**453---SYSTEME D'EXPLOITATION - e-learning - Séquence 19**

**Utilisateurs, groupes et droits – 2**

**Légende :**

Explications sur fond blanc

Exercice à accomplir sur fond rouge clair

Une ou plusieurs solutions possibles pour accomplir l’exercice sur fond vert clair

Dans un système Linux, chaque fichier (au sens large : fichier ordinaire, répertoire, etc.) est assorti de droits précisant les utilisateurs et les groupes d’utilisateurs qui sont habilités à y accéder, et de quelle façon.

Les catégories d’utilisateurs, reconnues par le noyau de Linux, sont :

u user (PROPRIETAIRE du fichier)

g group (GROUPE auquel est affilié le fichier)

o other (AUTRES utilisateurs)

a all (TOUS les utilisateurs)

Les droits, reconnus par le noyau de Linux, sont :

r read

w write (création et suppression d’entrées, dans le cas d’un répertoire)

x execute (accès aux fichiers, dans le cas d’un répertoire)

s SUID (Set-UID : appliqué à un fichier binaire exécutable : tout utilisateur ayant le droit de l’exécuter reçoit alors les mêmes droits que le propriétaire de ce fichier en ce qui concerne les accès réalisés lors de cette exécution)

s SGID (Set-GID : appliqué à un fichier binaire exécutable : tout utilisateur ayant le droit de l’exécuter reçoit alors les mêmes droits que le groupe de ce fichier en ce qui concerne les accès réalisés lors de cette exécution)

s SGID (Set-GID : appliqué à un répertoire : tout fichier créé dans ce répertoire reçoit alors comme groupe le groupe de ce répertoire)

t sticky bit (appliqué à un répertoire accessible en écriture à plusieurs utilisateurs : à part le propriétaire du répertoire, il faut alors être propriétaire d’un fichier qui y réside pour avoir le droit de le détruire)

Valeurs octales des droits :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Endossement ou sticky bit | | user | | group | | other | |
| 4000 | SUID | 400 | r | 40 | r | 4 | r |
| 2000 | SGID | 200 | w | 20 | w | 2 | w |
| 1000 | sticky bit | 100 | x (1) | 10 | x (2) | 1 | x (3) |

|  |  |  |  |
| --- | --- | --- | --- |
|  | (1) s=SUID+x  S=SUID | (2) s=SGID+x  S=SGID | (3) t=sticky bit+x  T=sticky bit |

**Quelques commandes :**

CHFN(1)

NOM

chfn - Modifier le nom complet et les informations associées à un utilisateur

SYNOPSIS

chfn [options] [LOGIN]

DESCRIPTION

La commande chfn modifie le nom complet d'un utilisateur, son numéro de bureau,

son numéro de téléphone professionnel, son extension, et son numéro de

téléphone personnel. Ces informations sont généralement affichées par finger(1)

ou d'autres programmes similaires. Un utilisateur normal ne peut modifier que

les informations associées à son propre compte, avec les restrictions précisées

dans /etc/login.defs. (Par défaut, les utilisateurs ne peuvent pas modifier

leur nom complet).

CHSH(1)

NOM

chsh - Changer l'interpréteur de commandes initial

SYNOPSIS

chsh [options] [LOGIN]

DESCRIPTION

La commande chsh modifie l'interpréteur de commandes initial (« login shell »)

de l'utilisateur qui sera invoqué lors des connexions de l'utilisateur. Un utilisateur

normal ne peut changer que l'interpréteur initial associé à son propre compte. Le

superutilisateur peut changer l'interpréteur initial de n'importe quel compte.

LS(1)

NOM

ls - Afficher le contenu de répertoires

SYNOPSIS

ls [OPTION]... [FICHIER]...

DESCRIPTION

Afficher les informations des FICHIERs (du répertoire courant par défaut).

Les entrées sont triées alphabétiquement si aucune des options

-cftuvSUX ou --sort n'est indiquée.

CHOWN(1)

NOM

chown - Modifier le propriétaire et/ou le groupe d'un fichier

SYNOPSIS

chown [OPTION]... [PROPRIÉTAIRE][:[GROUPE]] FICHIER...

chown [OPTION]... --reference=FICHIER-R FICHIER...

DESCRIPTION

Le programme chown modifie le propriétaire et/ou le groupe propriétaire de chacun

des fichiers indiqués. Si seul un propriétaire (un nom d'utilisateur ou un

identifiant numérique) est spécifié, celui-ci devient le propriétaire des fichiers

donnés, mais les groupes de ces fichiers ne sont pas modifiés.

CHGRP(1)

NOM

chgrp - Changer le groupe propriétaire d'un fichier

SYNOPSIS

chgrp [OPTION]... GROUPE FICHIER...

chgrp [OPTION]... --reference=FICHIER-R FICHIER...

DESCRIPTION

Changer le groupe d'appartenance de chaque FICHIER en GROUPE. Avec l'option

--reference, modifier le groupe de chaque fichier en celui de FICHIER-R.

CHMOD(1)

NOM

chmod - Modifier les bits de comportement (droits ou permissions, etc.) de fichier

SYNOPSIS

chmod [OPTION]... MODE[,MODE]... FICHIER...

chmod [OPTION]... MODE-OCTAL FICHIER

chmod [OPTION]... --reference=FICHIER-R FICHIER

DESCRIPTION

Le programme chmod modifie les bits de comportement (droits ou permissions, etc.)

de fichier de chacun des fichiers indiqués, en suivant l'indication de mode, qui peut

être une représentation symbolique des changements à effectuer, ou un nombre

octal représentant le motif binaire des nouveaux bits de comportement.

**LABORATOIRE – Utilisateurs, groupes et droits – 2**

**Les exercices des séquences 18 à 21 s’enchaînent.**

**Il faut donc les accomplir dans l’ordre prévu.**

**Dans la distribution Debian GNU/Linux :**

Connectez-vous dans un terminal sous le compte « root », c’est-à-dire le superutilisateur (Password du root)

Visualisez les mots de passe cryptés des nouveaux comptes utilisateurs et leur durée de vie

getent shadow

Structure du fichier /etc/shadow :

* Nom d'utilisateur. Case-sensitive. Exactement la même entrée que dans le fichier /etc/passwd.
* Mot de passe crypté. Une entrée "!" indique que le mot de passe n'a pas encore été configuré. Une entrée "\*" indique que le compte a été désactivé.
* La date (nombre de jours depuis le 1er janvier 1970) du dernier changement de mot de passe.
* Le nombre de jours avant que le mot de passe ne puisse être changé (un 0 indique qu'il peut être changé à n'importe quel moment).
* Le nombre de jours après lesquels le mot de passe doit être changé (99999 indique que l'utilisateur peut garder son mot de passe inchangé pendant beaucoup de temps).
* Le nombre de jours pour avertir l'utilisateur qu'un mot de passe ne va plus être valable (7 pour une semaine entière).
* Le nombre de jours avant de désactiver le compte après expiration du mot de passe.
* La date (nombre de jours depuis le 1er janvier 1970) à laquelle le compte est désactivé.
* Un champ réservé pour une utilisation future possible.

Affichez le manuel des commandes chfn et chsh

man chfn

man chsh

Pour le compte « UserX », changez de commentaire – nouveau commentaire = « UserX est un utilisateur X »

chfn -f 'UserX est un utilisateur X' UserX

Pour le compte « UserY », changez de commentaire – nouveau commentaire = « UserY est un utilisateur Y »

chfn -f 'UserY est un utilisateur Y' UserY

Pour le compte « UserZ », changez de commentaire – nouveau commentaire = « UserZ est un utilisateur Z »

chfn -f 'UserZ est un utilisateur Z' UserZ

Dans le même terminal, connectez-vous sous le compte « UserX », changez de mot de passe (New Password = UserX), affichez l’identification système du compte, affectez au compte un numéro de bureau, des numéros de téléphone professionnel et personnel, changez de shell (nouveau shell = /bin/bash), puis déconnectez-vous

su - UserX

passwd

userx

UserX

UserX

id

chfn

UserX

. . .

chsh

/bin/bash

exit

Dans le même terminal, connectez-vous sous le compte « UserY », changez de mot de passe (New Password = UserY), affichez l’identification système du compte, affectez au compte un numéro de bureau, des numéros de téléphone professionnel et personnel, changez de shell (nouveau shell = /bin/bash), puis déconnectez-vous

su - UserY

passwd

usery

UserY

UserY

id

chfn

UserY

. . .

chsh

/bin/bash

exit

Dans le même terminal, connectez-vous sous le compte « UserZ », changez de mot de passe (New Password = UserZ), affichez l’identification système du compte, affectez au compte un numéro de bureau, des numéros de téléphone professionnel et personnel, changez de shell (nouveau shell = /bin/bash), puis déconnectez-vous

su - UserZ

passwd

userz

UserZ

UserZ

id

chfn

UserZ

. . .

chsh

/bin/bash

exit

Créez sous /home un répertoire nommé : « Dossier des utilisateurs »

mkdir /home/'Dossier des utilisateurs'

Affichez le manuel de la commande ls afin d’examiner les options utilisables

man ls

Visualisez le propriétaire et le groupe du répertoire : « Dossier des utilisateurs »

ls -ld /home/'Dossier des utilisateurs'

Visualisez le contenu de ce répertoire, avec affichage long

ls -l /home/'Dossier des utilisateurs'

Dans ce répertoire, créez avec echo le fichier nommé « Cahier\_des\_charges » contenant la chaîne de caractères « Options du cahier des charges » et le fichier nommé « Contrats » contenant la chaîne de caractères « Options des contrats »

echo "Options du cahier des charges" > /home/'Dossier des utilisateurs'/Cahier\_des\_charges

echo "Options des contrats" > /home/'Dossier des utilisateurs'/Contrats

Visualisez le propriétaire et le groupe de ces fichiers

ls -l /home/'Dossier des utilisateurs'/Cahier\_des\_charges

ls -l /home/'Dossier des utilisateurs'/Contrats

Affichez le manuel des commandes chown, chgrp et chmod

man chown

man chgrp

man chmod

Utilisateurs :

u user (PROPRIETAIRE)

g group (GROUPE)

o other (AUTRES)

a all (TOUS)

Droits :

= affectation de droit(s)

+ ajouter un droit

- retirer un droit

r read

w write (création et suppression d’entrées, dans le cas d’un répertoire)

x execute (accès aux fichiers, dans le cas d’un répertoire)

s SUID (Set-UID : appliqué à un fichier binaire exécutable : tout utilisateur ayant le droit de l’exécuter reçoit alors les mêmes droits que le propriétaire de ce fichier en ce qui concerne les accès réalisés lors de cette exécution)

s SGID (Set-GID : appliqué à un fichier binaire exécutable : tout utilisateur ayant le droit de l’exécuter reçoit alors les mêmes droits que le groupe de ce fichier en ce qui concerne les accès réalisés lors de cette exécution)

s SGID (Set-GID : appliqué à un répertoire : tout fichier créé dans ce répertoire reçoit alors comme groupe le groupe de ce répertoire)

t sticky bit (appliqué à un répertoire accessible en écriture à plusieurs utilisateurs : à part le propriétaire du répertoire, il faut alors être propriétaire d’un fichier qui y réside pour avoir le droit de le détruire)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Endossement ou sticky bit | | user | | group | | other | |
| 4000 | SUID | 400 | r | 40 | r | 4 | r |
| 2000 | SGID | 200 | w | 20 | w | 2 | w |
| 1000 | sticky bit | 100 | x (1) | 10 | x (2) | 1 | x (3) |

|  |  |  |  |
| --- | --- | --- | --- |
|  | (1) s=SUID+x  S=SUID | (2) s=SGID+x  S=SGID | (3) t=sticky bit+x  T=sticky bit |

Examinez les droits sur les fichiers /etc/shadow et /usr/bin/passwd afin de comprendre pourquoi n’importe quel utilisateur a le droit de changer de mot de passe avec passwd

ls -l /etc/shadow

ls -l /usr/bin/passwd

Déconnectez-vous