Gestion des utilisateurs

La hiérarchie des utilisateurs :

Le système d'exploitation Linux est multi-utilisateur, les personnes utilisant ce système doivent être identifiées, afin d'assurer la confidentialité des informations.
Un utilisateur doit obligatoirement être membre d'un groupe d'utilisateurs.
L'appartenance à un groupe permet le partage de ressources entre les membres du groupes.

Les **utilisateurs** sont identifiés par un numéro unique : **UID** *(User's ID)*.
Les **groupes** d'utilisateurs sont identifiés par un numéro unique : **GID** *(Group's ID)*
Les utilisateurs et les groupes ne sont pas tous égaux, l'on peut distinguer **3** types de comptes utilisateurs:

root	**Utilisateur le plus important. Il n'est pas concerné par les droits d'accès aux fichiers et il peut tout faire**	Les UID et GID de root sont 0
bin, daemon, sync, apache, ...	**Ce sont des comptes qui ne sont pas affectés à des personnes physiques. Ils servent uniquement à faciliter la gestion des droits d'accès de certaines applications et démons**	Les UID et GID sont compris entre 1 et 499
jean, paul, robert, ...	**Ce sont des comptes utilisateurs qui sont liés à des personnes physiques. Ces comptes permettent à des utilisateurs standards de se connecter et d'utiliser les ressources de la machine**	Les UID et GID sont supérieurs à 499

Les uid et gid indiqués (sauf pour root) sont des conventions...

Connexion :

Le programme qui permet de se connecter à un système Linux s'appelle: **login**
Une fois connecté, il est possible de changer d'identité ou plus exactement de lancer un autre shell avec un autre UID.
La commande utilisée est **su** *(Substitute User identity).*

Je suis connecté avec mon compte **pharra01**, donc dans une console, je suis **Philippe Harrand**.. Je peux changer de compte avec la commande **su** (à condition de connaître le mot de passe

correspondant, ce qui ne doit jamais arriver).

[pharra01@capella pharra01]$ su rbidochon

Password:

[rbidochon@capella pharra01]$

Et maintenant, le système croit que je suis Robert Bidochon !

Commandes d'information de connexion :

A tout moment je peux savoir qui je suis et/ou sous quel compte je suis, grâce aux commandes :

[rbidochon@capella pharra01]$ whoami

rbidochon

(dans ce cas, le prompt me l'indiquait déjà !)

[rbidochon@capella pharra01]$ id

uid=30456(rbidochon) gid=30456(rbidochon) groupes=30456(rbidochon)

[rbidochon@capella pharra01]$ groups

rbidochon

Par défaut, les systèmes RedHat créent un groupe par utilisateur. Ce n'est pas le cas avec les anciennes distributions Mandrake, par exemple.

Création d'un utilisateur : **useradd ou adduser**

Suppression d'un utilisateur : **userdel ou deluser**

Modification d'un utilisateur : **usermod**

Dans certaines distribution, il s'agit de programmes différents, dans certaines autres de liens...

Création d'un groupe : **groupadd**

Suppression d'un groupe : **groupdel**

Modification d'un groupe : **groupmod**

On peut bien entendu utiliser des outils graphiques pour ce faire, ou mieux, écrire un script pour automatiser la création d'un liste d'utilisateurs

Fichiers de configuration des comptes utilisateurs :

Les informations concernant les comptes utilisateurs sont dans les fichiers :

/etc/passwd

Le fichier /etc/passwd contient la configuration des comptes utilisateurs.

Exemple :

Login:(utilisation de shadow):uid:gid:nom complet:repertoire perso:shell (lorsque le shell indiqué

est « /sbin/nologin » l'utilisateur n'a pas de shell)

*root:x:0:0:root,CRI Rotonde de l'Arpae,05.46.45.82.14,*www.univ-lr.fr/cri:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
.....
gdm:x:42:42::/var/gdm:/sbin/nologin
polochon:x:500:500:Paul Hauchon:/home/polochon:/bin/bash

/etc/shadow
Le fichier /etc/shadow contient les mots de passes cryptés (à l'aide de la fonction crypt(), voir man crypt) des comptes utilisateurs.

Ainsi que les informations sur la gestion du compte (date du dernier changement de mot de passe, durée de validité du compte, etc). Voir le manuel...

Lorsque des machines sont en libre service, il est utile d'avoir un système d'authentification central pour l'ensemble du parc. On utilise désormais un annuaire LDAP, couplé au module PAM_LDAP...

/etc/skel/

Ce répertoire contient tous les fichiers par défaut à copier dans le répertoire d'un nouvel utilisateur.

Configuration du shell des utilisateurs :

Un certain nombre de fichiers permettent de configurer le comportement du shell de l'utilisateur :

/etc/profile
Contient le paramétrage global de tous les utilisateurs du système. Il est exécuté à chaque login. Il fait la distinction entre root, les uid compris entre 0 et 499 et les autres. Il instancie quelque variables d'environnement comme « USER », « LOGNAME », etc et les exporte. Pour une configuration modulaire et donc plus facile à maintenir, les scripts contenus dans /etc/profile.d sont exécutés.

/home/$USER/.bash_profile
Exécuté à chaque login, modifiable par l'utilisateur

/home/$USER/.bashrc
Exécuté à chaque nouveau bash (et souvent par .bash_profile).

Les quotas :

L'attribution de quotas dans un système de fichiers est un outil qui permet de maîtriser l'utilisation de l'espace disque. Les quotas consistent à fixer une limite d'espace pour un utilisateur ou un groupe d'utilisateurs.

Pour la création de ces quotas, on définit **2 types de limites** :

- **La limite douce** (ou *soft limit* en bon français) : indique la quantité maximale d'espace qu'un utilisateur peut occuper sur le système de fichiers. Si cette limite est atteinte, l'utilisateur reçoit des messages d'avertissement quant au dépassement du quota qui lui a été attribué. Si son utilisation est combinée avec les *délais* (ou *grace period*), lorsque l'utilisateur continue à dépasser la soft limite après que se soit écoulé le délai de grâce, alors il se retrouve dans le même cas que dans l'atteinte d'une limite dure.
- **La limite dure** (ou *hard limit*) définit une limite absolue pour l'utilisation de l'espace. L'utilisateur ne peut pas dépasser cette limite. Passée cette limite, l'écriture sur ce système de fichiers lui est interdite.

De plus ces limites sont exprimées en blocs et en inodes. On a vu que le bloc étant une unité d'espace. Les quotas exprimés en nombre de blocs représentent donc une limite d'espace à ne pas dépasser. En ce qui concerne les quotas exprimés en nombre d'inodes, ils représentent le nombre maximum de fichiers et répertoires que l'utilisateur pourra créer.

Pour mémoire, les *délais* (ou *grace period*) fixent une période de temps avant que la limite douce ne se transforme en limite dure. Elle est fixée dans les unités suivantes : second, minute, hour, day, week.

Généralement dans la plupart des distributions, les quotas sont utilisables d'office. Vous devez vérifier 2 choses pour pouvoir utiliser les quotas :

- vous devez disposer des **outils de gestion des quotas** :
```
root@pingu# rpm -qa|grep quota
quota-3.X-Y
```
- la gestion des quotas doit être activée **dans le noyau** :
```
root@pingu# grep -i quota /boot/config-2.4.XXXX
CONFIG_QUOTA=y
```

Configuration de la gestion des quotas

Configuration de /etc/fstab

Les quotas ont activés au démarrage grâce à la commande `/sbin/quotaon` lancée par le script `/etc/rc.d/rc.sysinit`. Les quotas sont désactivés à l'arrêt du système par la commande `quotaoff`.

Vérifiez

Pour fixer les quotas sur un système de fichiers, il faut mettre à jour le fichier `/etc/fstab`. On va

pour cela ajouter les options de montage pour le ou les systèmes de fichiers concernés. Deux options peuvent être utilisées (et combinées bien sûr) :

- **`usrquota`** : active les quotas utilisateurs
- **`grpquota`** : active les quotas groupes

Exemple :
```
/dev/hdc1      /home    ext3   defaults,usrquota   1 1
/dev/hdc2      /tmp     ext3   defaults,usrquota   1 1
```

Création des structures nécessaires au fonctionnement des quotas

Un ou deux fichiers doivent être créés pour l'utilisation des quotas : `aquota.user` et `aquota.group`. C'est dans ces fichiers que l'on configurera les quotas attribués aux utilisateurs et/ou aux groupes. Ces fichiers doivent être créés à la racine des systèmes de fichiers qui comportent ces quotas.

Exemple :
```
root@pingu# touch /home/aquota.user
root@pingu# touch /tmp/aquota.group
```

Attention :ne pas oublier de **modifier les droits** sur ces fichiers ! Ils doivent comporter les droits en écriture et lecture pour root uniquement.

Exemple :
```
root@pingu# chmod 600 /home/aquota.user
root@pingu# chmod 600 /tmp/aquota.group
```

Remonter le ou les systèmes de fichiers concernés pour prendre en compte l'utilisation de quotas pour ce système de fichiers.
```
root@pingu# mount -o remount /home
root@pingu# mount -o remount /tmp
```

Après création de ces fichiers, il faut initialiser la base des quotas en exécutant la commande suivante :`quotacheck -auvg`. Dans le cas contraire, la sanction est immédiate :
```
edquota: Quota file not found or has wrong format.
No filesystems with quota detected.
```

Activer les quotas :
```
root@pingu# quotaon -a
```

Attribution et vérification des quotas

Fixer des quotas

L'attribution des quotas se fait grâce à la commande `edquota`, utilisable quelque soit le type de quota (utilisateur ou groupe). La commande ouvre un éditeur (vi ou emacs selon le contenu de votre variable EDITOR), qui vous permet de modifier directement les fichiers aquota.user ou aquota.group.

Syntaxe : *`edquota [-u user] [-g group] [-t]`*

- *`-u user`* *définit les quotas pour un ou plusieurs utilisateurs*

- `-g group` *définit les quotas pour un ou plusieurs groupes*
- `-t` *définit les délais*

Exemple :

root@pingu# edquota -u citrouille

Disk quotas for user anne (uid 500):

Filesystem	*blocks*	*soft*	*hard*	*inodes*	*soft*	*hard*
/dev/hdc1	*0*	*9000*	*10000*	*0*	*90000*	*10000*

Le fichier se compose de 6 colonnes :

- `Filesystem` *: système de fichiers concerné par les quotas*
- `blocks` *: nombre de blocs occupés par l'utilisateur dans le système de fichiers. Ici aucun fichier n'a encore été créé.*
- `soft` *: limite soft en nombre de blocs. Ici elle est fixée à 9 000 blocs soit environ 9 Mo*
- `hard` *: limite hard en nombre de blocs (environ 10 Mo)*
- `inodes` *: nombre d'inodes occupées par l'utilisateur dans le système de fichiers*
- `soft` *: limite soft en nombre d'inodes*
- `hard` *: limite hard en nombre d'inodes*

On procédera de la même façon pour l'attribution de quotas à un groupe. (Ne tentez pas d'éditer directement ces fichiers; ils ne sont pas en format texte.)

Fixer un délai

On a vu également qu'on pouvait moduler le délai fixé entre le moment où l'utilisateur atteint la limite soft et celui où on va lui interdire toute occupation supplémentaire dans le système de fichiers. On va donc fixer la durée de ce délai. elle sera la même quelque soit l'utilisateur et/ou le groupe.

***Syntaxe** : edquota -t*

Exemple :

root@pingu# edquota -t

Grace period before enforcing soft limits for users:

Time units may be: days, hours, minutes, or seconds

Filesystem	*Block grace period*	*Inode grace period*
/dev/hdc1	*7days*	*7days*

il suffit donc de remplacer les valeurs par vos valeurs dans l'unité qui vous convient : second, minute, hour, day, week.

Vérification et affichage des quotas

Les commandes suivantes vont vous permettre d'une part de vérifier les quotas affectés à chaque groupe et/ou utilisateur et éventuellement de synchroniser les informations nécessaires au système pour le suivi de ces quotas.

Edition des informations relatives aux quotas

La commande `repquota` permet d'afficher un résumé de l'utilisation des quotas et délais de grâce.

***Syntaxe** : `repquota [ -vug ] -a | filesystem`*

- **`-v`** *: mode verbeux, affiche des infos supplémentaires*
- **`-u`** *: affiche des informations sur les quotas utilisateurs*
- **`-g`** *: affiche des informations sur les quotas groupes*
- **`-a`** *: affiche des informations sur tous les systèmes de fichiers disposant de quotas*
- **`filesystem`** *: affiche des informations sur les quotas du système de fichiers spécifié*

On trouve ici les informations relatives au quota imposé aux utilisateurs. On trouvera autant de lignes que d'utilisateurs, groupes et systèmes de fichiers concernés.

Sont rappelés les quotas fixés en nombre de blocs et d'inodes. On trouve également le nombre de blocs et le nombre d'inodes utilisés. Quand un horodatage apparaît dans la colonne `grace`, comme par exemple pour Bob, cela signifie que l'utilisateur (ou le groupe) a dépassé la limite douce. Le délai de grâce est donc décompté.

Vous pouvez également utiliser la commande **`quota`** suivie du nom d'un utilisateur ou d'un groupe. Là encore vous obtiendrez toutes les informations relatives aux quotas et à l'utilisation de l'espace attribué.

Vérifications et synchronisation des fichiers de quotas

Il peut arriver que les fichiers de quotas deviennent incohérents. La gestion de ceux-ci devient alors impossible. D'autre part, lorsque vous ajoutez un nouvel utilisateur ou un nouveau groupe à l'aide de la commande `edquota`, il faut là encore synchroniser les fichiers pour la prise en compte de ces nouvelles informations.

***Syntaxe** : `quotacheck [ -vug ] -a | filesystem`*

- **`-v`** *: mode verbeux, affiche des infos supplémentaires*
- **`-u`** *: vérifie uniquement les fichiers de quotas utilisateurs*
- **`-g`** *: vérifie uniquement les fichiers de quotas groupes*
- **`-a`** *: vérifie les fichiers de quotas de tous les systèmes de fichiers en disposant*

- ***filesystem*** *: vérifie les fichiers de quotas du système de fichiers spécifié*

Exemple : *vérifier tous les fichiers de quotas, quelque soit le système de fichiers concerné*

```
root@pingu# quotaoff -a
root@pingu# quotacheck -auvg
quotacheck: Scanning /dev/hdc10 [/home/anne/quota] done
quotacheck: Checked 2 directories and 10 files
```

Dans notre cas, sachant que l'on fixe les quotas sur la racine du système de fichiers, il faut ajouter l'option « m » qui force la verification même si le FS reste monté en écriture.

Pour plus d'informations, consulter le man des commandes : `repquota, quotaon, quotaoff, quotacheck, edquota.`

En résumé, il faut créer le fichier de aquota.user ou group, remonter le système de fichiers, éditer les quotas, quotacheck, quotaon.

Exercice :

Créez un utilisateur « toto » et affectez lui un petit quota soft et un plus grand hard, mettez un délai de grace court et testez (utilisez repquota. Pour voir ce qui se passe).

RIP :

Zebra (qui maintenant s'appelle quagga) est un routeur modulaire. Chaque protocole est contrôlé par un démon distinct. Son langage de commande est très proche de celui de Cisco IOS. La syntaxe des commandes suit toujours le même principe :

Vous vous connectez au démon avec telnet, vous tapez le mot de passe.

Il y a plusieurs modes de commandes:

- le mode lecture
- le mode « enable » qui vous donne un peu de pouvoir
- le mode config (atteint depuis enable avec la commande « configure terminal)

etc.

Faites la configuration minimale pour zebra.conf et ripd.conf, à savoir :

hostname <nom>_zebra

password <mot de passe de connexion>

enable password <mot de passe enable>

hostname <nom>_rip

password <mot de passe de connexion>

enable password <mot de passe enable>

Comme ça on voit à qui on parle.

Sur le routeur :

toto_zebra>enable

toto_zebra#configure terminal

toto_zebra(config)#interface eth0

toto_zebra(config if)#ip address 10.2.10.X/24

toto_zebra(config)#interface eth1

toto_zebra(config if)#ip address 192.168.X.254/24

toto_zebra(config if)#end

toto_zebra(config=#exit

toto_rip>enable

toto_rip#configure terminal

toto_rip(config)#router rip

toto_rip(config)#network 10.2.10.0/24

toto_rip(config)#network 192.168.X.0/24// Pas indispensable voire déconseillé

toto_rip(config)#redistribute connected (ou kernel)

toto_rip(config)#exit

A partir de ce moment, vous devez voir des trames RIPV2 dans lesquelles votre routeur redistribue les routes qu'il connaît et les trames des autres routeurs. Au fur et à mesure que vous recevez des trames RIPV2 (response) votre table de routage s'enrichit.

OSPF

La configuration standard de OSPF est sensiblement identique (indiquer la zone dans « network »). Le dialogue se fait avec des paquets HELLO qui indiquent que les routeurs sont vivants. On aurait pu assister à l'élection du routeur maître et de son suppléant (mais ça se passe très vite). Le routeur maître, tant qu'il est vivant redistribue l'ensemble des routes de la zone dès que la carte change ou quand on lui en fait la demande. Les autres routeurs ne sont pas sensés donner d'informations, sauf quand les réseaux qu'ils redistribuent changent. Si vous faites redistribuer vos routes « kernel », étant donné qu'elles changent au fur et à mesure que les routeurs OSPF démarrent, vous assistez à une véritable cacophonie jusqu'à ce que tout converge.

toto_ospf>enable

toto_ospf#configure terminal

toto_ospf#router ospf

toto_ospf#network 10.2.10.0/24 area 0

toto_ospf#exit

Ca doit suffire ! La doc indique de mettre network 0.0.0.0/0 area 0, je n'ai pas essayé...

Les ports utilisés par les démons sont :

zebra : 2601

ripd : 2602

ospfd : 2604

Les protocoles de routage dialoguent en multicast. L'adresse de multicast est spécifique au protocole utilisé.

RIPV2 224.0.0.9

OSPF 224.0.0.5

DHCP

téléchargez le paquetage dhcp_3.0XXX depuis 10.2.10.183/RPM.
Configurez un serveur DHCP sur une de vos machines de telle sorte :

- Qu'il n'attribue d'adresses qu'à vos machines
- Que ces machines obtiennent des adresses conformes au plan d'adressage de la salle
- Qu'elles aient la bonne passerelle par défaut
- Qu'elles cherchent à renouveler leur adresse toutes les 30 secondes
- Qu'il fasse beau en sortant du TP
- Que le domaine soit tpX.org ou X est le numéro de votre table
- Qu'il indique comme DNS 10.2.10.183

```
ddns-update-style none;
subnet 192.168.X.0 netmask 255.255.255.0 {
    # Passerelle par défaut
    option routers                  192.168.X.254;
    option subnet-mask              255.255.255.0;
    option domain-name              "tpX.org";
    option domain-name-servers      10.2.10.183;
      option weather                        sun-shine;

    default-lease-time 60;
    max-lease-time 60;
      host tpMachin {
      option host-name "tpMachin.tpreseaux.fr";
      hardware ethernet 00:08:a1:1c:38:f1;//à adapter
      fixed-address 192.168.X.1;//à adapter
  }
```

```
        host tpTruc {
        option host-name "tptruc.tpreseaux.fr";
        hardware ethernet 00:08:a1:1c:ff:f1;//à adapter
        fixed-address 192.168.X.2;//à adapter
    }
}
```

Testez en configurant l'autre machine cliente DHCP.

Reconfigurez votre serveur DHCP pour qu'il attribue une plage d'adresses

```
ddns-update-style none;
subnet 192.168.X.0 netmask 255.255.255.0 {
        range dynamic-bootp 192.168.X 30 192.168.X.50
        # Passerelle par défaut
        option routers                  192.168.X.254;
        option subnet-mask              255.255.255.0;
        option domain-name              "tpX.org";
        option domain-name-servers      10.2.10.183;
          option weather                        sun-shine;
        default-lease-time 60;
        max-lease-time 60;
}
```