Ouverture d'une session

Quel que soit le matériel, le démarrage du système lance une série de tests et de détection de matériel. Le mécanisme `initrd` laisse ensuite la place au système de fichiers monté puis exécute la commande `init`, père de tous les autres processus. La différence entre un serveur et un poste de travail c'est que dans le premier on voit - et on recherche - plus d'informations, alors que pour le deuxième, la discrétion prime.

1. Sur un serveur

a. Phase de démarrage

Pour afficher plus de renseignements au démarrage, changez les lignes suivantes du fichier `/etc/default/grub` :

```
GRUB_TIMEOUT=-1
GRUB_CMDLINE_LINUX_DEFAULT=""
```

- Tapez ensuite (en root) la commande `update-grub`
- Redémarrez

Au prochain démarrage, des informations seront données par le système (il est toujours possible de les revoir une fois connecté à une session en tapant la commande `dmesg`).

L'ouverture de session se fait par l'entrée du `login` soit `root` et de son mot de passe, **compte normalement activé à l'installation**. La saisie du mot de passe s'effectue "en aveugle", c'est-à-dire sans affichage de retour de frappe, dans un but de sécurité (pour qu'on ne puisse déterminer la longueur du mot de passe). Une fois vérifiée, vous vous trouvez dans l'espace de travail de l'utilisateur (`/root`).

Lors d'une connexion réussie, l'identifiant s'affiche avant le prompt ainsi que le répertoire dans lequel vous vous trouvez (un tilde ou ~ indique le répertoire de l'utilisateur). Le dernier symbole se détermine comme un dièse dans le cas d'un statut administrateur (`root`) alors qu'un dollar indique un statut utilisateur.

La fermeture de la session se fait par :

- `exit` : le plus usité
- `<Ctrl + D>` : classique
- `logout` : explicite

Si les droits de l'utilisateur le permettent :

- `reboot` ou `<Ctrl + Alt + Suppr>` : redémarrage du système
- `poweroff` ou `shutdown -f now` : arrêt du système

b. Rétablir le compte de l'administrateur

Appelé `root` en anglais, il dispose de tous les pouvoirs et d'un répertoire séparé : `/root`. Les travaux d'administration se font à l'aide de ce compte. Sous Ubuntu, un utilisateur spécial peut prendre temporairement les droits administrateurs pour une commande par la commande `sudo` (`do` = faire) alors que le changement complet d'identité se fait par la commande `su`.

Attention : le répertoire de base du système noté `/`, s'appelle aussi `root` mais signifie racine. Il ne faut pas les confondre.

Seules les installations de la distribution Ubuntu en mode expert (CD-Rom de la version `server` ou `alternate`) propose l'utilisation classique du compte de l'administrateur (le root). Dans le cas contraire, un utilisateur spécial doté de pouvoirs avec le mécanisme `sudo` a été créé.

Ubuntu défend une politique restrictive sur les droits utilisateurs partant de deux principes :

- L'utilisateur courant, dans sa session de travail, ne doit pas avoir accès aux fichiers et processus systèmes, ni pouvoir les modifier.
- Le compte root est "désactivé" car facilement repérable aux attaques externes et trop dangereux dans une utilisation courante.

Pour lancer et travailler sous OpenOffice ou d'autres applications, nul besoin est de disposer des privilèges liés à l'administration du système. Toute la perception de cette limitation repose sur :

- D'une part, la nature du système : un serveur ou un poste de travail.
- D'autre part, la nature des opérations effectuées : tâches d'administration ou tâches plus courantes.

Le raisonnement est simpliste mais réel : si vous êtes un administrateur système sur une distribution serveur, l'utilisation de `sudo` pour prendre les droits va vite se révéler fastidieuse, n'en déplaise aux tenants du dogme... Dans tous les autres cas, on ne change rien pour suivre les préceptes cités plus haut.

Pour lancer une opération nécessitant les droits de l'administrateur, on fait précéder le terme `sudo` avant la commande :

```
sudo visudo
```

Le choix de l'exemple n'est pas anodin car il montre le contenu du fichier `sudoers` avec la commande spéciale `visudo`. Plusieurs remarques sont à faire :

- Le fichier `/etc/sudoers` ouvert par cette commande contient la configuration de l'outil `sudo`.
- La commande `visudo` édite dans un mode plus sécurisé le fichier en interdisant les éditions multiples, vérifie et détecte les erreurs de syntaxe.
- Sans la commande `sudo`, l'édition du fichier est impossible (permission refusée) car seul le `root` en a le droit.

Voici l'adresse du site Internet de `sudo` : http://www.gratisoft.us/sudo

L'utilisation temporaire de droits administrateurs par ce mécanisme est un choix d'administration sur la distribution Ubuntu. En voici les avantages, tous liés à une meilleure recherche de la sécurité :

- L'exécution de tâches critiques pour le système fait l'objet d'une demande d'autorisation supplémentaire, propre à la réflexion.
- Les droits de l'utilisateur privilégié sont modulables et étendus à d'autres utilisateurs.
- Le compte `root`, aisément repérable par un attaquant se trouve bloqué.

L'ouverture sans la commande `sudo` interdit la modification du fichier des caractéristiques utilisateurs. Quelquefois, l'ouverture elle-même est impossible.

Si malgré tout, la fatigue liée à l'emploi systématique de la commande `sudo` l'emporte sur le désir de sécurité (on peut l'imaginer sur un système non en réseau ou protégé par un pare-feu), le rétablissement du compte administrateur système est facile :

```
sudo passwd root
```

Après la saisie du mot de passe de l'utilisateur privilégié, la demande et sa confirmation du mot de passe `root` rétablira simplement le compte.

La seule différence réside dans l'absence du fichier caché `.bash_logout` effectuant un nettoyage de l'écran lors de la déconnexion. Il suffit de le copier à partir d'un compte utilisateur dans le répertoire `/root` pour y remédier.

Utilisation de sudo en tant qu'administrateur

Alors que la commande `sudo -V` en tant qu'utilisateur ne retourne que le nom du programme et sa version, lancée en tant qu'administrateur (ou `sudo sudo`), elle affiche (liste assez longue) les variables d'environnement toujours intéressantes :

```
sudo -V
```

L'édition et la modification d'un fichier peuvent se faire par le biais d'un tampon situé dans `/var/tmp/` :

```
sudo -e (ou sudoedit)
```

La syntaxe est vérifiée et en cas de problème, des choix d'enregistrements sont proposés.

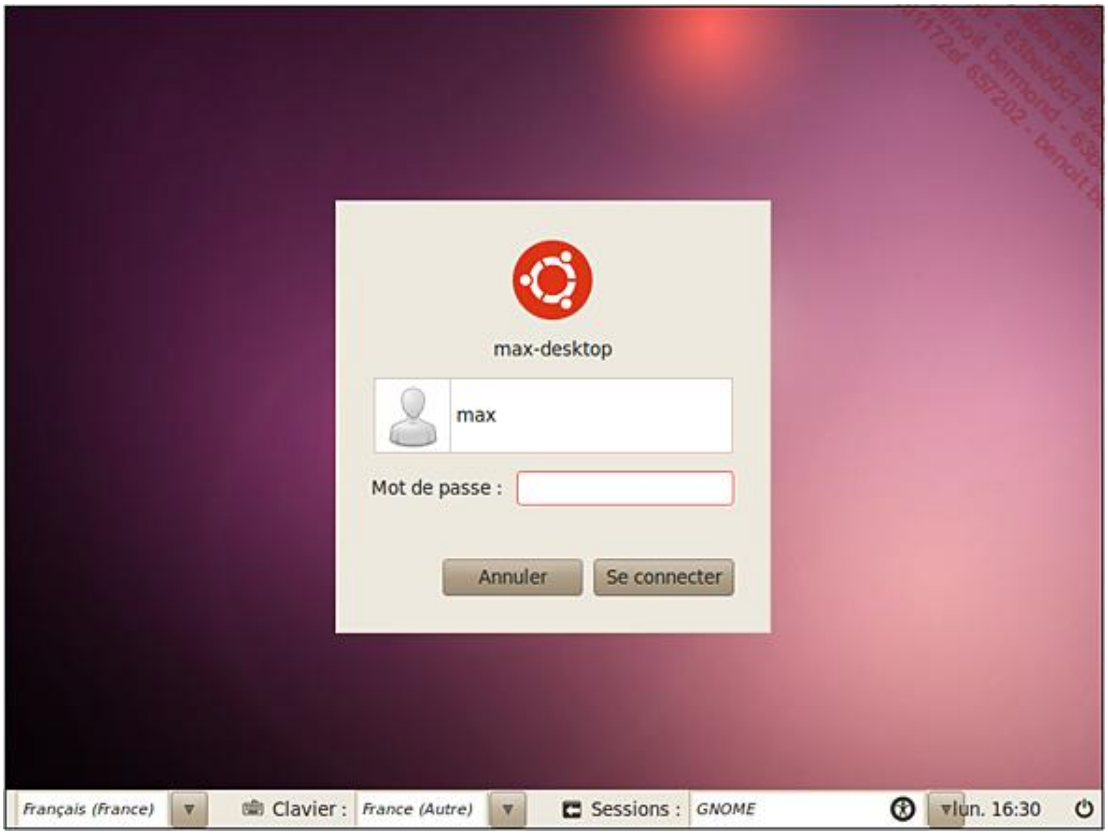
Une utilisation plus complète de la commande `sudo` vous est fournie lors de la gestion des comptes utilisateurs dans le chapitre Maintenance de base du système.

2. Sur un poste de travail

a. Interface GDM

L'environnement de bureau GNOME associe le gestionnaire **GDM** (*Gnome Display Manager*) pour l'ouverture d'une session graphique. Ce service dispose d'un espace personnel sur le site de GNOME : http://www.gnome.org/projects/gdm

Suivant le même principe du mode console, l'interface autorise les sessions, et donc les autorisations multiples. Sur une machine utilisée par un utilisateur unique, la session peut être ouverte automatiquement par GDM avec la dispense d'entrée de l'identifiant et du mot de passe.



Une session s'ouvre classiquement en indiquant son identifiant (`login`) et le mot de passe de l'utilisateur. Un sous-menu d'options est disponible avant la connexion et propose les actions suivantes : sélectionner une autre langue, une autre disposition de clavier, une autre interface de session, choisir des paramètres en fonction de handicaps et les classiques redémarrage et arrêt du système.

b. Réglages de l'interface

L'écran de connexion comporte beaucoup de paramètres et la configuration de celui-ci se lance par le menu **Système - Administration - Fenêtre de connexion**, soit le programme **gdmsetup** (nécessite le droit administration). Les changements les plus courants concernent :

- Émettre ou non un son lors de la connexion.
- Se connecter directement à la session sans avoir besoin d'entrer son mot de passe.
- Sélectionner le type de session.

3. Authentification locale

a. Principes d'une connexion

Comme tout système Linux, Ubuntu autorise une authentification multi-utilisateur par le biais du programme `login`. Son réglage se trouve dans le fichier `/etc/login.defs` que l'on ne change généralement pas, certaines options étant réécrites par le module d'authentification PAM (voir le chapitre sur la sécurité). Les consoles de connexion sont, quant à elles, définies dans le fichier `/etc/securetty`.

Le principe local constitue le schéma de base d'une authentification, mais il peut y en avoir d'autres dites distribuées :

- par un serveur d'annuaire de type **LDAP** (*Lightweight Directory Access Protocol*).
- par un contrôleur de domaine de type **Samba** ou serveur **Active Directory** (Windows).

Le mécanisme de connexion repose sur trois fichiers :

- `/etc/passwd`, contenant les informations d'un utilisateur.
- `/etc/shadow`, contenant les mots de passe cryptés.
- `/etc/group`, contenant les informations des groupes d'utilisateurs.

Cela introduit les trois grandes catégories de classement d'utilisateurs sous Ubuntu Linux : les **utilisateurs** normaux, les **groupes** d'utilisateurs et le **reste du monde** (ou plus simplement ceux qui n'appartiennent pas aux deux premières catégories).

b. Fichiers de connexion

L'ajout manuel d'un utilisateur à partir des fichiers correspond à :

- l'ajout de la ligne utilisateur dans le fichier `/etc/passwd`.
- l'ajout du groupe de base de l'utilisateur dans le fichier `/etc/group` (généralement du même nom).
- l'ajout du mot de passe crypté avec la commande `mkpasswd` (le cryptage MD5 se combinant avec un algorithme de hachage).
- la création du répertoire dans `/home`.
- la copie des fichiers du profil utilisateur provenant du répertoire `/etc/skel`.

Structure du fichier /etc/passwd

Ce fichier texte comprenant sept champs séparés par le caractère deux points (:), accessible par tous en lecture, possède la structure suivante :

- (1) **Nom de connexion** : identifiant de l'utilisateur ou nom du démon (*daemon* ou processus en cours).
- (2) **Caractère** : ancienne place du mot de passe (avant l'utilisation de la suite *shadow*) un x indiquant un mot de passe crypté dans `/etc/shadow`, une étoile (*) interdit la connexion au compte.
- (3) **Numéro de l'utilisateur** : UID (*user identifier* ou du processus) ou véritable identifiant pour le système (UID du root à 0, Ubuntu commence les UID utilisateurs à partir de 1000).
- (4) **Numéro du groupe** : GID (*group identifier* ou du processus), même principe de numérotation que pour les UID.
- (5) **Détail** : commentaire (en général vide), l'ajout ou la modification de ce champ s'exécute par la commande `chfn`.
- (6) **Répertoire d'accueil** : pour un utilisateur situé dans `/home`.
- (7) **Programme** : à lancer à la connexion (dans le cas d'un utilisateur, il s'agit du shell ou gestionnaire de commandes).

Exemple de fichier sous Ubuntu (serveur) :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
max:x:1000:1000:max,,,:/home/max:/bin/bash
```

Pour éditer le fichier `/etc/passwd`, on utilise de préférence la commande `vipw` qui interdit toute autre édition en même temps et passe par un fichier temporaire.

Structure du fichier /etc/shadow

Le processus d'authentification utilise le fichier des mots de passe cryptés pour vérifier que l'utilisateur est bien celui qu'il prétant être. Ce fichier, en lecture uniquement par le `root` et le groupe `shadow`, comprend 9 champs, séparés par le symbole deux points (:), avec :

- (1) **Nom de l'utilisateur** : le groupe de base est du même nom que l'utilisateur.

- (2) **Mot de passe** : mot de passe chiffré par un algorithme mathématique, une étoile signifie que le compte a été désactivé ou qu'il s'agit d'un processus.
- (3) **Date de changement** : en fait le nombre de jours entre le 01/01/1970 et la date ou le changement de mot de passe a été effectué.
- (4) **Intervalle avant changement** : classiquement un 0 car non utilisé, ce champ indique le nombre de jours avant de pouvoir changer le mot de passe.
- (5) **Intervalle de changement** : classiquement 99999 car peu utilisé, il représente le nombre de jours après quoi un changement de mot passe est obligatoire.
- (6) **Délai d'expiration** : nombre de jours indiquant le délai accordé à un utilisateur avant que son mot de passe n'expire.
- (7) **Expiration du compte** : nombre de jours avant l'expiration du mot de passe et donc désactivation du compte, vide car peu utilisé.
- (8) **Date de désactivation** : en fait le nombre de jours entre le 01/01/1970 et la date de désactivation du compte, vide car peu utilisé.
- (9) **Indicateur** : non utilisé.

Exemple de fichier sous Ubuntu (serveur) :

```
root:$1$qn3AweE7$EAWynH0v1sODbXZj/22O//:14044:0:99999:7:::
daemon:*:14044:0:99999:7:::
bin:*:14044:0:99999:7:::
sys:*:14044:0:99999:7:::
sync:*:14044:0:99999:7:::
games:*:14044:0:99999:7:::
man:*:14044:0:99999:7:::
lp:*:14044:0:99999:7:::
mail:*:14044:0:99999:7:::
news:*:14044:0:99999:7:::
uucp:*:14044:0:99999:7:::
proxy:*:14044:0:99999:7:::
www-data:*:14044:0:99999:7:::
backup:*:14044:0:99999:7:::
list:*:14044:0:99999:7:::
irc:*:14044:0:99999:7:::
gnats:*:14044:0:99999:7:::
nobody:*:14044:0:99999:7:::
libuuid:!:14044:0:99999:7:::
dhcp:*:14044:0:99999:7:::
syslog:*:14044:0:99999:7:::
klog:*:14044:0:99999:7:::
max:$1$5Mj/by.J$rqo.NociSqZIrJPlQeZH10:14044:0:99999:7:::
~
```

Structure du fichier /etc/group

Ce fichier, complément du fichier `/etc/passwd` comprend 4 champs, séparés par le symbole deux points (:), avec :

- (1) **Nom du groupe** : le groupe de base est du même nom que l'utilisateur.
- (2) **Caractère** : pour remplacer un mot de passe de groupe (non attribué maintenant).
- (3) **Numéro du groupe** : c'est-à-dire l'identifiant GID.
- (4) **Utilisateurs du groupe** : liste des membres supplémentaires du groupe séparés par une virgule.

Exemple de fichier sous Ubuntu (extrait d'un serveur) :

```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:max
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:max
fax:x:21:
voice:x:22:
cdrom:x:24:max
floppy:x:25:max
tape:x:26:
sudo:x:27:
audio:x:29:max
dip:x:30:max
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:max
sasl:x:45:
plugdev:x:46:max
staff:x:50:
"/etc/group" 52L, 653C
```