5.2 Leçon 1

Certification : Linux Essentials
Version : 1.6
Thème : 5 Sécurité et Permissions des Fichiers
Objectif : 5.2 Création d'Utilisateurs et de Groupes
Leçon: 1 sur 1

Introduction

La gestion des utilisateurs et des groupes sur une machine Linux est l'un des aspects clés de l'administration système. En fait, Linux est un système d'exploitation multi-utilisateurs dans lequel plusieurs utilisateurs peuvent utiliser la même machine en même temps.

Les informations sur les utilisateurs et les groupes sont stockées dans quatre fichiers dans l'arborescence du répertoire `/etc/` :

`/etc/passwd`

> un fichier de sept champs délimités par des deux points, contenant des informations de base sur les utilisateurs

`/etc/group`

> un fichier de quatre champs délimités par des deux points, contenant des informations de base sur les groupes

`/etc/shadow`

> un fichier de neuf champs délimités par des deux points, contenant les mots de passe hachés des utilisateurs

`/etc/gshadow`

> un fichier de quatre champs délimités par des deux points, contenant des mots de passe de groupe hachés

Tous ces fichiers sont mis à jour par une suite d'outils en ligne de commande pour la gestion des utilisateurs et des groupes, dont nous parlerons plus loin dans cette leçon. Ils peuvent également être gérés par des applications graphiques, spécifiques à chaque distribution Linux, qui fournissent des interfaces de gestion plus simples et plus immédiates.

Même si les fichiers sont en texte clair, ne les modifiez pas directement. Utilisez toujours les outils fournis avec votre distribution à cette fin.

Le Fichier `/etc/passwd`

`/etc/passwd` est un fichier lisible par tout le monde qui contient une liste d'utilisateurs, chacun sur une ligne séparée :

```
frank:x:1001:1001::/home/frank:/bin/bash
```

Chaque ligne se compose de sept champs délimités par des deux points :

Nom d'utilisateur

: Le nom utilisé lorsque l'utilisateur se connecte au système.

Mot de passe

: Le mot de passe haché (ou un `x` si des mots de passe *shadow* sont utilisés).

User ID (UID)

: Le numéro d'identification attribué à l'utilisateur dans le système.

Group ID (GID)

: Le numéro du groupe principal de l'utilisateur dans le système.

GECOS

: Un champ de commentaire optionnel, qui est utilisé pour ajouter des informations supplémentaires sur l'utilisateur (comme le nom complet). Le champ peut contenir plusieurs entrées séparées par des virgules.

Répertoire personnel

: Le chemin absolu du répertoire personnel de l'utilisateur.

Shell

: Le chemin absolu du programme qui est automatiquement lancé lorsque l'utilisateur se connecte au système (généralement un shell interactif tel que `/bin/bash`).

Le Fichier `/etc/group`

`/etc/group` est un fichier lisible par tout le monde qui contient une liste de groupes, chacun sur une ligne séparée :

```
developer:x:1002:
```

Chaque ligne est constituée de quatre champs délimités par des deux points :

Nom du groupe

: Le nom du groupe.

Mot de passe du groupe

Le mot de passe haché du groupe (ou un `x` si des mots de passe *shadow* sont utilisés).

Group ID (GID)

Le numéro d'identification attribué au groupe dans le système.

Liste des membres

Une liste, délimitée par des virgules, des utilisateurs appartenant au groupe, à l'exception de ceux pour lesquels il s'agit du groupe principal.

Le Fichier `/etc/shadow`

`/etc/shadow` est un fichier lisible uniquement par root et les utilisateurs ayant des privilèges de root, il contient les mots de passe hachés des utilisateurs, chacun sur une ligne séparée :

```
frank:$6$i9gjM4Md4MuelZCd$7jJa8Cd2bbADFH4dwtfvTvJLOYCCCBf/.jYbK1IMYx7Wh4fEr
Xcc2xQVU2N1gb97yIYaiqH.jjJammzof2Jfr/:18029:0:99999:7:::
```

Chaque ligne est constituée de neuf champs délimités par des deux points :

Nom d'utilisateur

Le nom utilisé lorsque l'utilisateur se connecte au système.

Mot de passe haché

Le mot de passe haché de l'utilisateur (si la valeur est `!` , le compte est verrouillé).

Date du dernier changement de mot de passe

La date du dernier changement de mot de passe, en nombre de jours depuis le 01/01/1970. Une valeur de `0` signifie que l'utilisateur doit changer le mot de passe lors du prochain accès.

Âge minimum du mot de passe

Le nombre minimum de jours, après un changement de mot de passe, qui doit s'écouler avant que l'utilisateur soit autorisé à changer à nouveau le mot de passe.

Âge maximum du mot de passe

Le nombre maximum de jours qui doivent s'écouler avant qu'un changement de mot de passe soit nécessaire.

Période d'avertissement du mot de passe

Le nombre de jours, avant l'expiration du mot de passe, pendant lesquels l'utilisateur est averti que le mot de passe doit être modifié.

Période d'inactivité du mot de passe

Le nombre de jours après l'expiration d'un mot de passe pendant lesquels l'utilisateur doit le mettre à jour. Après cette période, si l'utilisateur ne modifie pas le mot de passe, le compte sera désactivé.

Date d'expiration du compte

La date, en nombre de jours depuis le 01/01/1970, à laquelle le compte utilisateur sera désactivé. Un champ vide signifie que le compte utilisateur n'expirera jamais.

Un champ réservé

Un champ qui est réservé pour un usage futur.

Le Fichier `/etc/gshadow`

`/etc/gshadow` est un fichier lisible uniquement par root et par les utilisateurs disposant de privilèges root, qui contient des mots de passe hachés pour les groupes, chacun sur une ligne séparée :

```
developer:$6$7QUIhUX1WdO6$H7kOYgsboLkDseFHpk04lwAtweSUQHipoxIgo83QNDxYtYwgm
ZTCU0qSCuCkErmyR263rvHiLctZVDR7Ya9Ai1::
```

Chaque ligne est constituée de quatre champs délimités par des deux points :

Nom du groupe

Le nom du groupe.

Mot de passe haché

Le mot de passe haché du groupe (il est utilisé lorsqu'un utilisateur, qui n'est pas membre du groupe, veut rejoindre le groupe en utilisant la commande `newgrp` si le mot de passe commence par `!` personne n'est autorisé à accéder au groupe avec `newgrp`).

Administrateurs du groupe

Une liste, délimitée par des virgules, des administrateurs du groupe (ils peuvent changer le mot de passe du groupe et peuvent ajouter ou supprimer des membres du groupe avec la commande `gpasswd`).

Membres du groupe

Une liste des membres du groupe, délimitée par des virgules.

Maintenant que nous avons vu où sont stockées les informations sur les utilisateurs et les groupes, parlons des principaux outils en ligne de commande pour mettre à jour ces fichiers.

Ajout et Suppression de Comptes Utilisateurs

Sous Linux, vous ajoutez un nouveau compte utilisateur avec la commande `useradd`, et vous supprimez un compte utilisateur avec la commande `userdel`.

Si vous souhaitez créer un nouveau compte utilisateur nommé `frank` avec un paramètre par défaut, vous pouvez exécuter ce qui suit :

```
# useradd frank
```

Après avoir créé le nouvel utilisateur, vous pouvez définir un mot de passe à l'aide de `passwd` :

```
# passwd frank
Changing password for user frank.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Ces deux commandes requièrent les autorisations de root. Lorsque vous exécutez la commande `useradd`, les informations sur l'utilisateur et le groupe stockées dans les bases de données de mots de passe et de groupes sont mises à jour pour le compte utilisateur nouvellement créé et, si cela est spécifié, le répertoire personnel du nouvel utilisateur est créé ainsi qu'un groupe portant le même nom que le compte utilisateur.

N'oubliez pas que vous pouvez toujours utiliser l'utilitaire `grep` pour filtrer les bases de données de mots de passe et de groupes, en n'affichant que l'entrée qui se réfère à un utilisateur ou un groupe spécifique. Pour l'exemple ci-dessus, vous pouvez utiliser

```
cat /etc/passwd | grep frank
```

ou

```
grep frank /etc/passwd
```

pour voir les informations de base sur le compte `frank` nouvellement créé.

Les options les plus importantes qui s'appliquent à la commande `useradd` sont les suivantes :

`-c`

> Crée un nouveau compte utilisateur avec des commentaires personnalisés (par exemple le nom complet).

`-d`

> Crée un nouveau compte utilisateur avec un répertoire personnel défini.

`-e`

Crée un nouveau compte utilisateur en fixant une date précise à laquelle il sera désactivé.

`-f`

Crée un nouveau compte utilisateur en fixant le nombre de jours après l'expiration du mot de passe pendant lesquels l'utilisateur doit mettre à jour son mot de passe.

`-g`

Crée un nouveau compte utilisateur avec un GID spécifique

`-G`

Crée un nouveau compte utilisateur en l'ajoutant à plusieurs groupes secondaires.

`-m`

Crée un nouveau compte utilisateur avec son répertoire personnel.

`-M`

Crée un nouveau compte utilisateur sans son répertoire personnel.

`-s`

Crée un nouveau compte utilisateur avec un shell de connexion spécifique.

`-u`

Créer un nouveau compte utilisateur avec un UID spécifique.

Une fois le nouveau compte utilisateur créé, vous pouvez utiliser les commandes `id` et `groups` pour connaître son UID, son GID et les groupes auxquels il appartient.

```
# id frank
uid=1000(frank) gid=1000(frank) groups=1000(frank)
# groups frank
frank : frank
```

N'oubliez pas de vérifier et éventuellement de modifier le fichier `/etc/login.defs`, qui définit les paramètres de configuration qui contrôlent la création des utilisateurs et des groupes. Par exemple, vous pouvez définir la plage d'UID et de GID qui peuvent être attribués aux nouveaux comptes utilisateurs et de groupes, préciser qu'il n'est pas nécessaire d'utiliser l'option `-m` pour créer le répertoire personnel du nouvel utilisateur et si le système doit automatiquement créer un nouveau groupe pour chaque nouvel utilisateur.

Si vous souhaitez supprimer un compte utilisateur, vous pouvez utiliser la commande `userdel`. Cette commande permet notamment de mettre à jour les informations stockées dans les bases de données des comptes, en supprimant toutes les entrées se rapportant à l'utilisateur spécifié. L'option `-r` supprime également le répertoire personnel de l'utilisateur et tout son

contenu, ainsi que l'ensemble des courriers électroniques de l'utilisateur. Les autres fichiers, situés ailleurs, doivent être recherchés et supprimés manuellement.

```
# userdel -r frank
```

Comme auparavant, vous avez besoin de la permission de root pour supprimer des comptes utilisateurs.

Le Répertoire Squelette

Lorsque vous ajoutez un nouveau compte utilisateur, même en créant son répertoire personnel, le répertoire personnel nouvellement créé est rempli de fichiers et de dossiers qui sont copiés à partir du répertoire squelette (par défaut `/etc/skel`). L'idée est simple : un administrateur système veut ajouter de nouveaux utilisateurs ayant les mêmes fichiers et répertoires dans leur répertoire personnel. Par conséquent, si vous souhaitez personnaliser les fichiers et les dossiers qui sont créés automatiquement dans le répertoire personnel des nouveaux comptes utilisateurs, vous devez ajouter ces nouveaux fichiers et dossiers au répertoire squelette.

Notez que les fichiers de profil qui se trouvent généralement dans le répertoire du squelette sont des fichiers cachés. Par conséquent, si vous voulez lister tous les fichiers et dossiers du répertoire squelette, qui seront copiés dans le répertoire personnel des utilisateurs nouvellement créés, vous devez utiliser la commande `ls -Al`.

Ajout et Suppression de Groupes

Quant à la gestion des groupes, vous pouvez ajouter ou supprimer des groupes à l'aide des commandes `groupadd` et `grouppdel`.

Si vous souhaitez créer un nouveau groupe nommé `developer`, vous pouvez exécuter la commande suivante en tant que root :

```
# groupadd -g 1090 developer
```

L'option `-g` de cette commande crée un groupe avec un GID spécifique.

Si vous souhaitez supprimer le groupe `developer`, vous pouvez lancer la commande suivante :

```
# groupdel developer
```

N'oubliez pas que lorsque vous ajoutez un nouveau compte utilisateur, le groupe primaire et les groupes secondaires auxquels il appartient doivent exister avant de lancer la commande `useradd`. De même, vous ne pouvez pas supprimer un groupe s'il s'agit du groupe primaire d'un compte utilisateur.

La Commande `passwd`

Cette commande est principalement utilisée pour changer le mot de passe d'un utilisateur. Tout utilisateur peut changer son mot de passe, mais seul root peut changer le mot de passe de n'importe quel utilisateur.

Selon l'option de `passwd` utilisée, vous pouvez contrôler des aspects spécifiques du vieillissement des mots de passe :

`-d`

Supprime le mot de passe d'un compte utilisateur (ce qui désactive l'utilisateur).

`-e`

Force le compte utilisateur à changer le mot de passe.

`-l`

Verrouille le compte de l'utilisateur (le mot de passe haché est précédé d'un point d'exclamation).

`-u`

Déverrouille le compte utilisateur (il supprime le point d'exclamation).

`-S`

Produire des informations sur le statut du mot de passe pour un compte spécifique.

Ces options ne sont disponibles que pour root. Pour voir la liste complète des options, reportez-vous aux pages de manuel.

Exercices Guidés

1. Pour chacune des entrées suivantes, indiquez le fichier auquel elle se rapporte :
   - `developer:x:1010:frank,grace,dave`
   - `root:x:0:0:root:/root:/bin/bash`
   - `henry:$1$.AbCdEfGh123456789A1b2C3d4.:18015:20:90:5:30::`
   - `henry:x:1000:1000:User Henry:/home/henry:/bin/bash`

- `staff:!:dave:carol,emma`

2. Observez les résultats suivants pour répondre aux sept questions suivantes :

```
# cat /etc/passwd | tail -3
dave:x:1050:1050:User Dave:/home/dave:/bin/bash
carol:x:1051:1015:User Carol:/home/carol:/bin/sh
henry:x:1052:1005:User Henry:/home/henry:/bin/tcsh
# cat /etc/group | tail -3
web_admin:x:1005:frank,emma
web_developer:x:1010:grace,kevin,christian
dave:x:1050:
# cat /etc/shadow | tail -3
dave:$6$AbCdEfGh123456789A1b2C3D4e5F6G7h8i9:0:20:90:7:30::
carol:$6$q1w2e3r4t5y6u7i8AbcDeFgHiLmNoPqRsTu:18015:0:60:7:::
henry:!$6$123456789aBcDeFgHa1B2c3d4E5f6g7H8I9:18015:0:20:5:::
# cat /etc/gshadow | tail -3
web_admin:!:frank:frank,emma
web_developer:!:kevin:grace,kevin,christian
dave:!::
```

   - Quels sont l'ID utilisateur (UID) et l'ID groupe (GID) de `carol` ?

   - Quels sont les shells prévus pour `dave` et `henry` ?

   - Quel est le nom du groupe primaire de `henry` ?

   - Quels sont les membres du groupe `web_developer` ? Quels sont les administrateurs de ce groupe ?

   - Quel utilisateur ne peut pas se connecter au système ?

   - Quel utilisateur doit changer de mot de passe la prochaine fois qu'il se connectera au système ?

   - Combien de jours doivent s'écouler avant qu'un changement de mot de passe ne soit nécessaire pour `carol` ?

Exercices d’Exploration

1. En tant que root, exécutez la commande `useradd -m dave` pour ajouter un nouveau compte utilisateur. Quelles sont les opérations effectuées par cette commande ? Supposons que `CREATE_HOME` et `USERGROUPS_ENAB` dans `/etc/login.defs` soient définis sur *yes*.

2. Maintenant que vous avez créé le compte `dave`, cet utilisateur peut-il se connecter au système ?

3. Identifier l’ID utilisateur (UID) et l’ID groupe (GID) de `dave` et de tous les membres du groupe `dave`.

4. Créez les groupes `sys_admin`, `web_admin` et `db_admin` et identifiez leurs ID de groupe (GID).

5. Ajoutez un nouveau compte utilisateur nommé `carol` avec l’UID 1035 et définir `sys_admin` comme son groupe primaire et `web_admin` et `db_admin` comme ses groupes secondaires.

6. Supprimez les comptes utilisateurs `dave` et `carol` et les groupes `sys_admin`, `web_admin` et `db_admin` que vous avez créés précédemment.

7. Exécutez la commande `ls -l /etc/passwd /etc/group /etc/shadow /etc/gshadow` et décrivez la sortie qu’elle vous donne en termes de permissions de fichiers. Lesquels de ces quatre fichiers sont ombragés (*shadowed*) pour des raisons de sécurité ? Supposons que votre système utilise des mots de passe "shadow".

8. Exécutez la commande `ls -l /usr/bin/passwd`. Quel bit spécial est défini et quelle est sa signification ?