

GNU/Linux LABS : gestion des comptes

Exercice 1 :

- 1- Définir une stratégie de mot de passe qui doit être changer chaque 30 jours pour les utilisateurs nouvellement créés

```
# vim /etc/login.defs
```

```
# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#     PASS_MIN_LEN     Minimum acceptable password length.
#     PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   30
PASS_MIN_DAYS   0
PASS_MIN_LEN     5
PASS_WARN_AGE   7
```

- 2- À l'aide d'un fichier script addaccount.sh Créer 6 utilisateurs (user1 ...user6) avec **mot de passe « Redhat123 ! »**

Et deux groupes : **Sales** avec un GID 40000 & **Marketing** avec un GID 40001

```
File Edit View Search Terminal Help
#!/bin/bash

for ((i=1; i<7; i++))
do
useradd user$i ; echo "Redhat123" | passwd --stdin user$i

done

groupadd -g 40000 Sales
groupadd -g 40001 Marketing
```

- 3- Ajouter l'utilisateur **user1** au groupe supplémentaire Sales et modifier le login de cet utilisateur avec le shell **natif (sh)**

```
[root@ipasrv ~]#
[root@ipasrv ~]#
[root@ipasrv ~]# usermod -G Sales -s /bin/sh user1
[root@ipasrv ~]#
[root@ipasrv ~]# id user1
uid=1004(user1) gid=1004(user1) groups=1004(user1),40000(Sales)
[root@ipasrv ~]#
```

- 4- Ajouter l'utilisateur **user2** au groupe primaire Marketing

```
[root@ipasrv ~]#
[root@ipasrv ~]# usermod -g Marketing user2
[root@ipasrv ~]# id user2
uid=1005(user2) gid=40001(Marketing) groups=40001(Marketing)
```

- 5- Permettre à l'utilisateur **user2** d'avoir un privilège administratif

```
root@ipasrv ~]#
root@ipasrv ~]# usermod -aG wheel user2
```

- 6- Les comptes **user3** et **user4** devront être expirés après les prochains 90 Jours

```
[root@ipasrv ~]#
[root@ipasrv ~]# date -d "+90 days"
Mon Mar 25 12:31:29 WET 2019
[root@ipasrv ~]#
[root@ipasrv ~]# chage -E 2019-03-25 user3
[root@ipasrv ~]# chage -l user3
Last password change           : Dec 25, 2018
Password expires               : never
Password inactive              : never
Account expires                : Mar 25, 2019
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```

- 7- Changer la stratégie de mot de passe de l'utilisateur **user5** qui devrais être changé chaque 15

Jours

```
[root@ipasrv ~]# chage -M 15 user5
[root@ipasrv ~]# chage -l user5
Last password change           : Dec 25, 2018
Password expires                : Jan 09, 2019
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 15
Number of days of warning before password expires : 7
```

- 8- Forcer le compte **user6** a fin de changer son mot de passe au prochain premier login

```
[root@ipasrv ~]# chage -d 0 user6
[root@ipasrv ~]#
[root@ipasrv ~]# chage -l user6
Last password change           : password must be changed
Password expires                : password must be changed
Password inactive              : password must be changed
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
[root@ipasrv ~]#
[root@ipasrv ~]# su - user2
Last login: Tue Dec 25 12:35:27 WET 2018 on pts/0
[user2@ipasrv ~]$
[user2@ipasrv ~]$ su - user6
Password:
You are required to change your password immediately (root enforced)
Changing password for user6.
(current) UNIX password:
```