
INFRA51 Linux

— day one —

Who I am?

Gaël Prudhomme

Architecte - Consultant Cloud

Coach technique

J'utilise Linux depuis 23 ans

Composition du buffet du jour 1

Introduction

GNU/Linux et les Distrib'

Système de fichiers

ton ami le Shell

Les process

Installation de Linux

Installation de programmes

Un peu d'histoire

1970: Crédit du système Unix chez AT&T.

1973: Naissance de BSD (Berkeley Software Distribution)

1983: Début de l'initiative GNU (gcc) puis OS GNU/Horde 1990

1991: Un étudiant de l'université de l'Helsinki démarre le développement du noyau Linux

1993: Sortie des distributions Debian et Slackware

Les personnalités autour Linux



Linus Torvalds

⇒ Etudiant à l'initiative du Noyau Linux

⇒ Mainteneur principal du Noyau Linux

torvalds@kernel.org

Les personnalités autour Linux



Richard Stallman (rms)

⇒ Initiative GNU

⇒ Développeur de Gcc, GNU make et GNU emacs

⇒ Président de la Free Software Foundation

Richard Stallman (Chief GNUisance)

<rms@gnu.org>

L'ecosystème autour de GNU/Linux

Les Foundations: Promouvoir et soutenir des logiciels libres (Apache, Linux Foundation, Open Cloud Fondation)

Les éditeurs: Assure un support autour des logiciels libres

Les communautés: Développement et maintien des logiciels et des distributions

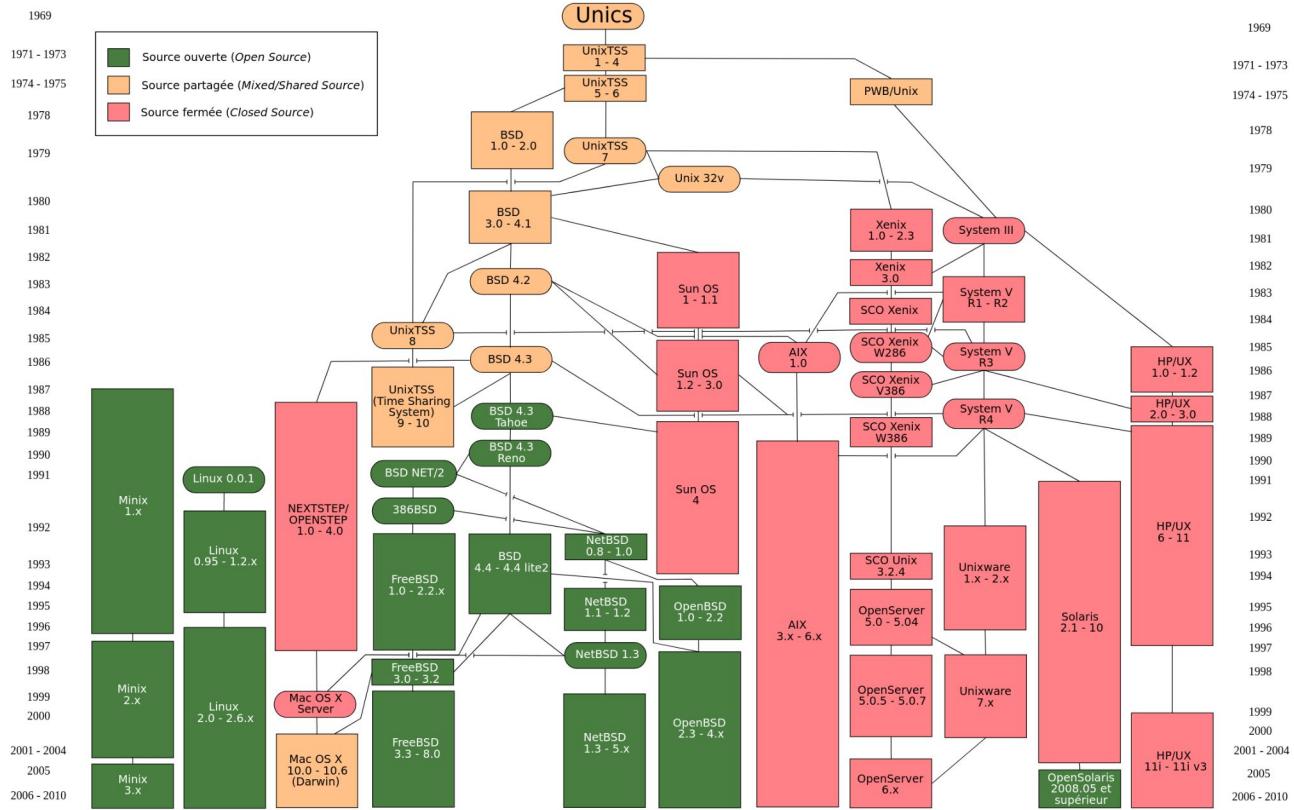
L'industrie: Principaux utilisateurs des logiciels

GNU

Gnu is Not Unix

Projet GNU : Suite d'outils servant au développement d'autre logiciel GNU

GNU GPL : GNU General Public Licence (Liberté d'utiliser, re-distribuer, adapter et obligation de partager les modifications)



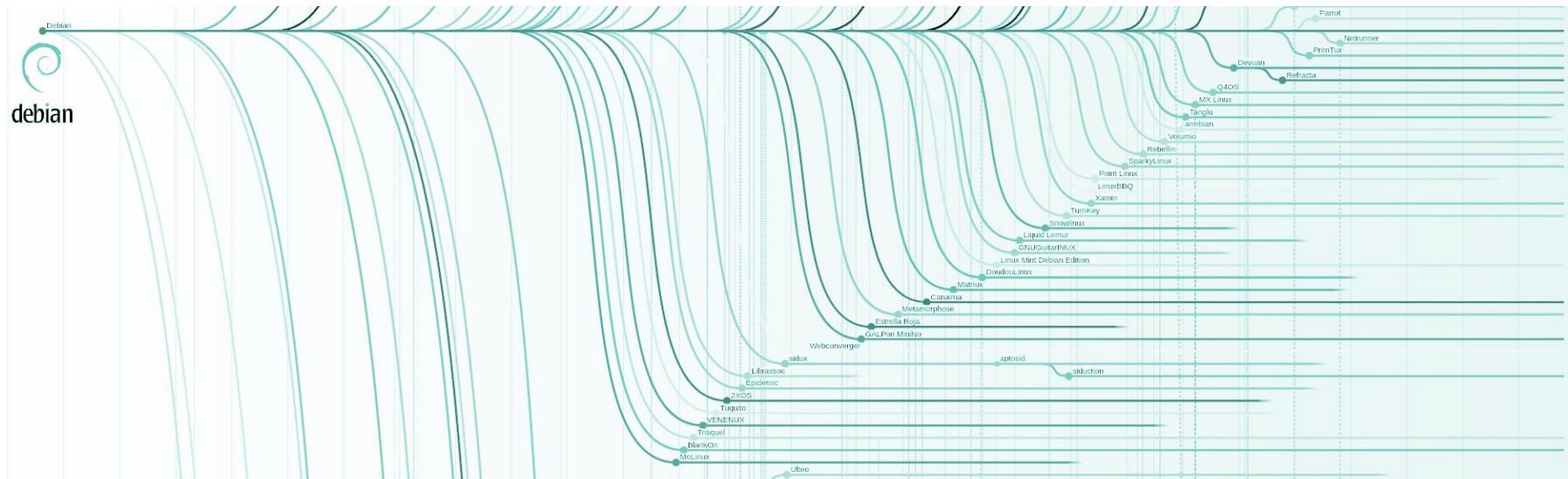
Unix/Linux/Minix/BSD

Et Maintenant !

Où trouve-t-on Linux ?

- SuperOrdinateur
- Internets (Serveurs équipements réseaux etc...)
- Dans vos téléphones & montres
- Dans l'embarqué (TV, Raspberry etc...)

Les distributions GNU/Linux



C'est quoi une distribution Linux?

Définition Wikipédia:

C'est un ensemble cohérent de logiciels assemblés autour du noyau Linux

Les distributions rassemblent les composants d'un système dans un ensemble cohérent et stable dont l'installation, l'utilisation et la maintenance sont facilitées. Elles comprennent donc le plus souvent un logiciel d'installation et des outils de configuration.

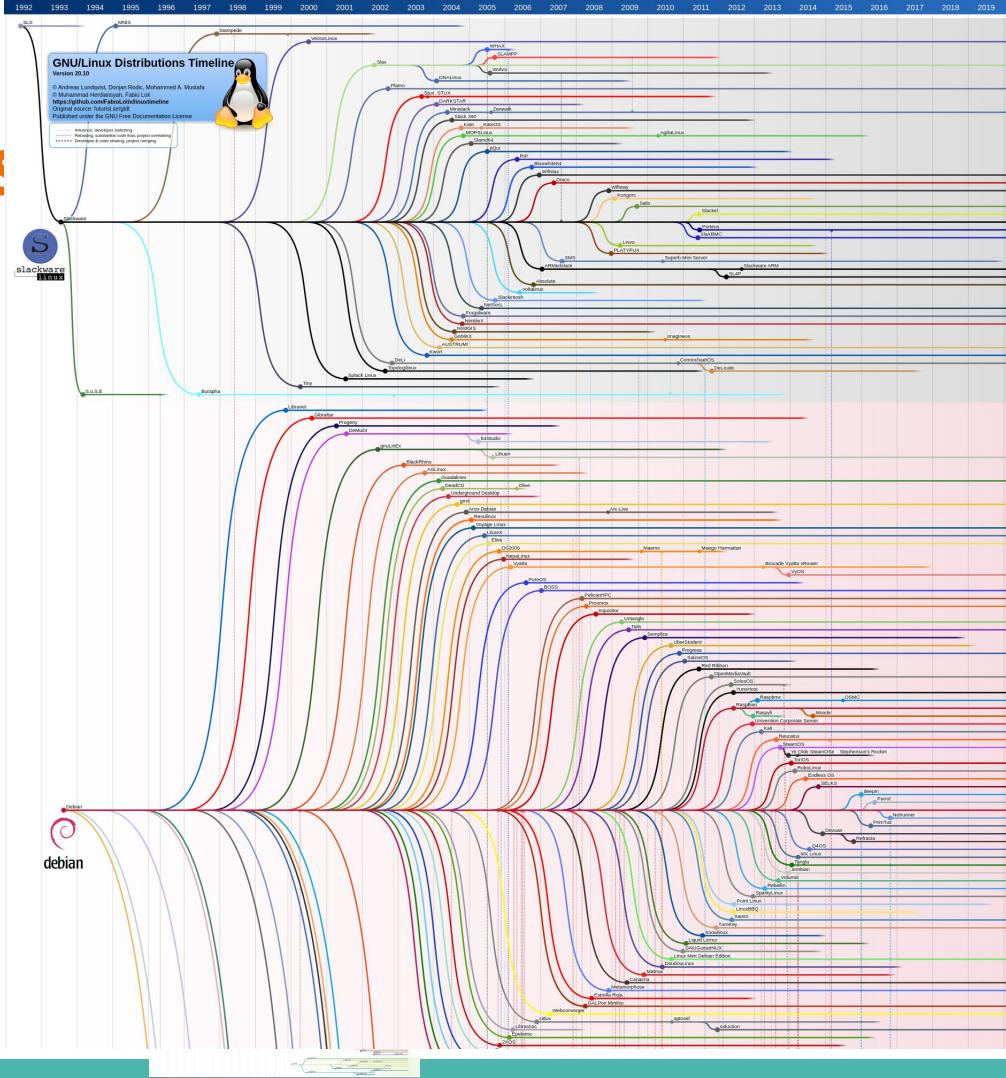
- Les généralistes: Debian, Ubuntu, Slackware, OpenSUSE, Gentoo, ArchLinux
- Les orientées entreprise :RedHat, SUSE Linux Entreprise
- Les spécifiques: PFsense, Raspbian, CoreOs, Amazon Linux etc...

Distribution

(par ex. Debian, Redhat, Mandriva, SuSE)



C'est quoi ta distro ?



Les plus présentes en entreprise



redhat®



CentOS



debian



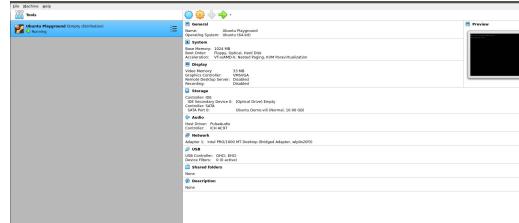
ubuntu®

Mon premier démarrage



Lancement de la box

Installation de la Box



Connection en ssh (putty)

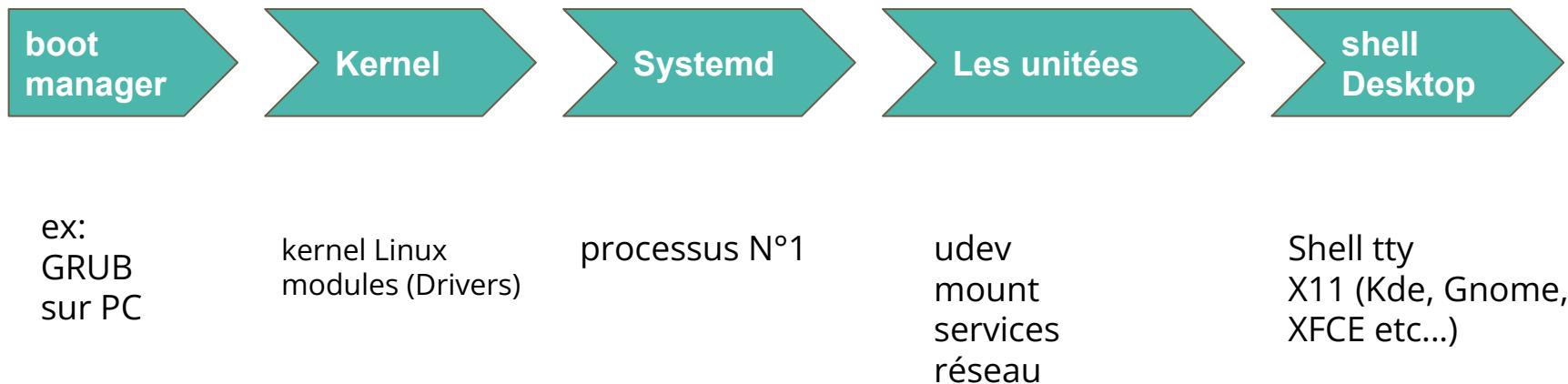
login: player

password: player

```
Ubuntu 20.04.3 LTS ubuntu-playground-1 tty2
ubuntu-playground-1 login: player
Password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

Tu peux t'y connecter via l'adresse ip 10.9.8.40
Tentes un truc du style ssh player@10.9.8.40
Last login: Wed Dec  1 20:16:57 CET 2021 from 10.9.8.105 on pts/0
> -                                         20:38:45
```

La séquence de démarrage



Exploration du démarrage

```
# dmesg
```

```
$ journalctl -k
```

Fichiers et systèmes de fichiers

file and file system



Les fichiers

```
drwxrwxr-x  
drwxr-xr-x  
-rwxrwxr-x  
-rw-rw-r--  
drwxrwxr-x
```

```
3 player player  
5 player player  
1 player player  
1 player player  
2 player player
```

```
4096 Dec 1 21:06 .  
4096 Dec 1 21:07 ..  
33 Dec 1 21:06 script.sh  
0 Dec 1 21:04 titi  
4096 Dec 1 21:01 tp1
```

rwXr-Xr--

droits du propriétaire (u)
droits des utilisateurs appartenant au groupe (g)
droits des autres utilisateurs (o)

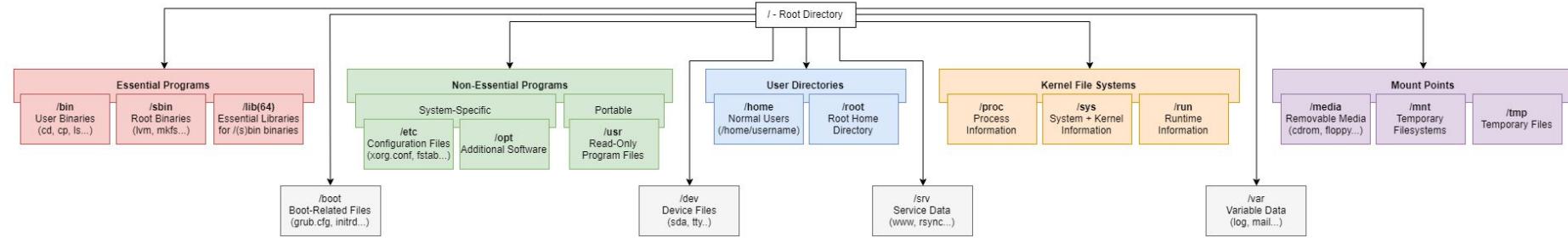
nb lien sur le fichier
propriétaire
groupe propriétaire

taille
date de modification
heure de modification
nom du fichiers

Sous Linux, TOUT est fichier !

/	Root (la racine)	/usr	programmes utilisateur
/dev	Devices (périphériques)	/var	Element sys variable
/boot	Démarrage	/opt	Programmes tiers
/root	Dossier de l'utilisateur root	/sbin	Commandes root
/home	Dossier des utilisateurs	/bin	Commandes utilisateurs
/proc	Informations système	/mnt	Point de montage

The Filesystem Hierarchy Standard (FHS)



Essential Programs:

Directories containing files needed to run essential programs

- **/bin** - Essential binaries such as 'cp' or 'ls' that all users have access to
- **/sbin** - Essential binaries only available to the root user
- **/lib(64)** - Libraries needed for essential binaries in (/sbin)

Non-Essential Programs (Secondary Hierarchy):

Directories containing files needed to run non-essential programs

- **/etc** - System-specific configuration files for programs in /usr and /opt
- **/opt** - Additional programs not found in distribution repositories
- **/usr** - Portable, read-only, non-essential programs and program files

User Directories:

Directories containing user-specific files

- **/home/(username)** - User files, configuration, and programs
- **/root** - Home directory for the root user

Mount Points:

Directories used for mounting devices and file systems

- **/media** - Removable media such as CD-ROMs and floppy drives
- **/mnt** - Temporary file systems such as USB drives
- **/tmp** - Pseudo-filesystem for temporary files. Cleared by the kernel on boot

Other directories:

- **/boot** - Files essential for booting the system such as initrd, kernel, and bootloader configuration
- **/dev** - Device files for physical devices such as HDDs as well as data streams (stdin, stdout...)
- **/srv** - Files used for services offered by the system such as www, rsync, and ftp
- **/var** - Variable (changing) files such as lock files, logs, and mail

Chemins absolu vs chemin relatif

• : Dossier courant

Chemin absolu

- '/proc/sys/net/ipv4/ip_forwarding'
- '~player/.ssh/'

•• : Dossier parent

~ : Dossier de l'utilisateur (Home directory)

Chemin relatif

- `../../../../dev/.../root/.../usr/lib/share/.../X11`

/ : Dossier Racine (Début des chemins absolus)

Systèmes de Fichiers (FileSystem)

Format des stockages des informations sur les unités de stockage physique

- Beaucoup de FS sont disponibles sous Linux
- Compatibilité avec d'autres OS
- Choix structurant
- Choisir en fonction des critères

Critères de sélection

- Maturité
- Compatibilité
- Limitations
- Fonctionnalités
- Est-il utilisé

Les différents systèmes de fichiers

NOM	Maturité	Compatibilité OS	Limitations	Fonctionnalités	Utiliser!
ext4	stable depuis 2008	Linux	FileSize < 16TB 1024PB (1eiB)	Compatible ext2-3 Journalisé, Quota	<input checked="" type="checkbox"/>
btrfs	stable depuis 2013	Linux	FileSize < 16EiB 16eiB	Journalisé, Quota Snapshot, Sub volume RAID, COW, Compression	<input checked="" type="checkbox"/>
NTFS	pas dans le kernel	Windows	NOT Posix	Windows NTFS compatible	<input type="checkbox"/>
VFAT(32)	2001	Windows, MS-DOS, Linux	NOT Posix	Compatible avec 'presque' tout les OS	<input type="checkbox"/>
ISO 9660	1993	Tous	lecteur seul	Fait pour le CD-ROM	<input type="checkbox"/>

Ton ami le shell

```
  android-sdk.com  
  license.html  
  Generating source files with sha1sums...  
ools-linux-4333796.zip ... Passed  
id-sdk.sh ... Passed  
id-sdk.csh ... Passed  
id ... ad
```

```
51208 saikiran  
22651 saikiran  
902 saikiran  
472 root  
21853 saikiran  
380 root  
1 root  
251 root  
568 root  
saikiran
```

Interfaces Homme Machines

- Interpréteur de commande
- Environnement de travail & outils de programmation
- csh, sh, bash, zsh , fish etc.... à chacun son shell

Prompt me

Prompt chemin/command arguments



```
prudprud@gael-laptop:~$ /usr/local/bin/glances --help
usage: glances [-h] [-V] [-d] [-C CONF_FILE] [--modules-list] [--disable-plugin DISABLE_PLUGIN] [--en
                 [-1] [-2] [-3] [-4] [-5] [-6] [--disable-history] [--disable-bold] [--disable-bg] [--e
                 [--sort-processes {cpu_percent,memory_percent,username,cpu_times,io_counters,name}] [-
                 [--export-json-file EXPORT_JSON_FILE] [--export-graph-path EXPORT_GRAPH_PATH] [-c CLIE
```

Les différents type de commandes:

```
prudprud@gael-laptop:~$ type -t type
builtin
prudprud@gael-laptop:~$ type -t glances
file
prudprud@gael-laptop:~$ type -t if
keyword
prudprud@gael-laptop:~$ type -t ls
alias
```

Les processus

Processus, fork, thread, child explication...

Un processus linux est caractérisé par :

- Un PID (**P**rocess **I**Dentifier)
- Un Parent (sauf pour le PID 1)
- Un Etat
- Un utilisateur

Un processus peut avoir :

- Des enfants (child)
- Des enfants clones (fork)
- Des sous taches (thread)

Les processus

ps auxf									
USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME COMMAND
syslog	364	0.0	0.4	224348	4808	?	Ssl	20:16	0:00 /usr/sbin/rsyslogd -n -iNONE
root	365	0.0	0.7	16696	7816	?	Ss	20:16	0:00 /lib/systemd/systemd-logind
root	388	0.0	0.6	12176	6760	?	Ss	20:16	0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root	443	0.0	0.9	13924	9096	?	Ss	20:16	0:00 _ sshd: player [priv]
player	476	0.0	0.5	14056	5928	?	S	20:16	0:00 _ sshd: player@pts/0
player	477	0.1	0.9	18668	9884	pts/0	Ss	20:16	0:06 _ zsh
player	1547	0.0	0.3	11644	3324	pts/0	R+	21:22	0:00 _ ps auxf
player	456	0.0	0.9	18272	9092	?	Ss	20:16	0:00 /lib/systemd/systemd --user
player	457	0.0	0.2	168276	2944	?	S	20:16	0:00 _ (sd-pam)
player	482	0.0	0.4	13404	4068	pts/0	S	20:16	0:00 -zsh
player	512	0.0	0.1	2568	1160	pts/0	Sl	20:16	0:00 _ /home/player/.cache/gitstatus/gitstatusd-linux-x86_64 -G
player	509	0.0	0.4	14544	4260	pts/0	S	20:16	0:00 -zsh
player	510	0.0	0.3	14528	3116	pts/0	S	20:16	0:00 -zsh
root	925	0.0	0.3	5988	3864	tty2	Ss	20:38	0:00 /bin/login -p --
player	954	0.0	0.9	18048	9056	tty2	S+	20:38	0:00 _ -zsh
player	994	0.0	0.5	14668	5124	tty2	S	20:38	0:00 -zsh
player	1002	0.0	0.0	2568	4	tty2	Sl	20:38	0:00 _ /home/player/.cache/gitstatus/gitstatusd-linux-x86_64 -G
player	995	0.0	0.4	14444	4324	tty2	S	20:38	0:00 -zsh
player	998	0.0	0.2	14428	2960	tty2	S	20:38	0:00 -zsh
root	1006	0.0	0.1	8428	1824	tty1	Ss+	20:39	0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux

Les signaux, “Hé! Toi le processus !!”

On peut envoyer un signal à processus

commande d'envoie de signal : **kill**

NOM	Valeur	Description
SIGKILL	9	Arrête le processus brutalement
SIGTERM	15	demande à processus de s'arrêter
SIGHUP	1	Message de rechargement de configuration

Les processus

```
top - 21:33:43 up 1:17, 2 users, load average: 0.00, 0.00, 0.00
Tasks: 88 total, 1 running, 87 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 981.2 total, 628.4 free, 97.4 used, 255.5 buff/cache
MiB Swap: 980.0 total, 980.0 free, 0.0 used. 745.4 avail Mem
```

Les utilisateurs et les groupes

un user sous linux

```
$ cat /etc/passwd
```

- Définit par un ID
- un login
- un nom complet
- Appartient à minimum à un groupe
- Possède un Home Directory (~)
- Possède un Shell

Voici mon /etc/passwd !

```
> 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
```

root: le super utilisateur

- id et gid: **0**
- A tout les droits
- Ne doit pas être utilisé !!

Les types d'utilisateurs (par convention)

utilisateur standard:

- shell
- ouvrir une session

- Ne peut ouvrir de session
- dédié aux daemons(service)

INFRA51 Linux

— Day two! —

Composition du buffet du jour 2

Installation d'un palntroduction

GNU/Linux et les Distrib'

Système de fichiers

ton ami le Shell

Les process

Installation de Linux

Installation de programmes

TP Day 2

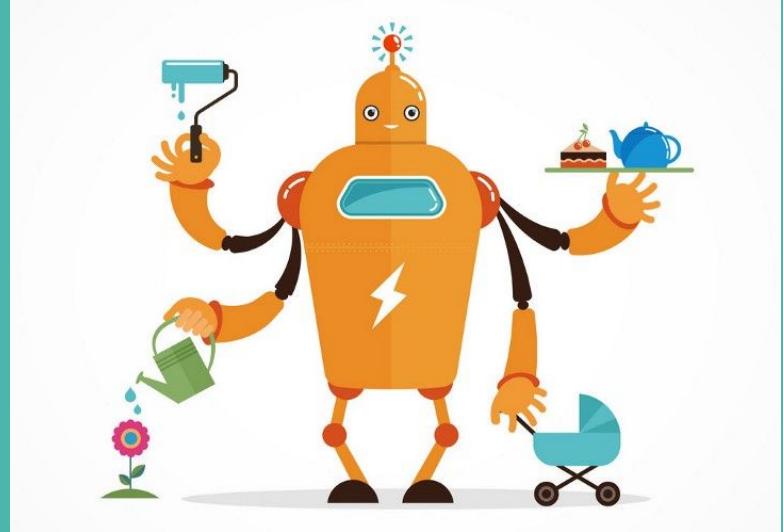
Install from Scratch

Installation from scratch

<https://github.com/minetest/minetest/tree/master>

systemd

avant il y avait SysV



systemd

- Trousse à outils: 70 binaires
- Rôle central d'un système Unix
- Est dans la majorité des distributions Linux

Multi rôles:

- Gestion des services
- Gestion des logs
- Gestion des tâches planifiés
- Configuration du serveur.

systemctl

Rechargement de la configuration des services

```
# systemctl daemon-reload
```

Activation/désactivation service au démarrage

```
# systemctl enable/disable <myservice>
```

Arret et demarrage d'un service

```
# systemctl stop/start <myservice>
```

systemctl

```
sudo vi /etc/systemd/system/minetest-server.service
```

```
[Unit]
Description=Minetest Server

[Service]
ExecStart=/home/gael/minetest/bin/minetest --server
User=gael

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

INFRA51 Linux

— Last day! —

Le réseau

ping localhost...not alive



Distribution spécifique

- Les Network Managers
- Focus Systemd

```
networkctl list  
networkctl status
```

/etc/systemd/network/enp0s3-ethernet.network.

```
[Match]  
Name=enp0s3  
[Network]  
DHCP=ipv4
```

```
[Match]  
Name=enp0s3  
[Network]  
Address=192.168.21.240/24  
Gateway=192.168.21.254  
DNS=1.1.1.1
```

La base: `ip`

- Ajout d'une adresse IP sur l'interface enp0s25

```
sudo ip addr add 10.102.66.200/24 dev enp0s25
```

- Ajout de la route par défaut

```
sudo ip route add default via 10.102.66.1
```

- Affichage des routes

```
ip route show
default via 10.102.66.1 dev eth0 proto dhcp src 10.102.66.200 metric 100
```

Diagnostic réseau

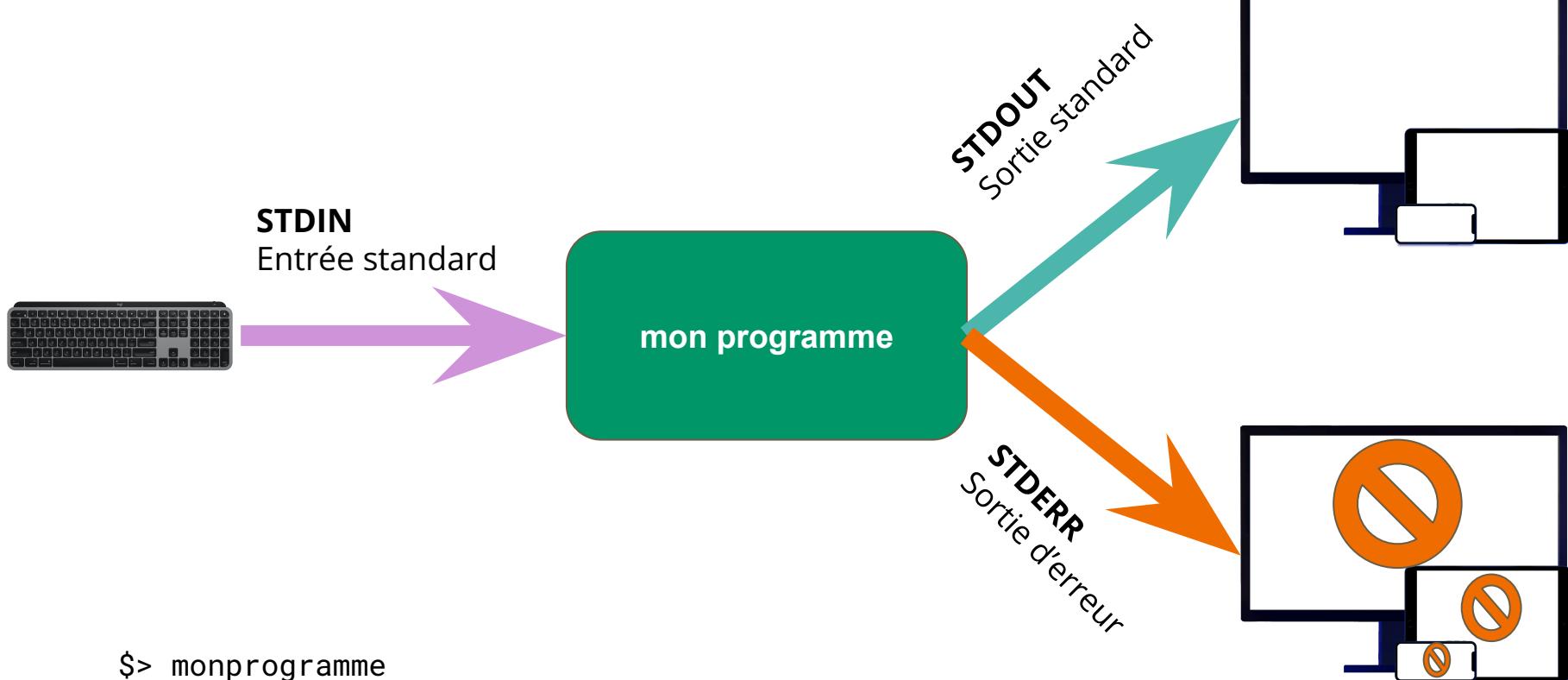
- ping
- traceroute
- tcpdump
- iperf

Les streams

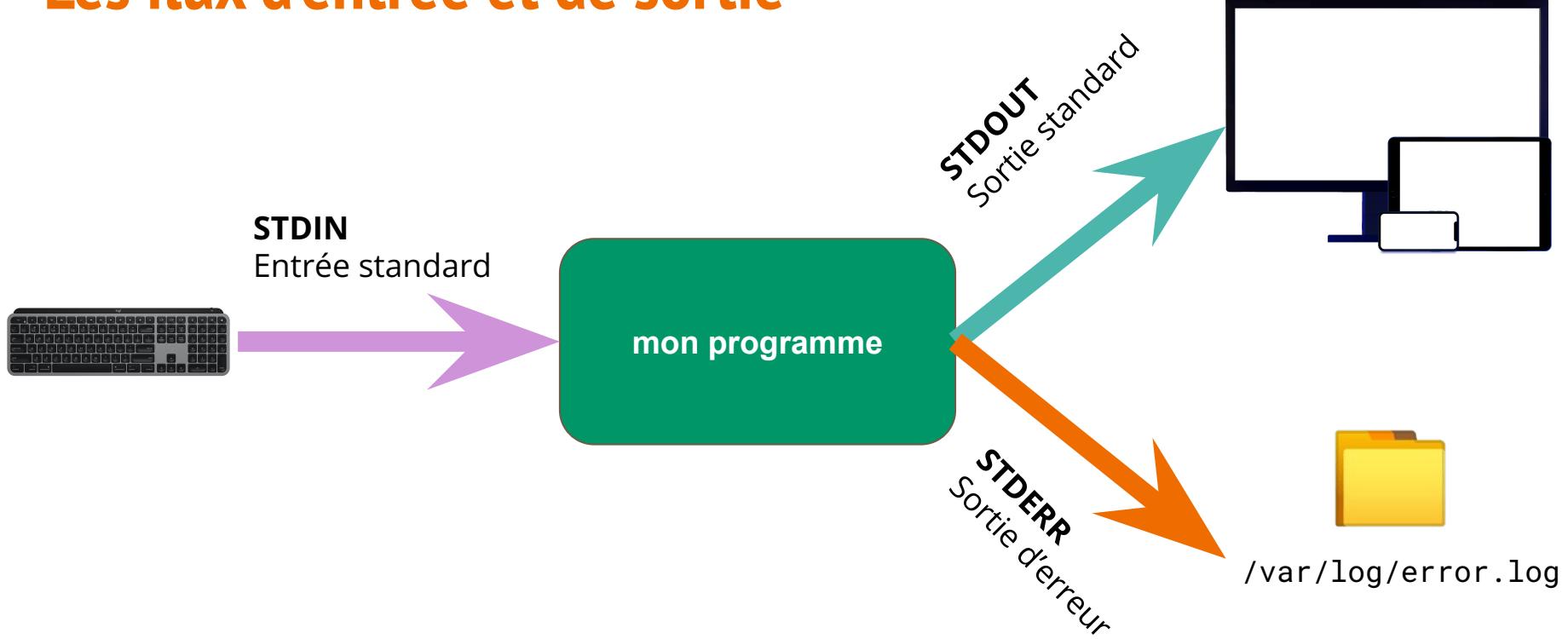
<> 2>&> |
Mais c'est quoi tout ça ?



Les flux d'entrée et de sortie



Les flux d'entrée et de sortie

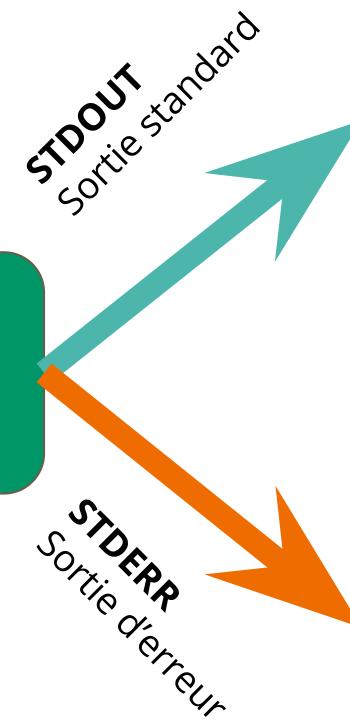
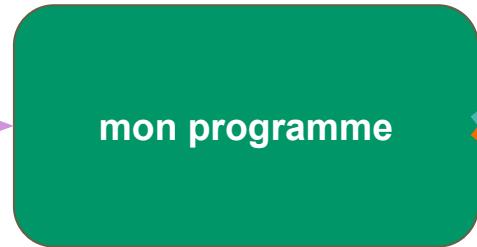


```
$> monprogramme 2> /var/log/error.log
```

Les flux d'entrée et de sortie



/var/log/monprogramme.log



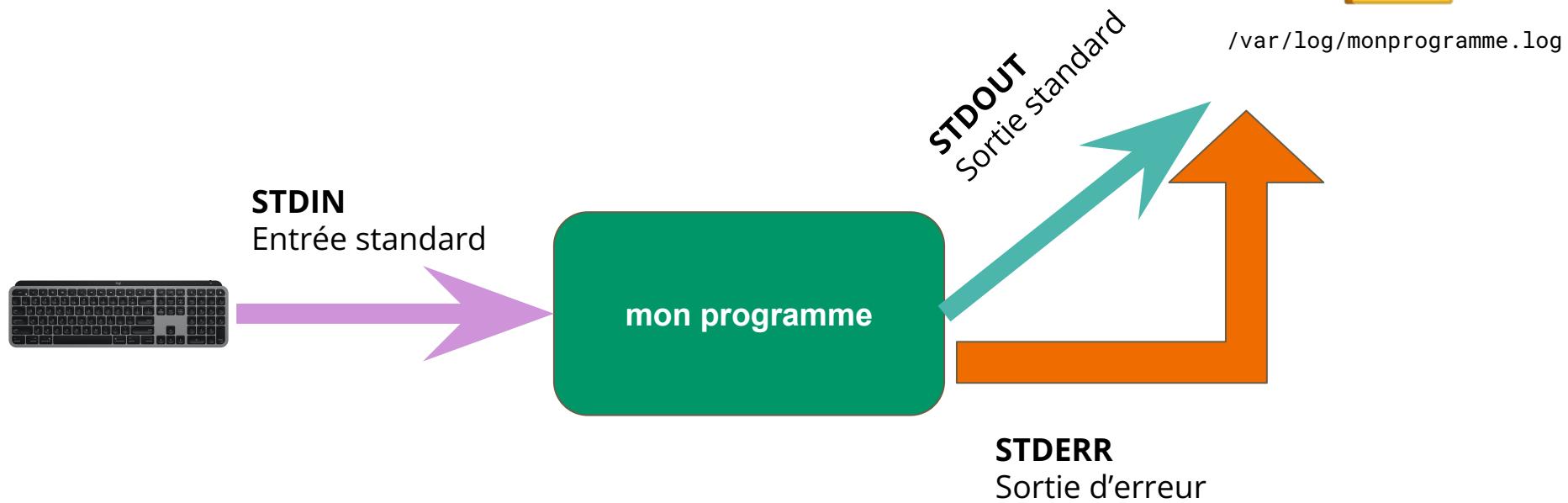
/var/log/error.log

```
$> monprogramme > /var/log/monprogramme.log 2> /var/log/error.log
```

Les flux d'entrée et de sortie

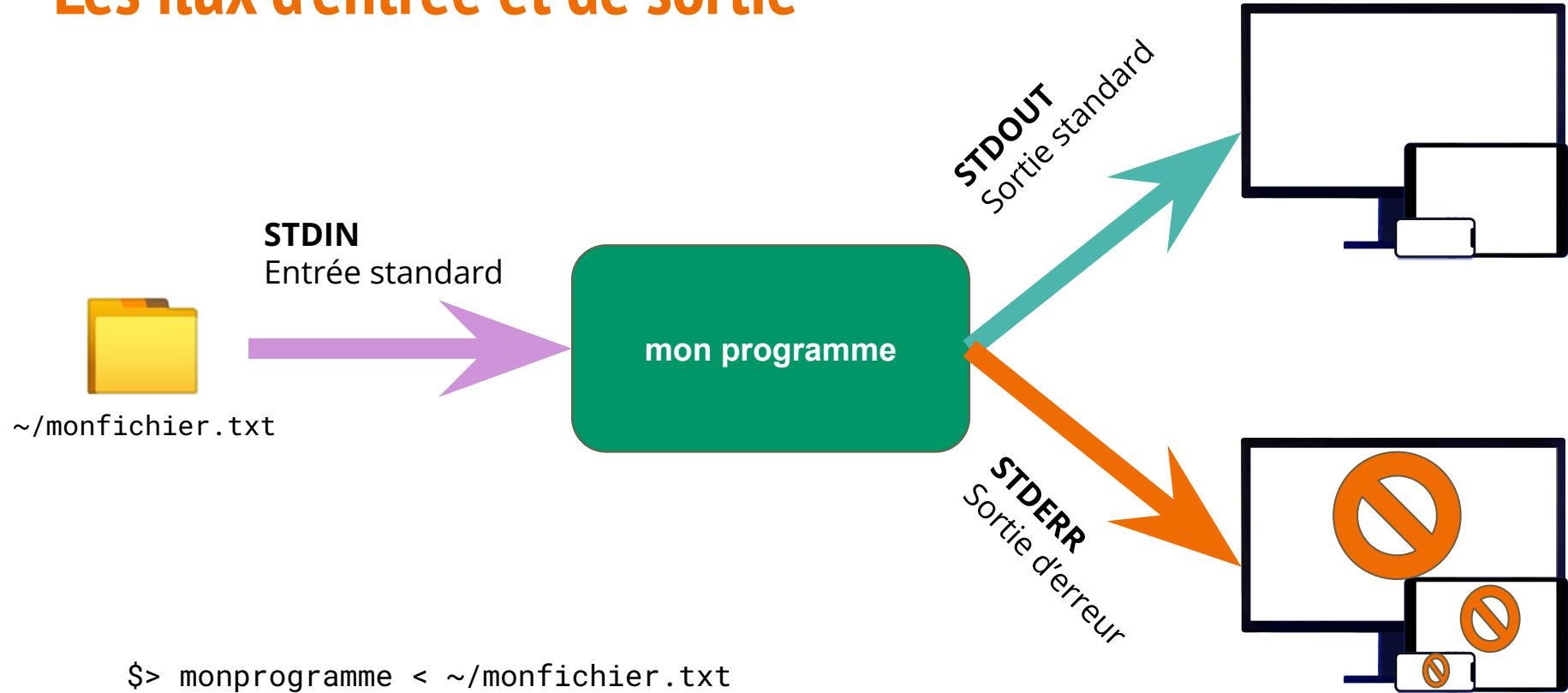


/var/log/monprogramme.log

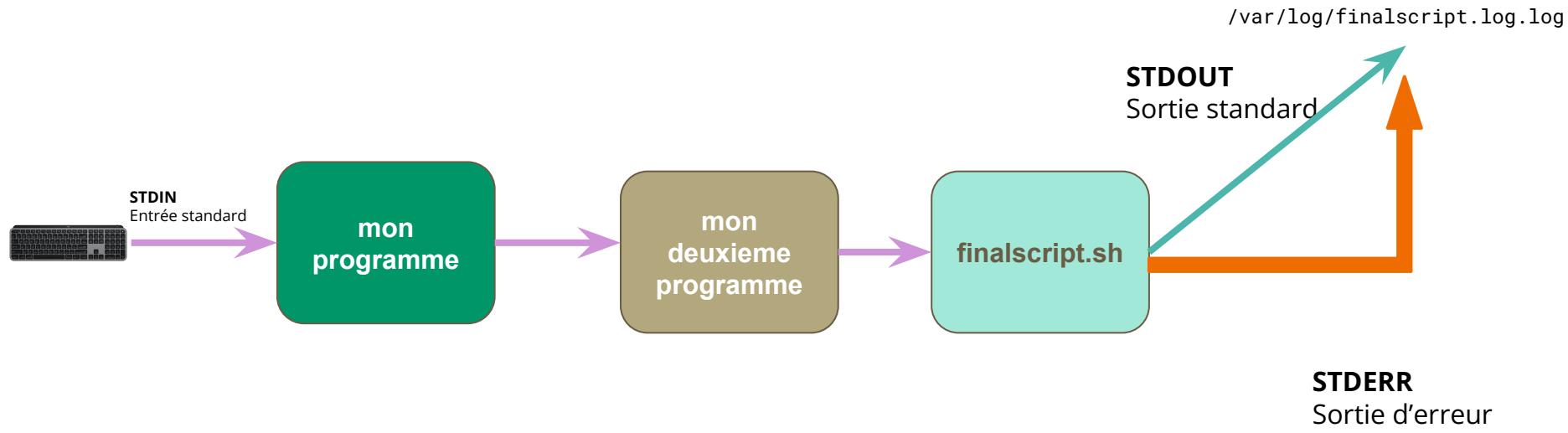


```
$> monprogramme > /var/log/monprogramme.log 2>&1
```

Les flux d'entrée et de sortie



Les flux d'entrée et de sortie



```
$> monprogramme | mondeuxiemeprogramme | ./finalscript.sh > /var/log/finalscript.log 2>&1
```

Manipulation de fichiers texte

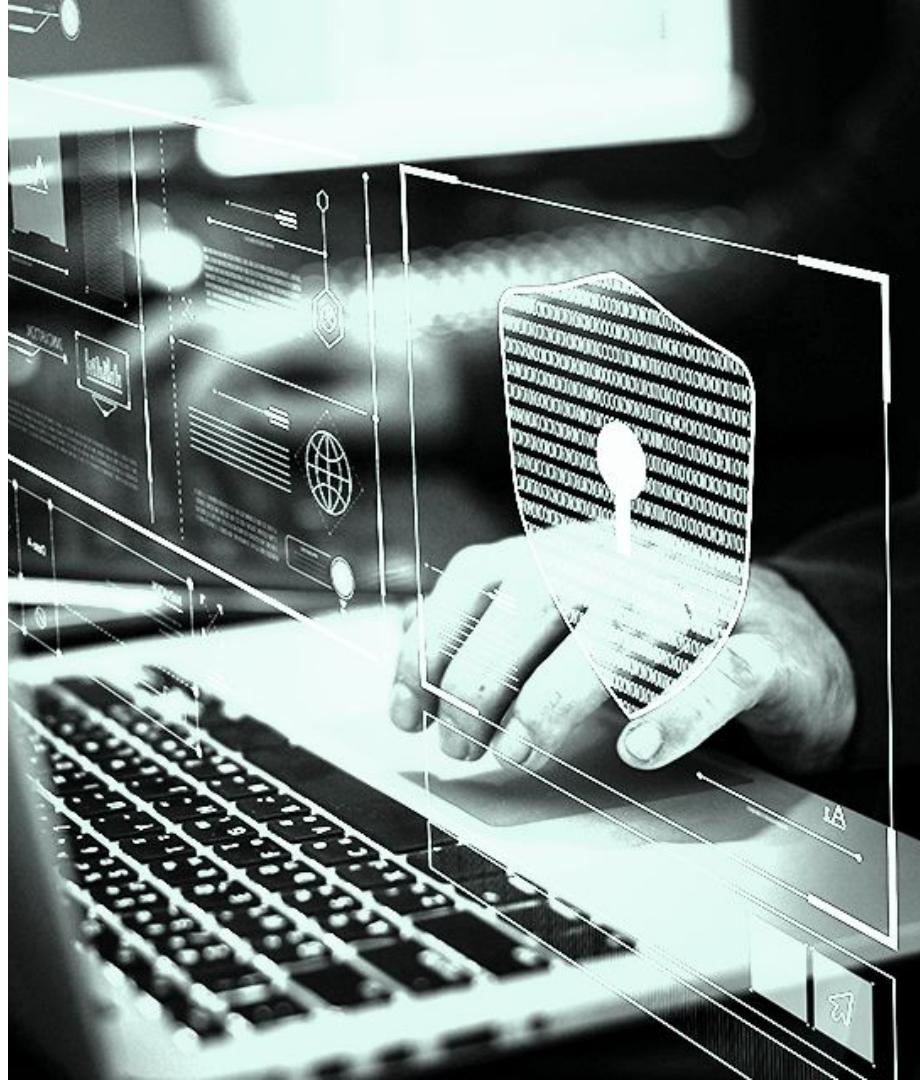
grep | sort | uniq | wc

Les commandes

- grep: recherche de motif de chaîne de caractères
- wc: Comptage du nombre de lignes, caractère et mot
- cut: extraire des champs dans une ligne
- sort: trie
- find: Recherche de fichiers

Securite sous linux

c'est comme ailleurs
le risque 0 n'existe pas



Vecteur physique

Vol de Pc

- Chiffrement des disques
 - dm-crypt
- Authentification forte en local
 - Clef physique
 - Biometrie
- Protection physique
 - Biometrie
 - surveillance
 - Clef/Verrou

Intrusion en Datacenter ou salle serveur

Vecteur OS - Logiciel bas niveau

Escalade de priviléges

- Maintenir ses OS et dépendances à jour
 - apt update
 - N'oubliez pas la couche de virtualisation

Faille dans les couches basses

- Aucune application en root !!!!
- Désactiver l'accès au kernel
 - /boot dans une partition séparée
 - Chiffrer la partition....
- Antivirus et Rootkit
 - Scanner votre parc souvent

Vecteur Applicatifs

Escalade de priviléges

Utilisation malveillance des ressources

- Isoler vos applications par User
 - 1 user = 1 application
- Mettre en place selinux
 - Trop souvent pas configuré car trop complexe malheureusement.
- Containeriser vos applications.
- Protéger correctement les fichiers contenant des credentials.
- Mettez à jour vos logiciels et dépendances
- N'ayez JAMAIS confiance dans un logiciel tiers

Vecteur Réseaux

Escalade de priviléges

Utilisation malveillance des ressources

- Mettez en place un pare feu
 - Netfiler avec iptables ou ufw
- Mettre en place selinux
 - Contrôle aussi les ouvertures de port
- Ne pas 'binder' sur toutes les cartes reseaux
 - Pas de bind sur l'ip : 0.0.0.0
- Si aucun accès externe, utiliser localhost /dev/lo
- si possible, changer les ports par défaut
- Automatiser la réponse securite
 - fail2ban
 - log, SIEM

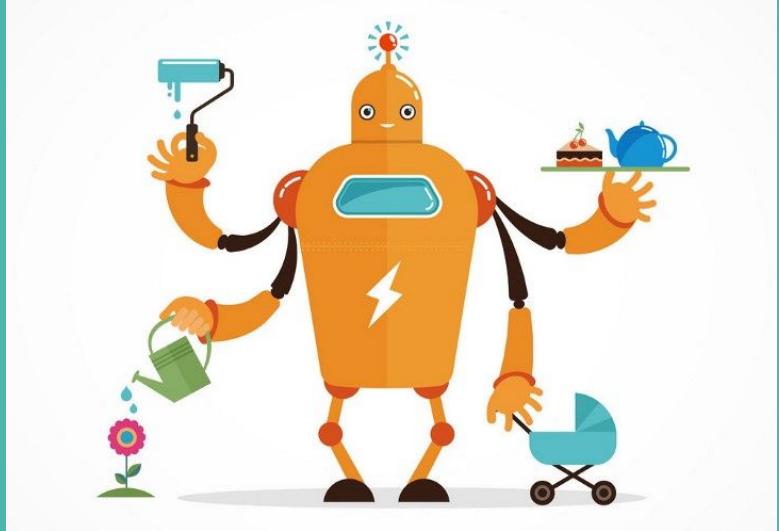
Vecteur Utilisateurs

Escalade de privilèges

Utilisation malveillance des ressources

- Authentification forte
 - PAM est ton ami
- Chiffrer les dossiers home
- Déléguer l'authentification
- Rotation des mots de passe
- Former les utilisateurs

Final Script



Final Script

Script de backup

Le script doit:

- Faire une copie des fichiers dans un dossier et compresser ce dossier qui doit avoir la date
- Avoir un fichier de log contenant la liste des fichiers sauvegardés et le nom et la taille de l'archive
- Avoir un fichier de logs d'erreur

```
archiveFiles <nom-du-dossier_destination> <nom-du-dossier_a_sauvegarder> <type de fichier>
```

```
archiveFiles /var/backup /usr *.h
```

Extra: semver

Semantic Versioning 2.0.0

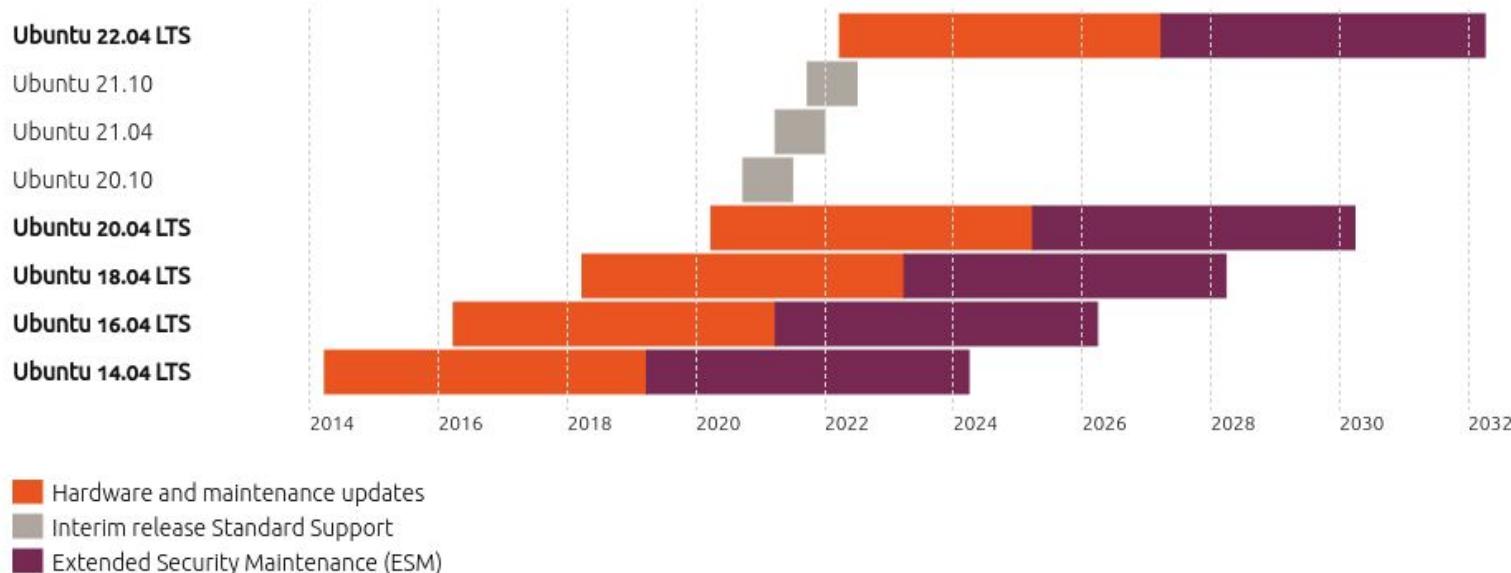
Summary

Given a version number MAJOR.MINOR.PATCH, increment the:

1. MAJOR version when you make incompatible API changes,
2. MINOR version when you add functionality in a backwards compatible manner, and
3. PATCH version when you make backwards compatible bug fixes.

Additional labels for pre-release and build metadata are available as extensions to the MAJOR.MINOR.PATCH format.

extra: Ubuntu Supported Version Lifecycle



RHEL8: planning suite example

RHEL 8 Planning Guide^{viii}

