Module Linux

Equipe Pédagogique

H. SLIMANI
S. BEN YAALA

Gestion des utilisateurs & groupes

2019-2020

+ Plan

- Faire des opérations en tant que root
- Gestion des utilisateurs
- Gestion des groupes
- Gestion des mots de passe utilisateur

Faire des opérations en tant que root Administrateur Linux

- Sous linux, l'administrateur est l'utilisateur root
  - Il dispose de tous les droits et permissions = DANGER
  - Son identifiant, ID 0 est traité de manière différente par le noyau
  - Certains Linux et MacOS X désactivent le compte root, il ne dispose pas de mots de passe. On peut toutefois ouvrir une session en tant qu'utilisateur root

Faire des opérations en tant que root Devenir administrateur

- La commande su (switch user) permet d'ouvrir un shell en tant qu'utilisateur
  - Ouvrir un shell en tant qu'utilisateur henry

    ludo@rhel7 /home/ludo $su henry

    henry@rhel7 /home/ludo $
  - Ouvrir un shell en tant qu'utilisateur henry et charger son profil : ludo@rhel7 /home/ludo $ su - henry

    henry@rhel7 /home/henry $
  - Ouvrir un shell en tant qu'utilisateur root et charger son profil utilisateur : ludo@rhel7 /home/ludo $ su –

    root@rhel7 /root #

Faire des opérations en tant que root Commande sudo

- La commande sudo (substitute user do) permet d'exécuter des commandes en tant qu'administrateur (root)
- L'administrateur peut contrôler le jeu de commandes autorisées aux utilisateurs
- La commande sudo journalise les commandes saisies et leurs arguments
- Sous Red hat Linux, les utilisateurs doivent appartenir au groupe WHEEL pour pouvoir utiliser la commande sudo

```
ludo@rhel7 /home/ludo $ sudo ma_commande

ludo is not in the sudoers file. This incident will be reported.


ludo@rhel7 ~ /$ usermod –G wheel ludo
```

Faire des opérations en tant que root Configuration de sudo

- La configuration de sudo s'effectue dans le fichier /etc/sudoers
- Ce fichier est éditable par le root avec la commande visudo
- On définit des groupes de machines, des groupes de commandes, et des groupes d'utilisateurs, pour ensuite les associer avec les autres.
  - Cmnd_Alias : les commandes dont dispose les utilisateurs du groupe associés
  - User_Alias : les utilisateurs qui peuvent exécuter les commandes de cmnd_allais
  - Hosts_Alias : les hôtes où l'on peut exécuter les commandes

Faire des opérations en tant que root Configuration de sudo

- On crée un groupe NET-GRP que l'on associe aux groupes de commandes NET-CMD
- On autorise NET-GRP à lancer toutes les commandes des groupes NET- CMD

- Ouvrir le fichier /etc/sudoer avec visudo
- root@rhel7 #visudo

  - User_Alias NET-GRP = alfred, brenda, charly
  - Cmnd_Alias NET-CMD = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables, /sbin/iwconfig, /sbin/mii-tool, /usr/sbin/mtr, /sbin/ip
  - NET-GRP ALL = NET-CMD

Gestion des utilisateurs & groupes locaux

- Un utilisateur = un compte
- Un utilisateur est identifié par un UID et un GID
  - UID = User Identifiant
  - GID = Groupe Identifiant
- Les utilisateurs sont stockés dans le fichier /etc/passwd
- Les groupes sont stockés dans le fichier /etc/group
- Les useradd et groupadd permettent de créer des utilisateurs et des groupes

Gestion des utilisateurs & groupes locaux

- Les utilisateurs sont stockés dans le fichier /etc/passwd
  * Affichage du fichier /etc/passwd

```
#cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
ludo:x:1000:1000:ludo le formateur:/home/ludo:/bin/bash
```

- On trouve plusieurs champs séparés par les deux points :
  * Nom utilisateur
  * UID et GID
  * Commentaire
  * Le répertoire personnel
  * Le shell de connexion

Gestion des utilisateurs & groupes locaux

- nombre identifiant
  - unique ???
- 0-99 : outils et fonctions spécifiques système
  - 0 : root
  - ex : 2 (Red Hat) daemon
- 100-500 ou 1000 : fonctions spécifiques liées à la distribution
  - ex : GID 100 : users (groupe par défaut)

Créer des utilisateurs

La commande useradd ou adduser (c'est un lien) crée un utilisateur :

#useradd ludo

Le fichier /etc/default/useradd définit des valeurs par défaut

#cat /etc/default/useradd

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

Créer des utilisateurs

- Modification des options par defaut

  - # useradd -b /home/groups/ -c "administrateur reseau" -g net-admin hamid

-b, --base-dir REP_BASE	répertoire de base pour le répertoire personnel du compte du nouvel utilisateur
-c, --comment COMMENTAIRE	définir le champ « GECOS » du compte du nouvel utilisateur
-g, --gid GROUPE	forcer l'utilisation de GROUPE pour le compte du nouvel utilisateur
-N, --no-user-group	ne pas créer de groupe de même nom que l'utilisateur
-u, --uid UID	forcer l'utilisation de l'identifiant « UID » pour le compte du nouvel utilisateur
-s, --shell INTERPRÉTEUR	interpréteur de commandes initial pour le compte du nouvel utilisateur

Modifier et supprimer des utilisateurs

- Modification d'un utilisateur

```
# usermod -d /home/hamid/ -c "administrateur reseau" -G sys-admin hamid
```

-c, --comment COMMENT	définir une nouvelle valeur pour le champ « GECOS »
-d, --home REP_PERS	définir un nouveau répertoire personnel pour le compte de l'utilisateur
-m, --move-home	déplacer le contenu du répertoire personnel vers le nouvel emplacement (à n'utiliser qu'avec -d)
-g, --gid GROUPE	forcer l'utilisation de GROUPE comme nouveau groupe primaire
-G, --groups GROUPES	définir une nouvelle liste de groupes supplémentaires
-s, --shell INTERPRÉTEUR	nouvel interpréteur de commandes initial pour le compte de l'utilisateur
-L, --lock	bloquer le compte de l'utilisateur

Modifier et supprimer des utilisateurs

- Suppression d'un utilisateur

```
# userdel hamid
```

- Suppression d'un utilisateur et suppression du repertoire personnel

```
# userdel -r hamid
```

Le profil de l'utilisateur

- Lors de la création d'un utilisateur, des options et des paramètres sont utilisés par défaut.
- Le fichier /etc/default/useradd : contient les options de création par défaut
- Le fichier /etc/login.defs : contient des paramètres de création du compte utilisateur
- Le répertoire /etc/skel : modèle de création des répertoires personnels

Les groupes

- Un groupe est identifié par un GID
- GID = Groupe Identifiant
- Les groupes sont stockés dans le fichier /etc/group
- Les commandes groupadd, groupdel, groups permettent de manipuler les groupes

Les groupes

- Les groupes sont stockés dans le fichier /etc/group
  - * Affichage du fichier /etc/group

```
#cat /etc/group
root:x:0:
net-admin:x:1001:ludo
sys-admin:x:1002:hamid
```

- On trouve plusieurs champs séparés par les deux points :
  - * Nom du groupe
  - * GID
  - * Utilisateurs du groupe

Lister les utilisateurs d'un groupe

- La commande groups permet de lister les utilisateurs d'un groupe :

```
# groups ludo
groups ludo
ludo : ludo net-admin
```

Créer et supprimer des groupes

- La commande groupadd crée un groupe :

  #groupadd db-admini

- La commande groupdel supprime un groupe:

  #groupdel db-admini

- Créer un utilisateur student avec le mot de passe tekup

Useradd student

Passwd student

- Changer le shell de cet utilisateur pour qu'il soit /bin/sh

Usermod –s /bin/sh student

- Affecter cet utilisateur à un groupe secondaire tekup

Usermod –aG tekup student

- Donner à cet utilisateur la permission d'utiliser sudo

Usermod –aG wheel student

- En tant que student, créer un fichier fich. Changer le groupe propriétaire de ce fichier pour qui'il soit tekup.

Su student touch fich chgrp tekup fich

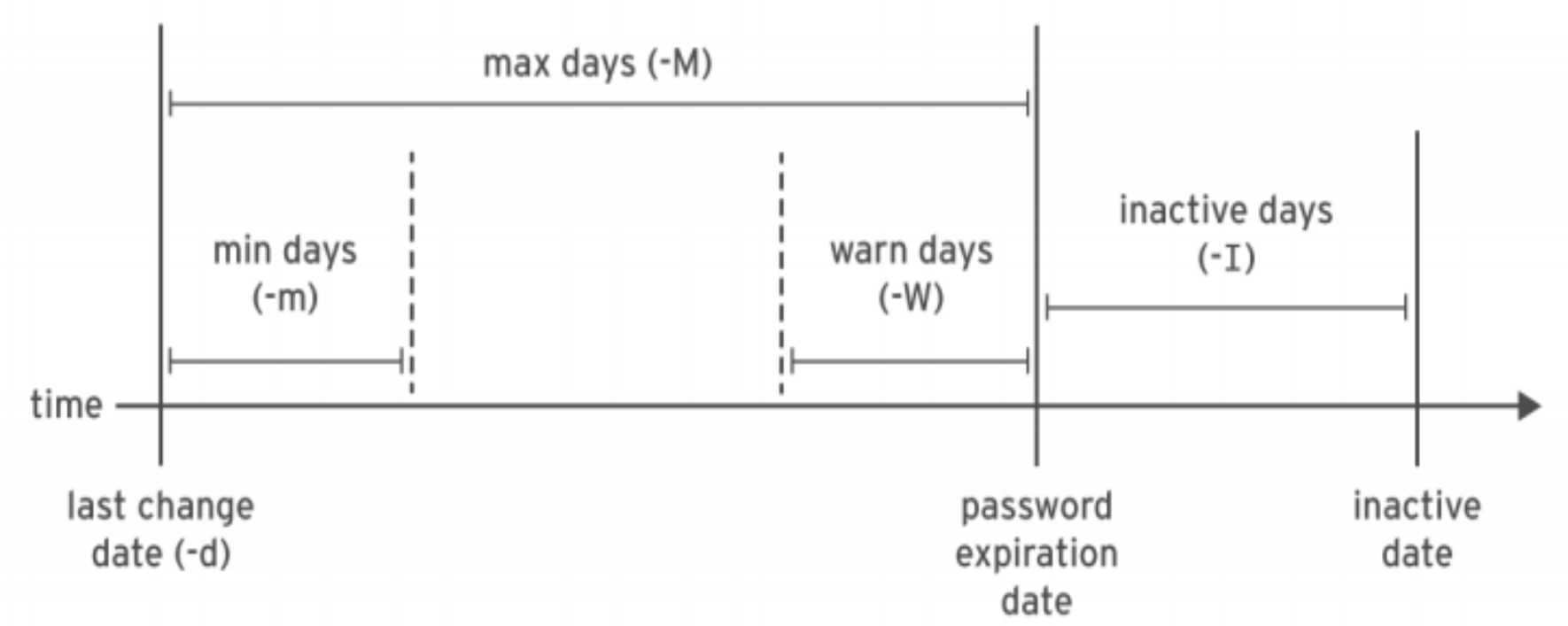
Chown :tekup fich

Gestion des mots de passe: /etc/shadow


```
1user03:2$6$CSsX...output omitted...:317933:40:599999:67:72:818113:9
```

1. Nom d'utilisateur du compte
2. Le mot de passe crypté de l'utilisateur.
3. Date de la dernière modification (en nombre de jours depuis le 1er janvier 1970). (chage –d)
4. Le nombre minimum de jours qui doivent s'écouler depuis le dernier changement de mot de passe avant que l'utilisateur ne peut le modifier à nouveau. (chage –m)
5. Le nombre maximum de jours qui peuvent s'écouler sans modification du mot de passe avant l'expiration du mot de passe. (Chage –M)
6. Nombre de jours durant lesquels l'utilisateur est prévenu de l'expiration de son mot de passe. (chage –W)
7. Période d'inactivité. Une fois le mot de passe expiré, il sera toujours accepté pour la connexion pour plusieurs jours. Une fois cette période écoulée, le compte sera verrouillé. (Chage –I)
8. Le jour où le mot de passe expire. Ceci est défini en nombre de jours depuis le 1970-01-01 . Un champ vide signifie qu'il n'expire pas à une date particulière. (Chage –E)
9. Le dernier champ est généralement vide et est réservé pour une utilisation future.

Gestion des mots de passe



Exemple :

- Créer un utilisateur consultant avec un mot de passe

tekup

- Définissez l'expiration de compte **consultant le 20-08-2021**
- forcez l'utilisateur à changer son mot de passe lors de la première connexion.
- L'utilisateur consultant doit pouvoir changer son mot de passe 10 jours après le jour du changement de mot de passe.
- Le mot de passe de consultant devrait expirer dans 30 jours depuis le dernier jour du changement de mot de passe.

Gestion des mots de passe dans Red hat

- La commande passwd permet de manipuler les mots de passe
- La commande chage permet de changer les paramètres du mot de passe

Modifier le shadow pour un utilisateur

- Modifier le mot de passe

```
# passwd [-k] [-l] [-u [-f]] [-d] [-S] [username]
```

Exemple : $ sudo passwd foulen

- Modifier les paramètres du mot de passe

```
# chage [-m min] [-M max] [-d dernier] [-I inactive] [-E
expire] [-W warning] [-l] utilisateur
```

Exemple : $ sudo chage -E 2019-12-1 foulen

$ sudo chage –m 7 –M 20 –w 7 –E 2019-12-1 foulen

$ sudo chage –I 30 foulen

Sécuriser les mots de passe

- Que trouve-t-on dans /etc/security/pwquality.conf ?

Contenu du fichier **/etc/security/pwquality.conf**

#cat /etc/security/pwquality.conf

difok =3 un minimum de 3 caractères différents dans un nouveau mot de passe
minlen = 8 le mot de passe d'un minimum de 8 caractères
ucredit = -1 Requiert au moins 1 lettre majuscule
lcredit = -1 Requiert au moins 1 lettre minuscule
dcredit = -1 nécessite au moins 1 chiffre
ocredit = -1 au moins 1 caractère non alphanumérique
minclass = 2 au moins 2 classes de caractères, majuscule, minuscule, chiffre et autres ($, &, %, ...)
maxrepeat = 3 rejets du mot de passe, si 4 occurrences identiques, plusieurs caractères répétitifs identiques
maxclassrepeat = 2 rejets du mot de passe, si 3 caractères consécutifs du même type (alphanumériques et autres)

Sécuriser les mots de passe

- case sensitive
- éviter les espaces
- doit commencer par une lettre
- maximum 32 caractères
  - privilégier un maximum de 8