

Linux administration

Sommaire 1/4

- Introduction
 - Historique
 - Types de licences
 - Distributions
 - Le rôle de l'admin et les aides
- Installation du systèmes
 - Les différents types d'installations
 - La mise a jour
 - Les environnements graphiques
- La gestion des logiciels
 - Administration des rpm
 - Exploitation de Yum, dpkg et aptitude
 - Installation à partir des sources

Sommaire 2/4

- La gestion du stockage
 - Terminologie
 - Tables de partitionnement MBT et GPT
 - Le partitionnement avec fdisk
 - La gestion de la swap
- La gestion des systèmes de fichiers
 - Les types de systèmes de fichiers
 - Création d'un systèmes de fichiers et contrôle d'intégrité
 - Montage d'un système de fichiers
 - Les commandes df et du
 - Les quotas
 - Systèmes de fichiers XFS : mise en oeuvre
- LVM
 - Présentation de LVM
 - Création et administration des volumes physiques
 - Des groupes de volumes
 - Des volumes logiques
 - Agrandissement
 - Suppression
 - Réduction

Sommaire 3/4

- Le RAID
 - Présentation des niveaux de RAIDs
 - Création et dépannage
 - Les diques hot-spare
- Le démarrage du système et des services
 - Séquence de démarrage
 - Grub Legacy, Grub2 et sécurisation
 - Les systèmes de démarrage sysinit, upstart et systemd
 - Ajout d'un service de démarrage
 - Arrêt du système
 - Le mode secours
- Administration des utilisateurs
 - Création, modification et suppression d'un compte
 - La sécurité avec PAM
 - La personnalisation de l'environnement utilisateur
 - Les permissions

Sommaire 4/4

- Sauvegarde et restauration
 - Les utilitaires de compression : gzip, bzip2, xy, zip
 - Les commandes tar, cpio, dd
 - La commande rsync
 - Les types de sauvegardes : totale, incrémentale, différentielle
 - Les commandes dump et restore
 - La procédure pour restaurer la racine
- Gestion des processus
 - Les états d'un processus
 - Les commandes ps, kill, pgrep, pkill, pstree, uptime, top
 - Les jobs
 - Execution différé avec at et crontab

Introduction

Historique

Types de licences

Distributions

Le rôle de l'administrateur et les aides

Historique

Linux est, au sens restreint, le noyau de système d'exploitation Linux, et au sens large, tout système d'exploitation fondé sur le noyau Linux.

- Créé en 1991 par Linus Torvalds, c'est un logiciel libre destiné en premier lieu pour les ordinateurs personnels compatibles PC, qui avec des logiciels GNU devait constituer un système d'exploitation à part entière.



Types de licences

- Une licence logicielle c'est quoi ?
 - C'est le contrat entre vous et le fournisseur du logiciel.
 - C'est un cadre juridique qui encadre l'utilisation du logiciel.
 - Ce qui est autorisé, ce qui est interdit.
 - Très bien, mais pourquoi on en a besoin, pourquoi sa existe ?

Types de licences

- Et bien produire un logiciel, sa coute chère...
 - Besoin d'une main d'oeuvre qualifié
 - Temps de développement long (des mois, voires années)
 - Et puis du code on peut le copié / collé :(
- Autant le cout de reproduction est faible, autant les couts initiaux sont très élevés.
- Une licences c'est l'outil juridique qui permet la propriété intellectuelle et sa protection, il encadre :

Types de licences

- Sa commercialité
 - Qui le vends, qui peut le vendre, au nom du qui et...
- Son utilisation, dans quel but
 - Est-ce que vous pouvez-vous en servir dans un cadre professionnel, ou juste pour un usage privé
 - Est-ce que vous pouvez modifier le logiciel.
- Ex d'un contrat apple :

Types de licences

1 / 397

100%

+



ENGLISH

APPLE INC.

SOFTWARE LICENSE AGREEMENT FOR OS X EL CAPITAN

For use on Apple-branded Systems

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING THE APPLE SOFTWARE. BY USING THE APPLE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT INSTALL AND/OR USE THE APPLE SOFTWARE AND, IF PRESENTED WITH THE OPTION TO "AGREE" OR "DISAGREE" TO THE TERMS, CLICK "DISAGREE". IF YOU ACQUIRED THE APPLE SOFTWARE AS PART OF AN APPLE HARDWARE PURCHASE AND IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, YOU MAY RETURN THE ENTIRE APPLE HARDWARE/SOFTWARE PACKAGE WITHIN THE RETURN PERIOD TO THE APPLE STORE OR AUTHORIZED DISTRIBUTOR WHERE YOU OBTAINED IT FOR A REFUND, SUBJECT TO APPLE'S RETURN POLICY FOUND AT http://www.apple.com/legal/sales_policies/. YOU MUST RETURN THE ENTIRE HARDWARE/SOFTWARE PACKAGE IN ORDER TO OBTAIN A REFUND.

machine-readable form for backup purposes only; provided that the backup copy must include all copyright or other proprietary notices contained on the original. Apple Boot ROM code and firmware is provided only for use on Apple-branded hardware and you may not copy, modify or redistribute the Apple Boot ROM code or firmware, or any portions thereof.

K. Migration of Existing Software. If you use Setup/Migration Assistant to transfer software from one Apple-branded computer to another Apple-branded computer, please remember that continued use of the original copy of the software may be prohibited once a copy has been transferred to another computer, unless you already have a licensed copy of such software on both computers. You should check the relevant software license agreements for applicable terms and conditions. Third party software and services may not be compatible with this Apple Software and installation of this Apple Software may affect the availability and usability of such third party software or services.

L. Open Source. Certain components of the Apple Software, and third party open source programs included with the Apple Software, have been or may be made available by Apple on its Open Source web site (<http://www.opensource.apple.com/>) (collectively the "Open-Sourced Components"). You may modify or replace only these Open-Sourced Components; provided that: (i) the resultant modified Apple Software is used, in place of the unmodified Apple Software, on Apple-branded computers you own or control, as long as each such Apple computer has a properly licensed copy of the Apple Software on it; and (ii) you otherwise comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components. Apple is not obligated to provide any updates, maintenance, warranty, technical or other support, or services for the resultant modified Apple Software. You expressly acknowledge that if failure or damage to Apple hardware results from modification of the Open-Sourced Components of the Apple Software, such failure or damage is excluded from the terms of the Apple hardware warranty.

M. No Reverse Engineering. You may not, and you agree not to or enable others to, copy (except as expressly permitted by this License or by the Usage Rules if they are applicable to you), decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify, or create derivative works of the Apple Software or any services provided by the Apple Software or any part thereof (except as and only to the extent any foregoing restriction is prohibited by applicable law or by licensing terms governing use of Open-Sourced Components that may be included with the Apple Software).

N. Compliance with Laws. You agree to use the Apple Software and the Services (as defined in Section 5 below) in compliance with all applicable laws, including local laws of the country or region in which you reside or in which you download or use the Apple Software and Services. Features of the Apple Software and the Services may not be available in all languages or regions and some features may vary by region. An Internet connection is required for some features of the Apple Software and Services.

Types de licences

- D'abord, on peut regrouper 5 types de logiciels :
 - Les logiciels propriétaires
 - Les logiciels du domaine public
 - Les gratuiciels «freeware »
 - Les partagiciels « sharewares »
 - Les logiciels libres

Les logiciels propriétaires

- Qui ont une licence qui ne permet que leur utilisation.
 - Accès au code source en général restreint.
 - Licences en général par utilisateur
-
- L'utilisateur n'a pas le droit d'en faire une copie
 - ex : un jeu vidéo

Les logiciels du domaine public

- Domaine public = pas de licence
- Pas de droits d'auteur
- L'entrée d'une œuvre dans le domaine public se fait en général au bout de 70 ans

Les gratuiciels «freeware»

- Logiciel distribué gratuitement à vie ou pour une durée de temp, permet de limiter les droits de copie/distribution
- En général fournit sans le code source, juste l'executable est distribué
- Ex : les antivirus grand public (Avast)

Les partagiciels « sharewares »

- Ressemble au freeware mais permet le partage du logiciel entre utilisateurs.

Les logiciels libres

- Un logiciel libre permet l'utilisation, l'étude, la modification, le partage et la duplication par autrui. (licences libres)
- Libre = ! gratuit
- Ex : Debian, le kernel/noyau linux

Licence libre

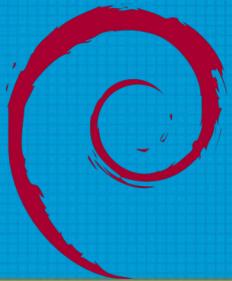
- Academic Free License : AFL
- [AiMSA License ↗ \[archive\]](#) : les restrictions apportées à la commercialisation, à la modification, à l'interprétation et à la représentation font de cette licence, au mieux, une licence de libre diffusion qui ne peut être considérée comme une licence libre.
- Apache License, Version 2.0 : AL20
- Apache Software License : ASL
- Apple Public Source Licenses : APSL
- [Association des bibliophiles universels](#) : Licence ABU³⁴
- BSD License : BSD
- Common Public License : CPL
- Licence CEA CNRS INRIA Logiciel Libre Version 2.0 : CeCILL
- Eiffel Forum Licence Version 2.0 : EFL version 2
- Eclipse Public License : EPL
- GNU General Public License : [GNU GPL](#)
- GNU Affero General Public License : [GNU AGPL](#)
- GNU Lesser General Public License : [GNU LGPL](#)
- IBM Public License : IBMPL
- Intel Open Source License : IOSL
- Microsoft Public License : Ms-PL
- [MIT Licence](#)
- Mozilla Public License Version 1.0 : MPL1.0
- Mozilla Public License Version 1.1 : MPL1.1
- Netscape Public License, Version 1.0 : NPL1.0
- Netscape Public License, Version 1.1 : NPL1.1
- Open Software License : OSL
- PHP License : PHPL
- Perl Artistic Licence : PAL
- Python License (CNRI Python License) : CNRIPPL
- [Python Software Foundation License](#) : PSFL
- QR COde
- Ruby license : [Licence Ruby](#)
- Sleepycat Software Product License : SL
- Sun Industry Standards Source License : SISSL
- Sun Public License : SPL
- [W3C Software License](#)
- [do What The Fuck you want to Public License](#) : WTFPL
- wxWindows Library License : WXWLL
- [zlib/libpng License](#) : ZLL
- Zope Public License : ZPL

Distributions

- Rappel :

Les distributions Linux sont des ensembles cohérents de logiciels, la plupart étant des logiciels libres, assemblés autour du noyau Linux, et formant un système d'exploitation pleinement opérationnel. Il existe une très grande variété de distributions Linux, chacune ayant des objectifs et une philosophie particulière.

Debian



- Se veut universelle, développé par le Debian Project
 - Organisation communautaire

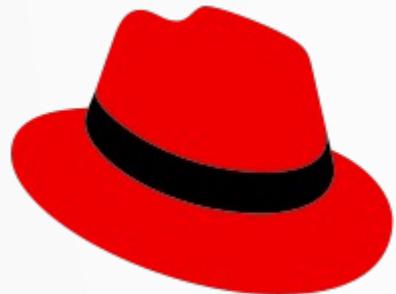
/usr/share/common-licenses



Ubuntu

- Basé sur Debian, Développée par une entreprise privée
- Vends du support pour leur distribution
- Déploie une maj stable tous les 6 mois
 - Une LTS (long term support) tous les 2 ans

Les distributions lié à l'entreprise Red Hat



RHEL - Red Hat
Enterprise Linux



Kali



- Basé sur Debian
- Distribution tourné vers :
 - la cybersécurité ou
 - la cybercriminalité
- Regroupe l'ensemble des outils nécessaires aux tests de sécurité,
 - test d'intrusion
 - Surveiller le réseau
 - casser les mots de passes
 - etc.

Licence libre

Développé par Offensive Security, entreprise privé



Le rôle de l'administrateur

- En tant qu'administrateur vous avez pour mission
 - La sécurité de votre systèmes d'informations
 - Son maintien en fonctionnement
 - La protection de vos données (perte et vol)
 - Son évolution dans son ensemble
 - L'inventaire du matériel informatique
 - Rédiger des procédures, les actualiser
 - Connaitre les normes, la réglementation
 - Piloter, Travailler en mode projet

Comment remplir vos missions

- Pour remplir cette missions, vous allez devoir :
 - Analyser le risque
 - Les points faibles de votre architecture
 - Les points forts
 - Les axes d'amélioration
 - Appliquer la stratégie du DSI
 - Piloter et l'appliquer
 - Etre force de proposition
 - Etre votre propre **MOTEUR**
 - Aller vers les autres, non l'inverse.

Comment remplir vos missions

- En perpetuelle apprentissage
 - Se documenter
 - Etre capable de faire ses propres recherches
- Gérer des projets, des prestataires
 - Notions gestion de projet
 - Agile
 - Scrum
 - Notions jour / homme
 - Prix, durée
 - Faire des devis, rediger un cahier des charge
- Bien Connaitre vos technos
- Superviser l'ensemble
 - Le Réseau
 - Les postes serveurs, clients

Installation du système

Les différents types d'installation et les étapes

La mise à jour

Les environnements graphiques

Prérequis

- En premier lieu, il nous faut le programme d'installation (image iso, image disque)
- Vous retrouverez en général plusieurs programmes d'installation par distribution
 - Les iso pour les serveurs
 - Les iso pour les stations de travail
 - En fonction de votre architecture pc (32bit - x86, 64bit x64, amd64)
- Leurs tailles peuvent varier en fonction de :
 - L'iso se veut minimaliste, une connexion internet est nécessaire
 - L'iso est complete, pas besoin d'internet
 - Iso + collections de programmes supplémentaires

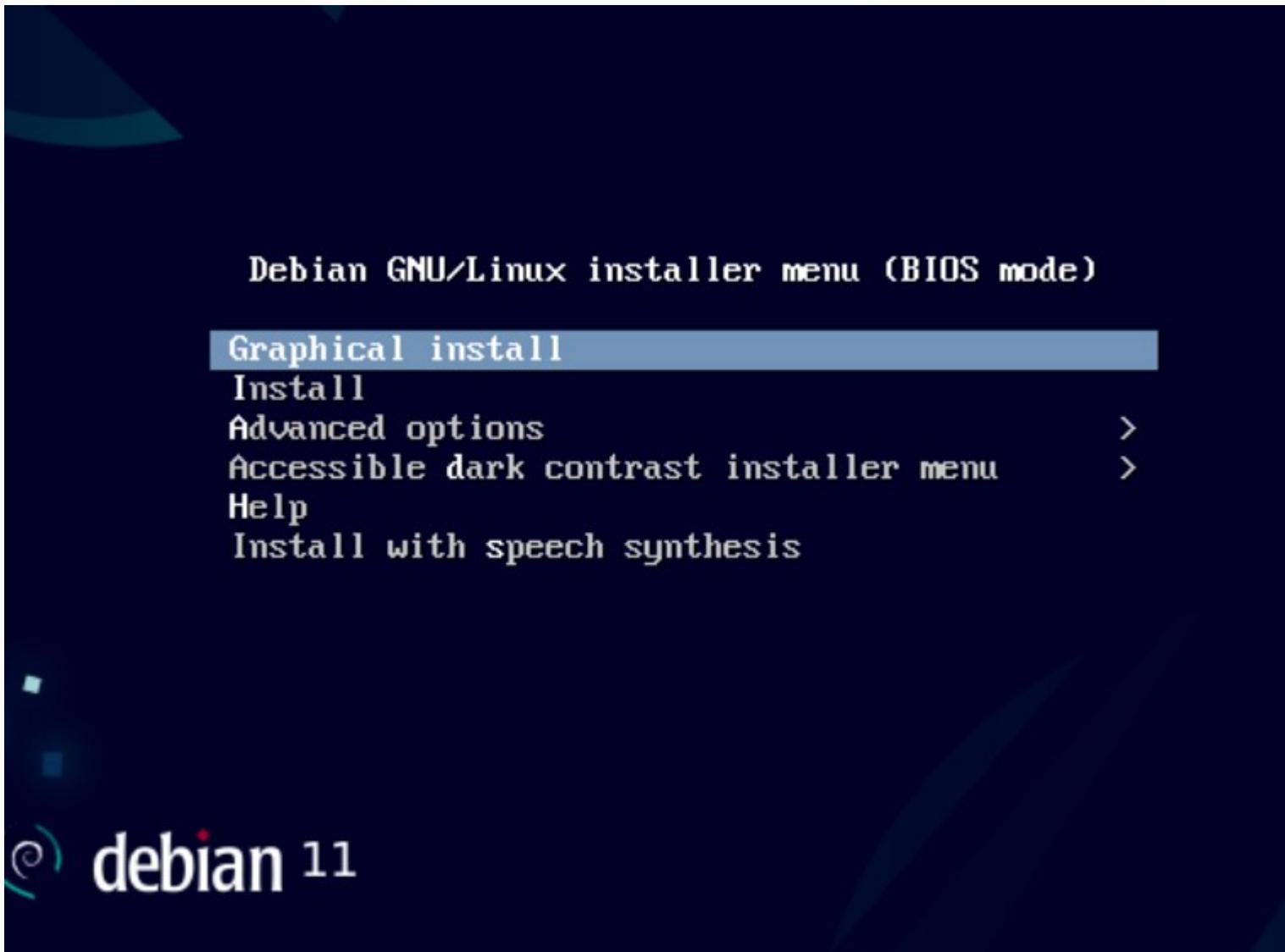
Prérequis

- Pour une vm (machine virtualisé):
 - Définir les spects techniques :ram, cpu, réseau, stockage
 - Définir le chemin vers l'iso
- Pour un poste non virtualisé :
 - Depuis un périphérique bootable (usb, disque, diquette, cd-rom) (ex : logiciel rufus)
 - Depuis le réseau (PXE : Preboot Execution Environment) PXELINUX
 - Modifier l'ordre du boot de votre machine depuis le bios, raccourci clavier à répéter juste après la mise sous tensions

Les différentes étapes

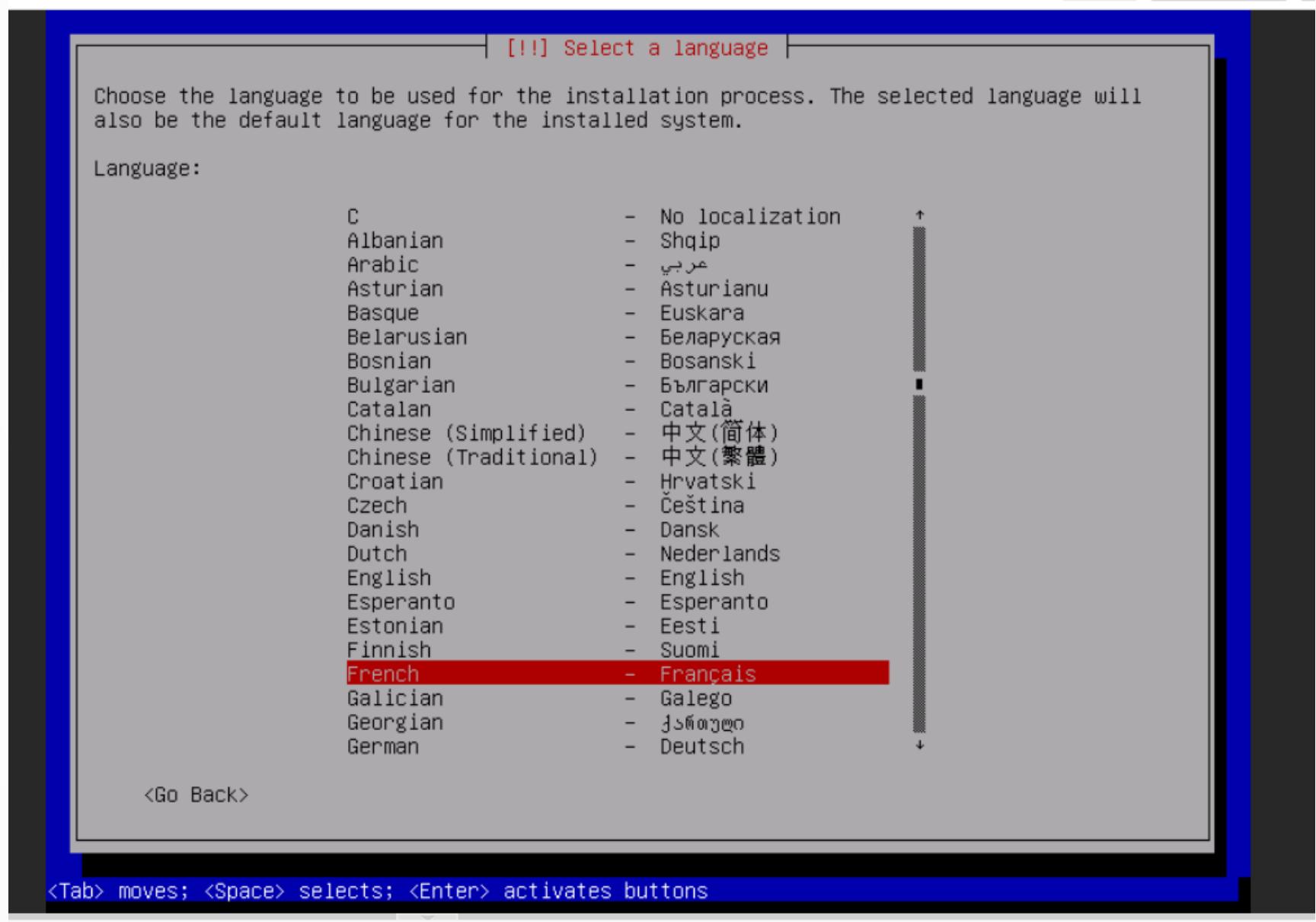
- Juste après avoir booter sur l'iso.
 - Un menu va apparaître
 - Plusieurs choix d'installation possible
 - Installation en mode graphique (souris intégré)
 - Installation normal (uniquement clavier)
 - Options avancées
 - Accès au mode sauvetage, rescue
 - Installations en mode expert (vue graphique, souris intégré)
 - Installation en mode expert (uniquement clavier)
 - Installations avec aide vocale
 - Page d'aide

Premier visuel

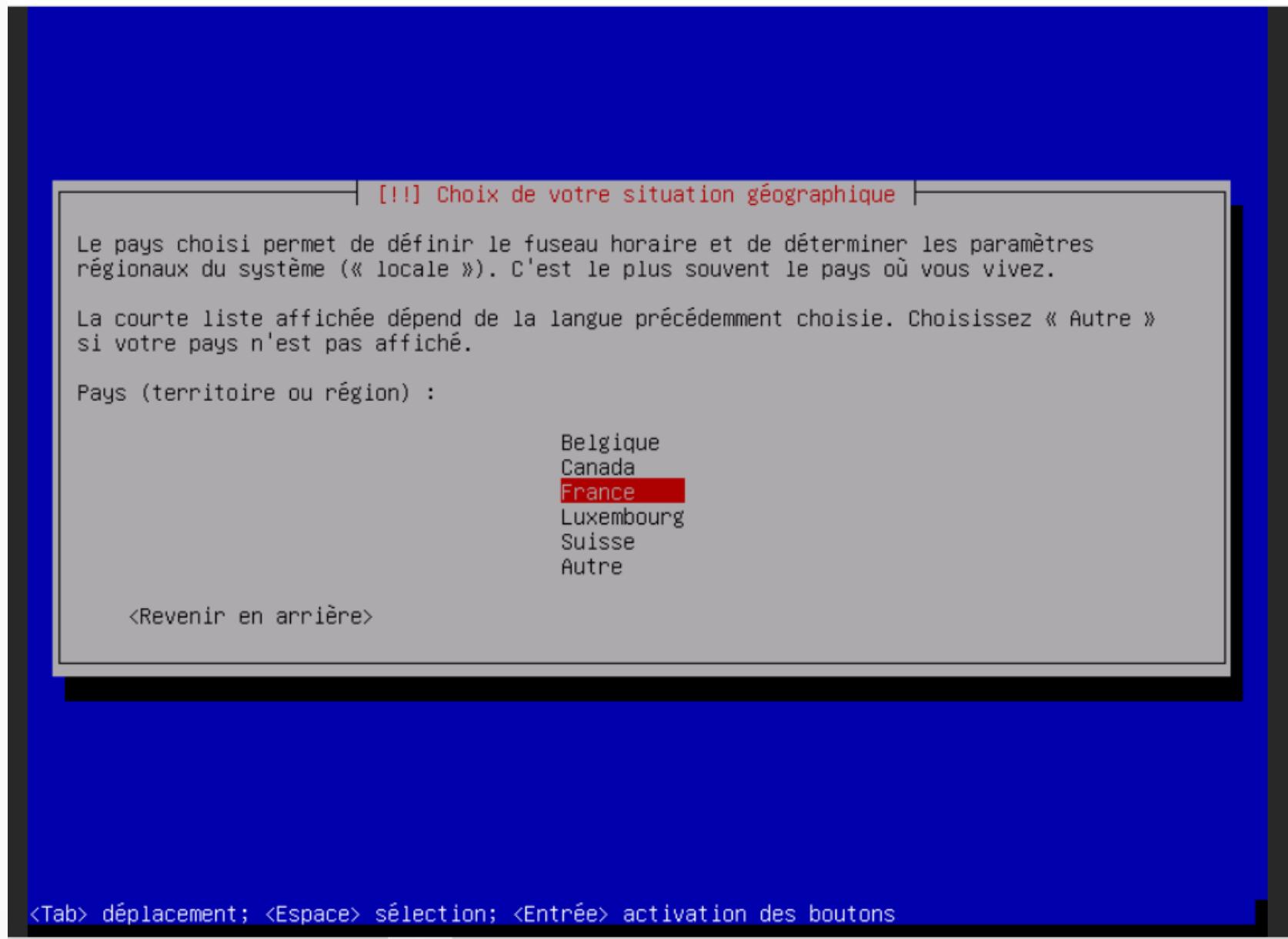


Pour une install simple

On se déplace avec les flèches, on choisit la langue puis entré



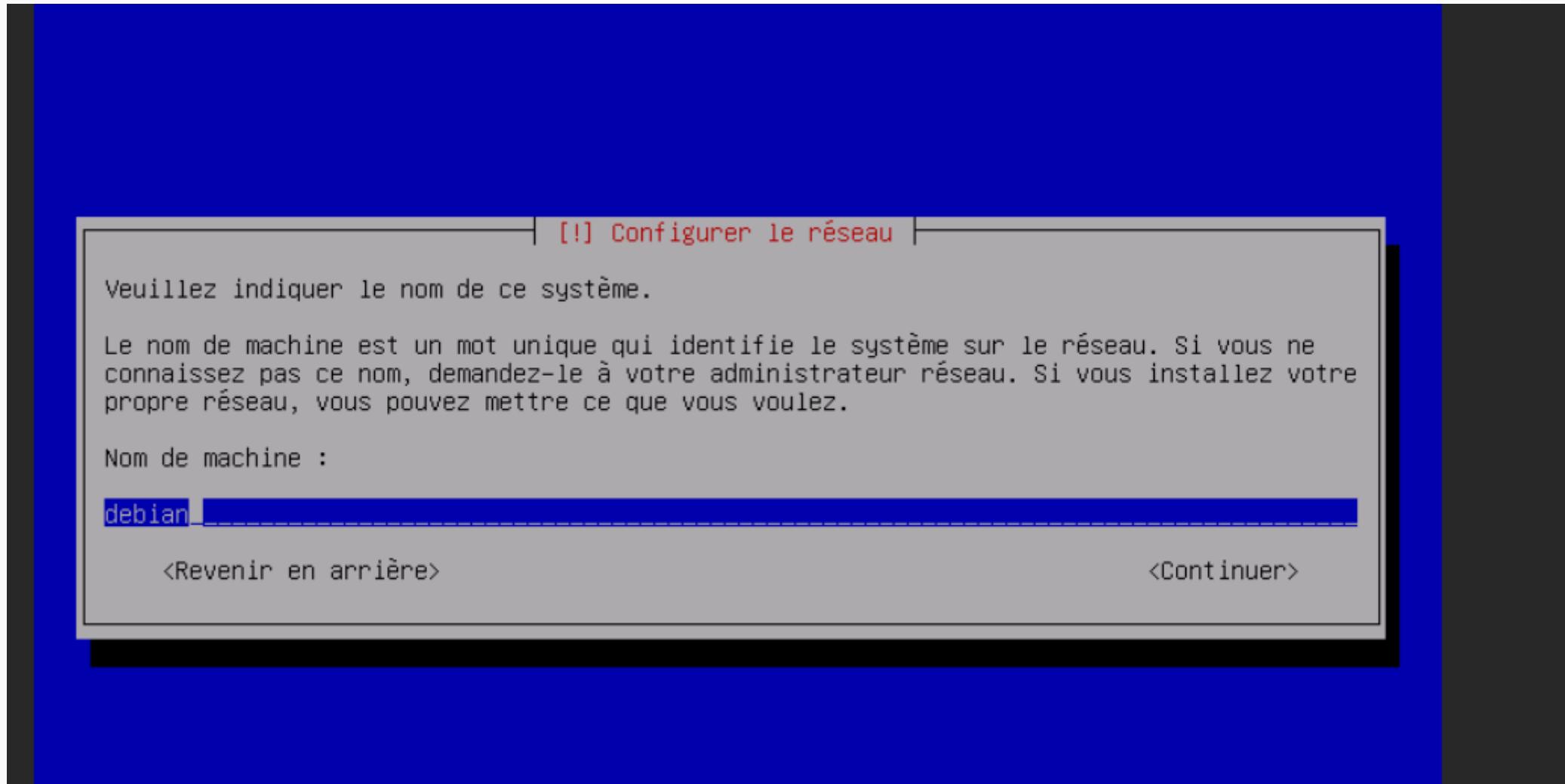
Situation géographique



Le choix du clavier

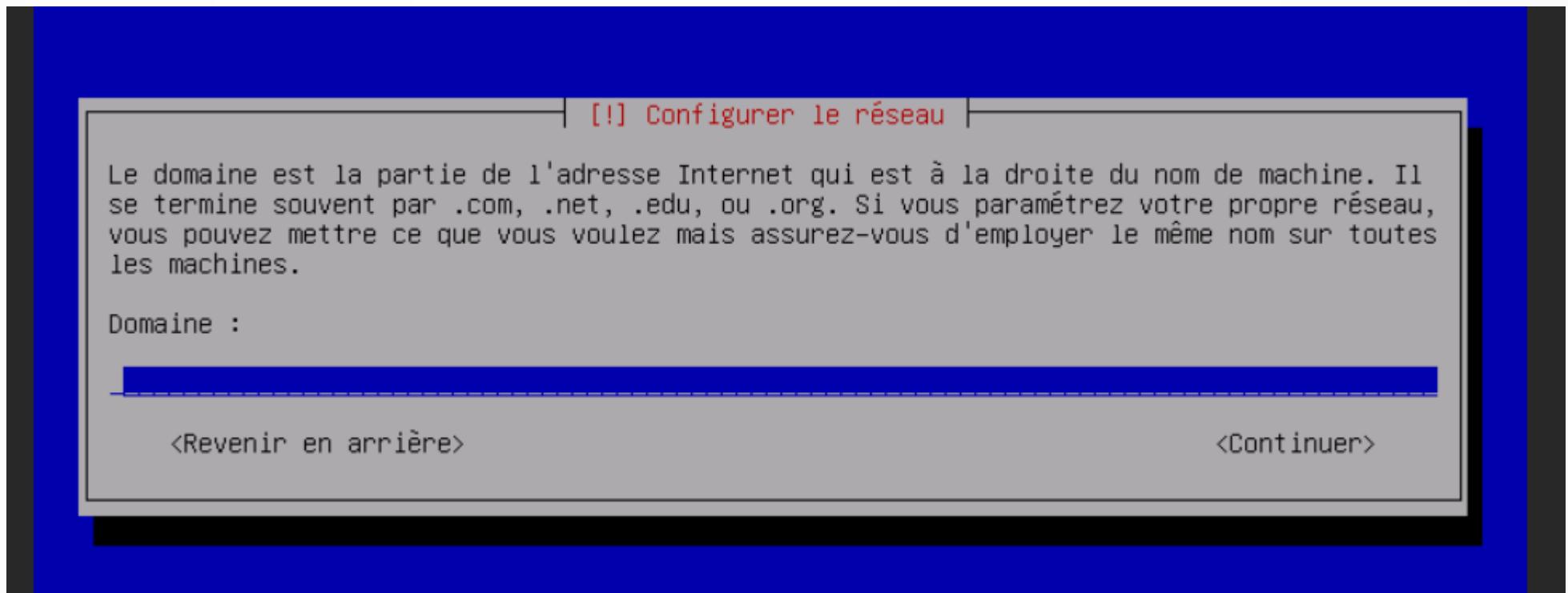


Configurer le nom de la machine



Le domaine

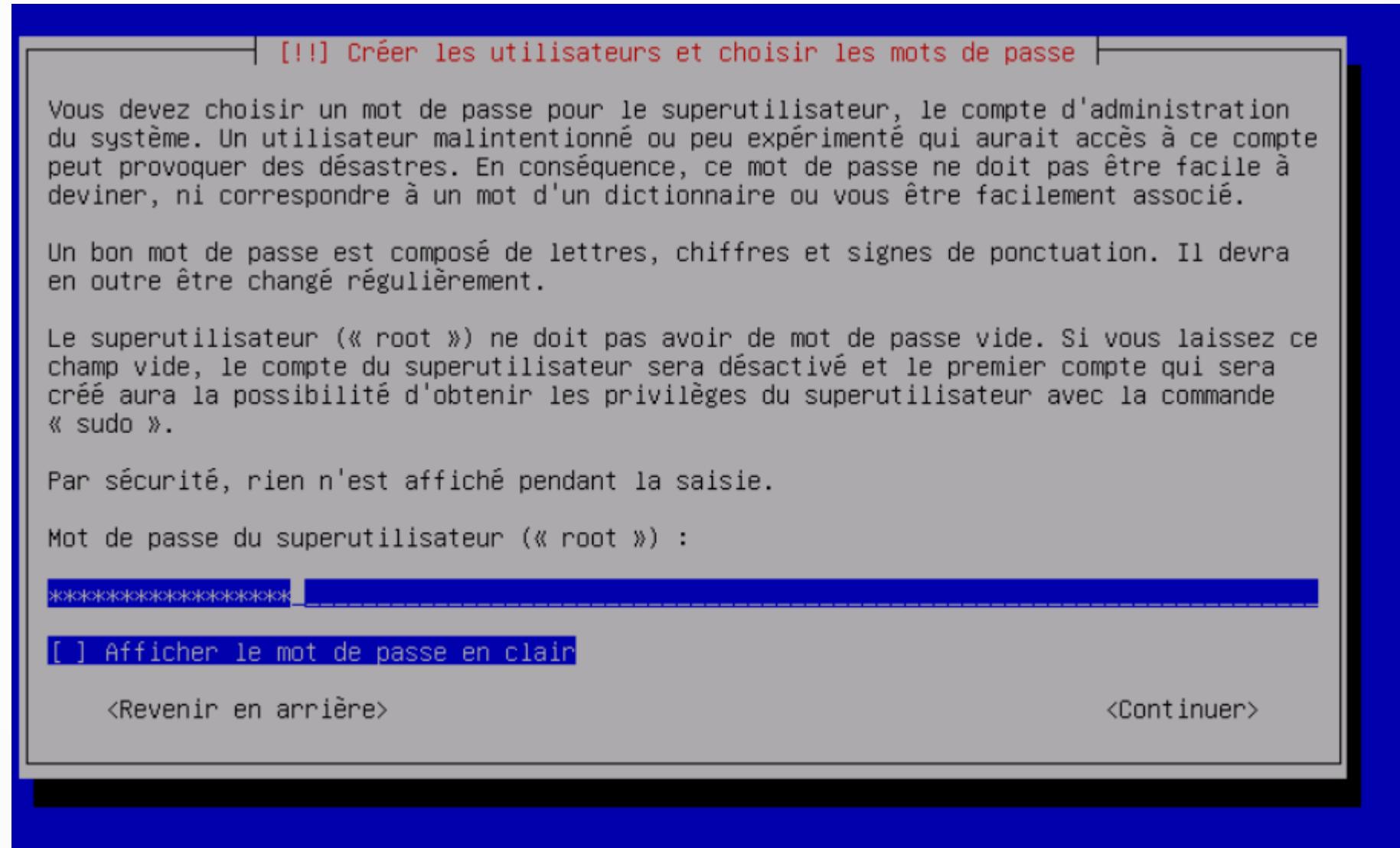
- Est-ce qu'on fait partie d'un domaine ?
 - Si oui l'indiquer, sinon le laisser vide



Le mot de passe de root

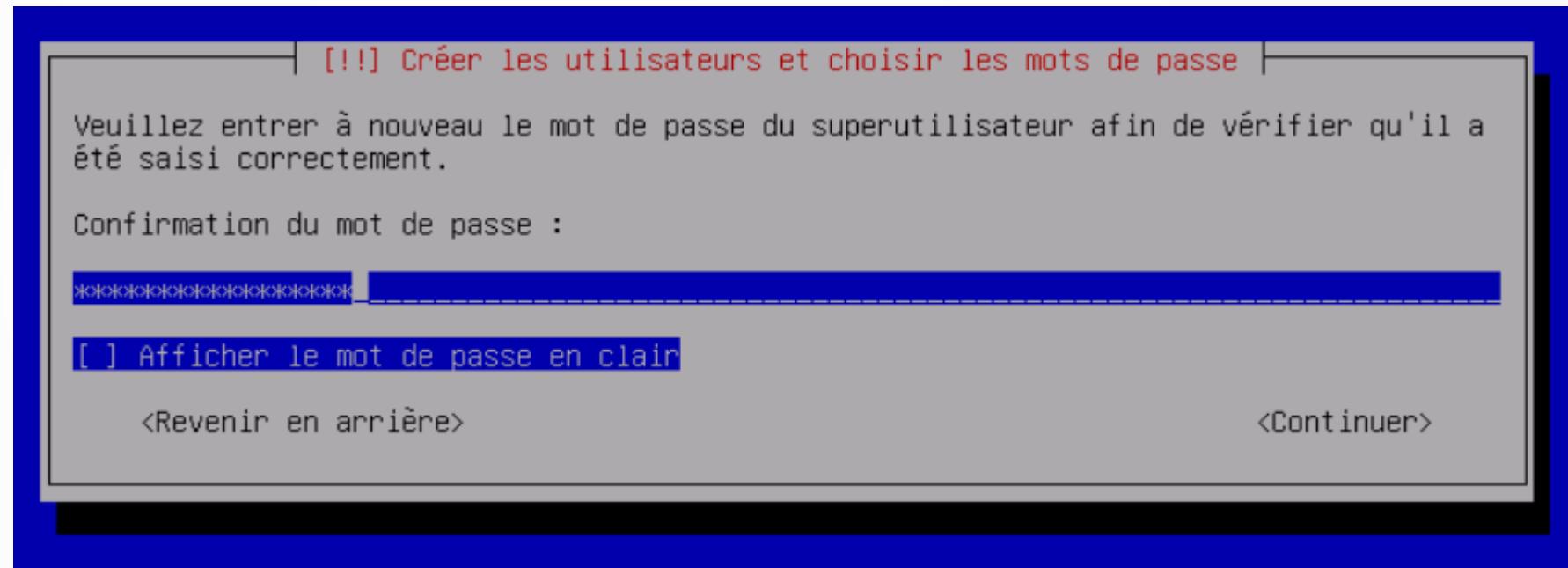
! Attention !
On crée toujours
un mot de passe
complexe.

8-10 caractère,
lettres
minuscules,
majuscules,
chiffres et
symboles



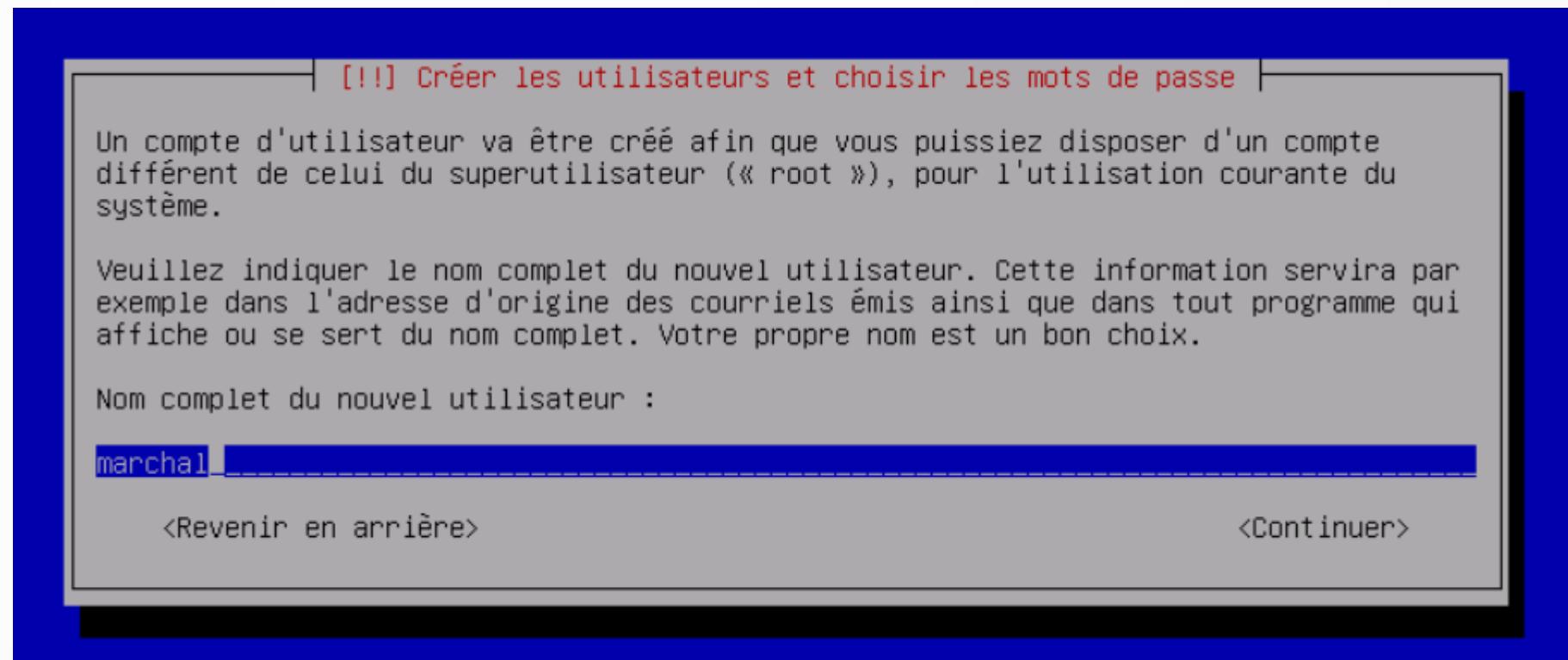
La confirmation

On confirme le mot de passe précédent



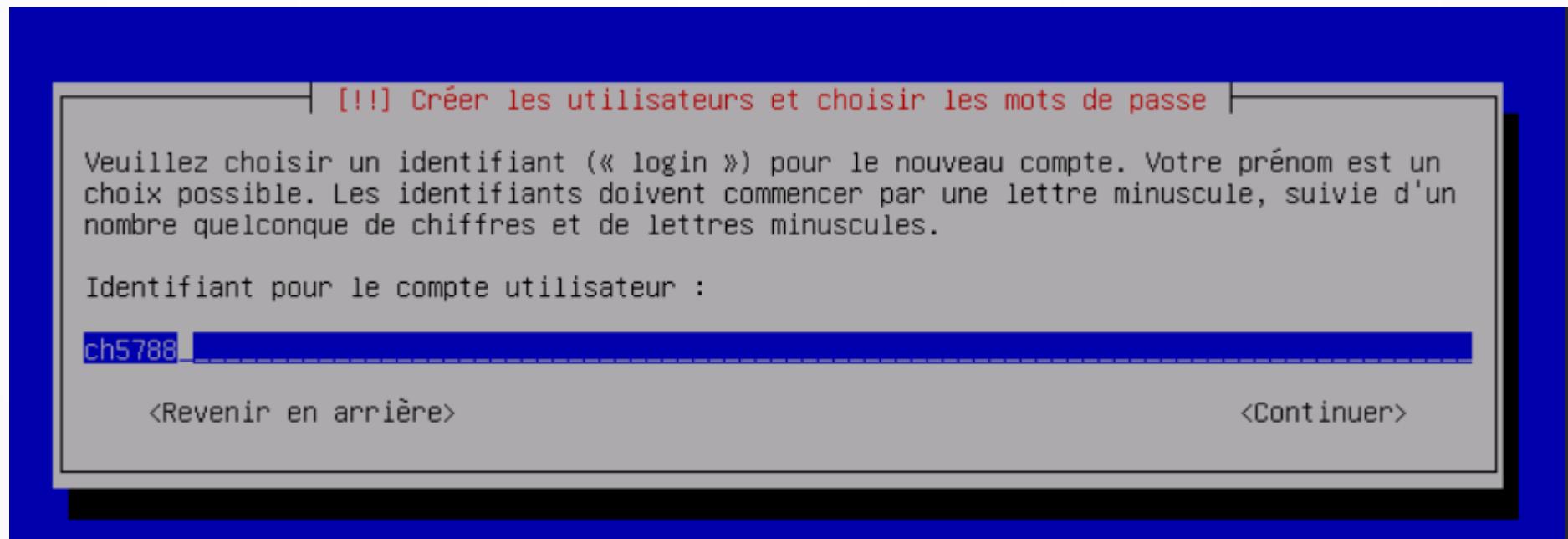
Le premier utilisateur normal

Nom,
pseudo,
Ce qui
permet de
vous
démarquer
sur le
système

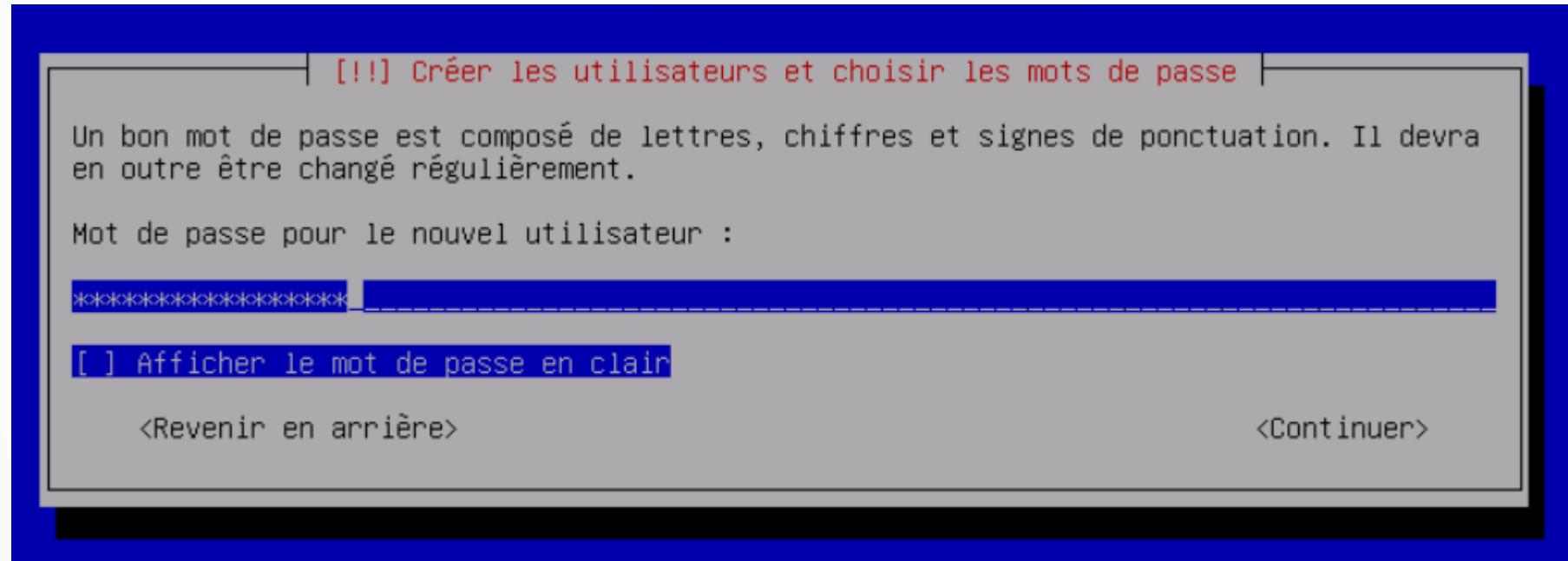


Notre identifiant sur le système

Un identifiant unique est recommandé



Le mot de passe de votre utilisateur



Confirmation du mot de passe

[!!] Créer les utilisateurs et choisir les mots de passe

Veuillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.

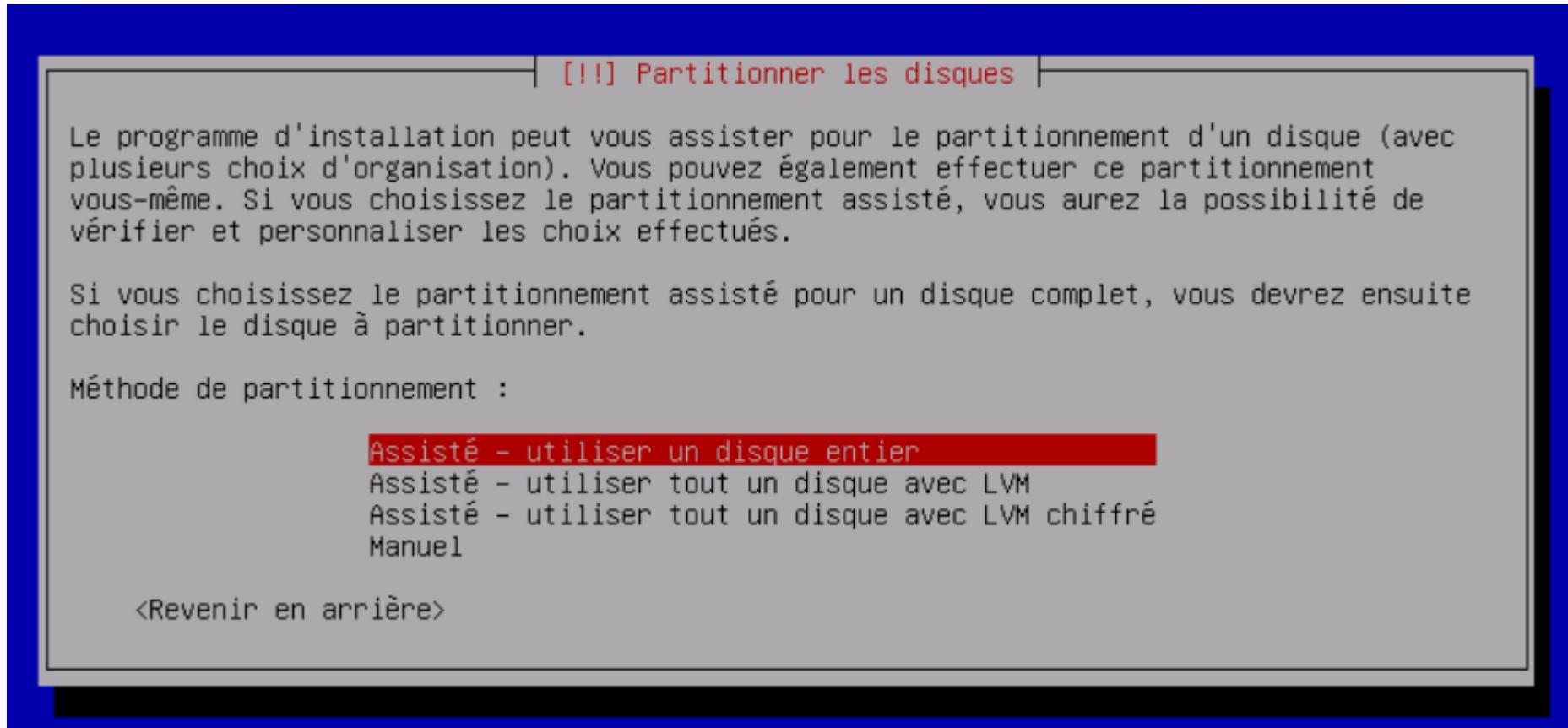
Confirmation du mot de passe :

[] Afficher le mot de passe en clair

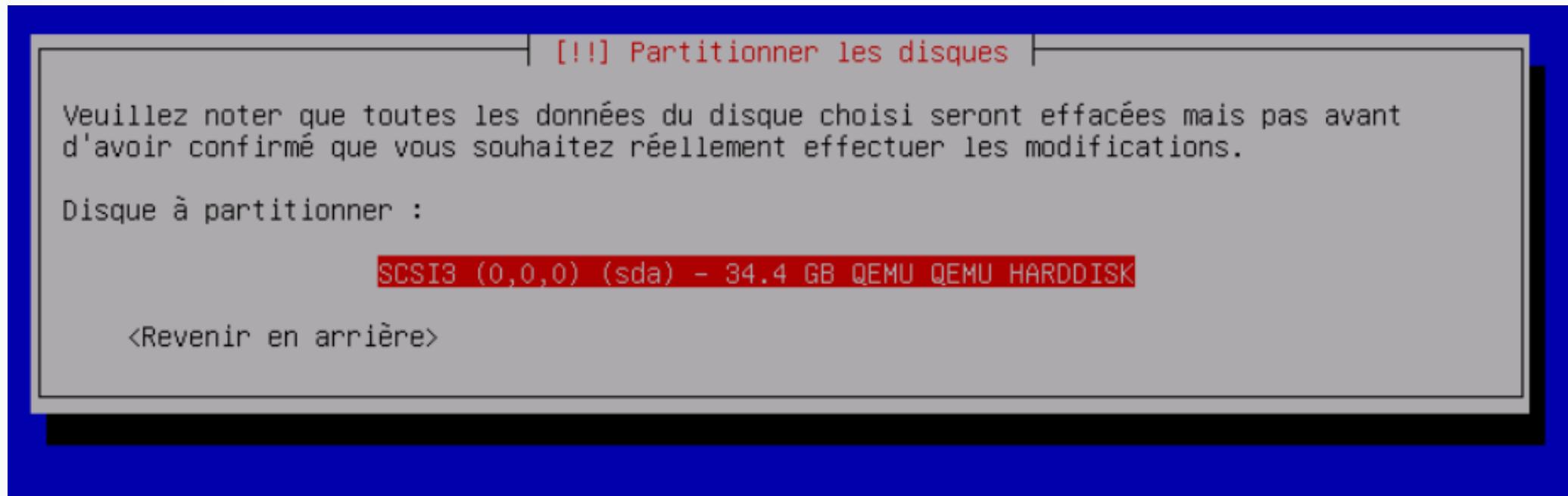
[<Revenir en arrière>](#) [<Continuer>](#)

Le partitionnement du/des disques

- Nous y reviendrons plus tard, pour l'instant on utilise un disque entier

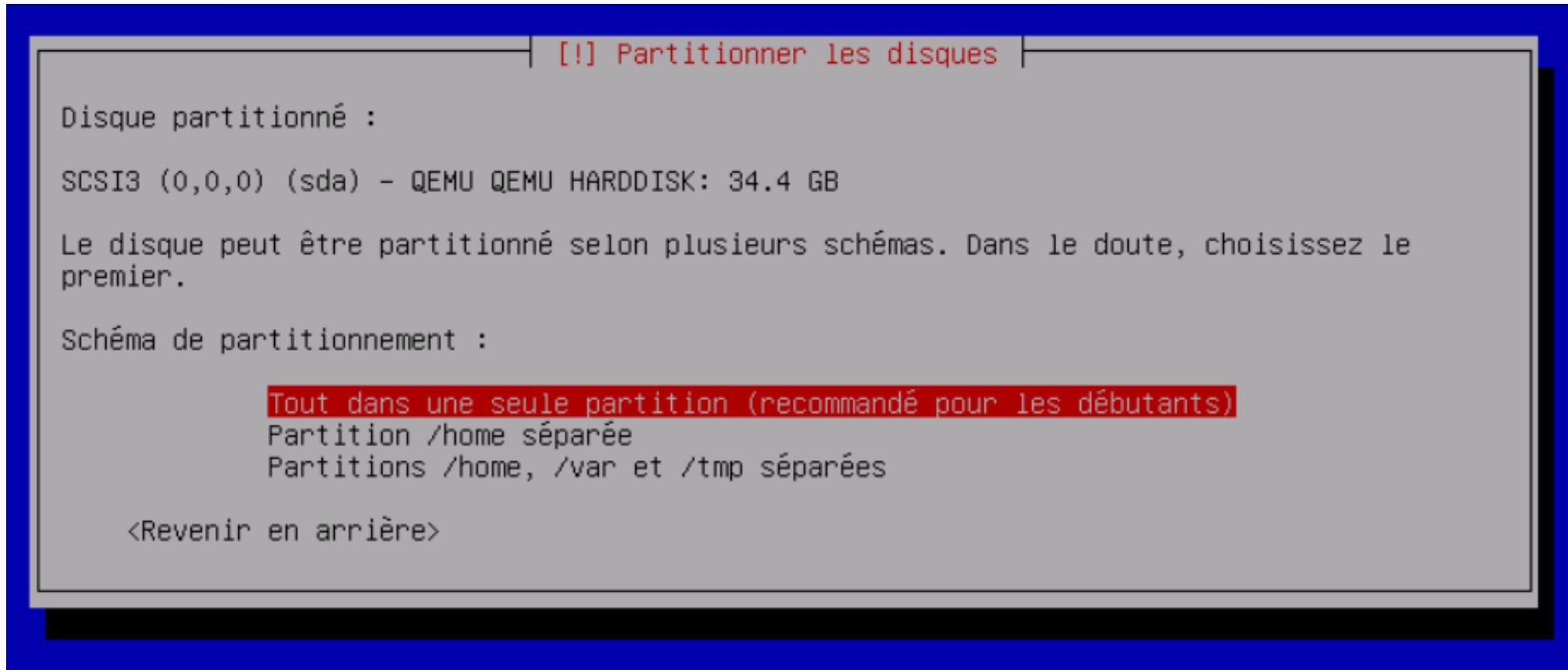


On sélectionne le bon disque



Pour l'instant tout dans une seule partition

- Nous y reviendrons plus tard, pour faire des partitions séparées



On applique les changements

[!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

Partitionnement assisté

Configurer le RAID avec gestion logicielle

Configurer le gestionnaire de volumes logiques (LVM)

Configurer les volumes chiffrés

Configurer les volumes iSCSI

SCSI3 (0,0,0) (sda) - 34.4 GB QEMU QEMU HARDDISK

n° 1 primaire 33.3 GB f ext4 /

n° 5 logique 1.0 GB f swap swap

Annuler les modifications des partitions

Terminer le partitionnement et appliquer les changements

<Revenir en arrière>

On confirme

[!!] Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :
SCSI3 (0,0,0) (sda)

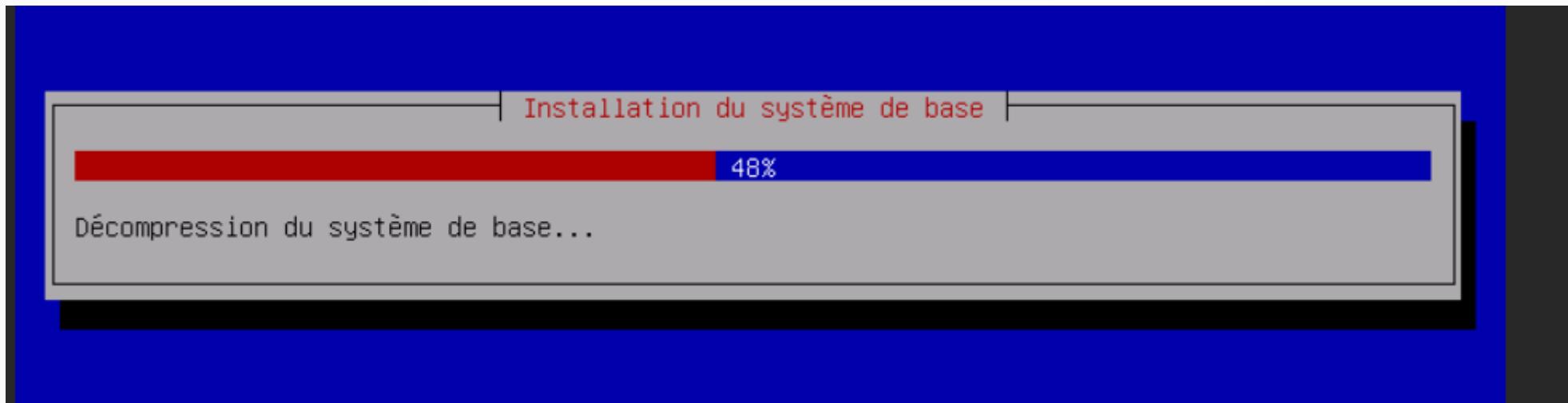
Les partitions suivantes seront formatées :
partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4
partition n° 5 sur SCSI3 (0,0,0) (sda) de type swap

Faut-il appliquer les changements sur les disques ?

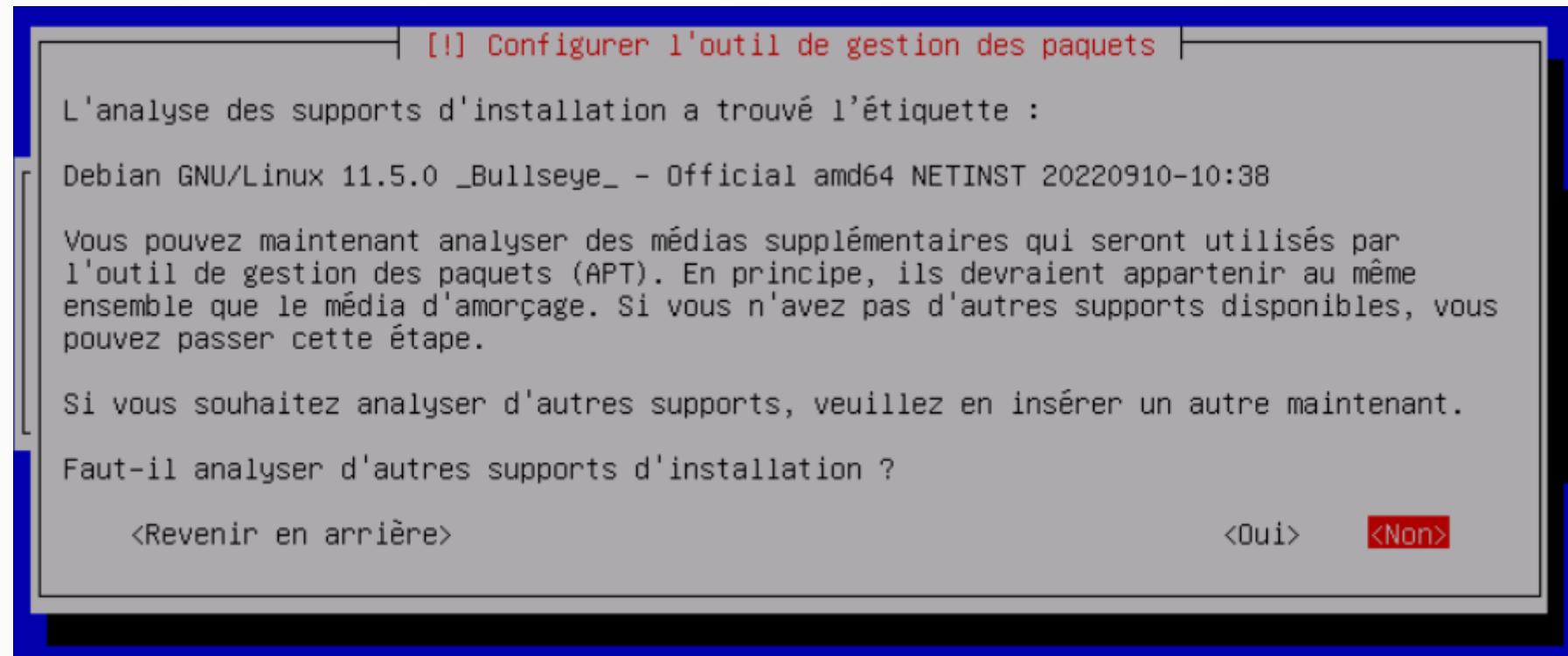
<Oui>

<Non>

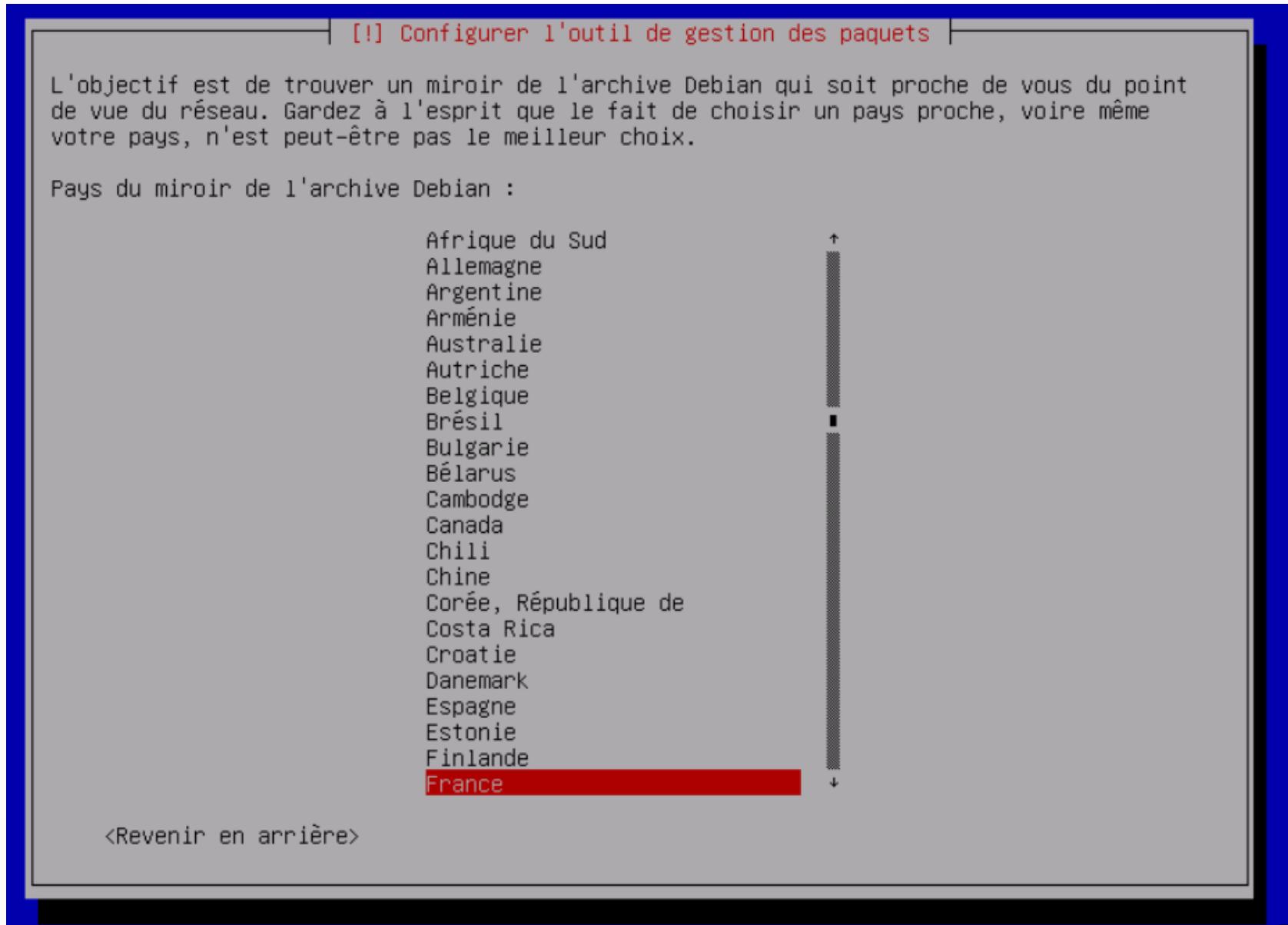
Une partie du système de base s'installe depuis l'iso



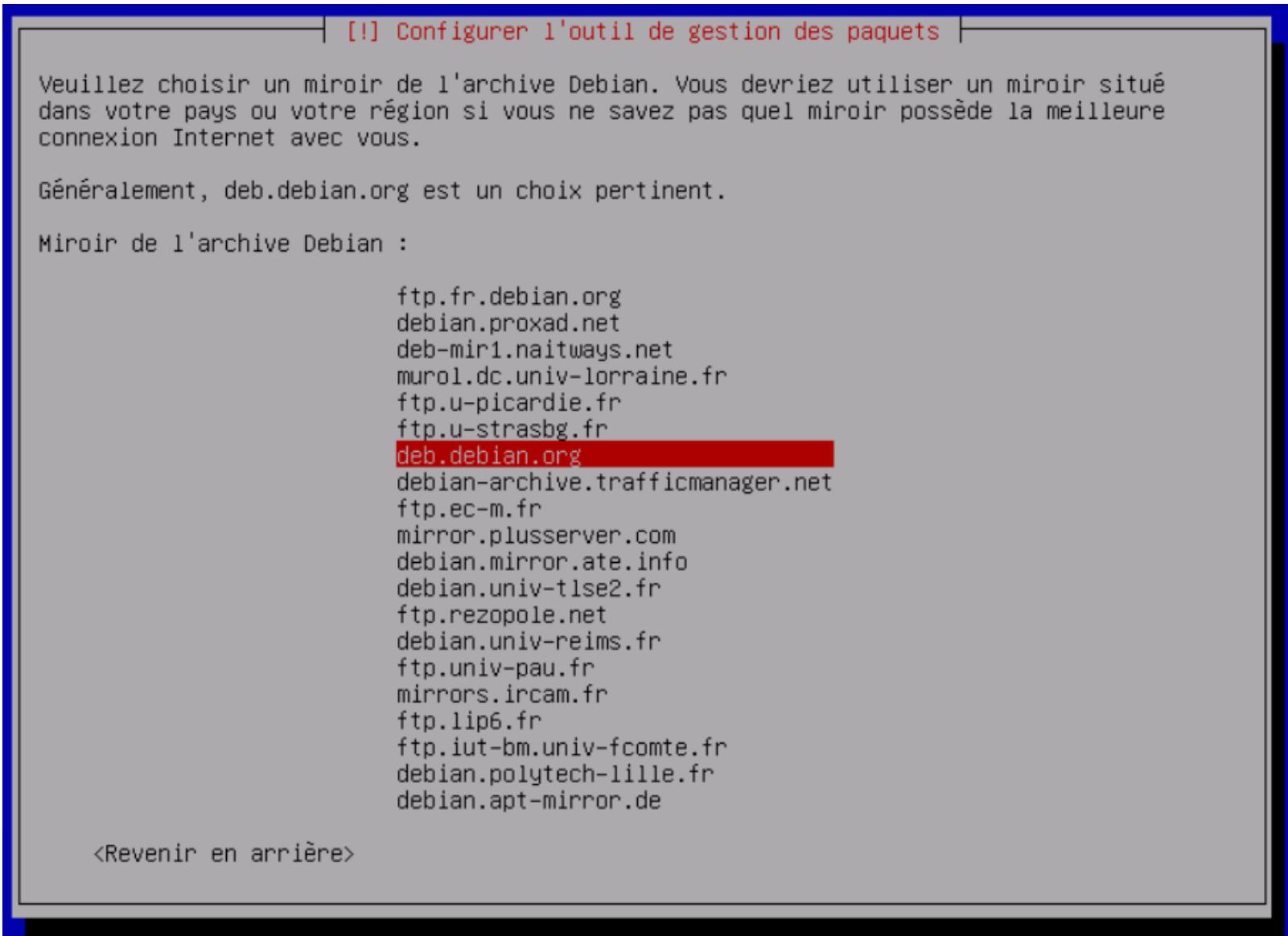
Ajouter des paquets depuis un autre support



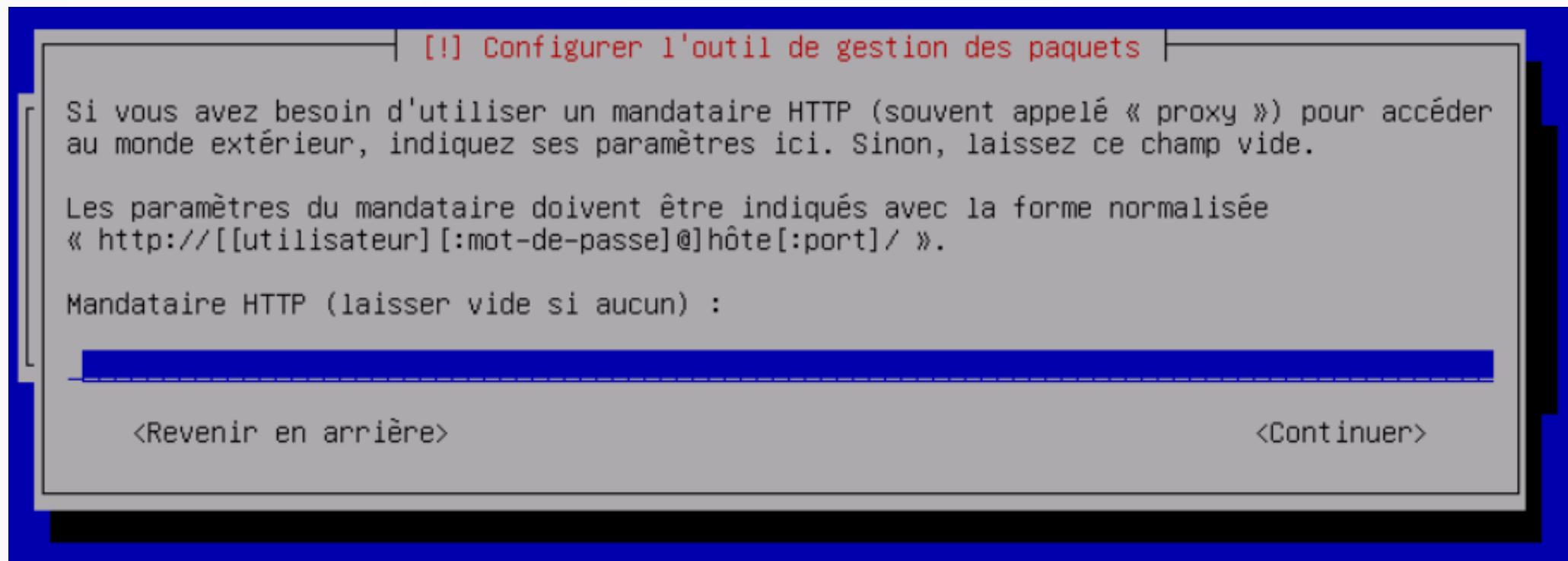
Depuis le pays ou on récupère nos paquets



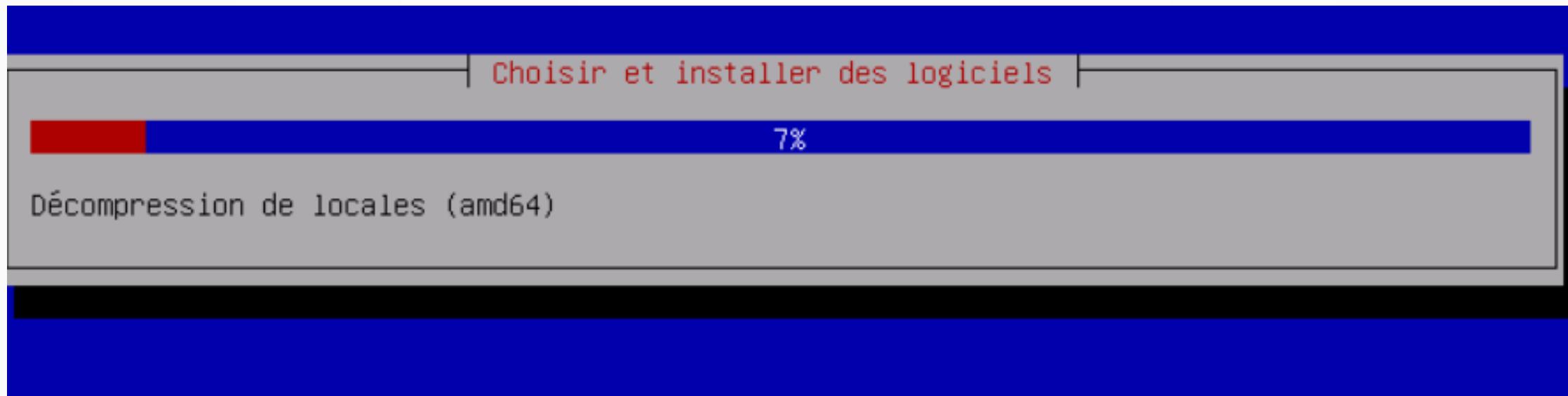
Le serveur qui nous envoie l'archive debian



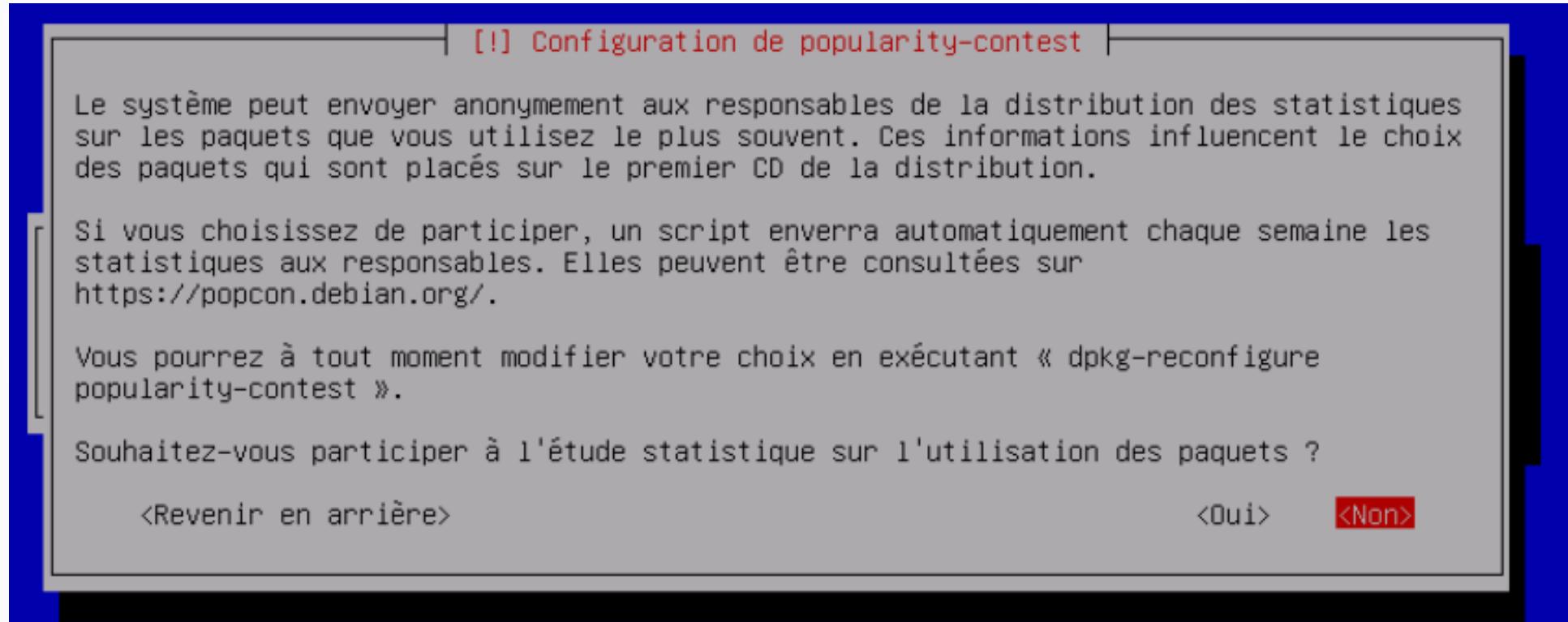
Si vous avez un proxy entre vous et le wan, par default laisser vide



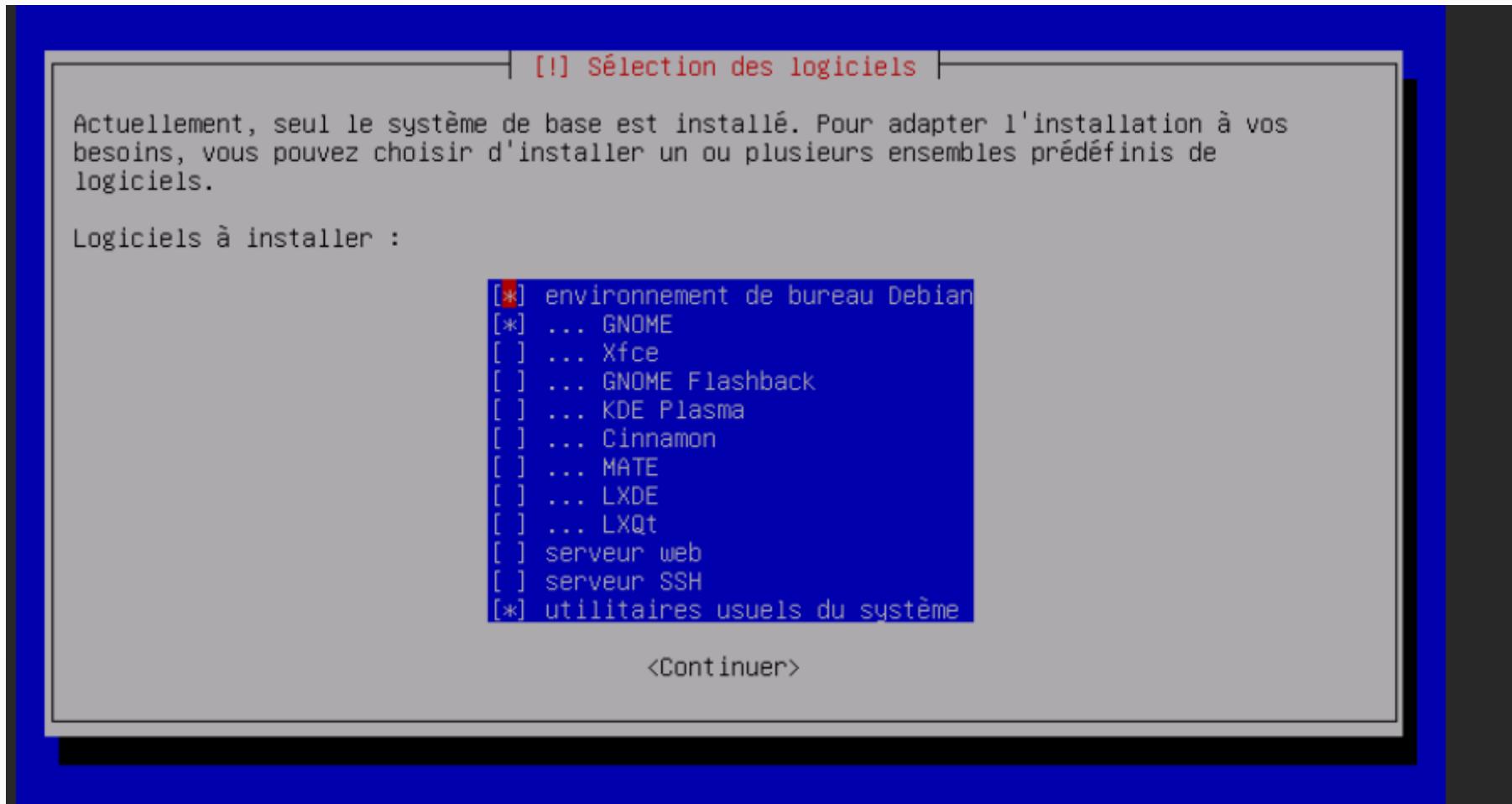
Les autres programmes s'installent



Oui / non : etude statistique

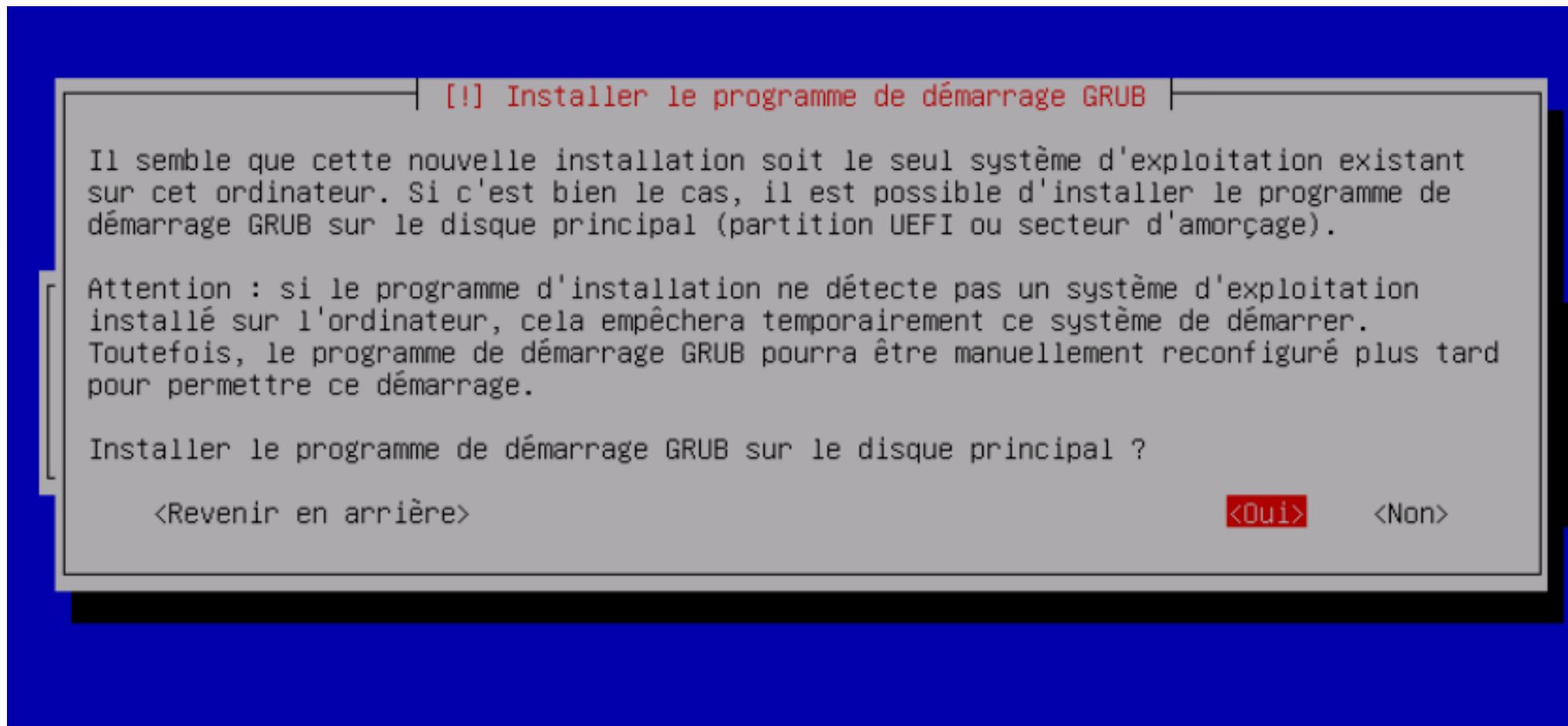


Programmes supplémentaire



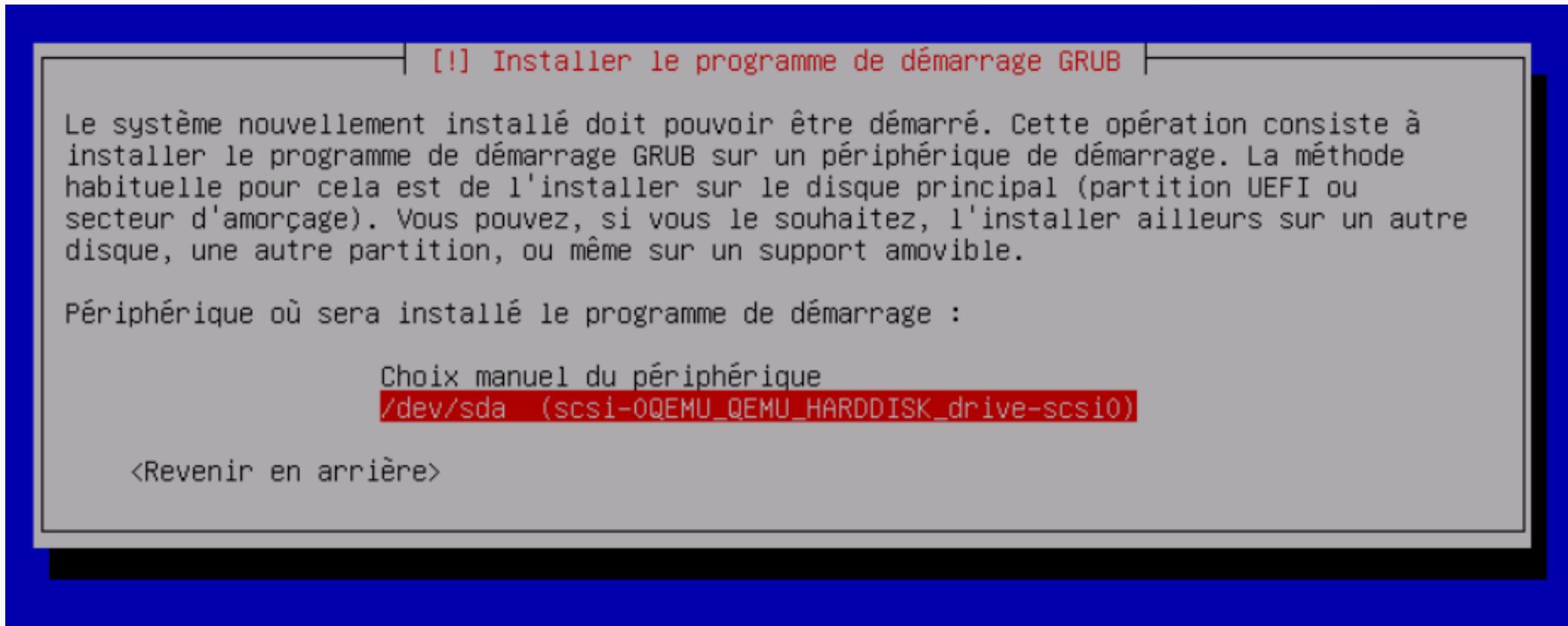
Grub, programme qui permet le chargement du système d'exploitation au démarage

On indique Oui



Le disque ou on installe grub

- En général votre disque primaire / disque qui contient votre os

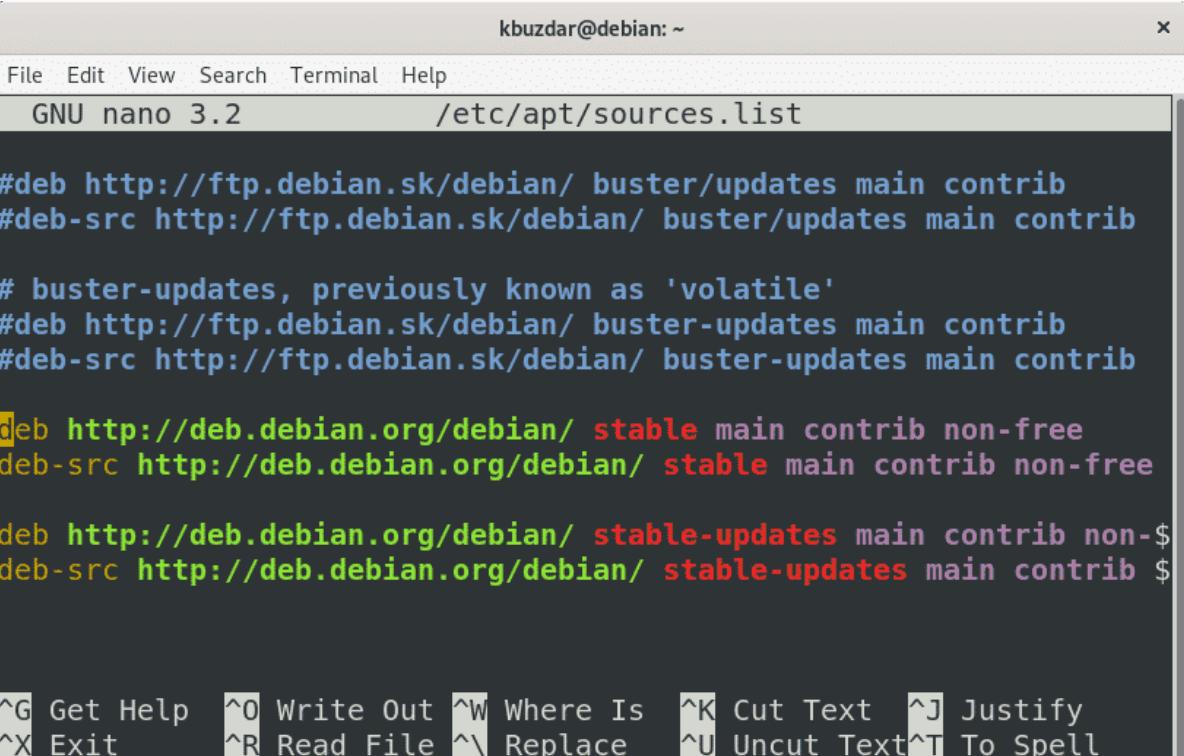


Mise à jour

- Les mises à jours sur les versions stables sont peu fréquentes.
- Pour à minima recevoir les patchs de sécurité :
 - Il faudra vérifier que vous ayer bien le dépôt correspondant dans vos sources
 - Pour debian/ubuntu depuis:
/etc/apt/sources.list
/etc/apt/sources.list.d/*
 - Pour RHEL / Centos / Fedora
/etc/yum.conf
/etc/yum.repos.d/*

Structure du fichier sources.list

- Si vous regardez votre fichier dans `/etc/apt/sources.list`
 - Vous devriez retrouver quelque chose comme ça



The screenshot shows a terminal window titled "kbuzdar@debian: ~". The window title bar also displays "File Edit View Search Terminal Help" and "GNU nano 3.2 /etc/apt/sources.list". The main content area of the terminal shows the following text:

```
#deb http://ftp.debian.sk/debian/ buster/updates main contrib
#deb-src http://ftp.debian.sk/debian/ buster/updates main contrib

# buster-updates, previously known as 'volatile'
#deb http://ftp.debian.sk/debian/ buster-updates main contrib
#deb-src http://ftp.debian.sk/debian/ buster-updates main contrib

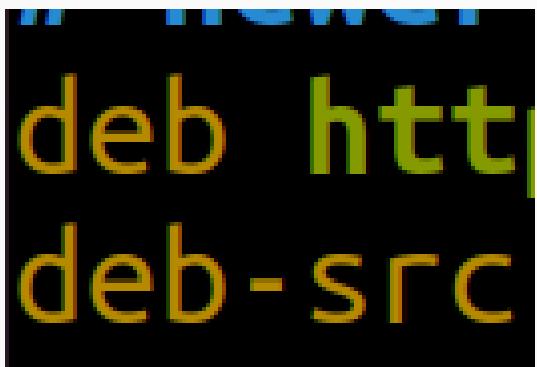
deb http://deb.debian.org/debian/ stable main contrib non-free
deb-src http://deb.debian.org/debian/ stable main contrib non-free

deb http://deb.debian.org/debian/ stable-updates main contrib non-
deb-src http://deb.debian.org/debian/ stable-updates main contrib $
```

At the bottom of the terminal window, there is a menu bar with various keyboard shortcuts for navigating the nano editor.

Structure du fichier sources.list

- On va faire la distinction entre :
 - Deb
 - La d'où vos paquets binaires viennent.
 - Deb-src
 - La d'où les sources des paquets sont récupéré.



Structure du fichier sources.list

- Ensuite on a l'emplacement du dépôt :
 - Le protocole utilisé puis son url :
 - http:
 - fr.archive.ubuntu.com (le srv web)
 - /ubuntu/ (la page demandé)
 - https:
 - Srv web
 - La page demandé
 - ftp:
 - Srv ftp
 - La page demandé

`http://fr.archive.ubuntu.com/ubuntu/
http://fr.archive.ubuntu.com/ubuntu/`

Structure du fichier sources.list

- Suivie du :
 - nom de code de votre distrib ou sa phase
 - Pour debian 11 : bullseye
 - Pour l'exemple précédent : stable



← → C ▲ Non sécurisé | <http://ftp.debian.org/debian/dists/>

Index of /debian/dists

Name	Last modified	Size
Parent Directory		-
Debian8.11/	2021-08-14 13:46	-
Debian9.13/	2021-08-14 07:47	-
Debian10.13/	2022-09-10 11:03	-
Debian11.5/	2022-09-10 09:42	-
README	2022-09-10 10:42	1.0K
bookworm-backports/	2022-07-19 02:00	-
bookworm-proposed-updates/	2022-07-19 02:00	-
bookworm-updates/	2022-07-19 02:01	-
bookworm/	2022-11-01 04:14	-
bullseye-backports-sloppy/	2022-07-19 02:03	-
bullseye-backports/	2022-07-19 02:03	-
bookworm_proposed_updates/	2022-10-30 15:17	-

```
deb http://deb.debian.org/debian/ stable main contrib non-free
```

Structure du fichier sources.list

Index of /debian/dists/stable

	Name	Last modified	Size
	Parent Directory		-
	ChangeLog	2022-09-10 09:32	3.2M
	InRelease	2022-09-10 10:27	113K
	Release	2022-09-10 10:18	111K
	Release.gpg	2022-09-10 10:27	2.4K
	contrib/	2022-09-10 10:18	-
	main/	2022-09-10 10:18	-
	non-free/	2022-09-10 10:18	-

Apache Server at ftp.debian.org Port 80

- Puis la branche :
 - Vous pouvez en indiquer plusieurs
 - Main :
 - libres et qui sont en accord avec le DFSG (Debian Free Software Guidelines)
 - Contrib :
 - Libres et en accord avec DFSG mais dépendent de paquets non-free
 - Non-free :
 - Libres mais ne sont pas en accord avec la DFSG

Pour plus de détails :

man 5 sources.list

```
deb http://deb.debian.org/debian/ stable main contrib non-free
```

Structure du fichier sources.list

- Sur d'autres distributions vous aurez des valeurs différentes, ex sur ubuntu :
 - Main : Logiciels libres, officiellement pris en charge par Canonical
 - Universe : Logiciels libres, NON-pris en charge par Canonical
 - Restricted : Logiciels NON-libres, officiellement pris en charge par Canonical (comme les drivers)
 - Multiverse : Logiciels NON-libres et NON-pris en charge par Canonical (Plugin Flash par exemple)
- Idem pour les noms de code ou de phase

Dossier sources.list.d/

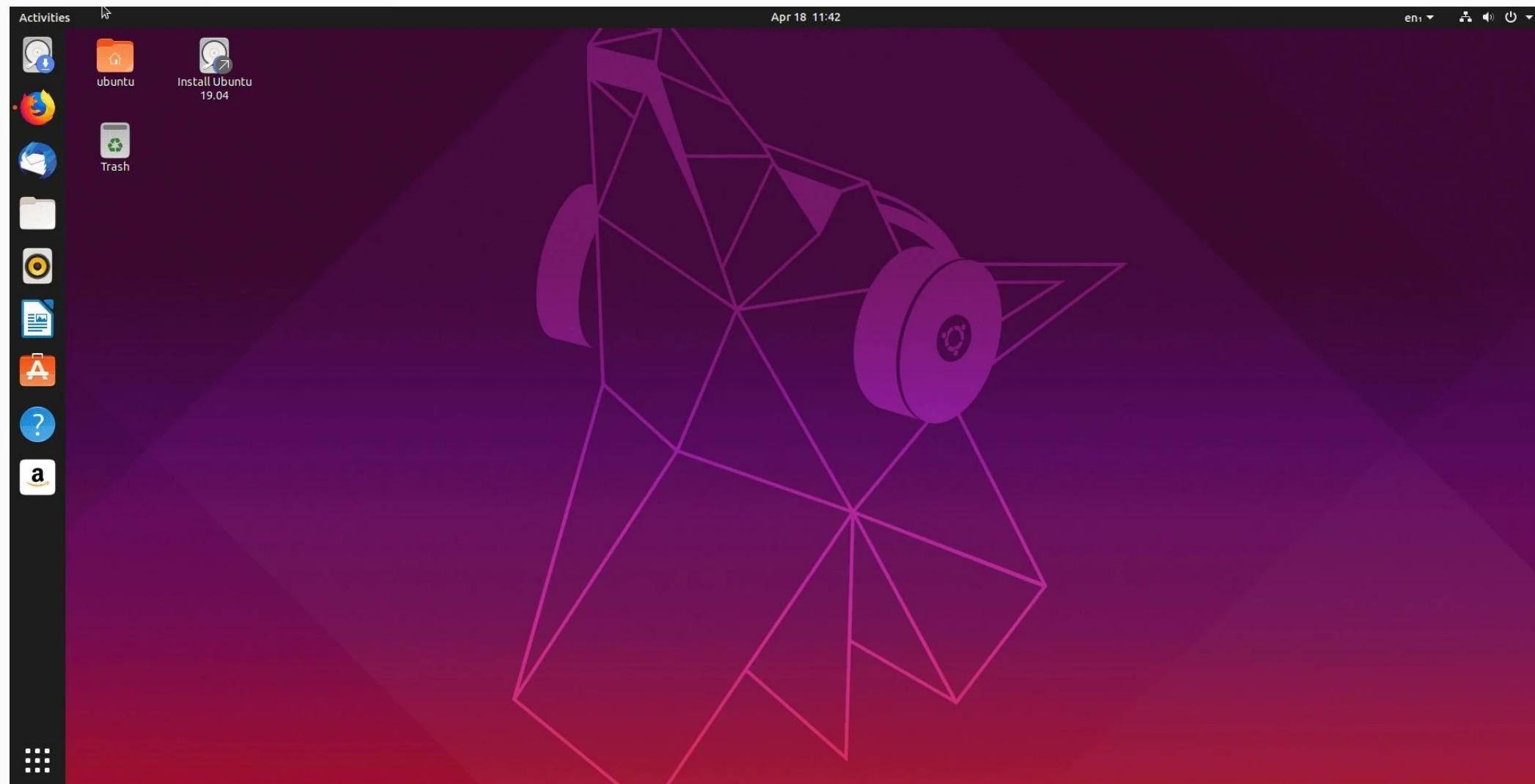
- Pour ajouter d'autres sources de fournisseur tiers,
la bonne pratique est de créer un fichier :
 - <nom_du_fichier>.list dans le dossier
/etc/apt/sources.list.d/
 - Qui contient uniquement une seule source :

```
## THIS FILE IS AUTOMATICALLY CONFIGURED ##
# You may comment out this entry, but any other modifications may be lost.
deb [arch=amd64] https://dl.google.com/linux/chrome/deb/ stable main
```

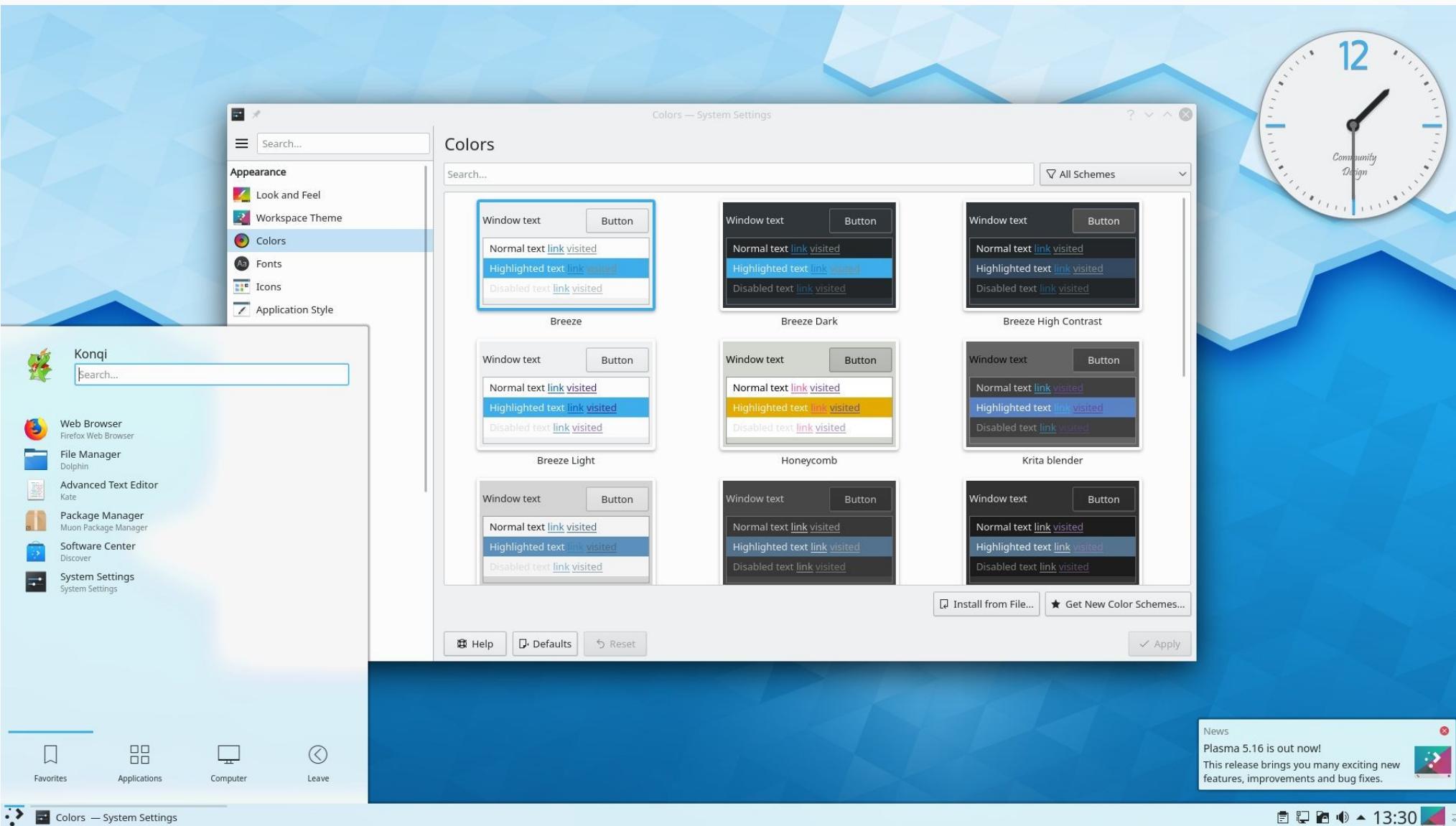
Les environnement graphiques

- Un environnement graphiques est un ensemble de programmes qui permettent de manipuler l'ordinateur à travers une interface graphique.
- Vous avez plusieurs choix possibles sur linux

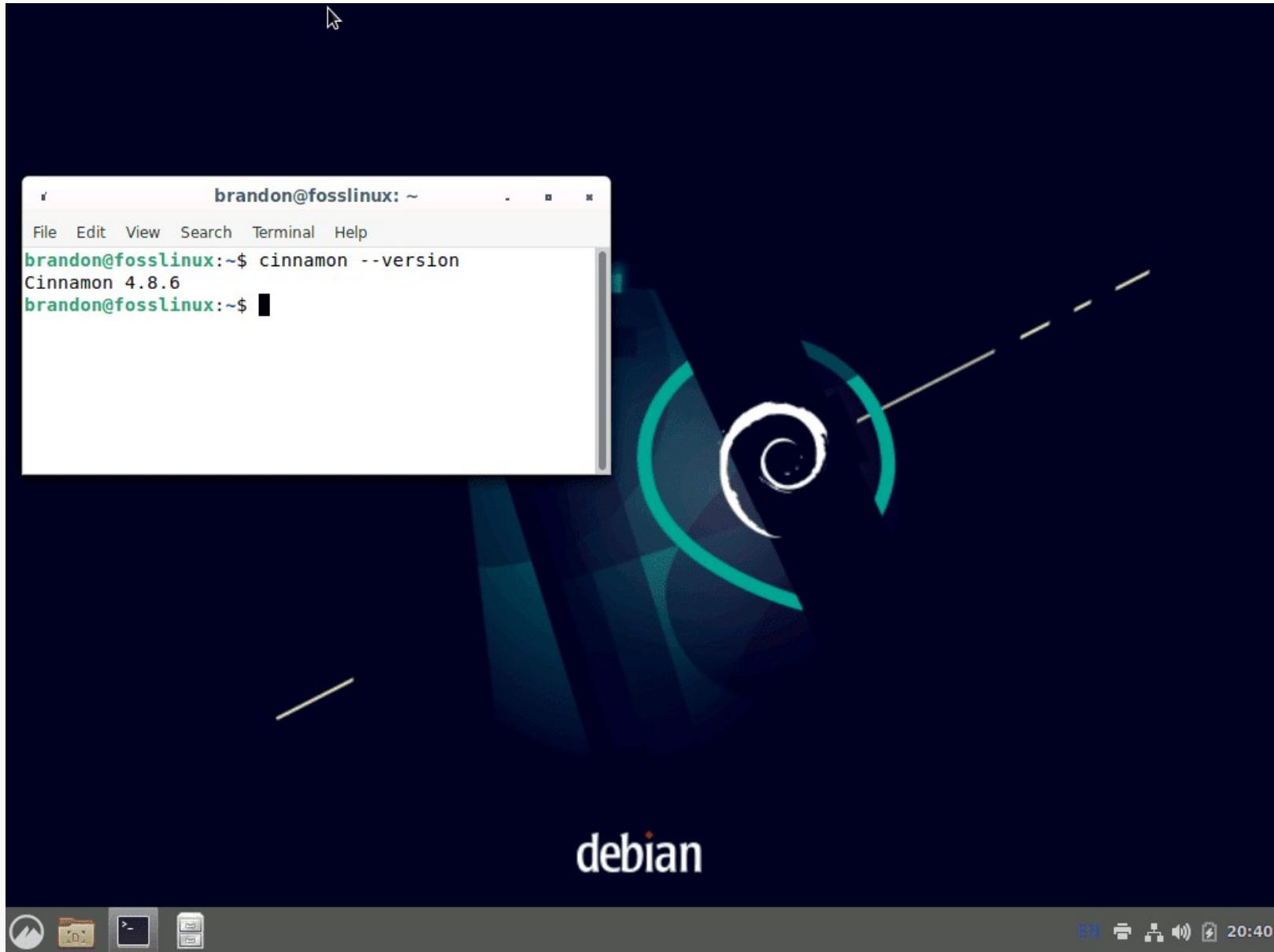
GNOME (GNU Network Object Model Environment)



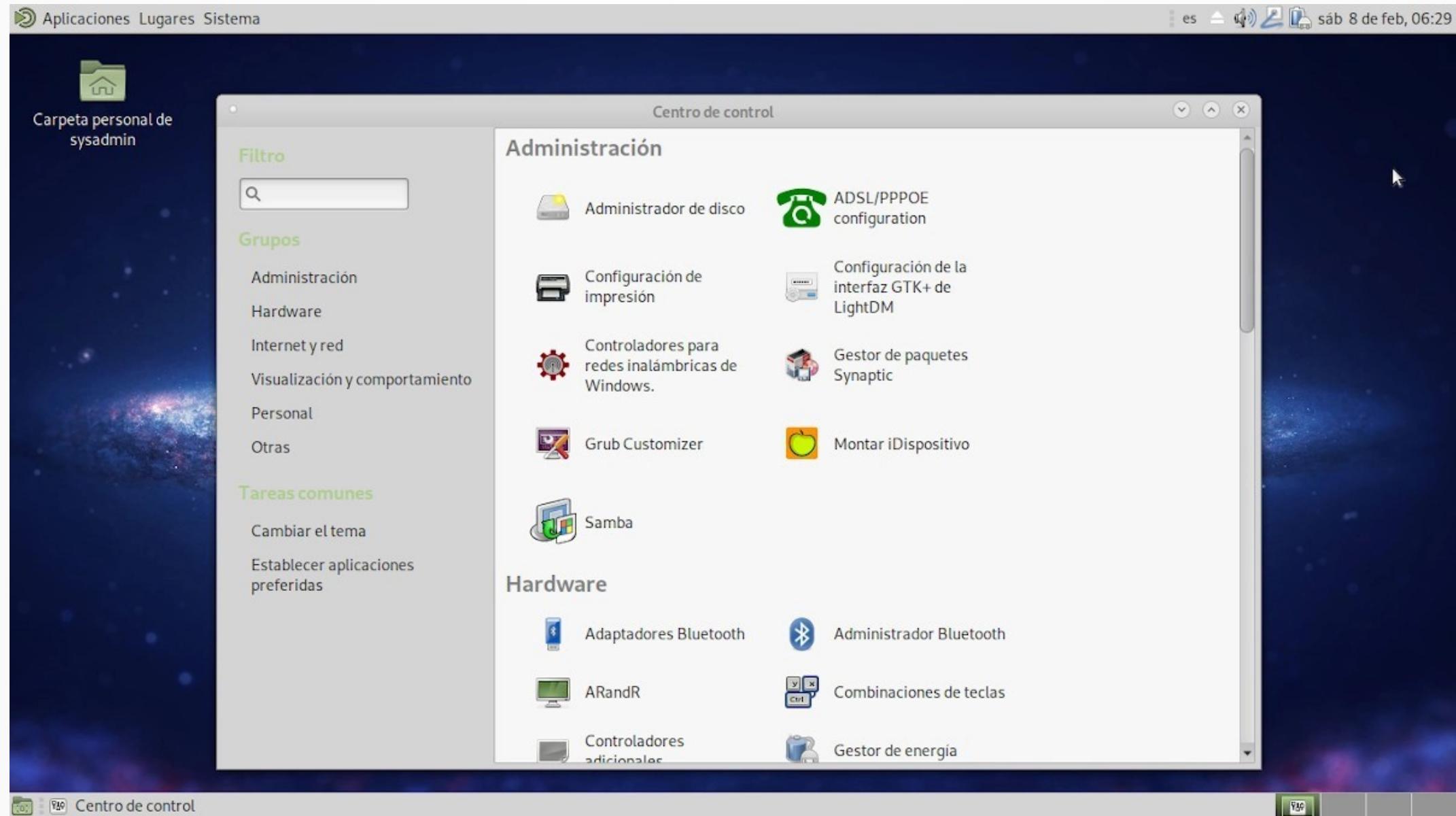
KDE (K Desktop Environment)



cinnamon



Mate



Et bien d'autre

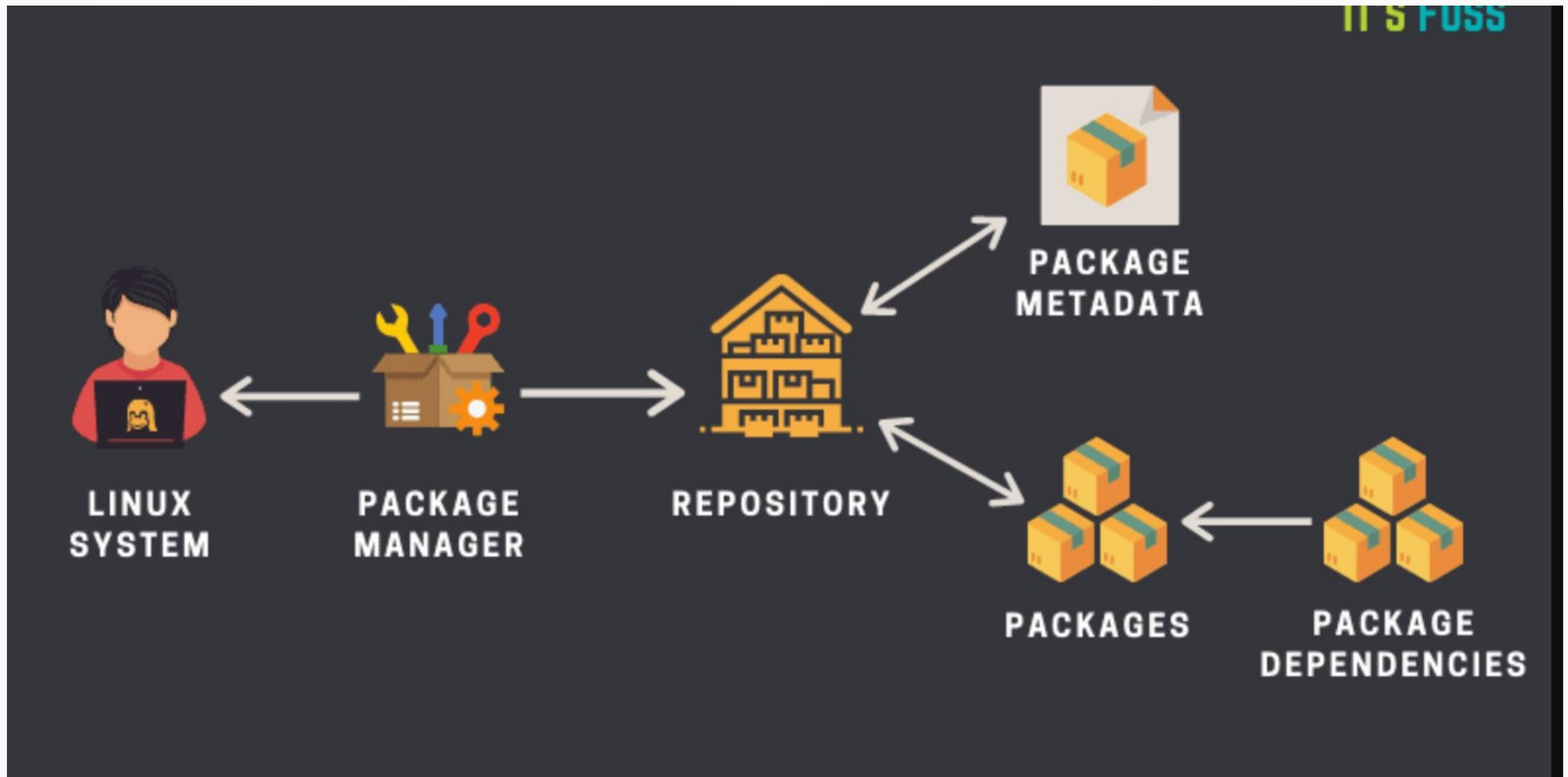


Ce sont des thèmes, uniquement pour illustrer.

La gestion des logiciels

**Administration des rpm
Exploitation de yum, dpkg et aptitude
Installation à partir des sources**

Administration des rpm

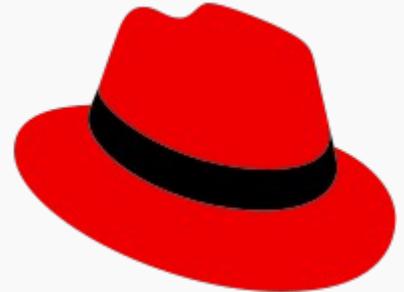
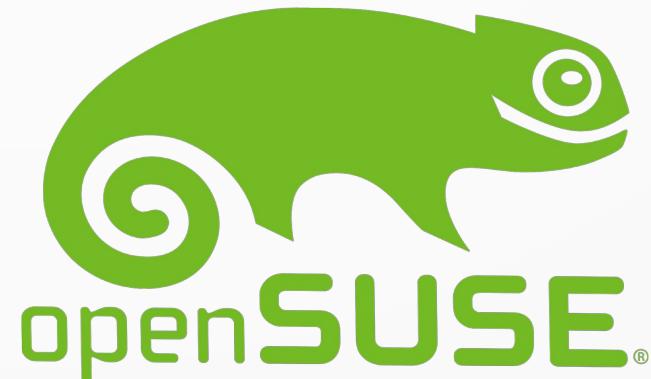


Administration des rpm

- RPM Package Manager (RPM) (a l'origine Red Hat Package Manager)
 - Est un gestionnaire de paquets gratuit et libre
 - Ces archives sont reconnaissable à leur extension en .rpm
 - A contrario de celles des systèmes debian en .deb



RHEL - Red Hat Enterprise Linux



Administration des rpm

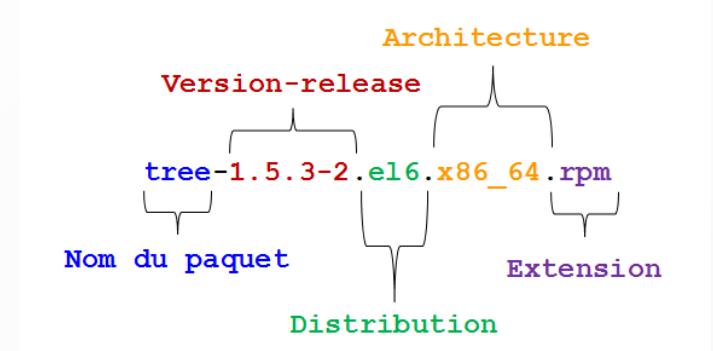
- A la différence d'autre gestionnaire de paquets.
 - Rpm ne gère pas les dépendances.
 - C'est à l'utilisateur de le gérer.
 - Un paquet RPM peut contenir :
 - Des fichiers binaires (les programmes executables, cat, cd, ls etc.)
 - Les fichiers de configurations lié au paquet
 - Des fichiers de documentation

Administration des rpm

- Format d'un fichier rpm :

<nom>-<version>-<VersionPublication>.<arch>.rpm (arch : architecture proc x86,x64, amd64 etc...)

- Installation : rpm -ivh
- Mise à jour : rpm -Uvh
- Désinstaller : rpm -evh
- Origine d'un fichier : rpm -qf chemin/fichier
- Obtenir des informations sur un paquet : rpm -q xxxx.rpm
- Obtenir la doc d'un paquet : rpm -qd
- On remarquera que les options sont parlantes (-q : query, -f : file, -i : install, -U : update)
- Les infos query viennent de : /var/lib/rpm
Arch : architecture (intel :)



Exploitation de yum

- Yum est une surcouche de RPM, il gère pour lui les dépendances et le téléchargement des paquets.
- Il facilite ainsi la mise à jour des paquets.
 - Syntaxe :
 - `yum update` # Sans Arg mets à jours tous vos paquets, sinon juste les paquets indiqués
 - `yum install <nom_de_paquet>` # installe un paquet
 - `yum repolist` # affiche la liste de tous les dépôts

Structure du fichier yum.conf

- Les différences avec le système yum
 - Notions de [main] et [repository]
 - Main : config globale
 - Repository: config d'un dépôt / d'une source

```
[main]
cachedir=/var/cache/yum/$basearch/$releasever
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
installonly_limit=3
```

```
[red-hat-enterprise-linux-scalable-file-system-for-rhel-6-entitlement-rpms]
name = Red Hat Enterprise Linux Scalable File System (for RHEL 6 Entitlement) (RPMS)
baseurl = https://cdn.redhat.com/content/dist/rhel/entitlement-6/releases/$releasever/
$basearch/scalablefilesystem/os
```

Structure du dossier yum.repos.d/

- La bonne pratique est de rajouter ces dépôts dans /etc/yum.repos.d
- On crée un fichier « nom.repo » pour notre dépôt :
- Dedans on indique le nom de son Dépôt

[NOM COURT DU DEPOT]

name=NOM COMPLET DU DEPOT

url=URL DU DEPOT

dpkg

- Dpkg c'est l'équivalent rpm de debian.
 - C'est lui qui installe, supprime les paquets sur debian.
 - Ne gère pas les dépendances
 - `dpkg -i <nom_du_fichier.deb>` #installer
 - `dpkg -r <nom_du_fichier.deb>` #supprimer
- apt et apt-get est l'équivalent yum sous debian.

aptitude

- Fonctionne sur apt, aptitude est un autre gestionnaire de paquets
 - Comme apt, apt-get, il possède différentes commandes :
 - sudo aptitude install ; remove; markauto, purge etc..
 - On retiendra surtout aptitude pour son interface interactive :
 - sudo aptitude

Quelques commandes apt

Apt :

- list # liste les paquets selon leur nom
- search # cherche dans les descriptions de paquet
- show # affiche les détails du paquet
- install # installes les paquets
- reinstall # réinstalle les paquets
- remove # supprime des paquets
- autoremove # Supprime automatiquement les dépendances inutilisées
- update # met à jour la liste des paquets disponibles
- upgrade # met à jour le système en installant/mettant à jour les paquets
- full-upgrade # met à jour le système en supprimant/installant/mettant à jour les paquets
- edit-sources # édite le fichier *etc/apt/sources.list*

Quelques commandes apt-get

Apt-get :

- update # Récupère les nouvelles listes de paquets
- upgrade # Réalise une mise à jour
- install # Installe de nouveaux paquets
- reinstall # Réinstaller les paquets
- remove # Supprime des paquets
- purge # Supprime des paquets et leurs fichiers de configuration
- autoremove # Supprime automatiquement les dépendances inutilisées
- dist-upgrade # Met à jour la distribution, reportez-vous à apt-get(8)
- clean # Supprime dans le cache local tous les fichiers téléchargés
- autoclean # Supprime dans le cache local les fichiers inutiles
- source # Télécharge les archives de sources
- download # Télécharge le paquet binaire dans le répertoire courant

Installer à partir des sources

- En premier, il faut pouvoir récupérer le code sources des applications.
 - Vérifier que vous avez bien les « deb-src » non commenté, dans votre dépôt

```
# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb http://fr.archive.ubuntu.com/ubuntu/ focal main restricted
deb-src http://fr.archive.ubuntu.com/ubuntu/ focal main restricted
```

- Ensuite récupérons pour l'exemple le code source de unzip
 - apt source unzip # on récupère le code source de unzip
 - On rentre dans le dossier code source
 - On installe les dépendances
 - sudo apt build-dep unzip
 - On crée le .deb
 - apt-get --build source unzip
 - Puis via dpkg on installe le .deb
 - dpkg -i <nom_du_fichier>

Installer à partir des sources

- L'installation depuis un code source se fait en plusieurs étapes et nécessite :
 - La gestion des dépendances
 - La transformation du code source en binaire.
 - un code source (format compréhensible par un humain, type ASCII) est transformé en code binaire, un langage compréhensible par votre ordinateur

La gestion du stockage

Terminologie

Les tables de partitionnement MBT et GPT

Le partitionnement avec fdisk

La gestion de la swap

Terminologie / lexique

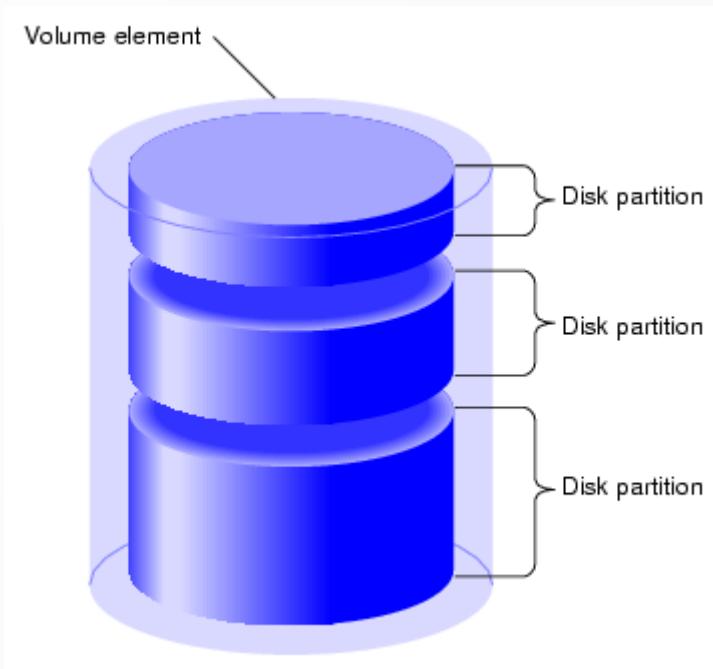
- La terminologie de vos périphériques de stockage est indiqué dans votre fichier :
 - `/lib/udev/rules.d/60-persistent-storage.rules`
- On notera que la syntaxe simplifié est :
 - [type de disque][numéro du disque][numéro de la partition]
 - Ex : `sda1`
 - `sd` = serial disk
 - `sd, hd, nvme`
 - Suivie d'une lettre qui symbolise le numéro de disque physique
 - `a,b,c,d,e` etc.
 - Suivie du numéro de partition
 - C'est lié au type de disque et à sa connectite sur la carte mère.

Terminologie / lexique

- Périphérique de stockage:
 - Tout périphérique voué à stocker des données :
 - Capables d'opérations
 - Lire
 - Ecrire
 - Supprimer

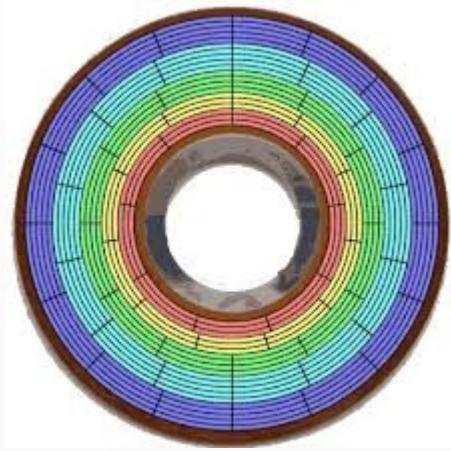
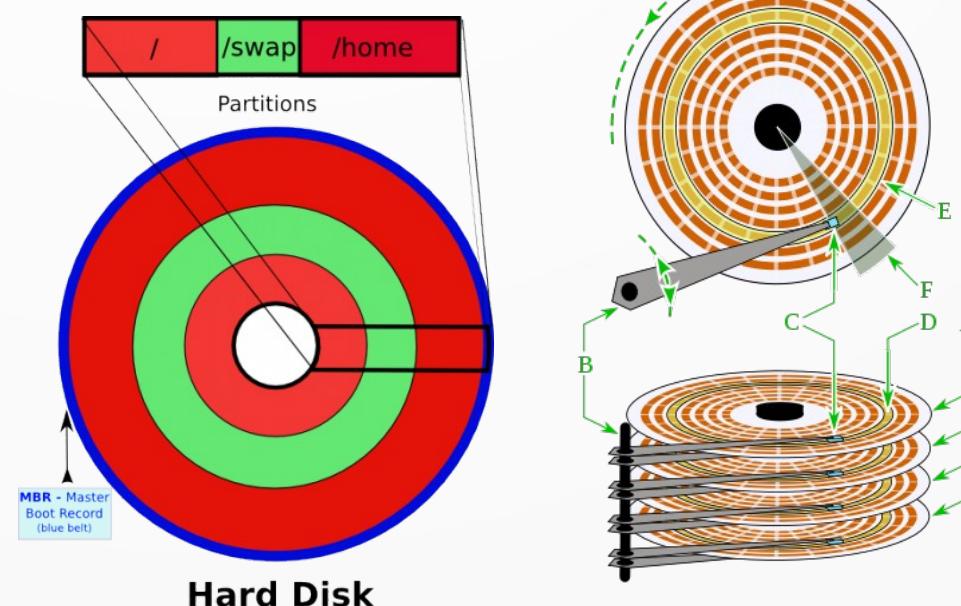
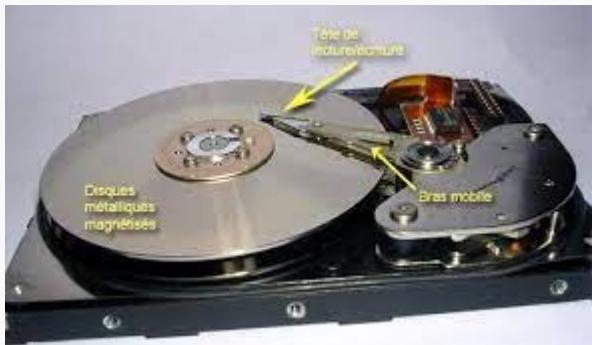
Terminologie / lexique

- Partition :
 - Découpage logique d'un périphérique de stockage



Partition

- Permet d'augmenter l'efficacité des disques à cylindre, les données ne se retrouvent ainsi pas trop séparer les unes des autres



Partition

- Sur des disques ssd, nvme.
 - Cela aura peu d'impacte sur les perfs, mais permet toujours de :
 - Segmenter partition os, partition data pour simplifier les opérations de sauvegarde.



Partition

- Un autre intérêt est de pouvoir avoir plusieurs systèmes de fichiers sur un même disque.

Les tables de partitionnement

- Il existe 2 type de table de partitionnement différent :
 - Mbr qui fonctionne avec le bios
 - Date : 1980
 - 4 Partitions primaires max (4 primaires ou 3 primaires + 1 étendue)
 - 2TO (TeraOctet)
 - 1 exemplaire
 - Gpt qui fonctionne avec UEFI
 - Date : 2000
 - 128 partitions max sur win, 255 sur linux. (les limites viennent des os non de gpt)
 - 18 EO (ExaOctet) = 18 874 368 TO (TeraOctet)
 - 2 exemplaire

Les tables de partitionnement

- C'est dans la table de partitionnement qu'est définie où commence et où finit une partition.
- C'est également cette table qui indique où est l'amorceur de démarrage.
 - Grub v1 pour mbr
 - Grub v2 pour gpt ou mbr

Le partitionnement avec fdisk

- Pour partitionner sur linux :
 - Soit lors de l'installation
 - Soit après l'installation grâce à la commande fdisk
- Fdisk :
- Utilisation :
 - `fdisk [options] <disque>` modifier les partitions
 - `fdisk [options] -l [<disque>]` afficher la table de partitions
- Description :

Afficher ou manipuler une table de partitions de disque.

Le partitionnement avec fdisk

- Commande fdisk :
 - [sudo] fdisk /dev/<disque>
 - m : pour l'aide
 - d : supprimer une partition
 - p : afficher la table de partition
 - n : ajouter une nouvelle partition
 - F : afficher l'espace libre non partitionné
 - x : fonctions avancées (réservées aux spécialistes)

La swap et sa gestion

- Swap : ram virtuelle
 - Permet d'utiliser du stockage comme fausse ram
 - Elle permet à votre système de l'utiliser en cas de surcharge
 - Elle possède une règle de priorité, vous pouvez prioriser une swap sur un ssd que sur un disque à tête (dans le cas où vous avez plusieurs swap).
 - Vous pouvez modifier la tendance de votre machine à l'utiliser avec la propriété système : «swappiness »
`echo VALEUR > /proc/sys/vm/swappiness #entre 0 et 100, default : 60`
 - Pour une modif permanente : `/etc/sysctl.conf` (insérer en fin de fichier : `vm.swappiness=VALEUR`)
- Ce n'est pas une solution magique
 - Les vitesses d'accès, écriture d'un disque n'a rien à voir avec la ram.

La swap et sa gestion

- Vous retrouverez ce机制 sous 2 formes :
 - Les partitions swap
 - Les fichiers swap
- Le fichier swap à l'avantage d'être plus facile à ajouter / supprimer.
- C'est plus difficile pour une partition swap.

La swap et sa gestion

- Voir l'utilisation de la swap
 - grep Swap /proc/meminfo
 - cat /proc/swaps
 - swapon -s
 - free -g # détaille en Gio
 - free -k # en Kio
 - free -m # Mio
- Vous la verrez sous l'intitulé partition d'échange(fr) ou swap(en)

Recommendations

- L'intérêt de votre swap va dépendre
 - Du type de travail que fait votre machine
- Les recommandations varie d'un éditeur à l'autre.
 - vous avez de ram plus votre swap va avoir tendance à égaler votre ram
 - + vous de ram moins votre swap va avoir besoin d'être grande
- L'évolution de sa taille n'est pas linéaire

Recommendations constructeur

- Red Hat

- Moins de 4Go → minimum 2Go de swap
- De 4 à 16Go → minimum 4Go swap
- De 16 à 64Go → min 8 swap
- 64 à 256Go → min 16 swap

- Centos

Ces valeurs peuvent évoluer dans le temps

Amount of RAM in the system	Recommended swap space	Recommended swap space if allowing for hibernation
< 2 GB	2 times the amount of RAM	3 times the amount of RAM
> 2 GB - 8 GB	Equal to the amount of RAM	2 times the amount of RAM
> 8 GB - 64 GB	At least 4 GB	1.5 times the amount of RAM
> 64 GB	At least 4 GB	Hibernation not recommended

La swap et sa gestion

Binary vs. decimal data measurements

BINARY SYSTEM			DECIMAL SYSTEM		
NAME	FACTOR	VALUE IN BYTES	NAME	FACTOR	VALUE IN BYTES
kibibyte (KiB)	2^{10}	1,024	kilobyte (KB)	10^3	1,000
mebibyte (MiB)	2^{20}	1,048,576	megabyte (MB)	10^6	1,000,000
gibibyte (GiB)	2^{30}	1,073,741,824	gigabyte (GB)	10^9	1,000,000,000
tebibyte (TiB)	2^{40}	1,099,511,627,776	terabyte (TB)	10^{12}	1,000,000,000,000
pebibyte (PiB)	2^{50}	1,125,899,906,842,624	petabyte (PB)	10^{15}	1,000,000,000,000,000
exbibyte (EiB)	2^{60}	1,152,921,504,606,846,976	exabyte (EB)	10^{18}	1,000,000,000,000,000,000
zebibyte (ZiB)	2^{70}	1,180,591,620,717,411,303,424	zettabyte (ZB)	10^{21}	1,000,000,000,000,000,000,000
yobibyte (YiB)	2^{80}	1,208,925,819,614,629,174,706,176	yottabyte (YB)	10^{24}	1,000,000,000,000,000,000,000,000

Byte = Octet en français

La gestion des systèmes de fichiers

Les types de systèmes de fichiers

Création d'un système de fichiers et contrôle d'intégrité

Montage d'un système de fichier

Les commandes df et du

Les quotas

Le système de fichier XFS : mise en oeuvre

Un systèmes de fichiers, c'est quoi ?

- système de fichiers (abrégé « FS » pour File System)
 - C'est comment est organiser les fichiers au sein d'une unité de stockage.
 - Très bonne vidéo pour le conceptualiser :
 - https://www.youtube.com/watch?v=iGO7N7eoqZU&ab_channel=Wandida%2CEPFL



Les types de systèmes de fichiers

- Ext4 : successeur à ext3, ext2, ext1
 - Pas de limites de sous-dossier
 - Tailles max des fichiers jusqu'à 16 To
 - Fs par default pour la plupart des distributions linux
 - Testé en permanence, stable, performant.
 - C'est le choix par default



Les types de systèmes de fichiers

- Btrfs
 - Tailles max partitions et fichiers 16 Eio
 - Moins rapides que Ext4, mais une meilleure résilience au crash (perds moins de donné)
 - Prometteur



Les types de systèmes de fichiers

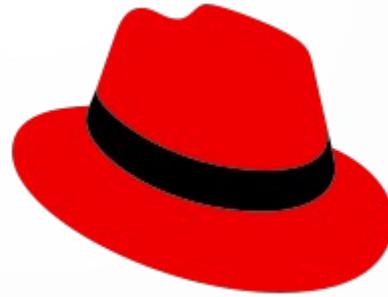
- F2FS : (en anglais « flash-friendly file system », signifiant, « Système de fichier adapté au flash »)
 - Fs orienté pour les disques à mémoires vives mais dont les données ne disparaissent pas lors d'une mise hors tension. (ssd, carte sd etc.)

SAMSUNG

Les types de systèmes de fichiers

- **Xfs :**

- Fs par default de RHEL
- Grande capacité de montée en charge
« scalle bien »



XFS	
Développeur	Silicon Graphics. Red Hat.
Structure	
Contenu des répertoires	B+ tree
Allocation de fichiers	B+ tree
Mauvais blocs	B+ tree ?
Limitations	
Taille maximale de fichier	8 exbibytes – 1 byte
Taille maximale du nom de fichiers	255 caractères
Taille maximale de volume	16 exbibytes
Caractères autorisés dans les noms de fichiers	tout caractère à l'exception de "/" et de NULL
Fonctionnalités	
Dates enregistrées	✓ Oui
Attributs	✓ Oui
Permissions	✓ Oui
Compression intégrée	✗ Non
Chiffrement intégré	✗ Non (fourni au niveau "block device")

Les types de systèmes de fichiers

- Pour les périphériques portables ont préférera ce qui est compatible entre constructeur :
 - Passe partout : fat32 (pas de notion de permissions)
 - On crypte les données sensibles
 - 4Gio max
 -

File System	Windows XP	Windows 7/8/10	macOS (10.6.4 and earlier)	macOS (10.6.5 and later)	Ubuntu Linux	Playstation 4	Xbox 360/One
NTFS	Yes	Yes	Read Only	Read Only	Yes	No	No/Yes
FAT32	Yes	Yes	Yes	Yes	Yes	Yes	Yes/Yes
exFAT	Yes	Yes	No	Yes	Yes (with ExFAT packages)	Yes (with MBR, not GUID)	No/Yes
HFS+	No	(read-only with <u>Boot Camp</u>)	Yes	Yes	Yes	No	Yes
APFS	No	No	No	Yes (macOS 10.13 or greater)	No	No	No
EXT 2, 3, 4	No	Yes (with third-party software)	No	No	Yes	No	Yes

Création d'un système de fichier et contrôle d'intégrité

**Comment on crée/applique un système de
fichier ?**

Comment on vérifie son intégrité ?

Création du système de fichier

- 1 ère étape :
 - On crée la partition avec fdisk
- 2 ème étape :
 - On la formate avec mkfs

Vérification d'intégrité

- On vérifie après la création du système de fichier
- Ou après un dysfonctionnements du système
 - Fsck : (commande qui vérifie l'intégrité du système de fichier)
 - Fsck # programme interactif, vous demande avant chaque action
 - fsck -p # corrige automatiquement les problèmes mineurs
 - Fsck [nom du disque /dev/sda1]
 - Attention : fsck va supprimer ce qu'il considère corrompu / endomagé (il demande la confirmation avant cependant y/n)

Changer de type de fichier

- Malgré que des convertisseurs existe, il est fortement recommandé de :
 - 1- Faire un backup de ses données.
 - 2- Formater le périphérique avec le nouveau fs
 - 3- Récupérer ses données

Montage d'un système de fichier

- Nos disques dans l'état même formaté ne sont pas utilisables

```
marchal@marchal-OMEN-Laptop-15-en1xxx:~$ cd /etc/nvme0n1p1
bash: cd: /etc/nvme0n1p1: Aucun fichier ou dossier de ce type
marchal@marchal-OMEN-Laptop-15-en1xxx:~$ ls -l /dev/nvme0n1p1
brw-rw---- 1 root disk 259, 1 nov. 1 20:23 nvme0n1p1
```

b

Fichier spécial : fichier bloc

- En premier lieu, il faut monter le périphérique :
 - Cad lui donner son emplacement dans l'arborescence

Montage d'un système de fichier

- On monte la partition avec la commande mount
 - umount # pour démonter
 - [sudo] mount /dev/disque /chemin/choisi

```
xx:~$  
xx:~$ sudo mount /dev/nvme0n1p1 /marchal█
```

Montage d'un système de fichier

- Pour rendre sa persistant (au redémarrage)
 - Dans /etc/fstab

```
# <file system> <mount point>  <type>  <options>      <dump>  <pass>
le disque      point de montage          fs      options
/dev/nvme0n1p1  /marchal                extf4  defaults        0        2
```

- Fs (file system) système de fichier
- Options : sans espace séparé d'une virgule
 - user (permet à n'importe qui de le monter et démonter)
 - ro (lecture seulement)
 - Etc...

Montage d'un système de fichier

- Dump (valeur pour l'utilitaire dump qui peut faire des sauvegardes)
- Pass (1= racine, 2=les autres partitions, 0 pour le swap) (c'est l'ordre de vérification lors du démarage)

Les commandes df et du

- df : (« disk free », commande pour voir l'espace utilisé et disponible)
 - -a, -all : inclut les systèmes de fichiers pseudo, dupliqués et inaccessibles.
 - -h, -human-readable : imprime les tailles en puissance de 1024
 - -i, -inodes : affiche les informations sur les inodes au lieu de l'utilisation des blocs.
 - -P, -portability : utiliser le format de sortie POSIX
 - -t, -type=TYPE : limiter la liste aux systèmes de fichiers de type TYPE
 - -T, -print-type : afficher le type de fs

Les commandes df et du

- du (liste l'espace pris par un fichier ou un dossier)
 - Par default le dossier courrant
 - Options :
 - max-depth= #
 - c # affiche la taille totale a la fin
 - h # affiche la taille en Gb
 - s # affiche juste le total
 - etc.. (man du)

Les quotas

- les solutions qui permettant de limiter l'espace disque alloué, sous linux vous avez 3 méthodes natif:
 - L'association d'un quota à un compte utilisateur appelée user quota
 - L'association d'un quota à un groupe utilisateur appelée group quota
 - L'association d'un quota à un répertoire appelée project quota (fonctionne uniquement sur XFS)

Le système de fichier XFS : mise en oeuvre

- Pour la mise en place d'un système de fichier xfs :
 - 1ère étape : Créer la partition
 - 2ème étape : On formate en XFS
 - 3ème étape : On monte le fs sur un dossier

Le RAID

**Les niveaux de RAIDs
Création et dépannage
Les disques de hot-spare**

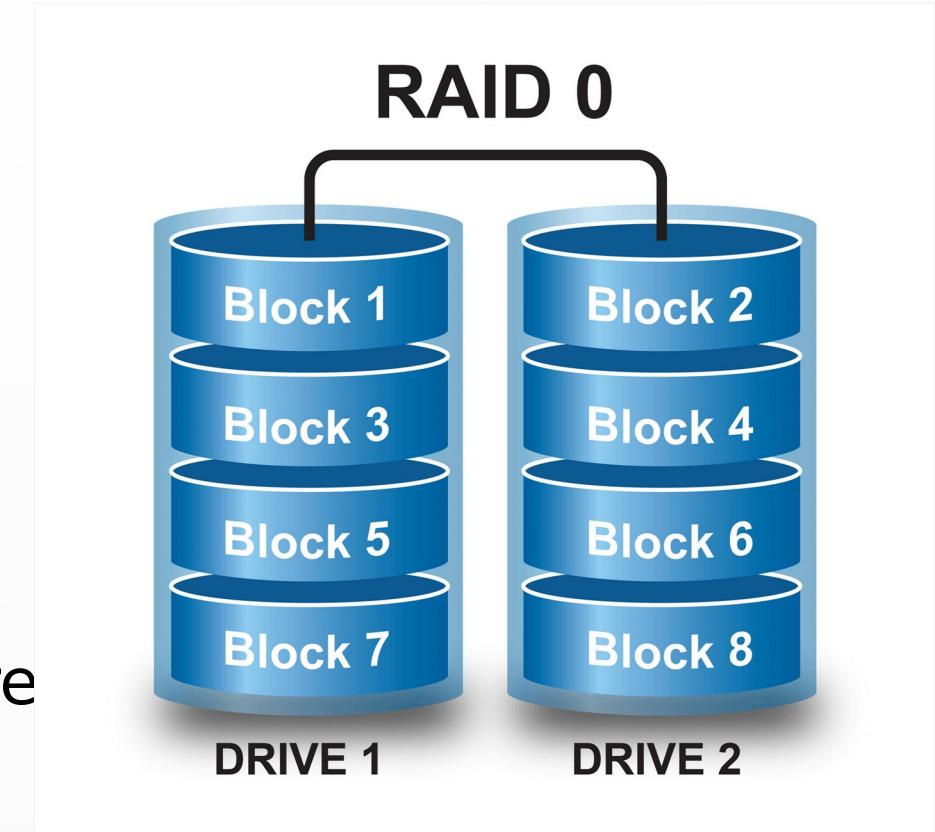
Présentation des niveaux de RAIDs

Le RAID est un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes.

- Vous retrouverez plusieurs niveaux de raid :

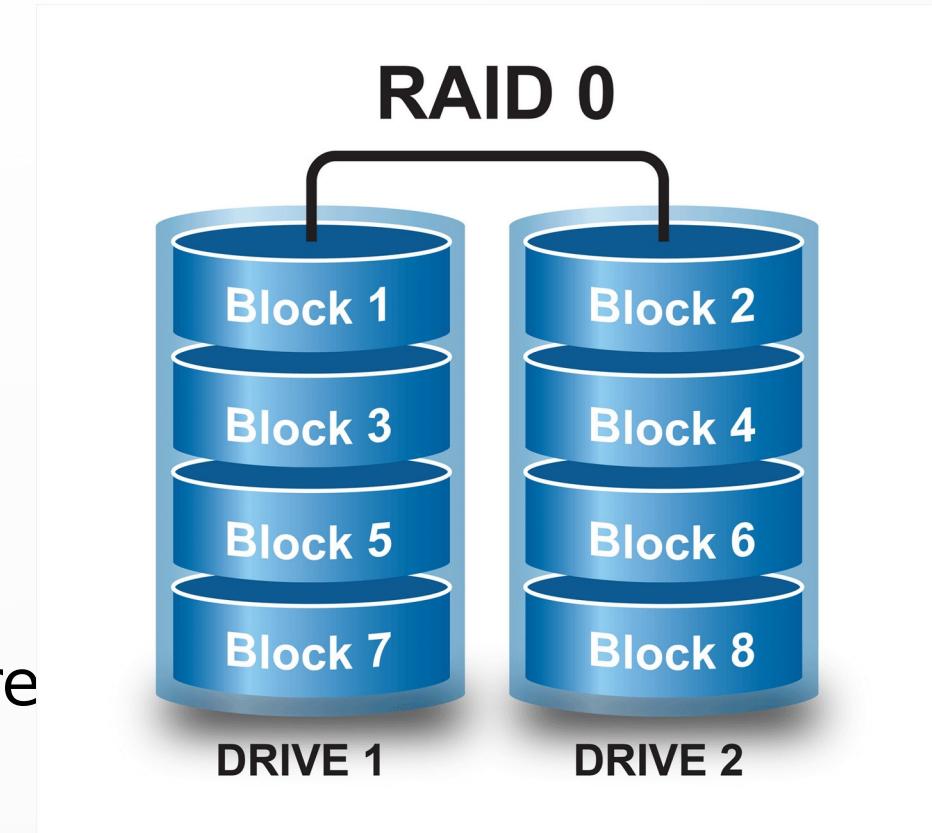
Présentation des niveaux de RAIDs

- Raid 0 :
 - 2 disques en parrallèles
 - Avantages :
 - Temps accès
 - Lecture
 - Ecriture
 - Faiblesses
 - Si 1 disque tombe, l'autre devient inutilisable
 -



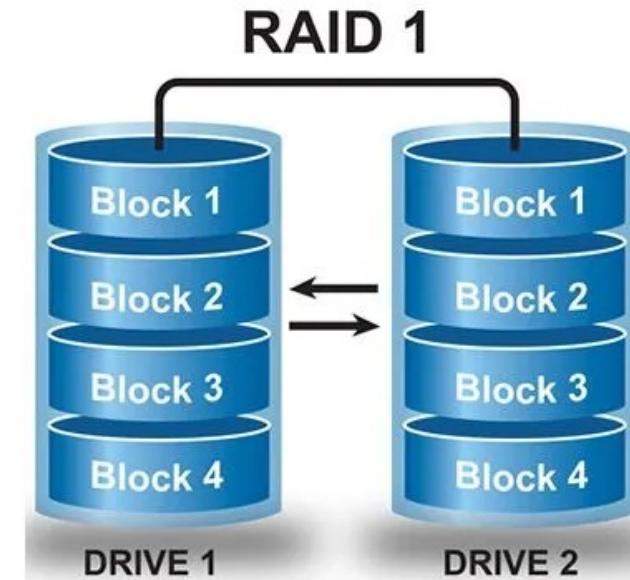
Présentation des niveaux de RAIDs

- Raid 0 :
 - 2 disques en parrallèles
 - Avantages :
 - I/O par seconde plus importante
 -
 - Faiblesses
 - Si 1 disque tombe, l'autre devient inutilisable
 -



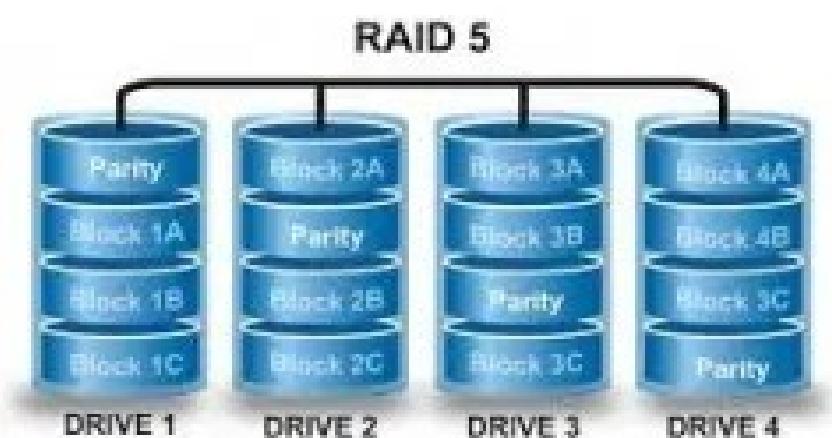
Présentation des niveaux de RAIDs

- Raid 1 :
 - 2 disques en miroirs
 - Avantages :
 - Tolérance au panne
 -
 - Faiblesses
 - Cout
 - Ecriture
 - Retour à la normale plus long



Présentation des niveaux de RAID

- Raid 5:
 - Au moins 3 disques 2 data et 1 parité
 - Avantages :
 - Ecriture / lecture
 -
 -
 - Faiblesses
 - Tolérance panne d'un seul disque
 -



Création et dépannage sur linux

Comment on créer un raid sur linux ?

- Une commande
- Disque
-

Création et dépannage sur linux

Comment on créer un raid sur linux ?

- On utilise la commande mdadm
 - En premier lieu (on l'installe « sudo apt install -y mdadm »)
- Pour un raid 0 il va nous falloir au minimum 2 disques :
 - sudo mdadm --create --verbose /dev/md0 --level=0 --raid-devices=2 /dev/sda1 /dev/sdb1

--create (pour créer un volume/array raid)

--verbose (pour nous retourner plus de détails en **stdout**)

--level (le niveau de raid)

--raid-devices (Le nombre de disques)

Création et dépannage sur linux

- Pour un raid 1, toujours avec 2 disques minimum :
 - sudo mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2 /dev/sda1 /dev/sdb1
- Pour un raid 5, cette fois avec 3 disques minimum :
 - sudo mdadm --create --verbose /dev/md0 --level=5 --raid-devices=3 /dev/sda1 /dev/sdb1 /dev/sdc1

Création et dépannage sur linux

- Pour vérifier que cela à bien fonctionner :
 - `sudo mdadm --detail /dev/md0`
--detail (nous retournes des infos sur notre raid)
 - On vient chercher la valeur de l'état (state)
 - State : clean # C'est fonctionnel
 - State : resyncing # les diques sont en train de se sync
 - State : degraded # Un disque est tombé
 - State : inactive # Le raid n'est pas en fonctionnement

Les disques de hot spare

- C'est la roue de secours du RAID.
 - Quand un disque tombe en panne et entraîne la dégradation du groupe de stockage, il vient prendre le relai pour retrouver un état sain plus rapidement.
- A savoir que un groupe de stockage ne peut être créé qu'à partir de disques du même type.

Le LVM

Présentation de LVM

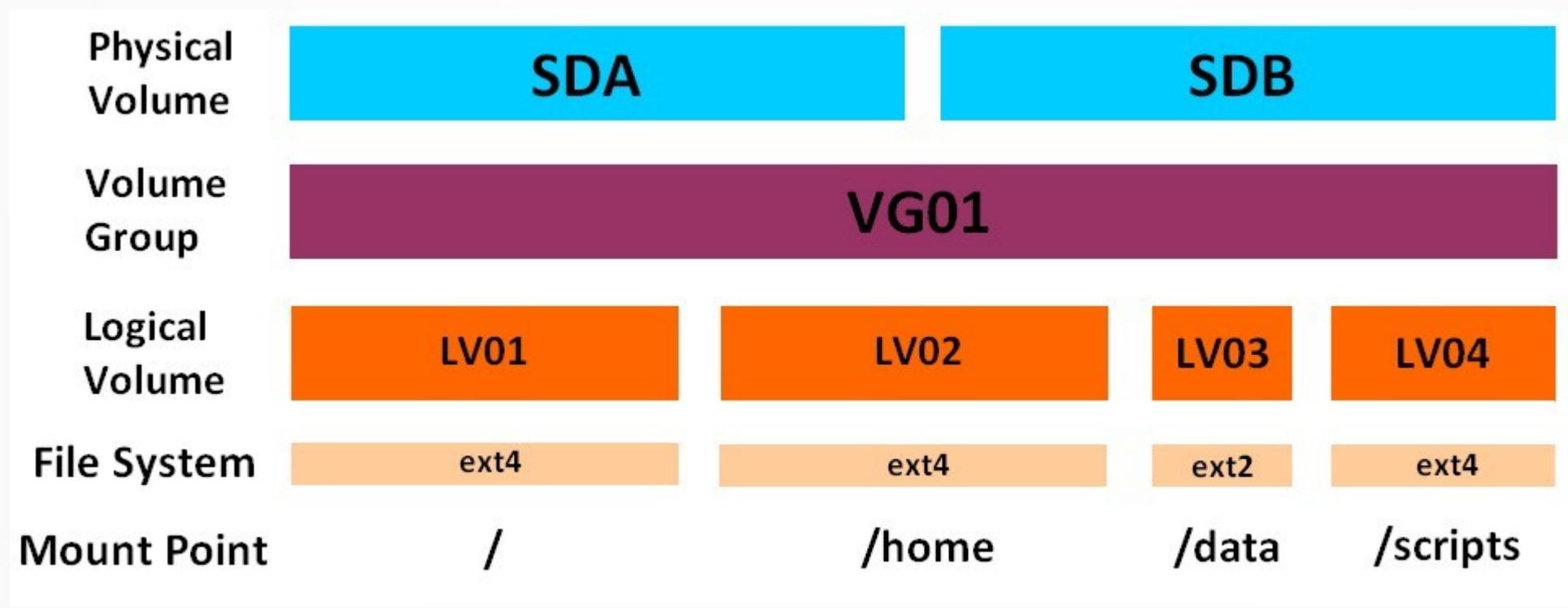
Création et administration des volumes physiques, des groupes de volumes et des volumes logiques

Agrandissement

Suppression

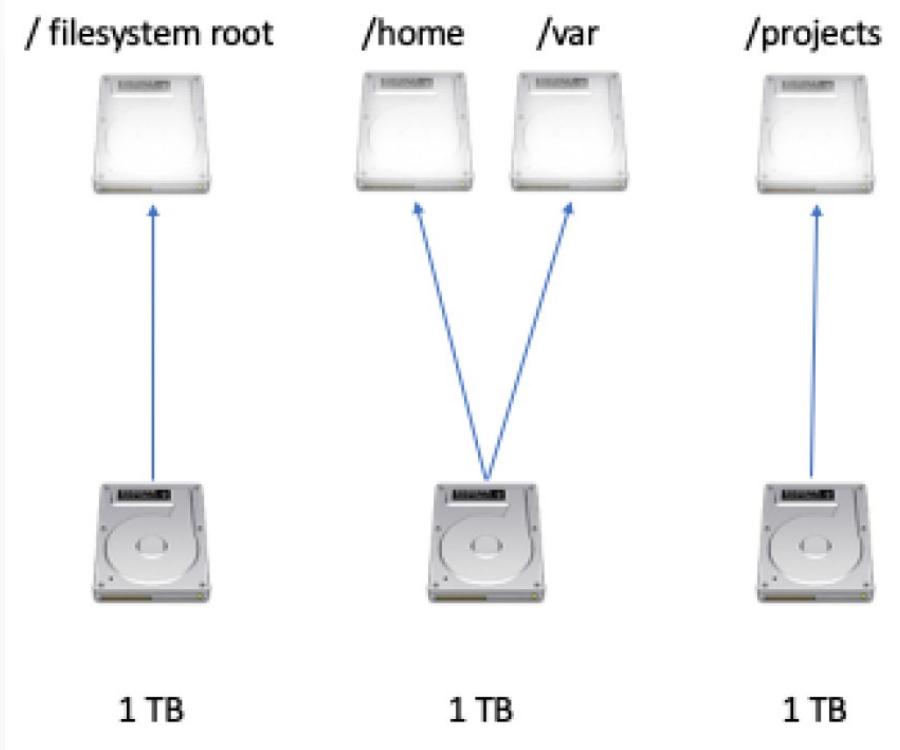
Présentation de LVM

- LVM, (Logical Volume Manager, ou gestionnaire de volumes logiques en français)

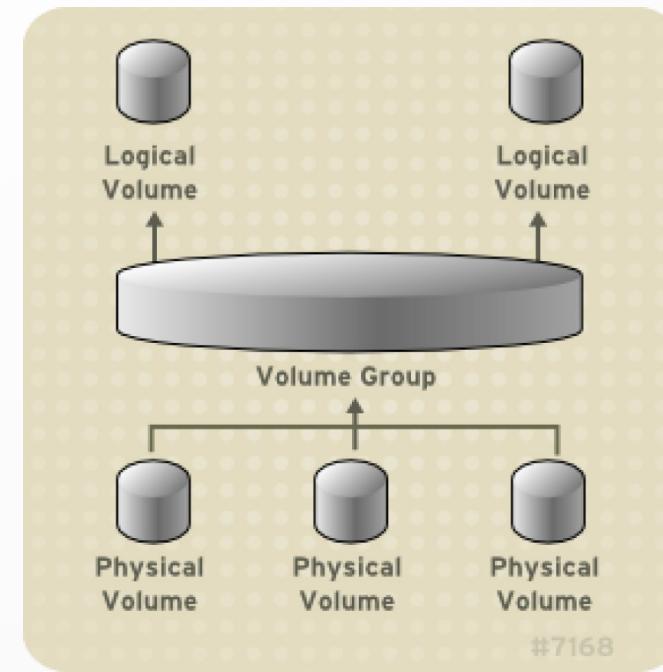


Présentation de LVM

Sans LVM

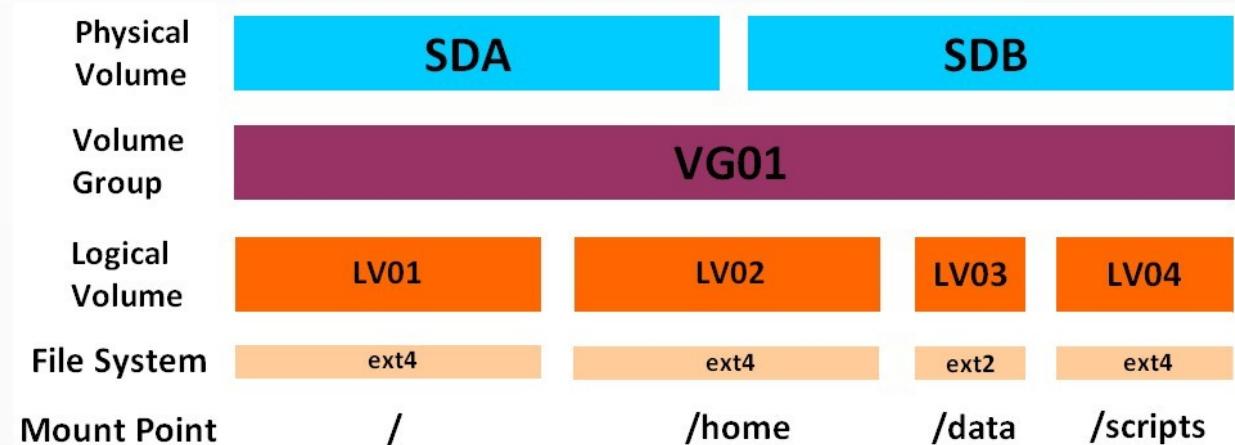


Avec LVM



Présentation de LVM

- Avec LVM on va pouvoir plus facilement :
 - Aggrandir
 - Réduire
 - La taille de nos volumes logiques
 - Intégré plus facilement de nouveaux disques !

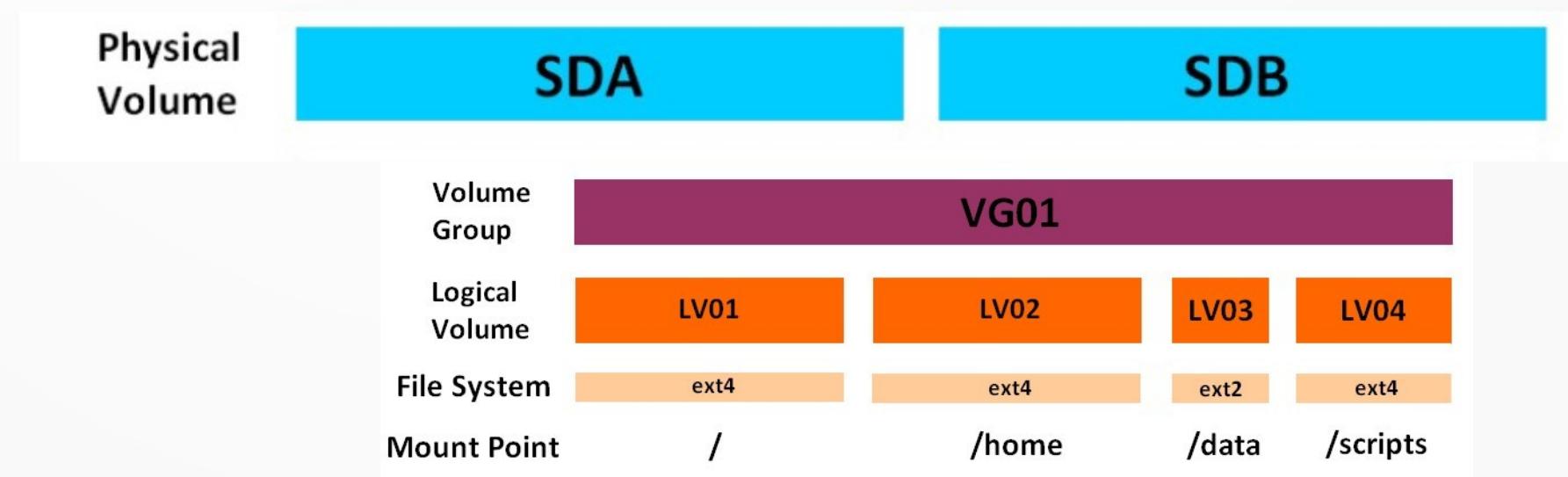


En pratique

On commence par déclarer nos volumes physiques :

pvcreate /dev/sda

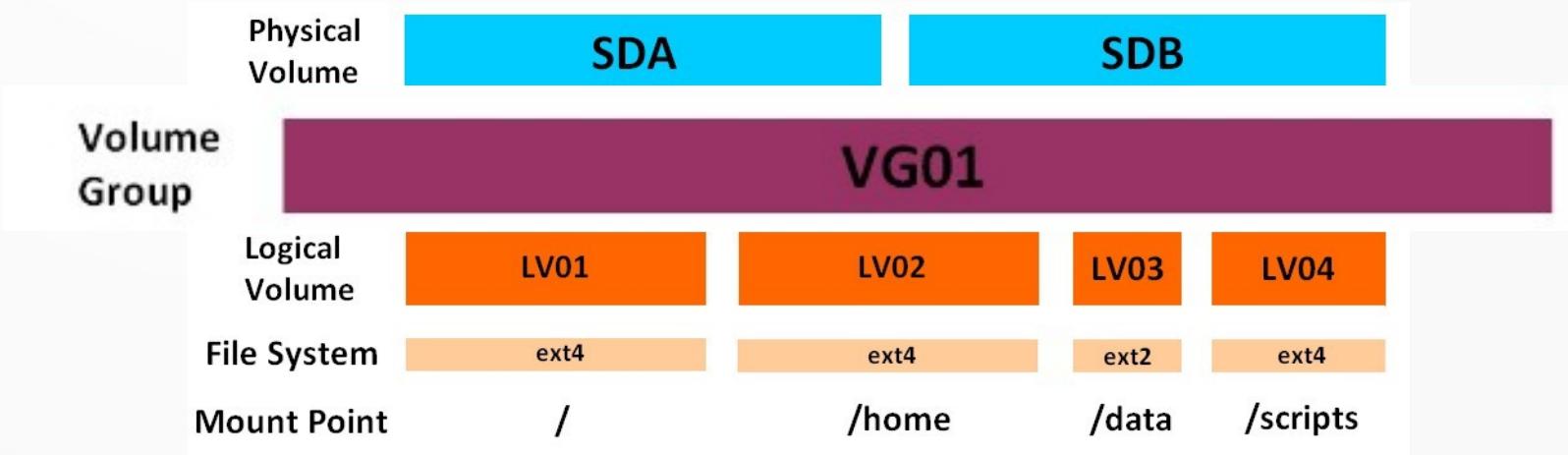
pvcreate /dev/sdb



En pratique

Ensute on déclare notre groupe de volume :

```
vgcreate mon_groupe_de_volume /dev/sda /dev/sdb
```

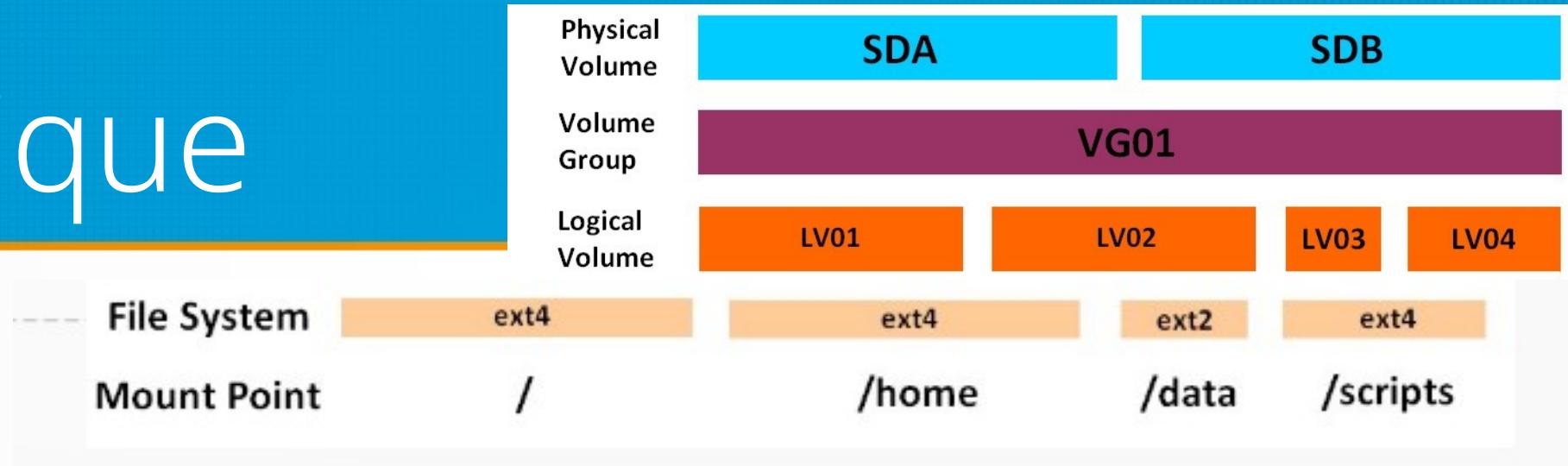


En pratique

- Puis on crée nos volumes logiques :
- lvcreate -n nom_de_volume1 -L 5G mon_groupe_de_volume
- lvcreate -n nom_de_volume2 -L 5G mon_groupe_de_volume
- lvcreate -n nom_de_volume3 -L 5G mon_groupe_de_volume



En pratique



- Il ne nous reste plus qu'à :
 - Formater le volume logique
- `Mkfs -t ext4 /dev/mon_groupe_de_volume/nom_de_volume3`
 - Fs – file system
- Puis le monter là où on le souhaite :
 - `mkdir /data`
 - `mount /dev/gv/nv /data`

Gérer la taille de nos volumes logiques

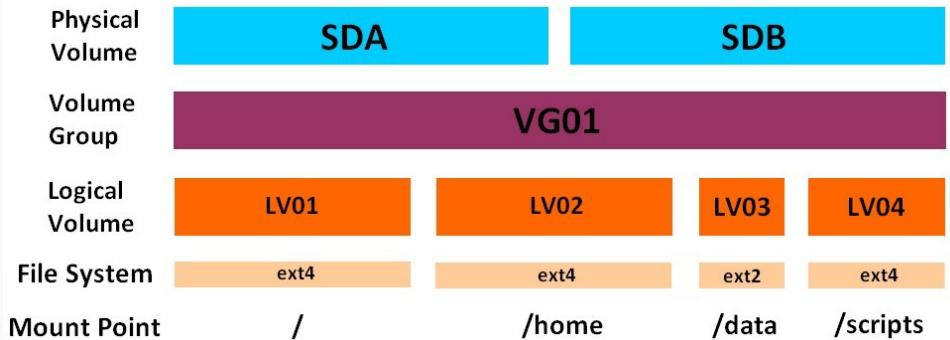
- Pour réduire la taille d'un volume logique :
 - lvreduce
- Pour augmenter la taille d'un volume logique :
 - lvextend
- Pour supprimer un volume logique :
 - lvremove

Gérer la taille de nos groupes de volumes

- Pour réduire la taille d'un groupe de volume:
 - `vgreduce`
- Pour augmenter la taille d'un groupe de volume:
 - `vgextend`
- Pour supprimer un volume logique :
 - `vgremove`

Gérer la taille de nos unités logiques

- En production :
 - Avant de manipuler, on s'assure que :
 - On a fait une sauvegarde de nos unités que l'on va manipuler.
 - En fonction de l'opération :
 - Pour réduire ou supprimer, on part de l'élément le plus bas de la pile
 - Pour augmenter, ajouter on commence par l'élément le plus haut.



Le démarrage du système et des services

Séquence de démarrage

Grub

Grub2 et sécurisation

Le système d'initialisation systemd

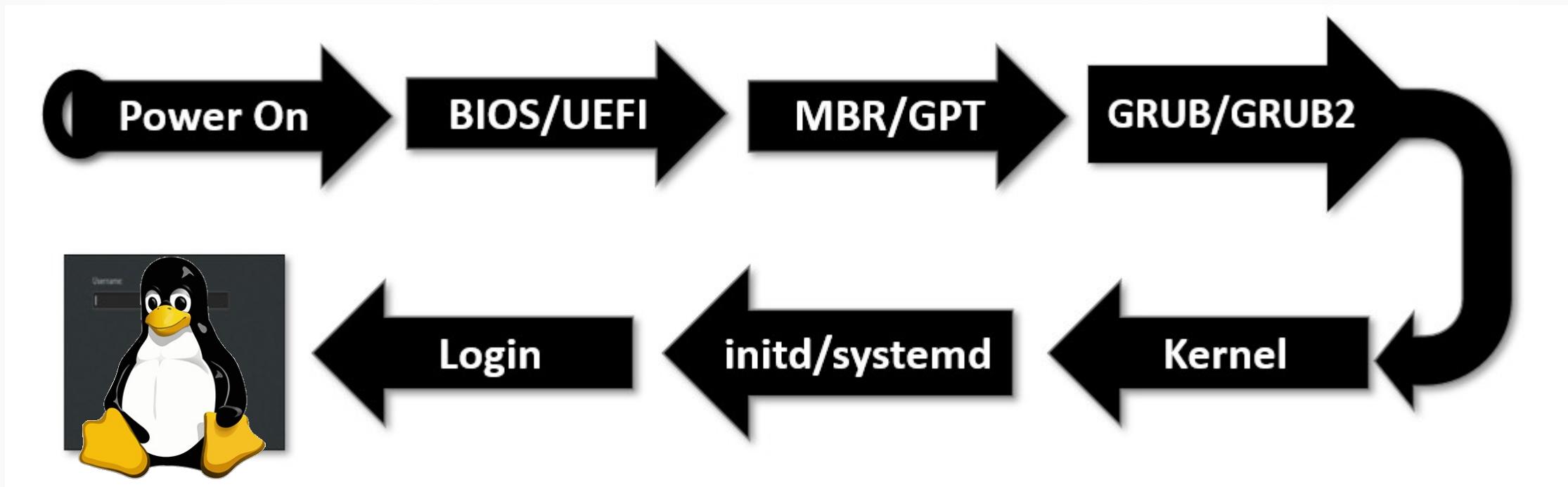
Ajout d'un service au démarrage

Arrêt du système

Le mode secours

Séquence de démarrage

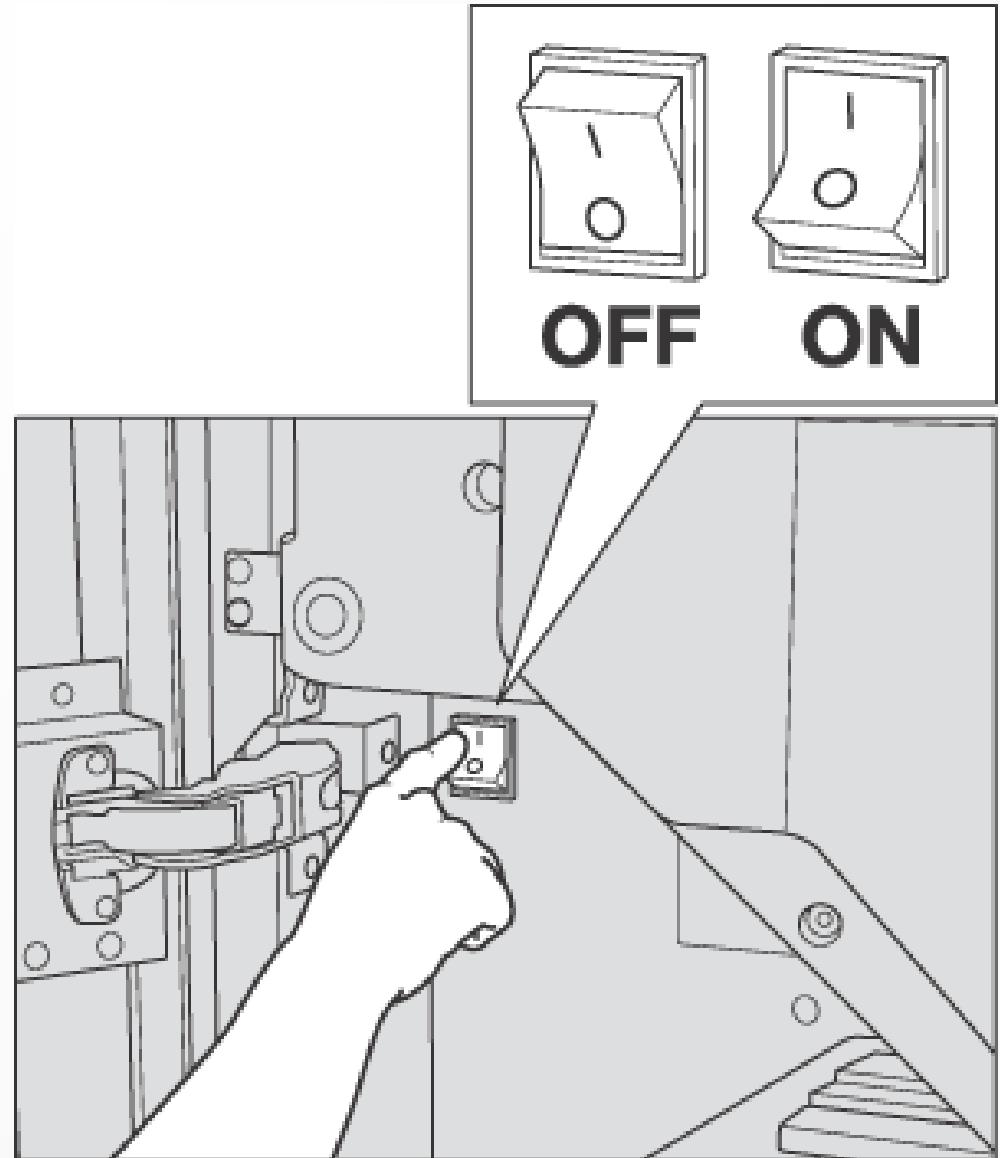
Mise sous tension → bios/uefi → Table de partition → Chargeur de démarrage → Noyau → systemd/init.d → page de login



Séquence de démarrage :

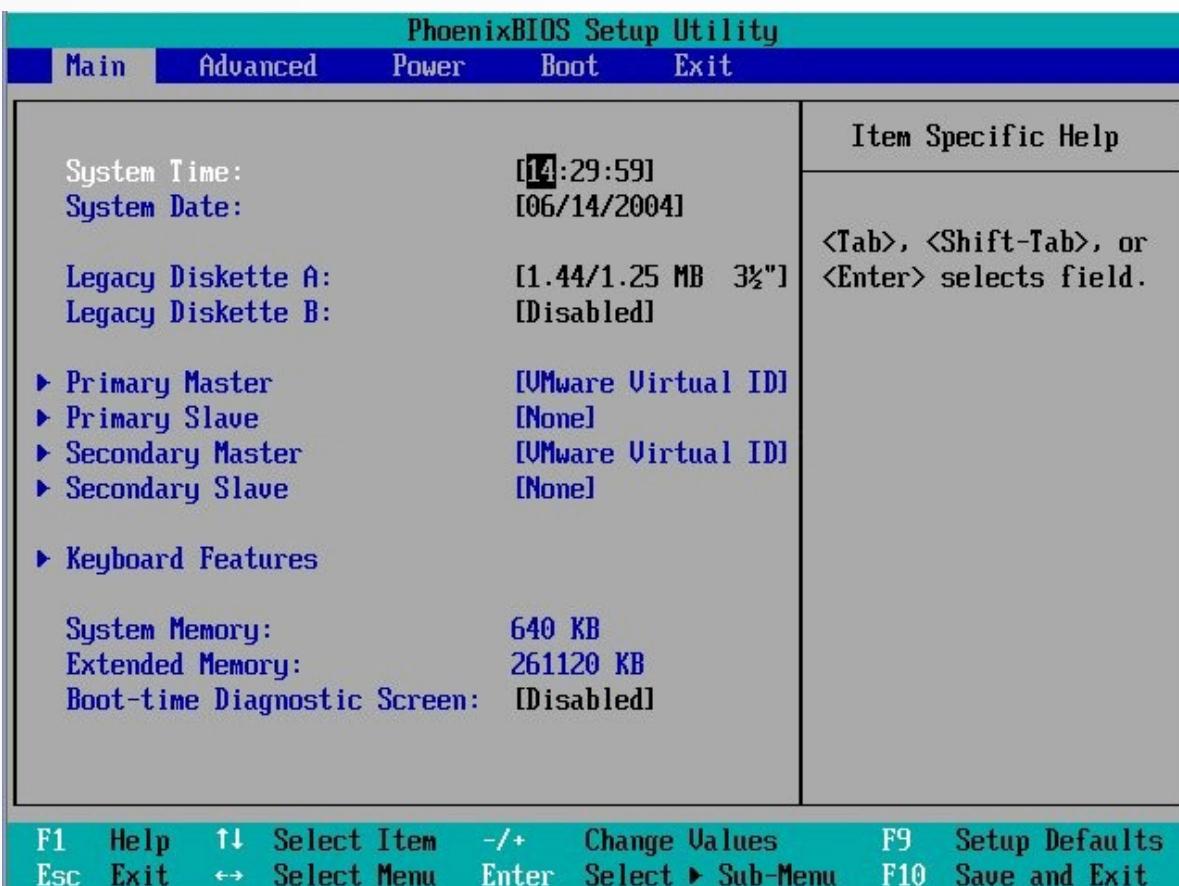
Mise sous tensions

- La mise sous tensions est une opération majoritairement manuelle. On autorise le courant vers l'alimentation du système
- La mises hors tensions sera principalement logiciel on laisse le temps au système de s'éteindre.



Séquence de démarrage : Bios/UEFI

- BIOS/UEFI est accessible juste après la mise sous tensions :
- Bios



Séquence de démarrage :

Bios/UEFI

- C'est d'ici qu'on va pouvoir modifier le comportement de notre hardware :
 - L'utilisation max de notre cpu
 - L'ordre de boot sur les périphériques (disque, cd, usb etc..)
 - Activation / désactivation d'option (virtualisation oui/non etc...)

Séquence de démarrage :

mbr/gpt

- Le démarrage suit son cours et essaye de booter sur chaque périphérique indiqué dans le bios dans un ordre définit.
 - A l'arrivé sur chaque périphérique, le système regarde la table de partition et cherche l'emplacement du chargeur d'amorçage (boot loader:windows, grub : linux)
 - Une fois le chargeur d'amorçage trouvé il lui passe la main.

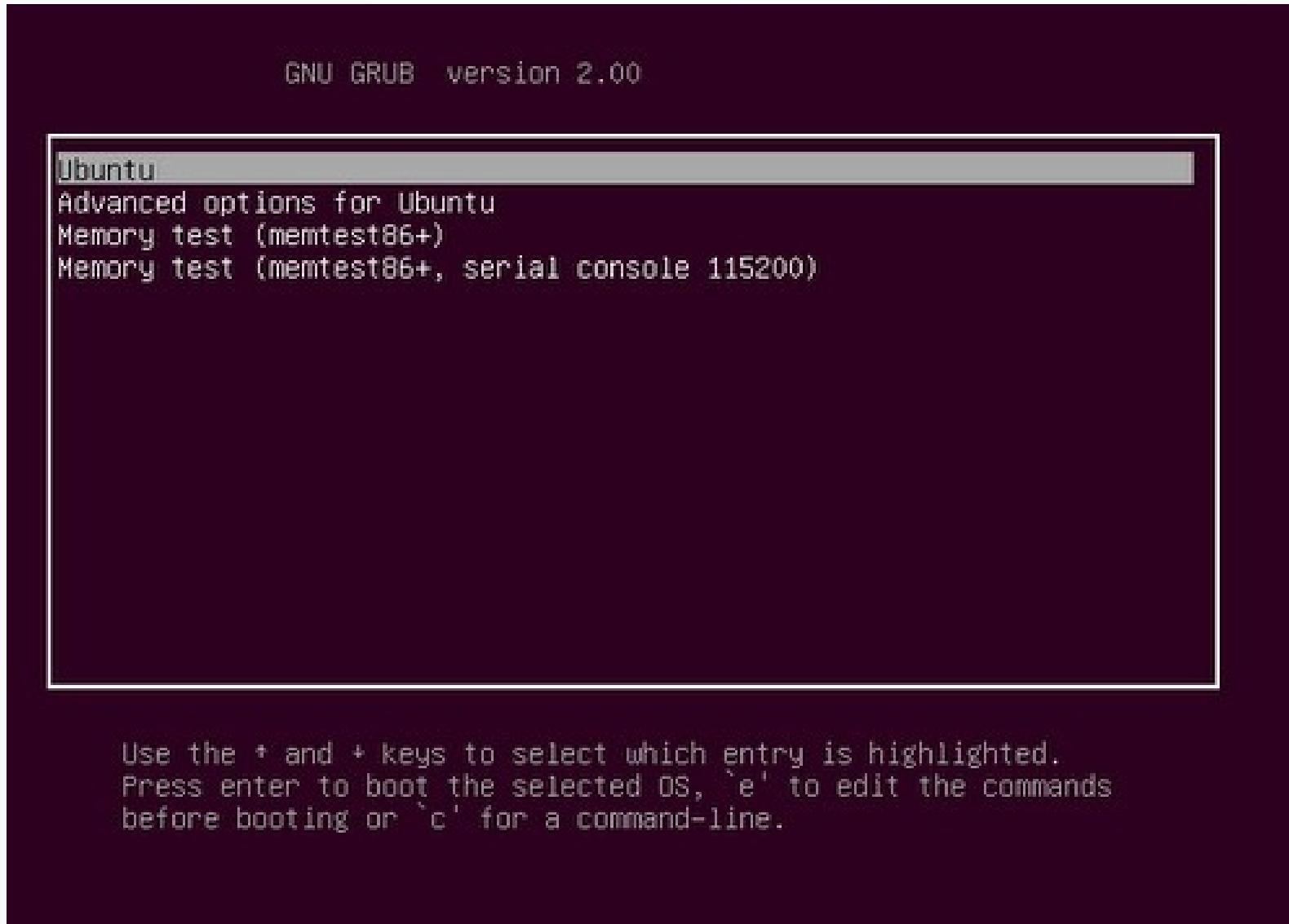
Séquence de démarrage :

Chargeur d'amorçage

- Le chargeur d'amorçage c'est le programme qui va préciser l'emplacement du kernel sur une partition ou sur un autre disque.
- C'est lui qui ensuite démarre le noyau de l'os.
- Quelques chargeurs d'amorçage : Lilo, grub, grub2, boot loader windows

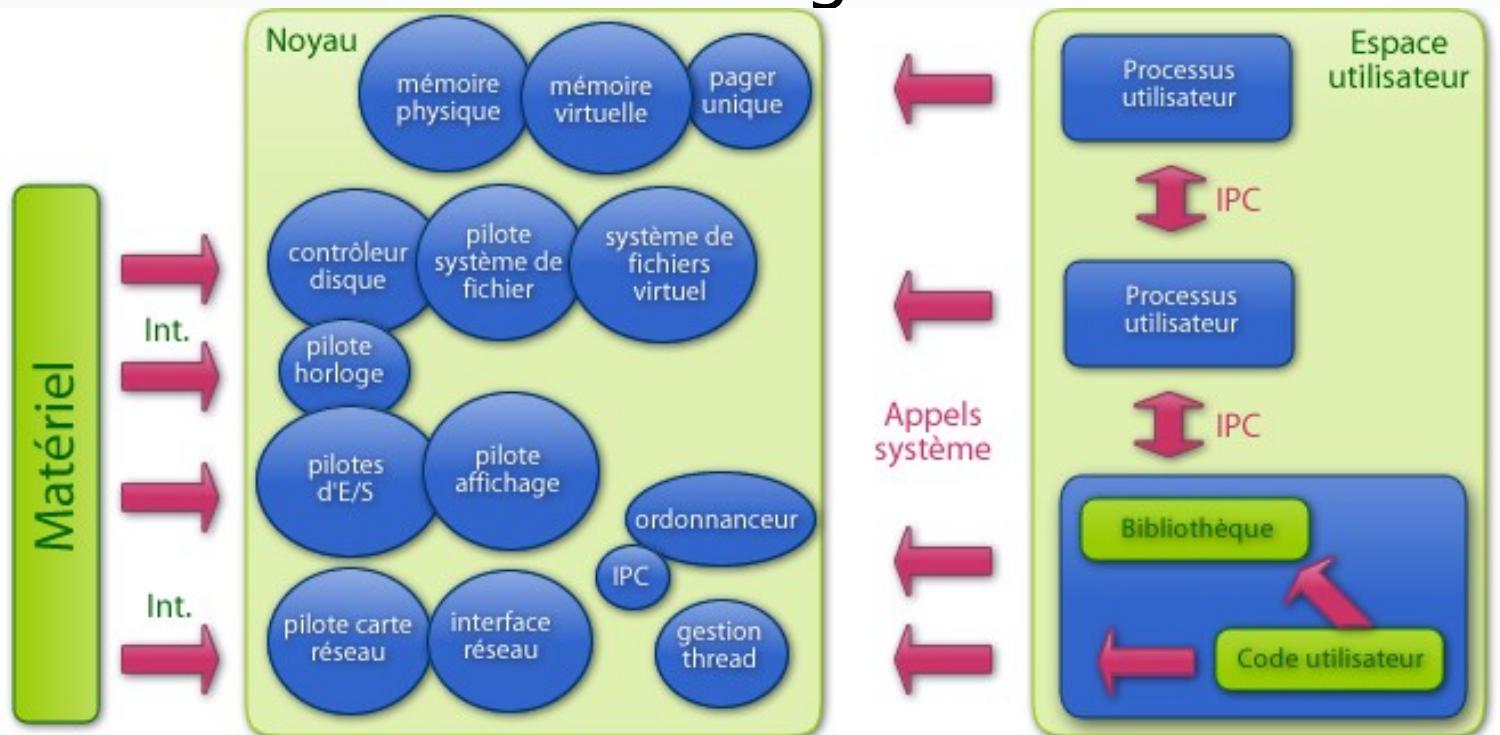
Séquence de démarrage :

Chargeur d'amorçage



Séquence de démarrage : Kernel / noyau

- C'est la partie centrale du système d'exploitation
 - Il gère les ressources du système en temps réel
 - Il permet la communication entre les composants matériels et logiciels



Une fois le kernel démaré il exécute son premier processus

Séquence de démarrage :

Système d'initialisation

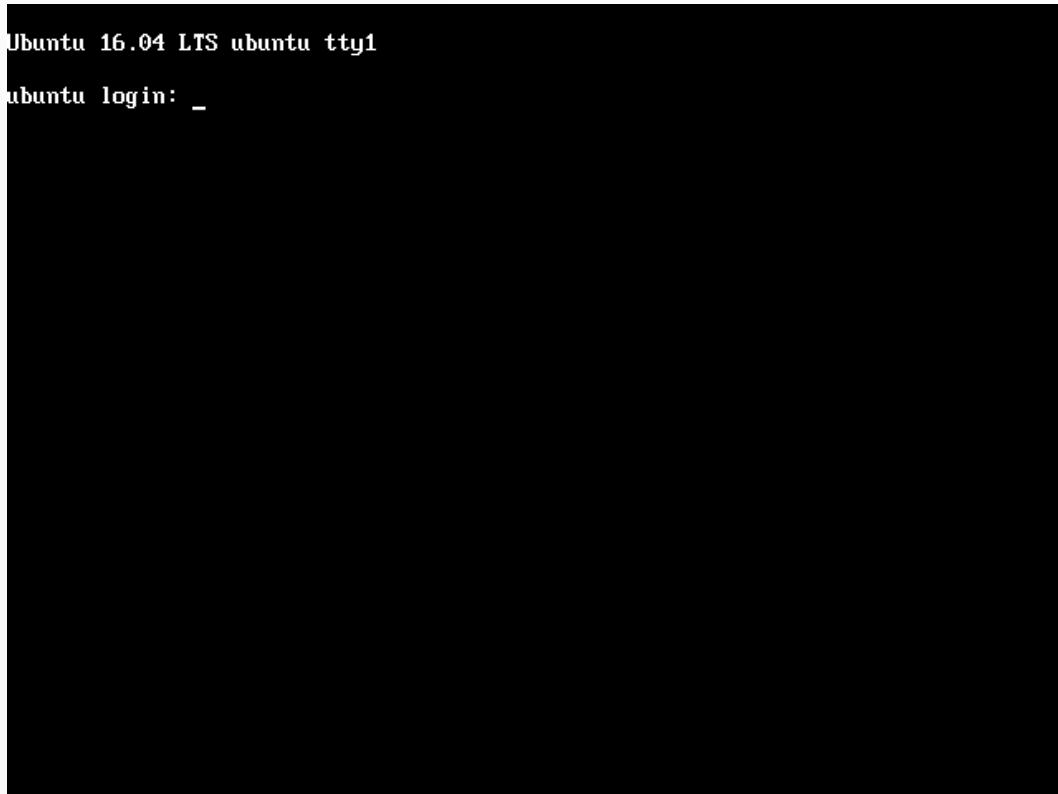
- Systemd est le premier processus démarré par le noyau :
 - Il a pour mission de démarrer les programmes essentielles à l'interactivité entre l'utilisateur et le système.
 - Le démarrage des programmes services/daemon
 - Il gère les dépendances pendant cette phase
 - L'ordre dans lequel est démarré les programmes

Séquence de démarrage : Système d'initialisation

```
Starting Accounts Service...
Starting Login Service...
[ OK ] Started VDO volume services.
[ OK ] Started Accounts Service.
[ OK ] Started Virtual Machine and Container Registration Service.
[ OK ] Started Login Service.
[ OK ] Started firewalld - dynamic firewall daemon.
[ OK ] Reached target Network (Pre).
      Starting Network Manager...
[ OK ] Started Network Manager.
[ OK ] Reached target Network.
      Starting Logout off all iSCSI sessions on shutdown...
      Starting Enable periodic update of entitlement certificates...
      Starting GSSAPI Proxy Daemon...
      Starting CUPS Scheduler...
      Starting OpenSSH server daemon...
[ OK ] Started Hyper-V KVP daemon.
      Starting Dynamic System Tuning Daemon...
      Starting Network Manager Wait Online...
[ OK ] Started Logout off all iSCSI sessions on shutdown.
[ OK ] Started Enable periodic update of entitlement certificates..
[ OK ] Started GSSAPI Proxy Daemon.
[ OK ] Reached target NFS client services.
      Starting Hostname Service...
[ OK ] Started OpenSSH server daemon.
[ OK ] Started CUPS Scheduler.
[ OK ] Started Hostname Service.
      Starting Network Manager Script Dispatcher Service...
```

Fin de la Séquence de démarrage : L'espace de login

- Une fois que la séquence de démarrage est terminé et le système est fonctionnel, nous arrivons sur l'espace de connection :



Maintenant que nous avons vu la séquence de démarrage.

Revenons sur quelques un de ses éléments :
Grub
Systemd

Grub legacy

Grub ou grub legacy ($\text{grub} \leq 1.99$ version) puis grub 2 ($\text{grub} \geq 2$ version).

C'est un programme libre, un boot loader / Chargeur d'amorçage.

- C'est lui qui démarre le kernel linux, il permet aussi le multi boot.
 - Multi boot : pouvoir démarrer sur différents systèmes d'exploitation depuis la même machine.

Grub2

- Grub 2 (version \geq 2)
 - Grub2 est compatible bios / uefi, mbr / gpt
 - C'est l'amorceur par default sous linux
 - Il utilise le fichier :
 - /boot/grub/**grub.cfg**
 - Ce fichier est construit via les fichiers de configurations suivants :
 - /etc/default/grub
 - /etc/grub.d/*
 - Le fichier **grub.cfg** peut être reconstruit via la commande :
 - grub-mkconfig -o /boot/grub/grub.cfg

Grub2

- Configurer Grub2 :
 - /etc/default/grub
 - Depuis ce fichier vous aller pouvoir faire du paramétrage :
 - Quel est le champ par défaut
 - Combien de temps avant de booter automatiquement sur le champ par défaut
 - La langue utilisé
 - Etc...
 - Ces paramètres sont représentés :
 - 1 paramètre par ligne
 - En Clé / Valeur : **GRUB_TIMEOUT=10**

Grub2

- Configurer Grub2 :
 - /etc/grub.d/*
 - Ce dossier contient tous les scripts qui seront utilisés (en respectant l'ordre de numérotation) par update-grub pour créer le fichier grub.cfg.

```
00_header
05_debian_theme
10_linux
10_linux_zfs
20_linux_xen
20_memtest86+
30_os-prober
30_uefi-firmware
35_fwupd
40_custom
41_custom
```

Grub2

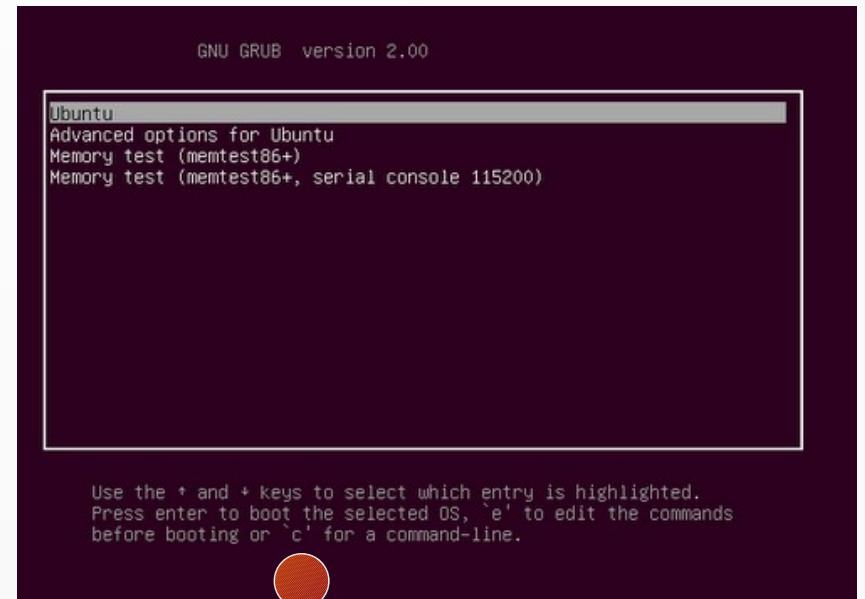
- Ces 2 fichiers travaillent de pairs :
 - /etc/default/grub # donne la valeur au variable
 - /etc/grub.d/* # utilise les valeurs définit dans /etc/default/grub

```
marchal@marchal-OMEN-Laptop-15-en1xxx:/etc/grub.d$ grep -r "GRUB_TIMEOUT" /etc/grub.d/
/etc/grub.d/00_header:if [ "x${GRUB_TIMEOUT}" = "x" ] ; then GRUB_TIMEOUT=5 ; fi
/etc/grub.d/00_header:if [ "x${GRUB_TIMEOUT_BUTTON}" = "x" ] ; then GRUB_TIMEOUT_BUTTON="$GRUB_TIMEOUT" ; fi
/etc/grub.d/00_header:    grub_warn "$(gettext "Setting GRUB_TIMEOUT to a non-zero value when GRUB_HIDDEN_TIMEOUT is set is no longer supported.")"
/etc/grub.d/00_header:    # No hidden timeout, so treat as GRUB_TIMEOUT_STYLE=menu
/etc/grub.d/00_header:make_timeout "${GRUB_HIDDEN_TIMEOUT_BUTTON}" "${GRUB_TIMEOUT_BUTTON}" "${GRUB_TIMEOUT_STYLE_BUTTON}"
/etc/grub.d/00_header:make_timeout "${GRUB_HIDDEN_TIMEOUT}" "${GRUB_TIMEOUT}" "${GRUB_TIMEOUT_STYLE}"
/etc/grub.d/00_header:make_timeout "${GRUB_HIDDEN_TIMEOUT}" "${GRUB_TIMEOUT}" "${GRUB_TIMEOUT_STYLE}"
```

- **Suivant** : Comment sécuriser grub

Grub2 et sécurisation

- Attention, Grub possède un shell minimaliste accessible via la touche « c »
 - N'importe qui avec un accès physique à votre machine peut s'en servir pour changer le mdp de root.
 - Il est possible de s'en protéger, en rajoutant une étape de login pour y accéder.



Grub2 et sécurisation

- Procédure:
 - 1) on fais un back up du fichier de config qu'on va manipuler :
 - sudo cp /etc/grub.d/00_header /etc/grub.d/header.00.bkp
 - 2) on génère un mdp hashé grub-mkpasswd-pbkdf2
 - On récupère le mdp hashé « grub.pbkdf2.sha512.10000... »
 - 3) on ajoute au script 00_header à la fin :

```
cat << EOF
set superusers="marchal"
password marchal grub.pbkdf2.sha512.10000
EOF
```

Grub2 et sécurisation

- On peut aussi ajouter une étape de login lors du choix de l'os sur lequel boot.
 - Depuis le script 30_os-prober
 - En ajoutant --users au menuentry

```
menuentry '$(echo "${LONGNAME} $onstr" | grub_quote)' $CLASS --class os \$menuentry_id_option 'osprober-chain-$({grub_get_device_id "${DEVICE}"})'{  
EOF
```

- Ex :

```
cat << EOF  
menuentry '$(echo "${LONGNAME} $onstr" | grub_quote)' $CLASS --class os \$menuentry_id_option 'osprober-chain-$({grub_get_device_id "${DEVICE}"})'--users  
EOF
```

-

Le système d'initialisation systemd

- **Systemd**
 - Systemd est le programme moderne d'initialisation du système. La plupart des distribs utilisent systemd comme programme d'initialisation par défaut.

Le système d'initialisation systemd

- C'est le premier processus lancé par le kernel :
 - C'est également le processus parent de tous les autres process

```
marchal@marchal-OMEN-Laptop-15-en1xxx:/etc/grub.d$ pstree
systemd─ModemManager─2*[{ModemManager}]
              └─NetworkManager─2*[{NetworkManager}]
                  ├─accounts-daemon─2*[{accounts-daemon}]
                  ├─acpid
                  ├─at-spi-bus-laun─dbus-daemon
                  │   └─3*[{at-spi-bus-laun}]
                  ├─at-spi2-registr─2*[{at-spi2-registr}]
                  ├─avahi-daemon─avahi-daemon
                  ├─bluetoothd
                  ├─colord─2*[{colord}]
                  ├─cron
                  ├─cups-browsed─2*[{cups-browsed}]
                  ├─cupsd
                  ├─dbus-daemon
                  ├─gdm3─gdm-session-wor─gdm-x-session─Xorg─20*[{Xorg}]
                  │   └─dbus-run-session─dbu
```

Systemd structure fichier

- Vous retrouverez les fichiers gérés par systemd

Dans :

- `/lib/systemd/system` # Unité par default
- `/etc/systemd/system` # Unité configuré, écrase celle de /lib/
- `/run/systemd/system` # Unité en cours de fonctionnement, écrase celle de /etc/ et /lib/

Systemd concept

- Systemd concerne tous les éléments qu'il gère comme des « unités », vous en trouverez 11 :

- .service 	# comment démarrer, arrêter le service
- .socket	# décrit la communication entre hôtes ou process
- .device	# permet de définir des dependances /dev/sda5 : dev-sda5.device
- .mount	# Définit un point de montage supervisé par systemd
- .automount	# Monte un point de montage sur demande, puis le démonte
- .swap	# Décrit un fichier ou partition swap
- .target 	# Groupe d'autre unité ensemble
- .path	# Décrit un emplacement de l'arbo géré par systemd
- .timer	# Equivalent à crontab
- .snapshot	# créée par systemctl snapshot, sauvegarde l'état actuelle
- .slice	# Définit un groupe de ressource pour un groupe de process
- .scope	# Définit un groupe de process indépendant

Le système d'initialisation systemd

- Comment travailler avec systemd :

- Systemctl

- Contrôle l'état des unités de systemd

- Systemctl **status** <nom_de_l'unité>
 start <nom_de_l'unité>
 stop <nom_de_l'unité>
 restart <nom_de_l'unité>
 reload <nom_de_l'unité>
 enable <nom_de_l'unité>
 disable <nom_de_l'unité>
 show <nom_de_l'unité>
 deamon-reload

Action	unité
--------	-------

systemctl

systemctl status ssh

- D'où est chargé l'unité de gestion :

```
marchal@demo:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2022-11-04 15:00:06 CET; 2 days ago
    Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 384 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 408 (sshd)
     Tasks: 1 (limit: 2335)
    Memory: 6.1M
      CPU: 58ms
     CGroup: /system.slice/ssh.service
             └─408 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.
```

systemctl

- Enabled = activé au démarrage (!désactivé = disable)
- Vendor preset = Etat préconfiguré par le fournisseur

```
marchal@demo:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2022-11-04 15:00:06 CET; 2 days ago
    Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 384 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 408 (sshd)
   Tasks: 1 (limit: 2335)
  Memory: 6.1M
    CPU: 58ms
   CGroup: /system.slice/ssh.service
           └─408 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.
```

systemctl

- L'état en cours, et depuis quand

```
marchal@demo:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2022-11-04 15:00:06 CET; 2 days ago
    Docs: man:sshd(8)
          man:sshd_config(5)
   Process: 384 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 408 (sshd)
    Tasks: 1 (limit: 2335)
   Memory: 6.1M
      CPU: 58ms
     CGroup: /system.slice/ssh.service
             └─408 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.
```

systemctl

- Ou trouver de la documentation :
 - man 8 sshd ; man 5 sshd_config (peut etre aussi une url)

```
marchal@demo:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2022-11-04 15:00:06 CET; 2 days ago
    Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 384 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 408 (sshd)
    Tasks: 1 (limit: 2335)
   Memory: 6.1M
      CPU: 58ms
     CGroup: /system.slice/ssh.service
             └─408 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.
```

systemctl

Numéro de process : 384, la commande executé au démarage (ExecStartPre etc.)

- Le code de retour 0 = succès

```
marchal@demo:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2022-11-04 15:00:06 CET; 2 days ago
    Docs: man:sshd(8)
          man:sshd_config(5)
   Process: 384 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 408 (sshd)
   Tasks: 1 (limit: 2335)
  Memory: 6.1M
     CPU: 58ms
    CGroup: /system.slice/ssh.service
             └─408 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.
```

systemctl

- Main PID : le process enfant de 384 celui qui gère l'unité ssh.service
- Tasks, Memory , cpu lié au cgroup

```
marchal@demo:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2022-11-04 15:00:06 CET; 2 days ago
    Docs: man:sshd(8)
          man:sshd_config(5)
   Process: 384 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 408 (sshd)
    Tasks: 1 (limit: 2335)
   Memory: 6.1M
      CPU: 58ms
     CGroup: /system.slice/ssh.service
             └─408 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.
```

systemctl

- Le groupe de contrôle c'est l'entité parente qui gère le process 408

```
marchal@demo:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
  Active: active (running) since Fri 2022-11-04 15:00:06 CET; 2 days ago
    Docs: man:sshd(8)
          man:sshd_config(5)
   Process: 384 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 408 (sshd)
   Tasks: 1 (limit: 2335)
  Memory: 6.1M
    CPU: 58ms
   CGroup: /system.slice/ssh.service
           └─408 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.
```

systemctl

- Les derniers logs du services

```
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2022-11-04 15:00:06 CET; 2 days ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 384 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 408 (sshd)
   Tasks: 1 (limit: 2335)
  Memory: 6.1M
    CPU: 58ms
   CGroup: /system.slice/ssh.service
           └─408 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

nov. 04 15:00:06 demo sshd[408]: Server listening on :: port 22.
nov. 04 15:00:06 demo systemd[1]: Started OpenBSD Secure Shell server.
nov. 04 16:10:30 demo sshd[672]: Accepted publickey for marchal from 2a01:cb16:23:9f85:3c7a:a447:f50>
nov. 04 16:10:30 demo sshd[672]: pam_unix(sshd:session): session opened for user marchal(uid=1000) b>
nov. 05 17:31:40 demo sshd[2573]: Accepted publickey for marchal from 2a01:cb16:2061:68bd:7c73:ae7c:>
nov. 05 17:31:40 demo sshd[2573]: pam_unix(sshd:session): session opened for user marchal(uid=1000) >
```

Suivant : travailler avec les logs de systemd

journalctl

- Naviger dans le journal de log de systemd
 - `Journalctl` # Tous le journal
 - `Journalctl -f` # Que les dernières entrées
 - `Journalctl -u` # Par service
 - `Journalctl _PID=` # Par process
 - `Journalctl /usr/sbin/sshd` # Par programme
 - `journalctl -p err` # Par erreurs
- Ces options se combinent

journalctl

- Filtré par date :
 - since "2016-02-10 21:00:00" # depuis le
 - until "2016-02-10 22:00:00" # jusqu'au
 - since "10 minutes ago" # Depuis 10 min
- Ces options se combinent aussi
- **Suivant** : ajouter un service au démarage

Ajouter un service au démarrage

- Pour ajouter un service il faut:
 - Créer un fichier <mon_service>.service dans l'un des dossier géré par systemd.
 - Indiqué la section [Unit], [Service], [Install]
 - Unit : On décrit :
 - Sa description, apres/avant quel service il est démaré
 - Service :
 - Le Type de process désiré
 - La commande de gestion de status ExecStart, ExecStop
 - Install :
 - Après quoi il est utilisable

Ajouter un service au démarrage

- Ex :

```
[Unit]
Description=OpenBSD Secure Shell server
Documentation=man:sshd(8) man:sshd_config(5)
After=network.target auditd.service

[Service]
ExecStartPre=/usr/sbin/sshd -t
ExecStart=/usr/sbin/sshd -D $SSHD_OPTS
ExecReload=/usr/sbin/sshd -t
ExecReload=/bin/kill -HUP $MAINPID

[Install]
WantedBy=multi-user.target
```

Suivant : Arrêt du système

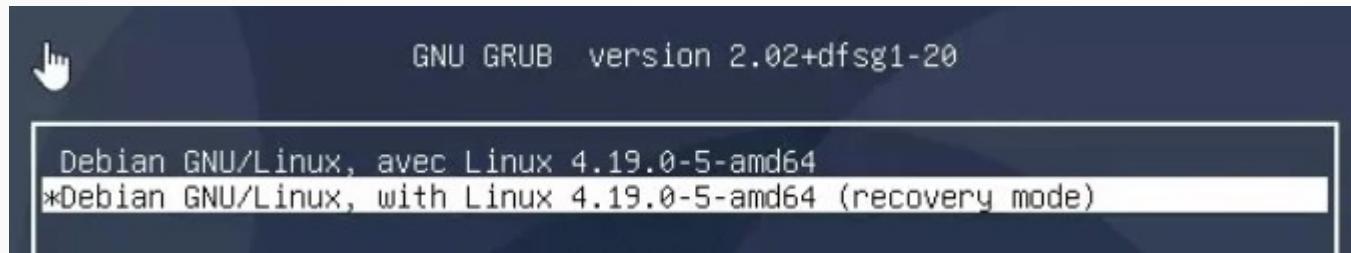
Arrêt du système

- Linux pour s'éteindre suit ce déroulé :
 - 1) systemd ferme les process dans le sens inverse de leur lancement
 - 2) le kernel s'éteint
 - 3) le hardware suis sa routine logique d'arrêt
- Pour envoyer le signal d'arrêt du système :
 - Via la commande
 - sudo shutdown -P now # arrêt immédiat du système
 - Shutdown # arrêt dans une minute
 - shutdown +m # ou m est le nombre de minute

Suivant : le mode secours

Le mode secours

- Dans tous les os vous avez un mode de secours :
 - Vous pouvez y accéder depuis grub, vous remarquerer un choix avec (recovery mode)



- En derniers recours vous pouvez booter sur un os live depuis un périphérique externe.
 - Généralement une clé usb qui contient l'iso d'installation

Suivant : Chapitre - Administration des utilisateurs

Administration des utilisateurs

**Création, modification et suppression d'un compte
La sécurité avec PAM
La personnalisation de l'environnement utilisateur
Les permissions**

- Sur linux il existe 3 types de comptes :
 - Utilisateurs normaux
 - Utilisé par un utilisateur. Jean viens au travail, il se connecte avec son compte Jean.
 - L'Administrateur
 - Utilisé par un administrateur, il a en général tous les droits sur la machine.
 - Les comptes systèmes
 - Associés à des services

- Avoir plusieurs types d'utilisateurs permet :
 - + de sécurité
 - + facilement suivre son utilisation (monitorer)

Suivant - Fichier lié au utilisateurs

- Sur linux vous retrouvez 2 fichiers qui référence vos utilisateurs :
 - /etc/passwd
 - /etc/shadow
- Chaque ligne indique une entrée / un utilisateur
- Les colonnes sont délimitées par « : »

Suivant - /etc/passwd structure

Création, Modification, suppression d'un compte

/etc/passwd

```
marchal@marchal-OMEN-Laptop-15-en1xxx:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```

- 1 : identifiant, 2 : Mot de passe, 3 : UID, 4 : GID
- 5 : détail, 6 : Répertoire d'utilisateur
- 7 : le chemin absolu vers son interpréteur
(cela peut être vers un interpréteur nologin ou false)

Suivant - /etc/shadow structure

Création, Modification, suppression d'un compte

/etc/shadow

```
marchal@marchal-OMEN-Laptop-15-en1xxx:~$ sudo cat /etc/shadow
[sudo] Mot de passe de marchal :
root:!:19215:0:99999:7:::
daemon:*:19046:0:99999:7:::
bin:*:19046:0:99999:7:::
sys:*:19046:0:99999:7:::
sync:*:19046:0:99999:7:::
games:*:19046:0:99999:7:::
man:*:19046:0:99999:7:::
```

- 1 : identifiant, 2 : Mot de passe crypté
- 3 : La dernière date de changement de mot de passe
- 4 : Le nombre de jours avant de pouvoir changer son mdp
- 5 : Le nombre de jours avant de forcer un changement de mdp
- 6 : Le jours à partir duquel l'utilisateur est prévenu
- 7 : Nb de jours après un mdp expiré, ou le compte est désactivé
- 8 : Le jour d'expiration du compte

Suivant - Groupe Concept

- Chaque utilisateur possède 1 groupe par default, définie lors de sa création et qui emprunte son nom. (ex : l'utilisateur toto est créé, un groupe toto est créé en même temp)
- Les comptes peuvent appartenir à plusieurs groupes.
- Appartenir à un groupe donne des droits d'accès sur des fichiers, dossiers ou programmes

- Avoir plusieurs groupes permet :
 - + de sécurité
 - + facilement suivre son utilisation (monitorer)
 - Simplifier ces 2 éléments

Suivant - Groupe fichier lié

- Sur linux vous retrouvez un fichier groupe qui recense les groupes et leurs membres:
 - /etc/group
 - /etc/gshadow
- Chaque ligne indique une entrée / un groupe
- Les colonnes sont délimitées par « : »

Suivant - /etc/group

Création, Modification, suppression d'un compte

/etc/group

```
marchal@demo:/etc$ cat group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
```

- 1 : Nom du groupe, 2 : mot de passe
- 3 : GID (pour les utilisateurs normaux > 999)
- 4 : la liste des utilisateurs qui en font partie délimité par une « , »

Suivant - /etc/gshadow

Création, Modification, suppression d'un compte

/etc/gshadow

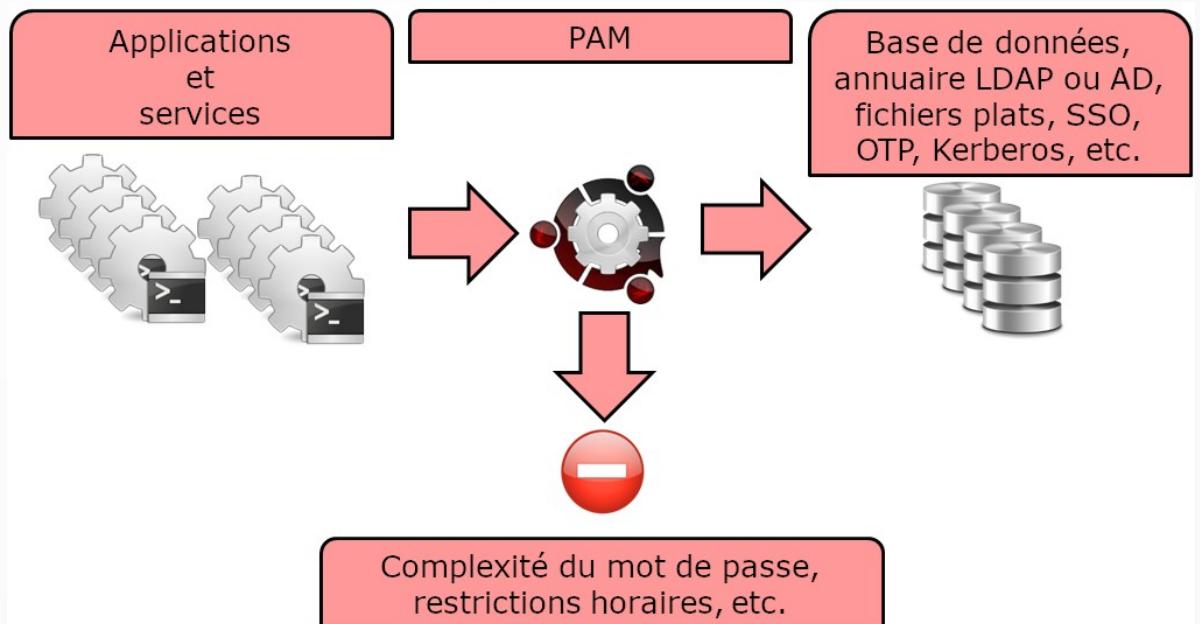
```
cat gshadow: permission non accordée  
marchal@demo:/etc$ sudo cat gshadow  
sudo: impossible de résoudre l'hôte d'  
root:*:::  
daemon:*:::  
bin:*:::  
sys:*:::  
adm:*:::  
tty:*:::
```


Suivant - Les commandes

- addgroup # man addgroup
- adduser # man adduser
- groupmod # man groupmod
- usermod # man usermod
- delgroup # man delgroup
- deluser # man deluser

La sécurité avec PAM - présentation

- Par la suite nous verrons via l'intégration de PAM
- Comment centraliser l'authentification des utilisateurs à des services
- De choisir sa méthode d'authenfication pour un service



Suivant – La personnalisation de l'environnement utilisateur

La personalisation de l'environnement utilisateur

- Chaque utilisateur possède un /home, un répertoire propre à son utilisation.
 - Tout ce qui est lié à la personalisation utilisateur sera toujours localisé dans son /home sous un fichier commençant par un « . »
 - Ces fichiers sont les fichiers de configurations utilisateurs.
 - Ils sont liés aux programmes que l'utilisateur va utiliser.

Suivant – Les permissions

Les permissions

- L'accès aux dossier, fichier etc...
- Est autorisé ou non en fonction de 3 droits:
 - r : read (lecture)
 - w : write (écriture)
 - x : execute (exécuter)
 - - : symbolisant l'absence de la permission
- Par rapport à 3 choses

Le propriétaire, le groupe propriétaire, les autres

```
drwxr-xr-x 1 jeanne jeanne 4096 Mar 25 10:12 dossier
-rw-r--r-- 1 jeanne jeanne      0 Mar 24 18:19 fichier1
groupe:user
```

Sauvegarde et restauration

Les utilitaires de compression : gzip, bzip2, xz, zip

Les commandes cpio, dd

La commande rsync

Les types de sauvegardes : totale, incrémentale, différentielle

Les commandes dump et restore

La procédure pour restaurer la racine

Les utilitaires de compression : gzip, bzip2, xz, zip

- Sur Linux, on utilise la commande tar pour créer des archives au format .tar
- Par défaut, une archive n'est pas compressée.
 - Il faudra utiliser un logiciel de compression (gzip, bzip2 ou xz) pour compresser l'archive, ce qui donnera une archive au format .tar.gz, .tar.bz2 ou .tar.xz.

Suivant - exemple

Les utilitaires de compression : gzip, bzip2, xz, zip

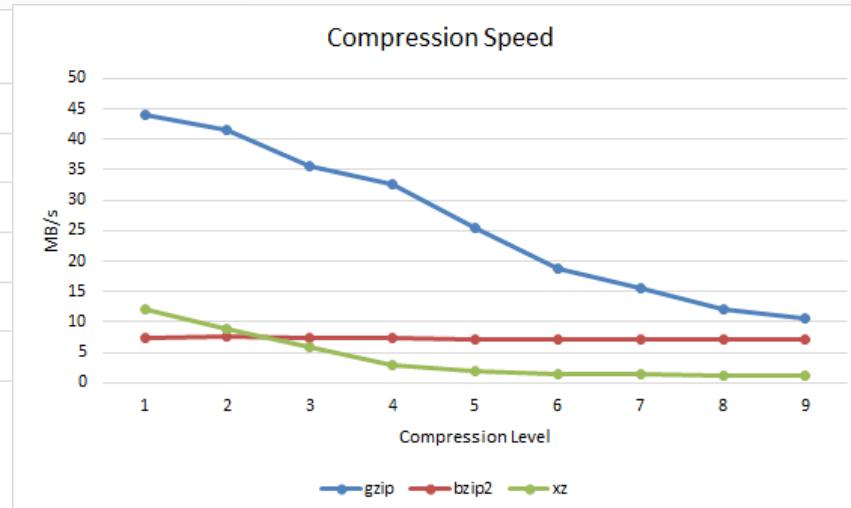
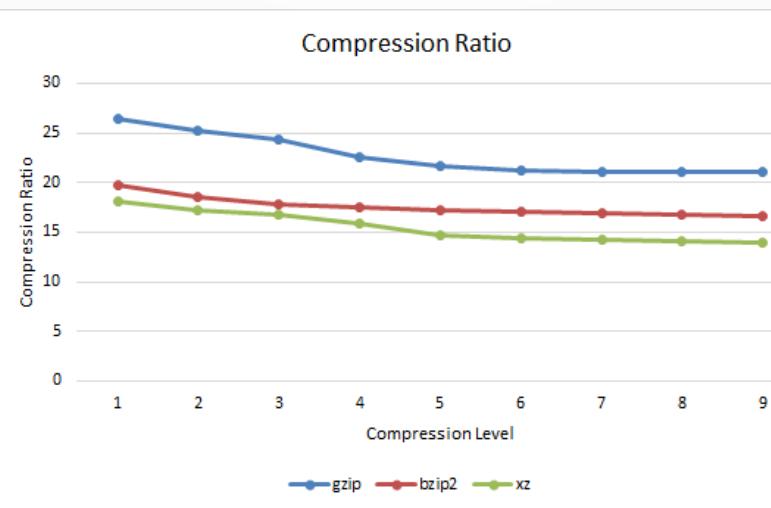
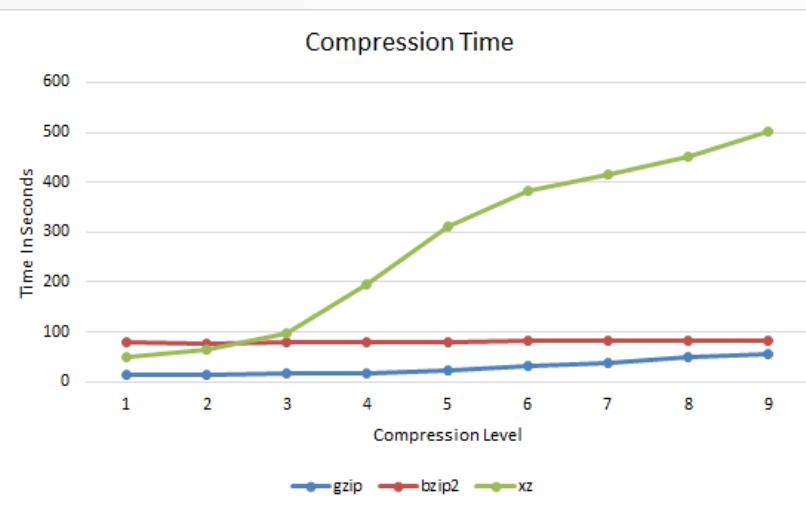
- On souhaite compresser notre répertoire /home/user :
 - D'abord on crée une archive (-c)
 - Ensuite on la compresse avec gzip (-z)
 - On veut pouvoir suivre la progression de l'opération (-v)
 - On veut nommer notre archive (-f)
- Cela donne :
`tar -czvf monArchive.tar.gz /home/userman`

Les utilitaires de compression : gzip, bzip2, xz, zip

- Pour compresser avec gzip : -zc
 - Décompresser : -zx
- Pour compresser avec bzip2: -jc
 - Décompresser : -jx
- Pour compresser avec xz : -Jc
 - Décompresser : -Jx
- Pour compresser avec zip :
 - zip <nomArchive> fichierOuDossier/
- Décompresser :
 - Unzip <nomArchive> destination

Comparaison

- De manière générale, on ne fera pas spécialement attention à la méthode de compression ou décompression.
 - Sous des contraintes de perf/temps/stockage.
 - On sera amené à faire +ou- du benchmark



Comparaison

- zip si les fichiers doivent être partagés avec des systèmes Windows.
- gzip si les fichiers doivent être utilisé sur n'importe quel système Unix/Linux.
- bzip2 utilise un algorithme différent de gzip, prend plus de temps mais fichiers plus petits en général.
- xz offre les meilleurs taux de compression, mais prend beaucoup plus de temps à s'exécuter. Il est plus récent que les autres outils et n'est pas présent sur tous les systèmes.

Les commandes cpio, dd

- cpio permet également de créer des archives à la différence qu'il garde les propriétaires, groupes, dates et droits d'origine.
- cpio récupère les fichiers et dossier qu'on lui envoie en stdout. On l'utilise avec d'autre commande, ex :
 - `find /home/user -name .* | cpio -o | gzip > configUser.cpio.gz`

dd

- dd copie tout ou partie d'un disque.
 - Il copie par blocs.
 - Secteur de démarrage
 - Table de partition
 - Traces laissées sur le disque par des fichiers effacés
 - Il copie même l'espace vide
 - Il copie à l'identique un disque/partition/volume.

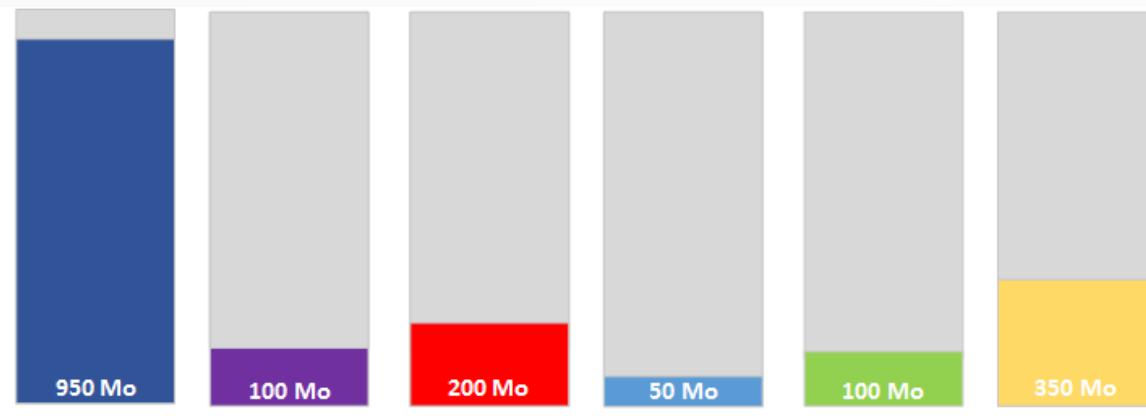
La commande rsync

- rsync (pour remote synchronization ou synchronisation à distance)
 - Est un Programme de synchronisation de fichiers.
 - Il est fréquemment utilisé pour mettre en place des systèmes de sauvegarde distante ou des points de restauration.
 - rsync synchronise, copie ou actualise les données d'une source (locale ou distante) vers une destination (locale ou distante) en ne transférant que les octets des fichiers qui ont été modifiés.

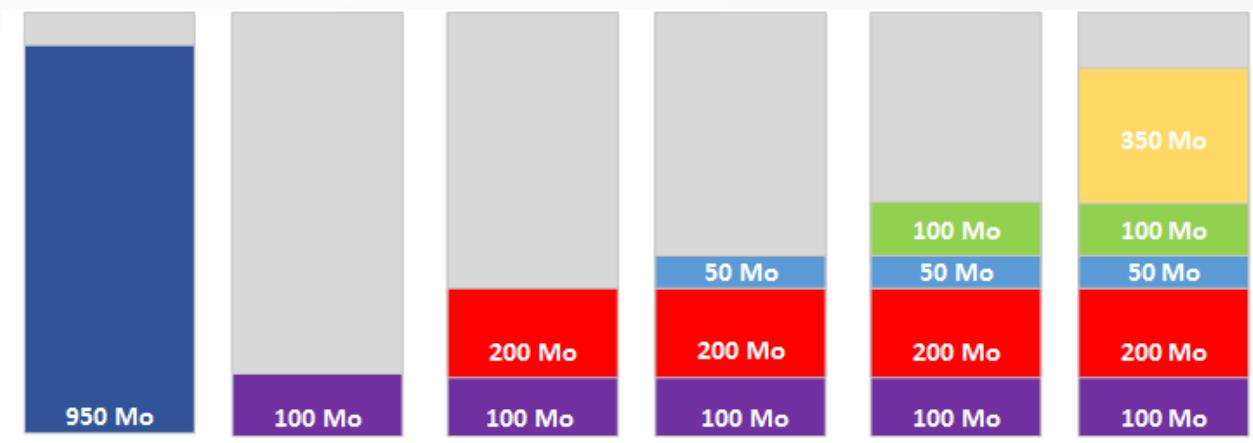
Types de sauvegardes

- Vous retrouverez 3 types de sauvegardes :
 - Totale
 - Sauvegarde complète

Incrémentale

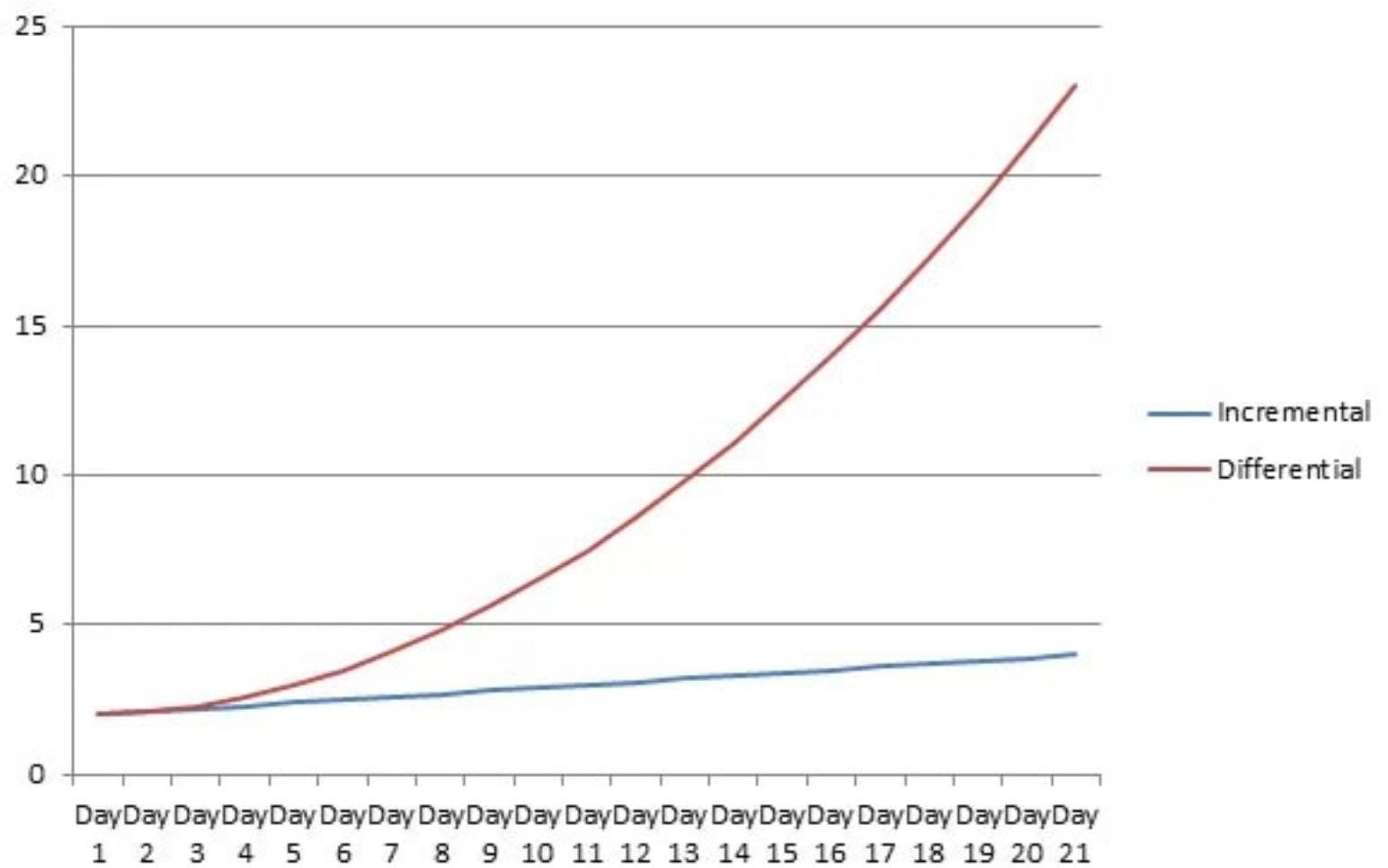


Différencielle



Types de sauvegardes

- Sur 21 jours
- Espace utilisé



Les commandes dump et restore

- dump est un programme complet pour faire des sauvegardes totales et incrémentales.
- restore fonctionne de pair avec dump, permet de restaurer une sauvegarde .dump.

résumé

- Cpio crée une archive compressable qui garde les droits, dates accès. stdin vers stdout (redirection)
- dd copie par blocs d'un input vers un ouput, il copie **TOUS**. Nécessite une destination de la même taille que la source.
- rsync copie une source vers une destination. Sauvegarde distante.
- Dump permet de faire des sauvegardes totales et incrémentales via des .dump file, compressables.
- Restore de restaurer un .dump.
 - Chaque programme dispose d'option (man ...), il existe des surcouches à ces applications qui peuvent simplifier les sauvegardes.

La procédure pour restaurer la racine

- Pour restaurer une racine linux :
 - On doit conserver les mêmes permissions.(idéalement les mêmes dates de création, modification, d'accès)
 - S'assurer que l'emplacement de restauration est assez grand.
 - S'assurer que l'hardware est compatible (architecture).
 - Pas besoin de restaurer le contenu de certains répertoires :
 - /tmp, /var/tmp
 - /run
 - /proc
 - /sys
 - /dev
 - /lost+found

Gestion des processus

Les états d'un processus

Les commandes ps, kill, pkill, pstree, uptime, top

Les jobs

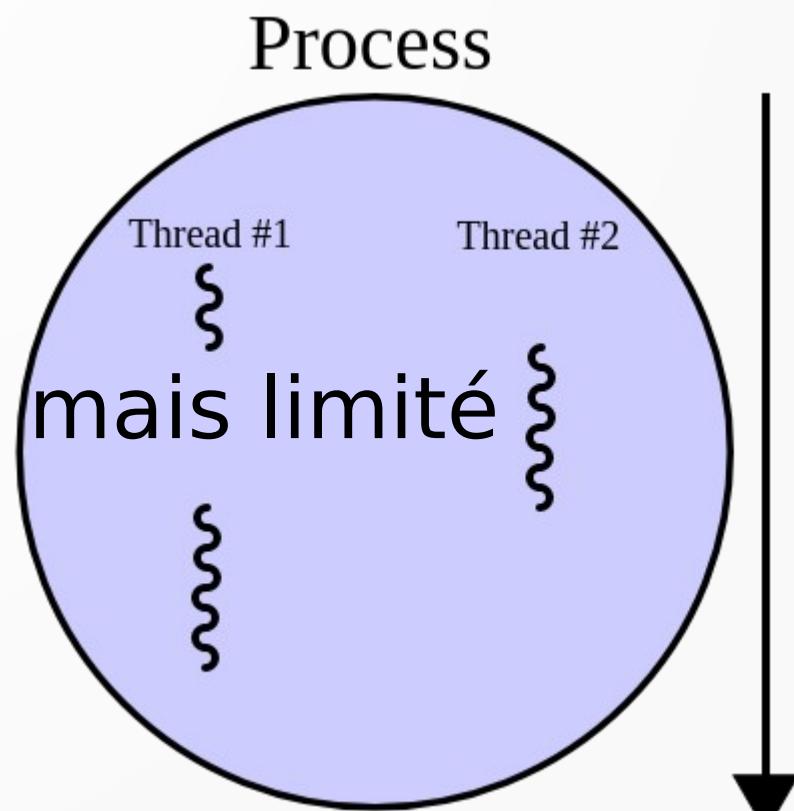
L'exécution différé avec at et crontab

Principe processus

- On appelle processus l'exécution d'un programme.
 - Chaque processus est identifié par un numéro appelé PID (Processus Identifier).
- À chaque processus est également associé :
 - l'identifiant de l'utilisateur par lequel il s'exécute (UID), qui détermine les droits du processus.
 - l'identifiant de son processus parent (PPID).

Processeur

- Un processeur ne peut executer qu'une petite quantité de choses à la fois.
- Par contre il est très rapide.
- Du coup notre système certe rapide mais limité doit s'organiser.



Thread = brique d'un processus.

Suivant - les états d'un processus

Les états d'un processus

- Il y a 9 états possibles pour un processus :

PROCESS STATE CODES

Here are the different values that the s, stat and state output specifiers (header "STAT")

D	uninterruptible sleep (usually IO)
I	Idle kernel thread
R	running or runnable (on run queue)
S	interruptible sleep (waiting for an event to complete)
T	stopped by job control signal
t	stopped by debugger during the tracing
W	paging (not valid since the 2.6.xx kernel)
X	dead (should never be seen)
Z	defunct ("zombie") process, terminated but not reaped by its parent

- man ps

Suivant – Les commandes
liés

Les commandes ps, kill, pgrep, pkill, pstree, uptime, top

- Ps :

- -u : montre tous les processus de l'utilisateur en cours
- -A : Affiche tous les processus en cours

```
marchal@marchal-OMEN-Laptop-15-en1xxx:~$ ps -u
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
marchal	2056	0.0	0.0	166764	6284	tty2	Ssl+	nov.05	0:00	/usr/lib
LL_SESSION_MODE=ubuntu										
marchal	2132	0.0	0.0	190964	12320	tty2	Sl+	nov.05	0:00	/usr/lib
--session=ubuntu										

```
marchal@marchal-OMEN-Laptop-15-en1xxx:~$ ps -A
```

PID	TTY	TIME	CMD
1	?	00:00:14	systemd
2	?	00:00:00	kthreadd
3	?	00:00:00	rcu_gp
4	?	00:00:00	rcu_par_gp
5	?	00:00:00	netns
10	?	00:00:00	mm_percpu_wq

Suivant - kill

Les commandes ps, kill, pgrep, pkill, pstree, uptime, top

- Kill [PID] ou kill [ns] [PID] :
 - envoie un signal à un processus
- Les différents signals : <https://www.cyberciti.biz/faq/unix-kill-command-examples/>
- Pgrep [motClé]:
 - Retourne les processus qui match.
- Pkill [motClé]:
 - Envoie un signal SIGTERM par default au processus qui match

Les commandes ps, kill, pgrep, pkill, pstree, uptime, top

- **Pstree [nom_utilisateur]:**
 - Affiche les processus en cours avec leur lien parent/enfant
- **Uptime**
 - Affiche en une seule ligne les informations :
 - Heure actuelle
 - Combien de temps depuis le démarrage
 - Nombres d'utilisateurs connectés
 - L'utilisation du système pour les dernières 1, 5 et 15 minutes

Les commandes ps, kill, pgrep, pkill, pstree, uptime, top

- Top :
 - Le programme top affiche en temps réel l'utilisation du système

```
top - 23:33:10 up 1 day, 13:18, 1 user, load average: 0,51, 0,33, 0,34
Tâches: 557 total, 2 en cours, 555 en veille, 0 arrêté, 0 zombie
%Cpu(s): 1,1 ut, 0,4 sy, 0,0 ni, 98,3 id, 0,0 wa, 0,0 hi, 0,1 si, 0,0 st
MiB Mem : 15339,2 total, 2484,1 libr, 9472,2 util, 3382,8 tamp/cache
MiB Éch: 2048,0 total, 1733,7 libr, 314,2 util. 4843,1 dispo Mem
```

PID UTIL.	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TEMPS+	COM.
2058 root	20	0	25,8g	206620	88140	S	7,6	1,3	45:11.72	Xorg
2288 marchal	20	0	6134260	307436	101584	S	7,0	2,0	54:20.91	gnome-shell
155621 marchal	20	0	1032804	54244	38548	S	5,6	0,3	0:02.55	gnome-screensho
126073 marchal	20	0	831812	60888	38584	S	1,7	0,4	0:09.14	gnome-terminal-
747 root	-2	0	0	0	0	S	1,0	0,0	6:15.26	gfx
72649 marchal	20	0	49,0g	299464	86340	S	1,0	1,9	44:51.10	Discord
84293 marchal	20	0	33,2g	808216	450604	S	1,0	5,1	15:10.70	chrome
72473 marchal	20	0	36,8g	126280	67164	S	0,7	0,8	2:43.52	Discord
307 root	-51	0	0	0	0	D	0,3	0,0	0:42.66	irq/39-SYNA32A5

Les jobs

- Dans Linux, pour exécuter une commande en arrière-plan, il faut ajouter Ampersand (&) à la fin d'une commande.

`jobs` Lister tous les jobs en cours

`bg %n` Place une tâche actuelle ou spécifiée en arrière-plan, où n est l'identifiant de la tâche

`fg %n` Déplace une tâche actuelle ou spécifiée au premier plan, où n est l'identifiant de la tâche

`kill%n` Tuer une tâche en arrière plan

L'exécution différée avec at et crontab

- Cron est un programme pour exécuter automatiquement des scripts, des commandes à une date et une heure spécifiée précise, ou selon un cycle défini à l'avance.
 - Chaque utilisateur a un fichier crontab, lui permettant d'indiquer les actions à exécuter.
 - Cron est parfois appelé « planificateur de tâches » ou « gestionnaire de tâches planifiées »

L'exécution différé avec at et crontab

- Quelques exemples :
 - 0 5 * * * /scripts/job.sh
 - 0 19 * * fri /scripts/job.sh # "fri" pour Friday (Vendredi)
- Chaque utilisateur à sa propre crontab
 - crontab -l # liste les crontab de l'utilisateur connecté
 - crontab -l -u Utilisateur # liste les crontab de l'utilisateur indiqué (sudo nécessaire)
 - crontab -e # ajouter une tache
- *Ressource : https://crontab.guru/#5_0_*_8_**

L'exécution différé avec at et crontab

- Ex d'un fichier crontab :

```
# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .---- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .--- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | |
# * * * * * user-name command to be executed
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

L'exécution différée avec at et crontab

- at permet de programmer rapidement une tâche à un moment de la journée :
 - Ex : at 09:00
 - at> command
 - Attention at n'affiche pas de retour dans le terminal
 - Pour tester son fonctionnement on utilise la redirection
 - Command > resultat.fichier