)

Souhaitez-vous envoyer cette information ?

☒ Oui, envoyer les informations système à Canonical

☐ Non, ne pas envoyer d'informations système

Figure 13: Remonté des informations pour les développeurs.

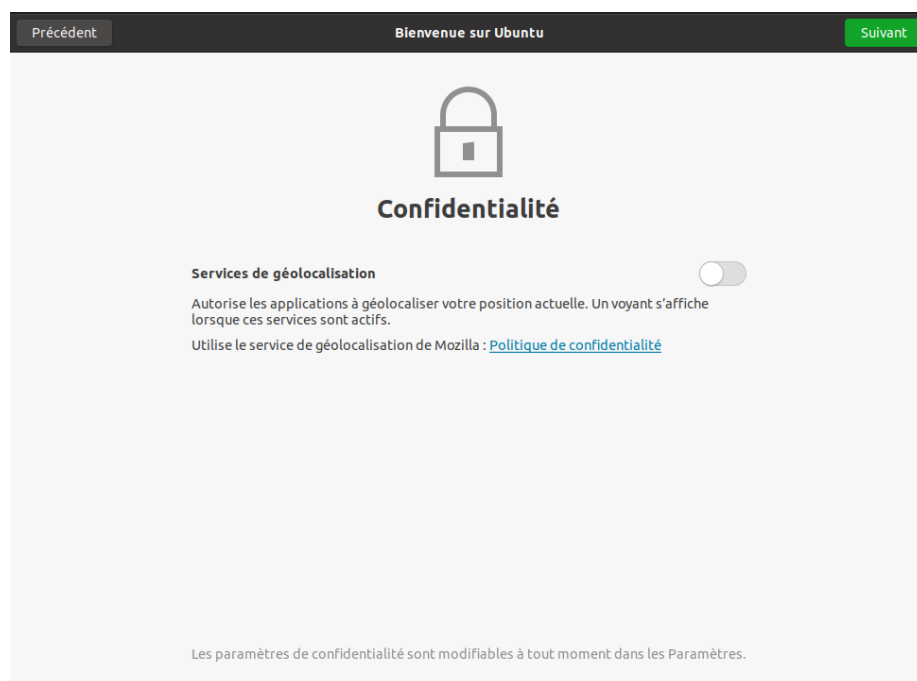


Figure 14: Autorisation de la géolocalisation.

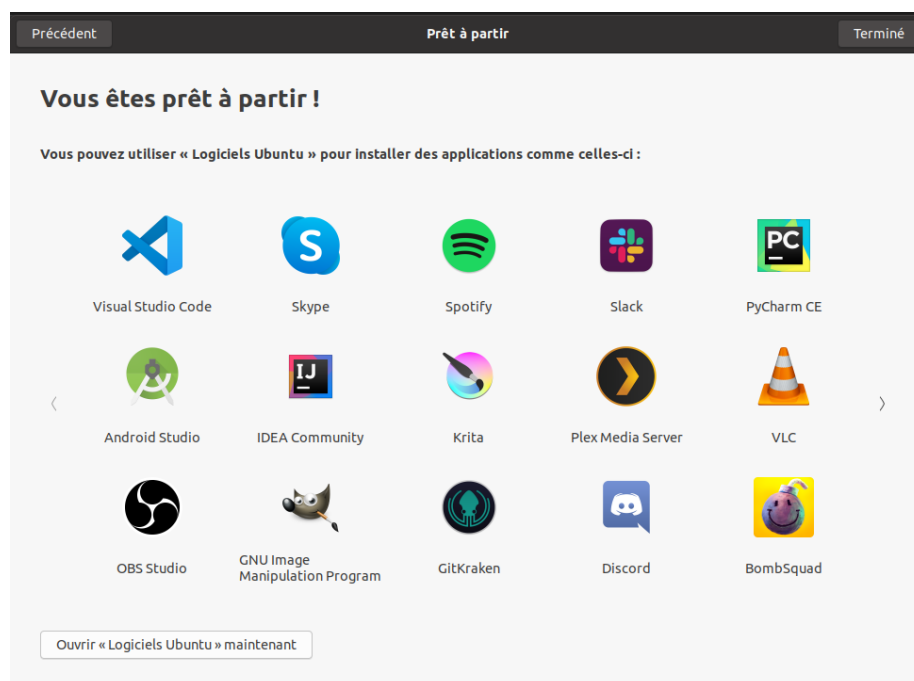


Figure 15: Fin d'installation.

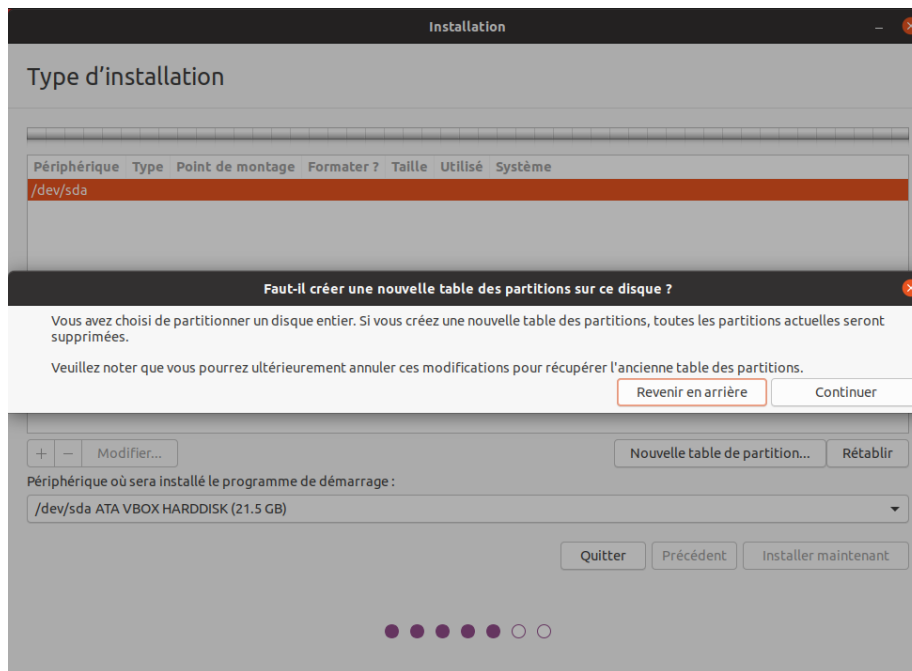


Figure 16: Création de la table de partition

Pour un serveur il vaut mieux opter pour les versions LTS (Long Term Support) des distributions.

Les différences entre "Debian server" et "Ubuntu server" sont liées aux versions du noyau et des bibliothèques utilisées, aux dépôts et fichiers de configurations par défaut.

Attention

Sous Ubuntu, il n'est pas possible de créer une partition /var, car le système y stocke des fichiers au démarrage, alors que les points de montage ne sont pas encore installés, ce qui provoque un plantage du système difficile à comprendre.

Travaux pratiques

Installation d'une Ubuntu server LTS

Utilisation de GNU/Linux

Présentation interactive du système d'exploitation:

- le bureau,
- les fenêtres d'application,

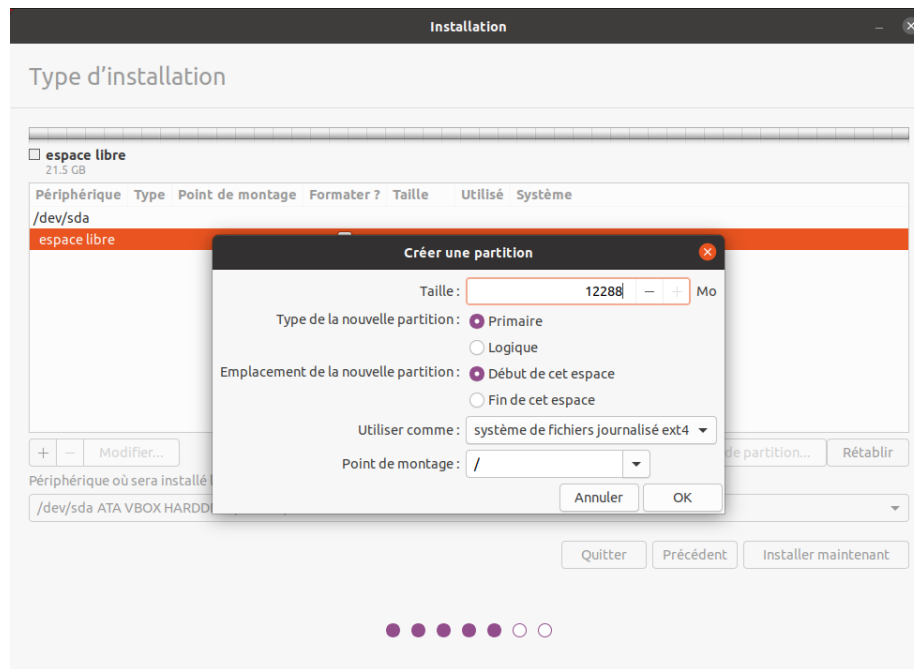


Figure 17: Création de la table de partition

- le tableau de bord.

Administration graphique du système:

- Configuration du réseau (Système (Flèche descendante de la barre de menus, à droite) > Wifi ou Filare (non) connecté ou Administration (Roue dentée) > Wifi ou Réseau)
- Synaptic (Pour l'installer <https://doc.ubuntu-fr.org/synaptic>): l'installation de logiciels (Système > Administration > Gestionnaire de paquets Synaptic)
- configuration des dépôts (Rechercher depuis le menu Activité -> Logiciels & mises à jour)
- personnalisations basiques https://doc.ubuntu-fr.org/personnalisation_basique
- la configuration de Gnome (installer gnome-tweaks)
- les applets
- la résolution graphique
- les bureaux virtuels
- les services (Système > Administration > Services)

Les logiciels d'administration ne sont que des surcouches graphiques (front-end) qui appellent les commandes en ligne, par conséquent leurs possibilités sont moindres.

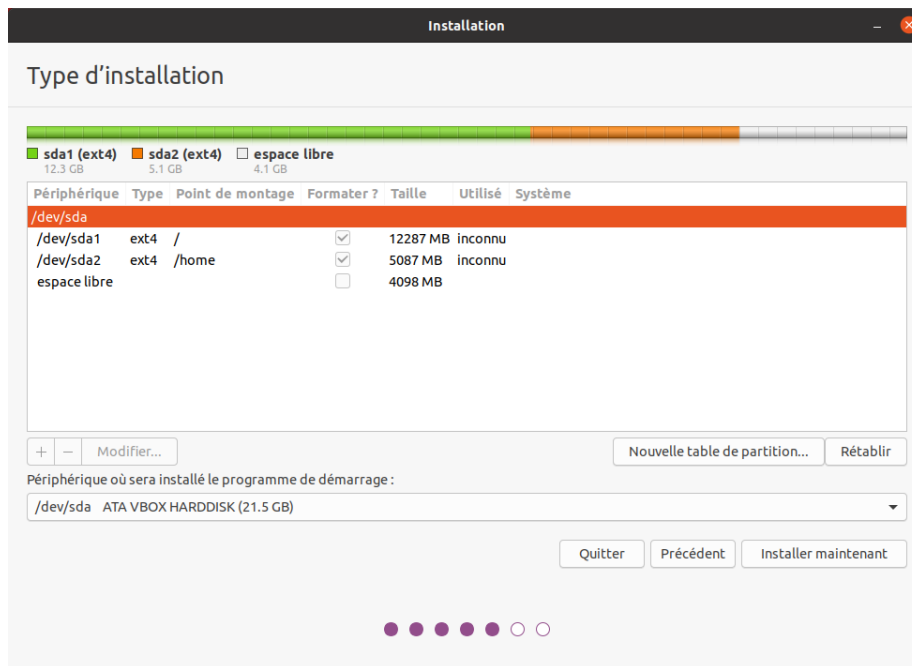


Figure 18: Création de la racine "/"

L'aide et la communauté

L'aide en ligne

En mode graphique, les applications possèdent un onglet "Aide" permettant d'ouvrir un navigateur sur l'aide en ligne. Cette aide est généralement accessible par la touche F1.

Dans un shell, la plupart des commandes unix acceptent l'option -h ou --help ou --usage :

```
michaellaunay@luciole:~$ apropos --help
Usage: apropos [OPTION...] KEYWORD...
Project-Id-Version: man-db 2.3.90
Report-Msgid-Bugs-To: Colin Watson <cjwatson@debian.org>
POT-Creation-Date: 2008-05-05 02:09+0100
PO-Revision-Date: 2008-08-19 20:37+0000
Last-Translator: Laurent Pelecq <laurent.pelecq@soleil.org>
Language-Team: French <traduc@traduc.org>
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
```

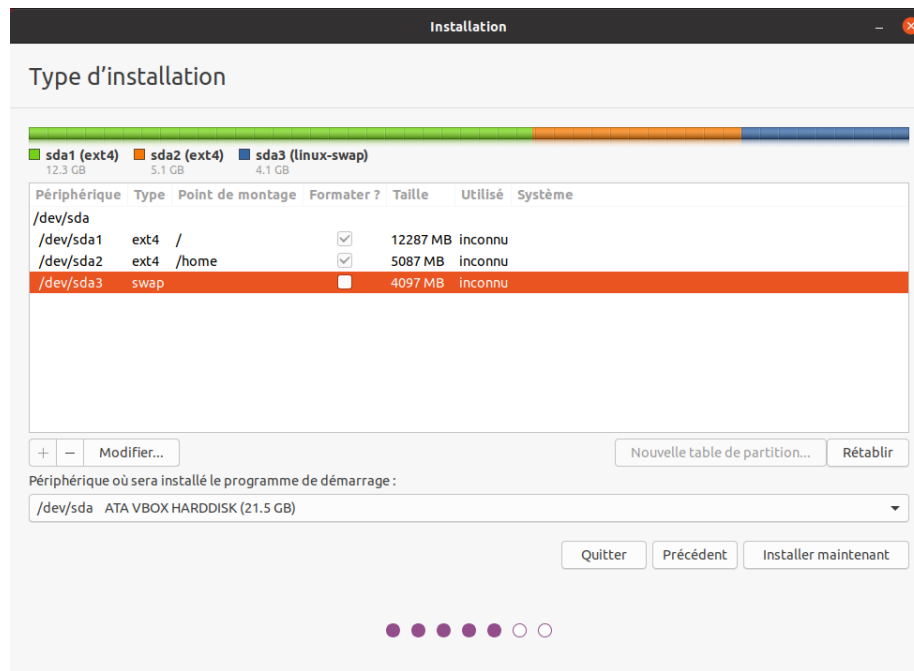


Figure 19: Création du swap

X-Launchpad-Export-Date: 2008-11-09 09:58+0000

X-Generator: Launchpad (build Unknown)

-d, --debug	emit debugging messages
-v, --verbose	print verbose warning messages
-e, --exact	search each keyword for exact match
-r, --regex	interpret each keyword as a regex
-w, --wildcard	the keyword(s) contain wildcards
-a, --and	require all keywords to match
-l, --long	do not trim output to terminal width
-C, --config-file=FICHIER	use this user configuration file
-L, --locale=LOCALE	define the locale for this search
-m, --systems=SYSTEM	use manual pages from other systems
-M, --manpath=CHEMIN	set search path for manual pages to PATH
-s, --section=SECTION	search only this section
-, --help	give this help list
-, --usage	give a short usage message
-V, --version	print program version

Mandatory or optional arguments to long options are also mandatory or optional for any corresponding short options.

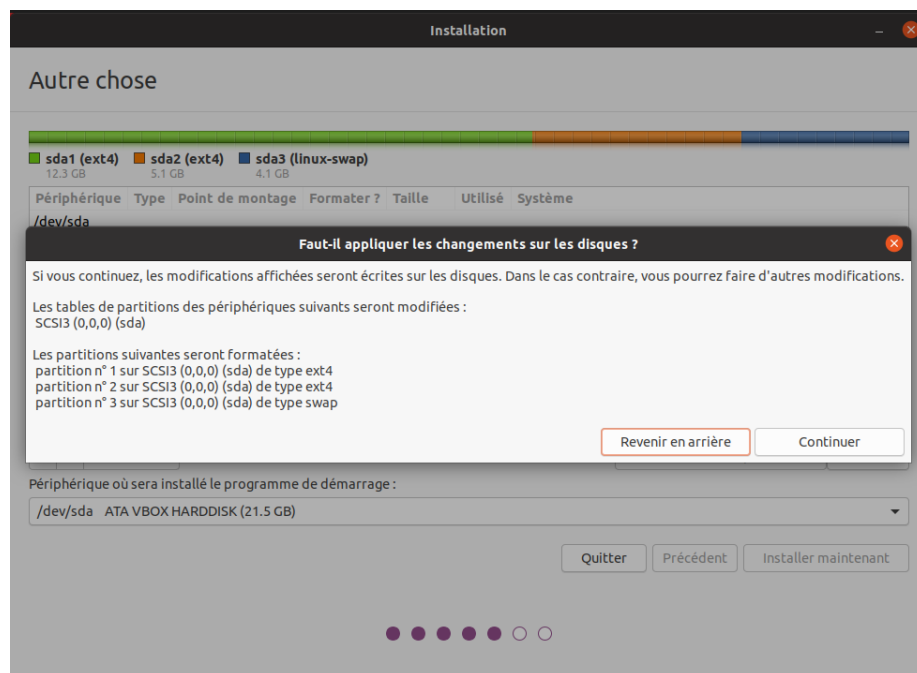


Figure 20: Création des partitions

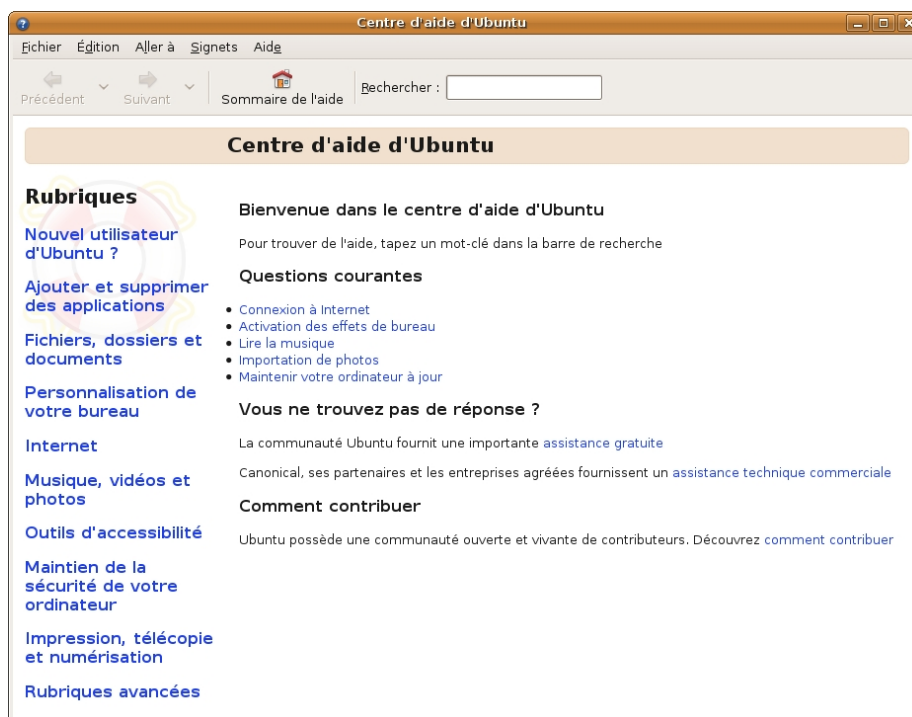


Figure 21: Aide en ligne d'Ubuntu (appelée avec F1)

The `--regex` option is enabled by default.

Report bugs to cjwatson@debian.org.

Pour trouver une commande il suffit de faire `apropos MotClé` qui affichera toutes les commandes comportant `MotClé` dans sa description courte. Toutefois la base des commandes peut avoir besoin d'être régénérée par **makewhatis**.

whatis NomDeCommande affichera la description courte de `NomDeCommande`.

Les man pages

Les applications et commandes possèdent toutes un manuel accessible en ligne de commande via la commande `man`.

Ce manuel est généralement traduit dans la langue de l'utilisateur :

```
michaellaunay@luciole:~$ man man
MAN(1)                  Utilitaires de l'afficheur des pages de manuel          MAN(1)
```

NOM

`man` - Interface de consultation des manuels de référence en ligne

SYNOPSIS

```
man [-c|-w|-tZ] [-H[navigateur]] [-T[périphérique]] [-adhu7V] [-i|-I]
[-m système[,...]] [-L langue] [-p chaîne] [-C fichier] [-M chemin]
[-P afficheur] [-r invite] [-S liste] [-e extension] [[section] page ...] ...
man -l [-7] [-tZ] [-H[navigateur]] [-T[périphérique]] [-p chaîne]
[-P afficheur] [-r invite] fichier ...
man -k [apropos options] expression_rationnelle ...
man -f [whatis options] page ...
```

DESCRIPTION

`man` est le programme de visualisation des pages de manuel. Chacun des arguments `page`, indiqué dans la ligne de commande de `man`, porte, en principe, le nom d'un programme, d'un utilitaire ou d'une fonction. La page de manuel correspondant à chaque argument est alors trouvée et affichée. Si une section est précisée alors `man` limite la recherche à cette section. Par défaut, il recherche dans toutes les sections disponibles, suivant un ordre prédéfini. Il n'affiche que la première page de manuel trouvée, même si d'autres pages de manuel existent dans d'autres sections.

Le tableau ci-dessous indique le numéro des sections de manuel ainsi que le type de pages qu'elles contiennent.

- 1 Programmes exécutables ou commandes de l'interpréteur de commandes (shell) ;

- 2 Appels système (Fonctions fournies par le noyau) ;
- 3 Appels de bibliothèque (fonctions fournies par les bibliothèques des programmes) ;
- 4 Fichiers spéciaux (situés généralement dans /dev) ;
- 5 Formats des fichiers et conventions. Par exemple /etc/passwd ;
- 6 Jeux ;
- 7 Divers (y compris les macropaquets et les conventions). Par exemple, man(7), groff(7) ;
- 8 Commandes de gestion du système (généralement réservées au superutilisateur) ;
- 9 Sous-programmes du noyau [hors standard].

Une page de manuel est constituée de plusieurs parties.

Elles peuvent être libellées NOM, SYNOPSIS, DESCRIPTION, OPTIONS, FICHIERS, VOIR AUSSI, BOGUES et AUTEUR.

Pour chercher les pages associées à un mot clé:

```
michaellaunay@luciole:~/Documents/ecreall/Cours/CoursGNULinux$ man -k manual
apropos (1)      - search the manual page names and descriptions
catman (8)      - create or update the pre-formatted manual pages
esdcompat (1)   - manual page for pulseaudio esd wrapper 0.9.5
grub-reboot (8) - manual page for grub-reboot 0.01
man (1)         - an interface to the on-line reference manuals
manconv (1)     - convert manual page from one encoding to another
mandb (8)      - create or update the manual page index caches
manpath (1)    - determine search path for manual pages
missing (7)    - missing manual pages
pulseaudio (1) - manual page for pulseaudio 0.9.5
readahead-list (8) - manual page for readahead-list: 0.20050517.0220
readahead-watch (8) - manual page for readahead-watch: 0.20050517.0220
update-apt-xapian-index (8) - manual page for update-apt-xapian-index 0.15
w3mman (1)     - an interface to the on-line reference manuals by w3m(1)
whatis (1)     - display manual page descriptions
whereis (1)    - locate the binary, source, and manual page files for a command
xman (1)       - Manual page display program for the X Window System
```

Les sites

Le site officiel de Linux <http://www.linux.org>

Un site dédié à Linux (Linux Entre Amis) : <http://www.lea-linux.org>

Une présentation de Linux <http://fr.wikipedia.org/wiki/Linux>

La communauté ubuntu française <http://www.ubuntu-fr.org/>

Les forums

Le forum de la communauté Ubuntu <http://ubuntuforums.org/>

Le forum de la communauté Debian française <http://forum.debian-fr.org>

Les LUGs

Un LUG est un groupe d'utilisateurs de Linux (Linux User Group) réuni généralement au sein d'une association loi 1901.

Dans la région lilloise on compte essentiellement Chtinux <http://www.chtinux.org/> anciennement Campux et CLX <http://clx.asso.fr/spip>

Les LUGs réalisent la promotion de Linux et des logiciels libres. Ils organisent des manifestations telles que des install party.

Shell & Commandes

Les terminaux (tty)

Historiquement, un terminal est une interface homme machine minimale issue des technologies de communication de la fin XIX et du début XX siècle, le Télétipe marque déposée en 1906 est l'ancêtre des claviers numériques des premiers ordinateurs.

L'abréviation tty de Télétipe a été utilisée pour décrire l'interface série de communication utilisée au début d'Unix. Par usage c'est le terme qui décrit l'interface de saisie et d'affichage avec l'humain. On trouve aussi l'appellation de terminal ou console.

La commande tty affiche le pseudo fichier associé à la saisie.

Dans l'environnement graphique XWindows on trouve des logiciels émulant les terminaux, on les appelle alors des terminaux virtuels (ex: xterm).

Les terminaux ne sont en charge que de la récupération des touches frappées, de leur transformation en lettre, et de l'affichage de celle-ci. L'interprétation de ce qui est saisi est dévolue au shell.

Les six premiers terminaux sont accessibles par la combinaison de touche Ctrl Alt F[1-6].

Le terminal graphique est accessible Ctrl Alt F7

La ligne de commande

Sous Unix la CLI (Command Line Interface) est la méthode privilégiée pour transmettre au système les ordres à exécuter.

Les différents shell

Le shell est un logiciel qui interprète séquentiellement les commandes saisies dans un terminal ou stockées dans un fichier (script) ou provenant d'un pseudo fichier.

La syntaxe et la sémantique de cette interprétation dépendent du shell employé.

Historiquement la première version est **sh** (1977 écrit par Stephen Bourne) qui évolua en **csh**, **ksh** et **bash** (Bourne again shell) le plus répandu.

Bash est l'interpréteur de commande par défaut des Unix libres et de Mac OS X.

Pour connaître la version de bash en cours d'utilisation:

```
michaellaunay@luciole:~$ echo $BASH
/bin/bash
michaellaunay@luciole:~$ echo $BASH_VERSION
4.3.39(1)-release
```

Pour modifier le shell par défaut associé à un utilisateur il faut modifier */etc/passwd* avec la commande **usermod -s /bin/bash login** :

```
michaellaunay@luciole:~$ grep michael /etc/passwd
michaellaunay:x:1000:1000:Michael Launay,,,:/home/michaellaunay:/bin/bash
michaellaunay@luciole:~$ sudo usermod -s /bin/sh michaellaunay
michaellaunay@luciole:~$ grep michael /etc/passwd
michaellaunay:x:1000:1000:Michael Launay,,,:/home/michaellaunay:/bin/sh
```

Pour créer un compte qui pourra se connecter sans avoir de shell (utilisation de tunnel) :

```
usermod -s /bin/false prestataire
```

Détails sur le format du fichier passwd

```
michaellaunay@luciole:~$ man 5 passwd
PASSWD(5) Formats et conversions de fich PASSWD(5)
```

NOM passwd - fichier des mots de passe

DESCRIPTION /etc/passwd contient différentes informations sur les comptes utilisateurs. Ces informations consistent en sept champs séparés par des deux-points (« : ») :

- nom de connexion de l'utilisateur (« login »)
- un mot de passe chiffré optionnel
- l'identifiant numérique de l'utilisateur
- l'identifiant numérique du groupe de l'utilisateur
- le nom complet de l'utilisateur ou un champ de commentaires

- le répertoire personnel de l'utilisateur
- l'interpréteur de commandes de l'utilisateur (optionnel)

Le champ du mot de passe chiffré peut être vide. Dans ce cas, aucun mot de passe n'est nécessaire pour s'authentifier avec le compte donné. Cependant, certaines applications qui lisent le fichier `/etc/passwd` peuvent décider de ne donner aucun accès si le mot de passe est vide. Si le mot de passe est un « x » minuscule, alors le mot de passe chiffré se trouve dans le fichier `shadow(5)` ; il doit y avoir une ligne correspondante dans le fichier `shadow`, sinon le compte de l'utilisateur n'est pas valide. Si le mot de passe est constitué d'une autre chaîne, alors il est considéré comme un mot de passe chiffré, comme indiqué dans `crypt(3)`.

Plus d'information : `man bash`

Lien : http://fr.wikipedia.org/wiki/Bourne-Again_shell

Les fichiers de ressources et de configuration de bash

Au lancement du shell celui-ci détermine s'il a été appelé de façon interactive ou pour exécuter un script ou en tant que shell de login. En fonction de la nature de son lancement, il exécutera plusieurs fichiers lui permettant de se paramétrer.

Scripts exécutés lors du lancement d'un shell interactif en ouverture de session (interactive login shell) : :

```
/etc/profile
~/.bash_profile #le ~ désigne le répertoire "home" de l'utilisateur
~/.bash_login  #si ~/.bash_profile n'existe pas
~/.profile     #si ~/.bash_login
```

Scripts exécutés lors d'un shell interactif : :

```
/etc/bash.bashrc
~/.bashrc
```

La modification de ces scripts nécessite la commande **source** pour une prise en compte immédiate dans le shell courant.

Scripts exécutés lors d'un script : :

`$BASH_ENV` #`BASH_ENV` est une variable. Si elle existe alors les scripts lancés essaient d'exécuter ce fichier.

Un petit exemple : :

```
michaellaunay@luciole:~$ echo "echo coucou" > /tmp/hello.sh #on crée un fichier hello.sh qui contient "echo coucou"
michaellaunay@luciole:~$ chmod +x /tmp/hello.sh           # on rend exécutable ce fichier
michaellaunay@luciole:~$ /tmp/hello.sh                    # on exécute ce fichier
coucou
```

```

michaellaunay@luciole:~$ echo $BASH_ENV           # on affiche le contenu de la variable BASH_ENV
michaellaunay@luciole:~$ BASH_ENV='/tmp/hello.sh' # on affecte la chaîne /tmp/hello.sh à la variable BASH_ENV
michaellaunay@luciole:~$ export BASH_ENV # maintenant BASH_ENV sera accessible à toute commande
michaellaunay@luciole:~$ echo "echo cuicui" > /tmp/oiseau.sh
michaellaunay@luciole:~$ bash /tmp/oiseau.sh # on exécute oiseau.sh avec bash, car on n'a pas de script
coucou
cuicui

```

Les variables d'environnement

Les variables d'environnement sont accessibles en consultation avec la commande

env :

```

michaellaunay@luciole:~$ env
SHELL=/bin/bash
TERM=xterm
HISTSIZE=1000
USERNAME=michaellaunay
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/home/michaellaunay
EDITOR=vim
LANG=fr_FR.UTF-8
HOME=/home/michaellaunay
LOGNAME=michaellaunay
DISPLAY=:0.0
OLDPWD=/home/michaellaunay

```

Signification des variables d'environnement :

BASH	# Le nom du fichier bash
DISPLAY	# Le numéro de serveur et de session d'affichage
EDITOR	# L'éditeur à utiliser par défaut
HISTSIZE	# La taille du fichier historique
HOSTNAME	# Le nom de la machine
HOME	# Le répertoire personnel de l'utilisateur
LANG	# La langue de l'utilisateur et l'encodage utilisé pour afficher cette langue
LOGNAME	# Le nom d'utilisateur lors de l'ouverture de la session
MAIL	# Le chemin vers la boîte mail de l'utilisateur
OLDPWD	# Le répertoire où nous étions avant le dernier cd
PATH	# Le chemin vers les exécutables
PS1	# Permet de constituer l'invite de commande
PS2	# Symbole affiché sur les lignes de commande débordant sur plusieurs lignes
PROMPT_COMMAND	# Le nom d'une commande à exécuter à chaque commande
PWD	# Le chemin actuel
SHELL	# Le shell de l'utilisateur
TERM	# Le type de terminal

USERNAME # Le nom d'utilisateur

Pour accéder au contenu d'une variable, il suffit de la référencer en la précédant de \$:

```
michaellaunay@luciole:~$ echo $HOME
/home/michaellaunay
```

Pour voir l'ensemble des définitions réalisées dans un shell (variable et fonction) il suffit de taper **set**.

Pour voir les lignes exécutées dans un script **set -x** en début de script.

Les caractères spéciaux

Les caractères suivants permettent de déclencher des comportements particuliers qui seront expliqués ci-après :

```
# # Mise en commentaire
> # Indirection vers un fichier
< # Indirection depuis un fichier
| # Pipe
? # Un caractère ou pas
. # Un caractère
* # Une chaîne de caractère
$ # Référencement d'une variable
\ # Échappement
/ # Séparateur
[ # Début d'un ensemble ou d'un test
] # Fin d'un ensemble ou d'un test
( # Sous shell ou évaluation
) # Fin de sous shell ou d'évaluation
: # Séparateur de groupe
; # Fin de commande
^ # Inversion ou début
@ # Adresse
` # Début ou fin d'interprétation
~ # Désigne le répertoire personnel
```

Si vous voulez les utiliser pour nommer par exemple un fichier sans que le comportement particulier soit déclenché vous avez l'obligation de les échapper avec **** ou de les mettre entre apostrophes**** ou guillemets ":

```
\# ou '#' ou "#"
\> ou '>' ou ">"
\< ou '<' ou "<"
\\ ou '|' ou "|"
\? ou '?' ou "?"
\. ou '.' ou "."
```



```

\* ou '*' ou "*"
\$ ou '$' ou "$"
\\ ou '\' ou "\"
\/ ou '/' ou "/"
\[ ou '[' ou "["
\] ou ']' ou "]"
\( ou '(' ou "("
\) ou ')' ou ")"
\: ou ':' ou ":"
\; ou ';' ou ";"
\^ ou '^' ou "^"

```

exemple :

```

michaellaunay@luciole:~$ echo lunettes > /tmp/\[\*\]\^\["''']
michaellaunay@luciole:~$ ls /tmp
[*]^[*]
michaellaunay@luciole:~$ cat /tmp/\[\*\]\^\[\*\]
lunettes

```

Variables spéciales

En plus des variables d'environnement vue précédemment nous avons :

```

$? # Qui fait référence au code de retour de la dernière commande exécuté.
$$ # Le pid du programme en cours d'exécution.
$! # Le pid de la dernière commande lancée en tâche de fond.
## # Le nombre de paramètres.
$0 # Le nom du programme en cours d'exécution.
$1 # Le premier paramètre passé.
$2 # Le second paramètre passé.
...
$9 # Le neuvième paramètre.
$, $@ # L'ensemble des paramètres

```

Création, affectation de variable

Pour créer une variable ou en modifier sa valeur il suffit de la définir :

```

michaellaunay@luciole:~$ VAR='Bonjour tout le monde'
michaellaunay@luciole:~$ echo $VAR
Bonjour tout le monde
michaellaunay@luciole:~$ VAR=Salut
michaellaunay@luciole:~$ echo $VAR
Salut
michaellaunay@luciole:~$ VAR=$VAR' à tous'
michaellaunay@luciole:~$ echo $VAR
Salut à tous

```

```
michaellaunay@luciole:~$ PATH=/home/michaellaunay/MesScripts:$PATH
michaellaunay@luciole:~$ echo $PATH
/home/michaellaunay/MesScripts:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

Pour supprimer une variable, on peut utiliser unset : :

michaellaunay@luciole:~$ unset BASH_ENV
```

Export de variable

Toute variable créée dans un shell n'est accessible que dans celui-ci.

Pour la rendre accessible aux commandes et scripts appelés après l'affectation il faut l'exporter : :

```
michaellaunay@luciole:~$ echo "echo \"\$SALUTATION\" > /tmp/cmd.sh"
michaellaunay@luciole:~$ /tmp/cmd.sh
```

```
michaellaunay@luciole:~$ SALUTATION=coucou
michaellaunay@luciole:~$ echo $SALUTATION
coucou
michaellaunay@luciole:~$ /tmp/cmd.sh
```

```
michaellaunay@luciole:~$ export SALUTATION
michaellaunay@luciole:~$ /tmp/cmd.sh
coucou
```

Les tests d'expressions et fichier, opérateurs de contrôle

La commande **test** permet de tester une expression et de retourner 0 si le test est vrai et 1 s'il est faux : :

```
michaellaunay@luciole:~$ test 1 = 1
michaellaunay@luciole:~$ echo $?
0
michaellaunay@luciole:~$ test 1 = 2
michaellaunay@luciole:~$ echo $?
1
```

On peut aussi remplacer **test** par des crochets, mais il faut alors encadrer les crochets par des espaces : :

```
michaellaunay@luciole:~$ [ 1 = 2 ]
michaellaunay@luciole:~$ echo $?
1
```

Les options de test sont très nombreuses. Faites man test.

Avec **test** et **if** il est possible d'exécuter conditionnellement des commandes : :

```
michaellaunay@luciole:~$ VAR=2
```

```

michaellaunay@luciole:~$ if [ $VAR = 2 ]; then echo Vrai; else echo Faux;fi
Vrai
michaellaunay@luciole:~$ VAR=$HOME
michaellaunay@luciole:~$ if [ -w $VAR ]
> then echo écriture possible dans $VAR
> else echo écriture impossible dans $VAR
> fi
écriture possible dans /home/michaellaunay

```

Exécution d'opérations arithmétiques

La construction `$[nombre1 opérateur nombre2]` permet de réaliser le calcul d'expression sur des entiers :

```

michaellaunay@luciole:~$ echo $[ 10 - 1 ]
9

```

La création de variable et sa modification :

```

michaellaunay@luciole:~$ CMPT=[0] # équivalent à la ligne suivante
michaellaunay@luciole:~$ let CMPT=0
michaellaunay@luciole:~$ echo $CMPT
0
michaellaunay@luciole:~$ let CMPT+=1
michaellaunay@luciole:~$ echo $CMPT
1
michaellaunay@luciole:~$ let CMPT+=1
michaellaunay@luciole:~$ echo $CMPT
2

```

La boucle while et until

While permet d'exécuter des commandes tant que la condition est satisfaite alors que **until** exécute des commandes tant que la condition échoue.

Exemple :

```

michaellaunay@luciole:~$ VAR=4
michaellaunay@luciole:~$ while [ $VAR -gt 0 ]
> do
> echo itération $VAR;
> VAR=$[ $VAR - 1 ]
> done
itération 4
itération 3
itération 2
itération 1

```

La boucle for

Pour chaque élément d'un ensemble, on exécute une commande :

```
michaellaunay@luciole:~$ NORD="Lille Roubaix"
michaellaunay@luciole:~$ CENTRE="Paris Chartres"
michaellaunay@luciole:~$ SUD="Nice Marseille"
michaellaunay@luciole:~$ for ville in $NORD $CENTRE $SUD
> do
> echo Visiter $ville
> done
Visiter Lille
Visiter Roubaix
Visiter Paris
Visiter Chartres
Visiter Nice
Visiter Marseille
```

Le choix multiple (case)

Permet de réaliser un branchement. Ne pas oublier les deux points-virgules à la fin d'un cas :

```
michaellaunay@luciole:~$ VAR=Lille
michaellaunay@luciole:~$ case $VAR in
> 'lille' | 'Lille' | 'LILLE' )
>   echo J\'y habite
> ;;
> 'paris' | 'Paris' | 'PARIS' )
>   echo J\'y ai habité
> ;;
> * )
>   echo Je ne connais pas
> ;;
> esac
J'y habite
```

Les opérateurs && et ||

L'opérateur && permet d'exécuter la commande suivante si la commande précédente réussit (retourne 0) :

```
michaellaunay@luciole:~$ grep refusée /var/log/user.log > /tmp/connexion.txt && vim /tmp/connexion.txt
```

L'opérateur || permet d'exécuter la commande suivante si la commande précédente a échoué (retour de 1) :

```
michaellaunay@luciole:~$ grep refusée /var/log/user.log > /dev/null || echo tout va bien
```

La commande trap

Elle permet de positionner une fonction qui sera exécuté lors de la réception d'un signal (man 7 signal) :

```
trap "echo Fin d\'exécution" EXIT
trap "echo Interruption violente Ctrl-c" SIGINT
trap "echo Fin demandée" SIGTERM
trap "echo Reprise d\'exécution" SIGCONT
trap "echo SignalUSR" SIGUSR1 SIGUSR2
```

La commande sed

Elle permet de faire des traitements sur les lignes d'un flux. Par exemple elle permet de trouver un motif et de le remplacer. On la rencontre dans de nombreux scripts.

Par exemple dans la ligne suivante :

```
ls -l | xargs -i echo mv {} {} | sed -e "s/Ubuntu20.04_//2" | bash
```

"ls -l" affiche le contenu du répertoire courant, une ligne par fichier.

Le résultat est envoyé à **xargs** qui pour chaque ligne va créer une chaîne de caractères "mv contenu_ligne contenu_ligne"

Le résultat est envoyé à **sed** qui supprime la seconde occurrence de la chaîne "Ubuntu20.04" qu'il rencontre.

Le résultat est exécuté par bash en transformant la chaîne de caractères reçu en ligne de commande.

Ici sed permet de renommer les fichiers de type Ubuntu20.04_00_EssayerOuInstaller.png en 00_EssayerOuInstaller.png.

À cette ligne complexe, on préférera renommer de façon plus élégante et rapide avec la ligne de cmd :

```
for filename in *; do mv $filename ${filename/Ubuntu20.04_/}; done
```

Pour plus d'information sur **sed** voir <https://www.commentcamarche.net/faq/9536-sed-introduction-a-sed-part-i>

L'expansion de paramètre

Liste des Filtres pour l'expansion de paramètre du Shell https://www.gnu.org/software/bash/manual/html_node/Shell-Parameter-Expansion.html :

\${parameter} sera remplacé par la valeur de parameter

michaellaunay@luciole:~\$ CMPT=\$((1 + 20 / 2)) # Réalise l'opération puis affecte CMPT pour

michaellaunay@luciole:~\$ echo \${CMPT}

11

michaellaunay@luciole:~\$ name[1]='un' # équivalent à 'declare -n name' voir <https://www.gnu.org>

```

michaellaunay@luciole:~$ name[2]='deux'
michaellaunay@luciole:~$ name[3]='trois'
michaellaunay@luciole:~$ echo ${name[2]}
deux
# équivalent à
michaellaunay@luciole:~$ name=('zero' 'un' 'deux' 'trois')
michaellaunay@luciole:~$ echo ${name[1]}
un
michaellaunay@luciole:~$ unset name[0]
michaellaunay@luciole:~$ echo ${name[0]}

michaellaunay@luciole:~$ echo ${name[1]}
un

```

Les scripts

Un script est un fichier qui contient une suite de commandes.

La première ligne permet d'indiquer le shell dans lequel doit être exécuté le script :

```

#!/bin/bash
echo c'est du bash

```

Cette ligne s'appelle le shebang.

Les fonctions

Une fonction est une portion de code nommée, réutilisable qui a accès à toutes les variables du script ou du shell d'où elle est appelée :

```

michaellaunay@luciole:~$ function carré() {
> echo $[ $1 * $1]
> }
michaellaunay@luciole:~$ carré 3
9

```

Lecture des saisies clavier

La commande **read** permet de lire la saisie clavier et de l'affecter avec une variable :

```

michaellaunay@luciole:~$ read VAR
coucou
michaellaunay@luciole:~$ echo $VAR
coucou

```

Exercice

Réalisez une calculatrice demandant la saisie de la première opérande puis de l'opérateur (symbole ou littéral), puis de la seconde opérande. Affichez le résultat puis exécutez à nouveau tant que le signal SIGUSR1 n'est pas reçu.

Les sous-programmes

Dans un shell on peut appeler un script directement en passant son nom si celui-ci est exécutable ou en le faisant interpréter par le shell pour lequel il a été écrit.

Lorsqu'on exécute un ensemble de commandes encadré par des parenthèses alors le shell courant démarre un sous shell pour exécuter les commandes :

```
michaellaunay@luciole:~$ VAR=0
michaellaunay@luciole:~$ (VAR=$(( $VAR + 1 )); echo $VAR)
1
michaellaunay@luciole:~$ echo $VAR
0
```

Il est également possible de forcer l'exécution de commande en utilisant ' : :

```
michaellaunay@luciole:~$ echo date
date
michaellaunay@luciole:~$ echo `date`
dimanche 19 avril 2020, 17:24:32 (UTC+0200)
```

La complétion de commande

En appuyant sur la touche tab le shell affiche toutes les commandes ayant pour préfixe les lettres déjà saisies sur la ligne de commande.

Historique des commandes

Les commandes saisies dans un shell sont enregistrées dans le fichier ~/.bash_history

Il est possible d'accéder aux anciennes commandes en utilisant les flèches.

Les commandes

Se déplacer dans l'arborescence

Les commandes :

```
ls          # Permet d'afficher les informations d'un fichier ou d'un répertoire
ls UnChemin # Affiche le contenu de UnChemin si c'est un répertoire, sinon affiche le nom de
ls -lah     # Affiche les détails, les fichiers cachés, et utilise des unités informatiques
ls -F       # Affiche un / derrière le nom des répertoires
info ls     # Permet de connaître le sens des colonnes des options de ls, par exemple le chiff
```

```
cd          # Permet de déplacer le répertoire courant
pwd         # Affiche le chemin du répertoire courant
```

exemple :

```
michaellaunay@luciole:~$ ls -lh /
total 2,1G
drwxr-xr-x  2 root root 12K avril 19 16:40 bin
drwxr-xr-x  4 root root 4,0K avril  8 06:51 boot
drwxr-xr-x  2 root root 4,0K mai 16 2019 cdrom
drwxr-xr-x 19 root root 4,6K avril 18 22:11 dev
drwxr-xr-x 158 root root 12K avril 15 06:43 etc
drwxr-xr-x  5 root root 4,0K août 22 2019 home
lrwxrwxrwx  1 root root 32 janv.  6 18:48 initrd.img -> boot/initrd.img-5.0.0-38-generic
lrwxrwxrwx  1 root root 32 janv.  6 18:48 initrd.img.old -> boot/initrd.img-5.0.0-37-generic
drwxr-xr-x 21 root root 4,0K mars  5 06:28 lib
drwxr-xr-x  2 root root 4,0K mars  5 06:28 lib32
drwxr-xr-x  2 root root 4,0K mars  5 06:28 lib64
drwx-----  2 root root 16K mai 16 2019 lost+found
drwxr-xr-x  3 root root 4,0K juin 24 2019 media
drwxr-xr-x  2 root root 4,0K févr. 10 2019 mnt
drwxr-xr-x  5 root root 4,0K août 26 2019 opt
dr-xr-xr-x 354 root root  0 avril 18 22:11 proc
drwx-----  8 root root 4,0K mars 25 10:16 root
drwxr-xr-x 39 root root 1,1K avril 19 10:15 run
drwxr-xr-x  2 root root 12K avril 19 16:40 sbin
drwxr-xr-x 17 root root 4,0K mars 22 22:44 snap
drwxr-xr-x  2 root root 4,0K févr. 10 2019 srv
-rw-----  1 root root 2,0G mai 16 2019 swapfile
dr-xr-xr-x 13 root root  0 avril 18 22:11 sys
drwxrwxrwt 24 root root 4,0K avril 19 17:20 tmp
drwxr-xr-x 14 root root 4,0K août  1 2019 usr
drwxr-xr-x 15 root root 4,0K juin 17 2019 var
lrwxrwxrwx  1 root root 29 janv.  6 18:48 vmlinuz -> boot/vmlinuz-5.0.0-38-generic
lrwxrwxrwx  1 root root 29 janv.  6 18:48 vmlinuz.old -> boot/vmlinuz-5.0.0-37-generic
```

```
michaellaunay@luciole:~/Documents/ecreall/Cours$ cd
michaellaunay@luciole:~$ pwd
/home/michaellaunay
```

Les jokers :

```
* # Désigne toute chaîne contiguë de caractères
? # Désigne un caractère
[...] # Permet de désigner des ensembles de caractères [4-69] accepte 4, 5, 6, et 9, [[] accepte
[^...] # Permet de désigner des ensembles à exclure
```


Un **chemin relatif** est un chemin qui permet de se déplacer jusqu'au fichier cible à partir du chemin courant :

```
michaellaunay@luciole:~$ cd ~ # identique à cd $HOME ou cd
michaellaunay@luciole:~$ ls -l ../../etc/passwd
-rw-r--r-- 1 root root 1583 2009-04-02 11:35 ../../etc/passwd
```

. indique le répertoire courant alors que .. indique le parent.

Un **chemin absolu** est un chemin qui commence à la racine / de l'arborescence et énonce tous les sous-répertoires jusqu'à la cible :

```
michaellaunay@luciole:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 1583 2009-04-02 11:35 /etc/passwd
```

Création / suppression de répertoire

La commande **mkdir** permet de créer des répertoires :

```
mkdir NomRep # Crée le répertoire NomRep.
mkdir -p Rep1/Rep2/Rep3 # Crée Rep3 et l'arborescence Rep1/Rep2 si nécessaire.
```

La commande **rmdir** permet de supprimer un répertoire vide, on peut aussi le faire avec **rm -r** dans le cas d'un répertoire non vide.

Lecture de fichier

La commande **cat** permet d'afficher le contenu d'un fichier.

La commande **strings** permet de n'afficher que les chaînes de caractères d'un fichier binaire.

Rechercher des fichiers

La commande **find** permet de réaliser des recherches basées sur les informations d'un fichier (nom, date de création, de modification etc.) :

```
michaellaunay@luciole:~$ find Documents/ecreall -name "*.pdf" -ctime -2
# recherche à partir de Documents/ecreall tous les fichiers finissant par pdf, créés depuis
Documents/ecreall/Cours/CoursGNULinux/CoursGNULinux.pdf
```

La commande **grep** permet de réaliser des recherches basées sur la présence d'une chaîne ou d'une expression régulière dans le contenu d'un fichier.

La commande **locate** permet de trouver un fichier si le chemin a été renseigné dans la base de données mise à jour par le super utilisateur avec **updatedb** ou **slocate -u**.

Archivage / Compression

zip, **unzip** permet de compresser et décompresser les fichiers aux format zip

gzip permet de compresser et décompresser les fichiers au format gzip

tar avec les options **cf** permet d'archiver une arborescence en conservant les informations de propriétaire, les dates de création, les permissions d'accès. Avec les options **xf**, permet d'extraire une archive.

tar cfz permet de combiner **tar** et **gzip** en une commande. L'option **--listed-incremental=nom_fichier.list** permet d'enregistrer un snapshot des fichiers archivés en vue de permettre des tar incrémentaux. C.f. https://doc.ubuntu-fr.org/tar#utilisation_en_archivage_incrementiel Attention il est indispensable que la première archive soit lancée avec cette option pour que l'incrémental soit possible !

Autres commandes

mv permet de déplacer un fichier ou une arborescence.

tail permet de n'afficher que les dernières lignes d'un fichier, l'option **-f** permet d'afficher le contenu au fur et à mesure de son arrivé dans le flux.

tee permet d'écrire le contenu de la sortie standard dans un fichier tout en laissant ce contenu dans la sortie standard ce qui permet dans un pipe d'avoir une capture du contenu sans casser le pipe.

ln permet de créer des liens. Ainsi **ln -s Source Destination** permet de créer un lien symbolique.

cp permet de copier un fichier dans un autre. **cp -r Rep1 Rep2** copie toute l'arborescence Rep1 vers Rep2.

script NOM_Fichier permet d'enregistrer la session (les interactions en ligne de commande) vers un fichier, ce qui permet de l'auditer voire de la rejouer. L'option **-t** permet d'enregistrer les dates des échanges vers le flux d'erreur. L'enregistrement sera arrêté par la commande **exit**. **scriptreplay** Permet de rejouer la session. Exemple : **NOM='date +%y%m%d%H%M%S'_upgrade_jessie;script -t 2>~/\$NOM.time -a ~/\$NOM.script**

Les noms de fichiers

Linux est sensible à la casse (majuscules vs minuscules).

Depuis 2007, l'ensemble du système utilise utf-8 comme encodage par défaut, en conséquence tous les caractères accentués peuvent être utilisés pour nommer les fichiers.

Les caractères spéciaux et les espaces peuvent être utilisés à la condition d'être échappés.

La taille des noms ne doit pas excéder 255 octets.

Si l'on utilise des caractères accentués ou asiatiques, le nombre de caractères maximal est inférieur à 255, car il faut 2 à 4 octets pour représenter un caractère autre que ASCII en utf-8.

Tout fichier ou répertoire commençant par un `.` sera caché et accessible uniquement avec l'option `-a` de `ls`.

Les attributs des fichiers

Les attributs de fichier permettent de gérer les permissions d'accès en lecture, écriture, exécution, traversée et également de connaître la nature du fichier.

Ainsi :

```
michaellaunay@luciole:~/Documents/ecreall/Cours$ ls -lh
total 24K
lrwxrwxrwx  1 michaellaunay users  11 2009-03-01 21:23 unLienSymbolique -> unFichier
drwxr-x--- 139 michaellaunay users 12K 2009-04-30 09:12 unSousRep
drwx-----  2 michaellaunay michaellaunay 16K 2009-03-01 21:21 lost+found
-rw-r-----  1 michaellaunay amis  32K 2009-04-02 11:35 unFichier
michaellaunay@luciole:~/Documents/ecreall/Cours/CoursGNUlinux$ ls -l /bin/mount
-rwsr-xr-x 1 root root 98440 2008-09-25 15:08 /bin/mount
michaellaunay@luciole:~/Documents/ecreall/Cours/CoursGNUlinux$ ls -l
drwxrwxrwt 19 root root 4096 2009-05-03 11:10 tmp
```

lrwxrwxrwx 1 michaellaunay users 11 2009-03-01 21:23 est la liste des attributs qui doit être décomposée comme ceci :

première lettre :

- `l` indique que le fichier est un lien symbolique (un raccourci).
- `d` indique que le fichier est un répertoire
- `-` indique que le fichier est un fichier ordinaire
- `c` périphérique de type caractère
- `b` périphérique de type bloc
- `s` socket
- `p` fifo

premier groupe de 3 lettres :

- `r--` indique que le propriétaire a le droit de lecture
- `-w-` indique que le propriétaire a le droit d'écriture
- `--x` indique que le propriétaire a le droit d'exécuter si le fichier est ordinaire
- `-` indique que le propriétaire a le droit de traverser si le fichier est un répertoire
- `--s` (SUID) indique qu'un utilisateur qui exécute le fichier usurpe les droits du propriétaire pour tous les accès effectués par l'exécutable.
- Le propriétaire a les droits d'exécuter ou de traverser (`--x` est positionné mais est `-`)
- `--S` (SUID) indique qu'un utilisateur qui exécute le fichier usurpe les droits du propriétaire
- Le propriétaire n'a pas les droits d'exécuter ou de traverser (`--x` n'est pas positionné)

second groupe de 3 lettres :

même signification que précédemment, mais pour les groupes et sauf pour le SUID.

--s (SGID) indique qu'un utilisateur appartenant au groupe qui exécute le fichier usurpe les droits du groupe et que le groupe a les droits d'exécution.

--S (SGID) indique qu'un utilisateur appartenant au groupe qui exécute le fichier usurpe les droits du groupe mais que le groupe n'a pas les droits d'exécuter ou de traverser.

troisième groupe de 3 lettres :

même signification que précédemment, mais pour tous les autres utilisateurs et sauf SGID

--t (Sticky bit) Indique que les utilisateurs ont le droit de modifier le contenu du fichier ou du répertoire, mais pas de le supprimer.

Les utilisateurs ont le droit d'exécution ou de traverser.

--T (Sticky bit) Idem mais les utilisateurs n'ont pas le droit d'exécuter ou de traverser.

Le fichier unFichier a pour propriétaire *michaellaunay* (owner) et pour groupe *amis* (owning group).

Les notions de permission et de groupe seront détaillées ci-après.

La taille du fichier unFichier est de 32ko.

La date est celle de dernière modification. La date du dernier accès est accessible avec la commande **ls -u -l**.

Les permissions d'un lien ne sont pas utilisées, car ceux sont celles de la cible qui sont vérifiées.

Si les permissions sont suivies d'un + alors des ACL sont positionnées.

Les types de fichiers

Outre les fichiers normaux, les répertoires et les liens, il existe de nombreux fichiers spéciaux sous Unix.

En effet la philosophie d'Unix est de vouloir que tout soit fichier : :

Les périphériques sont manipulés comme s'ils étaient des fichiers.

Les piles (fifo, lifo), les pipes nommées, sockets sont manipulés comme des fichiers.

Les caractéristiques du système sont traduites à travers une arborescence.

Le noyau lui-même est adressé à travers une arborescence qui permet de connaître son état et

Les processus sont eux même manipulés à travers une arborescence de fichiers.

/dev

Contient les fichiers de périphériques physiques ou virtuels : :

/dev/sda # Premier disk scsi ou sata ou usb

/dev/sda1 # Première partition de /dev/sda

/dev/sdb # Second périphérique scsi ou sata ou usb

/dev/cdrom # Lien vers le périphérique gérant le cdrom

/dev/null # Utile pour se débarrasser du contenu d'un flux

```
/dev/zero # Générateur d'octet nul
/dev/random # Générateur aléatoire
```

Exemple:

```
michaellaunay@luciole:~$ find /usr -name "*.pdf" 2> /dev/null
/usr/share/doc/shared-mime-info/shared-mime-info-spec.pdf
/usr/share/example-content/case_ubuntu_johnshopkins_v2.pdf
/usr/share/example-content/case_howard_county_library.pdf
/usr/share/example-content/case_oxford_archaeology.pdf
/usr/share/example-content/case_ubuntu_locatrix_v1.pdf
/usr/share/example-content/case_Skegness.pdf
/usr/share/example-content/case_Contact.pdf
/usr/share/example-content/case_OaklandUniversity.pdf
/usr/share/example-content/case_KRUU.pdf
/usr/share/example-content/case_Wellcome.pdf
/usr/share/evolution/2.24/help/quickref/fr/quickref.pdf
/usr/share/gnome/help/system-admin-guide/C/system-admin-guide.pdf
/usr/share/gnome/help/gnome-access-guide/C/gnome-access-guide.pdf
/usr/share/gnome/help/user-guide/C/user-guide.pdf
```

Dans ce cas tous les messages d'erreur ont été envoyés à la poubelle.

/sys

sysfs est une arborescence virtuelle résidant en mémoire qui exporte des informations sur les périphériques.

Cette arborescence offre plusieurs types de classement, une même information peut donc être trouvée de différente manière.

Les commandes telles que **lsusb** ou **lspci** vont chercher les informations dont elles ont besoin dans cette arborescence.

/sys/class/ montre les périphériques regroupés en classes :

```
michaellaunay@luciole:~$ ls /sys/class/
atm          firmware    ieee1394_protocol  pci_bus      scsi_disk    usb_host
backlight    gpio        ieee80211          pcmcia_socket scsi_generic  vc
bdi          graphics    input              power_supply  scsi_host     video_output
block        hidraw      leds               ppdev         sound         vtconsole
bluetooth    hwmon       mem                printer       spi_master
dma          ieee1394    misc               rfkill        thermal
dmi          ieee1394_host mmc_host           rtc           tty
drm          ieee1394_node net               scsi_device   usb_endpoint
```

```
michaellaunay@luciole:~$ cat /sys/class/thermal/cooling_device0/type
Processor
```

```
michaellaunay@luciole:~$ cat /sys/class/thermal/cooling_device0/cur_state
```

0

/proc

procfs est une arborescence virtuelle résidant en mémoire qui exporte des informations sur le noyau.

C'est dans cette arborescence que des commandes comme **ps** vont chercher des informations sur les processus.

Exemple :

```
michaellaunay@luciole:~$ cat /proc/cpuinfo
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 15
model name : Intel(R) Core(TM)2 Duo CPU L7500 @ 1.60GHz
stepping : 11
cpu MHz : 800.000
cache size : 4096 KB
physical id : 0
siblings : 2
core id : 0
cpu cores : 2
apicid : 0
initial apicid : 0
fpu : yes
fpu_exception : yes
cpuid level : 10
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
      mmx fxsr sse sse2 ss ht tm pbe syscall nx lm constant_tsc arch_perfmon pebs bts re
      nopl pni monitor ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm ida
bogomips : 3191.95
clflush size : 64
cache_alignment : 64
address sizes : 36 bits physical, 48 bits virtual
power management:
```

/proc permet en tant que root et selon l'état du processus observé d'analyser ses ressources et sa mémoire.

Ainsi il est possible de récupérer le contenu de la mémoire du processus arrêté. Voir <https://unix.stackexchange.com/questions/6301/how-do-i-read-from-proc-pid-mem-under-linux> et <https://unix.stackexchange.com/questions/6267/how-to-re-load-all-running-applications-from-swap-space-into-ram/6271#6271>

Enchaînement et parallélisation des commandes

Toute commande doit être vue comme une boîte noire ayant une entrée standard (stdin), une sortie standard (stdout) et une sortie d'erreur standard qui permet aussi d'afficher des informations (stderr).

Par défaut l'entrée standard est la saisie clavier et les sorties sont l'écran.

Les flux standards

Les flux standards stdin, stdout et stderr sont numérotés respectivement 0, 1 et 2.

En conséquence on peut utiliser ces numéros pour les désigner lors des redirections.

Input, Output

La notion d'input (entrée) et d'output (sortie) est relative à la commande, ainsi dans un pipe entre deux commandes l'entrée de la seconde commande et en fait la sortie de la première. Le système crée un flux entre les deux commandes nourri par la première et consommé par la seconde.

Les redirections

Les redirections vont permettre d'indiquer que faire des entrées et sorties standards.

Les redirections de fichier :

```
>, 1> # Stocke la sortie standard dans un fichier
2>    # Stocke la sortie des erreurs dans un fichier
&>    # Stocke les sorties dans un seul fichier
>&    # Idem
>>    # Concatène la sortie standard à la fin d'un fichier
<     # Utilise un fichier en entrée
|     # pipe, décrit ci-après
```

Les pipes

Le pipe permet d'enchaîner les commandes, l'entrée d'une commande est alors le résultat de la commande précédente.

L'intérêt est de pouvoir créer des comportements complexes à partir de commandes simples. Cette association peut à son tour être manipulée comme une boîte noire et être insérée dans un pipe plus complexe.

Exemple:

```
netstat -anp |grep 'tcp\|udp' | awk '{print $5}' | sed s/::ffff:// | cut -d: -f1 | sort | un
```

Les alias

La commande intégrée **alias** permet de redéfinir des commandes :

```
alias rm="echo 'ça va couper' && rm"
```

La commande **unalias** supprime les alias.

screen

La commande **screen** est un multiplexeur de terminaux il permet de gérer plusieurs shell et de se déconnecter sans tuer les shell dont les commandes ne sont pas encore finies.

L'intérêt est de pouvoir réaliser des tâches d'administration longues sans devoir rester connecté, ou si le réseau n'est pas fiable de ne pas perdre le travail accompli en reprenant là où la connexion s'est rompue.

Les options de bases :

```
michaellaunay@luciole:~$ screen -dmS Nom
michaellaunay@luciole:~$ screen -r Nom # Permet de se rattacher au terminal Nom
# Pour se détacher Ctrl-a Ctrl-d
# Pour un nouveau Ctrl-a Ctrl-c
# Pour passer de l'un à l'autre : Ctrl-a Ctrl-n
# man screen
```

ssh

La commande **ssh** permet de se connecter à distance sur une machine Unix ceci de façon chiffrée. Elle permet aussi d'ouvrir des tunnels chiffrés.

L'ouverture d'un tunnel entre 2 machines est de la forme :

```
ssh -L ${PORT_SOURCE}:${nom_machine_dest}:${PORT_DEST} ${USER}@${DEST}
```

où `${PORT_SOURCE}` est le numéro de port d'entrée du tunnel sur la machine où l'on est, `${nom_machine_dest}` est soit localhost soit le nom de la machine destination soit une adresse du réseau privé derrière le serveur destination, `${PORT_DEST}` est le numéro du port de sortie du tunnel sur la machine cible `${USER}` est le nom d'utilisateur `${DEST}` est le nom complet du serveur de destination

Exemple :

```
ssh -l 9880:localhost:80 michaellaunay@plateforme.test.com
```

Me permet d'ouvrir un tunnel entre ma machine et le serveur plateforme en utilisant mon compte michaellaunay.

Une fois mon mot de passe ou ma clé acceptée je me retrouve sur la machine distante et un tunnel est ouvert entre ma machine locale et plateforme.

Si j'ouvre un navigateur sur ma machine et que je mets comme adresse `http://localhost:9880`, la communication est chiffrée et envoyée sur plateforme où elle ressort sur le port 80 ce qui me permet d'accéder au serveur web de plateforme1 sans que quiconque ne sache ce que je fais.

Compréhension de ssh :

- <http://fr.wikipedia.org/wiki/Ssh>
- <http://web.archive.org/web/20110907084212/http://www.unixgarden.com/index.php/administration-systeme/principes-et-utilisation-de-ssh>

Si la clé d'une machine à laquelle on se connecte habituellement a changé (cas d'une réinstallation), on peut être amené à supprimer son entrée dans le fichier `~/.ssh/known_hosts`.

Le plus simple est alors d'utiliser la commande **ssh-keygen -R NomDeLaMachineDistant**.

L'installation du daemon **apt-get install ssh**

Pour sécuriser les connexions **ssh**, il faut éditer `/etc/ssh/sshd_config` et mettre l'option `PermitRootLogin=no` et ajouter en fin de fichier `AllowUsers idUtilisateurAutorise`.

La commande **screen** est très utilisée avec "ssh", elle permet de conserver le **tty** ouvert lors des déconnexions et donc de reprendre là où on en était. Il suffit de la relancer avec l'option "-r" pour rattacher une session précédente, de même en début de session on peut faire "Ctrl A" "esc" pour enregistrer les lignes et donc avoir la scroll bar.

Créer une clé:

ssh-keygen

Ajouter sa clé public à un serveur distant :

ssh-copy-id user@Serveur_Distant

Supprimer la clé d'un serveur distant :

ssh-keygen -R NomServeurDistant

On peut utiliser **tar** et **ssh** pour faire des archives à travers un flux sécurisé :

tar cf - RepertoireSource | ssh user@ServeurSauvegarde "cat > nom_archive.tar"

La restauration se fera alors comme suit :

ssh user@ServeurSauvegarde "cat nom_archive.tar" | tar xf

iptables et ufw

La commande **iptables** permet de consulter et modifier les règles du firewall.

Le service **ufw** est un "firewall" pré-configurer que l'on peut facilement compléter.

Pour l'installer il suffit de faire :

```
apt install ufw
```

Pour connaître la liste des applications pouvant être autorisées par ufw à passer le firewall :

```
root@luciole:~# ufw app list Applications disponibles :
```

```
Apache
Apache Full
Apache Secure
Bind9
Dovecot IMAP
Dovecot Secure IMAP
OpenLDAP LDAP
OpenLDAP LDAPS
OpenSSH
Postfix
Postfix SMTPS
Postfix Submission
```

On pourra alors : soit autoriser les ports manuellement, soit autoriser les ports utilisés par une application.

```
ufw allow OpenSSH
```

Modification du firewall pour permettre en entrée http, https, smtp :

```
vim /etc/ufw/ufw.conf # ENABLED=yes #si pas déjà positionné
ufw allow 22/tcp # Ouvre le port ssh à tous (on peut restreindre à
certaines adresses) ufw allow 80/tcp # Ouverture de http ufw allow
443/tcp # Ouverture de https ufw allow 25/tcp # Ouverture de
smtp (envoi des courriels) ufw enable # Rend actif ufw
```

Ces commandes permettent aussi de gérer ipv6

Vérification :

```
root@luciole:/etc/dovecot# ufw status État : actif
```

```
Vers Action De ---- -22/tcp ALLOW Anywhere 25/tcp ALLOW
Anywhere 80/tcp ALLOW Anywhere 443/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6) 25/tcp (v6) ALLOW Anywhere
(v6) 80/tcp (v6) ALLOW Anywhere (v6) 443/tcp (v6) ALLOW
Anywhere (v6)
```

Permettre le lancement au démarrage:

```
systemctl enable ufw
```

Un peu de configuration pour l'utilisation en ligne

Beaucoup de paramètre par défaut peuvent être modifier dans `/etc`

Configurer vim and bash

Décommenter "syntax on" dans `/etc/vim/vimrc`, ce qui permet d'avoir la coloration syntaxique.

Pour avoir la recherche dans l'historique des commandes en saisissant les premières lettres de la commande éditer `/etc/inputrc` et supprimer le guillemet de tête:

```
"\e[5~": history-search-backward
"\e[6~": history-search-forward
```

Pour faire de vim l'éditeur par défaut:

```
echo "export EDITOR=vim" > /etc/profile.d/editor.sh
```

Pour augmenter le nombre de ligne dans l'historique des commandes, créer `/etc/profile.d/history.sh` en mettant:

```
# https://wiki.ubuntu.com/Spec/EnhancedBash
shopt -s histappend
PROMPT_COMMAND="history -a; $PROMPT_COMMAND"
export HISTSIZE=1000
export HISTFILESIZE=1000
export GREP_OPTIONS='--color=auto'
```

Gestion des permissions et droits d'accès

Concepts

Tous les utilisateurs ont un compte qui permet de les identifier.

Les programmes fonctionnant en tâche de fond (services) sont lancés depuis des utilisateurs créés spécialement pour eux. Ainsi, le serveur html **apache** est lancé depuis le compte **www-data**.

Les utilisateurs peuvent appartenir à des groupes ce qui permet de donner des droits à un ensemble d'utilisateurs très facilement.

Tout fichier appartient à un utilisateur et à un groupe.

La gestion des droits d'accès et d'exécution se résume alors à gérer les types d'accès en fonction du propriétaire, du groupe, et du reste des utilisateurs.

Comme vu précédemment la commande **ls -l** permet d'afficher les attributs d'un fichier et donc ses permissions.

À la création d'un fichier, les droits sont automatiquement positionnés en fonction de la valeur par défaut du système et de **umask** :

```
michaellaunay@luciole:~$ umask
0022
michaellaunay@luciole:~/tmp$ touch test1
michaellaunay@luciole:~/tmp$ ls -lh test1
-rw-r--r-- 1 michaellaunay michaellaunay 0 avril  5 12:17 test1
michaellaunay@luciole:~/tmp$ umask 027
michaellaunay@luciole:~/tmp$ touch test2
michaellaunay@luciole:~/tmp$ ls -lh test2
-rw-r----- 1 michaellaunay michaellaunay 0 avril  5 12:18 test2
```

Le propriétaire est alors le créateur, et le groupe est généralement le groupe par défaut de l'utilisateur sauf dans le cas où le répertoire porte le SGID alors le groupe est celui du répertoire.

Changer le propriétaire ou le groupe propriétaire

La commande **chown** permet de changer le propriétaire et le groupe d'un fichier :

```
root@luciole:~$ ls -l /tmp/MonFichier
-rw-rw-rw- 1 michaellaunay michaellaunay 0 2009-05-03 19:08 /tmp/MonFichier
root@luciole:~# chown root:users /tmp/MonFichier
root@luciole:~# ls -l /tmp/MonFichier
-rw-rw-rw- 1 root users 0 2009-05-03 19:08 /tmp/MonFichier
```

Toutefois pour des raisons de sécurité (gestion des quotas : attaque sushi) la commande peut être réservée au super utilisateur.

On dispose aussi de la commande **chgrp** qui permet de changer le groupe d'un fichier.

Valeurs symboliques et octales des permissions

Les tableaux suivants donnent les équivalents symboliques octales des permissions.

DROIT	LETTRE	VALEUR
Lecture	r (read)	4
Écriture	w (write)	2
Exécution / Traversé	x (execute)	1

Ainsi les permissions *rwX* sont équivalentes à 7 et *rwXr-xr--* donne 754.

DROIT	LETTRE	VALEUR
-------	--------	--------

SUID	s si le propriétaire a x S si non	4
SGID	s si le groupe a x S sinon	2
Sticky Bit	t si les autres ont x T sinon	1

Ainsi *rwsr-sr-t* est équivalent à *7755*.

Si l'on a un S ou un T en majuscule cela signifie que les droits d'exécution n'ont pas été positionnés.

Ceci n'a pas de sens dans le cas général et indique une suppression du droit d'exécution avec oubli du SUID ou GUID ou Sticky Bit.

Sauf avec l'usage des ACLs, où un utilisateur particulier peut avoir le droit d'exécution et redonne du sens à S ou T.

Changer les permissions sur les fichiers

La commande **chmod** permet de modifier les droits des fichiers.

Mode chiffré

Exemple :

```
michaellaunay@luciole:~/tmp$ ls -l MonFichier
-rw-r--r-- 1 michaellaunay michaellaunay 0 2009-05-03 19:40 MonFichier
michaellaunay@luciole:~/tmp$ chmod 754 MonFichier
michaellaunay@luciole:~/tmp$ ls -l MonFichier
-rwxr-xr-- 1 michaellaunay michaellaunay 0 2009-05-03 19:40 MonFichier
```

Notation relative (aux droits existants)

Exemple :

```
michaellaunay@luciole:~/tmp$ ls -l MonFichier
-rwxr-xr-- 1 michaellaunay michaellaunay 0 2009-05-03 19:40 MonFichier
michaellaunay@luciole:~/tmp$ chmod u+s,g-x,o-r MonFichier
michaellaunay@luciole:~/tmp$ ls -l MonFichier
-rwsr----- 1 michaellaunay michaellaunay 0 2009-05-03 19:40 MonFichier
```

Attention aux modifications contradictoires :

```
michaellaunay@luciole:~$ echo coucou > /tmp/hello
michaellaunay@luciole:~$ ls -l /tmp/hello
-rw-r--r-- 1 michaellaunay michaellaunay 7 2009-05-07 09:45 /tmp/hello
michaellaunay@luciole:~$ sudo chmod u-w,o+w /tmp/hello
michaellaunay@luciole:~$ ls -l /tmp/hello
-r--r--rw- 1 michaellaunay michaellaunay 7 2009-05-07 09:45 /tmp/hello
```

```
michaellaunay@luciole:~$ echo bonjour >> /tmp/hello
bash: /tmp/hello: Permission non accordée
```

Notation absolue

Exemple : :

```
michaellaunay@luciole:~/tmp$ ls -l MonFichier
-rwsr----- 1 michaellaunay michaellaunay 0 2009-05-03 19:40 MonFichier
michaellaunay@luciole:~/tmp$ chmod u=rx,g=rx,o=rx MonFichier
michaellaunay@luciole:~/tmp$ ls -l MonFichier
-r-xr-xr-x 1 michaellaunay michaellaunay 0 2009-05-03 19:40 MonFichier
```

Umask

Par défaut le système applique les droits 0666 pour un fichier et 0777 pour les répertoires auxquels il applique encore le filtre **umask** qui par défaut vaut 0022, les droits sont alors 0644 (rw-r--r--) pour un fichier et 0755 (rwx-rx-rx) pour un répertoire.

Il est possible de changer la valeur du masque de permissions en appelant **umask nouvellevaleur**.

ACL

Le mécanisme de gestion des droits Unix couvre 95% des usages.

Il reste donc certains cas non couverts comme le fait d'attribuer les droits de modification d'un fichier à un utilisateur sans avoir à demander à l'administrateur de devoir créer un groupe (ce qui manque un peu de souplesse).

On peut aussi vouloir associer de nouveaux attributs aux fichiers pour par exemple gérer des informations de sécurités.

À l'inverse il est très difficile de restreindre les droits d'un utilisateur d'un groupe donné pour un seul fichier.

C'est pour répondre ce besoin qu'ont été implémentées les Access Control List

Les ACLs reposent sur le mécanisme des attributs étendus.

Pour les rendre disponibles, il faut que la partition soit montée avec les options *acl* et *user_xattr* (modifier en conséquence */etc/fstab*).

Les fonctions d'accès aux *acl* sont **getfacl**, **setfacl**, **getfattr**, **setfattr**.

Voir aussi les man pages de *acl* et *attr(5)*.

Attributs étendus

Les attributs étendus permettent de gérer simplement les métadonnées associées à un fichier.

Ceux sont ces attributs étendus qui recevront les informations liées aux ACLs.

Pour installer le paquet : **apt-get install attr**

Ajouter l'option *user_xattr* aux partitions dans */etc/fstab*.

Puis utiliser **setfattr** pour positionner les attributs et **getfattr** pour les afficher :

```
michaellaunay@excalibur:~$ echo test > MonFichier
michaellaunay@excalibur:~$ setfattr -n user.description -v 'Contient des données de test' MonFichier
michaellaunay@excalibur:~$ ls -l MonFichier
-rw-r--r-- 1 michaellaunay michaellaunay 5 2009-05-05 08:17 MonFichier
michaellaunay@excalibur:~$ getfattr -d MonFichier
#file: MonFichier
user.description="Contient des donn\305\251es de test"
```

Remarque : La présence d'attributs étendus n'est pas signalée par *ls*.

Affectation des ACL

Pour vérifier que les ACLs peuvent être activées :

```
michaellaunay@luciole:~$ grep -i acl /boot/config-`uname -r`
```

```
CONFIG_EXT2_FS_POSIX_ACL=y
CONFIG_EXT3_FS_POSIX_ACL=y
CONFIG_EXT4DEV_FS_POSIX_ACL=y
CONFIG_FS_POSIX_ACL=y
CONFIG_GENERIC_ACL=y
CONFIG_JFS_POSIX_ACL=y
CONFIG_NFSD_V2_ACL=y
CONFIG_NFSD_V3_ACL=y
CONFIG_NFS_ACL_SUPPORT=m
CONFIG_NFS_V3_ACL=y
CONFIG_REISERFS_FS_POSIX_ACL=y
CONFIG_TMPFS_POSIX_ACL=y
CONFIG_XFS_POSIX_ACL=y
```

Pour installer les ACL si besoin *apt-get install acl*.

Puis rendre la partition compatible avec les ACL (édition de *fstab*).

Exemple de changement de permissions :

```
root@excalibur:~# mkdir /tmp/MYDIR
root@excalibur:~# chacl u::rwx,u:michaellaunay:rwx,g::---,o::---,m::rwx /tmp/MYDIR
```

```

root@excalibur:~# ls -l /tmp
drwx-----+ 2 root      root      4096 2009-05-04 22:37 MYDIR
root@excalibur:~# su - michaellaunay
michaellaunay@excalibur:~$ touch /tmp/MYDIR/MonFichier
michaellaunay@excalibur:~$ ls -l /tmp/MYDIR/
-rw-r--r-- 1 michaellaunay michaellaunay 0 2009-05-04 22:50 /tmp/MYDIR/
michaellaunay@excalibur:~$ setfacl -m isabelle:r /tmp/MYDIR/MonFichier
michaellaunay@excalibur:~$ setfacl -m g:users:- /tmp/MYDIR/MonFichier
michaellaunay@excalibur:~$ getfacl /tmp/MYDIR/MonFichier
getfacl: Removing leading '/' from absolute path names
# file: tmp/MYDIR/MonFichier
# owner: michaellaunay
# group: michaellaunay
user::rw-
user:isabelle:r--
group::r--
group:users:---
mask::r--
other::r--

```

Les processus

Définition

Un processus est l'instance d'un programme en cours de fonctionnement.

Une application est constituée de un à plusieurs processus qui collaborent à la réalisation du travail demandé.

Chaque processus s'exécute en parallèle des autres.

Un processus correspond à un fichier exécutable.

Les processus utilisent des bibliothèques qui peuvent être statiques ou dynamiques selon qu'elles sont dans le code de l'application ou non.

L'extension des bibliothèques dynamiques est *.so* (shared object).

Un processus est lancé par un autre processus, ainsi il existe une relation père fils entre les processus.

Le processus ancêtre de tous les autres est *init* qui est lancé lors du démarrage par le noyau.

Son *PID* est 1.

Alt+F2 est un raccourci clavier permettant d'appeler le lanceur.

Attributs d'un processus

PID : Identifiant du processus (Process Identification),

PPID : Identifiant du processus père (Parent Process Identification),

PGID : Identifiant du groupe de processus qui permet de connaître l'application à laquelle appartient le processus,

UID : Le compte utilisateur ayant lancé le processus,

GIDs : Les groupes de l'utilisateur ayant lancé le processus,

TTY : Terminal où a été lancé le processus,

NICE : Priorité appliquée pour le scheduling,

CMD : La commande à l'origine du processus.

Cycle de vie d'un processus

Un processus est dans un état qui peut être "created", "ready", "running", "sleeping", "idle" (en attente de signal), "Terminated" = "zombie"

Created correspond à l'état du processus au moment de sa création lorsque les variables ne sont pas encore renseignées.

Ready le processus est en mémoire, les variables sont renseignées.

Running le processus est en cours d'exécution.

Sleeping le processus a été préempté.

Idle le processus attend un signal.

Zombie le processus a fini de s'exécuter, le code de retour attend sa lecture.

Voir : http://en.wikipedia.org/wiki/Process_states

Les différentes sortes de processus

On distingue les processus classiques des daemons qui sont les services unix.

Les daemons ou démons fonctionnent en arrière plan ils ont en général pour père le processus 1.

Les démons sont lancés et arrêtés à partir des scripts contenus dans **/etc/init.d**.

Envoi de signaux aux processus

L'envoi de signaux au processus se fait par la commande **kill** ou **pkill**.

Les processus peuvent établir entre eux une communication événementielle basé sur les signaux.

Seul les signaux **9 SIGKILL**, et **SIGSTOP** ne peuvent être attrapés.

Les commandes liées à la gestion des processus

La commande **free** affiche les ressources mémoires consommées.

La commande **fuser** liste les processus accédant à un fichier.

La commande **ldd** affiche la liste des bibliothèques utilisées par un exécutable.

La commande **lsuf** affiche les fichiers ouverts par un processus **lsuf -p PID**.

La commande **nice** et **renice** permette de modifier la priorité d'exécution.

La commande **pgrep** recherche un processus par son nom.

La commande **ps** affiche les processus en cours.

La commande **pstree** affiche l'arborescence des processus.

La commande **top** affiche la liste de processus classés par consommation décroissante.

La commande **uptime** affiche les informations de temps de fonctionnement, du nombre d'utilisateurs connectés, de la charge.

Arrière plan / Avant plan / Détachement

Pour lancer un processus en arrière plan on peut soit terminer la ligne de commande qui le lance avec **&**, soit le lancer, faire **Ctrl+z** puis **bg**.

Lors du **Ctrl+z** la commande **fg** ramène le processus au premier plan.

La commande **jobs** permet de lister les processus suspendus, on peut alors les rattacher avec **fg num__job**.

Les processus dont le père meure sans attendre le statut de ses enfants sont raccrochés à *init*.

Modification des priorités

Les processus ont des priorités fixées entre -20 (la plus haute) et +19.

Le *scheduler* gère l'ordre d'exécution des processus en fonction de cette priorité.

Par défaut un processus est lancé avec la priorité +10.

Seul l'administrateur peut donner des priorités négatives aux processus.

La commande **nice [COMMAND [ARG]]** permet de lancer une commande en lui donnant la priorité *p* si l'on passe l'option *-n p*.

La commande **renice** permet de modifier la priorité d'un processus.

Planification de tâches

Sous unix deux démons sont chargés de la planification des tâches : **atd** qui permet de programmer une tâche différée et **crond** qui permet de programmer les tâches répétitives.

La commande crontab

crond est un service qui peut être programmé grace à la commande **crontab**.

crontab -l liste les commandes déjà programmées pour l'utilisateur courant.

crontab -e permet d'éditer le fichier des commandes programmées pour l'utilisateur courant.

L'éditeur utilisé par **crontab -e** est celui désigné par la variable *EDITOR*.

Le fichier crontab système

Ils est possible d'éditer directement le fichier */etc/crontab* ou ceux contenu dans */var/spool/cron/crontabs/\${USER}*

Le format du fichier est le même que lors de l'édition avec *crontab -e*:

Minutes	Heures	Jour du mois	Mois	Jour de la semaine	Commande
(0-60)	(0-24)	(0-31)	(1-12)	(0-6)	un script

Le joker ******* permet d'indiquer que toutes les valeurs sont acceptées.

Pour les fichiers *cron* du système, une colonne *Utilisateur* s'intercale juste avant celle de la *commande*. Elle permet alors d'indiquer sous quel utilisateur doit être lancée la commande.

Exemple : :

```
root@serveur:~# crontab -l
# m h dom mon dow   command
00 4 * * * /usr/bin/webalizer -c /etc/webalizer/www_ecreall.conf
10 4 * * * /usr/bin/webalizer -c /etc/webalizer/ssl_ecreall.conf
* * * * * /root/load.sh update
0 * * * * /root/load.sh graph > /dev/null

root@serveur:~# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
```

```
# that none of the other crontabs do.
```

```
SHELL=/bin/sh
```

```
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

```
# m h dom mon dow user  command
```

```
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
```

```
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.da
```

```
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.we
```

```
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.mo
```

```
#
```

Sur la plupart des distributions */etc/crontab* lance les scripts contenus dans */etc/cron.hourly*, */etc/cron.daily*, */etc/cron.weekly*, */etc/cron.monthly*. Pour ajouter une tâche il suffit d'ajouter un script au répertoire désiré.

Les fichiers */etc/cron.allow* et */etc/cron.deny* permettent s'ils existent de nommer les utilisateurs pouvant programmer des tâches.

La commande at

at permet de lancer une commande à une heure donnée, la commande utilise le démon **atd**

atq permet de voir la liste des commandes en attente d'exécution.

atrm Permet de supprimer une commande programmée.

Exemple :

```
root@server:~# apt-get install mailutils # Pour avoir la commande mail
```

```
root@server:~# at 6:45; mail -s "Debout" michaelaunay@ecreall.com < reveil.msg
```

Les fichiers */etc/at.allow* et *at.deny* permettent comme pour cron de lister les utilisateurs pouvant ou non lancer **at**.

Les utilisateurs et les groupes

Unix est un système multi-utilisateurs.

Tout fichier est associé à un propriétaire et à un groupe.

La gestion des droits dépend des notions d'utilisateur, de propriétaire, de groupe, et des autres.

Ceci suppose :

- l'existence d'une base des comptes utilisateurs,
- l'existence d'une base des groupes d'utilisateurs,
- que tout fichier possède un utilisateur propriétaire et un groupe propriétaire,

- que tout processus hérite des droits de l'utilisateur l'ayant lancé et par conséquent de l'ensemble des droits des groupes de l'utilisateur,
- que l'utilisateur *root* a tous les droits pour pouvoir gérer le système.

Qu'est qu'un utilisateur ?

Chaque utilisateur d'un système Unix est associé à un identifiant unique qui lui permet de s'authentifier et d'accéder à son compte.

Ainsi au *login* le système demande à l'utilisateur son mot de passe.

Lorsque la connexion réussit le système associe à l'utilisateur l'**UID (User IDentification)** correspondant à son identifiant.

Le système associe également à l'utilisateur un **GID (Groupe IDentification)** qui est le groupe principal de l'utilisateur.

Ces numéros seront utilisés pour gérer les permissions des fichiers. Les commandes comme *ls* feront alors la correspondance entre les numéros et les noms d'utilisateurs et de groupes.

Un **UID** est associé à un répertoire personnel et à un shell.

L'UID 0 désigne l'utilisateur **root**

Un utilisateur peut ne pas être une personne physique mais être l'utilisateur d'exécution d'un démon.

En conséquence, les **UID** des personnes physiques commencent généralement à partir de 1000.

Qu'est qu'un groupe ?

Les groupes permettent de créer des ensembles d'utilisateurs afin de gérer collectivement les permissions.

Généralement la création d'un utilisateur engendre la création de son groupe principal ayant pour identifiant de groupe le même identifiant et pour **GID** la même valeur que l'**UID**.

Gestion des comptes

Ajouter un utilisateur

La création d'un nouvel utilisateur peut être faite à l'aide des commandes **useradd** ou **adduser** la seconde étant préférable, car interactive.

Supprimer un utilisateur

La commande **userdel** permet de supprimer un utilisateur.

Avec l'option **-r** cette commande supprimera en plus le répertoire personnel de l'utilisateur.

Désactiver un compte utilisateur

L'une des façons les plus propres d'interdire la connexion à un utilisateur est de lui associer le shell **nologin** :

```
root@server:~# usermod -s /usr/sbin/nologin indésirable
```

Changer le mot de passe d'un utilisateur

La commande **passwd** permet sous *root* de changer le mot de passe d'un utilisateur.

Si l'on est un utilisateur la commande demandera de saisir l'ancien mot de passe.

La commande **chpasswd** permet de scripter les changements de mots de passe.

Afficher des informations d'un utilisateur

La commande **id** permet d'afficher les informations de l'utilisateur :

```
michaellaunay@serveur:~$ id
uid=1000(michaellaunay) gid=1000(michaellaunay) groupes=4(adm),20(dialout),24(cdrom),25(floppy)
```

La commande **groups** permet d'afficher les informations de groupe :

```
michaellaunay@luciole:~/Documents/ecreall/Cours/CoursGNULinux$ groups
michaellaunay adm dialout cdrom plugdev lpadmin admin sambashare
```

La commande **who** permet de savoir qui est connecté sur la machine.

La commande **whoami** permet de savoir sous quelle identité on est connecté.

Modifier les informations d'un utilisateur

La commande **usermod** permet de modifier toutes les propriétés d'un utilisateur.

Faire *man usermod*

La commande **chsh** permet de changer le shell de connexion.

La commande **chfn** permet de changer la description d'un utilisateur.

Changer d'identité

La commande **su** permet de changer d'identité. **su -** permettra en plus d'utiliser l'environnement de l'utilisateur.

La commande **sudo** permet d'exécuter un script ou une commande en tant que *root*. **sudo -i** permet sous *Ubuntu* de se connecter en tant que *root*.

Gestion des groupes

Créer un groupe

Comme pour l'utilisateur nous pouvons utiliser **addgroup** ou **groupadd**

Afficher des informations sur les groupes

La commande **groups** déjà vu affiche les informations d'appartenance.

Ajouter un utilisateur à un groupe

On utilise la commande **usermod** de la façon suivante :

```
root@server~# usermod -a -G cdrom,dev michaelaunay
```

Ajouter un utilisateur au groupe des administrateurs

```
usermod -a -G sudo identifiant_de_l_utilisateur
```

Changer de groupe principal

La commande **newgrp** permet de changer de groupe principal.

Modifier un groupe

Pour modifier un groupe nous pouvons utiliser la commande **groupmod**.

Supprimer un groupe

La commande **groupdel** permet de supprimer un groupe.

Le fichier */etc/passwd*

Le fichier */etc/passwd* contient la définition de tous les comptes.

Le fichier */etc/shadow*

Le fichier */etc/shadow* contient les mots de passe des comptes définis dans */etc/passwd*

Le fichier */etc/group*

Le fichier */etc/group* contient la définition de tous les groupes.

Installation openldap

Ldap est un annuaire qui permet de gérer le utilisateur d'un service sans créer un compte unix.

Installation du serveur ldap :

```
apt install slapd ldap-utils
```

Modification de la configuration :

```
dpkg-reconfigure slapd # saisie de "ecreall.com" comme domaine
# saisie de "people" comme organization # saisie du mot de passe
(commence celui de l'utilisateur michaelaunay mais pour LDAP)
```

Attention ! Configurer LTS pour chiffrer les connexions si elles sont extérieures à la machine, car les mots de passe circulent en clair (voir https://wiki.debian.org/LDAP/OpenLDAPSetup#Enable_TLS.2FSSL)!

Activer le service au démarrage :

```
systemctl enable slapd
```

Rendre "ldap" accessible en éditant "/etc/ldap/ldap.conf" en ajoutant :

```
BASE dc=ecreall,dc=com URI ldap://127.0.0.1
```

Ajout d'une entrée LDAP :

Créer un fichier ecreall.ldif contenant :

```
dn: ou=People,dc=ecreall,dc=com ou: People objectClass:
top objectClass: organizationalUnit
```

```
dn: ou=Group,dc=ecreall,dc=com ou: Group objectClass:
top objectClass: organizationalUnit
```

```
dn: cn=Gérant,dc=ecreall,dc=com objectclass: organiza-
tionalRole cn: Gérant
```

```
ldapadd -x -D "cn=admin,dc=ecreall,dc=com" -W -f ecreall.ldif
```

Mettre à jour l'index (cache) :

```
systemctl stop slapd slapindex chown -R openldap:openldap
/var/lib/ldap systemctl start slapd
```

Vérification :

```
ldapsearch -x -b 'dc=ecreall,dc=com' '(objectclass=*)'
```

Ajout d'une OrganizationUnit :

Créer un fichier "e-services.ldif" et y mettre :

```
dn: ou=Études,dc=ecreall,dc=com objectClass: organiza-
tionalUnit ou: Études
```



```
ldapadd -x -D "cn=admin,dc=ecreall,dc=com" -W -f e-services.ldif
```

Ajouter une personne :

Exemple pour ajouter Michaël Launay, créer un fichier "ldif_files/michaellaunay.ldif" :

```
dn: cn=Michaël Launay, ou=People, dc=ecreall, dc=com
objectclass: top objectclass: person objectclass: organiza-
tionalPerson objectclass: inetorgperson cn: Michaël Lau-
nay sn: Launay gn: Michaël uid: michaellaunay title:
Gérant mail: michaellaunay@ecreall.com telephoneNum-
ber: 0320793290 officePostalAddress: 11 A Avenue de
l'Harmonie postalCode: 59650 l: Villeneuve d ASCQ
```

L'ajouter :

```
ldapadd -x -D "cn=admin,dc=ecreall,dc=com" -W -f
ldif_files/michaellaunay.ldif
```

Voir :

<https://wiki.debian.org/LDAP/OpenLDAPSetup> <https://guide.ubuntu-fr.org/server/openldap-server.html>
<http://www-sop.inria.fr/members/Laurent.Mirtain/ldap-livre.html>

Syslog

Syslog est le système chargé d'enregistrer les fichiers journaux.

Le démon **klogd** consigne les événements de type message du noyau, authentification, connexion alors que **syslogd** enregistre les message d'envoi ou réception de courrier, ceux d'erreur, etc.

Les fichiers de messages se trouvent dans */var/log*

syslogd est configuré avec le fichier */etc/syslog.conf*. Ce fichier permet d'indiquer les sources de messages et les destinations associées (fichier, tty, application ou syslog d'une autre machine). Pour être prise en compte, la modification du fichier de conf doit être suivie par un *kill 1 \$PID_SYSLOG*.

Toutefois de nombreux programmes n'utilisent pas *syslog* comme *CUPS*, *Samba*, etc.

Afin d'éviter que la taille des fichiers de logs n'explose la capacité du disque les fichiers sont compressés de façon régulière par **logrotate** dont la configuration est modifiable en éditant */etc/logrotate*

La commande **dmesg** permet d'afficher les messages du noyau.

Modification de la configuration de logrotate

Logrotate possède une configuration par défaut contenue dans `/etc/logrotate.conf` puis un répertoire avec les configurations des services pour compléter ou remplacer la configuration par défaut.

Il est fréquent que pour des raisons légales, on doive garder un ou deux ans de logs selon la nature des utilisateurs et des services. Souvent on garde 104 semaines de connexions et 52 semaines de navigation et 14 semaines pour les autres services.

Pour modifier la conf par défaut à 14 semaines on édite `/etc/logrotate.conf` :

- Remplacer `"rotate 4"` par `"rotate 14"` pour garder 3 mois de log par défaut
- Décommenter `"compress"` pour compresser les anciens fichiers log
- Ajouter `delaycompress` chaque vieux fichier de log
- Limiter la taille d'un fichier de log à 100M

On doit donc avoir dans `/etc/logrotate.conf` :

```
rotate 14 compress delaycompress size 100M
```

Puis on change `"rotate X"` à `"rotate 104"` dans les fichiers des services concernés se trouvant dans le répertoire `/etc/logrotate.d/`. Par exemple, on va modifier `/etc/logrotate.d/apache2` pour mettre `rotate` à 104, et modifier le fichier `/etc/logrotate.d/rsyslog` modifier les logs des services d'authentifications.

Périphérique disque et système de fichiers

Les disques durs sous Linux

L'organisation physique d'un disque est constituée de plateaux superposés divisés en pistes concentriques.

Chaque piste contenant un certain nombre de secteurs de 512 octets.

L'ensemble des pistes des différents plateaux accessible sans nouveau déplacement des têtes de lecture constitue un cylindre.

Voire http://fr.wikipedia.org/wiki/Disque_dur.

Le nommage des périphériques disques dépend de leur nature et de la façon dont ils sont gérés par le bios.

Ainsi `sda`, `sdb` correspondent à des disques durs alors que `nvme0n1p7` correspond à un disque `ssd` monté sur le connecteur `nvme`.

Depuis 2013 les nommages des périphériques suivent les règles *ifname* voir : https://access.redhat.com/documentation/fr-fr/red_hat_enterprise_linux/7/html/networking_guide/sec-understanding_the_device_renaming_procedure

Les concepts

Un disque est "découpé" en partitions.

Le premier secteur contient le MBR (Master Boot Record) qui décrit la table des 4 premières partitions et contient également le code du chargeur primaire (primary loader).

L'une des quatre partitions primaires peut être du type étendue et contenir des partitions logiques qui sont alors chaînées entre elles.

La taille des partitions est donnée en nombre de cylindres, ce qui fixe le nombre de secteurs de la partition.

La partition possède un type qui fixe son usage, par exemple 83 pour Linux, 82 pour le swap, 5 pour une partition étendue, etc.

Les systèmes de fichiers

Un système de fichier est une structure de données permettant de stocker et organiser les informations dans des fichiers.

Le système de fichier est généralement stocké dans une partition mais il peut l'être sur un disque amovible (USB) ou dans un fichier.

Partitions

La numérotation des partitions est réalisée en accolant au nom du périphérique le numéro de la partition. Ainsi :

sda est le premier disque complet
sda1 est la première partition
sda4 est généralement la partition étendue
sda5 est la première partition logique
sdb est le second disque

Utilitaires de partitionnement

Historiquement la commande permettant de créer les partitions était **fdisk**, mais elle est limitée à des partitions de taille inférieure à 2To.

Elle est remplacée par la commande **parted** et par sa version graphique **gparted** qui permettent de créer et retailler des partitions déjà existantes, mais il faut descendre le paquet.

La commande **partprobe** permet d'avertir le système que l'on a modifié la tables des partitions.

Arborescence standard et organisation du FHS

Le Filesystem Hierarchy Standard est l'organisation standard Unix utilisée par Linux

Tout est fichier. Les périphériques (scanner, imprimante, etc) sont manipulés sous forme de fichier dans lequel on va lire et écrire.

Arborescence de /

/ est la racine, elle a pour contenu :

- /bin contient les exécutables du système d'exploitation,
 - /boot les fichiers de démarrage,
 - /dev les périphériques sous forme de fichiers pouvant être lus ou écrits,
 - /etc les fichiers de configuration et ceux nécessaires au démarrage,
 - /home les répertoires des utilisateurs,
 - /lib les bibliothèques partagées et les modules du noyau dans le sous répertoire modules,
 - /mnt les dossiers des points de montage temporaires,
 - /proc les états du noyau,
 - /root le répertoire du super utilisateur root,
 - /sbin les exécutables du super utilisateur,
 - /sys contient les caractéristiques et informations sur les périphériques comme le nom du fabricant, les bus connectés,
 - /tmp les fichiers temporaires liés à l'exécution des applications ou services, ils sont effacés au reboot,
 - /usr les ressources du système non essentielles (Unix Système Ressources)
 - /var les fichiers tels que les bases de données, les pages html, les mails, les logs
- Pour une description plus complète C.f. http://en.wikipedia.org/wiki/Filesystem_Hierarchy_Standard

Arborescence de /usr

/usr contient :

- /usr/bin/ Binaires de l'utilisateur,
- /usr/include/ Entêtes des bibliothèques partagées,
- /usr/lib/ Bibliothèques partagées des logiciels utilisateurs,
- /usr/local/ Hiérarchie pour les données de locales.
- /usr/sbin/ Binaires pour l'administrateur,
- /usr/share/ Fichiers indépendants de la plateforme (non binaires),
- /usr/src/ Les sources du noyau,

Arborescence de /var

/var contient:

- /var/lib/ Données persistantes telles les bases de données,
- /var/lock Les fichiers de verrous,
- /var/log Les fichiers de Log
- /var/mail Les mails si la configurations précise qu'ils doivent être stockés ici
- /var/run Les informations d'exécution des daemons
- /var/spool Les queues de traitement (mail, impression, etc)
- /var/tmp Les fichiers temporaires à préserver des reboots

Formater une partition

La commande **mkfs** permet de formater une partition. Le type système de fichier est alors choisi à ce moment ex: **mkfs.ext3**.

Monter / Démonter une partition

Un système de fichier est accessible après son *montage* soit au démarrage, soit à l'aide de la commande **mount**.

Le démontage se fait à l'aide de la commande **umount**.

La commande **sshfs** permet de monter un disque distant à travers le protocole **ssh**. Pour démonter un système de fichier monté avec **sshfs** : **fusermount -u point_de_montage**.

Les tables de montage : /etc/fstab

Le fichier **/etc/fstab** contient les montages à réaliser au démarrage ou pour lesquels *root* a autorisé un montage manuel.

Tables systèmes, inodes

Un file system est composé de différentes tables systèmes :

- Le super-bloc contenant les informations de taille, d'état de montage.
- La table des *inodes* (nœud d'index) qui fait correspondre à chaque fichier un numéro d'identification unique et qui possède les informations des droits d'accès, de propriété.
- Les répertoires qui sont une table de correspondance *inode* vers nom de fichier.

La commande **ls -li** permet d'afficher l'inode d'un fichier.

Remarques :

- Les *inodes* ne contiennent pas le nom du fichier.
- Un *file system* est limité en *inodes*

Journalisation

La journalisation permet d'enregistrer les manipulations réalisées sur les fichiers et l'arborescence.

Pour certain système de fichier elle enregistre en plus les différences, ce qui permet de revenir à un état précédent.

Les système simples permettent néanmoins de revenir au dernier état cohérent en cas de plantage du système.

Toutefois, les coupures de courant peuvent aboutir à des états incohérents, ceci à cause du cache en écriture des disques durs.

Au redémarrage de la machine la journalisation va permettre d'accélérer le diagnostic des disques.

ext3 est un système journalisé de manière simple.

Contrôle des systèmes de fichiers

La commande **df** permet de lister les montages réalisés.

La commande **du** permet de calculer la taille d'une arborescence.

La commande **fsck** permet de vérifier l'état d'une partition. ATTENTION ! Il ne faut pas l'utiliser sur des partitions montées.

La commande **e2label** permet d'affecter un nom à un *file system*.

La commande **hdparm** permet avec l'option *-t* de connaître les performances d'un disque.

Montage des périphériques amovibles

La commande **lsusb** permet de voir les périphériques USB connectés.

La commande **lspci** permet de voir les périphériques PCI connectés.

Lorsqu'un périphérique de type blocs ou caractères est détecté par le noyau, un périphérique correspondant est ajouté dans */dev* par le démon **udev** du système **udev**.

Le système **udev** a pour rôle de gérer l'unicité des noms pour les périphériques et de maintenir */dev* en cohérence avec les périphériques présents.

Les fichiers de configuration de **udev** sont placés dans */etc/udev*. Il est possible de définir des règles dans */etc/udev/rules.d* qui seront évaluées dans l'ordre lexicographique.

Le démon HAL (Hardware Abstraction Layer) **hald** est notifié par **udev** de l'ajout d'un périphérique (règle */etc/udev/rules.d/90-hal.rules*).

HAL identifie alors le type des périphériques connectés, du système de fichiers, et en fonction des informations comme *VendorId* ou *ProductId* d'associer le contenu avec un type d'application.

La base de données des périphériques est située dans le répertoire */usr/share/hal/fdi/* :

```
michaellaunay@luciole:~$ grep -rl ipod /usr/share/hal/fdi/*  
/usr/share/hal/fdi/information/10freedesktop/10-usb-music-players.fdi
```

Une fois le périphérique complètement identifié, **HAL** envoie un message sur le bus de communication des applications **D-Bus**.

Les applications de l'environnement graphique vont alors monter le périphérique et le rendre accessible à l'utilisateur.

Sous **gnome** le comportement peut être modifié via le gestionnaire de fichiers **nautilus** dans Edition-Préférences-Supports**.

Exemple des noms persistants donnés par udev :

```
michaellaunay@luciole:~$ ls -lR /dev/disk
```

/dev/disk:

total 0

```
drwxr-xr-x 2 root root 260 avril 18 22:11 by-id  
drwxr-xr-x 2 root root 80 avril 18 22:11 by-partlabel  
drwxr-xr-x 2 root root 100 avril 18 22:11 by-partuuid  
drwxr-xr-x 2 root root 160 avril 18 22:11 by-path  
drwxr-xr-x 2 root root 100 avril 18 22:11 by-uuid
```

/dev/disk/by-id:

total 0

```
lrwxrwxrwx 1 root root 9 avril 18 22:11 ata-ST8000VN0022-2EL112_ZA1F9KQR -> ../../sda  
lrwxrwxrwx 1 root root 10 avril 18 22:11 ata-ST8000VN0022-2EL112_ZA1F9KQR-part1 -> ../../sda  
lrwxrwxrwx 1 root root 13 avril 18 22:11 nvme-eui.0025385491b00f2f -> ../../nvme0n1  
lrwxrwxrwx 1 root root 15 avril 18 22:11 nvme-eui.0025385491b00f2f-part1 -> ../../nvme0n1p1  
lrwxrwxrwx 1 root root 15 avril 18 22:11 nvme-eui.0025385491b00f2f-part2 -> ../../nvme0n1p2  
lrwxrwxrwx 1 root root 13 avril 18 22:11 nvme-Samsung_SSD_970_EVO_Plus_1TB_S4EWNFOM403887L -  
lrwxrwxrwx 1 root root 15 avril 18 22:11 nvme-Samsung_SSD_970_EVO_Plus_1TB_S4EWNFOM403887L-p  
lrwxrwxrwx 1 root root 15 avril 18 22:11 nvme-Samsung_SSD_970_EVO_Plus_1TB_S4EWNFOM403887L-p  
lrwxrwxrwx 1 root root 9 avril 18 22:11 usb-Generic_STORAGE_DEVICE-0:0 -> ../../sdb  
lrwxrwxrwx 1 root root 9 avril 18 22:11 wwn-0x5000c500b5c4d662 -> ../../sda  
lrwxrwxrwx 1 root root 10 avril 18 22:11 wwn-0x5000c500b5c4d662-part1 -> ../../sda1
```

/dev/disk/by-partlabel:

total 0

```
lrwxrwxrwx 1 root root 15 avril 18 22:11 'EFI\x20System\x20Partition' -> ../../nvme0n1p1
```

```
lrwxrwxrwx 1 root root 10 avril 18 22:11 Sauvegardes -> ../../sda1
```

```
/dev/disk/by-partuuid:
```

```
total 0
```

```
lrwxrwxrwx 1 root root 15 avril 18 22:11 54795468-79c2-48ce-9c7e-f6bd6aea6914 -> ../../nvme0n1p1  
lrwxrwxrwx 1 root root 15 avril 18 22:11 e9a9f238-ec93-4777-82e8-cbea7c8cf986 -> ../../nvme0n1p2  
lrwxrwxrwx 1 root root 10 avril 18 22:11 eeb50a63-ec05-4e34-b673-b90bc5ea2cfa -> ../../sda1
```

```
/dev/disk/by-path:
```

```
total 0
```

```
lrwxrwxrwx 1 root root 9 avril 18 22:11 pci-0000:00:14.0-usb-0:1:1.0-scsi-0:0:0:0 -> ../../sda1  
lrwxrwxrwx 1 root root 10 avril 18 22:11 pci-0000:00:14.0-usb-0:1:1.0-scsi-0:0:0:0-part1 -> ../../sda1  
lrwxrwxrwx 1 root root 9 avril 18 22:11 pci-0000:00:14.0-usb-0:5:1.0-scsi-0:0:0:0 -> ../../sda1  
lrwxrwxrwx 1 root root 13 avril 18 22:11 pci-0000:03:00.0-nvme-1 -> ../../nvme0n1  
lrwxrwxrwx 1 root root 15 avril 18 22:11 pci-0000:03:00.0-nvme-1-part1 -> ../../nvme0n1p1  
lrwxrwxrwx 1 root root 15 avril 18 22:11 pci-0000:03:00.0-nvme-1-part2 -> ../../nvme0n1p2
```

```
/dev/disk/by-uuid:
```

```
total 0
```

```
lrwxrwxrwx 1 root root 10 avril 18 22:11 0a2768a9-34ac-4944-83a2-2e10ed4c48a5 -> ../../sda1  
lrwxrwxrwx 1 root root 15 avril 18 22:11 aad5ec2d-1dce-4a2b-8b07-2cd2bef72410 -> ../../nvme0n1p1  
lrwxrwxrwx 1 root root 15 avril 18 22:11 C3AC-80CA -> ../../nvme0n1p1
```

Voir :

<https://doc.ubuntu-fr.org/udev> <https://web.archive.org/web/20100417131709/www.unixgarden.com/index.php/programmation/decouvertes-et-experimentation-avec-d-bus>

Utilitaire smartd

Smart signifie **Self-Monitoring, Analysis and Reporting Technology** c'est une technologie d'auto surveillance mise en œuvre par certains disques durs.

Le but de cette technologie est de permettre le suivi de l'usure "normale" des disques internes.

Lorsque les disques utilisés supportent les informations d'état **smart**, il devient possible de vérifier leur état, mais aussi de lancer un démon qui nous alerte en cas de risque.

Le contrôle se fait au détriment d'une légère perte de performance.

Installation :

```
root@luciole:~# apt-get install smartmontools
```

Le démon smartd est alors installé et peut prévenir l'administrateur par mail lorsque les informations d'état des disques atteindront les seuils d'alertes.

La vérification se fait au démarrage et est modifiable en éditant *etc/smartd.conf*.

Si les erreurs disque n'ont pas été corrigées il faut fortement songer à changer de disque...

Attention à l'usage de *smart* avec le *RAID* qui pose problème avec certains contrôleurs.

Pour savoir si *smart* est activé sur le disque :

```
root@luciole:~# smartctl -i /dev/sda
smartctl version 5.38 [x86_64-unknown-linux-gnu] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/
```

```
=== START OF INFORMATION SECTION ===
Device Model:          FUJITSU MHW2160BH PL
Serial Number:         K10FT7A25Y3B
Firmware Version:      0084001E
User Capacity:         160 041 885 696 bytes
Device is:              Not in smartctl database [for details use: -P showall]
ATA Version is:        8
ATA Standard is:        ATA-8-ACS revision 3b
Local Time is:          Sun May 24 18:33:45 2009 CEST
SMART support is:       Available - device has SMART capability.
SMART support is:       Enabled
```

```
root@luciole:~# smartctl -A /dev/sda
smartctl version 5.38 [x86_64-unknown-linux-gnu] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/
```

Pour l'activer si nécessaire :

```
root@luciole:~# smartctl -s /dev/sda
```

Consultation de l'état d'un disque :

```
=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 16
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
 1 Raw_Read_Error_Rate      0x000f   100    100   046   Pre-fail Always    -        18278
 2 Throughput_Performance    0x0005   100    100   030   Pre-fail Offline   -        39256
 3 Spin_Up_Time              0x0003   100    100   025   Pre-fail Always    -         1
 4 Start_Stop_Count          0x0032   099    099   000   Old_age  Always    -        603
 5 Reallocated_Sector_Ct     0x0033   100    100   024   Pre-fail Always    -       85899
 7 Seek_Error_Rate           0x000f   100    100   047   Pre-fail Always    -       1690
 8 Seek_Time_Performance     0x0005   100    100   019   Pre-fail Offline   -         0
 9 Power_On_Hours            0x0032   080    080   000   Old_age  Always    -      10494
10 Spin_Retry_Count          0x0013   100    100   020   Pre-fail Always    -         0
12 Power_Cycle_Count         0x0032   100    100   000   Old_age  Always    -        564
```

192	Power-Off_Retract_Count	0x0032	100	100	000	Old_age	Always	-	9
193	Load_Cycle_Count	0x0032	079	079	000	Old_age	Always	-	42276
194	Temperature_Celsius	0x0022	100	100	000	Old_age	Always	-	42 (1
195	Hardware_ECC_Recovered	0x001a	100	100	000	Old_age	Always	-	166
196	Reallocated_Event_Count	0x0032	100	100	000	Old_age	Always	-	45350
197	Current_Pending_Sector	0x0012	100	100	000	Old_age	Always	-	0
198	Offline_Uncorrectable	0x0010	100	100	000	Old_age	Offline	-	0
199	UDMA_CRC_Error_Count	0x003e	200	200	000	Old_age	Always	-	0
200	Multi_Zone_Error_Rate	0x000f	100	100	060	Pre-fail	Always	-	10052
203	Run_Out_Cancel	0x0002	100	100	000	Old_age	Always	-	37323
240	Head_Flying_Hours	0x003e	200	200	000	Old_age	Always	-	0

Lecture du résultat : :

TYPE :

Old_age : indique qu'un dépassement n'est pas critique, nous avons simplement dépassé la garantie par le constructeur.

Pre-fail : indique que tout dépassement risque de provoquer une perte du disque.

UPDATED :

Always : la valeur est maintenue à jour.

Offline : la valeur est calculée uniquement lors des tests.

VALUE : La valeur actuelle du disque. Une valeur comprise entre 100 et 255 indique généralement une bonne santé du disque.

WORST : La pire valeur enregistrée par le disque.

THRESH : La valeur seuil en dessous de laquelle le disque commence à souffrir.

RAW VALUE : est la conversion de VALUE dans les unités utilisées par le constructeur.

Il existe plusieurs types de tests pour mettre à jour les valeurs : :

offline : le disque ne doit pas être monté.

short : test court sur les performances, les problèmes électriques et lectures/écritures physiques.

long : version longue du précédent.

Lancement d'un test : :

```
root@luciole:~# smartctl -t long /dev/sda
```

```
smartctl version 5.38 [x86_64-unknown-linux-gnu] Copyright (C) 2002-8 Bruce Allen
```

```
Home page is http://smartmontools.sourceforge.net/
```

```
=== START OF OFFLINE IMMEDIATE AND SELF-TEST SECTION ===
```

```
Sending command: "Execute SMART Extended self-test routine immediately in off-line mode".
```

```
Drive command "Execute SMART Extended self-test routine immediately in off-line mode" successful
```

```
Testing has begun.
```

```
Please wait 92 minutes for test to complete.
```

Test will complete after Sun May 24 20:18:57 2009

Use `smartctl -X` to abort test.

Pour voir le résultat il faut soit consulter les *logs* soit :

```
smartctl -c /dev/sda
smartctl -l selftest /dev/sda
smartctl -A /dev/sda
```

Configuration de **smartd** :

Le man de **smartd** donne l'ensemble des informations permettant de configurer le démon qui scrute l'état des disques.

Informations :

- http://fr.wikipedia.org/wiki/Self-Monitoring,_Analysis_and_Reporting_Technology
- <http://linux-attitude.fr/post/Soyez-encore-plus-a-lecoute-de-vos-disques>

Les montages en raid

Le RAID (Redundant Array of Independent Disk) permet d'augmenter la tolérance aux pannes ou d'avoir un espace de stockage plus rapide ou plus grand que ce que l'on obtiendrait avec un seul disque.

La tolérance est obtenue soit par mirroring, soit par calcul de parité.

Les performances sont obtenues par multiplexage des disques, par exemple un mot de 4 octets voit chacun de ses octets écrits en parallèle sur 4 disques différent.

La concaténation permet elle de disposer virtuellement d'un seul disque dont la capacité est la somme de chacun des disques.

Voir : [http://fr.wikipedia.org/wiki/RAID_\(informatique\)](http://fr.wikipedia.org/wiki/RAID_(informatique))

Le RAID 0

On cherche les performances sans tolérance aux pannes.

Le RAID 1

L'information est dupliquée sur les disques qui sont donc montés en miroir.

Le RAID 5

Il nécessite au minimum 3 disques.

Les informations sont stockées par bande (strip).

Par exemple pour un système à 3 disques, deux bandes de données et une de parité sont écrites alternativement sur les 3 disques.

Les bandes de parités sont écrites alternativement sur tous les disques façon à accroître la résistance aux pannes.

Elles sont calculées en faisant un ou exclusif des bandes de données précédentes.

La gestion du RAID logiciel par Linux

La commande **mdadm** permet de gérer les disques *RAID*.

La commande **mdadm --create** permet d'initialiser un disque *RAID*.

La commande **mdadm --detail /dev/mdX** affiche l'état d'un *RAID*.

La commande **mdadm --daemonise /dev/mdX** démarre le *RAID*.

Le fichier */etc/mdadm/mdadm.conf* contient la configuration utilisée par **mdadm** au démarrage.

La commande **mdadm --detail --scan --verbose** permet de récupérer la configuration et si nécessaire de la stocker dans */etc/mdadm/mdadm.conf* pour le prochain démarrage.

Lien : http://doc.ubuntu-fr.org/raid_logiciel

Exemple creation d'un disque :

```
fdisk /dev/sda #Pour la création de /dev/sda1
fdisk /dev/sdb #Pour la création de /dev/sdb1
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sda1 /dev/sdb1
mdadm --daemonise /dev/md0
#sinon en éditant /etc/mdadm/mdadm.conf on peut y ajouter
#ARRAY /dev/md0 level=raid1 num-devices=2 devices=/dev/sda1,/dev/sdb1
```

Les périphérique *RAID* apparaissent sous */dev/md#*.

LVM

LVM Logical Volume Manager s'intercale entre le noyau et les partitions des disques afin de permettre :

- de redimensionner les partitions,
- de concaténer les disque,
- de réaliser des instantanés du système de fichier.

Sa mise en place doit être faite dès le partitionnement (type 8E).

GRUB ne fonctionne pas avec *LVM* il faut donc soit utiliser *Lilo* soit réserver *LVM* à */home*.

Glossaire :

PV *Physical Volume* est un disque ou un ensemble de disque utilisé par *LVM*,

VG *Volume Group* est un ensemble de PV,

LV *Logical Volume* est une partie du *VG* vue par l'utilisateur comme s'il s'agissait d'une partition,

PD *Physical Device* est ensemble de partition d'un disque utilisé par *LVM*,

PE *Physical Extent* est la plus petite unité de données gérée par *LVM* (\sim 4Mo).

Les modules de *LVM* doivent être montés avec *modprobe dm_load*.

La commande **vgscan** permet de lancer *LVM*.

La commande **pvcreeate** permet de créer un volume physique.

La commande **vgcreate** permet de regrouper le *PV* dans un groupe de volume.

La commande **lvcreate** permet de créer le volume logique.

Il ne faut pas oublier de formater un volume logique pour pouvoir s'en servir, on utilise alors *mkfs* classiquement.

La commande **lvextend** permet de modifier la taille d'un *LV*.

Pour retailer le système de fichier on utilisera la commande **resize2fs** après avoir démonté le système de fichier.

Python

Le scripting bash peut vite s'apparenter à du développement, alors pourquoi ne pas utiliser un vrai langage de programmation ?

Historique

Python a été créé fin 1986 par Guido van Rossum au CWI (Institut de recherche en mathématique et informatique de Hollande), à partir de la version 1.2 en 1995 le CNRI (Corporation of National Research Initiative) finance le projet.

En 2000 Python passe en version 2.0 au sein de Be.open, puis l'équipe rejoint Digital Creation (Futur Zope Corporation) en 2001. En mars 2001 création de la python foundation et libération complète du code.

La notion d'objet

Tout est objet.

La notion de classe

Tous les objets appartiennent à une classe.

L'instruction print

Exemple : :

```
print(1)
print("Hello world")
print('coucou')
```

Les primitives d'accès aux informations de type

id() renvoie l'identifiant d'un objet.

type() renvoie le type de l'objet.

dir() liste les attributs des objets.

Les commentaires

Le caractère **#** marque le début d'un commentaire.

Les chaînes de caractères

En python 3 l'encodage par défaut est UTF-8 qui est une représentation des types unicode.

On passe d'unicode au str en appelant la fonction encode (u"C'est la fête".encode('ISO-8859-15')).

On passe du str au unicode par la fonction decode.

Les délimiteurs et types de chaînes :

- Les guillemets " et """,
- Les apostrophes ',
- Les chaînes raw r",
- Les chaînes formatable f",

Les numériques

Les entiers (0 à 2^{32}) pour le type **int** et pour les entiers longs de type **long** on suffixe par un L ou l, la représentation octale commence par un 0 et l'hexadécimale par 0x.

Le type **bool** (True, False)

Les valeurs à virgule flottante (0.1 et 1e100) leur type est **float**.

Les nombres complexes (1 + 3j) leur type est **complex**.

Les types à valeur unique

None

NotImplemented

Les séquences

Les tuples ()

Les listes []

Les dictionnaires {}

Les opérateurs

L'affectation =

La division / (Attention identique au C donc $5/6 = 0$ mais $5.0/6 = 0.83333....$)

La division entière //

Le modulo % ou divmod(5,3) = (1,2)

La négation -

L'inversion bit à bit ~ (complément à un)

La puissance **

Appartenance in

Opérateurs binaires

Le et &

Le ou |

Le ou exclusif ^

Opérateurs de comparaison

Inférieur <

Supérieur >

Inférieur égal <=

Supérieur égal >=

égalité == différence != ou <>

le est is

le n'est pas is not

Ordre de traitement des opérations

Parenthèses, Exposants, Division, Multiplication, Addition, Soustraction

L'instruction pass

L'indentation

La création de block de code se fait par indentation.

Les structures conditionnelles

L'instruction if (else et elif)

L'instruction for in

L'instruction while

Les fonctions

La définition des fonctions se fait à l'aide de l'instruction « def ».

La fonction est un objet.

Le code doit être indenté.

Les paramètres ne sont pas typés.

Les paramètres peuvent recevoir une valeur par défaut $p1 = 0$.

Les paramètres non explicites (ex: `def f(**dict)`) sont placés dans un dictionnaires.

Les paramètres arbitraires (ex : `def f(*pars)`) sont placés dans un tuple.

Combinaison paramètres implicites et arbitraires (ex: `def f(*pars, **dict)`).

La directive return

La directive lambda

Les docstrings

Les fonctions du code peuvent être documentées, ce qui permet lors de l'exécution d'un code d'interroger une fonction pour savoir comment elle fonctionne.

Les décorateurs

On peut en python définir des fonctions qui compléteront d'autres fonctions sur le principe de la composition mathématique.

Exemple :


```
def mondecorateur(fonction) :
    def nouvellefonction() :
        print('execution de %s'%fonction.__name__)
        return fonction()
    return nouvellefonction
```

```
@mondecorateur
def f() :
    print('coucou')
```

```
f()
>>execution de f
>>coucou
```

Utile pour tester les pré-conditions des fonctions.

Les Classes

Les classes regroupent à la fois des données et des fonctions travaillant sur ces données.

Elles sont définies par l'instruction class

Les classes peuvent hériter d'autres classes.

Exemple : :

```
class Animal(object):
    def __init__(self):
        self.age = 0
        self.poids = 0

class Chat(Animal):
    def __init__(self, nom):
        super(Chat, self).__init__() # Permet de construire la partie Animal
        self.nom = nom
```

La notion de constructeur `__init__`

La notion de destructeur `__del__`

Les attributs privés

Les exceptions

Les erreurs sont signalées par le mécanisme des exceptions : :

```
>>> try:
...     PasDefinie = None
... except NameError:
```

```
...     print("Variable non définie")
...
Variable non définie
```

Les modules

Les bibliothèques de programmation en python s'appellent des modules.

Primitive import

Primitive reload

Les paquets

Les modules sont généralement découpés en paquets qui se traduisent par des dossiers sur le disque.

Les principaux modules

Contient les primitives

sys

Contient les informations relative à l'exécution en cours

os

Permet de gérer le système

gzip, zipfile

Permettent de gérer les fichiers compressés.

socket

Pour gérer les connexions TCP ou UDP

urllib2

Pour gérer les connexions http

Liens :

- <http://diveintopython.adrahon.org/>
- <http://docs.python.org/>
- <http://www.afpy.org/>

Initialisation du système et des services

La séquence de boot

Au démarrage de l'ordinateur, le bios cherche un périphérique d'amorçage selon l'ordre établi par sa séquence de boot.

Le bios lance le chargeur (loader) qui se trouve dans le MBR (Master Boot Record) et qui ne fait que 512 octets.

Si le chargeur est GRUB, alors le MBR ne contient que la 1er partie de GRUB appelée *stage 1* qui a pour unique rôle de charger *stage 1_5* et *stage 2*.

Stage *1_5* contient le code d'accès aux différents systèmes de fichiers. Il est contenu dans les premiers secteurs et peut avoir une taille de 33ko.

Puis *stage 2* est chargé, il peut être n'importe où sur le disque.

Stage 2 propose à l'utilisateur de choisir le système d'exploitation ou la version du noyau à démarrer à travers un menu.

L'utilisateur peut aussi modifier la configuration de démarrage en éditant le menu (appuyer sur *e*).

Stage 2 charge alors l'image du système d'exploitation choisi, le fichier se trouve généralement dans */boot* et porte un nom du type *vmlinuz-2.6.XXX*.

/boot contient aussi des fichiers *initrd* qui permettent de gérer les périphériques nécessitant le chargement de module spécifique (cas des systèmes de fichier non inclus au noyau).

Le menu de démarrage passe quelques options à l'image du système, notamment le nom du périphérique contenant la racine exemple : *root=/dev/sda1*.

Une fois le noyau lancé, il exécute */sbin/init* avec 1 comme PID.

init démarre les démons qui vont par exemple configurer les services réseau.

GRUB

GRUB est l'acronyme de GRand Unified Bootloader. C'est un programme GNU de démarrage permettant de choisir le système d'exploitation qui sera chargé.

Le fichier */boot/grub/menu.lst* permet de créer le menu de démarrage, et d'imposer un choix par défaut. + *GRUB* peut charger l'image du noyau depuis le réseau.

La version 2 est celle installée avec Ubuntu 20.04.

La mise à jour du noyau entraîne la modification du fichier */boot/grub/grub.cfg*, mais il est possible de la forcer avec la commande **update-grub**.

Pour customiser le bootloader on doit éditer le fichier */etc/grub.d/40_custom*

Lors du démarrage de Grub on peut passer des options au kernel en appuyant sur la touche "e".

Voir la doc : <https://doc.ubuntu-fr.org/grub-pc>

Démarrage du noyau

Il est possible de passer des options au noyau lors de son démarrage.

La syntaxe des options est :

`option1=valeur option2=valeur1,valeur2`

Les arguments ou paramètres du kernel

Les principales options d'amorçage du noyau sont :

- `root=/dev/sda1` indique la partition système,
- `ro` Indique que le système de fichier doit être monté en lecture seul,
- `init` permet de démarrer un autre processus à la place d'*init*,
- `single` ou `emergency` permet de passer en mode simple utilisateur et permet par exemple de pouvoir modifier le mot de passe root,
- `quiet` démarre en mode silencieux,
- `nosmp` n'utilise qu'un seul processeur,
- `noht` pas d'hyper threading,
- `noapic` pas de détection des interruptions,
- `nolapic` aucune gestion des interruptions,
- `apm=off` on désactive ou active la gestion de l'alimentation en énergie,
- `noresume` ne réveille pas une hibernation.

Systemd vs InitV vs upstart

@TODO Systemd

InitV signifie Init system V.

Ce système est remplacé par **upstart** sur les dernières Ubuntu et Fedora.

Au démarrage, le noyau lance *init*.

L'ancien système était paramétrable via le fichier */etc/inittab* qui est remplacé par la notion de *job*.

init lit le répertoire */etc/event.d* qui contient les jobs à lancer.

Chaque job réalise des actions en fonction du niveau d'exécution du noyau.

init se charge de maintenir les jobs opérationnels.

La commande **initctl** permet de communiquer avec **init**.

La liste des jobs démarrés est donnés par **initctl list** :

```
root@luciole:~# initctl list
control-alt-delete (stop) waiting
last-good-boot (stop) waiting
logd (stop) waiting
rc-default (stop) waiting
rc0 (stop) waiting
rc1 (stop) waiting
rc2 (stop) waiting
rc3 (stop) waiting
rc4 (stop) waiting
rc5 (stop) waiting
rc6 (stop) waiting
rcS (stop) waiting
rcS-sulogin (stop) waiting
sulogin (stop) waiting
tty1 (start) running, process 10354
tty2 (start) running, process 8436
tty3 (start) running, process 8437
tty4 (start) running, process 8429
tty5 (start) running, process 8430
tty6 (start) running, process 8439
```

Le lancement d'un job se fait par *initctl start rc0*, son arrêt par *initctl stop rc0*.

Liens :

- <http://www.digitbooks.fr/articles/2-upstart.html>

Les niveaux d'exécution (Run level)

Signification des niveaux pour Ubuntu :

Niveau S : Initialisation du système (le système de fichier est en read only),
Niveau 0 : Extinction,
Niveau 1 : Mode mono utilisateur,
Niveau 2 et 5 : Mode multi-utilisateurs avec réseau avec démarrage du serveur X,
Niveau 6 : Reboot.

Le système de démarrage des services

Lors du lancement d'*init* par le noyau, celui-ci transmet l'information de niveau à exécuter.

Ainsi *init* lance les jobs en leur précisant le niveau demandé.

Le job *rc5* lance */etc/init.d/rc 5*, qui à son tour va lancer les scripts contenu dans */etc/rc5.d* selon l'ordre lexicographique.

Les répertoires */etc/rcX.d* contiennent des liens vers les scripts de */etc/init.d*.

Les scripts contenus dans */etc/init.d* permettent de démarrer, arrêter, ou connaître le statut des démons.

Changement du niveau d'exécution

Il est possible de changer le niveau d'exécution.

Exemple pour arrêter la machine :

```
initctl emit runlevel 0
```

Modules

Le noyau Linux est modulaire.

La gestion de nombreux périphériques n'est pas faite dans le noyau mais dans des modules qui sont chargés à la demande.

La commande **modprobe** permet de charger un module directement par son nom.

La commande **lsmod** permet de connaître les modules déjà chargés.

La commande **rmmod** permet de supprimer un module du noyau.

Il est possible d'intégrer définitivement les modules au noyau en recompilant celui-ci.

Configuration réseau et outils TCP/IP

Introduction

L'unix BSD a été l'une des premières plateformes à supporter la pile protocolaire TCP/IP.

Dans cette tradition GNU/Linux regorge d'outils TCP, UDP, ICMP.

TCP signifie Transmission Control Protocol.

IP : Internet Protocol.

UDP : User Datagram Protocol.

ICMP : Internet Control Message Protocol.

Sous Ubuntu l'installation configure l'interface réseau en client DHCP (Dynamique Host Configuration Protocol).

De nombreux programmes communiquent entre eux sur la machine en utilisant l'interface réseau *loopback* de nom *localhost* et d'adresse *127.0.0.1* et ceci alors même que la connexion ne sort pas de la machine.

Liens :

- <http://fr.wikipedia.org/wiki/Tcp>
- http://fr.wikipedia.org/wiki/Internet_Protocol

Configuration automatique

Le protocole DHCP permet de demander à un serveur une adresse IP ainsi que les paramètres de connexion tels que le masque de sous réseau, les DNS, la passerelle.

La commande **dhclient**, permet de relancer la négociation avec le serveur.

Infos : <http://fr.wikipedia.org/wiki/DHCP>

La commande ip

La commande ip permet d'afficher et modifier toutes les interfaces réseaux.

ip addr : Affiche les adresses ip et toutes les informations. ip addr show dev em1 : Affiche les informations pour le périphérique em1 ip addr add 192.168.1.1/24 dev em1 : Ajoute l'adresse 192.168.1.1 avec le masque 24 au périphérique em1.

ip link : Gère et affiche toutes les interfaces réseaux. ip link show dev em1 : Affiche les informations pour em1. ip -s link : Affiche les interfaces statiques. ip link set dev eno12345678 up : Met en fonctionnement l'interface eno12345678. ip link set dev eno12345678 down : Éteint l'interface eno12345678.

ip route : Affiche et permet la modification de la table de routage.

ip maddr : Affiche et permet la gestion des adresses multicast. ip maddr show dev em1 : Affiche les informations multicast de em1

ip neigh : Affiche les objets voisins c'est à dire la table ARP pour IPv4. ip neigh show dev em1 : Affiche le cache ARP de l'interface em1

La commande ip permet de consulter et changer l'état ou les paramètres de tous les types de périphériques réseaux. Elle remplace les commandes ifconfig, iwconfig, ifup/ifdown, route que nous détaillerons ci après, car elles sont encore proposées par certaines docs.

voir :

<http://cpham.perso.univ-pau.fr/ENSEIGNEMENT/UERHD/DescriptifCmdIP.pdf>

https://access.redhat.com/sites/default/files/attachments/rh_ip_command_cheatsheet_1214_jcs_print.pdf

ifconfig (déprécié)

La commande **ifconfig** permet à la fois de consulter les paramètres réseau mais également de configurer les interfaces. Cette commande est aujourd'hui obsolète et remplacée par **ip** que nous détaillerons ci-après, on peut l'installer avec **apt install net-tools**. Toutefois elle est beaucoup plus simple, mais moins complète que **ip**.

Exemple de configuration :

```
root@luciole:~# ifconfig eth0 192.168.0.7 netmask 255.255.255.0
```

La configuration ainsi réalisée n'est pas permanent, elle sera perdue au prochain démarrage.

Pour modifier de façon permanente la configuration réseau il faut éditer */etc/network/interfaces*.

ifconfig est remplacé par la commande **ip addr** ou **ip a** **ifconfig eth0 192.168.0.11** est remplacé par **ip addr add 192.168.0.11/255.255.255.0 dev enxe4b97aef38eb** Les noms comme eth0 sont remplacés par la convention de nommage **ifname** pour éviter le changement de nom lors du reboot.

iwconfig (déprécié)

La commande **iwconfig** permet de configurer les cartes wifi.

ifup/ifdown (déprécié)

La commande **ifup** permet de démarrer une interface réseau en fonction de la configuration indiquée dans */etc/network/interfaces* Remplacée par **ip link set NOM_PERIPHERIQUE up**

La commande **ifdown** permet de l'arrêter. Remplacée par **ip link set NOM_PERIPHERIQUE down**

route (déprécié)

La commande **route** permet de consulter et de fixer l'adresse de la passerelle :

```
root@luciole:~# route add default gw 192.168.0.1
```

Remplacée par **ip route**

En consultation elle est identique à **netstat -nr**

ip

La commande **ip** est le couteau suisse de la configuration réseau, son paquet **iproute2** remplace les commandes du paquet **net-tools** :

Attribuer une adresse : ::

```
ip addr add 192.168.0.54/24 dev eth0
```

Connaitre son adresse : ::

```
ip -4c addr show #-4 affiche uniquement les IPv4, -c pour l'affichage couleur
```

Activer une interface réseau : ::

```
ip link set eth0 up
```

Désactiver une interface réseau : ::

```
ip link set eth0 down
```

Supprimer une adresse d'une interface : ::

```
ip addr del 192.168.0.54 dev eth0
```

Ajouter une gateway : ::

```
ip route add default via 192.168.0.1
```

Les interfaces virtuelles

La création d'interface virtuelle permet de donner plusieurs adresses IP à une même carte réseau.

Cela permet par exemple de créer une adresse ip fixe pour une entrée DNS tout en la redirigeant via l'interface du datacenter vers une autre ip.

La ligne de commande est du type : :

```
ip link add link DEVICE name NAME type vlan
```

Voir <https://www.systutorials.com/docs/linux/man/8-ip-link/>

Fixer le nom de machine

La commande **hostname** permet à la fois de consulter et de changer le nom de la machine.

Il est maintenant souhaitable d'utiliser la commande **hostnamectl** par exemple comme suit :

```
hostnamectl set-hostname luciole
```

En effet de nombreuses machines reçoivent leur nom par la couche réseau lors du boot comme par exemple les images cloud.

Attention il ne s'agit pas du Fully Qualified Domain Name, mais seulement du nom de la machine sans le nom de domaine.

Positionner le reverse

Pour ne pas être considéré comme spammeur lors de l'envoi de mail il faut positionner le "reverse" du serveur sur le même Fully Qualified Domain Name (fqdn), c'est à dire que si on fait une recherche du nom de la machine à partir de son adresse ip, le résultat doit être le nom de la machine suivi de son domaine. Pour cela il faut :

- Vérifier que dans la zone DNS de notre registrar, là où on a enregistré le nom de notre domaine ;
- Aller sur l'interface d'administration du serveur (Scaleway, OVH, Gandi, etc) ;
- Modifier le reverse en donnant le fqdn de la machine.

Pour vérifier, il suffira de comparer l'adresse obtenue avec "dig \$FQDN_Du_Serveur" avec "dig -x \$IP_Du_Serveur".

Démarrage et arrêt du réseau

La commande `/etc/init.d/networking start` permet de démarrer la couche réseau.

La résolution de nom

La commande **dig** permet de réaliser la résolution de nom.

La commande **dig -x \$ADRESSE_IP** permet de réaliser la résolution inverse.

Le fichier `/etc/resolv.conf` est utilisé pour connaître les adresses des DNS.

La modification du fichier `/etc/hosts`

Le fichier `/etc/hosts` contient les adresses et noms des machines connues.

On y trouve au minimum la définition du loopback et de la machine.

Les valeurs qui y sont primées sur la résolution DNS.

Exemple : :

```
michaellaunay@griffon:~$ cat /etc/hosts
127.0.0.1 localhost griffon griffon.ecreall.com
88.191.77.45 griffon.ecreall.com
```

La modification est triviale puisqu'il suffit d'ajouter une ligne \$Adresse \$Nom1 \$Nom2.

Les outils et commandes de tests réseau

ping

La commande **ping** permet d'envoyer des paquets ICMP à une machine distante pour tester la connectivité du réseau.

host

Un autre utilitaire de résolution de nom de domaine. Traceroute
+++++

La commande **traceroute** permet de connaître les noeuds du réseau nous séparant d'une machine cible.

netstat

La commande **netstat** permet de connaître le statut des connexions réseaux.

netstat -tp permet de voir les connexions restées ouvertes et les processus associés.

Exemple :

```
root@luciole:~# netstat -taupe
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale      Adresse distante     Etat      User
tcp      0      0 luciole.local:34978  ecs.amazonaws.com:ww ESTABLISHED michaelauna
tcp      1      0 luciole.local:35516  ecs.amazonaws.com:ww CLOSE_WAIT  michaelauna
tcp      1      0 luciole.local:50217  ecs.amazonaws.com:ww CLOSE_WAIT  michaelauna
tcp      1      0 luciole.local:35515  ecs.amazonaws.com:ww CLOSE_WAIT  michaelauna
tcp      0      0 luciole.local:34979  ecs.amazonaws.com:ww ESTABLISHED michaelauna
```

Permet de voir des connexions en direction du cloud d'Amazon, un `cat /proc/11400/cmd` donne :

```
root@luciole:~# cat /proc/11400/cmd
/usr/lib/gvfs/gvfsd-http--spawner:1.82/org/gtk/gvfs/exec_spaw/0
```

On voit que la commande est *spawnée* ce qui signifie que si on la *kill* elle sera relancée par le système.

Après quelques recherches, il s'avère que c'est l'application *Rhythmbox* qui va chercher les couvertures des albums écoutés en utilisant le service gvfs.

tcpdump

La commande **tcpdump** permet "d'espionner" ce qui se passe sur nos interfaces réseau.

nmap

La commande **nmap** permet de scanner les ports d'une machine et donc de faire un diagnostic des éventuelles portes d'entrées.

ngrep

La commande **ngrep** permet de n'afficher les paquets réseaux qu'à la condition qu'ils contiennent la chaîne cherchée.

wireshark

Permet d'écouter les paquets réseaux comme ceux enregistrés par **tcpdump**.
last +++++

La commande **last** permet de connaître les derniers *login* réalisés sur la machine, leur date et adresse d'origine.

Gestion des paquetages et installation de logiciels sous Ubuntu

Ubuntu, un système "Grand Public"

Ubuntu simplifie extrêmement l'installation et devient donc facile d'accès pour un non linuxien.

Quelle version choisir et pour quel usage ?

Il existe deux types de versions :

- Une version serveur, dépouillée d'interface graphique, permettant d'utiliser RAID et LVM,
- Une version pc de bureau, utilisant Gnome.

Les dépôts

Nous avons vu précédemment la gestion graphique des dépôts.

Nous pouvons éditer le fichier */etc/apt/sources.list* et ajouter des dépôts.

Exemple : :

```
echo "deb http://packages.medibuntu.org/ karmic free non-free" >> /etc/apt/sources.list*
```

Toutefois il faudra télécharger la clé d'authentification du nouveau dépôt et l'ajouter avec : :

```
wget -q http://fr.packages.medibuntu.org/medibuntu-key.gpg -O- | sudo apt-key add -
```

Puis mettre à jour le cache avec **apt update**

Installation de paquets

La commande **apt install \$NOM_PAQUET** permet d'installer des paquets
::

```
apt install libdvdread7 mkisofs dvdbackup dvdauthor oggvideotools ffmpeg
apt install libavcodec-58 libavdevice58 libavformat58
```

Suppression de paquets

Pour supprimer un paquet on utilise **apt remove \$NOM_PAQUET**.

Informations sur les paquetages

Pour avoir la liste des paquets installés **dpkg -l**.

Recherche de paquetages

La commande **apt search \$MOT_CLE** permet de chercher un paquet à partir d'un mot de sa description.

Mise à jour des paquetages

Pour mettre à jour la distribution : :

```
apt update
apt upgrade
```

Interfaces graphiques

Il existe deux types d'interfaces graphiques, une en mode texte **aptitude** et une dans X11 **synaptic**.

Commande alien

La commande **alien** permet de transformer un paquet *rpm* en paquet debian et donc de pouvoir l'installer.

Apache

Présentation

Apache est un serveur web pouvant être utilisé comme proxy, cache etc.

Il supporte le protocole https et est donc utilisé pour servir les applications web à sécuriser.

Installation

La commande **apt install apache2** permet d'utiliser une version récente d'Apache.

Configuration

Nous allons créer un petit site *www.monsite.com* et nous allons voir comment le sécuriser.

Dans un premier temps nous allons ajouter sur le poste client les entrées *www.monsite.com* pour réaliser des tests sans passer par le DNS.

Ajout de *ssl.monsite.com* */etc/hosts* :

```
192.168.0.7 www.monsite.com
```

Puis sur le serveur nous allons activer les modules utilisés pour la sécurisation :

```
root@monserveur:~# a2enmod ssl
```

Cette commande créer 2 liens dans */etc/apache2/mods-enabled* pointant vers *../mods-available/ssl.conf* et *../mods-available/ssl.load*.

Pour ajouter un site, il suffit de créer un fichier de configuration dans */etc/apache2/sites-available* puis de l'activer :

```
root@monserveur:~# vim /etc/apache2/sites-available/www.monsite.com
```

```
<VirtualHost *:443>
    ServerAdmin michaelaunay@ecreall.com
    ServerName www.monsite.com
    SSLEngine on
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
    SSLCertificateFile /etc/apache2/ssl/server.crt
    SSLCertificateKeyFile /etc/apache2/ssl/server.key
    <Directory /var/www/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
    DocumentRoot /var/www
</VirtualHost>

<VirtualHost *:80>
    ServerAdmin michaelaunay@ecreall.com
    ServerName www.monsite.com
    <Directory /var/www/>
        Options Indexes FollowSymLinks MultiViews
```

```

                AllowOverride None
                Order allow,deny
                allow from all
    </Directory>
    DocumentRoot /var/www
</VirtualHost>

```

Puis d'activer le site :

```

root@monserveur:~# a2ensite www.monsite.com
root@monserveur:~# /etc/init.d/apache2 restart

```

Sécurisation

La sécurisation se fait en ajoutant un certificat X 509 sous forme d'une clé privée et d'une clé publique.

Nous verrons au chapitre X 509 l'usage d'une clé auto-signée.

Traçage

La configuration des logs permet de surveiller les accès aux sites.

On constatera que pour un site mis en ligne sur internet les tentatives d'intrusions sont importantes.

Postfix

Présentation

Postfix est un distributeur de courrier.

Il a pour rôle de recevoir le courrier, de le stocker dans la boîte mail du destinataire ou de le relayer à un autre serveur de mail si la boîte destinataire n'est pas sur sa machine.

Nous allons voir comment utiliser spf et dkim pour authentifier les mails.

Ressources postfix, spf, dkim et test

<https://www.nextinpact.com/article/30341/109074-emails-avec-spf-dkim-dmarc-arcet-bimi-a-quoi-ca-sert-comment-en-profiter> <https://www.bortzmeyer.org/7208.html> <https://ubuntu.tutorials24x7.com/blog/install-mail-server-on-ubuntu-20-04-lts-using-postfix-dovecot-and-roundcube> <https://ubuntu.tutorials24x7.com/blog/set-up-dkim-domainkeys-with-postfix-on-ubuntu-20-04-lts> <https://www.linuxbabe.com/mail-server/setting-up-dkim-and-spf>

Pour tester <https://www.appmaildev.com/en/spf>

RFC en français <https://www.bortzmeyer.org/7208.html>

Les variables d'opendkim <http://www.opendkim.org/opendkim.8.html>

Installation

```
apt install postfix
```

Lors de l'installation il faut préciser le nom du host, mettez le FQDN. Il faut que le reverse ait été correctement positionné sinon les mails risquent d'être considérés comme du spam dès la connexion du serveur. On va en profiter pour installer spf et dkim, puis, dmarc,

Si postfix transmet des mails :

```
apt install opendkim opendkim-tools #Pour la chaîne de signature
apt install mailutils # Pour pouvoir tester l'envoi de mail avec la commande mail
```

Si postfix gère la réception des mails alors installer aussi :

```
apt install postfix-policyd-spf-python
vim /etc/postfix/master.cf
#Ajouter en fin de fichier
policyd-spf unix - n n - 0 spawn
user=policyd-spf argv=/usr/bin/policyd-spf
```

L'édition du fichier master permet de lancer le démon d'analyse des mails reçus.

Configuration

Le fichier de configuration est */etc/postfix/main.cf*

Selon que le serveur est la destination ou seulement un relai on précisera *mydestination* ou non.

Exemple pour un serveur destinataire : :

```
michaellaunay@monserveur:~$ cat /etc/postfix/main.cf
biff = no
append_dot_mydomain = no
readme_directory = no
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
home_mailbox = Maildir/
mail_spool_directory = /var/spool/mail/
myhostname = monserveur.masociete.com
mydomain = masociete.com
myorigin = $mydomain
header_checks = regexp:/etc/postfix/header_checks
```



```

alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
relayhost =
mydestination = masociete.org, masociete.com, localhost.localdomain, localhost
unknown_local_recipient_reject_code = 550
mynetworks_style = host
mynetworks = 127.0.0.1, 82.236.252.174
mailbox_size_limit = 4294967296
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
message_size_limit = 10240000
header_size_limit = 102400
bounce_size_limit = 512000
disable_vrfy_command = no
smtpd_helo_required = yes
smtpd_banner = $myhostname ESMTP
maps_rbl_domains = relays.ordb.org, sbl.spamhaus.org, list.dsbl.org
smtpd_helo_restrictions = reject_invalid_hostname, permit
smtpd_sender_restrictions = reject_unknown_sender_domain, reject_non_fqdn_sender, permit
smtpd_client_restrictions = permit_mynetworks, reject_rbl_client, permit
smtpd_recipient_restrictions = permit_mynetworks,
                               permit_sasl_authenticated,
                               reject_unauth_destination,
                               check_policy_service unix:private/policyd-spf

milter_protocol = 6
milter_default_action = accept
smtpd_milters = inet:localhost:8992
non_smtpd_milters = inet:localhost:8992

```

Configuration de spf :

Ajouter une entrée spf à vos entrées DNS sur votre Registrar.

Par exemple le registrar de ****ecreall.com**** est OVH et il faut ajouter une entrée SPF et la

```

Sous-domaine []**ecreall.com** #Préciser le sous domaine, ici il n'y en a pas donc on la
TTL [Par défaut] #Mais pour les tests [Personnalisé] on peut alors mettre une valeur faible
Autoriser l'IP de **ecreall.com** à envoyer des emails ? [v]oui # on autorisera les adresses
Autoriser les serveurs MX à envoyer des emails [v]oui #si MX est notre serveur
Autoriser tous les serveurs dont le nom se termine par **ecreall.com** [v]Non # permet de
D'autres serveurs ? # Mettre les autres adresses ou noms autorisés à envoyer

```

Sous Gandi il ne faut surtout pas utiliser le champ spf qui est documenté comme obsolète, à

Il faut alors mettre "v=spf1 a mx ip4:62.210.112.125 -all" dans le champ.

La valeur des champs spf est expliquée par Google ici <https://support.google.com/a/answer/33>

Pour tester :

```
nslookup -type=txt ecreall.com
#Ce qui donne
ecreall.com text = "v=spf1 a mx ip4:62.210.112.125 -all"
```

Configuration de opendkim :

```
vim /etc/opendkim.conf
#Ajoutez ou mettez les variables à :
Domain          ecreall.com
KeyFile          /etc/dkimkeys/dkim.private
Selector        dkim
UserID          opendkim
Socket inet:8992@localhost
```

Le champ "Domain" indique quels vont être les mails signés avec la clé contenue dans le fichier "Keyfile" Le champ "Selector" indique quelle clé dans le fichier utilisée pour ce domaine. UssetId indique l'utilisateur du démon, attention le fichier de la clé privée doit pouvoir être lu par cet utilisateur. Socket Indique la socket qui sera utilisée par postfix pour se connecter et signer les mails transmis.

Génération de la clé de signature des mails :

```
cd /etc/dkimkeys/
opendkim-genkey -t -s dkim -d nova-ideo.com
chown root:opendkim dkim.private
chmod 660 dkim.private
```

L'attribut "-s dkim" permet de préciser de signer différemment chaque mail selon son domaine dans le cas où le serveur gère plusieurs domaines.

On a alors :

```
root@luciole:/etc/dkimkeys# ls -lh
total 12K
-rw-rw---- 1 root opendkim 1,7K févr. 11 16:09 dkim.private
-rw----- 1 root root      508 févr. 11 16:09 dkim.txt
-rw-r--r-- 1 root root      664 déc. 27 2019 README.PrivateKeys
```

Vérifier la clé :

```
root@luciole:/# opendkim-testkey -d ecreall.com -s dkim -vvv
opendkim-testkey: using default configfile /etc/opendkim.conf
opendkim-testkey: /etc/dkimkeys/dkim.private: WARNING: unsafe permissions
opendkim-testkey: key loaded from /etc/dkimkeys/dkim.private
opendkim-testkey: checking key 'dkim._domainkey.ecreall.com'
opendkim-testkey: key not secure
opendkim-testkey: key OK
```

La ligne "opendkim-testkey: key not secure" est due au fait DNSSEC n'a pas été activé sur le dns.

Afficher le contenu de dkim.txt

```
cat /etc/dkimkeys/dkim.txt dkim._domainkey IN TXT ( "v=DKIM1; h=sha256; k=rsa;
      "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxvKAG6fOfx+BnzZX1DSOp
      "EDR3fSMYQmMQfBc2hR8nLArbCQj3HdJD5LITNQ9HlnM8dX56/MonWyavIKKWp3CV9IQZ
      ) ; ---- DKIM key dkim for ecreall.com
```

Configurer votre registrar :

Se connecter à la zone DNS de son domaine, par exemple pour Ecreall dans OVH, on ajoute une

Sous-domaine [dkim._domainkey]

Version [v]

Algorithme (hash) -256 [v]

Clé Publique [MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1YRDtepyDeIgVolfFz4bRgacdE0hxGF
]

Type de service []

Mode test [v] # Permet de demander aux serveur recevant nos mails de ne pas tenir compte d

Sous domaine [v] La clé publique n'est pas valide pour les sous-domaine

Quand tout est au point ne pas oublier d'éditer l'entrée pour enlever le mode de test.

dmARC

L'ajout de DMARC se fait par simple ajoute d'une entrée de type DMARC ou TXT pour le sous-domaine _dmARC avec les valeurs suivantes :

```
v=DMARC1;p=quarantine;pct=100;rua=mailto:michaellaunay+dmARC@ecreall.com;sp=quarantine;aspf=
```

Où V est la version du protocole,

p est la politique à appliquer pour les messages reçu soit disant de notre domaine mais qui échoue, None (rien faire) ou Quarantine marquer douteux, Reject rejeter.

pct le pourcentage à traiter.

rua l'uri de la ressource à prévenir en cas d'usurpation.

sp la politique des sous domainkeys.

aspf s'il faut suivre spf à la lettre.

MySQL

Présentation

MySQL est une base de données légère facile à mettre en œuvre et très utilisée par les sites web.

Son utilisation est libre mais si les sources de l'application réalisée ne sont pas en GPL, il faut s'acquitter de l'achat d'une licence commerciale.

Installation

La commande **apt install mysql-server** permet d'installer le serveur contenant la base de données alors que **apt-get install mysql-client** se contentera d'installer le client.

Configuration

À l'installation, il est fortement recommandé de donner un mot de passe à l'utilisateur root.

Liens :

- <http://www-fr.mysql.com/>
- <http://fr.wikipedia.org/wiki/MySQL>

Sécurisation

Certificat X 509

Les certificats X 509 sont utilisés à la fois pour l'authentification et pour le chiffrement des infrastructures à clés publiques (PKI) comme par exemple dans le protocole ssl lors des connexions ssh (port 22) ou https (port 443).

Ils sont délivrés par une autorité de certification et sont liés à une adresse électronique ou à une entrée DNS.

Si l'autorité de certification est connue du navigateur, la connexion se fera sans alerter l'utilisateur. Dans le cas contraire, il sera prévenu que le site n'est pas de confiance.

Toutefois, il est possible de disposer des avantages du chiffrement sans passer par une autorité *de confiance*, en utilisant un certificat *auto-signé* :

```
root@monserveur:~# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/ssl/apache2/ssl/ssl.monsite.com
root@monserveur:~# vim /etc/apache2/sites-available/ssl.monsite.com
#remove SSLCertificateFile and update SSLCertificateKeyFile with
SSLCertificateKeyFile /etc/apache2/ssl/ssl.monsite.com.pem
root@monserveur:~# service apache2 restart
```

Mais les certificats autosignés ont l'inconvénient de ne pas avoir d'autorité connue et donc d'être refusé.

Nous pouvons utiliser les service let's encrypt qui permet de générer nos certificats ssl :

Configuration de Let's Encrypt pour générer nos certificats ssl :

```
apt install apache2 #Si ce n'est pas fait, vérifier que le port http est ouvert sur ufw !
apt install certbot
certbot certonly --webroot -w /var/www/html -d URL_De_Mon_Site
```

Vérification de la génération :

```
root@triticale:~# openssl x509 -noout -text -in /etc/letsencrypt/live/URL_De_Mon_Site/fullchain.pem
Not After : Aug  5 11:25:06 2020 GMT
```

Modifier le cron de renouvellement "/etc/cron.d/certbot" et mettre :

```
0 */12 * * * root test -x /usr/bin/certbot -a \! -d /run/systemd/system && perl -e 'sleep 10'
```

Liens :

- http://doc.ubuntu-fr.org/tutoriel/securiser_apache2_avec_ssl
- <http://fr.wikipedia.org/wiki/X.509>

postgrey

postgrey est un paquet de configuration de *postfix* permettant de différer la réception des mails des serveurs inconnus.

Le but est d'éliminer les spams, car les serveurs de spams ne prennent pas la peine de renvoyer un courrier dont la réception est différée.

fail2ban

Fail2ban est un démon qui permet de modifier les règles du firewall pour bannir pendant un temps déterminé les adresses IP qui ont échoué plusieurs connexions de suite à l'un des services du serveur.

Le temps d'exclusion, le nombre de tentatives tolérées, les adresses non bannies sont configurables via les fichiers `/etc/fail2ban/fail2ban.conf` et `/etc/fail2ban/jail.conf`.