

# NFA083 – Réseau et Administration Web

## Introduction à l'Administration d'un Serveur Debian GNU/Linux

Sami Taktak

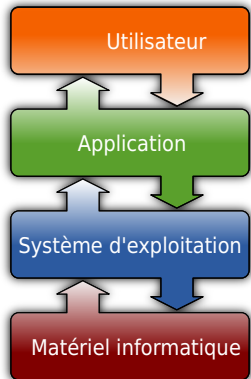
sami.taktak@cnam.fr

Centre d'Étude et De Recherche en Informatique et Communications  
Conservatoire National des Arts et Métiers

Février 2016



le **cnam**



## Definition

(Système d'exploitation) Le système d'exploitation (ou OS, pour *Operating System*) est un ensemble d'applications qui gère l'utilisation des capacités d'un ordinateur par des logiciels applicatifs.

**Objectif** : apporter commodité, efficacité et capacité d'évolution, permettant d'introduire de nouvelles fonctions et du nouveau matériel sans remettre en cause les logiciels existant

Le système d'exploitation :

- est le premier programme exécuté lors de la mise en marche de l'ordinateur après le système d'amorçage ;
- reçoit de la part des logiciels applicatifs des demandes de l'utilisation des ressources de l'ordinateur : allocation d'espace mémoire (mémoire vive ou mémoire de stockage), utilisation du processeur, ...
- fournis des services généraux facilitant la création de logiciels applicatifs ;

# Exemples de systèmes d'Exploitation

- 1977 : VMS, DEC : record de 17 ans en fonctionnement continu ;
- 1981 : DOS, IBM & Microsoft ;
- 1989 : Symbian OS, Symbian ;
- 1991 : Windows NT, Microsoft ;
- 1991 : GNU/Linux, communautaire, type UNIX ;
- 1994 : FreeBSD/OpenBSD/NetBSD : communautaire, type UNIX ;
- 1999 : MAC OS X, Apple, type UNIX ;
- 2007 : Android, Open Handset Alliance, type UNIX.

## Services offerts :

- Utilisation des périphériques : permet aux applications d'accéder aux périphériques de façon simple et homogène ;
- Gestion des fichiers : permet aux applications d'accéder aux fichiers en gérant les droits d'accès ;
- Accès aux ressources : gère l'accès aux ressources de garantir un accès équitable à l'ensemble des logiciels applicatifs ; Évite les cas d'usages abusifs ;
- Détection et récupération en cas d'erreur : en cas d'erreur matériel ou logiciel, assure leur traitement et prend les mesures nécessaires ;
- Contrôle du déroulement des opérations : réalise des statistique sur l'utilisation des ressources, les performances et la réactivité du système.



## GNU/Linux

- Système d'exploitation libre fonctionnent avec le noyau Linux
- Implémentation libre du système UNIX
- Respecte les spécifications POSIX
- Noyau initié par Linus Torvalds ; première version en 1991
- Ensemble des bibliothèques incluses dans le système provenant du projet GNU

- Système le plus répandu dans les supercalculateurs et les smartphones
- Très présent sur le marché des serveurs
- Très présent dans les systèmes embarqués : télévision, modem, GPS, ...
- Peu présent sur les ordinateurs personnels



Systeme GNU/Linux  
+  
Ensemble de logiciels applicatifs  
=  
Distribution Linux

- Debian
- OpenSuse
- Ubuntu (dérivé de Debian)
- Red Hat Enterprise Linux (RHEL) et Fedora
- Slackware



- Distribution communautaire
- Développé par l'organisation communautaire Debian
- Utilisée comme base par de nombreuses autres distributions (comme Ubuntu)
- Une des plus vieilles distributions encore en activité : première version en août 1993
- Disponible sur un grand nombre d'architecture : x86, SPARC, PowerPC, MIPS, IA-64, AMD64, ARM, ...
- <http://www.debian.org/>

## Distribution des logiciels

- 37 500 avec la version jessie
- Gérer par APT (*Advanced Packaging Tool* ou Utilitaire de gestion de paquets avancés) composé plusieurs programmes dont *apt-get* pour l'installation de paquets
  - `apt-get install nom-du-paquet` : installe le paquet nommé `nom-du-paquet`
  - `apt-get upgrade nom-du-paquet` : met à jour le paquet nommé `nom-du-paquet`
  - `apt-get dist-upgrade` : met à jour tous les paquets installés
  - `apt-get update` : met à jour les informations sur les paquets disponibles

# Gestion de Paquets avec Debian GNU/Linux

Paquet	Version installée	Dernière version	Description
sysvinit	2.86.ds1-61	2.86.ds1-61	System-V-like init utilities
sysvinit-utils	2.86.ds1-61	2.86.ds1-61	System-V-like utilities
sysv-rc	2.86.ds1-61	2.86.ds1-61	System-V-like runlevel change mechar
tasksel	2.78	2.78	Tool for selecting tasks for installatio
tasksel-data	2.78	2.78	Official tasks used for installation of D
udev	0.125-7	0.125-7	/dev/ and hotplug management daem
unattended-upgrades	0.25.1.debian1-0.1	0.25.1.debian1-0.1	Install security upgrades automaticall
update-inetd	4.31	4.31	inetd configuration file updater
aboot-base		1.0~pre20040408-3	base files required for bootable media
aboot-cross		1.0~pre20040408-3	utility to create bootable ISO-images f

**/dev/ and hotplug management daemon**  
udev is a daemon which dynamically creates and removes device nodes from /dev/, handles hotplug events and loads drivers at boot time. It replaces the hotplug package and requires a 2.6.18 or newer kernel version.

1043 paquets listés, 958 installés, 0 cassés. 0 à installer ou mettre à jour, 0 à désinstaller

Trois versions toujours disponibles :

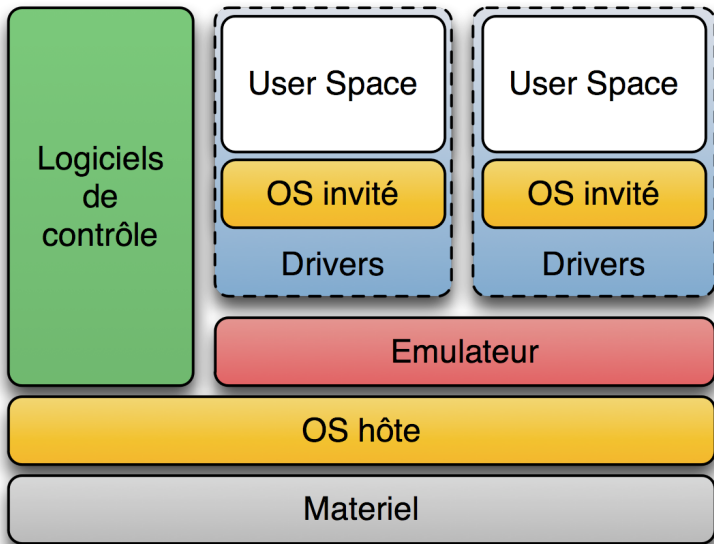
- **stable** : version figée où les seules mises à jour sont des correctifs de sécurité ;  
actuellement, il s'agit de la version 8.7 nommé jessie
- **testing** : future version stable où seuls les paquets suffisamment matures peuvent rentrer ;  
actuellement, il s'agit de la version 8.0 nommé *jessie*
- **unstable** : surnommée *sid*, version en constante évolution, continuellement mise à jours

En TP nous utiliseront la version stable actuelle : Debian jessie

- consiste à simuler l'existence de plusieurs machines informatiques en utilisant une seule
- Permet de diminuer les coûts d'achat de matériel : un serveur ordinaire de 2008 n'utilise que 10% des capacités du matériel
- Permet de gagner du temps : simplifie le déploiement des serveurs et leur maintenance
- Permet d'utiliser une seule machine pour faire tourner plusieurs système d'exploitation
- Nécessite un *hyperviseur*

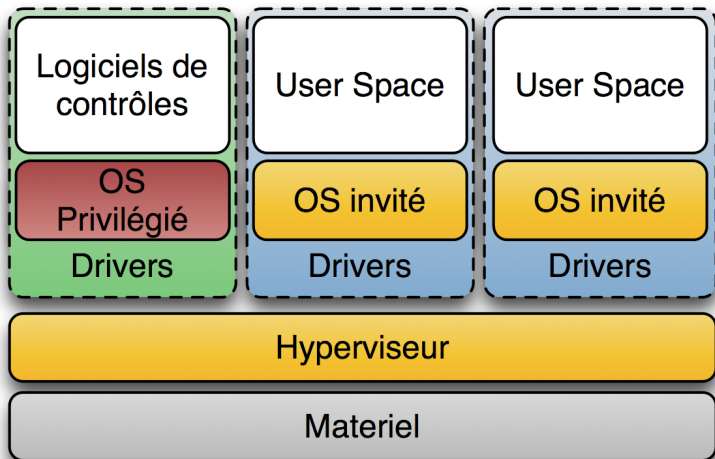
- Logiciel qui tourne sur l'OS hôte
- Permet de lancer un ou plusieurs OS invités sur l'OS hôte
- Virtualise ou émule le matériel pour les OS invités
- Situation comparable à un émulateur, mais microprocesseurs et mémoire vive directement accessibles aux machines virtuelles
- Exemple de logiciel de virtualisation : KVM, QEMU, VMware, VirtualBox, Xen

# Architecture QEMU





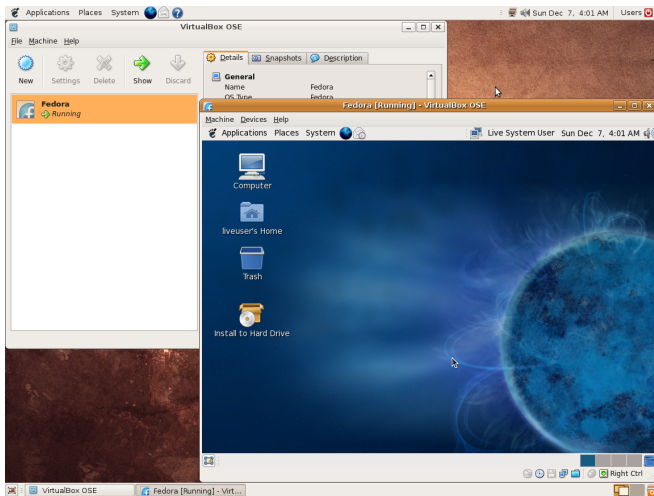
# Architecture QEMU-KVM



- L'illusion d'un appareil informatique créée par un logiciel d'émulation ou de virtualisation
- Appelé système Invité
- Tourne sur un système Hôte
- Concrètement : un fichier contenant les données du disque dure virtuel qui lui est associé

# Oracle VM VirtualBox

- Anciennement VirtualBox
- Logiciel libre de virtualisation publié par Oracle



le cnam

# TP Installation de Debian

- Création d'une image disque virtuel
- Téléchargement de l'image d'installation de Debian
- Démarrage de la machine virtuel
- Installation du système Debian
- Redémarrage de la machine virtuelle sur le nouvel OS

- Premier programme exécuté lorsque que s'identifie en mode texte
- Programme exécuter lorsque l'on ouvre un émulateur de terminal en mode graphique
- Programme interactif : permet de saisir des commandes et d'afficher leurs résultats
- Interpreteur de commande
- Le plus répandu sous GNU/Linux : bash
- Autres shell : csh, ksh, ...
- Le prompt : curseur clignotant précédé d'un caractère #, \$, >, ...

# Prompt Bash

```
Debian GNU/Linux 6.0 NFA083-VM tty1
NFA083-VM login: eleve
Password:
Last login: Thu Apr 18 14:26:55 CEST 2013 on tty1
Linux NFA083-VM 2.6.32-5-amd64 #1 SMP Mon Feb 25 00:26:11 UTC 2013 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
eleve@NFA083-VM:~$
```

Syntaxe générale des commandes :

commande [OPTIONS] [PARAMÈTRES]

- Composée d'un code mnémonique en minuscule
- Peut prendre un ou plusieurs arguments séparés par des espaces
- Deux types d'arguments :
  - les options : précédées d'un signe moins (-). Certaines options peuvent prendre un paramètre propre
  - paramètres : en générale des noms de fichiers ou de répertoire

# Exemple : la Commande ls

```
eleve@NFA083-VM:~$ ls
```

```
Bureau Documents      Images  Modèles  Musique  
Public  Téléchargements  Vidéos
```

```
eleve@NFA083-VM:~$ ls /
```

```
bin    dev    home    lib    lib64    media  
opt    root   selinux sys    usr      vmlinuz  
boot   etc    initrd.img lib32  lost+found mnt  
proc   sbin   srv     tmp    var
```



# Exemple : la Commande ls

```
eleve@NFA083-VM:~$ ls -l /
total 88
drwxr-xr-x  2 root root  4096 15 avril 13:45 bin
drwxr-xr-x  3 root root  4096 15 avril 14:19 boot
drwxr-xr-x 12 root root 2940 18 avril 14:37 dev
drwxr-xr-x 89 root root  4096 18 avril 14:37 etc
drwxr-xr-x  3 root root  4096 15 avril 13:53 home
lrwxrwxrwx  1 root root    30 15 avril 13:32 initrd.img
-> boot/initrd.img-2.6.32-5-amd64
drwxr-xr-x 13 root root 12288 15 avril 14:16 lib
drwxr-xr-x  2 root root  4096 15 avril 13:41 lib32
lrwxrwxrwx  1 root root    4 15 avril 12:13 lib64 -> /lib
drwx----- 2 root root 16384 15 avril 12:12 lost+found
drwxr-xr-x  4 root root  4096 15 avril 12:13 media
drwxr-xr-x  2 root root  4096 14 févr. 11:15 mnt
```

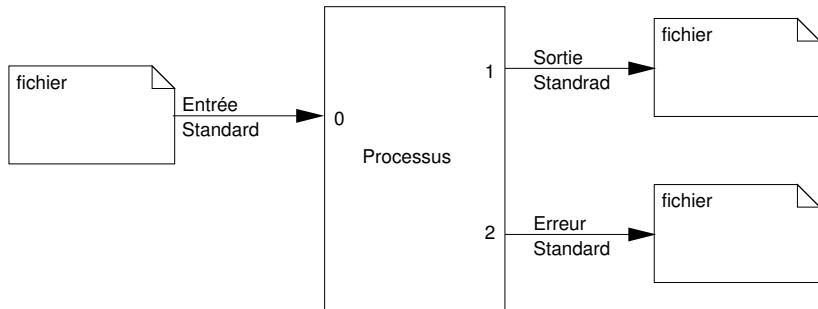


# Exemple : la Commande echo et cat

```
eleve@NFA083-VM:~$ echo 'Bonjour le monde !' > \  
    bonjour.txt  
eleve@NFA083-VM:~$ cat bonjour.txt  
Bonjour le monde !
```

- Le caractère \ permet de passer à la ligne sans exécuter la commande
- Le caractère > redirige la *sortie standard* de la commande echo vers le fichier bonjour.txt

# Redirection des Entrées-Sorties



# Redirection des Entrées-Sorties

- `<` suivi d'un nom de fichier : indique la redirection de l'entrée standard depuis ce fichier
- `>` suivi d'un nom de fichier : indique la redirection de la sortie standard vers ce fichier. Si le fichier existe, son contenu est écrasé
- `>>` suivi d'un nom de fichier : indique la redirection de la sortie standard vers ce fichier. Les données seront enregistrées à la fin du fichier
- `2 >` ou `2 >>` suivi d'un nom de fichier : indique la redirection de la sortie d'erreur standard vers ce fichier. Les données contenu dans ce fichier seront soit écrasées `2 >`, soit conservées `2 >>`
- `& >` suivi d'un nom de fichier : indique la redirection de la sortie standard et de la sortie d'erreur standard vers ce fichier

# Redirection des Entrées-Sorties

```
eleve@NFA083-VM:~$ ls > liste
eleve@NFA083-VM:~$ ls /etc/ >> liste_etc
eleve@NFA083-VM:~$ cat < liste
bonjour.txt
Bureau
Documents
Images
liste
Modèles
Musique
Public
Téléchargements
Vidéos
```

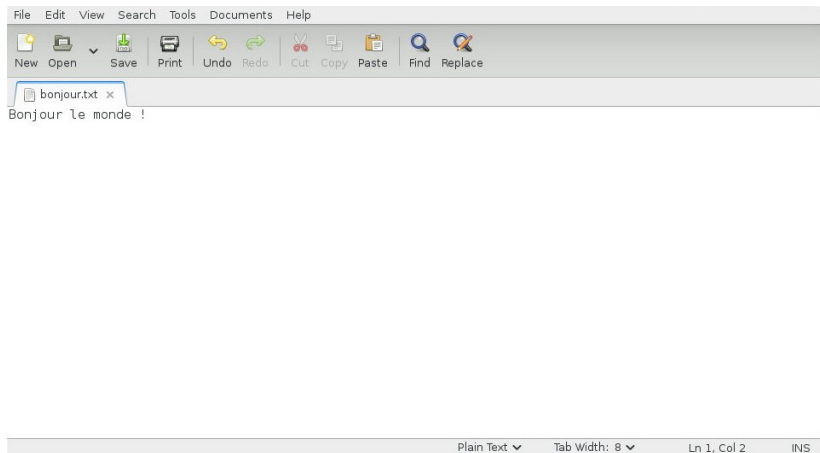
- Logiciel destiné à la création et l'édition de fichiers textes
- Orienté lignes de code plutôt que paragraphes
- Fichier ne contenant pas de mise en forme (taille et genre de la police, ...).
- Exemples d'éditeur de texte : Notepad, gedit, nano, emacs, vi, ...

# L'Éditeur de Texte nano

```
GNU nano 2.2.4      Fichier : bonjour.txt
Bonjour le monde !

[ Lecture de 1 ligne ]
^G Aide          ^O Écrire        ^R Lire fich.   ^Y Page préc.   ^K Couper       ^C Pos. cur.
^X Quitter      ^J Justifier    ^W Chercher    ^V Page suiv.   ^U Coller       ^T Orthograp.
```

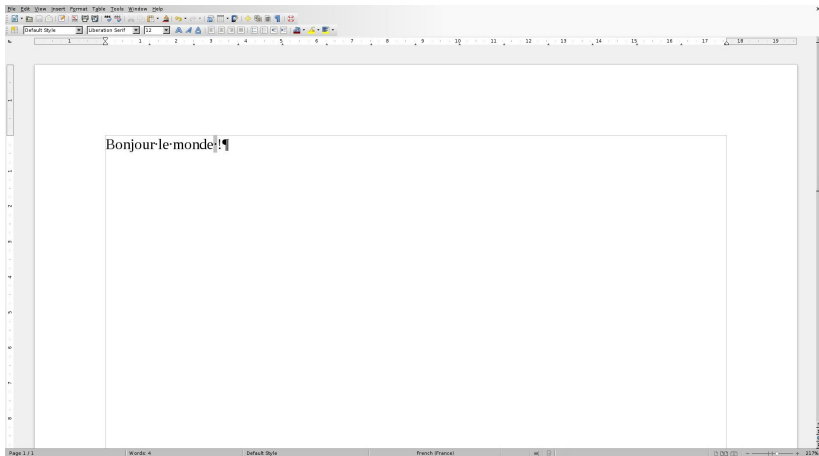
# L'Éditeur de Texte gedit





- Format de fichiers élaboré
- Contenant les informations de présentation
- Mise en page complexe
- Support des tableaux, tables des matières, index, . . .
- Sert à mettre en forme de documents
- Ne convient pour l'édition de fichiers de configuration

# Traitement de Texte libreoffice



# Contenu de bonjour.odt

```
eleve@NFA083-VH:~$ cat bonjour.odt
P0k0B^02
  'mimetypeapplication/vnd.oasis.opendocument.textP0k0B\Z~33Thumbnails/thumbnail.png@PNG

IHDRg??IDATx000J\nk00h00X
0040A0C00?00a^00y0050i09370L0Ag0/0001I01I01I01I01I01I01I01I[RG6GKKK000+++0/.66610000~0z
                                   ggg0^0z0U000000
0?)00000000qpD60000/_01o0000000{({_0~000[[[0?kvv0~gaa00700001mm0000000033300?0//00^0x00000007o00d2000Y
c00Ccg,g705x|R00C/_0000f00000g0xj00L7E);0m00K0gH01Lw000xj0||`=0;0aqqqwvw:04500#00_01I01I01I01I01I01I01I
1I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I
01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I
I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I01I
1I01I01I01I01I0
700v00dIEND0B`0k0B
                                   content.xml0W0n0600)T-070q0
                                   $j000hR0W001v)RX)0~0}0>Y00EK00p80|0_00i0\0
0<c0000"000_0?000000ETI
                                   0hKS0"o0,100000a00*000
'0D000-0Te00t0<0.50R00:T0T0T)0z0_X1000000n~00
0000F040V
p3^00w^ukb09000 0?00Z0u0/000j0$3000J0H0)00to00?0<@wg0000005"h000D
060Lc000    010I0>=>05000#.0X000y0X0F0L0M000nw'0+]0'0@g000I00C>00
                                   00 0X|O'0s00;L1c(00000*0J00)0a0;^0
0,nT0Pi000x0q00E00{&00~0N00_0i004070_00
                                   f1000dy600h0$00t0000a00$F\A0p040r
                                   0g          hu9B40R000/00.0)n0K0bs0oZ0(0000~00w0Bqg,
0/08000W0I
0d0I00p0000Tq0Ik0,000U0G|0E_00
```

- Ajout d'un utilisateur :  
`adduser identifiant_utilisateur`
- Suppression d'un utilisateur :  
`userdel identifiant_utilisateur`
- Modification d'un utilisateur :  
`moduser identifiant_utilisateur`
- Changement du mot de passe d'un utilisateur :  
`passwd identifiant_utilisateur`

## Création d'un nouvel utilisateur Alice

```
# useradd -d /home/alice -m -U Alice
```

- `-d /home/alice` : nom du répertoire personnel pour le compte du nouvel utilisateur Alice
- `-m` : créer le répertoire personnel pour le compte du nouvel utilisateur
- `-U` : créer un groupe ayant le même nom que l'utilisateur

# Compte Administrateur ou root

- Droits limités pour les simples utilisateurs
  - Permet de séparer les fichiers entre chaque utilisateurs
  - Augmente la sécurité du système : un simple utilisateur ne peut pas modifier la configuration du système
  - Utilisateur root possède tous les droits : super-utilisateur
    - Peut modifier la configuration du système
    - Peut accéder aux fichiers de tous les utilisateurs
- ⇒ il est dangereux de travailler en tant que root
- un minimum d'action doivent-êtré effectuer en tant que super-utilisateur

# Exécuter une Commande avec les Droit d'un Autre Utilisateur

## La commande sudo

- Utilitaire permettant d'exécuter une commande avec les droit d'un autre utilisateur
- Très utiliser pour exécuter une commande avec les droit de super-utilisateur
- Invocation :  
> `sudo ls /root/`
- Nécessite seulement le mot de passe de l'utilisateur appelant sudo
- Tous les utilisateurs appartenant au groupe sudo peuvent exécuter une commande avec les droits de super-utilisateur

# Appel de sudo

```
eleve@NFA083-VM:~$ sudo ls /root
```

We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
[sudo] password for eleve:
```

```
eleve is not in the sudoers file. This incident will be reported.
```

```
eleve@NFA083-VM:~$ id
```

```
uid=1000(eleve) gid=1000(eleve) groupes=1000(eleve),  
24(cdrom),25(floppy),29(audio),30(dip),44(video)  
eleve@NFA083-VM:~$
```



le cnam



# Ajout d'un Utilisateur à un groupe

La commande `usermod` permet d'ajouter un utilisateur à un groupe

Opération à effectuer en tant que `root` :

```
# usermod -a -G sudo eleve
```

- `-a` ajoute l'utilisateur à un/des groupe(s) secondaire(s).  
À utiliser uniquement avec l'option `-G`
- `-G` liste des groupes secondaires

Autres options :

- `-d` indique le nouveau répertoire home de l'utilisateur
- `-g` change le groupe primaire de l'utilisateur
- `-l` change l'identifiant de l'utilisateur



le cnam

## Nouvel appel à sudo

Après déconnexion et reconnexion de l'utilisateur eleve :

```
eleve@NFA083-VM:~$ id
uid=1000(eleve) gid=1000(eleve) groupes=1000(eleve),
24(cdrom),25(floppy),27(sudo),29(audio),30(dip),
44(video)
eleve@NFA083-VM:~$ sudo ls /root
fichier_secret_de_root
```

- Outil de connexion à distance
- Protocole de communication sécurisé
- Basée sur un échange de clefs de chiffrement
- Conçu dans l'objectif de remplacer rlogin, telnet, rsh, rcp et ftp
- Port attribué : 22
- Utilisé principalement pour ouvrir un shell sur un ordinateur distant

# SSH : Authentification

- Authentification par mot de passe
- Authentification par clefs
- Cryptographie asymétrique ou à clef publique
- Chaque utilisateur dispose d'une clef privée et d'une clef publique
- Clef publique placée sur les machines distantes
- Clef privée doit rester secrète
- Clef privée pouvant être protégé par mot de passe

- OpenBSD Secure Shell
- Implémentation libre du protocole SSH
- Ensemble d'outils informatiques permettant des communications sécurisées :
  - `ssh` : permet de se connecter à une machine distante (remplace `rlogin` et `telnet`)  
`ssh utilisateur@mondomaine.fr`
  - `scp` : permet de copier des fichiers sur une machine distante (remplace `rcp`)  
`scp fichier_src utilisateur@mondomaine.fr:~/rep/`
  - `sftp` : permet de se connecter à un serveur sftp (remplace `ftp`)  
`sftp utilisateur@mondomaine.fr`

# Connection à un Hôte Distant

- `ssh nom_de_hote -l login -p port`

- Première connection :

```
ssh lmi80.cnam.fr -l taktaks
```

```
The authenticity of host 'lmi80.cnam.fr (163.173.228.80)'  
can't be established.
```

```
ECDSA key fingerprint is 2f:0e:9c:c8:7c:fd:47:2d:64:48:c8  
:60:2d:f9:c4:fe.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added 'lmi80.cnam.fr' (ECDSA) to the  
list of known hosts.
```

```
Password:
```

- Clef publique de l'hôte mémorisée dans

```
.ssh/known_hosts
```

- Suppression de la Clef d'un hôte :

```
> ssh-keygen -R lmi80.cnam.fr
```

```
~/ssh/known_hosts updated.
```

```
Original contents retained as ~/ssh/known_hosts.old
```

Cédric le cnam

- Clefs stockées dans le répertoire `~/.ssh/`
- Clef de type DSA, ECDSA ou RSA
- Pour utiliser SSH, générer au moins une clef stocké dans :
  - `~/.ssh/identity`, `~/.ssh/id_ecdsa`, `~/.ssh/id_dsa` ou `~/.ssh/id_rsa`
  - Chaque clef privée associée à une clef publique : par exemple `~/.ssh/id_rsa.pub`
- Clef protéger par mots de passe : mot de passe demandé à chaque utilisation

# Génération d'une Clef

- `ssh-keygen` : programme de génération, gestion et conversion des clefs
  - > `ssh-keygen`  
Generating public/private rsa key pair.  
Enter file in which to save the key (~/`.ssh/id_rsa`):
- Copie de la clef publique sur l'hôte distant dans le fichier `.ssh/authorized_keys`

```
scp .ssh/id_rsa.pub lmi80.cnam.fr:clef.pub
ssh lmi80.cnam.fr
echo clef.pub >> .ssh/authorized_keys
```
- `.ssh/authorized_keys` contient des clef publique autorisées pour établir une connections



- `ssh-agent` : agent de gestion des clefs privées de l'utilisateur

```
ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-a4m4eaCYv4W6/agent.18492; \
export SSH_AUTH_SOCK;
SSH_AGENT_PID=18493; export SSH_AGENT_PID;
echo Agent pid 18493;
```

- `ssh-add` : utilitaire permettant d'ajouter de nouvelles clefs à l'agent de gestion de clefs

```
$ ssh-add
Enter passphrase for /home/taktaks/.ssh/id_rsa:
Identity added: ~/.ssh/id_rsa (~/.ssh/id_rsa)
```