Administration avancée des utilisateurs et des groupes

Identification et authentification

- **L’identification**, c’est savoir qui est qui, afin de déterminer les droits de la personne qui se connecte. Un utilisateur est identifié par un **login**.
- **L’authentification**, c’est apporter la preuve de qui on est, par exemple via un secret partagé entre l’utilisateur et le système, et connus d’eux seuls. L’utilisateur est authentifié par **un mot de passe**.

Les utilisateurs

Un utilisateur est l'association d'un nom de connexion, le login, à un UID et au moins un GID.

- **UID** : User ID.
- **GID** : Group ID

Les utilisateurs

L'UID identifie l'utilisateur (ou le compte applicatif) tout au long de sa connexion. Il est utilisé pour le contrôle de ses droits et de ceux des processus qu'il a lancé. Ce sont les UID et GID qui sont stockés au sein de la table des inodes, dans la table des processus, etc., et non les logins.

L'utilisateur dispose des attributs de base suivants :

- un nom de connexion appelé le login
- un mot de passe
- un UID
- un GID correspondant à son groupe principal
- un descriptif
- un répertoire de connexion
- une commande de connexion

Les utilisateurs

- D’autres attributs sont disponibles via l’utilisation de la sécurité des mots de passe via shadow
- Les UID d’une valeur inférieure à 100 sont en principe associés à des comptes spéciaux avec des droits étendus. Ainsi l’UID de root, l’administrateur, est 0. Selon les distributions, à partir de 100, 500 ou 1000, et ce jusqu’à environ 60000, ce sont les UID des utilisateurs sans pouvoirs particuliers

Les utilisateurs

- Un login accepte la plupart des caractères. Il ne doit pas commencer par un chiffre.
- Il est possible de modifier la liste des caractères autorisés et de forcer la longueur et la complexité via les mécanismes d’authentification PAM et le fichier /etc/login.defs

Les groupes

- Chaque utilisateur fait partie d'au moins un groupe. Un groupe regroupe des utilisateurs.
- Comme pour les logins, le GID du groupe accompagne toujours l'utilisateur pour le contrôle de ses droits. Un utilisateur peut faire partie de plusieurs groupes, auquel cas il faut distinguer son groupe primaire des groupes secondaires.

Les groupes – Groupe primaire

- Les groupes sont aussi des numéros.
- Il existe des groupes spécifiques pour la gestion de certaines propriétés du système et notamment l'accès à certains périphériques
- Le groupe primaire est celui qui est toujours appliqué à la création d'un fichier.

Exemple

Si l'utilisateur alain a pour groupe primaire users, alors les fichiers créés par alain auront comme groupe d'appartenance users.

Les groupes - Groupe secondaire

- Un utilisateur dispose de tous les droits associés à ses groupes secondaires.

  Exemple

  Si alain a comme groupe secondaire video et qu'un fichier dispose des droits d'écriture pour ce groupe, alors alain aura le droit de modifier son contenu.

- La commande id permet de connaître les informations essentielles sur un utilisateur : uid, gid, groupes secondaires.

Les mots de passe

- Les mots de passe permettent d'authentifier les utilisateurs. Ils doivent être assez complexes pour ne pas être découverts facilement, mais assez intuitifs pour qu'ils s'en souviennent.
- Les mots de passe sont cryptés (MD5, DES par exemple) et ne sont pas directement lisibles sous leur forme cryptée par l'utilisateur afin que personne ne puisse tenter de le décrypter via un quelconque traitement.
- Un utilisateur devrait changer régulièrement son mot de passe, ne jamais l'écrire quelque part ni le conserver sur lui.
- Il est possible de contraindre l'utilisateur à appliquer des règles de nommage et de durée de conservation.

Le fichier /etc/passwd

- Le fichier /etc/passwd contient la liste des utilisateurs du système local.
- Il est lisible par tout le monde.
- Les informations qu'il contient sont publiques et utiles tant pour le système que pour les utilisateurs.
- Chaque ligne représente un utilisateur et est composée de sept champs :

Le fichier /etc/passwd

- **Champ 1** : le login ou nom d'utilisateur.
- **Champ 2** : sur les vieilles versions, le mot de passe crypté. Si un x est présent, le mot de passe est placé dans /etc/shadow. Si c'est un point d'exclamation le compte est verrouillé
- **Champ 3** : le User ID.
- **Champ 4** : le GID, c'est-à-dire le groupe principal.
- **Champ 5** : un commentaire ou descriptif. C'est un champ d'information.
- **Champ 6** : le répertoire de travail, personnel, de l'utilisateur. C'est le répertoire dans lequel il arrive lorsqu'il se connecte
- **Champ 7** : le shell par défaut de l'utilisateur. Mais ce peut être toute autre commande, y compris une commande interdisant la connexion.

/etc/group

Le fichier /etc/group contient la définition des groupes d'utilisateurs et pour chacun la liste des utilisateurs dont il est le groupe secondaire. Chaque ligne est composée de quatre champs :

- Champ 1 : le nom du groupe.
- Champ 2 : le mot de passe associé
- Champ 3 : le Group Id .
- Champ 4 : la liste des utilisateurs appartenant à ce groupe.

Il est inutile de replacer dans le quatrième champ les utilisateurs ayant ce groupe pour groupe principal, c'est induit.

/etc/group

- Un groupe peut avoir un mot de passe
- Il se sert à se connecter, il est impossible de se connecter en tant que groupe
- Mais l'administrateur peut mettre en place un mot de passe sur le groupe pour protéger l'accès à ce groupe en tant que groupe principal et empêcher un utilisateur de le changer de groupe secondaire en groupe principal pour son propre compte avec la commande **newgrp**

/etc/shadow

- Le fichier /etc/shadow accompagne le fichier /etc/passwd. C’est là qu’est stocké, entre autres, le mot de passecrypté des utilisateurs
- Il contient toutes les informations sur le mot de passe et sa validité dans le temps. Chaque ligne est composée de 9 champs séparés par des :

/etc/shadow

- Champ 1 : le login.
- Champ 2 : le mot de passé crypté. Le xx initial indique le type de cryptage.
- Champ 3 : nombre de jours depuis le 1er janvier 1970 du dernier changement de mot de passe.
- Champ 4 : nombre de jours avant lesquels le mot de passe ne peut pas être changé (0 : il peut être changé n'importe quand).
- Champ 5 : nombre de jours après lesquels le mot de passe doit être changé.
- Champ 6 : nombre de jours avant l'expiration du mot de passe durant lesquels l'utilisateur doit être prévenu.
- Champ 7 : nombre de jours après l'expiration du mot de passe après lesquels le compte est désactivé.
- Champs 8 : nombre de jours depuis le 1er janvier 1970 à partir du moment où le compte a été désactivé.
- Champ 9 : réservé

/etc/gshadow

- Le fichier /etc/gshadow est le pendant du fichier /etc/shadow mais pour les groupes.
- Il n’est pas supporté par défaut sur la plupart des distributions Linux.
- Les mots de passe des groupes sont placés dans /etc/group.

Gestion des utilisateurs - Ajout

La création d’un utilisateur pourrait être entièrement effectuée à la main car Linux (et les autres Unix) s’appuient sur une suite de commandes qui ne font « que » modifier des fichiers plats déjà existants et qui créent et recopient des fichiers et dossiers au bon endroit avec les bons droits.

Gestion des utilisateurs - Ajout

La création d’un utilisateur consiste à :

- rajouter une ligne dans /etc/passwd,
- rajouter d’une ligne dans /etc/shadow,
- rajouter d’éventuelles informations dans /etc/group,
- créer le répertoire personnel et mettre à jour son contenu avec /etc/skel,
- changer les permissions et le propriétaire du répertoire personnel,
- changer le mot de passe (encodé).

Gestion des utilisateurs - Ajout

- Vous pouvez créer directement un compte en éditant les fichiers avec un éditeur, bien que ce soit plutôt déconseillé.
- Pour cela il faut utiliser la commande **vipw** qui va mettre à jour les divers caches associés à la gestion des comptes.
- La commande vipw admet trois arguments :
  - -p : édition de /etc/passwd.
  - -g : édition de /etc/group.
  - -s : édition de /etc/shadow.

Gestion des utilisateurs - Ajout

La commande useradd permet d'ajoute un nouveau compte et effectuer les principales opérations :

- création de l'utilisateur et remplissage des fichiers,
- création d'un groupe privé d'utilisateur (de même nom que celui-ci),
- création du répertoire personnel, remplissage et modification des droits.

Si aucune option n'est précisée, les valeurs par défaut sont récupérées au sein du fichier /etc/defaults/useradd.

La commande useradd -D permet d'afficher les valeurs par défaut de useradd

Le tableau suivant présente toutes les options de useradd

Option user add	Rôle
-m	Crée aussi le répertoire personnel. Elle est parfois comprise par défaut, mais il vaut mieux vérifier si le répertoire personnel est présent après l'utilisation de la commande si vous n'utilisez pas cette option.
-u	Précise l'UID numérique de l'utilisateur, pour le forcer. Autrement l'UID est calculé selon les règles du fichier login.defs et les UID existants.
-g	Précise le groupe principal de l'utilisateur, par GID ou par son nom (variable GROUP)
-G	Précise les groupes additionnels (secondaires, de l'utilisateur) séparés par des virgules (variable GROUPS).
- d	Chemin du répertoire personnel. Généralement /home/<login>, mais n'importe quel chemin peut être précisé (variable HOME/<login>).
-c	Un commentaire associé au compte. Il peut être quelconque mais est parfois utilisé par certaines commandes comme finger. Son contenu peut être modifié par l'utilisateur avec la commande chfn.
-k	Chemin du répertoire contenant le squelette de l'arborescence du répertoire utilisateur. C'est généralement /etc/skell (variable SKEL).
-s	Shell (commande de connexion) par défaut de l'utilisateur (variable SHELL). L'utilisateur peut le changer via la commande chsh.
-p	Le mot de passe de l'utilisateur. Attention ! le mot de passe doit déjà être crypté

Gestion des utilisateurs – gestion des mots de passe

- La commande useradd ne crée pas de mot de passe, sauf si on utilise l'option –p et on introduit le mot de passe de crypté
- Pour créer un mot de passe d'un utilisateur qu'on vient de créer avec useradd Il faut le faire avec la commande **passwd**.
- La commande **passwd** permet de gérer les mots de passe mais aussi les autorisations de connexion et la plupart des champs présents dans /etc/shadow.

Gestion des utilisateurs – gestion des mots de passe

- Tout utilisateur a le droit de changer son mot de passe, dans le délai précisé par le champ 4 de /etc/shadow.
- L’action par défaut est de changer le mot de passe de l’utilisateur courant. L’ancien mot de passe est demandé par sécurité
- La saisie est masquée.

Gestion des utilisateurs – gestion des mots de passe

- Les modules **PAM** (Pluggable Authentification Module) peuvent imposer des contraintes plus ou moins sévères pour le choix du mot de passe : avoir une certaine longueur, ne pas être basé sur un mot du dictionnaire, etc.
- L'utilisateur root a le droit de modifier les mots de passe de tous les utilisateurs du système, sans avoir à connaître le précédent mot de passe. Mieux : il peut forcer l'utilisation d'un mot de passe même si celui-ci n'est pas validé par PAM

Gestion des utilisateurs – gestion des mots de passe
Gérer les informations de validité

Tous les champs de /etc/shadow peuvent être modifiés par la commande **passwd**.

Voici quelques options disponibles de la commande passwd:

Gestion des utilisateurs – gestion des mots de passe
Gérer les informations de validité

Option	Rôle
-l	Lock : verrouille le compte en rajoutant un ! devant le mot de passe crypté.
-u	Unlock : déverrouille le compte. Il n'est pas possible de déverrouiller un compte qui n'a pas de mot de passe, il faut utiliser en plus -f pour cela.
-d	(root) Supprime le mot de passe du compte.
-n <j>	(root) Durée de vie minimale en jours du mot de passe.
-x <j>	(root) Durée de vie maximale en jours du mot de passe
-w <j>	(root) Nombre de jours avant avertissement.
- i <j>	(root) Délai de grâce avant désactivation si le mot de passe est expiré.
-S	(root) Statut du compte

Gestion des utilisateurs - Modification

La commande usermod permet modifier un compte.

Elle prend la même syntaxe et les mêmes options que useradd.

Gestion des utilisateurs - Modification

Liste des options de usermod

Option	Rôle
-l	Lock du compte, comme passwd -l .
-u	Unlock : déverrouille le compte. Comme passwd -u
-e <n>	Expire : le mot de passe expire n jours après le 01/01/1970.
-u <UID>	Modifie l'UID associé au login. Le propriétaire des fichiers appartenant à l'ancien UID au sein du répertoire personnel est modifié en conséquence.
-l <login>	Modifie le nom de login.
-m	Move : implique la présence de -d pour préciser un nouveau répertoire personnel. Le contenu de l'ancien répertoire est déplacé dans le nouveau.

Gestion des utilisateurs - Suppression

- la commande **userdel** permet de supprimer un utilisateur.
- Par défaut le répertoire personnel n’est pas supprimé, pour le faire il faut passer l’option -r.

Gestion des Groupes - Ajout

On peut créer un groupe directement dans le fichier /etc/group ou passer par les commandes associées.

- Pour modifier manuellement le fichier /etc/group on peut utiliser la commande vigr (ou vipw -g).
- La commande groupadd permet de créer un groupe. Sa syntaxe simple accepte l’argument -g pour préciser un GID précis

Gestion des Groupes - Modification

La commande groupmod permet de modifier un groupe. Ses paramètres sont les suivants :

Option	**Rôle**
-n <nom>	Renomme le groupe.
-g <GID>	Modifie le GID. Attention, le groupe d'appartenance des fichiers concernés n'est pas modifié.
-A <user>	Ajoute l'utilisateur spécifié dans le groupe (groupe secondaire).
-R <user>	Supprime l'utilisateur spécifié du groupe

Gestion des Groupes - Suppression

- La commande **groupdel** supprime un groupe. La commande vérifie d'abord si le groupe qu'on veut supprimer est le groupe principal d'un utilisateur. Dans ce cas le groupe ne peut pas être supprimé.
- Par contre aucune action autre que celle consistant à supprimer la ligne correspondant dans /etc/group n'est effectuée : c'est à vous de vérifier le système de fichiers (et la configuration des applications si besoin) pour supprimer toute trace de ce groupe.

Vérification de la cohérence

Il peut être utile de lancer des outils de vérification de la cohérence des fichiers des groupes et des mots de passe.

Si on a l'habitude de modifier ces fichiers à la main, rien ne garantit que tout est correct : un groupe peut être manquant, un shell inexistant, un répertoire personnel absent, etc.

La commande **pwck** effectue une vérification des fichiers /etc/passwd et /etc/shadow et reporte les erreurs.

Vérification de la cohérence

La commande **grpck** fait la même chose pour les groupes. Dans ce cas les contrôles sont moins étendus, se limitant aux doublons et à l'existence des utilisateurs pour les groupes secondaires.

Attention s'il n'y a pas d'erreurs rien n'est affiché

Vérifier les connexions

On peut tracer les connexions sur votre machine à l'aide de deux commandes:

- La commande **lastlog** se base sur le contenu de /var/log/lastlog.

Elle accepte les paramètres -u (précision d'un utilisateur) et -t pour rechercher les connexions des n derniers jours.

- La commande **last** fait à peu près la même chose, mais se base sur /var/log/wtmp qui fournit des informations supplémentaires comme l'origine de la connexion (IP, nom de la console, etc.) et les dates de connexion et de déconnexion, ainsi que la durée de connexion et si l'utilisateur est encore connecté.

Actions de l’utilisateur

L’utilisateur dispose de certaines actions sur les informations de son compte. Il peut notamment :

- changer son shell de connexion,
- changer ses informations personnelles,
- changer de groupe principal,
- prendre l’identité de quelqu’un d’autre.

Actions de l’utilisateur – changer de shell

- La commande **chsh** permet à l’utilisateur de modifier définitivement (ou jusqu’à la prochaine commande chsh) de shell de connexion.
- Il ne peut pas choisir n’importe quoi.
- Le shell (ou toute autre commande) doit être présent dans /etc/shells.
- Cette liste est accessible via le paramètre -l de la commande.
- La modification est faite au sein de /etc/passwd.
- Seul root a le droit de le modifier pour d’autres utilisateurs. Le nouveau shell est précisé avec l’option **-s**

Actions de l’utilisateur -Changer le commentaire

- Le commentaire du fichier /etc/passwd peut être modifié par l’utilisateur à l’aide de la commande **chfn**.
- Il est préférable d’utiliser la commande **chfn** de manière interactive (le passage de paramètre en mode non interactif est réservé à root).

Actions de l’utilisateur - Changer de groupe principal

- La commande **newgrp** permet de changer à titre temporaire de groupe principal, à condition que le nouveau groupe précisé soit un groupe secondaire de l’utilisateur et/ou que l’utilisateur dispose du mot de passe du groupe.
- Utilisée seule, **newgrp** revient au groupe d’origine.
- Les modifications sont temporaires, le fichier des mots de passe n’est pas modifié

Actions de l’utilisateur - Changer d’identité

L’utilisateur peut endosser, le temps d’une commande ou de toute une session, l’identité d’une autre personne.

Il s’agit généralement de root, car vous savez qu’il ne faut jamais (ou au moins éviter) de se connecter en permanence en tant que root. Donc pour les tâches administratives il faut pouvoir devenir root (ou un autre utilisateur) le temps nécessaire.

La commande (substitute user) permet d’ouvrir une session, ou d’exécuter un shell ou une commande donnée avec une autre identité, il faut bien sûr connaître le mot de passe de cet utilisateur.

Si aucun utilisateur n’est précisé, c’est root qui est utilisé.

Notifications à l’utilisateur

/etc/issue

Lorsqu’un utilisateur se connecte depuis la console, un message est généralement affiché juste avant l’invite de saisie de son login .

Ce message est contenu dans le fichier **/etc/issue**.

C’est un message d’accueil et à ce titre il peut contenir tout ce qu’on veut.

Par défaut, il contient généralement le nom de la distribution Linux et le numéro de version du noyau

Notifications à l’utilisateur

/etc/issue.net

Le message d’accueil peut être différent lorsqu’un utilisateur se connecte depuis une console distante (telnet, ssh,etc.).

Pour modifier ce message spécifique, éditez le contenu du fichier **/etc/issue.net**.

Notifications à l’utilisateur

/etc/motd

Motd signifie Message of the day, le message du jour. Une fois l’utilisateur connecté depuis une console (locale ou distante), un message peut être affiché.

L’administrateur peut modifier ce message en éditant le fichier **/etc/motd**.

Par défaut il est vide. On peut modifier ce fichier pour prévenir les utilisateurs qu’un reboot de maintenance aura lieu tel jour à telle heure, ceci évitant d’envoyer n mails…

L’environnement utilisateur

/etc/skel

À la création d’un utilisateur et de son répertoire personnel, l’environnement de l’utilisateur est mis en place.

L’environnement contient par exemple les variables d’environnement, les alias, l’exécution de divers scripts. Il est contenu dans des fichiers chargés au démarrage de l’interpréteur de commandes (shell).

Lors de la création d’un compte, les divers fichiers de configuration sont copiés depuis le contenu du

répertoire /etc/skel (skeleton) vers le répertoire personnel.

Si on veut modifier les environnements de façon globale AVANT la création des utilisateurs, on peut placer dans /etc/skel tous les fichiers qu’on souhaite souhaite et les modifier selon notre convenance.

Ainsi si par exemple on souhaite que tout le monde dispose des mêmes icônes par défaut sur son bureau, et la même configuration par défaut du bureau, placez-y les répertoires Desktop

et .kde d’un compte modèle.

Scripts de configuration

À la connexion d'un utilisateur, les scripts suivants sont exécutés dans cet ordre :

• **/etc/profile** : définit les variables d'environnement importantes comme PATH, LOGNAME, USER, HOSTNAME, HISTSIZE, MAIL et INPUTRC.

• **/etc/profile.d/*** : /etc/profile appelle tous les scripts présents dans ce répertoire. Ces scripts peuvent compléter la configuration globale en ajoutant par exemple la configuration des paramètres linguistiques, des alias globaux, etc.

• **~/.bash_profile** : si le shell est bash, c'est le script suivant à être exécuté. Il est dans le répertoire utilisateur et appelle un autre script : ~/.bashrc qui appelle lui-même /etc/bashrc. Vous pouvez définir dans .bash_profile des variables supplémentaires, alors que vous aurez tendance à définir dans ~/.bashrc des alias et des fonctions. Il n'y a pas de règles strictes.

• **/etc/bashrc** est utilisé pour définir les fonctions et alias pour tout le système et tous les utilisateurs sous bash