**453---SYSTEME D'EXPLOITATION - e-learning - Séquence 21**

**Utilisateurs, groupes et droits – 4**

**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

**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.

SU(1)

NOM

su - Changer d'identifiant d'utilisateur ou devenir superutilisateur

SYNOPSIS

su [options] [nom\_utilisateur]

DESCRIPTION

La commande su permet de devenir un autre utilisateur pour la durée d'une session.

Invoqué sans nom d'utilisateur, le comportement par défaut de su est de devenir

superutilisateur. Le paramètre optionnel - permet d'obtenir un environnement

similaire à celui que l'utilisateur aurait obtenu lors d'une connexion directe.

RM(1)

NOM

rm - Effacer des fichiers et des répertoires

SYNOPSIS

rm [OPTION]... FICHIER...

DESCRIPTION

Le programme rm efface chaque fichier listé.

Par défaut, il n'efface pas les répertoires.

CP(1)

NOM

cp - Copier des fichiers et des répertoires

SYNOPSIS

cp [OPTION]... [-T] SOURCE CIBLE

cp [OPTION]... SOURCE... RÉPERTOIRE

cp [OPTION]... -t RÉPERTOIRE SOURCE...

DESCRIPTION

Copier la SOURCE vers la CIBLE, ou de multiples SOURCEs vers le RÉPERTOIRE.

La commande « umask » permet de configurer les droits qui seront affectés à un nouveau fichier ou un nouveau répertoire. L’effet de la commande umask est limité à la durée de vie du shell. Une modification permanente nécessite une mise à jour du fichier système : « ~/.profile » (ou « ~/.bash\_profile », selon les versions).

Les « droits normaux » sont 0666 en octal pour un fichier ordinaire (argument mode de l’appel système open) et 0777 en octal pour un répertoire (argument mode de l’appel système mkdir). La commande umask agit en soustraction pour le calcul des droits effectifs. La valeur par défaut typique en octal pour l’umask d’un processus est 022 en octal. Dès lors :

les permissions affectées en général lors de la création d’un fichier ordinaire sont :

0666 & ~022 = 0644, c’est-à-dire : rw−r−−r−−

les permissions affectées en général lors de la création d’un répertoire sont :

0777 & ~022 = 0755, c’est-à-dire : rwxr−xr−x

UMASK(2)

NAME

umask - Set file mode creation mask

SYNOPSIS

#include <sys/types.h>

#include <sys/stat.h>

mode\_t umask(mode\_t mask);

GETFACL(1)

NAME

getfacl - Get file access control lists

SYNOPSIS

getfacl [-aceEsRLPtpndvh] file ...

getfacl [-aceEsRLPtpndvh] -

DESCRIPTION

For each file, getfacl displays the file name, owner, the group, and the Access

Control List (ACL). If a directory has a default ACL, getfacl also displays the

default ACL. Non-directories cannot have default ACLs.

SETFACL(1)

NAME

setfacl - Set file access control lists

SYNOPSIS

setfacl [-bkndRLPvh] [{-m|-x} acl\_spec] [{-M|-X} acl\_file] file ...

setfacl --restore=file

DESCRIPTION

This utility sets Access Control Lists (ACLs) of files and directories. On the

command line, a sequence of commands is followed by a sequence of files (which

in turn can be followed by another sequence of commands, ...).

**LABORATOIRE – Utilisateurs, groupes et droits – 4**

**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)

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 |

S’il n’est pas encore installé, installez le C shell csh

apt-get install csh

aptitude install csh

Affichez le manuel de la commande csh

man csh

Dans le même terminal, connectez-vous sous le compte « UserT », changez de mot de passe (New Password = UserT), affectez au compte un numéro de bureau, des numéros de téléphone professionnel et personnel, changez de shell (nouveau shell = /bin/csh), puis déconnectez-vous

su - UserT

passwd

usert

UserT

UserT

chfn

UserT

. . .

chsh

/bin/csh

exit

Interrogez les annuaires en ce qui concerne le compte utilisateur UserT

getent passwd UserT

Dans le même terminal, testez la nouvelle connexion au compte « UserT », listez les caractéristiques du répertoire de connexion, puis déconnectez-vous

su - UserT

ls -ld ~

exit

Supprimez le compte utilisateur UserT, ainsi que son répertoire de connexion

userdel -r UserT

Recherchez le répertoire de connexion nommé « Utilisateur Test »

find / -name "Utilisateur Test" -print

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

man su

Dans le répertoire /home/'Dossier des utilisateurs', essayez de créer successivement le fichier f0 contenant « fichier zéro » sous le compte root, le fichier f1 contenant « fichier un » sous le compte UserX, le fichier f2 contenant « fichier deux » sous le compte UserY et le fichier f3 contenant « fichier trois » sous le compte UserZ – TOUT CELA EST-IL PERMIS ET POURQUOI ?

echo "fichier zéro" > /home/'Dossier des utilisateurs'/f0

su UserX -c "echo 'fichier un' > /home/'Dossier des utilisateurs'/f1"

su UserY -c "echo 'fichier deux' > /home/'Dossier des utilisateurs'/f2"

su UserZ -c "echo 'fichier trois' > /home/'Dossier des utilisateurs'/f3"

Visualisez le propriétaire et le groupe de ces différents fichiers (en se rappelant des droits configurés pour le répertoire /home/'Dossier des utilisateurs')

ls -l /home/'Dossier des utilisateurs'/f?

Sous le compte UserY, essayez de détruire le fichier f1 (en se rappelant des droits configurés pour le répertoire /home/'Dossier des utilisateurs'), puis déconnectez-vous

su - UserY

rm /home/'Dossier des utilisateurs'/f1

exit

Supprimez le sticky bit (appliqué au répertoire /home/'Dossier des utilisateurs')

chmod -t /home/'Dossier des utilisateurs'

Sous le compte UserY, essayez à nouveau de détruire le fichier f1, puis vérifiez et déconnectez-vous

su - UserY

rm /home/'Dossier des utilisateurs'/f1

ls -l /home/'Dossier des utilisateurs'/f1

exit

Restaurez le sticky bit (appliqué au répertoire /home/'Dossier des utilisateurs')

chmod +t /home/'Dossier des utilisateurs'

Sous le compte UserX, essayez de détruire les fichiers f0 et f2 (en se rappelant des caractéristiques du répertoire /home/'Dossier des utilisateurs'), puis déconnectez-vous – TOUT CELA EST-IL PERMIS ET POURQUOI ?

su - UserX

rm /home/'Dossier des utilisateurs'/f0

rm /home/'Dossier des utilisateurs'/f2

exit

Cherchez qui a le droit de formater la partition /dev/sda6

ls -l /dev/sda6

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

man cp

Copiez les fichiers du répertoire /home/'Dossier des utilisateurs' dans le répertoire /tmp, de façon à ce que les attributs des fichiers copiés soient conservés – en particulier le groupe de chaque fichier, puis vérifiez la conservation

cp -p /home/'Dossier des utilisateurs'/\* /tmp

ls -l /tmp/Cahier\_des\_charges /tmp/Contrats

Changez de propriétaire le fichier /tmp/Contrats (nouveau propriétaire : UserX), puis visualisez ce changement

chown UserX /tmp/Contrats

ls -l /tmp/Contrats

Sous le compte UserX, testez les accès (r,w,x) au fichier /tmp/Contrats (en se rappelant des droits configurés pour ce fichier), puis déconnectez-vous – TOUT CELA EST-IL PERMIS ET POURQUOI ?

su - UserX

cat /tmp/Contrats

echo "11111" >> /tmp/Contrats

/tmp/Contrats

exit

Sous le compte UserY, testez les accès (r,w,x) au fichier /tmp/Contrats (en se rappelant des droits configurés pour ce fichier), puis déconnectez-vous – TOUT CELA EST-IL PERMIS ET POURQUOI ?

su - UserY

cat /tmp/Contrats

echo "22222" >> /tmp/Contrats

/tmp/Contrats

exit

Sous le compte UserZ, testez les accès (r,w,x) au fichier /tmp/Contrats (en se rappelant des droits configurés pour ce fichier), puis déconnectez-vous – TOUT CELA EST-IL PERMIS ET POURQUOI ?

su - UserZ

cat /tmp/Contrats

echo "33333" >> /tmp/Contrats

/tmp/Contrats

exit

Sous le compte root, testez les accès (r,w,x) au fichier /tmp/Contrats (en se rappelant des droits configurés pour ce fichier) – TOUT CELA EST-IL PERMIS ET POURQUOI ?

cat /tmp/Contrats

echo "00000" >> /tmp/Contrats

/tmp/Contrats

Affichez le manuel de la commande umask

man umask

L’effet de la commande umask est limité à la durée de vie du shell. Une modification permanente nécessite une mise à jour du fichier système : « ~/.profile » (ou « ~/.bash\_profile », selon les versions).

Les « droits normaux » sont 0666 en octal pour un fichier ordinaire (argument mode de l’appel système open) et 0777 en octal pour un répertoire (argument mode de l’appel système mkdir). La commande umask agit en soustraction pour le calcul des droits effectifs. La valeur par défaut typique en octal pour l’umask d’un processus est 022 en octal. Dès lors :

les permissions affectées en général lors de la création d’un fichier ordinaire sont :

0666 & ~022 = 0644, c’est-à-dire : rw−r−−r−−

les permissions affectées en général lors de la création d’un répertoire sont :

0777 & ~022 = 0755, c’est-à-dire : rwxr−xr−x

Affichez le manuel des commandes getfacl et setfacl

man getfacl

man setfacl

Ces commandes permettent de gérer les ACL (listes de contrôle d’accès), qui offrent la possibilité de ne pas se limiter aux trois catégories : propriétaire – groupe – autres.

Déconnectez-vous