Chapitre 4

Prérequis

Pour compléter certaines parties de ce chapitre, il faut savoir :

- ☒ Créer des répertoires et des fichiers, connaître la ligne de commande (chapitre Découverte de la ligne de commande).
- ☒ Installer un nouveau paquet, ou logiciel (chapitre Gestion des systèmes).
- ☒ Avoir configuré les machines au niveau du réseau (chapitre Réseau : configuration et sécurité).
- ☒ Savoir accéder à un partage NFS (chapitre Systèmes de fichiers).

Objectifs

La gestion des utilisateurs est un élément clé de l'administration d'un serveur Red Hat Enterprise Linux.

En effet, sous Linux, tout est fichier. Des fichiers réels à l'état du processeur et de la mémoire, en passant par les périphériques, tout est représenté d'une manière ou d'une autre sous la forme de fichiers. Ainsi, gérer qui a accès à ces fichiers, et comment, est une tâche essentielle qu'il faut comprendre et maîtriser.

Dans ce chapitre, vous apprendrez à gérer des utilisateurs et des groupes. Les bases de données utilisateurs peuvent être soit locales, c'est-à-dire stockées sur le système, soit partagées, c'est-à-dire stockées sur un serveur central dans un annuaire LDAP (*Lightweight Directory Access Protocol*).

Vous apprendrez également à définir des droits d'accès aux fichiers, en explorant les droits standards UNIX, les droits étendus avec les ACL (*Access Control List*), et le contrôle fin avec SELinux qui sera ici démystifié.

Les objectifs couverts sont les suivants :

- ☒ Créer, supprimer et modifier des comptes utilisateur locaux.
- ☒ Modifier les mots de passe et ajuster la durée de validité des mots de passe pour les comptes utilisateur locaux.
- ☒ Créer, supprimer et modifier des groupes locaux et des appartenances de groupe.
- ☒ Configurer un système pour utiliser un service d'authentification existant pour les informations utilisateur et groupe.
- ☒ Répertorier, définir et modifier des autorisations `ugo/rwx` standards.
- ☒ Détecter et résoudre les problèmes d'autorisation sur les fichiers.
- ☒ Créer et configurer des répertoires SetGID pour la collaboration.
- ☒ Créer et gérer des listes de contrôle d'accès.
- ☒ Définir des modes d'application de règles et permissifs pour SELinux.
- ☒ Répertorier et identifier le contexte des fichiers et des processus SELinux.
- ☒ Restaurer les contextes des fichiers par défaut.
- ☒ Utiliser des paramètres booléens pour modifier les paramètres SELinux du système.
- ☒ Détecter et gérer les violations des politiques SELinux de routine.

Préparation

Pour ce chapitre, la majorité des manipulations se font sur votre serveur principal.

Cependant, la section Authentification centralisée utilise un serveur LDAP avec un éventuel partage NFS, dont la configuration est expliquée dans l'Annexe.

A. Utilisateurs et groupes

1. Principes généraux

Utilisateurs, groupes et rôles

Les utilisateurs peuvent être des personnes réelles ou des applications. Les personnes réelles se connectent à la machine, manipulent des fichiers, lancent des programmes.

Les services sont des programmes exécutant des tâches sur la machine, par exemple un travail consistant à répondre à des requêtes, ou des tâches de maintenance.

Autant les utilisateurs réels que les services manipulent des fichiers, et possèdent donc un compte sur la machine.

Les groupes sont des ensembles d'utilisateurs, réels ou applicatifs, regroupés dans un but commun.

Bien sûr, comme les machines travaillent avec des chiffres, les comptes utilisateurs et groupes se voient attribuer des numéros :

- **UID** (*User Identifier*), ou userid (identifiant d'utilisateur) : le numéro de compte d'un utilisateur.
- **GID** (*Group Identifier*), ou groupid (identifiant de groupe) : le numéro de compte d'un groupe.

Différents rôles

Sur les systèmes d'exploitation UNIX/Linux, en général, il faut distinguer un utilisateur spécial : **l'administrateur de la machine**, qui possède un compte appelé `root` avec un userid 0 (zéro).

L'utilisateur root **a tout pouvoir** sur la machine. C'est lui l'administrateur, il peut donc lire, modifier, ou supprimer n'importe quel fichier. Il peut éteindre et redémarrer la machine. Mais son travail principal consistera à effectuer des **tâches d'administration**, diverses et variées, en fait à peu près tout ce qui est décrit dans ce livre.

Bien sûr, l'administrateur de la machine est une personne réelle, qui possède son propre compte, mais qui devra devenir utilisateur root le temps d'effectuer des tâches d'administration sur le système.

Les **autres utilisateurs**, quant à eux, ont des **pouvoirs qui se limitent** aux fichiers qu'ils possèdent. La plupart du temps, ces fichiers sont stockés dans leur répertoire utilisateur. Cela signifie qu'un utilisateur mal intentionné ne pourra faire que très peu de dégâts sur le serveur Red Hat Enterprise Linux.

De même, les **services** possèdent des **comptes système**, similaires aux comptes utilisateurs en ce qu'ils sont limités dans l'étendue des fichiers qu'ils peuvent atteindre sur le système. Ainsi, **si un service est corrompu par un pirate, l'impact est réduit**.

Il est judicieux que toutes les personnes réelles et les applications aient un compte utilisateur pour faire leur travail. **Le compte root ne devra être utilisé que rarement**.

Fichiers et permissions

Chaque fichier sur la machine est la **propriété d'un utilisateur**, qui dispose d'un accès à ce fichier en lecture, en écriture, en exécution. Il s'agit de l'utilisateur propriétaire de ce fichier.

Un fichier a également **un groupe propriétaire**, qui dispose lui aussi d'un accès en lecture, en écriture, en exécution. Tous les utilisateurs de ce groupe ont les mêmes droits d'accès à ce fichier.

Ainsi, un fichier possède des droits d'accès pour :

- Son utilisateur propriétaire, en lecture, écriture, exécution.
- Son groupe propriétaire, en lecture, écriture, exécution.
- Tous les *autres* utilisateurs, en lecture, écriture, exécution.

Bien sûr, tous les droits ne sont pas « activés » de la même manière pour ces trois catégories. L'utilisateur propriétaire peut, par exemple, avoir le droit de lire et d'écrire dans le fichier, le groupe seulement le droit de lire le fichier, et les autres utilisateurs n'auront aucun droit.

Les répertoires possèdent le même type de droits.

☞*Nous définissons dans la suite de ce chapitre quelles sont les implications de ces droits, ou permissions, sur les fichiers et répertoires.*

2. Créer, supprimer et modifier des comptes utilisateur locaux

a. Créer un compte utilisateur local

Pour ajouter un utilisateur sur la machine, utilisez la commande :

```
useradd <nom d'utilisateur>
```

Le compte de l'utilisateur est « verrouillé » : l'utilisateur n'a pas de mot de passe, il ne peut donc pas s'authentifier.

Créez un mot de passe temporaire :

```
passwd <nom d'utilisateur>
```

Définissez alors son mot de passe temporaire. Une fois authentifié avec ce mot de passe, l'utilisateur devra le changer avec la même commande, sans préciser de nom d'utilisateur.

Il est également possible de créer un compte sans mot de passe, que l'utilisateur devra **définir à la première connexion**. Voir plus loin la section Ajuster la durée de validité des mots de passe pour les comptes utilisateur locaux.

Par exemple, nous créons ici un compte pour Robert Smith avec un mot de passe temporaire pour la première connexion de l'utilisateur.

```
[root@cobb ~]# useradd rsmith
[root@cobb ~]# passwd rsmith
Changement de mot de passe pour l'utilisateur rsmith.

Nouveau mot de passe :
MOT DE PASSE INCORRECT : basé sur un mot du dictionnaire
MOT DE PASSE INCORRECT : est trop simple
Retapez le nouveau mot de passe :
```

```
passwd : mise à jour réussie de tous les jetons d'authentification.
```

☞*Notez ici qu'il y a une vérification sur la « qualité » du mot de passe défini. Pour un utilisateur quelconque, le système refuse tout simplement de créer le mot de passe s'il est de faible niveau de sécurité. Cependant, root ayant tous les droits,* ***le mot de passe « faible » est quand même pris en compte****, après avoir été confirmé.*

L'utilisateur `rsmith` se connecte maintenant sur la machine. Il définit son nouveau mot de passe. Notez les différents refus du système pour des mots de passe peu sécurisés. La définition du mot de passe ne réussit qu'après trois tentatives :

```
ssh rsmith@cobb
rsmith@cobb's password:
[rsmith@cobb ~]$ passwd
Changement de mot de passe pour l'utilisateur rsmith.
Changement du mot de passe pour rsmith.
Mot de passe UNIX (actuel) :

Nouveau mot de passe :
MOT DE PASSE INCORRECT : trop court

Nouveau mot de passe :
MOT DE PASSE INCORRECT : basé sur votre nom d'utilisateur

Nouveau mot de passe :
Retapez le nouveau mot de passe :

passwd : mise à jour réussie de tous les jetons d'authentification.
[rsmith@cobb ~]$
```

b. Modifier un compte utilisateur local

Il est possible de modifier un compte utilisateur, même après sa création, avec la commande `usermod` :

```
usermod <options> <utilisateur>
```

Vous trouverez un détail des options les plus utiles dans le tableau ci-dessous.

Ajout et modification : Options avancées

À la création avec la commande `useradd`, il est possible de changer certains paramètres du compte utilisateur.

Il est également possible de changer certains paramètres une fois le compte créé, avec la commande `usermod`.

Options intéressantes de useradd/usermod	
Options communes	**Description**
`-c '<informations>'`	Définissez des informations sur l'utilisateur. Vous pouvez mettre n'importe quelle chaîne de caractères, entre simples quotes. Il est recommandé de mettre au moins le nom complet de l'utilisateur, mais vous pouvez par exemple ajouter son rôle dans l'organisation.
`-d <répertoire_utilisateur>`	Vous pouvez définir un répertoire différent du répertoire standard dans `/home`.
`-e <date>`	Date d'expiration du compte, au format `AAAA-MM-JJ`. Très utile pour des comptes temporaires.
`-s <chemin_du_shell>`	Précise un shell différent du shell standard. Par défaut, c'est Bash qui est utilisé, mais l'utilisateur peut désirer une autre version du shell.
`-r`	Création d'un **compte système**, qui n'a pas de shell, de répertoire utilisateur et dont le UID est inférieur à 500.
`-u <UID> / -g <GID>`	Choix des UID / GID de l'utilisateur.

☞*Il est possible de changer les options par défaut utilisées à la création d'un utilisateur, dans `/etc/default/useradd`. De plus, le répertoire de l'utilisateur est créé par le système en copiant les fichiers `/etc/skel` vers `/home`, dans un répertoire portant le **login**, ou nom de l'utilisateur sur la machine.*

Options intéressantes spécifiques à usermod	
Options	**Description**
`-a -G <groupes>`	Ajoute l'utilisateur à un ou plusieurs groupes supplémentaires (séparés par des virgules).
`-L`	Verrouille (*lock*) le compte de l'utilisateur, si bien qu'il ne peut plus se connecter.
`-U`	Déverrouille (*unlock*) le compte utilisateur.
`-m -d <nouveau_répertoire_utilisateur>`	Change le répertoire utilisateur vers un nouvel endroit.

c. Supprimer un compte utilisateur local

Pour supprimer un utilisateur du système, il suffit de taper :

```
userdel <utilisateur>
```